



Soho360

User Guide

Table of Contents

About this document.....	7
Related Documentation.....	7
ThoughtData Soho360 - for the Soho Network.....	8
Stable internet for Soho businesses.....	8
Soho360 v/s typical challenges.....	9
Unstable Internet Connection.....	9
Bandwidth usage and cost optimization.....	9
Slow performance of applications over internet.....	10
Problems in VPN connectivity to networks.....	10
Monitoring Children's Internet Activity.....	11
Cyber Threat Monitoring.....	11
Deployment Options.....	11
ThoughtData Solution Components	12
The Soho360 Application.....	12
NetSense (packet sensor).....	12
Getting started with Soho360.....	13
Data capture and analysis with Soho360.....	13
Initial Log in.....	13
Soho360 Users.....	15
Soho360 default display.....	15
Landing page.....	16
Soho360 – Important Dashboards.....	18
Real Time Internet Monitoring Dashboard.....	18
Graphs in this dashboard.....	18
ClientIP.....	23
ServerIP.....	24
Response Time.....	24
Traffic-Monitor.....	25
Top Traffic Entities.....	26
Top N links Over-time graphs.....	26
Top Traffic Volume Graphs.....	26
Top 10 Servers, Clients and Vlans.....	26
Top N Links Statistics table.....	27
Application-Monitor.....	28
The Top Graphs and Alerts.....	29

Alerts.....	29
The Over-time Graphs.....	29
The Conversations table.....	30
Host-Monitor	31
Hosts entities and Events Graphs	32
Client - Top Apps by Connections, Failures and Avg RT - table	32
Server - Top Apps by Connections, Failures and Avg RT - table	33
Top app Conversations	33
Client - Top 20 Servers metrics - graphs	34
Server- Top 20 Clients metrics - graphs	34
Secure web Map Monitor.....	35
Options in the secure web map dashboard	36
Client Connections in the selected conversation	37
Server Connections in the selected conversation	38
SSL-Monitor.....	41
SSL Events and Entities	43
Alerts.....	43
SSL Client-Server, EURT Over-time graphs	43
SSL Client/Server and Sessions graphs.....	43
Top SSL Tables.....	43
SSL Errors, and Version Distribution	44
SSL Over-time graphs.....	44
Top 50 SSL Conversations	44
SSL connections by TCP/UDP	45
Web-Monitor	46
HTTP entities and Events - graphs	47
HTTP Over time graphs -1	47
HTTP Traffic and TCP States for HTTP Sessions	47
Top HTTP Entities.....	48
HTTP Over time graphs -2	48
Top HTTP Conversations with Errors - table	48
Top 10 HTTP Host Names with URLs - table	49
Top 10 HTTP Referrers - table.....	49
MIME Distribution over time - graph.....	49
HTTP host names and version distribution graphs	49
Top 50 HTTP Conversations by worst response time	49
End User Experience & Connection Statistics - table.....	50
Cyber-Threat-Monitor	52
What are Cyber Threats.....	55
Top Sites, Total Cyber threats and Events.....	56
Top Hosts involved, Top Threat types and Over-time graphs.....	57
Top 10 graph panels.....	59
Top Threats by Threat Count Table	59
STIX Bad Reputation Threats Table.....	60
Top Network Anomalies Table	60
STIX-TAXII Dashboard	61

SSL Session Analysis Monitor	62
Connections Over-time	62
SSL Session Summary	63
Session Analysis	63
Soho360 User Interface - options and features	64
Left Menu pane	65
Preferences	66
Preferences > Edit Profile	66
Preferences > UI Theme, Home Dashboard, TimeZone	66
Change Password	67
Filter Options	68
Top menu options	69
Graphs	70
Zoom-in to Trending and Over-time Graphs	71
Dashboard Settings	72
Apply time range	72
Extended data display	72
Panel Menu	72
Edit Panel	75
Miscellaneous Workflows.....	77
Certificate-Monitor	78
The Top Graphs and Alerts	79
Alerts	79
The Graph Panels 1 to 3	80
The Top 50 certificates table	81
DCE-Monitor	82
DCE Events	83
DCE Over-time graphs	83
DCE Traffic and operations graphs	83
The Top DCE Servers	84
The Top DCE Clients	84
TCP Connections states and DCE Named Pipes	84
Top DCE Conversations with Errors /Worst Latency table	84
DHCP-Monitor	85
Top DHCP	86
DHCP Over time graphs	86
Top DHCP Attributes	86
Top DHCP Conversations table	87
DNS-Monitor	88
DNS Entities and Events	90
DNS Client Vs Server Traffic	90
DNS Over-time graphs	90
The Top DNS Entities	90
Top DNS Conversations with Failures table	91
Top DNS Conversations by Traffic Volume	91

Top DNS Conversations with worst response time table	91
DNS connections graph.....	91
DNS-Response-Monitor	92
DNS Responses over time	93
Top DNS Entities/events	93
DNS Over-time graphs	93
DNS Response Record Types Graph.....	93
FTP-Monitor	94
FTP Entities and Events	95
FTP Over time graphs.....	95
FTP Entities and event graphs.....	95
The Top FTP Conversations with Errors/Worst Latency table	96
ICMP-Monitor.....	97
ICMP Entities and Events	98
ICMP Over time graphs.....	98
ICMP Client Vs Server Traffic graph	98
Top ICMP graphs.....	98
Top ICMP Conversations table.....	99
Inventory-Monitor.....	100
Kerberos-Monitor.....	101
Kerberos Events	102
Kerberos Over time, traffic and connections graphs.....	102
Top Kerberos graphs	103
Top Kerberos Conversations table.....	103
Kerberos connections - graph	104
License Monitor.....	105
Soho360 License Details table	105
Alert	106
Product Usage.....	106
NTLM-Monitor.....	107
NTLM Events	108
NTLM Failed Connections and Errors.....	108
The Top NTLM Entities and Events	108
Top NTLM Conversations table.....	108
RDP-Monitor	110
RDP Events and Entities	111
RDP over-time graphs	111
RDP Traffic and Connections graphs.....	111
Top RDP Servers, Clients graphs	112
Top RDP Conversations table.....	112
Sensor-Health-Monitor	113
Packet Sensor Health Stats	114
Packet Sensor Graphs	115
Log Sensor Health Stats	115
Log Sensor Graphs	115
SIP-Monitor	116

SIP Entities and Events	118
SIP Alerts	118
SIP Failures Over-time Graphs	118
Call Volume and Latency Graphs	118
SIP Registration Graphs.....	118
SIP Callers, SIP Client-Server traffic.....	118
Top SIP Callee, and Caller.....	119
Top SIP Caller and Media Protocol.....	119
Top Callee Domain and Top Caller Domain	119
Top SIP Media Type by #Calls and SIP Connections by TCP/UDP	119
Top SIP Failed Calls.....	119
Top SIP Failed Registrations	120
SMB-Monitor	121
SMB Entities and Events	122
SMB Over time	122
SMB Traffic and Latency over-time.....	122
SMB Errors and Read/Write Traffic	122
Top SMB Server Traffic and Client Errors	123
Top SMB Version and Client Traffic	123
SMB Anonymous User and Connections	123
Top SMB commands, Guest User Usage.....	123
SMB Map Path, TCP Connection states	123
Top SMB Conversations	123
SMB Inner VLANs, Share Type	124
SMB-File-Monitor.....	125
SMB Read, Write, Traffic.....	125
SMB File Paths table	125
SMB-Map-Monitor	126
SMB Read, Write, Traffic.....	126
SMB Map Conversations table.....	126
Email-Monitor.....	128
SMTP Events and Entities.....	129
SMTP Ove-time Graphs.....	129
SMTP Traffic, TCP Connection State	129
Top SMTP graphs	130
SMTP Connections, Sender Host names.....	130
Top SMTP Conversations	130
Top SMTP Sender User Agents Over-time	130
SQL-Monitor.....	131
SQL Events.....	132
SQL Over-time Graphs	133
SQL Client-server traffic, SQL Connections.....	133
Top SQL Graphs.....	133
SQL Version, Statistics, Users, TCP Connection	133
SQL Top Users, TCP Connection.....	133
Top SQL Conversations	134
SSH-Monitor.....	135
Default Panels.....	136

SSH Events and Entities.....	136
SSH Over-time Graphs	136
SSH Client-Server Traffic, TCP State.....	136
Top 10 SSH Servers - Errors table	137
Top 10 SSH Clients - Errors table	137
Top 10 SSH Graphs.....	137
SSH Over-time Graphs	137
SSH version distribution and Top SSH users over time.....	137
Top 50 SSH Conversations	138
Statistics-Dashboard	139
Left Panel graphs	139
Right Panel Table	140
TCP-Monitor.....	141
TCP Events - graphs.....	143
Alerts.....	143
TCP Over-time graphs	144
The Top TCP Servers/clients – snapshot views	145
Top Conversations table	146
Top TCP Anomalies by #Anomalies.....	146
Unknown Monitor	147
Top 10	148
Unknown apps over time graphs.....	148
Top 10 Clients and Servers.....	148
Top 20 Unknown Apps Conversations Table	149
Appendix A: Soho360 Administration – For advanced users	150
Copyright	191
About ThoughtData Inc.....	192

About this document

This guide is meant to help *ThoughtData Soho360* users to get familiar with ThoughtData's Soho360 app, and the features in its user interface, for monitoring their home or small-business internet, regularly on a day-to-day basis.

Note: *The scope of this document does not include description of the deployment scenarios and setting up of the application. Soho360. Refer to the ThoughtData Soho360 Getting Started Guide for related details.*

Related Documentation

For details about the ThoughtData Soho360 solution refer to the documentation described in the table below.

Information type	Document name
Setup, quick start	ThoughtData Soho360 Getting Started Guide
Troubleshooting	ThoughtData Soho360 Troubleshooting Guide

Table 1. Reference Documentation

ThoughtData Soho360 - for the Soho Network

We live in a connected world today even when it comes to network intensive activities - for home and small-businesses. With internet becoming one of the most critical requirements in our daily lives, any down-time or poor performance severely impact access to critical information, productivity and profitability.

As the "work from home" lifestyle continues to grow a high performing internet connection becomes an essential requirement. It goes without saying that productivity in home/small-business depends on a reliable and high-speed internet connection.

When smart media and entertainment gadgets become part of such small networks, the same internet connection has to afford users seamless entertainment and value for money.

If applications in your phone, computer, or media devices perform poorly even when your internet connection is up and running, you may have no means to identify whether the performance issue is because of

- your smart device,
- the internet link,
- the application service in use.

In most cases users live with the problem or call their internet service provider (ISP) just to hear that the ISP side of the network is fine and problem free. The ISP may even persuade users to upgrade their internet connection to a higher bandwidth to resolve the complaint. With very little idea of their current internet bandwidth usage such users may even be forced to pay for upgrades or more expensive internet services.

Thus there is clearly a big case for monitoring and maintaining a high internet uptime for the Small-office and Home-office (Soho) network. ThoughtData Soho360 is a timely answer to the challenges faced by this user community.

Stable internet for Soho businesses

Commonly reported situations that small offices and home offices, (Soho in short) face include the following:

- unstable internet connection
- unplanned bandwidth usage and inability to optimize connectivity costs
- slow performance of applications over internet
- problems in VPN connectivity to networks
- monitoring children's internet activity
- cyber threat monitoring

ThoughtData's Soho360 provides the much-needed real time visibility into internet usage, bandwidth consumption and all the application traffic flowing on your internet connection. It can locate application failures and poor performance to help you troubleshoot point of performance bottlenecks. This in turn enables you to take appropriate action for correcting problems.

Soho360 v/s typical challenges

Soho360 can help small-business and home users overcome challenges related to unstable internet connectivity. Users can:

- see and track problem-events related to internet connectivity and applications performance, and troubleshoot them.
- make informed decisions about increasing their bandwidth speed and improving their connectivity experience.
- manage their internet connection costs with their internet service provider (ISP).

Unstable Internet Connection

Unstable internet connectivity is a frequently occurring issue in small-business and home networks. Adding to that problem is the time taken for resolution by the internet service provider (ISP). Such instances can ruin productivity.

With Soho360 in small-business and home networks, users can:

- troubleshoot the real-time performance of their internet connection,
- understand down-time, link errors and network latency connecting to ISP networks.
- talk to the ISP with evidence of the problem when internet connectivity is down or is unstable, to correct the issue from their side of the network.

Bandwidth usage and cost optimization

In most cases users subscribe to internet connection speeds with no prior idea of their actual needs. Internet speed(s) offered by service providers

- is only for last mile to the home or small-business,
- does not represent the actual internet experience.

As more smart devices that constantly communicate with the internet get added to home or small-business networks users are never sure whether they are

- under using or over using the internet bandwidth,
- getting the actual internet speed they subscribed for.

With Soho360 in your small-business or home network you can:

- get visibility into current and historical internet bandwidth usage,
- monitor visually the actual performance of your link,
- make the decision to increase or decrease your internet speed or bandwidth to manage your subscription costs.

Slow performance of applications over internet

Slow performance of apps on phone, computers and TVs is a constant day to day problem. When applications perform slowly, it is difficult to nail the source of problem. Users give up easily stating that the issue is with the network, whereas the problem could be in

- their own devices,
- the service provider network or
- application servers in the internet.

Should they call the ISP or application service provider or in case of VPN, their office's IT team, or fix the problem on their devices?

With a shaky internet connection, productivity is already disrupted and if it has to do with streaming media or app subscriptions it can lead to a waste of money. For the right action to fix the problem, users need real time visibility into:

- each app connection,
- the performance of every device in the network,
- the actual location in the network experiencing latency.

With Soho360 in your small-business or home network you can get real time understanding about applications such as:

- general internet browsing
- social networking apps such as Facebook, Instagram, Twitter
- streaming media such as Netflix, Amazon video, Hulu, Disney, CBS, Xfinity etc.
- web conferencing apps such as Zoom, Teams, WebEx, GoToMeeting, Blue Jeans etc.
- email apps
- online games
- VoIP and Chat apps such as WhatsApp, skype, telegram
- SaaS apps for small-business and office productivity

You can troubleshoot each application connection failure and poor performance issue to understand the root cause to talk to the right persons and correct the issue.

Problems in VPN connectivity to networks

Productivity in work-from-home situations relies highly on secure VPN connectivity to employers' networks from home internet connections. Failures and slow VPN connections can hamper productivity and slow down the ability to meet deadlines.

With Soho360 in your small-business or home network you can

- troubleshoot VPN connection failures,
- reduce instances of poor network performance,
- improve your work from home experience.

Monitoring Children's Internet Activity

Monitoring internet usage by children and youngsters is a major concern for modern day parents.

With Soho360 in small-business or home network you can:

- keep a tab on all the internet activity of your children.
- get visibility into
 - web sites visited, apps usage, time spent on social networking apps.
 - performance problems associated with apps for online classes.

Cyber Threat Monitoring

Ransomware, Malware and Phishing scams are always on the rise. Sensitive data stored in your computers and devices are under constant threat from cyber-attacks from your internet connection. Don't let your identity and sensitive information in your devices stolen by hackers.

With Soho360 in your small-business or home network you can:

- detect cyber threats on your home and small-business devices,
- understand nature of cyber threats and their source.
- use information from Soho360 to block traffic from unwanted sources in your small-business or home internet gateway firewalls.

Deployment Options

ThoughtData Inc. offers the following 2 deployment options

- ThoughtData - Soho360 - Small-Business
- ThoughtData - Soho360 - Home

Table 2 illustrates the differences between these options.

	<i>Soho360 – Small-Business</i>	<i>Soho360 - Home</i>
<i>Target Usage</i>	To handle small-business internet traffic.	To handle home internet traffic.
<i>Monitoring Capability/ Performance</i>	Single Port 1Gbps Ethernet with 100 - 150k packets per second.	Single Port 1Gbps Ethernet with 50k packets per second.
<i>Data Retention and Storage</i>	Supports SSD based storage - up to 3 month's aggregated data storage plus packet store.	Supports SD card-based storage - up to 1 month's aggregated data storage.
<i>Packet recording/ evidence</i>	Supported.	Not supported.

Table 2. Soho360-Home and Soho360-Small-Business

ThoughtData Solution Components

ThoughtData's integrated solution comprises the following components, pre-installed and configured in your Soho360:

- Soho360 application - small office and home network monitoring solution
- NetSense - packet sensor application

When deployed, the Soho360 platform:

- collects and correlates relevant data
- derives meaningful information and
- organizes related information in different troubleshooting workflows for early triage and prioritization.

The Soho360 Application

This is the software component of the Soho360 small-business and home platform. Instant visibility of problems and investigation using its workflows ensure that:

- there is no loss of work or business opportunity,
- the network experience is optimal,
- performance of your network and applications improves,
- threats are checked in time and the network is re-secured.

NetSense (packet sensor)

ThoughtData NetSense (packet sensor) is a software component of the *Soho360 – Small-Business* and *Soho360 - Home* package. It works in the background to feed continuous data to Soho360. The lossless data capture and analysis by this component helps solve use-cases related to problems in the following key aspects of your small-business or home network:

- performance of your network, applications and smart devices
- cyber threats

Getting started with Soho360

Complete the following steps before you can get started with Soho360.

- Unbox Soho360 – Small-Business or Soho360 – Home, based on what you have purchased.
- Make the connections
- Complete the configuration

Note: For the procedures and steps in getting started with Soho360 (both deployments) refer to the ThoughtData Soho360 Getting Started guide.

Data capture and analysis with Soho360

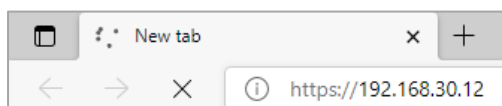
To roll out data *capture* and *analysis* with Soho360, complete the steps described in this section in the prescribed order.

Note: Unboxing the package, making network connections and starting up services are expected to be complete at this point. For details refer to the ThoughtData Soho360 Getting Started Guide.

Initial Log in

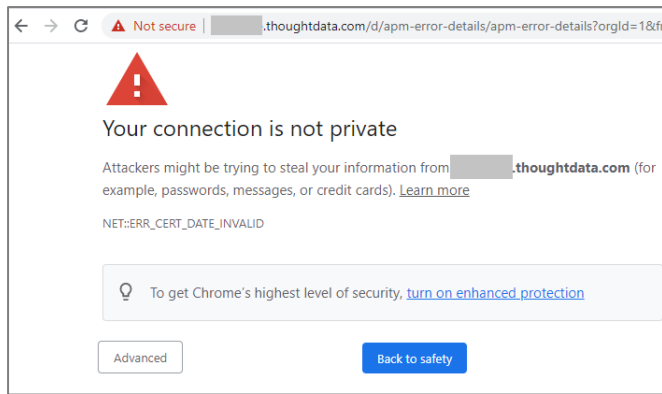
Perform the following steps to get started.

Step 1. Launch the browser (any browser of your choice) from any smart device (phone, tablet or computer) connected to your WiFi network and type the WiFi IP address of your Soho360 device in the address bar. For example: `https:// 192.168.1.112`



Note: The IP address(es) provided as examples are for guidance only. Do not use them in these steps that you perform for getting started. Keep your small-business or home WiFi address ready for reference and use that while you complete the steps.

Step 2. If the browser displays the self-signed certificate warning, click Advanced .



Step 3. In the next tab click [Proceed to \[redacted\].thoughtdata.com \(unsafe\)](#)

Note: The warning messages in the steps above may appear differently in different browsers or their versions. Take the browser-appropriate action to bypass the certificate error.

The Soho360 login page appears as illustrated below.

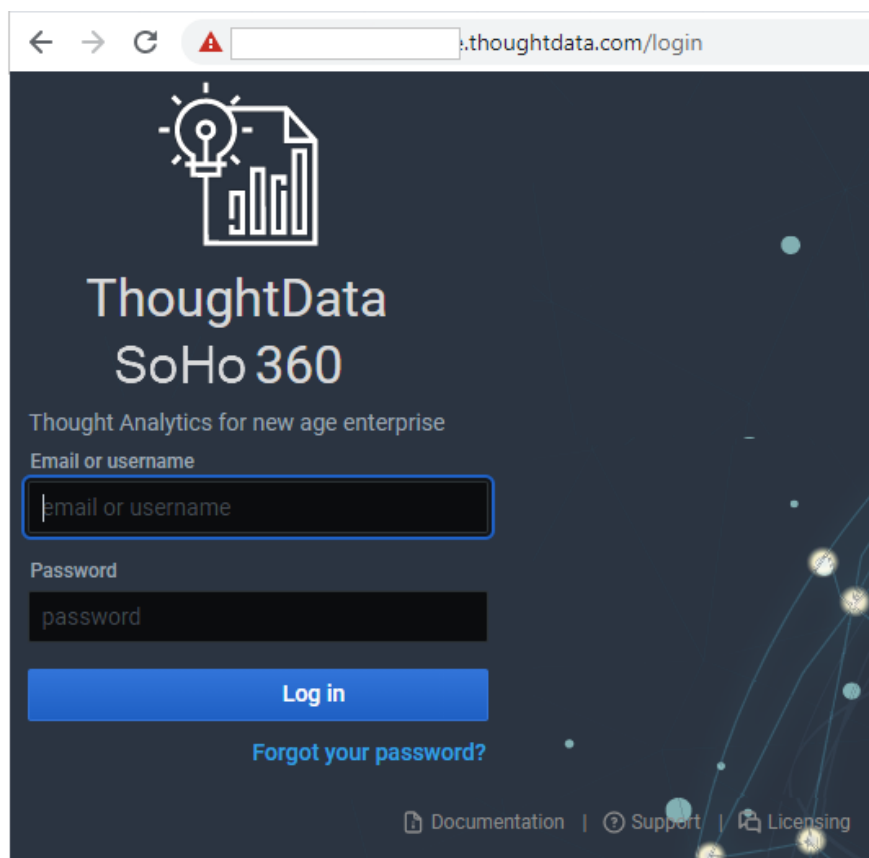


Figure 1. Login page

Step 4. In the login page enter the default username and password credentials as indicated below:

Username - **soho360**

Password - **password**

Step 5. Click **Log in**

Note: You need to make your account secure by changing the default to a strong and secure password that only you are aware of. The username can be retained, but the password has to be changed at the earliest. To do so, refer to "[Change Password](#)".

Soho360 Users

All users logging in using the above default credentials are categorised as "Viewers". As a viewer-user you have access to the menus and options of the Soho360 application's graphic user interface (GUI) for monitoring your network in real-time.

Soho360 default display

In all dashboards the visible area of the screen is divided into multiple panels displaying graphs and data related to the context of the dashboard.

In all these panels the following standard utilities are available:

- Filters in the menu bar above the graphs/tables to change the content that is displayed.
- Panel Menu drop-down options for drill-down information.

Note: Soho360 includes the user type "admin" (administrator). This user has access to options that can alter the default settings in Soho360. See Appendix A: *Soho360 Administration – For advanced users*.

Landing page

After a successful login, the Soho360 landing page is displayed as illustrated below. This is the **Real Time Internet Monitoring dashboard**. It is the default dashboard for your Soho360 - Small-Business or Soho360 - Home network.



Figure 2. Landing page – the Real-time Internet Monitoring dashboard

Of all the Soho360 multiple troubleshooting workflows, the **Real Time Internet Monitoring** dashboard is the most important.

It includes the most relevant workflows for small-business and home networks and therefore the starting point for all troubleshooting steps. Supporting this dashboard in this scenario are workflows for monitoring

- Traffic
- Applications
- Cyber Threats

The following sections describe these key dashboards in detail.

Soho360 – Important Dashboards

Workflows in the following dashboards are important for small-business and home networks.

- Real-Time Internet Monitoring (also known as the landing page)
- Traffic Monitor
- Application Monitor
- Host Monitor
- Secure Web Map
- SSL Monitor
- Cyber Threat Monitor
- SSL Session Analysis Monitor

Real Time Internet Monitoring Dashboard

Key data displayed on this dashboard are in the form of line-graphs for over-time trends, pie charts and gauge graphs for snapshots and a table of statistical data for internet-conversations.

Note:

Dashboard images in this document are samples only. They may not match what is displayed on your Soho360 dashboards.

Use the filter options in the top left to change the ClientIP and ServerIP selection and those in the top right of the graph panel to set the time related coordinates for generating the graphs.
See

Filter Options.

Graphs in this dashboard

The graphs in the 10 parts of this dashboard give you a trend view and snapshot view of internet data as described in the sections below.

Total internet traffic vs Network Latency graph

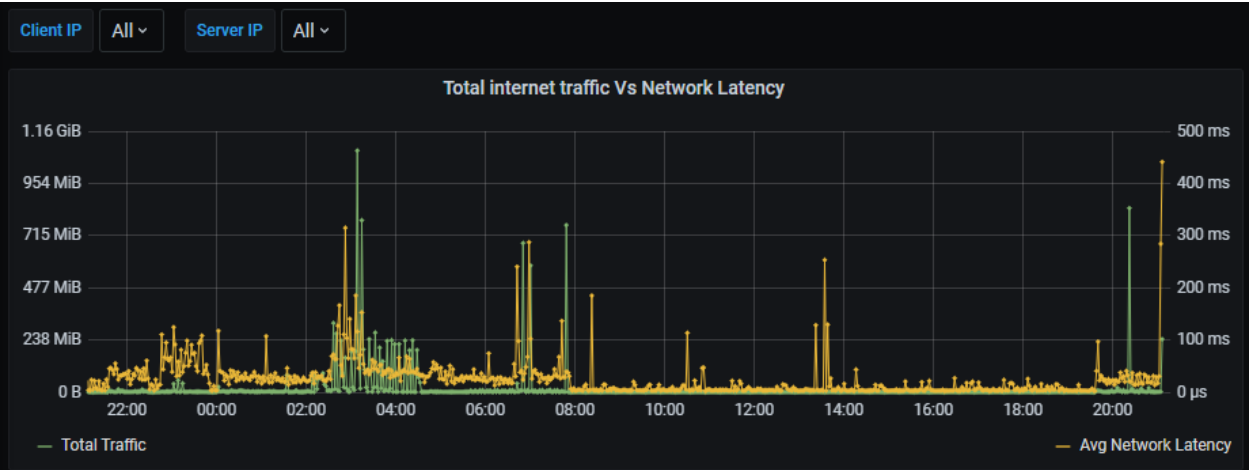


Figure 3. Total internet traffic v/s Network Latency

Network latency is the time taken for the network to respond to the traffic being sent by a client/user.

This chart...	shows...
Total Internet traffic Vs Network Latency	<div>the total bandwidth usage on your internet link.</div> <div><div>- the left part of the pane shows the network traffic. It represents the extent of bandwidth usage.</div><div>- the right side shows network latency.</div></div> <div>It helps you visualize bandwidth usage over a period of time vis-a-vis the actual latency - the time taken to connect and stay connected to your service provider network.</div>

Table 3. Total internet traffic v/s Network Latency

Top Apps consuming bandwidth graph

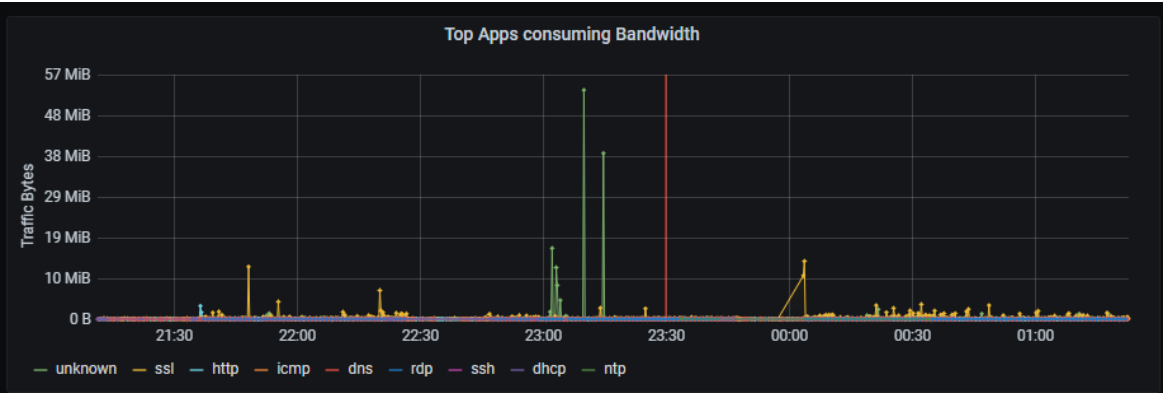


Figure 4. Top Apps consuming bandwidth

<i>This chart...</i>	<i>shows the top ...</i>
Top Apps consuming bandwidth	Applications consuming the most amount of bandwidth.
	Of the applications that are using the highest bandwidth at that point in time, the one consuming the most is at the top of the list.
	Move the mouse over the graph to see the application that tops the list.

2021-07-08 05:05:00

- ssl: 106 MiB
- http: 389 KiB
- unknown: 333 KiB
- icmp: 174 KiB
- dns: 21 KiB
- ssh: 9 KiB
- rdp: 2 KiB
- dhcp: 2 KiB
- ntp: 456 B

Table 4. Top apps consuming the highest bandwidth

Top Clients and Servers graphs

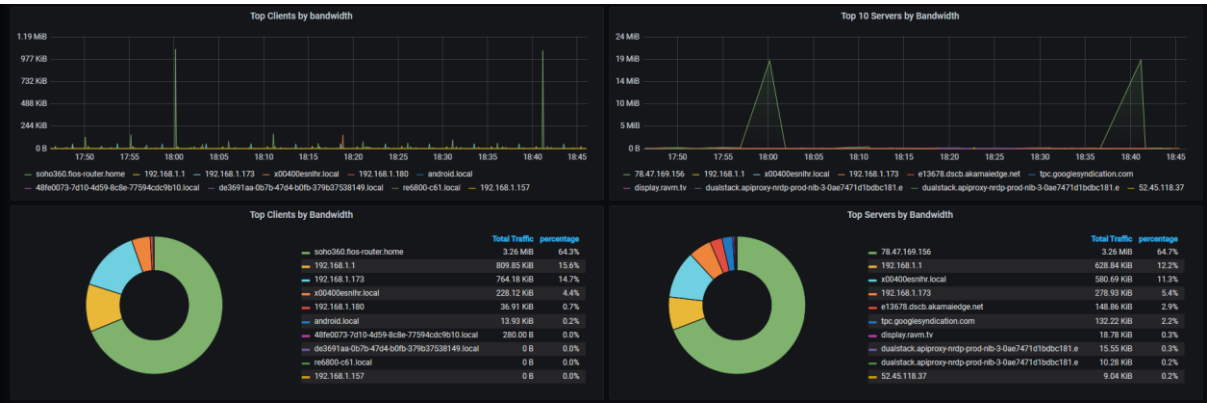


Figure 5. Top Clients and Servers Graphs

Note: Panels on the left side show the client/user data while the right side shows the server data.

<i>This chart...</i>	<i>shows the ...</i>
Top Clients by bandwidth (over-time trend graph)	top users in the network consuming the most amount of bandwidth. This is a trend chart of bandwidth usage. Read this trend graph with the snapshot graph below it.
Top Clients by bandwidth (snapshot)	top users in the network that are highest consumers of bandwidth. This is a snapshot view that lists the consumers with maximum bandwidth usage with the highest consumer at the top of the list. This view represents total bandwidth consumed in the given time frame whereas the over-time graph provides usage over time (not the sum during that period)
Top 10 Servers by bandwidth (trend chart)	top internet servers that are highest consumers of bandwidth. This is a trend chart of usage. Read this trend graph with the snapshot graph below.
Top Servers by bandwidth (snapshot)	top internet servers in that are highest consumers of bandwidth. This is a snapshot view that lists the servers with maximum bandwidth usage with the highest at the top of the list.

Table 5. Top 10 Clients and Servers Graphs

Secure and Non Secure Traffic Graphs

Websites/servers use either the HTTP (insecure) or the HTTPS (secure) service. These charts provide details about distribution of secure and non secure internet traffic.



Figure 6. Secure and Non Secure Traffic Graphs

<i>This chart...</i>	<i>Is a trend graph of the Top 10...</i>
Top 10 Secure Web Server Traffic over time	secure internet web servers (https) where most of your internet traffic is going to.
Top 10 Secure Web Traffic with Worst Latency	secure internet web servers (https) where your internet traffic is experiencing the highest latency.
Top 10 Non Secure Web Server Traffic over time	non-secure (http) internet web servers where most of your internet traffic is going to.
Top 10 Non Secure Web Traffic with Worst Latency	non-secure (http) internet web servers where your internet traffic is experiencing the highest latency.

Table 6. Top 10 Secure and Non Secure Traffic Graphs

Secure Web End-User Experience & Connection Statistics table

ClientIP	ClientIP	Server Ho	Web Server Nan	ServerIP	User R	Network F	Server	Applica	End to End User Experience Response Time	Status	In Traffic	Out Traffic	C-Ref	S-Ref	#Connect
192.168.1.174	192.168.1.174	invitation.e...	-	17.138.144.4	0 μs	1.2 s	25.9 ms	0 μs	1.3 s	Success	224.0 B	283.0 B	0	0	1
soho360.l...	192.168.1.171	78.47.169...	78.47.169.156	78.47.169.156	6.0 ms	124.6 ms	114.1 ms	564.8 ms	809.4 ms	Success	72.4 KiB	61.8 KiB	0	17	2
192.168.1.174	192.168.1.174	k-0002.k-m...	outlook.office.com	13.107.18.11	115.4 ms	25.5 ms	16.3 ms	617.1 ms	774.3 ms	Success	19.1 KiB	13.9 KiB	7	4	2
x00400esnl...	192.168.1.182	34.240.79...	api-global.netflix...	34.240.79.168	20.7 ms	95.1 ms	99.0 ms	287.9 ms	502.6 ms	Success	8.9 KiB	10.5 KiB	0	0	1
192.168.1.174	192.168.1.174	skypedatap...	self.events.data...	52.114.88.20	7.9 ms	86.3 ms	82.5 ms	289.7 ms	466.4 ms	Success	14.1 KiB	8.2 KiB	0	0	2
192.168.1.174	192.168.1.174	gsp64-ssl.l...	gsp64-ssl.is.appl...	17.57.12.11	10.9 ms	85.1 ms	82.1 ms	287.4 ms	465.4 ms	Success	4.1 KiB	2.0 KiB	0	0	1
192.168.1.174	192.168.1.174	gateway.fe...	gateway.icloud.c...	17.248.138.44	40.5 ms	10.9 ms	14.1 ms	311.5 ms	377.1 ms	Success	11.3 KiB	7.5 KiB	7	2	1
x00400esnl...	192.168.1.182	liberty.logs...	liberty.logs.roku...	52.72.25.210	16.5 ms	19.9 ms	42.3 ms	155.4 ms	234.2 ms	Success	3.6 KiB	2.7 KiB	0	1	1
192.168.1.174	192.168.1.174	mnz-efz.m...	outlook.office36...	52.96.15.2	12.7 ms	32.1 ms	40.9 ms	143.0 ms	228.7 ms	Success	35.4 KiB	16.4 KiB	3	0	2
192.168.1.174	192.168.1.174	mnz-efz.m...	outlook.office36...	52.96.33.82	49.5 ms	24.1 ms	23.0 ms	108.7 ms	205.3 ms	Success	947.8 KiB	96.3 KiB	13	39	4
192.168.1.174	192.168.1.174	invitation.e...	-	17.138.128.4	0 μs	114.4 ms	79.8 ms	0 μs	194.3 ms	Success	328.0 B	438.0 B	0	0	2
192.168.1.174	192.168.1.174	mnz-efz.m...	outlook.office36...	52.96.88.98	19.7 ms	34.0 ms	27.3 ms	109.2 ms	190.2 ms	Success	152.6 KiB	113.3 KiB	21	1	3
x00400esnl...	192.168.1.182	configavc.c...	configavc.cs.rok...	107.23.68.69	3.9 ms	17.6 ms	30.8 ms	125.4 ms	177.7 ms	Success	5.2 KiB	4.4 KiB	1	0	1
192.168.1.174	192.168.1.174	invitation.e...	-	17.138.126.4	0 μs	95.2 ms	80.6 ms	0 μs	175.8 ms	Success	492.0 B	657.0 B	0	0	3

Figure 7. Secure Web End-User Experience & Connection Statistics Table

This table contains very important statistics for real-time internet monitoring. Each row in this table represents an instance of a *secure web conversation*.

With respect to the conversation each row indicates:

- who in your small-business or home network is talking to whom in the internet,
- whether they are facing a problem,
- if yes, where in the conversation is the problem occurring.

Table Entry(in each row)	indicates...
ClientHostName	the host name of the client or user. It indicates the user participating in the conversation in the selected time frame.
<u>ClientIP</u>	the IP address of the client or user. This drilldown link provides overall secure web transactions from the user without the context of the conversation. On clicking this drilldown-link the workflow navigates to the Secure Web Map monitor for further trouble shooting.
Server HostName	the server name.
Web Service Name	the name of the web service in the conversation.
<u>ServerIP</u>	The ip address of the web server. Clicking this drilldown-link activates the workflow and navigates to the Secure Web map monitor to continue with trouble shooting. This map shows all server connections made by the selected client/user during the specific time period.
User Response Time	The time taken represented in seconds or milliseconds or microseconds, by the users device to initiate a request to web server. As this points at user devices in the small-business or home network, a high value here means the problem could be at the user's device.
Network Response Time	The time taken represented in seconds or milliseconds or microseconds for the network to respond to the user's request. As this points at the service provider end, a high value here means the problem could be at the service provider's network.
Server Response Time	The time taken represented in seconds or milliseconds or microseconds, by the web server to respond to the user's request. As this points at the internet server - for example, the YouTube server or Netflix server a high value here means the problem could be at the internet server hosting these applications.
Application Response Time	The time taken represented in seconds or milliseconds or microseconds, by the application on the web server to respond to the user's request.
End to End User Experience Response Time	the end to end latency experienced by the end user. The number here is the sum of the 4 above response time metrics. The transition from green to red in the color bar is

Table Entry(in each row)	indicates...
	indicative of the actual experience. See Figure 7 .
Status	the status of the connection – whether <i>success</i> , <i>failure</i> or <i>error</i> . This is a clear indication of serious problem at the server end, when there is a failure.
In Traffic	total volume of traffic coming in from the server to the user/client.
Out Traffic	total volume of of traffic going out from the user/client to the server.
C-ReTrans	total number of client initiated retransmissions.
S-ReTrans	total number of server initiated retransmissions.
<u>#Connections</u>	<p>number of connections for a selected conversation (row in the table). This drilldown-link takes the context of the conversation. This field shows all the connections between the specific client and server. This drilldown-hyperlink leads to the SSL Session Analysis monitor as part of the trouble shooting workflow.</p> <p>Note: Each conversation can have multiple connections.</p>

Table 7. Secure Web End-User Experience & Connection Statistics Table

The 3 key data items pertaining to each conversation in this table are hyperlink-drilldowns that lead you to the next level of investigation. Note that they are highlighted in the table.

- Client IP
- Server IP
- Connections

ClientIP

ClientIP is not part of the context/conversation that is listed in each row of this table. It indicates what the client/user was involved in over the selected time period.

However, because it indicates the **client IP** (in fact the **user**), it becomes useful in a scenario of multiple *connections* in the selected conversation, where one of them is consuming more bandwidth and impeding an important connection.

It detects the show-stopper so that the less important connection can be stopped and the more important one can continue. For example:

- one user of the **client ip** is watching a video stream (say Netflix)

and

- another user is connecting to a conference call (say Zoom).

If the phone call is stalling due to bandwidth issues, the video-streaming connection can be stopped for the time being.

This would release some bandwidth to let the phone connection continue unhindered.

ServerIP

This is part of the conversation captured in each row of this table. It provides statistical information pertaining to the client /user and server within the context of the selected time.

Response Time

The response time metrics in this table include the following and are very useful in trouble shooting.

- User Response time
- Network Response Time
- Server Response Time
- Application Response Time
- End to End User Experience Response Time
- Status

For example: If the conversation involves a user trying to run a YouTube video experiences constant buffering issues, the conversation table could show the following latency data.

- High User Response Time - indicates that the latency is caused by the user's device (laptop/TV/smart phone etc.). This could be due to any hardware or memory issues on your device. Perform the necessary checks to resolve those issues and retry.
- High Network Response Time - indicates that the latency is caused at the service provider network end.
- High Server Response Time - indicates that the latency is caused at the internet server (in this case, the YouTube server that is providing the video content).
- Application Response Time - indicates that the latency is caused by the application (in this case, the YouTube application).
- End to End User Experience Response Time - is the total latency experienced by the user in the selected conversation. It is the sum of the above 4 response time metrics.
- Status - indicates whether the connection to the internet/server/application is successful or is failing.

In case of a "High User Response Time" you have to resolve your device issue yourself. For all other cases of latency you can contact the person(s) responsible for uptime and seek resolution of the problem or reimbursement of subscription fees as the case may be.

To troubleshoot from the real-time monitoring dashboard you can:

- Click **ClientIP** and view the **Secure Web Map** monitor. The graphic map displays the top 20 servers communicating with the selected ClientIP/user that experience the worst/highest response time. This could be due to a latency issue or a failure. See

- [Secure web Map](#) Monitor.
- Click **ServerIP** to view the **Secure Web map** monitor. The graphic map displays the client and the server with all statistical information in the context of the conversation.
- Click **#Connections** to see the number of connections involved in the selected client-server conversation in the **SSL Session Analysis** monitor. See [SSL Session Analysis Monitor](#).

Traffic-Monitor

Traffic monitor provides a platform for comprehensive investigation into network performance within your network. It provides the trending of traffic analysis upto the last 3 months in comparison with the *Real Time Monitor* which can only provide the trending upto the last 4 days.

