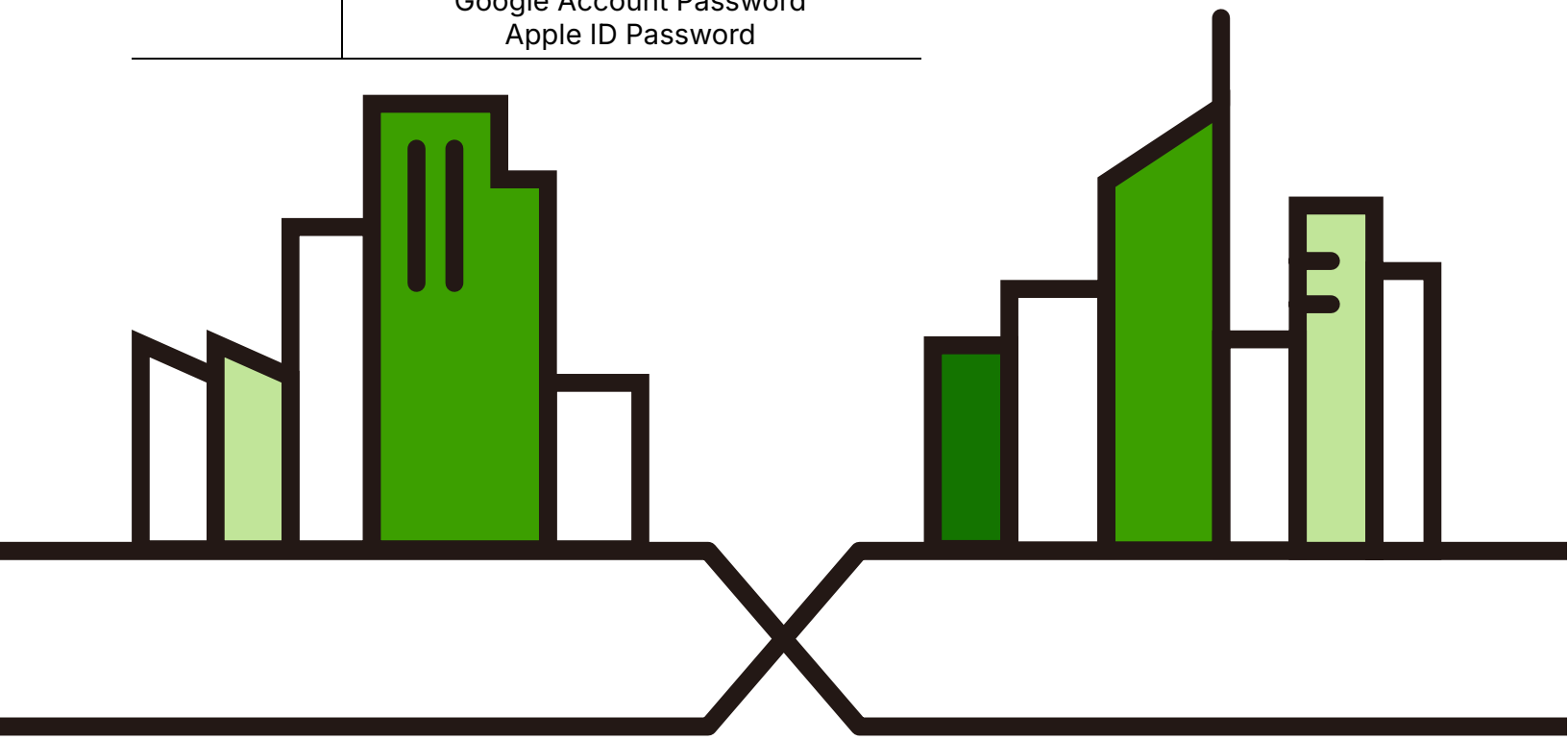
User's Guide

SecuReporter

Version 2.5.25 Edition 1, 09/2025

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 Nebula Control Center (NCC) portal to get the NCC User's Guide to see more information about SecuReporter.

- More Information

  Go to *https://www.zyxel.com/products_services/Security-Service-Cloud-CNM-SecuReporter/license-and-spec* for more information about SecuReporter.

  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

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
USG LITE 60AX (Traffic Logs only)	Version 2.20 or later

Note: SecuReporter supports log sending from the Zyxel Device managed through NCC (Nebula Control Center). Log sending is disabled by default on the Zyxel Device. To view logs in SecuReporter, you must enable logs to be sent to SecuReporter in the Web Configurator of the Zyxel Device or NCC. However, the traffic logs of the ZyWALL ATP series and USG FLEX series on-cloud models are sent to NCC and are not available in SecuReporter.

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	USG LITE 60AX SERIES
Sandboxing	Yes	Yes (with Gold Security Pack)	No	Yes	No
Reputation Filter	Yes	Yes (with Gold Security Pack)	No	Yes	Yes
Web Filtering	Yes	Yes	Yes	Yes	No
Anti-Malware	Yes	Yes	No	Yes	No
IPS	Yes	Yes	No	Yes	No
Application Patrol	Yes	Yes	No	Yes	No
Device Insight	Yes	Yes	Yes	Yes	No
Traffic Usage	Yes	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

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 Nebula Control Center (NCC). 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 access points, switches and gateways. Your network can also be managed through your smartphone using the Nebula Mobile app.

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 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 log	Yes	Yes
View security event log	Yes	Yes
View User/Device/DHCP events	Yes	Yes
View CPU/memory/session usage	No	Yes

Note: Event logs are available by default. However, traffic logs will not be generated unless you enable them. To view traffic logs in SecuReporter, you must enable traffic log sending in the Web Configurator of the Zyxel Device or through NCC.

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 *https://account.zyxel.com* and click Create an account, or sign in with your Google account, Apple account, or Microsoft Entra ID.

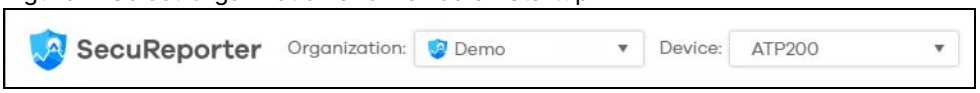
3 After you register the Zyxel Devices, follow the on-screen instructions to activate the SecuReporter license for the registered Zyxel Devices.

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

Note: See Section 2.1 on page 20 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



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 available apps provided by Zyxel.
myZyxel	Click this to open the myZyxel website login page in a new tab or window.
Nebula	Click this to open the NCC 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 in 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 SecuPilot

SecuPilot is a multilingual AI chatbot that supports more than 40 languages. It analyzes SecuReporter logs to answer security-related prompts about traffic going through your Zyxel Device and provide information on security data, traffic logs, and alerts. SecuPilot can organize data for analysis and provide charts or tables for download.

Note: You must enable SecuReporter on your Zyxel Device and have logs sent to SecuReporter in order to use SecuPilot. SecuPilot responds based on relevant logs and question clarity. The more precise your question, the better the results.

Note: At the time of writing, SecuPilot only analyzes logs from the past 7 days.

For example, if the Zyxel Device detects unusual traffic, such as high usage, you can use SecuPilot to identify the cause:

- Show traffic information for today.
- Check which applications, users, or hostnames had the highest usage during the busiest time period.

Click on the SecuPilot icon in the upper-corner of the Dashboard screen to open SecuPilot and start a conversation.

Figure 3 Dashboard

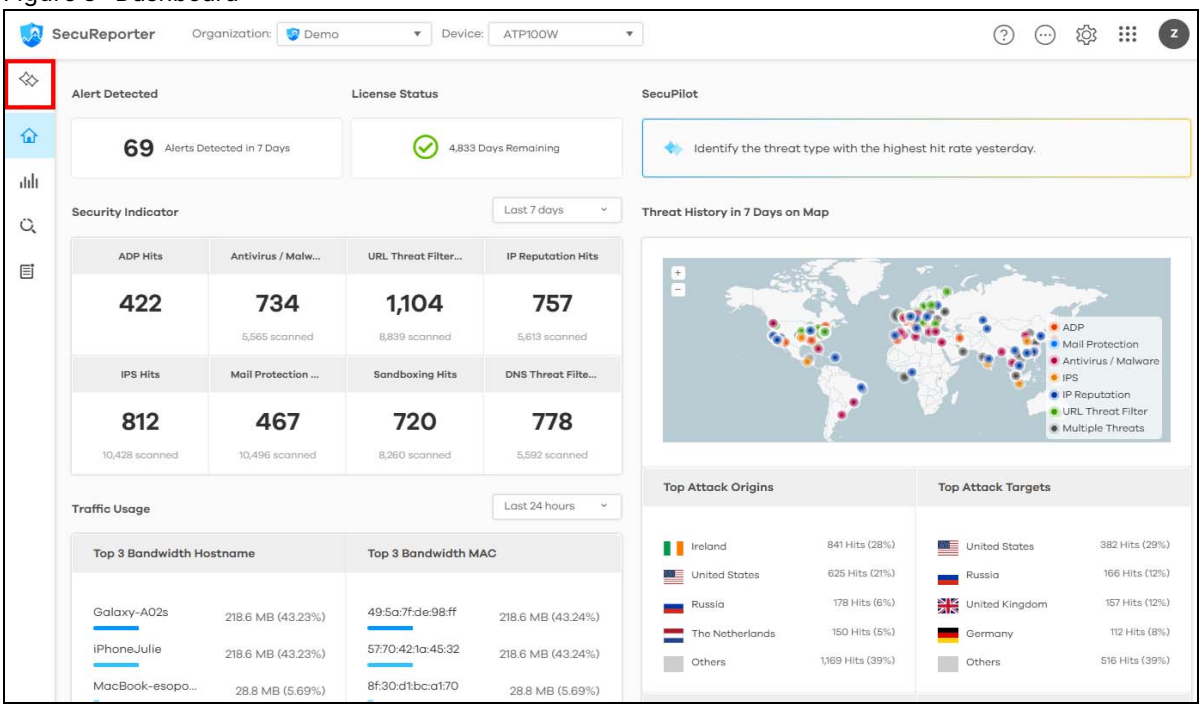
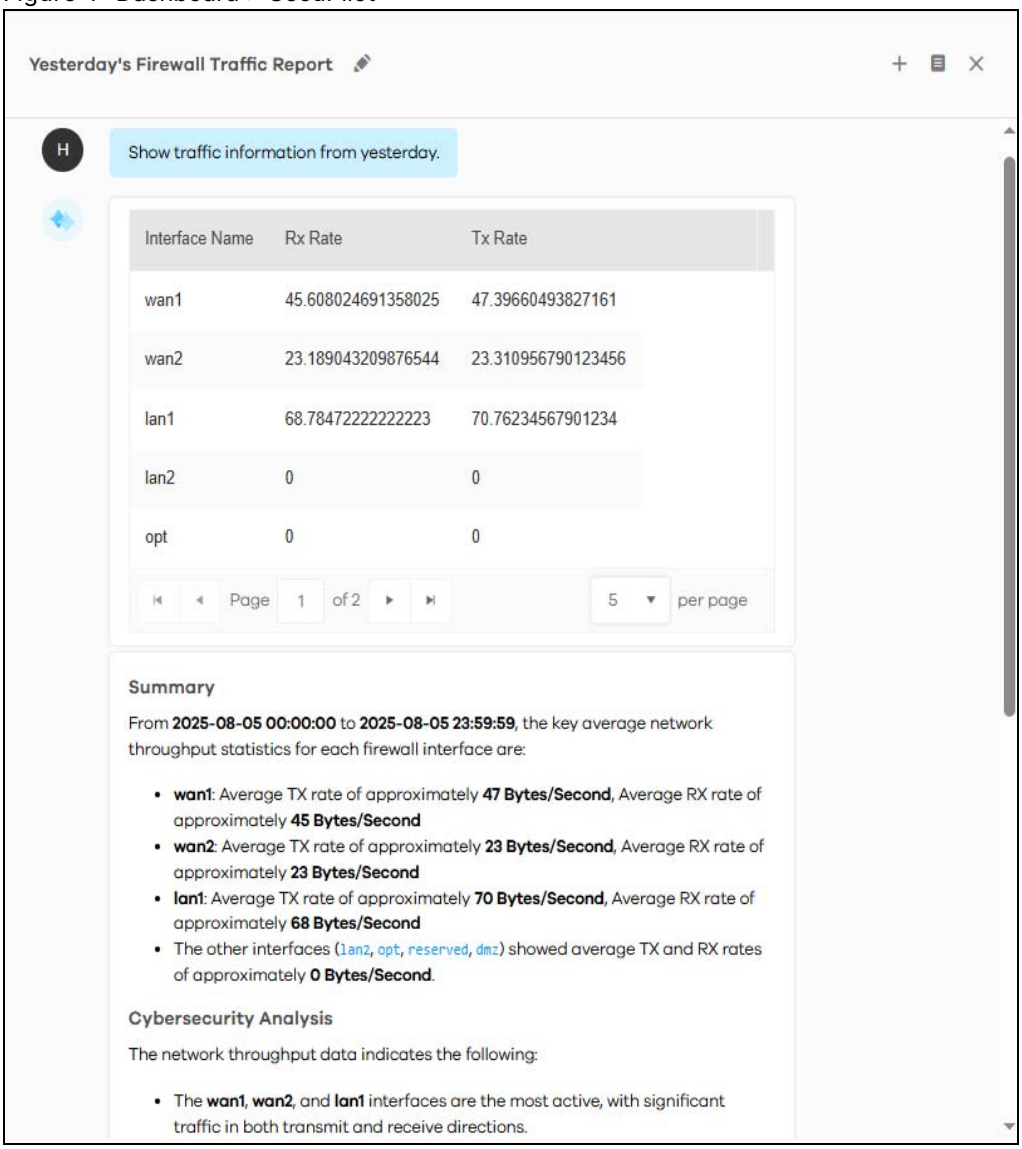


Figure 4 Dashboard > SecuPilot



The following table describes the labels on this screen.

Table 7 Dashboard > SecuPilot

ICON	DESCRIPTION
Edit conversation name	Click this to rename the current conversation.
New chat	Click this to open a new conversation without referencing previous conversations.
History	Click this to view, rename or delete your conversation history with SecuPilot. Conversations older than 30 days or more than 100 entries are deleted. See Section 1.4.1 on page 14 for more information.
Close	Click this to close the chatbox.
Like	Click this to send positive feedback to SecuPilot.
Dislike	Click this to send negative feedback to SecuPilot and specify your reason. SecuPilot uses these responses to improve future replies.

Table 7 Dashboard > SecuPilot

ICON	DESCRIPTION
Download chart as image Download grid to Excel	Download chart as image - If the current chart type is a bar chart, column chart, donut chart, pie chart, or trend chart, you can click this to save the chart to your computer as an image. Download grid to Excel - If the chart type is set to grid, you can click this to save it to your computer as an Excel file.
Change chart type	SecuPilot displays the most suitable chart based on your questions. Click this to switch between chart types, including grid, bar chart, column chart, donut chart, pie chart, or trend chart.
Send	Click this to submit your prompt to SecuPilot.

1.4.1 View SecuPilot Conversation History

You can view, rename and delete your conversation history with SecuPilot in the Dashboard > SecuPilot > History screen.

Figure 5 Dashboard > SecuPilot > History

The following table describes the icons on this screen.

Table 8 Dashboard > SecuPilot > History

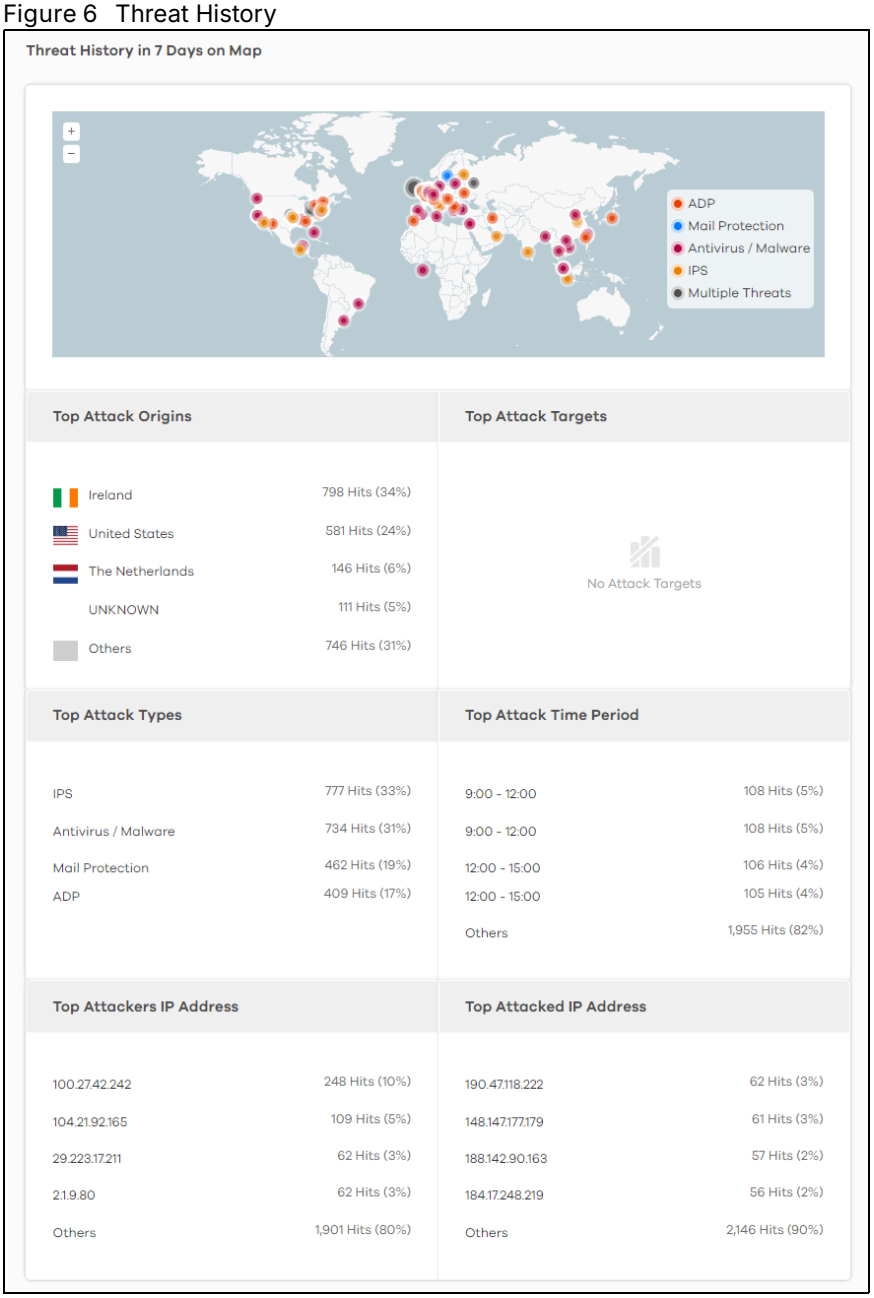
ICON	DESCRIPTION
Rename	Click ••• > next to the conversation you want to rename, then enter and save a new title.
Delete	Click ••• > next to the conversation you want to delete. The whole conversation will be removed.
View	Click on the title of the conversation to view the complete conversation history with SecuPilot.

1.5 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.

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

Figure 6 Threat History



The following table describes the labels on this screen.

Table 9 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 address.
Top Attacked IP Address	This displays each threat's destination IP address.

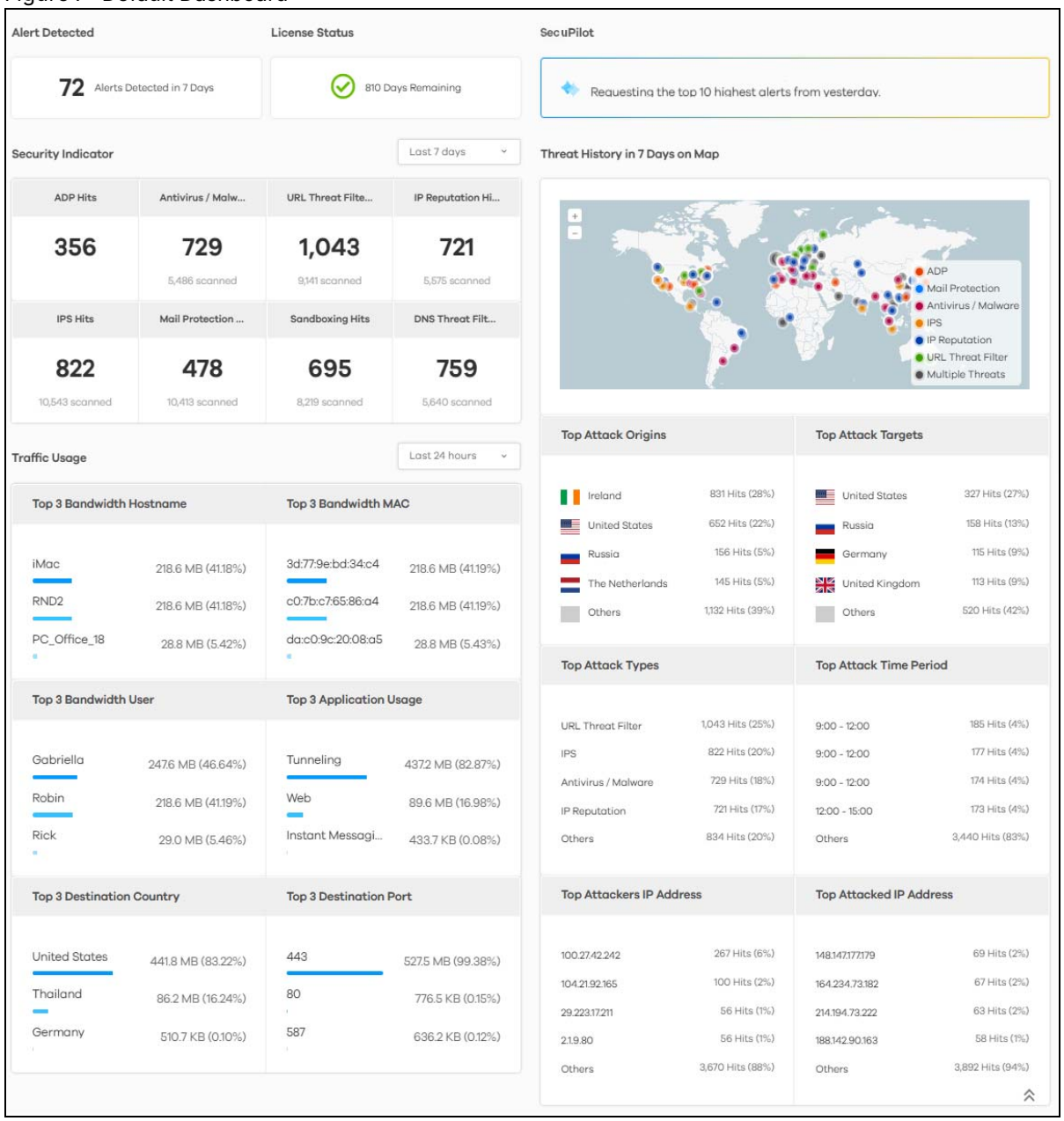
1.6 Dashboard

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 7 Default Dashboard



The following table describes the widgets on the default dashboard:

Table 10 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. This displays Active if you are using a PAYG license. Note: A Pay As You Go (PAYG) license allows you to charge monthly payments to your credit card instead of paying in full in advance.

Table 10 Default Dashboard (continued)

LABEL	DESCRIPTION
Security Indicator	
	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 Prevention System) 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.

1.6.1 Introduction to PAYG

Pay As You Go (PAYG) is a new license payment method for specific organizations, known as 'PAYG Orgs'. Instead of paying in full for a license in advance, you reserve your credit card for future monthly payments.

PAYG is charged for a Gold Security Pack license or a Nebula Professional Pack license for each Nebula Device in the 'PAYG Org'. Each Nebula Device in a PAYG Org will be charged for at least a Nebula Professional Pack license.

- For example, if you enabled PAYG Org A on June 1st, disabled it on June 5th, and re-enabled it on Jun 15th, then on July 1st, your credit card will be billed for 20/31 month for each Nebula Device in PAYG Org A.
- As another example, if you enabled PAYG Org A on June 1st, then moved one Nebula Device 'X' in PAYG Org A to PAYG Org B on Jun 15th, then on July 1st, your credit card will be billed for 15/31 month for Nebula Device 'X' in PAYG Org A, and 15/31 month for Nebula Device 'X' in PAYG Org B.

In Zyxel Device, you first assign an Org with On-cloud (Nebula) Devices as a 'PAYG Org'. This Org then becomes a Nebula Pro Org. PAYG is charged for each Nebula Device you have in the 'PAYG Org'. All Nebula Device in a PAYG Org will be charged for at least a Nebula Professional Pack license.

Note: The Gold Security Pack includes a Nebula Professional Pack license.

