

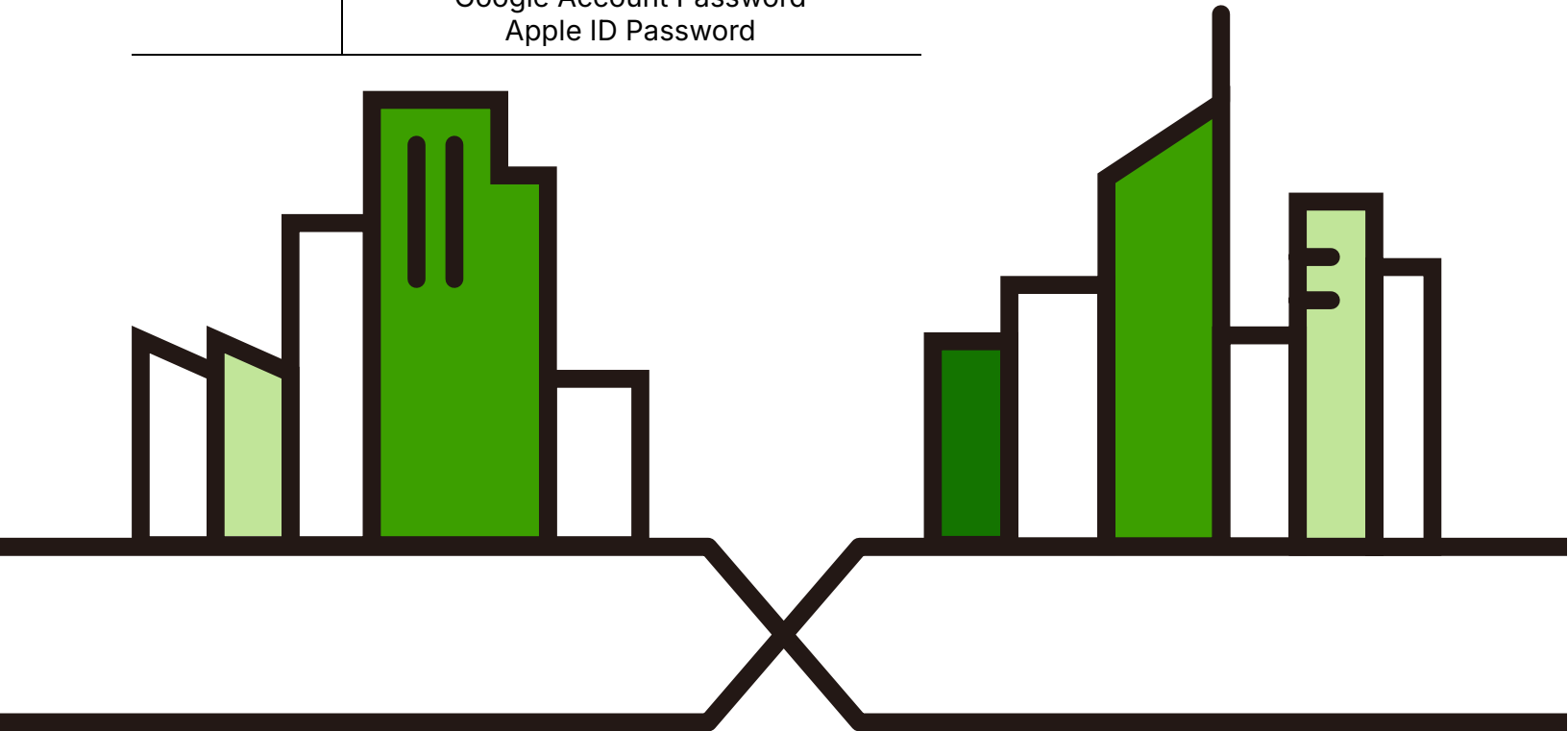
User's Guide

SecuReporter

Default Login Details

Version 2.5.26 Edition 1, 12/2025

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

Document Conventions	3
Table of Contents.....	4
Chapter 1	
Introduction.....	7
1.1 Overview	7
1.1.1 Supported Zyxel Devices and Firmware Versions	7
1.1.2 SecuReporter Management Privileges	8
1.1.3 License Options	8
1.1.4 Cloud Mode	9
1.2 Get Started	9
1.2.1 Set up Passkey	10
1.3 Title Bar	16
1.4 SecuPilot	17
1.4.1 View SecuPilot Conversation History	20
1.5 Threat History	21
1.6 Dashboard	22
1.6.1 Introduction to PAYG	24
Chapter 2	
Settings.....	26
2.1 Overview	26
2.2 Organization & Device	26
2.2.1 Add a Zyxel Device to an Organization	27
2.2.2 Claimed Device	30
2.2.3 Generate API Token	30
2.3 User Account	32
Chapter 3	
Analysis.....	35
3.1 Overview	35
3.1.1 Tutorial	35
3.1.2 Sandboxing	38
3.2 Analysis Overview	40
3.3 Security Indicators	40
3.3.1 ADP	41
3.3.2 IP Reputation	43
3.3.3 IPS	47
3.3.4 DNS Threat Filter	50

3.3.5 URL Threat Filter	55
3.3.6 Antivirus / Malware	59
3.3.7 Sandboxing	61
3.3.8 Mail Protection	63
3.4 Network Activity	65
3.4.1 DNS Content Filter	66
3.4.2 App Patrol	68
3.4.3 Web Content Filter	70
3.5 Traffic	73
3.6 Device	74
3.6.1 CPU/Memory/Session	74
3.6.2 Device Health Anomaly Detection	75
3.6.3 Interface Traffic	80
 Chapter 4	
Logs.....	83
4.1 Overview	83
4.2 Search Log	83
4.2.1 Log Search Privileges	84
4.2.2 Download Logs	84
4.2.3 Security Indicator Logs	88
4.2.4 Network Activity Logs	94
4.2.5 Traffic Logs	97
4.2.6 Event Logs	99
4.3 Search Activity	102
4.3.1 Security Search	103
4.3.2 Network Search	104
4.3.3 Traffic Search	105
4.3.4 Account Search	105
 Chapter 5	
Alerts	107
5.1 Overview	107
5.2 Trend & Details	107
5.3 Alert Settings	110
 Chapter 6	
Report.....	115
6.1 Overview	115
6.2 All Reports	115
6.3 Report Settings	116
6.3.1 Smart Summaries	116

Chapter 7
Troubleshooting 120
 7.1 Getting More Troubleshooting Help 123
Appendix A Customer Support 124
Appendix B Legal Information 129
Index..... 131

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	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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	<ul style="list-style-type: none"> 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.

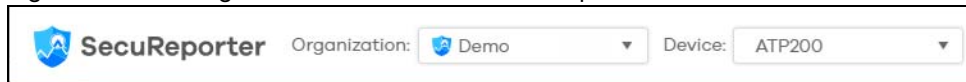
- 2 Register the Zyxel Devices using the same Zyxel Account. To open an account at Zyxel, go to <https://account.zyxel.com> and click Create an account, or sign in with your Google account, Apple account, Microsoft Entra ID, or Passkey.
- 3 After you register the Zyxel Devices, follow the on-screen instructions 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 26](#) 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



1.2.1 Set up Passkey

A passkey is a password-less login method that lets you log in using the same way you unlock your device — fingerprint, Face ID, or PIN. You can use passkeys to log into portals such as SecuReporter or NCC.

When you create a passkey, your computer or mobile device generates two keys:

- Public key – stored on the Zyxel server.
- Private key – stored locally on your computer or mobile device.

Your device's PIN or biometrics (for example, fingerprint, Face ID) is used only to unlock the private key, and is only stored locally on your computer or mobile device.

Note: The passkey limit for each account is shown below.

Table 6 Passkey Limit

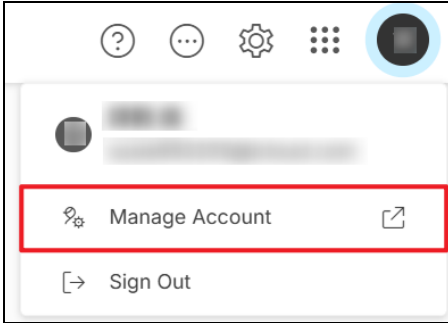
Maximum number of passkeys	5
----------------------------	---

Note: The following are the minimum computer or mobile device operating system and web browser version requirements to run passkey:

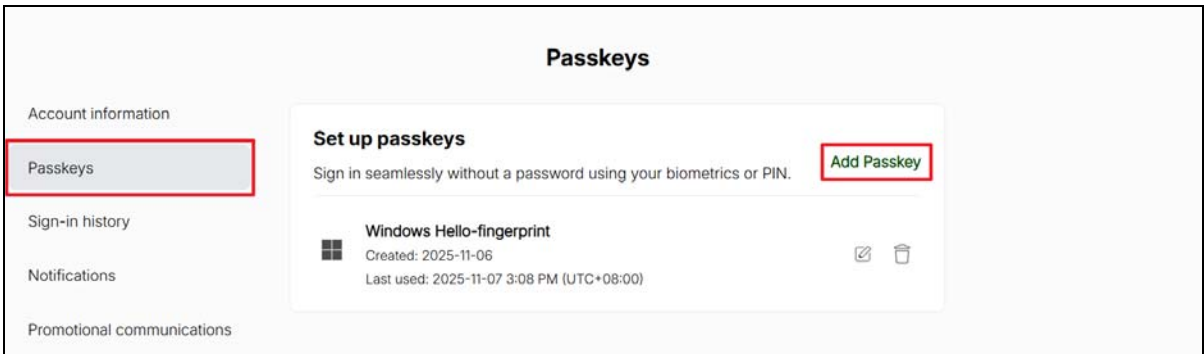
COMPUTER OS VERSION	MOBILE DEVICE OS VERSION	BROWSER VERSION
Windows 10 or later	iOS 16 or later	Chrome 109 or later
macOS 13 Ventura or later	iPadOS 16 or later	Safari 16.1 or later
ChromeOS 109 or later	Android 9 or later	Edge 109 or later

To set up passkey and sign in using your PIN or biometrics, do the following:

- 4 Log in to SecuReporter, click the Account icon at the top right corner, select Manage Account.



- 5 Go to the Passkeys tab and click Add Passkey.



- 6 Your device will prompt you to authenticate using biometrics (fingerprint / Face ID) or your PIN.

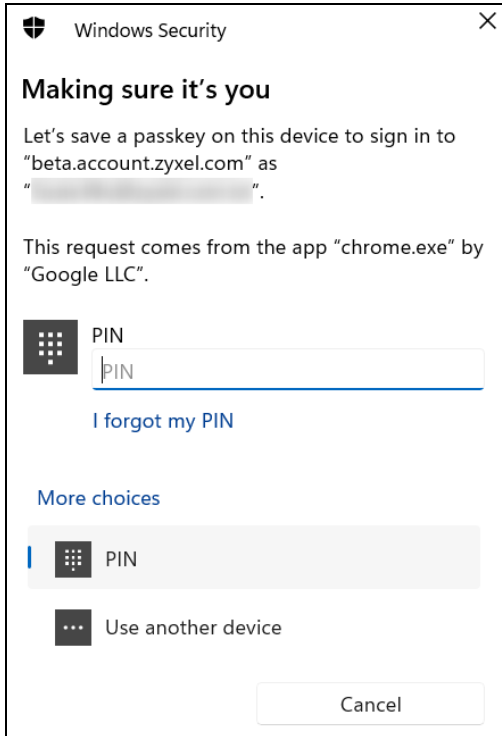
Note: Your device must have one of the following sign-in options enabled: PIN, fingerprint, or Face ID. To set up these sign-in options on your Windows computer, go to Settings > Accounts > Sign-in options.

Note: For biometrics, your computer or mobile device must have a fingerprint reader or camera for Face ID. If not, select the PIN option instead.

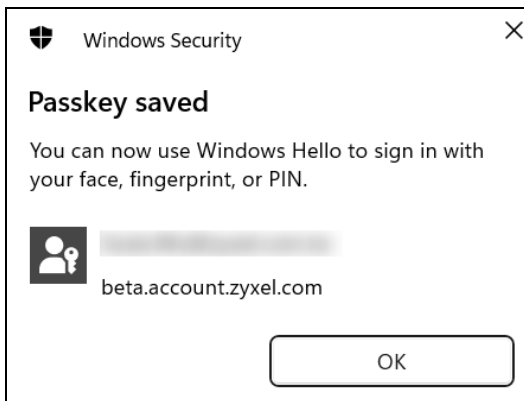
PIN Option

On a Windows computer, select PIN, and enter the 6-digit PIN that you already set on your device.

Note: The PIN option is only available on Windows computers as a Windows Hello sign-in method. If you're logging in from a mobile device, you will be prompted to use fingerprint or Face ID instead.

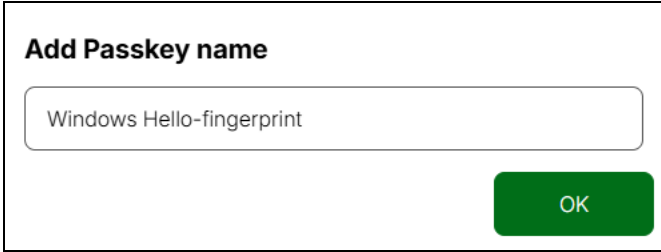


The passkey is now saved on this device for SecuReporter.



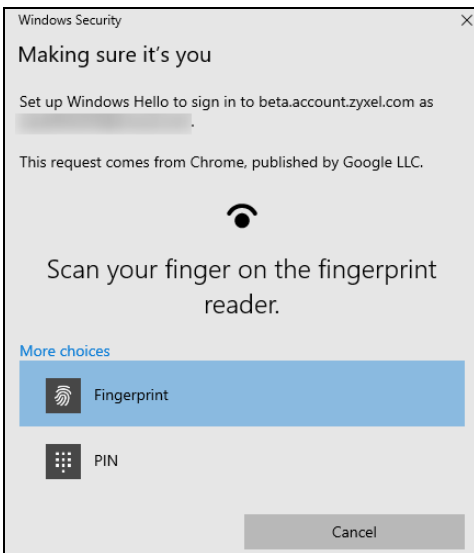
If you lose your PIN, do the following:

- In Windows OS:
Go to Settings > Accounts > Sign-in options > PIN (Windows Hello) > I forgot my PIN. You will be prompted to re-authenticate using your Microsoft Account password or recovery options.
 - In macOS:
Use your Apple ID to reset the passcode, or restore from another Apple device where you are still signed in.
 - For Cloud Password Managers:
If you forget it, you can usually log in again using your master password or account recovery flow.
- 7 Name your passkey after completing the PIN authentication, and then click OK.

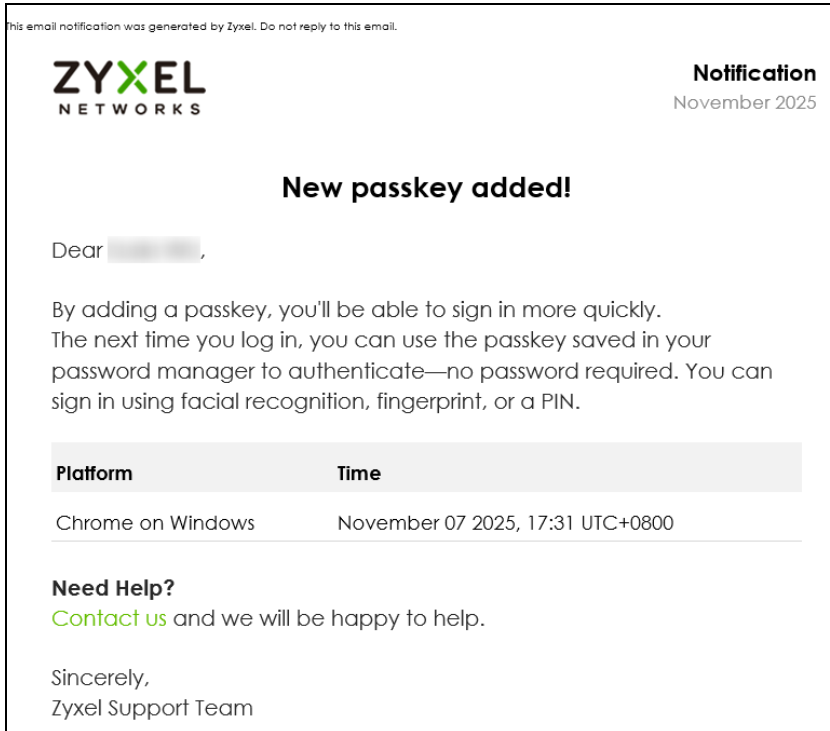


Biometrics Option

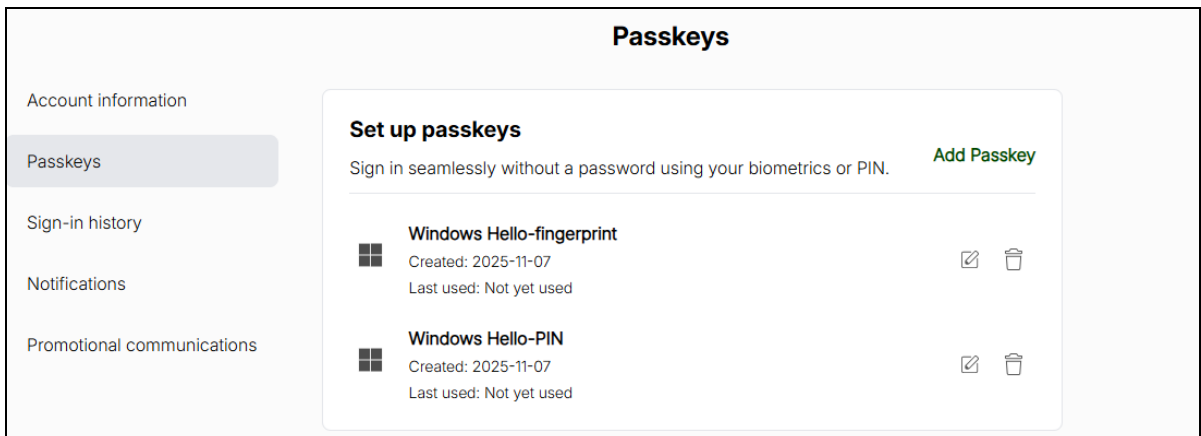
Select Fingerprint. Scan your fingerprint to use it as your sign-in method. The following example uses fingerprint.

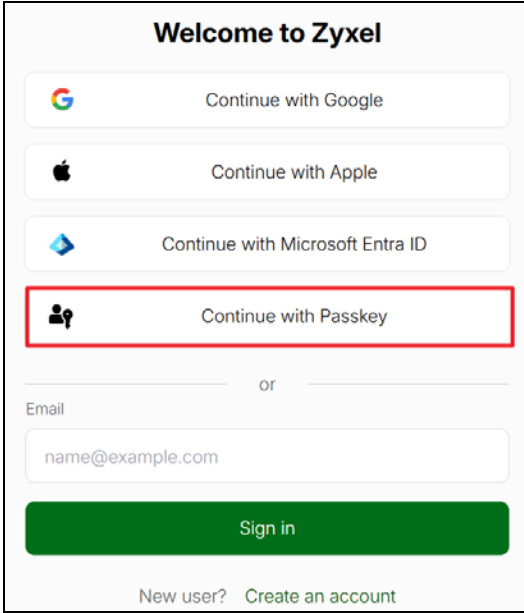


- 8 Name your passkey after completing the fingerprint authentication, and then click OK.
- 9 New passkey added! Email will be sent to the same email address used for your Zyxel Account.

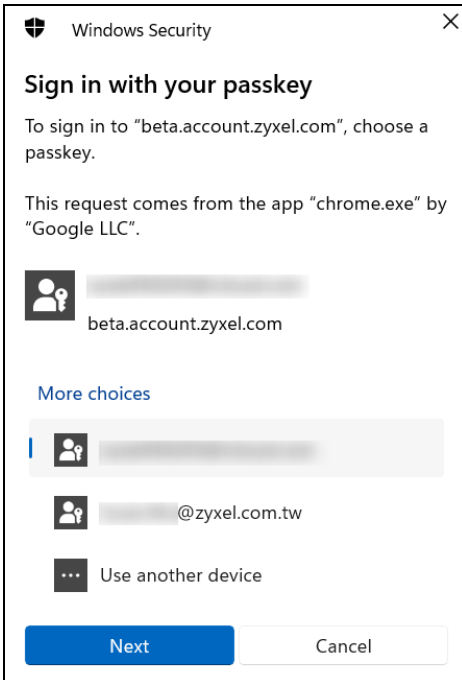


- 10 You can view all your saved passkeys on the Manage Account > Passkeys page. Select the passkey that matches the device you're using to sign in.