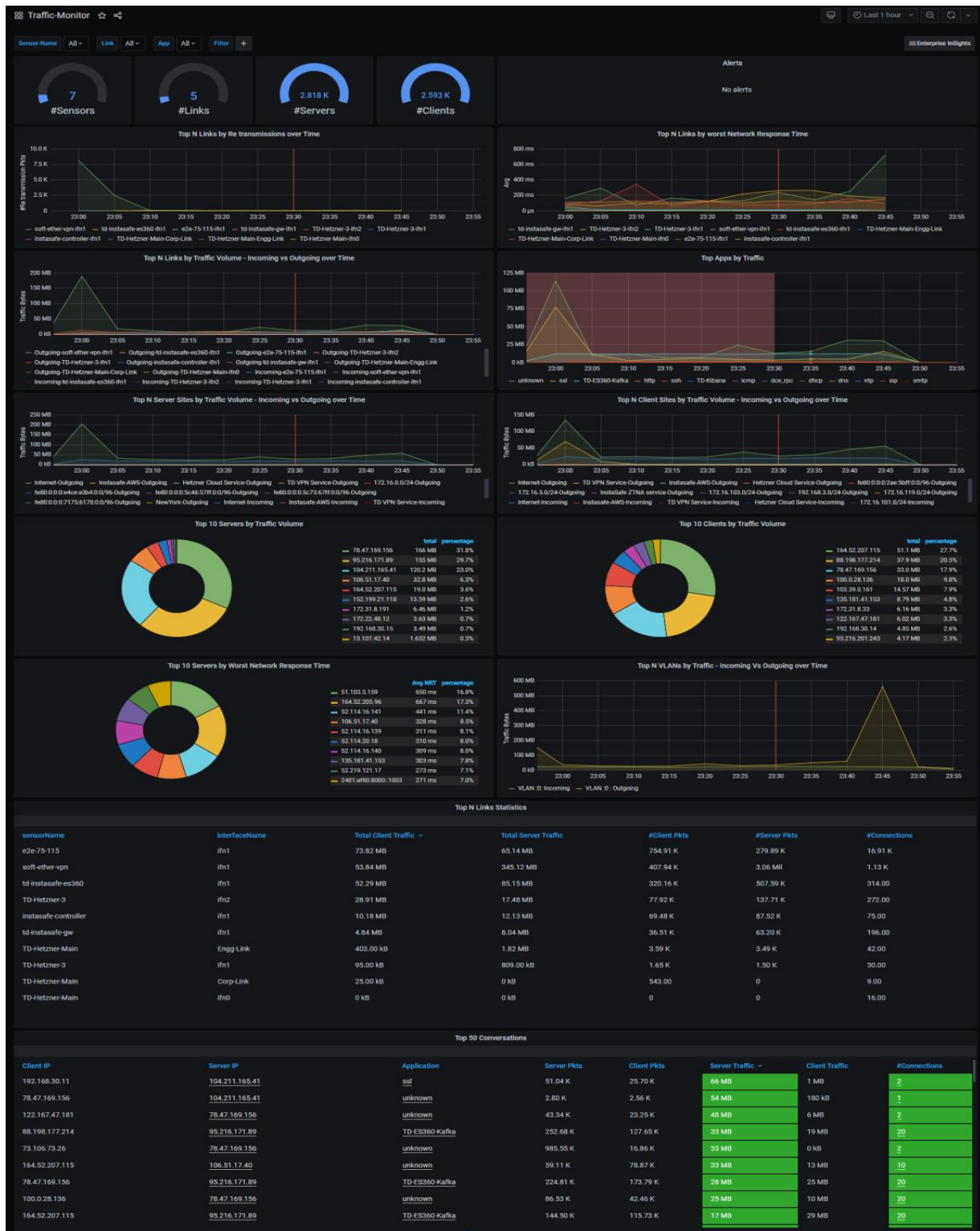


Figure 8. Traffic Monitor – Default Panels

Use the traffic monitor to:

- discover instances of links being in the up/down states
- track site level traffic performance
- view link and application throughput rates
- recognize transmission, congestion and traffic bottlenecks in the network
- identify top servers, clients and conversations taking maximum traffic bandwidth
- study link performance

This dashboard is a multi-part display of contextual panels with multiple genres of internet traffic related information. Each part pertains to a specific context and has 2 or more panels, named to indicate its contents.

Top Traffic Entities

Multiple graphs in this panel give at one glance a view of the following

- #Sensors
- #Links
- #Servers
- #Clients

Alerts – This panel space can be used to define Alerts for tracking the traffic and related issues. See "[Creating Alerts](#)".

Top N links Over-time graphs

This part displays the trending status of retransmission and network response related traffic issues over time.

- Top N Links By Retransmissions - The N Links that experienced the highest retransmission at specific points in time.
- Top N Links By worst network response time - The N Links that experienced the worst network response at specific points in time.

Top Traffic Volume Graphs

This part displays the following status of traffic in the network.

- Top N Links By Traffic Volume - Incoming vs Outgoing over Time - The N Links that experienced the highest traffic volume.
- Top Apps - The apps that experienced high volume of traffic.

Top 10 Servers, Clients and Vlans

This part displays the trending status of clients, servers and Vlans that experienced the most traffic.

- Top 10 Servers by Traffic Volume - servers that experienced the highest traffic volume at specific points in time.
- Top 10 Clients by Traffic Volume - clients that experienced the highest traffic volume at specific points in time.

- Top 10 Servers by the worst response time - servers that displayed the worst response time at specific points in time.
- Top 10 Vlans by traffic incoming v/s outgoing - Vlans that experienced highest volume of incoming and outgoing traffic.

Top N Links Statistics table

This table has statistical details about N links in the network. Use the hyperlinks (underlined fields) to view details.

<i>This field...</i>	<i>indicates...</i>
sensorName	The name of the sensor capturing this data.
interfaceName	The name of the interface configured for the sensor.
Total Client Traffic	Total traffic at the client..
Total Server Traffic	Total traffic at the server.
#Client Pkts	Number of client packets.
#Server Pkts	Number of server packets.
#Connections	The number of connections.

Table 8. Top N Links Statistics table

Application-Monitor

This dashboard is a set of panels to help you understand and troubleshoot most common applications in the network.



Figure 9. Application Monitor - Default Panels

The *Application monitor* provides a consolidated view of all applications to understand high level failures and performance issues across applications

Each chart in the panels of this monitor is a use-case related to application monitoring in the network.

The details in these panels are described in the following section.

The Top Graphs and Alerts

This panel displays the number of apps running in the client and server nodes of the network. The gauge-format by default displays the total number of these 3 entities across the network.

Label	Description
#Apps	Number of apps in the network.
#Servers	Number of servers in the network.
#Clients	Number of clients in the network.

Alerts

At the initial instance of usage this panel would be empty. Alerts are created and configured by users in the "admin" role for tracking trends over-time. Once they are defined, alerts created to track application status are displayed in this panel. See "[Creating Alerts](#)" for details.

The Over-time Graphs

The next 3 parts of the dashboard display the trending status that is important for tracking apps with respect to clients, servers, connections and traffic across the network.

Top 10 Apps by...	A trend chart...shows the user...
Failures over time	The applications that are failing so much as to become potential performance issues.
Traffic Volume over time	The Traffic volume leading to potential performance issues.
Top 10	A pie chart...shows the user...
Busiest Servers by #Connections	The top 10 busiest servers in the network by the number of connections.
Servers by App Failures	The top 10 busiest servers in the network by the number of App failures.
Servers by Traffic Volume	The top 10 busiest servers in the network by the traffic volume.
Top 10	A pie chart...shows the user...
Busiest Clients by #Connections	The top 10 busiest clients in the network by the number of connections.
Clients by App Failures	The top 10 busiest clients in the network by the number of App failures.
Clients by Traffic Volume	The top 10 busiest clients in the network by the traffic volume.

The Conversations table

This is a summary of the top Site-Site App Conversations with Worst Failures/Performance.

<i>Table Entry</i>	<i>This entry indicates...</i>
<u>Application</u>	The application that is failing or performing badly. It is a hyperlink. Click to see the "DNS Monitor".
Application Message	The message from the application.
Client Site	The name of the client site.
Server Site	Site of the Server IP – defaults to IP subnet if site is not defined.
Client IP	IP address of the client.
Client User@Host	IP address of the client.
<u>Server IP</u>	The server IP address related to the client.
<u>Srv Hostname</u>	The hostname of the server related to the client.
<u>Avg Response Time</u>	Application response time of the transaction.
#Failure connections	Number of failed transactions.
<u>#Success connections</u>	Number of successful transactions.

Host-Monitor

The *Host monitor* provides a dashboard for comprehensive investigation into problems associated with individual hosts in the network. Users can start investigation with a hostname or a host IP address.



Figure 10. Host Monitor – default panels

This monitor provides full visibility into host traffic analysis with *client-hosts traffic data* on left hand side of the charts and *server-hosts traffic data* on right hand side of the charts.

Use this monitor to:

- understand applications running on the host, traffic volumes, application latencies, errors.
- track top conversations and traffic key performance indicators (KPIs) per conversation.
- detect cyber threats on the host.
- investigate into other application monitors with context and drill down to investigate host traffic sets in detail.

This is a multi-part display of contextual panels with multiple genres of information related to hosts. The following sections describe each chart in the panels of this monitor.

Hosts entities and Events Graphs

Title	Purpose
Client hosts graphs	<p>The left side graphs in this panel give a view of the following:</p> <ul style="list-style-type: none"> - #Client App failures - #Client network errors - #Client Connections - #Client Threats - #Client- Average client response time (CRT) - #Client-Average network response time (NRT) - #Client-Average Application response time (ART) - #Client Resets
Server host graphs	<p>The right side graphs in this panel give a view of the following:</p> <ul style="list-style-type: none"> - #Server App failures - #Server network errors - #Server Connections - #Server Threats - #Server-Average client response time (CRT) - #Server-Average network response time (NRT) - #Server-Average Application response time (ART) - # Server Resets

Table 9. Hosts entities and Events Graphs

Note: In all graphs here the color indicates if the number is within (green) approaching (orange) or exceeding (red) the error limit set for each of the KPIs.

Client - Top Apps by Connections, Failures and Avg RT - table

This left side table has specific details about the highest incidence of applications on clients and their related data in the network. As a standard step, use the hyperlinks (underlined fields) to view details.

<i>This field...</i>	<i>indicates...</i>
Client IP	The client IP address.
<u>App</u>	The application. Click to go to the selected app's dashboard/monitor E.g. If the app is "SSH" you will see the SSH Monitor..
#Connections	The number of connections in the client.
Avg RT	The average response time in microsecond.

#Failures	The number of failures.
#Success	The number of successes.

Table 10.Client - Top Apps by Connections, Failures and Avg RT table

Server - Top Apps by Connections, Failures and Avg RT - table

This right side table has specific details about the highest incidence of applications on servers and their related data in the network. As a standard step, use the hyperlinks (underlined fields) to view details.

<i>This field...</i>	<i>indicates...</i>
Server Ip	The server IP address.
<u>App</u>	The application. Click to go to the selected app's dashboard/ monitor E.g. If the app is "SSH" you will see the SSH Monitor..
#Connections	The number of connections in the server.
Avg RT	The average response time in microsecond.
#Failures	The number of failures.
#Success	The number of successes.

Table 11.Server - Top Apps by Connections, Failures and Avg RT table

Top app Conversations

The left side table has specific details about 50 hosts (clients) with the highest traffic volume. The right side table has the same specific details about 50 hosts (servers) with the highest traffic volume. Use the hyperlinks (underlined fields) to view details.

<i>This field...</i>	<i>indicates...</i>
<u>App</u>	The application. Click to go to the selected app's dashboard/ monitor, e.g. If the app is "SSH" you will see the SSH Monitor..
ClientIP	The client's IP address.
ServerIP	The server's IP address.
#ClientTraffic	the volume of traffic into the client.
#ServerTraffic	the volume of traffic into the server.
AvgCRT	the average client response time in microseconds.
AvgSRT	the average server response time in microseconds.
AvgNRT	the average network response time in microseconds.
AvgDuration	the average duration of app usage in seconds.
#CPkts	the number of client packets.
#SPkts	the number of server packets.
#NetErrors	the number of network errors.

<i>This field...</i>	<i>indicates...</i>
#CyberThreats	the number of cyber threats.
#InfraIssues	the number of infra issues
#AppErrors	the number of application errors
#Conn	the number of connections. Click to go to the "Connections session analysis monitor".

Table 12.Top app Conversations

Client - Top 20 Servers metrics - graphs

The left side of this part has data about top 20 clients that have server issues.

<i>Client - Top 20 Servers graph...</i>	<i>Displays...</i>
Client - Top 20 Servers by App Failures	The 20 servers at the client end with the highest application failures.
Client - Top 20 Servers by worst ART	The 20 servers at the client end with the worst application response time in seconds.
Client- Top 20 Links by worst NRT	The 20 links at the client end with the worst network response time.
Client- Top 10 Worst Server Sites by ART	The 10 server sites at the client end with the worst application response time

Table 13.Client - Top 20 Servers metrics - graphs

Server- Top 20 Clients metrics - graphs

The left side of this part has data about top 20 servers that have client issues.

<i>Server - Top 20 clients graph...</i>	<i>Displays...</i>
Server - Top 20 Clients by App Failures	The 20 clients at the server end with the highest application failures.
Server - Top 20 Clients by worst ART	The 20 clients at the server end with the worst application response time in seconds.
Server- Top 20 Links by highest traffic	The 20 links at the server end with the highest traffic.
Server- Top 10 Worst Client Sites by ART	The 10 client sites at the server end with the worst application response time

Table 14.Server- Top 20 Clients metrics - graphs

Secure web Map Monitor

On clicking **ClientIP** in the “Secure Web End-User Experience & Connection Statistics” table, the secure web map appears as illustrated in [Figure 11](#). It provides a network view of how clients - servers in the network are interconnected and the flow of traffic across them. It serves as the starting point for visually troubleshooting the failing or poorly performing connections in the Soho network.

Note: The icons in this map represent nodal network entities - client and servers. You have the option of clicking the central node (representing the client/user in the secure web conversation) or any of the peripheral nodes (the servers in the conversation).



Figure 11. Secure Web Map in a Soho network

The map displays the servers that are having trouble communicating with the selected ClientIP. The red highlight of a server node indicates that it is experiencing the **worst/highest response time** at the time of selecting the row in the “Secure Web End-User Experience & Connection Statistics” table.

Options in the secure web map dashboard

Use the elements of the graphic user interface (GUI) as described below.

Filters -top left

The left side of this map has 2 fields - Client IP and Server IP. These serve as filters. You can use them to display only those connections belonging to the conversation that you wish to view and troubleshoot.

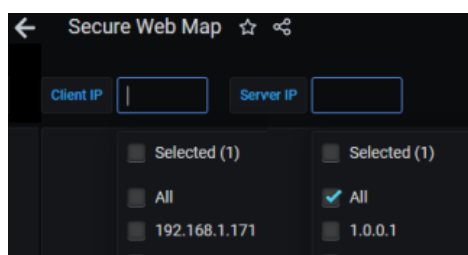


Figure 12. Filter

Display controls - top right

The right side of this map, has options for you to control the display, as illustrated in the table below.






Icon...	Click to...
	Start or stop seeing the flow of incoming and outgoing data. This lets you toggle start/stop.
	Restore the display to the center of page after zoom-in/zoom-out.
	Restore and center the display
	Zoom in to enlarge the display
	Zoom out to minimize the display.

Table 15. Map icons

Note: You can use the mouse scroll-wheel to enlarge or reduce the display size of the map. You can then use either of the icons to restore the default size.

Client Connections in the selected conversation

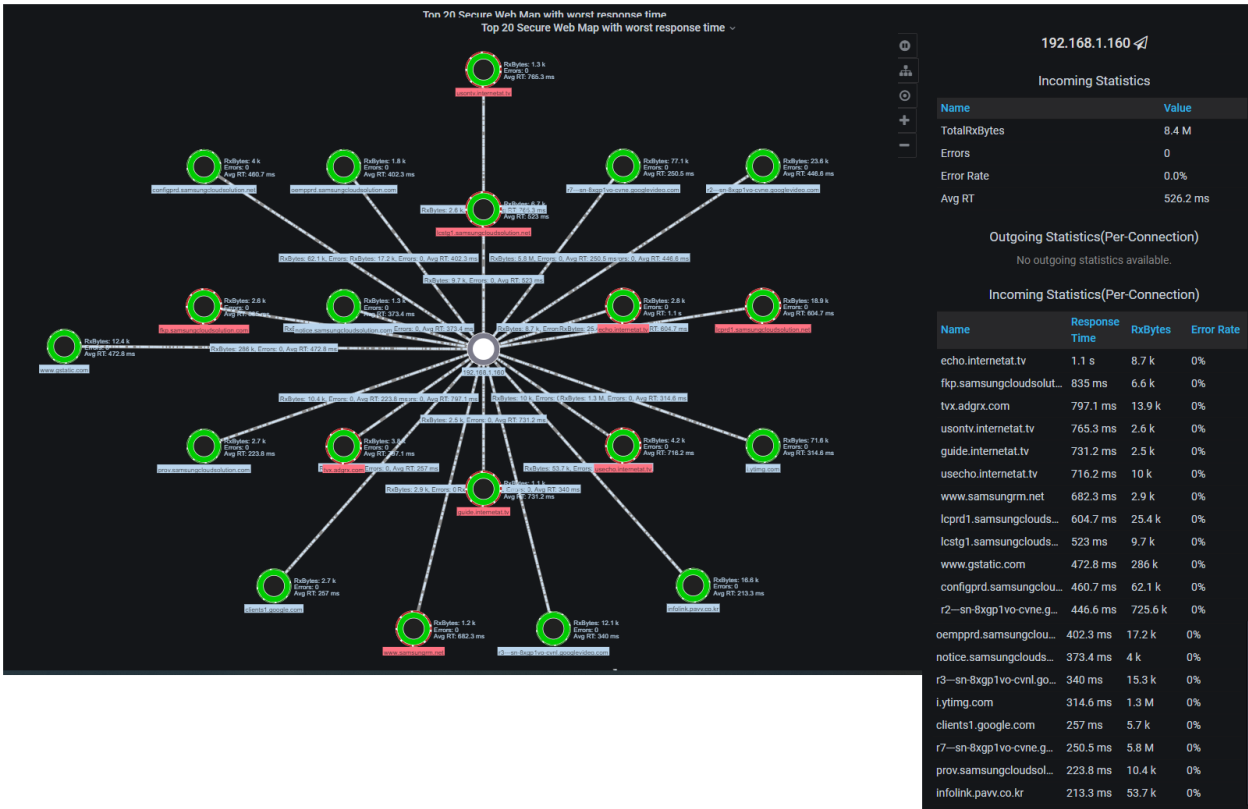


Figure 13. Incoming Statistics for the client and its connections in the selected conversation

Click the central (client) node to view related statistics, or drill down for further details, as illustrated in the table below.

Option/panel...	indicates...
	<p>This indicates the client node in the selected row of the table. It is the central node in the map.</p> <p>Click to see the selected client's statistics panel to the right of the map:</p>
	<p>This panel displays incoming statistics for the selected client – 192.168.1.160 in the sample page.</p> <ul style="list-style-type: none">- Total RX bytes: 8.4 MB of total received bytes from all the connections.- Errors: 0 errors from these connections- Error Rate: 0% error rate- Avg RT: 526.2 millisecond
	<p>Out-going statistics for the servers connecting to the client are not included in this display.</p>

Option/panel...

Name	Response Time	RxBytes	Error Rate
echo.internetat.tv	1.1 s	8.7 k	0%
fkp.samsungcloudsol...	835 ms	6.6 k	0%
tvx.adgrx.com	797.1 ms	13.9 k	0%
usontv.internetat.tv	765.3 ms	2.6 k	0%
guide.internetat.tv	731.2 ms	2.5 k	0%
usecho.internetat.tv	716.2 ms	10 k	0%
www.samsungrm.net	682.3 ms	2.9 k	0%
lcprd1.samsungclouds...	604.7 ms	25.4 k	0%
lcstg1.samsungclouds...	523 ms	9.7 k	0%
www.gstatic.com	472.8 ms	286 k	0%
configprd.samsungclou...	460.7 ms	62.1 k	0%
r2--sn-8xgp1vo-cvne.g...	446.6 ms	725.6 k	0%
oempprd.samsungclou...	402.3 ms	17.2 k	0%
notice.samsungclouds...	373.4 ms	4 k	0%
r3--sn-8xgp1vo-cvnl.go...	340 ms	15.3 k	0%
lytimg.com	314.6 ms	1.3 M	0%
clients1.google.com	257 ms	5.7 k	0%
r7--sn-8xgp1vo-cvne.g...	250.5 ms	5.8 M	0%
prov.samsungcloudsol...	223.8 ms	10.4 k	0%
infolink.pavv.co.kr	213.3 ms	53.7 k	0%


indicates...

Incoming statistics per connection displayed as a table in the right panel.


- the Name column includes all the servers connected to the selected client, in the selected conversation.
- the Response time column indicates the response time for each of the servers in the conversation.
- the RxBytes column indicates the number of "received bytes" in KB/MB for each server.
- the Error rate column indicates the percentage of error experienced by each server in the conversation.

Note:

- the "Total RX bytes" in the Client's incoming statistics is the sum of the numbers in the "RxBytes" column in this table.
- the "Avg RT" in the Client's incoming statistics is the average of the numbers in the "Response Time" column in this table.



A drill-down option for more data.

Click the  to see the SSL-Monitor related to this conversation.

For details about this monitor and how to use the drill-down data see "[SSL-Monitor](#)".

Table 16.Client Node in the selected conversation

Server Connections in the selected conversation

Click any of the peripheral connected nodes (servers in the selected conversation) to view related statistics, as illustrated below. This is a server experiencing errors in the network.

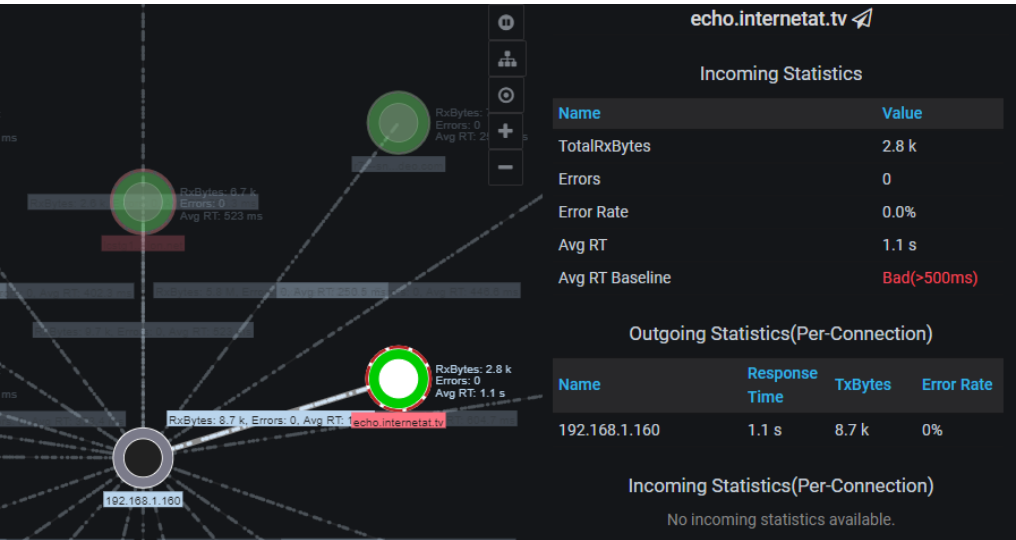
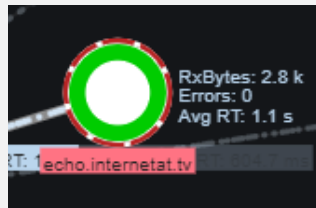


Figure 14. Incoming Statistics for an error prone server in the selected conversation

Option/panel.....**indicates...**

A server in the network which could be affected by latency or an error issue.

For the selected Client IP 192.168.1.160, click any server node with a red outer circle to see:

- the server's incoming statistics
- outgoing statistics per server

echo.internetat.tv

Incoming Statistics

Name	Value
TotalRxBytes	2.8 k
Errors	0
Error Rate	0.0%
Avg RT	1.1 s
Avg RT Baseline	Bad(>500ms)

Incoming statistics for the selected server is displayed as a table in the right panel.

- the TotalRxBytes field indicates the number of "received bytes" in KB/MB for that server.
- the Errors field indicates the errors experienced by that server.
- the Error rate column indicates the percentage of error experienced by the server.
- the Avg RT field indicates the average response time experienced by that server.
- the Avg RT Baseline field indicates the baseline/threshold set for response time before it begins to turn into a bottleneck for dataflow.
- The red highlight indicates that the error is because response time has exceeded the threshold.

Outgoing Statistics(Per-Connection)

Name	Response Time	TxBytes	Error Rate
192.168.1.160	1.1 s	8.7 k	0%

Outgoing statistics per connection displayed as a table in the right panel.


- the Name column includes the client that this server is connected to.
- the Response time column indicates the response time for each of the server-connections.
- the RxBytes column indicates the number of "transmitted bytes" in KB/MB for each server.
- the Error rate column indicates the percentage of error experienced by the server.



Error free servers in the network.

These may be error free at the current point in time, but if their latency has crossed the set threshold or is approaching the threshold they may fall in the **top**-list and included in the map.

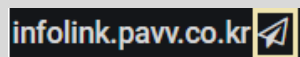
Option/panel.....

infolink.pavv.co.kr 			
Incoming Statistics			
Name	Value		
TotalRxBytes	15.8 k		
Errors	0		
Error Rate	0.0%		
Avg RT	243.7 ms		
Avg RT Baseline	Good(<=500ms)		
Outgoing Statistics(Per-Connection)			
Name	Response Time	TxBytes	Error Rate
192.168.1.160	243.7 ms	56 k	0%
Incoming Statistics(Per-Connection)		No incoming statistics available.	


indicates...

The statistical data are self explanatory.

The green highlight indicates that there is no response time error is because it is within the threshold.



A drill-down option for more data.

Click the  to see the SSL-Monitor related to this connection.

The *SSL Monitor* covers all secure web applications within the network. For details about how to use the drill-down data see "[SSL-Monitor](#)".

Table 17.Server Nodes in the conversation

SSL-Monitor

80% of the world's web traffic runs over *SSL(Secure Sockets Layer)*. It provides a secure mechanism to transact traffic over the internet. The *SSL Monitor* provides a dashboard for comprehensive investigation into secure web applications within the network.



Figure 15. SSL Monitor default panels - 1

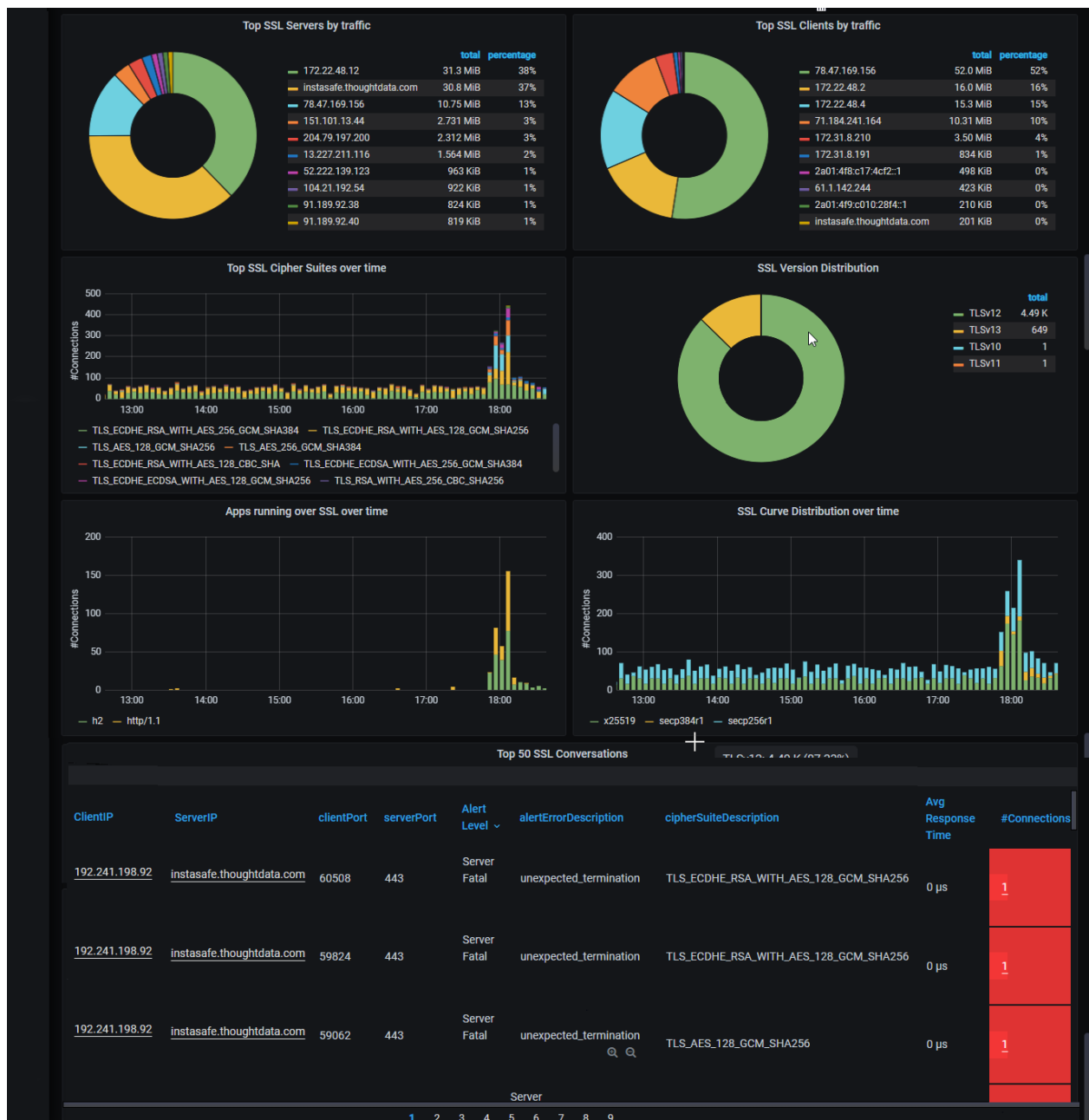


Figure 16. SSL Monitor – default panels -2

Use this monitor to:

- understand the SSL servers running on your web applications in your network
- recognize failure conditions and poor performance connecting to web applications.
- identify the users who get impacted.
- understand various secure algorithms which are used in SSL transactions for authentication, key exchange, compression and encryption.
- improve your SSL security by studying SSL servers running insecure algorithms and methods.
- identify the version of SSL and TLS protocol being used by servers. Older SSL versions are outdated and insecure and can severely compromise your secure web applications.

- study the performance and failure conditions per user SSL transaction and drilldown into further session level investigation.
- discover applications running over SSL sessions.

This is a multi-part display of contextual panels of SSL related information. Each of the 10 parts in this dashboard pertains to a specific context and has 2 or more panels, named to indicate its contents.

SSL Events and Entities

Multiple gauge graphs in this panel give a view of the following:

- Avg Handshake RT
- Server Fatal Errors
- Client Fatal Errors
- Rejected Connections
- Successful Connections
- #Resets
- #SSL Servers
- #SSL Clients

Multiple numeric graphs in this panel give a view of the following:

- Total TCP Timeouts
- Total SSL Connections
- Total SSL Server Traffic
- Total SSL Client Traffic

Alerts

This panel-space can be used for defining alerts for tracking SSL issues.

See "[Creating Alerts](#)".

SSL Client-Server, EURT Over-time graphs

This panel has graphs of the following at specific points in time.

- Client Vs Server Errors over time
- EURT over time

SSL Client/Server and Sessions graphs

This panel has graphs of the following.

- SSL Client Vs Server Traffic
- TCP Connection States for SSL Sessions

Top SSL Tables

The top *Servers with Errors* table, has the following related details:

- Server IP
- alertLevelDescription
- #Connections

Click the hyperlink to go to the SSL Session Analysis page.

The top “Clients with Errors” table has the following related details:

- Client IP
- alertLevelDescription
- #Connections

Click the hyperlink to go to the SSL Session Analysis page.

- Top SSL Servers by traffic - is a graph of servers with the highest SSL traffic.
- Top SSL Clients by traffic – is a graph of clients with the highest SSL traffic.

SSL Errors, and Version Distribution

This panel displays the following graphs.

- SSL Error Codes Distribution over time
- SSL Version Distribution

SSL Over-time graphs

This panel displays the status of the following at specific points in time.

- Top SSL Cipher Suites over time – the highest SSL Cipher suites at specific points in time.
- SSL Curve Distribution over time
- Apps running over SSL over time - the number of apps running at specific points in time.
- SSL Server Name Distribution over time

Top 50 SSL Conversations

This table has specific details about SSL conversations that are most rampant and their related data in the network. Use the hyperlinks (underlined fields) to view details in the related monitor.

<i>This field...</i>	<i>indicates...</i>
ClientIP	The IP address of the client.
ServerIP	The IP address of the server.
clientPort	The port number of the client.
serverPort	The port number of the server.
Alert Level	The level of seriousness of the SSL alert.
alertErrorDescription	Description of the alert level.
cipherSuiteDescription	The cipher suite that is securing the connection. A cipher suite is a set of algorithms used to secure a network connection. Cipher suites usually contain: a key exchange algorithm, a bulk encryption algorithm, and a message authentication code (MAC) algorithm.
sslVersionDescription	Description of the SSL version.
Avg Response Time	Average response time.

<i>This field...</i>	<i>indicates...</i>
#Connections	Number of connections. This is a hyperlink. Click to go to the related monitor.

Table 18.Top 50 SSL Conversations

SSL connections by TCP/UDP

This panel displays the following graph.

- SSL connections by TCP/UDP

Web-Monitor

Web monitor provides a comprehensive board for investigation into problems associated with applications using HyperText Transfer protocol (HTTP), the popular and widely used one for web applications in the network.

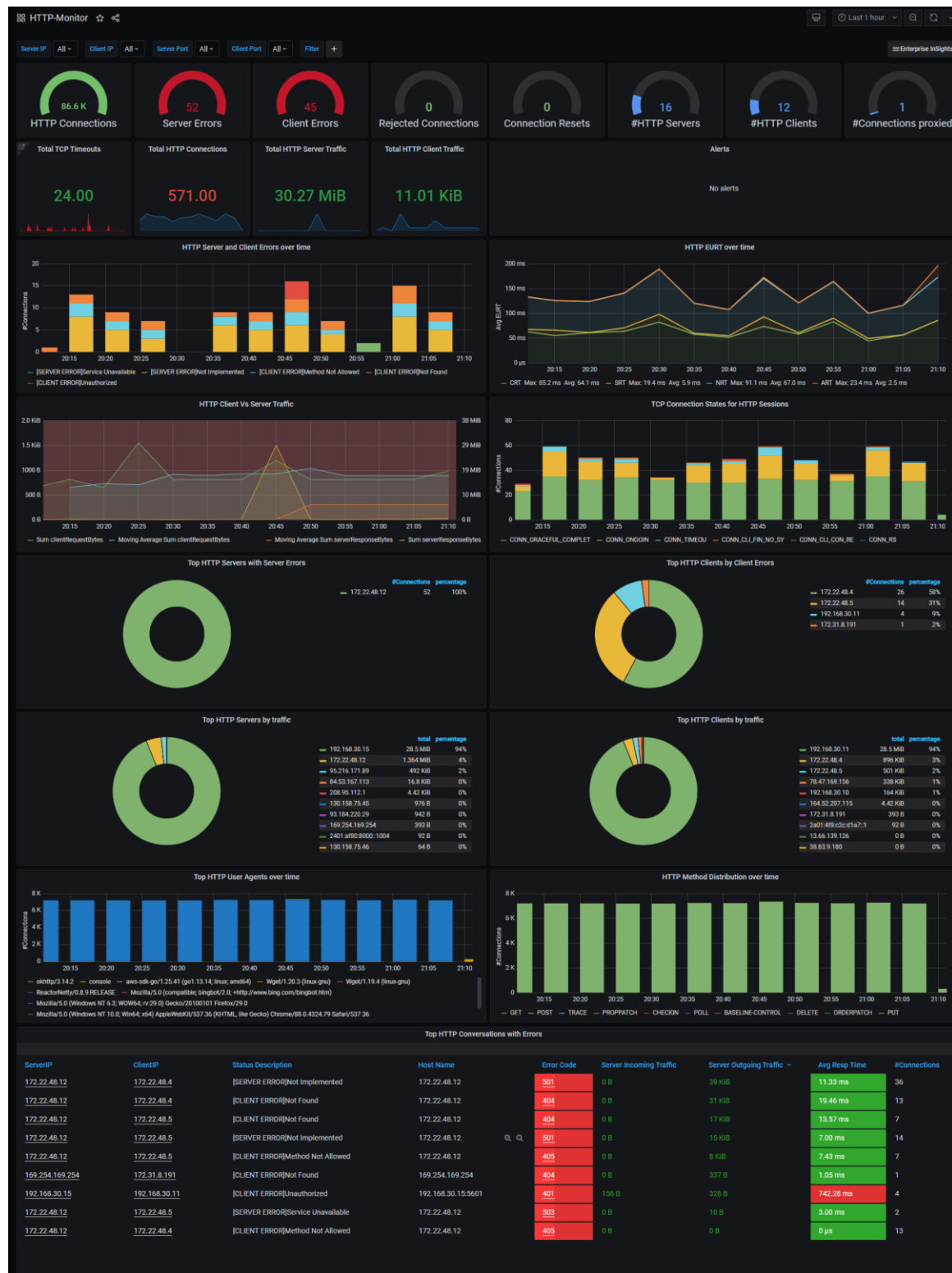


Figure 17. HTTP Monitor – default panels

Use this monitor with respect to web applications, to:

- troubleshoot problems related to transactions such as end user latencies, failures, server, client errors,
- realize HTTP transaction distribution and load on servers,
- recognize which servers are failing or loaded and poorly performing.
- understand the following
 - web traffic distribution across various HTTP versions,
 - types of traffic being transacted over HTTP.
 - URLs accessed by the user, errors and latencies.
 - HTTP proxies in the network, user agents etc.

This is a multi-part display of contextual panels with HTTP related information. The following sections describe each chart in the panels of this monitor.

HTTP entities and Events - graphs

The gauge graphs in this panel give a view of the following:

- HTTP Connections
- Server Errors
- Client Errors
- Rejected Connections
- Connection Resets
- #HTTP Servers
- #HTTP Clients
- #Connections proxied

The line graphs in this panel give a view of the following:

- Total TCP Timeouts
- Total HTTP Connections
- Total HTTP Server Traffic
- Total HTTP Client Traffic

Alerts - Alerts can be defined to track the HTTP issues. See "[Creating Alerts](#)".

HTTP Over time graphs -1

The graphs in this panel display the trending status of errors and EURT over time.

- HTTP Server and Client Errors over time
- HTTP EndUser Response Time (EURT) over time

HTTP Traffic and TCP States for HTTP Sessions

The graphs in this panel display the traffic and TCP states for HTTP sessions.

- HTTP Client Vs Server Traffic
- TCP Connection States for HTTP Sessions

Top HTTP Entities

The graphs in this panel display the HTTP entities experiencing the highest errors and traffic.

- Top HTTP Servers with Server Errors - servers with the maximum HTTP errors.
- Top HTTP Clients by Client Errors - clients with the maximum HTTP errors.
- Top HTTP Servers by traffic - servers with the maximum HTTP traffic.
- Top HTTP Clients by traffic - clients with the maximum HTTP traffic at specific points in time.

HTTP Over time graphs -2

The graphs in this panel display the trending status of user agents and method distribution over time.

- Top HTTP User Agents over time - HTTP user agents with the highest incidence at specific points in time.
- HTTP Method Distribution over time - The most rampant HTTP method distribution at specific points in time.

Top HTTP Conversations with Errors - table

This table has specific details about HTTP conversations that have the most errors and their related data in the network. Use the hyperlinks (underlined fields) to view details in the *Server Infra Monitor*, *Connection Log Monitor* and *HTTP Session Analysis Monitor* respectively.

<i>This field...</i>	<i>indicates...</i>
<u>ServerIP</u>	The IP address of the server. This is a hyperlink. Click to go to <i>Server Infra Monitor</i> .
<u>ClientIP</u>	The IP address of the client. This is a hyperlink. Click to go to <i>Connection Log Monitor</i> .
Status Description	The error status.
Host Name	The name/IP address of the host.
Error Code	The error code. This is a hyperlink. Click to go to <i>HTTP Session Analysis Monitor</i> .
Server Incoming Traffic	The volume of incoming traffic at the server.
Server Outgoing Traffic	The volume of outgoing traffic at the server.
Avg Resp Time	The average response time in microsecond.
#Connections	The number of connections.

Table 19. Top HTTP Conversations with Errors

Top 10 HTTP Host Names with URLs - table

This table has specific details about HTTP host names that have URLs and their related data.

<i>This field...</i>	<i>indicates...</i>
Host Name	The IP address of the host.
URL	The Unique resource locator (URL) name assigned to the host.
#Connections	The number of connections.
Server Incoming Traffic	The volume of incoming traffic at the server.

Table 20.Top 10 HTTP Host Names with URLs

Top 10 HTTP Referrers - table

This table has specific details about HTTP referrers and their related data.

<i>This field...</i>	<i>indicates...</i>
Referrer	The IP address of the referrer.
#Connections	The number of connections.
Server Incoming Traffic	The volume of incoming traffic at the server.

Table 21.Top 10 HTTP Referrers

MIME Distribution over time - graph

The graphics in this panel display the status of Multipurpose Internet Mail Extensions (MIME) formats distribution in the clients and servers in the network at specific points of time

- Server MIME Distribution Over-time
- Client MIME Distribution Over-time

HTTP host names and version distribution graphs

<i>Graph...</i>	<i>To show...</i>
Top HTTP Hostnames	The hostnames with the maximum connections.
HTTP Version Distribution	The distribution of HTTP version.

Table 22.HTTP host names and version distribution graphs

Top 50 HTTP Conversations by worst response time

This table has specific details about HTTP conversations that have the worst response time and their related data in the network. Use the hyperlinks (underlined fields) to view details in the ***"Error! Reference source not found."***, and *HTTP Session Analysis Monitor* respectively.

<i>This field...</i>	<i>indicates...</i>
Client IP	The IP address of the client.
ServerIP	The IP address of the server. This is a hyperlink. Click to go to

This field...	indicates...
	<i>Server Infra Monitor.</i>
Status	The error code. This is a hyperlink. Click to go to <i>HTTP Session Analysis Monitor</i> .
Host Name	The IP address of the host.
<u>URL</u>	The URL in the conversation that is experiencing the worst response time. This is a hyperlink. Click to go to APM dashboard/monitor.
S-Port	The server port number.
C-Port	The client port number.
Status Description	Description of the status of the connection.
C-Traffic	The volume of incoming traffic at the client.
S-Traffic	The volume of outgoing traffic at the server.
Avg Response Time	The average response time in microseconds.
#Trans	The number of transmissions.

Table 23. Top 50 HTTP Conversations by worst response time

End User Experience & Connection Statistics - table

This table has specific details about connection statistics. End user experience is a significant part of these statistics.

This field...	indicates...
ClientIP	The IP address of the client.
ClientHostName	The IP address of the host (client)
ServerIP	The IP address of the server.
ServerHostName	The IP address of the host (server)
C-Port	The server port number.
S-Port	The client port number.
NRT	The network response time in microseconds.
CRT	The client response time in microseconds.
SRT	The server response time in microseconds.
ART	The average response time in microseconds.
EURT	The end user response time in microseconds – this is the sum of the above 4 response times, indicating the latency experienced by the user.
ServerTraffic	The volume of incoming traffic at the server.
ClientTraffic	The volume of outgoing traffic at the client.

This field...	indicates...
C-ReTrans	The number of retransmissions by the client.
S-ReTrans	The number of retransmissions by the server.
#Conn	The number of connections in each conversation.

Table 24. End User Experience & Connection Statistics

Cyber-Threat-Monitor

The cyber threat monitor supports proactive monitoring of all ongoing cyber threats inside your network. It displays the threats according to threat categories. Under each category the cyber threat monitor also reveals methods used by threat actors to spread those threats inside the network.