Note: Only owners of 'PAYG Orgs' can designate an Org as a 'PAYG Org'. Delegated admins cannot.

CHAPTER 2
Settings

2.1 Overview

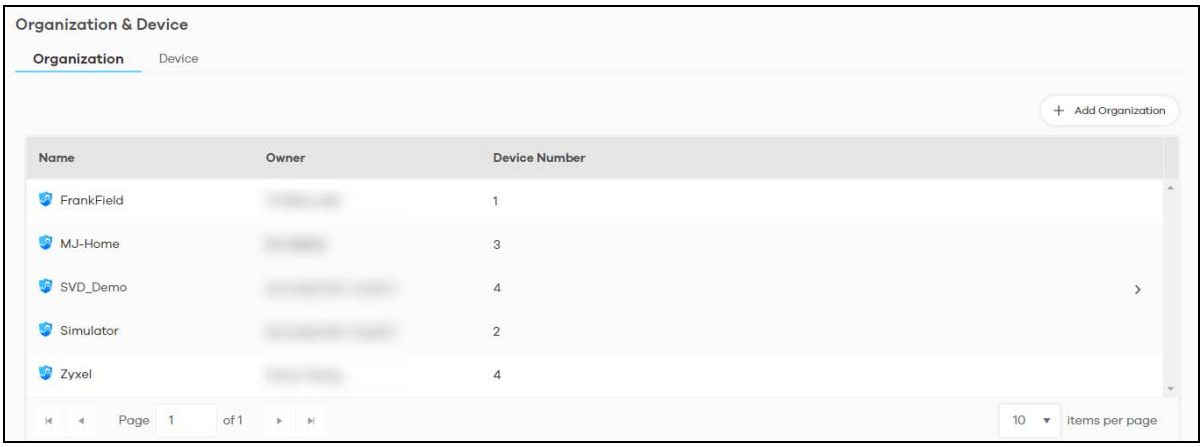
First, register your Zyxel Device at *https://account.zyxel.com*, activate the SecuReporter license, and enable SecuReporter in the Zyxel Device using its Web Configurator or commands. You can then add your Zyxel Device to an organization at the SecuReporter web portal.

Note: Only the Zyxel Device owner, that is the person who has registered the Zyxel Device at *https://account.zyxel.com*, and activated the SecuReporter license, can add a Zyxel Device to an organization. See Table 3 on page 8 for details on management privileges.

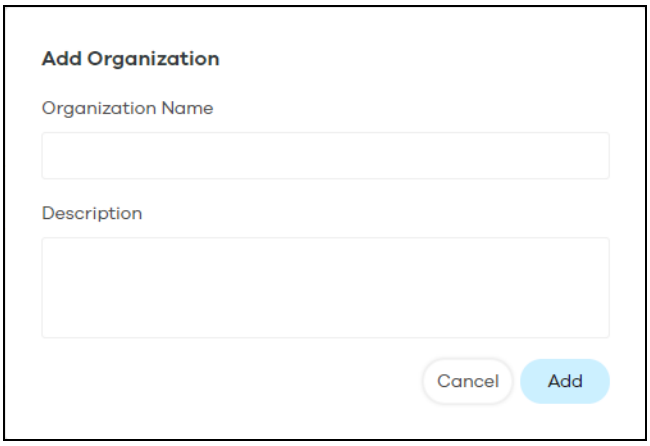
2.2 Organization & Device

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.



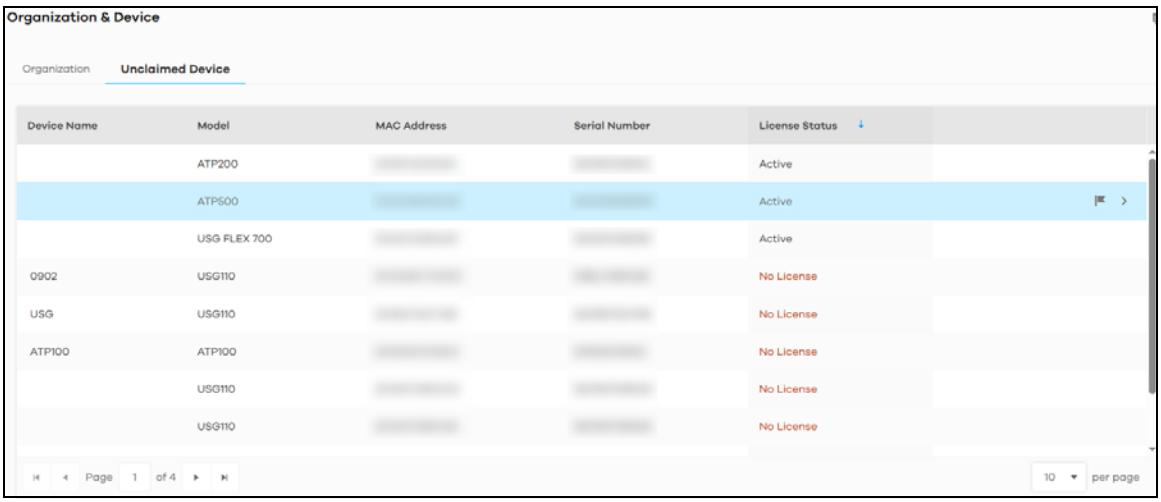
2 Enter a name of up to 255 characters and description for the organization.



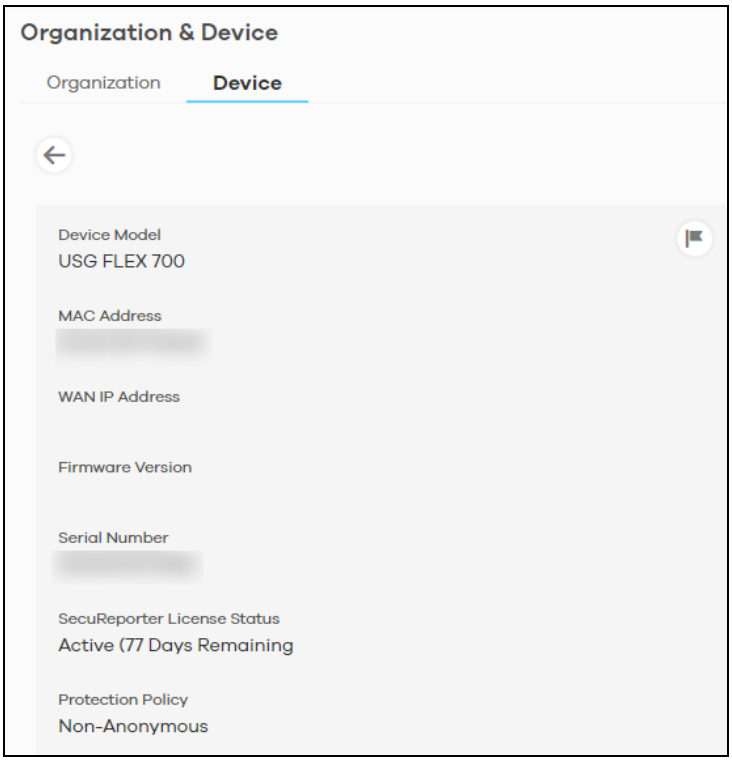
2.2.1 Add a Zyxel Device to an Organization

The Unclaimed Device tab displays the Zyxel Devices that are available to be added to this organization by the Zyxel Device owner.

Note: Some models, such as the USG FLEX H series, can only be added through NCC.

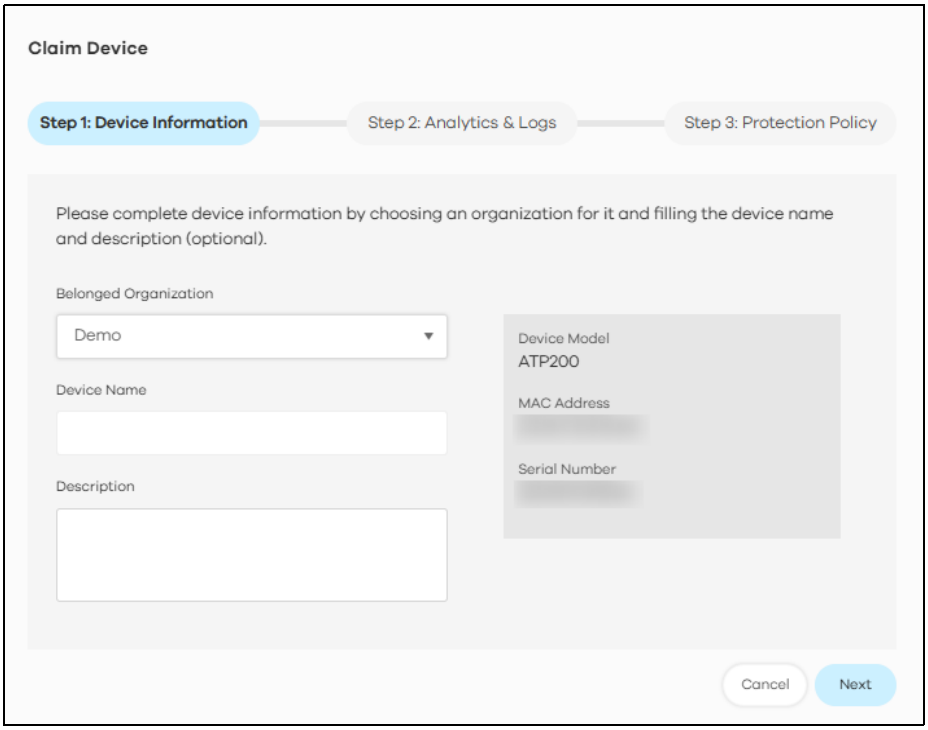


1 Click a model to see details of Zyxel Devices that are available to be added.

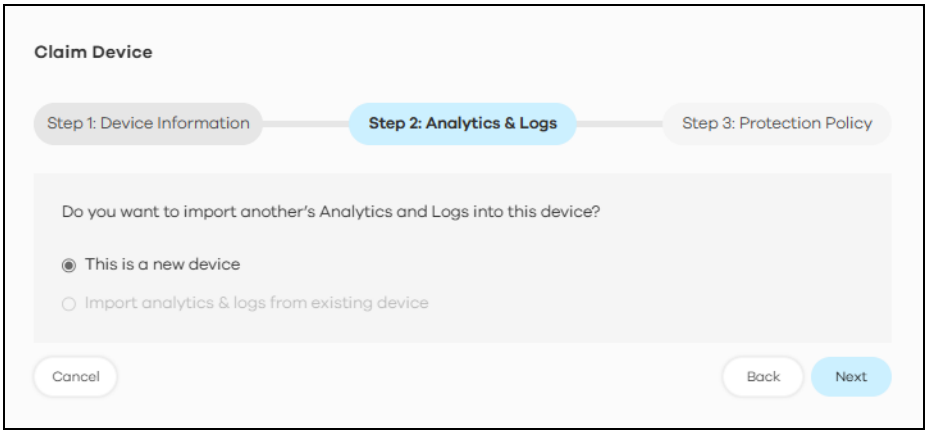


2 You will see the icon on the right when you hover the mouse on the registered Zyxel Devices that have activated SecuReporter licenses. This icon will not appear for registered Zyxel Devices that do not have activated SecuReporter license.

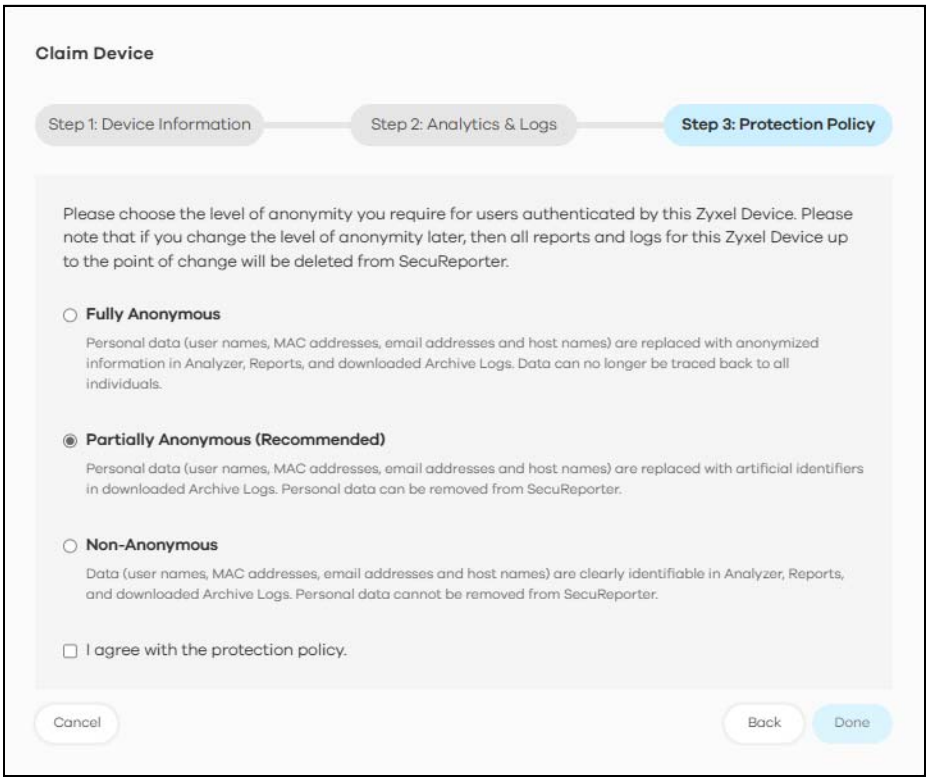
3 Click the icon to add the Zyxel Device into an organization. Select an Organization and enter an identifying name for this Zyxel Device in Device Name and an optional Description, and then click Next.



4 If this Zyxel Device was in SecuReporter before or if this is a replacement Zyxel Device for a Zyxel Device that was in SecuReporter before, then select Import Analytics & Logs from existing device; otherwise select This is a new device. Then click Next.



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

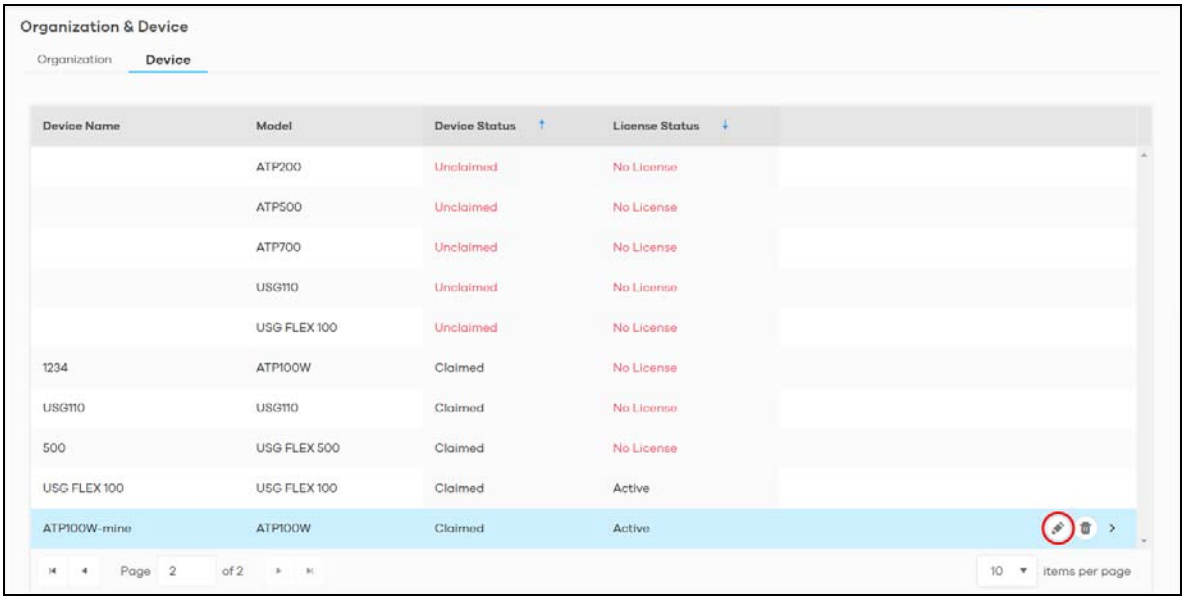


Note: You can change the level of data protection later, but all logs and reports created for the Zyxel Device up to that point will be lost.

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

2.2.2 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.



2.2.3 Generate API Token

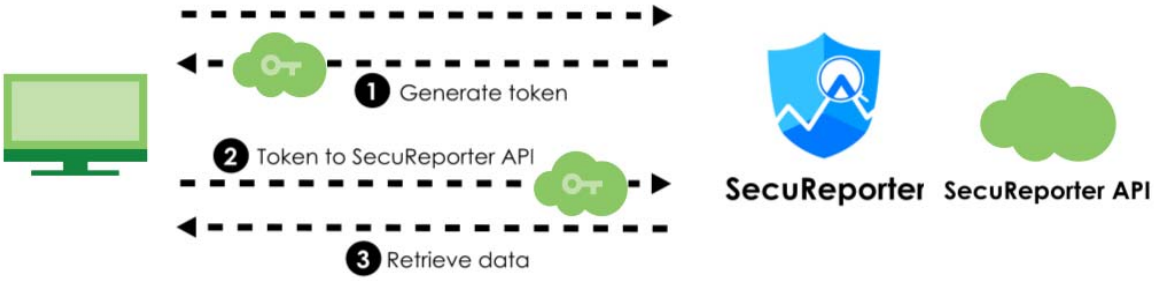
An API (Application Programming Interface) token is a secret string that verifies a user's access to API resources, allowing one software application to share data with another.

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.

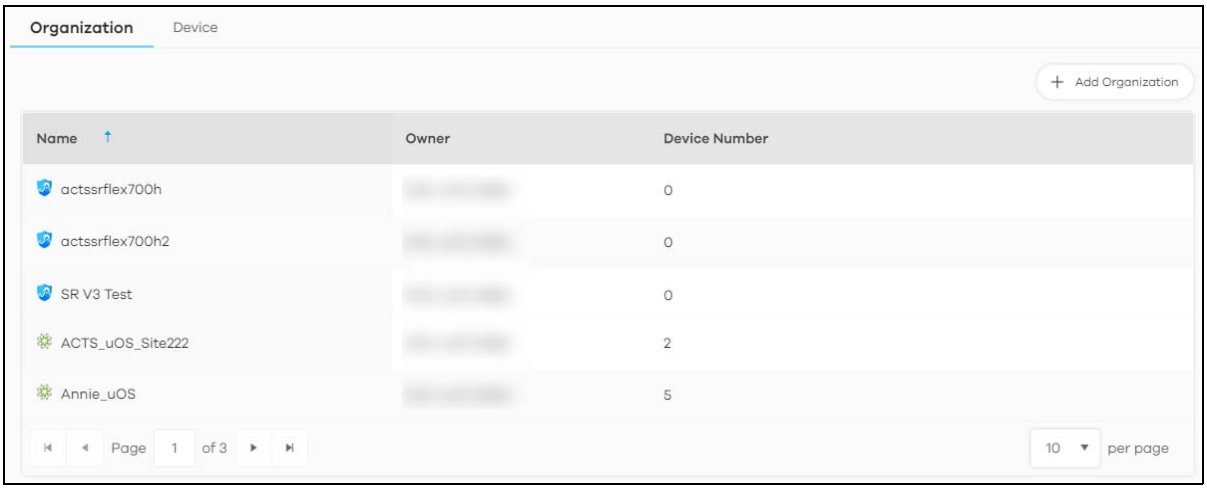
Figure 8 Overview of API Authorization



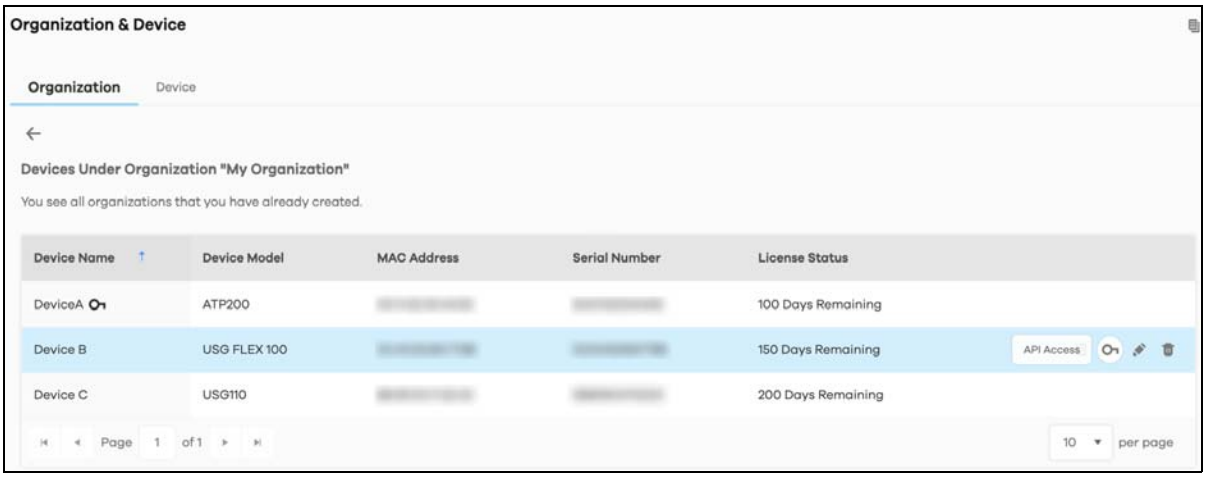
Generate an API token

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

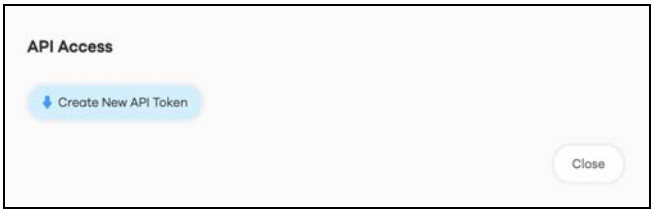
1 Click on the organization to which the Zyxel Device you want to share data with belongs.



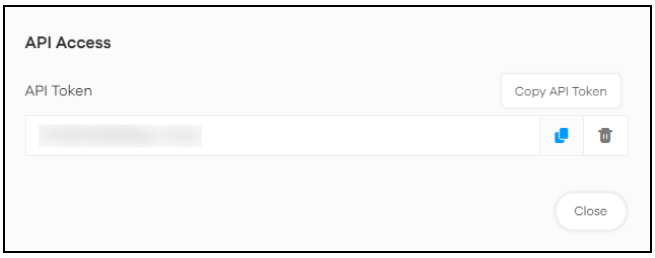
2 Click the API Access button next to the Zyxel Device you want to share data with. Make sure the Zyxel Device has a valid device license.



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.



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 I failed to retrieve SecuReporter logs through API in a third-party software application. to see what to do if your API request is rejected.

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

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

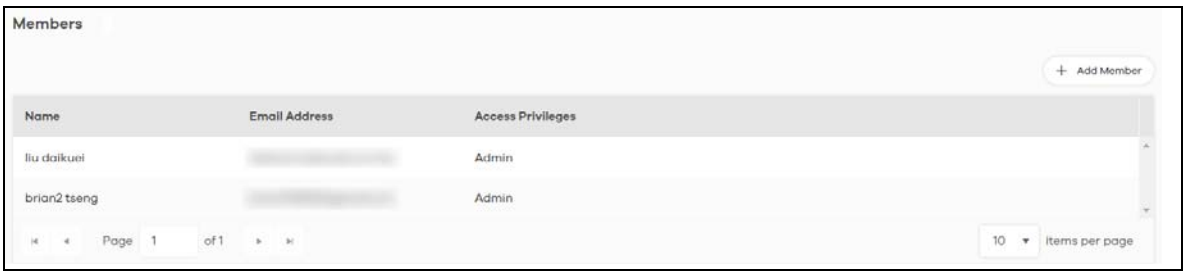
Retrieve SecuReporter Data

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

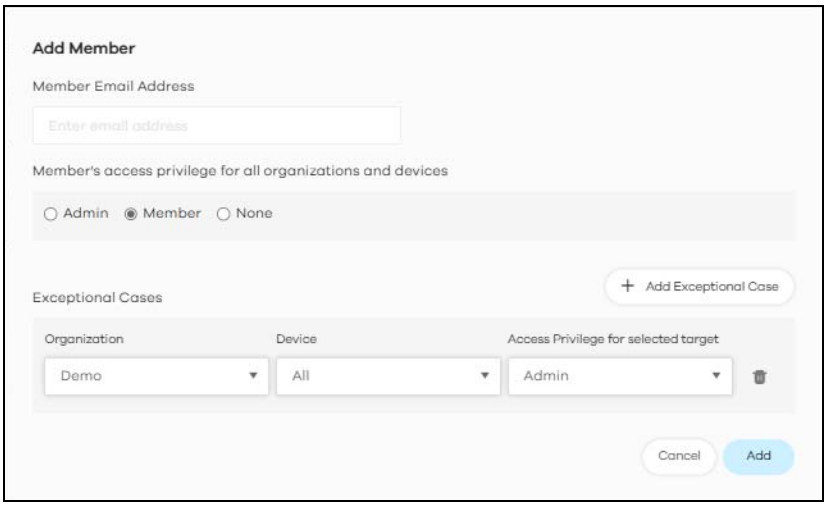
2.3 User Account

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.



