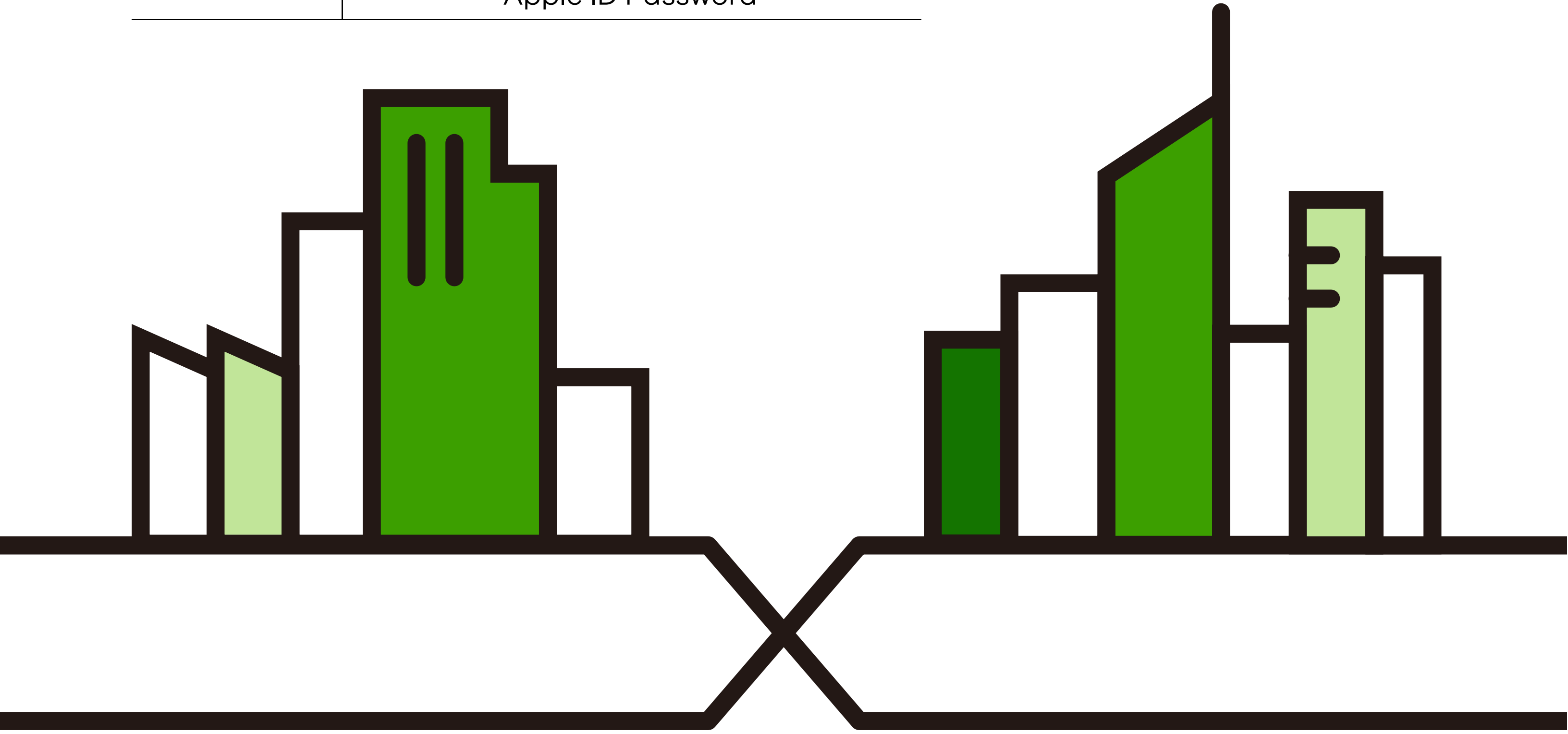
User's Guide

SecuReporter

Version 2.5.19 Edition 1, 08/2024

Default Login Details

Login URL	https://secureporter.cloudcnm.zyxel.com
Email	Zyxel Account Email Google Account Email Apple ID Email
Password	Zyxel Account Password Google Account Password Apple ID Password



IMPORTANT!

READ CAREFULLY BEFORE USE.

KEEP THIS GUIDE FOR FUTURE REFERENCE.

Screenshots and graphics in this book may differ slightly from what you see due to differences in release versions or your computer operating system. Every effort has been made to ensure that the information in this manual is accurate.

Note: The version number on the cover page refers to the version number you can see on the bottom of the log in screen of the SecuReporter.

Related Documentation

- User's Guides

  Go to the download library of the Zyxel website to get a supported Zyxel Device User's Guide to see how to configure the Zyxel Device using the Web Configurator on the Zyxel Device.

  Go to the download library of the Zyxel website to get a supported Zyxel Device Command Line Interface (CLI) Reference Guide to see how to configure the Zyxel Device using the CLI on the Zyxel Device.

  Go to the Zyxel Nebula Control Center portal to get the NCC User's Guide to see more infromation about SecuReporter.

- More Information

  Go to *support.zyxel.com* to find other information on SecuReporter.

Document Conventions

Warnings and Notes

These are how warnings and notes are shown in this guide.

Warnings tell you about things that could harm you or your device.

Note: Notes tell you other important information (for example, other things you may need to configure or helpful tips) or recommendations.

Syntax Conventions

- The Cloud CNM SecuReporter may be referred to as “SecuReporter” in this guide.
- Product labels, screen names, field labels and field choices are all in **bold** font.
- A right angle bracket (>) within a screen name denotes a mouse click. For example, **Analysis** > **Security Indicator** > **URL Threat Filter** > **by Destination IP** means you first click **Analysis** in the navigation panel, then the **Security Indicator** sub menu, then the **URL Threat Filter** tab, and finally the **by Destination IP** tab to get to that screen.

Table of Contents

Document Conventions 3

Table of Contents 4

Chapter 1
Introduction 6

1.1 Overview 6
1.1.1 Supported Zyxel Devices and Firmware Versions 6
1.1.2 SecuReporter Management Privileges 7
1.1.3 License Options 8
1.1.4 Cloud Mode 8
1.2 Get Started 8
1.3 Title Bar 9
1.4 Threat History 10
1.4.1 Details 11
1.5 Dashboard 12

Chapter 2
Analysis 15

2.1 Overview 15
2.1.1 Tutorial 15
2.1.2 Sandboxing 18
2.2 Analysis Overview 20
2.3 Security Indicators 24
2.3.1 ADP 24
2.3.2 IP Reputation 26
2.3.3 IPS 30
2.3.4 DNS Threat Filter 33
2.3.5 URL Threat Filter 38
2.3.6 Antivirus / Malware 42
2.3.7 Sandboxing 44
2.3.8 Mail Protection 46
2.4 Network Activity 48
2.4.1 DNS Content Filter 49
2.4.2 App Patrol 51
2.4.3 Web Content Filter 53
2.5 Traffic 56
2.6 Device 57
2.6.1 CPU/Memory/Session 57
2.6.2 Interface Traffic 58

Chapter 3
Logs 61

3.1 Overview 61
3.2 Search Log 61
3.2.1 Log Search Privileges 62
3.2.2 Download Logs 62
3.2.3 Security Indicator Logs 65
3.2.4 Network Activity Logs 71
3.2.5 Traffic Logs 74
3.2.6 Event Logs 76
3.3 Search User 79
3.3.1 Details 80

Chapter 4
Alerts 82

4.1 Overview 82
4.2 Trend & Details 82
4.3 Alert Settings 84

Chapter 5
Report...89

5.1 Overview 89
5.2 All Reports 89
5.3 Report Settings 91

Chapter 6
Settings...94

6.1 Overview 94
6.2 Organization & Device 94
6.2.1 Add a Zyxel Device to an Organization 95
6.2.2 Claimed Device 98
6.2.3 Generate API Token 99
6.3 User Account 101

Chapter 7
Troubleshooting...104

7.1 Getting More Troubleshooting Help 106

Appendix A Customer Support 107

Appendix B Legal Information.. 112

Index 113

CHAPTER 1
Introduction

1.1 Overview

SecuReporter is a cloud-based analytics tool that is part of the Cloud CNM suite developed by Zyxel. It can aggregate logs from up to 40,000 supported Zyxel Security Appliances across distributed locations, giving network administrators a centralized view of security events and flow data, including the hostname, IP address, MAC address of the client devices.

Reports are generated using security intelligence techniques and automated data correlation with real-time traffic analytics, as opposed to merely relying on static and predefined rules. Insights relevant to a network's security environment are available at a glance on an intuitive dashboard.

1.1.1 Supported Zyxel Devices and Firmware Versions

At the time of writing of this User's Guide, SecuReporter supports the following Zyxel Devices:

Table 1 Supported Zyxel Devices and Firmware Versions

SUPPORTED MODELS	SUPPORTED VERSION
USG FLEX 100	Version 4.50 or later
USG FLEX 200	
USG FLEX 500	
USG FLEX 100W	Version 4.60 or later
USG FLEX 700	
USG FLEX 100AX	Version 5.37 or later
USG FLEX 100H(P)	Version 1.10 or later
USG FLEX 200H(P)	
USG FLEX 500H	
USG FLEX 700H	
USG FLEX 50H(P)	Version 1.30 or later

Note: If your product is not listed in the table above, please refer to the official announcement posted in *https://www.zyxel.com/products_services/Security-Service-Cloud-CNM-SecuReporter/license-and-spec* for the SecuReporter's availability.

Note: At the time of writing, the ZyWALL ATP series, ZyWALL USG FLEX series, ZyWALL USG FLEX 50(AX) series, and ZyWALL VPN series have reached End of Life, but device license services are still available.

Screens and widgets vary depending on the Zyxel Devices that you use. This table summarizes some of the features that are only available for the USG FLEX H series, ZyWALL ATP series, ZyWALL USG FLEX series, and ZyWALL USG FLEX 50(AX) series.

Table 2 Features Supported on the Zyxel Devices

SUPPORTED FEATURES	USG FLEX H SERIES	USG FLEX SERIES	USG FLEX 50(AX) SERIES	ATP SERIES
Sandboxing	Yes	Yes (with Gold Security Pack)	No	Yes
Reputation Filter	Yes	Yes (with Gold Security Pack)	No	Yes
Web Filtering	Yes	Yes	Yes	Yes
Anti-Malware	Yes	Yes	No	Yes
IPS	Yes	Yes	No	Yes
Application Patrol	Yes	Yes	No	Yes
Device Insight	Yes	Yes	Yes	Yes
Traffic Usage	Yes	Yes	Yes	Yes

1.1.2 SecuReporter Management Privileges

A Zyxel Device owner can register a Zyxel Device at *https://account.zyxel.com*. Only an owner can add Zyxel Devices to an organization. However, an owner can assign other people to manage Zyxel Devices.

This table summarizes SecuReporter privileges at each level of the model:

Table 3 SecuReporter Management Privileges

ROLE TYPES	SIGN IN AT ZYXEL ACCOUNT?	PRIVILEGES
Agent (Owner)	Yes	• Can add/delete Zyxel Devices to/from an organization • Can add/edit organizations • Can add/edit admin/user accounts • Can configure alert notifications • Can configure dashboard widgets • Can configure analyses and reports • Can create request for transfer of analytics and logs • Can import analytics and logs • Can create log download request and download archived logs
Admin	Yes	• Can add/edit organizations • Can configure alert notifications • Can configure dashboard widgets • Can configure analyses and reports • Can import analytics and logs • Can download archived logs
User	Yes	• Can configure dashboard widgets • Can view analyses and report • Can configure alert notifications • Can import analytics and logs

1.1.3 License Options

You can use SecuReporter with a free 30-day Trial license or buy a 1-year device license. You will receive a renewal notification before either expires. In addition, for the SecuReporter license, you will have an extra 15 day grace period to renew.

Note: SecuReporter will automatically delete logs when the grace period has expired.

1.1.4 Cloud Mode

In cloud mode, you can manage and monitor the Zyxel Device through the Zyxel Nebula cloud-based network management system. This means you can manage devices remotely without the need of connecting to each device directly. It offers many features to better manage and monitor not just the Zyxel Device, but your network as a whole, including supported switches and gateways. Your network can also be managed through your smartphone using the Nebula Mobile app.

The Nebula Control Center (NCC) allows different levels of management. You can configure each device on its own or configure a set of devices together as a site. You can also monitor groups of sites called organizations, as shown below.

Table 4 NCC management Levels

Organization			
Site A		Site B	
Device A-1	Device A-2	Device B-1	Device B-2

Some features are not supported for certain models in cloud mode. Please go to the NCC to view or configure them.

Table 5 Features Supported in Cloud Mode

FEATURES	ATP / USG FLEX / USG FLEX 50 (AX) / VPN SERIES	USG FLEX H SERIES
Add/delete Zyxel Devices to/from an organization	No	No
Add/edit admin/user accounts	No	No
Configure alert notifications	No	No
View traffic/event log	No	Yes
View CPU/memory/session usage	No	Yes

1.2 Get Started

Use a browser that supports HTML5, such as Google Chrome, Mozilla Firefox, Safari, or Microsoft Edge. The recommended minimum screen resolution is 1366 by 768 pixels. In order to use SecuReporter you need to allow web browser pop-up windows from your computer.

To set up SecuReporter:

1 You must enable SecuReporter on a supported Zyxel Device. Refer to the User’s Guide of the supported Zyxel Device for instructions.

2 Register the Zyxel Devices using the same Zyxel Account. To open an account at Zyxel, go to *account.zyxel.com* and click **Create an account,** or sign in with your Google or Apple account.

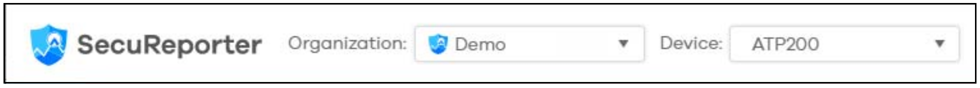
3 After you register the Zyxel Devices, follow the on-screen instructions to activate the SecuReporter license for the registered Zyxel Devices.

Once you are in the SecuReporter web portal, configure an organization with the Zyxel Devices.

Note: See Section 6.1 on page 94 for an overview of how to get started using SecuReporter.

On your next login after configuring an organization, select an **Organization** first. Your registered devices will be shown in **Device**.

Figure 1 Select Organization and Device on Startup

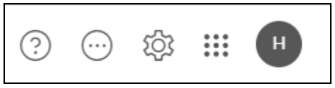


SecuReporter Organization: Demo ▾ Device: ATP200 ▾

1.3 Title Bar

The title bar provides some useful links that always appear over the screens below. If your Zyxel Device is in NCC mode, not all icons will be available in the Title Bar.

Figure 2 Title Bar



The icons provide the following functions.

Table 6 Title Bar: Web Configurator Icons

LABEL	DESCRIPTION
?	Click this to open the help, access the Download Library, or visit the Community.
⋯	Click this to set up the following: • Organization & Device – you see all organizations that you have already created and the Zyxel Devices (Model, Device and License Status). • Members – to assign an administrator or user for organizations or Zyxel Devices within organizations that you created.
⚙	Click this to turn on or off SecuReporter's dark mode display.
⠿	Click this to show a list of apps provided by Zyxel available.
myZyxel	Click this to open the myZyxel website login page in a new tab or window.
Nebula	Click this to open the Nebula portal login page in a new tab or window.
SecuReporter	Click this to open the SecuReporter website login page in a new tab or window.

Table 6 Title Bar: Web Configurator Icons (continued)

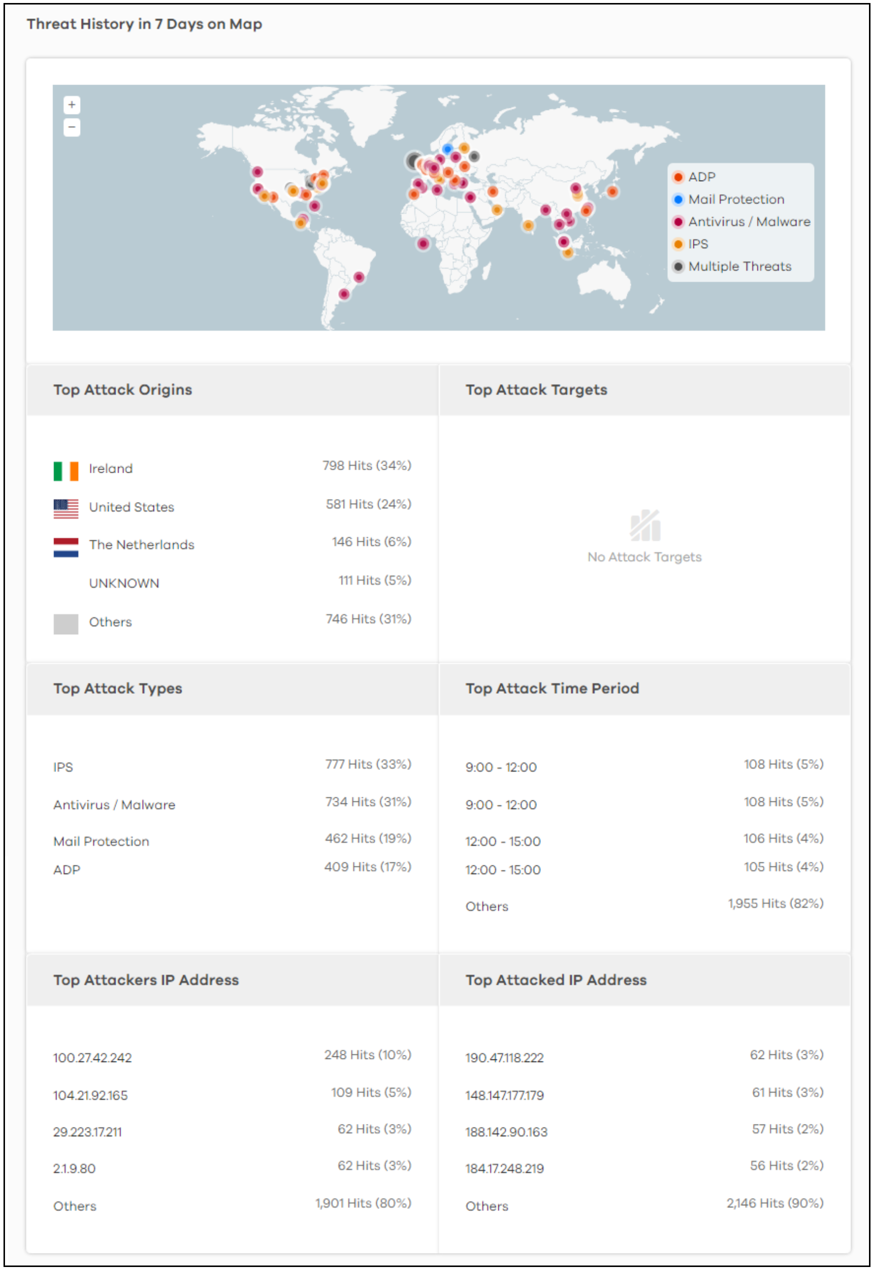
LABEL	DESCRIPTION
Astra	Click this to open the Astra website login page in a new tab or window.
Circle	Click this to open the Circle website login page in a new tab or window.
Marketplace	Click this to open the Zyxel Account website login page in a new tab or window. You will be redirected to the Marketplace after you log in.
Store	Click this to open the Zyxel store website lin a new tab or window.
Education	Click this to open the Education Center website in a new tab or window.
Community	Click this to go to Zyxel Community, where you can get the latest Zyxel Device information and have conversations with other people by posting your messages.
H	Click this to view your account name, manage your account information (edit Profile, change Password, set up Two-Factor Authentication), or to log out.

1.4 Threat History

Refer to the right portion of the **Dashboard** to view the origins of attack packets detected by SecuReporter over the last 7 days.

The map pins identify the locations from which threats had originated. Pin color indicates the type of the attacks. A bigger pin means more threats.

Figure 3 Threat History



Threat History in 7 Days on Map

Top Attack Origins	
🟩🟧 Ireland	798 Hits (34%)
United States	581 Hits (24%)
The Netherlands	146 Hits (6%)
UNKNOWN	111 Hits (5%)
Others	746 Hits (31%)

Top Attack Targets

No Attack Targets

Top Attack Types	
IPS	777 Hits (33%)
Antivirus / Malware	734 Hits (31%)
Mail Protection	462 Hits (19%)
ADP	409 Hits (17%)

Top Attack Time Period	
9:00 - 12:00	108 Hits (5%)
9:00 - 12:00	108 Hits (5%)
12:00 - 15:00	106 Hits (4%)
12:00 - 15:00	105 Hits (4%)
Others	1,955 Hits (82%)

Top Attackers IP Address	
100.27.42.242	248 Hits (10%)
104.21.92.165	109 Hits (5%)
29.223.17.211	62 Hits (3%)
2.1.9.80	62 Hits (3%)
Others	1,901 Hits (80%)

Top Attacked IP Address	
190.47.118.222	62 Hits (3%)
148.147.177.179	61 Hits (3%)
188.142.90.163	57 Hits (2%)
184.17.248.219	56 Hits (2%)
Others	2,146 Hits (90%)

1.4.1 Details

Click a pin on the **Threat History in 7 Days on Map** to view more information about the threats detected from that location.

The following table describes the labels on this screen.

Table 7 Threat History

LABEL	DESCRIPTION
Attack Type	This displays the type of attack that was detected coming from the site. Common types of attacks include ADP, IPS, Malware (Anti Virus), spam, content filter, and mixed.
Hits	This displays the number of times a single threat was sent from a site and blocked by the Zyxel Device. Click the arrow to arrange the threats by the number of hits.
Top Attack Origins	This displays the percentage of the threat's source country.
Top Attack Targets	This displays the percentage of the threat's destination country.
Top Attack Types	This displays the percentage of the type of attack.
Top Attack Time Period	This displays the percentage of the 3-hour time frame when the attacks occur.
Top Attackers IP Address	This displays each threat's source IP.
Top Attacked IP Address	This displays each threat's destination IP.

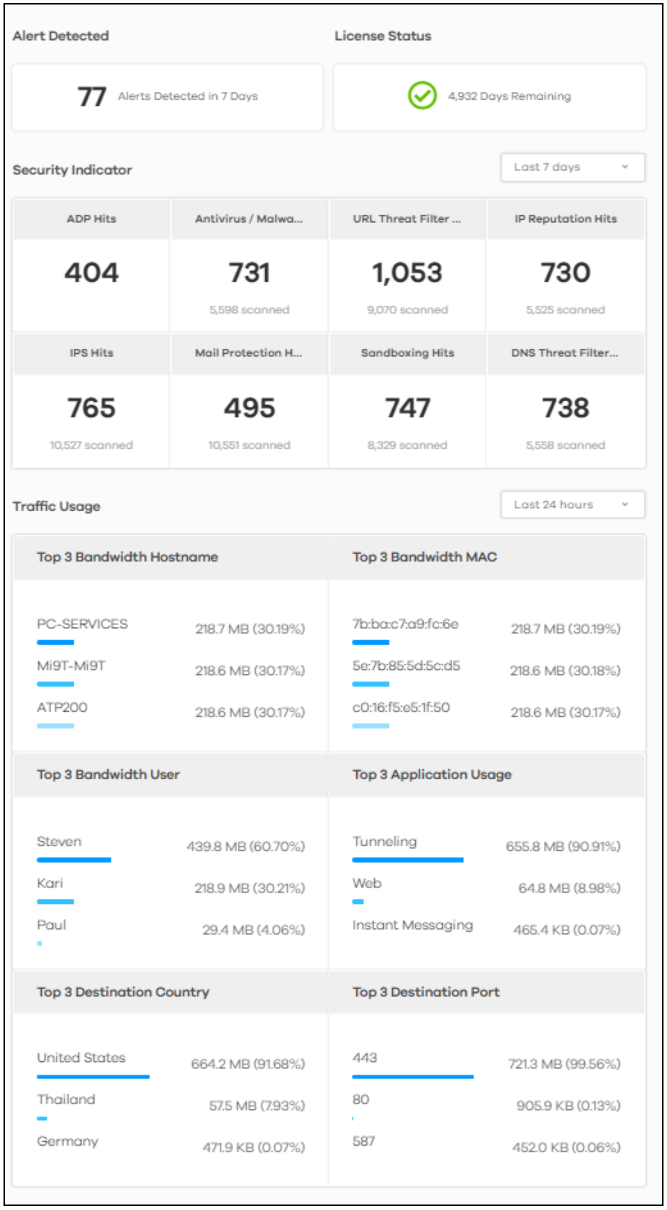
1.5 Dashboard

The **Dashboard** shows the key facts about your network's security environment that were collected by SecuReporter in the last 30 days, 7 days, 24 hours, one hour, or custom range.

You need to create an organization with at least one Zyxel Device for information to display in the **Dashboard** – go to (More) ⋯ (upper right icon) > **Organization & Device** > **Add Organization**.

By default, the dashboard will have the **Alert Detected**, **License Status**, **Security Indicator**, and **Traffic Usage** widgets. Widgets are miniature views of SecuReporter's data visualizations, the full versions of which are available under the Security Indicators, Network Activity, Traffic and Device screens.

Figure 4 Default Dashboard



Alert Detected

77 Alerts Detected in 7 Days

License Status

✓ 4,932 Days Remaining

Security Indicator

Last 7 days ⌄

ADP Hits	Antivirus / Malwa...	URL Threat Filter ...	IP Reputation Hits
404	731 5,598 scanned	1,053 9,070 scanned	730 5,525 scanned

IPS Hits	Mail Protection H...	Sandboxing Hits	DNS Threat Filter...
765 10,527 scanned	495 10,551 scanned	747 8,329 scanned	738 5,558 scanned

Traffic Usage

Last 24 hours ⌄

Top 3 Bandwidth Hostname		Top 3 Bandwidth MAC	
PC-SERVICES	218.7 MB (30.19%)	7b:ba:c7:a9:fc:6e	218.7 MB (30.19%)
Mi9T-Mi9T	218.6 MB (30.17%)	5e:7b:85:5d:5c:d5	218.6 MB (30.18%)
ATP200	218.6 MB (30.17%)	c0:16:f5:e5:1f:50	218.6 MB (30.17%)

Top 3 Bandwidth User		Top 3 Application Usage	
Steven	439.8 MB (60.70%)	Tunneling	655.8 MB (90.91%)
Kari	218.9 MB (30.21%)	Web	64.8 MB (8.98%)
Paul	29.4 MB (4.06%)	Instant Messaging	465.4 KB (0.07%)

Top 3 Destination Country		Top 3 Destination Port	
United States	664.2 MB (91.68%)	443	721.3 MB (99.56%)
Thailand	57.5 MB (7.93%)	80	905.9 KB (0.13%)
Germany	471.9 KB (0.07%)	587	452.0 KB (0.06%)

The following table describes the widgets on the default dashboard:

Table 8 Default Dashboard

LABEL	DESCRIPTION
Alert Detected	This is the total number of the latest alerts sent to administrators of a network in the last 7 days.
License Status	This shows if your SecuReporter license is active or inactive, and the number of days remaining.
Security Indicator	

Table 8 Default Dashboard (continued)

LABEL	DESCRIPTION
	Select the time frame to show your network's security environment collected by SecuReporter. • Last hour • Last 24 hours • Last 7 days • Last 30 days • Custom Range – click an allowed start and end day, select the time frame, and then click **Apply**.
ADP Hits	This displays the total number of anomalies detected by the Zyxel Devices. Anomalies are based on violations of protocol standards (RFCs – Requests for Comments) or abnormal flows such as port scans.
Antivirus / Malware Hits	This displays the total number of the most common malware and viruses detected and blocked by the Zyxel Device.
URL Threat Filter Hits	This displays the total number of times the Zyxel Device's URL Threat filtering service detected and blocked connection attempts to or from a site in an URL threat category.
IP Reputation Hits	This displays the total number of times packets coming from an IPv4 address with a bad reputation occur and the number of times connection attempts to an IPv4 address with a bad reputation occur.
IPS Hits	This displays the total number of malicious or suspicious packets detected by IPS in the Zyxel Devices. IPS (Intrusion, Detection and Prevention) uses signatures to detect malicious or suspicious packets to protect against network-based intrusions.
Mail Protection Hits	This displays the total number of the most common traffic classified as spam received by the Zyxel Devices.
Sandboxing Alerts	This displays the total number of files that have been scanned through the sandboxing function.
DNS Threat Filter Hits	This displays the total number of URLs of FQDNs classified as a security threat to network devices behind the Zyxel Device.
Traffic Usage	
	Select the time frame to show your network traffic collected by SecuReporter. • Last hour • Last 24 hours • Last 7 days • Custom Range – click an allowed start and end day, select the time frame, and then click **Apply**.
Top 3 Bandwidth User	This displays the top three users of bandwidth on the network including percentage over a selected time frame, which is 7 days by default.
Top 3 Application Usage	This displays the network applications with the greatest bandwidth usage including percentage over a selected time frame, which is 7 days by default.
Top 3 Destination Country	This displays the top three countries that received the most data traffic from Zyxel Devices including percentage, over a selected time frame.
Top 3 Destination Port	This displays the top three destination ports by bandwidth usage including percentage, over a specified time frame, which is 7 days by default.

CHAPTER 2 Analysis

2.1 Overview

Analysis is a set of charts, tables, and other visualizations of data collected from Zyxel Devices. Analysis provides a big-picture overview of network activity, while making it easy to "drill down" into granular detail on what users are doing.

2.1.1 Tutorial

In the **Analysis** section, the charts can be clicked to reveal event records.

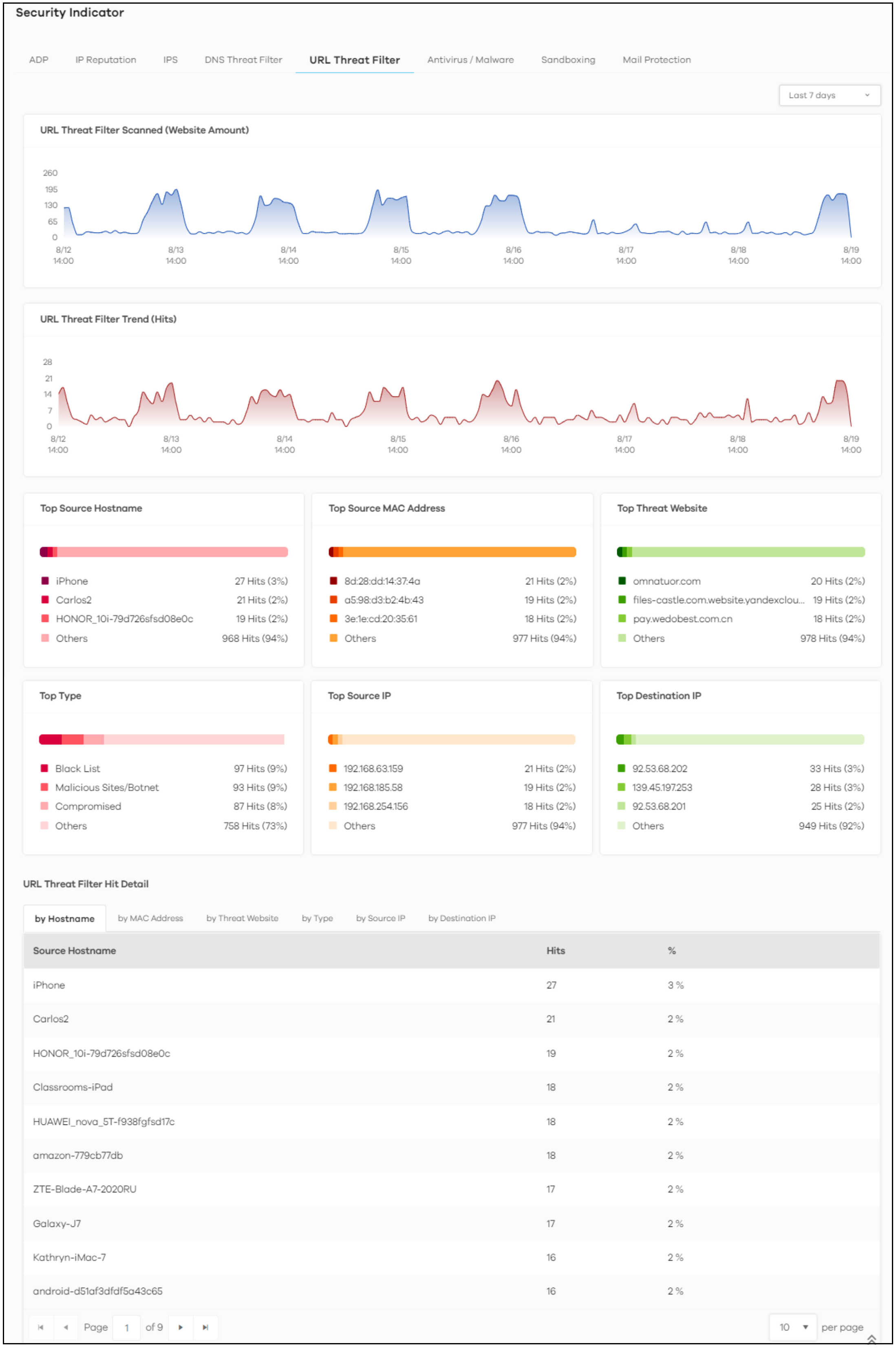
In most cases, you can choose to analyze data collected over one of five time frames (see Section 1.5 on page 12):

- Last hour
- Last 24 hours
- Last 7 days
- Last 30 days
- Custom Range – click an allowed start and end day, select the time frame, and then click **Apply**.

This tutorial uses the following example to show how to explore an URL threat filter hit detail that you want to investigate, specifically by destination IP.

1 Click **Analysis** > **Security Indicator** > **URL Threat Filter.**

Figure 5 Top URL Threat Filter



Top Source Hostname

■ iPhone	27 Hits (3%)
■ Carlos2	21 Hits (2%)
■ HONOR_10i-79d726sfsd08e0c	19 Hits (2%)
■ Others	968 Hits (94%)

Top Source MAC Address

■ 8d:28:dd:14:37:4a	21 Hits (2%)
■ a5:98:d3:b2:4b:43	19 Hits (2%)
■ 3e:1e:cd:20:35:61	18 Hits (2%)
■ Others	977 Hits (94%)

Top Threat Website

■ omnatuor.com	20 Hits (2%)
■ files-castle.com.website.yandexclou...	19 Hits (2%)
■ pay.wedobest.com.cn	18 Hits (2%)
■ Others	978 Hits (94%)

Top Type

■ Black List	97 Hits (9%)
■ Malicious Sites/Botnet	93 Hits (9%)
■ Compromised	87 Hits (8%)
■ Others	758 Hits (73%)

Top Source IP

■ 192.168.63.159	21 Hits (2%)
■ 192.168.185.58	19 Hits (2%)
■ 192.168.254.156	18 Hits (2%)
■ Others	977 Hits (94%)

Top Destination IP

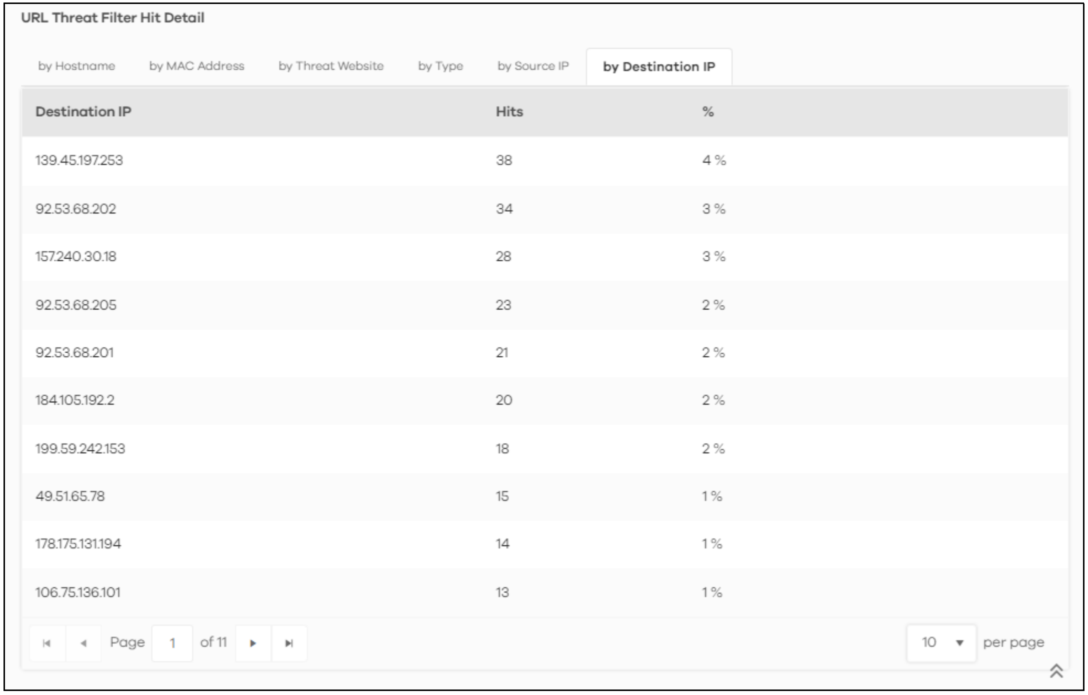
■ 92.53.68.202	33 Hits (3%)
■ 139.45.197.253	28 Hits (3%)
■ 92.53.68.201	25 Hits (2%)
■ Others	949 Hits (92%)

URL Threat Filter Hit Detail

Source Hostname	Hits	%
iPhone	27	3 %
Carlos2	21	2 %
HONOR_10i-79d726sfsd08e0c	19	2 %
Classrooms-iPad	18	2 %
HUAWEI_nova_5T-f938fgfsd17c	18	2 %
amazon-779cb77db	18	2 %
ZTE-Blade-A7-2020RU	17	2 %
Galaxy-J7	17	2 %
Kathryn-iMac-7	16	2 %
android-d51af3dfdf5a43c65	16	2 %

2 Click the **by Destination IP** tab. To display the next set of malware or viruses, click the arrow on the lower left of the screen.

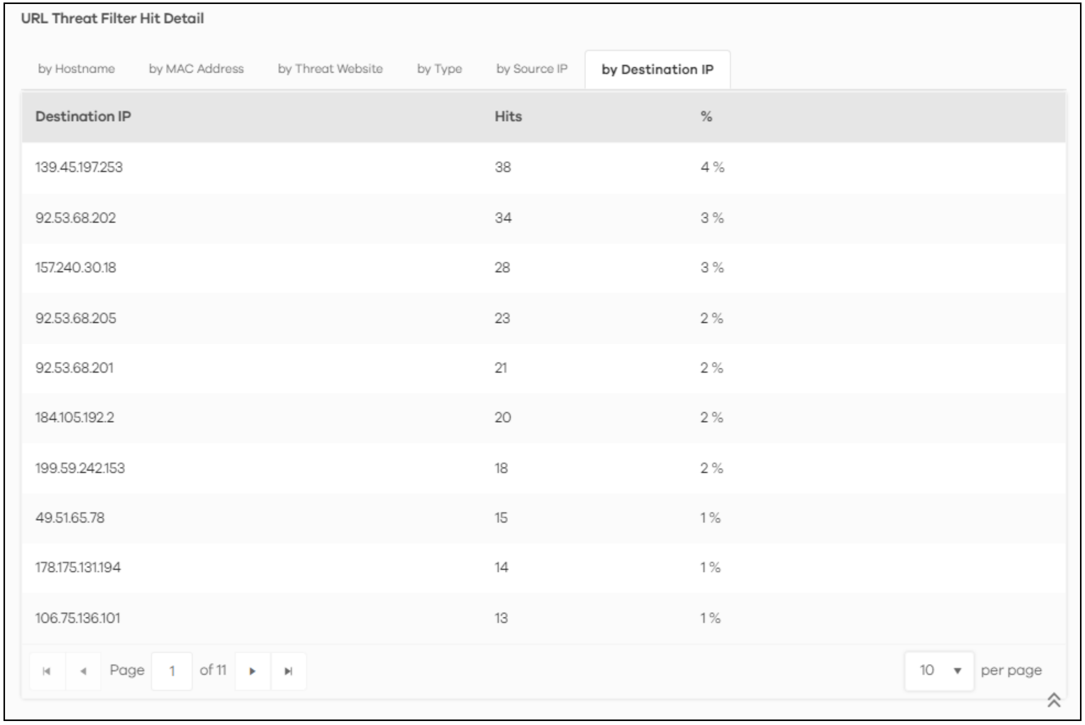
Figure 6 Top 10 URL Threat Filter Hit Detail > by Destination IP



Destination IP	Hits	%
139.45.197.253	38	4 %
92.53.68.202	34	3 %
157.240.30.18	28	3 %
92.53.68.205	23	2 %
92.53.68.201	21	2 %
184.105.192.2	20	2 %
199.59.242.153	18	2 %
49.51.65.78	15	1 %
178.175.131.194	14	1 %
106.75.136.101	13	1 %

The following screen appears.

Figure 7 Next Set of Top URL Threat Filter Hit Detail > by Destination IP

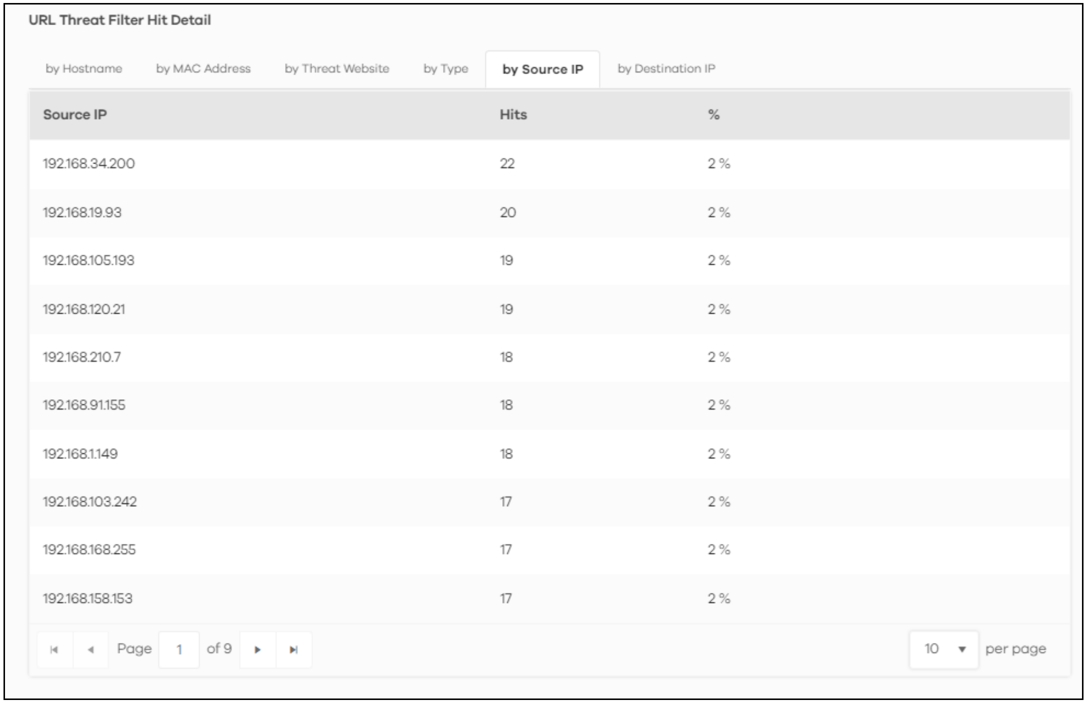


Destination IP	Hits	%
139.45.197.253	38	4 %
92.53.68.202	34	3 %
157.240.30.18	28	3 %
92.53.68.205	23	2 %
92.53.68.201	21	2 %
184.105.192.2	20	2 %
199.59.242.153	18	2 %
49.51.65.78	15	1 %
178.175.131.194	14	1 %
106.75.136.101	13	1 %

3 Clicking a **Destination IP** will display its **Threat Website** address, the number of **Hits**, and the percentage (**%**) of hits to the destination IP address.