Figure 18. Cyber Threat Monitor Default Panels (part 1)

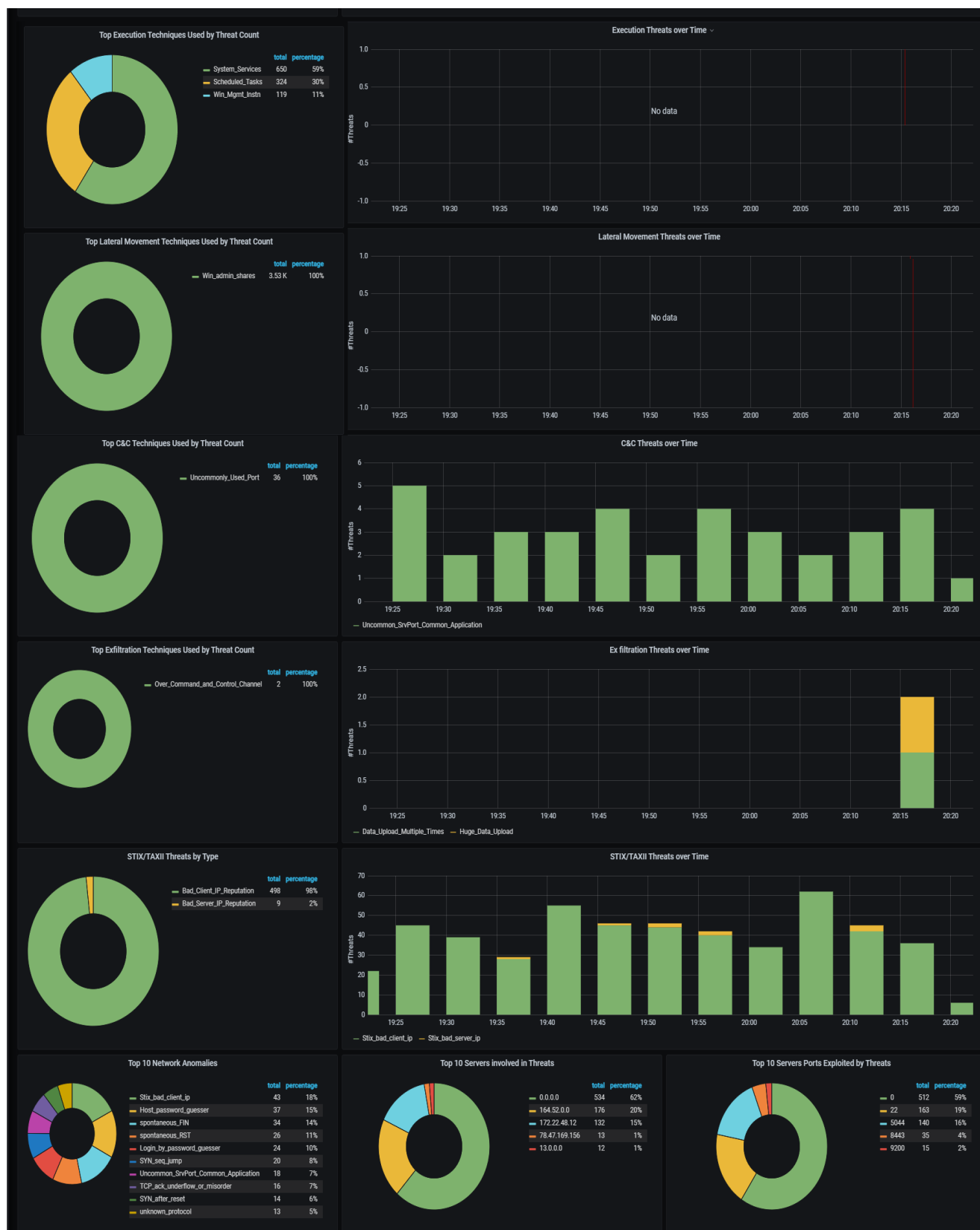


Figure 19. Cyber Threat Monitor Default Panels (part 2)

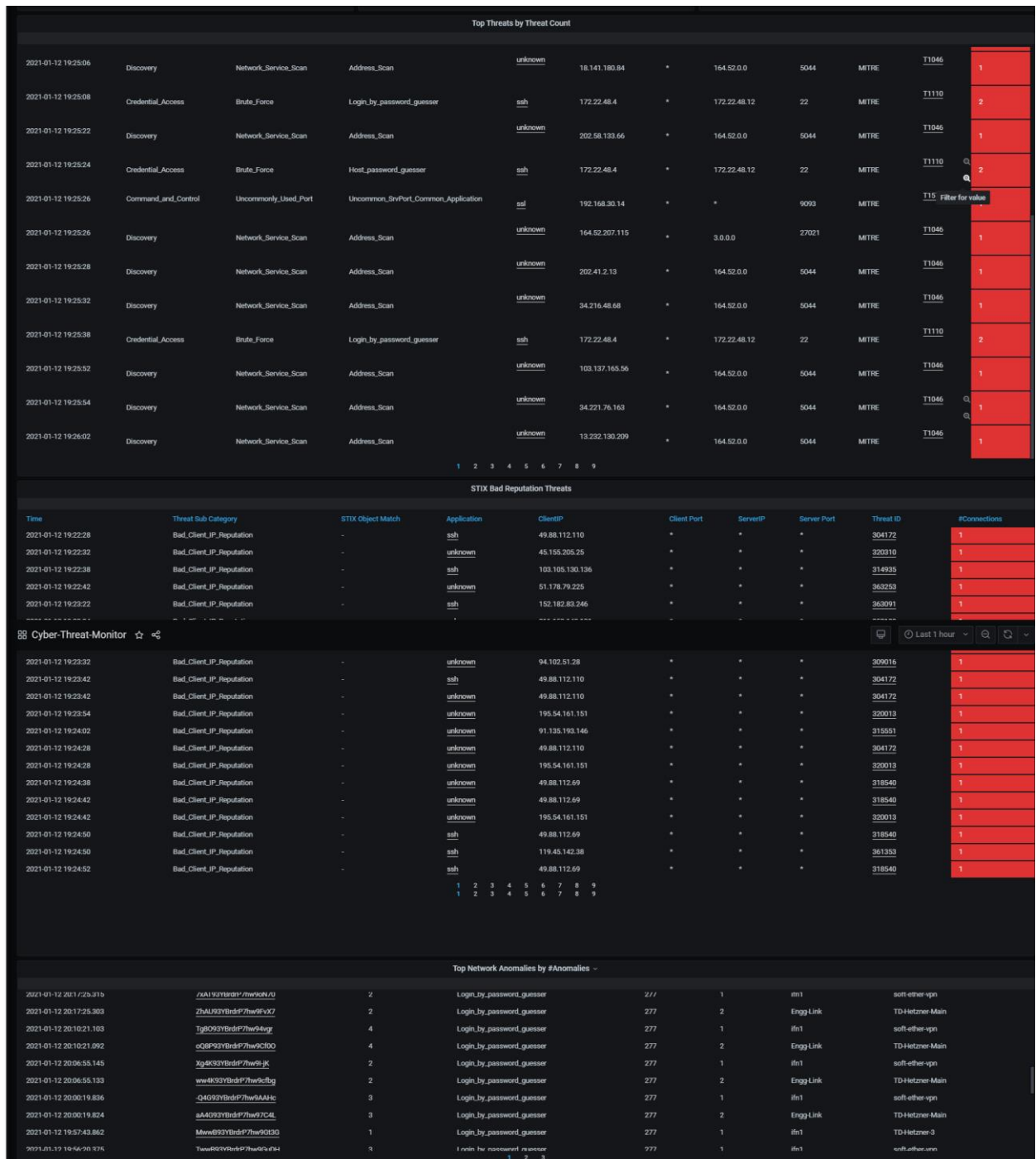


Figure 20. Cyber Threat Monitor Default Panels (part 3)

This is a multi-part display of contextual panels with multiple genres of cyber threat related information. Each part in this dashboard pertains to a specific context and has 2 or more panels. These panels list each threat, the time of its detection and provide drilldown-links into specific application monitors for users to perform investigation on each cyber threat to identify the impact of the threat

- number of systems involved in the threat

The cyber threat monitor:

- exposes weak points in your network exploited by threat actors and provides information to take corrective actions to plug the security loop holes in your network.
- provides STIX/TAXII based detected threats and investigation for bad reputation IP, DNS and HTTP URL connections ongoing in the network.

What are Cyber Threats

Multiple categories of cyber threats can affect any network. The following table describes the threat categories and examples.

<i>Threat category</i>	<i>Description</i>
Initial Access	<p><i>Initial access</i> attempts are actions by hackers to gain initial entry into a network. Techniques used to gain entry include targeted spear phishing and using weaknesses in public-facing web servers.</p> <p>By obtaining access to valid accounts and use of external remote services, these entries may allow the hacker continued use, or due to changing passwords the entries may be of limited-use only.</p>
Credential Access	<p>These are attempts to steal credentials like account names and passwords. Techniques used to get credentials include keylogging or credential dumping.</p> <p>Once they obtain legitimate credentials hackers get access to systems, become hard to detect, and easily create multiple accounts to achieve their objective.</p>
Command & Control	<p>Techniques used to communicate with systems in a victim-network include mimicking normal, expected traffic to avoid detection.</p> <p>Establishing command and control with various levels of stealth takes into account the victim-network's structure and defenses.</p> <p>For example, when an end-user clicks a suspicious link in a phishing email a ransomware could get installed without the user's knowledge and a command control incident could be triggered.</p>
Discovery	<p>This is a post-compromise stage. The objective is information-gathering. In this stage of cyber-threat the attacker tries to figure out the environment before taking action. Their plan would be to</p> <ul style="list-style-type: none"> - get an idea of what is close to the entry point - understand how it could benefit their objective. <p>Native operating system tools are often used for getting information. For example when the auto-installed ransomware gets auto-invoked it starts discovering the contents of the local computer or network system.</p>
Execution	<p>Execution techniques that run malicious code are often paired with techniques from all other tactics to achieve broader goals, like</p>

Threat category	Description
	<p>exploring a network or stealing data.</p> <p>For example, a remote access tool can be used to run a <i>PowerShell script</i> that performs <i>Remote System Discovery</i>.</p>
Lateral Movement	<p><i>Lateral movement</i> techniques are used to:</p> <ul style="list-style-type: none"> - explore, find the target network - enter and control remote systems on the target network - move through its multiple systems - gain access to accounts. <p>Attackers may install their own remote access tools or use the stealthier method of using legitimate credentials with native network and operating system tools.</p>
Exfiltration	<p>In this stage of the attacker is attempting to steal data.</p> <p>Exfiltration techniques that may be used to steal data out of a target network typically include</p> <ul style="list-style-type: none"> - transferring it over their command and control channel or - an alternate channel and may also include putting size limits on the transmission. <p>The attacker packages the collected data to avoid detection while removing it by compression and encryption.</p>

Table 25.Cyber Threats

Top Sites, Total Cyber threats and Events

This graph...	Shows...
Top Sites Impacted by Cyber Threats	<p>When the administrator has configured sites with geo co-ordinates, this panel shows hot-spots of the sites impacted by cyber threats.</p> <p>Mouse over these hot-spots to see the threat type and number in that site.</p>
Total Cyber Threats	<p>This panel displays the number of each of the following 7 threat types, in the network.</p> <ul style="list-style-type: none"> - Command & Control, - Credential Access - Discovery, - Execution - Exfiltration - Initial Access, - Lateral Movement.
STIX/TAXII Bad Reputation Threats	<p>This panel displays the STIX/TAXII (Structured Threat Information eXpression/Trusted Automated eXchange of Intelligence Information), description of the cyber threats on:</p> <ul style="list-style-type: none"> - Client IPs – DNS - Server IPs - URLs - Network Anomalies - #Hosts -#Servers

<i>This graph...</i>	<i>Shows...</i>
CyberThreat Events	<p>STIX represents the informational part of threat intelligence, while TAXII defines how that information is relayed.</p> <p>This panel is for use by the administrator to set cyber threat related Alerts.</p> <p>Alerts are not part of the default workflow. They are set by users in the "admin" role. See "Creating Alerts".</p>

Table 26.Part 1 - Top Sites, Total Cyber threats and Events

Top Hosts involved, Top Threat types and Over-time graphs

<i>This graph...</i>	<i>Shows...</i>
Top 10 Hosts involved in Threats	<p>This panel gives a graph view of the 10 hosts in the network that have the highest number of threats.</p> <p>Every host's IP address, total threats and percentage threats.</p>
Threats by Phases over Time	The time-line graph indicates how the threats acted on the top 10 over time. Mouse over the bars in the chart to get a quick view of the time-line of the attacks.
<i>Initial Access:</i> Top Initial Access Techniques Used by Threat Count	This panel gives a graphic view of the <i>initial-attacks</i> techniques that have the highest incidence, the number and percentage of each of them.
Initial Access Threats over Time	The time-line graph indicates how these threats occurred over time. Mouse over the bars in the chart to get a quick view of the time-line of the threats.
<i>Credential Access:</i> Top Credential Access Techniques Used by Threat Count	This panel gives a graphic view of the <i>credential access</i> techniques that have the highest incidence, their number and percentage of each of them.
Credential Access Threats over Time	The time-line graph indicates how these threats occurred over time. Mouse over the bars in the chart to get a quick view of the time-line of the threats.
<i>Discovery Techniques:</i> Top Discovery Techniques Used by Threat Count	This panel gives a graphic view of the <i>discovery techniques</i> that have the highest incidence, the number and percentage of each of them.
Discovery Threats over Time	The time-line graph indicates how these threats occurred over time. Mouse over the bars in the chart to get a quick view of the time-line of the threats.

Title	Purpose
Execution Techniques: Top Execution Techniques Used by Threat Count	Gives a graphic view of the <i>discovery</i> techniques that have the highest incidence, the number and percentage of each of them.
Execution Threats over Time	The time-line graph indicates how these threats occurred over time. Mouse over the bars in the chart to get a quick view of the time-line of the threats.
Lateral Movement: Top Lateral Movement Techniques Used by Threat Count	Gives a graphic view of the <i>Lateral movement</i> techniques that have the highest incidence, the number and percentage of each of them.
Lateral Movement Techniques over Time	The time-line graph indicates how these threats occurred over time. Mouse over the bars in the chart to get a quick view of the time-line of the threats.
C&C : Top C&C Techniques Used by Threat Count	Gives a graphic view of the <i>Command & Control</i> (C&C) techniques that have the highest incidence, the number and percentage of each of them.
C&C Threats over Time	The time-line graph indicates how these threats occurred over time. Mouse over the bars in the chart to get a quick view of the time-line of the threats.
Exfiltration: Top Exfiltration Techniques Used by Threat Count	Gives a graphic view of the <i>ex-filtration</i> techniques that have the highest incidence, the number and percentage of each of them.
Ex filtration Threats over Time	The time-line graph indicates how these threats occurred over time. Mouse over the bars in the chart to get a quick view of the time-line of the threats.
STIX/TAXII: STIX/TAXII Threats by type	Gives a graphic view of the <i>STIX/TAXII</i> techniques that have the highest incidence, and the type of these techniques.
STIX/TAXII Threats over Time	The time-line graph indicates how these threats occurred over time. Mouse over the bars in the chart to get a quick view of the time-line of the threats.

Table 27. Part 2 - Top Hosts involved, Top Threat Types and Numbers

Note: See "[What are Cyber Threats](#)" for the names and description of threat types.

Top 10 graph panels

<i>This graph...</i>	<i>shows...</i>
Top 10 Network Anomalies	a graphic view of of the 10 network anomalies that show the highest incidence in the network. The anomalies are listed with the total number of each anomaly in the system and their percentage.
Top 10 Servers involved in Threats	a graphic view of of the 10 servers that are most involved in the threats. The servers are listed with the total number of threats in each of them and their percentage.
Top 10 Servers Ports Exploited by Threats	a graphic view of of the 10 server ports that are experiencing the highest exploitation by the threats. The port numbers are listed with the total number of each anomaly in the network and their percentage.

Table 28. Part 3 -Top 10 Graphs

Top Threats by Threat Count Table

This table has specific details about top threats and their numbers in the network. As a standard step, use the drill-down hyperlinks (underlined fields) to view related details.

<i>This Field...</i>	<i>indicates...</i>
Time	The date and time the threat occurred in yyyy-dd-mm hr:min:sec format.
Threat Sub Category	The type of threat. For example: C&C, Exfiltration etc.
Threat Technique Type	The type of threat technique. For example: C&C, Exfiltration etc.
Threat Description	A brief description of the threat.
Application	<p>The application affected by the threat. For example: SIP, HTTP, etc. This is a drill-down hyperlink. Click to see the application's threat details.</p> <p>If this field has the entry "unknown", it means the application is of the non-standard type. See " Change Role option</p> <p>App Definition".</p>
ClientIP	The IP address of the client affected by the threat.
Client Port	The port ID of the client affected by the threat.
ServerIP	The IP address of the server affected by the threat.
Server Port	The port ID of the server affected by the threat.
Threat Category	The category of threat. For example MITRE.
<u>Threat ID</u>	The ID of the threat. Click to see the MITRE page with details about

<i>This Field...</i>	<i>indicates...</i>
	the threat.
#Connection	The number of connections affected by the threat.

Table 29.Part 4 - Top Threats by Threat Count Table

STIX Bad Reputation Threats Table

This table has specific details about STIX Bad reputation Threats network. As a standard step, use the drill-down hyperlinks (underlined fields) to view related details.

<i>This Field...</i>	<i>indicates...</i>
Time	The date and time the threat occurred in yyyy-dd-mm hr:min:sec format.
Threat Sub Category	The type of threat. For example: C&C, Exfiltration etc.
STIX Object Match	The type of threat technique. For example: C&C, Exfiltration etc.
Application	The application affected by the threat. For example: SIP, HTTP, etc. This is a drill-down hyperlink. Click to see the application's threat details. If this field has the entry "unknown", it means the application is of the non-standard type. See " Change Role option
	App Definition".
ClientIP	The IP address of the client affected by the threat.
Client Port	The port ID of the client affected by the threat.
ServerIP	The IP address of the server affected by the threat.
Server Port	The port ID of the server affected by the threat.
Threat ID	The ID of the threat. This is a hyperlink. Click to see the MITRE page with details about the threat.
#Connection	The number of connections affected by the threat.

Table 30.Part 5 - STIX Bad Reputation Threats Table

Top Network Anomalies Table

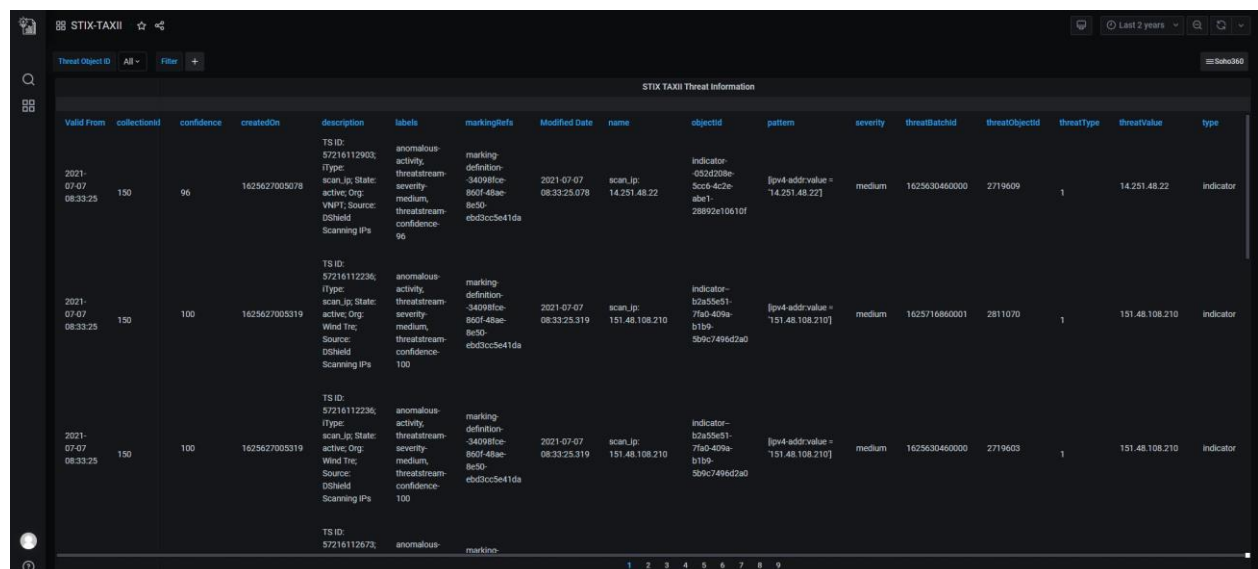
This table has specific details about anomalies that are most rampant and their numbers in the network.

<i>This Field...</i>	<i>indicates...</i>
Time	The date and time the threat occurred in yyyy-dd-mm hr:min:sec format.
Session ID	The unique number assigned to the session that is affected by the anomaly. This is a hyperlink. Click to view anomaly details.

<i>This Field...</i>	<i>indicates...</i>
Anomaly count	The number of times the anomaly occurred.
Anomaly description	The description of the anomaly. For e.g. Address scan.
anomalyId	The ID assigned to the anomaly.
interfaceId	The ID of the interface configured for the sensor.
interfaceName	Name of the interface configured for the sensor. For e.g. lfn1, eth0
sensorName	Name of the sensor that registered the anomaly.

Table 31.Part 6 - Top Network Anomalies Table

STIX-TAXII Dashboard



The screenshot shows the STIX-TAXII Dashboard interface. At the top, there's a header with 'STIX-TAXII' and a search icon. Below the header, there's a filter bar with 'Threat Object ID' and 'Filter'. The main content area is titled 'STIX TAXII Threat Information' and displays a table of threat data. The table has columns for 'Valid From', 'collectionId', 'confidence', 'createdOn', 'description', 'labels', 'markingInfo', 'Modified Date', 'name', 'objectid', 'pattern', 'severity', 'threatBatchId', 'threatObjectid', 'threatType', 'threatValue', and 'type'. The table contains three rows of data, each representing a threat object. The first row has a 'Valid From' of '2021-07-07 08:33:25', a 'collectionId' of '150', a 'confidence' of '96', a 'createdOn' of '1625627005078', a 'description' of 'anomaly-activity, threatstream-severity: medium, threatstream-confidence: 96', a 'labels' of 'anomaly-activity, threatstream-severity: medium, threatstream-confidence: 96', a 'markingInfo' of 'marking-definition: 34098f0e-860f-48ae-8c50-eb3cc5e41da', a 'Modified Date' of '2021-07-07 08:33:25.078', a 'name' of 'scan.jp', an 'objectid' of '14.251.48.22', a 'pattern' of '[ipv4-addr:value = "14.251.48.22"]', a 'severity' of 'medium', a 'threatBatchId' of '1625630460000', a 'threatObjectid' of '2719409', a 'threatType' of '1', a 'threatValue' of '14.251.48.22', and a 'type' of 'indicator'. The second row has a 'Valid From' of '2021-07-07 08:33:25', a 'collectionId' of '150', a 'confidence' of '100', a 'createdOn' of '1625627005319', a 'description' of 'anomaly-activity, threatstream-severity: medium, threatstream-confidence: 100', a 'labels' of 'anomaly-activity, threatstream-severity: medium, threatstream-confidence: 100', a 'markingInfo' of 'marking-definition: 34098f0e-860f-48ae-8c50-eb3cc5e41da', a 'Modified Date' of '2021-07-07 08:33:25.319', a 'name' of 'scan.jp', an 'objectid' of '151.48.108.210', a 'pattern' of '[ipv4-addr:value = "151.48.108.210"]', a 'severity' of 'medium', a 'threatBatchId' of '1625716860001', a 'threatObjectid' of '2811070', a 'threatType' of '1', a 'threatValue' of '151.48.108.210', and a 'type' of 'indicator'. The third row has a 'Valid From' of '2021-07-07 08:33:25', a 'collectionId' of '150', a 'confidence' of '100', a 'createdOn' of '1625627005319', a 'description' of 'anomaly-activity, threatstream-severity: medium, threatstream-confidence: 100', a 'labels' of 'anomaly-activity, threatstream-severity: medium, threatstream-confidence: 100', a 'markingInfo' of 'marking-definition: 34098f0e-860f-48ae-8c50-eb3cc5e41da', a 'Modified Date' of '2021-07-07 08:33:25.319', a 'name' of 'scan.jp', an 'objectid' of '151.48.108.210', a 'pattern' of '[ipv4-addr:value = "151.48.108.210"]', a 'severity' of 'medium', a 'threatBatchId' of '1625630460000', a 'threatObjectid' of '2719403', a 'threatType' of '1', a 'threatValue' of '151.48.108.210', and a 'type' of 'indicator'. The table is paginated with 9 pages shown at the bottom.

Figure 21. STIX-TAXII

The *STIX-TAXII Monitor* is an extension to the Cyber threat monitor. It provides Cyber Threat information received from STIX and TAXII threat feeds.

It includes all threat information about bad reputation IP, DNS and URL based threats matched inside the network.

Note: Soho360 provides integration with multiple open and commercial STIX TAXII threat feeds, Contact ThoughtData customer support to learn more about how to integrate your STIX-TAXII threat feeds to Soho360.

SSL Session Analysis Monitor

Session analysis monitors have details of each connection under the conversation, per connection. Users can check all the details when the connection occurs and all details of metrics per connection.

Note: Session Analysis monitors are available for all application based monitors, for instance: SSL session Analysis. Soho360 uses a standard user interface across all session analysis monitors. This section describes the SSL Session Analysis Monitor as an example. You can refer to this section for related details about other session analysis monitors.

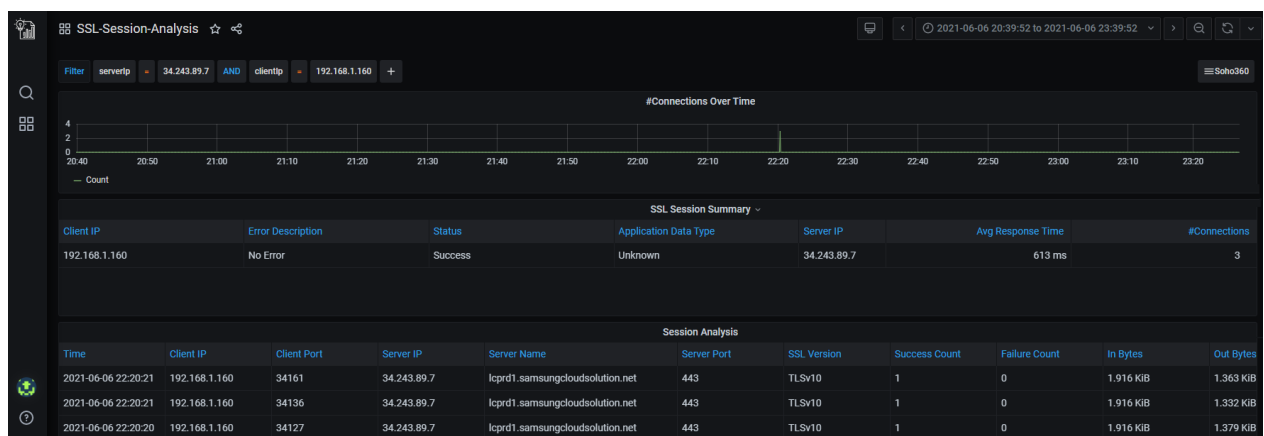
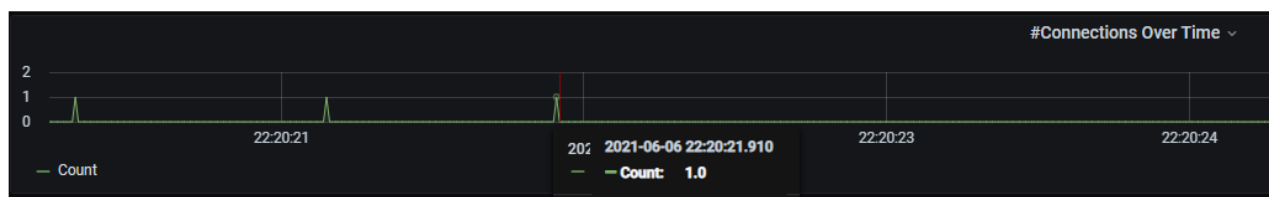


Figure 22. Unknown Monitor – default panels

This is a 3-part display of contextual panels with information related to *applications*.

- The 1st panel is an over-time graph of the number of connections.
- The 2nd is a tabular summary of sessions.
- The 3rd is a tabular presentation of the analysis details.

Connections Over-time



The graph in this panel displays the count of connections at specific points in time. Move the mouse on the projections in the graph to see related details.

SSL Session Summary

SSL Session Summary ▾						
Client IP	Error Description	Status	Application Data Type	Server IP	Avg Response Time	#Connections
192.168.1.160	No Error	Success	Unknown	34.243.89.7	613 ms	3

This table is a summary of the Client connections in the selected conversation. The details are self-explanatory.

Session Analysis

Time	Client IP	Client Port	Server IP	Server Name	Server Port	SSL Version	Success Count	Failure Count	In Bytes	Out Bytes
2021-06-06 22:20:21	192.168.1.160	34161	34.243.89.7	lcprd1.samsungcloudsolution.net	443	TLSv10	1	0	1.916 KiB	1.363 KiB
2021-06-06 22:20:21	192.168.1.160	34136	34.243.89.7	lcprd1.samsungcloudsolution.net	443	TLSv10	1	0	1.916 KiB	1.332 KiB
2021-06-06 22:20:20	192.168.1.160	34127	34.243.89.7	lcprd1.samsungcloudsolution.net	443	TLSv10	1	0	1.916 KiB	1.379 KiB

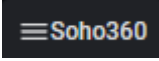
This table is has entries for each server connected to the Client in the selected conversation. The analytical details are self-explanatory.

Soho360 User Interface - options and features

Soho360's user interface includes a pre-designed set of monitoring and session analysis workflows to help the network administrator in home/small-business networks to troubleshoot network incidents.

These workflows cover the entire gamut of known and frequently occurring network events. You can speed up responding to network-events using these out-of-box investigation workflows for most common applications/protocols like:

- Cyber Threat • DHCP • HTTP • RDP • SMB • SSL
- Certificates • DNS • ICMP • RPC • SMTP
- DCE • FTP • NTLM • SIP • SSH

On clicking  at the top right of the landing page (Real time monitoring) dashboard page, the list of built-in workflows is displayed.

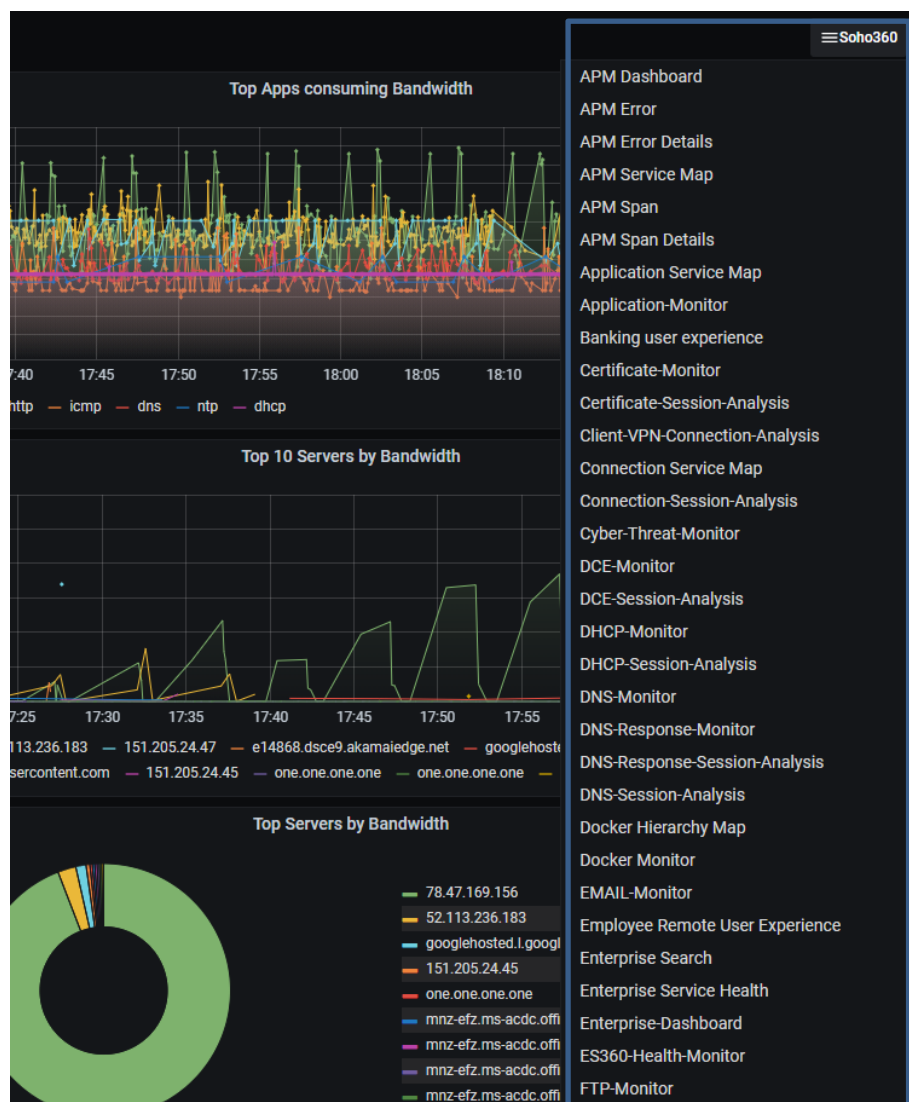


Figure 23. The Soho360 Dashboard – list of out-of-the-box workflows

Click to select any of the dashboards to view how related entities from various databases interact to present a comprehensive view of the status of the Soho360 network over the selected time frame.

The user interface in these dashboards, has standard features and options for user interaction. The sections below describe how to use the elements of the user interface.

Left Menu pane



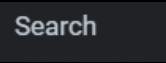

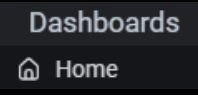

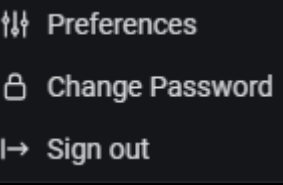

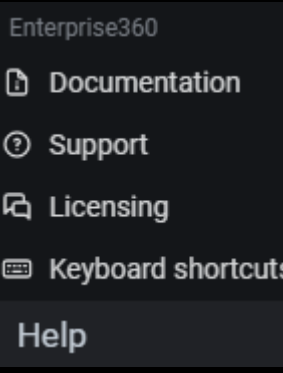


Option	Sub Options(tasks)	User Type...	Use to...
		All users	Go to the Soho360 Home Dashboard. Also known as the landing page.
		All users	Search/locate dashboards saved in the system.
	 Dashboards Home	All users	Return to the home dashboard if you have navigated to any other dashboard.
	 Preferences Change Password Sign out	All users	Set your user preferences. Change password. Sign out of Soho360. Note: This is the logged-in user's menu.
	 Enterprise360 Documentation Support Licensing Keyboard shortcuts Help	All users	All roles can use options in this menu for online help and other useful details.

Table 32.Left-pane Options, Tasks and Roles

While most options here are click-to-go and self-explanatory, note the following while using the logged in user's menu from the left menu option - .

Preferences

Step 1. Click  (user) > Preferences as illustrated below.

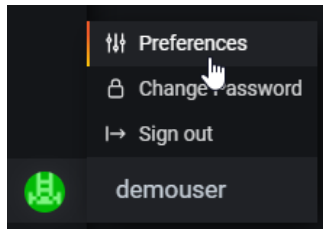


Figure 24. Set Preferences

Preferences > Edit Profile

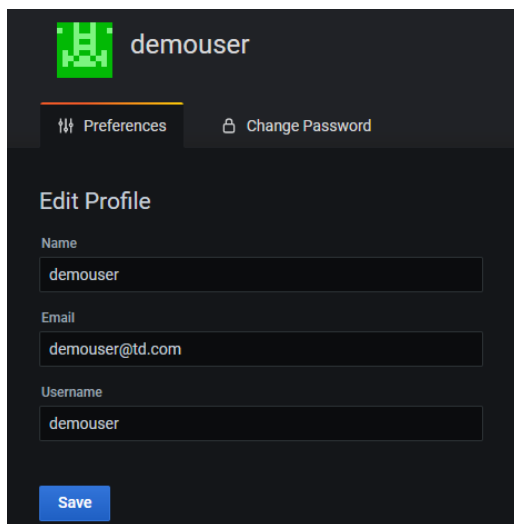
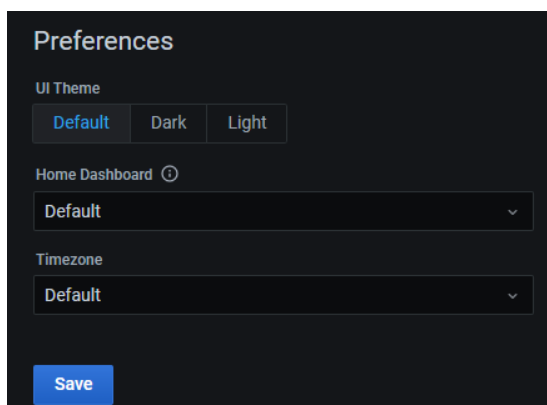
The 'Edit Profile' form is displayed on a dark background. At the top, there is a green user icon and the name 'demouser'. Below this are two tabs: 'Preferences' (active) and 'Change Password'. The 'Edit Profile' section contains three text input fields: 'Name' with 'demouser', 'Email' with 'demouser@td.com', and 'Username' with 'demouser'. A blue 'Save' button is at the bottom left.


Figure 25.

Step 2. In the "Edit Profile" section retain the entries as they are. **Do not make any changes.**

Preferences > UI Theme, Home Dashboard, TimeZone

The 'Preferences' form is shown. It has a title 'Preferences' at the top. Below it are three sections: 'UI Theme' with three buttons ('Default', 'Dark', 'Light'), 'Home Dashboard' with a dropdown menu set to 'Default', and 'Timezone' with a dropdown menu set to 'Default'. A blue 'Save' button is at the bottom left.

Step 3. In the "UI Theme" section, retain the default selection. **Do not change it.**


Step 4. In the "Home Dashboard" section click the drop-down icon  to view the list of dashboards and click to select any preferred name from the drop-down list.

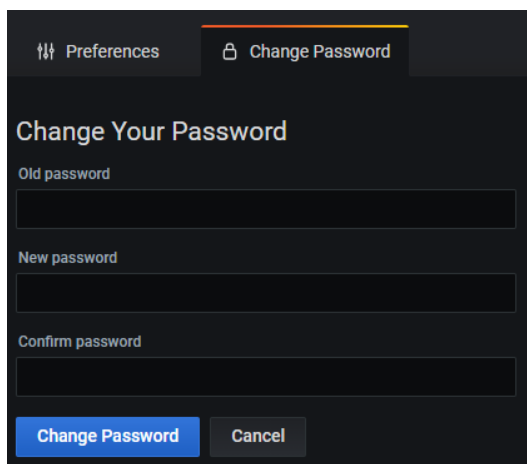
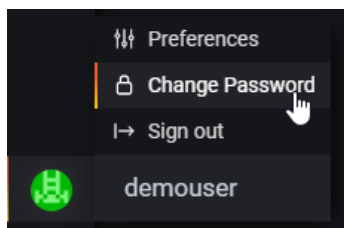
Step 5. Click .

Note the indicator 

Step 6. In the "Timezone" section. Retain the default selection. **Do not change it.**

Change Password

Step 7. Click  (user) > Change Password.

The 'Change Your Password' form is displayed. It has three input fields: 'Old password', 'New password', and 'Confirm password'. At the bottom, there are two buttons: 'Change Password' (highlighted in blue) and 'Cancel'.

Step 8. Do as directed below in the 3 fields:

- In the "Old Password" box, type your current password.
- In the "New Password" box, type a new password. Make sure it is a strong password.
- In the "Confirm Password" box re-type the strong password you entered in the above step.
- Click "Change Password" to save the new password. Click "Cancel" if you do not wish to save the change and continue to use your current password.

Filter Options

Every workflow presents a filter at the top of display with items relevant to that work flow. Use them to filter for the data of your choice. For instance in case of the "Application Monitor", the filter drop-down lists cover all data related to Apps running on the machines in the network.

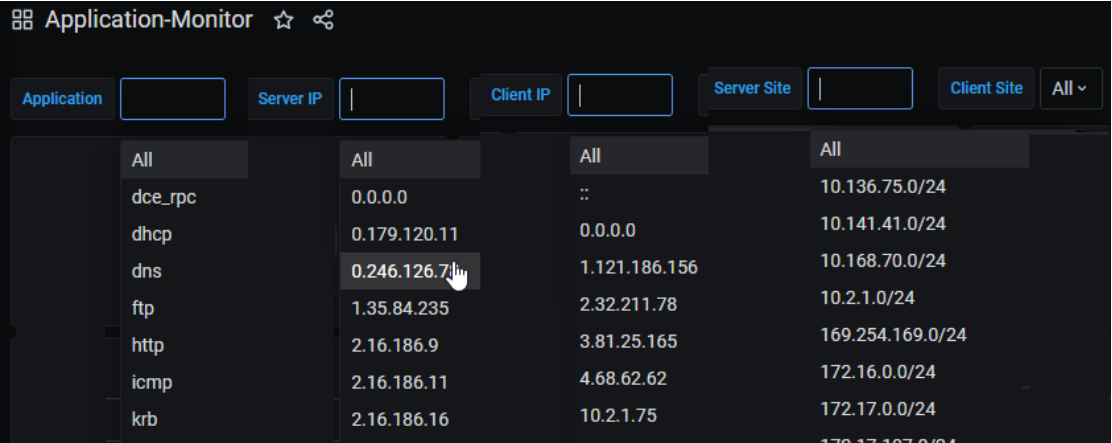
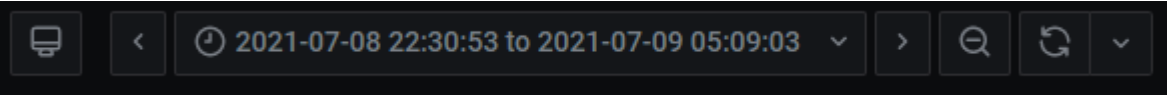


Figure 26. Sample Filters

Click to select any of the items in the lists and see how the data presentation changes to match the selection.