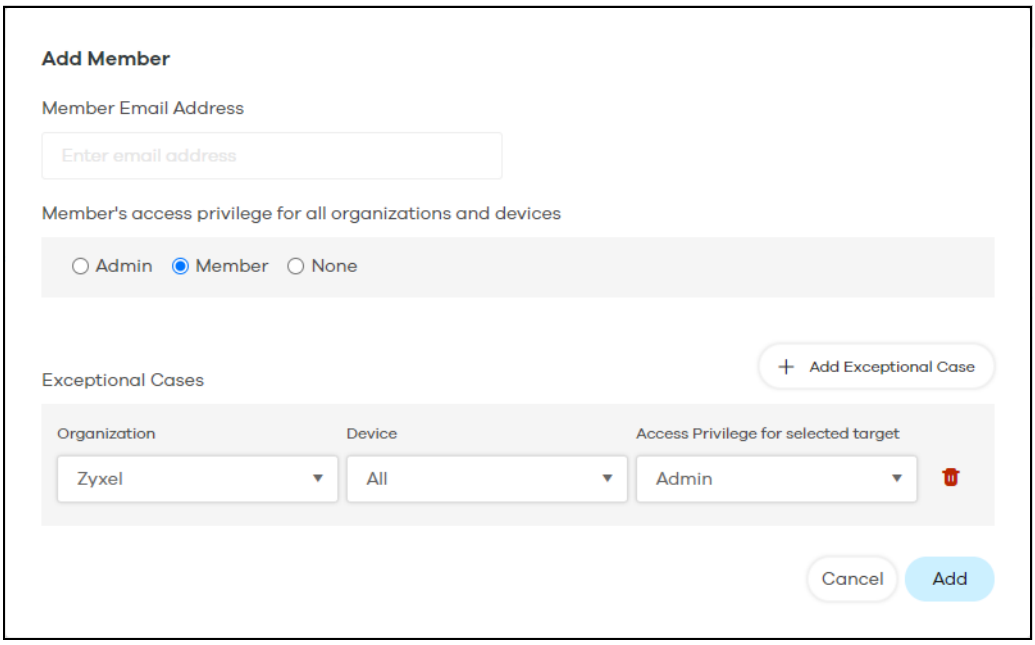
2 Enter the email address of the person that you want to be administrator in Member Email Address.



Note: 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.

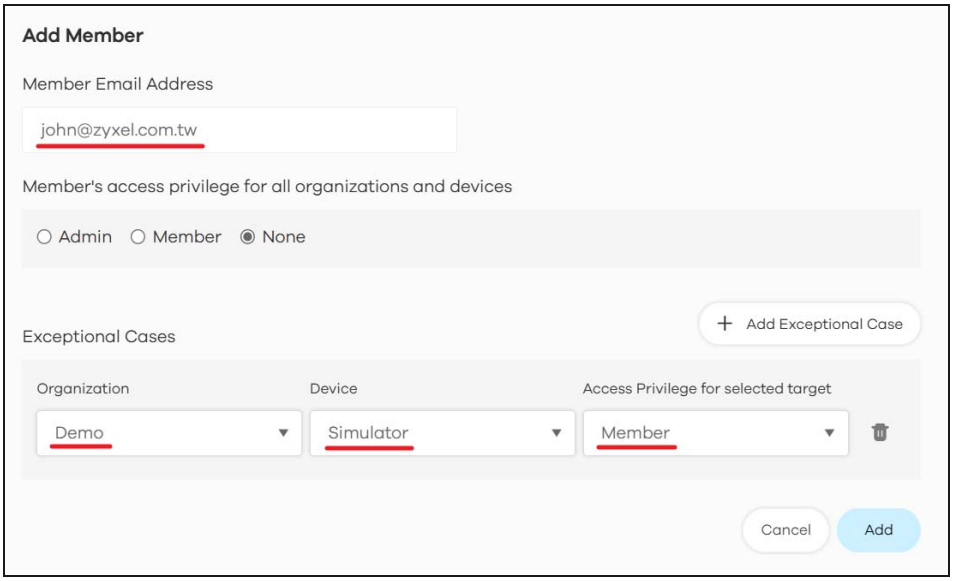


You may configure specific privileges by clicking Add Exceptional Case for individual Zyxel Devices within this organization.

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

- Organization
- Device
- Access Privilege for selected target

For example, you may want to assign this account with just Member privileges and only for the Zyxel Device named Simulator.



Note: See Table 3 on page 8 for details on management privileges.

4 Click Add when finished.

CHAPTER 3
Analysis

3.1 Overview

Analysis is a set of charts, tables, and other visualizations of data collected from the 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.

3.1.1 Tutorial

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

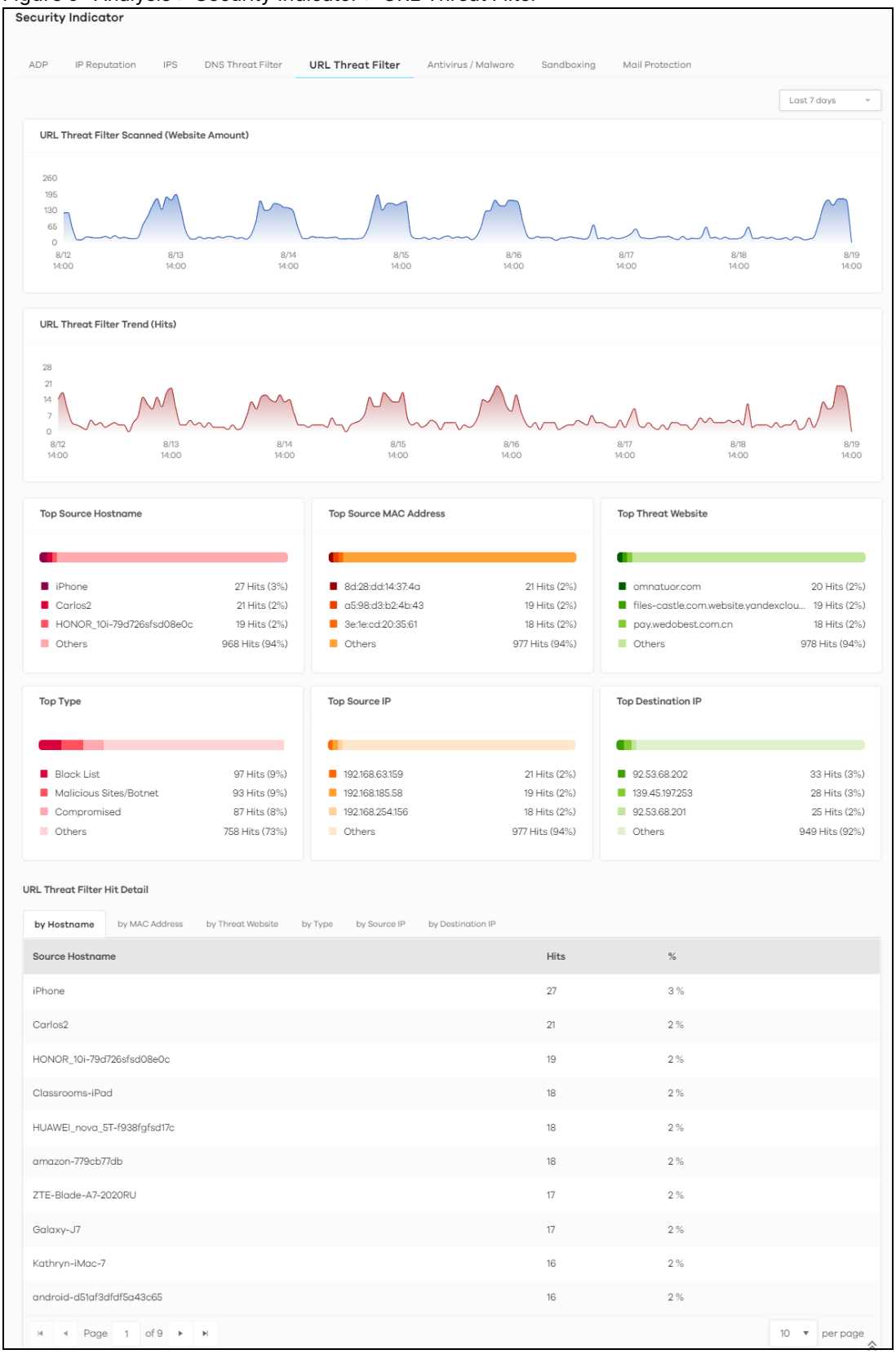
In most cases, you can choose to analyze data collected over one of five time frames (see Section 1.6 on page 16):

- 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 9 Analysis > Security Indicator > URL Threat Filter



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 10 Analysis > Security Indicator > URL Threat Filter > by Destination IP

URL Threat Filter Hit Detail

by Hostname | by MAC Address | by Threat Website | by Type | by Source IP | 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 %

Page 1 of 11 10 per page

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 11 Analysis > Security Indicator > URL Threat Filter > by Source IP

URL Threat Filter Hit Detail

by Hostname | by MAC Address | by Threat Website | by Type | by Source IP | by Destination IP

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 %

Page 1 of 9 10 per page

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 12 Source IP Information

3.1.2 Sandboxing

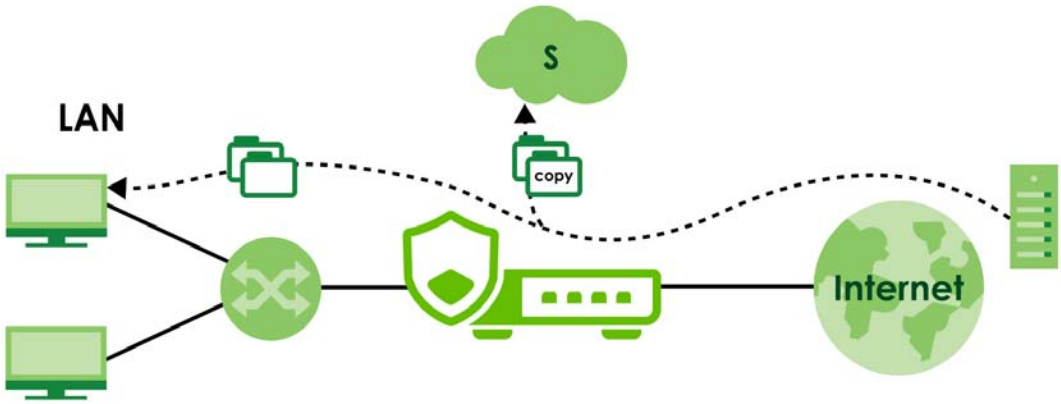
Zyxel cloud sandboxing is a security mechanism which provides a safe environment to separate running programs from your network and host devices. Unknown or untrusted programs or codes are uploaded to a cloud server and executed within an isolated virtual machine (VM) to monitor and analyze the zero-day 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 sandboxing 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 (S) 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.

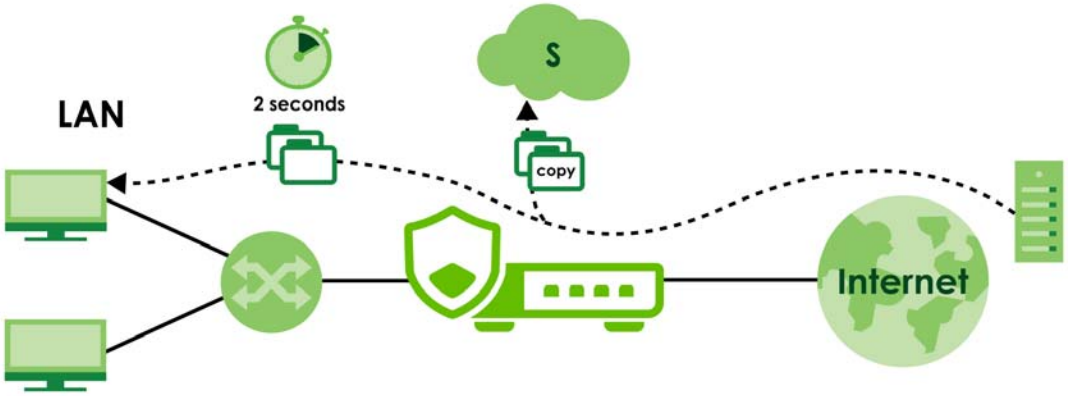
Note: The scan result is removed from the Zyxel Device cache after the Zyxel Device restarts, so all files are once again 'unknown'.

Figure 13 General Zyxel Sandboxing Inspection



In the Zyxel Device, you can configure Advanced Zyxel Sandboxing 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 14 Advanced Zyxel Sandboxing Inspection



3.1.2.1 Supported File Types for Sandboxing Inspection

Sandboxing 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 Sandboxing.

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.

3.1.2.2 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.

3.1.2.3 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 sandboxing (or Security Cloud) removed infected portions of files that were suspicious or malicious.

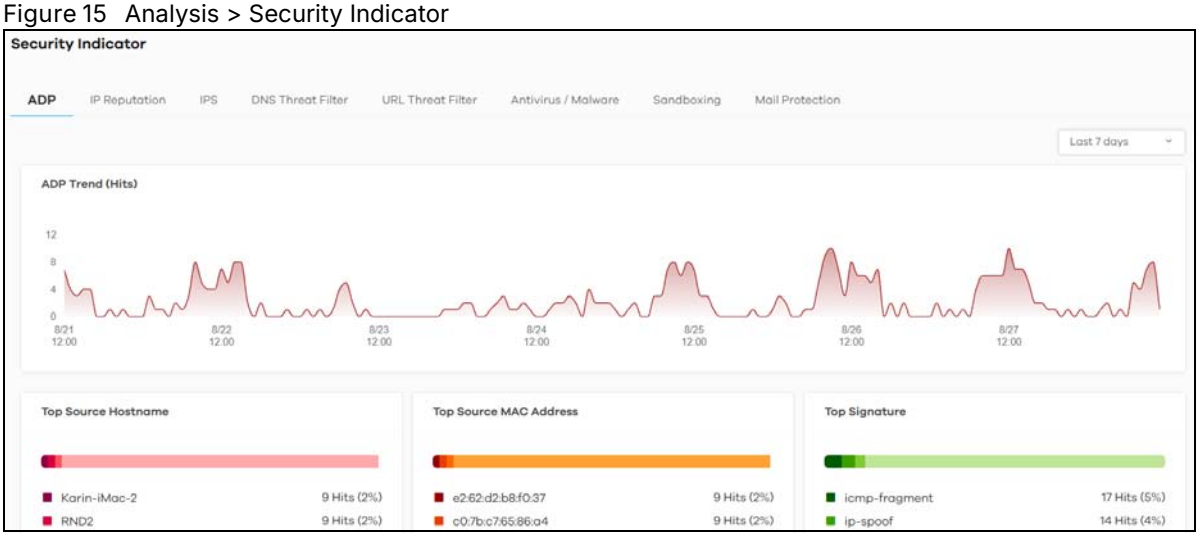
Note: In this case the receiver of the file will not be able to open the file. The Zyxel Device administrator should contact the receiver of the file to let him or her know.

3.2 Analysis Overview

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

Data is displayed in the Analysis menus as follows.

Figure 15 Analysis > Security Indicator



3.3 Security Indicators

Security Indicators data visualizations are categorized as:

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

- Sandboxing
- Mail Protection

3.3.1 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

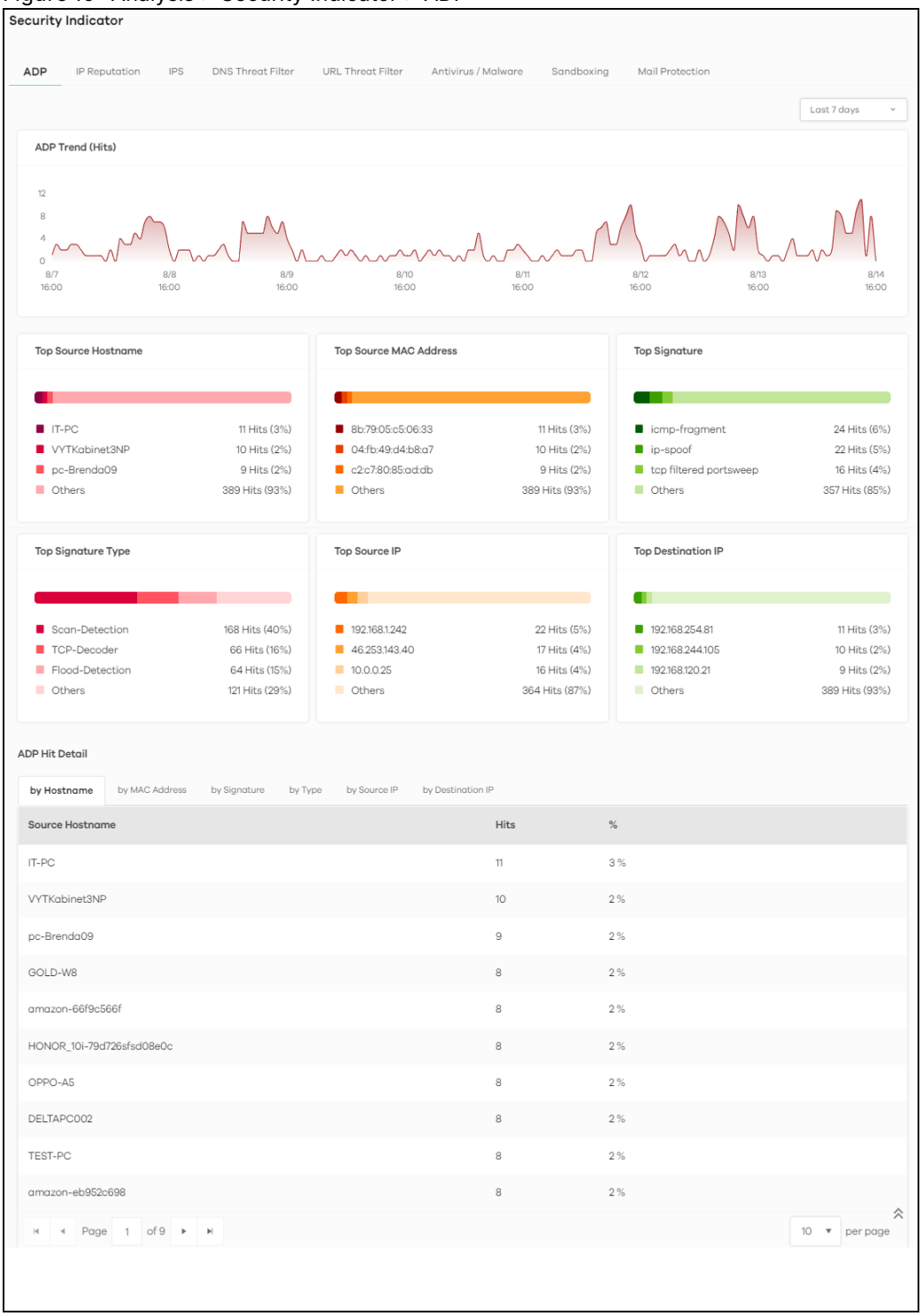
Protocol anomalies are packets that do not comply with the relevant RFC (Request For Comments). Protocol anomaly detection includes:

- 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 16 Analysis > Security Indicator > ADP



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

Table 11 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.

3.3.2 IP Reputation

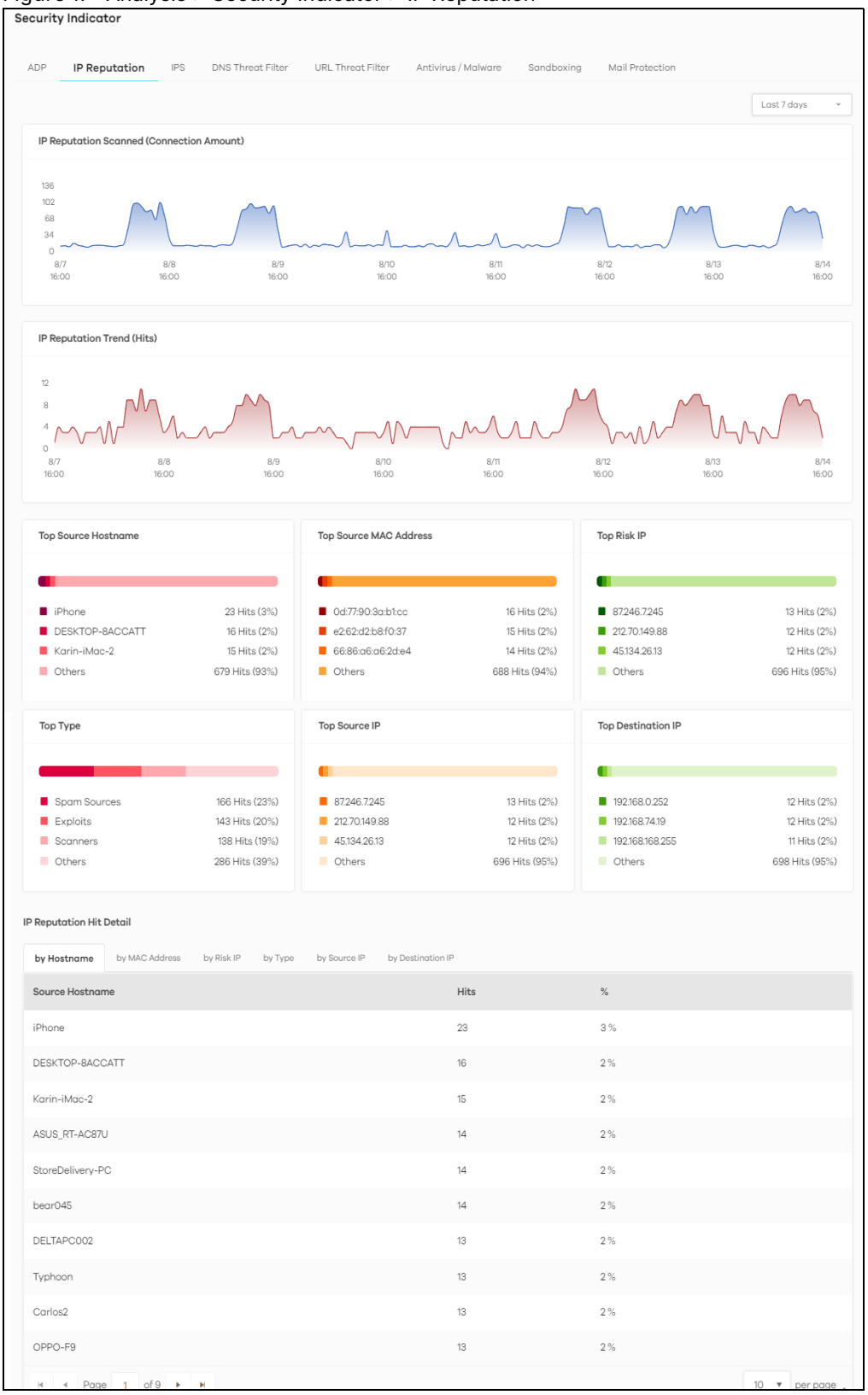
When you register for and enable the IP reputation service, your Zyxel Device downloads signature files that identifies reputation of IPv4 addresses. You can have the Zyxel Device forward, block, and/or log packets from IPv4 addresses based on these signatures and categories.

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 17 Analysis > Security Indicator > IP Reputation



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

Table 12 Analysis > Security Indicator > IP Reputation

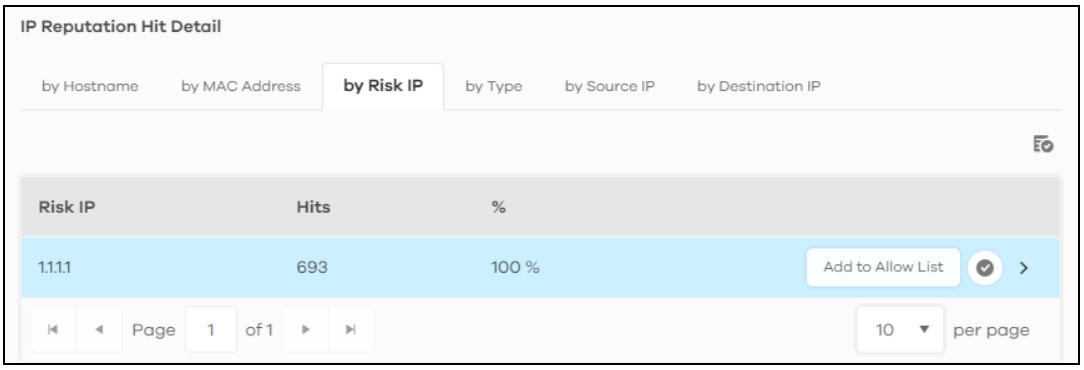
LABEL	DESCRIPTION
IP Reputation Scanned (Connection Amount)	This chart displays the total number of connections detected by the Zyxel Device. Move your cursor over a trend line to display the number of connections encountered over time.
IP Reputation Trend (Hits)	This chart displays the number of IP 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 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 3.3.2.1 on page 39 for more information on how to add or remove a risk IP address from the allow list.