Note: You could select different metrics by clicking a tab to view the information of the selected metric.

Figure 8 by Source IP

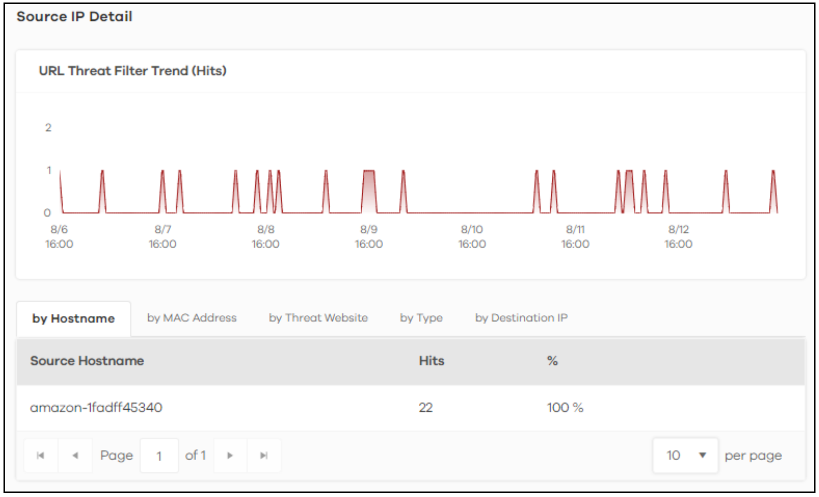


URL Threat Filter Hit Detail

Source IP	Hits	%
192.168.34.200	22	2 %
192.168.19.93	20	2 %
192.168.105.193	19	2 %
192.168.120.21	19	2 %
192.168.210.7	18	2 %
192.168.91.155	18	2 %
192.168.1.149	18	2 %
192.168.103.242	17	2 %
192.168.168.255	17	2 %
192.168.158.153	17	2 %

4 Clicking a **Source IP** will display its **Threat Website** address, the number of **Hits**, and the percentage (**%**) of hits from the source IP address.

Figure 9 Source IP Information



Source IP Detail

URL Threat Filter Trend (Hits)

Source Hostname	Hits	%
amazon-1fadff45340	22	100 %

2.1.2 Sandboxing

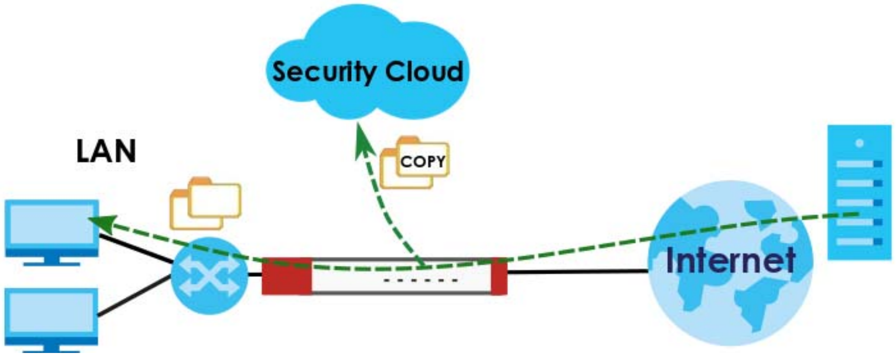
Zyxel cloud sandboxing is a security mechanism which provides a safe environment to separate running programs from your network and host devices. Unknown or untrusted programs or codes are uploaded to a cloud server and executed within an isolated virtual machine (VM) to monitor and analyze the zero-day malware and advanced persistent threats (APTs) that may evade the Zyxel Device's detection, such as anti-malware. Results of cloud sandboxing are sent from the server to the Zyxel Device.

The Zyxel Device sandbox checks all received files against its local cache for known malicious or suspicious codes. Files with no detected malicious or suspicious codes found in the cache ('unknown') are copied and uploaded to the security cloud server for further inspection. The scan result from the cloud server is added to the Zyxel Device cache and used for future inspection.

Note: The Zyxel Device forwards all unknown files to users. For files with known malicious or suspicious codes, you can configure the Zyxel Device to take specific actions, such as dropping the file.

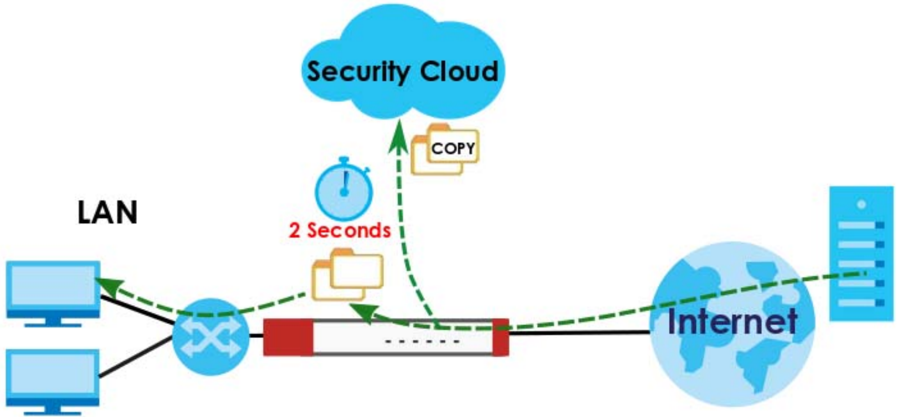
Note: The scan result is removed from the Zyxel Device cache after the Zyxel Device restarts, so all files are once again 'unknown'.

Figure 10 General Zyxel Sandbox Inspection



In the Zyxel Device, you can configure **Advanced Zyxel Sandbox Inspection** to hold and inspect unknown downloaded files for up to 2 seconds. After 2 seconds the Zyxel Device forwards the file even if the inspection is incomplete.

Figure 11 Advanced Zyxel Sandbox Inspection



2.1.2.1 Supported File Types for Sandboxing Inspection

Sandbox can only check the types of files listed under **File Submission Options** in the **Sandboxing** screen of the Zyxel Device. If you disabled **Scan and detect EICAR test virus** in the **Anti Malware** screen, then EICAR test files will be sent to Sandbox.

The EICAR test file is a standardized test file for signature based anti-malware scanners. When the scanner detects the EICAR file, it responds in the same way as if it found a real malware. Besides straightforward detection, the EICAR file can also be compressed to test whether the anti-malware software can detect it in a compressed file.

Note: Configure this setting on your Zyxel Device.

2.1.2.2 Turning on Sandboxing on Your Zyxel Device

To use the sandboxing function, you need to register your Zyxel Device and activate the service license at myZyxel, and then turn on the sandboxing function on the Zyxel Device.

2.1.2.3 Sandboxing Alerts

SecuReporter sends sandboxing alerts to Zyxel Device administrators when:

1 The Zyxel Device forwarded files that were later discovered to be suspicious or malicious.

Note: In this case the Zyxel Device administrator should immediately contact the receiver of the file and advise him or her not to open it. If he or she already opened it, then urge him or her to run an up-to-date anti-malware scanner.

2 The Zyxel Device sandbox (or Security Cloud) removed infected portions of files that were suspicious or malicious.

Note: In this case the receiver of the file will not be able to open the file. The Zyxel Device administrator should contact the receiver of the file to let him or her know.

2.2 Analysis Overview

Click **Analysis** > **Security Indicator** to show data visualizations related to the network's security, management and what was blocked. The following screens will be displayed.

Data is displayed in the **Analysis** menus as follows.

Table 9 Analysis Overview

LABEL	TYPE	DESCRIPTION
Security Indicator	ADP	ADP Trend (Hits)
		Top Source Hostname
		Top Source MAC Address
		Top Signature
		Top Signature Type
		Top Source IP
		Top Destination IP
		ADP Hit Detail
	IP Reputation	IP Reputation Scanned (Connection Amount)
		IP Reputation Trend (Hits)
		Top Source Hostname
		Top Source MAC Address
		Top Risk IP
		Top Type
		Top Source IP
		Top Destination IP
		IP Reputation Hit Detail
	IPS	IPS Scanned (Connection Amount)
		IPS Trend (Hits)
		Top Source Hostname
		Top Source MAC Address
		Top Signature
		Top Signature Type
		Top Source IP
		Top Destination IP
		IPS Hit Detail
	DNS Threat Filter	DNS Threat Filter Scanned (Connection Amount)
		DNS Filter Trend (Hits)
		Top Source Hostname
		Top Source MAC Address
		Top Threat Domain
		Top Threat Category
		Top Source IP
		Top Query Type
		DNS Threat Filter Hit Detail
		URL Threat Filter Scanned (Website Amount)

Table 9 Analysis Overview (continued)

LABEL	TYPE	DESCRIPTION
Security Indicator	URL Threat Filter	URL Threat Filter Trend (Hits)
		Top Source Hostname
		Top Source MAC Address
		Top Threat Website
		Top Type
		Top Source IP
		Top Destination IP
		URL Threat Filter Hit Detail
	Antivirus / Malware	Antivirus / Malware Scanned (File Amount)
		Antivirus / Malware Trend (Hits)
		Top Source Hostname
		Top Source MAC Address
		Top Virus / Malware
		Top Source IP
		Top Destination IP
		Antivirus / Malware Hit Detail
	Sandboxing	Sandboxing Scanned (File Amount)
		Sandboxing Trend (Hits)
		Top Source Hostname
		Top Source MAC Address
		Top File Type
		Top File Name
		Top File Hash
		Top User
		Top Source IP
		Top Destination IP
		Sandboxing Hit Detail
	Mail Protection	Mail Protection Scanned (Mail Amount)
		Mail Protection Trend (Hits)
		Top Source Hostname
		Top Source MAC Address
		Top Spam Email Subject
		Top Spam Sender Email
		Top Spam Received IP
		Top Spam Sender IP
		Mail Protection Hit Detail

Table 9 Analysis Overview (continued)

LABEL	TYPE	DESCRIPTION
Network Activity	DNS Content Filter	DNS Content Filter Scanned (Connection Amount)
		Blocked Domain Access Trend (Hits)
		Allowed Domain Access Trend (Hits)
		Top Accessed Blocked Domain
		Top Accessed Blocked Category
		Top Accessed Allowed Domain
		Top Accessed Allowed Category
		Top Source IP (To Blocked Domain)
		Top Accessed Blocked Query Type
		Top Source IP (To Allowed Domain)
		Top Accessed Allowed Query Type
		Blocked Domain Access History
		Allowed Domain Access History
	App Patrol	Blocked Application Access Trend (Hits)
		Allowed Application Access Trend (Hits)
		Top Accessed Blocked Application
		Top Accessed Blocked Application Type
		Top Accessed Allowed Application
		Top Accessed Allowed Application Type
		Blocked Application Access History
		Allowed Application Access History
	Web Content Filter	Website Scanned (Website Amount)
		Blocked Website Access Trend (Hits)
		Allowed Website Access Trend (Hits)
		Top Accessed Blocked Website
		Top Accessed Blocked Website Type
		Top Accessed Allowed Website
		Top Accessed Allowed Website Type
		Top Source IP (To Blocked Website)
		Top Destination IP (To Blocked Website)
		Top Source IP (To Allowed Website)
		Top Destination IP (To Allowed Website)
		Blocked Website Access History
		Allowed Website Access History
Traffic	Top Source Hostname	
	Top Source MAC Address	
	Top Bandwidth User	
	Top Application Usage	
	Top Destination Country	
	Top Destination Port	
	Traffic Detail	

Table 9 Analysis Overview (continued)

LABEL	TYPE	DESCRIPTION
Device	CPU/Memory/Session	CPU Usage Trend
		Memory Usage Trend
		Session Usage Trend
	Interface Traffic	DMZ Traffic Usage Trend
		LAN1 Traffic Usage Trend
		LAN2 Traffic Usage Trend
		OPT Traffic Usage Trend
		RESERVED Traffic Usage Trend
		WAN1 Traffic Usage Trend
		WAN2 Traffic Usage Trend

2.3 Security Indicators

Security Indicators data visualizations are categorized as:

- ADP
- IP Reputation
- IPS
- DNS Threat Filter
- URL Threat Filter
- Antivirus / Malware
- Sandboxing
- Mail Protection

2.3.1 ADP

Anomaly Detection and Prevention (ADP) protects against anomalies based on violations of protocol standards (RFCs – Requests for Comments) and abnormal flows such as port scans. This section introduces ADP, anomaly profiles and applying an ADP profile to a traffic direction.

Traffic Anomalies

Traffic anomaly policies look for abnormal behavior or events such as port scanning, sweeping or network flooding. They operate at OSI layer-2 and layer-3. Traffic anomaly policies may be updated when you upload new firmware.

Protocol Anomalies

Protocol anomalies are packets that do not comply with the relevant RFC (Request For Comments). Protocol anomaly detection includes:

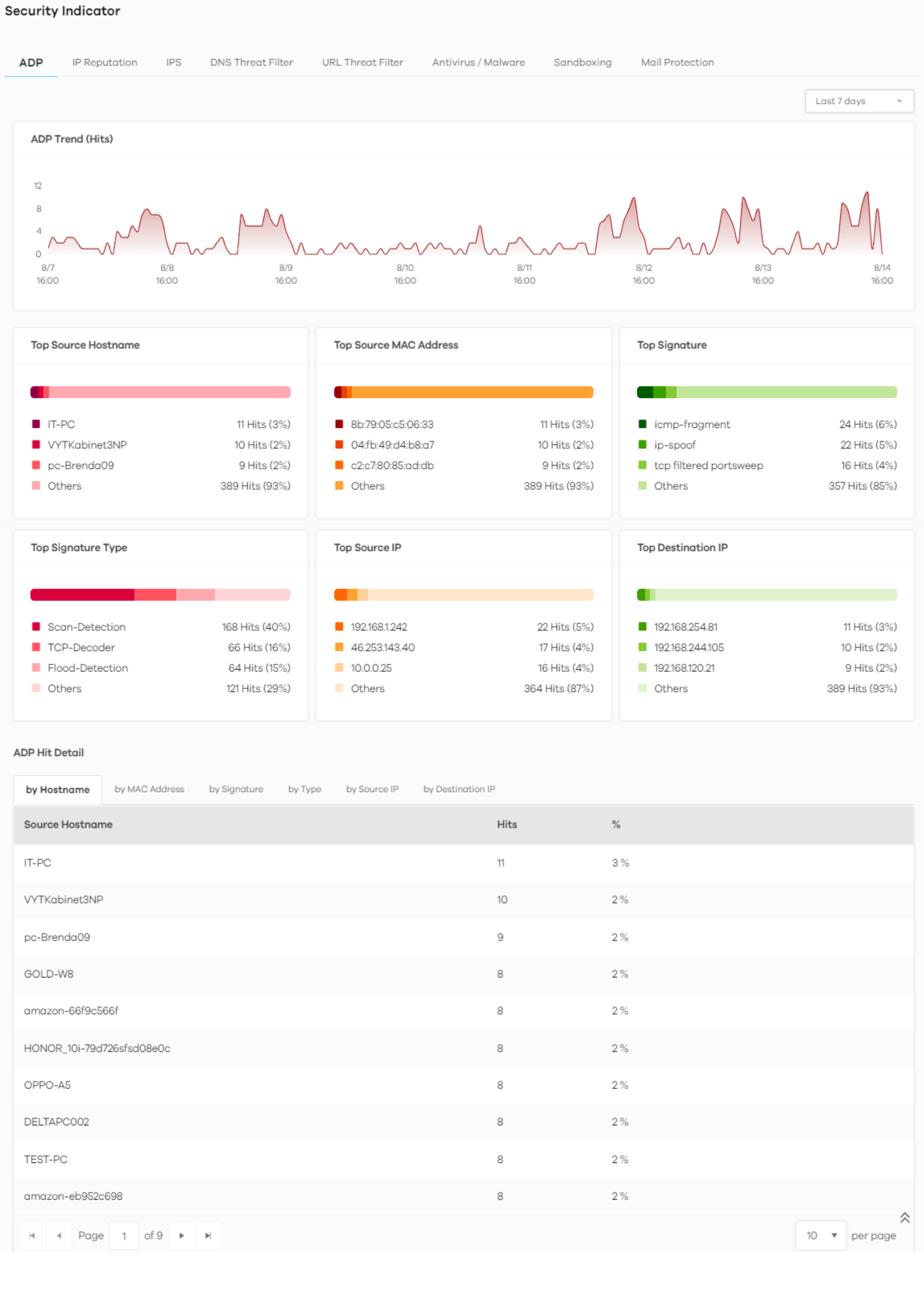
- TCP Decoder

- UDP Decoder
- ICMP Decoder

Protocol anomaly policies may be updated when you upload new firmware.

The following figure shows the **Analysis** > **Security Indicator** > **ADP** data visualizations.

Figure 12 Analysis > Security Indicator > ADP



Top Source Hostname

IT-PC	11 Hits (3%)
VYTKabinet3NP	10 Hits (2%)
pc-Brenda09	9 Hits (2%)
Others	389 Hits (93%)

Top Source MAC Address

8b:79:05:c5:06:33	11 Hits (3%)
04:fb:49:d4:b8:a7	10 Hits (2%)
c2:c7:80:85:ad:db	9 Hits (2%)
Others	389 Hits (93%)

Top Signature

icmp-fragment	24 Hits (6%)
ip-spoof	22 Hits (5%)
tcp filtered portsweep	16 Hits (4%)
Others	357 Hits (85%)

Top Signature Type

Scan-Detection	168 Hits (40%)
TCP-Decoder	66 Hits (16%)
Flood-Detection	64 Hits (15%)
Others	121 Hits (29%)

Top Source IP

192.168.1.242	22 Hits (5%)
46.253.143.40	17 Hits (4%)
10.0.0.25	16 Hits (4%)
Others	364 Hits (87%)

Top Destination IP

192.168.254.81	11 Hits (3%)
192.168.244.105	10 Hits (2%)
192.168.120.21	9 Hits (2%)
Others	389 Hits (93%)

ADP Hit Detail

Source Hostname	Hits	%
IT-PC	11	3 %
VYTKabinet3NP	10	2 %
pc-Brenda09	9	2 %
GOLD-W8	8	2 %
amazon-66f9c566f	8	2 %
HONOR_10i-79d726sfsd08e0c	8	2 %
OPPO-A5	8	2 %
DELTAPC002	8	2 %
TEST-PC	8	2 %
amazon-eb952c698	8	2 %

The following table describes the labels on the **Analysis** > **Security Indicator** > **ADP** screen.

Table 10 Analysis > Security Indicator > ADP

LABEL	DESCRIPTION
ADP Trend (Hits)	This chart displays patterns in anomalies detected by the Zyxel Device. Anomalies are based on violations of protocol standards (RFCs – Requests for Comments) or abnormal flows such as port scans. Move your cursor over a trend line to display the number of threats encountered over time. An anomaly hit is an anomaly detected by the Zyxel Device.
Top Source Hostname	This chart displays the names of three devices that mostly send traffic to anomalous connections. Scroll down to **ADP Hit Detail** and click the **by Hostname** tab to display details about the anomalies that were detected.
Top Source MAC Address	This chart displays the MAC addresses of the three devices that mostly send traffic to anomalous connections. Scroll down to **ADP Hit Detail** and click the **by MAC Address** tab to display details about the anomalies that were detected.
Top Signature	This chart displays the three most common anomalies detected by the Zyxel Device. Scroll down to **ADP Hit Detail** and click the **by Signature** tab to display details about the anomalies that were detected.
Top Signature Type	This chart displays the three most common anomaly types detected by the Zyxel Device. Scroll down to **ADP Hit Detail** and click the **by Type** tab to display details about the anomalies that were detected.
Top Source IP	This chart displays the IP addresses of the three devices that mostly send traffic to anomalous connections. Scroll down to **ADP Hit Detail** and click the **by Source IP** tab to display details about the anomalies that were detected.
Top Destination IP	This chart displays the IP addresses of the three devices that mostly receive traffic from anomalous connections. Scroll down to **ADP Hit Detail** and click the **by Destination IP** tab to display details about the anomalies that were detected.
ADP Hit Detail	This displays the number of anomalies detected by the Zyxel Device, categorized by hostname, MAC address, signature, signature type, source IP address, and destination IP address.

2.3.2 IP Reputation

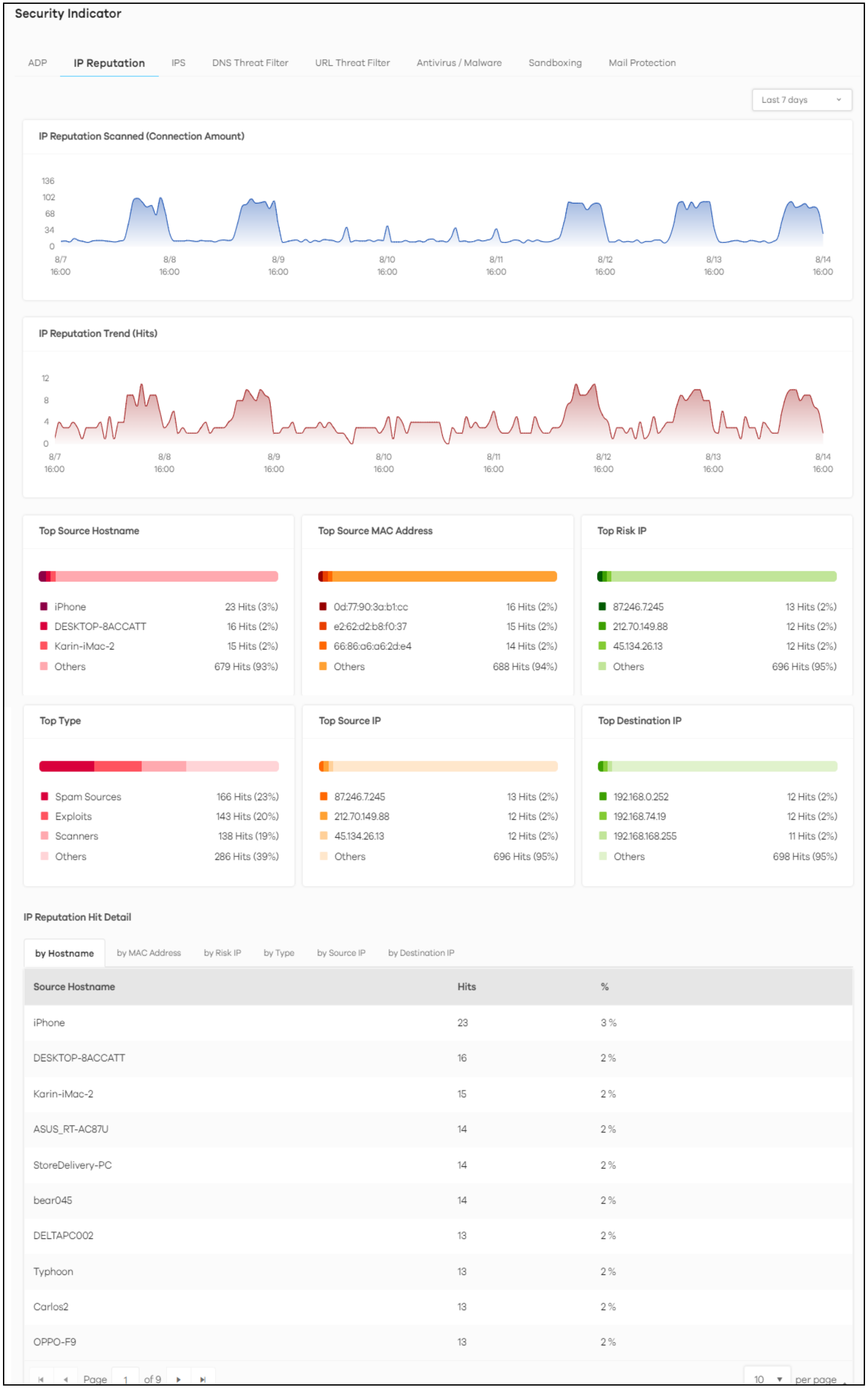
When you register for and enable the IP reputation service, your Zyxel Device downloads signature files that identifies reputation of IPv4 addresses. You can have the Zyxel Device forward, block, and/or log packets from IPv4 addresses based on these signatures and categories.

The priority for IP Reputation checking is as below:

- White List
- Black List
- External Black List
- Local Zyxel Device Signatures

The following figure shows the **Analysis** > **Security Indicator** > **IP Reputation** data visualizations.

Figure 13 Analysis > Security Indicator > IP Reputation



Top Source Hostname

iPhone	23 Hits (3%)
DESKTOP-8ACCATT	16 Hits (2%)
Karin-iMac-2	15 Hits (2%)
Others	679 Hits (93%)

Top Source MAC Address

0d:77:90:3a:b1:cc	16 Hits (2%)
e2:62:d2:b8:f0:37	15 Hits (2%)
66:86:a6:a6:2d:e4	14 Hits (2%)
Others	688 Hits (94%)

Top Risk IP

87.246.7.245	13 Hits (2%)
212.70.149.88	12 Hits (2%)
45.134.26.13	12 Hits (2%)
Others	696 Hits (95%)

Top Type

Spam Sources	166 Hits (23%)
Exploits	143 Hits (20%)
Scanners	138 Hits (19%)
Others	286 Hits (39%)

Top Source IP

87.246.7.245	13 Hits (2%)
212.70.149.88	12 Hits (2%)
45.134.26.13	12 Hits (2%)
Others	696 Hits (95%)

Top Destination IP

192.168.0.252	12 Hits (2%)
192.168.74.19	12 Hits (2%)
192.168.168.255	11 Hits (2%)
Others	698 Hits (95%)

IP Reputation Hit Detail

Source Hostname	Hits	%
iPhone	23	3 %
DESKTOP-8ACCATT	16	2 %
Karin-iMac-2	15	2 %
ASUS_RT-AC87U	14	2 %
StoreDelivery-PC	14	2 %
bear045	14	2 %
DELTAPC002	13	2 %
Typhoon	13	2 %
Carlos2	13	2 %
OPPO-F9	13	2 %

The following table describes the labels on the **Analysis** > **Security Indicator** > **IP Reputation** screen.

Table 11 Analysis > Security Indicator > IP Reputation

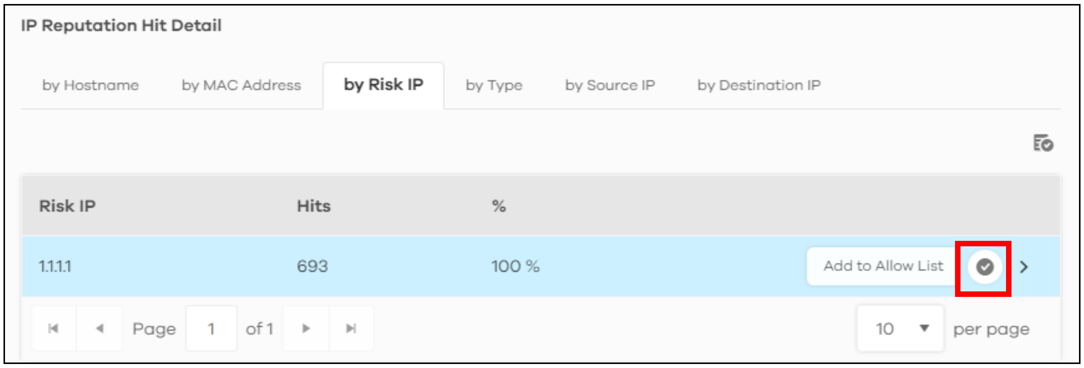
LABEL	DESCRIPTION
IP Reputation Scanned (Connection Amount)	This chart displays the total number of connections detected by the Zyxel Device. Move your cursor over a trend line to display the number of connections encountered over time.
IP Reputation Trend (Hits)	This chart displays the number of IP reputation threats detected by the Zyxel Device. Move your cursor over a trend line to display the number of threats encountered over time.
Top Source Hostname	This chart displays the hostnames of the three devices that mostly send traffic to connections with IP addresses of poor reputation. Scroll down to **IP Reputation Hit Detail** and click the **by Hostname** tab to display details about the source hostnames that were detected.
Top Source MAC Address	This chart displays the MAC addresses of the three devices that mostly send traffic to connections with IP addresses of poor reputation. Scroll down to **IP Reputation Hit Detail** and click the **by MAC Address** tab to display details about the source MAC addresses that were detected.
Top Risk IP	This chart displays the the IP addresses of the three devices that caused the most IP reputation threats. Scroll down to **IP Reputation Hit Detail** and click the **by Risk IP** tab to display details about the IP addresses that were detected by IP Reputation. Click an IP address to display the details.
Top Type	This chart displays the three most common threats posed by IPs detected by the Zyxel Device as detected by IP Reputation. Threat categories include **Negative Reputation**, **TOR Proxies**, **Denial of Service**, **Scanners**, **Web Attacks**, **Exploits**, **Spam Sources**, **Anonymous Proxies**, **Phishing**, and **Botnets**. Scroll down to **IP Reputation Hit Detail** and click the **by Type** tab to display details about the threats posed by IPs detected by the Zyxel Device as detected by IP Reputation. Note: See more details of threat categories in the ZyWALL User's Guide.
Top Source IP	This chart displays the IP addresses of the three devices that mostly send traffic to connections with IP addresses of poor reputation. Scroll down to **IP Reputation Hit Detail** and click the **by Source IP** tab to display details about the source IP addresses that were detected.
Top Destination IP	This chart displays the IP addresses of the three devices that mostly receive traffic from connections with IP addresses of poor reputation. Scroll down to **IP Reputation Hit Detail** and click the **by Destination IP** tab to display details about the destination IP addresses that were detected.
IP Reputation Hit Detail	This displays the number of IP reputation threats detected by the Zyxel Device, categorized by hostname, MAC address, risk IP address, threat type, source IP address, and destination IP address. See Section 2.3.2.1 on page 28 for more information on how to add or remove a risk IP address from the allow list.

2.3.2.1 Add or Remove a Risk IP Address to the Allow List

There is a blue check mark ✓ next to the risk IP addresses that are in the allow list.

Do the following to add a risk IP address to the allow list:

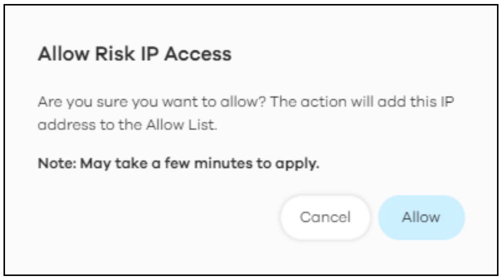
1 Go to the **Analysis** > **Security Indicator** > **IP Reputation** screen and scroll down to **IP Reputation Hit Detail** and click the **by Risk IP** tab. click the ✓ button next to the risk IP address.



IP Reputation Hit Detail

Risk IP	Hits	%
1.1.1.1	693	100 %

2 The following window pops up, click **Allow** to add the risk IP address to the allow list.



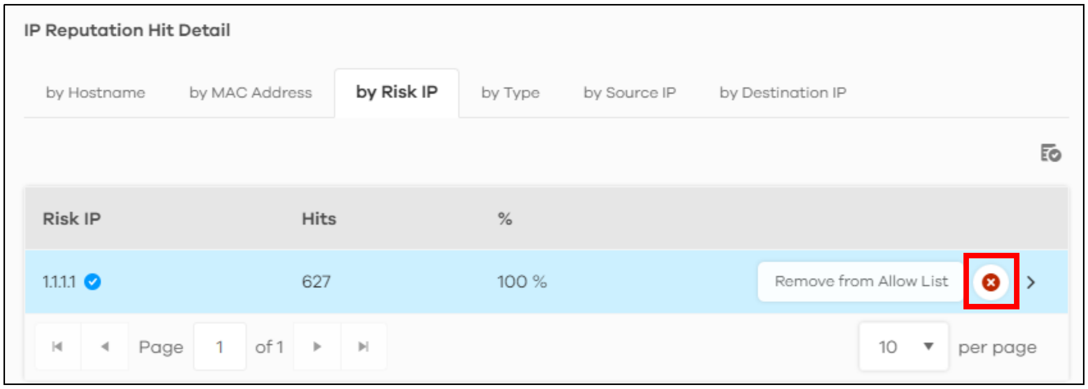
Allow Risk IP Access

Are you sure you want to allow? The action will add this IP address to the Allow List.

Note: May take a few minutes to apply.

Do the following to remove a risk IP address from the allow list:

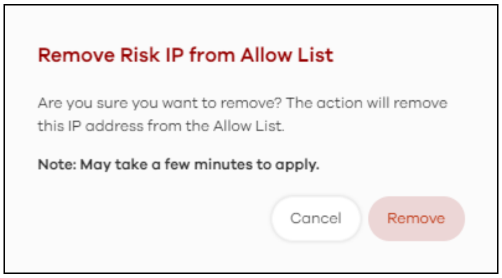
1 Go to the **Analysis** > **Security Indicator** > **IP Reputation** screen and scroll down to **IP Reputation Hit Detail** and click the **by Risk IP** tab. Click the ✕ button next to the risk IP address.



IP Reputation Hit Detail

Risk IP	Hits	%
1.1.1.1 ✓	627	100 %

2 The following window pops up, click **Remove** to remove the IP address from the allow list.



Remove Risk IP from Allow List

Are you sure you want to remove? The action will remove this IP address from the Allow List.

Note: May take a few minutes to apply.

2.3.3 IPS

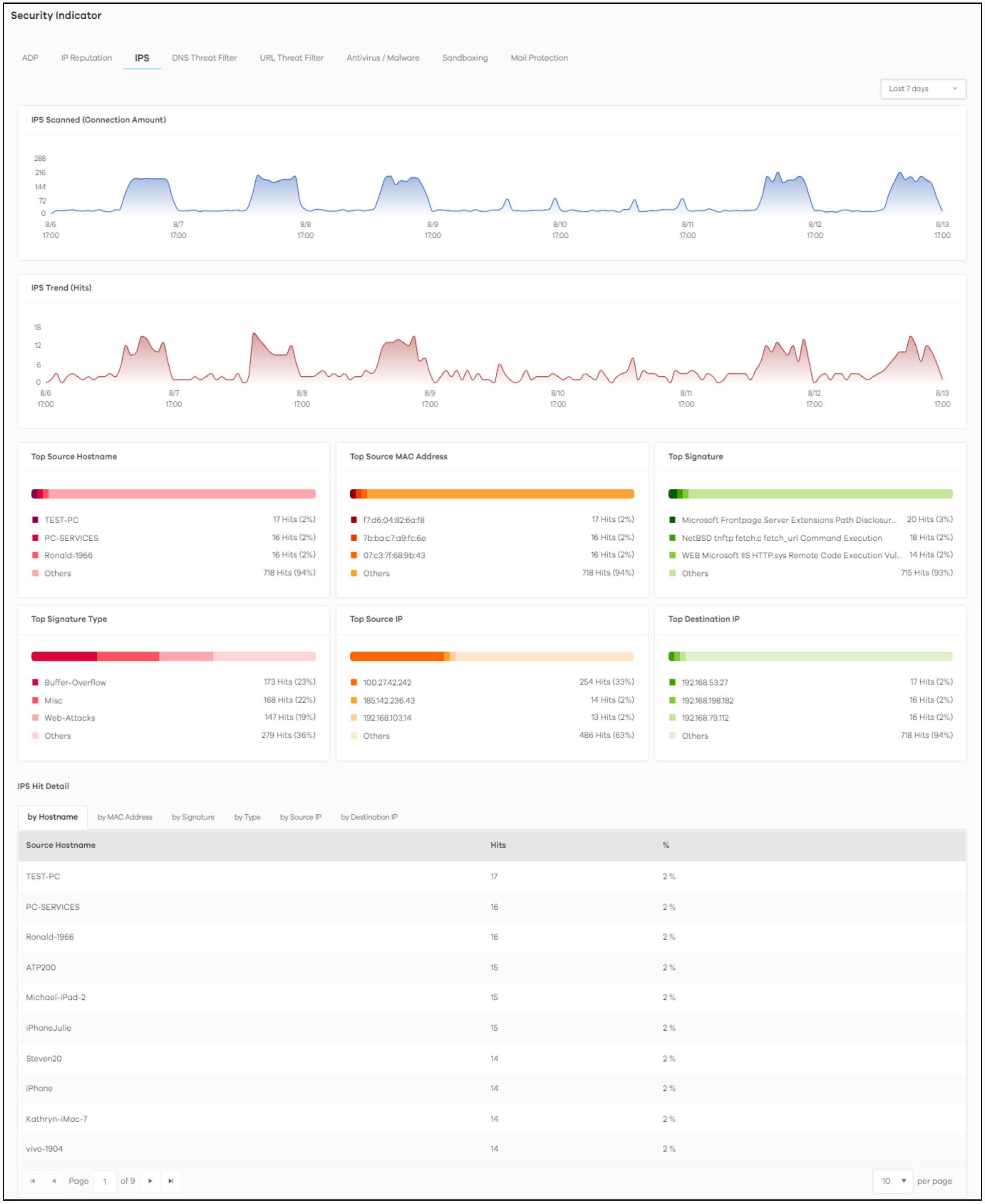
An IPS profile is a set of packet inspection signatures.

A signature is a pattern of malicious or suspicious packet activity. You can specify an action to be taken if the system matches a stream of data to a malicious signature. You can change the action in the profile screens. Packet inspection examine OSI (Open System Interconnection) layer-4 to layer-7 packet contents for malicious data. Generally, packet inspection signatures are created for known attacks while anomaly detection looks for abnormal behavior.

Changes to the Zyxel Device's IPS settings affect new sessions, but not the sessions that already exists before you apply the new settings.

The following figure shows the **Analysis** > **Security Indicator** > **IPS** data visualizations.

Figure 14 Analysis > Security Indicator > IPS



Top Source Hostname

■ TEST-PC	17 Hits (2%)
■ PC-SERVICES	16 Hits (2%)
■ Ronald-1966	16 Hits (2%)
■ Others	718 Hits (94%)

Top Source MAC Address

■ f7:d6:04:82:6a:f8	17 Hits (2%)
■ 7b:ba:c7:a9:fc:6e	16 Hits (2%)
■ 07:c3:7f:68:9b:43	16 Hits (2%)
■ Others	718 Hits (94%)

Top Signature

■ Microsoft Frontpage Server Extensions Path Disclosur...	20 Hits (3%)
■ NetBSD tnftp fetch.c fetch_url Command Execution	18 Hits (2%)
■ WEB Microsoft IIS HTTP.sys Remote Code Execution Vul...	14 Hits (2%)
■ Others	715 Hits (93%)

Top Signature Type

■ Buffer-Overflow	173 Hits (23%)
■ Misc	168 Hits (22%)
■ Web-Attacks	147 Hits (19%)
■ Others	279 Hits (36%)

Top Source IP

■ 100.27.42.242	254 Hits (33%)
■ 185.142.236.43	14 Hits (2%)
■ 192.168.103.14	13 Hits (2%)
■ Others	486 Hits (63%)

Top Destination IP

■ 192.168.53.27	17 Hits (2%)
■ 192.168.198.182	16 Hits (2%)
■ 192.168.79.112	16 Hits (2%)
■ Others	718 Hits (94%)

IPS Hit Detail

Source Hostname	Hits	%
TEST-PC	17	2 %
PC-SERVICES	16	2 %
Ronald-1966	16	2 %
ATP200	15	2 %
Michael-iPad-2	15	2 %
iPhoneJulie	15	2 %
Steven20	14	2 %
iPhone	14	2 %
Kathryn-iMac-7	14	2 %
vivo-1904	14	2 %

The following table describes the labels on the **Analysis** > **Security Indicator** > **IPS** screen.

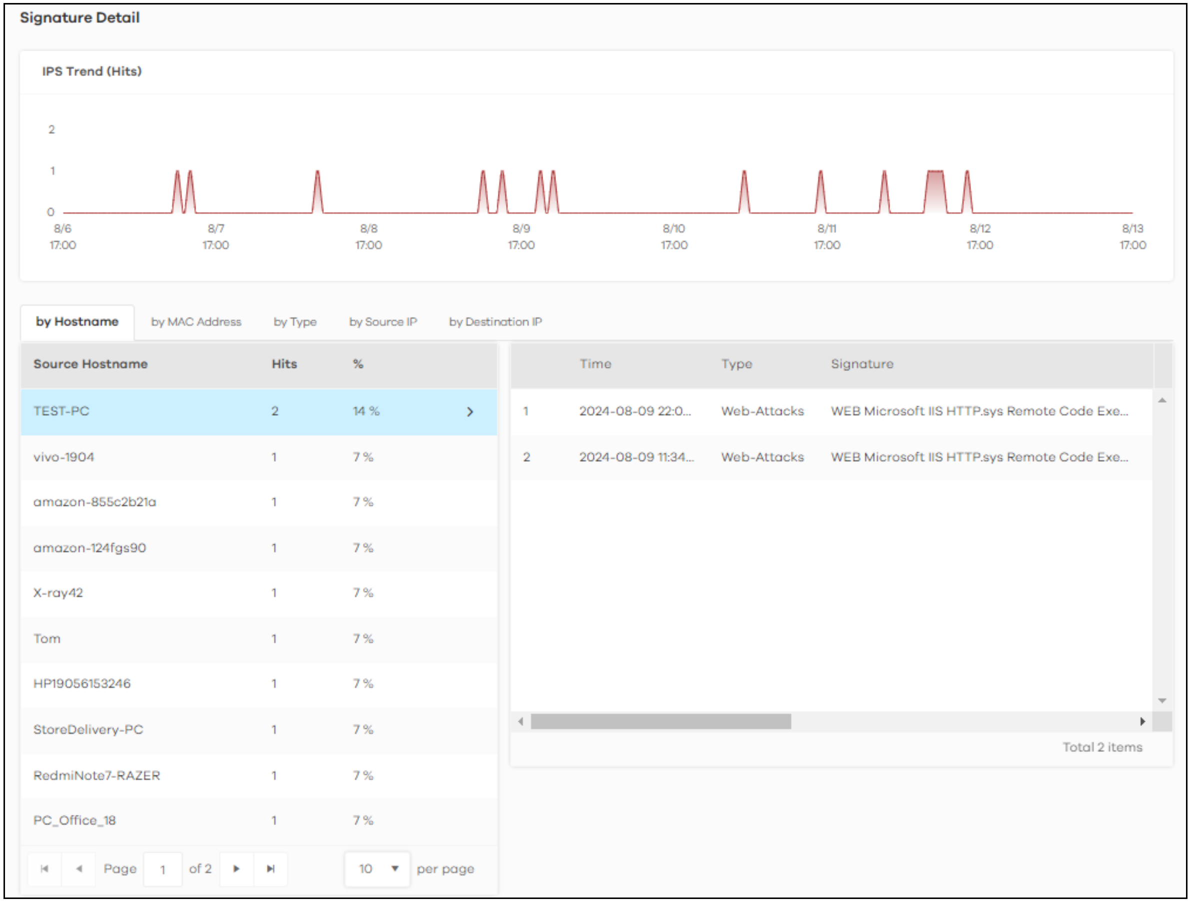
Table 12 Analysis > Security Indicator > IPS

LABEL	DESCRIPTION
IPS Scanned (Connection Amount)	This chart displays the total number of connections detected by the Zyxel Device. Move your cursor over a trend line to display the number of connections encountered over time.
IPS Trend (Hits)	This chart displays the number of malicious or suspicious packets detected by IPS in the Zyxel Devices. IPS (Intrusion Prevention System) uses signatures to detect malicious or suspicious packets to protect against network-based intrusions. Move your cursor over a trend line to display the number of threats encountered over time.
Top Source Hostname	This chart displays the hostnames of the three devices that mostly send traffic to malicious or suspicious connections. Scroll down to **IP Reputation Hit Detail** and click the **by Hostname** tab to display details about the source host names that were detected.
Top Source MAC Address	This chart displays the MAC addresses of the three devices that mostly send traffic to malicious or suspicious connections. Scroll down to **IP Reputation Hit Detail** and click the **by MAC Address** tab to display details about the source MAC addresses that were detected.
Top Signature	This chart displays the top three malicious or suspicious packets detected by IPS in the Zyxel Devices. Scroll down to **IPS Hit Detail** and click the **by Signature** tab to display details about the intrusions that were detected.
Top Signature Type	This chart displays the top three malicious or suspicious packet types detected by IPS in the Zyxel Devices. Scroll down to **IPS Hit Detail** and click the **by Type** tab to display details about the intrusions that were detected.
Top Source IP	This chart displays the source IP addresses of the top three incoming malicious or suspicious packets detected by IPS in the Zyxel Devices. Scroll down to **IPS Hit Detail** and click the **by Source IP** tab to display details about the source IP addresses of the incoming malicious or suspicious packets.
Top Destination IP	This chart displays the destination IP addresses of the top three incoming malicious or suspicious packets detected by IPS in the Zyxel Devices. Scroll down to **IPS Hit Detail** and click the **by Destination IP** tab to display details about the destination IP addresses of the incoming malicious or suspicious packets.
IPS Hit Detail	This displays the number of malicious or suspicious packets detected by the Zyxel Device, categorized by hostname, MAC address, signature, signature type, source IP address, and destination IP address.