Top menu options



Option	Action
	Cycle view mode /Kiosk view mode
	<p>Select and apply time range for the panels of the dashboard</p> <div><div><p>Absolute time range</p><p>From</p><p>now-1h</p><p>To</p><p>now</p><p>Apply time range</p><p>It looks like you haven't used this timer picker before. As soon as you enter some time intervals, recently used intervals will appear here.</p><p>Read the documentation to find out more about how to enter custom time ranges.</p></div><div><p>Relative time ranges</p><p>Last 5 minutes</p><p>Last 15 minutes</p><p>Last 30 minutes</p><p>Last 1 hour ✓</p><p>Last 3 hours</p><p>Last 6 hours</p><p>Last 12 hours</p><p>Last 24 hours</p><p>Last 2 days</p><p>Last 7 days</p></div><div><p>Browser Time IST</p><p>UTC+05:30</p><p>Change time zone</p></div></div>
or Ctrl-z.	<p>Time-range, Zoom out.</p> <p>Click to return to minimized view after zooming-in to a time-range in a graph.</p>
	<p>Refresh the dashboard – set time for refresh or set option “off” for no refresh.</p> <div><div><p>Off</p><p>5s</p><p>10s</p><p>30s</p></div><div><p>1m</p><p>5m ✓</p><p>15m</p><p>30m</p></div><div><p>30m</p><p>1h</p><p>2h</p><p>1d</p></div></div>

Table 33.Top-menu options

Graphs

All dashboards contain graphs that match the troubleshooting workflows relevant to each dashboard. The 3 default graph types in the dashboards are:

- overtime and trend views
- Snapshot views
- Snapshot total but no distribution views

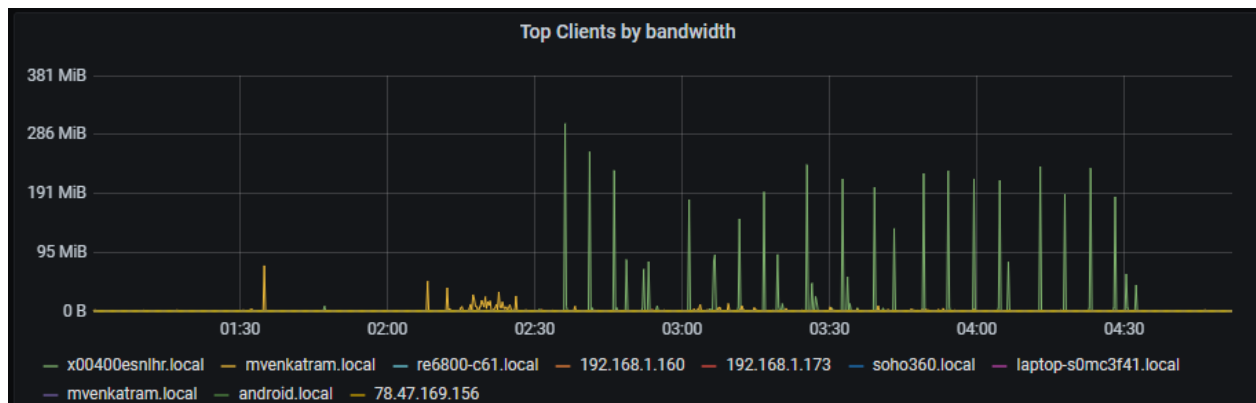


Figure 27. Trend View

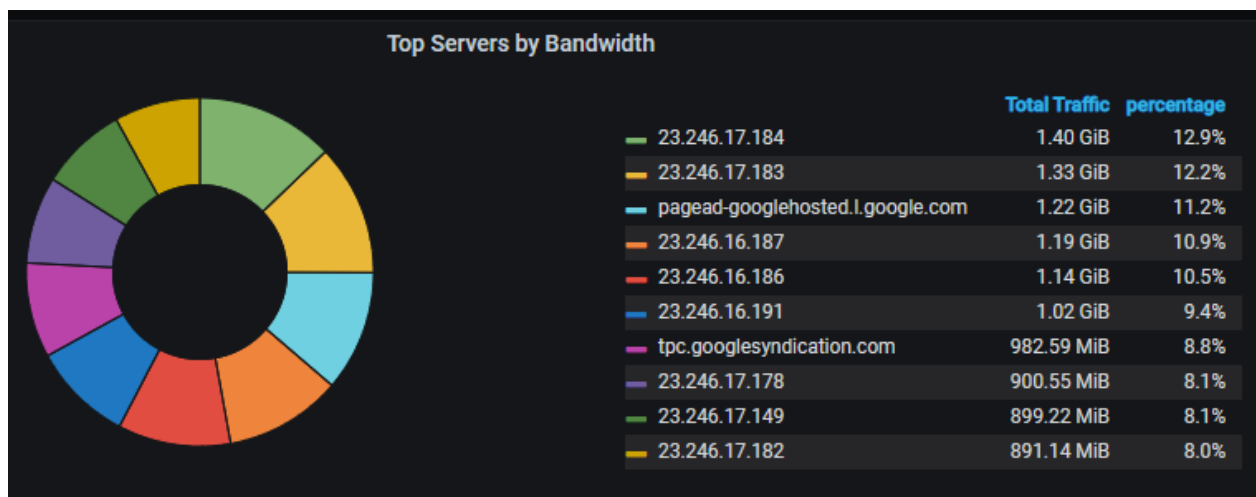


Figure 28. Snapshot view

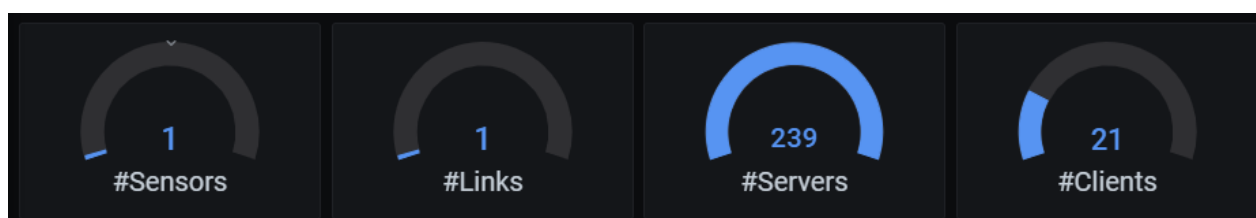


Figure 29. Snapshot total but no distribution view

These varied views help users understand and interpret the data for easier troubleshooting.

Zoom-in to Trending and Over-time Graphs

Across all dashboards, you can get a clearer time-range view of trending and over-time Graphs using the following step:

Step 1. Left-click and drag the mouse to the left or right in any graph, as illustrated below.

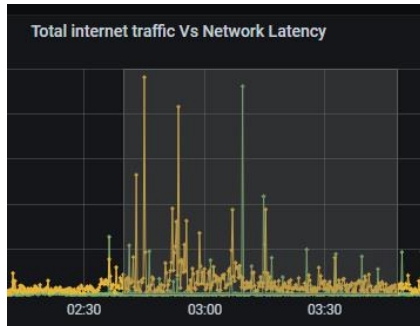
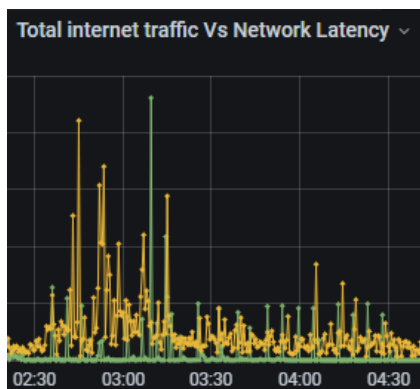


Figure 30. Zoom-in to time-ranges in the dashboard.

The graph zooms-in to the selected time range, as illustrated below.



Note: When you zoom-in to expand one graph for a selected time-range in the dashboard, all the graphs auto-zoom-in to display the expanded view.

Once zoomed-in, the expanded view of the graphs remains on display. To return to the default display, click the top menu option.



or Ctrl-z.

Dashboard Settings

Figure 31. Dashboard Settings

Apply time range

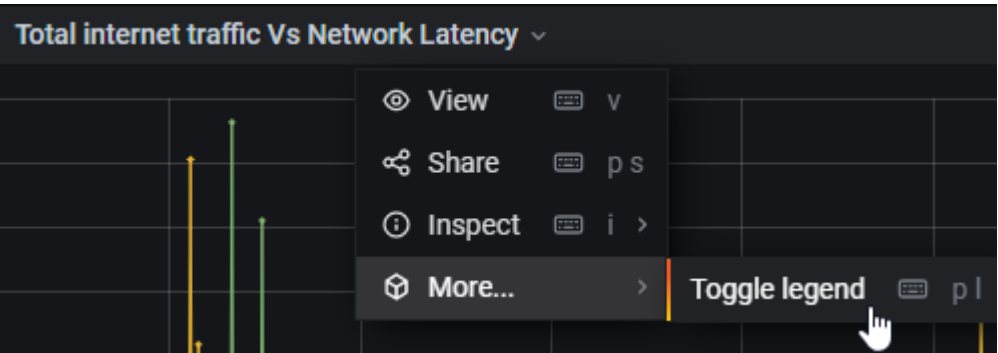
Figure 32. Time Range

Extended data display





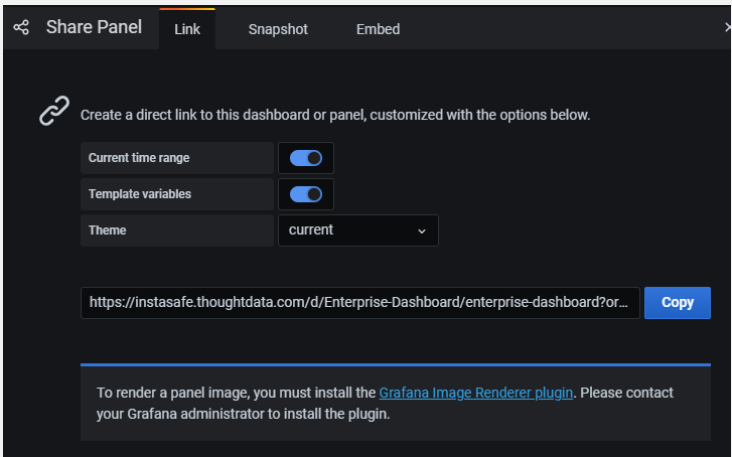
Each of these panels includes the options to View, share and inspect data in each panel. Click the drop-down menu option to see the options and click to select one.

Panel Menu

Each panel has options that allow users to drill deeper and get pin pointed views of the data described by the panel name.



Click the panel drop-down menu as illustrated, for the view, share, and inspect options. Use the icon or the key illustrated in the menu for the related option.

Click or type...	For...
 View or  v	The selected panel to be exclusively displayed.
 Share or  p s (both keys simultaneously)	The Share panel with the 3 options for sharing the Panel as a Link, a Snapshot or as an embedded web-resource. The pop-up options for these are self-explanatory as illustrated below and easy to use.
	

Click or type...

For...

Share Panel

Link

Snapshot

Embed

A snapshot is an instant way to share an interactive dashboard publicly. When created, we **strip sensitive data** like queries (metric, template and annotation) and panel links, leaving only the visible metric data and series names embedded into your dashboard.

Keep in mind, your **snapshot can be viewed by anyone** that has the link and can reach the URL. Share wisely.

Snapshot name

Enterprise-Dashboard

Expire

Never

You may need to configure the timeout value if it takes a long time to collect your dashboard's metrics.

Timeout (seconds)

4

Local Snapshot

Cancel

Share Panel

Link

Snapshot

Embed

Current time range

Template variables

Theme

current

The html code below can be pasted and included in another web page. Unless anonymous access is enabled, the user viewing that page need to be signed into grafana for the graph to load.

<iframe src="https://instasafe.thoughtdata.com/d-solo/Enterprise-Dashboard/enterprise-dashboard?orgId=1&refresh=5m&var-applicationDescription=All&var-serverIp=All&var-clientIp=All&var-serverSite=All&var-clientSite=All&var-sensorName=All&var-interfaceName=All&from=1611000160558&to=1611003760558&panelId=45" width="450" height="200" frameborder="0"></iframe>

Inspect

or i

The Inspect panel with the 3 options for Data, Statistics and JSON views of the Panel. The pop-up options for these are self-explanatory as illustrated below and easy to use.

Inspect: Top Enterprise Client Sites by Highest Traffic Volume

1 queries with total query time of 1 s

Data

Stats

JSON

Download CSV

clientSite	clientGeo	Sum
Hetzner Cloud Service	u0y	6254
TD VPN Service	thr	31182
Instasafe-AWS	te7	5998
Internet	pg2	682822
NewYork	dr5	0

More...

Toggle legend

Hand cursor icon

Toggling the legend in the selected graph panel.

ThoughtData confidential

76

Click or type...	For...
Or pl	Click once to remove it from the display click again to have it back on display.

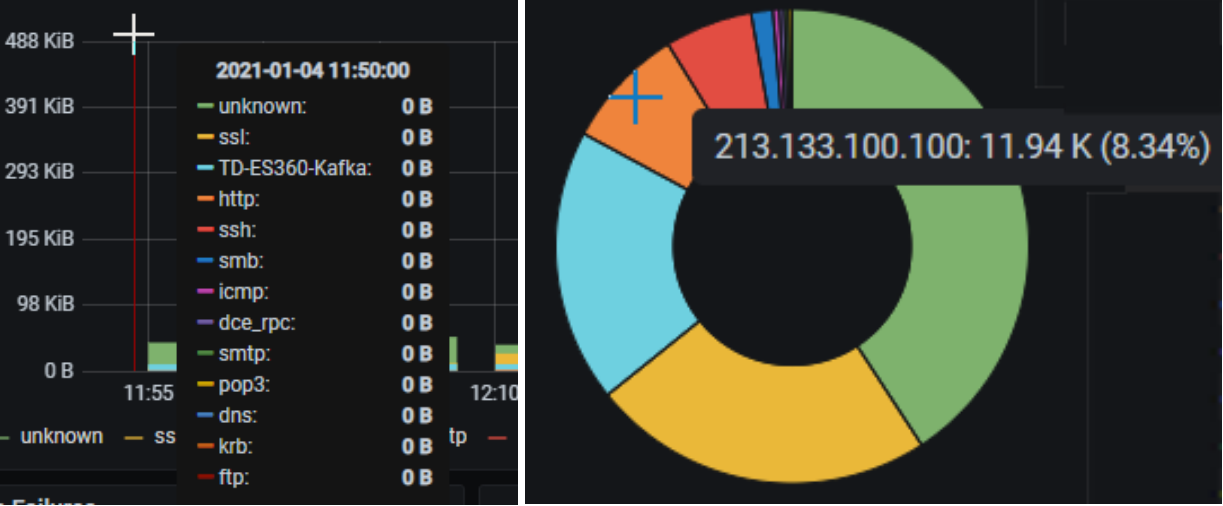


Figure 33. Hover over the graphs, pie-charts for graphical data

Edit Panel

Refer to "

Top menu options" for details about adding/editing panels.

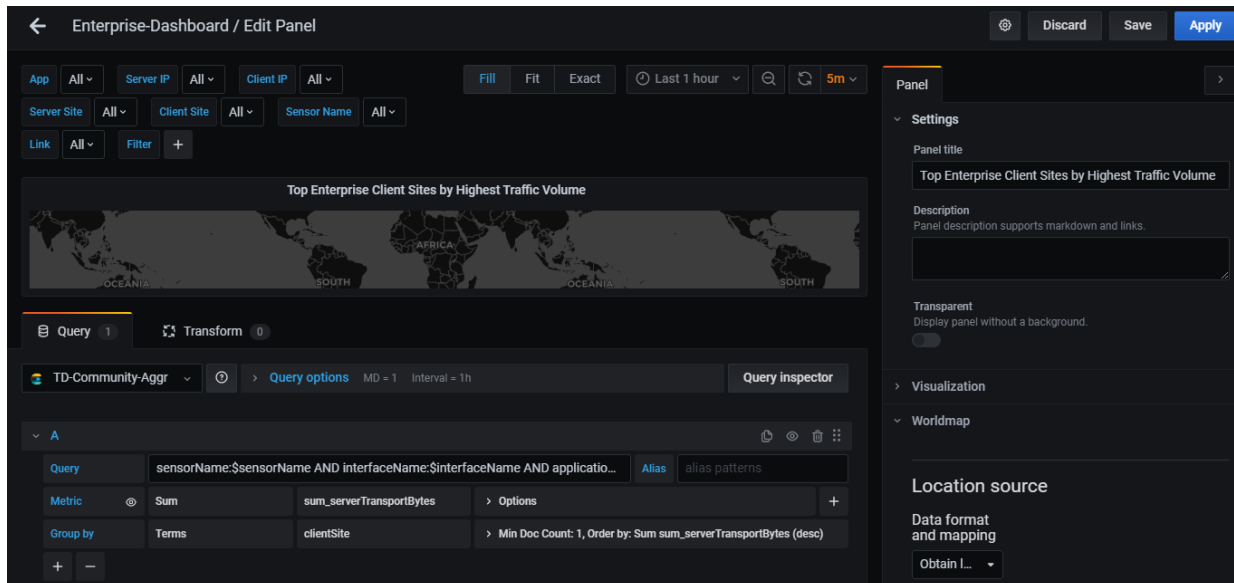
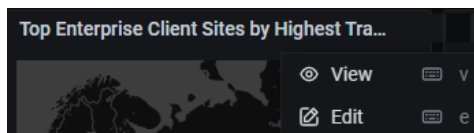


Figure 34.

Only Users in the Admin role can avail of the utilities described in the previous sections to

- make changes to the built-in workflows described in the rest of this section.
- create their own workflows and personalize their dashboards after gaining sufficient familiarity with the:
 - data sources
 - features of both Soho360 and the ThoughtData platform.

Miscellaneous Workflows

Soho360's built-in (out of the box) dashboards provide workflows that help users monitor their home or small-business networks and troubleshoot whenever there is a problem.

The default landing page represents the most important dashboard for home and small-business networks - the Real Time Internet Monitoring dashboard. See [Figure 2](#) for a compact view of the "Real Time Internet Monitoring" dashboard.

The following sections provide an overview of the workflow-dashboards. Each dashboard is a multi-part display of related information. Each part of the dashboard is actually a use-case pertaining to a specific context related to the network, with drilldown options for more data that can be used in troubleshooting. The display-parts are named to indicate their contents.

Note: *The dashboards are organised in alphabetical order and not in any order of importance.*

Certificate-Monitor

The certificate monitor provides a comprehensive workflow to solve SSL related certificate issues in the network.



Figure 35. Certificate Monitor - Default Panels

Secure web servers use SSL certificates for their operation. SSL certificates:

- can be issued as self-signed or signed by a proper certificate authority.
- SSL certificates are set with an expiry date.

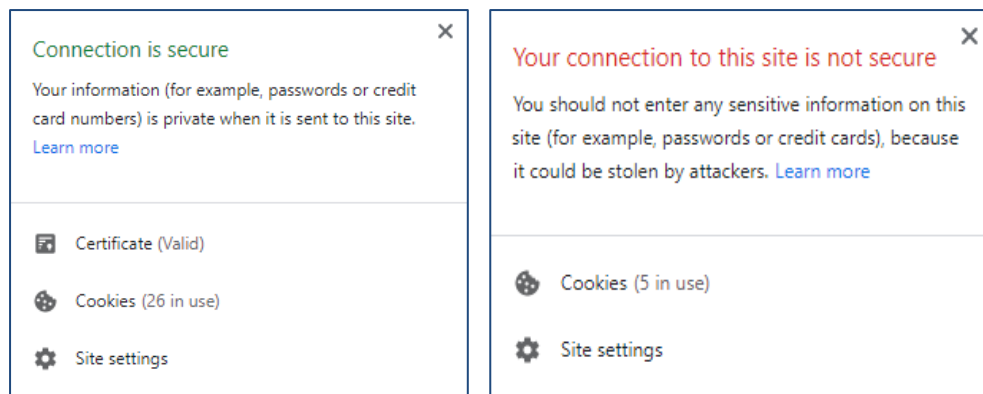


Figure 36. Sample Apps - with valid certificate and with a self-signed (invalid) certificate

Web administrators need to

- be aware of secure servers running untrusted or self-signed certificates in the network and take corrective actions to improve the security of web servers.
- keep track of which web server certificates are expiring or expired and take corrective actions to fix the web servers.

Failure to renew certificates on time will render the server inaccessible to dependent servers leading to service disruption for end users.

The *Certificate monitor* helps users to troubleshoot all aspects of SSL certificates in a network.

The following sections describe each chart in the panels of this monitor.

The Top Graphs and Alerts

This panel displays the number of applications across categories of certification running in the client and server nodes of the network. The gauge-graph displays the total number of apps whose certificates are in one of the following 5 categories, across the network.

Label...	Number of apps in the network with...
#Untrusted	"untrusted" certificates.
#SelfSigned	"self-signed" certificates.
#Expired	"expired" certificates.
#Expiring in 30 days	certificates that will "expire" in the next 30 days.
#Not yet activated	certificates are yet to be activated.

Alerts

At the initial instance of usage this panel would be empty. Alerts are created and configured by users in the "admin" role for tracking trends over-time. Once they are defined, alerts created to track certificate status are displayed in this panel. See "[Creating Alerts](#)" for details.

The Graph Panels 1 to 3

These are graph panels that display information about certificates and their status in the network.

Title	To give at one glance...
Certificates with Days to Expiry	The current state of validity of certificates. The color coding in green/amber/red gives a clue to the administrators. Green items can wait while the red ones would be due for renewal.
Top Servers with Expired Certificates	To give a tabular view of the servers with "expired" certificates. Details include: the server IP address, Issuer name, Owner and the number of certificates in that state.

Table : Part 1

Title	To give at a glance...
Trusted Vs UnTrusted Certificates	The number and % view of the number of certificates issued by trusted authorities v/s the number of certificates issued by untrusted certificate authorities.
Self-Signed Certificates	The number of self-signed certificates in the system. Note: a self-signed certificate is one that is not signed by a certificate authority (CA). Such a certificate is signed by the person creating it. Though, free of cost and easy to make self-signed certificates do not provide all of the security properties that certificates signed by a CA do.

Table : Part 2

The Top 20...	To give at a glance...
Certificate Issuers	The names of the top 20 issuers of certificates. The entity that has verified the certificate's contents is termed the issuer. Some examples include: IdenTrust, DigiCert, Sectigo, GoDaddy, GlobalSign etc.
SubjectName/Certificate Owners	The names of the top 20 certificate owners. The identity of "owners" is also called the "subject".
Hosts by Expired Certificates	The IP addresses of the top 20 hosts with "expired" certificates and the number of "expired" certificates in each host.
Certificates Pending Activation	The total number of certificates pending action across the network and the percentage

Table : Part 3

The Top 50 certificates table

This table has specific details about each of the top 50 certificates in the network. As a standard step, use the hyperlinks (underlined fields) to view details in the Certificate-Session-analysis Monitor.

<i>This Field...</i>	<i>indicates...</i>
Owner	The name of the certificate-owner.
Issuer	The issuer of the certificate.
Self-Signed	If the certificate is self-signed.
Trusted	If the certificate is from a trusted source.
Days to expiry	The number of days before the certificate "expires".
Hierarchy	The certificate hierarchy. This is a structure of certificates that allows individuals to verify the validity of a certificate's issuer.
Mins to Activate	????
Host Type	The type of host in the network.
Cert Serial#	The serial number of the certificate
Expiry Date	The expiry date of the certificate.
Activate Date	The date of activation of the certificate.
Signature	The certificate's signature.
CA Serial#	The serial number chosen by the Certificate Authority.
#Servers	The number of servers.

DCE-Monitor

DCE Monitor provides comprehensive investigation into the DCE-RPC application. This dashboard is a set of panels that help you understand and troubleshoot DCE-RPC issues.



Figure 37. DCE Monitor - Default Panels

DCE-Distributed Computing environment / Remote procedure call application is primarily used over SMB protocol in Windows-based applications to invoke remote commands and actions on servers to accomplish a specified task. DCE-RPC Monitor provides visibility into all

- ongoing DCE-RPC connections in the network,
- connections resulting in errors.

Thus helping you find reasons behind the failures and troubleshoot

- latency related problems on RPC commands.
- command failures from servers.

This is a multi-part display of contextual panels with multiple genres of DCE-RPC related information. The following sections describe each chart in the panels of this monitor.

DCE Events

<i>Panel</i>	<i>Purpose</i>
Multiple graphs	<p>The graphs in this panel give at one glance a view of the following</p> <ul style="list-style-type: none"> - Avg DCE Latency - Connection Resets - #DCE Servers - #DCE Clients
Numeric displays	<p>The numbers in this panel give a quick insight into the total number of instances of the following across the network:</p> <ul style="list-style-type: none"> - DCE-RPC Failures - Total DCE Connections - Total DCE Server Traffic - Total DCE Client Traffic

Table 34.DCE Events

DCE Over-time graphs

This part of the dashboard displays the trending status of the following DCE issues at specific points in time. These graphs can be set with alerts so that users can address issues before they cause serious problems in the network.

- DCE Errors over time.
- DCE Latency Over time

DCE Traffic and operations graphs

This part shows graphs displaying:

- DCE Client v/s Server Traffic - The total client and server traffic.
- DCE Connection by end point and operation - The total number of connections – endpoints and operations.

The Top DCE Servers

This part shows

- Top DCE servers By Errors - DCE servers with the maximum errors.
- Top DCE servers By traffic - DCE servers with the maximum traffic.
- Top server sites for DCE Connections - server sites with the maximum DCE connections.

The Top DCE Clients

This part shows graphs displaying:

- Top DCE clients By Errors - DCE clients with the maximum errors.
- Top DCE clients By traffic - DCE clients with the maximum traffic.
- Top Client sites For DCE Connections - client sites with the maximum DCE connections.

TCP Connections states and DCE Named Pipes

This part shows graphs displaying:

- TCP Connection States for DCE Sessions - The state of TCP connections for DCE sessions.
- Top Named Pipes by Connections - The named pipes with highest DCE connections.

Top DCE Conversations with Errors /Worst Latency table

This table has specific details about DCE conversations that experience the worst latency and related information. Use the hyperlinks (underlined fields) to view details in the related Monitor.

<i>This Field...</i>	<i>indicates...</i>
ServerIP	The IP address of the DCE server.
ClientIP	The IP address of the DCE client.
Named Pipe	The named DCE-RPC pipe.
Server Site	The name of the server site involved in the conversation.
Client Site	The name/IP address of the client site involved in the conversation.
Status	The status of the connection involved in the conversation.
End point	The DCE endpoint resolution point involved in the conversation.
Operation	The DCE operation involved in the conversation.
Average Response time	The average response time for the connection.
#Connections	The number of DCE-RPC connections involved in the conversation.

Table 35.Top DCE Conversations with Errors /Worst Latency table

DHCP-Monitor

DHCP monitor provides comprehensive investigation into problems associated with Dynamic Host Configuration Protocol (DHCP) which is a very popular and widely used protocol for allocating dynamic IP addresses to computing nodes inside a network.

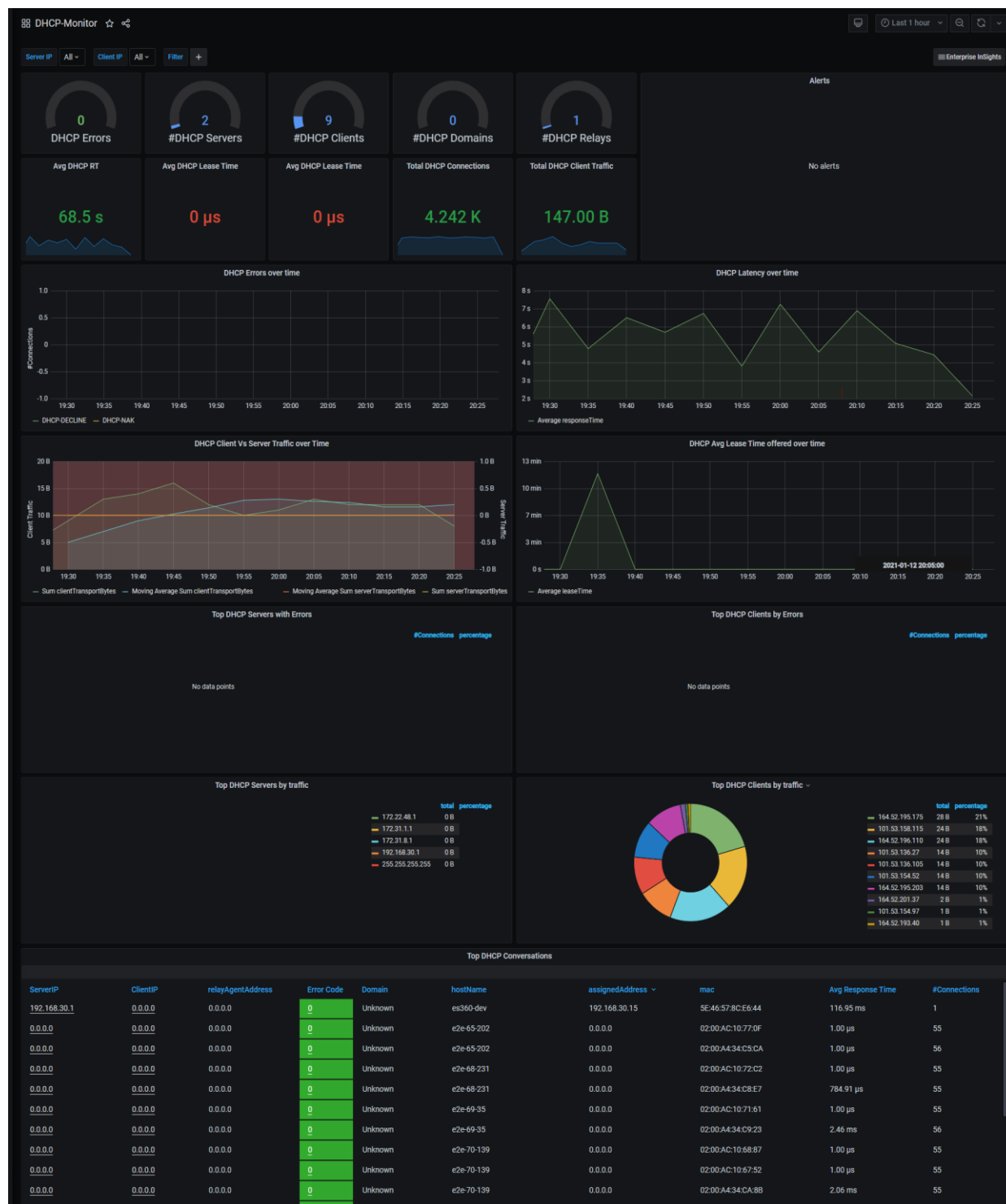


Figure 38. DHCP Monitor - Default Panels

Use this monitor to:

- troubleshoot problems related to latencies and DHCP errors while allocating IP addresses,
- manage overlapping IP pools leading to duplicate IPs in the network.
- get a better understanding of the following
 - IP pool ranges
 - DHCP servers and
 - relays working in your network and their performance.

The dashboard is a multi-part display of DHCP related information. The following sections describe each chart in the panels of this monitor.

Top DHCP

Panel...	Purpose...
DHCP panels	The graphs in this panel give at one glance a view of the following DHCP Errors - #DHCP Servers - #DCHP Clients #DHCP Domains - #DHCP Relays
Avg and total panels	The graphs in this panel give at one glance a view of the following Avg DHCP RT - Avg DHCP Lease Time Total DHCP Connections - Total DHCP Client Traffic
Alerts	At the initial instance of usage this panel would be empty. See " Creating Alerts " for details.

Table 36.Top DHCP

DHCP Over time graphs

This part of the dashboard displays the trending status of the following DHCP issues at specific points in time. These graphs can be set with alerts so that users can address issues before they cause serious problems in the network.

- DHCP errors
- DHCP Latency (average response time)
- DHCP Client v/s Server Traffic
- DHCP Avg Lease Time offered

Top DHCP Attributes

- Top DHCP Servers with Errors - Servers with maximum errors.
- Top DHCP Clients by Errors - Clients with maximum errors.
- Top DHCP Servers by traffic - Servers with maximum extent of traffic.
- Top DHCP Clients by traffic - Clients with maximum extent of traffic.

Top DHCP Conversations table

This table has specific details about DHCP conversations that are most rampant and their related data in the network. Use the hyperlinks (underlined fields) to view details in the Unknown Monitor.

<i>This field...</i>	<i>Indicates the...</i>
ServerIP	IP address of the server.
ClientIP	IP address of the client.
relayAgentAddress	IP address of the relay agent.
Error Code	number of the error code.
Domain	domain name.
hostName	name of the host.
assignedAddress	IP address assigned to the device.
mac	MAC address of the device.
Avg Response Time	average response in microseconds.
#Connections	number of connections.

Table 37.Top DHCP Conversations table

DNS-Monitor

DNS monitor provides a comprehensive dashboard for investigation into problems associated with the DNS application or protocol. This dashboard is a set of panels to help you understand and troubleshoot DNS monitoring.

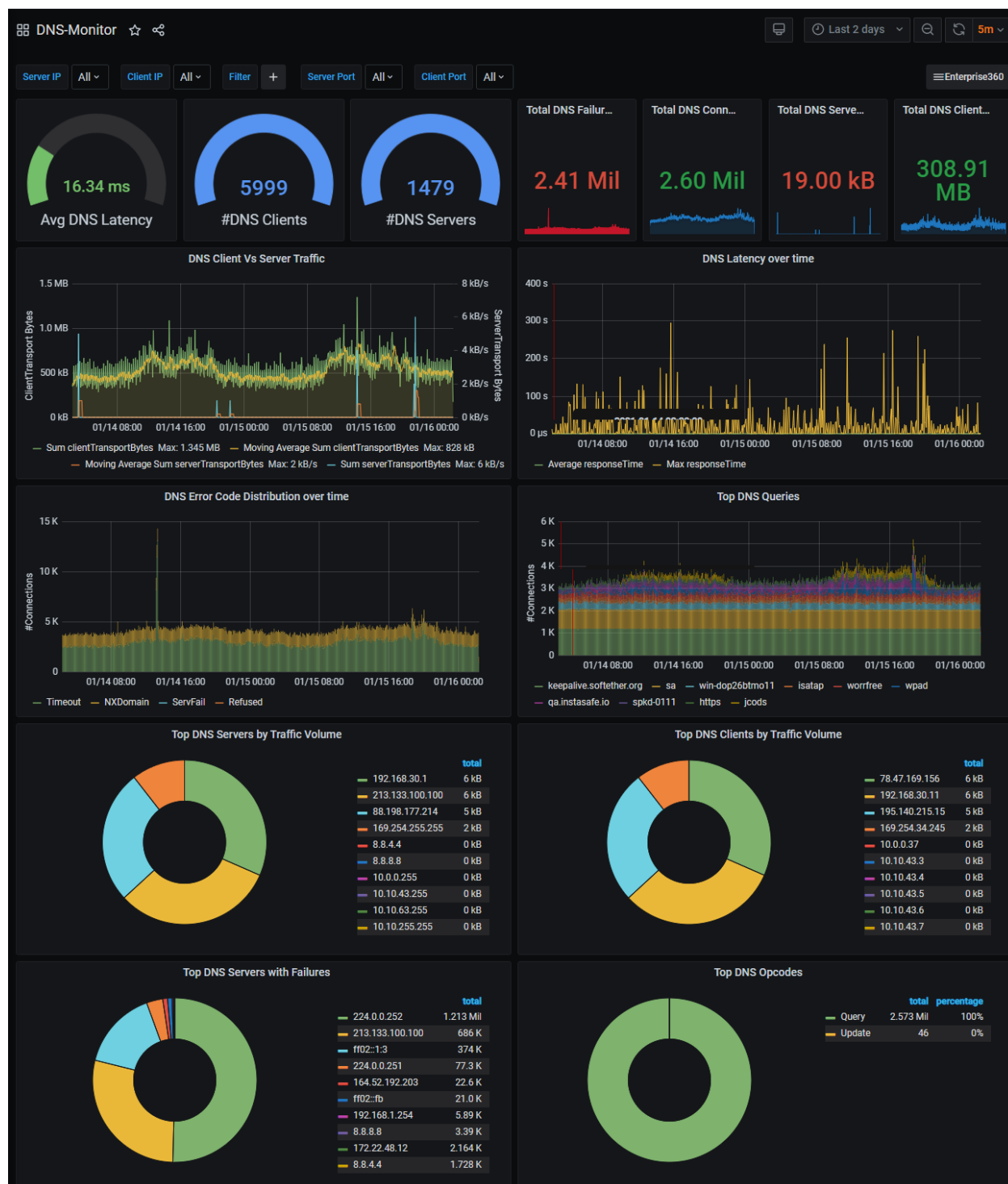


Figure 39. DCE Monitor - Default Panels - 1

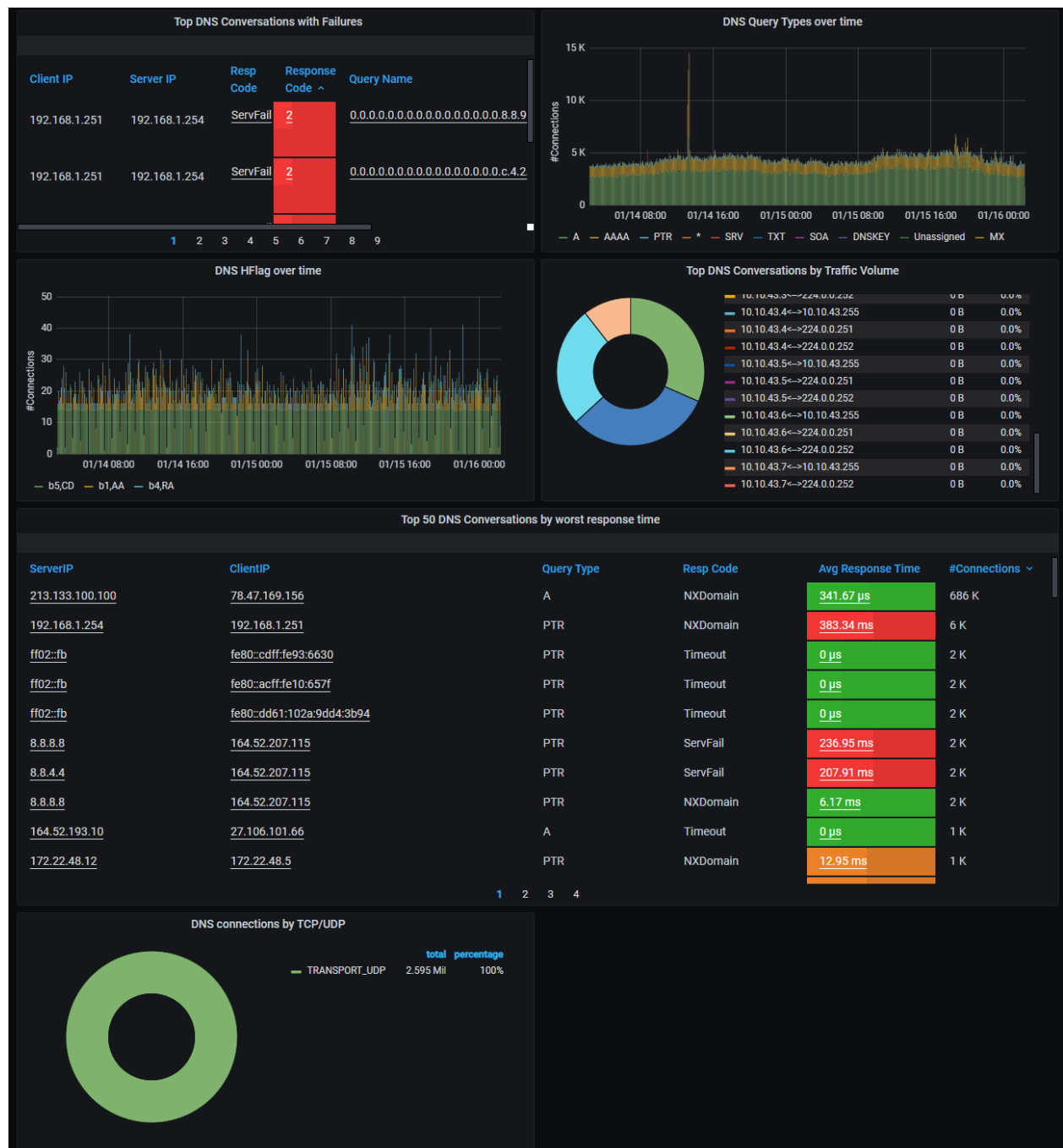


Figure 40. DCE Monitor - Default Panels - 2

DNS is a very popular and widely used protocol for resolving domain names to IP addresses in the internet as well as within the network. Users can

- Troubleshoot problems related to DNS resolution latencies and DNS errors while resolving domain names.
- Understand where the DNS queries are resulting in poor performance and errors.
- Recognize the DNS servers in the network, their traffic load and performance.

Each chart in the panels of this monitor is a use-case related to DNS in the network. The following sections describe each chart in the panels of this monitor.

DNS Entities and Events

<i>Panel</i>	<i>Purpose</i>
The gauges and numbers in the panels	To give at one glance a view of the following Average DNS Latency #DNS Clients #DNS Servers
The graphs and numbers in the panels	To give at one glance a view of total instances of the following DNS Failures DNS Connections DNS Server Traffic DNS Client Traffic

DNS Client Vs Server Traffic

This graph displays the total and average client and server traffic.

DNS Over-time graphs

This part displays the trending status of the following DNS issues at specific points in time. These graphs can be set with alerts so that users can address issues before they cause serious problems in the network.

- DNS Latency over time
- DNS Error Code Distribution over time
- DNS Query types over time
- HFlag over time (header flags)

The Top DNS Entities

The graphs in this part display the following.

- Top DNS Queries - DNS-queries that occur the maximum number of times.
- Top Servers by Traffic Volume - DNS servers with the maximum volume of traffic.
- Top Clients by Traffic Volume - DNS clients with the maximum volume of traffic.
- Top Servers with Failures - DNS servers with the maximum failures.
- Opcodes - commands made to the DNS servers

Top DNS Conversations with Failures table

This table has specific details about DNS conversations where failures are most rampant and their related data. Use the hyperlinks (underlined fields) to view details in the DNS Monitor.

<i>This field...</i>	<i>Indicates the...</i>
ClientIP	IP address of the client.
ServerIP	IP address of the server.
RespCode	name of the failure.
Response Code	code number of the failure.
Query Name	name of the query.
Count	number of failures returned by the query.

Table 38. Top DNS Conversations with Failures table

Top DNS Conversations by Traffic Volume

This graph displays the DNS servers with maximum volume of traffic and their relative percentage.

Top DNS Conversations with worst response time table

This table has specific details about 50 DNS conversations where response time has been the worst and their related data. As a standard step, use the hyperlinks (underlined fields) to view details in the DNS Monitor.

<i>This field...</i>	<i>indicates...</i>
ServerIP	The IP address of the server.
ClientIP	The IP address of the client.
Query Type	
RespCode	The name of the failure.
Avg Response Time	Average Response time.
#Connections	The number of connections.

Table 39.

DNS connections graph

This graph displays the type of DNS connections and their relative percentage.

- DNS connections by TCP/UDP - The type of DNS connections – TCP or UDP.

DNS-Response-Monitor

The *DNS Response monitor* is a subset of DNS monitor and provides detailed investigation for DNS responses for a given DNS transaction. Details of DNS responses are available only in DNS response monitor but not in DNS monitor.



Figure 41. DNS Response Monitor - Default Panels

After identifying the DNS query that is causing problem users can launch the DNS response monitor using the context of that DNS query to further check the responses for a given query and response performance and failures in detail.

Each chart in the panels of this monitor is a use-case related to DNS Response in the network. The following sections describe each chart in the panels of this monitor.

DNS Responses over time

The graph in this panel shows DNS Responses at specific points in time.

Top DNS Entities/events

The graphs in these panels display the following.

- Top DNS Resolutions.
- Top DNS Queries - a table display of the queries and its related details.
 - Query Name
 - Query Type
 - Number of connections ([hyperlink](#))

Click the hyperlink to view analytical details in the DNS Response Session analysis monitor.

- Top DNS Query Types - a view of the top DNS query types.

DNS Over-time graphs

The next panels display the trending status of DNS issues at specific points in time.

- DNS Responses Query Names
- DNS Response Query Class

DNS Response Record Types Graph

The graph in this panel shows DNS Response records at specific points in time.

FTP-Monitor

The *FTP monitor* provides comprehensive investigation into problems associated with file transfer applications using FTP protocol. FTP is a popular and widely used protocol for transferring files between computers inside the network.



Figure 42. FTP-Monitor – default panels

Users can

- troubleshoot problems related to FTP file transfer latencies and FTP errors during transfer.
- understand unusual and large file transfers hogging network bandwidth and unusual file transfers and attempts to transfer.
- recognize the FTP servers in their network and their traffic load and performance.

This is a multi-part display of contextual panels with various FTP related information at one glance. The following sections describe each chart in the panels of this monitor.

FTP Entities and Events

Multiple graphs in this panel give a view of the following

- Avg FTP Latency - the average latency experienced by FTP clients/users
- Connection Resets – the number of times FTP connections were reset
- #FTP Servers - the number of FTP servers
- #FTP Clients – the number of FTP clients

Numeric displays in this panel give a view of the following

- Total TCP Timeouts (in number)
- Total FTP Connections (in number)
- Total FTP Server Traffic (in bytes)
- Total FTP Client Traffic (in bytes)

FTP Over time graphs

This part of the dashboard displays the trending status of FTP issues and events over time.

- FTP Errors over time
- FTP EURT over time
- FTP Client Vs Server Traffic
- FTP Latency over time

FTP Entities and event graphs

This part of the dashboard displays the clients, servers and users' experience with respect to the FTP application.