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

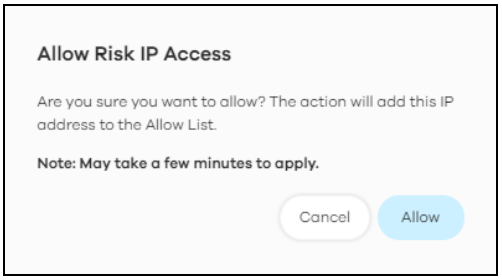
There is a blue check mark ✓ next to the risk IP addresses that are in the allow list.

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.



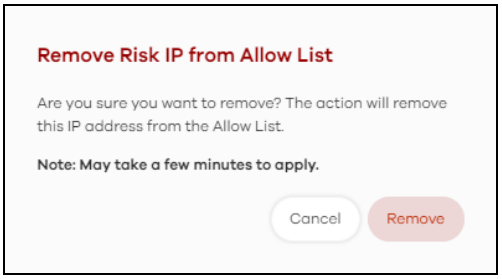
2 The following window pops up, click Allow to add the risk IP address to the allow list.



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.

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



3.3.3 IPS

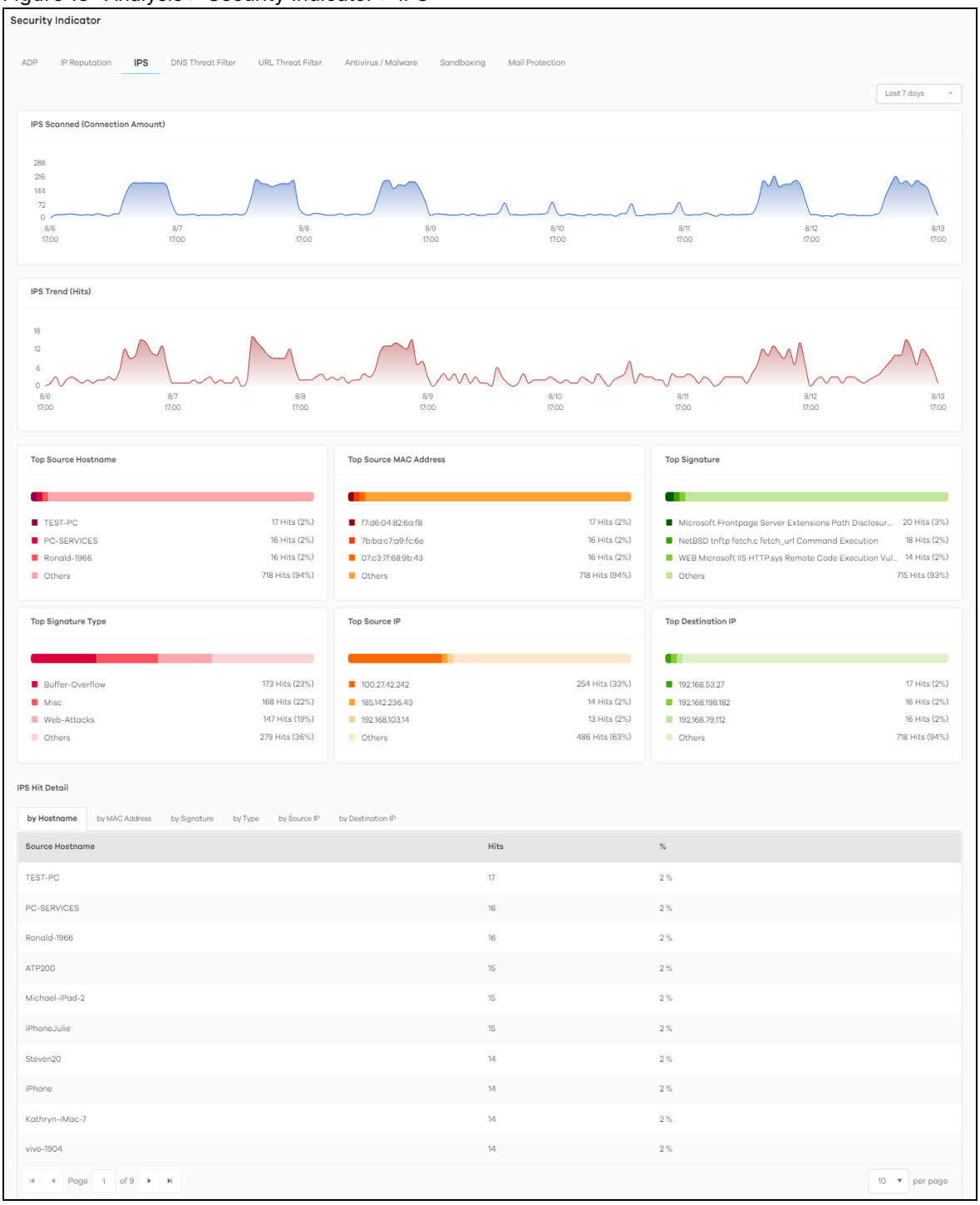
An IPS profile is a set of packet inspection signatures.

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 18 Analysis > Security Indicator > IPS



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

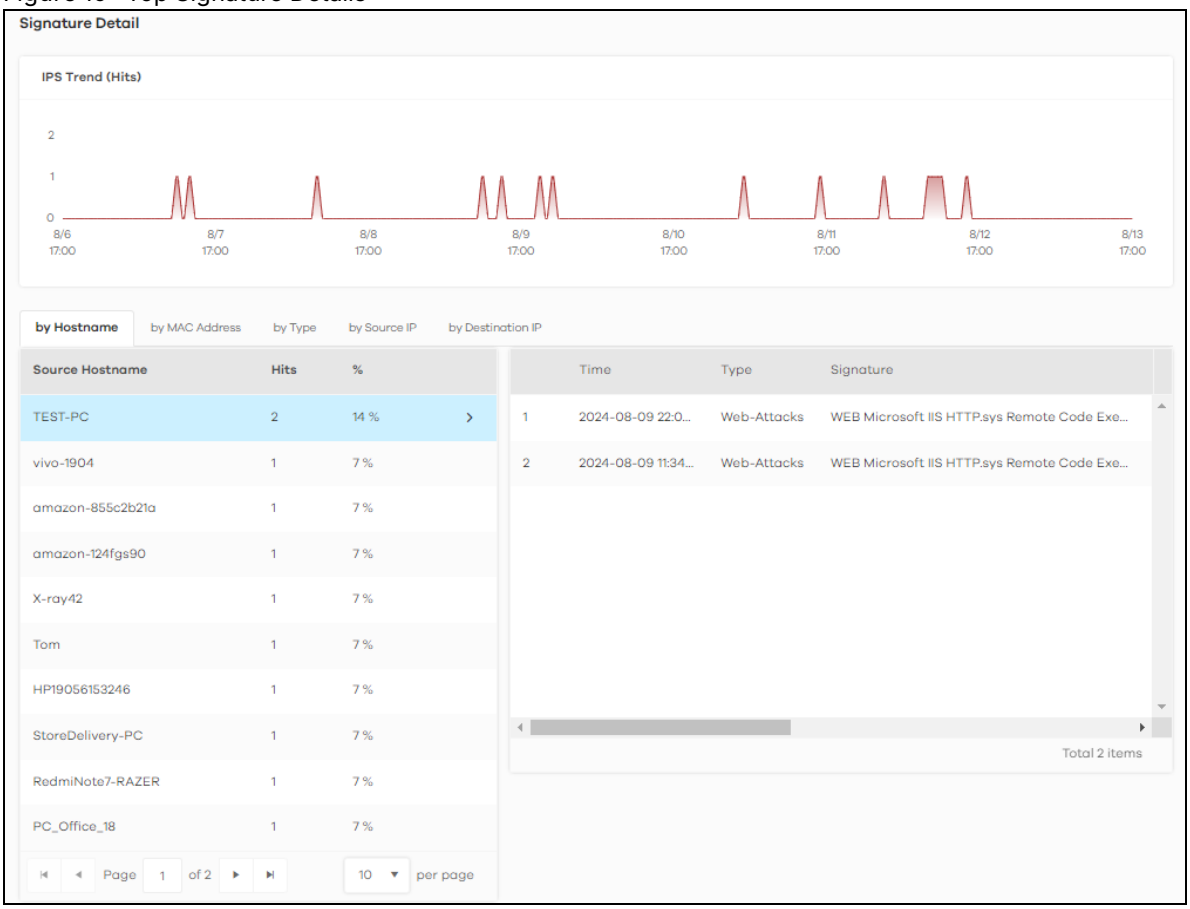
Table 13 Analysis > Security Indicator > IPS

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.

3.3.3.1 Threat Intelligence

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

Figure 19 Top Signature Details



3.3.4 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 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

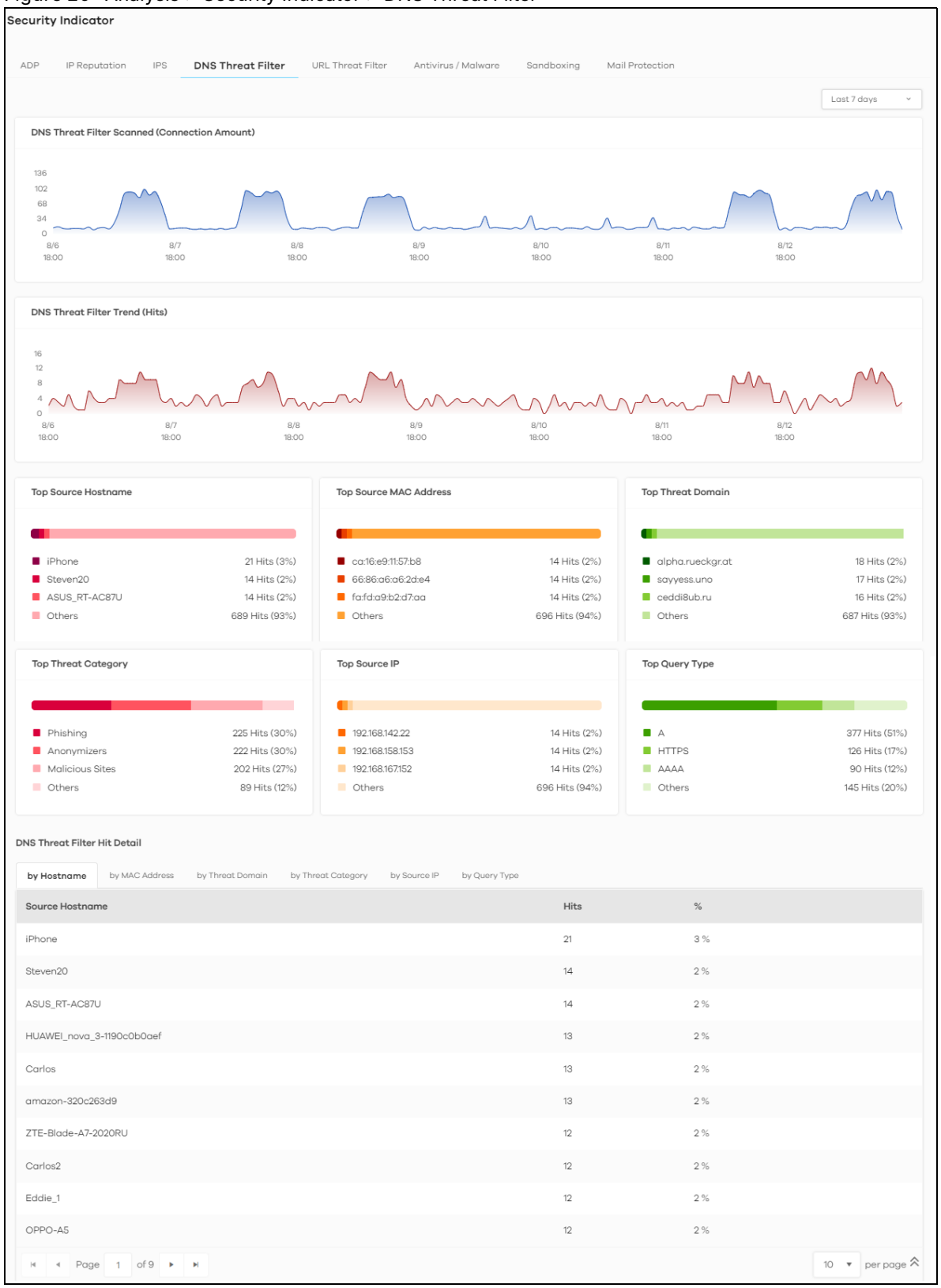
The Zyxel Device replies with a DNS server error for the following types of DNS queries:

- 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 20 Analysis > Security Indicator > DNS Threat Filter



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

Table 14 Analysis > Security Indicator > DNS Threat Filter

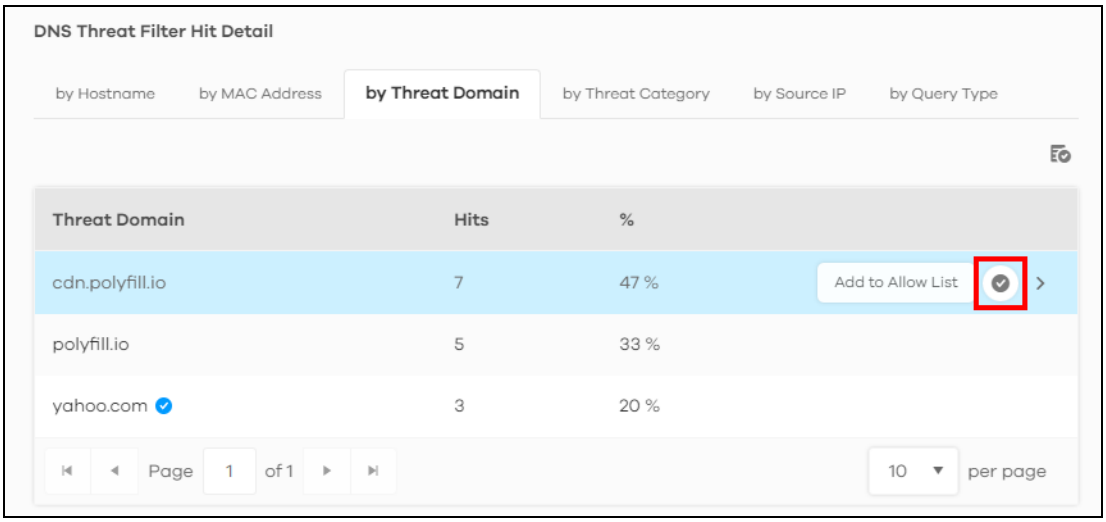
LABEL	DESCRIPTION
DNS Threat Filter Scanned (Connection Amount)	This chart displays the total number of connections detected by the Zyxel Device. Move your cursor over a trend line to display the number of connections encountered over time.
DNS Threat Filter Trend (Hits)	This chart displays the number 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 common types of DNS 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 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 3.3.4.1 on page 47 for more information on how to add or remove a threat domain from the allow list.

3.3.4.1 Add or Remove a Threat Domain to the Allow List

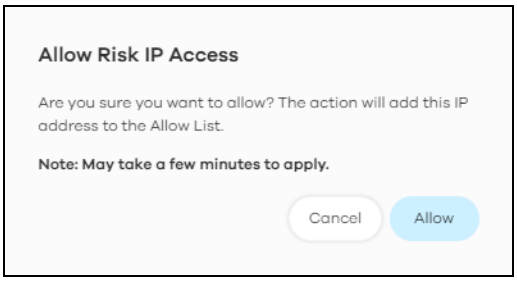
There is a blue check mark next to the threat domains that are in the allow list.

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.

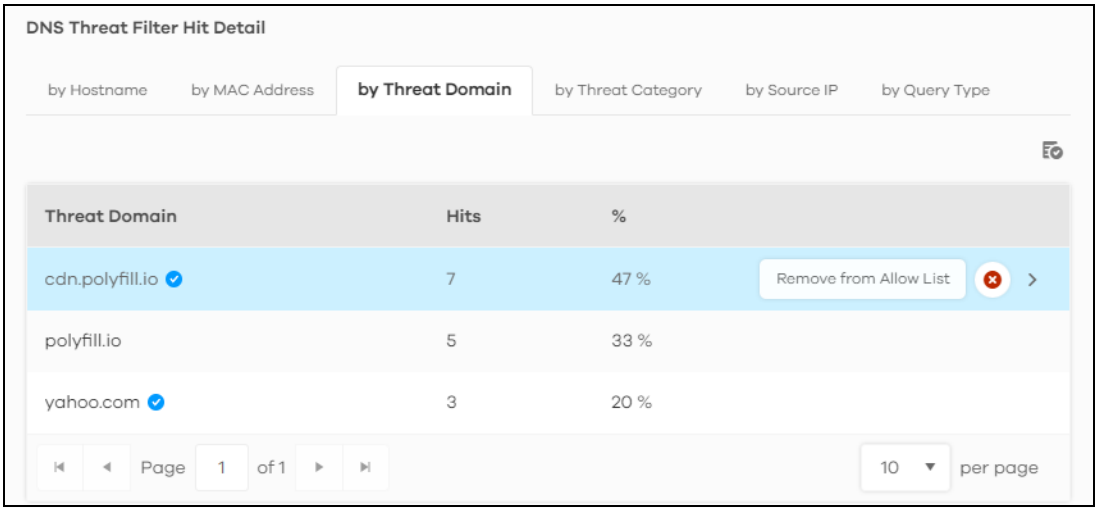


2 The following window pops up, click Allow to add the domain to the allow list.

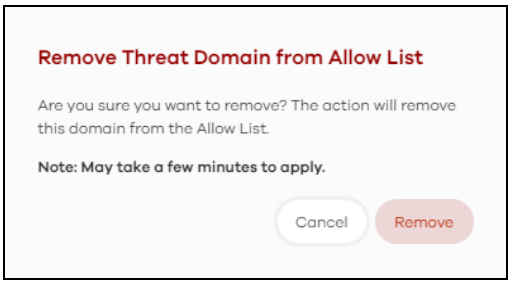


Do the following to remove a threat domain from the allow list:

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.



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



3.3.5 URL Threat Filter

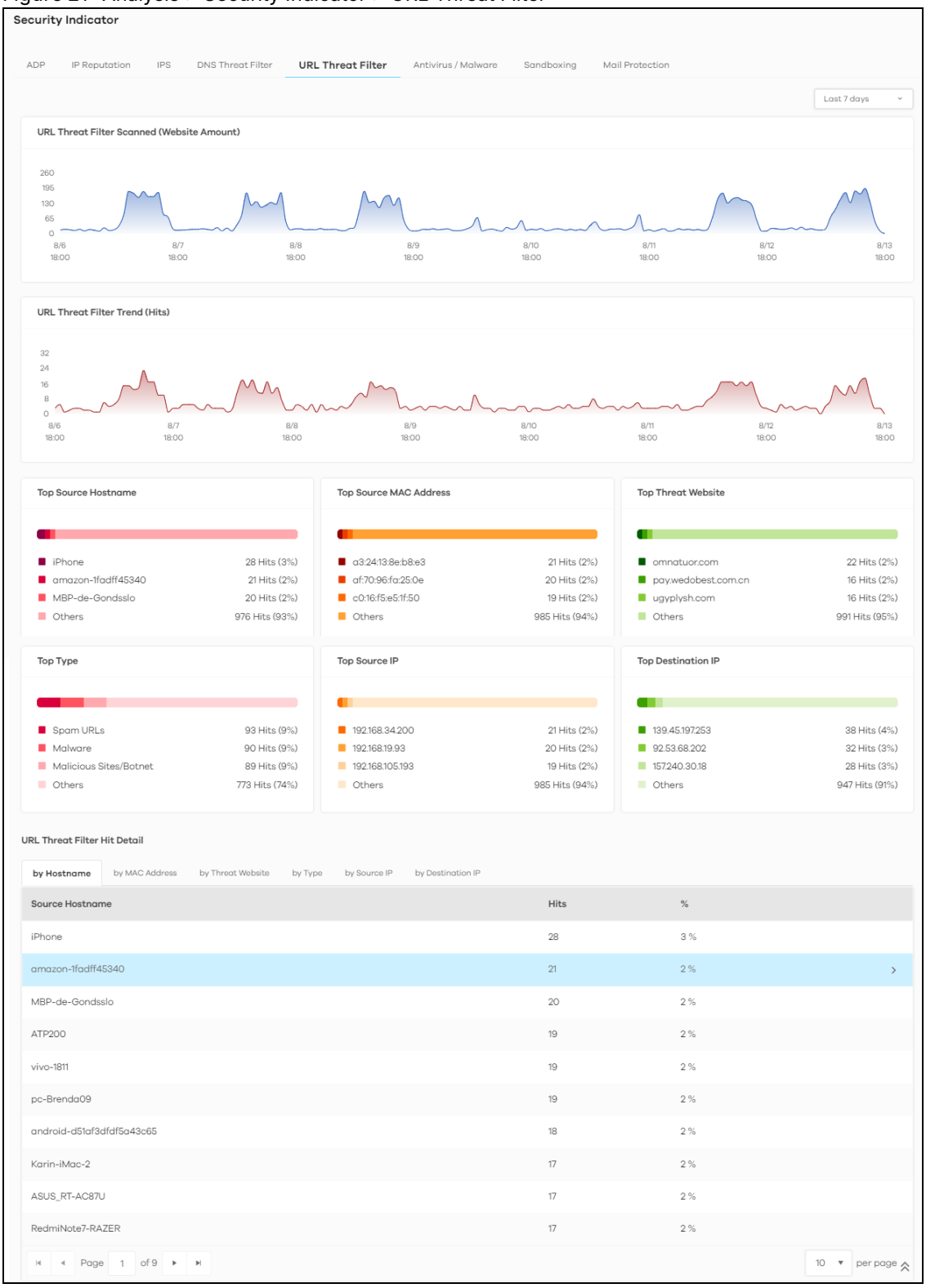
When you enable the URL Threat filtering service, your Zyxel Device downloads signature files that contain known URL Threat domain names and IP addresses. The Zyxel Device will also access an external database that has millions of web sites categorized based on content. You can have the Zyxel Device 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 21 Analysis > Security Indicator > URL Threat Filter



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

Table 15 Analysis > Security Indicator > URL Threat Filter

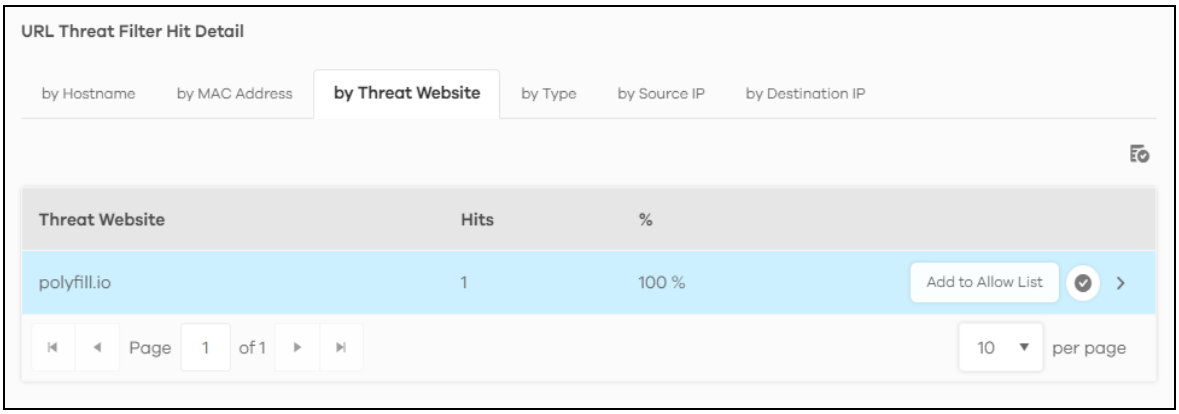
LABEL	DESCRIPTION
URL Threat Filter Scanned (Website Amount)	This chart displays the total number of connections detected by the Zyxel Device. Move your cursor over a trend line to display the number of connections encountered over time.
URL Threat Filter Trend (Hits)	This chart displays the number of 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 3.3.5.1 on page 51 for more information on how to add or remove a domain from the allow list.