2.3.3.1 Threat Intelligence

Click any item in the **by Signature** table to view the malicious or suspicious packets detected by IPS in detail.

Figure 15 Top Signature Details



Source Hostname	Hits	%
TEST-PC	2	14 %
vivo-1904	1	7 %
amazon-855c2b21a	1	7 %
amazon-124fgs90	1	7 %
X-ray42	1	7 %
Tom	1	7 %
HP19056153246	1	7 %
StoreDelivery-PC	1	7 %
RedmiNote7-RAZER	1	7 %
PC_Office_18	1	7 %

	Time	Type	Signature
1	2024-08-09 22:0...	Web-Attacks	WEB Microsoft IIS HTTP.sys Remote Code Exe...
2	2024-08-09 11:34...	Web-Attacks	WEB Microsoft IIS HTTP.sys Remote Code Exe...

2.3.4 DNS Threat Filter

A Domain Name System (DNS) server records mappings of FQDN (Fully Qualified Domain Names) to IP addresses. A FQDN consists of a host and domain name. For example, www.zyxel.com is a fully qualified domain name, where “www” is the host, “zyxel” is the second-level domain, and “com” is the top level domain.

DNS filtering inspects DNS queries made by clients on your network and compares the queries against a database of blocked or allowed Fully Qualified Domain Names (FQDNs).

If a user attempts to connect to a suspect site, where the DNS query packet contains an FQDN with a bad reputation, then a DSN query is sent from the user’s computer and detected by the DNS Filter.

The Zyxel Device DNS threat filter will either drop the DNS query or reply to the user with a fake DNS response using the default dnsft.cloud.zyxel.com URL (where the user will see a “Web Page Blocked!” page) or a custom IP address.

The following type of DNS queries is allowed by the Zyxel Device:

- Type “A” for IPv4 addresses

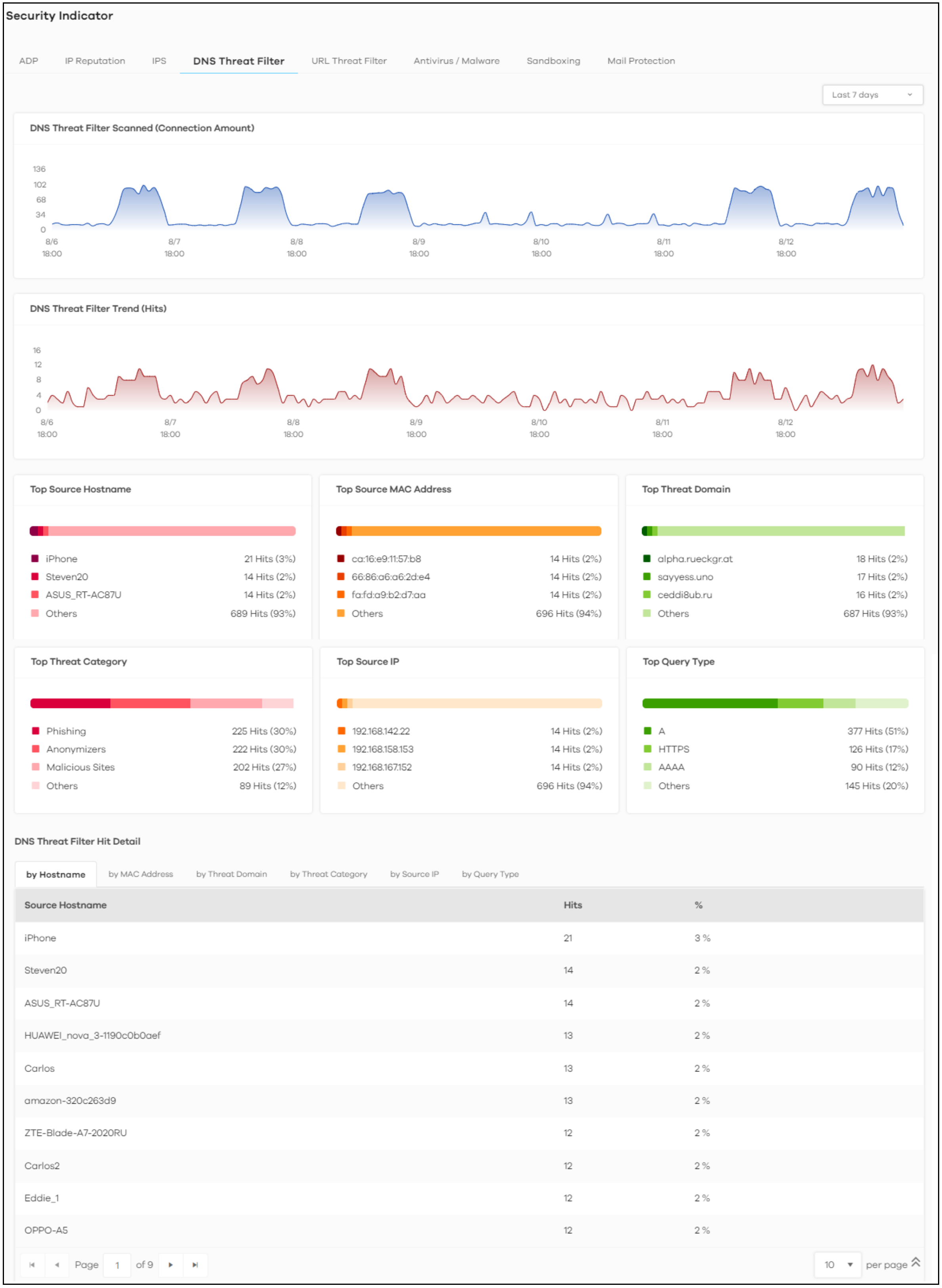
The Zyxel Device replies with a DNS server error for the following types of DNS queries:

- Enter “AAAA” for IPv6 addresses

- Enter “NS” (Name Server) to get information about the authoritative name server
- Enter “MX” (Mail eXchange) to request information about the mail exchange server for a specific DNS domain name
- Enter “CNAME” (Canonical Names) that specifies a domain name that has to be queried in order to resolve the original DNS query
- Enter “PTR” (Pointer) that specifies a reverse query (requesting the FQDN corresponding to the IP address you provided
- Enter “SOA” (Start Of zone Authority) used when transferring zones

Click **Analysis** > **Security Indicator** > **DNS Threat Filter** to display the configuration screen as shown next.

Figure 16 Analysis > Security Indicator > DNS Threat Filter



Top Source Hostname

🟥 iPhone	21 Hits (3%)
🟥 Steven20	14 Hits (2%)
🟥 ASUS_RT-AC87U	14 Hits (2%)
🟥 Others	689 Hits (93%)

Top Source MAC Address

🟥 ca:16:e9:11:57:b8	14 Hits (2%)
🟧 66:86:a6:a6:2d:e4	14 Hits (2%)
🟧 fa:fd:a9:b2:d7:aa	14 Hits (2%)
🟧 Others	696 Hits (94%)

Top Threat Domain

🟩 alpha.rueckgr.at	18 Hits (2%)
🟩 sayyess.uno	17 Hits (2%)
🟩 ceddi8ub.ru	16 Hits (2%)
🟩 Others	687 Hits (93%)

Top Threat Category

🟥 Phishing	225 Hits (30%)
🟥 Anonymizers	222 Hits (30%)
🟥 Malicious Sites	202 Hits (27%)
🟥 Others	89 Hits (12%)

Top Source IP

🟧 192.168.142.22	14 Hits (2%)
🟧 192.168.158.153	14 Hits (2%)
🟧 192.168.167.152	14 Hits (2%)
🟧 Others	696 Hits (94%)

Top Query Type

🟩 A	377 Hits (51%)
🟩 HTTPS	126 Hits (17%)
🟩 AAAA	90 Hits (12%)
🟩 Others	145 Hits (20%)

DNS Threat Filter Hit Detail

by Hostname | by MAC Address | by Threat Domain | by Threat Category | by Source IP | by Query Type

Source Hostname	Hits	%
iPhone	21	3 %
Steven20	14	2 %
ASUS_RT-AC87U	14	2 %
HUAWEI_nova_3-1190c0b0aef	13	2 %
Carlos	13	2 %
amazon-320c263d9	13	2 %
ZTE-Blade-A7-2020RU	12	2 %
Carlos2	12	2 %
Eddie_1	12	2 %
OPPO-A5	12	2 %

Page 1 of 9 10 per page

The following table describes the labels on the **Analysis** > **Security Indicator** > **DNS Threat Filter** screen.

Table 13 Analysis > Security Indicator > DNS Threat Filter

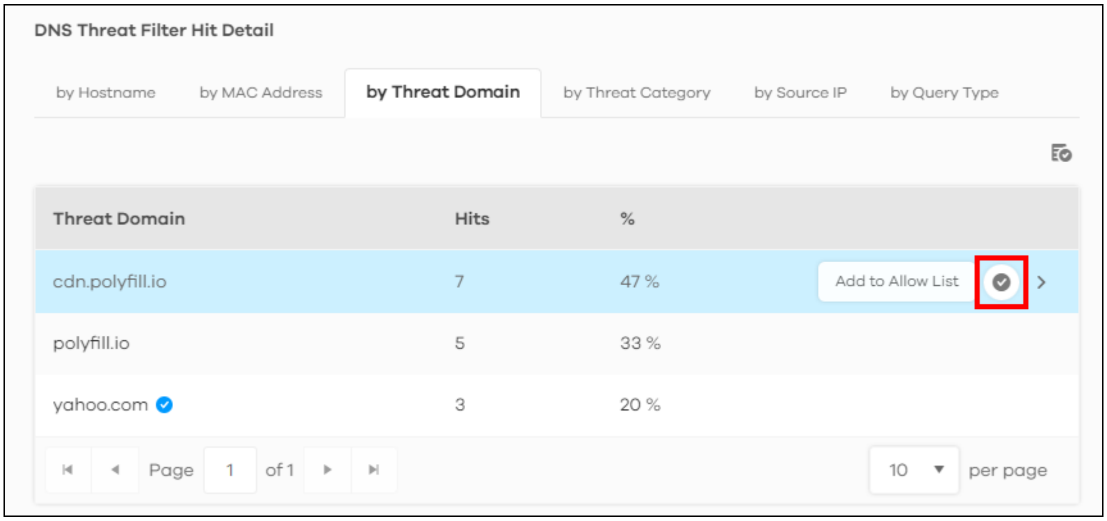
LABEL	DESCRIPTION
DNS Threat Filter Scanned (Connection Amount)	This chart displays the total number of connections detected by the Zyxel Device. Move your cursor over a trend line to display the number of connections encountered over time.
DNS Threat Filter Trend (Hits)	This chart displays the number of URLs of FQDNs that may pose a security threat to network devices that were scanned. Move your cursor over a trend line to display the number of URLs of FQDNs encountered over time.
Top Source Hostname	This chart displays the three most common source hostnames of the incoming malicious or suspicious files. Scroll down to **DNS Filter Hit Detail** and click the **by Hostname** tab to display details about the source hostnames.
Top Source MAC Address	This chart displays the three most common source MAC addresses of the incoming malicious or suspicious files. Scroll down to **DNS Filter Hit Detail** and click the **by MAC Address** tab to display details about the source MAC addresses.
Top Threat Domain	This chart displays the three most common URLs of FQDNs that may pose a security threat to network devices behind the Zyxel Device. Scroll down to **DNS Filter Hit Detail** and click the **by DNS Filter Domain** tab to display details about the URLs of FQDNs.
Top Threat Category	This chart displays the three most common categories of FQDNs that may pose a security threat to network devices behind the Zyxel Device. Scroll down to **DNS Filter Hit Detail** and click the **by Threat Category** tab to display details about the categories of FQDNs.
Top Source IP	This chart displays the three most common source IP addresses of the incoming malicious and/or suspicious files. Scroll down to **DNS Filter Hit Detail** and click the **by Source IP** tab to display details about the source IP addresses.
Top Query Type	This chart displays the three most commaon types of DNS (Domain Name System) record of the security threat to network devices behind the Zyxel Device. Scroll down to **DNS Filter Hit Detail** and click the **by Query Type** tab to display details about the DNS (Domain Name System) record type.
DNS Threat Filter Hit Detail	This displays the number of malicious or suspicious packets detected by the Zyxel Device, categorized by hostname, MAC address, threat domain, threat category, source IP address, and destination IP address. See Section 2.3.4.1 on page 36 for more information on how to add or remove a threat domain from the allow list.

2.3.4.1 Add or Remove a Threat Domain to the Allow List

There is a blue check mark ✓ next to the threat domains that are in the allow list.

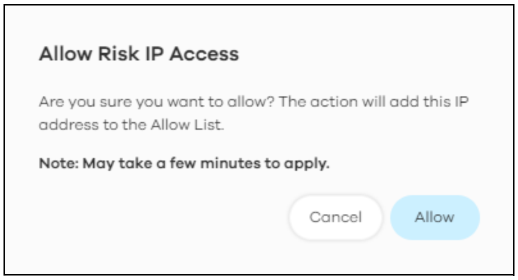
Do the following to add a threat domain to the allow list:

1 Go to the **Analysis** > **Security Indicator** > **DNS Threat Filter** screen and scroll down to **DNS Threat Filter Hit Detail** and click the **by Threat Domain** tab. click the ✓ button next to the threat domain.


DNS Threat Filter Hit Detail

Threat Domain	Hits	%	
cdn.polyfill.io	7	47 %	Add to Allow List
polyfill.io	5	33 %	
yahoo.com ✓	3	20 %	

2 The following window pops up, click **Allow** to add the domain to the allow list.

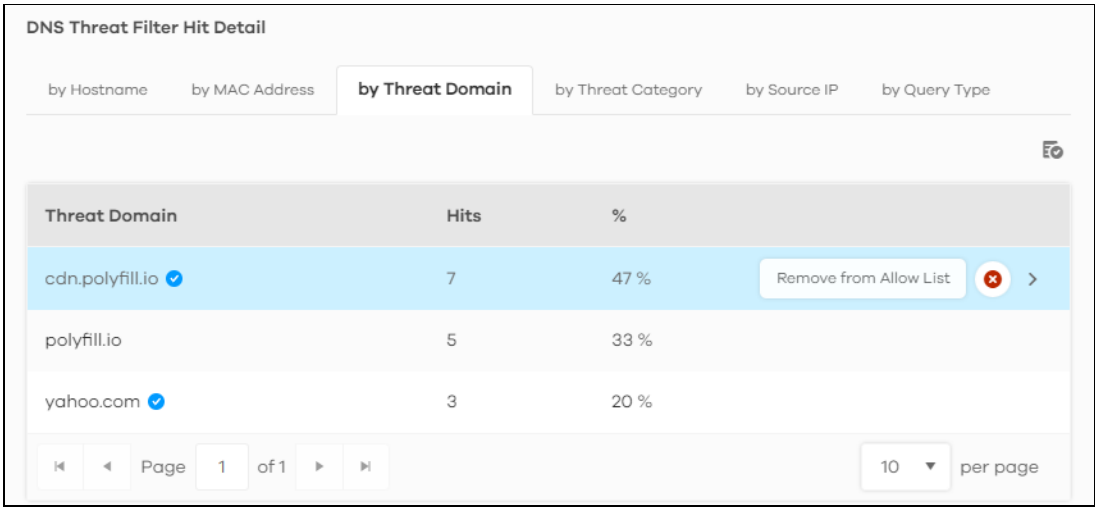

Allow Risk IP Access

Are you sure you want to allow? The action will add this IP address to the Allow List.

Note: May take a few minutes to apply.

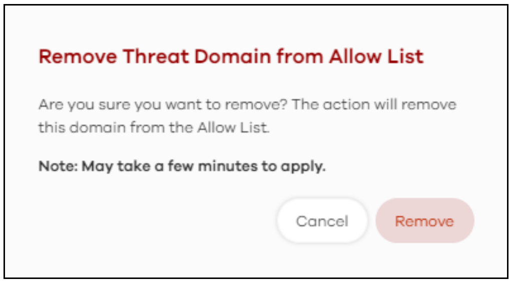
Do the following to remove a threat domain from the allow list:

1 Go to the **Analysis** > **Security Indicator** > **DNS Threat Filter** screen and scroll down to **DNS Threat Filter Hit Detail** and click the **by Threat Domain** tab. Click the ✖ button next to the threat domain.


DNS Threat Filter Hit Detail

Threat Domain	Hits	%	
cdn.polyfill.io ✓	7	47 %	Remove from Allow List
polyfill.io	5	33 %	
yahoo.com ✓	3	20 %	

2 The following window pops up, click **Remove** to remove the threat domain from the allow list.



Remove Threat Domain from Allow List

Are you sure you want to remove? The action will remove this domain from the Allow List.

Note: May take a few minutes to apply.

2.3.5 URL Threat Filter

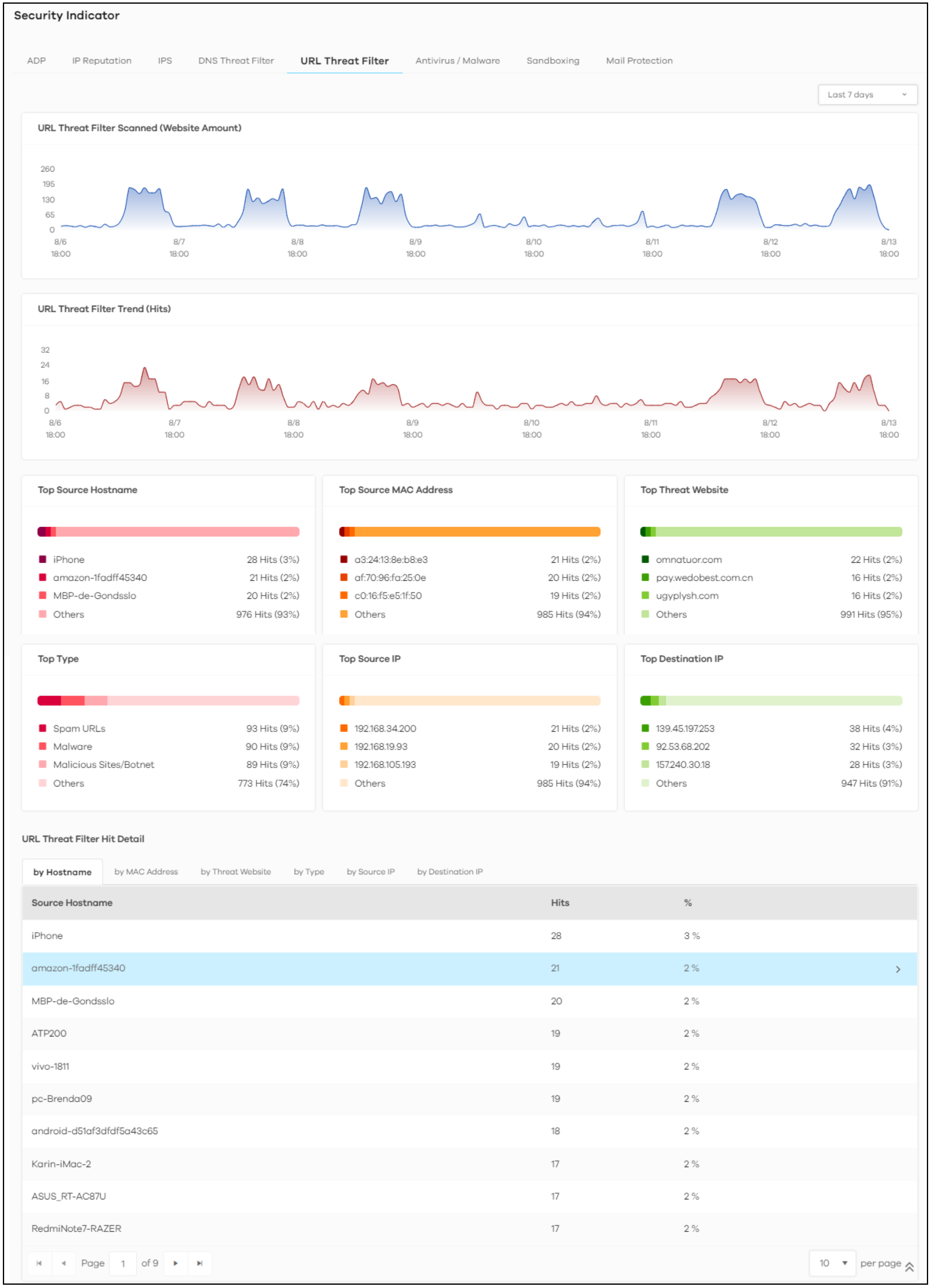
When you enable the URL Threat filtering service, your Zyxel Device downloads signature files that contain known URL Threat domain names and IP addresses. The Zyxel Device will also access an external database that has millions of web sites categorized based on content. You can have the Zyxel Device allow, block, warn and/or log access to web sites or hosts based on these signatures and categories.

The priority for URL Threat checking is as below:

- White List
- Black List
- External Black List
- Local Zyxel Device Signatures
- Cloud Query Cache
- Cloud Query

The following figure shows the **Analysis** > **Security Indicator** > **URL Threat Filter** data visualizations.

Figure 17 Analysis > Security Indicator > URL Threat Filter



Security Indicator

URL Threat Filter Scanned (Website Amount)

URL Threat Filter Trend (Hits)

Top Source Hostname

iPhone	28 Hits (3%)
amazon-1fadff45340	21 Hits (2%)
MBP-de-Gondsslo	20 Hits (2%)
Others	976 Hits (93%)

Top Source MAC Address

a3:24:13:8e:b8:e3	21 Hits (2%)
af:70:96:fa:25:0e	20 Hits (2%)
c0:16:f5:e5:1f:50	19 Hits (2%)
Others	985 Hits (94%)

Top Threat Website

omnatuor.com	22 Hits (2%)
pay.wedobest.com.cn	16 Hits (2%)
ugyplysh.com	16 Hits (2%)
Others	991 Hits (95%)

Top Type

Spam URLs	93 Hits (9%)
Malware	90 Hits (9%)
Malicious Sites/Botnet	89 Hits (9%)
Others	773 Hits (74%)

Top Source IP

192.168.34.200	21 Hits (2%)
192.168.19.93	20 Hits (2%)
192.168.105.193	19 Hits (2%)
Others	985 Hits (94%)

Top Destination IP

139.45.197.253	38 Hits (4%)
92.53.68.202	32 Hits (3%)
157.240.30.18	28 Hits (3%)
Others	947 Hits (91%)

URL Threat Filter Hit Detail

Source Hostname	Hits	%
iPhone	28	3 %
amazon-1fadff45340	21	2 %
MBP-de-Gondsslo	20	2 %
ATP200	19	2 %
vivo-1811	19	2 %
pc-Brenda09	19	2 %
android-d51af3dfdf5a43c65	18	2 %
Karin-iMac-2	17	2 %
ASUS_RT-AC87U	17	2 %
RedmiNote7-RAZER	17	2 %

The following table describes the labels on the **Analysis** > **Security Indicator** > **URL Threat Filter** screen.

Table 14 Analysis > Security Indicator > URL Threat Filter

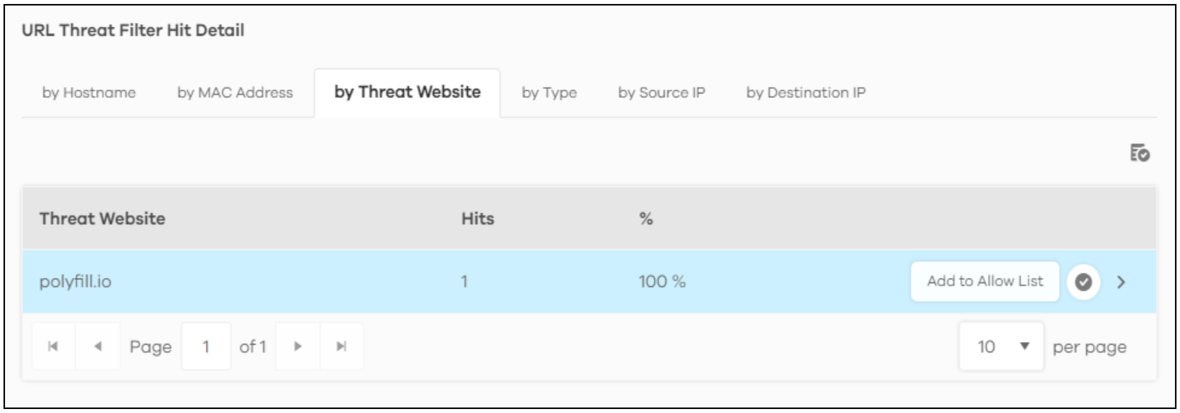
LABEL	DESCRIPTION
URL Threat Filter Scanned (Website Amount)	This chart displays the total number of connections detected by the Zyxel Device. Move your cursor over a trend line to display the number of connections encountered over time.
URL Threat Filter Trend (Hits)	This chart displays the number of threats posed by websites detected by the Zyxel Devices. Move your cursor over a trend line to display the number of threats encountered over time.
Top Source Hostname	This chart displays the three most common source hostnames of the incoming malicious or suspicious files. Scroll down to **DNS Filter Hit Detail** and click the **by Hostname** tab to display details about the source hostnames.
Top Source MAC Address	This chart displays the three most common source MAC addresses of the incoming malicious or suspicious files. Scroll down to **DNS Filter Hit Detail** and click the **by MAC Address** tab to display details about the source MAC addresses.
Top Threat Website	This chart displays the top three threat websites detected by the Zyxel Device. Scroll down to **URL Threat Filter Hit Detail** and click the **by Threat Website** tab to display details about the specific websites that were detected.
Top Type	This chart displays the top three most common types of threats posed by websites detected by the Zyxel Devices. Threat categories include **Spam URL**, **Malicious Sites/ Botnet**, **Black List**, **Anonymizers**, **Spyware Adware Keylogger**, **Browser Exploits**, and **Phishing**. Scroll down to **URL Threat Filter Hit Detail** and click the **by Type** tab to display details about the threats posed by websites that were detected. Note: See more details of threat categories in ZyWALL User's Guides.
Top Source IP	This chart displays the source IP addresses of the three most common incoming threat websites. Scroll down to **URL Threat Filter Hit Detail** and click the **by Source IP** tab to display details about the source IP addresses of the incoming threat websites that were detected.
Top Destination IP	This chart displays the destination IP addresses of the three most common incoming threat websites. Scroll down to **URL Threat Filter Hit Detail** and click the **by Destination IP** tab to display details about the destination IP addresses of the incoming threat websites that were detected.
URL Threat Filter Hit Detail	This displays the number of threat websites detected by the Zyxel Device, categorized by hostname, MAC address, threat website, threat type, source IP address, or destination IP address. See Section 2.3.5.1 on page 40 for more information on how to add or remove a domain from the allow list.

2.3.5.1 Add or Remove a Threat Website to the Allow List

There is a blue check mark ✓ next to the domain in the allow list.

Do the following to add a domain to the allow list:

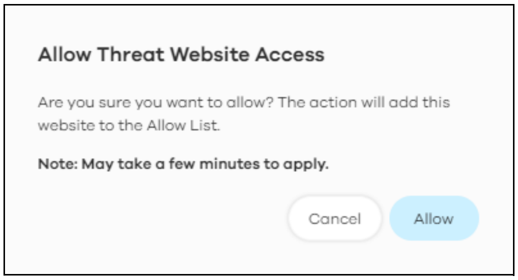
1 Go to the **Analysis** > **Security Indicator** > **URL Threat Filter** screen and scroll down to **URL Threat Filter Hit Detail** and click the **by Threat URL** tab. click the ✓ button next to the threat website.



URL Threat Filter Hit Detail

Threat Website	Hits	%
polyfill.io	1	100 %

2 The following window pops up, click **Allow** to add the threat website to the allow list.



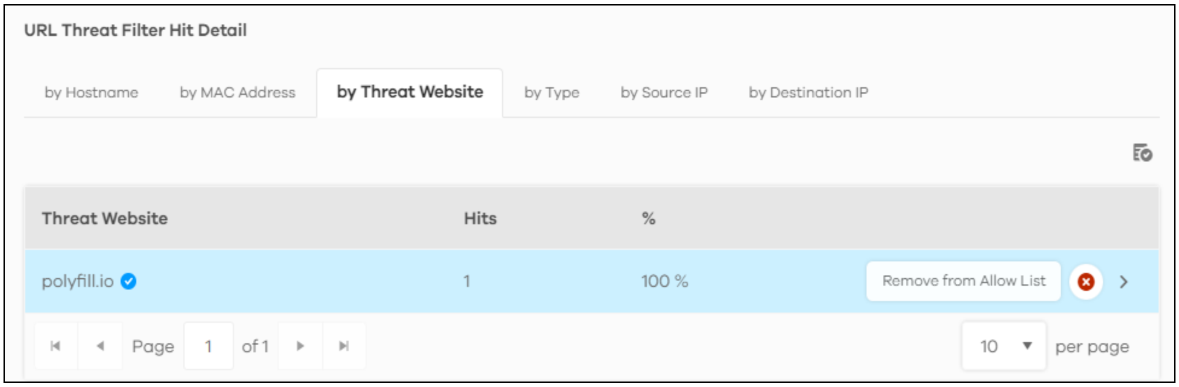
Allow Threat Website Access

Are you sure you want to allow? The action will add this website to the Allow List.

Note: May take a few minutes to apply.

Do the following to remove a threat website from the allow list:

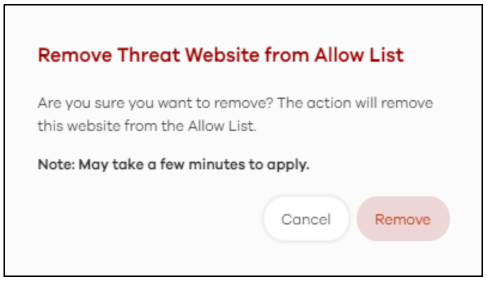
1 Go to the **Analysis** > **Security Indicator** > **URL Threat Filter** screen and scroll down to **URL Threat Filter Hit Detail** and click the **by Threat Website** tab. Click the ✗ button next to the threat website.



URL Threat Filter Hit Detail

Threat Website	Hits	%
polyfill.io ✓	1	100 %

2 The following window pops up, click **Remove** to remove the threat website from the allow list.



Remove Threat Website from Allow List

Are you sure you want to remove? The action will remove this website from the Allow List.

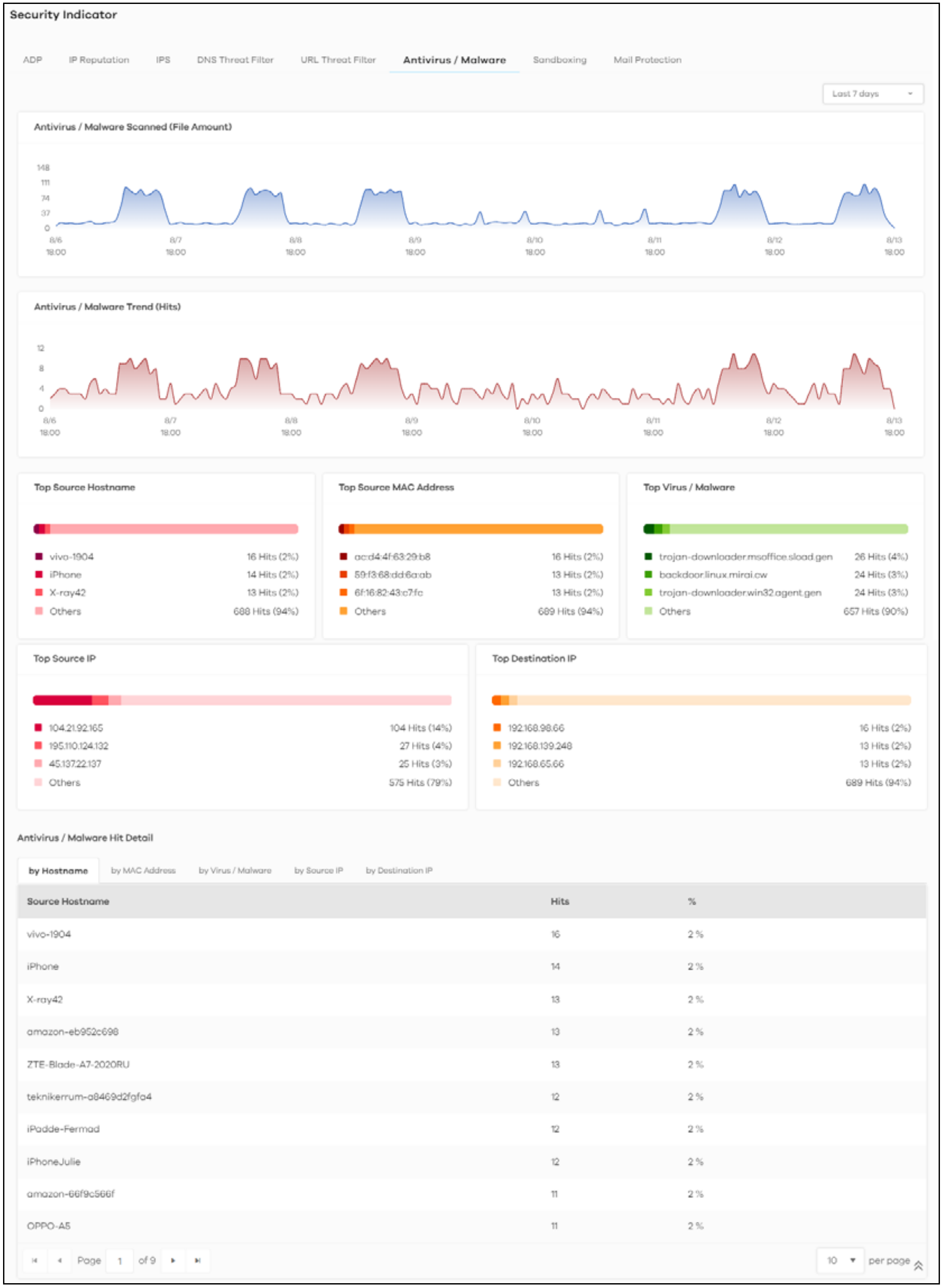
Note: May take a few minutes to apply.

2.3.6 Antivirus / Malware

Malware is short for malicious software, such as computer viruses, worms and spyware. The Zyxel Device antivirus / malware feature protects your connected network from malware by scanning traffic coming in from the WAN and going out from the WAN. The traffic scanned by the Zyxel Device may include FTP traffic and email with attachments.

The following figure shows the **Analysis** > **Security Indicator** > **Antivirus** / **Malware** data visualizations.

Figure 18 Analysis > Security Indicator > Antivirus / Malware



Top Source Hostname

vivo-1904	16 Hits (2%)
iPhone	14 Hits (2%)
X-ray42	13 Hits (2%)
Others	688 Hits (94%)

Top Source MAC Address

ac:d4:4f:63:29:b8	16 Hits (2%)
59:f3:68:dd:6a:ab	13 Hits (2%)
6f:16:82:43:c7:fc	13 Hits (2%)
Others	689 Hits (94%)

Top Virus / Malware

trojan-downloader.msoffice.sload.gen	26 Hits (4%)
backdoor.linux.mirai.cw	24 Hits (3%)
trojan-downloader.win32.agent.gen	24 Hits (3%)
Others	657 Hits (90%)

Top Source IP

104.21.92.165	104 Hits (14%)
195.110.124.132	27 Hits (4%)
45.137.22.137	25 Hits (3%)
Others	575 Hits (79%)

Top Destination IP

192.168.98.66	16 Hits (2%)
192.168.139.248	13 Hits (2%)
192.168.65.66	13 Hits (2%)
Others	689 Hits (94%)

Antivirus / Malware Hit Detail

Source Hostname	Hits	%
vivo-1904	16	2 %
iPhone	14	2 %
X-ray42	13	2 %
amazon-eb952c698	13	2 %
ZTE-Blade-A7-2020RU	13	2 %
teknikerrum-a8469d2fgfa4	12	2 %
iPadde-Fermad	12	2 %
iPhoneJulie	12	2 %
amazon-66f9c566f	11	2 %
OPPO-A5	11	2 %

The following table describes the labels on the **Analysis** > **Security Indicator** > **Antivirus** / **Malware** screen.

Table 15 Analysis > Security Indicator > Antivirus / Malware

LABEL	DESCRIPTION
Antivirus / Malware Scanned (File Amount)	This chart displays the total number of connections detected by the Zyxel Device. Move your cursor over a trend line to display the number of connections encountered over time.
Antivirus/Malware Trend (Hits)	This chart displays patterns in threats by the number of virus or malware attacks detected by the Zyxel Device. Move your cursor over a trend line to display the number of threats encountered over time.
Top Source Hostname	This chart displays the three most common source hostnames of virus or malware attacks detected by the Zyxel Device. Scroll down to **DNS Filter Hit Detail** and click the **by Hostname** tab to display details about the source hostnames.
Top Source MAC Address	This chart displays the three most common source MAC addresses of virus or malware attacks detected by the Zyxel Device. Scroll down to **DNS Filter Hit Detail** and click the **by MAC Address** tab to display details about the source MAC addresses.
Top Virus / Malware	This chart displays the three most common malware and viruses detected by the Zyxel Device. Scroll down to **Antivirus / Malware Hit Detail** and click the **by Virus / Malware** tab to display details about the malware and viruses that were detected.
Top Source IP	This chart displays the source IP addresses of the three most common malware and viruses detected by the Zyxel Device. Scroll down to **Antivirus / Malware Hit Detail** and click the **by Source IP** tab to display details about the source IP addresses of the incoming malicious and/or suspicious files.
Top Destination IP	This chart displays the destination IP addresses of the three most common malware and viruses detected by the Zyxel Device. Scroll down to **Antivirus / Malware Hit Detail** and click the **by Destination IP** tab to display details about the destination IP addresses of the incoming malicious and/or suspicious files.
Antivirus / Malware Hit Detail	This displays the number of antivirus and malware detected by the Zyxel Device, categorized by hostname, MAC address, virus and malware, source IP address, or destination IP address.

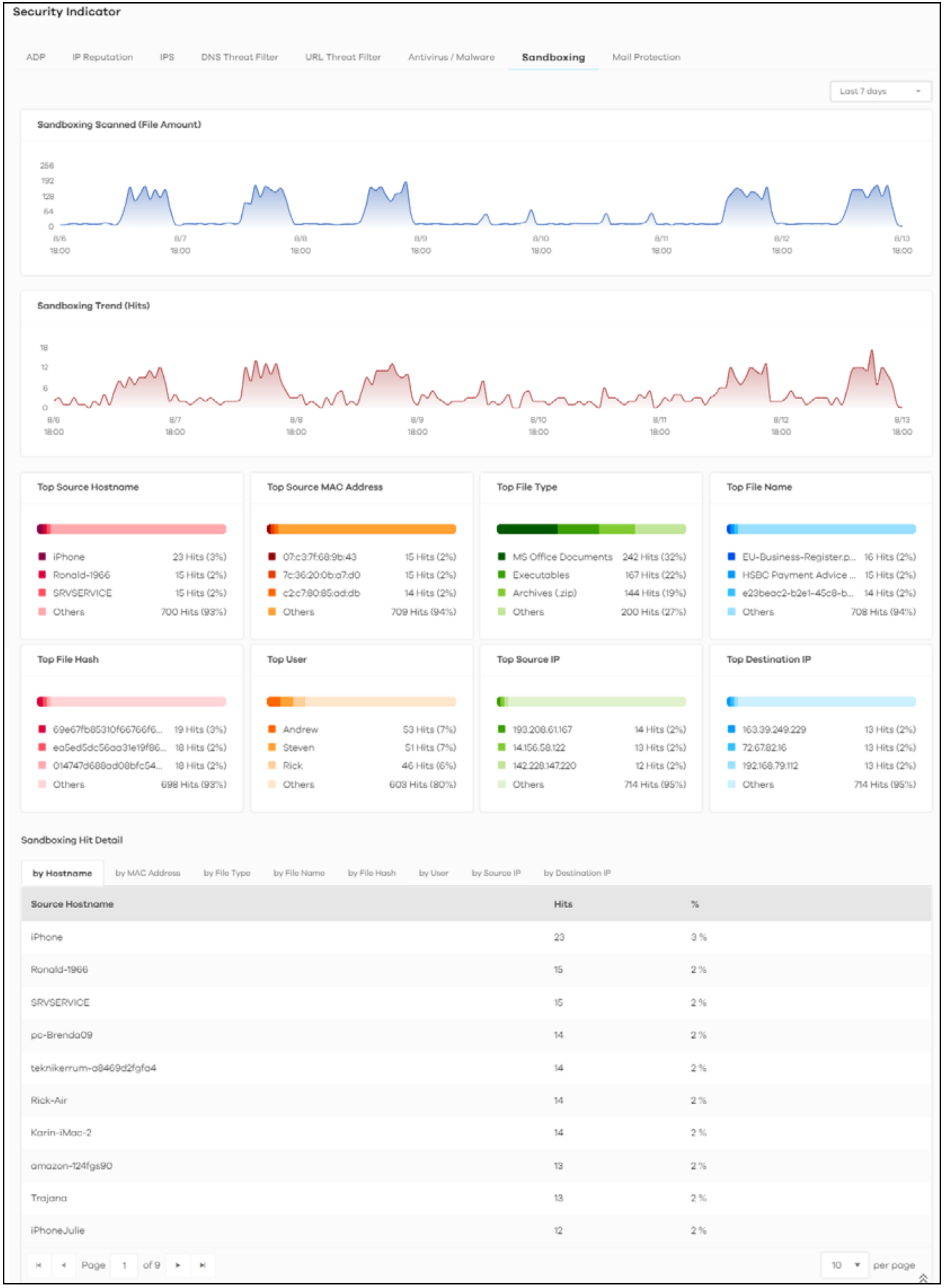
2.3.7 Sandboxing

This screen displays sandboxing statistics. See Section 2.1.2 on page 18 for more information about sandboxing.

Sandboxing statistics will automatically be removed from the list after one month.

The following figure shows the **Analysis** > **Security Indicator** > **Sandboxing** data visualizations.