- Top FTP Servers with Errors - The FTP servers with the maximum errors.
- FTP Connections - by command - The FTP servers with connections started by use of the command.
- Top FTP Servers by traffic - The FTP servers with the maximum traffic.
- Top FTP Clients by Errors - The FTP clients with the maximum errors.
- FTP Top Users by Connections - The FTP users with the maximum connections.
- Top FTP Clients by traffic - the FTP clients with the maximum traffic.
- Top Server Sites for FTP Connections - the FTP server sites with the maximum connections.
- TCP Connection States for FTP Sessions - the TCP connection states for FTP sessions.
- Top Client Sites for FTP Connections – the Client sites with the maximum FTP connections.

The Top FTP Conversations with Errors/Worst Latency table

This table has specific details about FTP conversations that have the most errors and worst latency in the network. Use the hyperlinks (underlined fields) to view details in the related Monitor.

<i>This field...</i>	<i>Indicates the...</i>
Server IP	IP address of the server.
Client IP	IP address of the client.
Status	Status of the operation.
File Operation	requested file operation.
Server Site	name of the server site.
Client Site	name of the client site.
UserName	user name.
Avg Resp Time	average response time.
Avg File Size	average file size.
Connections	number of connection. This is a hyperlink. Click to go to the "FTP Analysis" monitor.

Table 40.The Top FTP Conversations with Errors/Worst Latency table

ICMP-Monitor

The *ICMP monitor* provides a comprehensive board for investigation into problems associated with Internet Control Message Protocol (ICMP), which is a very popular and widely used protocol for testing network connectivity by various applications.



Figure 43. ICMP Monitor – default panels

Use this monitor to:

- Troubleshoot problems related to ICMP transactions
- Understand traffic volumes and conversations, latencies
- Capture ICMP failures, error codes, ICMP-redirects etc.

This is a multi-part display of contextual panels with ICMP related information. Each of the 6 parts in this dashboard pertains to a specific context and has 2 or more panels, named to indicate its contents.

ICMP Entities and Events

- Multiple gauge graphs in this panel give a view of the following:
 - ICMP Connections
 - # Errors – number of ICMP errors
 - #ICMP Clients – number of ICMP clients
 - # ICMP Servers – number of ICMP servers
 - Total ICMP Clients Traffic – total volume of traffic across ICMP clients
 - Total ICMP Server Traffic - total volume of traffic across ICMP server
- Alerts – this panel space can be used to define alerts for tracking the ICMP issues. See "[Creating Alerts](#)".

ICMP Over time graphs

The graphs in this panel display the trending status of ICMP errors and response time over time.

- ICMP Errors over time - ICMP Errors at specific points in time.
- ICMP RT over time - ICMP Response time at specific points in time.

ICMP Client Vs Server Traffic graph

This panel displays the following graph:

- ICMP Client Vs Server Traffic - Total traffic on the client and server sides.

Top ICMP graphs

- Top ICMP Message Types over time - the ICMP message types that are most rampant at specific points in time.
- Top ICMP Clients with Errors - The ICMP clients with the highest number of errors.
- Top ICMP Clients by traffic - The ICMP clients with the highest traffic.
- Top ICMP Servers with Errors - The ICMP servers with the highest number of errors.
- Top ICMP Servers by traffic - The ICMP servers with the highest traffic.

Top ICMP Conversations table

This table has specific details about ICMP conversations that are most rampant and their related data in the network. Use the hyperlinks (underlined fields) to view details in the related dashboard/monitor.

<i>This field...</i>	<i>indicates...</i>
<u>ServerIP</u>	The IP address of the server. This is a hyperlink. Click to go to <i>Server Infra Monitor</i> .
<u>ClientIP</u>	The IP address of the client. This is a hyperlink. Click to go to <i>Log Monitor</i> .
Message Type	Message type id.
#Messages	Number of messages
<u>Error Code</u>	The error code. This is a hyperlink. Click to go to <i>ICMP Session Analysis Monitor</i> .
#Errors	The number of errors.
Avg Resp Time	The average response time.
#Connections	The number of connections.

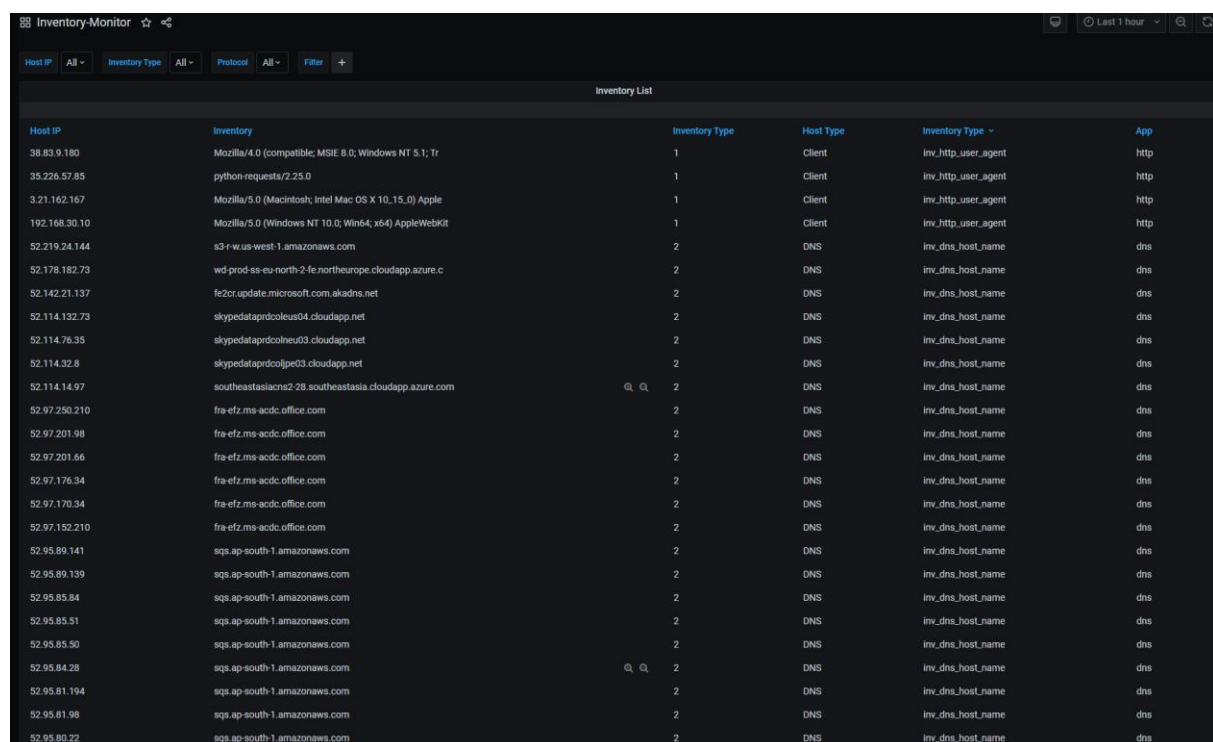
Table 41.

Inventory-Monitor

The *Inventory monitor* provides information on various aspects associated with a given host in the network. Soho360 learns through its discovery process the various aspects of a host in a network, such as:

- its IP address
- host name
- the operating system (OS) version running on the host
- software and their versions being used etc.

All information collected for a given host is available in the Inventory monitor. The minimum context of Host required for viewing all the discovered information is its IP address.



The screenshot shows the 'Inventory-Monitor' application window. At the top, there are filters for 'Host IP', 'Inventory Type', 'Protocol', and 'Filter'. Below the filters is a table titled 'Inventory List' with the following columns: Host IP, Inventory, Inventory Type, Host Type, Inventory Type (dropdown), and App. The table contains 20 rows of data, including host IP addresses, inventory names (e.g., Mozilla/4.0, python-requests/2.25.0), inventory types (1, 2), host types (Client, DNS), and applications (http, dns).

Host IP	Inventory	Inventory Type	Host Type	Inventory Type	App
38.83.9.180	Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 5.1; Tr	1	Client	inv_http_user_agent	http
35.226.57.85	python-requests/2.25.0	1	Client	inv_http_user_agent	http
3.21.162.167	Mozilla/5.0 (Macintosh; Intel Mac OS X 10.15.0) Apple	1	Client	inv_http_user_agent	http
192.168.30.10	Mozilla/5.0 (Windows NT 10.0; Win64; x64) AppleWebKit	1	Client	inv_http_user_agent	http
52.219.24.144	s3-rw-us-west-1.amazonaws.com	2	DNS	inv_dns_host_name	dns
52.178.182.79	wd-prod-sa-eu-north-2-fe.northeurope.cloudapp.azure.c	2	DNS	inv_dns_host_name	dns
52.142.21.137	fe2cr.update.microsoft.com.akadns.net	2	DNS	inv_dns_host_name	dns
52.114.132.79	skypedatprdc0eus04.cloudapp.net	2	DNS	inv_dns_host_name	dns
52.114.76.35	skypedatprdc0eus03.cloudapp.net	2	DNS	inv_dns_host_name	dns
52.114.32.8	skypedatprdc0eus03.cloudapp.net	2	DNS	inv_dns_host_name	dns
52.114.14.97	southeastasia2-28.southeastasia.cloudapp.azure.com	2	DNS	inv_dns_host_name	dns
52.97.250.210	fra-efz.ms-acdc.office.com	2	DNS	inv_dns_host_name	dns
52.97.201.98	fra-efz.ms-acdc.office.com	2	DNS	inv_dns_host_name	dns
52.97.201.66	fra-efz.ms-acdc.office.com	2	DNS	inv_dns_host_name	dns
52.97.176.34	fra-efz.ms-acdc.office.com	2	DNS	inv_dns_host_name	dns
52.97.170.34	fra-efz.ms-acdc.office.com	2	DNS	inv_dns_host_name	dns
52.97.152.210	fra-efz.ms-acdc.office.com	2	DNS	inv_dns_host_name	dns
52.95.89.141	sqs.ap-south-1.amazonaws.com	2	DNS	inv_dns_host_name	dns
52.95.89.139	sqs.ap-south-1.amazonaws.com	2	DNS	inv_dns_host_name	dns
52.95.85.84	sqs.ap-south-1.amazonaws.com	2	DNS	inv_dns_host_name	dns
52.95.85.51	sqs.ap-south-1.amazonaws.com	2	DNS	inv_dns_host_name	dns
52.95.85.50	sqs.ap-south-1.amazonaws.com	2	DNS	inv_dns_host_name	dns
52.95.84.28	sqs.ap-south-1.amazonaws.com	2	DNS	inv_dns_host_name	dns
52.95.81.194	sqs.ap-south-1.amazonaws.com	2	DNS	inv_dns_host_name	dns
52.95.81.98	sqs.ap-south-1.amazonaws.com	2	DNS	inv_dns_host_name	dns
52.95.80.22	sqs.ap-south-1.amazonaws.com	2	DNS	inv_dns_host_name	dns

Figure 44. Inventory Monitor – default panels

The panel in this monitor displays the Inventory list with the specific details about the inventory.

<i>This field...</i>	<i>indicates...</i>
Host IP	The IP address of the host.
Inventory	The name of the inventory.
Inventory Type	The type ID of inventory.
Host Type	Whether the host is a client or server.
Inventory Type	The type of the inventory.
App	The app being used on the Inventory.

Table 42.

Kerberos-Monitor

Kerberos monitor provides comprehensive investigation into problems associated with AAA applications using Kerberos protocol.



Figure 45. Kerberos Monitor – default panels

Kerberos is a very popular and widely used security protocol for authentication, authorization and administration (AAA) services in the network.

You can use this monitor to:

- troubleshoot Kerberos issues like latency, errors and types of errors.
- resolve problems related to individual failing Kerberos transactions.
- understand failure codes and reasons for server to reject AAA functions.
- discover AAA servers in the network, end users connecting to those AAA servers, traffic volumes, conversations, latencies, Kerberos failures and error codes.

This is a multi-part display of contextual panels with DCE-RPC related information. Each of the 7 parts in this dashboard pertains to a specific context and has 2 or more panels, named to indicate its contents.

Kerberos Events

Multiple gauge graphs in this panel give a view of the following

- Avg Kerberos Latency
- Connection Resets
- #Kerberos Servers – number of Kerberos servers
- #Kerberos Clients – number of Kerberos clients

Multiple Numeric displays in this panel give a view of the following

- Total Kerberos Failures
- Total Kerberos Connections
- Total Kerberos Server Traffic
- Total Kerberos Client Traffic

Kerberos Over time, traffic and connections graphs

The graphs in this panel display the following trending status of Kerberos over time.

- Kerberos Errors over time
- Kerberos Latency over time
- Kerberos Client Vs Server Traffic
- Kerberos Connections - by endpoint and operation

Top Kerberos graphs

The graphs in this panel display the following entities with the maximum status/action related to the Kerberos application.

<i>This field...</i>	<i>indicates...</i>
Kerberos Top Realms by Connections	realms with the maximum connections.
Kerberos Top Request Types by Connections	maximum request types.
Kerberos Top Services by Connections	maximum connections.
Kerberos Top Servers with Errors	servers with maximum errors.
Kerberos Top Servers by Traffic	servers with maximum traffic.
Kerberos Top Server Sites for Kerberos Connections	server sites with maximum Kerberos connections
Kerberos Top Clients by Errors	clients with maximum errors.
Kerberos Top Clients by Traffic	clients with maximum traffic.
Kerberos Top Client Sites for Kerberos Connections	client sites with maximum Kerberos connections.
Kerberos Top TCP Connection States for Kerberos Sessions	Maximum TCP connection states for Kerberos sessions.
Kerberos Top Users by Connections	Maximum users by connections.
Kerberos Top Ciphers by Connections	Maximum ciphers by connections.

Top Kerberos Conversations table

This table has specific details about Kerberos conversations that are most rampant and their related data in the network. Use the hyperlinks (underlined fields) to view details in the related monitor.

<i>This field...</i>	<i>indicates...</i>
ServerIP	The IP address of the server.
ClientIP	The IP address of the client.
Status Description	Description of the status.
Cipher Alg	The cipher algorithm.
Server Site	IP address of the server site.
Client Site	IP address of the client site.
Service	The service name.
Request Type	The request type.
Renewable	Whether renewable or not.

<i>This field...</i>	<i>indicates...</i>
Forwardable	Whether forwardable or not.
User Name	The user name.
Valid till	The duration of validity.
Avg Resp time	The average response time on seconds.
Connections	The number of connections.

Table 43.

Kerberos connections - graph

<i>This field...</i>	<i>indicates...</i>
Kerberos connections by TCP/UDP	The total number of TCP and UDP connections and their percentage.

Table 44.

License Monitor

The *License monitor* provides information pertaining to the Soho360 license and its usage over the period of installation.

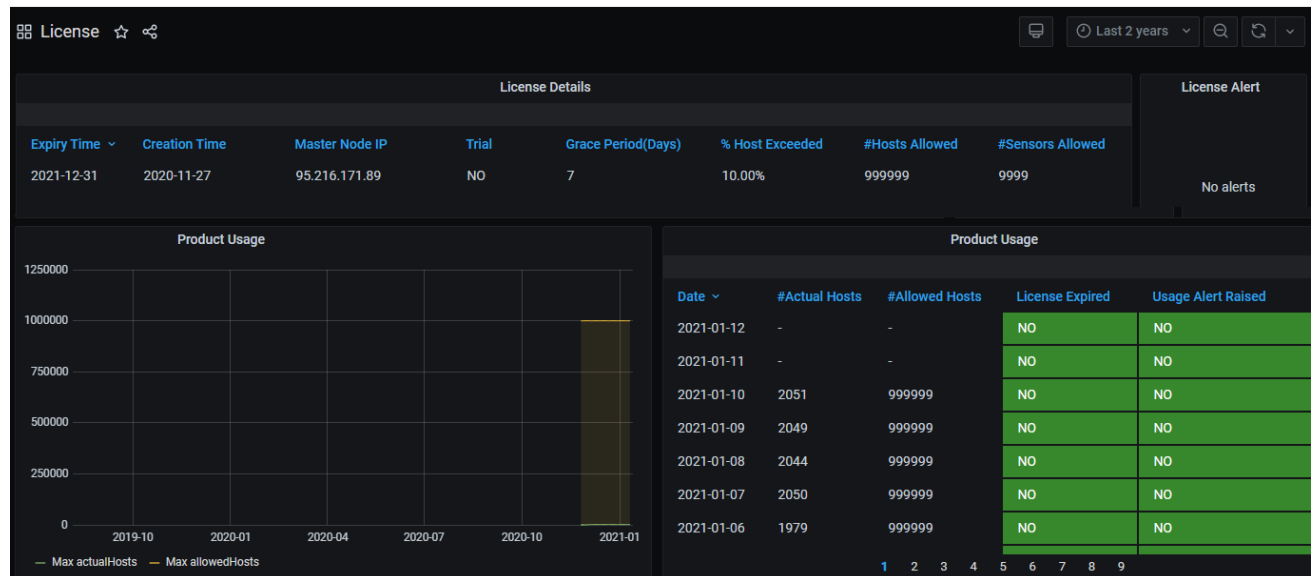


Figure 46. Licence Monitor – default panels

Use this monitor to:

- Understand the Soho360 license type, and the following associated entities:
 - license expiry dates,
 - number of active hosts Soho360 is monitoring in the network
 - sensors attached to Soho360
 - maximum allowed hosts and sensors for your license.
- set alerts for the license as its date of expiry approaches.
- recognize warnings if Soho360 is running above the permitted capacity of number of hosts for which it is licensed.

This is a multi-part display of contextual panels with license related information.

Soho360 License Details table

Field...	Description...
Expiry Time	The date beyond which the license will be invalid.
Creation Time	The date on which the license was created.
Master Node IP	The master node configured for the Soho360 network.
Trial	Whether the license is a trial version.
Grace Period(Days)	Extra time the license would be valid.
% Host Exceeded	Percentage of hosts in excess of the permitted number in the license.

Field...	Description...
#Hosts Allowed	Number of hosts included in the license.
#Sensors Allowed	Number of sensors included in the license

Table 45.

Alert

This panel-space can be used to define alerts for tracking the license and taking action for renewal etc. See "[Creating Alerts](#)".

Product Usage

Panel...	Purpose...
Product usage graph	To get a view of how Soho360 is being used with respect to the stipulations in the license.
Product Usage table	<p>To view all details of the license by date:</p> <p>Date – click to set the ascending or descending order of the date associated with the license.</p> <p>#Actual Hosts - the actual hosts in the network.</p> <p>#Allowed Hosts - the number of permitted hosts as in the license.</p> <p>License Expired - indication whether the license is valid or expired.</p> <p>Usage Alert Raised - indication whether a usage alert has been raised.</p>

Table 46.

NTLM-Monitor

NTLM (NT LAN Manager) monitor is a board for comprehensive investigation into problems associated with microsoft based NTLM protocol which provides authentication, integrity and confidentiality services in the network.



Figure 47. NTLM Monitor – default panels

Use this monitor to:

- troubleshoot NTLM issues like latency, errors and types of errors.
- resolve problems related to individual failing NTLM transactions.
- understand failure codes and reasons for server to reject NTLM functions.
- discover NTLM servers in the network, end users connecting to those NTLM servers, traffic volumes, conversations, latencies, NTLM failures and error codes.

This is a multi-part display of contextual panels with multiple genres of NTLM related information at one glance. Each of the 5 parts in this dashboard pertains to a specific context and has 2 or more panels, named to indicate its contents.

NTLM Events

Multiple graphs in this panel give a view of the NTLM entities and events.

- Gauge graphs display the following NTLM events and entities
 - Avg NTLM Latency
 - Total NTLM Failures
 - #NTLM Servers
 - #NTLM Clients
 - Total NTLM Connections
- The *NTLM Latency over time* shows NTLM Latency at specific points in time.
- Alerts - this space can be used for defining alerts to track NTLM issues. See "[Creating Alerts](#)".

NTLM Failed Connections and Errors

Graphs in this panel display the following NTLM events

- NTLM Failed Connections - by user
- NTLM Errors by Error Code

The Top NTLM Entities and Events

Graphs in this panel display the following NTLM events and entities

- NTLM Top Users by Connections
- Top NTLM Servers with Errors
- Top NTLM Clients by Errors
- Top Server Sites for NTLM Connections
- Top Client Sites for NTLM Connections

Top NTLM Conversations table

This table has specific details about NTLM conversations that are active and their related data in the network. Use the hyperlinks (underlined fields) to view details.

<i>This Field...</i>	<i>Indicates...</i>
Server IP	The IP address of the server.
Client IP	The IP address of the client.
Status Code	The status code.
Domain Name	The domain name.
Host Name	The host name.
Client Site	IP address of the client site.
User Name	The user name.

<i>This Field...</i>	<i>Indicates...</i>
Avg Resp Time	The average response time.
Connections	The connection number. This is a hyperlink. Click to go to the related Monitor.

Table 47.

RDP-Monitor

The *RDP monitor* provides a board for comprehensive investigation into problems associated with Remote desktop protocol (RDP). RDP provides administrators to remotely connect to windows-based machines in the network to troubleshoot problems on the windows machines. RDP is also a major security concern in any network. Threat actors can use RDP to remotely gain access to machines and infiltrate threats.



Figure 48. RDP Monitor – default panels

Use this monitor to:

- troubleshoot RDP issues like latency, errors and types of errors.
- resolve problems related to individual failing RDP transactions.
- understand failure codes and reasons for machines to reject RDP functions.
- detect machines where RDP is enabled and unknown RDP transactions have taken place in the past to explore cyber threats associated to RDP connections.

This is a multi-part display of contextual panels of RDP related information. Each of the 8 parts in this dashboard pertains to a specific context and has 2 or more panels, named to indicate its contents.

RDP Events and Entities

Multiple gauge graphs in this panel give a view of the following

- RDP Handshake RT
- Connection Resets
- #RDP Servers
- #RDP Clients

Multiple numeric displays in this panel give a view of the following

- Total TCP Timeouts
- Total RDP Connections
- Total RDP Server Traffic
- Total RDP Client Traffic
- RDP Errors over time

RDP over-time graphs

The graphs in this panel describe the following at specific points in time.

- RDP Errors over time.
- Handshake RT (response time) over time

RDP Traffic and Connections graphs

The graphs in this panel display the following RDP events and entities

- *RDP Client Vs Server Traffic* - The comparative volume of RDP traffic to clients and the servers
- *Connections - by encryption level* - The RDP connections with respect to the encryption levels

Top RDP Servers, Clients graphs

The graphs in this panel display the following RDP events and entities

<i>This Field...</i>	<i>Indicates...</i>
Top RDP Servers with Errors	servers with the highest RDP errors.
Top Clients by Errors	clients with the highest RDP errors.
Top Servers by traffic	servers with the highest traffic.
Top Clients by traffic	clients with the highest traffic.
Top RDP Encryption Method by connections	most common RDP Encryption method.
Top TCP Connection States for RDP Sessions	highest number of TCP connection states for the RDP connections
Top Server Sites for RDP Connections	server sites with highest RDP connections.
Top Client Sites for RDP Connections	client sites with highest RDP connections

Table 48.

Top RDP Conversations table

This table has specific details about RDP conversations that are most active and their related data in the network. Use the hyperlinks (underlined fields) to view details in the related Monitor.

<i>This field...</i>	<i>indicates...</i>
Server IP	The IP address of the server.
Client IP	The IP address of the client.
Status	The status of the connection – whether success or failed with error.
Desktop Height	Dimension of the Desktop Height in pixels.
Desktop Width	Dimension of the Desktop width in pixels.
Encryption Level	The level of encryption for the RDP connection..
Encryption Method	The method used for encryption.
HiColor Depth	Color depth property.
Status Code	State of the RDP connection whether Enabled/Disabled.
Security protocol	Description of the security protocol used.
Avg. Resp Time	Average time taken for the response.
Connections	Number of connections. This is a hyperlink. Click to go to the related monitor.

Table 49.

Sensor-Health-Monitor

The Sensor health monitor provides a board for comprehensive investigation into performance and health of all sensors connected to Soho360 platform.



Figure 49. Sensor Health Monitor – default panels

Optimal performance of sensors is crucial for successful network monitoring.

The sensor health monitor provides visibility into proper functioning of the sensor deployment for Soho360 platform in your network.

Use this monitor to

- discover which sensors are
 - up/down in your network
 - not seeing data
 - dropping packets and logs
 - failing to produce telemetry datasets for Soho360.
- study traffic throughput rates on each interface of every sensor and
- determine which sensor interfaces and sensors are over the performance capacity and need traffic re-routing and load balancing for optimal performance.

This is a multi-part display of contextual panels with sensor health related. Each of the 10 parts in this dashboard pertains to a specific context and has 2 or more panels, named to indicate its contents.

Packet Sensor Health Stats

This panel includes a table with NetSense (packet sensor) data.

Field...	Indicates the...
Sensor Name	name of the sensor
Link Name	name of the link
#PktsRejected	number of packets rejected by the sensor.
#PktsDropped	number of packets dropped by the sensor.
#BytesRcvd	number of bytes received by the sensor.
#CurrentConnections	number of current connections
#TCPConnections	number of TCP connections
#UDPCConnections	number of UDP connections
#64-128BytesPkts	number of packets of size between 64 and 128 bytes
#129-256BytesPkts	number of packets of size between 129 and 256 bytes
#257-512BytesPkts	number of packets of size between 257 and 512 bytes
#513-1024BytesPkts	number of packets of size between 513 and 1024 bytes
#1025-1518BytesPkts	number of packets of size between 1025 and 1518 bytes
#1519-9018BytesPkts	number of packets of size between 1519 and 9018 bytes
#>9018BytesPkts	number of packets of size greater than 9018 bytes
#Pagefaults	number of page faults
#PktsRecvd	number of packets received

Table 50. Packet Sensor Health Stats

Packet Sensor Graphs

This panel includes sensor throughput data and sensor performance over-time graphs.

- Packet Sensors - Packet Throughput in Bytes
- Over-time graphs that display the following details at at specific points in time.
- Packet Sensors - PacketDrops and PacketsRejected Over Time - Number of packets dropped and rejected.
- Packet Sensor Memory Usage Over Time - Memory usage by the NetSense (packet sensor)
- Packet Sensors - Connection Stats Over Time - Connection statistics of the NetSense (packet sensor)
- Anomaly Counts Over Time
- Packet Sensor - Page Faults Over Time- Number of packet sensor page faults

Log Sensor Health Stats

This panel includes a table showing InfraSense (log sensor) data.

Field...	Indicates the...
Sensor Name	name of the sensor
Interface ID	name of the interface of the sensor
#Page Faults	number of page faults
#Records Match	number of records matched
#Pkt Sensor Events	number of bytes received by the sensor.
Max Thread Count	maximum thread count.
#Records Ignored	number of records ignored
#Records Lookup Fail	number of failed record lookups
#Records Parsed	number of records parsed
Total Virtual Memory	total virtual memory used.

Table 51. Log Sensor Health Stats

Log Sensor Graphs

Over-time graphs that display the following InfraSense (log sensor) details at specific points in time.

- Log Sensor Memory Usage Over Time
- Log Sensors - Records Parsing

SIP-Monitor

The *SIP Monitor* provides a board for deep investigation to VOIP performance for the unified communication application *Session Initiation Protocol* (SIP) in the network.



Figure 50. SIP Monitor – default panels

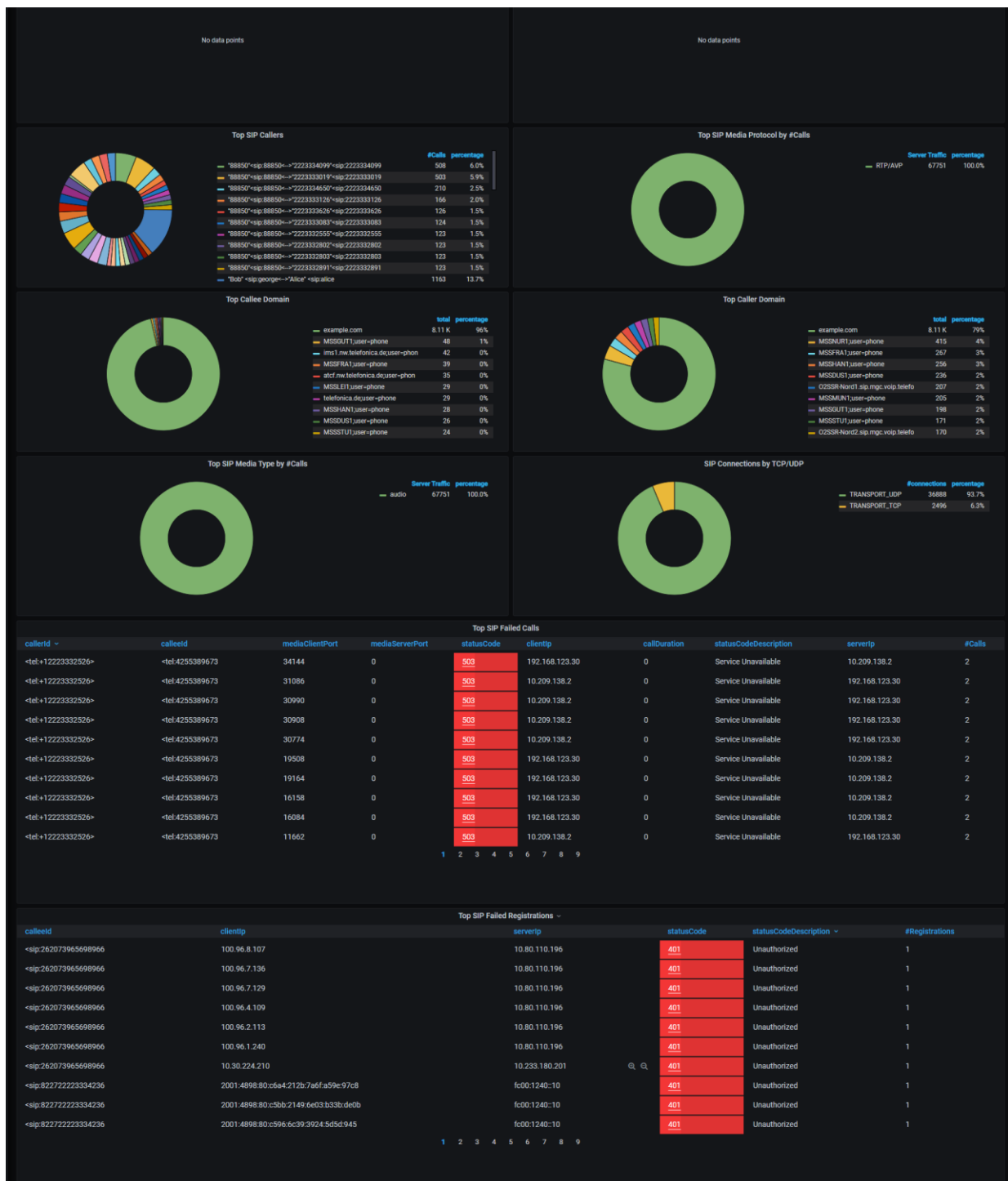


Figure 51. SIP Monitor – default panels (contd)

Use this monitor to determine:

- failures and performance of your SIP registration as well as control plane services.
- number of users impacted.
- call volumes, call latency, call failures, call traffic throughput rates for each SIP call,
- reason behind poor performance and failures.
- call volumes per servers and failure conditions on per server to isolate problems.
- top callers and their traffic volumes.

- media protocol running over SIP calls and SIP call transaction volumes per SIP domain.
- investigate further to session level intelligence to understand per SIP user session level issues.

This is a multi-part display of contextual panels with multiple disk usage related information at one glance. Each of the 11 parts in this dashboard pertains to a specific context and has 2 or more panels, named to indicate its contents.

SIP Entities and Events

Multiple gauge graphs in this panel give a view of the following

- number of SIP Callers
- number of SIP Callees
- Average SIP Call Duration
- Total SIP Client Traffic
- Total SIP Client Traffic
- Number of Registration Servers
- Number of SIP Calls
- Number of SIP Failures
- Number of SIP Registrations
- Number of SIP Registration Failures

SIP Alerts

This panel space can be used for defining alerts to track SIP issues. See "[Creating Alerts](#)".

SIP Failures Over-time Graphs

This panel shows the failures at specific points in time.

- SIP Failures with Status Code over time - gives a view of SIP failures with status code
- SIP Registration Failures with Status Code over time - gives a view of SIP registration failures with status code.

Call Volume and Latency Graphs

This panel has graphs showing the call volume and latency at specific points in time.

- SIP Call Volume - indicates the audio volume changes in calls.
- SIP Latency over time - indicates the latency in calls.

SIP Registration Graphs

This panel has graphs showing the extent and latency of registration at specific points in time.

- SIP Registration Volume – number of registrations
- SIP Registration Latency over time – time taken in terms of latency of registration

SIP Callers, SIP Client-Server traffic

This panel has graphs showing the highest number of calls per caller and the extent of traffic at the client and server ends.

- Top SIP Callers by #Calls - callers making the highest number of calls.

- SIP Client Vs Server Traffic - comparison of the extent of traffic at the SIP client end and that at the SIP server end.

Top SIP Callee, and Caller

This panel has graphs showing the number and percentage of callees and callers involved in the highest number of calls.

- Top SIP Callee by #Calls - callee involved in the highest number of calls.
- Top SIP Caller by #Calls - caller involved in the highest number of calls.

Top SIP Caller and Media Protocol

This panel has graphs showing the caller involved in the highest number of calls v/s the percentage and the most highly used media protocol.

- Top SIP Callers - callers involved in the highest number of calls.
- Top SIP Media Protocol by #Calls - media protocol involved in the highest number of calls.

Top Callee Domain and Top Caller Domain

This panel has graphs showing the callee and caller domains involved in the highest number of calls v/s the percentage.

- Top callee domain - callee domains involved in the highest number of calls with percentage.
- Top caller domain - caller domains involved in the highest number of calls with percentage.

Top SIP Media Type by #Calls and SIP Connections by TCP/UDP

This panel has graphs showing the media type and transport type involved in the highest number of calls v/s the percentage.

- Top SIP media type by #calls - the media type involved in the highest number of calls e.g. audio or video or streaming and the percentage of the media usage.
- SIP Connections by TCP/UDP Protocol by #Calls - the transport involved in the highest number of calls e.g. TCP or UDP and the percentage of the protocol usage.

Top SIP Failed Calls

This table has specific details about SIP failed calls and related data. Use the hyperlinks (underlined fields) to view details in the related Monitor.

<i>This field...</i>	<i>Indicates the...</i>
callerId	caller id
calleId	callee id
mediaClientPort	media client port number
mediaServerPort	media server port number
<u>statusCode</u>	status code. This is a hyperlink. Click to view the related monitor.
clientIp	client IP address
callDuration	call duration
statusCode Description	status code description

<i>This field...</i>	<i>Indicates the...</i>
serverIp	server IP address
#calls	number of calls

Table 52.Top SIP Failed Calls

Top SIP Failed Registrations

This table has specific details about SIP failed registrations and related data. Use the hyperlinks (underlined fields) to view details in the related Monitor.

<i>This field...</i>	<i>Indicates the...</i>
calleId	callee id
clientIp	client IP address
serverIp	server IP address
<u>statusCode</u>	status code. This is a hyperlink. Click to view the related monitor.
statusCode Description	status code description
#registrations	number of registrations

Table 53.Top SIP Failed Registrations

SMB-Monitor

The *SMB Monitor* provides a board for comprehensive investigation into Server Message Block (SMB) Protocol/application running in the network. SMB is a very popular Windows™ file transfer application used in Microsoft environments.



Figure 52. SMB Monitor - default panels

Use this monitor to discover

- SMB servers running in the network,
- The number of SMB transactions and end users using SMB.
- Servers and users experiencing SMB failures and poor SMB latency.
- traffic throughput volumes of SMB application per server and study servers performing poorly due to huge number of connections or traffic volume.

The SMB monitor links to SMB response Monitor and SMB map monitor to facilitate deep study of

- file paths,
- file names in each SMB transaction.

This is a multi-part display of contextual panels with SMB related information.

Each of the 7 parts in this dashboard pertains to a specific context and has 2 or more panels, named to indicate its contents. Each panel has options for users to drill deep for pointed views of the data described by the panel name.

SMB Entities and Events

Multiple gauge graphs in this panel give a view of the following

- Avg SMB latency - Average SMB latency
- Connection resets - number of connection resets
- # Servers - number of SMB servers

Multiple line graphs in this panel give a view of the following

- Total SMB failures
- Total SMB connections
- Total SMB server traffic
- Total SMB client traffic

SMB Over time

This panel has graphs that give a view of the following at specific points in time.

- SMB Errors over time
- SMB EURT over time (SMB End user response time)

SMB Traffic and Latency over-time

This panel gives a view of the traffic and SMB latency at specific points in time.

- SMB Client Vs Server Traffic - traffic in SMB clients and Servers.
- SMB Latency over time - latency of the SMB application at specific points in time.

SMB Errors and Read/Write Traffic

This panel has graphs that give a view of the SMB errors and traffic.

- Top SMB Servers with Errors - the SMB Servers with the highest errors.
- SMB Traffic - Read Vs Write Extent of read and write of SMB traffic.

Top SMB Server Traffic and Client Errors

This panel has graphs that give a view of the SMB servers and clients.

- Top SMB Servers by traffic - SMB servers with the highest traffic - the total and individual percentage.
- Top SMB Clients by Errors - SMB clients with the highest errors - the total and individual percentage.

Top SMB Version and Client Traffic

This panel has graphs that give a view of SMB version and client traffic.

- SMB Version Distribution – the way SMB versions are distributed in the network.
- Top SMB Clients by traffic – the SMB clients with the highest traffic.

SMB Anonymous User and Connections

This panel has graphs that give a view of usage by the anonymous users and connection types.

- SMB Anonymous User Usage - Extent of usage by SMB Anonymous user.
- SMB Connections Encrypted Vs Non Encrypted - Number of Encrypted and non-encrypted connections.

Top SMB commands, Guest User Usage

This panel has graphs that give a view of SMB commands and usage by the guest user.

- Top SMB Commands over time - Most used SMB commands at specific points in time.
- SMB Guest User Usage - Extent of usage by SMB guest user.

SMB Map Path, TCP Connection states

- SMB Map Path Distribution - The table in this panel gives a view of the following
 - Tree ID
 - Map Path (this is a hyperlink).
 - #Sessions (this is a hyperlink)

Click the hyperlinks to go to SMB response Monitor and SMB map monitor for further investigation in case of SMB issues.

- TCP Connection States for SMB Sessions
 - This graph displays the states of TCP Connection for SMB sessions.

Top SMB Conversations

This table has specific details about SMB conversations that are most rampant and related data. Use the hyperlinks (underlined fields) to view details in the SMB session Analysis Monitor.

<i>This field...</i>	<i>indicates...</i>
ServerIP	The IP address of the server.
ClientIP	The IP address of the client.
Command	The SMB command.

<i>This field...</i>	<i>indicates...</i>
Status code	The status code.
Error description	Description of the error.
Connections	Number of connections. This is a hyperlink. Click the hyperlink to go to the SMB Session Analysis Monitor.

SMB Inner VLans, Share Type

The graphs in this panel display the following details about SMB in the network.

- SMB Inner VLans over time - SMB connections in the VLans of the network.
- SMB Share Type Distribution - the percentage distribution of the various share types in the network.

SMB-File-Monitor

The *SMB File Monitor* is part of *SMB Monitor* and provides a board for investigation into number of files, names and path of files and file size data (read vs write) volumes transacted in each SMB connection selected from the “*Top* SIP Failed Registrations

SMB-Monitor”.

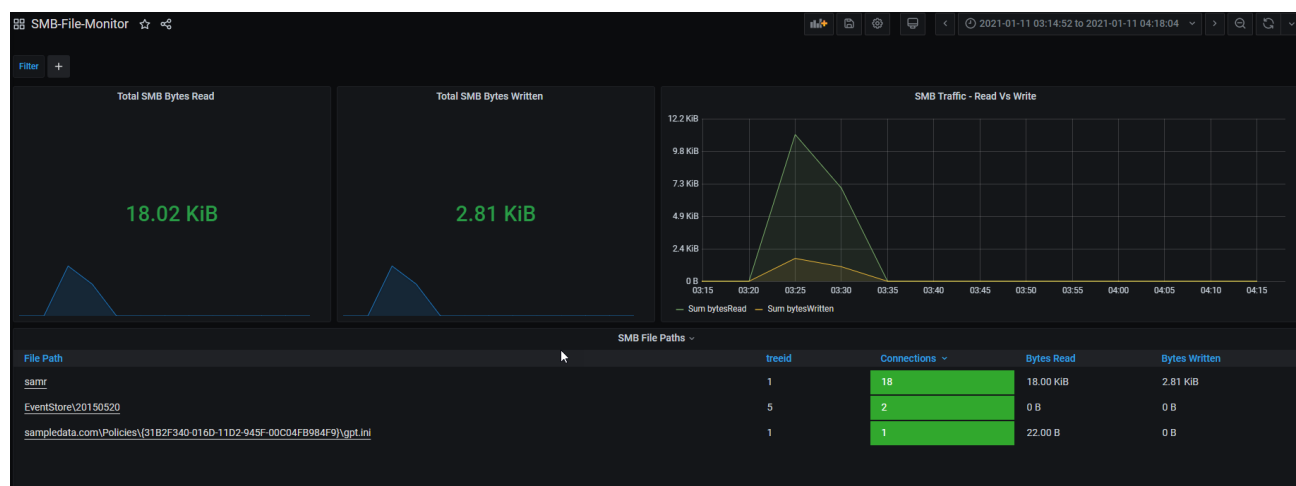


Figure 53. SMB File Monitor - Default panels

This is a multi-part display of contextual panels of SMB File related information. Each of the 2 parts in this dashboard pertains to a specific context and has 2 or more panels, named to indicate its contents.

SMB Read, Write, Traffic

The graphs in this panel display the following.

- Total SMB Bytes Read
- Total SMB Bytes Written
- SMB Traffic - Read Vs Write - Combined SMB Traffic of Read bytes and written bytes.

SMB File Paths table

This table has specific details about SMB file paths and related data. As a standard step, use the hyperlinks (underlined fields) to view details in the related Monitor.

Field	Indicates...
File Path	The file path. This is a hyperlink. Click to go to the related monitor.
treeid	Tree ID of SMB file.
Connections	The number of connections.
Bytes read	The number of bytes read.
Bytes written	The number of bytes written.

SMB-Map-Monitor

The *SMB Map monitor* is part of SMB monitor and facilitates investigation into tree IDs, SMB dialects used and map paths for each SMB transaction selected from the “*Top* SIP Failed Registrations

SMB-Monitor”.