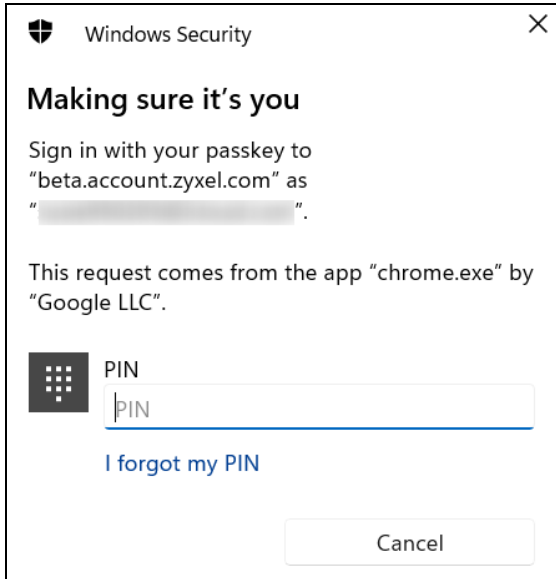




- 2 Select the account email you want to sign in with, and click Next.



- 3 Complete the biometric authentication by using your device's fingerprint reader to scan your fingerprint, or camera to map your face, or by entering a PIN to log in to the portal.



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 7 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: <ul style="list-style-type: none"> 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.
	Click this to open the myZyxel website login page in a new tab or window.
	Click this to open the NCC portal login page in a new tab or window.

Table 7 Title Bar: Web Configurator Icons (continued)

LABEL	DESCRIPTION
 SecuReporter	Click this to open the SecuReporter website login page in a new tab or window.
 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

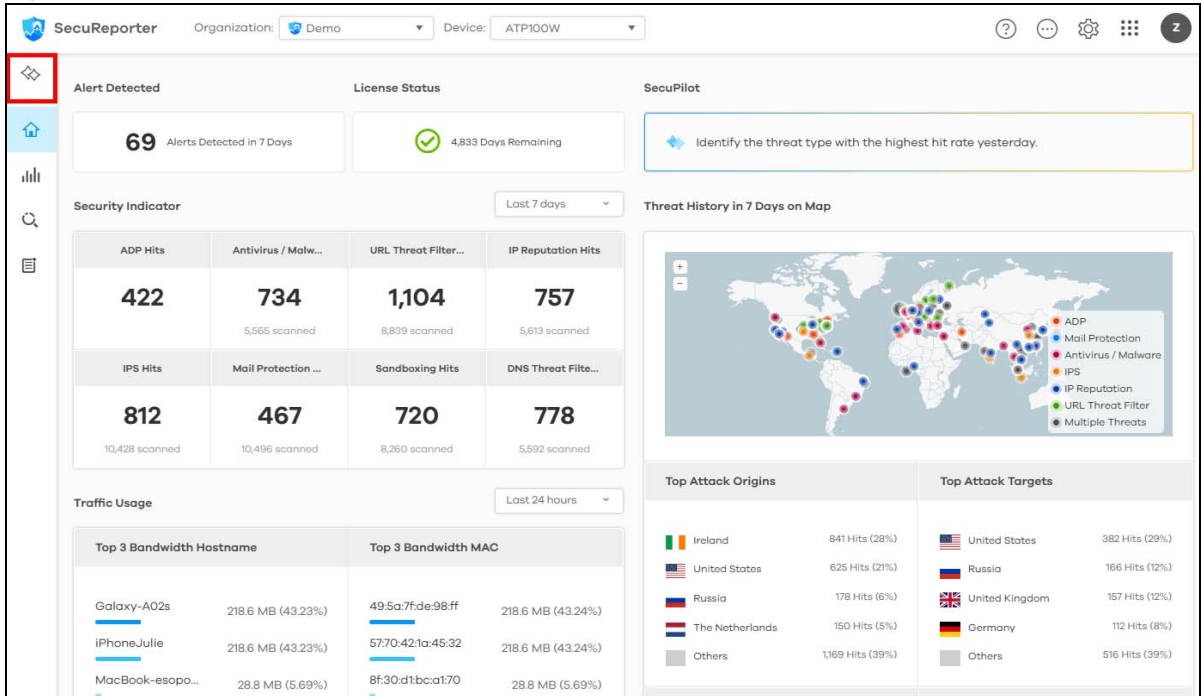
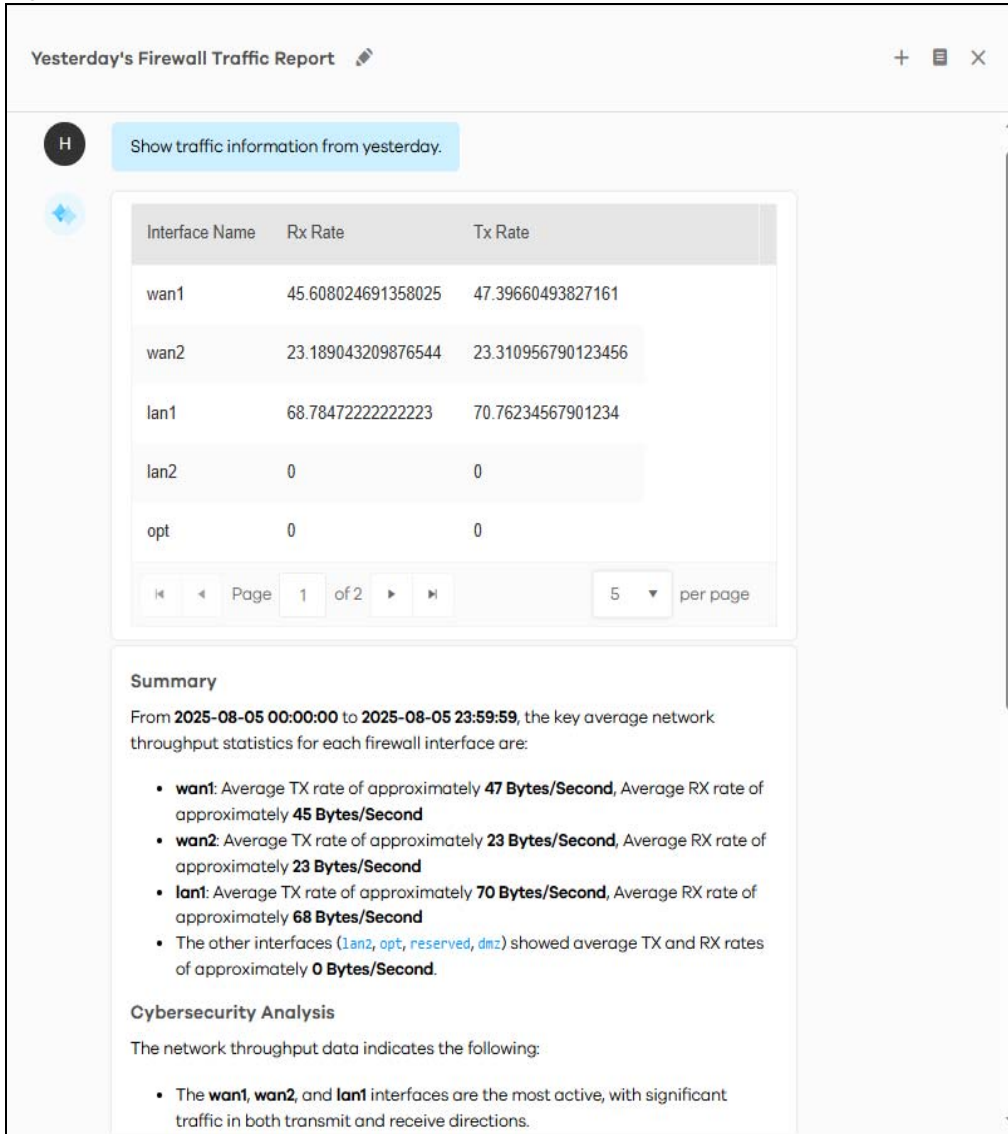


Figure 4 Dashboard > SecuPilot






The following table describes the labels on this screen.

Table 8 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 20 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.

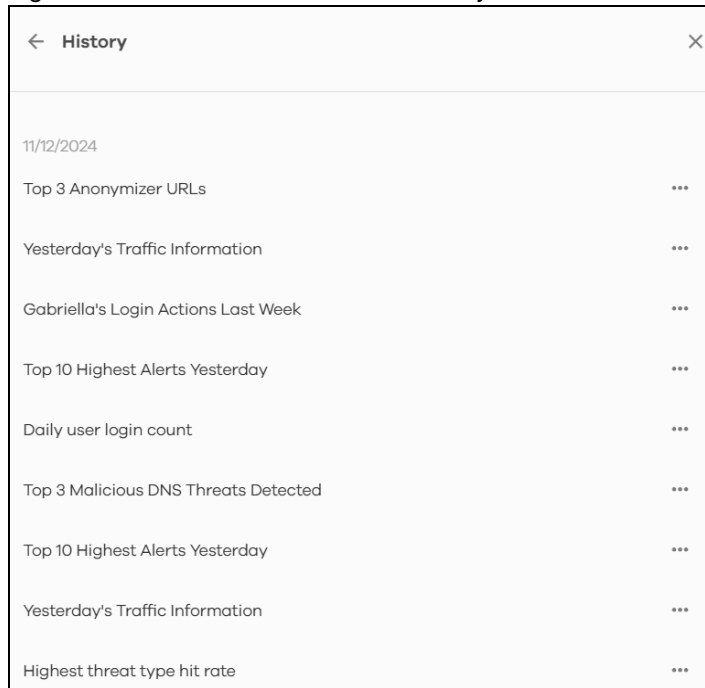
Table 8 Dashboard > SecuPilot

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 9 Dashboard > SecuPilot > History

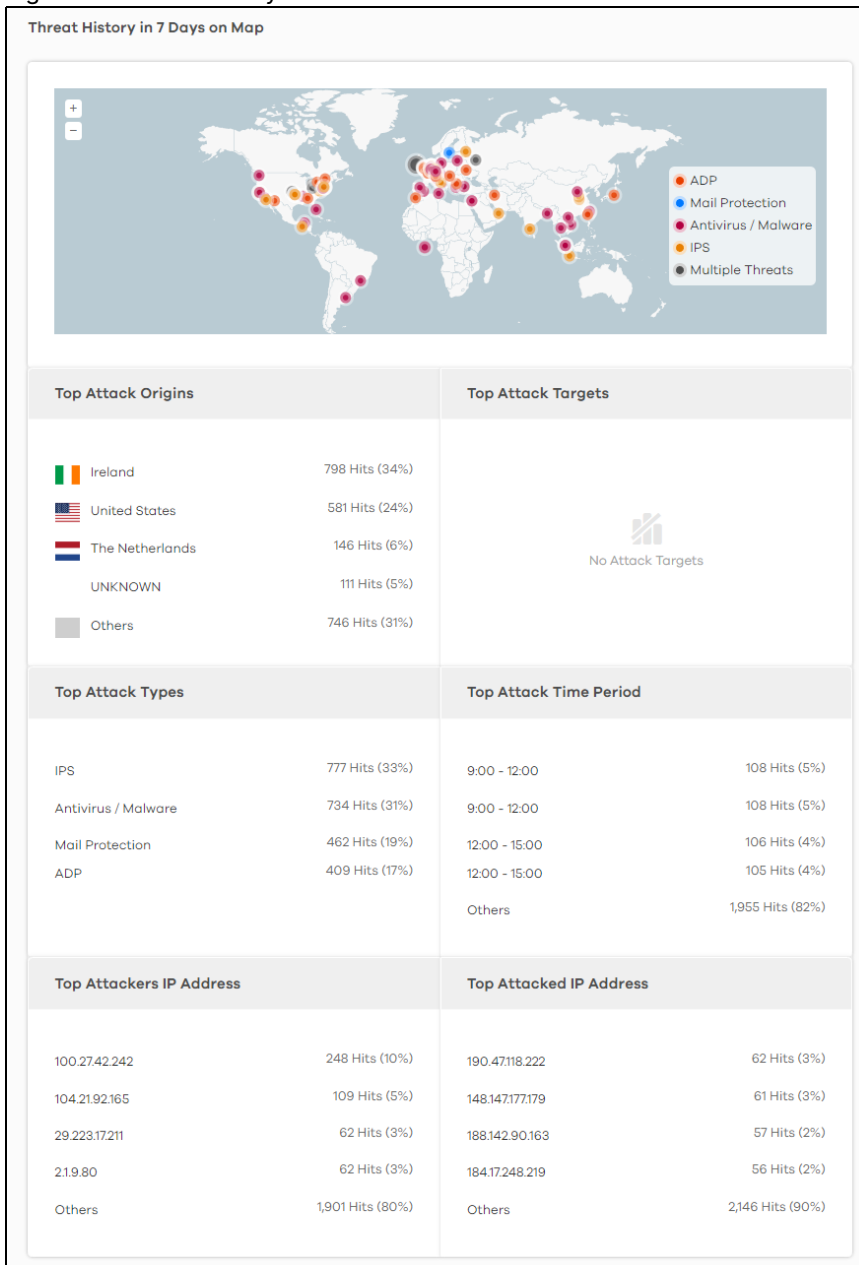
ICON	DESCRIPTION
Rename 	Click ... >  next to the conversation you want to rename, then enter and save a new title.
Delete 	Click ... >  next to the conversation you want to delete. The whole conversation will be removed.
View	Click on the title of the conversation to view the complete conversation history 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 10 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.

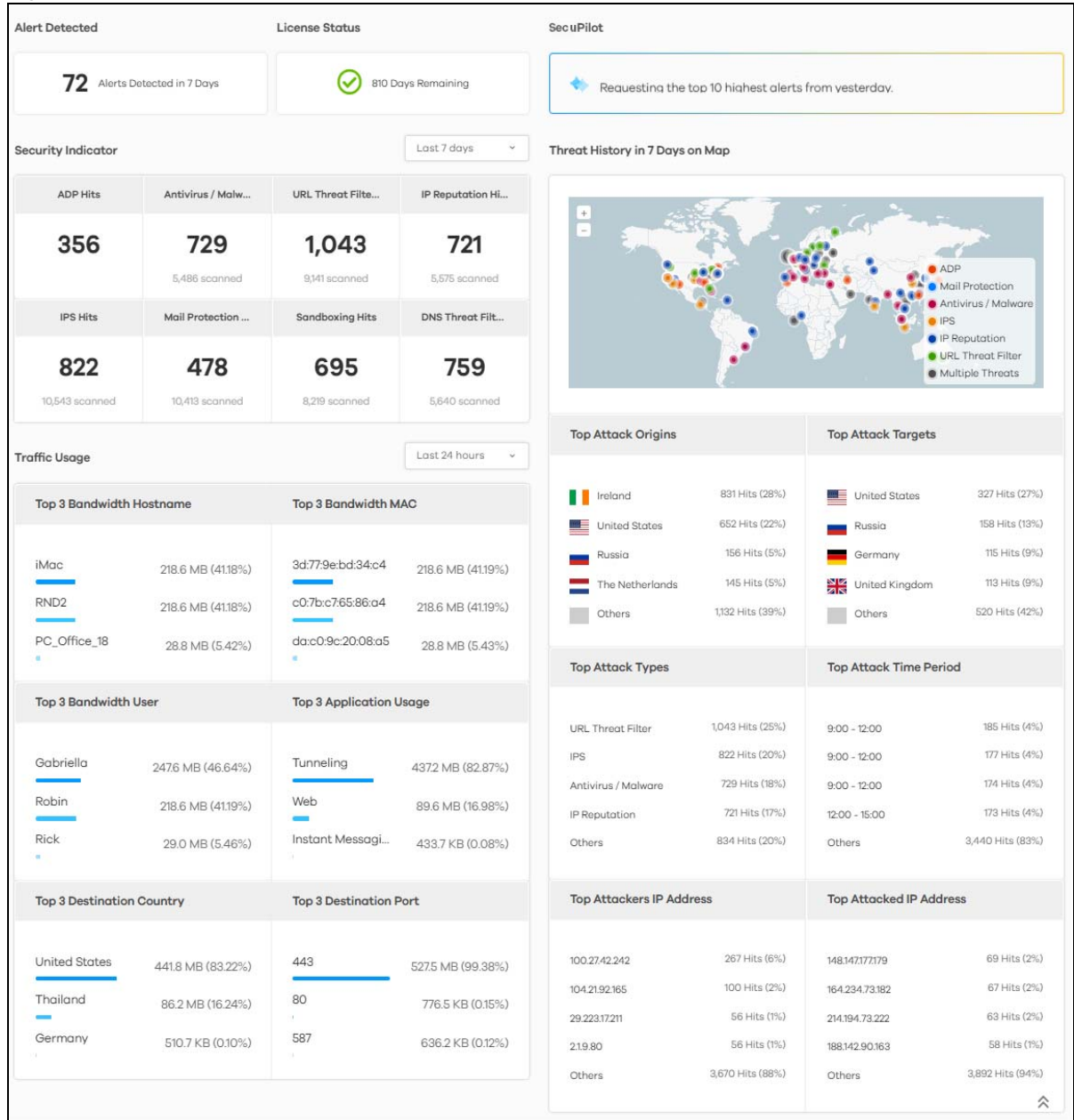
1.6 Dashboard

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 11 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 11 Default Dashboard (continued)

LABEL	DESCRIPTION
Security Indicator	
	Select the time frame to show your network's security environment collected by SecuReporter. <ul style="list-style-type: none"> • 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. <ul style="list-style-type: none"> • 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.

Add Organization

Organization Name

Description

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.

Organization & Device

Organization Unclaimed Device

Device Name	Model	MAC Address	Serial Number	License Status
	ATP200			Active
	ATP600			Active
	USG FLEX 700			Active
0902	USG110			No License
USG	USG110			No License
ATP100	ATP100			No License
	USG110			No License
	USG110			No License

Page 1 of 4 10 per page

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

Organization & Device

Organization **Device**

←

Device Model 🚩
USG FLEX 700

MAC Address



WAN IP Address

Firmware Version

Serial Number

SecuReporter License Status
Active (77 Days Remaining)

Protection Policy
Non-Anonymous

- 2 You will see the  icon on the right when you hover the mouse on the registered Zyxel Devices that have activated SecuReporter licenses. This icon will not appear for registered Zyxel Devices that do not have activated SecuReporter license.
- 3 Click the  icon to add the Zyxel Device into 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.

Claim Device

Step 1: Device Information Step 2: Analytics & Logs Step 3: Protection Policy

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

Belonged Organization
Demo

Device Name

Description

Device Model
ATP200

MAC Address

Serial Number

Cancel Next

- 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.

The screenshot shows the 'Claim Device' interface with three steps: Step 1: Device Information, Step 2: Analytics & Logs (highlighted), and Step 3: Protection Policy. The main content area asks, 'Do you want to import another's Analytics and Logs into this device?' with two radio button options: 'This is a new device' (selected) and 'Import analytics & logs from existing device'. At the bottom, there are 'Cancel', 'Back', and 'Next' buttons.


- 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.

The screenshot shows the 'Claim Device' interface with three steps: Step 1: Device Information, Step 2: Analytics & Logs, and Step 3: Protection Policy (highlighted). The main content area asks, 'Please choose the level of anonymity you require for users authenticated by this Zyxel Device. Please note that if you change the level of anonymity later, then all reports and logs for this Zyxel Device up to the point of change will be deleted from SecuReporter.' There are three radio button options: 'Fully Anonymous', 'Partially Anonymous (Recommended)' (selected), and 'Non-Anonymous'. Each option has a brief description of its implications. At the bottom, there is a checkbox for 'I agree with the protection policy.' and 'Cancel', 'Back', and 'Done' buttons.

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.

Organization & Device

Organization Device

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

Page 2 of 2

10 items per page

2.2.3 Generate API Token

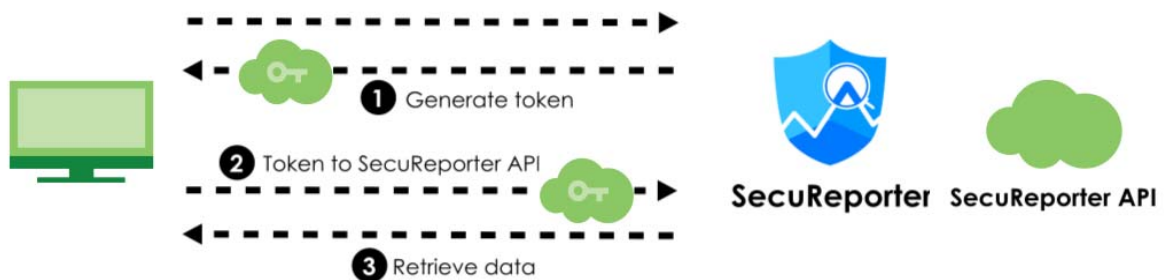
An API (Application Programming Interface) token is a secret string that verifies a user's access to API resources, allowing one software application to share data with another.

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.