3.3.5.1 Add or Remove a Threat Website to the Allow List

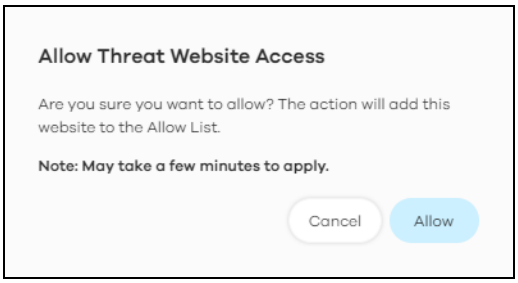
There is a blue check mark  next to the domain in the allow list.

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.

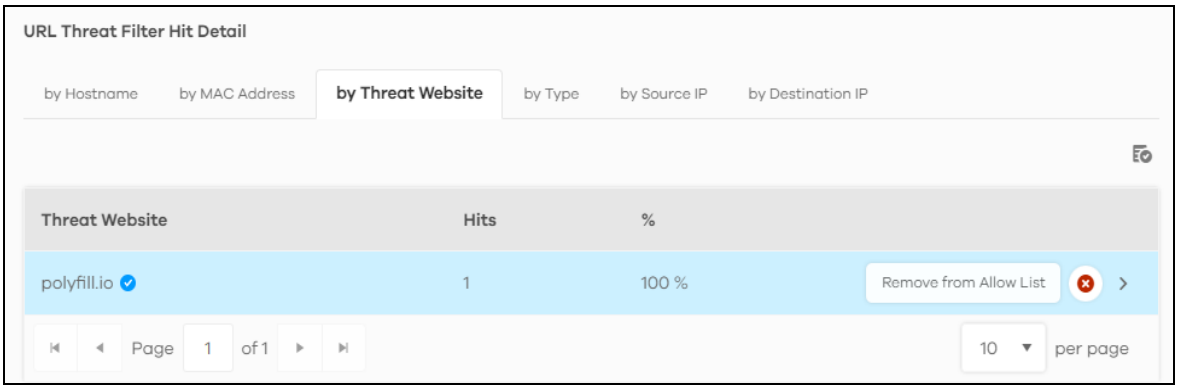


2 The following window pops up, click Allow to add the threat website to the allow list.

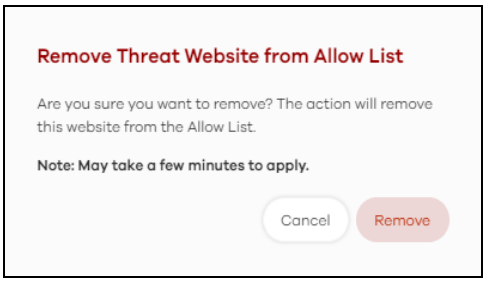


Do the following to remove a threat website from the allow list:

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.



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

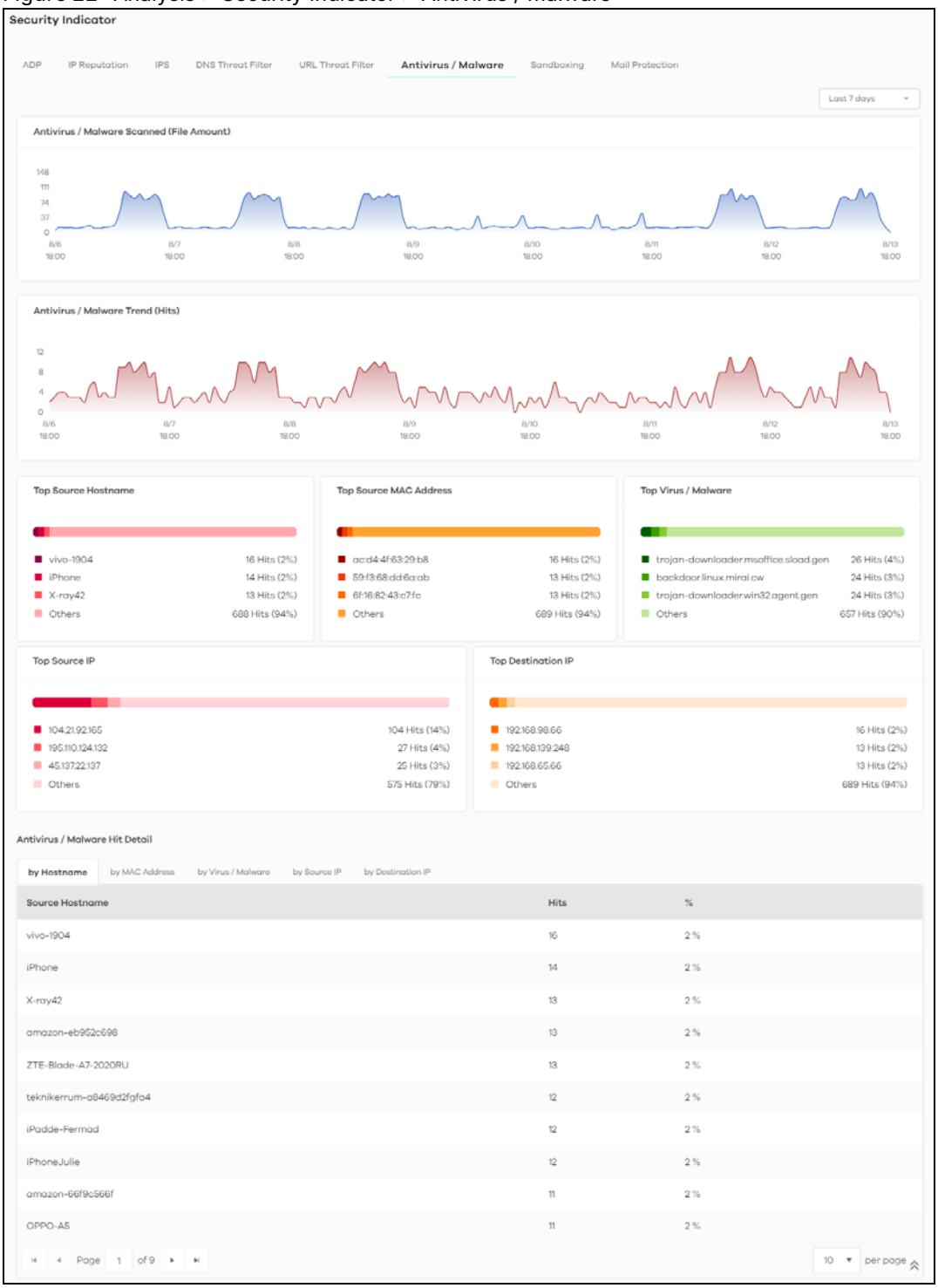


3.3.6 Antivirus / Malware

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 22 Analysis > Security Indicator > Antivirus / Malware



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

Table 16 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.

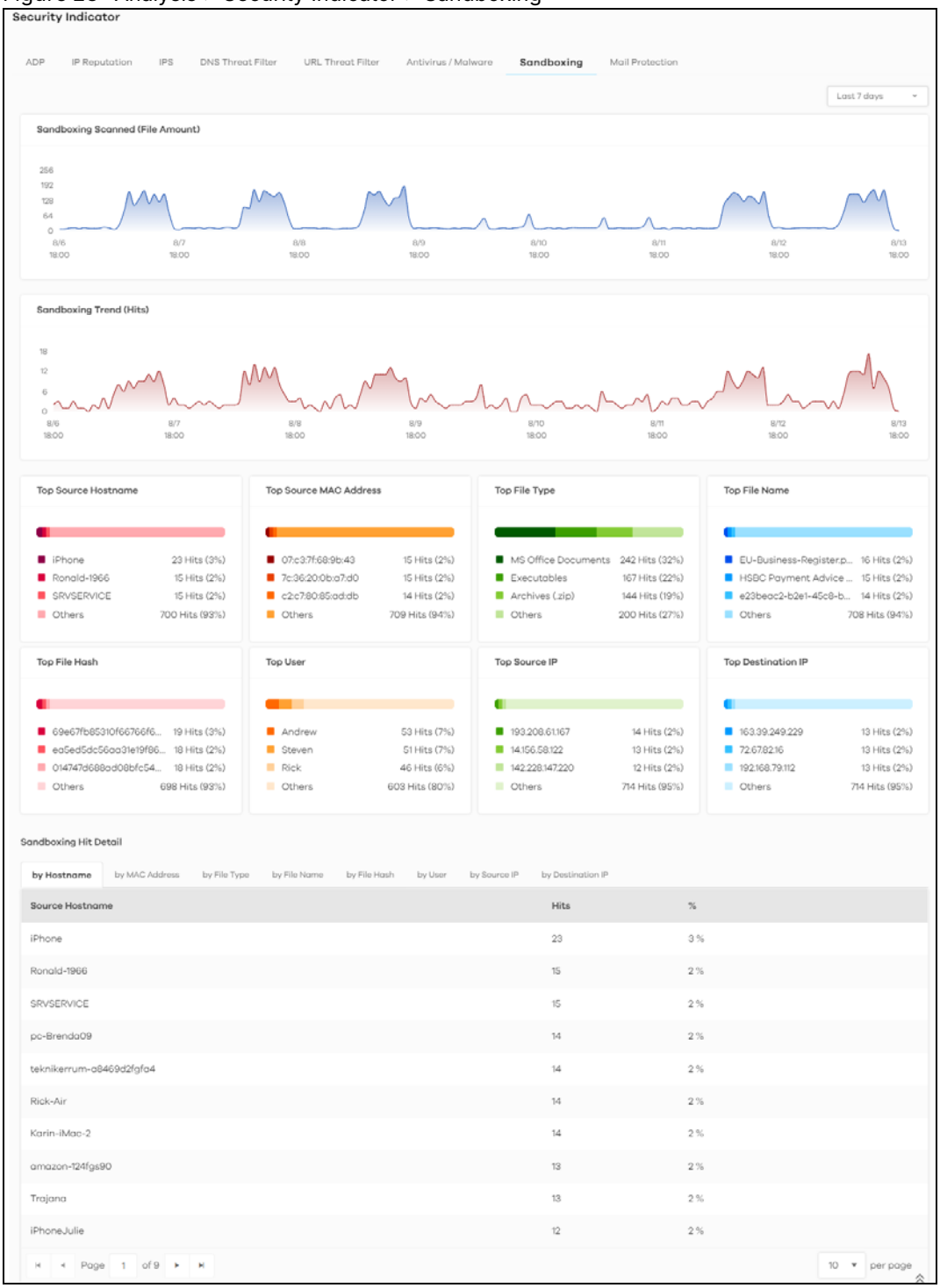
3.3.7 Sandboxing

This screen displays sandboxing statistics. See Section 3.1.2 on page 32 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 23 Analysis > Security Indicator > Sandboxing



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

Table 17 Analysis > Security Indicator > Sandboxing

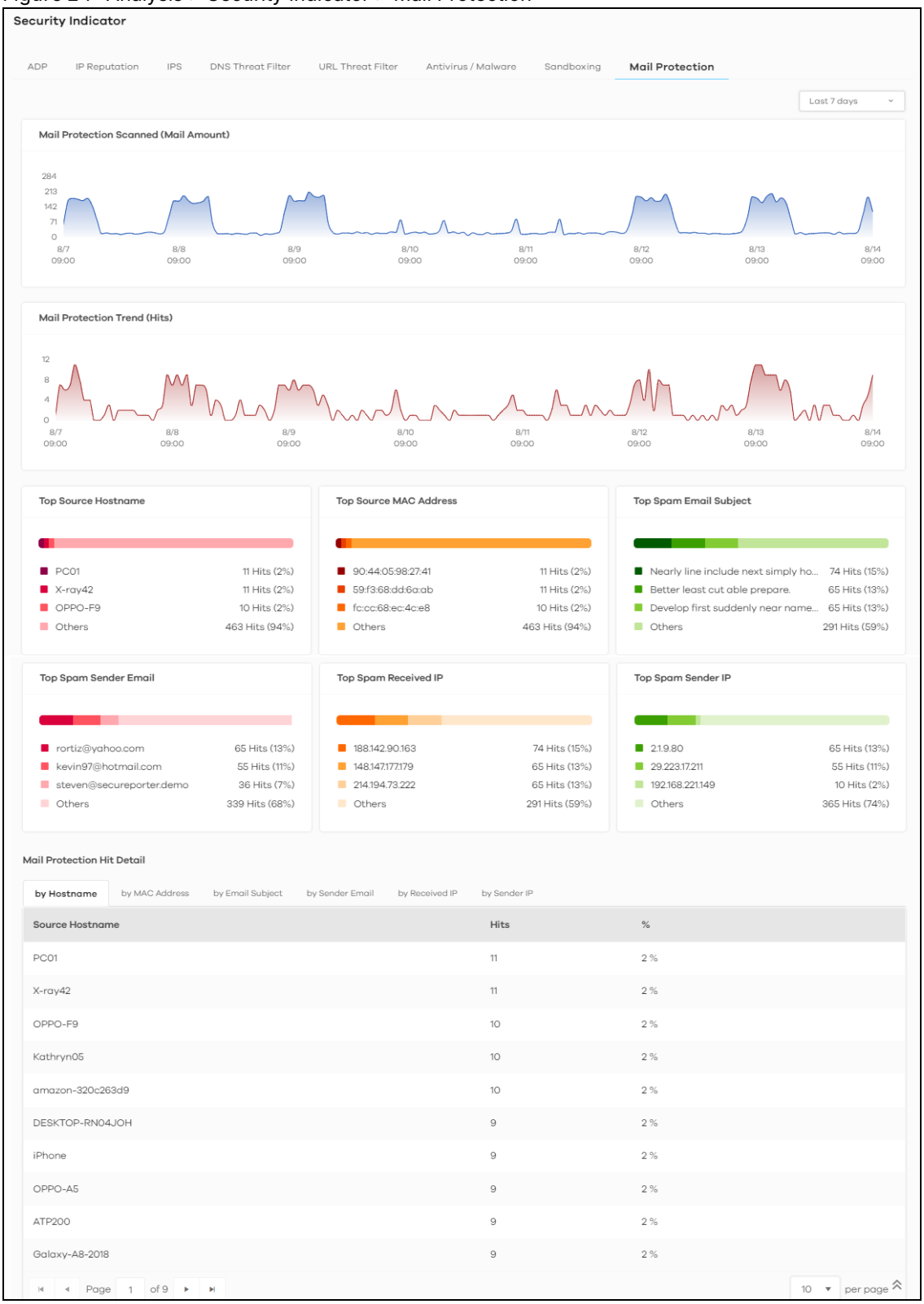
LABEL	DESCRIPTION
Sandboxing Scanned (File Amount)	This chart displays the total number of connections detected by the Zyxel Device. Move your cursor over a trend line to display the number of connections encountered over time.
Sandboxing Trend (Hits)	This chart displays the number of malicious and/or 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.

3.3.8 Mail Protection

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

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

Figure 24 Analysis > Security Indicator > Mail Protection



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

Table 18 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.

3.4 Network Activity

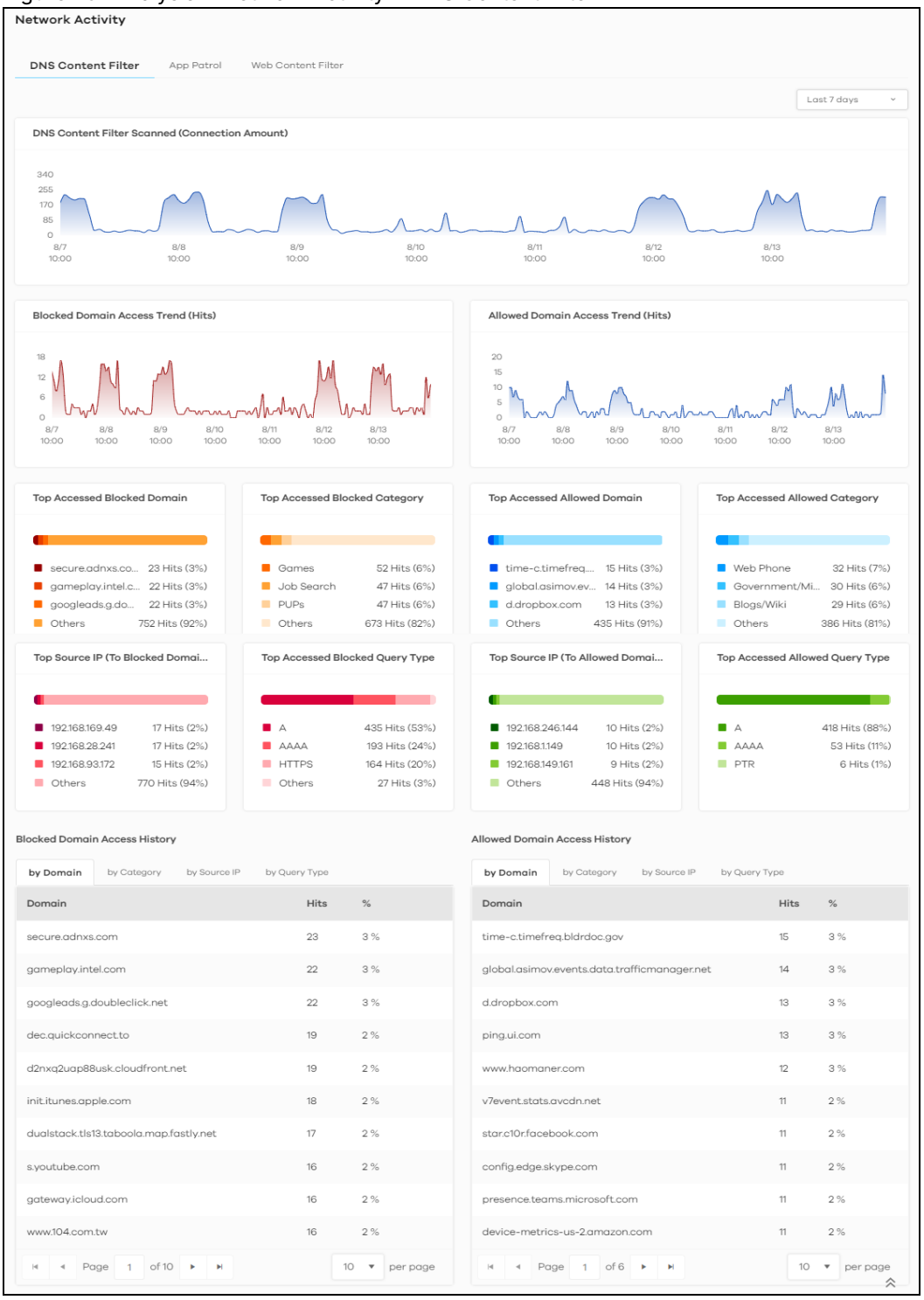
Network Activity data visualizations are categorized as:

- DNS Content Filter
- App Patrol
- Web Content Filter

3.4.1 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 25 Analysis > Network Activity > DNS Content Filter



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

Table 19 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.

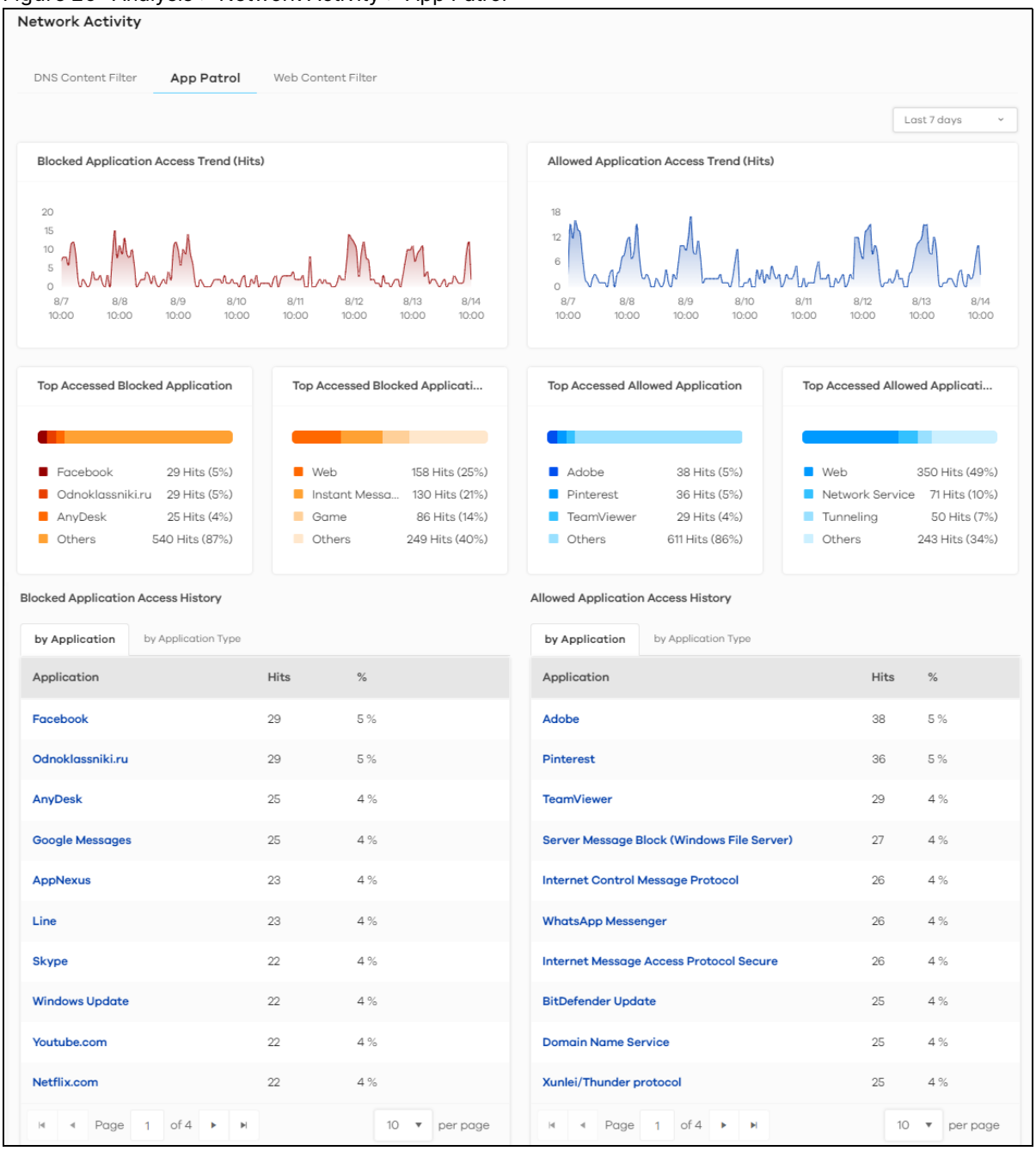
3.4.2 App Patrol

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 Activity > App Patrol data visualizations.

Figure 26 Analysis > Network Activity > App Patrol



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

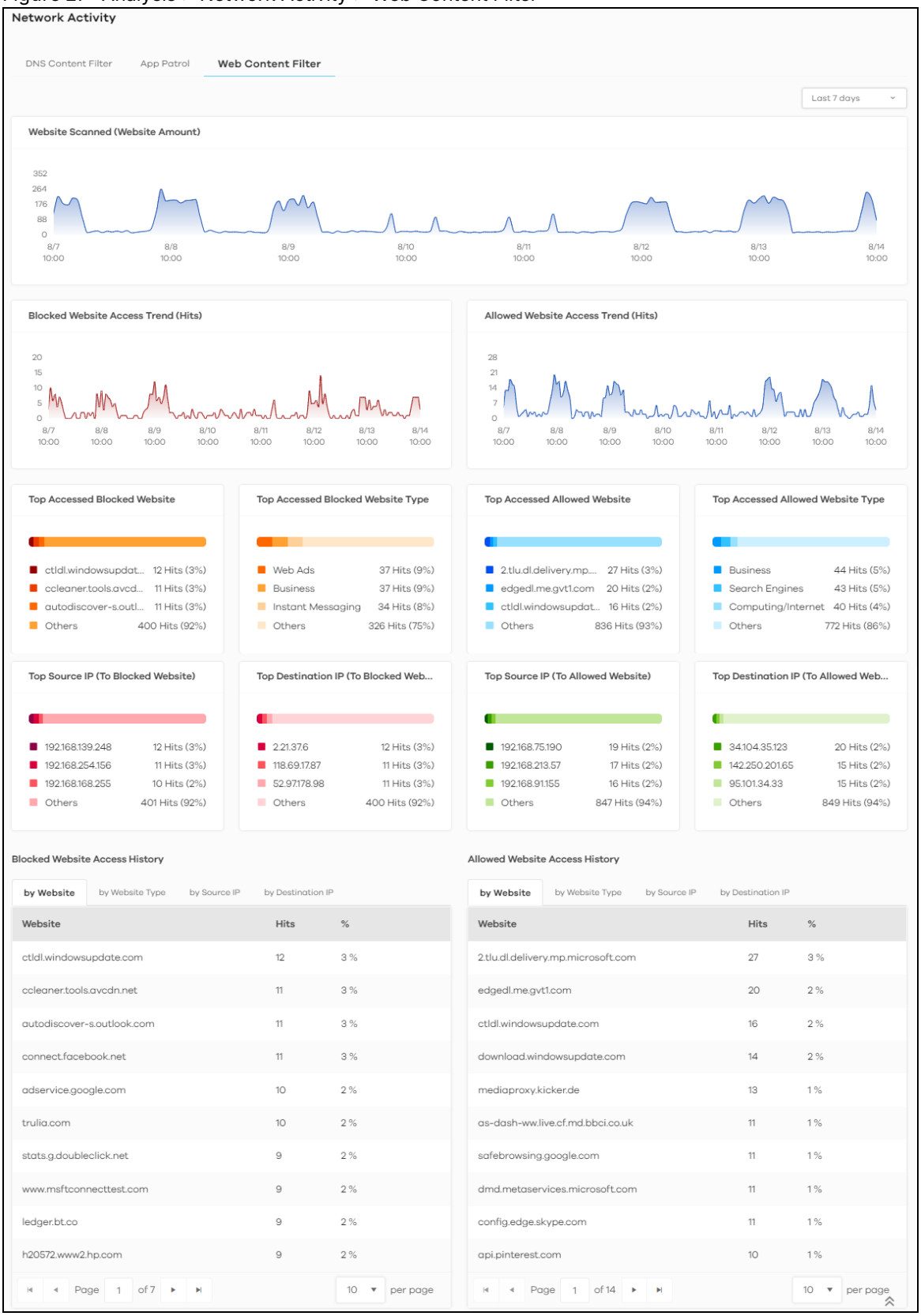
Table 20 Analysis > Network Activity > App Patrol

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.