Figure 19 Analysis > Security Indicator > Sandboxing



Top Source Hostname

iPhone	23 Hits (3%)
Ronald-1966	15 Hits (2%)
SRVSERVICE	15 Hits (2%)
Others	700 Hits (93%)

Top Source MAC Address

07:c3:7f:68:9b:43	15 Hits (2%)
7c:36:20:0b:a7:d0	15 Hits (2%)
c2:c7:80:85:ad:db	14 Hits (2%)
Others	709 Hits (94%)

Top File Type

MS Office Documents	242 Hits (32%)
Executables	167 Hits (22%)
Archives (.zip)	144 Hits (19%)
Others	200 Hits (27%)

Top File Name

EU-Business-Register.p...	16 Hits (2%)
HSBC Payment Advice ...	15 Hits (2%)
e23beac2-b2e1-45c8-b...	14 Hits (2%)
Others	708 Hits (94%)

Top File Hash

69e67fb85310f66766f6...	19 Hits (3%)
ea5ed5dc56aa31e19f86...	18 Hits (2%)
014747d688ad08bfc54...	18 Hits (2%)
Others	698 Hits (93%)

Top User

Andrew	53 Hits (7%)
Steven	51 Hits (7%)
Rick	46 Hits (6%)
Others	603 Hits (80%)

Top Source IP

193.208.61.167	14 Hits (2%)
14.156.58.122	13 Hits (2%)
142.228.147.220	12 Hits (2%)
Others	714 Hits (95%)

Top Destination IP

163.39.249.229	13 Hits (2%)
72.67.82.16	13 Hits (2%)
192.168.79.112	13 Hits (2%)
Others	714 Hits (95%)

Sandboxing Hit Detail

Source Hostname	Hits	%
iPhone	23	3 %
Ronald-1966	15	2 %
SRVSERVICE	15	2 %
pc-Brenda09	14	2 %
teknikerrum-a8469d2fgfa4	14	2 %
Rick-Air	14	2 %
Karin-iMac-2	14	2 %
amazon-124fgs90	13	2 %
Trajana	13	2 %
iPhoneJulie	12	2 %

The following table describes the labels on the **Analysis** > **Security Indicator** > **Sandboxing** screen.

Table 16 Analysis > Security Indicator > Sandboxing

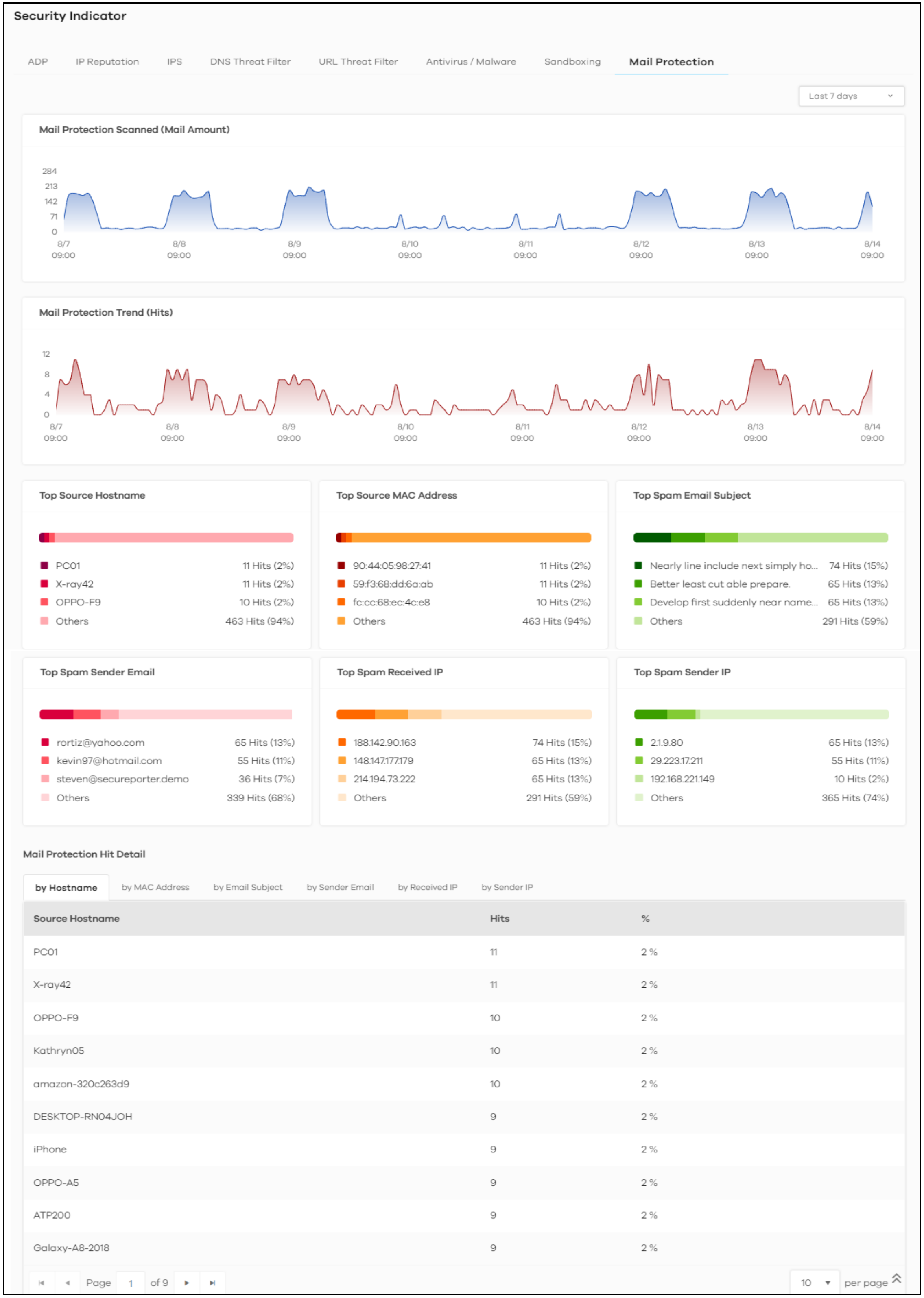
LABEL	DESCRIPTION
Sandboxing Scanned (File Amount)	This chart displays the total number of connections detected by the Zyxel Device. Move your cursor over a trend line to display the number of connections encountered over time.
Sandboxing Trend (Hits)	This chart displays the number of malicious and/or suspicious files that were scanned. Move your cursor over a trend line to display the number of malicious and/or suspicious files encountered over time.
Top File Type	This chart displays the three most common types of malicious and/or suspicious files. Scroll down to **Sandboxing Hit Detail** and click the **by File Type** tab to display details about the malicious and/or suspicious file types.
Top File Name	This chart displays the file names of the three most common incoming malicious and/or suspicious files. Scroll down to **Sandboxing Hit Detail** and click the **by File Name** tab to display details about the file names of the incoming malicious and/or suspicious files.
Top File Hash	This chart displays the hash values of the three most common incoming malicious and/or suspicious files. Scroll down to **Sandboxing Hit Detail** and click the **by File Hash** tab to display details about the hash values of the incoming malicious and/or suspicious files.
Top User	This chart displays the three users who receive malicious and/or suspicious files the most. Scroll down to **Sandboxing Hit Detail** and click the **by User** tab to display details about the users that are at risk of malicious and/or suspicious files.
Top Source IP	This chart displays the source IP addresses of the three most common incoming malicious and/or suspicious files. Scroll down to **Sandboxing Hit Detail** and click the **by Source IP** tab to display details about the source IP addresses of incoming malicious and/or suspicious files.
Top Destination IP	This chart displays the three destination IP addresses that receive the most incoming malicious and/or suspicious files. Scroll down to **Sandboxing Hit Detail** and click the **by Destination IP** tab to display details about the destination IP addresses of incoming malicious and/or suspicious files.
Sandboxing Hit Detail	This displays the number of malicious and/or suspicious files detected by the Zyxel Device, categorized by hostname, MAC address, file type, file name, file hash, user, source IP address, or destination IP address.

2.3.8 Mail Protection

Mail protection mark or discard spam (unsolicited commercial or junk email). This screen shows you the information of spam mails detected by Zyxel Device.

The following figure shows the **Analysis** > **Security Indicator** > **Mail Protection** data visualizations.

Figure 20 Analysis > Security Indicator > Mail Protection



Top Source Hostname

PC01	11 Hits (2%)
X-ray42	11 Hits (2%)
OPPO-F9	10 Hits (2%)
Others	463 Hits (94%)

Top Source MAC Address

90:44:05:98:27:41	11 Hits (2%)
59:f3:68:dd:6a:ab	11 Hits (2%)
fc:cc:68:ec:4c:e8	10 Hits (2%)
Others	463 Hits (94%)

Top Spam Email Subject

Nearly line include next simply ho...	74 Hits (15%)
Better least cut able prepare.	65 Hits (13%)
Develop first suddenly near name...	65 Hits (13%)
Others	291 Hits (59%)

Top Spam Sender Email

rortiz@yahoo.com	65 Hits (13%)
kevin97@hotmail.com	55 Hits (11%)
steven@secureporter.demo	36 Hits (7%)
Others	339 Hits (68%)

Top Spam Received IP

188.142.90.163	74 Hits (15%)
148.147.177.179	65 Hits (13%)
214.194.73.222	65 Hits (13%)
Others	291 Hits (59%)

Top Spam Sender IP

2.1.9.80	65 Hits (13%)
29.223.17.211	55 Hits (11%)
192.168.221.149	10 Hits (2%)
Others	365 Hits (74%)

Mail Protection Hit Detail

Source Hostname	Hits	%
PC01	11	2 %
X-ray42	11	2 %
OPPO-F9	10	2 %
Kathryn05	10	2 %
amazon-320c263d9	10	2 %
DESKTOP-RN04JOH	9	2 %
iPhone	9	2 %
OPPO-A5	9	2 %
ATP200	9	2 %
Galaxy-A8-2018	9	2 %

The following table describes the labels on the **Analysis** > **Security Indicator** > **Mail Protection** screen.

Table 17 Analysis > Security Indicator > Mail Protection

LABEL	DESCRIPTION
Mail Protection Scanned (Mail Amount)	This chart displays the total number of mails detected by the Zyxel Device. Move your cursor over a trend line to display the number of mails sent and received over time.
Mail Protection Trend (Hits)	This chart displays the number of spam mails detected by the Zyxel Device. Move your cursor over a trend line to display the number of threats encountered over time.
Top Source Hostname	This chart displays the three most common spam email sender hostnames detected by the Zyxel Device. Scroll down to **Email Spam Hit Detail** and click the **by Hostname** tab to display details about the spam email sender hostnames that were detected.
Top Source MAC Address	This chart displays the three most common spam email sender MAC addresses detected by the Zyxel Device. Scroll down to **Email Spam Hit Detail** and click the **by MAC Address** tab to display details about the spam email sender MAC addresses that were detected.
Top Spam Email Subject	This chart displays the three most common spam email subjects detected by the Zyxel Device. Scroll down to **Email Spam Hit Detail** and click the **by Email Subject** tab to display details about the spam email subjects that were detected.
Top Spam Sender Email	This chart displays the three most common spam email senders detected by the Zyxel Device. Scroll down to **Email Spam Hit Detail** and click the **by Sender Email** tab to display details about the spam email senders that were detected.
Top Spam Received IP	This chart displays the three most common traffic classified as spam received by the internal users of the Zyxel Device. Scroll down to **Email Spam Hit Detail** and click the **by Received IP** tab to display details about the spam email recipients that were detected.
Top Spam Sender IP	This chart displays the three most common traffic classified as spam sent from the internal users of the Zyxel Device. Scroll down to **Email Spam Hit Detail** and click the **by Sender IP** tab to display details about the spam traffic source that were detected.
Mail Protection Hit Detail	This displays the information of spam mails detected by the Zyxel Device, categorized by hostname, MAC address, email subject, sender email, sender IP address, or received IP address.

2.4 Network Activity

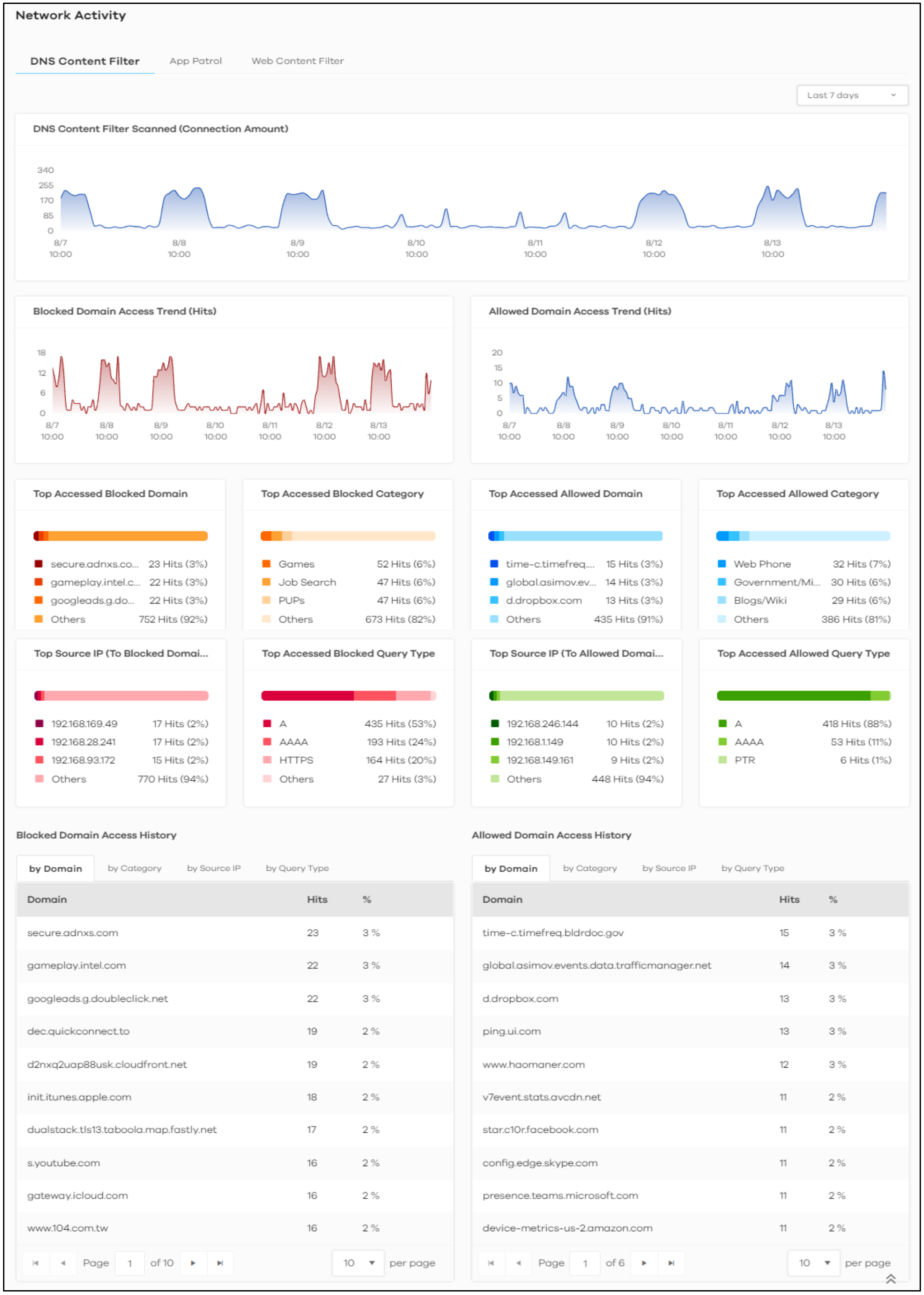
Network Activity data visualizations are categorized as:

- DNS Content Filter
- App Patrol
- Web Content Filter

2.4.1 DNS Content Filter

DNS (Domain Name System) content filter blocks or allow access to websites based on domain names. The following figure shows the **Analysis** > **Network Activity** > **DNS Content Filter** data visualizations.

Figure 21 Analysis > Network Activity > DNS Content Filter



DNS Content Filter Scanned (Connection Amount)

Blocked Domain Access Trend (Hits)

Allowed Domain Access Trend (Hits)

Top Accessed Blocked Domain

secure.adnxs.co...	23 Hits (3%)
gameplay.intel.c...	22 Hits (3%)
googleads.g.do...	22 Hits (3%)
Others	752 Hits (92%)

Top Accessed Blocked Category

Games	52 Hits (6%)
Job Search	47 Hits (6%)
PUPs	47 Hits (6%)
Others	673 Hits (82%)

Top Accessed Allowed Domain

time-c.timefreq....	15 Hits (3%)
global.asimov.ev...	14 Hits (3%)
d.dropbox.com	13 Hits (3%)
Others	435 Hits (91%)

Top Accessed Allowed Category

Web Phone	32 Hits (7%)
Government/Mi...	30 Hits (6%)
Blogs/Wiki	29 Hits (6%)
Others	386 Hits (81%)

Top Source IP (To Blocked Domai...

192.168.169.49	17 Hits (2%)
192.168.28.241	17 Hits (2%)
192.168.93.172	15 Hits (2%)
Others	770 Hits (94%)

Top Accessed Blocked Query Type

A	435 Hits (53%)
AAAA	193 Hits (24%)
HTTPS	164 Hits (20%)
Others	27 Hits (3%)

Top Source IP (To Allowed Domai...

192.168.246.144	10 Hits (2%)
192.168.1.149	10 Hits (2%)
192.168.149.161	9 Hits (2%)
Others	448 Hits (94%)

Top Accessed Allowed Query Type

A	418 Hits (88%)
AAAA	53 Hits (11%)
PTR	6 Hits (1%)

Blocked Domain Access History

by Domain | by Category | by Source IP | by Query Type

Domain	Hits	%
secure.adnxs.com	23	3 %
gameplay.intel.com	22	3 %
googleads.g.doubleclick.net	22	3 %
dec.quickconnect.to	19	2 %
d2nxq2uap88usk.cloudfront.net	19	2 %
init.itunes.apple.com	18	2 %
dualstack.tls13.taboola.map.fastly.net	17	2 %
s.youtube.com	16	2 %
gateway.icloud.com	16	2 %
www.104.com.tw	16	2 %

Page 1 of 10 · 10 per page

Allowed Domain Access History

by Domain | by Category | by Source IP | by Query Type

Domain	Hits	%
time-c.timefreq.bldrdoc.gov	15	3 %
global.asimov.events.data.trafficmanager.net	14	3 %
d.dropbox.com	13	3 %
ping.ui.com	13	3 %
www.haomaner.com	12	3 %
v7event.stats.avcdn.net	11	2 %
star.c10r.facebook.com	11	2 %
config.edge.skype.com	11	2 %
presence.teams.microsoft.com	11	2 %
device-metrics-us-2.amazon.com	11	2 %

Page 1 of 6 · 10 per page

The following table describes the labels on the **Analysis** > **Network Activity** > **DNS Content Filter** screen.

Table 18 Analysis > Network Activity > DNS Content Filter

LABEL	DESCRIPTION
DNS Content Filter Scanned (Connection Amount)	This chart displays the total number of connections detected by the Zyxel Device. Move your cursor over a trend line to display the number of connections encountered over time.
Blocked Domain Access Trend (Hits)	This chart displays the number of accesses to blocked domains that were scanned. Move your cursor over a trend line to display the number of accesses to blocked domains encountered over time.
Allowed Domain Access Trend (Hits)	This chart displays the number of accesses to allowed domains that were scanned. Move your cursor over a trend line to display the number of accesses to allowed domains encountered over time.
Top Accessed Blocked Domain	This chart displays the three most commonly accessed blocked domains. Scroll down to **Blocked Domain Access History** and click the **by Domain** tab to display details about the accesses to blocked domains that were scanned.
Top Accessed Blocked Category	This chart displays the three most common categories of blocked domains accessed. Scroll down to **Blocked Domain Access History** and click the **by Category** tab to display details about the accesses to blocked domains that were scanned.
Top Accessed Allowed Domain	This chart displays the three most commonly accessed allowed domains. Scroll down to **Allowed Domain Access History** and click the **by Domain** tab to display details about the accesses to allowed domains that were scanned.
Top Accessed Allowed Category	This chart displays the three most common categories of allowed domains accessed. Scroll down to **Allowed Domain Access History** and click the **by Category** tab to display details about the accesses to allowed domains that were scanned.
Top Source IP (To Blocked Domain)	This chart displays the source IP addresses of the three most commonly accessed blocked domains. Scroll down to **Blocked Domain Access History** and click the **by Source IP** tab to display details about the source IP addresses of the blocked domains.
Top Accessed Blocked Query Type	This chart displays the three most common DNS record types for accessed domains that were blocked. Scroll down to **Blocked Domain Access History** and click the **by Query Type** tab to display details about the DNS record types of the blocked domains.
Top Source IP (To Allowed Domain)	This chart displays the source IP addresses of the three most commonly accessed allowed domains. Scroll down to **Allowed Domain Access History** and click the **by Source IP** tab to display details about the source IP addresses of the allowed domains.
Top Accessed Allowed Query Type	This chart displays the three most common DNS record types for accessed domains that were allowed. Scroll down to **Allowed Domain Access History** and click the **by Query Type** tab to display details about the DNS record types of the allowed domains.
Blocked Domain Access History	This displays the domains that are blocked by the Zyxel Device, categorized by domain name, category, source IP address, and DNS record types.
Allowed Domain Access History	This displays the domains that are allowed by the Zyxel Device, categorized by domain name, category, source IP address, and DNS record types.

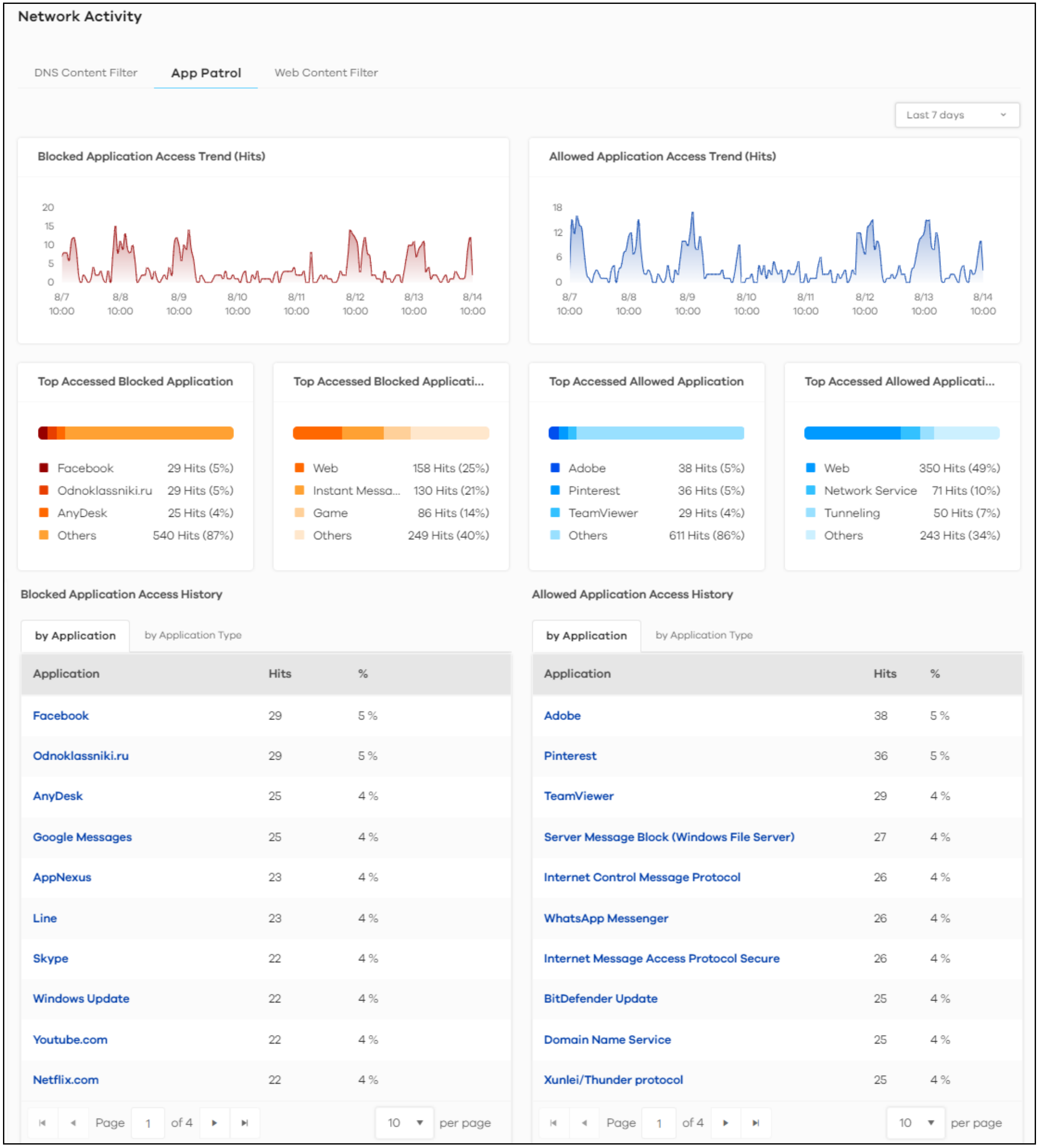
2.4.2 App Patrol

Application Patrol provides a convenient way to manage the use of various applications on the network. It manages general protocols (for example, HTTP and FTP) and instant messenger (IM), peer-to-peer (P2P), Voice over IP (VoIP), and streaming (RSTP) applications. You can even control the use of a particular application's individual features (like text messaging, voice, video conferencing, and file transfers).

Application Patrol examines every TCP and UDP connection passing through the Zyxel Device and identifies what application is using the connection. Then, you can specify whether or not the Zyxel Device continues to route the connection. Traffic not recognized by the application patrol signatures is ignored.

The following figure shows the **Analysis** > **Network Acitivity** > **App Patrol** data visualizations.

Figure 22 Analysis > Network Acitivity > App Patrol



Network Activity

DNS Content Filter

App Patrol

Web Content Filter

Last 7 days

Blocked Application Access Trend (Hits)

Allowed Application Access Trend (Hits)

Top Accessed Blocked Application

■ Facebook	29 Hits (5%)
■ Odnoklassniki.ru	29 Hits (5%)
■ AnyDesk	25 Hits (4%)
■ Others	540 Hits (87%)

Top Accessed Blocked Applicati...

■ Web	158 Hits (25%)
■ Instant Messa...	130 Hits (21%)
■ Game	86 Hits (14%)
■ Others	249 Hits (40%)

Top Accessed Allowed Application

■ Adobe	38 Hits (5%)
■ Pinterest	36 Hits (5%)
■ TeamViewer	29 Hits (4%)
■ Others	611 Hits (86%)

Top Accessed Allowed Applicati...

■ Web	350 Hits (49%)
■ Network Service	71 Hits (10%)
■ Tunneling	50 Hits (7%)
■ Others	243 Hits (34%)

Blocked Application Access History

by Application | by Application Type

Application	Hits	%
Facebook	29	5 %
Odnoklassniki.ru	29	5 %
AnyDesk	25	4 %
Google Messages	25	4 %
AppNexus	23	4 %
Line	23	4 %
Skype	22	4 %
Windows Update	22	4 %
Youtube.com	22	4 %
Netflix.com	22	4 %

Page 1 of 4 | 10 per page

Allowed Application Access History

by Application | by Application Type

Application	Hits	%
Adobe	38	5 %
Pinterest	36	5 %
TeamViewer	29	4 %
Server Message Block (Windows File Server)	27	4 %
Internet Control Message Protocol	26	4 %
WhatsApp Messenger	26	4 %
Internet Message Access Protocol Secure	26	4 %
BitDefender Update	25	4 %
Domain Name Service	25	4 %
Xunlei/Thunder protocol	25	4 %

Page 1 of 4 | 10 per page

The following table describes the labels on the **Analysis** > **Network Acitivity** > **App Patrol** screen.

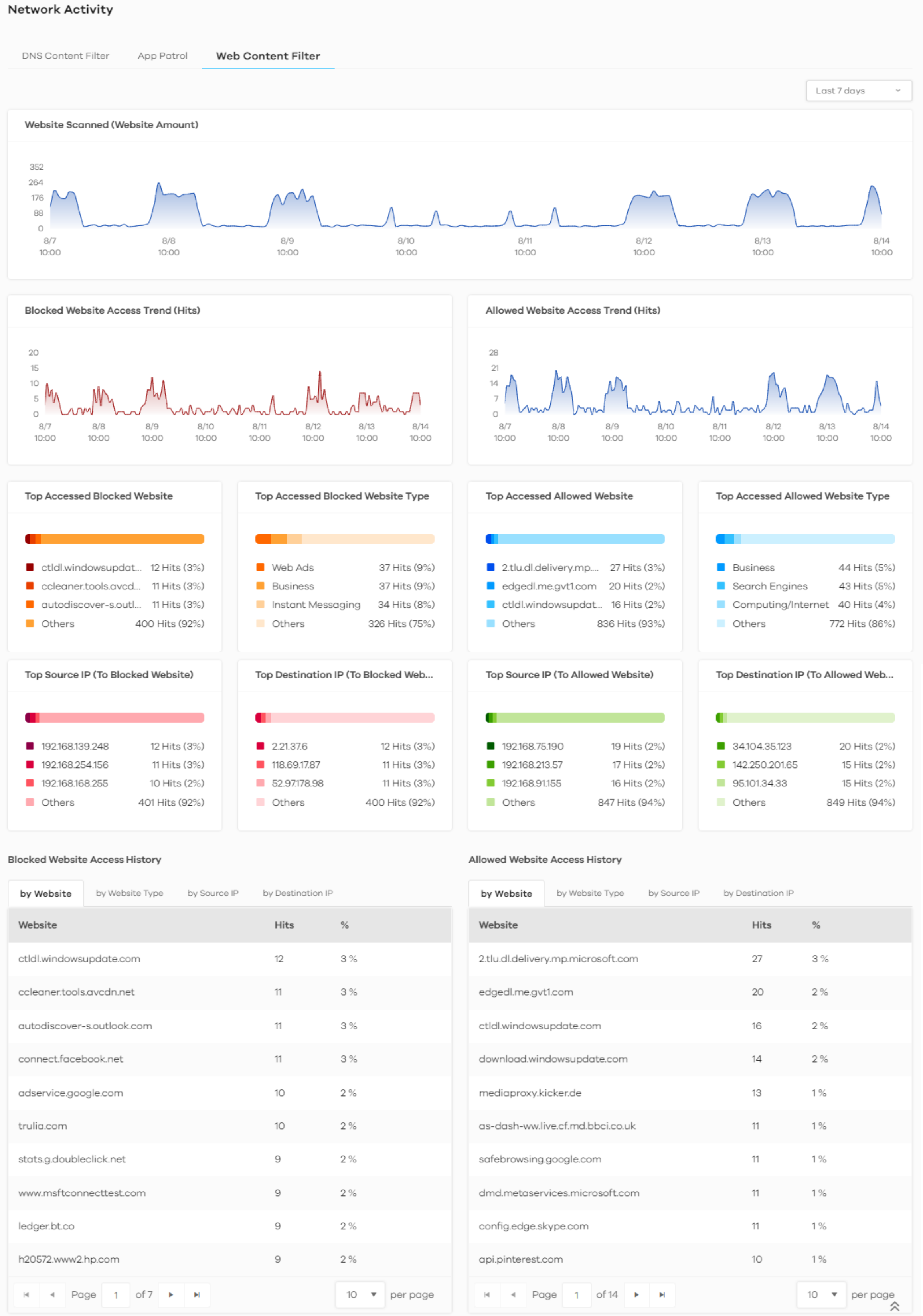
Table 19 Analysis > Network Acitivity > App Patrol

LABEL	DESCRIPTION
Blocked Application Access Trend (Hits)	This chart displays the most commonly used applications accessed through the Zyxel Device as detected and blocked by Application Patrol. Move your cursor over a trend line to display the number of threats encountered over time.
Allowed Application Access Trend (Hits)	This chart displays the number of most frequently visited applications through the Zyxel Device as detected by Application Patrol. Application Patrol manages general protocols (for example, HTTP and FTP, instant messenger (IM), peer-to-peer (P2P), Voice over IP (VoIP), streaming (RSTP) applications and even an application's individual features (like text messaging, voice, video conferencing, and file transfers). Move your cursor over a trend line to display the number of threats encountered over time.
Top Accessed Blocked Application	This chart displays the three applications that were blocked the most frequently by the Zyxel Device. Scroll down to **Blocked Application Access History** and click the **Application Name** tab to display details about the specific applications that were blocked.
Top Accessed Blocked Application Type	This chart displays the three types of application that were blocked the most frequently by the Zyxel Device. Scroll down to **Blocked Application Access History** and click the **Application Type** tab to display details about the specific application types that were blocked.
Top Access Allowed Application	This chart displays the three applications that were accessed the most frequently by the Zyxel Device. Scroll down to **Allowed Application Access History** and click the **Application Name** tab to display details about the specific applications that were accessed.
Top Access Allowed Application Type	This chart displays the three applications that were accessed the most frequently by the Zyxel Device. Scroll down to **Allowed Application Access History** and click the **Application Type** tab to display details about the specific application types that were accessed.
Blocked Application Access History	This displays the applications that are blocked by the Zyxel Device, categorized by application and application type.
Allowed Application Access History	This displays the applications that are allowed by the Zyxel Device, categorized by application and application type.

2.4.3 Web Content Filter

Web content filter restrict access to specific websites based on the policy you set on the Zyxel Device. The following figure shows the **Analysis** > **Network Acitivity** > **Web Content Filter** data visualizations.

Figure 23 Analysis > Network Acitivity > Web Content Filterl



Top Accessed Blocked Website

■ ctldl.windowsupdat...	12 Hits (3%)
■ ccleaner.tools.avcd...	11 Hits (3%)
■ autodiscover-s.outl...	11 Hits (3%)
■ Others	400 Hits (92%)

Top Accessed Blocked Website Type

■ Web Ads	37 Hits (9%)
■ Business	37 Hits (9%)
■ Instant Messaging	34 Hits (8%)
■ Others	326 Hits (75%)

Top Accessed Allowed Website

■ 2.tlu.dl.delivery.mp...	27 Hits (3%)
■ edgedl.me.gvt1.com	20 Hits (2%)
■ ctldl.windowsupdat...	16 Hits (2%)
■ Others	836 Hits (93%)

Top Accessed Allowed Website Type

■ Business	44 Hits (5%)
■ Search Engines	43 Hits (5%)
■ Computing/Internet	40 Hits (4%)
■ Others	772 Hits (86%)

Top Source IP (To Blocked Website)

■ 192.168.139.248	12 Hits (3%)
■ 192.168.254.156	11 Hits (3%)
■ 192.168.168.255	10 Hits (2%)
■ Others	401 Hits (92%)

Top Destination IP (To Blocked Web...

■ 2.21.37.6	12 Hits (3%)
■ 118.69.17.87	11 Hits (3%)
■ 52.97.178.98	11 Hits (3%)
■ Others	400 Hits (92%)

Top Source IP (To Allowed Website)

■ 192.168.75.190	19 Hits (2%)
■ 192.168.213.57	17 Hits (2%)
■ 192.168.91.155	16 Hits (2%)
■ Others	847 Hits (94%)

Top Destination IP (To Allowed Web...

■ 34.104.35.123	20 Hits (2%)
■ 142.250.201.65	15 Hits (2%)
■ 95.101.34.33	15 Hits (2%)
■ Others	849 Hits (94%)

Blocked Website Access History

by Website | by Website Type | by Source IP | by Destination IP

Website	Hits	%
ctldl.windowsupdate.com	12	3 %
ccleaner.tools.avcdn.net	11	3 %
autodiscover-s.outlook.com	11	3 %
connect.facebook.net	11	3 %
adservice.google.com	10	2 %
trulia.com	10	2 %
stats.g.doubleclick.net	9	2 %
www.msftconnecttest.com	9	2 %
ledger.bt.co	9	2 %
h20572.www2.hp.com	9	2 %

Page 1 of 7 ▸ ▸| 10 ▾ per page

Allowed Website Access History

by Website | by Website Type | by Source IP | by Destination IP

Website	Hits	%
2.tlu.dl.delivery.mp.microsoft.com	27	3 %
edgedl.me.gvt1.com	20	2 %
ctldl.windowsupdate.com	16	2 %
download.windowsupdate.com	14	2 %
mediaproxy.kicker.de	13	1 %
as-dash-ww.live.cf.md.bbci.co.uk	11	1 %
safebrowsing.google.com	11	1 %
dmd.metaservices.microsoft.com	11	1 %
config.edge.skype.com	11	1 %
api.pinterest.com	10	1 %

Page 1 of 14 ▸ ▸| 10 ▾ per page

The following table describes the labels on the **Analysis** > **Network Acitivity** > **Web Content Filter** screen.

Table 20 Analysis > Network Acitivity > Web Content Filter

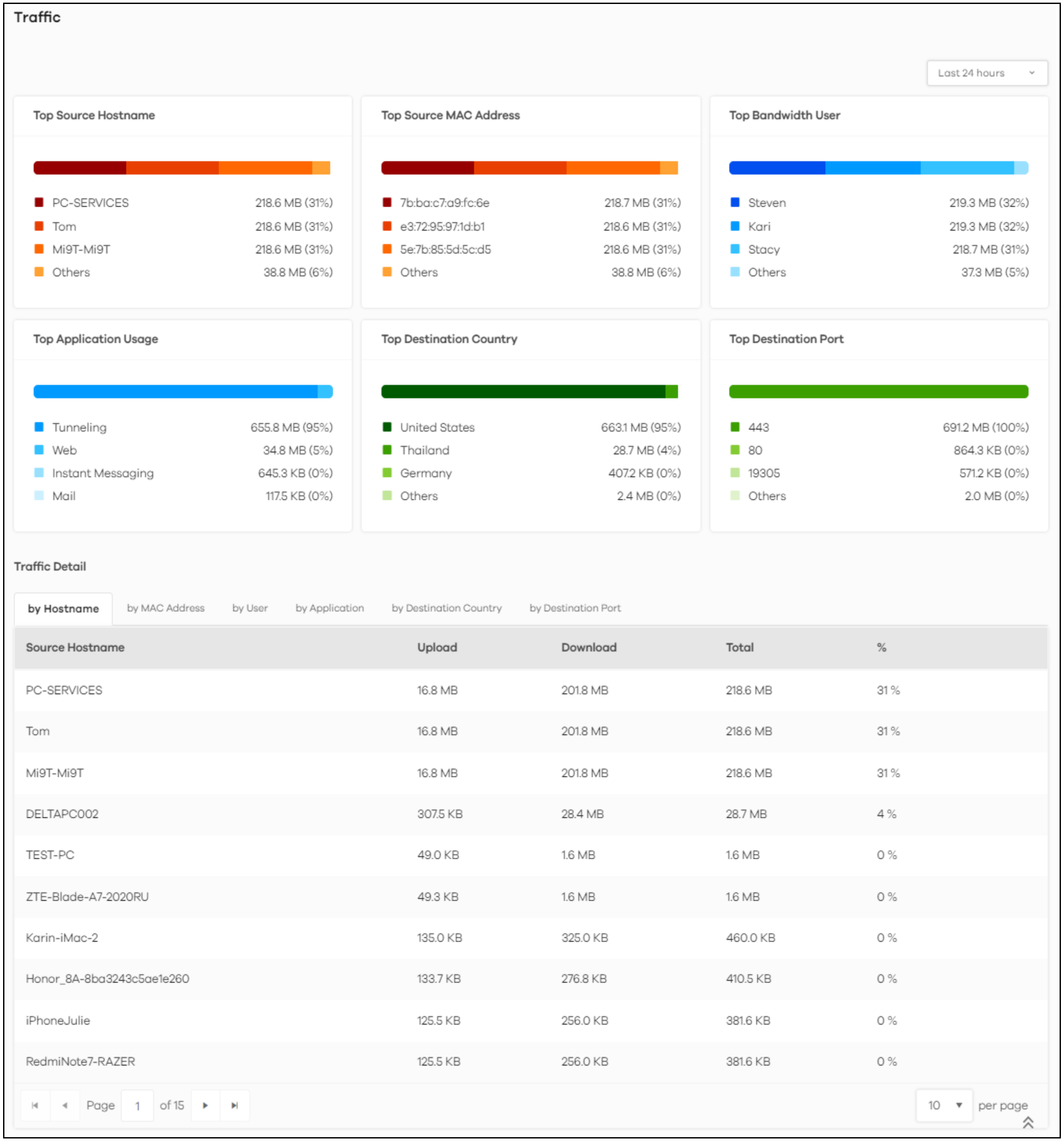
LABEL	DESCRIPTION
Website Scanned (Website Amount)	This chart displays the total number of websites detected by the Zyxel Device. Move your cursor over a trend line to display the number of websites encountered over time.
Blocked Website Access Trend (Hits)	This chart displays the number of accesses to blocked websites that were scanned. Move your cursor over a trend line to display the number of accesses to blocked websites encountered over time.
Allowed Website Access Trend (Hits)	This chart displays the number of accesses to allowed websites that were scanned. Move your cursor over a trend line to display the number of accesses to allowed websites encountered over time.
Top Accessed Blocked Website	This chart displays the three most commonly accessed blocked websites. Scroll down to **Blocked Website Access History** and click the **by Website** tab to display details about the accesses to blocked websites that were scanned.
Top Accessed Blocked Website Type	This chart displays the three most common types of blocked websites accessed. Scroll down to **Blocked Website Access History** and click the **by Website Type** tab to display details about the types of blocked websites that were scanned.
Top Accessed Allowed Website	This chart displays the three most commonly accessed allowed websites. Scroll down to **Allowed Website Access History** and click the **by Website** tab to display details about the accesses to blocked websites that were scanned.
Top Accessed Allowed Website Type	This chart displays the three most common types of allowed websites accessed. Scroll down to **Allowed Website Access History** and click the **by Website Type** tab to display details about the types of allowed websites that were scanned.
Top Source IP (To Blocked Website)	This chart displays the source IP addresses of the three most commonly accessed blocked websites. Scroll down to **Allowed Website Access History** and click the **by Source IP** tab to display details about the source IP addresses of the blocked websites.
Top Destination IP (To Blocked Website)	This chart displays the destination IP addresses of the three most commonly accessed blocked websites. Scroll down to **Blocked Website Access History** and click the **by Destination IP** tab to display details about the destination IP addresses of the blocked websites.
Top Source IP (To Allowed Website)	This chart displays the source IP addresses of the three most commonly accessed allowed websites. Scroll down to **Allowed Website Access History** and click the **by Source IP** tab to display details about the source IP addresses of the allowed websites.
Top Destination IP (To Allowed Website)	This chart displays the destination IP addresses of the three most commonly accessed allowed websites. Scroll down to **Allowed Website Access History** and click the **by Destination IP** tab to display details about the destination IP addresses of the allowed websites.
Blocked Website Access History	This displays the blocked websites accessed the most frequently as detected by the Zyxel Device, categorized by website, website type, source IP address, and destination IP address.
Allowed Website Access History	This displays the allowed websites accessed the most frequently as detected by the Zyxel Device, categorized by website, website type, source IP address, and destination IP address.

2.5 Traffic

Use this screen to view the details about the bandwidth usage on the network. The following figure shows the **Analysis** > **Traffic** data visualizations.

Note: At the time of writing, the ZyWALL ATP series, ZyWALL USG FLEX series, ZyWALL USG FLEX 50(AX) series, and ZyWALL VPN series devices in cloud mode do not support the **Traffic** screen. Please go to the Nebula portal to view the traffic log.