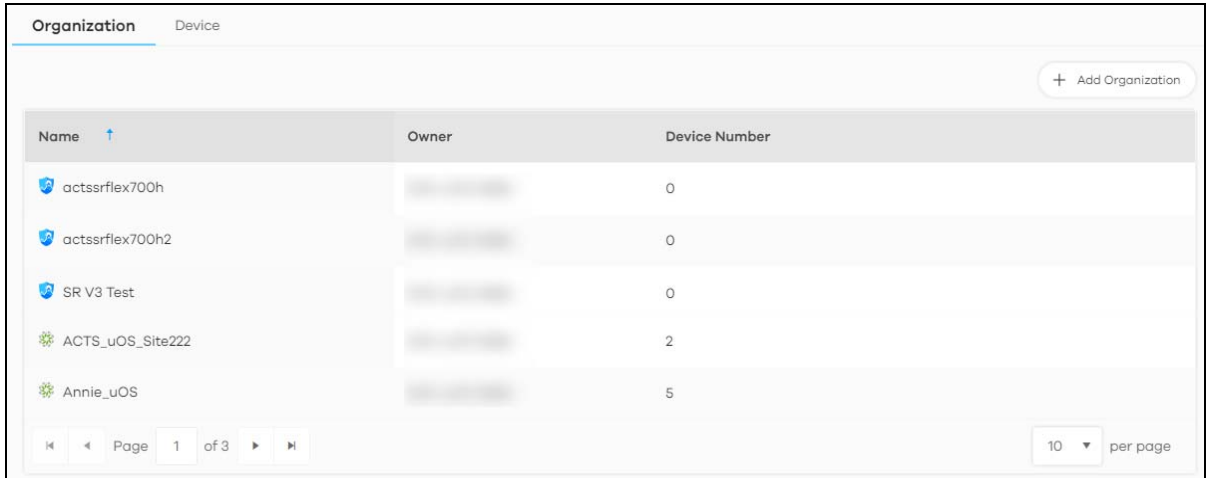
Figure 8 Overview of API Authorization



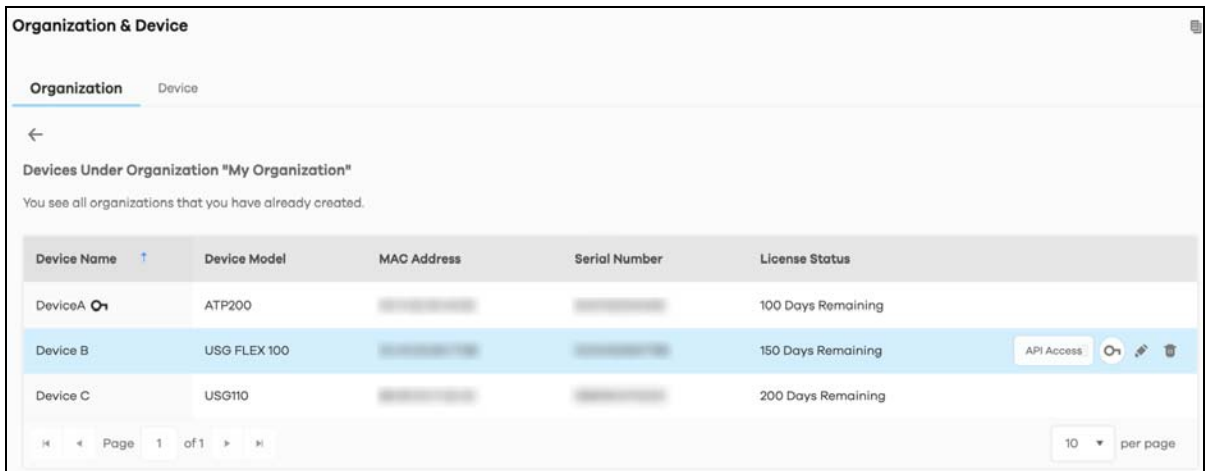
Generate an API token

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.




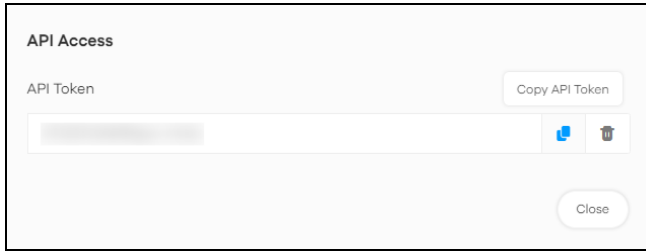
- 2 Click the API Access  button next to the Zyxel Device you want to share data with. Make sure the Zyxel Device has a valid device license.



- 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.

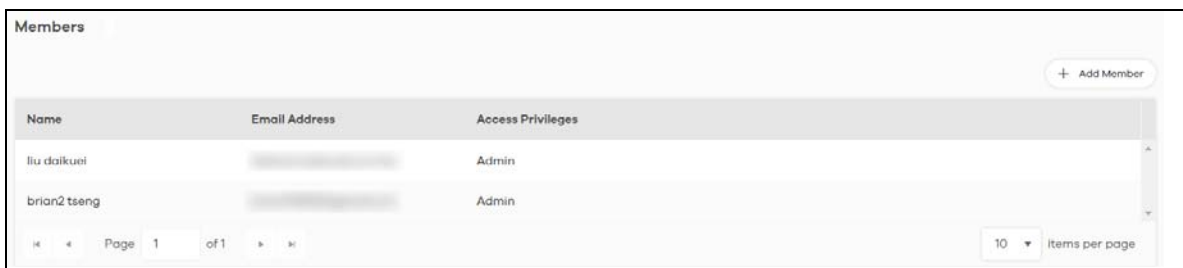
Retrieve SecuReporter Data

- 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.

Add Member

Member Email Address

Enter email address

Member's access privilege for all organizations and devices

Admin Member None

Exceptional Cases + Add Exceptional Case

Organization	Device	Access Privilege for selected target
Demo	All	Admin

Cancel Add

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.

Add Member

Member Email Address

Enter email address

Member's access privilege for all organizations and devices

Admin Member None

Exceptional Cases + Add Exceptional Case

Organization	Device	Access Privilege for selected target
Zyxel	All	Admin

Cancel Add

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.

Add Member

Member Email Address

john@zyxel.com.tw

Member's access privilege for all organizations and devices

Admin Member None

Exceptional Cases + Add Exceptional Case

Organization	Device	Access Privilege for selected target
Demo	Simulator	Member

Cancel Add

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.

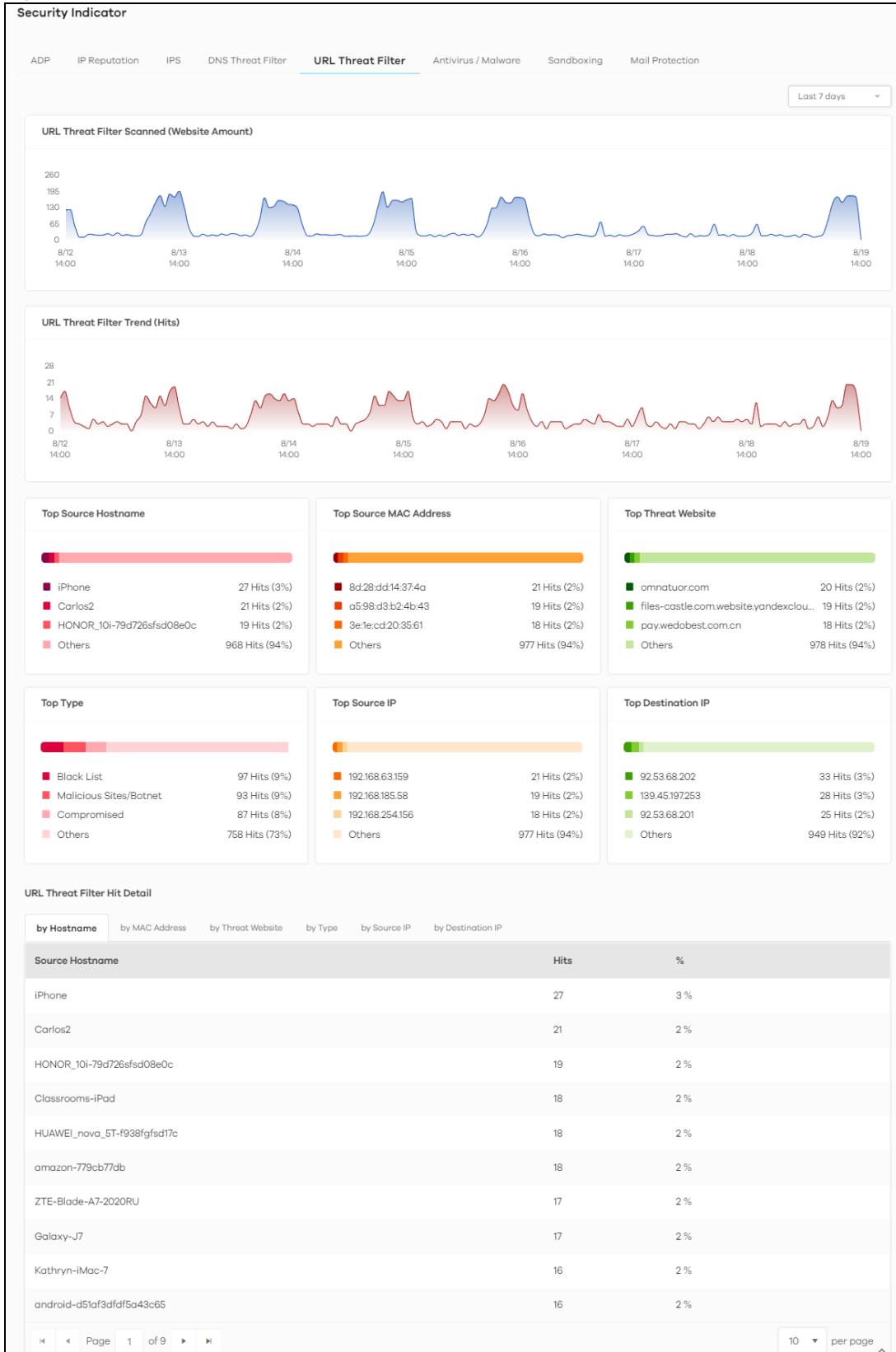
In most cases, you can choose to analyze data collected over one of five time frames (see [Section 1.6 on page 22](#)):

- 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



- 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

- 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

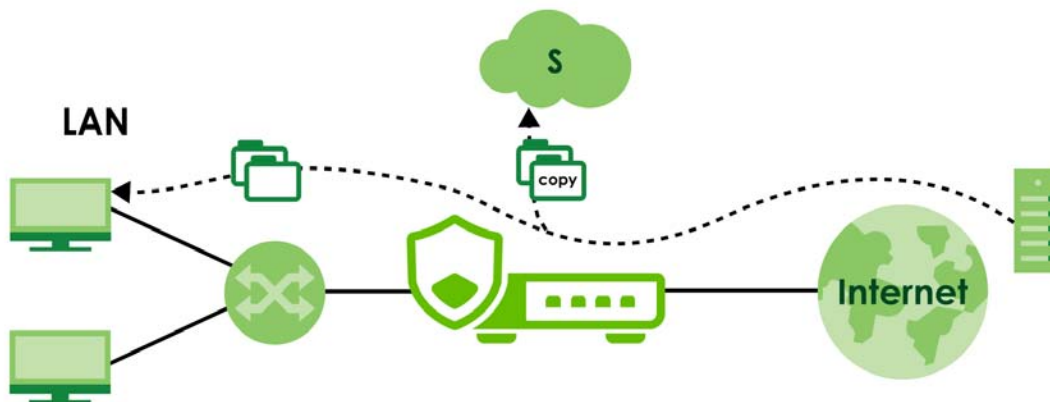
Zyxel cloud sandboxing is a security mechanism which provides a safe environment to separate running programs from your network and host devices. Unknown or untrusted programs or codes are uploaded to a cloud server and executed within an isolated virtual machine (VM) to monitor and analyze the zero-day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

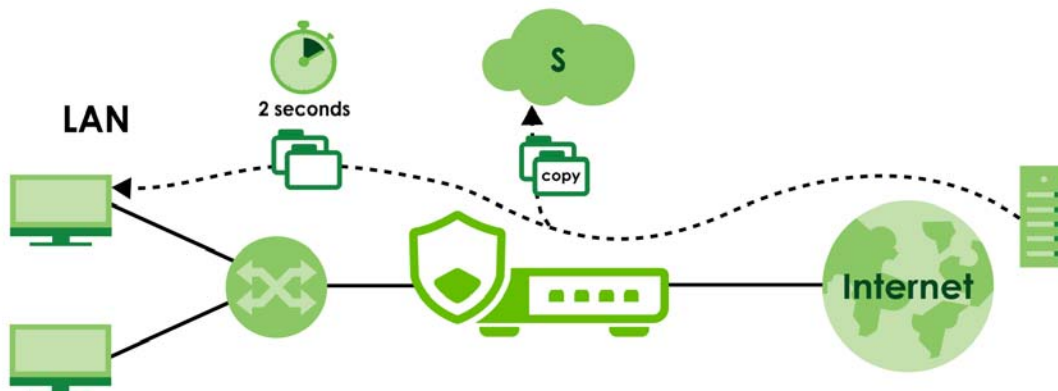
Note: The scan result is removed from the Zyxel Device cache after the Zyxel Device restarts, so all files are once again 'unknown'.

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.

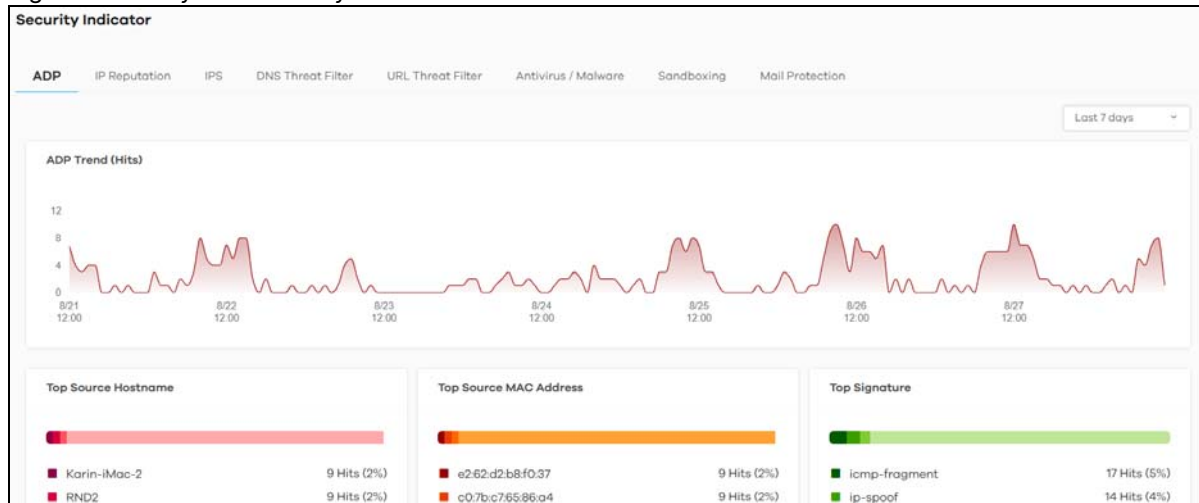
Note: In this case the receiver of the file will not be able to open the file. The Zyxel Device administrator should contact the receiver of the file to let him or her know.

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

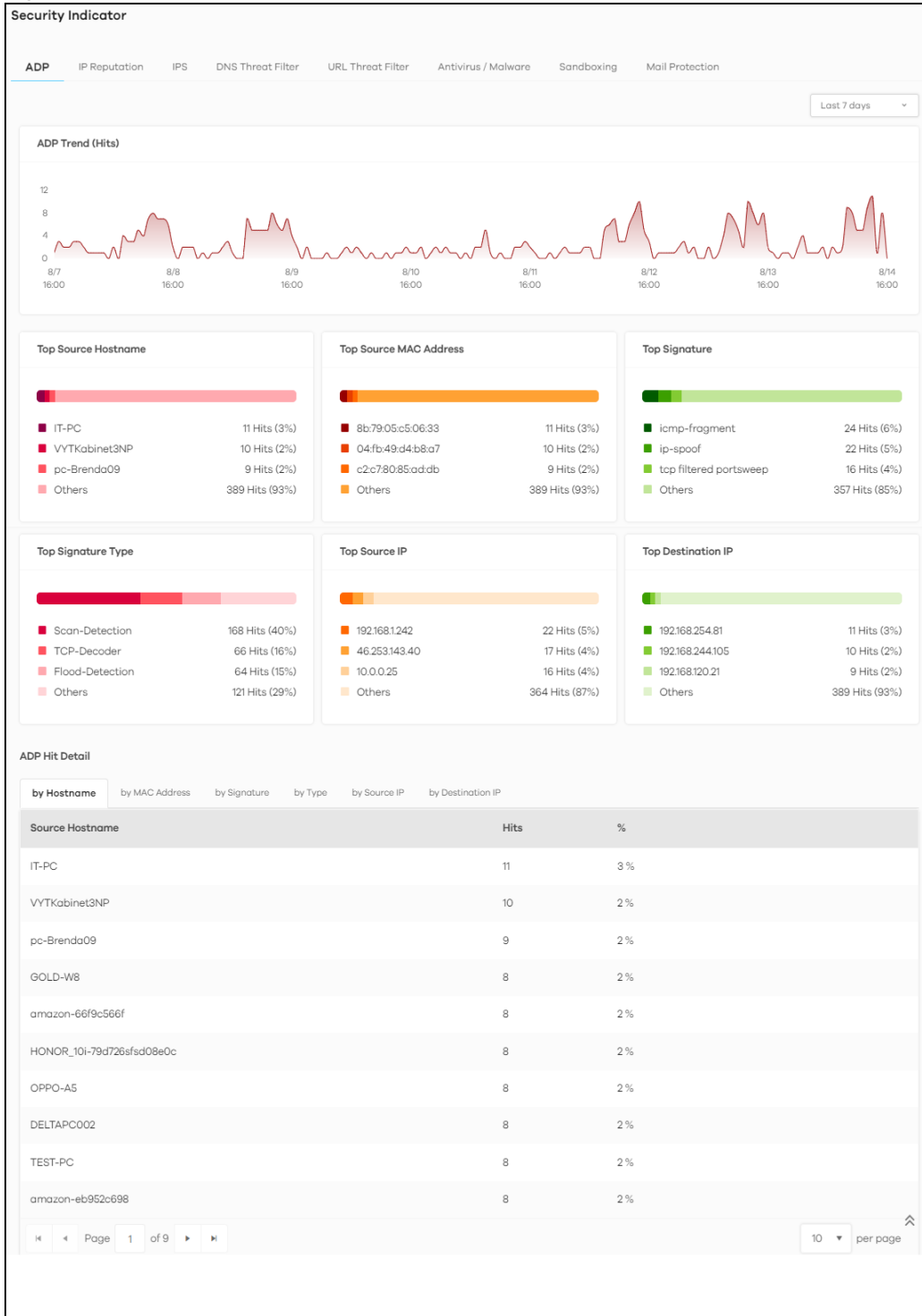
Protocol anomalies are packets that do not comply with the relevant RFC (Request For Comments). Protocol anomaly detection includes:

- 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 12 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

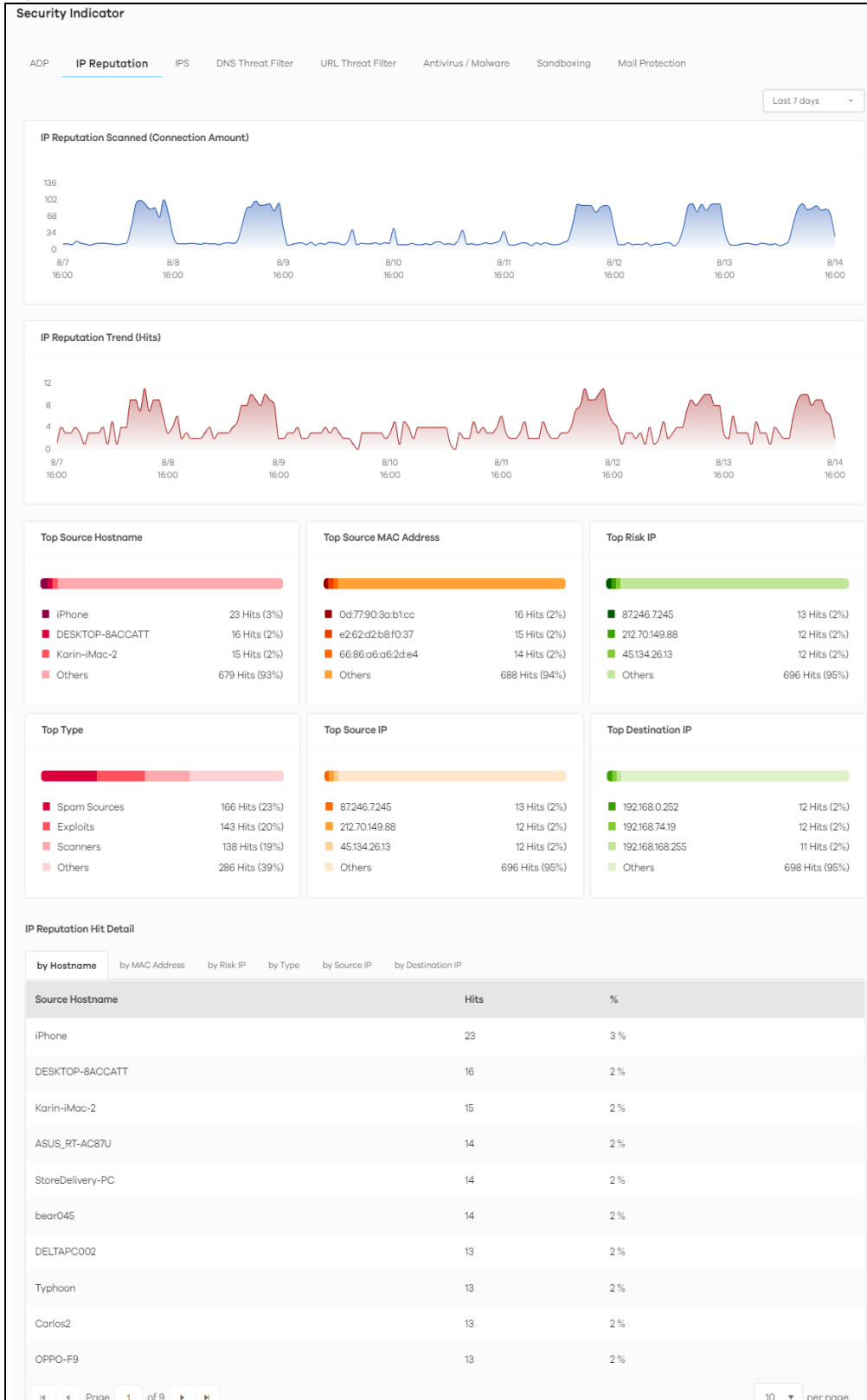
When you register for and enable the IP reputation service, your Zyxel Device downloads signature files that identifies reputation of IPv4 addresses. You can have the Zyxel Device forward, block, and/or log packets from IPv4 addresses based on these signatures and categories.