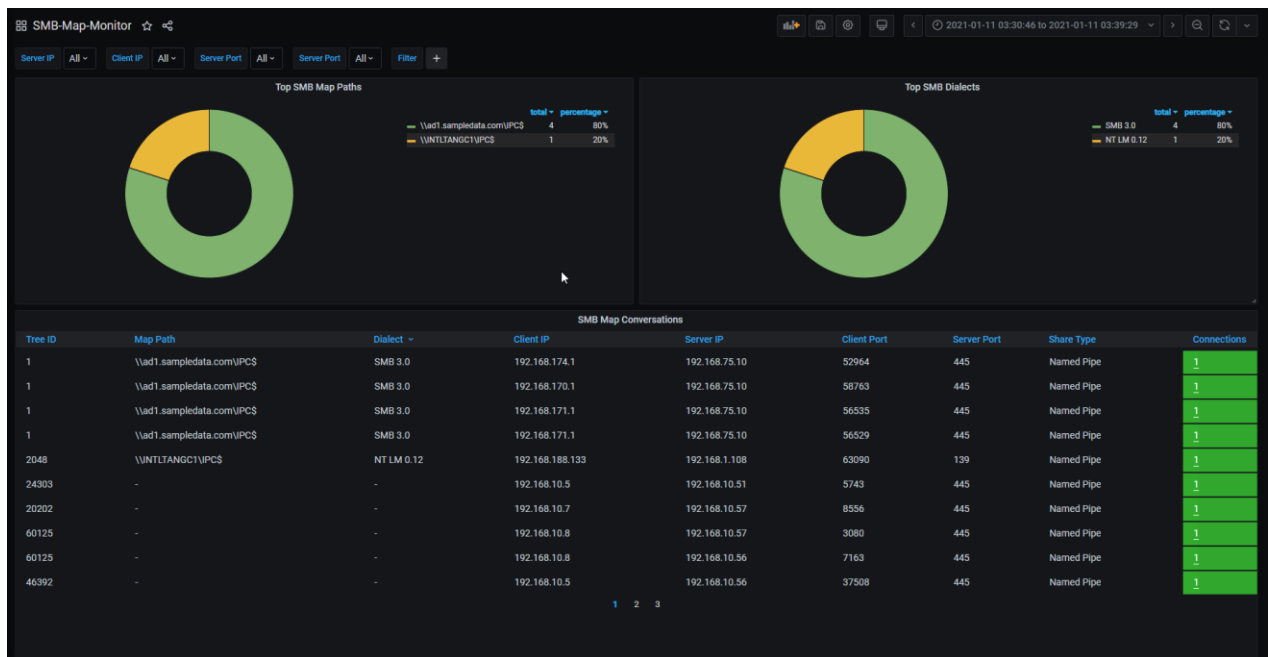


Figure 54. SMB Map Monitor – default panels

This is a multi-part display of contextual panels with multiple genres of SMB Map related information. Each of the 2 parts in this dashboard pertains to a specific context and has 2 or more panels, named to indicate its contents.

SMB Read, Write, Traffic

The graphs in this panel display the following.

- Top SMB Map Paths - The SMB maps most used in the network.
- Total SMB Dialects - The total number of SMB dialects (versions) used in the network.

SMB Map Conversations table

This table has specific details about SMB file paths and related data. As a standard step, use the hyperlinks (underlined fields) to view details in the related monitor.

Field	Indicates...
treeid	Tree ID of SMB file.
Map Path	The file path.
Dialect	The version of SMB/NTLM

Field	Indicates...
Client IP	The IP address of the client
Server IP	The IP address of the server
Client Port	Port number of the client
Server Port	Port number of the server
Share Type	Type of share.
Connections	The number of connections. This is a hyper link. Click to go to the related monitor.

Table 54.

Email-Monitor

The *Email-Monitor* provides a board for comprehensive investigation into application failures and performance for the email application in your network. SMTP (Simple Mail Transfer Protocol) is the most common email application used in networks.



Figure 55. SMTP Monitor - default panels

Use this monitor to discover

- SMTP email servers and users experiencing failures poor performance using the email application.
- reasons behind failures and email traffic load conditions on each server.
- top domains where the email traffic is received from or sent to.

Use each failing SMTP transaction to further investigate every user-level session intelligence to understand the reasons behind the SMTP transaction failures and poor performance.

This is a multi-part display of contextual panels with SMTP related information.

Each of the 8 parts in this dashboard pertains to a specific context and has 2 or more panels, named to indicate its contents.

SMTP Events and Entities

Multiple gauge graphs in this panel give a view of the following

- Avg SMTP Latency
- Transient Errors
- Permanent Errors
- Rejected Connections
- Connection Resets
- #SMTP Servers
- #SMTP Clients
- #SMTP Sending Host

Multiple number graphs in this panel give a view of the following

- Total TCP Timeouts
- Total SMTP Connections
- Total SMTP Server Traffic
- Total SMTP Client

Alerts Alerts can be defined here to track SMTP issues. See "[Creating Alerts](#)".

SMTP Ove-time Graphs

The graphs in this panel give a view of the following at specific points in time.

- SMTP Errors over time
- SMTP EURT over time - End user response time

SMTP Traffic, TCP Connection State

The graphs in this panel give a view of the following.

- SMTP Client Vs Server Traffic
- TCP Connection States for SMTP Sessions

Top SMTP graphs

The graphs in this panel give a view of the following at specific points in time.

- Top SMTP Servers with Errors - SMTP servers with maximum errors, the number of connections and the percentage.
- Users by Errors - SMTP users with maximum errors, the number of connections and the percentage.
- Servers by traffic - SMTP servers with maximum traffic, the total traffic and the percentage.
- Clients by traffic -SMTP clients with maximum traffic, the total traffic and the percentage.

SMTP Connections, Sender Host names

The graphs in this panel give a view of the following.

- SMTP Secured Vs Unsecured Connections - Total secured and un-secure connections and their percentage.
- Top SMTP Sender Host Names over time - Sender host names that have the maximum connections at specific points in time.

Top SMTP Conversations

This table has specific details about SMTP conversations that are most frequently occurring and their related data. Use the hyperlinks (underlined fields) to view details in the related monitor.

<i>This field...</i>	<i>indicates...</i>
ClientIP	The IP address of the client. This is a hyperlink. Click to go to the " <i>LogMonitor</i> "
Mail From	The "from" address in the email.
ServerIP	The IP address of the server. This is a hyperlink. Click to go to the " <i>Server Infrastructure Monitor</i> ".
Mail To	The "to" address in the email.
Sending Hostname	The hostname from where the email is sent.
Status Code	The status code on the email. This is a hyperlink. Click to go to the SMTP Session Analysis monitor.
Status Description	The description in words of the status code.
clientSite	Name of the client site.
serverSite	Name of the server site.
#Connections	The number of connections.
Avg Response Time	Average response time.

Table 55.

Top SMTP Sender User Agents Over-time

This panel has the following graph.

- Top SMTP Sender User agents over time - names of user-agents that have sent the maximum emails at specific points in time.

SQL-Monitor

THE SQL monitor provides comprehensive investigation into MYSQL data base application. MySQL is a very popular application protocol used by many commercial data base applications to provide data base services to end users.

Most non SQL database applications also use MYSQL for providing database services to end users.



Figure 56. SQL Monitor – default panels

In most commercial database servers, performance is determined by their query response time. Use this monitor to:

- troubleshoot failing and poorly performing database servers and impacted end users in the network.
- understand reasons for failures, traffic through put rates on each MYSQL database server.
- recognize the top queries resulting in failures and poor performance to trace the problematic data-sets in the database servers.
- investigate how the database servers perform during extremely large queries to understand server behaviour and performance limits.
- drill into each user and SQL query to determine failure and performance issues concerning individual users to understand reasons for poor performance and user experience using database applications.

This is a multi-part display of contextual panels of DCE-RPC related information.

Each of the 7 parts in this dashboard pertains to a specific context and has 2 or more panels, named to indicate its contents.

SQL Events

Multiple graphs in this panel give a view of the following

- Avg SQL Latency
- Connection Resets
- #SQL Servers
- #SQL Clients

Numeric displays in this panel give a quick insight into instances of the following across the network:

- Avg Connection Duration
- Total SQL Connections
- Total SQL Connections
- Total SQL Client Traffic

SQL Over-time Graphs

This panel has graphs of the following at specific points in time.

- SQL Errors over time
- SQL EURT over time

Where EURT is *end-user response time*.

SQL Client-server traffic, SQL Connections

This panel has graphs of the following SQL details.

- SQL Client Vs Server Traffic – comparative total of the volumes of SQL client and server traffic.
- SQL Connections over time by Command - SQL connections made by use of the related command at specific points in time.

Top SQL Graphs

This panel has graphs of the following SQL details.

- Top SQL DB Names by #connections - names of the most used databases and their number of connections.
- Table Names by #connections - names of the most used database tables and their number of connections
- Servers by traffic - Names of the most used SQL servers and the extent of traffic.
- Clients by traffic - Names of the most used SQL clients and the extent of traffic.

SQL Version, Statistics, Users, TCP Connection

This panel has graphs of the following SQL details.

- SQL Version Distribution - the SQL version, in use and their number of connections.
- SQL Statistics – this is a table with data related to:
 - DB name
 - Command
 - tableNames.keyword
 - Status
 - Rows affected
 - #Connections

Click the hyperlink to go to the related monitor.

SQL Top Users, TCP Connection

This panel has graphs of the following SQL details.

- *SQL Top Users by Connection* - Names of the top users of the SQL databases and their number of connections.
- *TCP Connection States for SQL Sessions*

Top SQL Conversations

This table has specific details about SQL conversations that are most frequently occurring and their related data. Use the hyperlinks (underlined fields) to view details in the related monitor.

<i>This field...</i>	<i>Indicates...</i>
ServerIP	The IP address of the server.
ClientIP	The IP address of the client.
Command	The SQL command.
DB Name	The SQL database name.
Table Name	The database table name.
Status	The status code.
Rows Affected	The number of rows affected by the command.
User Name	The name of the database user.
Connections	The number of connections to the database. This is a hyperlink. Click to go to the related monitor.

Table 56.

SSH-Monitor

The *SSH monitor* provides a board for comprehensive investigation into the SecureShell (SSH) application which is very commonly used for secure access to critical servers by network administrators.



Figure 57. SSH-Monitor

Use this monitor to:

- detect failing SSH servers, impacted users and poor performance of remote SSH connectivity for end users.
- understand reasons for failures and traffic throughput rates of SSH traffic per server.
- identify users who are logging into secure servers in network and determine if they are genuine user accounts.
- track unusual SSH activity on critical SSH servers in the network using SSH monitor. SSH applications are also a key target for threat actors to gain secure access to application servers, which can severely compromise network security.

Default Panels

This is a multi-part display of contextual panels with multiple genres of SSH related information. Each of the 9 parts in this dashboard pertains to a specific context and has 2 or more panels, named to indicate its contents.

SSH Events and Entities

Multiple gauge and line graphs in this panel give a view of the following

- Avg SSH Latency
- Login Failures
- Handshake Failures
- GSS Failures
- Rejected Connections
- #Resets
- #SSH Servers
- #SSH Clients
- Total SSH Connections
- Total SSH Server Traffic
- Total SSH Client Traffic
- #SSH Users

Alerts

This panel-space can be used for defining alerts for tracking SSH issues. See "[Creating Alerts](#)".

SSH Over-time Graphs

This panel has graphs of the following at specific points in time.

- SSH Errors over time
- SSH latency over time

SSH Client-Server Traffic, TCP State

This panel has graphs of the following.

- SSH Client Vs Server Traffic
- TCP Connection States for SSH Sessions

Top 10 SSH Servers - Errors table

This table has specific details about top SSH servers with errors.
Use the hyperlinks (underlined fields) to view details in the related Monitor.

<i>This field...</i>	<i>Indicates...</i>
Server IP	The server IP address
UserName	The SSH user name
Status Code	The status code
Status Description	The status description
#Connections	The number of connections. This is a hyperlink.

Table 57.

Top 10 SSH Clients - Errors table

This table has specific details about top SSH clients with errors; use the hyperlinks (underlined fields) to view details in the related monitor.

<i>This field...</i>	<i>Indicates...</i>
Client IP	The client IP address
UserName	The SSH user name
Status Code	The status code
Status Description	The status description
#Connections	The number of connections. This is a hyperlink.

Table 58.

Top 10 SSH Graphs

This panel has graphs of the following.

- Top SSH Servers by traffic - the servers with maximum traffic. Total and %age
- Top SSH Clients by traffic - the clients with maximum traffic. Total and %age

SSH Over-time Graphs

This panel has graphs of the following at specific points in time.

- Cipher Suites over time
- Key Exchange types over time
- MAC Alg types over time
- Server Host Key types over time

SSH version distribution and Top SSH users over time

This panel has graphs of the following.

- SSH Version Distribution by #connections
- Top SSH Users over time

Top 50 SSH Conversations

This table has specific details about SSH conversations that are most frequently occurring and their related data in the network. Use the hyperlinks (underlined fields) to view details in the related monitor.

<i>This field...</i>	<i>Indicates...</i>
ClientIP	The IP address of the client. This is a hyperlink. Click to go to the <i>"Log monitor"</i>
ServerIP	The IP address of the server. This is a hyperlink. Click to go to the <i>"Error! Reference source not found."</i>
Status Description	Description of the status.
Cipher Alg	The type of cipher algorithm.
Key X Alg	The type of key exchange algorithm.
MAC Alg	The type of MAC algorithm.
User Name	The SSH user name.
Status Code	The status code.
#Attempts	The number of attempts
Version	The version number.
Avg Response Time	The average response time of the application.
#Connections	The number of connections.

Statistics-Dashboard

The statistics dashboard provides a perspective of the number of hosts being monitored by Soho360 in the network. It separates the hosts into servers and clients, and demarcates the hosts internal to the network from those external to the network.

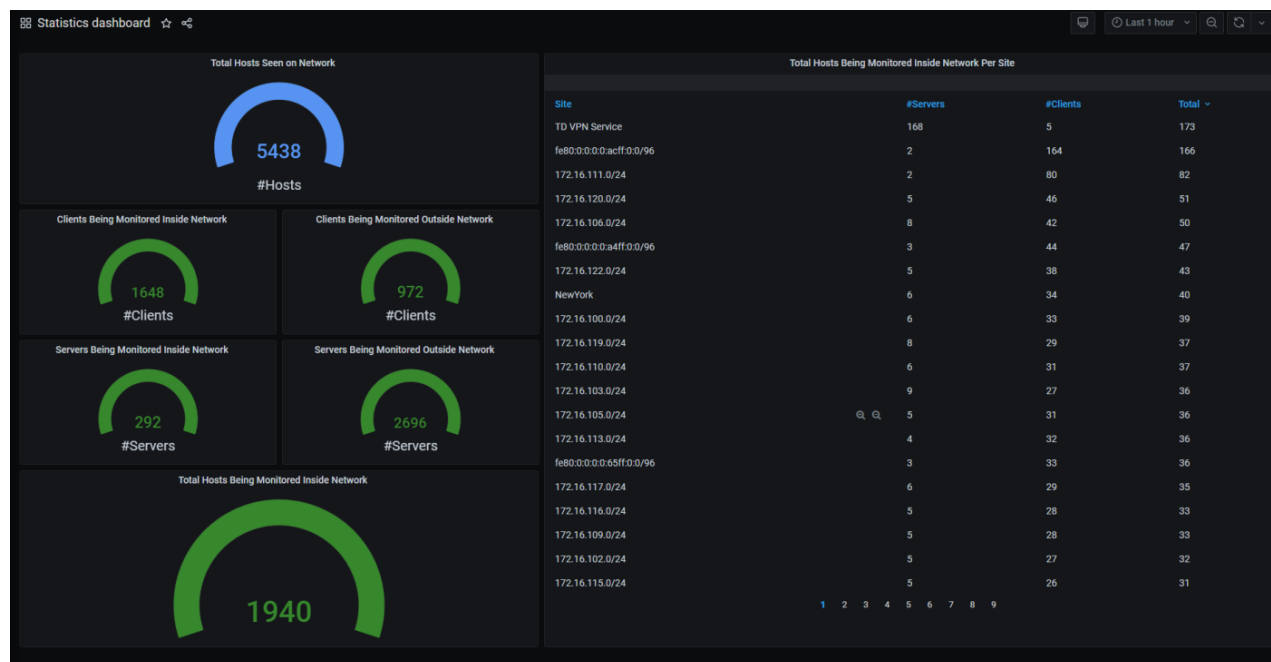


Figure 1. Statistics Dashboard

The Soho360 license and subscription is based on number of internal hosts monitored inside the network. The license comes with total number of hosts monitored inside the network. The *License Monitor* also shows how many hosts are being monitored and if they are above or below the capacity associated with the Soho360 license.

This is a display of contextual panels with multiple statistical data.

Left Panel graphs

The graphs in the left panel display the following details.

- Total Hosts Seen on Network
- Clients Being Monitored Inside Network
- Clients Being Monitored Outside Network
- Servers Being Monitored Inside Network
- Servers Being Monitored Outside Network
- Total Hosts Being Monitored Inside Network

Right Panel Table

This table lists all the hosts being monitored inside network per site.

<i>This field...</i>	<i>indicates...</i>
Site	The site name in the network.
#Servers	The number of servers in the site.
#Clients	The number of clients in the site.
Total	The total number of clients and servers per site.

Table 59.

TCP-Monitor

The *TCP Monitor* provides a board for comprehensive investigation into TCP layer related issues for applications running over TCP. Most applications use TCP as transport protocol at Layer 4.



Figure 58. TCP-Monitor – default panels

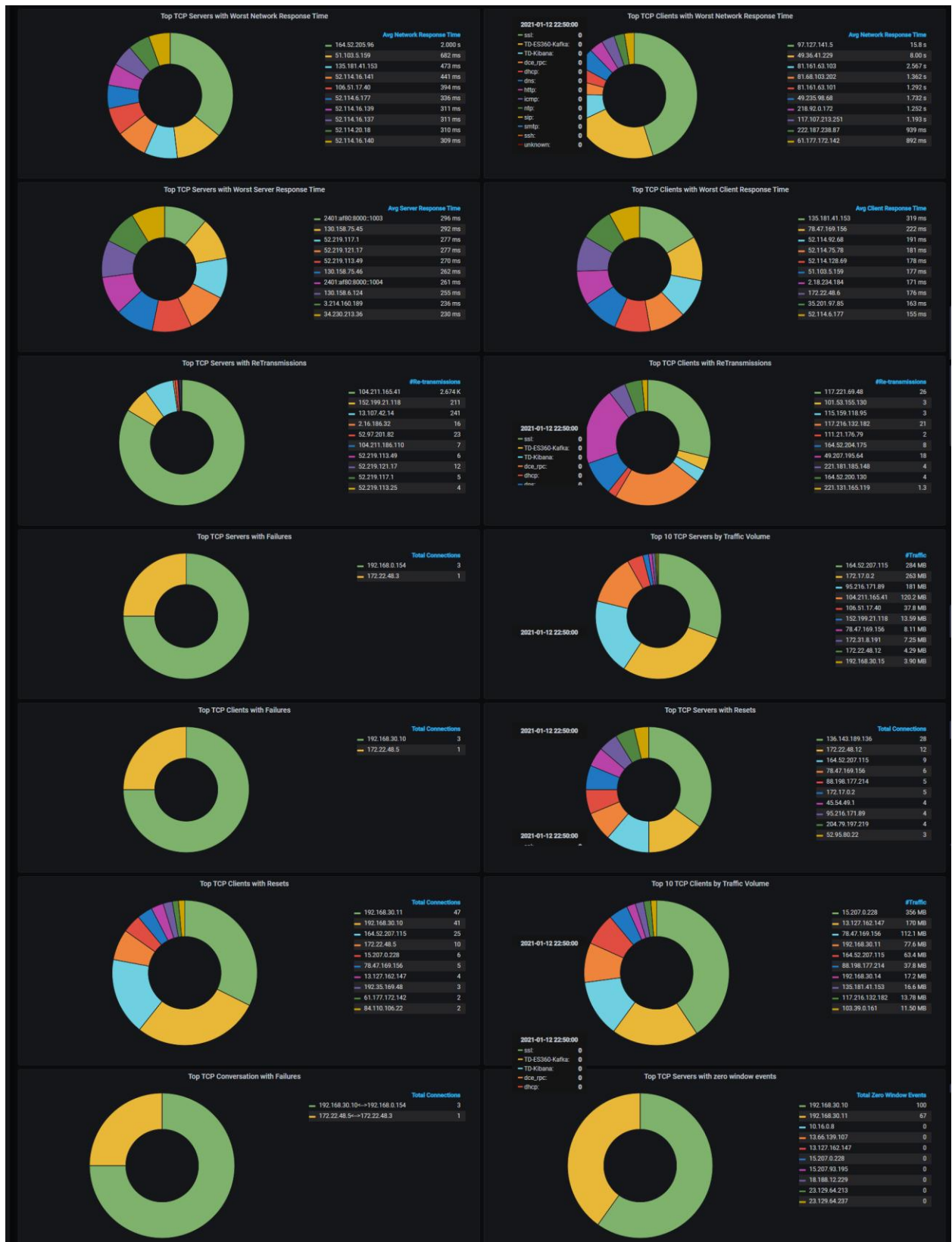


Figure 59. TCP-Monitor – default panels (contd.)

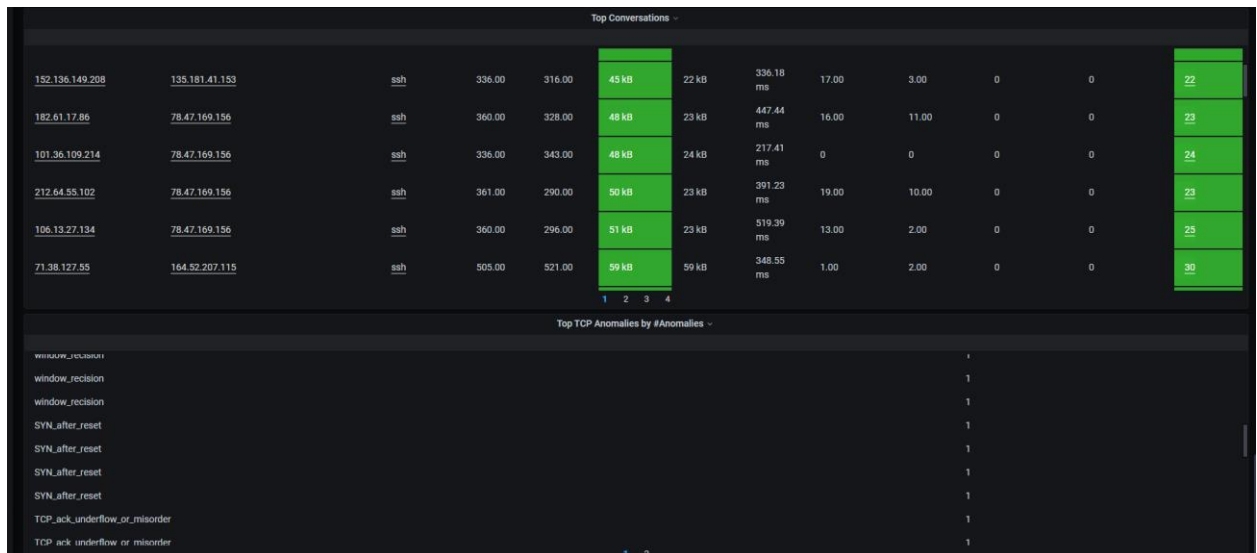


Figure 60. TCP-Monitor – default panels (contd.)

Use this dashboard- monitor to:

Troubleshoot Network Response/TCP handshake time for connections, retransmission errors, TCP timeouts, TCP client, server reset conditions, TCP zero window instances, TCP client and server errors and many other common TCP related issues using TCP Monitor.

During Application performance related investigations, users can drilldown into TCP Monitor from respective application monitors to triage if the end user application failures and experience are related to transport layer(TCP) or application layer to narrow down the root cause.

This is a multi-part display of contextual panels with multiple genres of TCP related information.

The details in these panels are described in the following sections.

TCP Events - graphs

Multiple graphs in this panel give a view of the following:

- #Failures
- Client Resets
- #Timeouts
- Server Resets
- Zero Window Instances
- #TCP Servers
- #TCP Clients
- #TCP Connections

Note: In all graphs the color indicates if the number is within (green) approaching (orange) or exceeding (red) the error limit set for each of the KPIs.

Alerts

Alerts can be set for tracking TCP issues. Once the administrator defines and saves such an alert in the system it will be displayed in this panel. See "[Creating Alerts](#)".

TCP Over-time graphs

This part of the dashboard displays the trending status of TCP issues/events/data at specific points in time.

<i>This graph...</i>	<i>Displays...</i>
TCP Network Response Time over Time	Network response time over a period of time.
Connection Status Distribution over Time	Connection status distribution over a period of time.
TCP App Rejects over time	Number of rejects experienced by the TCP app.
TCP Resets over Time	Number of resets experienced by the TCP app.
TCP Server Re-Transmission Packets over Time	Number of server retransmission packets over time.
TCP Client Re-Transmission Packets over Time	Number of client retransmission packets over time.
TCP Server Response Time	TCP server response time over a period of time.
TCP Client Response Time	TCP client response time over a period of time.
TCP Server Zero Window Instances over Time	Number of TCP server zero windows over a period of time.
TCP Client Zero Window Instances over Time	Number of TCP client zero windows over a period of time.

Table 60.TCP Over-time graphs

Note: Check these trend graphs to see the exact time during the selected phase (for example "last 1 hour") when the TCP issue or event or data occurred. Drag your mouse over the graph and left-click to select a portion of this graph to get a focused view of the extent of TCP network response time at that point.

The Top TCP Servers/clients – snapshot views

This part of the dashboard displays the snapshot view of the status of TCP issues at specific points in time.

<i>This graph...</i>	<i>Displays a snapshot view ...</i>
Top TCP Servers with Worst Network Response Time	Of the TCP servers with worst network response time, with the highest at the top of the list.
Top TCP Servers with Worst Server Response Time	of the TCP servers with worst server response time, with the highest at the top of the list.
Top TCP Servers with Re-Transmissions	of the TCP servers with the most re-transmissions. The highest is at the top of the list.
Top TCP Servers with Failures	of the TCP servers with the most failures. The highest is at the top of the list.
Top TCP Clients with Failures	of the TCP clients with the most failures. The highest is at the top of the list.
Top TCP Clients with Resets	of the TCP clients with the most resets. The highest is at the top of the list.
Top TCP Conversation with Failures	of the TCP conversations with the most failures. The highest is at the top of the list.
Top TCP Servers with zero window events	Of the TCP servers with the highest number of Zero window instances. TCP Zero Window events tell the sender to stop sending data because the receiver's buffer is full. This indicates a problem on the receiver that might be a server incapable of allocating memory/space.

Table 61.

Top Conversations table

This table has specific details about TCP conversations that are most frequently occurring and their related data in the network. Use the hyperlinks (underlined fields) to view details in the Connection Log Monitor, Server Infra Monitor, App Monitor, and Connection Session Analysis Monitor respectively.

<i>This field...</i>	<i>indicates...</i>
Client IP	The Client IP address. This is a hyperlink. Click to go to the Connection Log Monitor.
Server IP	The server IP address. This is a hyperlink. Click to go to the Server Infra Monitor.
Application	The application. This is a hyperlink. Click to go to the Connection Session Analysis monitor.
Server Pkts	Number of server packets
Client Pkts	Number of client packets.
Server Traffic	The volume of server traffic.
Client Traffic	The volume of client traffic.
Avg NRT	Average network response time.
#Server Re-trans	Number of server retransmissions.
#Client Re-trans	Number of client retransmissions.
#Client 0 Window	Number of client 0 window.
#Server 0 Window	Number of server 0 window.
#Connections	Number of connections.

Table 62. Top Conversations table

Top TCP Anomalies by #Anomalies

This table has specific details about TCP anomalies that are most frequently occurring and their number in the network.

<i>This field...</i>	<i>Has...</i>
Anomaly Description	The name of the anomaly
Count	The number of each anomaly in the network.

Table 63. Top TCP Anomalies

Unknown Monitor

The Unknown monitor provides visibility into the non-standard and custom applications running in your network.



Figure 61. Unknown Monitor – default panels

By default Soho360 recognizes every application running in the network. However only applications running over standard ports are the ones on which Soho360 applies the appropriate names automatically. Soho360 tags all traffic running over non-standard ports as **unknown**. All of them are listed as "unknown" in the *unknown monitor* as well as the other related monitors.

Note: Admin users are expected to discover their custom/non-standard apps using the "unknown" link as context in the conversation table of the unknown monitor and provide the right name in the App-definition utility. See "

Discovering Non-standard Apps using Unknown Monitor". Once custom apps are defined as described in the highlighted section, Soho360 names the application as per definition, classifies the associated traffic properly and displays the defined name in all monitors.

This is a multi-part display of contextual panels with information related to *applications*. Each part in this dashboard pertains to a specific context and has 2 or more panels, named to indicate its contents.

Top 10

The graphs in this panel display the following status about Unknown Apps.

Title	Purpose
Top 10 Unknown Apps by #Connections	This graph gives a view of the 10 unknown apps that have the maximum presence in the network. It indicates them by the number of connections v/s the %.
Top 10 Unknown Apps by Traffic Volume	This graph gives a view of the 10 unknown apps with the maximum volume of traffic in the network. It indicates them by the volume v/s the %.

Unknown apps over time graphs

The graphs in this panel display the following status about Unknown Apps at specific points in time.

- Unknown Apps Total Connections by Server Port
- Unknown Apps Total traffic over Time by Server Port

Top 10 Clients and Servers

The graphs in this panel display the following status about Unknown Apps

- Top 10 Servers with Unknown Traffic
- Top 10 Clients initiating Unknown Traffic

Top 20 Unknown Apps Conversations Table

This table has specific details about unknown apps conversations. These apps are the most rampant in the network. Use the hyperlinks (underlined fields) to view and configure the unknown application in the " [*Change*](#) Role option

App Definition" page.

<i>This field...</i>	<i>Indicates...</i>
Server IP	The IP address of the server.
clientIp	The IP address of the client.
Server Port	The port ID of the server.
Server Packets	The number of packets involved in the unknown app's traffic at the server.
Server Traffic Bytes	The number of bytes involved in the unknown app's traffic at the server.
Client Packets	The number of client packets involved in the unknown app's traffic at the client.
Client Traffic Bytes	The number of bytes involved in the unknown app's traffic at the client.
#Connections	The number of connections involved in the unknown app's functioning in the network.

Appendix A:

Soho360 Administration – For advanced users

Soho360 supports advanced “administrator” access to all of its configurations and settings. This access is available with the **admin** account.

Important: As already explained Soho360 provides default dashboards with pre-configured settings. The **admin** account allows full access to the configuration and settings, however, it is highly recommended **not to change** any settings using this account. Changing the settings in the dashboards or deleting workflows can impact your Soho360 adversely causing irrecoverable effects. Users in this role are expected to be able to troubleshoot issues if any arise in the network, using the default dashboards and their workflows. However, in case of any difficulty with respect to using the advanced administrative features, contact ThoughtData technical support for assistance.

Administrator access to Soho360

Administrator access is available with the following credentials:

- account/username: **admin**
- password: thoughtdata1

Perform the following steps when you see the log in page on starting up Soho360 (see Figure 1).

Step 1. Click **Log in**

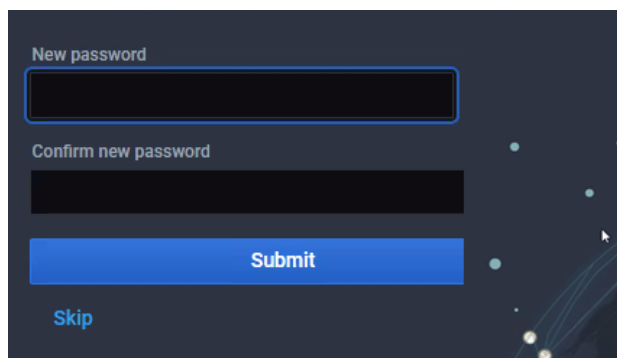
The image shows a dark-themed user interface for changing a password. At the top, there is a label 'New password' above a rectangular input field. Below this is another label 'Confirm new password' above a second rectangular input field. Underneath the input fields is a prominent blue button with the word 'Submit' in white text. To the left of the 'Submit' button, there is a 'Skip' link in a lighter blue color. The background of the interface is dark with some faint, abstract light patterns on the right side.

Figure 62. Change password or “Skip” to continue

Step 2. If you opt to change the password at this point:

A. Type as described below.

- In the **New password** box: type your preferred password. Ensure it is a strong password.
- In the **Confirm password** box: re-type the password.
- Click **Save** to save the changed password.

Note: The new password has to be at least 4 characters long.

B. You can opt to skip this step if you do not wish to change the password.






Click **Skip** to continue.

Role Privileges

Soho360 includes 3 categories or roles of users:

1. Admin – the user with the maximum privilege. Users in this role can define users in all three roles.
2. Editor – this role is meant for all network users who will use the workflows and the options available across the system. Editors cannot define users in the system.
3. Viewer - this is the default role assigned to every newly created user. In this role users cannot execute the options in Soho360. They can merely view the user interface, data and the menu options.

The left pane includes options specific to the tasks that they are permitted to perform in their roles. The table below illustrates the option-icon, the related role and the action.

Option	Sub Options(tasks)	Role	Action
		All roles	Go to the starred Soho360 Home Dashboard.
	Search	All roles	Search/locate dashboards saved in the system.
	Create Dashboard Folder Import	Admin Editor	Create dashboards, folders, import dashboards saved as JSON files.
	Dashboards Home Manage Playlists Snapshots	Admin Editor	Manage Dashboards and folders, playlists and snapshots.
	Explore	Admin Editor	Run queries on the database and format the result in multiple formats.




















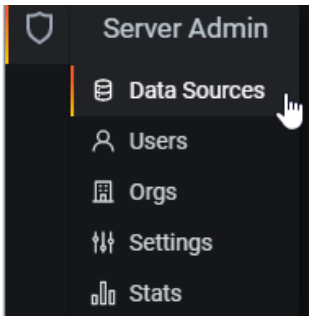
Option	Sub Options(tasks)	Role	Action
	Alerting  Alert Rules  Notification channels	Admin Editor	Set alert rules and notification channels.
	Configuration Sensor Management App Definitions Site Definitions	Admin	Oversee the status of the sensors, applications and sites in the network.
	Server Admin  Data Sources  Users  Orgs  Settings  Stats	Admin	Control the entities listed in the menu.
	 Preferences  Change Password  Sign out	All roles	This is the logged-in user's menu, with relevant options.
	Enterprise360  Documentation  Support  Licensing  Keyboard shortcuts Help	All roles	All roles can use options in this menu for online help and other useful details.

Table 64.Left-pane Options, Tasks and Roles

Soho Administration

Persons with administrative responsibilities in the network are expected to be assigned the “admin” role and associated privileges.

Important: Other end-users are not expected to be designated as “admin” and therefore will not see and use this functionality. The options in this menu have to be used with care and responsibility.



Note: users who are not in “admin” roles can skip this section of this document.

Option	For
Data Sources	Viewing (only). Administrators can explore data sources that are auto provisioned out of box.
Users	Adding and saving <i>users</i> according to the roles they will be assigned with respect to their responsibilities in the small-business or home network.
Orgs	Viewing (only) of the organizations .
Settings	Viewing system settings across Soho360. Note that these cannot be changed and saved from this interface. All settings must be defined in the system files. <ul style="list-style-type: none">- grafana.ini or- custom.ini or- overridden in ENV variables.
Stats	Viewing statistics related to users and user types, active users, roles, sessions and more in the Soho360 system.

Table 65. Admin options

Note: Admin users can set their own order of usage of the options in the Server-Admin menu. However, it is recommended to get started by setting up users in Soho360.

Adding Users

Soho360 users can be one of the following:

- Admin
- Editor
- Viewer

Soho360 allows the following methods of adding users

- static method - using the Soho360's "Add User" option to add one user at a time.
- single sign-on - using a key to allow users to login using their Office 365 credentials.

Adding Static users

Perform the following steps to add users

Step 1. Click **Server Admin** > Users in the left pane menu. The manage users page appears as illustrated.

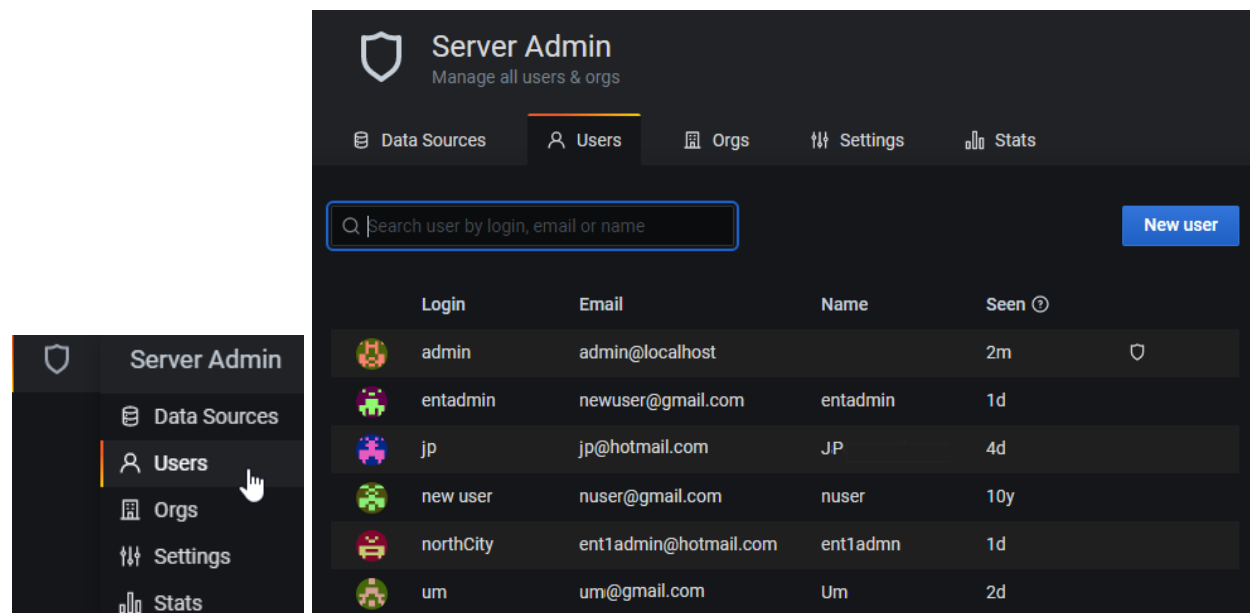


Figure 63. Server- Admin > Users > Manage all users and orgs

Step 2. Click **New user**.

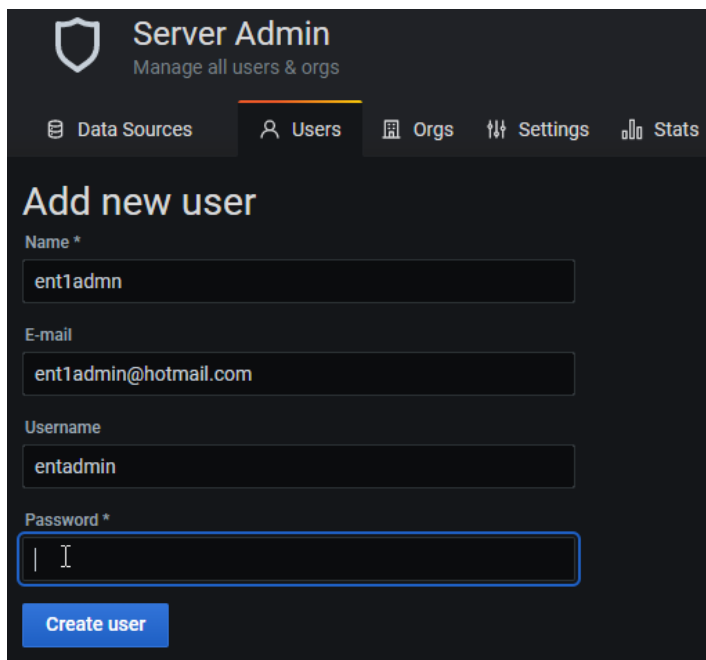


Figure 64. Add new user window

Step 3. In the fields here type details as described below.

Field...	Type...
Name	Any text to give a meaningful identity for the user. This can even be the proper name of the user – even First-Name Second-Name.
Email	A unique email id that works for the user. This has to be unique and not previously used for any user in the system.
Username	Any text to give a meaningful identity for the user. This is for use during login.
Password	A unique string of text of at least 4 characters. Note that the end-user can change this to a combination of alphabet, numeric and special characters to make it a strong and secure password known only to the user.

Table 66. User Information

Step 4. Click **Create user**.

In case of duplicate entry in any of the fields here the error message appears as illustrated.

 **User with email 'ent1admin@hotmail.com' or username 'entadmin' already exists**

Step 5. Make corrections and do as in step 4.

The pop-up  **User created**  appears to indicate that the step is complete.

Changing User Properties

Users created by either of the methods described above, are by default designated as “viewer”. Based on their official role the administrator can perform the following for the selected user:

- Change any or all of the “user information” details
- Delete from the database
- Disable from using the system temporarily
- Change role

Note: *The options*

- “Add to an organization” need not be used because users are added by default to **main org** by default.
- “Remove from the organization” is not recommended for use.
- “Disable user” is recommended for use to stop access to Soho360.

Change user information

Step 1. From the Server- Admin > Users window (see Figure 63) highlight a user’s row in the table. Click to select the user.

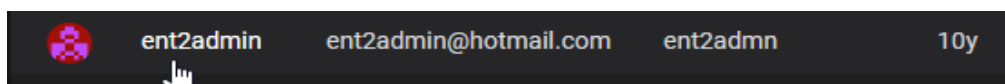


Figure 65. Select a user from the table

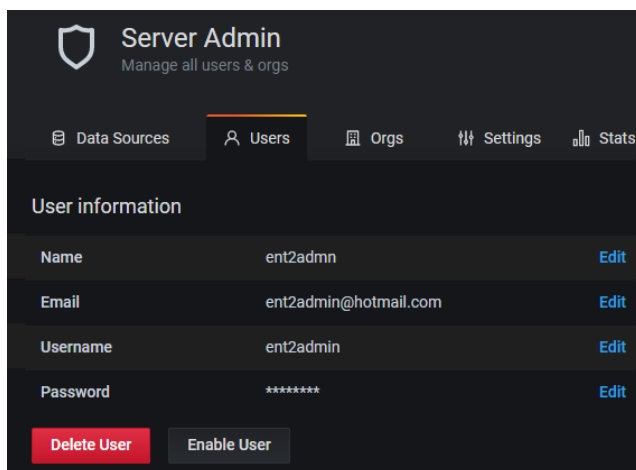


Figure 66. Users > Selected user window – 1 User information tab

Step 2. Use the options here as described below.

Option...	Click to...
Edit	Make changes to Name, email, username and password of the selected user.
Delete user	Delete the user.
Enable user	Enable the user.

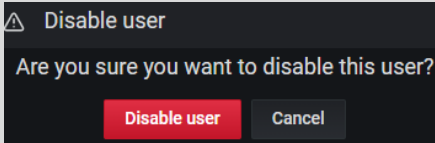
Option...	Click to...
	Note: When enabled, the option appears as Disable User , click to change.
Disable user	<p>Disable the selected user.</p>  <p>The user table indicates that the user is disabled.</p>

Table 67. User Information

Step 3. Use the option in the permissions section as described below

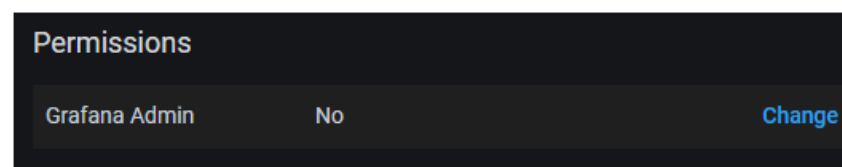


Figure 67. Users > Selected user window – 2 - Permissions

Option...	Click to...
Change	Change the "Grafana Admin" privilege for the selected user. Note that this privilege is not applicable for users other than those in the "Admin" role.
Yes/No	To grant the privilege/to delete the privilege. This is one way of changing the user role from "Viewer".
Change/Cancel	<p>Change the permission or cancel the change request.</p> <p>Note: When enabled, the option appears as Disable User. Click to change to enabled.</p>

Important: The next option in this page Organization is **not** for use by any role.
Do keep in mind that

- no user should add a **new organization**.
- by default new users are added to **main org** therefore users need not be added to an organization.
- the existing data concerning Organization should **not** be changed.