Figure 24 Analysis > Network Acitivity > Traffic



Traffic

Top Source Hostname

■ PC-SERVICES	218.6 MB (31%)
■ Tom	218.6 MB (31%)
■ Mi9T-Mi9T	218.6 MB (31%)
■ Others	38.8 MB (6%)

Top Source MAC Address

■ 7b:ba:c7:a9:fc:6e	218.7 MB (31%)
■ e3:72:95:97:1d:b1	218.6 MB (31%)
■ 5e:7b:85:5d:5c:d5	218.6 MB (31%)
■ Others	38.8 MB (6%)

Top Bandwidth User

■ Steven	219.3 MB (32%)
■ Kari	219.3 MB (32%)
■ Stacy	218.7 MB (31%)
■ Others	37.3 MB (5%)

Top Application Usage

■ Tunneling	655.8 MB (95%)
■ Web	34.8 MB (5%)
■ Instant Messaging	645.3 KB (0%)
■ Mail	117.5 KB (0%)

Top Destination Country

■ United States	663.1 MB (95%)
■ Thailand	28.7 MB (4%)
■ Germany	407.2 KB (0%)
■ Others	2.4 MB (0%)

Top Destination Port

■ 443	691.2 MB (100%)
■ 80	864.3 KB (0%)
■ 19305	571.2 KB (0%)
■ Others	2.0 MB (0%)

Traffic Detail

Source Hostname	Upload	Download	Total	%
PC-SERVICES	16.8 MB	201.8 MB	218.6 MB	31 %
Tom	16.8 MB	201.8 MB	218.6 MB	31 %
Mi9T-Mi9T	16.8 MB	201.8 MB	218.6 MB	31 %
DELTAPC002	307.5 KB	28.4 MB	28.7 MB	4 %
TEST-PC	49.0 KB	1.6 MB	1.6 MB	0 %
ZTE-Blade-A7-2020RU	49.3 KB	1.6 MB	1.6 MB	0 %
Karin-iMac-2	135.0 KB	325.0 KB	460.0 KB	0 %
Honor_8A-8ba3243c5ae1e260	133.7 KB	276.8 KB	410.5 KB	0 %
iPhoneJulie	125.5 KB	256.0 KB	381.6 KB	0 %
RedmiNote7-RAZER	125.5 KB	256.0 KB	381.6 KB	0 %

The following table describes the labels on the **Analysis** > **Network Acitivity** > **Traffic** screen.

Table 21 Analysis > Network Acitivity > Traffic

LABEL	DESCRIPTION
Top Source Hostname	This chart displays the three hostnames with the greatest bandwidth usage on the network. Scroll down to **Traffic Detail** and click the **by Hostname** tab to display details about the hostnames that send the most traffic.
Top Source MAC Address	This chart displays the three MAC addresses with the greatest bandwidth usage on the network. Scroll down to **Traffic Detail** and click the **by MAC Address** tab to display details about the MAC addresses that send the most traffic.
Top Bandwidth User	This displays the top three users of bandwidth on the network. Scroll down to **Traffic Detail** and click the **by User** tab to display details about the users that use the most bandwidth on the network.
Top Application Usage	This displays the network applications with the greatest bandwidth usage on the network. Scroll down to **Traffic Detail** and click the **by Application** tab to display details about the applications that use the most bandwidth on the network.
Top Destination Country	This displays the top three countries that received the most data traffic from the Zyxel Device. Scroll down to **Traffic Detail** and click the **by Destination Country** tab to display details about the countries that received the most bandwidth on the network.
Top Destination Port	This displays the top three destination ports by bandwidth usage over a This displays the network applications with the greatest bandwidth usage. Scroll down to **Traffic Detail** and click the **by Destination Port** tab to display details about the ports that received the most bandwidth on the network.
Traffic Detail	This displays the information of the traffic passing through the Zyxel Device, categorized by hostname, MAC address, user, application, destination country, and destination port.

2.6 Device

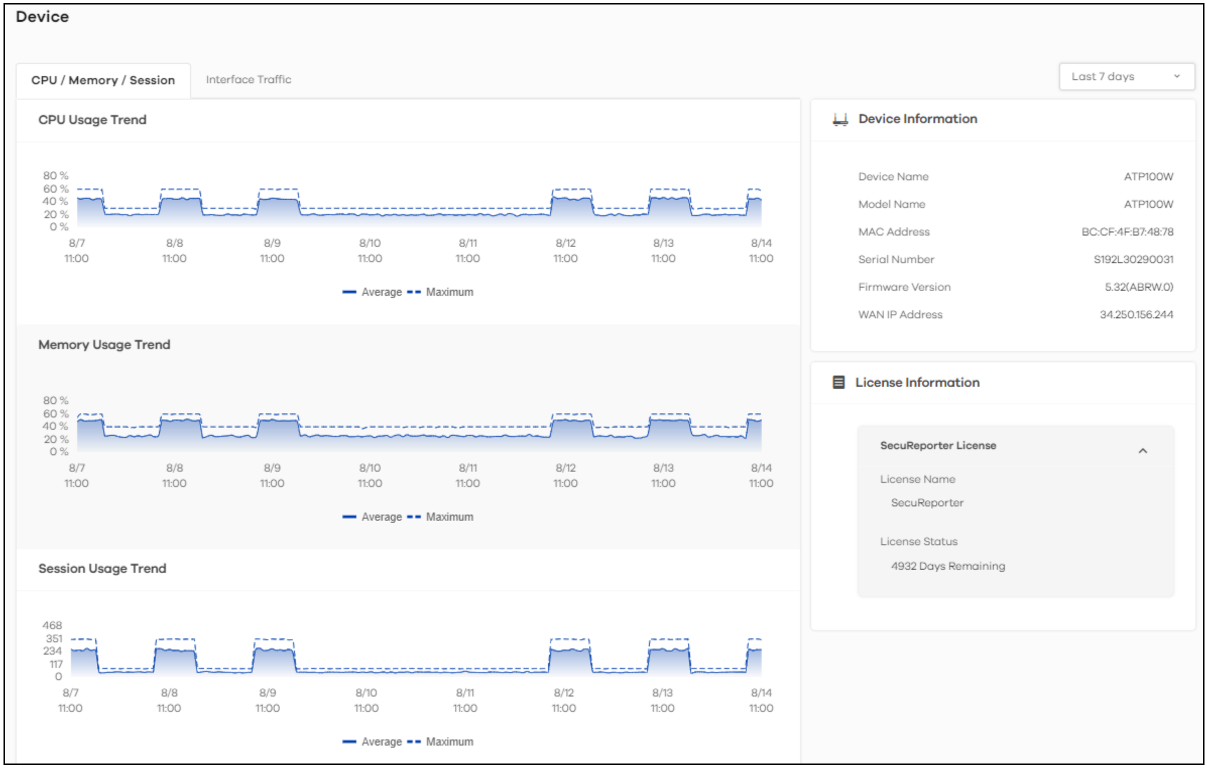
Device data visualizations are categorized as:

- CPU/Memory/Session
- Interface Traffic

2.6.1 CPU/Memory/Session

The following figure shows the **Analysis** > **Device** > **CPU / Memory / Session** data visualizations.

Figure 25 Analysis > Device > CPU / Memory / Session



Device Information

Device Name ATP100W
Model Name ATP100W
MAC Address BC:CF:4F:B7:48:78
Serial Number S192L30290031
Firmware Version 5.32(ABRW.0)
WAN IP Address 34.250.156.244

License Information

SecuReporter License

License Name
SecuReporter

License Status
4932 Days Remaining

The following table describes the labels on the **Analysis** > **Device** > **CPU / Memory / Session** screen.

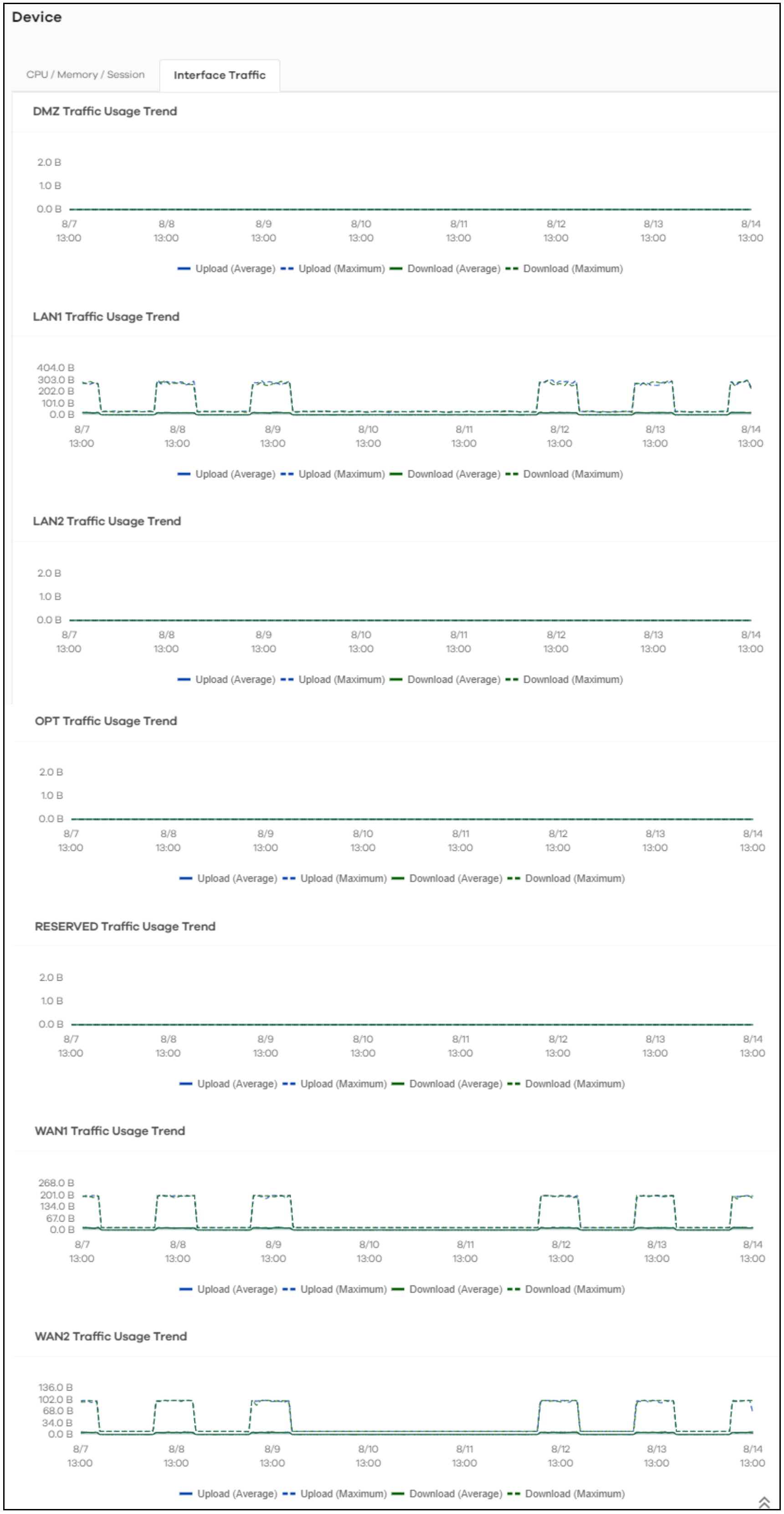
Table 22 Analysis > Device > CPU / Memory / Session

LABEL	DESCRIPTION
CPU Usage Trend	This field displays the current CPU utilization percentage used on the Zyxel Device.
Memory Usage Trend	This field displays the percentage of current DRAM memory utilization used on the Zyxel Device.
Session Usage Trend	This field displays the number of concurrent NAT/security policies traffic sessions the Zyxel Device is using.
Device Information	
Device Name	This field displays the device name of the Zyxel Device.
Model Name	This field displays the model name of the Zyxel Device.
MAC Address	This field displays the MAC address of the Zyxel Device.
Serial Number	This field displays the serial number of the Zyxel Device.
Firmware Version	This field displays the firmware version of the Zyxel Device.
WAN IP Address	This field displays the IP address of the Zyxel Device on the network.
License Information	
License Name	This field displays the name of the license that is linked to the Zyxel Device.
License Status	This field displays the remaining valid days of the service's license.

2.6.2 Interface Traffic

The following figure shows the **Analysis** > **Device** > **Interface Traffic** data visualizations.

Figure 26 Analysis > Device > Interface Trafficl



The following table describes the labels on the **Analysis** > **Device** > **Interface Traffic** screen.

Table 23 Analysis > Device > Interface Traffic

LABEL	DESCRIPTION
DMZ Traffic Usage Trend	This chart displays the amount of data that is transmitted on the DMZ interface over time.
LAN1 Traffic Usage Trend	This chart displays the amount of data that is transmitted on the LAN1 interface over time.
LAN2 Traffic Usage Trend	This chart displays the amount of data that is transmitted on the LAN2 interface over time.
OPT Traffic Usage Trend	This chart displays the amount of data that is transmitted on the OPT interface over time.
RESERVED Traffic Usage Trend	This chart displays the amount of data that is transmitted on the RESERVED interface over time.
WAN1 Traffic Usage Trend	This chart displays the amount of data that is transmitted on the WAN1 interface over time.
WAN2 Traffic Usage Trend	This chart displays the amount of data that is transmitted on the WAN2 interface over time.

CHAPTER 3
Logs

3.1 Overview

SecuReporter saves logs of your Zyxel Device every 10 minutes.

To have SecuReporter save sandboxing logs, some criteria needs to be met:

- See Section 1.1.2 on page 7 for more information on the Zyxel Devices that support sandboxing.
- Make sure sandboxing is selected in the **Categories** field of the **Configuration** > **Cloud CNM** > **SecuReporter** screen.

Otherwise, sandboxing logs are dropped. See the User's Guide of the supported Zyxel Device for instructions.

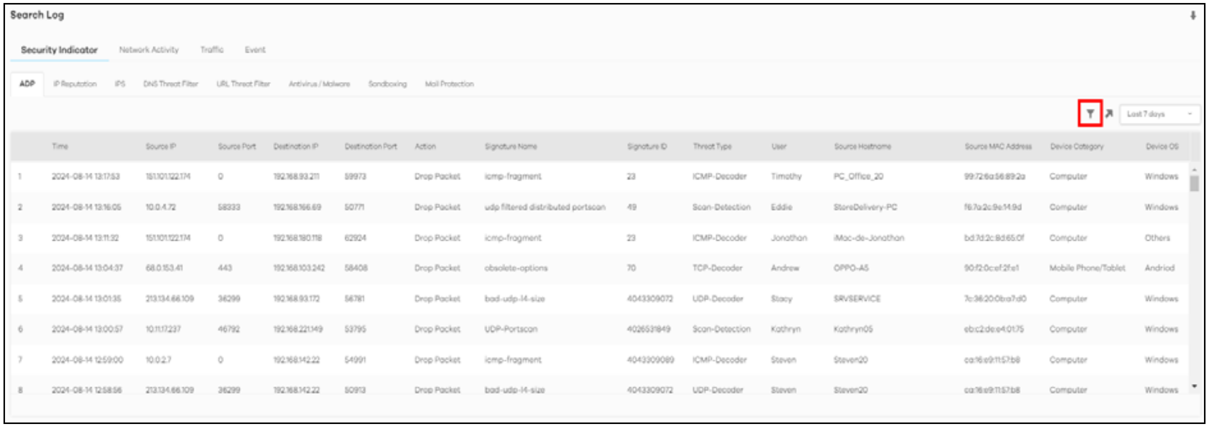
Note: Sandboxing logs will be removed after you reboot the Zyxel Device.

The Zyxel Device and SecuReporter may be in different time zones. It may take up to one day to archive logs depending on the amount of logs requested and how old the logs are. A Zyxel Device's log file is kept in archive by SecuReporter up to 1 year.

3.2 Search Log

Search log allows you to display Zyxel Device logs based on a time frame and also export them in CSV format for further analysis. You can select **Security Indicator**, **Network Activity**, **Traffic** and **Event** logs to view. The field on the right of ↗ allow you to select a specific time frame to view. The default is the last 7 days. You can change the time frame depending on your license type, see Table 25 on page 66 for details.

Figure 27 Search Log

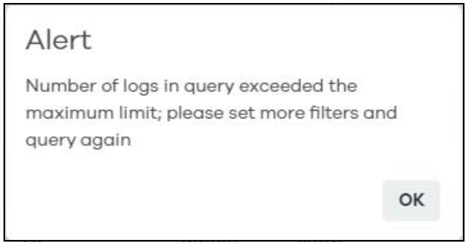


	Time	Source IP	Source Port	Destination IP	Destination Port	Action	Signature Name	Signature ID	Threat Type	User	Source Hostname	Source MAC Address	Device Category	Device OS
1	2024-08-14 13:17:53	151.101.122.174	0	192.168.93.211	59973	Drop Packet	icmp-fragment	23	ICMP-Decoder	Timothy	PC_Office_20	99:72:6a:56:89:2a	Computer	Windows
2	2024-08-14 13:16:05	10.0.4.72	58333	192.168.166.69	50771	Drop Packet	udp filtered distributed portscan	49	Scan-Detection	Eddie	StoreDelivery-PC	f6:7a:2c:9e:14:9d	Computer	Windows
3	2024-08-14 13:11:32	151.101.122.174	0	192.168.180.118	62924	Drop Packet	icmp-fragment	23	ICMP-Decoder	Jonathan	iMac-de-Jonathan	bd:7d:2c:8d:65:0f	Computer	Others
4	2024-08-14 13:04:37	68.0.153.41	443	192.168.103.242	58408	Drop Packet	obsolete-options	70	TCP-Decoder	Andrew	OPPO-A5	90:f2:0c:ef:2f:e1	Mobile Phone/Tablet	Andriod
5	2024-08-14 13:01:35	213.134.66.109	36299	192.168.93.172	56781	Drop Packet	bad-udp-l4-size	4043309072	UDP-Decoder	Stacy	SRVSERVICE	7c:36:20:0b:a7:d0	Computer	Windows
6	2024-08-14 13:00:57	10.11.17.237	46792	192.168.221.149	53795	Drop Packet	UDP-Portscan	4026531849	Scan-Detection	Kathryn	Kathryn05	eb:c2:de:e4:01:75	Computer	Windows
7	2024-08-14 12:59:00	10.0.2.7	0	192.168.142.22	54991	Drop Packet	icmp-fragment	4043309089	ICMP-Decoder	Steven	Steven20	ca:16:e9:11:57:b8	Computer	Windows
8	2024-08-14 12:58:56	213.134.66.109	36299	192.168.142.22	50913	Drop Packet	bad-udp-l4-size	4043309072	UDP-Decoder	Steven	Steven20	ca:16:e9:11:57:b8	Computer	Windows

You can set the search log criteria by clicking ▼ , see Table 25 on page 66 for details.

A maximum of 10,000 search results are allowed at a time. The following screen appears if the search result exceeds 10,000. Add filters to narrow down the search log criteria.

Figure 28 Number of Logs Exceeds the Limit



Alert

Number of logs in query exceeded the maximum limit; please set more filters and query again

3.2.1 Log Search Privileges

This table summarizes the SecuReporter log search privileges:

Table 24 SecuReporter Log Search Privileges

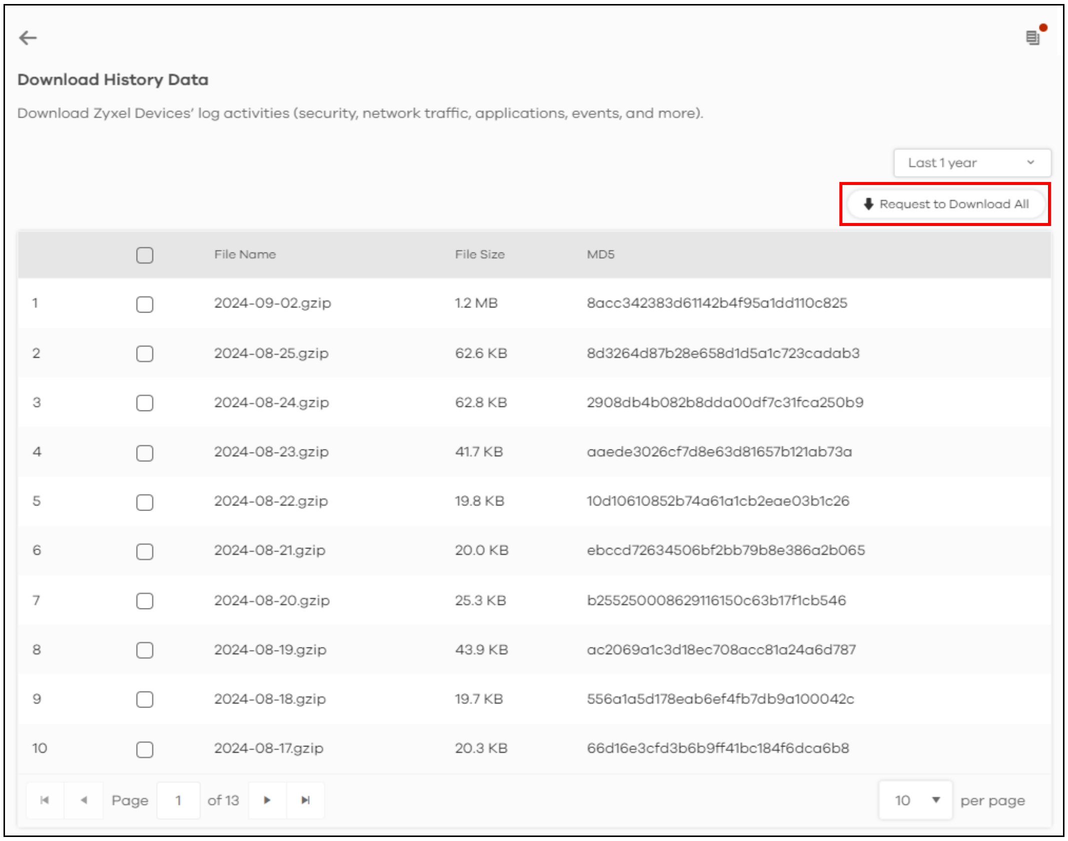
TYPE	SECUREPORTER
Security Logs Date Range	Past 30 days
Traffic Logs Date Range	Past 7 days
Custom Range	Yes
Filters	Yes
Frequency	No limitation
CSV file download	Yes

3.2.2 Download Logs

You can download the Zyxel Device’s logs by doing the following steps.

1 Go to the **Log** screen. Click the **Download History Data** icon ⬇ at the upper-right corner.

2 Select the log files you want and click **Request to Download**, or click **Request to Download All** to download all log files from up to 1 year at once.

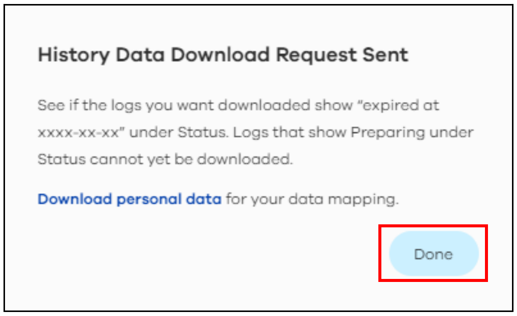


Download History Data

Download Zyxel Devices' log activities (security, network traffic, applications, events, and more).

	□	File Name	File Size	MD5
1	□	2024-09-02.gzip	1.2 MB	8acc342383d61142b4f95a1dd110c825
2	□	2024-08-25.gzip	62.6 KB	8d3264d87b28e658d1d5a1c723cadab3
3	□	2024-08-24.gzip	62.8 KB	2908db4b082b8dda00df7c31fca250b9
4	□	2024-08-23.gzip	41.7 KB	aaede3026cf7d8e63d81657b121ab73a
5	□	2024-08-22.gzip	19.8 KB	10d10610852b74a61a1cb2eae03b1c26
6	□	2024-08-21.gzip	20.0 KB	ebccd72634506bf2bb79b8e386a2b065
7	□	2024-08-20.gzip	25.3 KB	b25525000862911615 0c63b17f1cb546
8	□	2024-08-19.gzip	43.9 KB	ac2069a1c3d18ec708acc81a24a6d787
9	□	2024-08-18.gzip	19.7 KB	556a1a5d178eab6ef4fb7db9a100042c
10	□	2024-08-17.gzip	20.3 KB	66d16e3cfd3b6b9ff41bc184f6dca6b8

3 The following window pops up. Click **Done** to proceed.

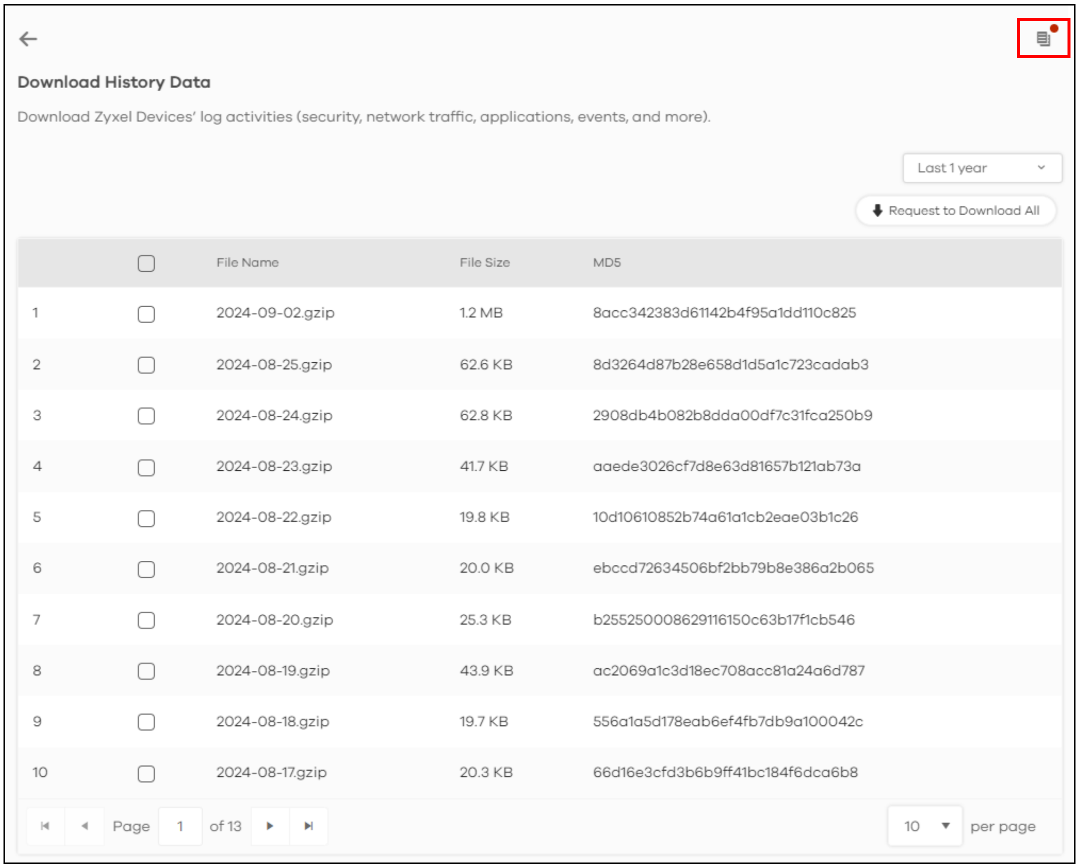


History Data Download Request Sent

See if the logs you want downloaded show "expired at xxxx-xx-xx" under Status. Logs that show Preparing under Status cannot yet be downloaded.

Download personal data for your data mapping.

4 Click the **History Data** icon at the upper-right corner.

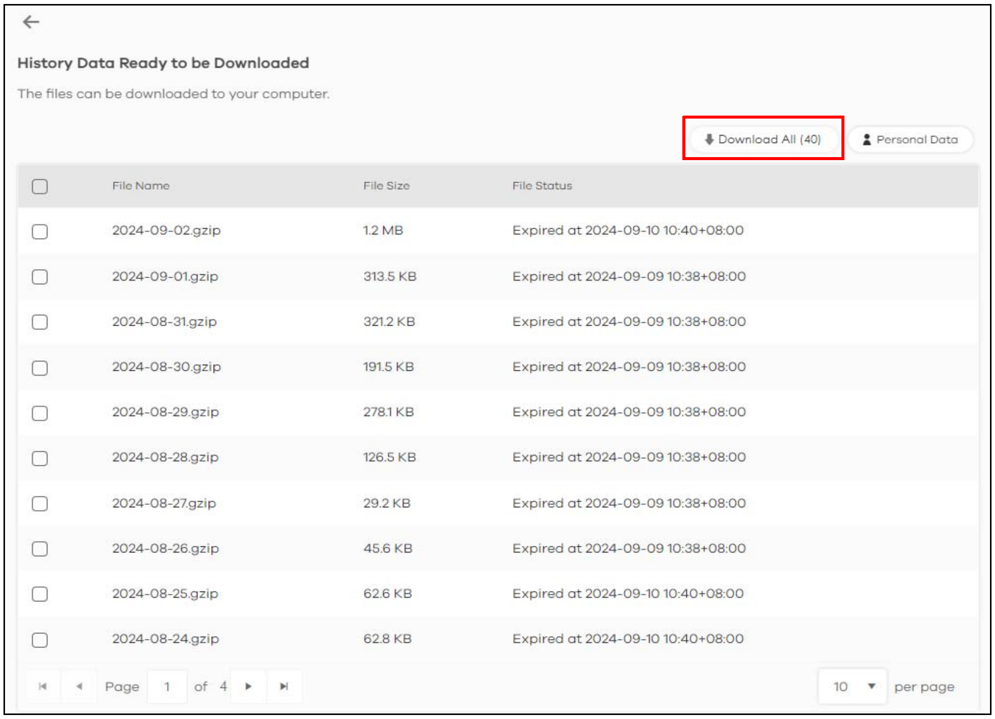


Download History Data

Download Zyxel Devices' log activities (security, network traffic, applications, events, and more).

	□	File Name	File Size	MD5
1	□	2024-09-02.gzip	1.2 MB	8acc342383d61142b4f95a1dd110c825
2	□	2024-08-25.gzip	62.6 KB	8d3264d87b28e658d1d5a1c723cadab3
3	□	2024-08-24.gzip	62.8 KB	2908db4b082b8dda00df7c31fca250b9
4	□	2024-08-23.gzip	41.7 KB	aaede3026cf7d8e63d81657b121ab73a
5	□	2024-08-22.gzip	19.8 KB	10d10610852b74a61a1cb2eae03b1c26
6	□	2024-08-21.gzip	20.0 KB	ebccd72634506bf2bb79b8e386a2b065
7	□	2024-08-20.gzip	25.3 KB	b25525000862911615 0c63b17f1cb546
8	□	2024-08-19.gzip	43.9 KB	ac2069a1c3d18ec708acc81a24a6d787
9	□	2024-08-18.gzip	19.7 KB	556a1a5d178eab6ef4fb7db9a100042c
10	□	2024-08-17.gzip	20.3 KB	66d16e3cfd3b6b9ff41bc184f6dca6b8

5 The log files ready for download will be displayed on this screen. Select the log files you want and click **Download** to download them in ZIP format, or click **Download All** to download all logs from up to 1 year in ZIP format to your computer.

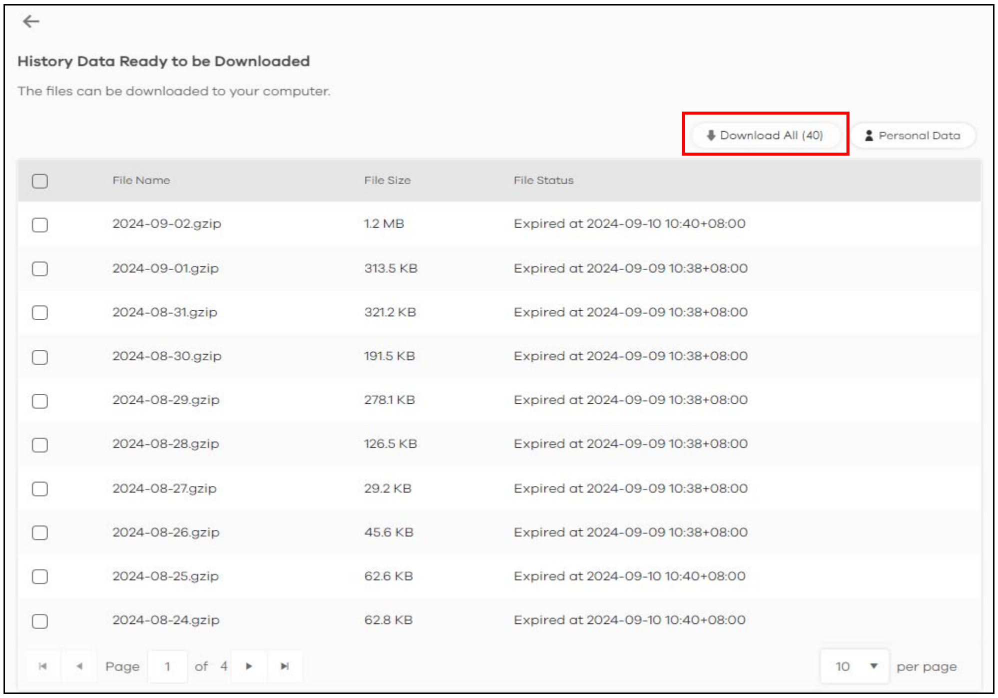


History Data Ready to be Downloaded

The files can be downloaded to your computer.

□	File Name	File Size	File Status
□	2024-09-02.gzip	1.2 MB	Expired at 2024-09-10 10:40+08:00
□	2024-09-01.gzip	313.5 KB	Expired at 2024-09-09 10:38+08:00
□	2024-08-31.gzip	321.2 KB	Expired at 2024-09-09 10:38+08:00
□	2024-08-30.gzip	191.5 KB	Expired at 2024-09-09 10:38+08:00
□	2024-08-29.gzip	278.1 KB	Expired at 2024-09-09 10:38+08:00
□	2024-08-28.gzip	126.5 KB	Expired at 2024-09-09 10:38+08:00
□	2024-08-27.gzip	29.2 KB	Expired at 2024-09-09 10:38+08:00
□	2024-08-26.gzip	45.6 KB	Expired at 2024-09-09 10:38+08:00
□	2024-08-25.gzip	62.6 KB	Expired at 2024-09-10 10:40+08:00
□	2024-08-24.gzip	62.8 KB	Expired at 2024-09-10 10:40+08:00

6 If you select **Fully Anonymous** as the **Protection Policy**, the hostname in the log files will be encrypted. You will need to download **Personal Data** to refer to the hostname.



History Data Ready to be Downloaded

The files can be downloaded to your computer.

□	File Name	File Size	File Status
□	2024-09-02.gzip	1.2 MB	Expired at 2024-09-10 10:40+08:00
□	2024-09-01.gzip	313.5 KB	Expired at 2024-09-09 10:38+08:00
□	2024-08-31.gzip	321.2 KB	Expired at 2024-09-09 10:38+08:00
□	2024-08-30.gzip	191.5 KB	Expired at 2024-09-09 10:38+08:00
□	2024-08-29.gzip	278.1 KB	Expired at 2024-09-09 10:38+08:00
□	2024-08-28.gzip	126.5 KB	Expired at 2024-09-09 10:38+08:00
□	2024-08-27.gzip	29.2 KB	Expired at 2024-09-09 10:38+08:00
□	2024-08-26.gzip	45.6 KB	Expired at 2024-09-09 10:38+08:00
□	2024-08-25.gzip	62.6 KB	Expired at 2024-09-10 10:40+08:00
□	2024-08-24.gzip	62.8 KB	Expired at 2024-09-10 10:40+08:00

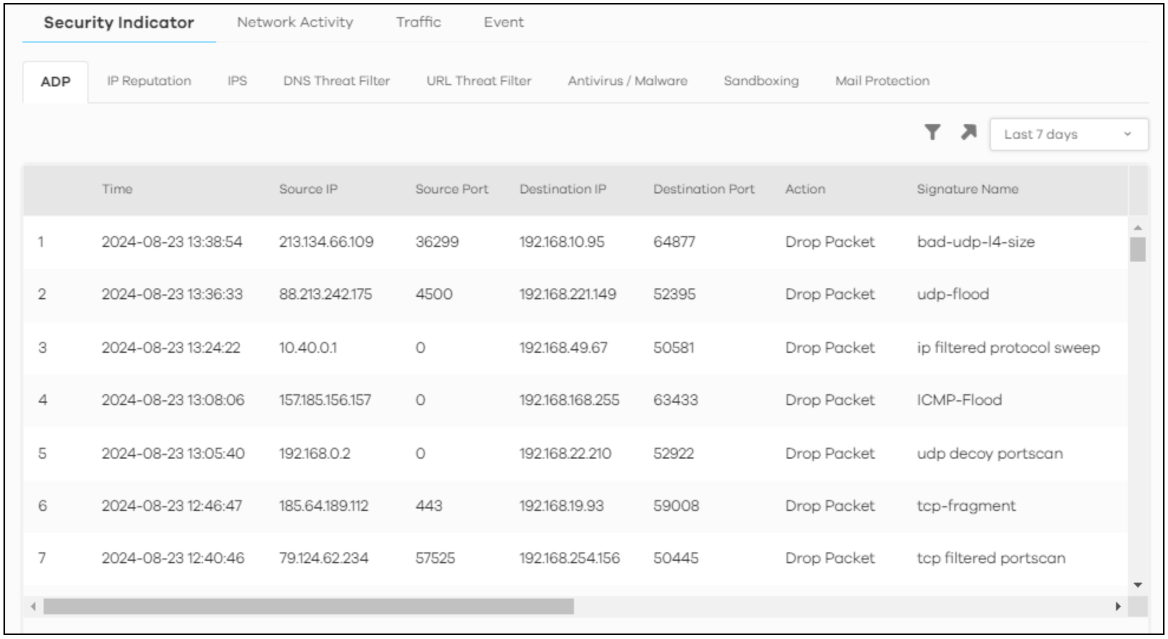
3.2.3 Security Indicator Logs

Security Indicator logs are categorized as follows:

- ADP
- IP Reputation
- IPS
- DNS Threat Filter
- URL Threat Filter
- Antivirus / Malware
- Sandboxing
- Mail Protection

The following figure shows the **Search** > **Log** > **Security Indicator** screen.

Figure 29 Search > Log > Security Indicator



	Time	Source IP	Source Port	Destination IP	Destination Port	Action	Signature Name
1	2024-08-23 13:38:54	213.134.66.109	36299	192.168.10.95	64877	Drop Packet	bad-udp-l4-size
2	2024-08-23 13:36:33	88.213.242.175	4500	192.168.221.149	52395	Drop Packet	udp-flood
3	2024-08-23 13:24:22	10.40.0.1	0	192.168.49.67	50581	Drop Packet	ip filtered protocol sweep
4	2024-08-23 13:08:06	157.185.156.157	0	192.168.168.255	63433	Drop Packet	ICMP-Flood
5	2024-08-23 13:05:40	192.168.0.2	0	192.168.22.210	52922	Drop Packet	udp decoy portscan
6	2024-08-23 12:46:47	185.64.189.112	443	192.168.19.93	59008	Drop Packet	tcp-fragment
7	2024-08-23 12:40:46	79.124.62.234	57525	192.168.254.156	50445	Drop Packet	tcp filtered portscan

The following table describes the labels on the **Search** > **Log** > **Security Indicator** screen.

Table 25 Search > Log > Security Indicator Screen

LABEL	DESCRIPTION
▼	Click **Clear All** to discard the filtering rules. Click **Add Rule** to create and manage the detailed filtering rules for each label. Click **Search** to apply the filtering rule to the search log. Click **--Please Select--** to set the filtering rule for each label. Click ⊗ to discard a filtering rule. The ⚠ will appear for the following reasons. Hover the mouse cursor on it to know the type of error. • **Please select a field**. This occurs when you click the **Search** button without selecting a field. • **Please enter a value before clicking 'Search'.** This occurs when you click the **Search** button without entering or selecting a value in the **contains** field. • **Press 'Enter' to apply.** This occurs when you click the **Search** button without pressing the **Enter** key for the **contains** field that can accept multiple values. • **The value cannot be found.** This occurs when you enter a none existent value in the **contains** field. • **No log available.** This occurs when no log is available for the filter value you enter or select. • **The value cannot be found.** This occurs when entering the wrong character format in the **contains** field (for example, entering alphabetic characters for the **Source IP** field).
↗	Click ↗ to have SecuReporter save the result of your search log to your computer in a CSV file. Maximum of 10,000 search results. Fields that do not have a value in the search log result will appear as blanks in the CSV file.
	Depending on your license type, select the time frame by clicking a 'from' and 'to' dates. You can also specify the 'from' and 'to' hh:mm time range (24-hour format). Then click **Apply** to display those logs.

Table 25 Search > Log > Security Indicator Screen (continued)

LABEL	DESCRIPTION
Time	Select the year-month-date hour:minute:second of the log. When adding this as a filter rule, click the drop-down field on the right of the screen to select the time frame.
Source IP	Enter the IPv4 or IPv6 address of the original sender of the packet. When adding this as a filter rule, enter the complete IP address or enter a wildcard such as 192.168.221.* (it will search for logs with any IP within 192.168.221.0 - 192.168.221.255).
Source Port	Enter the port number of the original sender of the packet. When adding this as a filter rule, enter the port number and press **Enter**. More than one port number can be entered after the first filter rule by entering another port number and pressing **Enter**. Multiple port number filters are entered one at a time.
Destination IP	Enter the IPv4 or IPv6 address of the final destination of the packet. When adding this as a filter rule, enter the complete IP address or enter a wildcard such as 210.61.209.* (it will search for logs with any IP within 210.61.209.0 - 210.61.209.255).
Destination Port	Enter the port number of the final destination of the packet. When adding this as a filter rule, enter the port number and press **Enter**. More than one port number can be entered after the first filter rule by entering another port number and pressing **Enter**. Multiple port number filters are entered one at a time.
Action (IPS/ADP)	Enter the response the Zyxel Device takes when a packet matches a signature. A signature is a pattern of malicious or suspicious packet activity. This is defined in the profile screen of your Zyxel Device's Web Configurator. The Zyxel Device checks all signatures and continues searching even after a match is found. If two or more rules have conflicting actions for the same packet, then the Zyxel Device applies the more restrictive action (**Reject Both**, **Reject Receiver** or **Reject Sender**, **Drop Packet**, **No Action** in this order). If a packet matches a rule for **Reject Receiver** and it also matches a rule for **Reject Sender**, then the Zyxel Device will **Reject Both**. When adding this as a filter rule, enter the first letter to enable SecuReporter auto suggestion. More than one action can be entered after the first filter rule by entering another action and pressing **Enter**. Multiple action filters are entered one at a time.
Action (IP Reputation)	IP Reputation checks the reputation of an IP address from a database. An IP address with bad reputation associates with suspicious activities, such as spam, virus, and/or phishing. Enter how the Zyxel Device will respond when there are packets coming from an IPv4 address with bad reputation (**ACCESS BLOCK** and **ACCESS FORWARD**). When adding this as a filter rule, enter the action or part of the action you want to find to enable SecuReporter auto suggestion. Both **ACCESS BLOCK** and **ACCESS FORWARD** can be entered as a filter rule by entering **ACCESS BLOCK** and pressing **Enter**, and then entering **ACCESS FORWARD** and pressing **Enter**.
Action (DNS Filter)	Enter how the Zyxel Device handle threats posed by FQDNs (**Block**, **Redirect**). When adding this as a filter rule, enter the first letter to enable SecuReporter auto suggestion. More than one action can be entered after the first filter rule by entering another action and pressing **Enter**. Multiple action filters are entered one at a time.
Action (URL Threat Filter)	Enter how the Zyxel Device handle threats posed by URLs (Uniform Resource Locators) (**ACCESS BLOCK**, **ACCESS WARNING**, **ACCESS PASS**). When adding this as a filter rule, enter the first letter to enable SecuReporter auto suggestion. More than one action can be entered after the first filter rule by entering another action and pressing **Enter**. Multiple action filters are entered one at a time.