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 13 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 45 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.



IP Reputation Hit Detail

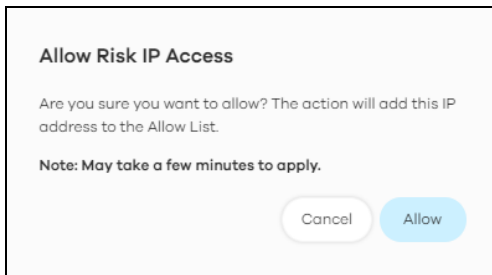
by Hostname by MAC Address **by Risk IP** by Type by Source IP by Destination IP

Risk IP	Hits	%
1.1.1	693	100 %

Add to Allow List  >

Page 1 of 1 10 per page

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




Allow Risk IP Access

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

Note: May take a few minutes to apply.

Cancel Allow

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

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



IP Reputation Hit Detail

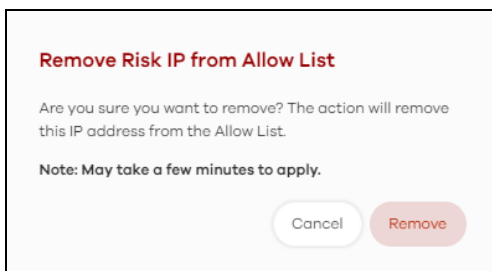
by Hostname by MAC Address **by Risk IP** by Type by Source IP by Destination IP

Risk IP	Hits	%
1.1.1 	627	100 %

Remove from Allow List  >

Page 1 of 1 10 per page

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



Remove Risk IP from Allow List

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

Note: May take a few minutes to apply.

Cancel Remove

3.3.3 IPS

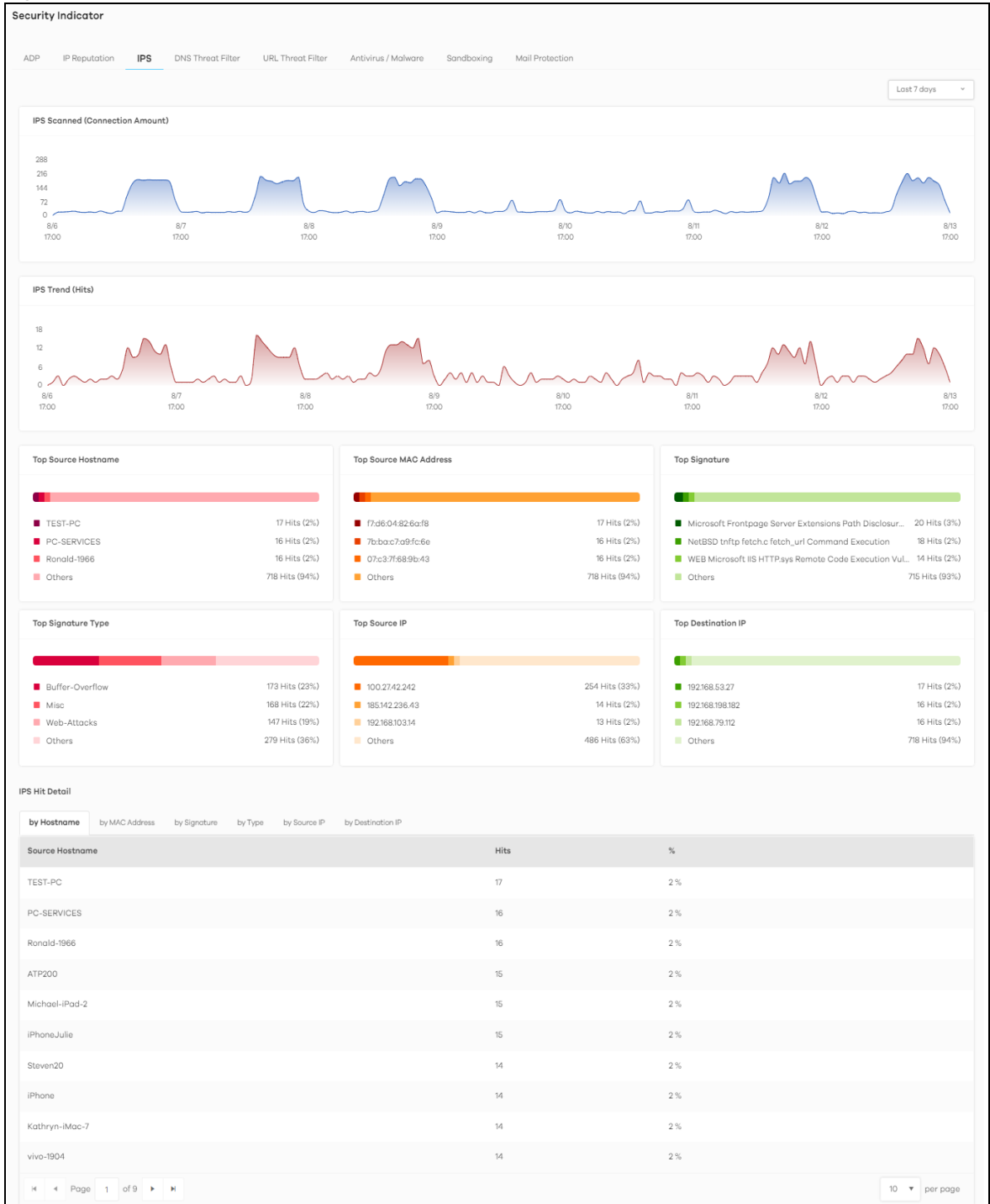
An IPS profile is a set of packet inspection signatures.

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.

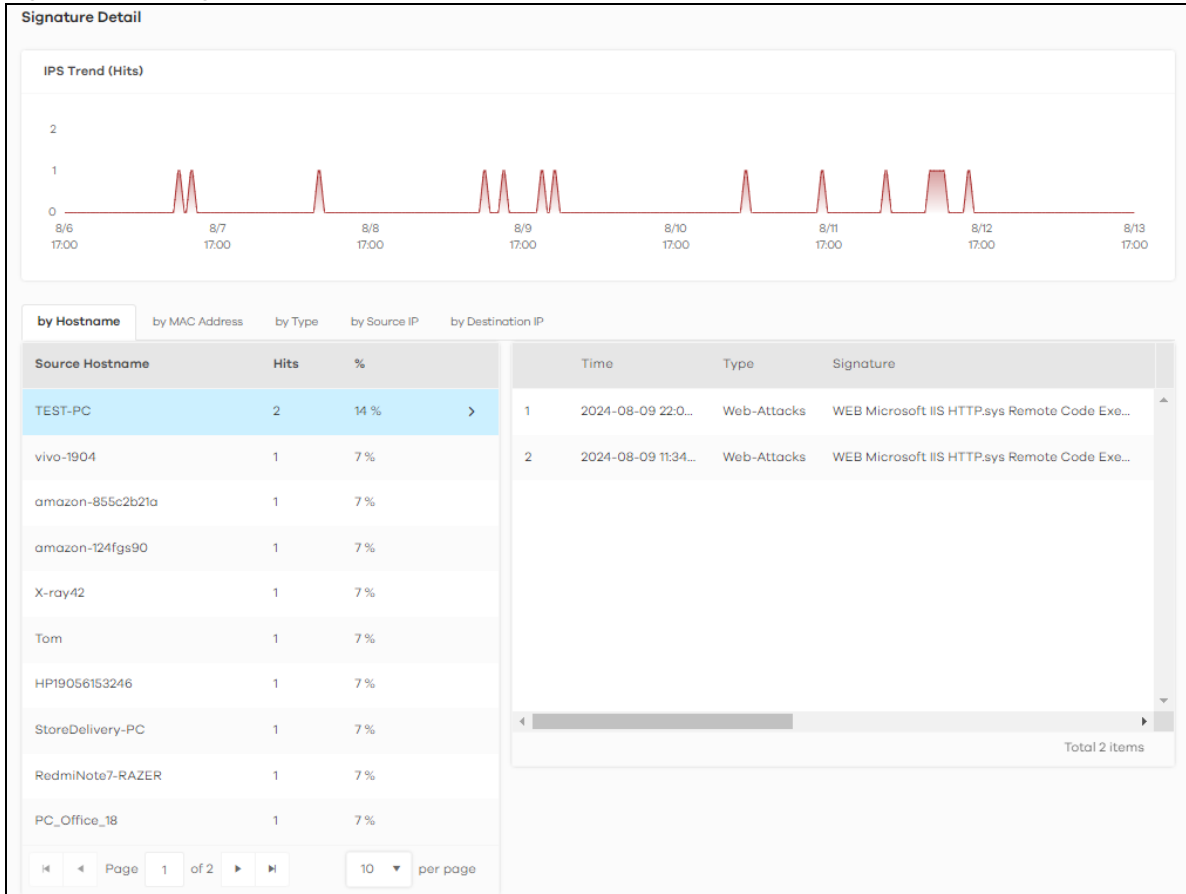
Table 14 Analysis > Security Indicator > IPS

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

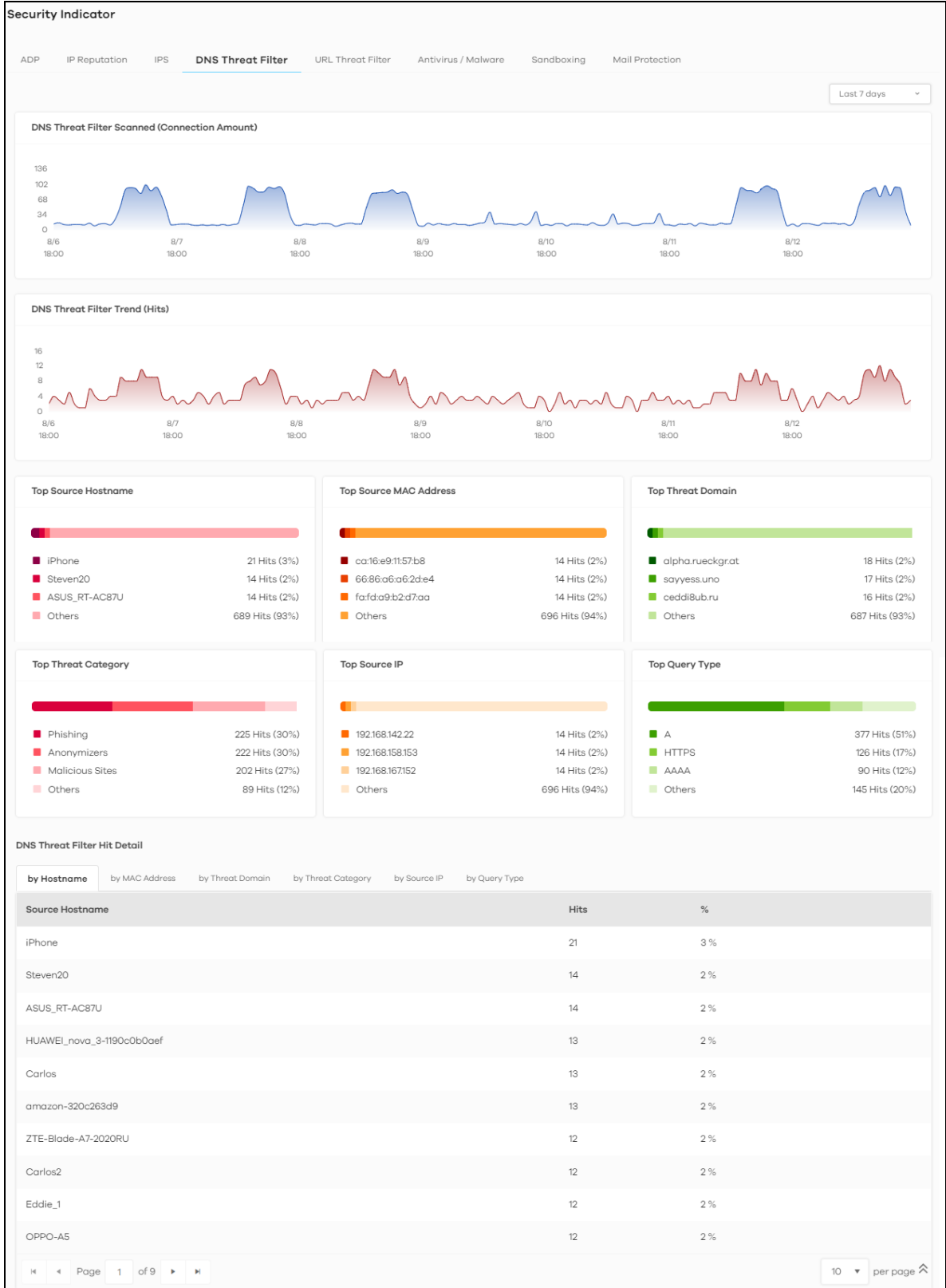
The Zyxel Device replies with a DNS server error for the following types of DNS queries:

- 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 15 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 53 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.

DNS Threat Filter Hit Detail

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

Threat Domain	Hits	%	
cdn.polyfill.io	7	47 %	Add to Allow List <input checked="" type="checkbox"/> >
polyfill.io	5	33 %	
yahoo.com <input checked="" type="checkbox"/>	3	20 %	

Page 1 of 1 10 per page

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


Allow Risk IP Access

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

Note: May take a few minutes to apply.


Cancel Allow

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

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

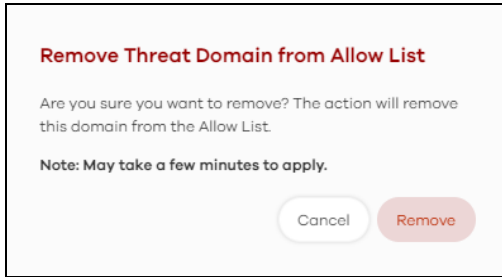
DNS Threat Filter Hit Detail

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

Threat Domain	Hits	%	
cdn.polyfill.io <input checked="" type="checkbox"/>	7	47 %	Remove from Allow List  >
polyfill.io	5	33 %	
yahoo.com <input checked="" type="checkbox"/>	3	20 %	

Page 1 of 1 10 per page

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



3.3.5 URL Threat Filter

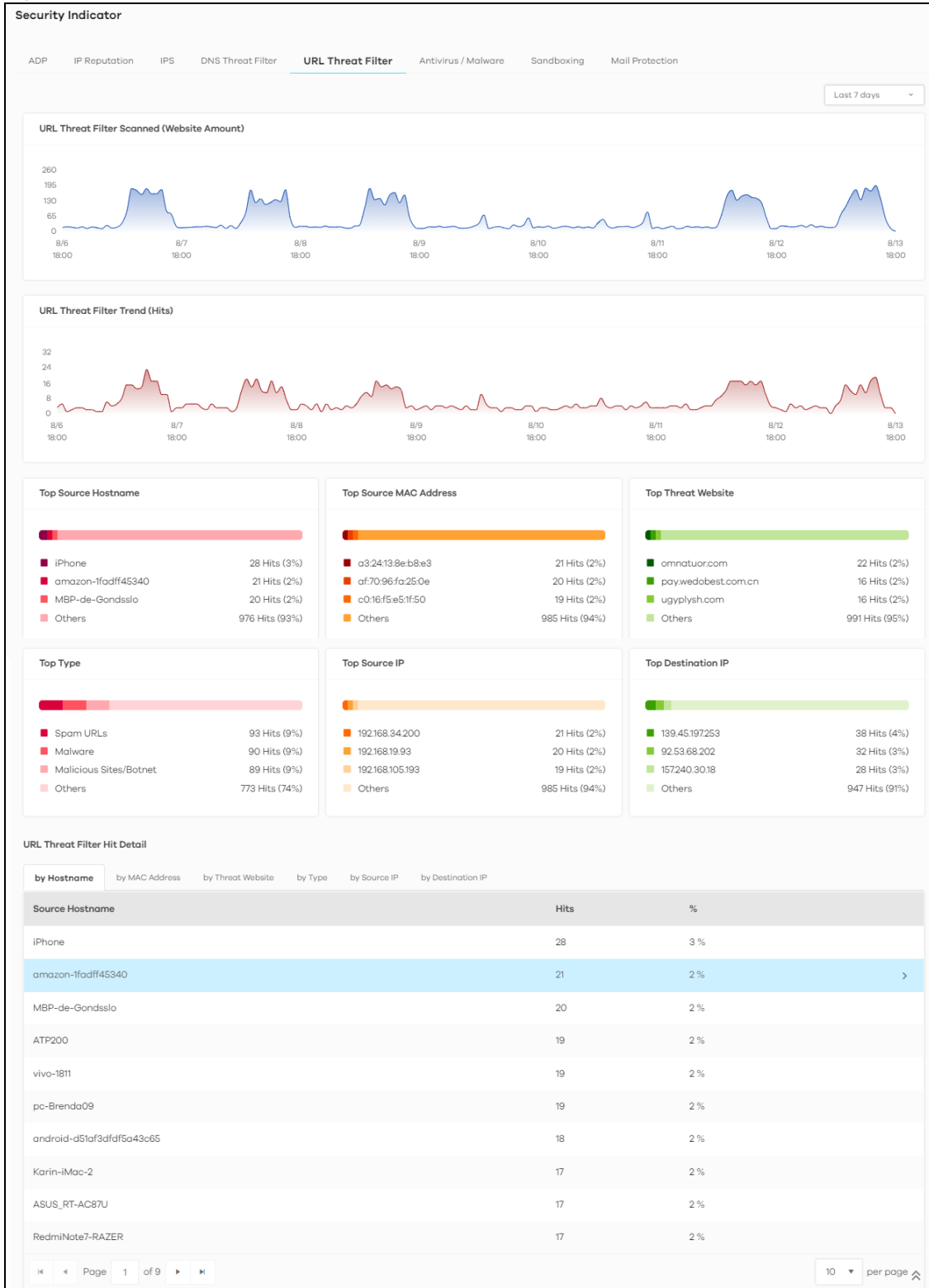
When you enable the URL Threat filtering service, your Zyxel Device downloads signature files that contain known URL Threat domain names and IP addresses. The Zyxel Device will also access an external database that has millions of web sites categorized based on content. You can have the Zyxel Device 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 16 Analysis > Security Indicator > URL Threat Filter

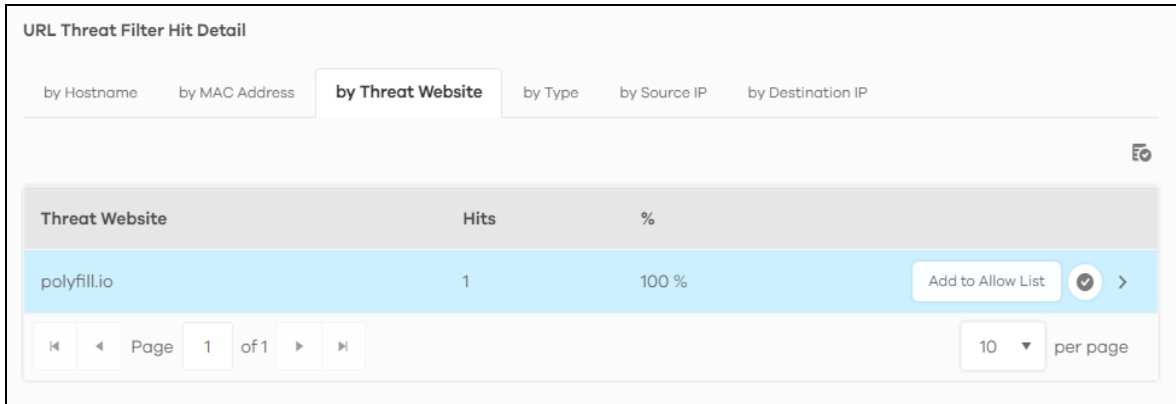
LABEL	DESCRIPTION
URL Threat Filter Scanned (Website Amount)	This chart displays the total number of connections detected by the Zyxel Device. Move your cursor over a trend line to display the number of connections encountered over time.
URL Threat Filter Trend (Hits)	This chart displays the number of 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 57 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

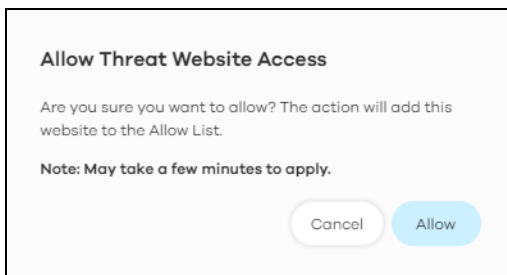
There is a blue check mark  next to the domain in the allow list.