3.4.3 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 Activity > Web Content Filter data visualizations.

Figure 27 Analysis > Network Activity > Web Content Filter



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

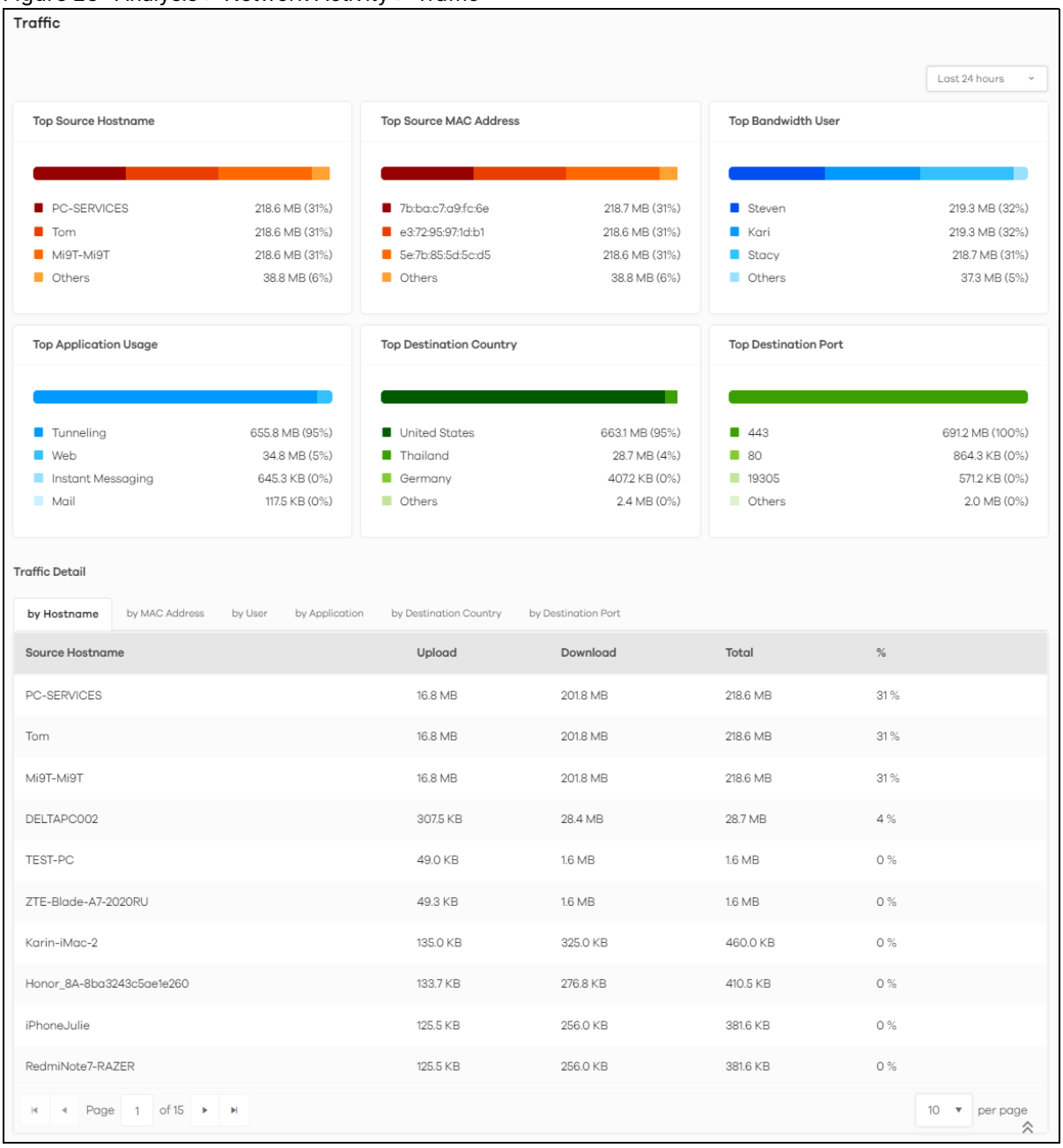
Table 21 Analysis > Network Activity > Web Content Filter

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.

3.5 Traffic

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

Figure 28 Analysis > Network Activity > Traffic



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

Table 22 Analysis > Network Activity > 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.

3.6 Device

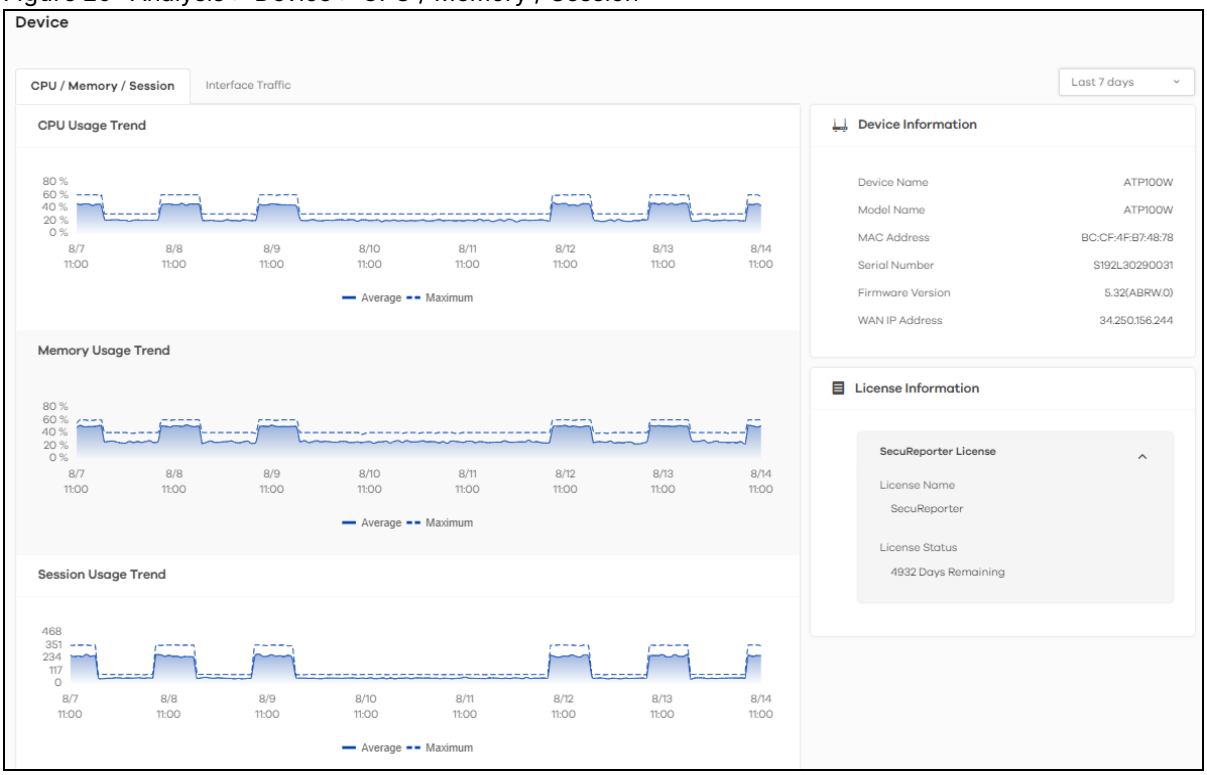
Device data visualizations are categorized as:

- CPU/Memory/Session
- Interface Traffic

3.6.1 CPU/Memory/Session

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

Figure 29 Analysis > Device > CPU / Memory / Session



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

Table 23 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. This displays Active if you are using a PAYG license.

3.6.2 Interface Traffic

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

Figure 30 Analysis > Device > Interface Traffic

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

Table 24 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 4
Logs

4.1 Overview

SecuReporter saves logs of your Zyxel Device every 10 minutes.

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

- See Table 2 on page 8 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.

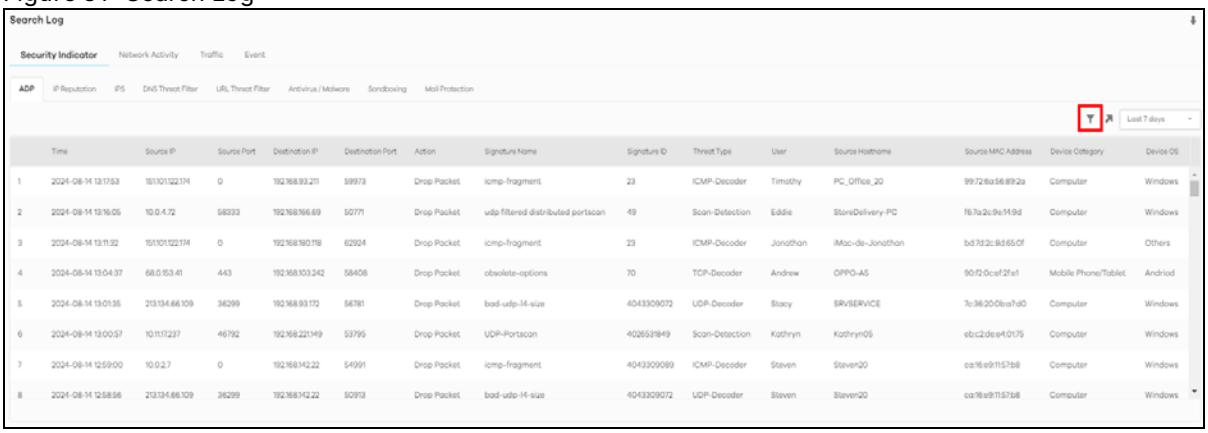
Note: Sandboxing logs will be removed after you reboot the Zyxel Device.

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.

4.2 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 must enable logs to be sent to SecuReporter in the Web Configurator of the Zyxel Device or NCC. 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 27 on page 84 for details.

Figure 31 Search Log



You can set the search log criteria by clicking , see Table 27 on page 84 for details.

The screen displays 100 search results at a time. Scroll down to load the next 100.

4.2.1 Log Search Privileges

This table summarizes the SecuReporter log search privileges:

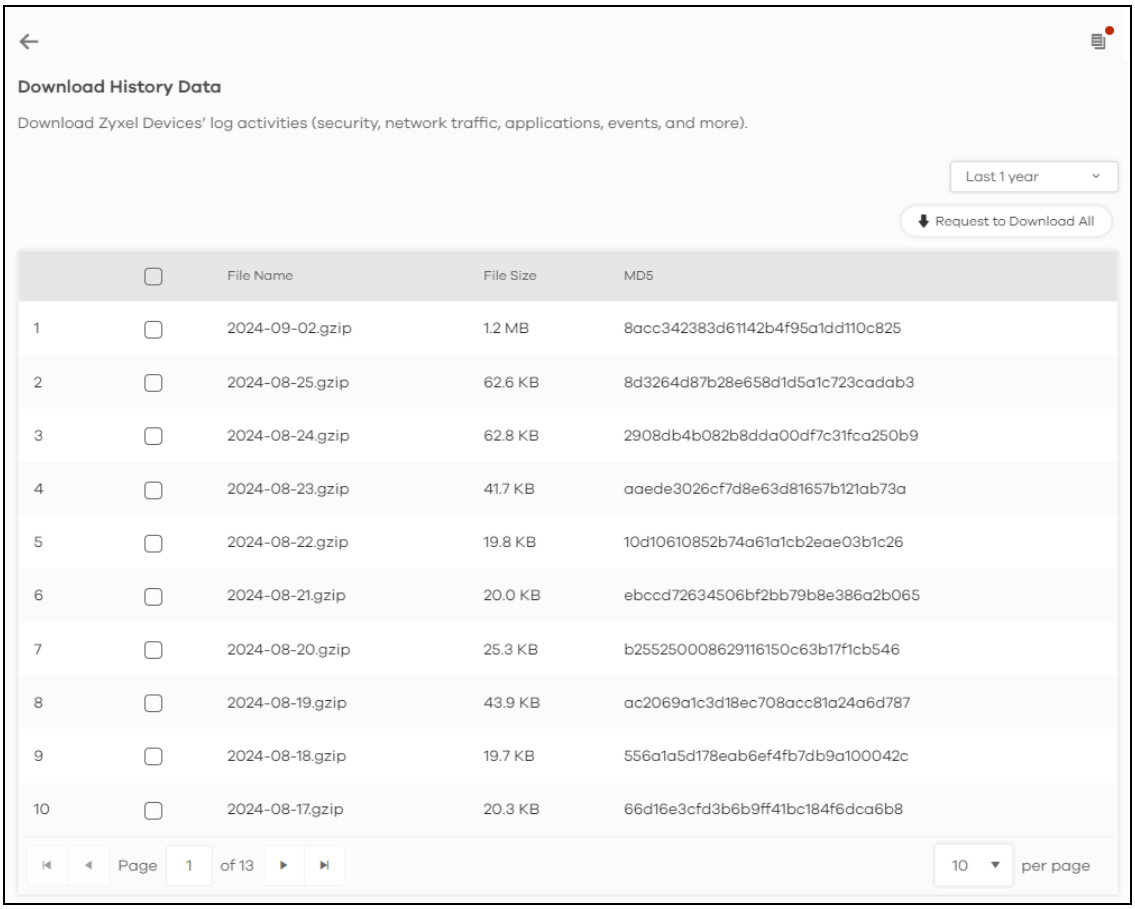
Table 25 SecuReporter Log Search Privileges

TYPE	SECUREPORTER
Security Logs Date Range	Past 30 days
Traffic Logs Date Range	Past 7 days
Custom Range	Yes
Filters	Yes
CSV file download	Yes

4.2.2 Download Logs

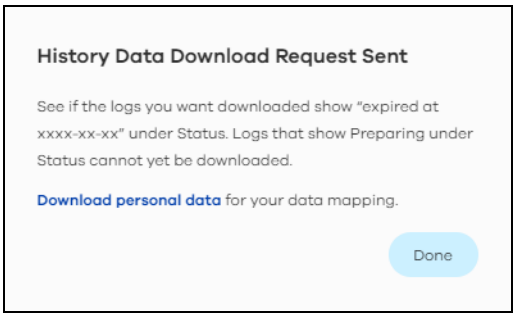
You can download the Zyxel Device's logs by doing the following steps.

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.

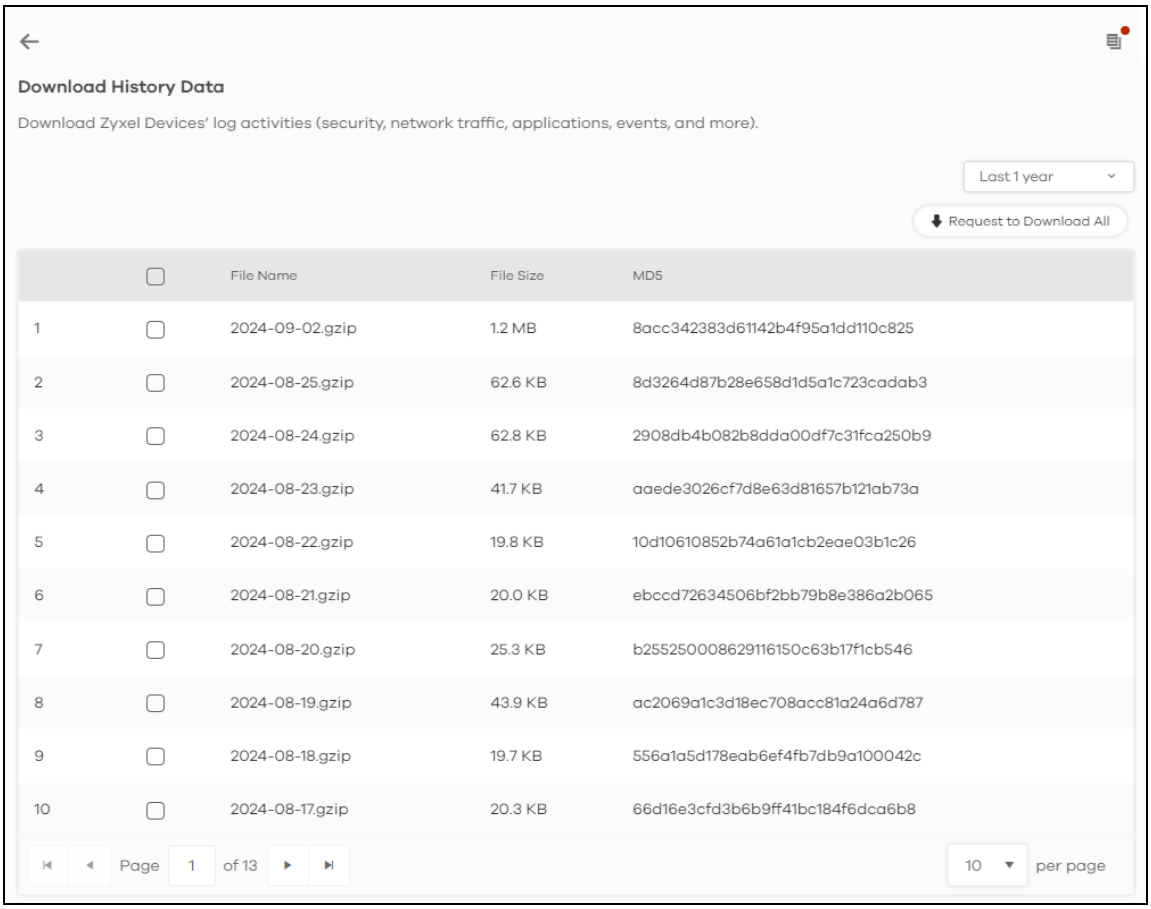


	File Name	File Size	MD5
1	2024-09-02.gzip	1.2 MB	8acc342383d61142b4f95a1dd110c825
2	2024-08-25.gzip	62.6 KB	8d3264d87b28e658d1d5a1c723cadab3
3	2024-08-24.gzip	62.8 KB	2908db4b082b8dda00df7c31fca250b9
4	2024-08-23.gzip	41.7 KB	aaede3026cf7d8e63d81657b121ab73a
5	2024-08-22.gzip	19.8 KB	10d10610852b74a61a1cb2eae03b1c26
6	2024-08-21.gzip	20.0 KB	ebccd72634506bf2bb79b8e386a2b065
7	2024-08-20.gzip	25.3 KB	b255250008629116150c63b17f1cb546
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.

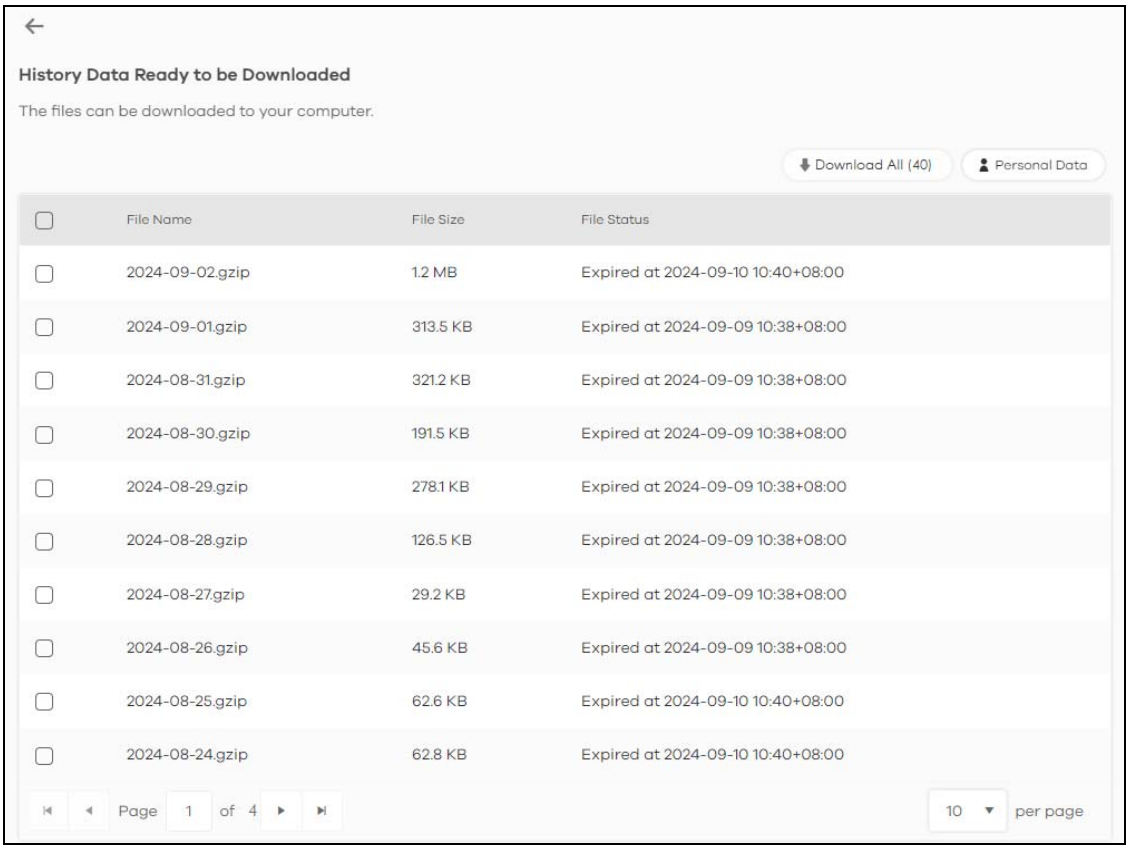


4 Click the History Data icon at the upper-right corner.

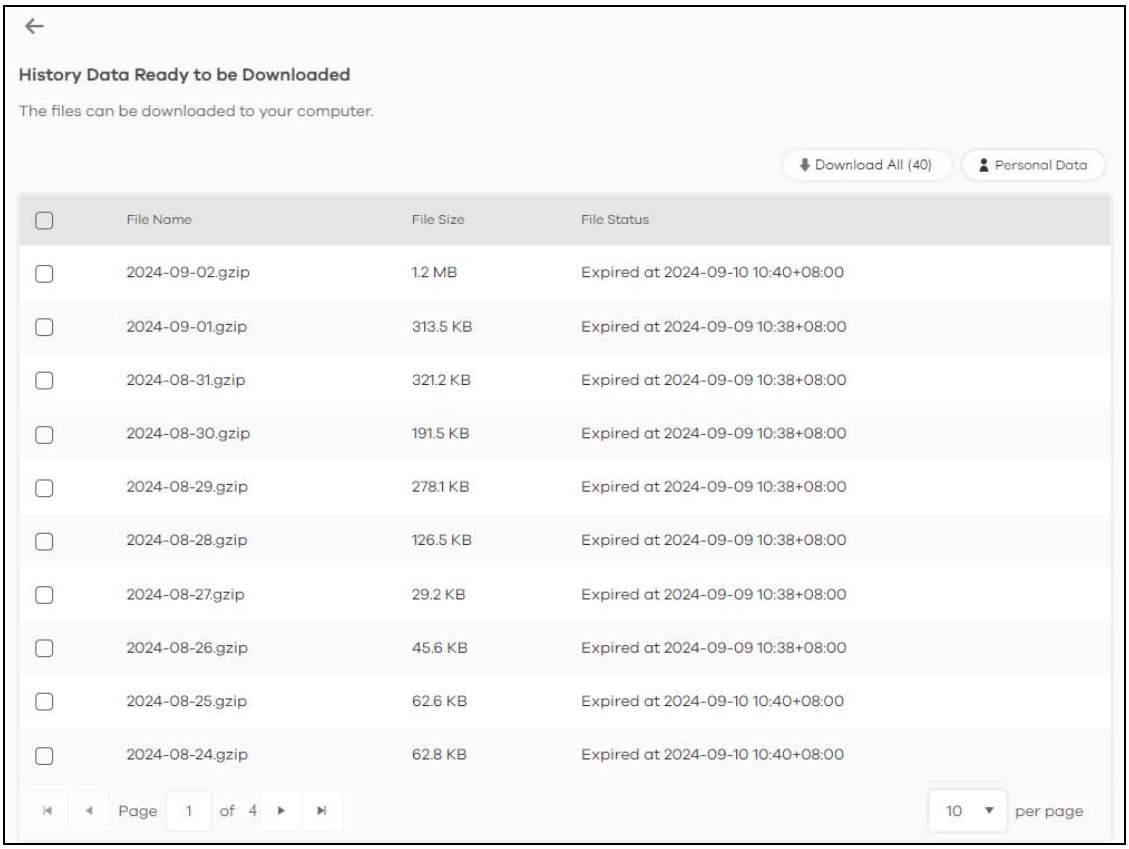


		File Name	File Size	MD5
1		2024-09-02.gzip	1.2 MB	8acc342383d61142b4f95a1dd110c825
2		2024-08-25.gzip	62.6 KB	8d3264d87b28e658d1d5a1c723cadab3
3		2024-08-24.gzip	62.8 KB	2908db4b082b8dda00df7c31fca250b9
4		2024-08-23.gzip	41.7 KB	aaede3026cf7d8e63d81657b121ab73a
5		2024-08-22.gzip	19.8 KB	10d10610852b74a61a1cb2eae03b1c26
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.