Table 25 Search > Log > Security Indicator Screen (continued)

LABEL	DESCRIPTION
Action (Antivirus / Malware)	Enter **ACCESS FORWARD** when a service can be used to access the Zyxel Device. Otherwise, it is **ACCESS BLOCK**. Enter **FILE FORWARD** when a file is allowed. Otherwise, it is **FILE DESTROY**. When adding this as a filter rule, enter the first letter to enable SecuReporter auto suggestion. More than one action can be entered after the first filter rule by entering another action and pressing **Enter**. Multiple action filters are entered one at a time.
Action (Sandboxing)	The Zyxel Device sandbox checks all received files against its local cache for known malicious or suspicious codes. Enter how the Zyxel Device handle sandboxing (**Pass**, **Detected, Destroy**). When adding this as a filter rule, enter the first letter to enable SecuReporter auto suggestion. More than one action can be entered after the first filter rule by entering another action and pressing **Enter**. Multiple action filters are entered one at a time.
Action (Mail Protection)	Enter how the Zyxel Device handle spam SMTP/POP3 email (**MAIL FORWARD**, **MAIL DROP**). When adding this as a filter rule, enter the action or part of the action you want to find to enable SecuReporter auto suggestion. Both **MAIL FORWARD** and **MAIL DROP** can be entered as a filter rule by entering **MAIL FORWARD** and pressing **Enter**, and then entering **MAIL DROP** and pressing **Enter**.
User	Depending on the data protection policy (see Section 6.2.1 on page 95 for details), the following will be displayed: • For **Partially Anonymous** users, the user name is displayed but log search is disabled. • For **Fully Anonymous** users, copy a Hash value to search for logs. For example, USER-698a9b31-cea4-523c-8955-ffad47db967e. • For **Non-Anonymous** users, enter plain text (unlimited number of characters, case sensitive) for log search.
Signature Name	Enter the name (case sensitive, a wildcard is allowed) of a signature. When adding this as a filter rule, enter the name or part of the name of the signature you want to find to enable SecuReporter auto suggestion.
Signature ID	Enter the identification number of the signature. When adding this as a filter rule, enter the ID or part of the ID of the signature you want to find to enable SecuReporter auto suggestion.
Threat Type	Enter the signature (case sensitive) by threat type. When adding this as a filter rule, enter the threat type or part of the threat type you want to find to enable SecuReporter auto suggestion. More than one threat type can be entered after the first filter rule by entering another threat type and pressing **Enter**. Multiple threat type filters are entered one at a time.
Mail From	Depending on the data protection policy (see Section 6.2.1 on page 95 for details), the following will be displayed: • For **Partially Anonymous** users, the sender is displayed but log search is disabled. • For **Fully Anonymous** users, copy a Hash value to search for logs. For example, MAIL-108cef2d-b591-5460-af79-71994d126cc7. • For **Non-Anonymous** users, enter plain text (unlimited number of characters, case sensitive) for log search.
Mail To	Depending on the data protection policy (see Section 6.2.1 on page 95 for details), the following will be displayed: • For **Partially Anonymous** users, the recipient is displayed but log search is disabled. • For **Fully Anonymous** users, copy a Hash value to search for logs. For example, MAIL-108cef2d-b591-5460-af79-71994d126cc7. • For **Non-Anonymous** users, enter plain text (unlimited number of characters, case sensitive) for log search.
Mail Subject	This is the title header of the incoming email.

Table 25 Search > Log > Security Indicator Screen (continued)

LABEL	DESCRIPTION
Protocol (Sandboxing)	Enter the method email is sent or received through the Zyxel Device (**SMTP**, **POP3**, **HTTP**, **FTP**, and **Unknown**). When adding this as a filter rule, enter the protocol or part of the protocol you want to find to enable SecuReporter auto suggestion. More than one protocol can be entered after the first filter rule by entering another protocol and pressing **Enter**. Multiple protocol filters are entered one at a time.
Protocol (Mail Protection)	Enter the method email is sent or received through the Zyxel Device (**SMTP** and **POP3**). When adding this as a filter rule, enter the protocol or part of the protocol you want to find to enable SecuReporter auto suggestion. Both **SMTP** and **POP3** can be entered as a filter rule by entering **SMTP** and pressing **Enter**, and then entering **POP3** and pressing **Enter**.
URL	Enter the URL (a wildcard is allowed) where the threat was detected. When adding this as a filter rule, enter the URL or part of the URL you want to find to enable SecuReporter auto suggestion.
File Type	Enter the type of file sent for sandbox inspection (**Archives (.zip)**, **Executables**, **MS Office Documents**, **Macromedia Flash Data**/**PDF**/**RTF**). When adding this as a filter rule, enter the file type or part of the file type you want to find to enable SecuReporter auto suggestion. More than one file type can be entered after the first filter rule by entering another file type and pressing **Enter**. Multiple file type filters can be entered one at a time.
Score Level	Enter the score given by the Defend Center for malware characteristics that has been detected through the sandboxing function (**Malicious**, **Suspicious**, and **Clean**). When adding this as a filter rule, enter the score level or part of the score level you want to find to enable SecuReporter auto suggestion. More than one score level can be entered after the first filter rule by entering another score level and pressing **Enter**. Multiple score level filters can be entered one at a time.
Hash	Copy the hash value (a wildcard is allowed) of the file that was sent for sandbox inspection. When adding this as a filter rule, copy the hash value or part of the hash value you want to find to enable SecuReporter auto suggestion.
Rule Number	Enter the log search rule number. This is assigned by the Zyxel Device. When adding this as a filter rule, enter the rule number and press **Enter**. More than one rule number can be entered after the first filter rule by entering another rule number and pressing **Enter**. Multiple rule number filters are entered one at a time.
Scan Result	Enter the scan result (**White-List**, **Black-List**, **IP-Reputation**, **DNSBL**, **DNSBL-timeout**, **Spam**, **Virus**, **Spam-Virus**, **Timeout**, **Clear**, and **Phishing**). When adding this as a filter rule, enter the scan result or part of the scan result you want to find to enable SecuReporter auto suggestion. More than one scan result can be entered after the first filter rule by entering another scan result and pressing **Enter**. Multiple scan result filters are entered one at a time.
Severity	Enter the severity levels as defined in the Zyxel Device. (**1**) Very-Low, (**2**) Low, (**3**) Medium, (**4**) High, and (**5**) Severe. The number in brackets is the number you use when adding this as a filter rule. More than one severity level can be entered after the first filter rule by entering another severity level and pressing **Enter**. Multiple severity level filters are entered one at a time.
Category Name	Enter the most common types of URL threats (case sensitive) as detected by the Zyxel Device. Threat categories include **Malware**, **Spam Sites**, and so on. When adding this as a filter rule, enter the category name or part of the category name you want to find to enable SecuReporter auto suggestion. More than one category name can be entered after the first filter rule by entering another category name and pressing **Enter**. Multiple category name filters can be entered one at a time.

Table 25 Search > Log > Security Indicator Screen (continued)

LABEL	DESCRIPTION
Threat Name	Enter the name of the threat (a wildcard is allowed) as detected by the Zyxel Device. The value depends on the Zyxel Device. When adding this as a filter rule, enter the threat name you want to find.
Risk	Enter the threshold threat level to which the Zyxel Device will take action. (**High**, **Medium**, and **Low**). The threat level is determined by the IP reputation engine. It grades IPv4 addresses. When adding this as a filter rule, enter the threshold threat level or part of the threshold threat level you want to find to enable SecuReporter auto suggestion. More than one threshold threat level can be entered after the first filter rule by entering another threshold threat level and pressing **Enter**. Multiple threshold threat level filters can be entered one at a time.
Threat Category	Enter the most common type of threats posed by IPs blocked by the Zyxel Device as detected by IP Reputation. Threat categories include **Exploits**, **Spam Sources**, **Phishing**, and **BotNets**. When adding this as a filter rule, enter the threat category or part of the threat category you want to find to enable SecuReporter auto suggestion. More than one threat category can be entered after the first filter rule by entering another threat category and pressing **Enter**. Multiple threat category filters can be entered one at a time.
Risk IP	Enter the IPv4 or IPv6 address where the threat was detected. When adding this as a filter rule, enter the complete IP address or enter a wildcard such as 210.61.209.* (it will search for logs with any IP within 210.61.209.0 – 210.61.209.255).
Virus Name	Enter the name (case sensitive, a wildcard is allowed) of a virus. When adding this as a filter rule, enter the first letter to enable SecuReporter auto suggestion.
File Name	Enter the name (a wildcard is allowed) of the file. When adding this as a filter rule, enter the first letter to enable SecuReporter auto suggestion.
Application Category Name	Enter the most common types of applications as detected by the Zyxel Device. Application categories include **Application Service**, **Instant Messaging**, **Web**, **Encrypted**, and so on. When adding this as a filter rule, enter the first letter to enable SecuReporter auto suggestion. More than one application category can be entered after the first filter rule by entering another application category and pressing **Enter**. Multiple application category filters are entered one at a time.
Application Name	Enter the most frequently visited applications (a wildcard is allowed) as detected by the Zyxel Application Patrol. App Patrol manages general protocols (for example, HTTP and FTP), instant messenger (IM), peer-to-peer (P2P), Voice over IP (VoIP), streaming (RSTP) applications and even an application's individual features (like text messaging, voice, video conferencing, and file transfers). When adding this as a filter rule, enter the first letter to enable SecuReporter auto suggestion. More than one application name can be entered after the first filter rule by entering another application name and pressing **Enter**. Multiple application name filters are entered one at a time.
Web Category Name	Enter the most common types of threats posed by websites blocked by the Zyxel Device as detected by the URL Threat Filter. Threat categories include **Unrated**, **Anonymizers**, **Compromised**, **Phishing and Fraud**, **Spam Sites**, **Malware**, **Botnets**, and so on. When adding this as a filter rule, enter the web category name or part of the web category name you want to find to enable SecuReporter auto suggestion. More than one web category name can be entered after the first filter rule by entering another web category name and pressing **Enter**. Multiple web category name filters can be entered one at a time.

Table 25 Search > Log > Security Indicator Screen (continued)

LABEL	DESCRIPTION
Website	Enter the name of the website (a wildcard is allowed) tasked with screening for the most common types of threats posed by websites blocked by the Zyxel Devices. When adding this as a filter rule, enter the website or part of the website you want to find to enable SecuReporter auto suggestion.
Query Type	Enter the type of IP address that may pose a security threat to network devices behind the Zyxel Device. When adding this as a filter rule, select from the drop-down list. More than one query type can be entered after the first filter rule by entering another query type and pressing **Enter**. Multiple query type filters are entered one at a time.
Domain	Enter the URL of FQDNs that may pose a security threat to network devices behind the Zyxel Device. When adding this as a filter rule, select from the drop-down list. More than one domain can be entered after the first filter rule by entering another domain and pressing **Enter**. Multiple domain filters are entered one at a time.

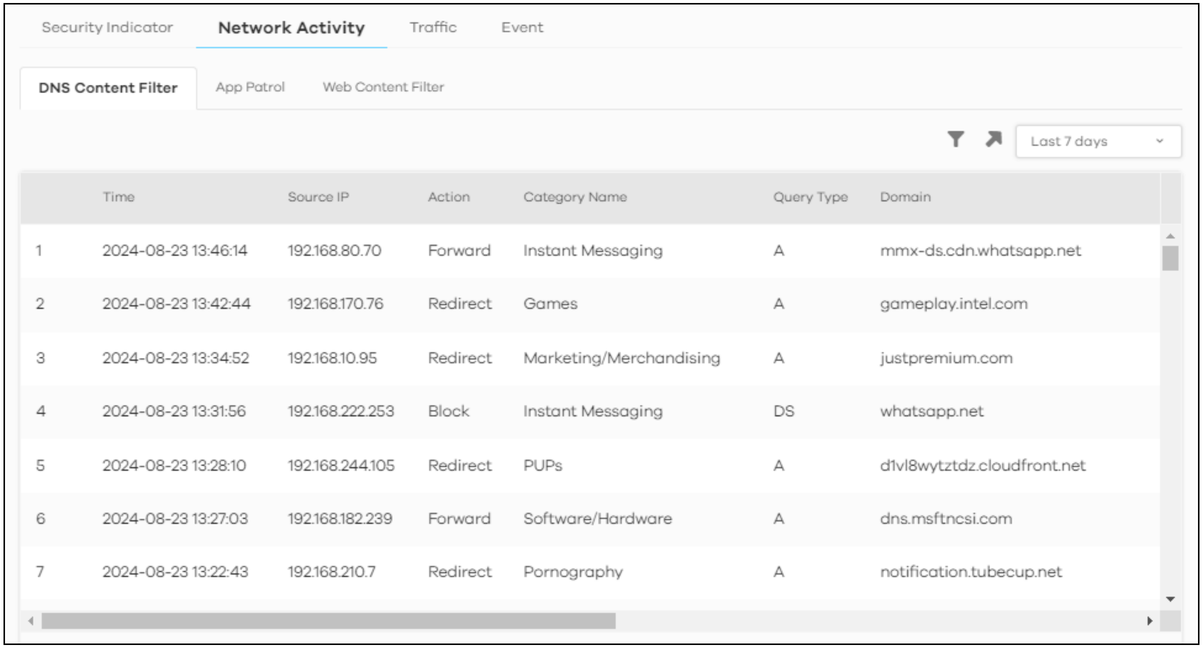
3.2.4 Network Activity Logs

Network activity logs are categorized as follows:

- DNS Content Filter
- App Patrol
- Web Content Filter

The following figure shows the **Search** > **Log** > **Network Activity** screen.

Figure 30 Search > Log > Network Activity



	Time	Source IP	Action	Category Name	Query Type	Domain
1	2024-08-23 13:46:14	192.168.80.70	Forward	Instant Messaging	A	mmx-ds.cdn.whatsapp.net
2	2024-08-23 13:42:44	192.168.170.76	Redirect	Games	A	gameplay.intel.com
3	2024-08-23 13:34:52	192.168.10.95	Redirect	Marketing/Merchandising	A	justpremium.com
4	2024-08-23 13:31:56	192.168.222.253	Block	Instant Messaging	DS	whatsapp.net
5	2024-08-23 13:28:10	192.168.244.105	Redirect	PUPs	A	d1vl8wytztdz.cloudfront.net
6	2024-08-23 13:27:03	192.168.182.239	Forward	Software/Hardware	A	dns.msftncsi.com
7	2024-08-23 13:22:43	192.168.210.7	Redirect	Pornography	A	notification.tubecup.net

The following table describes the labels on the **Search** > **Log** > **Network Activity** screen.

Table 26 Search > Log > Network Activity Screen

LABEL	DESCRIPTION
▼	Click **Clear All** to discard the filtering rules. Click **Add Rule** to create and manage the detailed filtering rules for each label. Click **Search** to apply the filtering rule to the log search. Click **--Please Select--** to set the filtering rule for each label. Click ☒ to discard a filtering rule. The ⚠ will appear for the following reasons. Hover the mouse cursor on it to know the type of error. • **Please select a field**. This occurs when you click the **Search** button without selecting a field. • **Please enter a value before clicking 'Search'.** This occurs when you click the **Search** button without entering or selecting a value in the **contains** field. • **Press 'Enter' to apply.** This occurs when you click the **Search** button without pressing the **Enter** key for the **contains** field that can accept multiple values. • **The value cannot be found.** This occurs when you enter a none existent value in the **contains** field. • **No log available.** This occurs when no log is available for the filter value you enter or select. • **The value cannot be found.** This occurs when entering the wrong character format in the **contains** field (for example, entering alphabetic characters for the **Source IP** field).
↗	Click ↗ to have SecuReporter save the result of your log search to your computer in a CSV file. Maximum of 10,000 search results. Fields that do not have a value in the log search result will appear as blanks in the CSV file.
	Depending on your license type, select the time frame by clicking a 'from' and 'to' dates. You can also specify the 'from' and 'to' hh:mm time range (24-hour format). Then click **Apply** to display those logs.
Time	Select the year-month-date hour:minute:second of the log. When adding this as a filter rule, click the drop-down field on the right of the screen to select the time frame.
Source IP	Enter the IPv4 or IPv6 address of the original sender of the packet. When adding this as a filter rule, enter the complete IP address or enter a wildcard such as 192.168.221.* (it will search for logs with any IP within 192.168.221.0 – 192.168.221.255).
Source Port	Enter the port number of the original sender of the packet. When adding this as a filter rule, enter the port number and press **Enter**. More than one port number can be entered after the first filter rule by entering another port number and pressing **Enter**. Multiple port number filters are entered one at a time.
Destination IP	Enter the IPv4 or IPv6 address of the final destination of the packet. When adding this as a filter rule, enter the complete IP address or enter a wildcard such as 210.61.209.* (it will search for logs with any IP within 210.61.209.0 – 210.61.209.255).
Destination Port	Enter the port number of the final destination of the packet. When adding this as a filter rule, enter the port number and press **Enter**. More than one port number can be entered after the first filter rule by entering another port number and pressing **Enter**. Multiple port number filters are entered one at a time.
Action (DNS Content Filter)	Enter how the Zyxel Device handle threats posed by domains (**Block**, **Redirect, Forward**). When adding this as a filter rule, enter the first letter to enable SecuReporter auto suggestion. More than one action can be entered after the first filter rule by entering another action and pressing **Enter**. Multiple action filters are entered one at a time.

Table 26 Search > Log > Network Activity Screen (continued)

LABEL	DESCRIPTION
Action (App Patrol)	Enter how the Zyxel Device handle threats posed by applications (**reject, drop, forward**). When adding this as a filter rule, enter the first letter to enable SecuReporter auto suggestion. More than one action can be entered after the first filter rule by entering another action and pressing **Enter**. Multiple action filters are entered one at a time.
Action (Web Content Filter)	Enter how the Zyxel Device handle threats posed by websites (**forward, block, warning**). When adding this as a filter rule, enter the first letter to enable SecuReporter auto suggestion. More than one action can be entered after the first filter rule by entering another action and pressing **Enter**. Multiple action filters are entered one at a time.
User	Depending on the data protection policy (see Section 6.2.1 on page 95 for details), the following will be displayed: • For **Partially Anonymous** users, the user name is displayed but log search is disabled. • For **Fully Anonymous** users, copy a Hash value to search for logs. For example, USER-698a9b31-cea4-523c-8955-ffad47db967e. • For **Non-Anonymous** users, enter plain text (unlimited number of characters, case sensitive) for log search.
Application Category Name	Enter the most common types of applications as detected by the Zyxel Device. Application categories include **Application Service**, **Instant Messaging**, **Web**, **Encrypted**, and so on. When adding this as a filter rule, enter the first letter to enable SecuReporter auto suggestion. More than one application category can be entered after the first filter rule by entering another application category and pressing **Enter**. Multiple application category filters are entered one at a time.
Application Name	Enter the most frequently visited applications (a wildcard is allowed) as detected by the Zyxel Application Patrol. App Patrol manages general protocols (for example, HTTP and FTP), instant messenger (IM), peer-to-peer (P2P), Voice over IP (VoIP), streaming (RSTP) applications and even an application's individual features (like text messaging, voice, video conferencing, and file transfers). When adding this as a filter rule, enter the first letter to enable SecuReporter auto suggestion. More than one application name can be entered after the first filter rule by entering another application name and pressing **Enter**. Multiple application name filters are entered one at a time.
Web Category Name	Enter the most common types of threats posed by websites blocked by the Zyxel Device as detected by the URL Threat Filter. Threat categories include **Unrated**, **Anonymizers**, **Compromised**, **Phishing and Fraud**, **Spam Sites**, **Malware**, **Botnets**, and so on. When adding this as a filter rule, enter the web category name or part of the web category name you want to find to enable SecuReporter auto suggestion. More than one web category name can be entered after the first filter rule by entering another web category name and pressing **Enter**. Multiple web category name filters can be entered one at a time.
Website	Enter the website (a wildcard is allowed) to screen the most common threats by websites blocked by the Zyxel Device. When adding this as a filter rule, enter the website or part of the website you want to find to enable SecuReporter auto suggestion.
Query Type	Enter the DNS record types for accessed domains that were blocked. DNS record types include **A**, **AAAA, HTTPS, TXT** and so on. When adding this as a filter rule, select from the drop-down list. More than one query type can be entered after the first filter rule by entering another query type and pressing **Enter**. Multiple query type filters are entered one at a time.

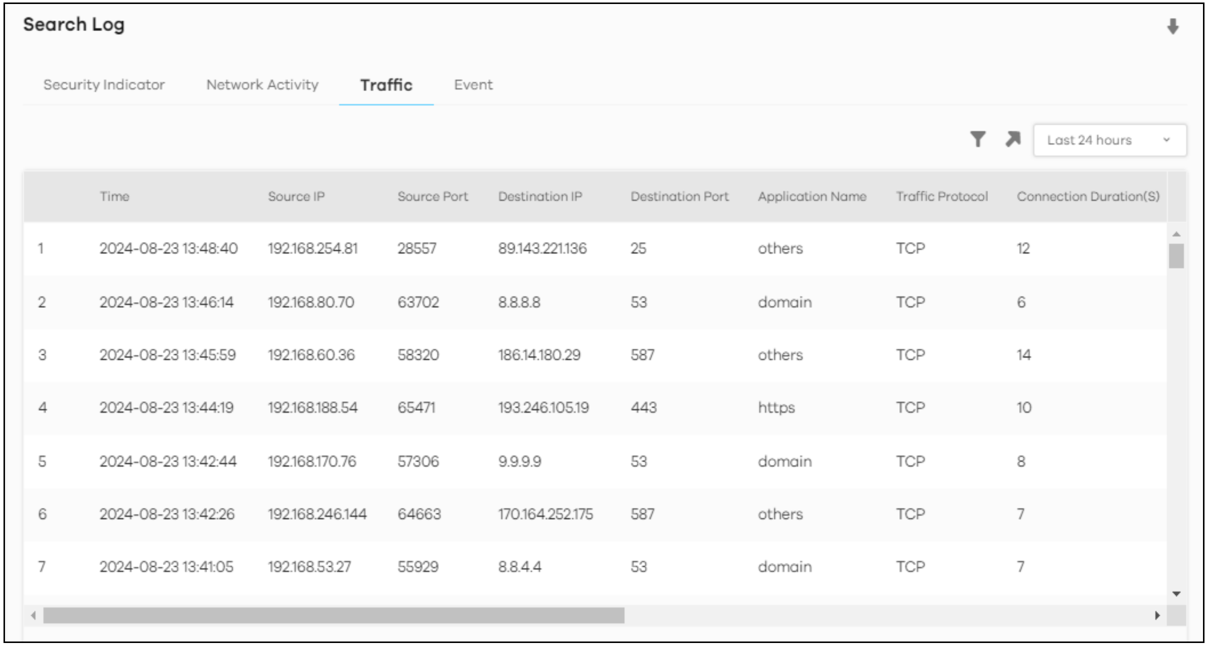
Table 26 Search > Log > Network Activity Screen (continued)

LABEL	DESCRIPTION
Domain	Enter the URL of FQDNs that may pose a security threat to network devices behind the Zyxel Device. When adding this as a filter rule, select from the drop-down list. More than one domain can be entered after the first filter rule by entering another domain and pressing **Enter**. Multiple domain filters are entered one at a time.
Rule	Enter the name of the policy control rule the the connection is using. When adding this as a filter rule, select from the drop-down list. More than one rule can be entered after the first filter rule by entering another domain and pressing **Enter**. Multiple domain filters are entered one at a time.
Source Hostname	This is the hostname of the original sender of the packet.
Source MAC Address	This is the MAC address of the original sender of the packet.
Device Category	This is the device type of the original sender of the packet.
Device OS	This is the device operatiing system of the original sender of the packet.

3.2.5 Traffic Logs

The following figure shows the **Search** > **Log** > **Traffic** screen.

Figure 31 Search > Log > Traffic



	Time	Source IP	Source Port	Destination IP	Destination Port	Application Name	Traffic Protocol	Connection Duration(S)
1	2024-08-23 13:48:40	192.168.254.81	28557	89.143.221.136	25	others	TCP	12
2	2024-08-23 13:46:14	192.168.80.70	63702	8.8.8.8	53	domain	TCP	6
3	2024-08-23 13:45:59	192.168.60.36	58320	186.14.180.29	587	others	TCP	14
4	2024-08-23 13:44:19	192.168.188.54	65471	193.246.105.19	443	https	TCP	10
5	2024-08-23 13:42:44	192.168.170.76	57306	9.9.9.9	53	domain	TCP	8
6	2024-08-23 13:42:26	192.168.246.144	64663	170.164.252.175	587	others	TCP	7
7	2024-08-23 13:41:05	192.168.53.27	55929	8.8.4.4	53	domain	TCP	7

The following table describes the labels on the **Search** > **Log** > **Traffic** screen.

Table 27 Search > Log > Traffic

LABEL	DESCRIPTION
▼	Click **Clear All** to discard the filtering rules. Click **Add Rule** to create and manage the detailed filtering rules for each label. Click **Search** to apply the filtering rule to the log search. Click **--Please Select--** to set the filtering rule for each label. Click ⊗ to discard a filtering rule. The ⚠ will appear for the following reasons. Hover the mouse cursor on it to know the type of error. • **Please select a field**. This occurs when you click the **Search** button without selecting a field. • **Please enter a value before clicking 'Search'.** This occurs when you click the **Search** button without entering or selecting a value in the **contains** field. • **Press 'Enter' to apply.** This occurs when you click the **Search** button without pressing the **Enter** key for the **contains** field that can accept multiple values. • **The value cannot be found.** This occurs when you enter a none existent value in the **contains** field. • **No log available.** This occurs when no log is available for the filter value you enter or select. • **The value cannot be found.** This occurs when entering the wrong character format in the **contains** field (for example, entering alphabetic characters for the **Source IP** field).
↗	Click ↗ to have SecuReporter save the result of your log search to your computer in a CSV file. Maximum of 10,000 search results. Fields that do not have a value in the log search result will appear as blanks in the CSV file.
	Depending on your license type, select the time frame by clicking a 'from' and 'to' dates. You can also specify the 'from' and 'to' hh:mm time range (24-hour format). Then click **Apply** to display those logs.
Time	Select the year-month-date hour:minute:second of the log. When adding this as a filter rule, click the drop-down field on the right of the screen to select the time frame.
Source IP	Enter the IPv4 or IPv6 address of the original sender of the packet. When adding this as a filter rule, enter the complete IP address or enter a wildcard such as 192.168.221.* (it will search for logs with any IP within 192.168.221.0 – 192.168.221.255).
Source Port	Enter the port number of the original sender of the packet. When adding this as a filter rule, enter the port number and press **Enter**. More than one port number can be entered after the first filter rule by entering another port number and pressing **Enter**. Multiple port number filters are entered one at a time.
Destination IP	Enter the IPv4 or IPv6 address of the final destination of the packet. When adding this as a filter rule, enter the complete IP address or enter a wildcard such as 210.61.209.* (it will search for logs with any IP within 210.61.209.0 – 210.61.209.255).
Destination Port	Enter the port number of the final destination of the packet. When adding this as a filter rule, enter the port number and press **Enter**. More than one port number can be entered after the first filter rule by entering another port number and pressing **Enter**. Multiple port number filters are entered one at a time.

Table 27 Search > Log > Traffic (continued)

LABEL	DESCRIPTION
Application Name	Enter the most frequently visited applications (case sensitive) as detected by the Zyxel Application Patrol. APP Patrol manages general protocols (for example, HTTP and FTP), instant messenger (IM), peer-to-peer (P2P), Voice over IP (VoIP), streaming (RSTP) applications and even an application's individual features (like text messaging, voice, video conferencing, and file transfers). When adding this as a filter rule, enter the first letter to enable SecuReporter auto suggestion. More than one application can be entered after the first filter rule by entering another application and pressing **Enter**. Multiple application filters are entered one at a time.
Traffic Protocol	Enter the type of transport packet being carried (**TCP**/**UDP**/**OTHERS**). When adding this as a filter rule, enter the first letter to enable SecuReporter auto suggestion. More than one traffic protocol can be entered after the first filter rule by entering another traffic protocol and pressing **Enter**. Multiple traffic protocol filters are entered one at a time.
Connection Duration(S)	This is the length of the network session in seconds.
Inbound Traffic	This is the amount of information received by the source in the network session.
Outbound Traffic	This is the amount of information transmitted by the source in the network session.
User	Depending on the data protection policy (see Section 6.2.1 on page 95 for details), the following will be displayed: • For **Partially Anonymous** users, the user name is displayed but log search is disabled. • For **Fully Anonymous** users, copy a Hash value to search for logs. For example, USER-698a9b31-cea4-523c-8955-ffad47db967e. • For **Non-Anonymous** users, enter plain text (unlimited number of characters, case sensitive) for log search.
Astra Email	This is the Astra user's mail address of the original sender of the packet.
Source Hostname	This is the hostname of the original sender of the packet.
Source MAC Address	This is the MAC address of the original sender of the packet.
Device Category	This is the device type of the original sender of the packet.
Device OS	This is the device operatiing system of the original sender of the packet.

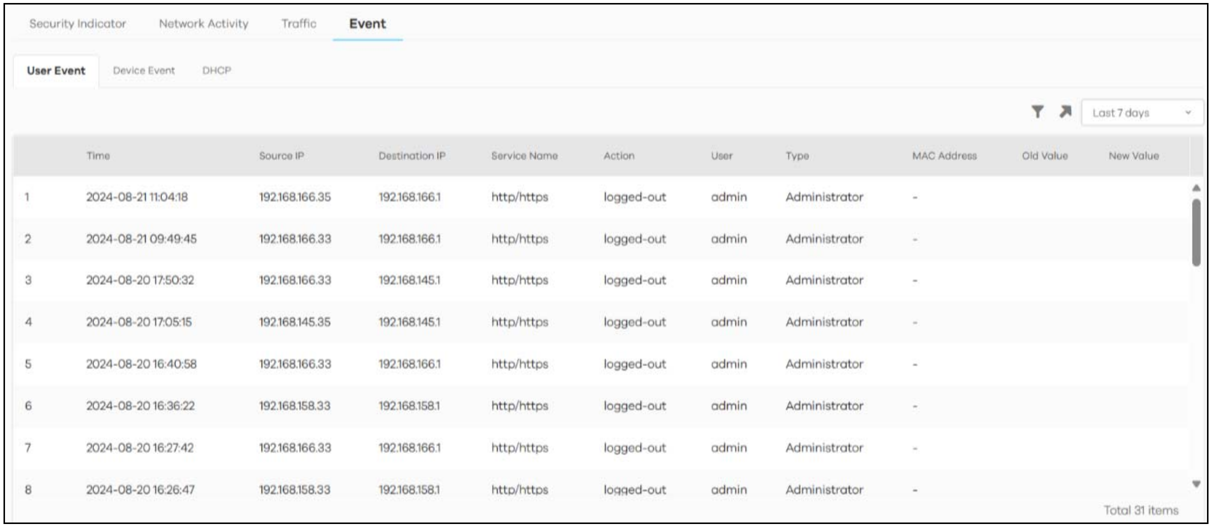
3.2.6 Event Logs

Event logs are categorized as follows:

- User Login
- Device Event
- DHCP

The following figure shows the **Search** > **Log** > **Event** screen.

Figure 32 Search > Log > Event



	Time	Source IP	Destination IP	Service Name	Action	User	Type	MAC Address	Old Value	New Value
1	2024-08-21 11:04:18	192.168.166.35	192.168.166.1	http/https	logged-out	admin	Administrator	-		
2	2024-08-21 09:49:45	192.168.166.33	192.168.166.1	http/https	logged-out	admin	Administrator	-		
3	2024-08-20 17:50:32	192.168.166.33	192.168.145.1	http/https	logged-out	admin	Administrator	-		
4	2024-08-20 17:05:15	192.168.145.35	192.168.145.1	http/https	logged-out	admin	Administrator	-		
5	2024-08-20 16:40:58	192.168.166.33	192.168.166.1	http/https	logged-out	admin	Administrator	-		
6	2024-08-20 16:36:22	192.168.158.33	192.168.158.1	http/https	logged-out	admin	Administrator	-		
7	2024-08-20 16:27:42	192.168.166.33	192.168.166.1	http/https	logged-out	admin	Administrator	-		
8	2024-08-20 16:26:47	192.168.158.33	192.168.158.1	http/https	logged-out	admin	Administrator	-		

Total 31 items

The following table describes the labels on the **Search** > **Log** > **Event** screen.

Table 28 Search > Log > Event Screen

LABEL	DESCRIPTION
▼	Click **Clear All** to discard the filtering rules. Click **Add Rule** to create and manage the detailed filtering rules for each label. Click **Search** to apply the filtering rule to the log search. Click **--Please Select--** to set the filtering rule for each label. Click ⊗ to discard a filtering rule. The ⚠ will appear for the following reasons. Hover the mouse cursor on it to know the type of error. • **Please select a field**. This occurs when you click the **Search** button without selecting a field. • **Please enter a value before clicking 'Search'.** This occurs when you click the **Search** button without entering or selecting a value in the **contains** field. • **Press 'Enter' to apply.** This occurs when you click the **Search** button without pressing the **Enter** key for the **contains** field that can accept multiple values. • **The value cannot be found.** This occurs when you enter a none existent value in the **contains** field. • **No log available.** This occurs when no log is available for the filter value you enter or select. • **The value cannot be found.** This occurs when entering the wrong character format in the **contains** field (for example, entering alphabetic characters for the **Source IP** field).
↗	Click ↗ to have SecuReporter save the result of your log search to your computer in a CSV file. Maximum of 10,000 search results. Fields that do not have a value in the log search result will appear as blanks in the CSV file.
	Depending on your license type, select the time frame by clicking a 'from' and 'to' dates. You can also specify the 'from' and 'to' hh:mm time range (24-hour format). Then click **Apply** to display those logs.
Time	Select the year-month-date hour:minute:second of the log. When adding this as a filter rule, click the drop-down field on the right of the screen to select the time frame.

Table 28 Search > Log > Event Screen (continued)

LABEL	DESCRIPTION
Source IP	Enter the IPv4 or IPv6 address of the original sender of the packet. When adding this as a filter rule, enter the complete IP address or enter a wildcard such as 192.168.221.* (it will search for logs with any IP within 192.168.221.0 – 192.168.221.255)
Destination IP	Enter the IPv4 or IPv6 address of the final destination of the packet. When adding this as a filter rule, enter the complete IP address or enter a wildcard such as 210.61.209.* (it will search for logs with any IP within 210.61.209.0 – 210.61.209.255).
Service Name	Enter the login method (**console**, **http/https**, **ssh**). When adding this as a filter rule, enter the service name or part of the service name you want to find to enable SecuReporter auto suggestion. More than one service name can be entered after the first filter rule by entering another service name and pressing **Enter**. Multiple service name filters can be entered one at a time.
Action Event > User Login	Enter the status of the login attempt (**Failed-login** / **logged-in** / **logged-out**). When adding this as a filter rule, enter the first letter to enable SecuReporter auto suggestion. More than one action can be entered after the first filter rule by entering another action and pressing **Enter**. Multiple action filters are entered one at a time.
Action Event > DHCP	Enter the action of assigning an IP address to a device by the DNS server or release (**assigned** and **release**). When adding this as a filter rule, enter the action or part of the action you want to find to enable SecuReporter auto suggestion. Both **assigned** and **release** can be entered as a filter rule by entering **assigned** and pressing **Enter**, and then entering **release** and pressing **Enter**.
Assign IP	This is the IPv4 or IPv6 address currently assigned to a DHCP client or reserved for a specific MAC address. When adding this as a filter rule, enter the complete IP address or enter a wildcard such as 192.168.221.* (it will search for logs with any IP within 192.168.221.0 – 192.168.221.255)
User	Depending on the data protection policy (see Section 6.2.1 on page 95 for details), the following will be displayed: • For **Partially Anonymous** users, the user name is displayed but log search is disabled. • For **Fully Anonymous** users, copy a Hash value to search for logs. For example, USER-698a9b31-cea4-523c-8955-ffad47db967e. • For **Non-Anonymous** users, enter plain text (unlimited number of characters, case sensitive) for log search.
Type	Enter the role type (a wildcard is allowed) of the event's login attempt (**Administrator**, **Limited-Admin**, **User**). When adding this as a filter rule, enter the role type or part of the role type you want to find to enable SecuReporter auto suggestion.
MAC Address Event > User Login	Enter the Zyxel Device's MAC address (case sensitive) during the event's login attempt. Depending on the data protection policy (see Section 6.2.1 on page 95 for details), the following will be displayed: • For **Partially Anonymous** users, the MAC address is displayed but log search is disabled. • For **Fully Anonymous** users, copy a Hash value to search for logs. For example, MAC-5ba49d8a-d027-5c76-bf28-a45857f780bc. • For **Non-Anonymous** users, enter plain text (unlimited number of characters, case sensitive) for log search.

Table 28 Search > Log > Event Screen (continued)

LABEL	DESCRIPTION
MAC Address Event > DHCP	Enter the MAC address (case sensitive) to which the IP address is currently assigned or for which the IP address is reserved. Depending on the data protection policy (see Section 6.2.1 on page 95 for details), the following will be displayed: • For **Partially Anonymous** users, the MAC address is displayed but log search is disabled. • For **Fully Anonymous** users, copy a Hash value to search for logs. For example, MAC-5ba49d8a-d027-5c76-bf28-a45857f780bc. • For **Non-Anonymous** users, enter plain text (unlimited number of characters, case sensitive) for log search.
Device Event	This displays **boot-up** as the Zyxel Device event.
Host Name	Enter the unique name (case sensitive) by which a device is known on a network. The Zyxel Device learns these from the DHCP client requests. Depending on the data protection policy (see Section 6.2.1 on page 95 for details), the following will be displayed: • For **Partially Anonymous** users, the host name is displayed but log search is disabled. • For **Fully Anonymous** users, copy a Hash value to search for logs. For example, HOST-8c9f2269-c7fa-55e5-b36f-d8987efd11ee. • For **Non-Anonymous** users, enter plain text (unlimited number of characters, case sensitive) for log search.

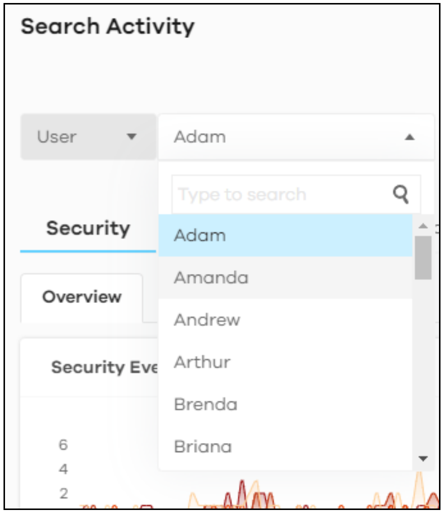
3.3 Search User

The **Search** > **Activity** screen allows administrators to look up network activity by user. A user-aware user is a user who must log in to the Zyxel Device, so that the Zyxel Device can apply specific routing policies and security settings to this user. The Zyxel Device is ‘aware’ of the user who is logged in and therefore can store ‘user-aware’ analytics and logs.

To perform a search, click **Search** > **Activity**.

In the field at the top-left of the screen, enter a username. You may also enter a partial term to generate a list of matching results.

Figure 33 Search > Activity > User



3.3.1 Details

Click an entry in your search results to open up a report of the user's recent security events, application usage, website usage, top destination countries, and login or logout history.

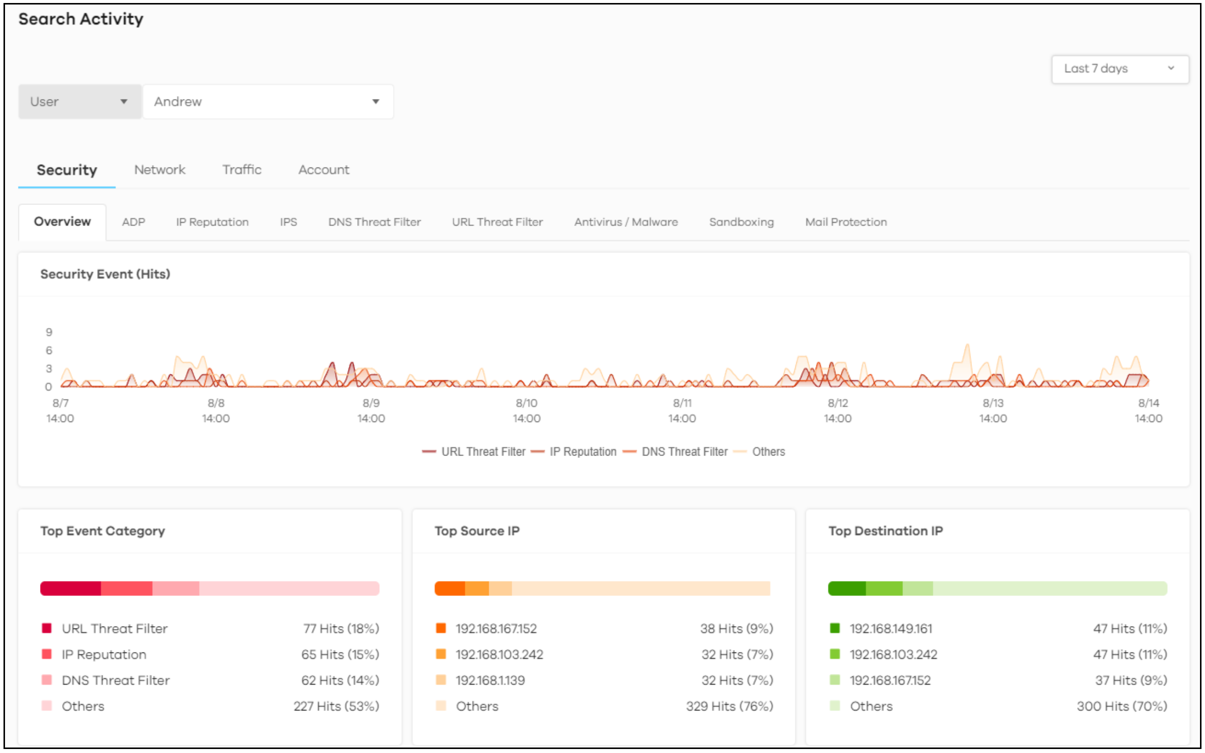
Security events include anomalies, app patrol, malware, spam, threats (IPS), unsafe websites, and web protection (websites blocked by web security policies). The following table shows severity levels for security events.

Table 29 Security Events Severity Levels

SECURITY EVENT	SEVERITY DEFINITION
IPS	IPS: highest is 5, lowest is 1 Severity from 1 – 5
Malware	Severity 4
Spam	Severity 3
Unsafe website access	For these categories, severity is 4 • Botnets • Compromised • Malware • Phishing & Fraud
	Spam sites: severity 3
	Anonymizers: severity 2
	Network errors: severity 1
Anomaly	Severity 2

Select an username in **Search** > **Acitivity** > **User** to display the following figure.

Figure 34 Search > Acitivity > User



Top Event Category

URL Threat Filter	77 Hits (18%)
IP Reputation	65 Hits (15%)
DNS Threat Filter	62 Hits (14%)
Others	227 Hits (53%)

Top Source IP

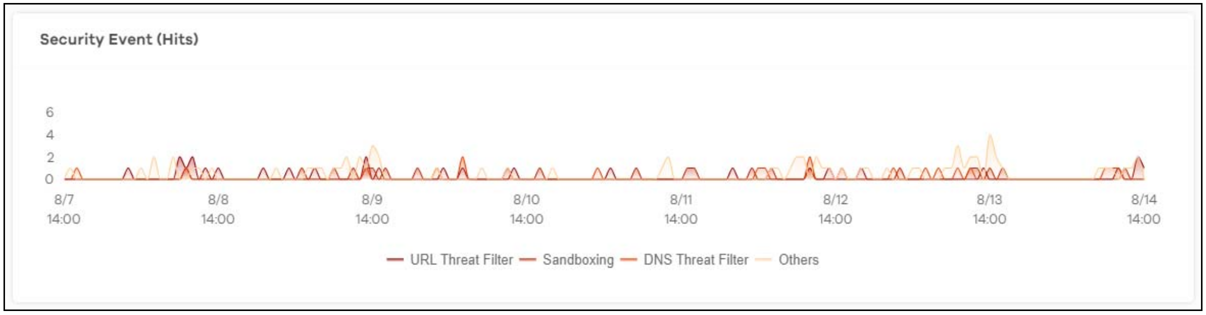
192.168.167.152	38 Hits (9%)
192.168.103.242	32 Hits (7%)
192.168.1.139	32 Hits (7%)
Others	329 Hits (76%)

Top Destination IP

192.168.149.161	47 Hits (11%)
192.168.103.242	47 Hits (11%)
192.168.167.152	37 Hits (9%)
Others	300 Hits (70%)

Click a graph to see further usage details for this user. The following figure shows details on security events through the selected Zyxel Device for this user.