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.

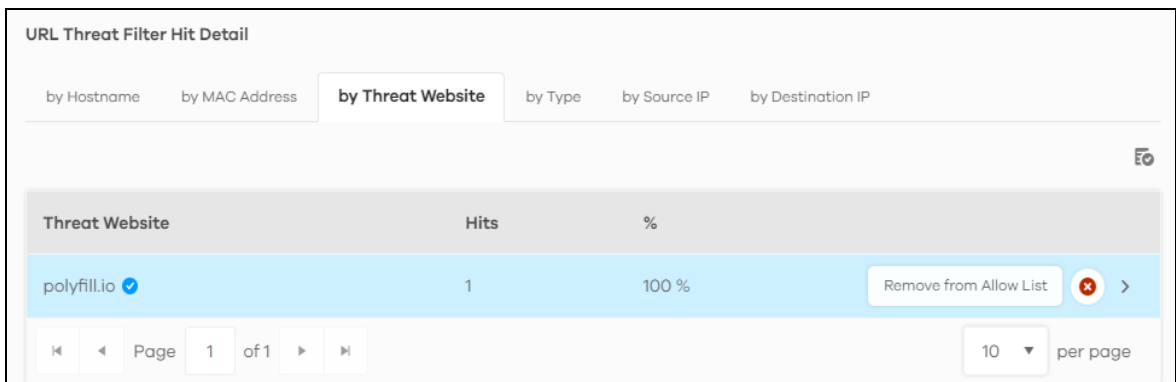


- 2 The following window pops up, click Allow to add the threat website to the allow list.

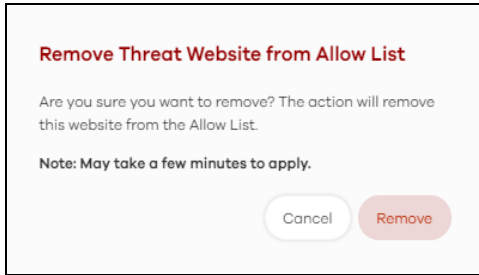


Do the following to remove a threat website from the allow list:

- 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.

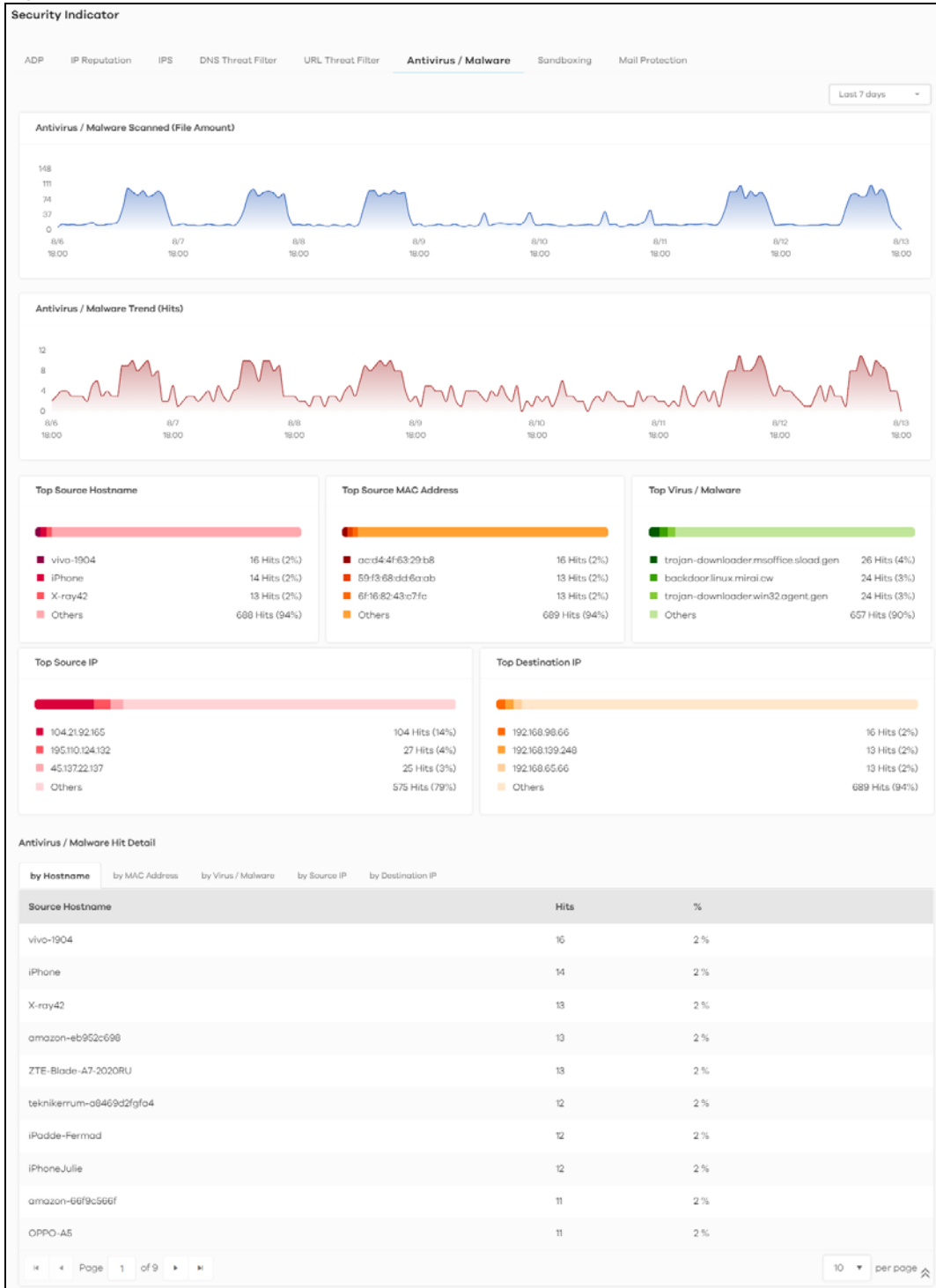


3.3.6 Antivirus / Malware

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 17 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.

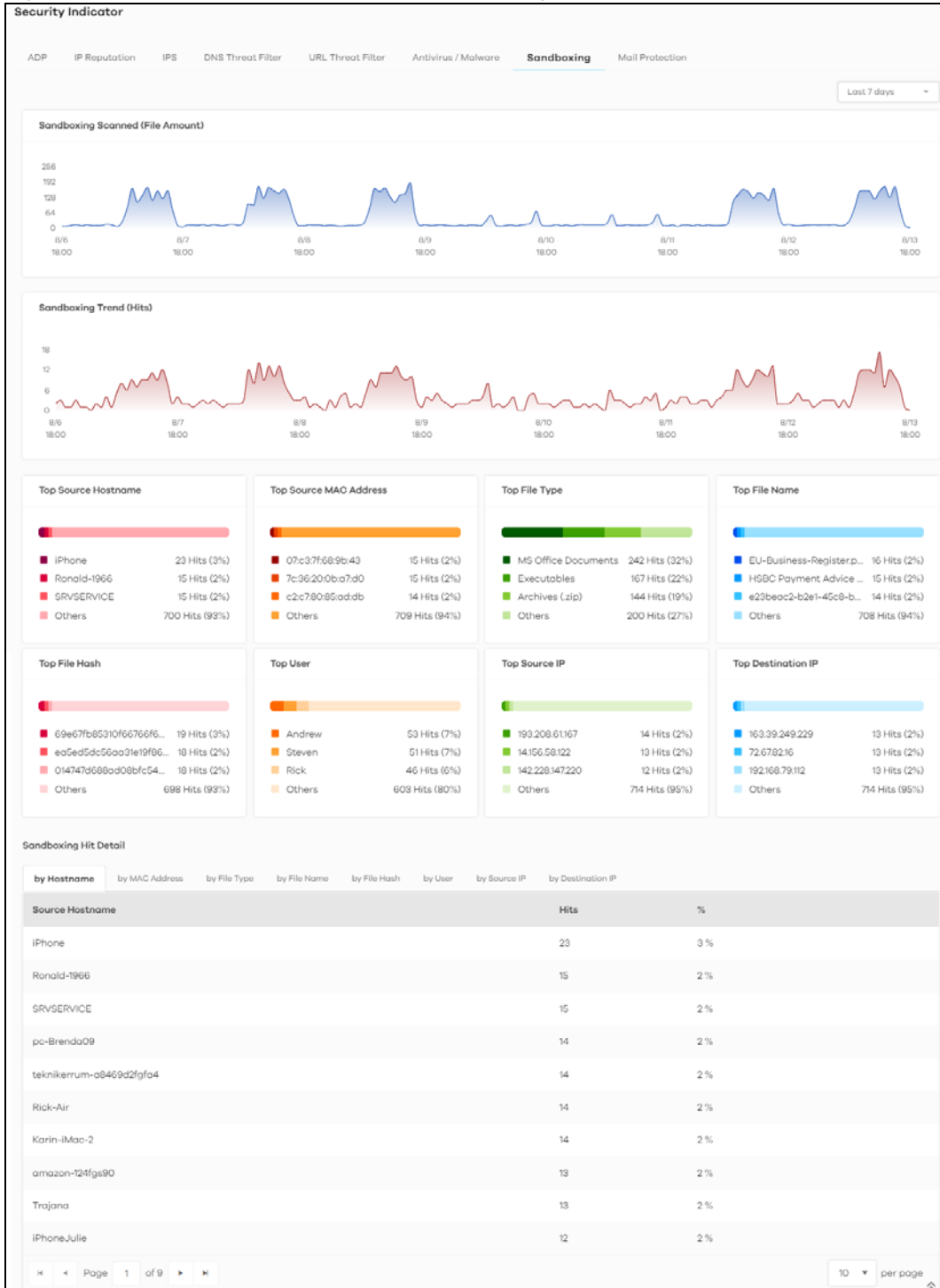
3.3.7 Sandboxing

This screen displays sandboxing statistics. See [Section 3.1.2 on page 38](#) 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 18 Analysis > Security Indicator > Sandboxing

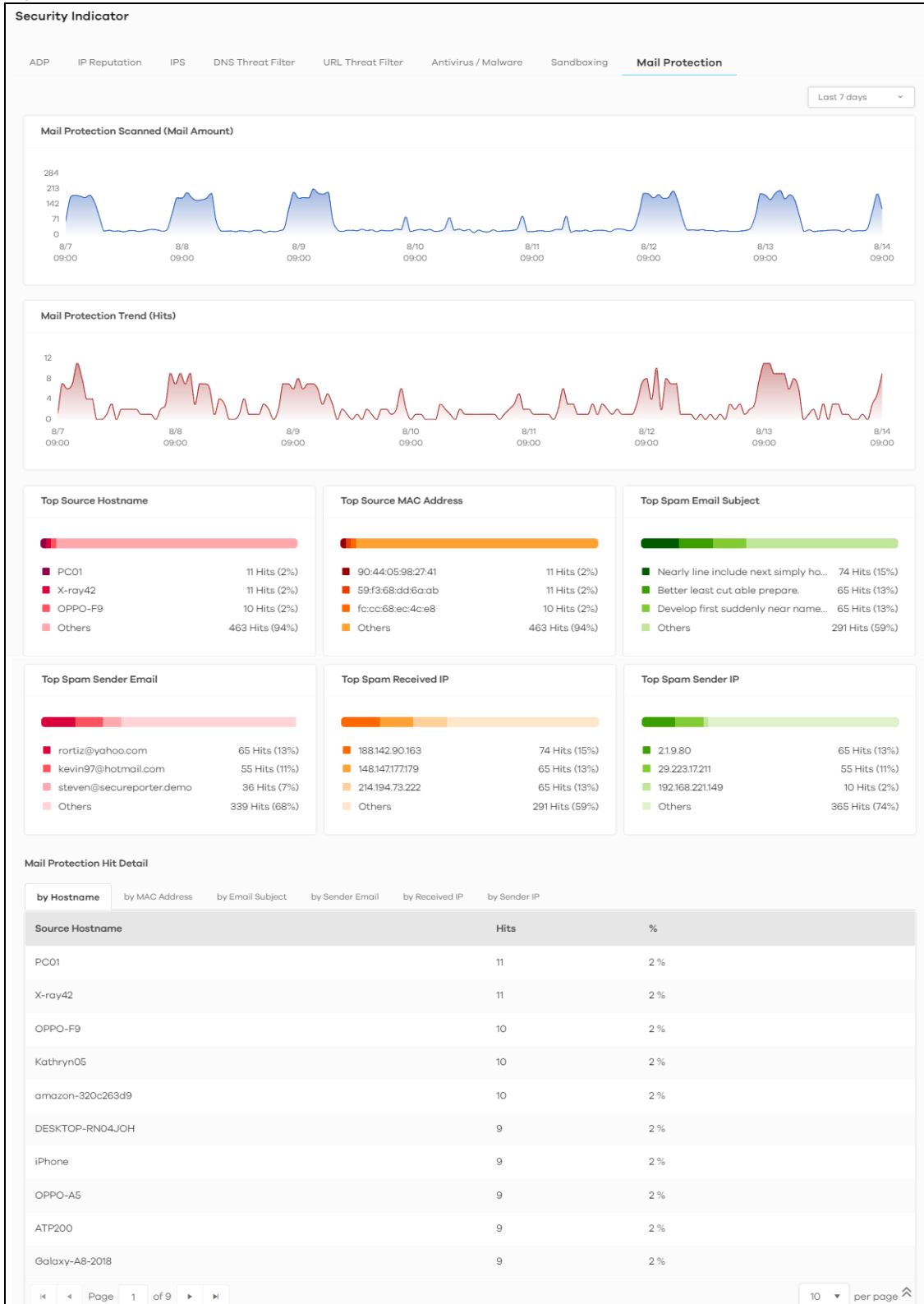
LABEL	DESCRIPTION
Sandboxing Scanned (File Amount)	This chart displays the total number of connections detected by the Zyxel Device. Move your cursor over a trend line to display the number of connections encountered over time.
Sandboxing Trend (Hits)	This chart displays the number of malicious and/or 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 19 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

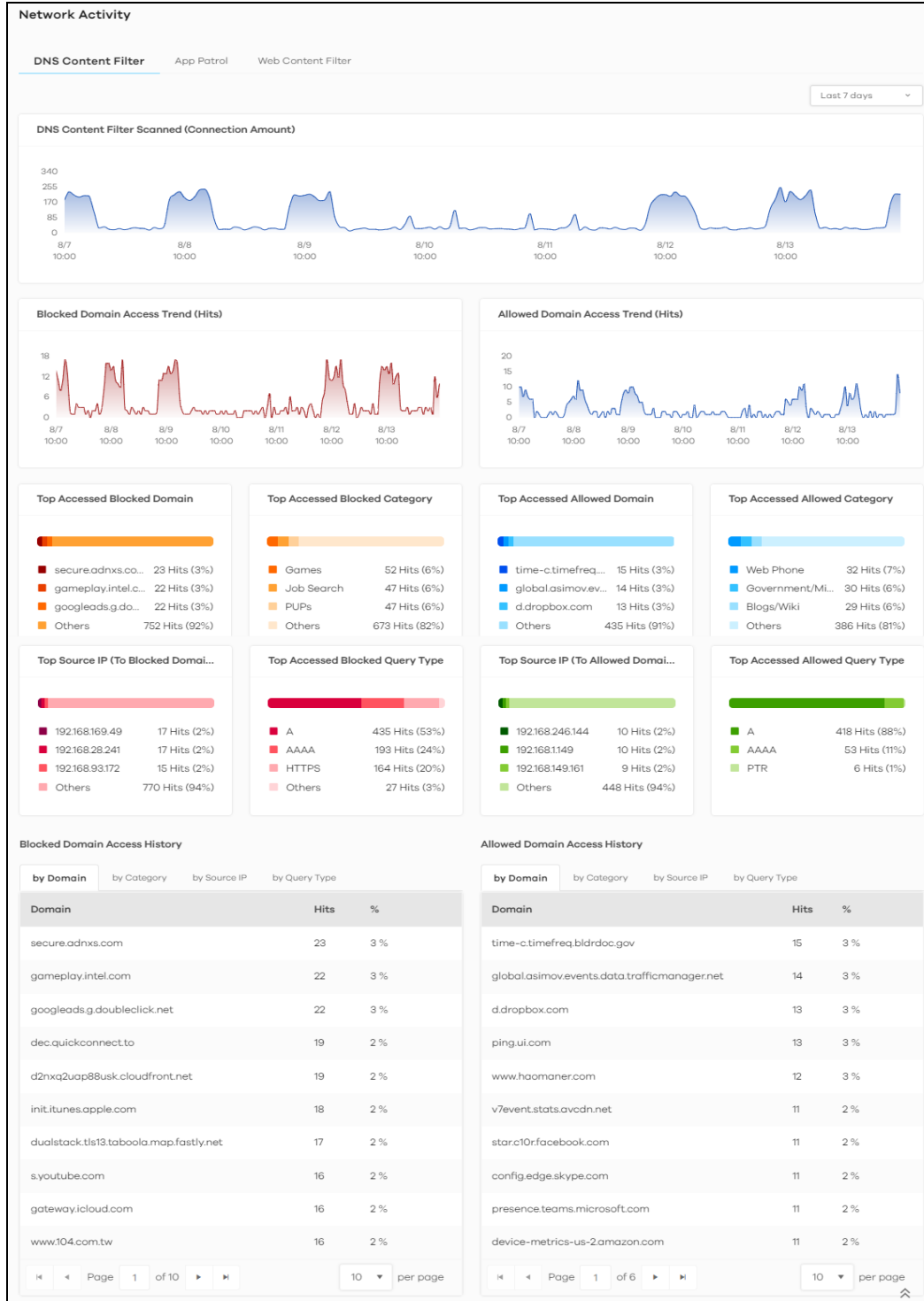
Network Activity data visualizations are categorized as:

- [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 20 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.