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.



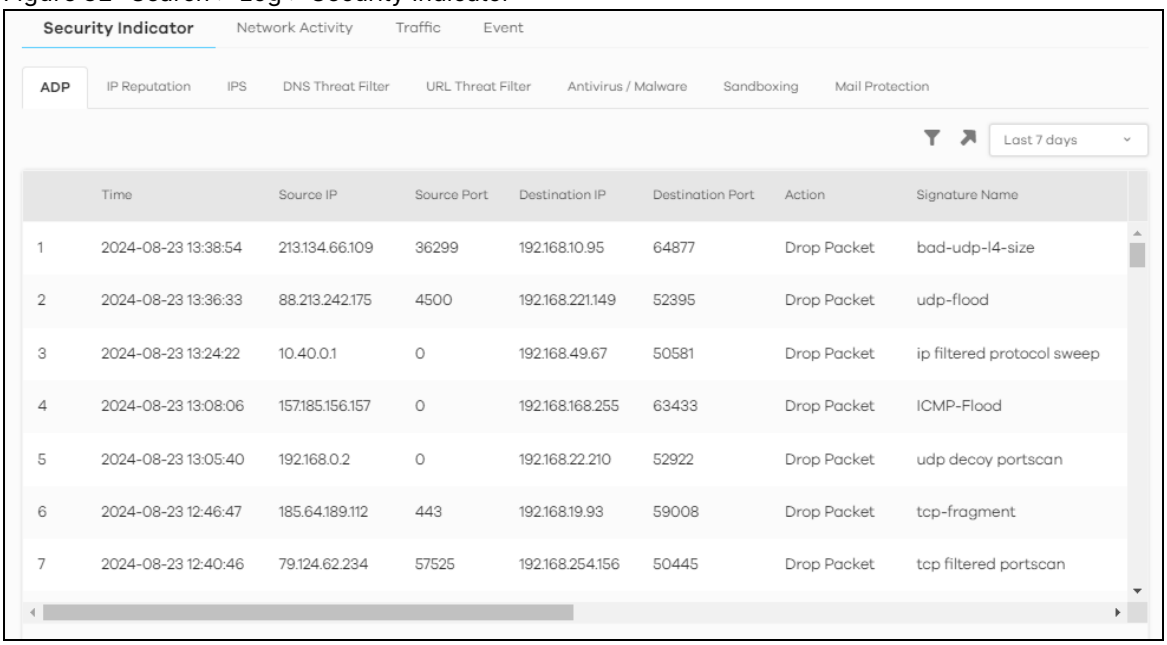
4.2.3 Security Indicator Logs

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 32 Search > Log > Security Indicator



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

Table 26 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 26 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 26 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 sandboxing 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 2.2.1 on page 21 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 2.2.1 on page 21 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 2.2.1 on page 21 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.

Table 26 Search > Log > Security Indicator Screen (continued)

LABEL	DESCRIPTION
Mail Subject	This is the title header of the incoming email.
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 sandboxing 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 sandboxing 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.

Table 26 Search > Log > Security Indicator Screen (continued)

LABEL	DESCRIPTION
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.
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.

Table 26 Search > Log > Security Indicator Screen (continued)

LABEL	DESCRIPTION
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 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.

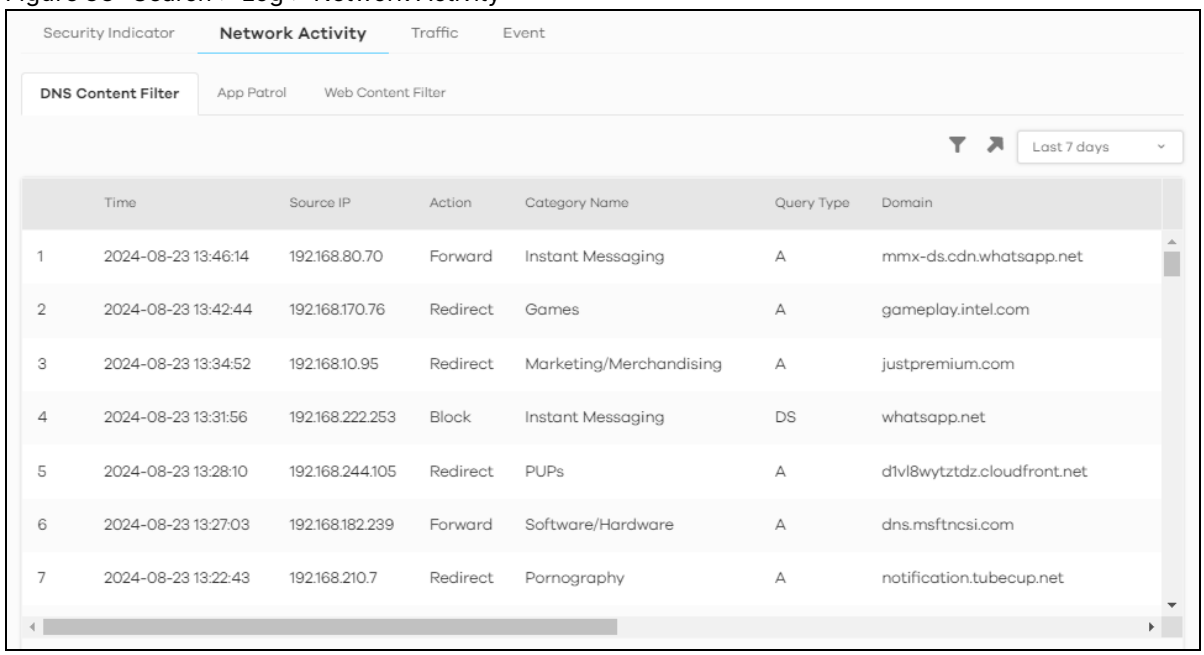
4.2.4 Network Activity Logs

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 33 Search > Log > Network Activity



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

Table 27 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.

Table 27 Search > Log > Network Activity 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 (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.
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 2.2.1 on page 21 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.

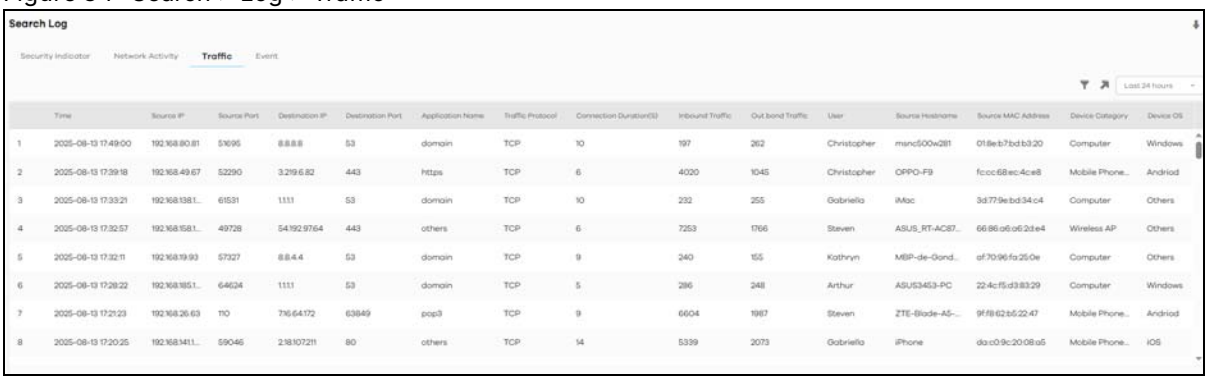
Table 27 Search > Log > Network Activity Screen (continued)

LABEL	DESCRIPTION
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.
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 operating system of the original sender of the packet.

4.2.5 Traffic Logs

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

Figure 34 Search > Log > Traffic



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

Table 28 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).

Table 28 Search > Log > Traffic (continued)

LABEL	DESCRIPTION
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.
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 2.2.1 on page 21 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. You see this only if devices on your network are using Astra, which is an email identification service that helps trace suspicious traffic back to the specific user account.
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 operating system of the original sender of the packet.

4.2.6 Event Logs

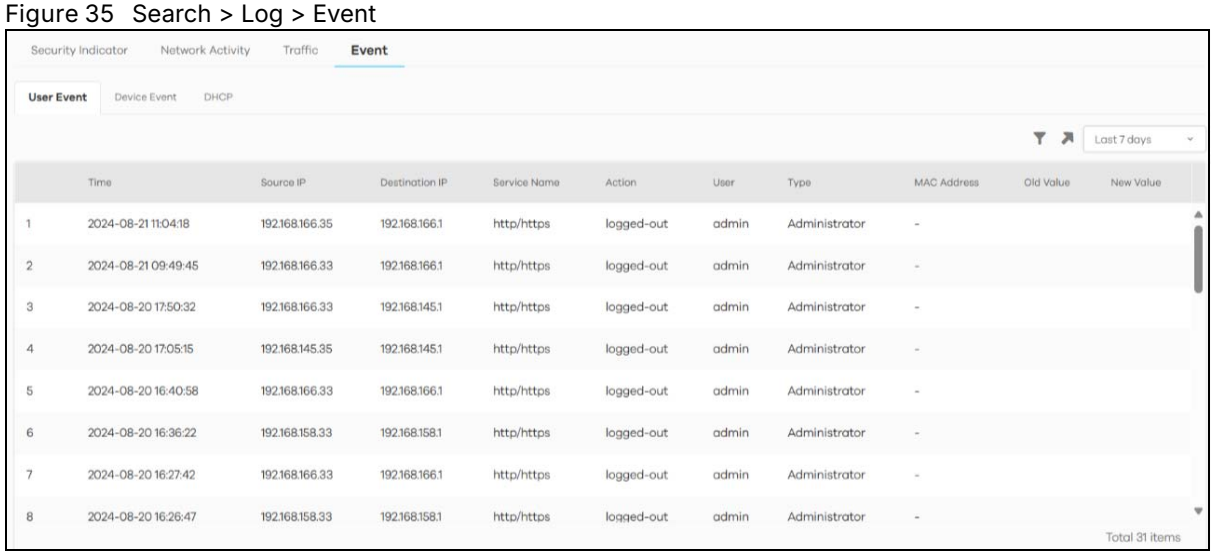
Event logs are categorized as follows:

- User Login

- Device Event
- DHCP

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

Figure 35 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	-		

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

Table 29 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.

Table 29 Search > Log > Event 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).
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 2.2.1 on page 21 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 2.2.1 on page 21 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 29 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 2.2.1 on page 21 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 2.2.1 on page 21 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.

4.3 Search Activity

The Search > Activity screen allows administrators to look up network activity by:

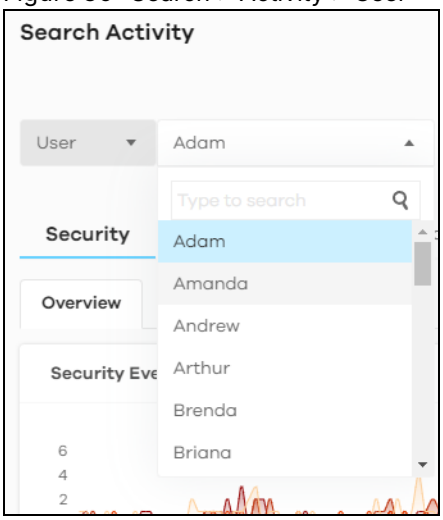
- User
- IP address
- MAC address or
- Hostname of the client device.

For each item, you can see related Security, Network, Traffic and Account (not for Hostname) information.

To perform a search, click Search > Activity.

For a search, first select one of the above items. You may also enter a partial term to generate a list of matching results.

Figure 36 Search > Activity > User



For each item above, you may perform related searches for Security, Network, Traffic or Account.

Table 30 Search Activities

SECURITY		NETWORK	TRAFFIC	ACCOUNT
• Overview	• URL Threat Filter	• DNS Content Filter	Top Destination Country	• All
• ADP	• Antivirus / Malware	• App Patrol	Top Destination Port	• Sign In
• IP Reputation	• Sandboxing	• Web Content Filter		• Sign in Failed
• IPS	• Mail Protection			• Sign Out
• DNS Threat Filter				

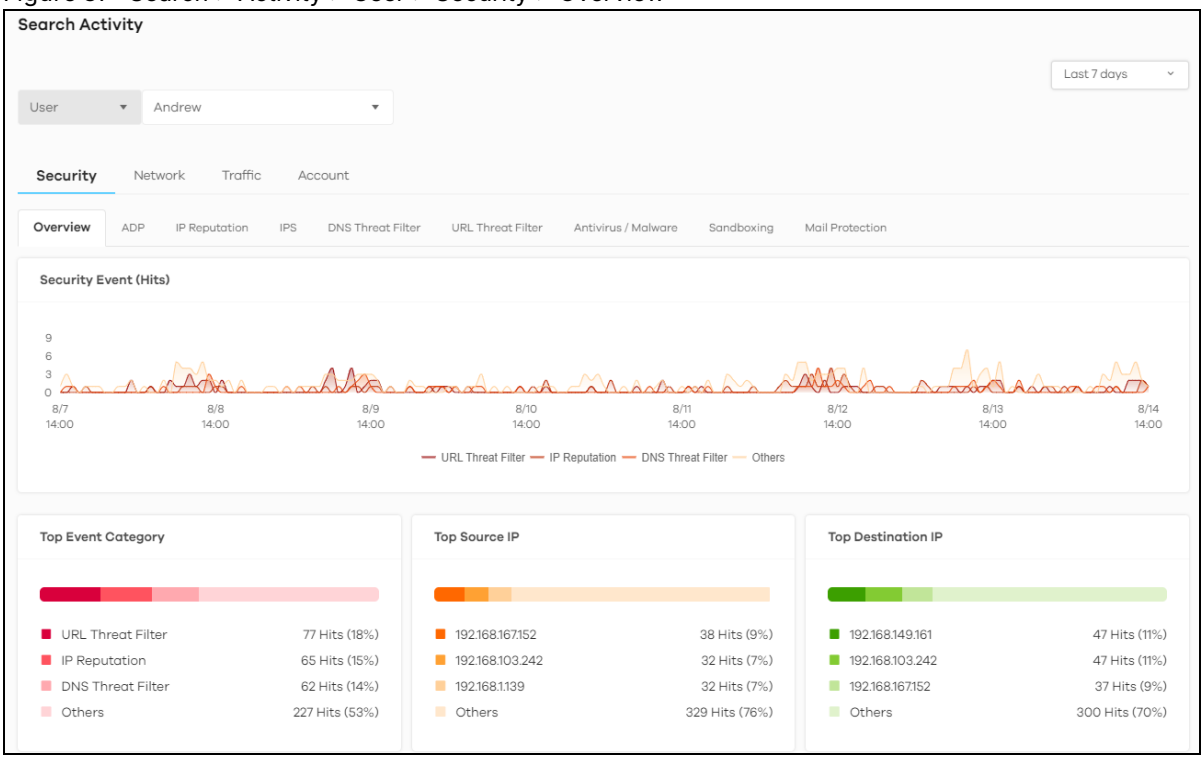
4.3.1 Security Search

Security searches include:

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

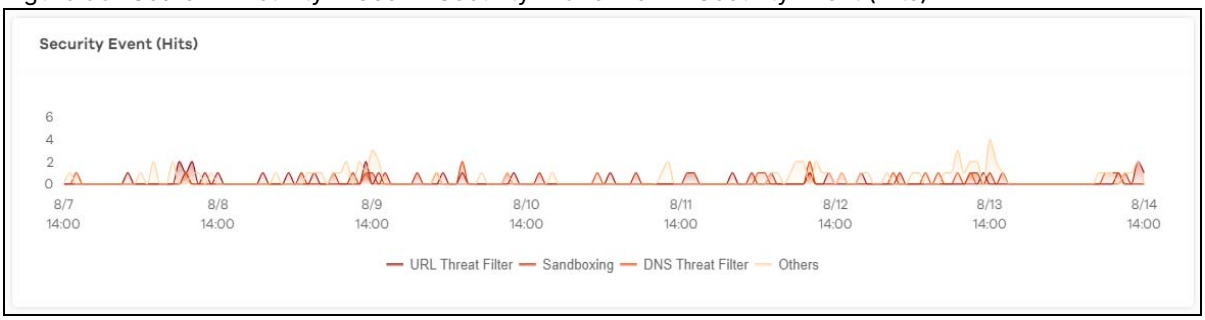
For a User, click Search > Activity > User > Security > Overview to display the following figure.

Figure 37 Search > Activity > User > Security > Overview



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 38 Search > Activity > User > Security > Overview > Security Event (Hits)



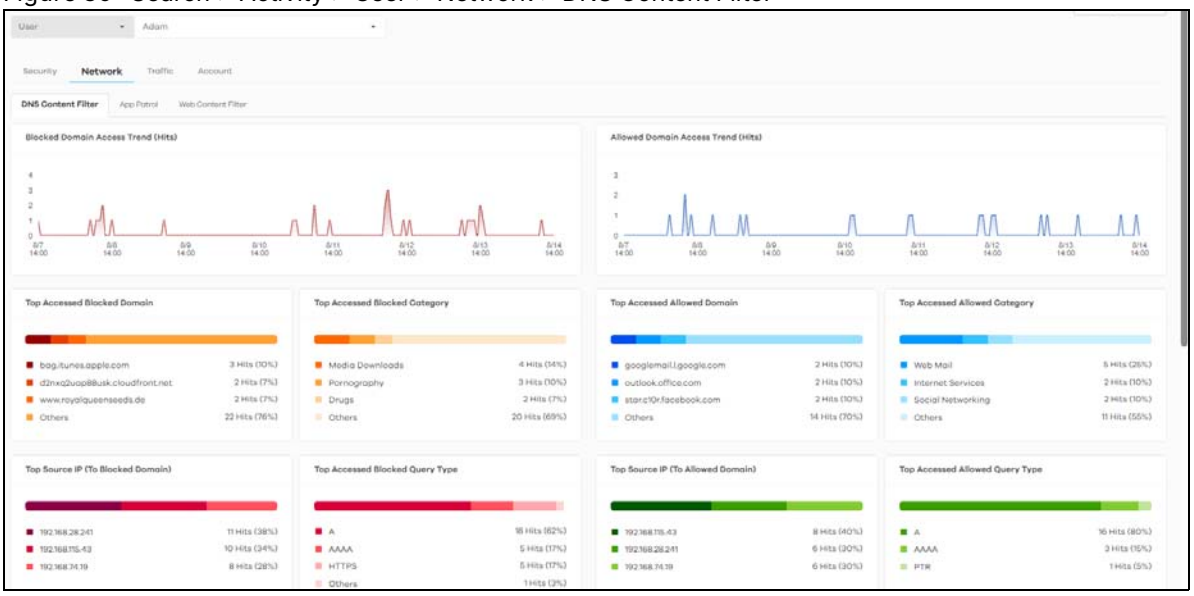
4.3.2 Network Search

Network searches include:

- DNS Content Filter
- App Patrol
- Web Content Filter

For a User, click Search > Activity > User > Network > DNS Content Filter to display the following figure.

Figure 39 Search > Activity > User > Network > DNS Content Filter

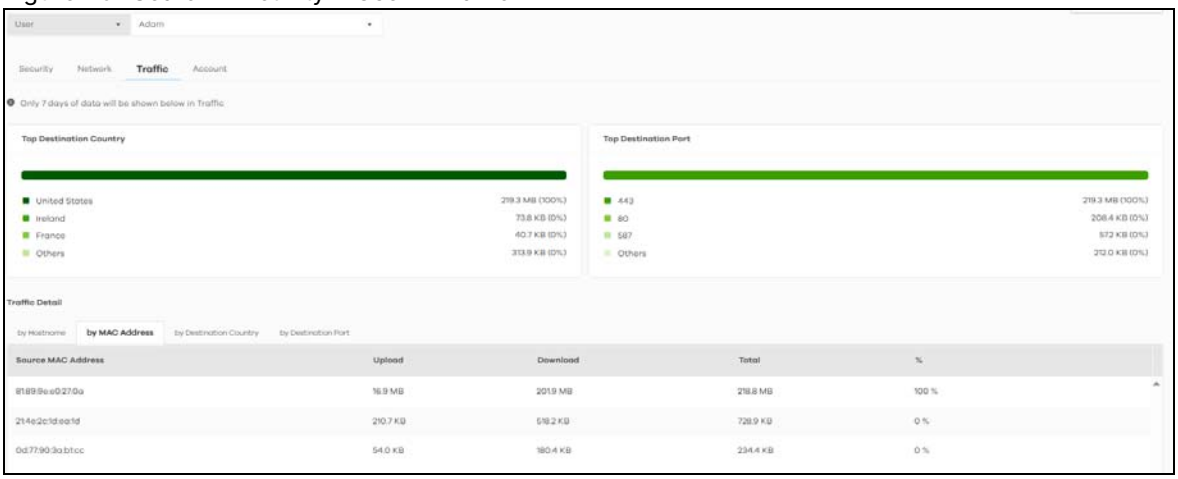


4.3.3 Traffic Search

Traffic searches are for up to seven days of data.

For a User, click Search > Activity > User > Traffic to display the following figure.

Figure 40 Search > Activity > User > Traffic



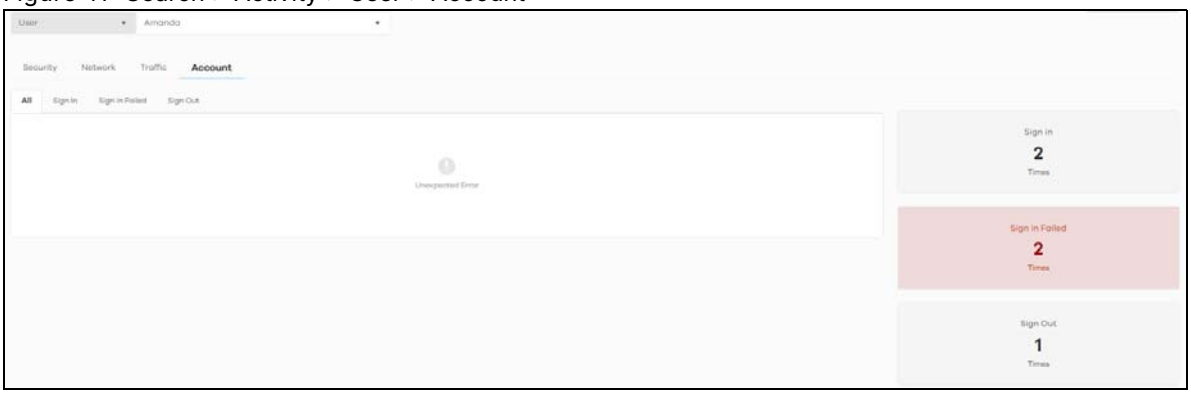
4.3.4 Account Search

Account searches include:

- All
- Sign In
- Sign in Failed
- Sign Out

For a User, click Search > Activity > User > Account to display the following figure.

Figure 41 Search > Activity > User > Account



CHAPTER 5
Alerts

5.1 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.

5.2 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.