Figure 35 Search > User > Details > Security Event (Hits)



CHAPTER 4 Alerts

4.1 Overview

An alert is a notification about a potential security problem. SecuReporter offers several ways for you to monitor the security environment of your network. One way is by generating alerts when it detects potential security problems. Using user behavior analytics, SecuReporter is able to identify anomalous and suspicious activity, creating alerts to bring them to your attention.

4.2 Trend & Details

To see the alerts that have been raised by SecuReporter, click **History** > **Alert**.

On the screen, a graph sorts your recent alerts by the severity of the threat they pose to the network. The alert classifications are as follows:

- High severity – Events that are exceptionally harmful, such as attacks by viruses.
- Medium severity – Events that could collect users' personal information or adversely affect the network.
- Low severity – Events that usually have no adverse effect on a network.

By default, trend lines for alerts of all three severity levels will appear in this graph. To hide the trend line of a severity level, click on its corresponding color block on the top.

Below the chart, you can view a complete log of all SecuReporter alerts that have been created. To order the alerts by variables such as **Time**, **Category, Event Type**, and **Severity**.

The following table shows event categories, types and criteria supported by SecuReporter at the time of writing.

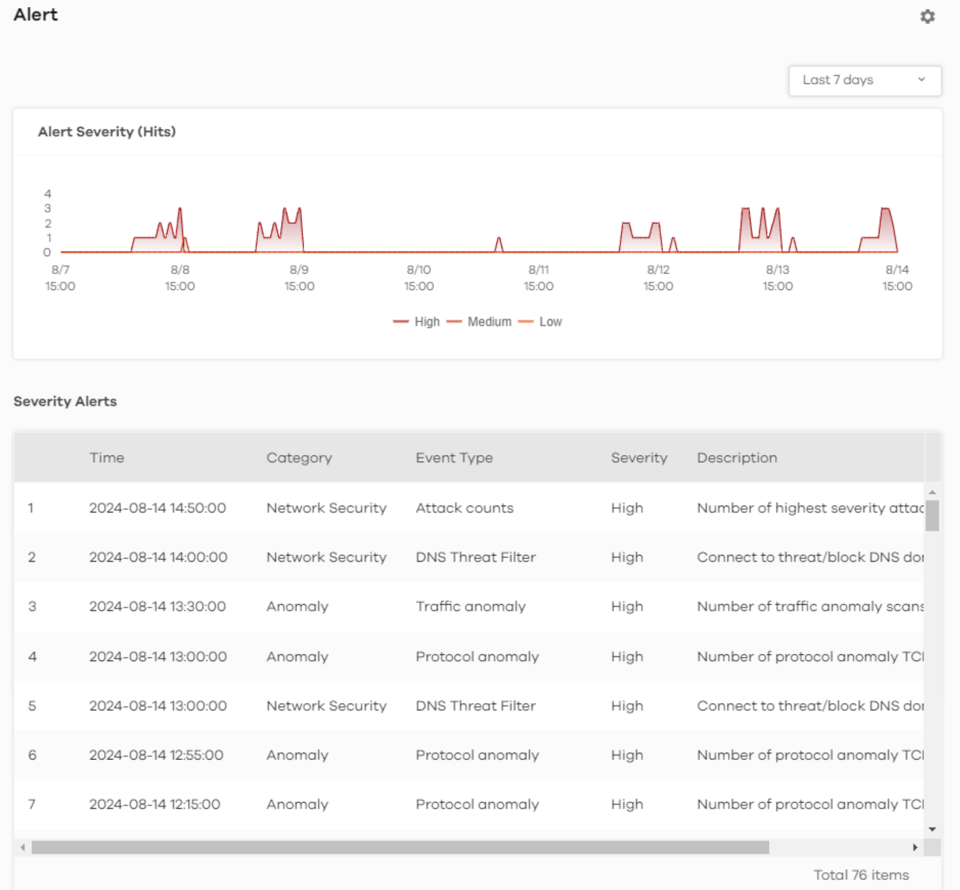
Table 30 Event Categories, Types and Criteria

CATEGORY	EVENT TYPES	CRITERIA	TIME ALLOWED
Network Security	URL Threat Filter	Number of times connection attempts to or from a site in an URL threat category detected and blocked is greater than the threshold	60 minutes
Network Security	IP Reputation-Incoming	Number of times packets coming from an IPv4 address with bad reputation occurred is greater than the threshold	10 minutes
Network Security	IP Reputation-Outgoing	Number of times connection attempt to an IPv4 address with bad reputation occurred is greater than the threshold within	60 minutes
Network Security	Sandboxing malicious file	Number of malicious files destroyed is greater than the threshold	5 minutes

Table 30 Event Categories, Types and Criteria (continued)

CATEGORY	EVENT TYPES	CRITERIA	TIME ALLOWED
Network Security	Sandboxing suspicious file	Number of suspicious files destroyed is greater than the threshold	5 minutes
Network Security	DNS Filter	Number of times connection attempt to a FQDN that is blocked or in the threat category	60 minutes
Network Security	Attack counts	Number of highest severity attacks greater than the threshold	5 minutes
Network Security	Attack counts	Number of attacks greater than the threshold	5 minutes
Network Security	Malware/virus detection	Malware or virus attack count greater than the threshold	5 minutes
Network Security	Malware/virus detection	Number of times the same malware/virus is detected greater than the threshold	15 minutes
Network Security	Alert counts	Number of alerts greater than the threshold	1 minute
Device	Online status	Device offline for more than {threshold} minutes	15 minutes
Device	Reboot	Reboot	–
Device	Concurrent sessions	Session numbers greater than the {threshold} %	–
Anomaly	Login failure	Number of login failures over threshold	1 minute
Anomaly	Traffic anomaly	Number of scans/floods detected greater than the threshold	5 minutes
Anomaly	Protocol anomaly	Number of TCP/UDP/ICMP/IP decoders greater than the threshold	5 minutes

Figure 36 History > Alert



	Time	Category	Event Type	Severity	Description
1	2024-08-14 14:50:00	Network Security	Attack counts	High	Number of highest severity attac
2	2024-08-14 14:00:00	Network Security	DNS Threat Filter	High	Connect to threat/block DNS do
3	2024-08-14 13:30:00	Anomaly	Traffic anomaly	High	Number of traffic anomaly scans
4	2024-08-14 13:00:00	Anomaly	Protocol anomaly	High	Number of protocol anomaly TC
5	2024-08-14 13:00:00	Network Security	DNS Threat Filter	High	Connect to threat/block DNS do
6	2024-08-14 12:55:00	Anomaly	Protocol anomaly	High	Number of protocol anomaly TC
7	2024-08-14 12:15:00	Anomaly	Protocol anomaly	High	Number of protocol anomaly TC

Total 76 items

The following table describes the labels on this screen.

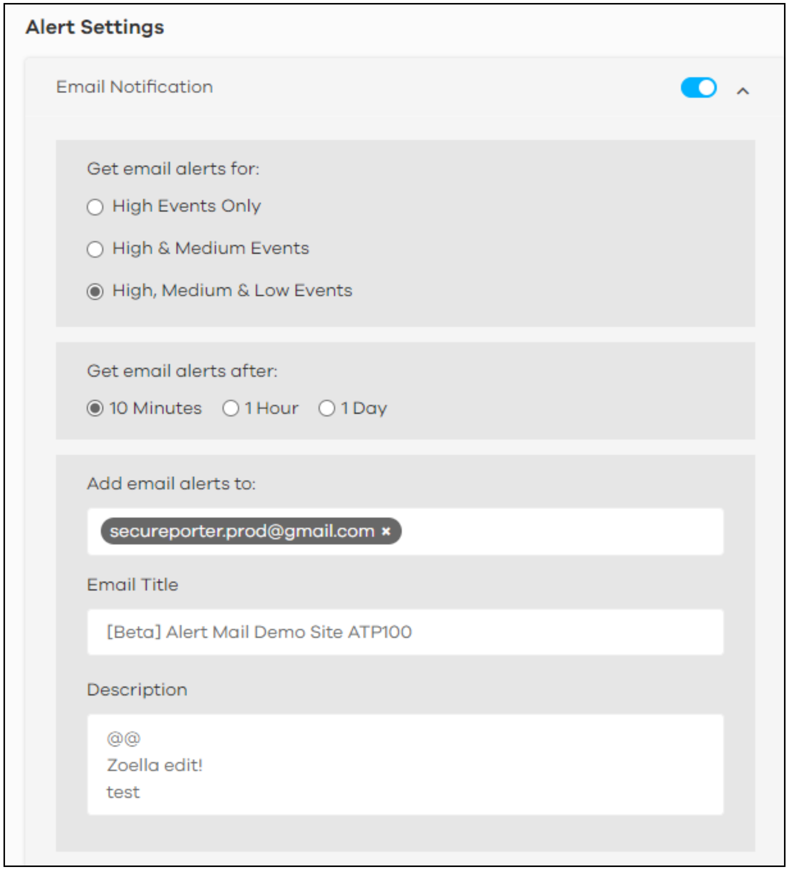
Table 31 History > Alert

LABEL	DESCRIPTION
Alert Severity (Hits)	Use this interactive graph to view trends in the severity of all the alerts that have been triggered on the network. The event severity classifications are as follows: High severity – Events that are exceptionally harmful, such as attacks by viruses [OR: 10 potential malware attacks within 5 minutes] Medium severity – Events that could collect users' personal information or adversely affect the network [OR: 2 potential malware or virus attacks within 15 minutes] Low severity – Events that usually have no adverse effect on a network. Trend lines for all security classifications appear on the graph by default. Click on a color block to hide its corresponding trend line.
Severity Alerts	This table shows a list of recent security events.
Time	This displays the year-month-date hour:minute:second that the threat occurred.
Category	This displays the alerts by category.
Event type	This displays the type of alert that was triggered. Examples of alert types are IPS, Spam, Virus and Web.
Severity	This displays the severity level as outlined in Table 7 on page 12.
Description	This displays the further information on this alert.

4.3 Alert Settings

Configure alert settings, such as recipients, email subject, event severity levels to email, and event triggering thresholds in the **History** > **Alert** > **Alert Settings** screen.

Figure 37 History > Alert > Alert Settings > Email Notification



Alert Settings

Email Notification

Get email alerts for:

○ High Events Only

○ High & Medium Events

● High, Medium & Low Events

Get email alerts after:

● 10 Minutes ○ 1 Hour ○ 1 Day

Add email alerts to:

secureporter.prod@gmail.com ×

Email Title

[Beta] Alert Mail Demo Site ATP100

Description

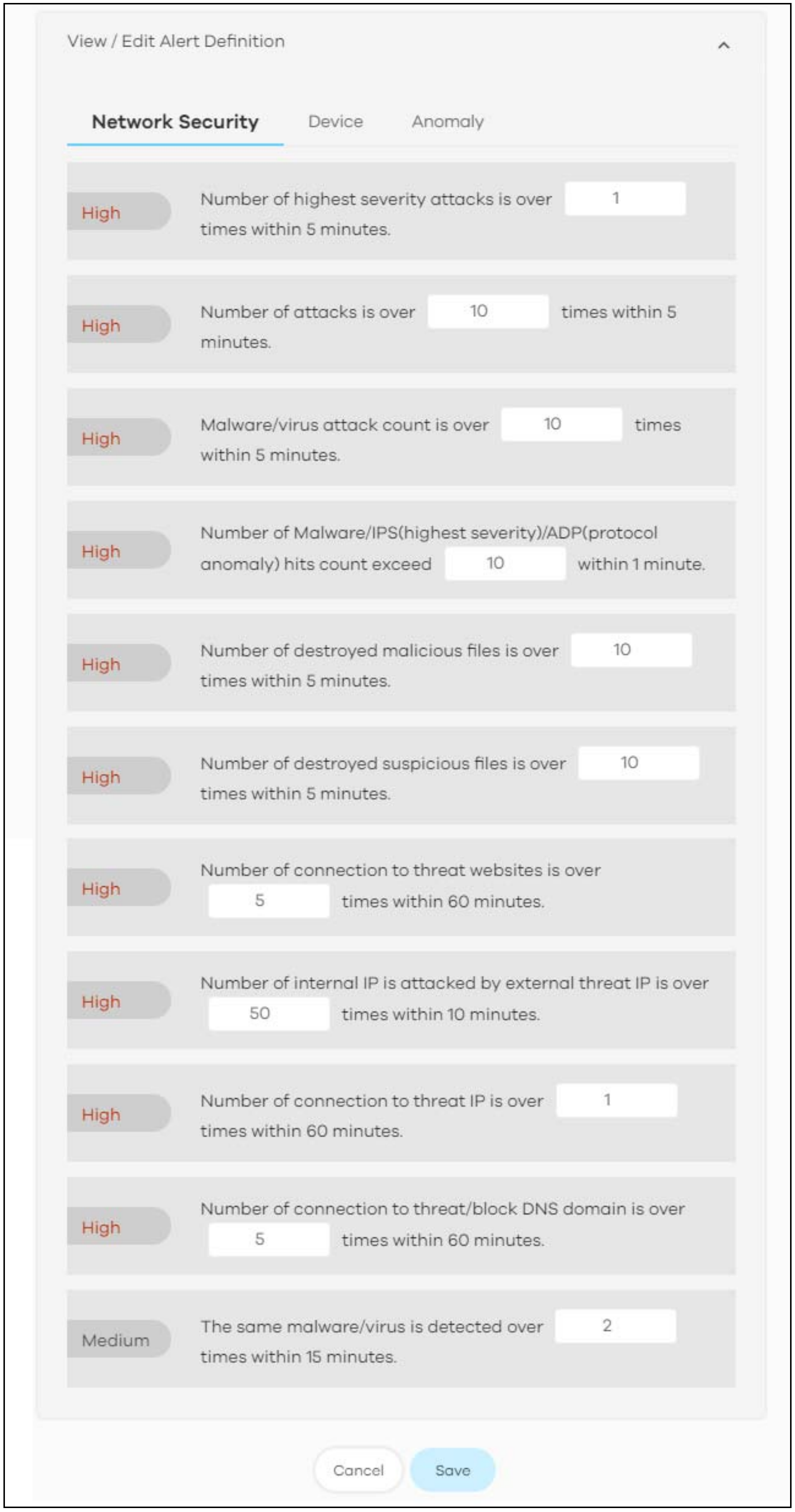
@@
Zoella edit!
test

The following table describes the labels in this screen.

Table 32 History > Alert > Alert Settings > Email Notification

LABEL	DESCRIPTION
Email Notification	Off means no alerts are emailed to any recipients. Select On (slide switch to the right) to have alerts emailed to the selected recipients.
Get email alerts for	Select the severity levels of the security events for which you wish to send out email notifications. • High Events Only – Events that are exceptionally harmful, such as attacks by viruses or a high frequency of attacks. • High & Medium Events – Events that are exceptionally harmful, and events that usually have no adverse effect on a network or a low frequency of attacks. • High, Medium & Low Events – Events that are exceptionally harmful, events that usually have no adverse effect on a network, and events that could collect users' personal information or adversely affect the network or a medium frequency of attacks.
Get email alert after	Select **10 Minutes**, **1 Hour**, or **1 Day** to choose how often you want to receive alert notifications.
Add email alerts to	This is where you can add users to the mailing list for event notifications. To add a user, click the field window to select one or more names from the box.
Email Title	Type an email subject here.
Description	Type a description of the emails to be sent here. For example, maybe these emails are just for high severity events.

Figure 38 History > Alert > Alert Settings > View/Edit Alert Definition > Network Security



View / Edit Alert Definition

Network Security Device Anomaly

High — Number of highest severity attacks is over 1 times within 5 minutes.

High — Number of attacks is over 10 times within 5 minutes.

High — Malware/virus attack count is over 10 times within 5 minutes.

High — Number of Malware/IPS(highest severity)/ADP(protocol anomaly) hits count exceed 10 within 1 minute.

High — Number of destroyed malicious files is over 10 times within 5 minutes.

High — Number of destroyed suspicious files is over 10 times within 5 minutes.

High — Number of connection to threat websites is over 5 times within 60 minutes.

High — Number of internal IP is attacked by external threat IP is over 50 times within 10 minutes.

High — Number of connection to threat IP is over 1 times within 60 minutes.

High — Number of connection to threat/block DNS domain is over 5 times within 60 minutes.

Medium — The same malware/virus is detected over 2 times within 15 minutes.

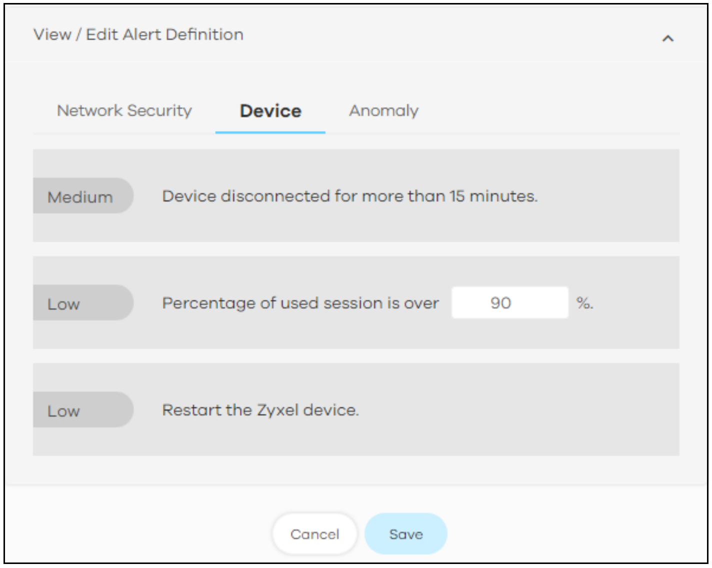
The following table describes the labels in this screen.

Table 33 History > Alert > Alert Settings > View/Edit Alert Definition > Network Security

LABEL	DESCRIPTION
View/Edit Alert Definition	
Network Security	This table shows a list of recent network security events.
(set the threshold)	The threshold is the number that triggers an alert. If the threshold is adjustable, a blank field will appear. Set the threshold for the alert by entering the numeric value or by pressing the up- and down-arrows. Adjustable values vary and include frequency, rate of occurrence, and the time period.

The table shows a list of recent Zyxel Device usage events.

Figure 39 History > Alert > Alert Settings > View/Edit Alert Definition > Device



View / Edit Alert Definition

Medium Device disconnected for more than 15 minutes.

Low Percentage of used session is over 90 %.

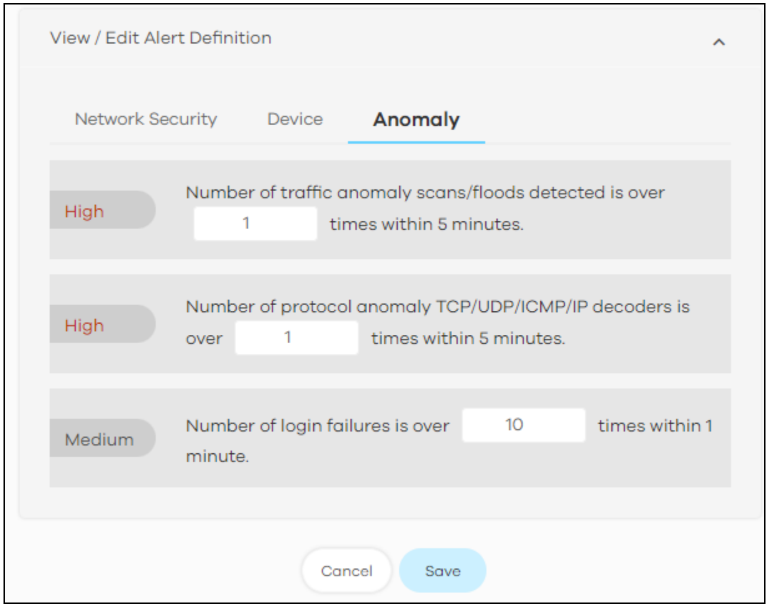
Low Restart the Zyxel device.

The following table describes the labels in this screen.

Table 34 History > Alert > Alert Settings > View/Edit Alert Definition > Device

LABEL	DESCRIPTION
View/Edit Alert Definition	
Percentage of used session is over %	The Zyxel Device has a limit on the number of concurrent active connections allowed. You can set a percentage threshold of this limit, and an alert will be sent if the number of connections exceeds this threshold.

Figure 40 History > Alert > Alert Settings > View/Edit Alert Definition > Anomaly



View / Edit Alert Definition

High — Number of traffic anomaly scans/floods detected is over 1 times within 5 minutes.

High — Number of protocol anomaly TCP/UDP/ICMP/IP decoders is over 1 times within 5 minutes.

Medium — Number of login failures is over 10 times within 1 minute.

The following table describes the labels in this screen.

Table 35 History > Alert > Alert Settings > View/Edit Alert Definition > Anomaly

LABEL	DESCRIPTION
View/Edit Alert Definition	
Anomaly	This table shows a list of recent traffic and protocol anomalies.
(set the threshold)	The threshold is the number that triggers an alert. If the threshold is adjustable, a blank field will appear. Set the threshold for the alert by entering the numeric value or by pressing the up- and down-arrows. Adjustable values vary and include frequency, rate of occurrence, and the time period.

CHAPTER 5
Report

5.1 Overview

A report is a summary of activities for a claimed Zyxel Device over a period of time. It is available in HTML or PDF format. The SecuReporter's Report allows you to define the title and description, what to include in the report, and who to send it to. Customize your reports based on the traffic diversity of your organization.

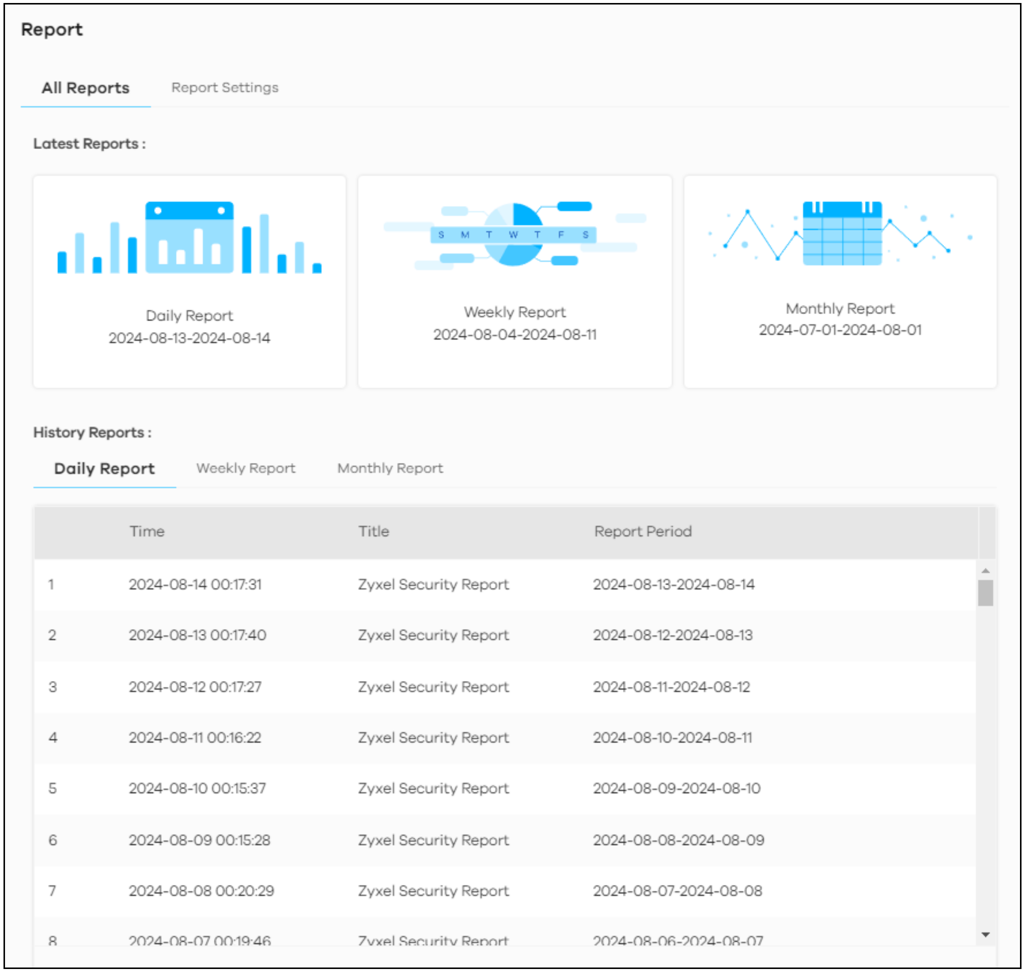
You can choose to generate reports of analyzed data collected over one of three time frames:

- Last 24 hours
- Last 7 days
- Last 30 days

5.2 All Reports

Click **History** > **Report** > **All Report** to view and manage a list of SecuReporter reports generated over the last 365 days. Reports will automatically be removed from the list after one year.

Figure 41 History > Report > All Reports



Report

All Reports | Report Settings

Latest Reports :

Daily Report
2024-08-13-2024-08-14

Weekly Report
2024-08-04-2024-08-11

Monthly Report
2024-07-01-2024-08-01

History Reports :

Daily Report | Weekly Report | Monthly Report

	Time	Title	Report Period
1	2024-08-14 00:17:31	Zyxel Security Report	2024-08-13-2024-08-14
2	2024-08-13 00:17:40	Zyxel Security Report	2024-08-12-2024-08-13
3	2024-08-12 00:17:27	Zyxel Security Report	2024-08-11-2024-08-12
4	2024-08-11 00:16:22	Zyxel Security Report	2024-08-10-2024-08-11
5	2024-08-10 00:15:37	Zyxel Security Report	2024-08-09-2024-08-10
6	2024-08-09 00:15:28	Zyxel Security Report	2024-08-08-2024-08-09
7	2024-08-08 00:20:29	Zyxel Security Report	2024-08-07-2024-08-08
8	2024-08-07 00:19:46	Zyxel Security Report	2024-08-06-2024-08-07

The following table describes the labels on this screen.

Table 36 History > Report > All Reports

LABEL	DESCRIPTION
Latest Reports	Get a summary report of activities in HTML or PDF format. **Latest Reports** are classified according to the following: • Daily Report • Weekly Report • Monthly Report Clicking any of the above will allow you to view the report online. You can then download it in PDF format or print it.
History Reports	This displays the type of report by clicking on the tab. • Daily Report • Weekly Report • Monthly Report
Time	This displays the reports in order of the date and time they were created, starting with the most recent one.
Title	This displays the title of each report as configured in **Report Settings**.

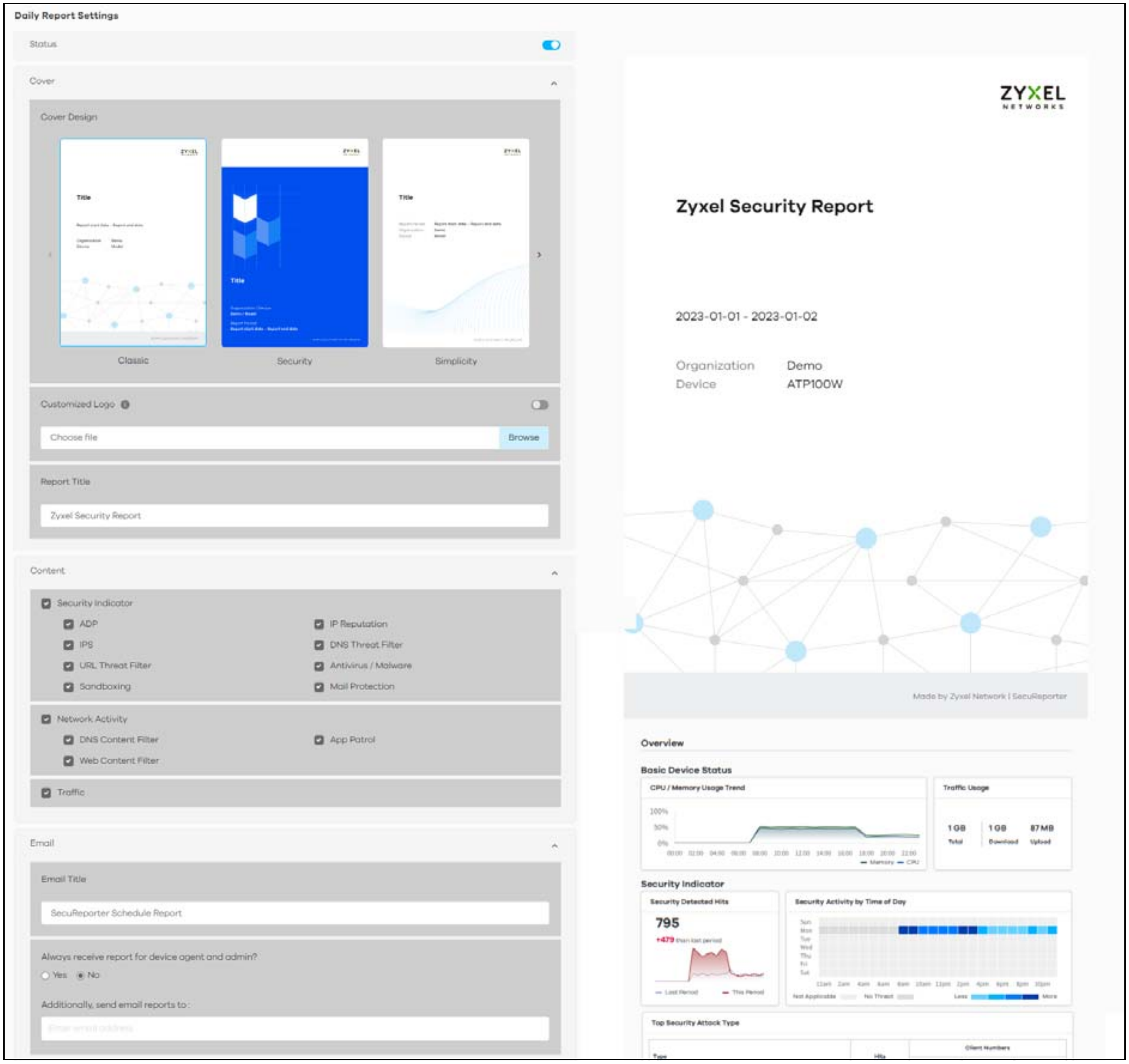
Table 36 History > Report > All Reports (continued)

LABEL	DESCRIPTION
Report Period	This displays the date that the report covers. For a daily type of report a range of two consecutive dates will be displayed. For a weekly type of report a range of seven consecutive dates will be displayed. For a monthly type of report a range of 30 consecutive dates will be displayed.
Action	Click a row to display the report online. You can then download it in PDF format or print it. Click ⋖ to send a report in PDF format to the designated email recipients. Enter an email address and press **Enter**. Note: You can configure up to 30 email addresses. Click ⬇ to save a report in PDF format to your computer. Upon clicking (Download), you will be asked where you want to save the report in your computer.

5.3 Report Settings

Click **History** > **Report** > **Report Settings** to enable or disable a report profile, and configure what to include in your customized report. You can also make changes to existing report configurations.

Figure 42 History > Report > Report Settings



Daily Report Settings

Status

Cover

Cover Design

Classic Security Simplicity

Customized Logo

Choose file Browse

Report Title

Zyxel Security Report

Content

☑ Security Indicator

☑ ADP ☑ IP Reputation

☑ IPS ☑ DNS Threat Filter

☑ URL Threat Filter ☑ Antivirus / Malware

☑ Sandboxing ☑ Mail Protection

☑ Network Activity

☑ DNS Content Filter ☑ App Patrol

☑ Web Content Filter

☑ Traffic

Email

Email Title

SecuReporter Schedule Report

Always receive report for device agent and admin?

○ Yes ● No

Additionally, send email reports to :

Enter email address

ZYXEL NETWORKS

Zyxel Security Report

2023-01-01 - 2023-01-02

Organization Demo
Device ATP100W

Made by Zyxel Network | SecuReporter

Overview

Basic Device Status

CPU / Memory Usage Trend

Traffic Usage

1 GB Total | 1 GB Download | 87 MB Upload

Security Indicator

Security Detected Hits

795

+479 than last period

Security Activity by Time of Day

Top Security Attack Type

The following table describes the labels on this screen.

Table 37 History > Report > Report Settings

LABEL	DESCRIPTION
Status	Click the button to enable or disable the scheduled report.
Cover	
Cover Design	Select a cover style for your report.
Customized Logo	Click the button to show or hide the logo you uploaded. Click **Browse** and select a graphic in JPG, PNG, or GIF format that is smaller than 100KB to use as your logo. This logo will be displayed on the cover page of the report.
Report Title	Enter a title to display on the cover page of your report. You can enter up to 144 characters.
Content	The widgets are the security services and traffic indicators that you can select to be included in the report profile. Refer to Chapter 2 Analysis for a description of the widgets. Click an item (with check mark) to include it in the report profile.

Table 37 History > Report > Report Settings (continued)

LABEL	DESCRIPTION
Email	
Email Title	This field allows you to enter a descriptive name for the report title (for example Zyxel Security Report). Up to 255 characters are allowed for the **Email Title** including special characters inside the square quotes [~!@#$%^&*()_+{} | :"<>?-=[] \;',./].
Always receive report for device agent and admin?	Select **Yes** to enable the sending of a report in PDF format to the Zyxel Device's agent and admin. Refer to Table 3 on page 7 for the privileges of agent and admin. Note: **No** must be selected if agent and admin do not wish to receive the report through email. A summary of activities over the selected period of time is still generated.
Additionally, send email reports to:	This field allows you to enter the report's designated email recipients other than the Zyxel Device's agent and admin. Use a comma (,) to separate the email addresses with no space in between two email addresses. A maximum of 30 email recipients is allowed. (Example: adam@zyxel.com, brenda@zyxel.com)
Cancel	Click **Cancel** to restore your previously saved settings.
Save	Click **Save** to save your changes.

CHAPTER 6
Settings

6.1 Overview

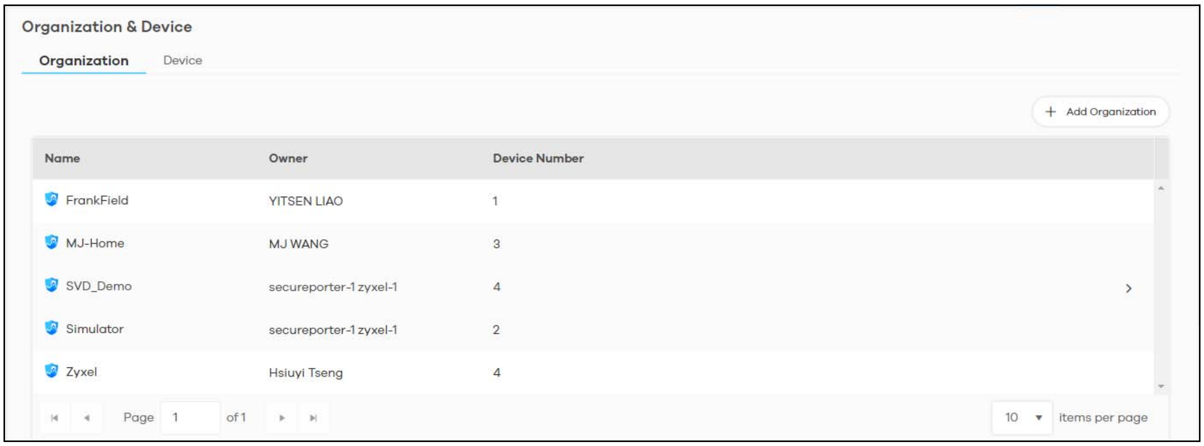
First, register your Zyxel Device at *myZyxel.com*, activate the SecuReporter license, and enable SecuReporter in the Zyxel Device using its Web Configurator or commands. You can then add your Zyxel Device to an organization at the SecuReporter web portal.

Note: Only the Zyxel Device owner, that is the person who has registered the Zyxel Device at *myZyxel.com*, and activated the SecuReporter license, can add a Zyxel Device to an organization. See Table 3 on page 7 for details on management privileges.

6.2 Organization & Device

In (More) ⋯ (upper right icon) > **Organization & Device**, you see all organizations that you have already created. You do not see organizations other people created.

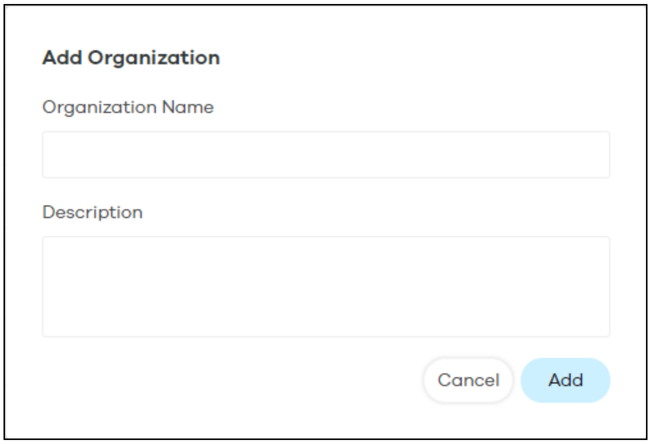
1 Click **Add Organization** to create a new organization.



Organization & Device

Name	Owner	Device Number
FrankField	YITSEN LIAO	1
MJ-Home	MJ WANG	3
SVD_Demo	secureporter-1 zyxel-1	4
Simulator	secureporter-1 zyxel-1	2
Zyxel	Hsiuyi Tseng	4

2 Enter a name of up to 255 characters and description for the organization.



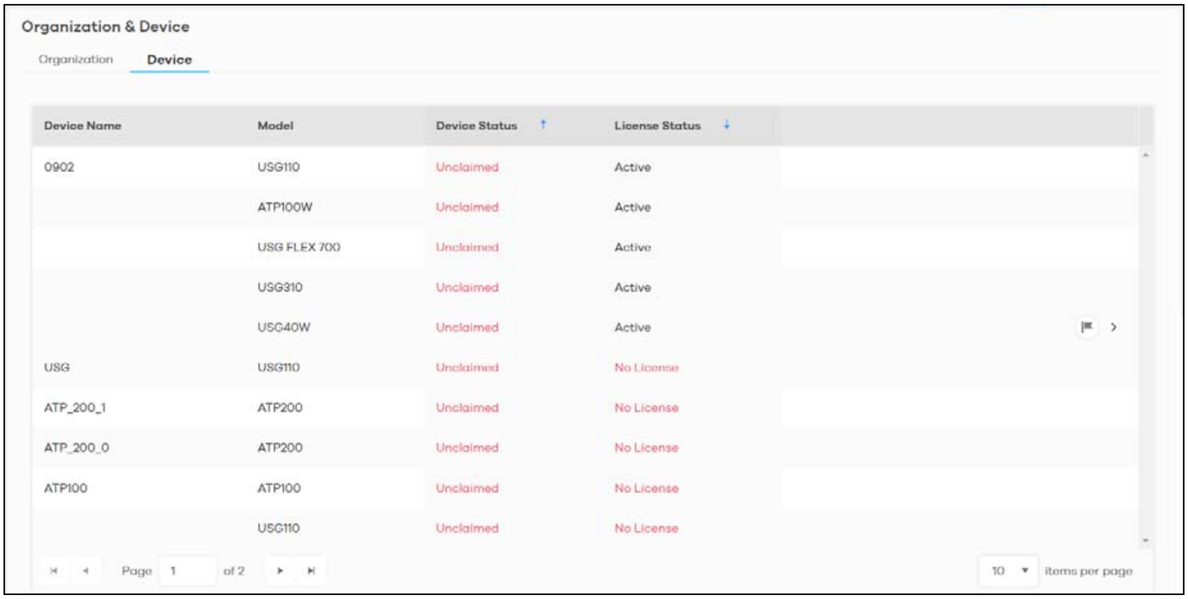
Add Organization

Organization Name

Description

6.2.1 Add a Zyxel Device to an Organization

On the **Device** tab, the hyperlink under **Unclaimed** displays the Zyxel Devices that are available to be added to this organization by the Zyxel Device owner.



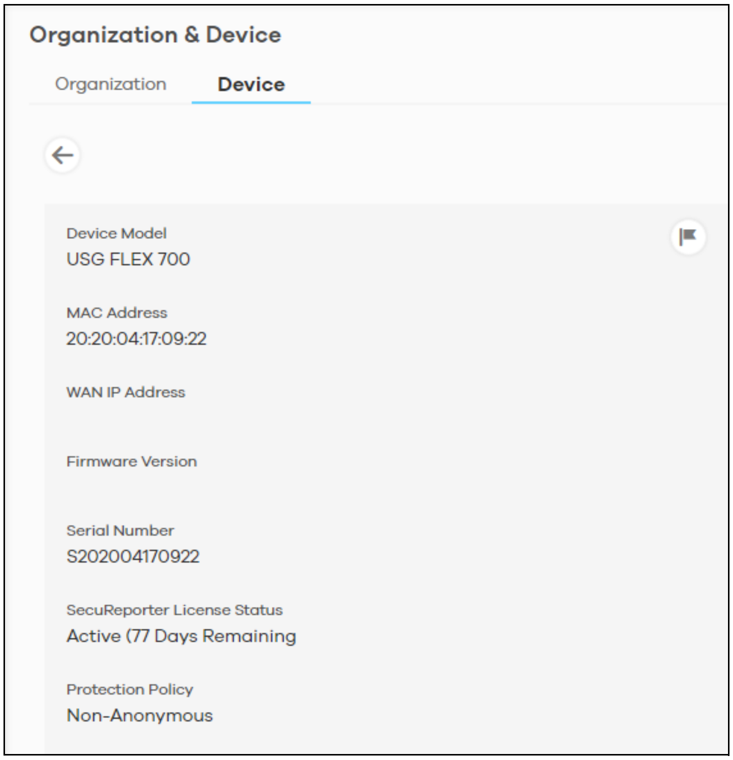
Organization & Device

Device Name	Model	Device Status ↑	License Status ↓
0902	USG110	Unclaimed	Active
	ATP100W	Unclaimed	Active
	USG FLEX 700	Unclaimed	Active
	USG310	Unclaimed	Active
	USG40W	Unclaimed	Active
USG	USG110	Unclaimed	No License
ATP_200_1	ATP200	Unclaimed	No License
ATP_200_0	ATP200	Unclaimed	No License
ATP100	ATP100	Unclaimed	No License
	USG110	Unclaimed	No License

Page 1 of 2

10 items per page

1 Click the hyperlink under **Unclaimed** to add Zyxel Devices to this organization. You will see details of Zyxel Devices that are available to be added.