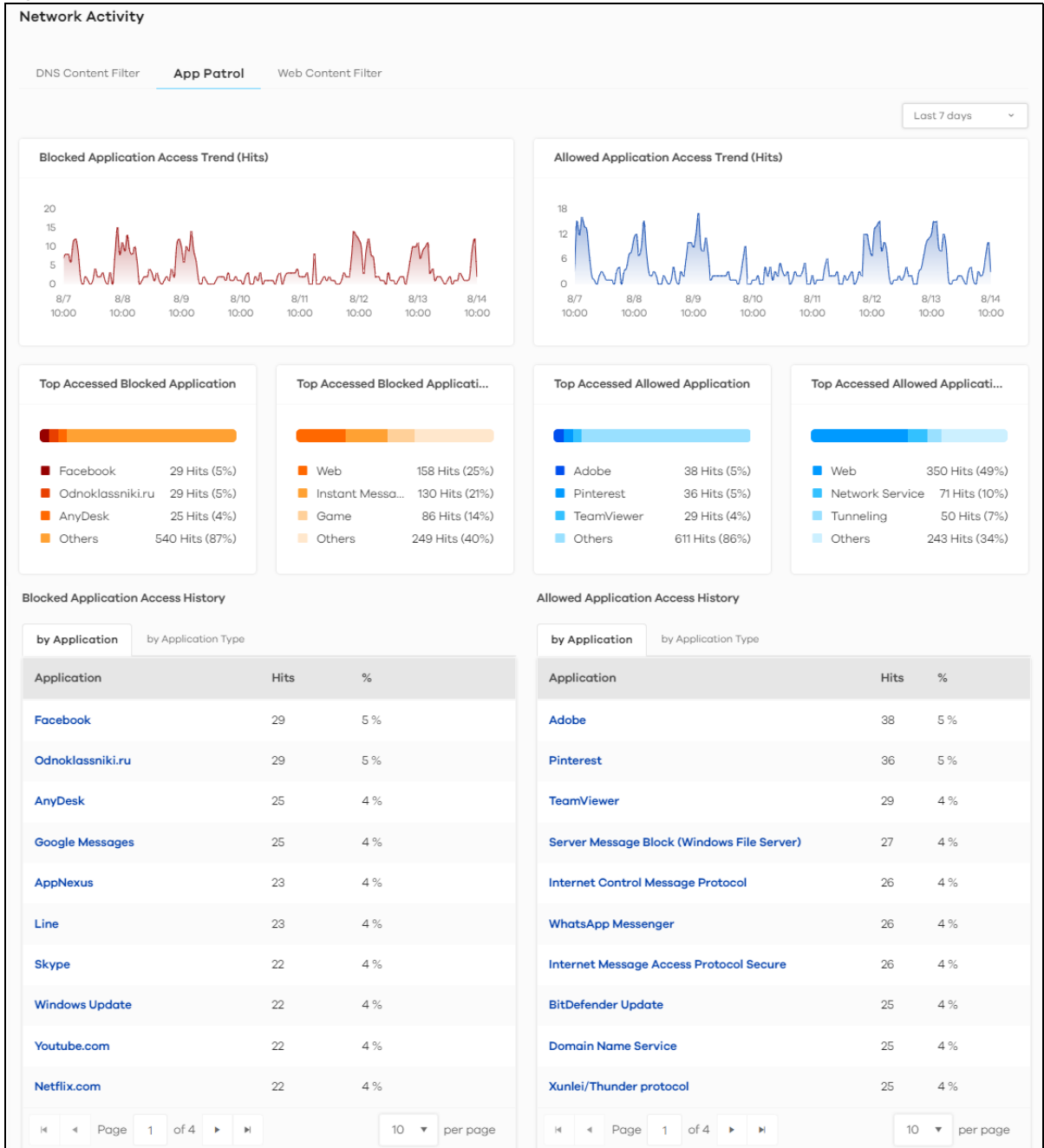
3.4.2 App Patrol

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.

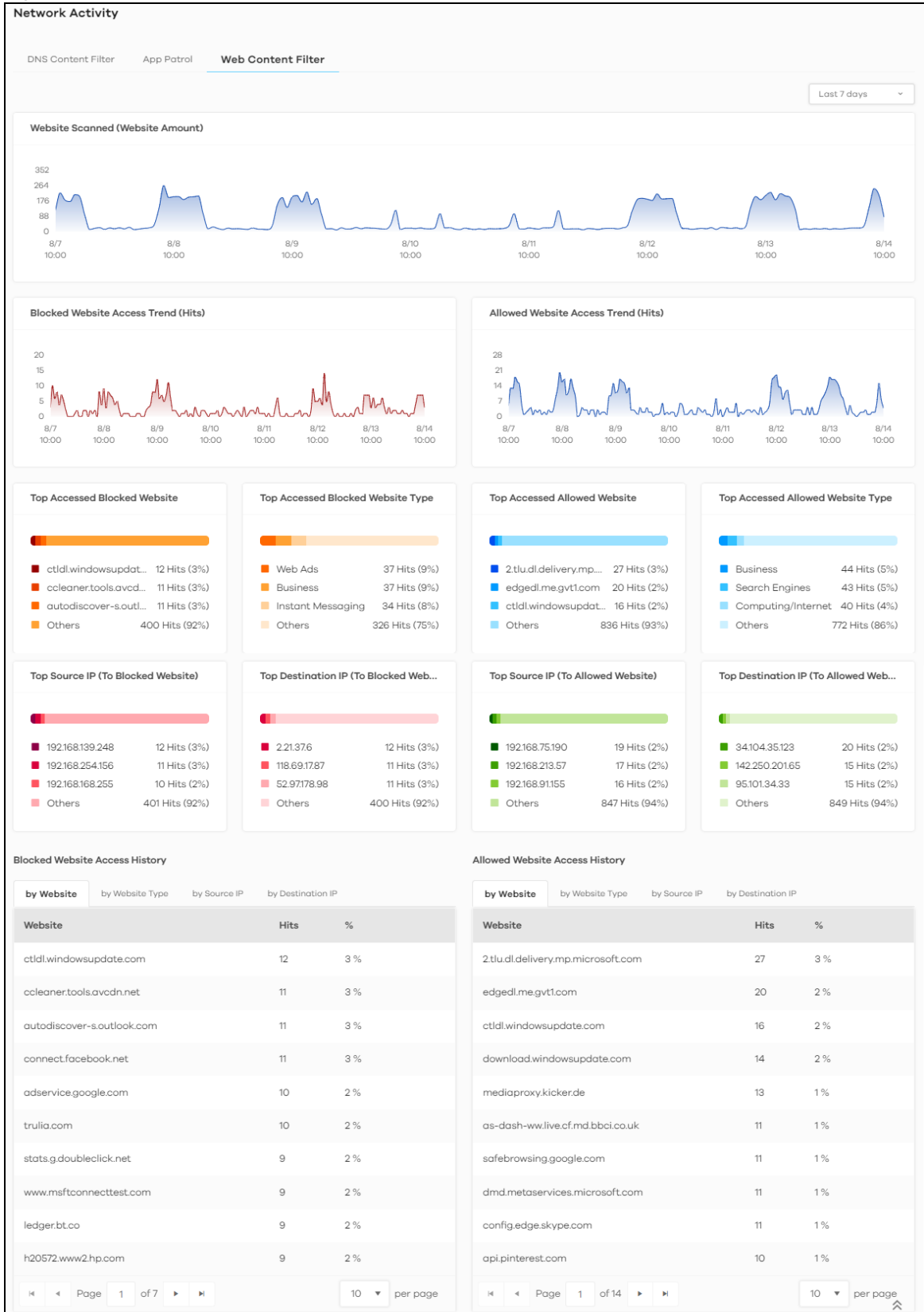
Table 21 Analysis > Network Activity > App Patrol

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.

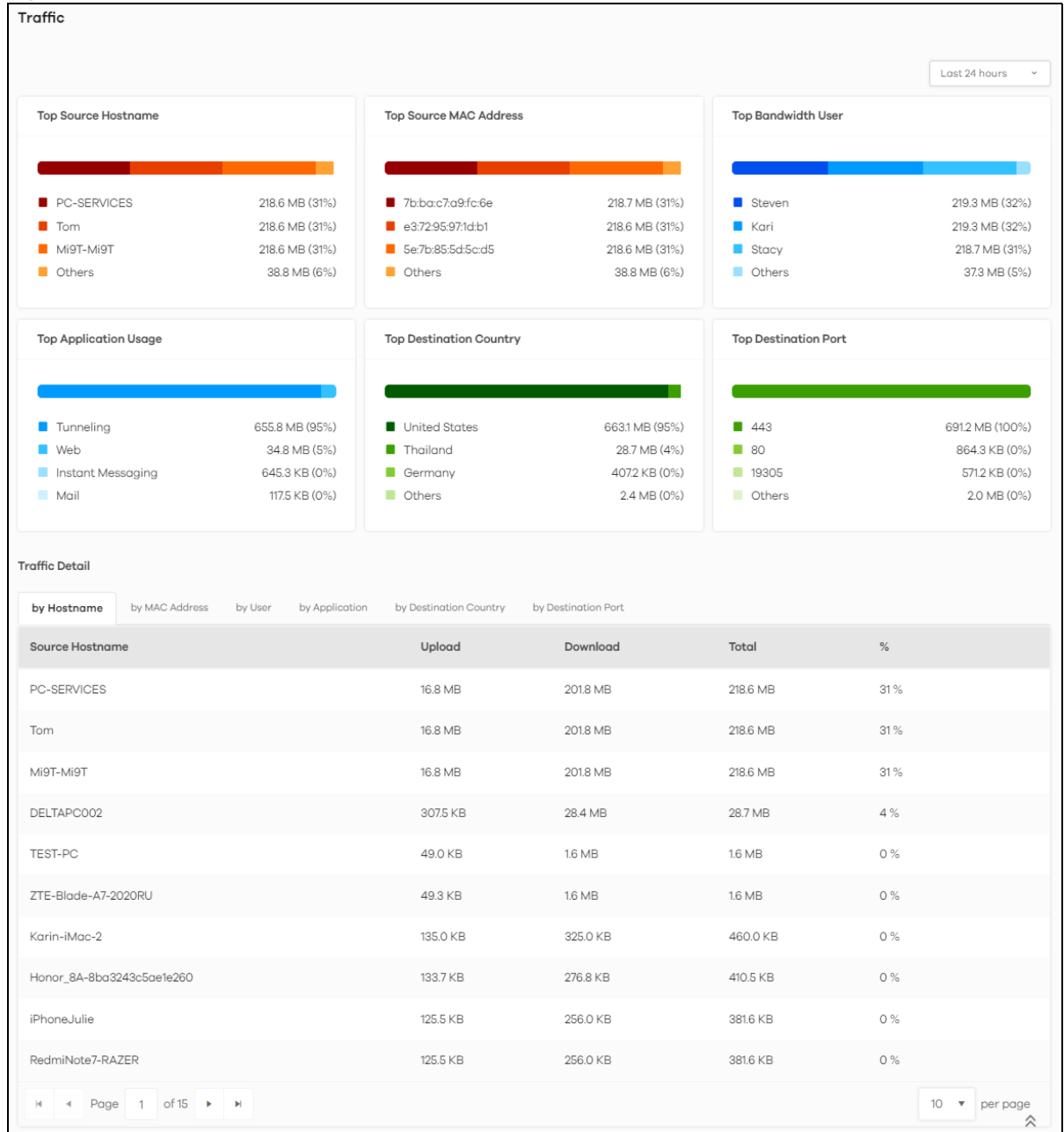
Table 22 Analysis > Network Activity > Web Content Filter

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 23 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

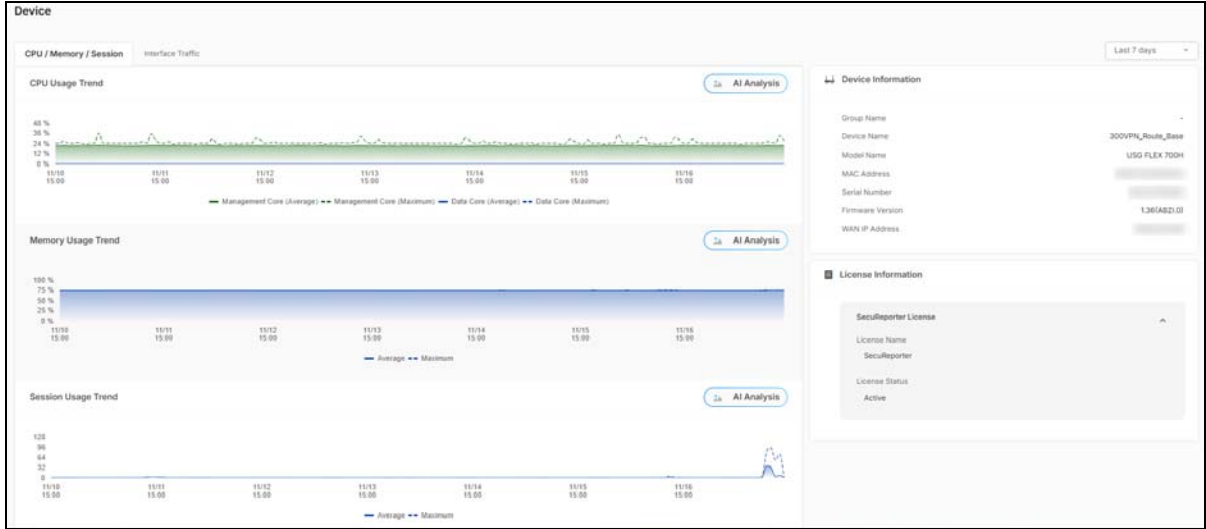
Device data visualizations are categorized as:

- [CPU/Memory/Session](#)
- [Device Health Anomaly Detection](#)
- [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 24 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.
AI Analysis	Click this to see the anomaly events detected by the system.
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 Device Health Anomaly Detection

Device Health Anomaly Detection helps administrators identify unusual CPU, memory, and session usage. SecuReporter uses previous week's behavior and reports on differences in the current week. If it detects a drastic change, it flags the event as an anomaly.

At the time of writing, SecuReporter collects CPU, memory, and session logs and analyzes them regularly. After gathering at least 3 days of data within a week, consecutive or not, it will build an AI baseline.

When SecuReporter finds an anomaly, it generates a summary. The summary highlights usage trends, timelines, durations, and key event details. Administrators can review these highlights and quickly trace logs to identify root causes.

Note: If your device is offline, data collection will stop. Any period without recorded data is flagged as an anomaly.

Note: The system always uses the previous week’s data as the baseline, even if anomalies occurred. The AI only highlights significant deviations. Determining whether that behavior is truly abnormal requires human judgment.

At the time of writing, Device Health Anomaly Detection is available only for the following models:

Table 25 Supported Models

USG FLEX 500H
USG FLEX 700H

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

Figure 30 Analysis > Device > CPU / Memory / Session > AI Analysis



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

Table 26 Analysis > Device > CPU / Memory / Session > AI Analysis

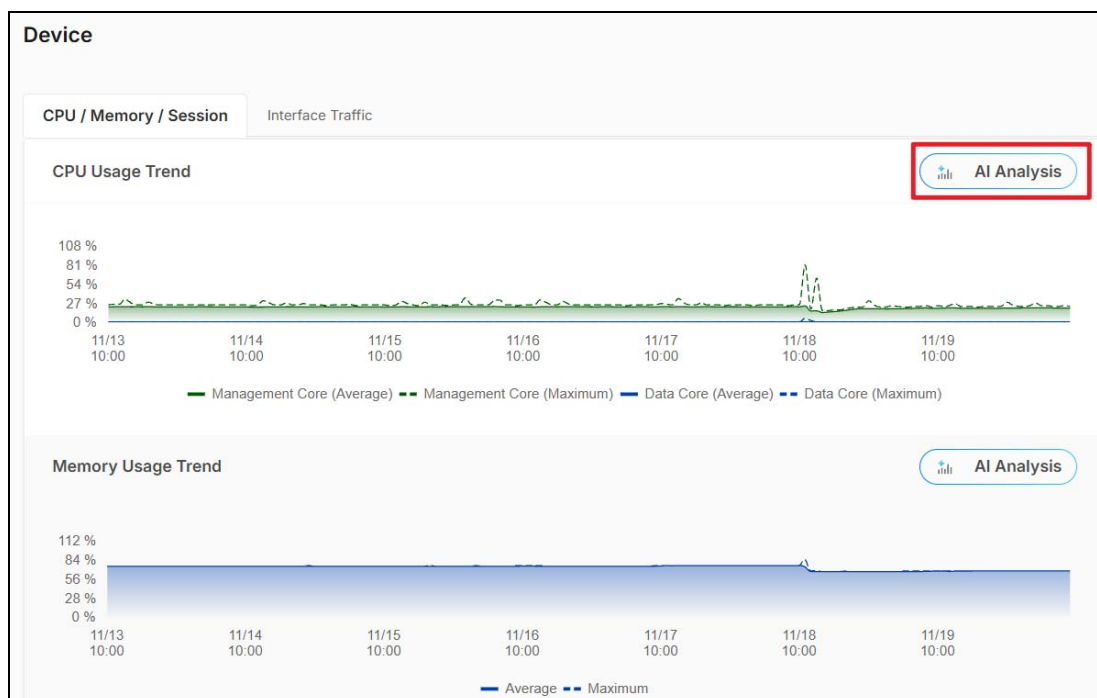
LABEL	DESCRIPTION
Management CPU	Click this to view the management-related CPU usage and anomalies.
Data CPU	Click this to view the data-related CPU usage and anomalies.
Summary	This displays an overview of the anomaly, possible causes and recommended actions. Note: This summary is generated by AI and is not perfect. Verification is still required.
Event Timeline	This displays the start time, end time and the duration of the anomalies.

Table 26 Analysis > Device > CPU / Memory / Session > AI Analysis (continued)

LABEL	DESCRIPTION
Advanced Settings	
Sensitivity	<p>Select the sensitivity level (Low, Medium, or High) from the drop-down menu. Higher sensitivity detects smaller deviations. See Section Table 27 on page 80 for the duration threshold for each level at the time of writing.</p> <p>Note: When you change the sensitivity level, it takes effect within an hour.</p> <p>Note: It is recommended to set the sensitivity level to Medium.</p>

3.6.2.1 How to View the Anomalies

- To view the anomalies, make sure your device is powered on and online. Go to Analysis > Device > CPU / Memory / Session, and click AI Analysis.



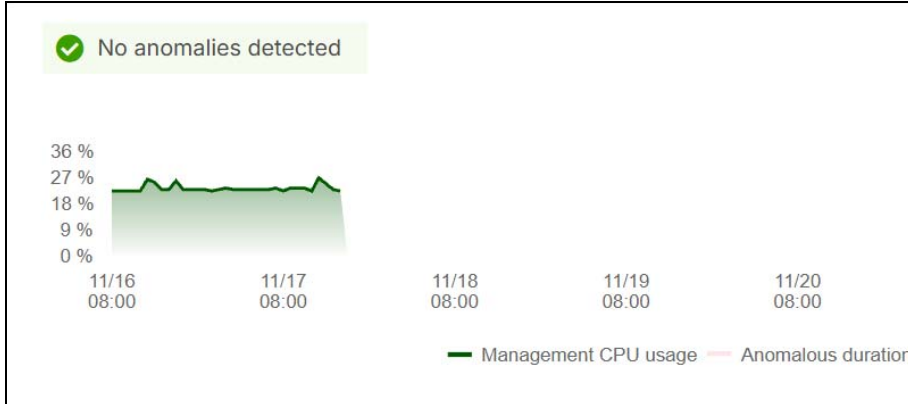
There are three types of messages you may see:

- [No anomalies detected](#)
- [Anomaly events](#)
- [Insufficient baseline data](#)

No anomalies detected

If SecuReporter does not detect any anomalies this week, the banner will display 'No anomalies detected'. Both the Summary and Event Timeline tabs will display no data.

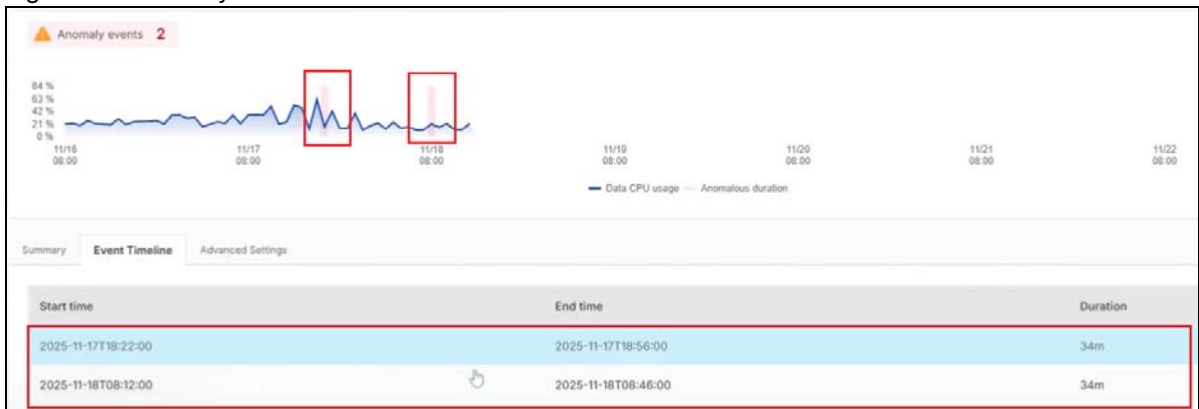
Figure 31 No anomalies detected



Anomaly events

If anomalies are found, the banner will display the number of the anomalies detected this week. The anomalies are shown in pink. [Click the Summary tab to get an overview of the anomalies.](#)

Figure 32 Anomaly events

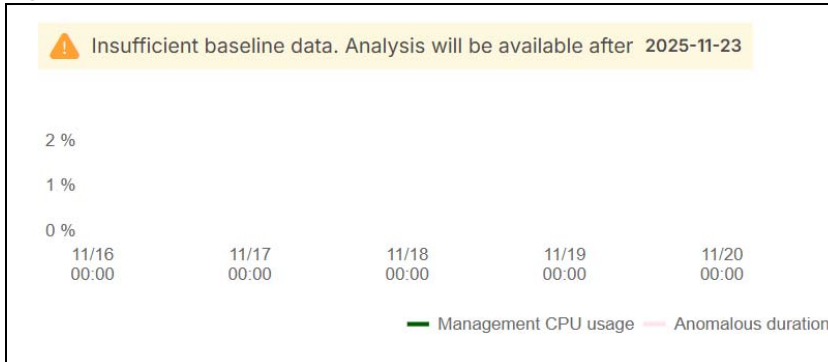


In this example, the first anomaly of the week occurred on 11/17 from 18:22 to 18:56, lasting 34 minutes. The second anomaly occurred on 11/18 from 08:12 to 08:46, also lasting 34 minutes. You can hover over the chart to view the hourly usage.