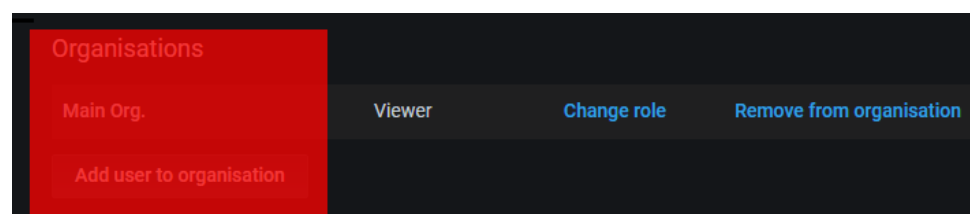


Figure 68. Organization section and options – not for use

Important:

Soho360 users can belong to **one** or **more** organizations, but each would have the following unique resources which cannot be shared across organizations.

- dashboards
- data sources
- configurations

In both cases, since these resources are associated with the definition of the organization, making alterations to it can amount to a “factory reset” situation and force users to re-do all the customization accomplished till date.

Step 4. Click **Change role**

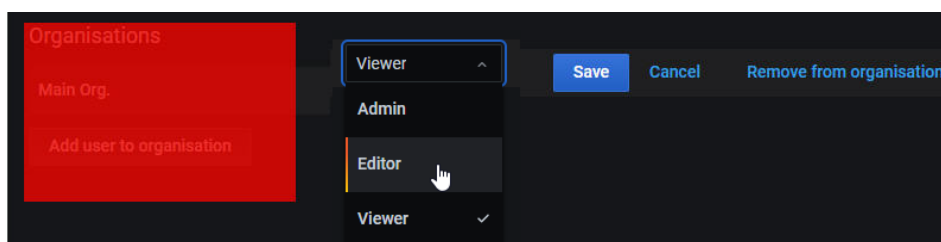


Figure 69.

Step 5. Use the **Change role** option in the Organizations section, as described below.

Option...	Click to...
Roles drop-down menu	View the list of roles. You can then click <ul style="list-style-type: none"> - Editor to set that as the role for the user. - Admin if the user has administrative responsibilities.
“Save”	Set the selected role for the user.
“Cancel”	Retain the Viewer role for the user.
“Add to organization”	By default new users are added to the default organization. “Main Org.” Note: Users can ignore this option.
“Remove from Organization”	View the option to confirm removal. <div> <div>Confirm removal</div> <div>Cancel</div> </div> <p>Click “Confirm Removal” option to remove the user from the selected organization.</p> <p>Note: Use this option with care. It is recommended to use the options “Delete User” or “Disable user”, instead.</p>

Table 68. Change Role option

App Definition

NetSense (packet sensors) instrumented in the network “auto detect” the applications deployed and running in the network.

Applications which use *standard ports* also termed “standard applications” are recognized by Soho360. Network users don’t have to concern themselves about configuring details about such apps. However, customer-applications and other applications that use *non-standard ports* need to be discovered and identified using the “App Definition” options in this page.

Note: Till they are configured in Soho360 all such applications are classified as “unknown”. The “App Definitions” option provides a mechanism for users to name such applications. Once defined Soho360 removes the unknown label and classifies them in the main data sources with the new name.

Perform the following steps to manage apps in the Soho360.

Step 1. Click  in the left pane menu.

Step 2. Click “App Definitions”.

Or if you are already in the configuration page, click “App Definitions”.

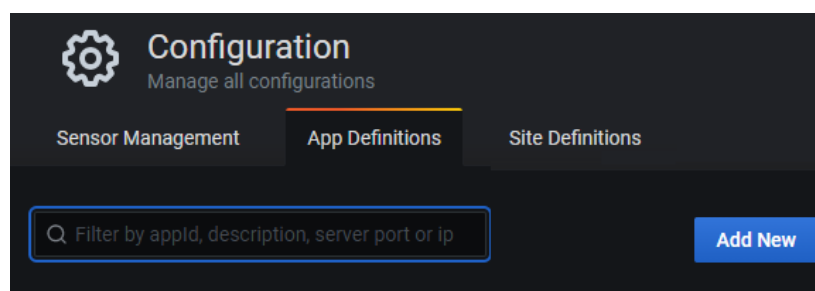


Figure 24. Apps to be added in the system

The apps in the system would be listed in this page.

Important: The App Definitions list is blank during the 1st instance of using Soho360. The administrator is responsible for locating the non-standard apps by using the in-built Soho360 workflow “unknown monitor” and adding to this list.

Discovering Non-standard Apps using Unknown Monitor

Any network would have several custom or off-the-shelf applications (also referred to as apps) running continually. As the network administrator, it is assumed that you are aware of the **port number** assigned to the non-standard applications functioning across your network. Based on this data you should be able to locate these app(s).

Perform the following steps to locate non-standard apps.

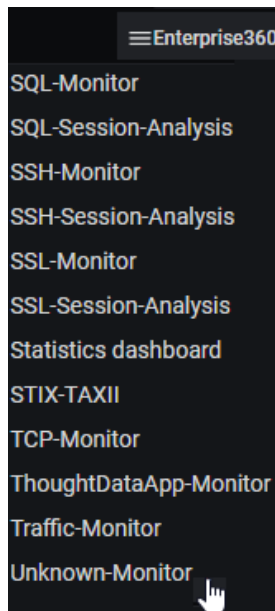


Figure 70. Soho360 Menu of dashboards

Step 1. In the top right **Enterprise360** menu scroll to and click **Unknown-Monitor** as illustrated.

The **Unknown-Monitor** dashboard is displayed with details about traffic that is getting classified as unknown, number of connections and volumes of that type of traffic.

Typical controls in this dashboard are:

- Top 10 Unknown Apps by #Connections
- Top 10 Unknown Apps by Traffic Volume
- Unknown Apps Total Connections over Time by Server Port
- Unknown Apps Total Traffic over Time by Server Port
- Top 10 Servers with Unknown Traffic
- Top 10 Clients initiating Unknown Traffic
- Top 20 Unknown Apps Conversations

The table “Unknown Apps Conversation” at the base of this dashboard has the essential attributes of the unknown apps and serves as a context for defining the app in Soho360.

See highlight in Figure 71.

Note: All dashboard illustrations are to be considered as typical samples only. They are used for providing a visual reference only. Your set up may not match with the illustrations in this document.



Figure 71. Unknown Monitor – multiple client and server views – unknown Apps

Each record in the table “Top 20 Unknown Apps Conversations” represents an *application conversation* that runs on non-standard ports and not recognised by Soho360. As the administrator it is assumed that you are aware of these apps based on the server port id detected. Use the context option in this table – see the highlight in Figure 71 above, to define each app in the system now.

Perform the following steps to define the app in Soho360.

Step 2. Click the ip-address field or the server port field in this table as illustrated below.

Top 20 Unknown Apps Conversations						
<u>95.217.167.136</u>	8.6.144.233	<u>1194</u>	Define App	325.35 K	10.59 KiB	5 K
<u>78.47.169.156</u>	162.253.68.117	<u>1194</u>		298.54 K	9.72 KiB	5 K

The New App Definition page appears as displayed.

Step 3. Type the name of the application assigned to the port as illustrated in the example below.

New App Definition

Description

internet-banking-www

Server Port

1194

Server IP

95.217.167.136

Create

Cancel

Figure 72. Enter App details -example

In the Field...	Type the...
Description	Name of the App that runs on the selected server port number.
Server Port	Port number used by the app – as displayed in the dashboard table.
Server IP	IP address to be associated with the app – as displayed in the dashboard table. This is an optional entry.

Note: If you want a specific custom app e.g. internet-banking-www to run on a selected server, only that Server IP address needs to be identified for that custom app.

If you do not wish to associate the server IP with the app, you can leave this field blank. In which case all Server IP addresses with the selected server port number (in this case 1194) will be associated with the specified app definition - as in this example: internet-banking-www.

Step 4. Click **Create** to save the app definition.

Repeat Step 1 to Step 4 for all the apps detected by the unknown monitor workflow.

If you wish to make changes to the entries at any point use the left pane options as illustrated.

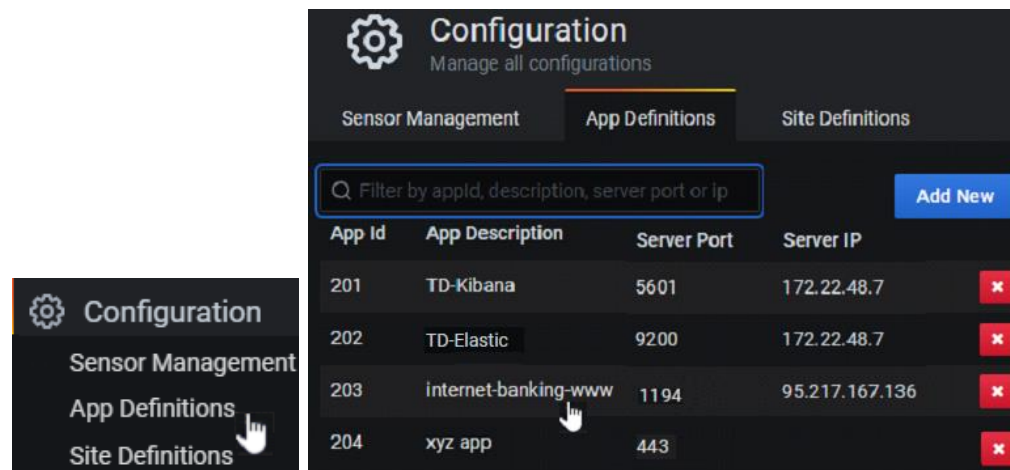


Figure 73. App Definitions – with multiple non-standard apps identified in Soho360

Step 5. Click the relevant App Description.

The selected app's details are displayed as illustrated below. Note that the highlighted text indicates that the fields can be changed. Others fields are read-only.

Label...	Description ...
App Id	203
Description	internet-banking-www
Server Port	9200
Server IP	95.217.167.136

Figure 74. Edit a selected App details

Label...	Description ...
App Id	Indicates the App's ID in the network.
Description	Indicates the name of the App. Users can make changes to this entry.
Server Port	Indicates the port assigned to the app. Users can make changes to this entry.
Server IP	Indicates the IP address assigned to the app.

Step 6. Make changes in the fields if you wish to: "Description" "Server port" and "Server IP".

Step 7. Click **Update** to save the change.

Note:

- Changes made to site definition become effective after 15 minutes of saving the changes.
- Historical data – including the data that existed prior to this change, will not be amended by the changes made to site definitions.

Site Definition

NetSense (packet sensors) use the client and server IP addresses observed in the traffic to automatically recognize network subnets within the network. By default:

- all internet IP addresses (servers and clients) are auto-classified in Soho360. Users need not define these sites. By default subnet IP ranges are used as site names, which can be changed to proper site names.
- all subnets seen in the traffic are classified as *IP subnet pools* and have to be given site names in Soho360.
- in addition, the geo location of the physical site has to be specified.

Soho360 then:

- removes the *IP subnet pools* and classifies the sites with the site names.
- uses the geo location configuration for plotting the sites on map based visualizations.

Perform the following steps to manage sites in the Soho360.

Step 1. Click  in the left pane menu.

Step 2. Click "Site Definitions"

Or if you are already in the configuration page, click "Site Definitions".

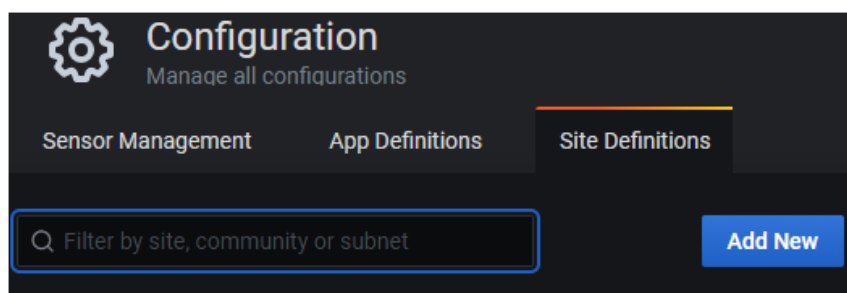
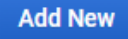


Figure 75. Site Definitions page

The Site Definitions table in this page is blank during the 1st instance of using Soho360. Administrators who are responsible for naming the sites can get started by:

- clicking , if they are well aware of their virtual sites and the geographies they belong to.

or

- using the in-built workflow "Site Monitor" and adding to this list.

Note: "Site-Site Conversation Tables" are available in multiple in built workflows. Site monitor is one of them. The Soho360 dashboard also has site-site conversation data. This section explains the procedure to define sites using the "Site Monitor" workflow.

Creating Alerts

Workflow alerts and notifications enable network support staff to take timely action on events that reach and exceed a pre-determined time and value threshold.

Users can set alerts on

- existing time series based charts in any of the out of box dashboards and
- custom built time series charts in their custom dashboards.

Alerts can be set for over-time trend charts, as in the sample illustrated below, while creating or editing a dashboard or workflow. You can add alerts and configure them in the “Alert Tab” of any dashboard’s graph panel.

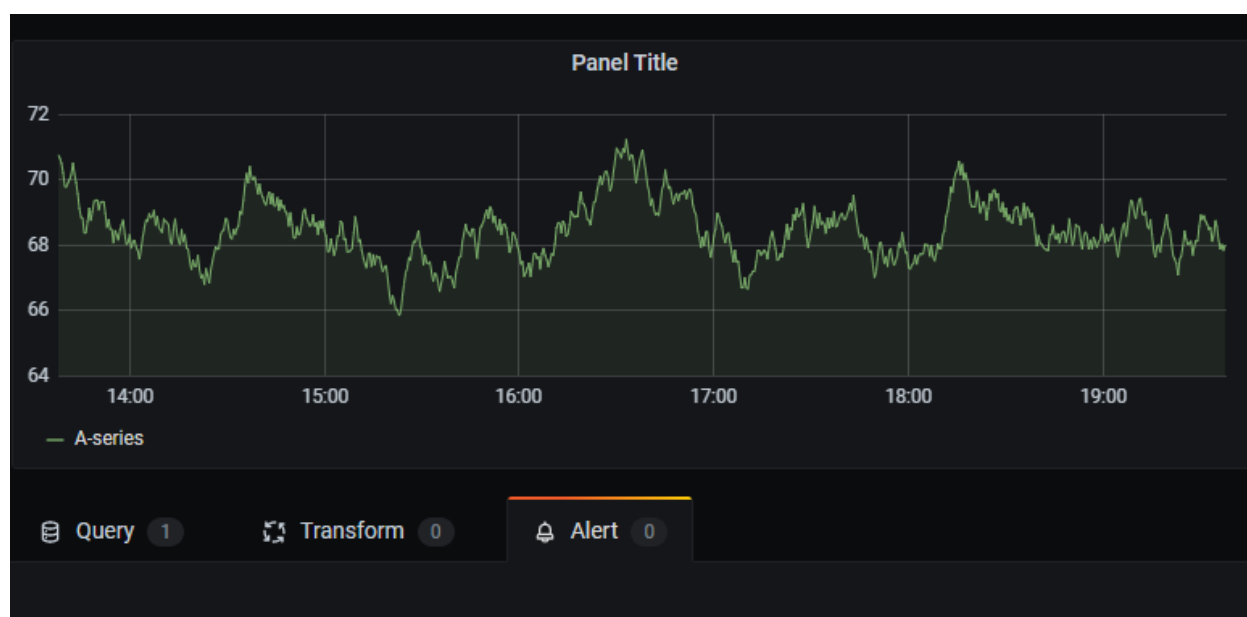


Figure 76. Graph Panel - Alert Tab

The following elements synch up in the steps to create Soho360 alerts:

- database **queries** created using relevant data sources.
- **rules** with time and threshold **conditions** set against the queries.
- notification channels

The data sources that support creation of database queries must be used while creating alerts.

Rules can be set in workflows that include time based charts, and can be managed from using this option.

Notification channels such as email, text-sms can be set for a target group to receive the notification when particular workflow rule is triggered.

Note: If the selected data source is not relevant to the workflow you may see the error message indicating that the data source does not support alerting queries.

Sample Alert – App Latency over Time

This sample chart “Worst Apps by Average App Latency over time” is part of the Soho360 dashboard. It also has panels for query, rule, conditions and alert, as illustrated below.

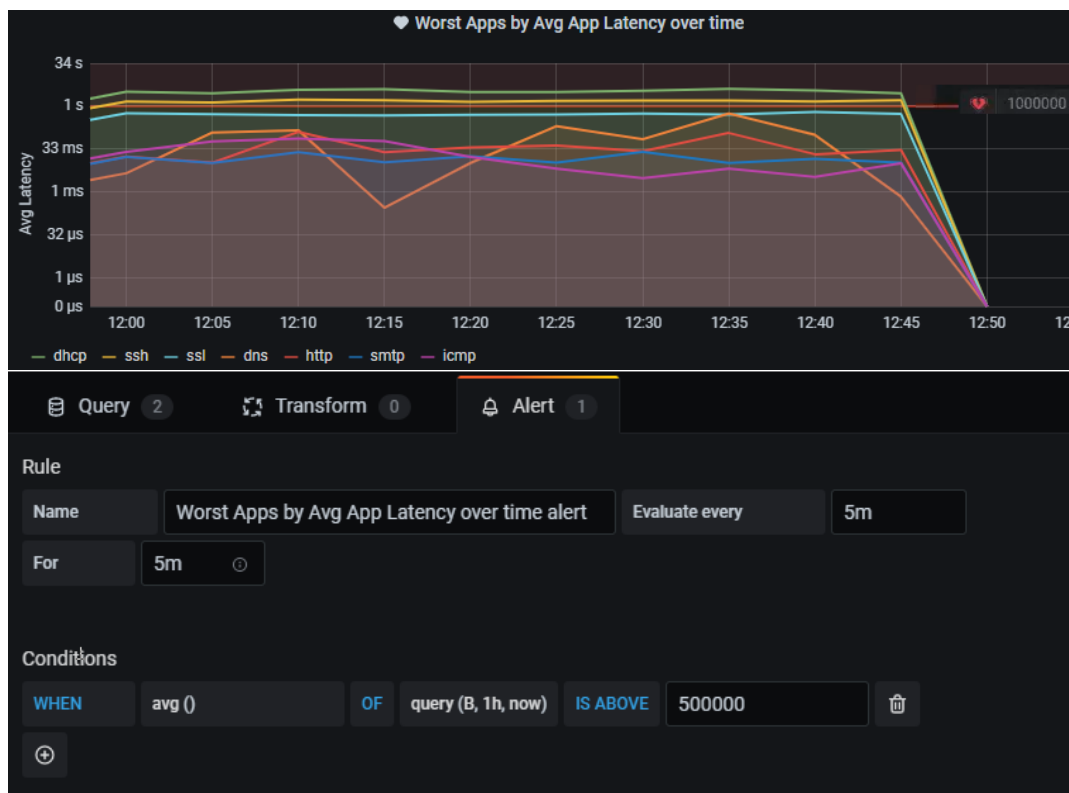


Figure 77. Sample Over-time trend chart - Query, Rule and Condition

You can define an alert per query. Note that in this sample chart

- there are 2 queries and one alert.
- query “B” indicates that the alert is being defined for query B.
- when the alert is active, the threshold is highlighted at the top of chart.

Condition

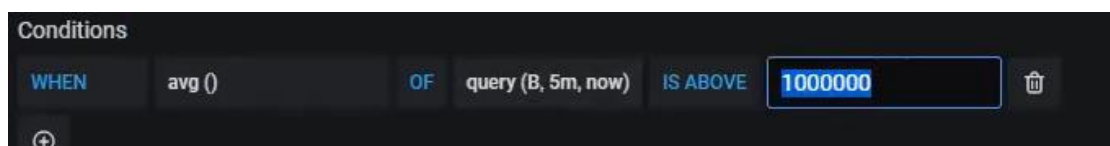


Figure 78.

The condition for the alert, is when

- **avg ()** average of query B,
- **query (B, 5m, now)** 5 minutes from now
- is greater than **1000000**.

Rule

Rule					
Name	Worst Apps by Avg App Latency over time alert	Evaluate every	5m	For	5m ⓘ

The rule is to evaluate the condition every 5 minutes for 5 minutes.

Query

Query B uses the following criteria

- Average response time
- application
- and timestamp

To find

- the application with the highest “average response time” an
- if the average response time is greater than **1000000**.

Test the alert

State history	Test rule	Delete
---------------	-----------	--------

Click **Test rule** to test if the conditions function as expected.

```
Testing rule
Object
  firing: false
  state: "no_data"
  conditionEvals: "false = false"
  timeMs: "46.253ms"
  logs: Array[3]
    0: Object
      message: "Condition[0]: Query"
      data: Object
    1: Object
      message: "Condition[0]: Query Result"
      data: Object
    2: Object
      message: "Condition: Eval: false, Query Returned No Series (reduced to null/no value)"
      data: null
```

Figure 79. Test Rule

Notification

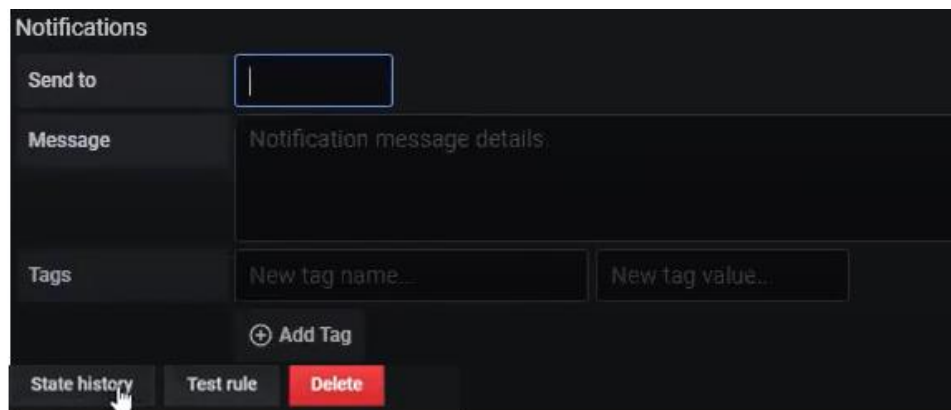
The screenshot shows a dark-themed interface for the 'Notifications' tab. At the top, there's a 'Send to' field with a dropdown arrow. Below it is a 'Message' field with a placeholder text 'Notification message details'. Underneath the message field are two input fields for 'Tags': 'New tag name...' and 'New tag value...'. A '+ Add Tag' button is located below the tag fields. At the bottom of the interface, there are three buttons: 'State history' (with a mouse cursor hovering over it), 'Test rule', and a red 'Delete' button.

Figure 80. Notification tab

If notification channels – email, text etc. have been added in the system, use the Notification tab to:

- Specify the channel
- Add the notification message
- Add recipients

Troubleshooting alert

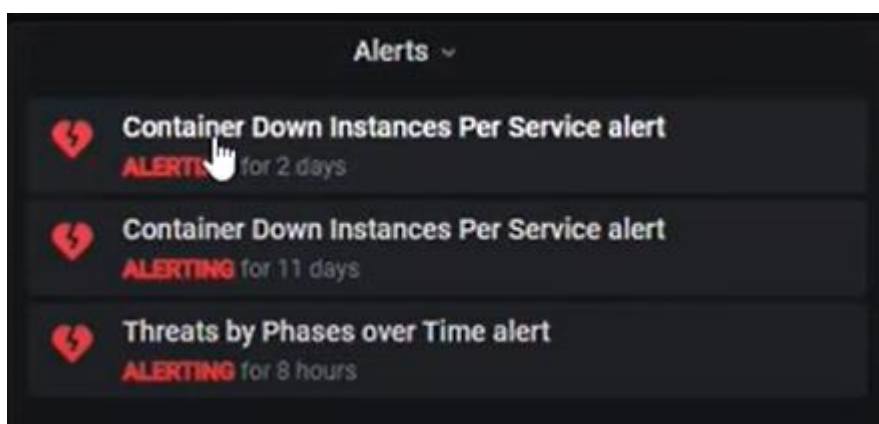


Figure 81. Alerts Panel

Note:

- to make the alert rule and changes to the rule permanent, save the dashboard.
- when the alert is fired the marker and alert appear on the panel graph.
- you can troubleshoot the alert from the chart and adjust the alert conditions if needed.

Managing Alerts

Workflow alerts and notifications can be created in workflows/dashboards as described in “Creating Alerts”. The alerts and notification channels are centrally managed using the left pane menu option and sub options as illustrated below.

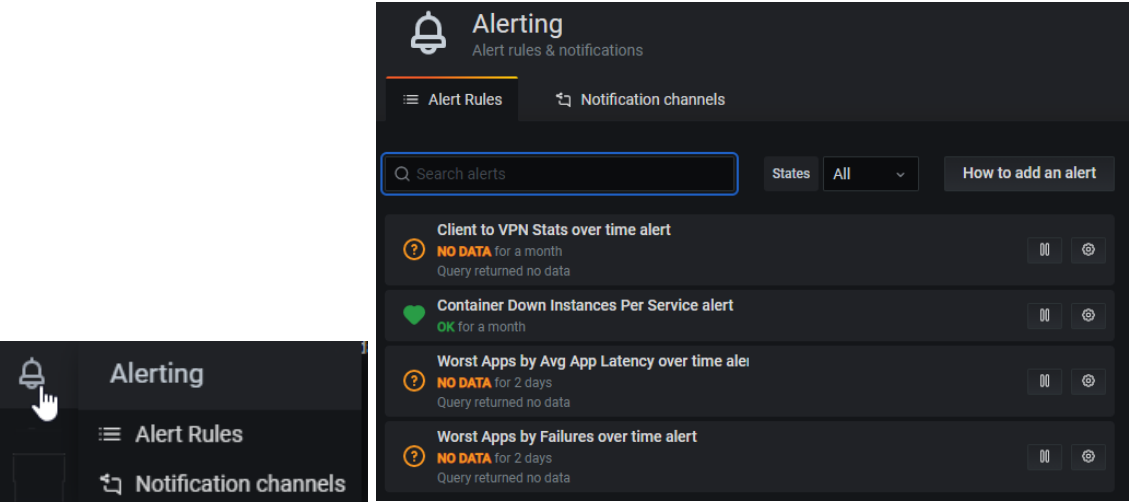


Figure 82. Alerting > Alert Rules – in the system across workflows.

Alert Rules

Alerts and notifications are created as part of creating or modifying the workflows or the Soho360 Dashboard. However, all alerts created and saved in the system can be centrally managed from the “Alerting” Page.

In the table of alerts in this page:




Menu option...	Description ...
 Client to VPN Stats over time alert NO DATA for a month Query returned no data	These are alerts set in the system. Click each alert to <ul style="list-style-type: none">- view it in its dashboard panel,- troubleshoot it and- edit it.
	Click to <i>pause</i> an alert rule. Note the warning and take appropriate action.
	Click to edit the rule.
How to add an alert	Click to read a short note about adding alerts.

Table 69. Alerts Table

Notification Channels

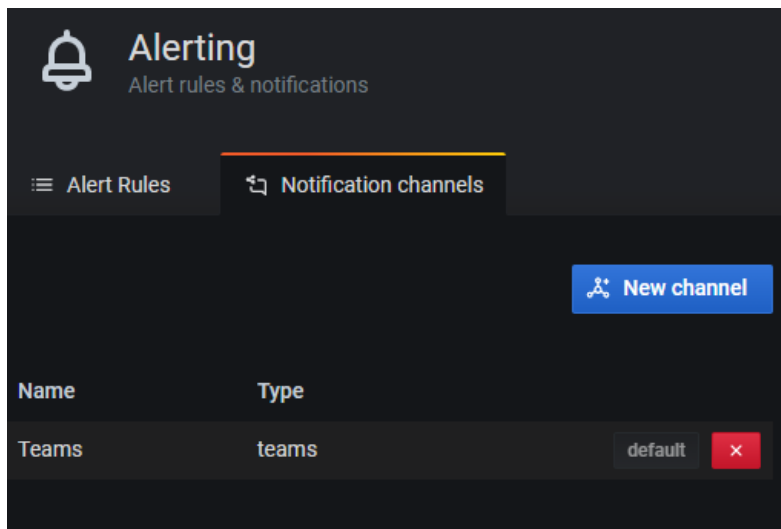


Figure 83. Multiple Notification Channels for sending the alerts

Perform the following steps to set notification channels for the alert.

Step 1. Click **New channel** to select any of the configured channels in the system as illustrated.

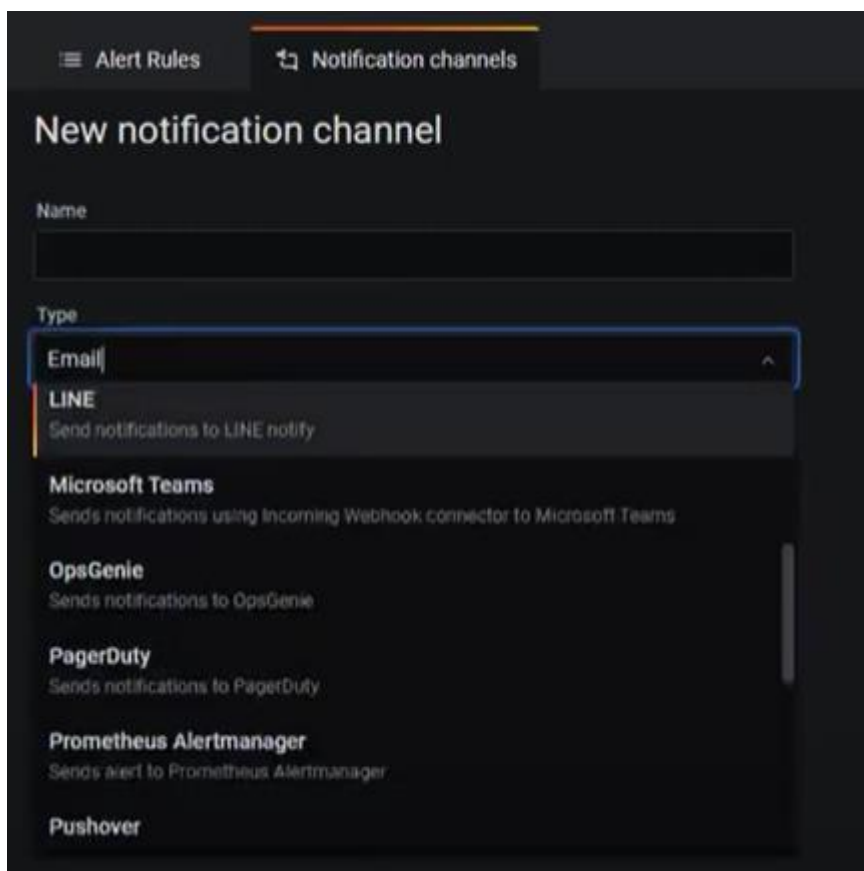
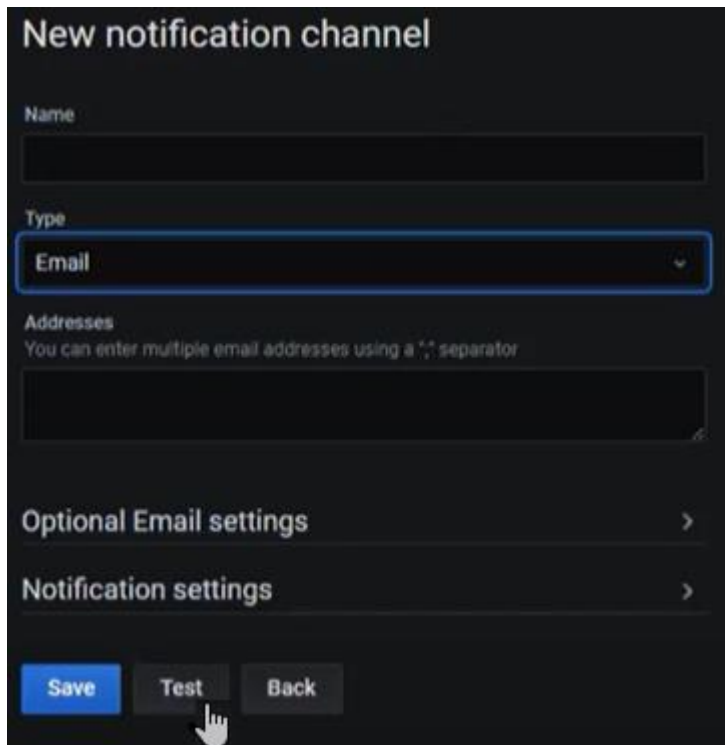


Figure 84. Adding Notification channels



New notification channel

Name

Type

Email

Addresses

You can enter multiple email addresses using a "," separator

Optional Email settings >

Notification settings >

Save Test Back

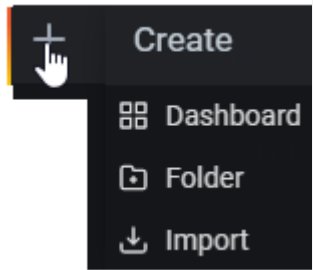
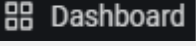
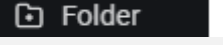
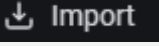
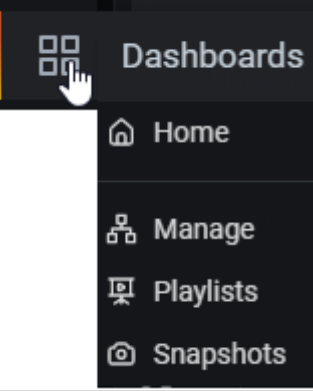
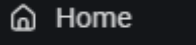
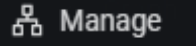
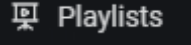
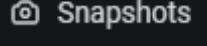
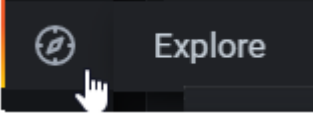
Figure 85. Test the Notification Channel

After the notification channels are added and tested, they can be specified in the workflow. Based on the settings the notification is sent to the target recipients.

Explore to build your own Dashboards

The left pane options are available to the roles "Admin" and "Editor" for

- Exploring the Soho360 Data Sources
- Creating Dashboards
- Setting up folders in which to save them

Menu icon...	Description ...
	Available for Admin.  Dashboard - click to create dashboard  Folder - click to create a folder  Import - click to import
	Available for Admin and Editor.  Home  Manage  Playlists  Snapshots
	Available for Admin. Click to explore the Soho360 data sources, prior to getting started with creating personal dashboards.

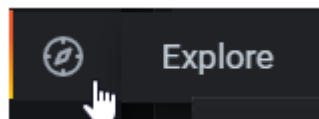
Exploring the Data Sources

Soho360 auto provisions all data sources during installation with relevant configurations

Users in the role “Admin” can explore these data sources, to understand them prior to:

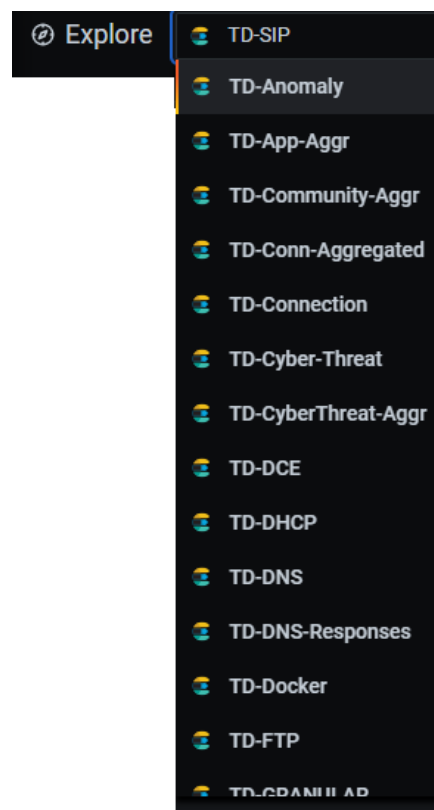
- building their own dashboards with visualizations spanning across multiple data sources, or
- edit the readymade/out of the box dashboards to format their preferred workflows.

This section describes the structure of a record in each data source, the fields in each record and the values in each of the fields. Users can refer to the tables in this section to understand the data to structure their queries and dashboards.



Step 1. Click

Step 2. Click the drop-down ion and select any data source.



Types of Data Tables

The Soho360 database supports the following types of data tables.

- Raw data tables
- Aggregation data tables

Raw Data Tables

These tables hold data as received directly from NetSense (packet sensors) and InfraSense (log sensors) in the network. Soho360 adds and maps description to values in some of the fields.

The data tables are referred to as **granular data** and represent the lowest granularity of data available in Soho360 for troubleshooting.

Granular data is required for detailed troubleshooting only for incidents and represents the highest volume of data in Soho360.

Data retention in your storage resources depends not only on the available disk space; it also depends on the **retention period** configuration set for the granular data tables.

This configuration is set during installation of Soho360, however, network administrators can change the retention period setting post installation after a first-hand experience of data collection and size of data required for troubleshooting in your network.

Aggregation Data Tables

Soho360 performs hourly, daily, weekly and monthly data aggregations on granular tables to keep summary information for various critical KPI(key performance indicators) for longer time periods.

The volume of aggregated data retained in Soho360 depends on size of disk available and configuration set for various aggregated data tables retention periods during installation.

Data retention in your storage resources depends not only on the available disk space; it also depends on the **retention period** configuration set for the Aggregation data tables.

This configuration is set during installation of Soho360, however, network administrators can change the retention period setting post installation after a first-hand experience of data collection and size of data required for troubleshooting in your network.

Note: Refer to the **ThoughtData Data Sources Guide** to understand the data organization and characteristics of the data sources. Use this information to build and save your dashboards.

Important: in addition to creating dashboards of your own, you can tweak the Soho360 default out-of-the-box workflow or dashboards. However, before you get started on that course, make sure you save a copy of the dashboard file, work on the copy, refine it till everything works to your preference.

Create your Own Dashboard

With a working knowledge of the data sources you can build a dashboard.

Use the procedure below to create the following:

- A sample dashboard with:
- a timeline graph of server traffic in bytes per application
- a pie chart of the same data both from a single data source.
- a mixed graph from multiple data sources.

Graph - Top Apps by Server Traffic

This is based on the data source TD-Connection; it shows over time the number of applications in the network vis-à-vis their traffic volume on the server side.

Step 1. Select data source TD-Connection



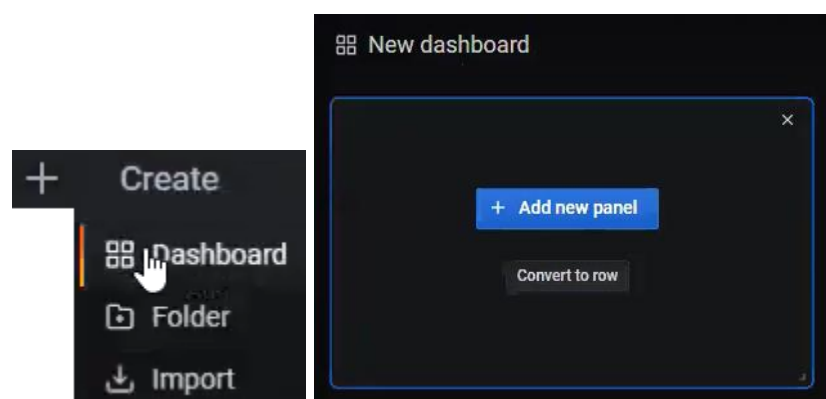
Figure 86. Select Data source TD-Connection

Step 2. In the data source, open a record and view the fields of the data source.

Step 3. Note that you should select "applicationDescription" "serverTransportBytes" and ts (timestamp)



Step 4. Click Create > Dashboard from the left pane menu as illustrated



Step 5. Click “Add new panel”.

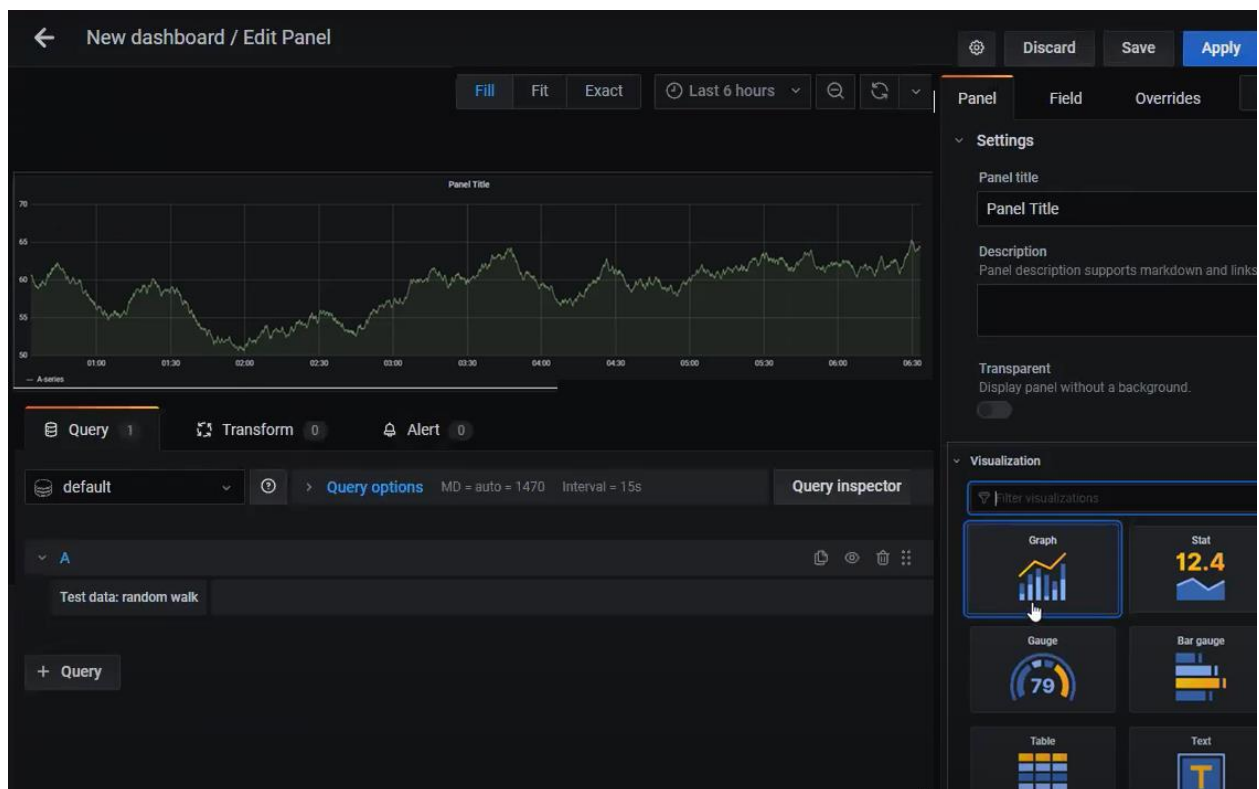


Figure 87. New Dashboard Edit Panel

Step 6. In the bottom right “Visualization” panel click Graph – note that the default visualization is “Graph”

Step 7. Select the data source TD-Connection

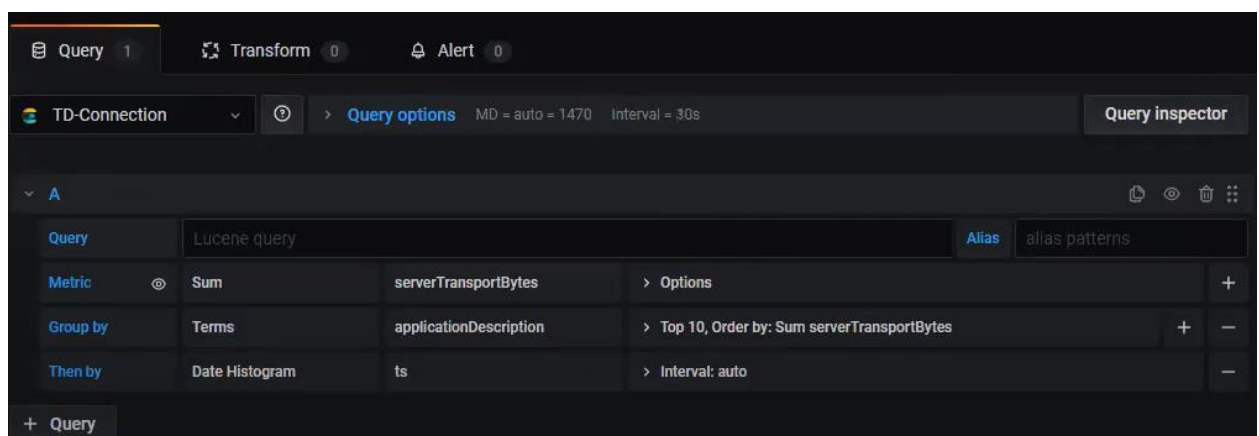


Figure 88. select table/ds/ > td connection

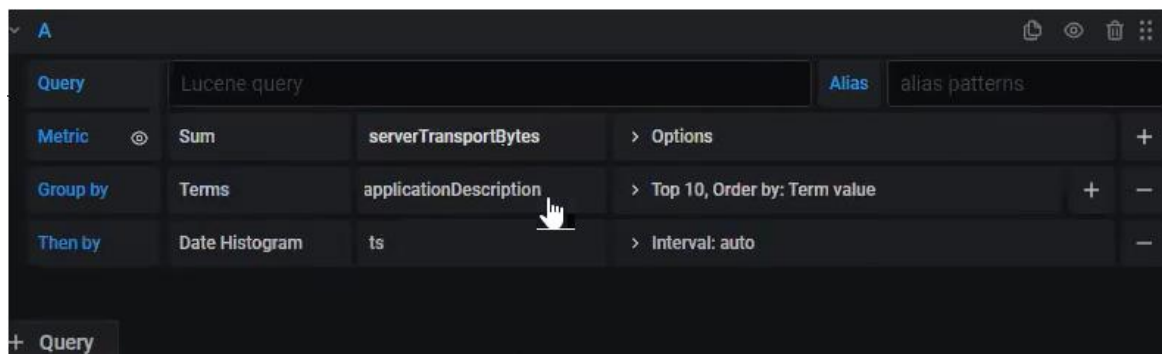
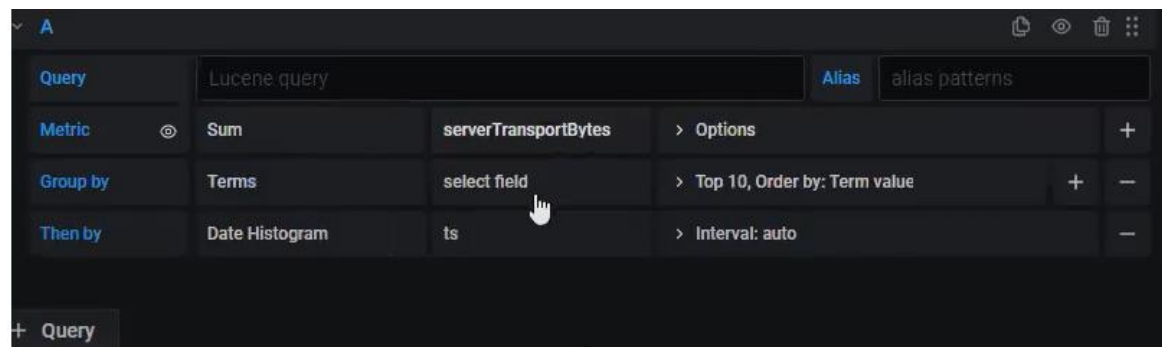
Step 8. Add Metric and Group by terms to the query.