Organization & Device

Organization Device

Device Model
USG FLEX 700

MAC Address
20:20:04:17:09:22

WAN IP Address

Firmware Version

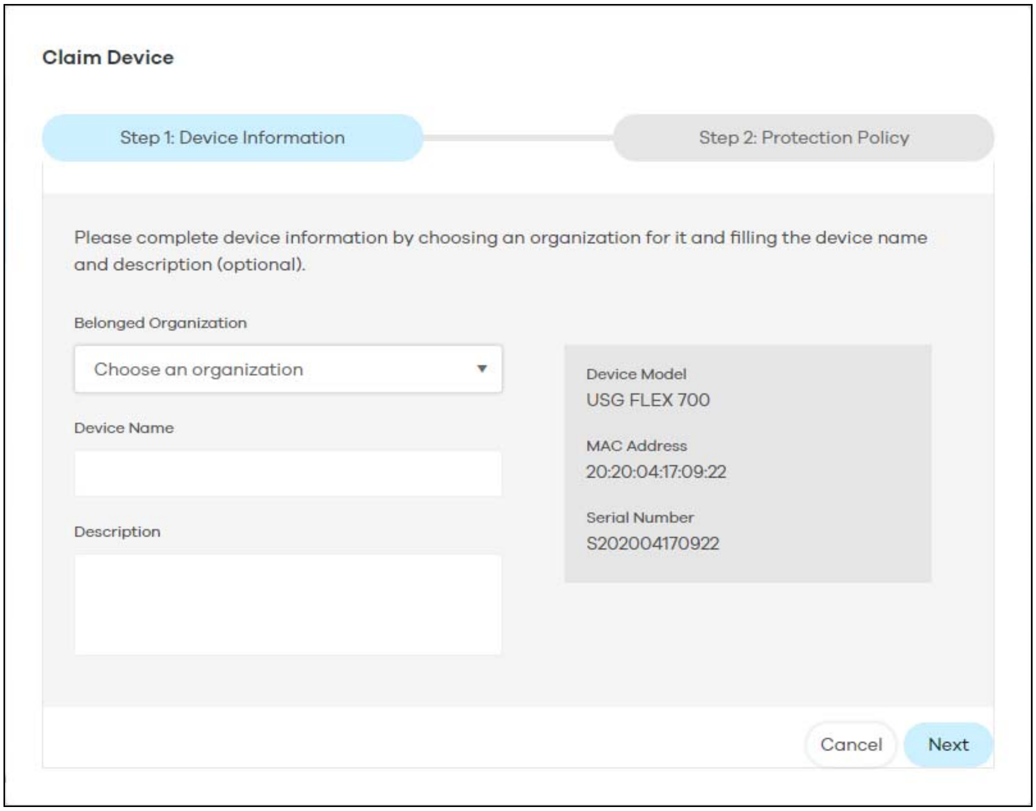
Serial Number
S202004170922

SecuReporter License Status
Active (77 Days Remaining

Protection Policy
Non-Anonymous

2 You will see the ⚑ icon on the right when you hover the mouse on the registered Zyxel Devices that have activated SecuReporter licenses. This icon will not appear for registered Zyxel Devices that do not have activated SecuReporter license.

3 Click the ⚑ icon to add the Zyxel Device into this organization. Enter an identifying name for this Zyxel Device in **Device Name** and an optional **Description**, and then click **Next**.



Claim Device

Please complete device information by choosing an organization for it and filling the device name and description (optional).

Belonged Organization: Choose an organization ▾

Device Name:

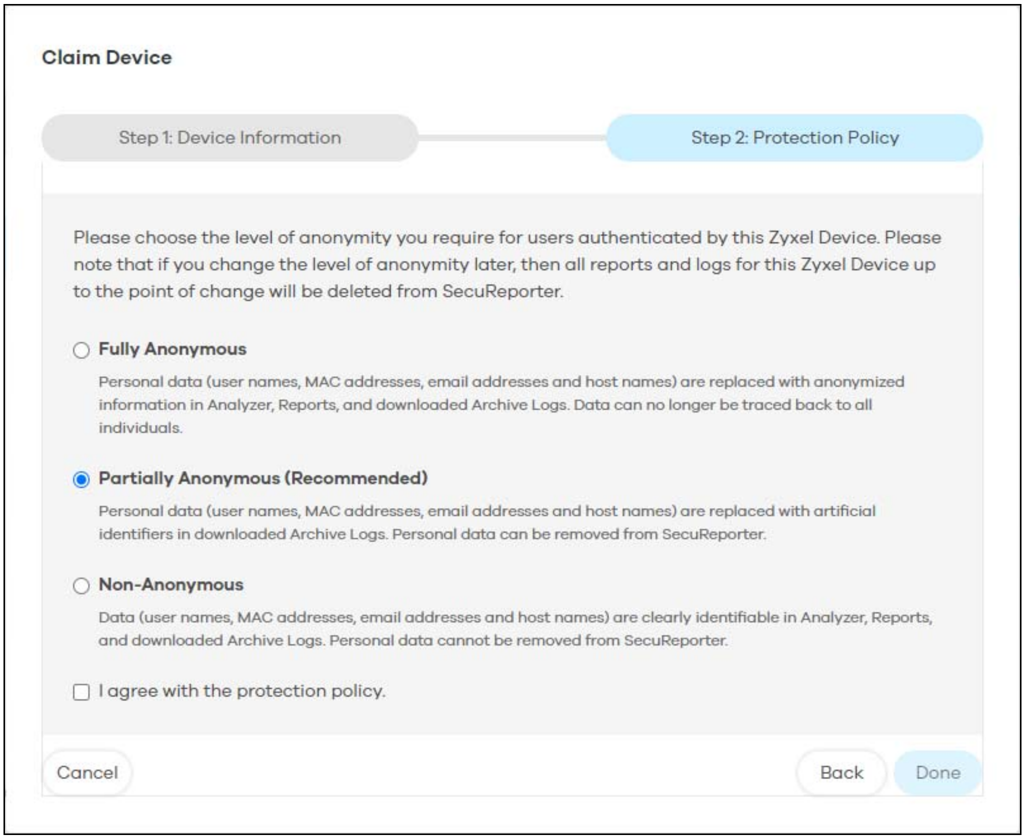
Description:

Device Model: USG FLEX 700

MAC Address: 20:20:04:17:09:22

Serial Number: S202004170922

4 Read the data protection policy and then choose the level of data protection for traffic going through this Zyxel Device. Finally click **Save** to have the **Unclaimed** device become a **Claimed** device.



Please choose the level of anonymity you require for users authenticated by this Zyxel Device. Please note that if you change the level of anonymity later, then all reports and logs for this Zyxel Device up to the point of change will be deleted from SecuReporter.

○ **Fully Anonymous**

Personal data (user names, MAC addresses, email addresses and host names) are replaced with anonymized information in Analyzer, Reports, and downloaded Archive Logs. Data can no longer be traced back to all individuals.

● **Partially Anonymous (Recommended)**

Personal data (user names, MAC addresses, email addresses and host names) are replaced with artificial identifiers in downloaded Archive Logs. Personal data can be removed from SecuReporter.

○ **Non-Anonymous**

Data (user names, MAC addresses, email addresses and host names) are clearly identifiable in Analyzer, Reports, and downloaded Archive Logs. Personal data cannot be removed from SecuReporter.

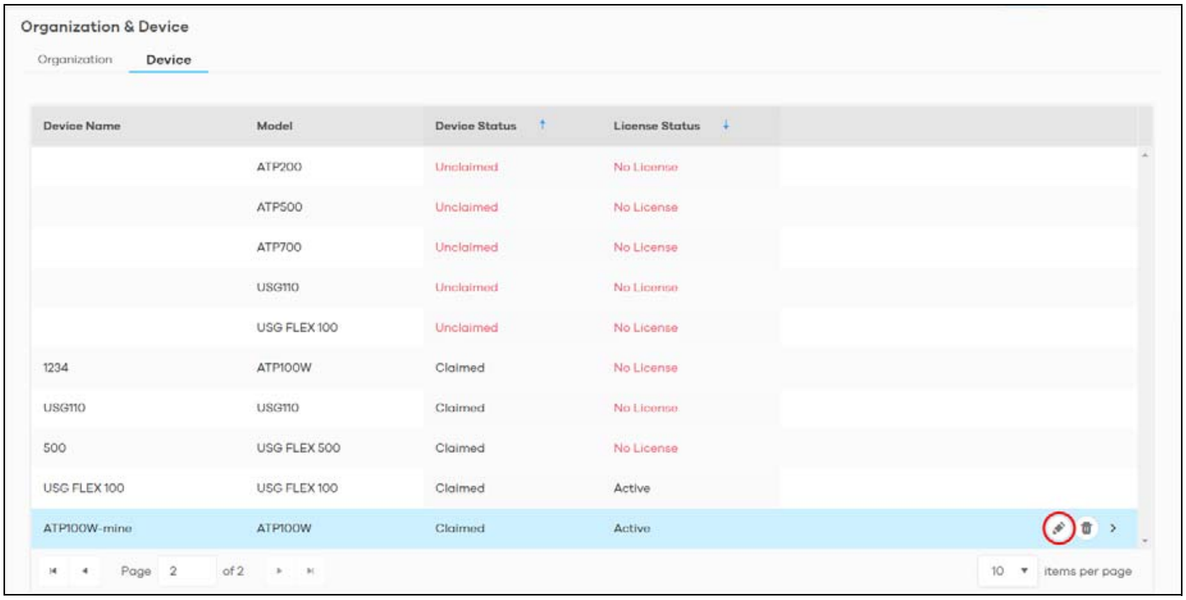
□ I agree with the protection policy.

Note: You can change the level of data protection later, but all logs and reports created for the Zyxel Device up to that point will be lost.

To hide the user name or email address of an existing record set as **Partially Anonymous**.

6.2.2 Claimed Device

The hyperlink under **Claimed** device displays the Zyxel Devices that have been added to this organization. Click the edit ✎ icon to change the settings including the **Protection Policy**.



Organization & Device

Organization | Device

Device Name	Model	Device Status ↑	License Status ↓
	ATP200	Unclaimed	No License
	ATP500	Unclaimed	No License
	ATP700	Unclaimed	No License
	USG110	Unclaimed	No License
	USG FLEX 100	Unclaimed	No License
1234	ATP100W	Claimed	No License
USG110	USG110	Claimed	No License
500	USG FLEX 500	Claimed	No License
USG FLEX 100	USG FLEX 100	Claimed	Active
ATP100W-mine	ATP100W	Claimed	Active

Page 2 of 2

10 items per page

6.2.3 Generate API Token

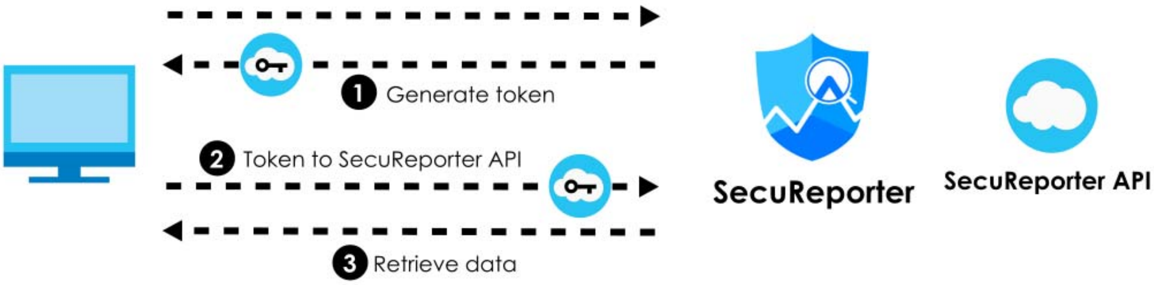
An API (Application Programming Interface) token is a secret string that verifies a user's access to API resources, allowing one software application to share data with another.

You can generate an API token on SecuReporter to securely share the data on SecuReporter with a third-party software application.

Overview of API Authorization

The following figure shows the process of generating an API token and using it to grant a third-party software application access to SecuReporter data.

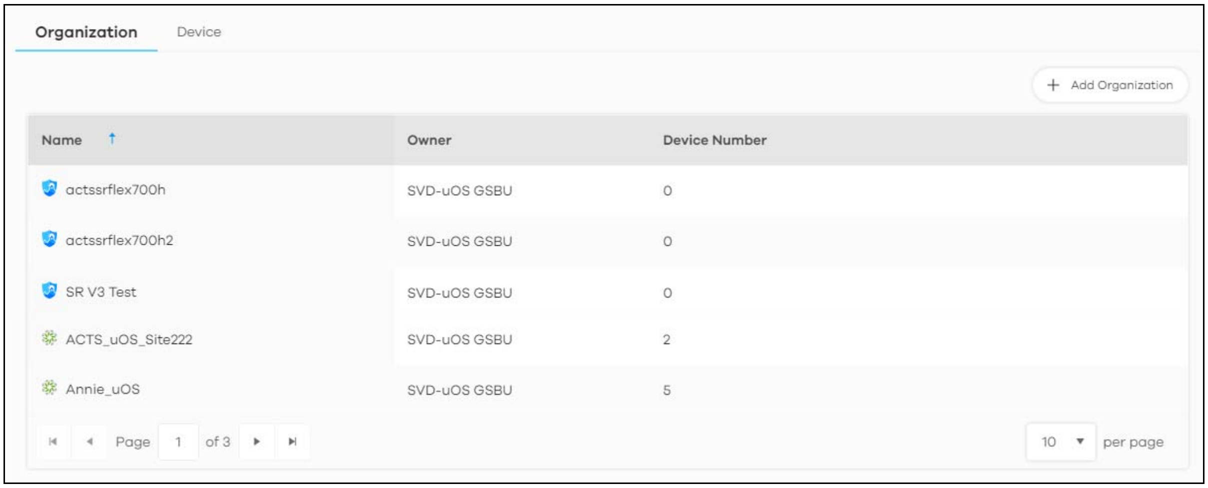
Figure 43 Overview of API Authorization



Generate an API token

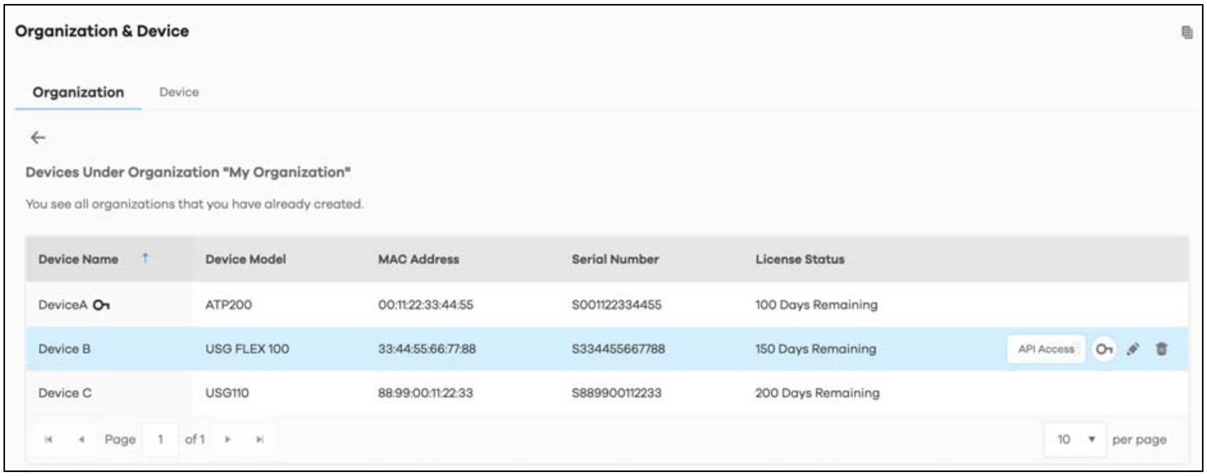
To generate an API token, click **More** ⋯ (upper right icon) > **Organization & Device** > **Organization**.

1 Click on the organization to which the Zyxel Device you want to share data with belongs.



Name	Owner	Device Number
actssrflex700h	SVD-uOS GSBU	0
actssrflex700h2	SVD-uOS GSBU	0
SR V3 Test	SVD-uOS GSBU	0
ACTS_uOS_Site222	SVD-uOS GSBU	2
Annie_uOS	SVD-uOS GSBU	5

2 Click the **API Access** button next to the Zyxel Device you want to share data with. Make sure the Zyxel Device has a valid device license.

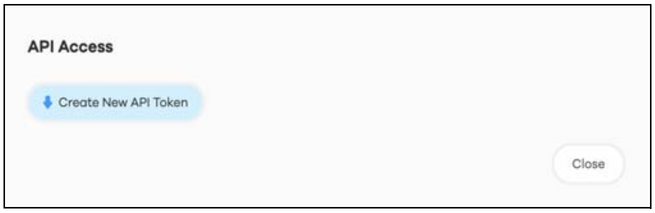


Devices Under Organization "My Organization"

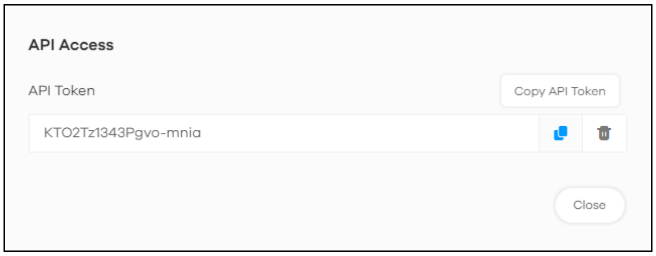
You see all organizations that you have already created.

Device Name	Device Model	MAC Address	Serial Number	License Status
DeviceA	ATP200	00:11:22:33:44:55	S001122334455	100 Days Remaining
Device B	USG FLEX 100	33:44:55:66:77:88	S334455667788	150 Days Remaining
Device C	USG110	88:99:00:11:22:33	S889900112233	200 Days Remaining

3 The following window pops up. Click **Create New API Token** to generate a secret string.



4 Click **Copy API Token** to copy the API token and paste it into a third-party program to authorize access to SecuReporter data.



KTO2Tz1343Pgvo-mnia

Send the API Token to SecuReporter API

The API token acts as a secure way to authenticate your request. By sending the API token to the SecuReporter API, you verify that your request is coming from an authorized source. See page 106 to see what to do if your API request is rejected.

5 Store the token securely and test your API request to ensure that the API token and request setup are correct.

6 Send the API request from the third-party application to the SecuReporter API to verify authorization.

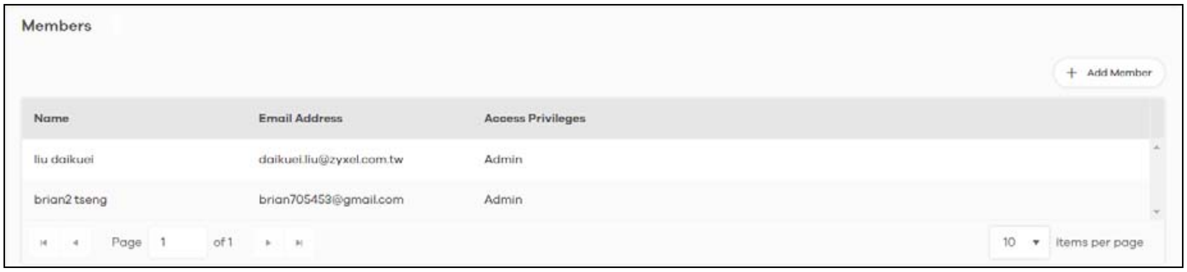
Retrieve SecuReporter Data

7 After your request is verified by the SecuReporter API, The SecuReporter data will be downloaded to your server.

6.3 User Account

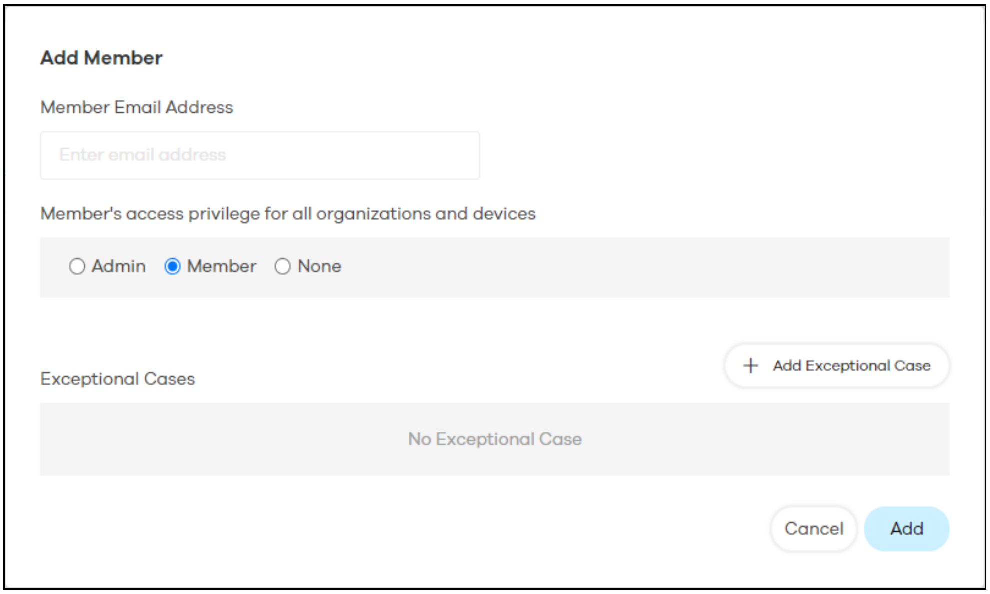
To assign an administrator or user for organizations or Zyxel Devices within organizations that you created, click (More) ⋯ (upper right icon) > **Members**.

1 Click **Add Member**.



Name	Email Address	Access Privileges
liu daikuei	daikuei.liu@zyxel.com.tw	Admin
brian2 tseng	brian705453@gmail.com	Admin

2 Enter the email address of the person that you want to be administrator in **Member Email Address**.


Add Member

Member Email Address

Enter email address

Member's access privilege for all organizations and devices

○ Admin ● Member ○ None

Exceptional Cases

No Exceptional Case

You cannot change the email address later. You have to delete this user account and create a new one to create a different email address. Also, you cannot add your own email address.

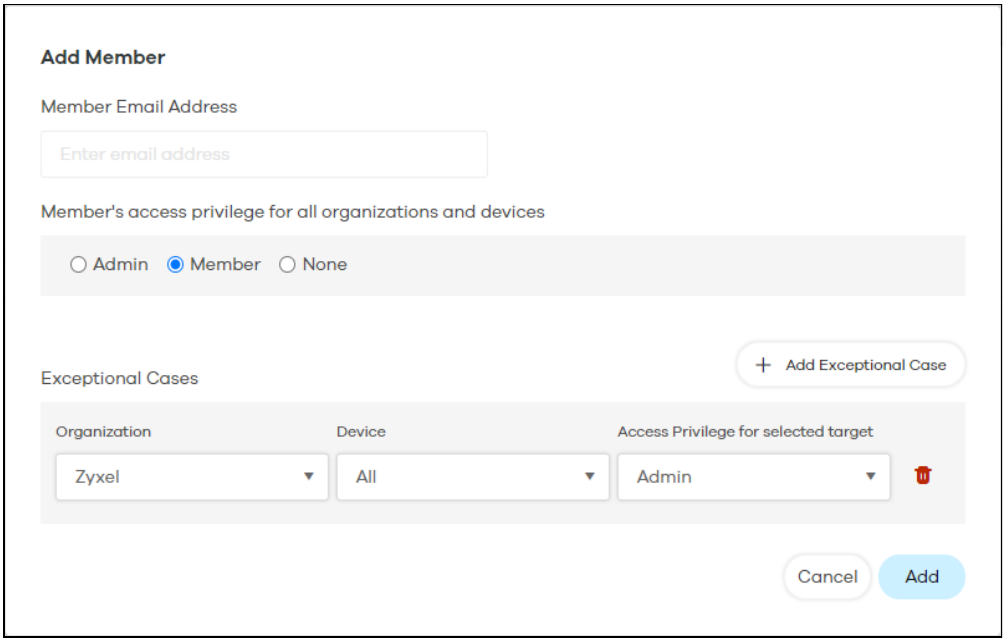
3 Select this **Member's access privilege for all organizations and devices** for all new Zyxel Devices added to this organization after the user account was created.

- Select **Admin** if you want this user to have full administration privileges for all new Zyxel Devices added to this organization after the user account was created.
- Select **Member** if you want this user to have restricted administration privileges for all new Zyxel Devices added to this organization after the user account was created.
- Select **None** if you do not want this user to see new Zyxel Devices added to this organization after the user account was created.

You may configure **Exceptional Cases** by clicking **Add Exceptional Case** for individual Zyxel Devices within this organization.

The administration privilege priority for exceptional cases field checking is as below:

- Device
- Organization
- Access Privilege for selected target



Add Member

Member Email Address

Member's access privilege for all organizations and devices

○ Admin ● Member ○ None

Exceptional Cases

Organization	Device	Access Privilege for selected target
Zyxel	All	Admin

Note: See Table 3 on page 7 for details on management privileges.

4 Click **Add** when finished.

CHAPTER 7 Troubleshooting

This chapter offers some suggestions to solve problems you might encounter.

I cannot access the SecuReporter portal.

- Check that you are using the correct URL: *https://secureporter.cloudcnm.zyxel.com*
- Make sure your computer's Ethernet card is installed and functioning properly.
- Check that you have Internet access. Open **Command Prompt** on your computer, enter 'ping' followed by a website such as 'zyxel.com'. If you get a reply try to ping 'secureporter.cloudcnm.zyxel.com'.
- Use a browser that supports HTML5, such as Google Chrome, Mozilla Firefox, Safari, or Microsoft Edge. The recommended minimum screen resolution is 1366 by 768 pixels. In order to use SecuReporter you need to allow web browser pop-up windows from your computer.

I cannot log into the SecuReporter portal.

- Open your web browser and go to *https://secureporter.cloudcnm.zyxel.com*. Sign in with the correct email and password. Click **Create an account** if you do not have a Zyxel Account to sign up.

There is no data shown at SecuReporter.

- Make sure your Zyxel Device supports SecuReporter. See Section 1.1.1 on page 6 for the supported Zyxel Devices.
- Make sure the firmware version of your Zyxel Device supports SecuReporter. See Section 1.1.1 on page 6 for the supported firmware versions.
- Make sure you activated the SecuReporter license at myZyxel. See Section 1.2 on page 8 for more information.
- Make sure your license is not expired. See the User's Guide of the supported Zyxel Device for how to check your license status.
- Make sure you enabled SecuReporter on your Zyxel Device. See the User's Guide of the supported Zyxel Device for how to enable and activate SecuReporter.
- Make sure you selected the categories that you want your Zyxel Device to send to the SecuReporter portal. See the User's Guide of the supported Zyxel Device for instructions.
- Make sure you added your Zyxel Device to an organization. See Section 6.2 on page 94 or the User's Guide of the supported Zyxel Device for instructions.

SecuReporter does not show the sandboxing screens.

Make sure that your Zyxel Device supports sandboxing. See Table 2 on page 7 for the Zyxel Devices that support sandboxing.

Some files types cannot be inspected through sandboxing.

Sandbox can only check the types of files listed under **File Submission Options** in the **Sandboxing** screen of the Zyxel Device. See the User's Guide of the Zyxel Device that supports sandboxing for instructions.

I want to prevent malicious code from passing through my web browser, therefore allowing cyber criminals to run malicious code on my computer.

1. Upgrade your web browser to the latest version.
2. Make sure you enable **URL Blocking** under **Configuration** > **Security Service** > **Reputation Filter** > **URL Threat Filter** > **General** on your Zyxel Device's Web Configurator. See the User's Guide of the Zyxel Device that supports URL Threat Filter for instructions.

My Top Type and Top Threat Website charts are not showing any data.

Make sure you enable **URL Blocking** under **Configuration** > **Security Service** > **Reputation Filter** > **URL Threat Filter** > **General** on your Zyxel Device's Web Configurator. See the User's Guide of the Zyxel Device that supports URL Threat Filter for instructions.

IP Reputation does not work on IPv6 addresses.

At the time of writing, IP Reputation is only for IPv4 addresses.

My Top Type and Top Risk IP charts are not showing any data.

Make sure you enable **IP Blocking** under **Configuration** > **Security Service** > **Reputation Filter** > **IP Reputation** > **General** on your Zyxel Device's Web Configurator. See the User's Guide of the Zyxel Device that supports URL Threat Filter for instructions.

I cannot add my Zyxel Device to an organization.

Only an owner can add Zyxel Devices to an organization. See Section 1.1.2 on page 7 for the privileges of different role types.

Some fields cannot be used as filters for search log.

For **Partially Anonymous** users, search log for some of the fields are disabled.

I get a **Number of logs in query exceeded the maximum limit** warning.

A maximum of 10,000 search results are only allowed at a time. Add filters to narrow down the search log criteria.

I want to use a wildcard when entering the filter criteria for a field in search log.

Upon clicking ▼ > **Add Rule** > **Please Select**, the word **contains** should appear after the name of the field, not '**=**'.

I failed to retrieve SecuReporter logs through API in a third-party software application.

- **Check API token**: Ensure that the API token is correct and has not expired. If needed, generate a new token and try again.
- **Check API request format**: Review the API request for any errors or formatting issues. Refer to *https://www.zyxel.com/global/en/products/management-and-reporting/management-and-reporting-cloud-cnm-secureporter/open-api* for more information on API request format.
- **Verify license status**: Ensure that the Zyxel device's license is valid.

7.1 Getting More Troubleshooting Help

Search for support information for your model at *www.zyxel.com* for more troubleshooting suggestions.

APPENDIX A
Customer Support

In the event of problems that cannot be solved by using this manual, you should contact your vendor. If you cannot contact your vendor, then contact a Zyxel office for the region in which you bought the device.

For Zyxel Communication offices, see *https://service-provider.zyxel.com/global/en/contact-us* for the latest information.

For Zyxel Network offices, see *https://www.zyxel.com/index.shtml* for the latest information.

Please have the following information ready when you contact an office.

Required Information

- Product model and serial number.
- Warranty Information.
- Date that you received your device.
- Brief description of the problem and the steps you took to solve it.

Corporate Headquarters (Worldwide)

Taiwan

- Zyxel Communications (Taiwan) Co., Ltd.
- *https://www.zyxel.com*

Asia

China

- Zyxel Communications Corporation–China Office
- *https://www.zyxel.com/cn/sc*

India

- Zyxel Communications Corporation–India Office
- *https://www.zyxel.com/in/en-in*

Kazakhstan

- Zyxel Kazakhstan
- *https://www.zyxel.com/ru/ru*

Korea

- Zyxel Korea Co., Ltd.
- *http://www.zyxel.kr/*

Malaysia

- Zyxel Communications Corp.
- *https://www.zyxel.com/global/en*

Philippines

- Zyxel Communications Corp.
- *https://www.zyxel.com/global/en*

Singapore

- Zyxel Communications Corp.
- *https://www.zyxel.com/global/en*

Taiwan

- Zyxel Communications (Taiwan) Co., Ltd.
- *https://www.zyxel.com/tw/zh*

Thailand

- Zyxel Thailand Co., Ltd.
- *https://www.zyxel.com/th/th*

Vietnam

- Zyxel Communications Corporation–Vietnam Office
- *https://www.zyxel.com/vn/vi*

Europe

Belarus

- Zyxel Communications Corp.
- *https://www.zyxel.com/ru/ru*

Belgium (Netherlands)

- Zyxel Benelux
- *https://www.zyxel.com/nl/nl*
- *https://www.zyxel.com/fr/fr*

Bulgaria

- Zyxel Bulgaria

- *https://www.zyxel.com/bg/bg*

Czech Republic

- Zyxel Communications Czech s.r.o.
- *https://www.zyxel.com/cz/cs*

Denmark

- Zyxel Communications A/S
- *https://www.zyxel.com/dk/da*

Finland

- Zyxel Communications
- *https://www.zyxel.com/fi/fi*

France

- Zyxel France
- *https://www.zyxel.com/fr/fr*

Germany

- Zyxel Deutschland GmbH.
- *https://www.zyxel.com/de/de*

Hungary

- Zyxel Hungary & SEE
- *https://www.zyxel.com/hu/hu*

Italy

- Zyxel Communications Italy S.r.l.
- *https://www.zyxel.com/it/it*

Norway

- Zyxel Communications A/S
- *https://www.zyxel.com/no/no*

Poland

- Zyxel Communications Poland
- *https://www.zyxel.com/pl/pl*

Romania

- Zyxel Romania
- *https://www.zyxel.com/ro/ro*

Russian Federation

- Zyxel Communications Corp.
- *https://www.zyxel.com/ru/ru*

Slovakia

- Zyxel Slovakia
- *https://www.zyxel.com/sk/sk*

Spain

- Zyxel Iberia
- *https://www.zyxel.com/es/es*

Sweden

- Zyxel Communications A/S
- *https://www.zyxel.com/se/sv*

Switzerland

- Studerus AG
- *https://www.zyxel.com/ch/de-ch*
- *https://www.zyxel.com/fr/fr*

Turkey

- Zyxel Turkey A.S.
- *https://www.zyxel.com/tr/tr*

UK

- Zyxel Communications UK Ltd.
- *https://www.zyxel.com/uk/en-gb*

Ukraine

- Zyxel Ukraine
- *https://www.zyxel.com/ua/uk-ua*

South America

Argentina

- Zyxel Communications Corp.
- *https://www.zyxel.com/co/es-co*

Brazil

- Zyxel Communications Brasil Ltda.

- *https://www.zyxel.com/br/pt*

Colombia

- Zyxel Communications Corp.
- *https://www.zyxel.com/co/es-co*

Ecuador

- Zyxel Communications Corp.
- *https://www.zyxel.com/co/es-co*

South America

- Zyxel Communications Corp.
- *https://www.zyxel.com/co/es-co*

Middle East

Israel

- Zyxel Communications Corp.
- *https://il.zyxel.com*

North America

USA

- Zyxel Communications, Inc. – North America Headquarters
- *https://www.zyxel.com/us/en-us*

APPENDIX B Legal Information

Copyright

Disclaimer

Zyxel does not assume any liability arising out of the application or use of any products, or software described herein. Neither does it convey any license under its patent rights nor the patent rights of others. Zyxel further reserves the right to make changes in any products described herein without notice. This publication is subject to change without notice.

Viewing Certifications

Go to *https://www.zyxel.com* to view this product's documentation and certifications.

Zyxel Limited Warranty

Zyxel warrants to the original end user (purchaser) that this product is free from any defects in material or workmanship for a specific period (the Warranty Period) from the date of purchase. The Warranty Period varies by region. Check with your vendor and/or the authorized Zyxel local distributor for details about the Warranty Period of this product. During the warranty period, and upon proof of purchase, should the product have indications of failure due to faulty workmanship and/or materials, Zyxel will, at its discretion, repair or replace the defective products or components without charge for either parts or labor, and to whatever extent it shall deem necessary to restore the product or components to proper operating condition. Any replacement will consist of a new or re-manufactured functionally equivalent product of equal or higher value, and will be solely at the discretion of Zyxel. This warranty shall not apply if the product has been modified, misused, tampered with, damaged by an act of God, or subjected to abnormal working conditions.

Note

Repair or replacement, as provided under this warranty, is the exclusive remedy of the purchaser. This warranty is in lieu of all other warranties, express or implied, including any implied warranty of merchantability or fitness for a particular use or purpose. Zyxel shall in no event be held liable for indirect or consequential damages of any kind to the purchaser.

To obtain the services of this warranty, contact your vendor. You may also refer to the warranty policy for the region in which you bought the device at *https://www.zyxel.com/global/en/support/warranty-information*.

Open Source Licenses

This product may contain in part some free software distributed under GPL license terms and/or GPL-like licenses.

To request the source code covered under these licenses, please go to: *https://www.zyxel.com/form/gpl_oss_software_notice.shtml.*

Index

A

account name
  view 10
administration privilege
  prioriy 102
ADP
  hits 14, 26
ADP data visualization 25
ADP screen 26
advanced persistent threat (APT) 18
Advanced Zyxel Sandbox Inspection 19
alert
  SecuReporter 82
  severity 84
alert notification
  interval 85
Alert screen 82
Alert Settings screen 84
Alerts Detected 12
allowed application
  hits 53
Analysis 15
anomaly detection 30
Anomaly Detection and Prevention (ADP) 24
anti malware
  data visualization 42
  filter rule 68
Anti Malware screen 19, 44
anti virus
  data visualization 42
Anti Virus screen 44
anti-malware scanner
  run 20
app list
  view 9
app patrol data visualization 51
App Patrol screen 53
application
  with most bandwidth usage 14, 57
application category name
  filter rule 70, 73
application name
  filter rule 70, 73, 76
assign IP
  filter rule 78
attack
  destination of threat 12
  source of threat 12
  time period percentage 12
attack type 12
  percentage 12

B

blocked application
  hits 53

C

cache
  Zyxel Device 19
category name
  filter rule 69
certifications
  viewing 112
Circle web site 10
claimed Zyxel Device 98
Cloud CNM suite 6
cloud sandboxing
  results 19
cloud-based analytics tool 6
CNAME (Canonical Name) 34
configuration
  report 91
connection duration 76
contact information 107
copyright 112

countries
received most data traffic from Zyxel Device 14, 57
CSV file 66, 72, 75, 77
CSV format 61
customer support 107

D

Dark Mode 9
Dashboard screen 12
data protection
change level 98
data protection policy 68, 73, 76, 78, 97
Defend Center
for malware characteristics 69
destination IP
filter rule 67, 72, 75, 78
destination IP address 17
destination port
bandwidth usage 14, 57
filter rule 67, 72, 75
Device tab 95
DHCP
filter rule 78
disclaimer 112
display
Dark Mode 9
DNS (Domain Name System) 36
DNS Filter 33
filter rule 67
hits 14
DNS Filter screen 36, 37, 41
DNS query
type 33
DNS query packet 33
DNS response
fake 33
domain
filter rule 71, 74
second-level 33
top level 33
Domain Name System (DNS) server 33

E

EICAR test file 20
email alert
description 85
email protection
filter rule 68, 69
email spam
hits 14
email subject 85
event
high 85
low 85
medium 85
event category 82
event log
category 76
event notification
email list 85
Event screens 77
exceptional case
add 102

F

features
supported list 6
File Submission Options 19
file type
filter rule 69
filename
filter rule 70
filter rule
anti malware 68
anti virus 68
application category name 70, 73
application name 70, 73, 76
assign IP 78
category name 69
destination IP 67, 72, 75, 78
destination port 67, 72, 75
DHCP 78
DNS Filter 67, 72, 73
domain 71, 74
email protection 68, 69

file type 69
filename 70
hash value 69
IDP/ADP 67
IP Reputation 67
query type 71, 73
risk 70
risk IP 70
role type 78
rule number 69
sandboxing 68, 69
scan result 69
score level 69
service name 78
severity 69
signature ID 68
signature name 68
source IP 67, 72, 75, 78
source port 67, 72, 75
threat category 70
threat name 70
threat type 68
time 67, 72, 75, 77
traffic protocol 76
URL 69
URL threat 67
user login 78
virus name 70
web category name 70, 73
website 71, 73
firmware version
supported 6
flow data 6
FQDN (Fully Qualified Domain Name) 33
Fully Anonymous user 68, 73
Fully Qualified Domain Name (FQDN) 33

G

grace period
expired 8
license renewal 8

H

hash value
filter rule 69
Help page
link 9
high event 85
high severity 82, 84
Hits
number of 17, 18

I

ICMP decoder 25
icon
account name 10
Circle web site 10
Help 9
list of apps 9
Marketplace 10
More 9
myZyxel web site 9
NCC web site 9
SecuReporter web site login page 9
Setting 9
Zyxel Biz Forum 10
IDP
hits 14, 32
IDP (Intrusion, Detection and Prevention) 14, 32
IDP data visualization 30
IDP profile 30
IDP screen 32
IDP/ADP
filter rule 67
inbound traffic 76
instant messenger (IM) 51, 76
IP
destination of threat 12
source of threat 12
IP address
custom 33
destination 78
source 36, 40, 44
IP Reputation
hits 14, 28

IP Reputation check
  priority 26

IP Reputation data visualization 26

IP Reputation screen 28, 29

IP Reputation service 26

IPv4 address
  reputation 26
  source 67, 72

IPv6 address 33
  source 67, 72

J

junk email
  mark or discard 46

L

layer-4 packet content 30

layer-7 packet content 30

license
  SecuReporter 9

license option 8

license status 12, 13

log
  search 61
  search privilege 65

log out
  Web Configurator 10

log search criteria 62

log search privileges 62

login attempt
  status 78

logs
  save 61
  supported Zyxel Device 6

low event 85

low severity 82, 84

M

MAC address
  corresponding IP address 79
  Zyxel Device 78

mail protection 46
  hits 48

mail protection data visualization 46

malicious file 14

malware
  hits 14, 44

malware detected
  most common 14

management
  data visualization 20

management privileges
  SecuReporter 7

map
  threat 10

Marketplace 10

medium event 85

medium severity 82, 84

member
  email address 101

Members screen 99, 101

MX (Mail eXchange) 34

myZyxel
  open account 9

myZyxel web site 9

N

NCC management level 8

NCC mode 9

NCC web site 9

Nebula Mobile app 8

network activity
  by user 79

network flooding 24

network security
  data visualization 20

network session
  length 76

Non-Anonymous user 68, 73

NS (Name Server) 34

O

organization
  add a Zyxel Device 95
  create new 94
  monitor 8
Organization tab 94
OSI (Open System Interconnection) 30
OSI layer-2 24
OSI layer-3 24
outbound traffic 76

P

packet
  destination 78
packet inspection signature 30
packet match a signature
  response 67
Partially Anonymous 98
Partially Anonymous user 68, 73
peer-to-peer (P2P) 51, 76
percentage
  of hits from source IP address 18
  of hits to destination IP address 17
pin color
  frequency of attacks 10
pin size
  threat volume 10
port scanning 24
port sweeping 24
privilege
  full administration 102
  none administrative 102
  restricted administration 102
problems 104
protocol anomaly 88
protocol anomaly detection 24
PTR (Pointer) 34

Q

query type
  filter rule 71, 73

R

real-time traffic analytics 6
report
  automatic removal 89
  configuration 91
  period 91
  SecuReporter 89
  title 90, 93
Report screen 89
Report Settings screen 91
RFCs – Requests for Comments 24
risk
  filter rule 70
risk IP
  filter rule 70
role type
  admin 7
  agent (owner) 7
  filter rule 78
  user 7
rule number
  filter rule 69

S

sandbox inspection 19
sandboxing 18
  alerts 14
  filter rule 68, 69
  turn on 20
sandboxing alerts 20
Sandboxing data visualization 44
sandboxing inspection
  supported file types 19
sandboxing log
  drop 61
  remove 61
sandboxing logs
  save criteria 61
Sandboxing screen 19, 46
sandboxing statistics 44

scan result 19
filter rule 69
score level
filter rule 69
search result
maximum 62, 66, 72, 75, 77
SecuReporter
activate license 9
enable 94
set up 8
web portal 94
SecuReporter license
activate 94, 96
SecuReporter Premium 62
SecuReporter web site login page
new tab or window 9, 10
Security 15
Security Cloud 20
security event 6
detail 84
severity level 80
security indicator 12, 13, 15, 20, 24
security log
category 65, 71
Security screens 66
service license
activate 20
service name
filter rule 78
severity
filter rule 69
high 82, 84
low 82, 84
medium 82, 84
severity level
security event 80
signature 30
malicious 30
signature ID
filter rule 68
signature name
filter rule 68
SOA (Start Of zone Authority) 34
source IP
filter rule 75, 78
source IP address 18
filter rule 67, 72
source port
filter rule 67, 72, 75
Standard license 8
streaming (RSTP) application 51
supported firmware version 6
supported model 6

T

TCP decoder 24
threat
destination IP 12
severity 82
source country 12
source IP 12
target country 12
threat category
filter rule 70
Threat Intelligence 32
threat level
threshold 70
threat map
details 11
threat name
filter rule 70
threat type
filter rule 68
time
filter rule 67, 72, 75, 77
time frame
data collection 15
report generation 89
Timestamp 90
title bar
NCC mode 9
Top Signature table 32
top users
with most bandwidth 14, 57
traffic
anomaly 88
inbound 76
outbound 76
traffic anomaly policy 24
traffic log

categories 74
traffic protocol
filter rule 76
Traffic screen 75
traffic usage 12
transport packet
type 76
Trial license 8
troubleshooting 104

U

UDP decoder 25
unclaimed Zyxel Device 95
URL
filter rule 69
URL (Uniform Resource Locator) 67
URL threat 69
hits 14
URL threat check
priority 38
URL threat domain name 38
URL threat filter 48
hits 40
top 10 17
URL Threat Filter data visualization 38
URL Threat Filter screen 15, 40
URL Threat filtering 14
URL threat IP address 38
user
user-aware 79
user login
filter rule 78

V

version number
SecuReporter 2
virtual machine (VM) 18
virus
hits 14, 44
virus name
filter rule 70
viruses detected
most common 14
Voice over IP (VoIP) 51, 76

W

warranty 112
note 112
web category name
filter rule 70, 73
Web Page Blocked! page 33
website
filter rule 71, 73
Website screen 50
Widget 12

Z

Zyxel Biz Forum 10
Zyxel Device
add to an organization 94
register 94
register at 9
supported 6
Zyxel Device cache 19