Insufficient baseline data

SecuReporter requires at least 3 days of data within a week, consecutive or not, to build a baseline. Otherwise, the banner will display 'Insufficient baseline data', and show you when the analysis will be available.

Figure 33 Insufficient baseline data



- 2 Click the Summary tab to get an overview of the anomalies.

Summary Event Timeline Advanced Settings

Diagnostic Report

1. Executive Summary

- The overall CPU health of the 300VPN_Route_Base device appears to be experiencing significant anomalies.
- Numerous CPU spikes and sustained high CPU utilization were detected, indicating potential performance and stability issues.
- The severity of these anomalies is assessed as **High**, as they could significantly impact the device's functionality and service delivery.

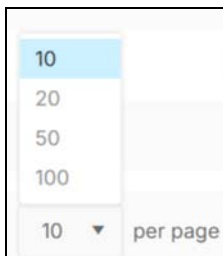
Power by AI, it isn't perfect, we would appreciate your help in making it better.

- 3 Use the Event Timeline tab to see the start/end time and duration of each anomaly. Click each column header to sort the data according to their occurrence or duration time.

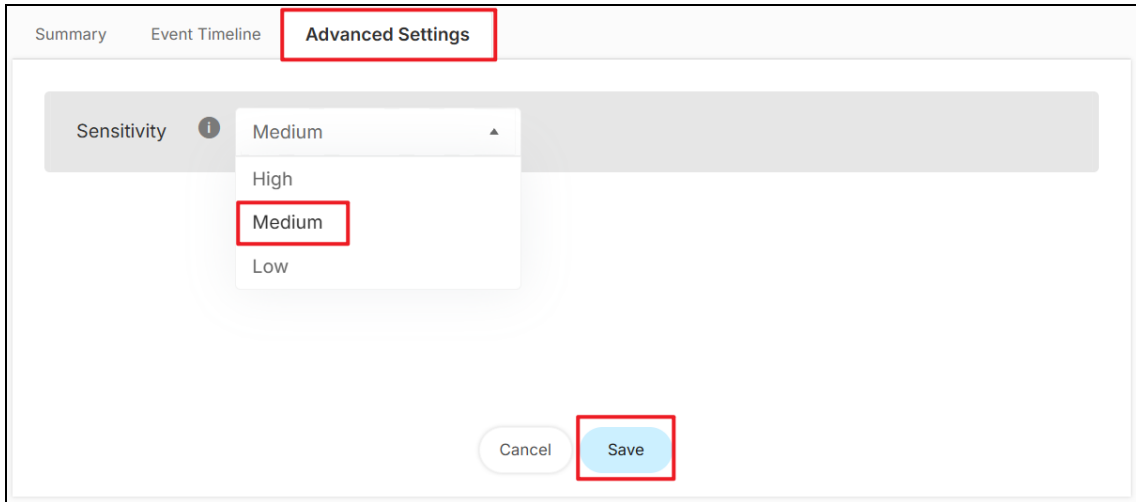
Summary **Event Timeline** Advanced Settings

Start time	End time	Duration
2025-11-19T16:04:00	2025-11-19T16:32:00	28m
2025-11-19T10:34:00	2025-11-19T10:56:00	22m
2025-11-19T10:16:00	2025-11-19T10:28:00	12m

Note: By default, 10 entries are displayed per page, and only entries from the current week are retained. You can use the menu in the bottom-right corner to select how many entries to display per page (10/20/50/100).



- 4 To adjust the detection sensitivity, click Advanced Settings and select a sensitivity level from Low to High from the drop-down menu. Then, click Save. For details on each level, see [See Table 27](#).



Note: The sensitivity level determines how long an anomaly must last before the system reports it. For example, at the time of writing, the duration threshold for each level is shown in the following table.

Table 27 Sensitivity Level Example

LEVEL	DESCRIPTION
High	Detects anomaly that lasts more than 10 minutes.
Medium	Detects anomaly that lasts more than 30 minutes.
Low	Detects anomaly that lasts more than 40 minutes.

Note: If SecuReporter is seemingly reporting too many anomalies, then the lower the Sensitivity, for example from High to Medium. If SecuReporter is seemingly reporting too few anomalies, then the raise the Sensitivity, for example from Low to Medium.

3.6.3 Interface Traffic

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

Figure 34 Analysis > Device > Interface Traffic



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

Table 28 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


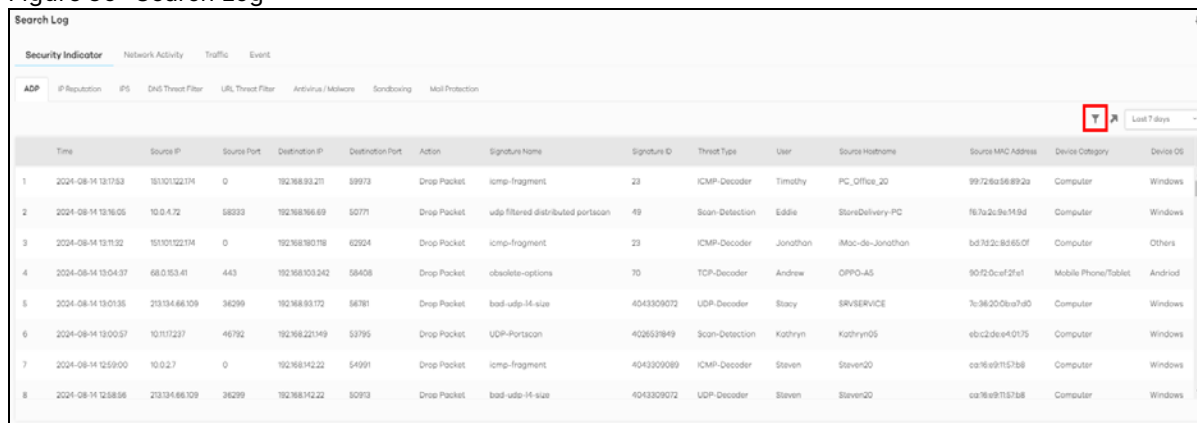

Search log allows you to display Zyxel Device logs based on a time frame and also export them in CSV format for further analysis. You must enable logs to be sent to SecuReporter in the Web Configurator of the Zyxel Device or NCC. You can select Security Indicator, Network Activity, Traffic and Event 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 31 on page 95](#) for details.

Figure 35 Search Log



Time	Source IP	Source Port	Destination IP	Destination Port	Action	Signature Name	Signature ID	Threat Type	User	Source Hostname	Source MAC Address	Device Category	Device OS
2024-08-14 13:17:53	192.168.93.211	0	192.168.93.211	8973	Drop Packet	icmp-fragment	23	ICMP-Decoder	Timothy	PC_Office_20	99728a58892a	Computer	Windows
2024-08-14 13:16:05	10.0.4.72	58233	192.168.166.69	50771	Drop Packet	wsp-filtered-distributed-portscan	49	Scan-Detection	Eddie	StareDelivery-PC	167a2c9e149d	Computer	Windows
2024-08-14 13:11:52	192.168.103.121	0	192.168.103.121	62924	Drop Packet	icmp-fragment	23	ICMP-Decoder	Jonathan	iMac-de-Jonathan	bd732c8d650f	Computer	Others
2024-08-14 13:04:37	68.0.65.41	443	192.168.103.242	58408	Drop Packet	obsolete-options	70	TCP-Decoder	Andrew	OPPO-A5	90f20caf2fe1	Mobile Phone/Tablet	Android
2024-08-14 13:01:35	213.134.66.109	34299	192.168.93.172	58781	Drop Packet	bad-udp-14-size	4043309072	UDP-Decoder	Stacy	SRVSERVICE	7c36200b07d0	Computer	Windows
2024-08-14 13:00:57	10.117.237	46792	192.168.221.149	53795	Drop Packet	UDP-Portscan	4026527849	Scan-Detection	Kathryn	Kathryn05	ebc23ee40175	Computer	Windows
2024-08-14 12:59:00	10.0.2.7	0	192.168.142.22	54991	Drop Packet	icmp-fragment	4043309089	ICMP-Decoder	Steven	Steven20	ca76e81157b8	Computer	Windows
2024-08-14 12:58:56	213.134.66.109	36299	192.168.142.22	50913	Drop Packet	bad-udp-14-size	4043309072	UDP-Decoder	Steven	Steven20	ca76e81157b8	Computer	Windows

You can set the search log criteria by clicking , see [Table 31 on page 95](#) 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 29 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.

Download History Data

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

Last 1 year

Request to Download All

	<input type="checkbox"/>	File Name	File Size	MD5
1	<input type="checkbox"/>	2024-09-02.gzip	1.2 MB	8acc342383d61142b4f95a1dd110c825
2	<input type="checkbox"/>	2024-08-25.gzip	62.6 KB	8d3264d87b28e658d1d5a1c723cadab3
3	<input type="checkbox"/>	2024-08-24.gzip	62.8 KB	2908db4b082b8dda00df7c31fca250b9
4	<input type="checkbox"/>	2024-08-23.gzip	41.7 KB	aaede3026cf7d8e63d81657b121ab73a
5	<input type="checkbox"/>	2024-08-22.gzip	19.8 KB	10d10610852b74a61a1cb2eae03b1c26
6	<input type="checkbox"/>	2024-08-21.gzip	20.0 KB	ebccd72634506bf2bb79b8e386a2b065
7	<input type="checkbox"/>	2024-08-20.gzip	25.3 KB	b255250008629116150c63b17f1cb546
8	<input type="checkbox"/>	2024-08-19.gzip	43.9 KB	ac2069a1c3d18ec708acc81a24a6d787
9	<input type="checkbox"/>	2024-08-18.gzip	19.7 KB	556a1a5d178eab6ef4fb7db9a100042c
10	<input type="checkbox"/>	2024-08-17.gzip	20.3 KB	66d16e3cfd3b6b9ff41bc184f6dca6b8

Page 1 of 13

10 per page

- The following window pops up. Click Done to proceed.

History Data Download Request Sent

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

[Download personal data](#) for your data mapping.

Done

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

←

Download History Data

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

Last 1 year

Request to Download All

	<input type="checkbox"/>	File Name	File Size	MD5
1	<input type="checkbox"/>	2024-09-02.gzip	1.2 MB	8acc342383d61142b4f95a1dd110c825
2	<input type="checkbox"/>	2024-08-25.gzip	62.6 KB	8d3264d87b28e658d1d5a1c723cadab3
3	<input type="checkbox"/>	2024-08-24.gzip	62.8 KB	2908db4b082b8dda00df7c31fca250b9
4	<input type="checkbox"/>	2024-08-23.gzip	41.7 KB	aaede3026cf7d8e63d81657b121ab73a
5	<input type="checkbox"/>	2024-08-22.gzip	19.8 KB	10d10610852b74a61a1cb2eae03b1c26
6	<input type="checkbox"/>	2024-08-21.gzip	20.0 KB	ebccd72634506bf2bb79b8e386a2b065
7	<input type="checkbox"/>	2024-08-20.gzip	25.3 KB	b255250008629116150c63b17f1cb546
8	<input type="checkbox"/>	2024-08-19.gzip	43.9 KB	ac2069a1c3d18ec708acc81a24a6d787
9	<input type="checkbox"/>	2024-08-18.gzip	19.7 KB	556a1a5d178eab6ef4fb7db9a100042c
10	<input type="checkbox"/>	2024-08-17.gzip	20.3 KB	66d16e3cfd3b6b9ff41bc184f6dca6b8

Page 1 of 13

10 per page

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

←

History Data Ready to be Downloaded

The files can be downloaded to your computer.

Download All (40) Personal Data

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

Page 1 of 4 10 per page

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

←

History Data Ready to be Downloaded

The files can be downloaded to your computer.

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

Page 1 of 4

per page

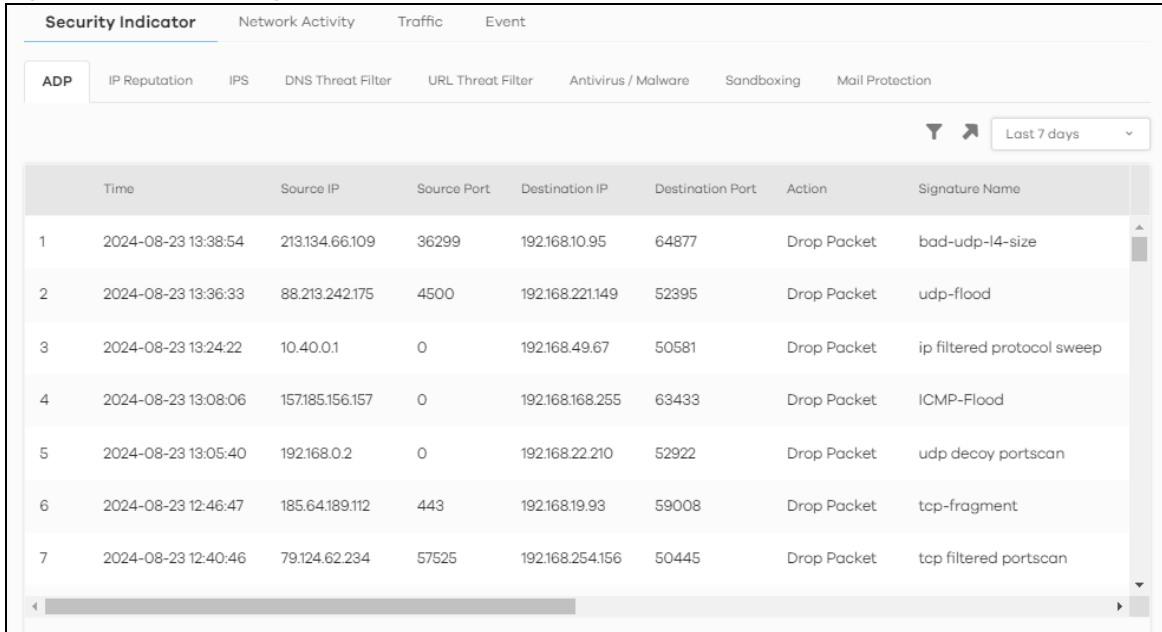
4.2.3 Security Indicator Logs

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 36 Search > Log > Security Indicator



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

Table 30 Search > Log > Security Indicator Screen






LABEL	DESCRIPTION
	<p>Click Clear All to discard the filtering rules.</p> <p>Click Add Rule to create and manage the detailed filtering rules for each label.</p> <p>Click Search to apply the filtering rule to the search log.</p> <p>Click --Please Select-- to set the filtering rule for each label.</p> <p>Click  to discard a filtering rule.</p> <p>The  will appear for the following reasons. Hover the mouse cursor on it to know the type of error.</p> <ul style="list-style-type: none"> • 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).
	<p>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.</p>
	<p>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).</p> <p>Then click Apply to display those logs.</p>

Table 30 Search > Log > Security Indicator Screen (continued)

LABEL	DESCRIPTION
Time	<p>Select the year-month-date hour:minute:second of the log.</p> <p>When adding this as a filter rule, click the drop-down field on the right of the screen to select the time frame.</p>
Source IP	<p>Enter the IPv4 or IPv6 address of the original sender of the packet.</p> <p>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).</p>
Source Port	<p>Enter the port number of the original sender of the packet.</p> <p>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.</p>
Destination IP	<p>Enter the IPv4 or IPv6 address of the final destination of the packet.</p> <p>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).</p>
Destination Port	<p>Enter the port number of the final destination of the packet.</p> <p>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.</p>
Action (IPS/ADP)	<p>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.</p> <p>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.</p>
Action (IP Reputation)	<p>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).</p> <p>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.</p>
Action (DNS Filter)	<p>Enter how the Zyxel Device handle threats posed by FQDNs (Block, Redirect).</p> <p>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.</p>
Action (URL Threat Filter)	<p>Enter how the Zyxel Device handle threats posed by URLs (Uniform Resource Locators) (ACCESS BLOCK, ACCESS WARNING, ACCESS PASS).</p> <p>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.</p>

Table 30 Search > Log > Security Indicator Screen (continued)

LABEL	DESCRIPTION
Action (Antivirus / Malware)	<p>Enter ACCESS FORWARD when a service can be used to access the Zyxel Device. Otherwise, it is ACCESS BLOCK.</p> <p>Enter FILE FORWARD when a file is allowed. Otherwise, it is FILE DESTROY.</p> <p>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.</p>
Action (Sandboxing)	<p>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).</p> <p>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.</p>
Action (Mail Protection)	<p>Enter how the Zyxel Device handle spam SMTP/POP3 email (MAIL FORWARD, MAIL DROP).</p> <p>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.</p>
User	<p>Depending on the data protection policy (see Section 2.2.1 on page 27 for details), the following will be displayed:</p> <ul style="list-style-type: none"> • 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	<p>Enter the name (case sensitive, a wildcard is allowed) of a signature.</p> <p>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.</p>
Signature ID	<p>Enter the identification number of the signature.</p> <p>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.</p>
Threat Type	<p>Enter the signature (case sensitive) by threat type.</p> <p>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.</p>
Mail From	<p>Depending on the data protection policy (see Section 2.2.1 on page 27 for details), the following will be displayed:</p> <ul style="list-style-type: none"> • 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	<p>Depending on the data protection policy (see Section 2.2.1 on page 27 for details), the following will be displayed:</p> <ul style="list-style-type: none"> • 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 30 Search > Log > Security Indicator Screen (continued)

LABEL	DESCRIPTION
Mail Subject	This is the title header of the incoming email.
Protocol (Sandboxing)	<p>Enter the method email is sent or received through the Zyxel Device (SMTP, POP3, HTTP, FTP, and Unknown).</p> <p>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.</p>
Protocol (Mail Protection)	<p>Enter the method email is sent or received through the Zyxel Device (SMTP and POP3).</p> <p>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.</p>
URL	<p>Enter the URL (a wildcard is allowed) where the threat was detected.</p> <p>When adding this as a filter rule, enter the URL or part of the URL you want to find to enable SecuReporter auto suggestion.</p>
File Type	<p>Enter the type of file sent for sandboxing inspection (Archives (.zip), Executables, MS Office Documents, Macromedia Flash Data/PDF/RTF).</p> <p>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.</p>
Score Level	<p>Enter the score given by the Defend Center for malware characteristics that has been detected through the sandboxing function (Malicious, Suspicious, and Clean).</p> <p>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.</p>
Hash	<p>Copy the hash value (a wildcard is allowed) of the file that was sent for sandboxing inspection.</p> <p>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.</p>
Rule Number	<p>Enter the log search rule number. This is assigned by the Zyxel Device.</p> <p>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.</p>
Scan Result	<p>Enter the scan result (White-List, Black-List, IP-Reputation, DNSBL, DNSBL-timeout, Spam, Virus, Spam-Virus, Timeout, Clear, and Phishing).</p> <p>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.</p>
Severity	<p>Enter the severity levels as defined in the Zyxel Device. (1) Very-Low, (2) Low, (3) Medium, (4) High, and (5) Severe.</p> <p>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.</p>

Table 30 Search > Log > Security Indicator Screen (continued)

LABEL	DESCRIPTION
Category Name	<p>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.</p> <p>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.</p>
Threat Name	<p>Enter the name of the threat (a wildcard is allowed) as detected by the Zyxel Device. The value depends on the Zyxel Device.</p> <p>When adding this as a filter rule, enter the threat name you want to find.</p>
Risk	<p>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.</p> <p>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.</p>
Threat Category	<p>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.</p> <p>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.</p>
Risk IP	<p>Enter the IPv4 or IPv6 address where the threat was detected.</p> <p>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).</p>
Virus Name	<p>Enter the name (case sensitive, a wildcard is allowed) of a virus.</p> <p>When adding this as a filter rule, enter the first letter to enable SecuReporter auto suggestion.</p>
File Name	<p>Enter the name (a wildcard is allowed) of the file.</p> <p>When adding this as a filter rule, enter the first letter to enable SecuReporter auto suggestion.</p>
Application Category Name	<p>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.</p> <p>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.</p>
Application Name	<p>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).</p> <p>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.</p>