Metric - is the actual value that you wish to see in this chart – in this case select Sum of the ServerTransportBytes

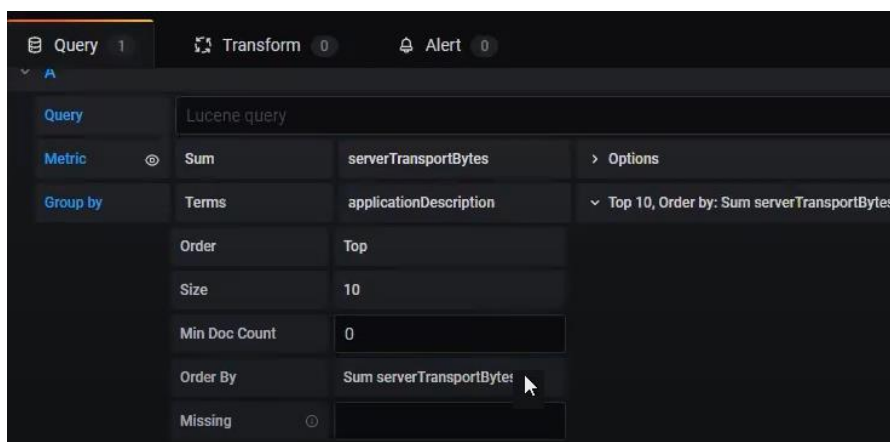
Group by - is the entity by which the information has to be grouped.

Then by - has to be the time stamp - it is selected by default-

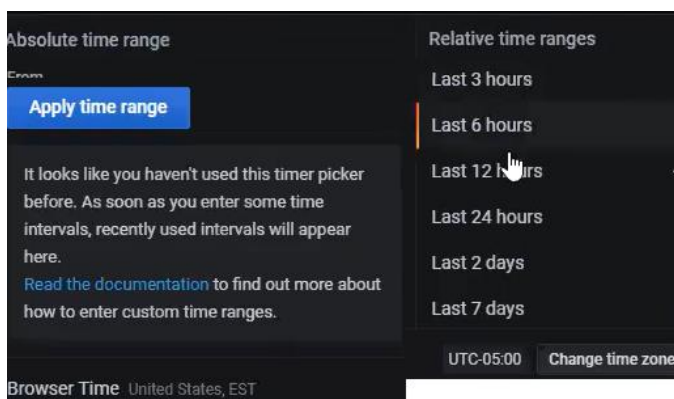
Step 9. Click  to add



Step 10. Set "order by" "Sum serverTransportBytes" for sorting.



Step 11. Apply a time range.

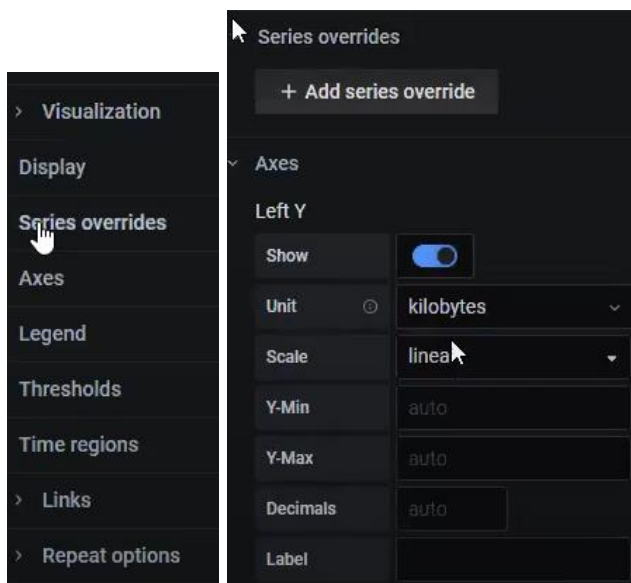


Step 12. Wait for data refresh.

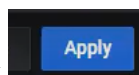
The desired graph is displayed as illustrated. It depicts how “serverTransportBytes” is changing over a period of time across each application.



Step 13. To set proper graph titles click “series Overrides” in the “Visualization” panel.

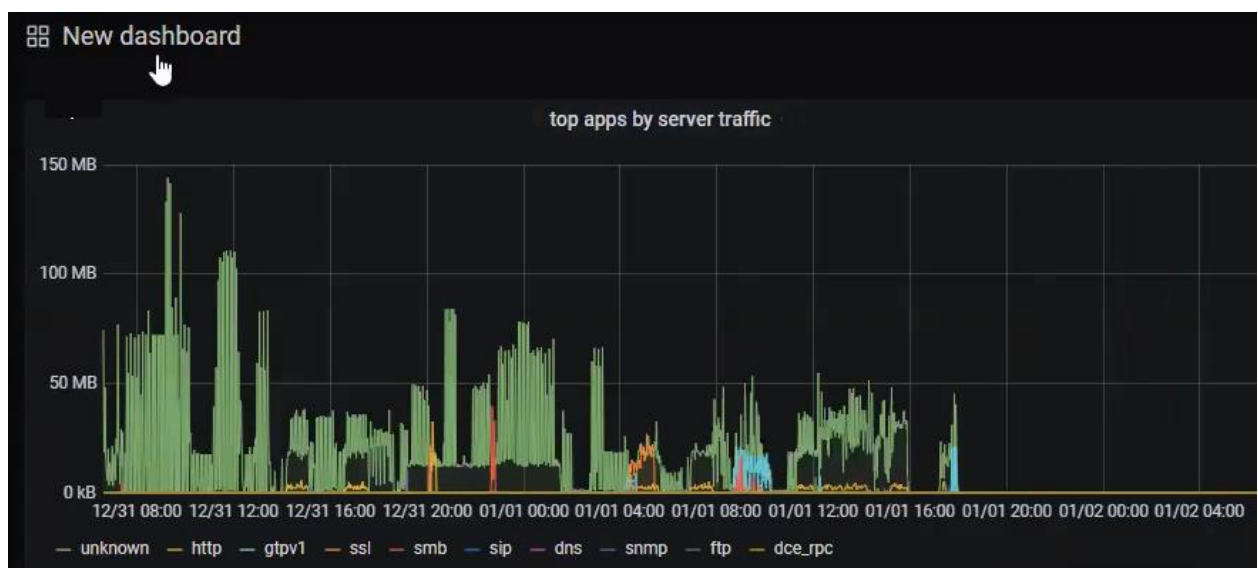
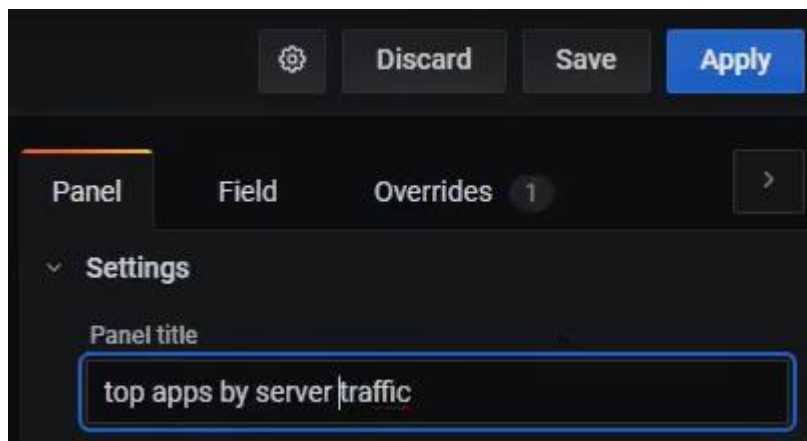


Step 14. For the Left Y Axis set unit as “kilobytes” from the drop-down menu.



Step 15. Click **Apply** in the top right menu.

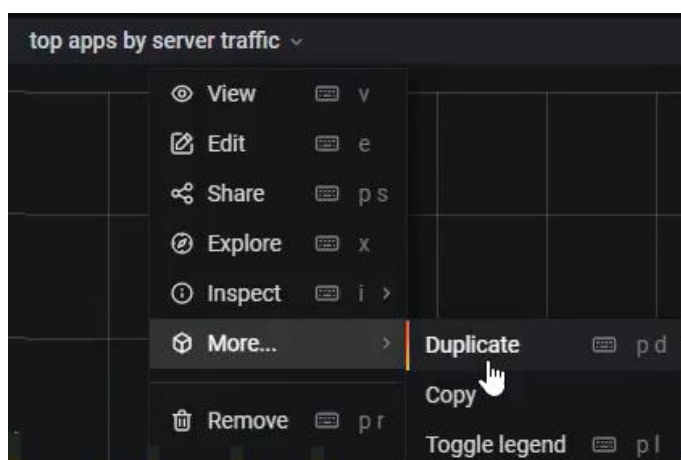
Step 16. In the top-right “Panel Settings” section, type a matching title for the graph, as illustrated.



Pie Chart - Top Apps by Server Traffic

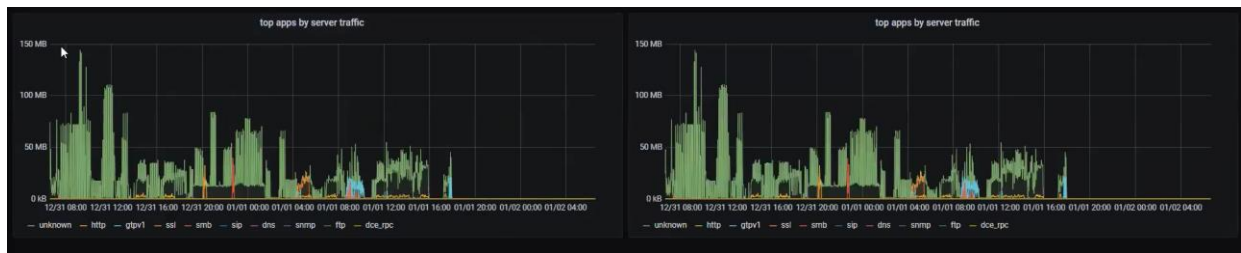
In this sample procedure, use the same query data to form a pie chart. In effect you get a Snapshot view instead of an over-time view.

Step 17. Click More > Duplicate from the drop-down menu at the top of chart.



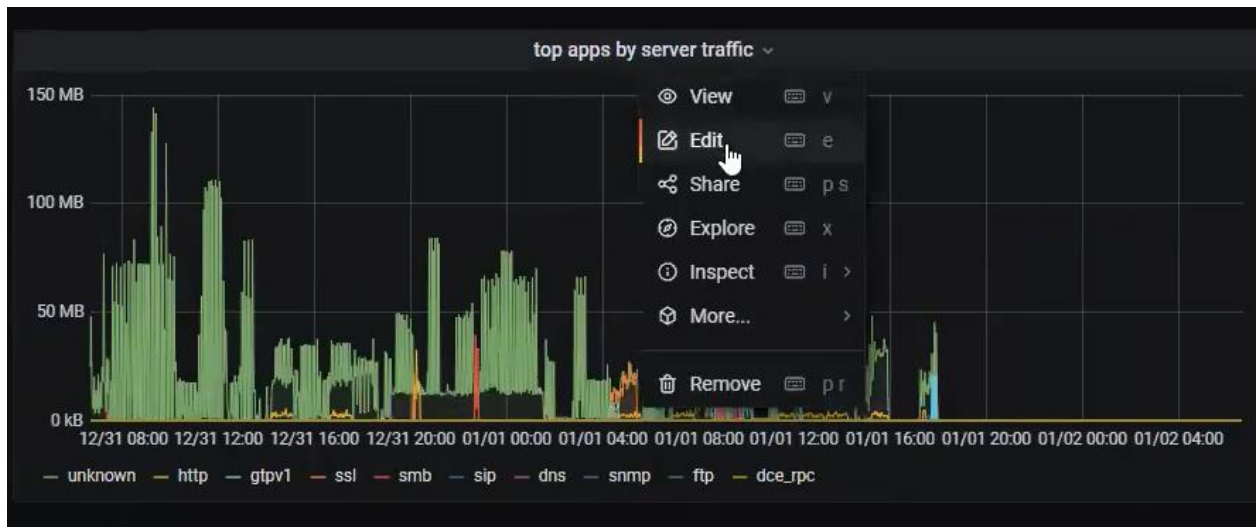
The duplicate view is at the right of the original.

Appendix A: Soho360 Administration – For advanced users

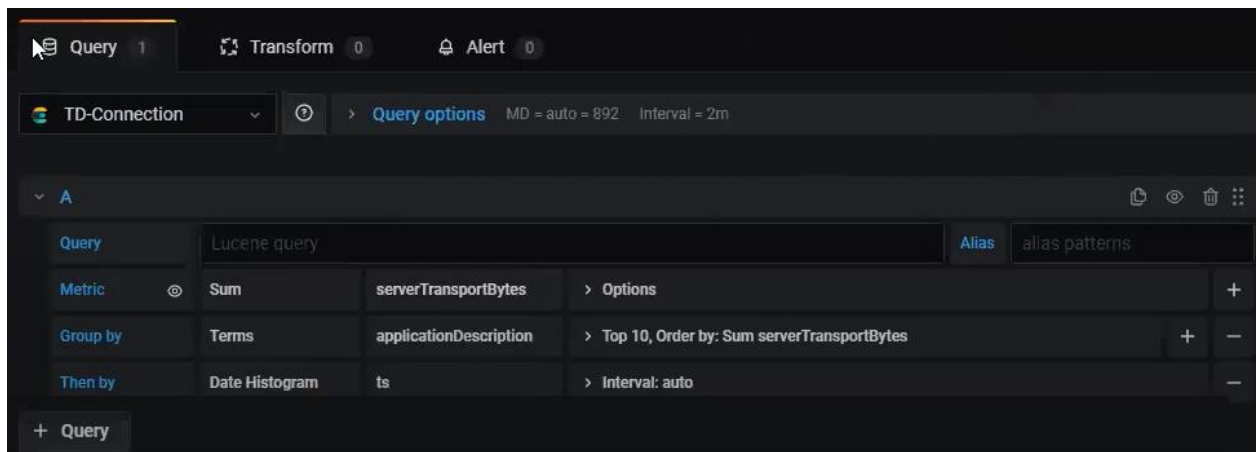


This lets you retain the query with all the related inputs as the basis of this chart, and only change the visualization.

Step 18. Click “Edit” from the top-menu in the duplicate graph.



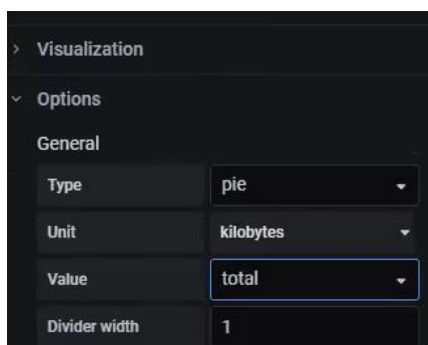
The old query details are displayed. You can view and make the necessary changes.



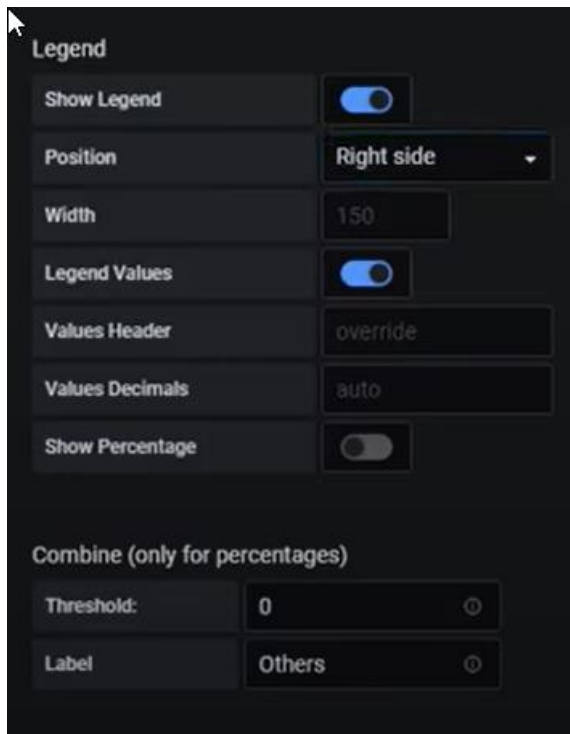
Step 19. From the right panel, “Visualization” menu select pie-chart.



Step 20. Minimize the Visualization Menu and specify Unit and Value for the pie chart.



Step 21. Change the position of the legend of the pie chart.

A configuration panel for a legend. It contains several settings: 'Show Legend' (toggle on), 'Position' (dropdown set to 'Right side'), 'Width' (input field with '150'), 'Legend Values' (toggle on), 'Values Header' (input field with 'override'), 'Values Decimals' (input field with 'auto'), and 'Show Percentage' (toggle off). Below these is a section titled 'Combine (only for percentages)' with 'Threshold:' (input field with '0') and 'Label' (input field with 'Others').

Legend

Show Legend ☒

Position **Right side**

Width 150

Legend Values ☒

Values Header override

Values Decimals auto

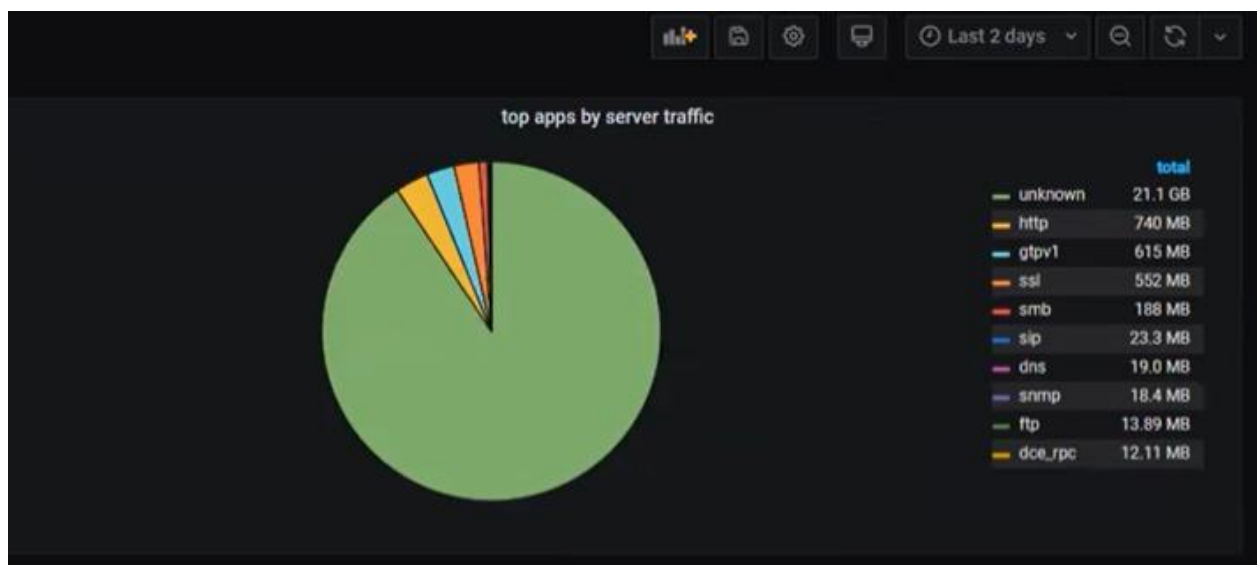
Show Percentage ☐

Combine (only for percentages)

Threshold: 0

Label Others

The pie chart now is a snapshot of which application consumed the most traffic during the specified time.



You can change the visualization further to get a “gauge” view and get a presentation of individual server data instead of total distributed server data.

Gauge Chart- Top Apps by Server Traffic

Step 1. Repeat Step 17 and Step 18 in the previous procedure.

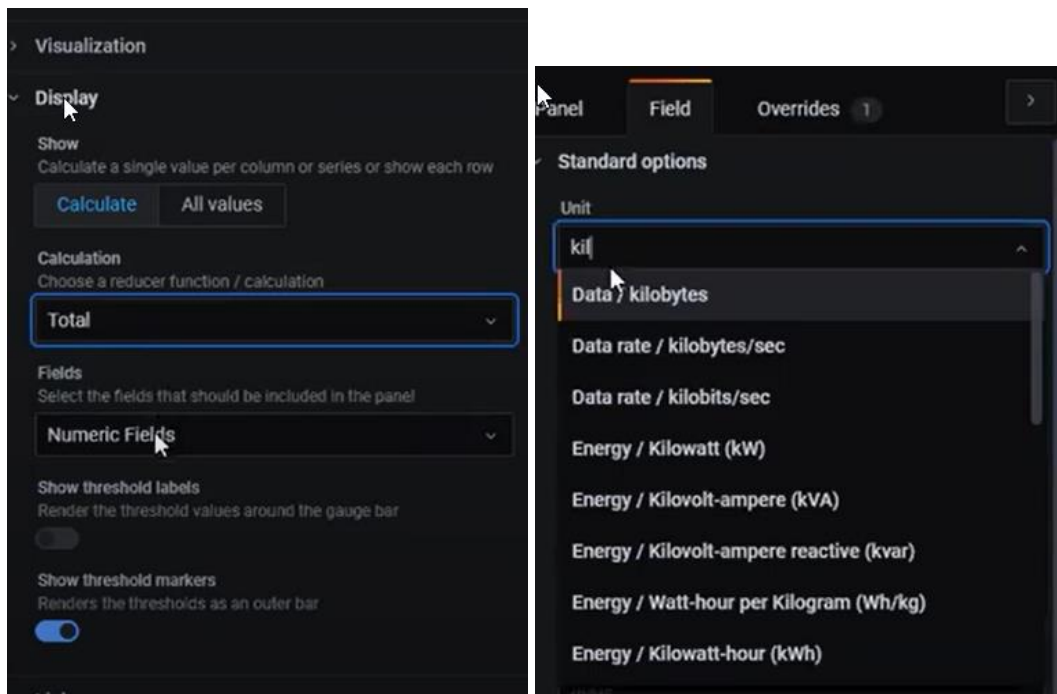
Step 2. In the right hand visualization menu click “gauge”



The new graph changes to display the query data in a gauge view.

Step 3. In the Visualization menu, change Calculation field to "Total"

Step 4. In the Unit field select "kilobytes".



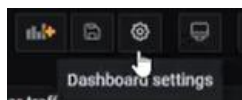
The new chart changes as illustrated.





Three different charts using the same query serving 3 different purposes:

- overtime trend
- Snap-shot view
- Snap-shot total but no distribution



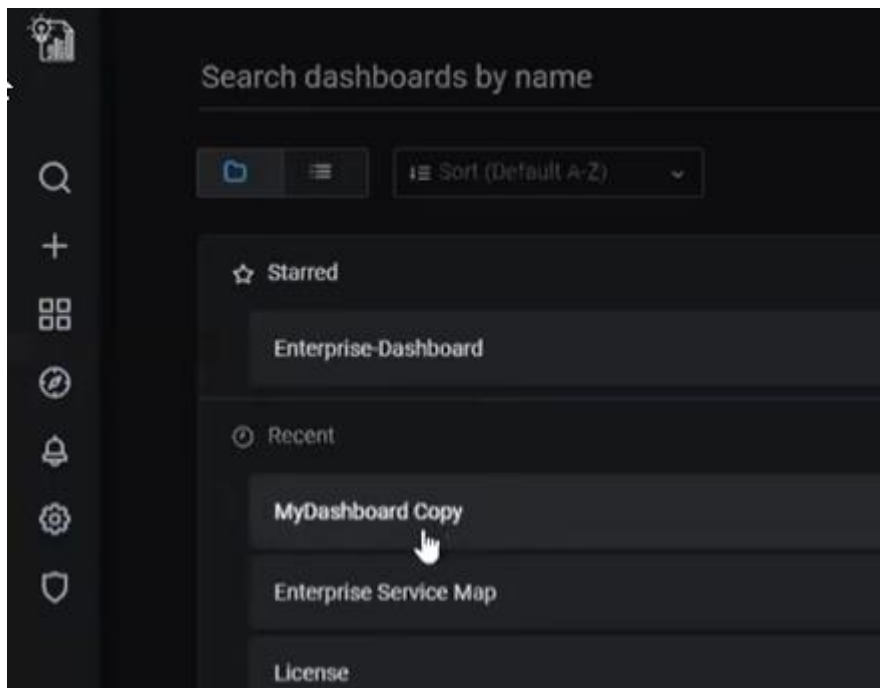
Step 5. Click **Dashboard settings** in the top-right menu to save the dashboard.

A screenshot of the 'New dashboard / Settings' form. The form is titled 'General' and contains fields for Name, Description, Tags, Folder, Editable, Time Options, and Panel Options. The 'Name' field is filled with 'MyDashboard'. The 'Folder' is set to 'General'. The 'Editable' toggle is turned on. The 'Time Options' section includes 'Timezone' (Default), 'Auto-refresh' (5s,10s,30s,1m,5m,15m,30m,1h,2h,1d), 'Now delay now-' (0m), and 'Hide time picker' (toggle). The 'Panel Options' section includes 'Graph Tooltip' (Default). A 'Save dashboard' button is visible in the left pane menu.

Step 6. In the "Name" field type a name for the dashboard.

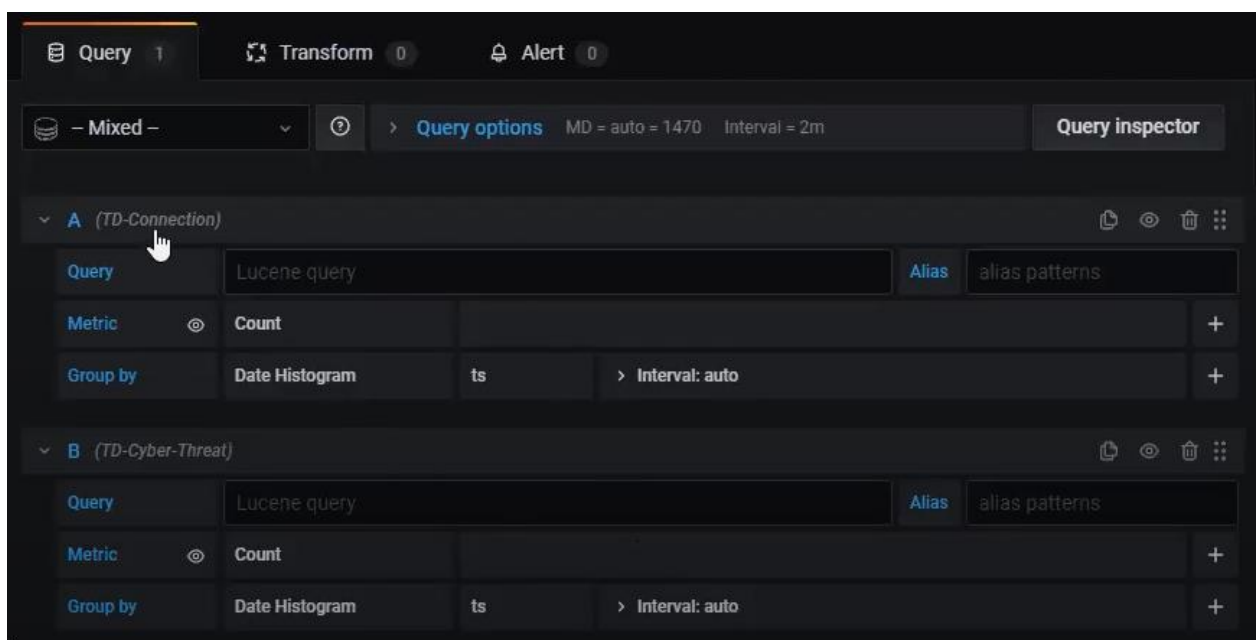
Step 7. Click Save dashboard in the left pane menu.

The new dashboard is now available for use.



From the next instance of use, this dashboard will load with the “last 2 days” data.

Mixed Query for Graph from multiple data sources

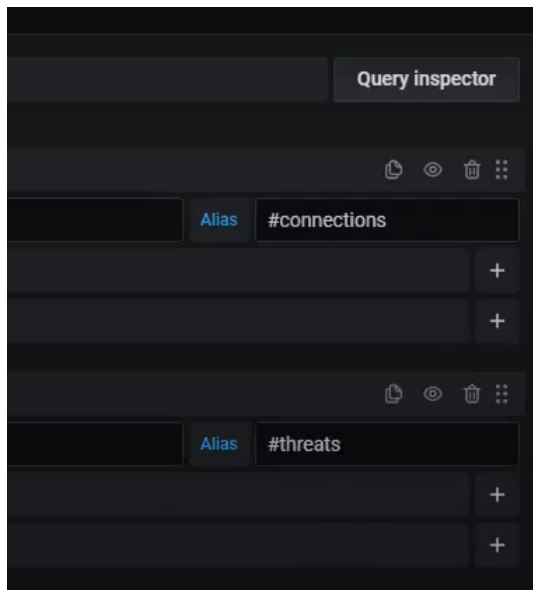


Step 8. Select “Mixed” in the query drop-down menu.

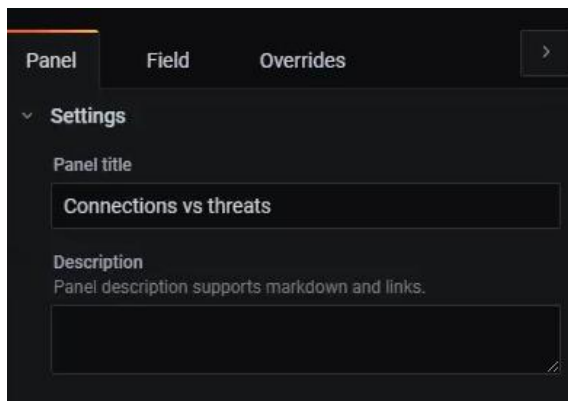
Step 9. Add a query with TD-Connection as data source

Step 10. Add a query with TD-Cyber-Threat as data source

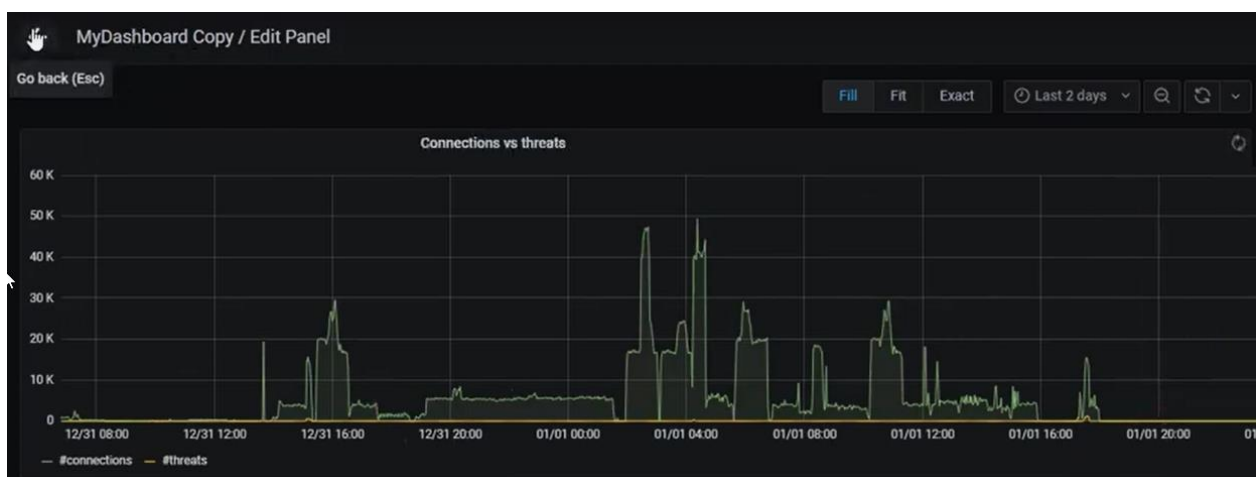
Step 11. Specify Alias patterns to separate the inputs from the 2 different sources.



Step 12. Provide Panel title for the graph, to indicate that the input is from two different data sources



The mixed query graph is displayed as illustrated.



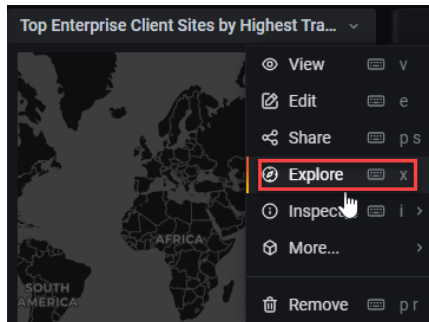
Step 13. Save "My dashboard".

Continue to explore the data sources and build expertise with creating workflows to suit your specific requirements.

Admin Role Options in the Dashboards

In addition to the options described so far, the drop-down Menu “Explore” and “More” are available in every data related panel of the workflows – also referred to as monitors in the rest of this document for users in the “Admin” role.

Explore



Use this option to set one or more of the following for your network

- study the data sources
- create queries and alerts
- set rules for running the queries and setting the alerts

Refer to “Creating Alerts” for details.

More

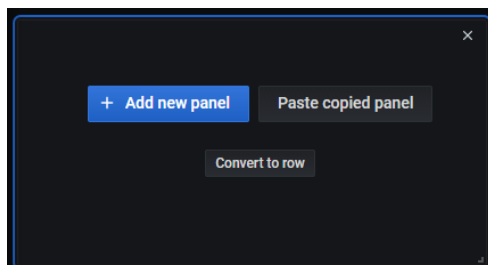


Click “Duplicate” for the system to auto-create a copy of the panel.

Click “Copy” for the system to save a copy of the panel in its clip-board. The pop-up appears as illustrated to indicate this.



Click **Add panel** in the top-panel menu.

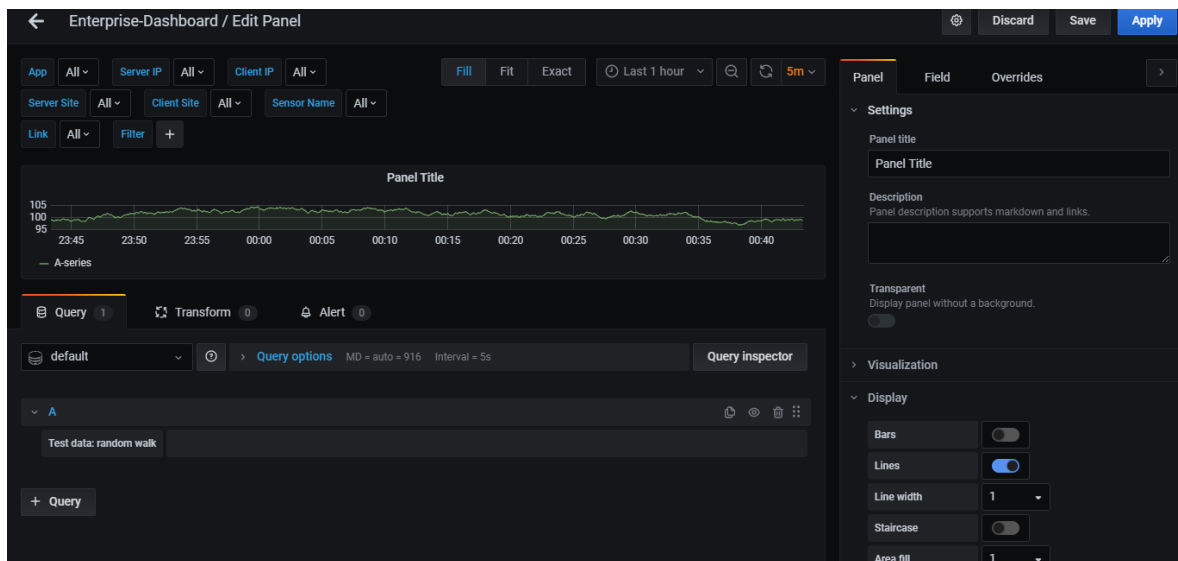


You can click

- **+ Add new panel** to add it as a new panel or
- **Paste copied panel** to paste the copied panel or
- **Convert to row** to Convert it to a Row

Add/Edit Panel

In the Add/Edit page as illustrated below, make appropriate changes to add the copied panel to the dashboard.



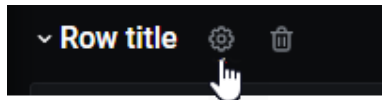
Refer to “


Top menu options” for details about adding panels.

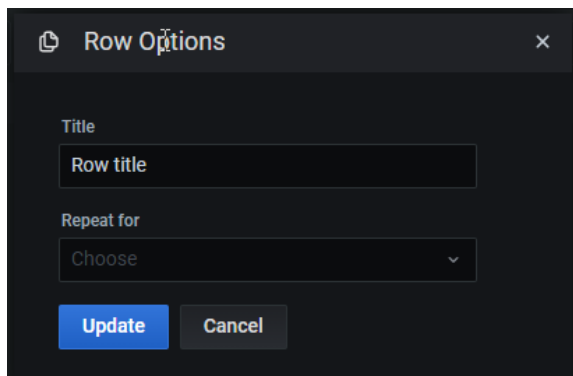
Paste Copied Panel

The panel is pasted to the dashboard on selecting this option.

Convert to Row



In the “Row Title” menu as illustrated, click .

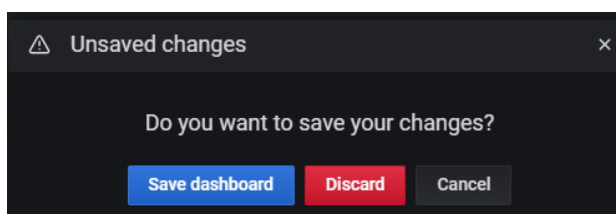


Option	Description
Title	Type a title for the row.
Repeat for	Click <input checked="" type="checkbox"/> and select an option from the drop down list.
Update	Click to update the changes.

Manage changes

After making changes you can:

- Click the back option in your browser or,
- Close the Soho360 dashboard page
- The pop-up appears as illustrated.



- Click “Save dashboard” to save all changes made to the dashboard.
- Click “Discard” if you do not wish to save the changes.

Important: Users should keep in mind that incorrect usage can lead to tampering of the data and visualization pre-set in the default workflows and cause undesirable results. Since these are saved

in the system as files, always save a copy of the system files to make changes and publish them for use only after they meet everybody's expectations.

Copyright

This documentation is furnished under license from ThoughtData Inc. and may only be used in accordance with the terms of the license. No part of this documentation may be reproduced by any means nor modified, decompiled, disassembled, published, reproduced or distributed, in whole or in part, or translated to any electronic or other medium, without the prior written consent of *ThoughtData*. All right, title and interest in and to the documentation and the software and applications described in the documentation are and shall remain the exclusive property of *ThoughtData* and its licensors. This documentation and its content are subject to change without notice.

ThoughtData and its licensors assume no responsibility or liability for any errors, inaccuracies or omissions in this documentation.

Nothing in this documentation should be construed as a commitment or warranty of any kind.

ThoughtData, *Soho360*, *NetSense*, *InfraSense* and *ThoughtData's* stylized logo are either trademarks or registered trademarks of *ThoughtData Software, Inc.* or its subsidiaries. Microsoft®, Windows® SQL Server® Linux, Ubuntu, CentOS and Fedora are registered trademarks of their respective owners. Other company and product names mentioned in this documentation are trademarks or registered trademarks of their respective owners.

Visit our Web site at: <https://www.thoughtdata.com>

Contact *ThoughtData* - info@thoughtdata.com

ThoughtData, Inc.
9 Ledgerock Way, Acton,
MA 01720
413.404.0030

©2020 *ThoughtData* Inc. All rights reserved.

ThoughtData is a registered trademark of *ThoughtData* Inc.

Thank you for using *ThoughtData*.

About ThoughtData Inc.

ThoughtData provides unified visibility solutions to small-business and home network users. Our solutions offer a single unified platform that blends innovative network, application, infrastructure, cloud performance and enterprise cyber security technologies. With this unique approach, ThoughtData's solutions reduce cost, mean time to respond (MTTR), tool clutter and increases end to end visibility into such networks in one single solution.