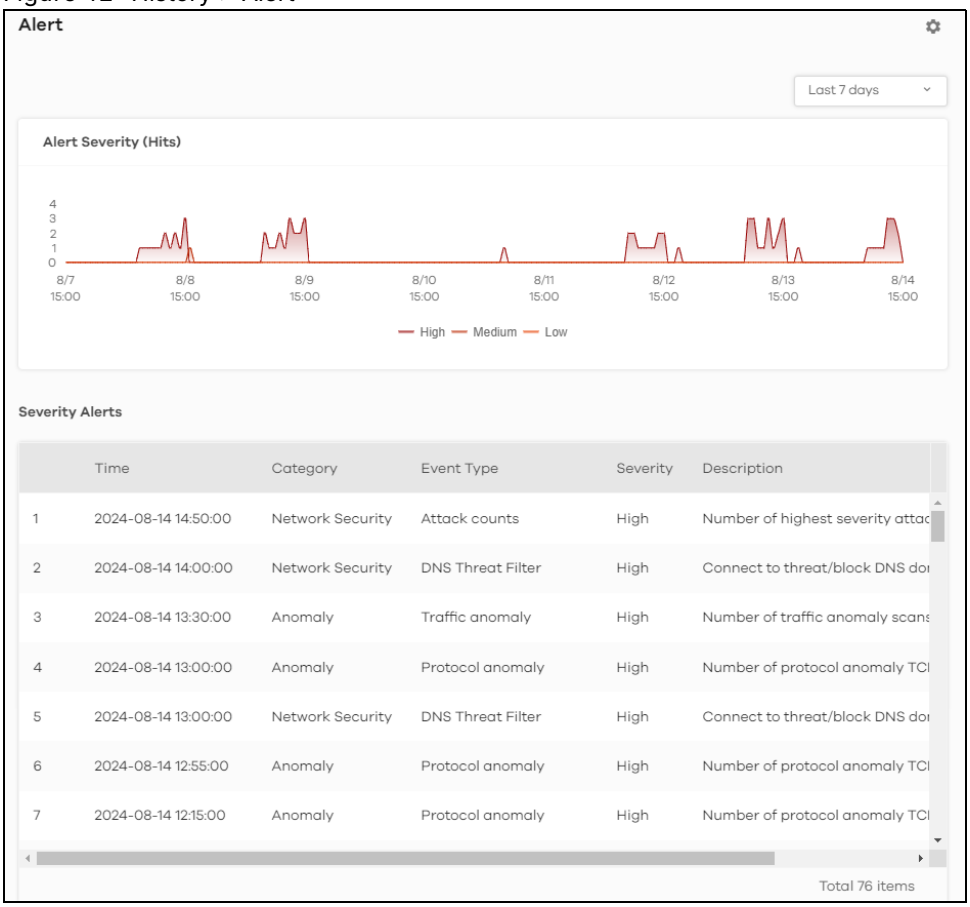
Table 31 Event Categories, Types and Criteria

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 31 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 42 History > Alert



The following table describes the labels on this screen.

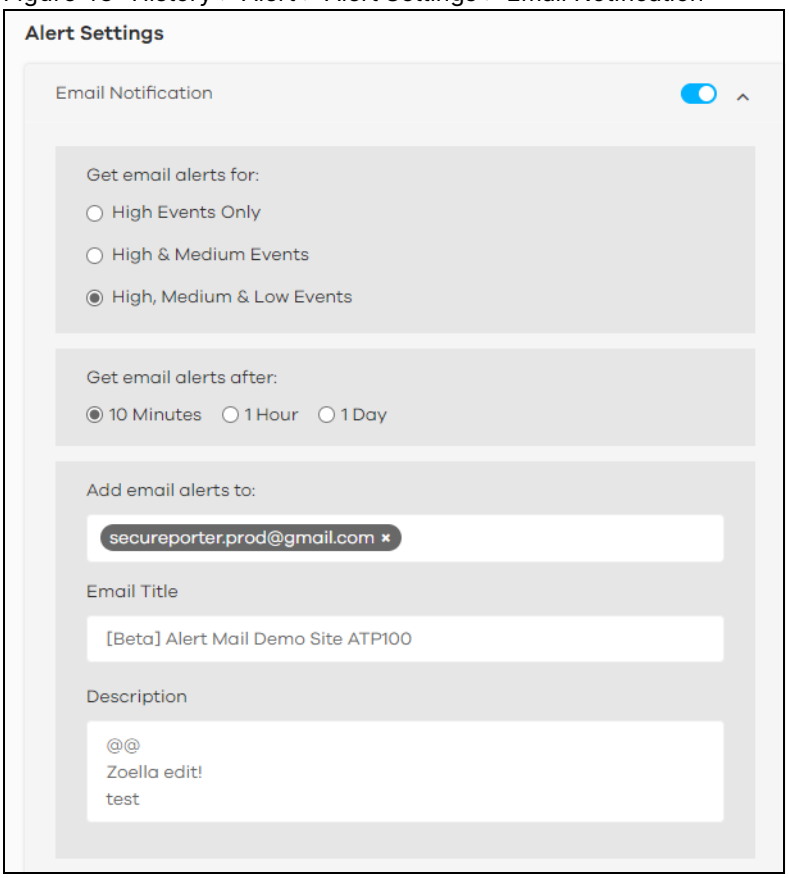
Table 32 History > Alert

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 9 on page 16.
Description	This displays the further information on this alert.

5.3 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 43 History > Alert > Alert Settings > Email Notification



The following table describes the labels in this screen.

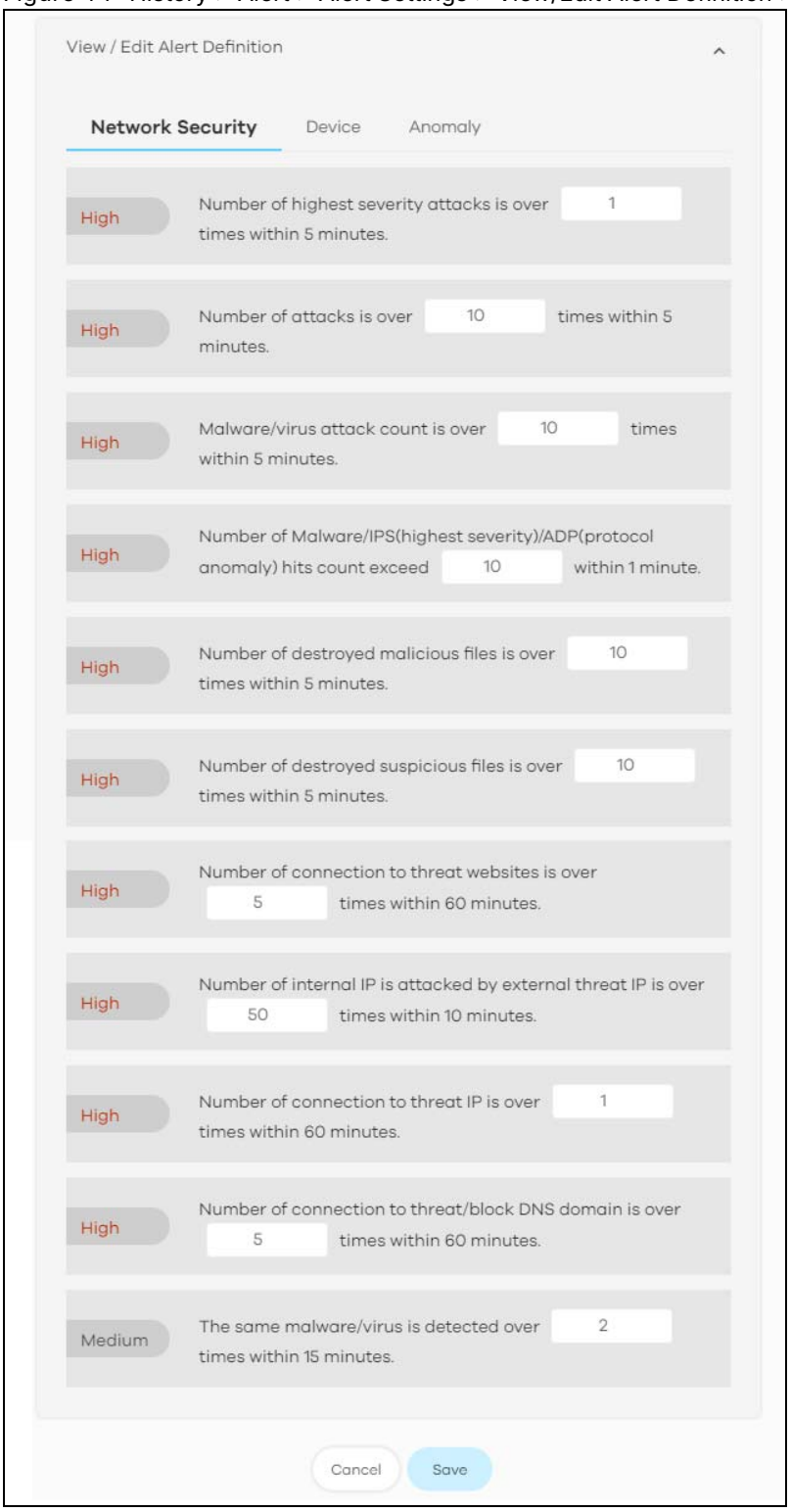
Table 33 History > Alert > Alert Settings > Email Notification

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.

Table 33 History > Alert > Alert Settings > Email Notification (continued)

LABEL	DESCRIPTION
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 44 History > Alert > Alert Settings > View/Edit Alert Definition > Network Security



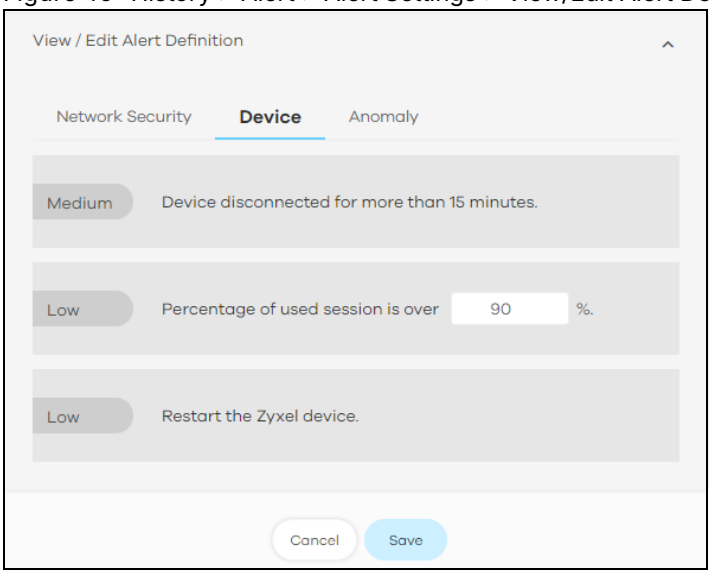
The following table describes the labels in this screen.

Table 34 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 45 History > Alert > Alert Settings > View/Edit Alert Definition > Device

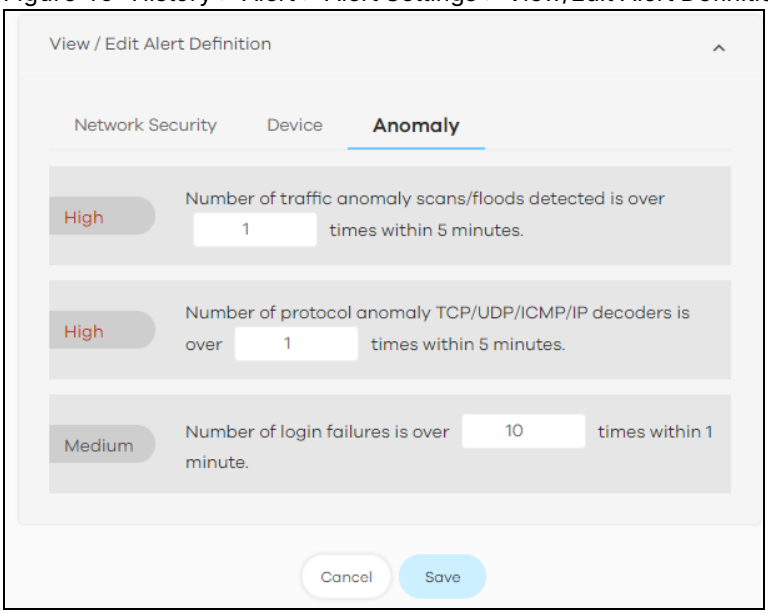


The following table describes the labels in this screen.

Table 35 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 46 History > Alert > Alert Settings > View/Edit Alert Definition > Anomaly



The following table describes the labels in this screen.

Table 36 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 6
Report

6.1 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.

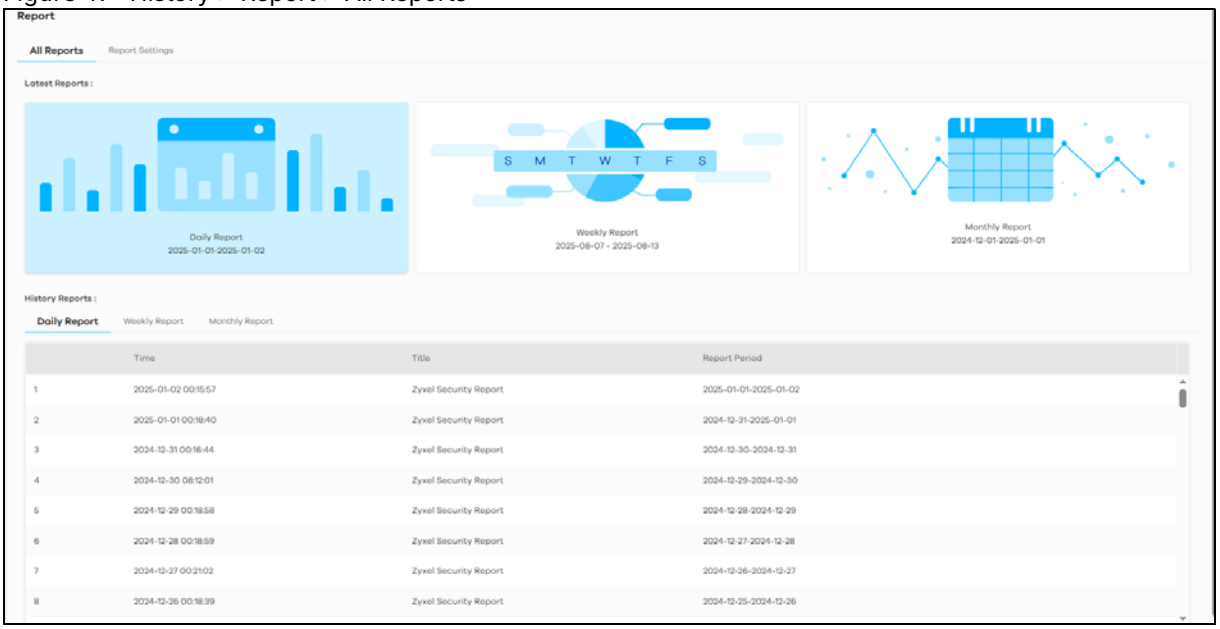
You can choose to generate reports of analyzed data collected over one of three time frames:

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

6.2 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 47 History > Report > All Reports



The following table describes the labels on this screen.

Table 37 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.
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.

6.3 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.

6.3.1 Smart Summaries

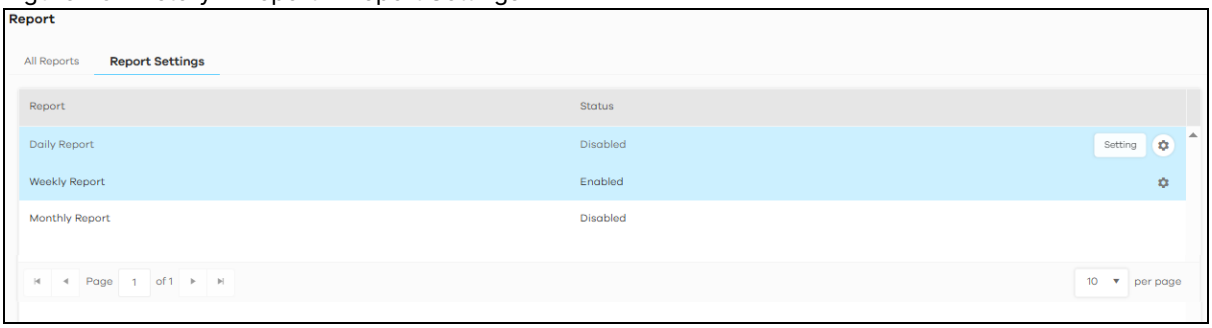
AI generates smart summaries based on the (raw) data collected from the weekly report. Created summaries allow you to identify key insights quickly and act promptly if need be.

Recommendations and possible causes are provided for abnormal security detection events based on data evidence, such as a significant increase in ADP, IPS, URL Threat Filter, or Sandboxing threats.

The smart summaries feature is enabled by default and included in the report notification email. When network performance is normal, no recommendations are given.

Note: At the time of writing, smart summaries and report scheduling are available for weekly reports only.

Figure 48 History > Report > Report Settings



The following table describes the labels on this screen.

Table 38 History > Report > Report Settings

LABEL	DESCRIPTION
Report	This displays the report type: daily, weekly or monthly report.
Status	This displays whether this report type is enabled or disabled.
Setting	Click this icon to go to a screen to enable or disable the report, configure a cover page, configure what contents to display, and configure who to send it to.
Cancel	Click Cancel to restore your previously saved settings.
Save	Click Save to save your changes.

Figure 49 History > Report > Report Settings > Weekly Report Settings

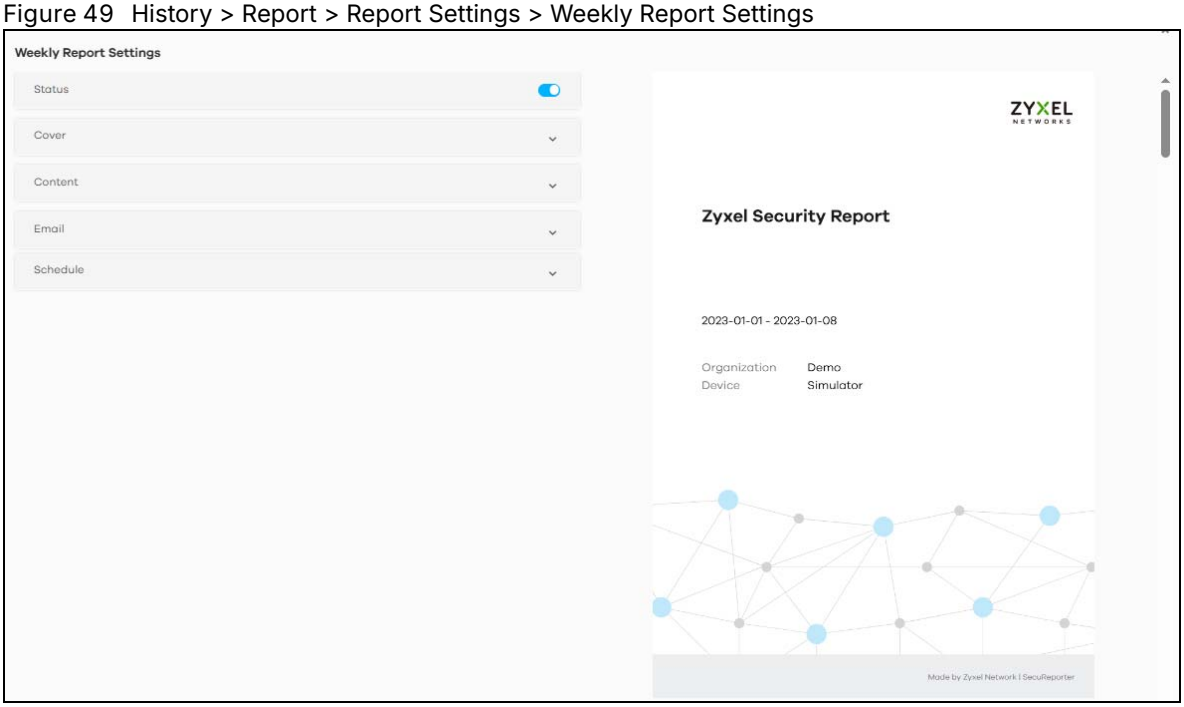
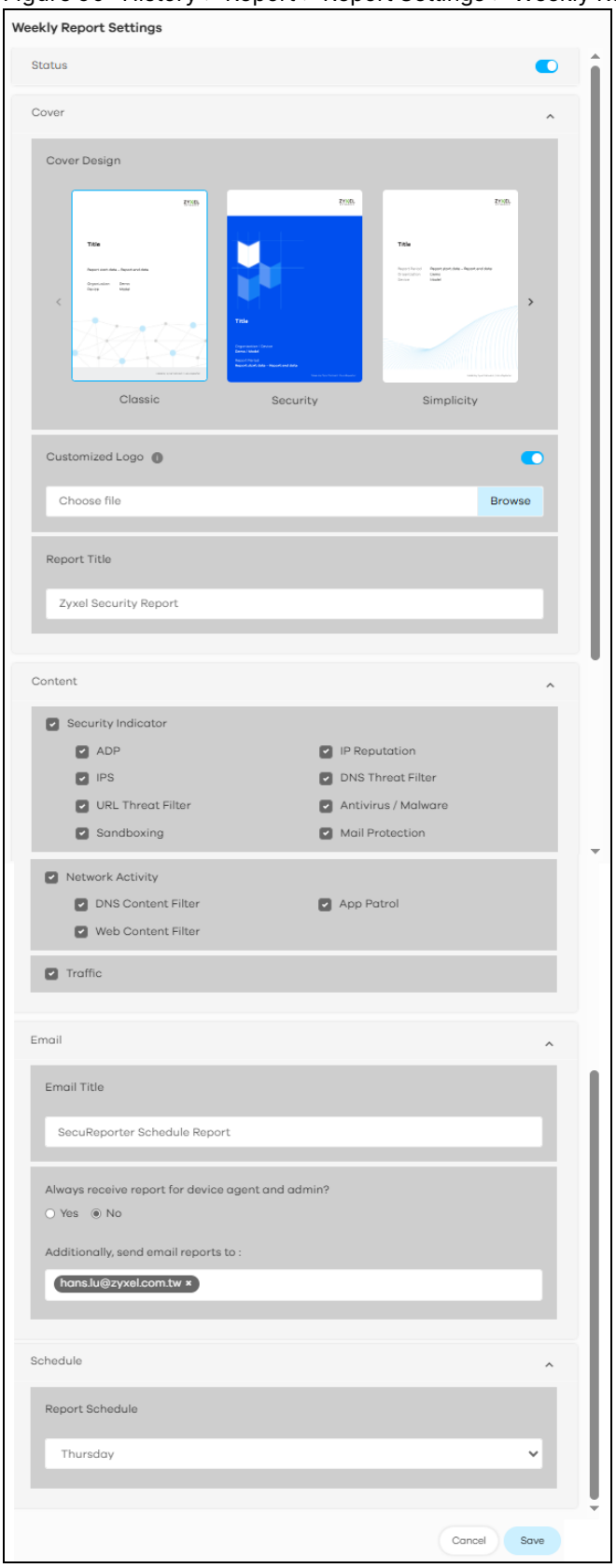


Figure 50 History > Report > Report Settings > Weekly Report Settings



The following table describes the labels on this screen.

Table 39 History > Report > Report Settings > Weekly 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 3 Analysis for a description of the widgets. Select an item (with check mark) to include it in the report profile.
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 8 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) Inform recipients to first check their email junk/spam folder for SecuReporter reports and to then classify them as not junk/spam, so that they may be received in the email Inbox.
Schedule	You can only schedule weekly reports.
Report Schedule	Select a day of the week to have reports sent.
Cancel	Click Cancel to restore your previously saved settings.
Save	Click Save to save your changes.

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 7 for the supported Zyxel Devices.
- Make sure the firmware version of your Zyxel Device supports SecuReporter. See Section 1.1.1 on page 7 for the supported firmware versions.
- Make sure you activated the SecuReporter license at myZyxel. See Section 1.2 on page 9 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 2.2 on page 20 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 8 for the Zyxel Devices that support sandboxing.

Some file types cannot be inspected through sandboxing.

Sandboxing 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 Table 3 on page 8 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 didn't receive any reports even though I added my email address in the Report Settings.

- Check your email spam or junk folder for SecuReporter reports. If found, mark them as not spam to ensure future reports are delivered to your Inbox.
- Go to Report Settings and verify that the email address you entered is correct and properly formatted.

My report does not include Smart Summaries.

Smart summaries appear in the report notification email and are only generated when abnormal security detection events occur. If network activity is normal, the notification email will not include a smart summary.

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

B

C

D

E

F

G

H

I

J

L

M

N

O

P

Q

R

S

T

U

V

W

Z