Table 30 Search > Log > Security Indicator Screen (continued)

LABEL	DESCRIPTION
Web Category Name	<p>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.</p> <p>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.</p>
Website	<p>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.</p> <p>When adding this as a filter rule, enter the website or part of the website you want to find to enable SecuReporter auto suggestion.</p>
Query Type	<p>Enter the type of IP address that may pose a security threat to network devices behind the Zyxel Device.</p> <p>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.</p>
Domain	<p>Enter the URL of FQDNs that may pose a security threat to network devices behind the Zyxel Device.</p> <p>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.</p>

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 37 Search > Log > Network Activity

	Time	Source IP	Action	Category Name	Query Type	Domain
1	2024-08-23 13:46:14	192.168.80.70	Forward	Instant Messaging	A	mmx-ds.cdn.whatsapp.net
2	2024-08-23 13:42:44	192.168.170.76	Redirect	Games	A	gameplay.intel.com
3	2024-08-23 13:34:52	192.168.10.95	Redirect	Marketing/Merchandising	A	justpremium.com
4	2024-08-23 13:31:56	192.168.222.253	Block	Instant Messaging	DS	whatsapp.net
5	2024-08-23 13:28:10	192.168.244.105	Redirect	PUPs	A	d1v18wytztdz.cloudfront.net
6	2024-08-23 13:27:03	192.168.182.239	Forward	Software/Hardware	A	dns.msftncsi.com
7	2024-08-23 13:22:43	192.168.210.7	Redirect	Pornography	A	notification.tubecup.net

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

Table 31 Search > Log > Network Activity Screen

LABEL	DESCRIPTION
	<p>Click Clear All to discard the filtering rules.</p> <p>Click Add Rule to create and manage the detailed filtering rules for each label.</p> <p>Click Search to apply the filtering rule to the log search.</p> <p>Click --Please Select-- to set the filtering rule for each label.</p> <p>Click to discard a filtering rule.</p> <p>The will appear for the following reasons. Hover the mouse cursor on it to know the type of error.</p> <ul style="list-style-type: none"> • 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).
	<p>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.</p>
	<p>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).</p> <p>Then click Apply to display those logs.</p>

Table 31 Search > Log > Network Activity Screen (continued)

LABEL	DESCRIPTION
Time	<p>Select the year-month-date hour:minute:second of the log.</p> <p>When adding this as a filter rule, click the drop-down field on the right of the screen to select the time frame.</p>
Source IP	<p>Enter the IPv4 or IPv6 address of the original sender of the packet.</p> <p>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).</p>
Source Port	<p>Enter the port number of the original sender of the packet.</p> <p>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.</p>
Destination IP	<p>Enter the IPv4 or IPv6 address of the final destination of the packet.</p> <p>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).</p>
Destination Port	<p>Enter the port number of the final destination of the packet.</p> <p>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.</p>
Action (DNS Content Filter)	<p>Enter how the Zyxel Device handle threats posed by domains (Block, Redirect, Forward).</p> <p>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.</p>
Action (App Patrol)	<p>Enter how the Zyxel Device handle threats posed by applications (reject, drop, forward).</p> <p>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.</p>
Action (Web Content Filter)	<p>Enter how the Zyxel Device handle threats posed by websites (forward, block, warning).</p> <p>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.</p>
User	<p>Depending on the data protection policy (see Section 2.2.1 on page 27 for details), the following will be displayed:</p> <ul style="list-style-type: none"> • 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	<p>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.</p> <p>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.</p>

Table 31 Search > Log > Network Activity Screen (continued)

LABEL	DESCRIPTION
Application Name	<p>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).</p> <p>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.</p>
Web Category Name	<p>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.</p> <p>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.</p>
Website	<p>Enter the website (a wildcard is allowed) to screen the most common threats by websites blocked by the Zyxel Device.</p> <p>When adding this as a filter rule, enter the website or part of the website you want to find to enable SecuReporter auto suggestion.</p>
Query Type	<p>Enter the DNS record types for accessed domains that were blocked. DNS record types include A, AAAA, HTTPS, TXT and so on.</p> <p>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.</p>
Domain	<p>Enter the URL of FQDNs that may pose a security threat to network devices behind the Zyxel Device.</p> <p>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.</p>
Rule	<p>Enter the name of the policy control rule the the connection is using.</p> <p>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.</p>
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 38 Search > Log > Traffic

Time	Source IP	Source Port	Destination IP	Destination Port	Application Name	Traffic Protocol	Connection Duration(S)	Inbound Traffic	Outbound Traffic	User	Source Hostname	Source MAC Address	Device Category	Device OS
2025-08-13 17:49:00	192.168.80.81	53695	8.8.8.8	53	domain	TCP	10	197	262	Christopher	mand500v281	018e37bd3320	Computer	Windows
2025-08-13 17:59:18	192.168.49.67	52290	3.219.6.82	443	https	TCP	6	4020	1045	Christopher	OPPO-F8	fcc668ec4ca8	Mobile Phone...	Android
2025-08-13 17:33:21	192.168.138.1	61531	1111	53	domain	TCP	10	232	255	Gabriella	iMac	3d779ebd34c4	Computer	Others
2025-08-13 17:32:57	192.168.158.1	49728	54.192.97.64	443	others	TCP	6	7253	1766	Steven	ASUS_RT-AC67...	6686a6c623e4	Wireless AP	Others
2025-08-13 17:32:11	192.168.19.93	57327	8.8.4.4	53	domain	TCP	9	240	155	Kathryn	MBP-de-Gond...	af7096fa250e	Computer	Others
2025-08-13 17:28:22	192.168.185.1	64634	1111	53	domain	TCP	5	286	248	Arthur	ASUS3453-PC	224c15d38329	Computer	Windows
2025-08-13 17:21:23	192.168.26.63	110	736.64.72	63849	pop3	TCP	9	6604	1987	Steven	ZTE-Blade-A5...	9f8f62652247	Mobile Phone...	Android
2025-08-13 17:20:25	192.168.141.1	59046	2.38.107.21	80	others	TCP	14	5339	2073	Gabriella	iPhone	da039c2008a5	Mobile Phone...	iOS

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

Table 32 Search > Log > Traffic

LABEL	DESCRIPTION
	<p>Click Clear All to discard the filtering rules.</p> <p>Click Add Rule to create and manage the detailed filtering rules for each label.</p> <p>Click Search to apply the filtering rule to the log search.</p> <p>Click --Please Select-- to set the filtering rule for each label.</p> <p>Click to discard a filtering rule.</p> <p>The will appear for the following reasons. Hover the mouse cursor on it to know the type of error.</p> <ul style="list-style-type: none"> • 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).
	<p>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.</p>
	<p>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).</p> <p>Then click Apply to display those logs.</p>
Time	<p>Select the year-month-date hour:minute:second of the log.</p> <p>When adding this as a filter rule, click the drop-down field on the right of the screen to select the time frame.</p>
Source IP	<p>Enter the IPv4 or IPv6 address of the original sender of the packet.</p> <p>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).</p>

Table 32 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 27 for details), the following will be displayed: <ul style="list-style-type: none"> • 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 39 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 33 Search > Log > Event Screen

LABEL	DESCRIPTION
	<p>Click Clear All to discard the filtering rules.</p> <p>Click Add Rule to create and manage the detailed filtering rules for each label.</p> <p>Click Search to apply the filtering rule to the log search.</p> <p>Click --Please Select-- to set the filtering rule for each label.</p> <p>Click to discard a filtering rule.</p> <p>The will appear for the following reasons. Hover the mouse cursor on it to know the type of error.</p> <ul style="list-style-type: none"> • 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).
	<p>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.</p>
	<p>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).</p> <p>Then click Apply to display those logs.</p>

Table 33 Search > Log > Event Screen (continued)

LABEL	DESCRIPTION
Time	<p>Select the year-month-date hour:minute:second of the log.</p> <p>When adding this as a filter rule, click the drop-down field on the right of the screen to select the time frame.</p>
Source IP	<p>Enter the IPv4 or IPv6 address of the original sender of the packet.</p> <p>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).</p>
Destination IP	<p>Enter the IPv4 or IPv6 address of the final destination of the packet.</p> <p>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).</p>
Service Name	<p>Enter the login method (console, http/https, ssh).</p> <p>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.</p>
Action Event > User Login	<p>Enter the status of the login attempt (Failed-login / logged-in / logged-out).</p> <p>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.</p>
Action Event > DHCP	<p>Enter the action of assigning an IP address to a device by the DNS server or release (assigned and release).</p> <p>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.</p>
Assign IP	<p>This is the IPv4 or IPv6 address currently assigned to a DHCP client or reserved for a specific MAC address.</p> <p>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).</p>
User	<p>Depending on the data protection policy (see Section 2.2.1 on page 27 for details), the following will be displayed:</p> <ul style="list-style-type: none"> • 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	<p>Enter the role type (a wildcard is allowed) of the event's login attempt (Administrator, Limited-Admin, User).</p> <p>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.</p>
MAC Address Event > User Login	<p>Enter the Zyxel Device's MAC address (case sensitive) during the event's login attempt.</p> <p>Depending on the data protection policy (see Section 2.2.1 on page 27 for details), the following will be displayed:</p> <ul style="list-style-type: none"> • 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 33 Search > Log > Event Screen (continued)

LABEL	DESCRIPTION
MAC Address Event > DHCP	<p>Enter the MAC address (case sensitive) to which the IP address is currently assigned or for which the IP address is reserved.</p> <p>Depending on the data protection policy (see Section 2.2.1 on page 27 for details), the following will be displayed:</p> <ul style="list-style-type: none"> • 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	<p>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.</p> <p>Depending on the data protection policy (see Section 2.2.1 on page 27 for details), the following will be displayed:</p> <ul style="list-style-type: none"> • 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:

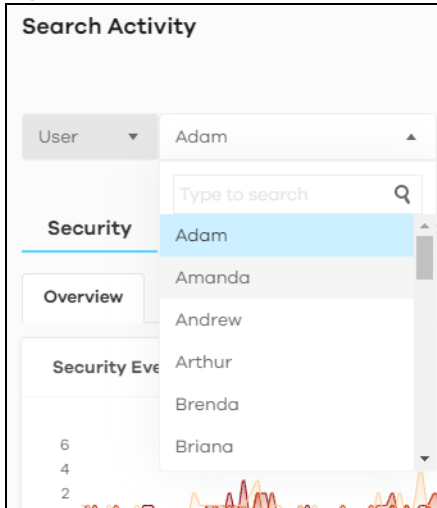
- User
- IP address
- MAC address or
- Hostname of the client device.

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 40 Search > Activity > User



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

Table 34 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				

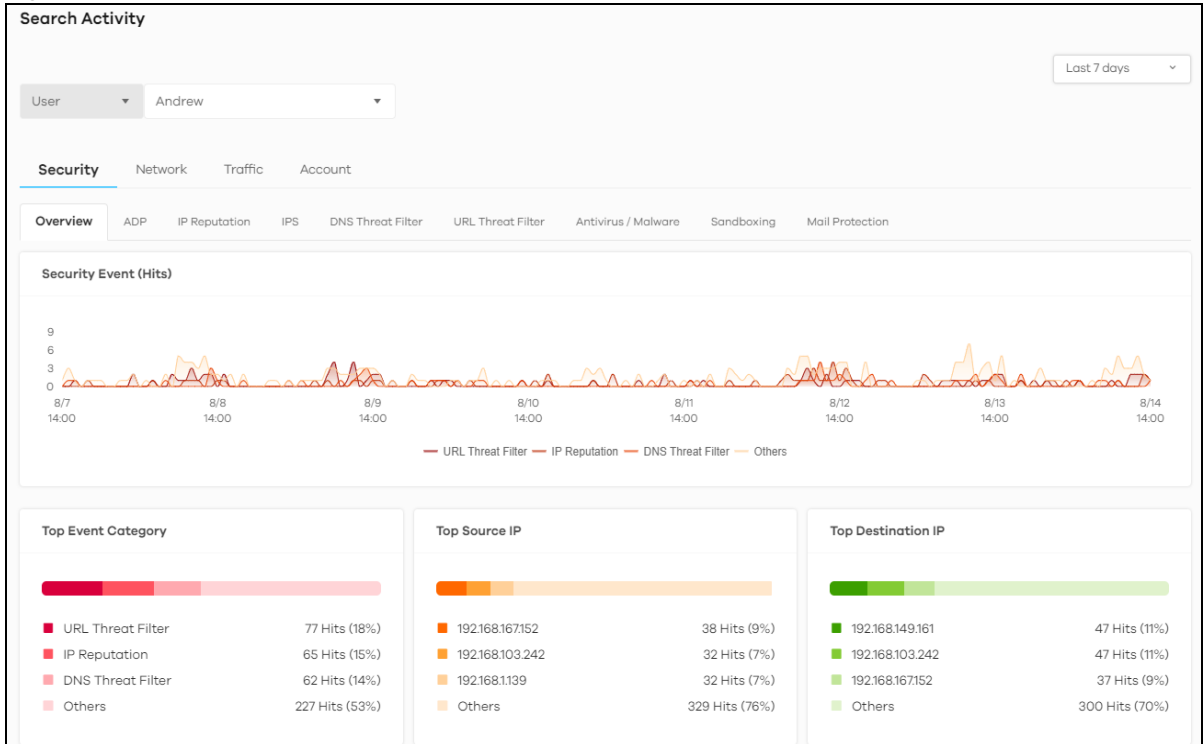
4.3.1 Security Search

Security searches include:

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

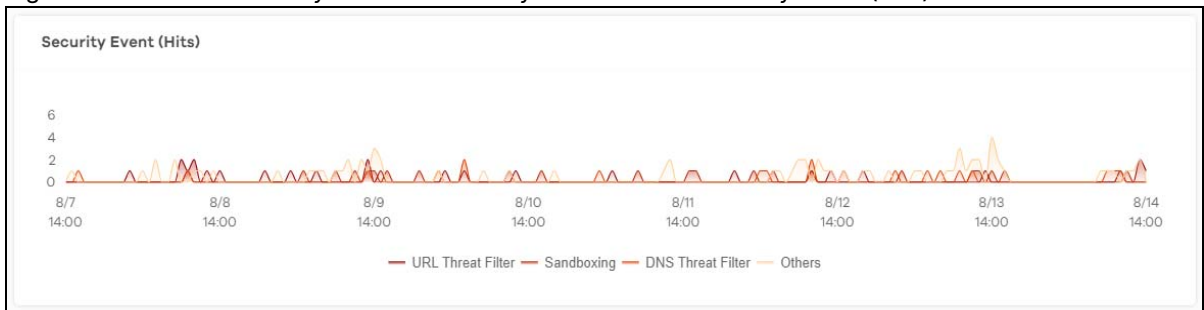
For a User, click Search > Activity > User > Security > Overview to display the following figure.

Figure 41 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 42 Search > Activity > User > Security > Overview > Security Event (Hits)



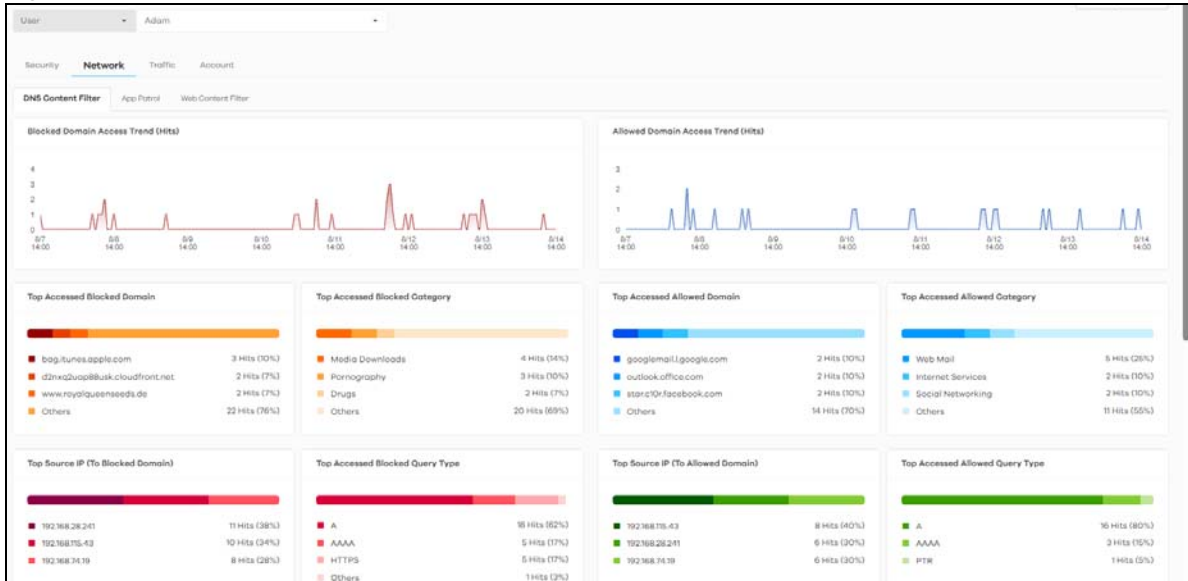
4.3.2 Network Search

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 43 Search > Activity > User > Network > DNS Content Filter

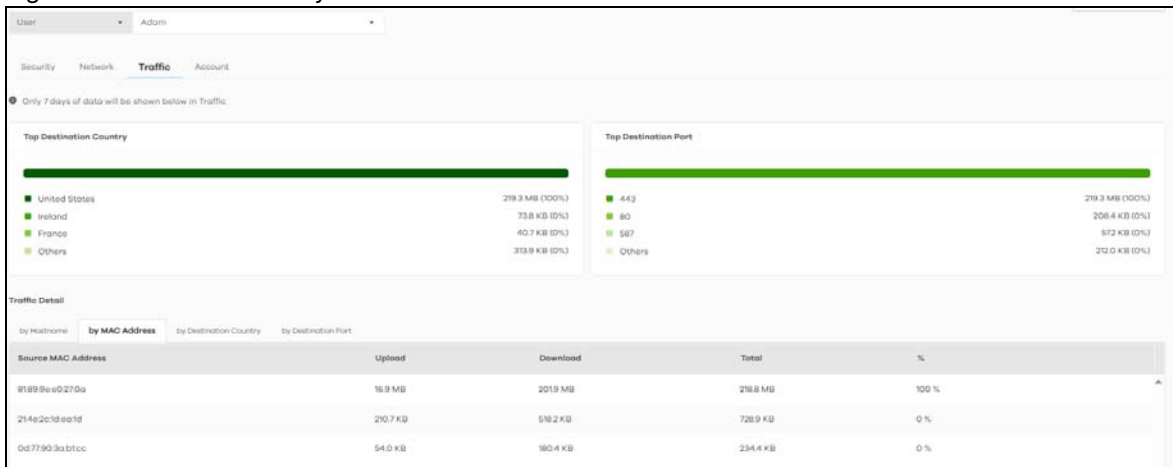


4.3.3 Traffic Search

Traffic searches are for up to seven days of data.

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

Figure 44 Search > Activity > User > Traffic



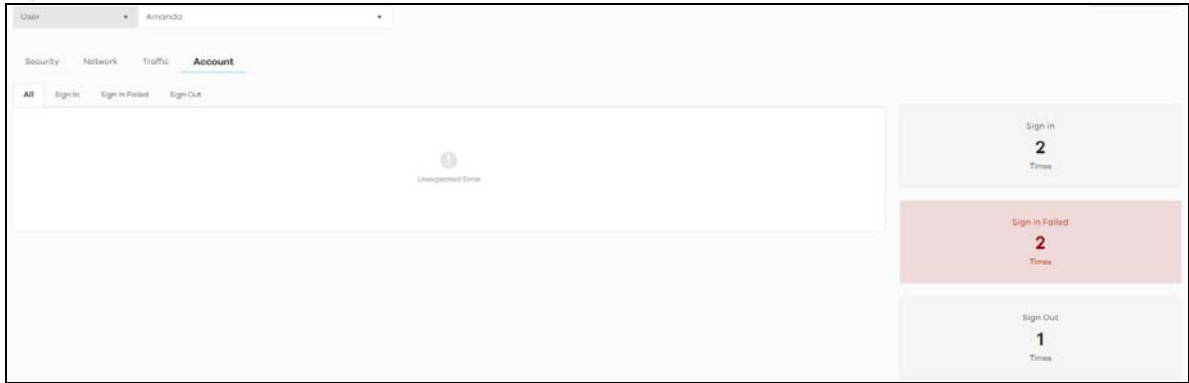
4.3.4 Account Search

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 45 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.

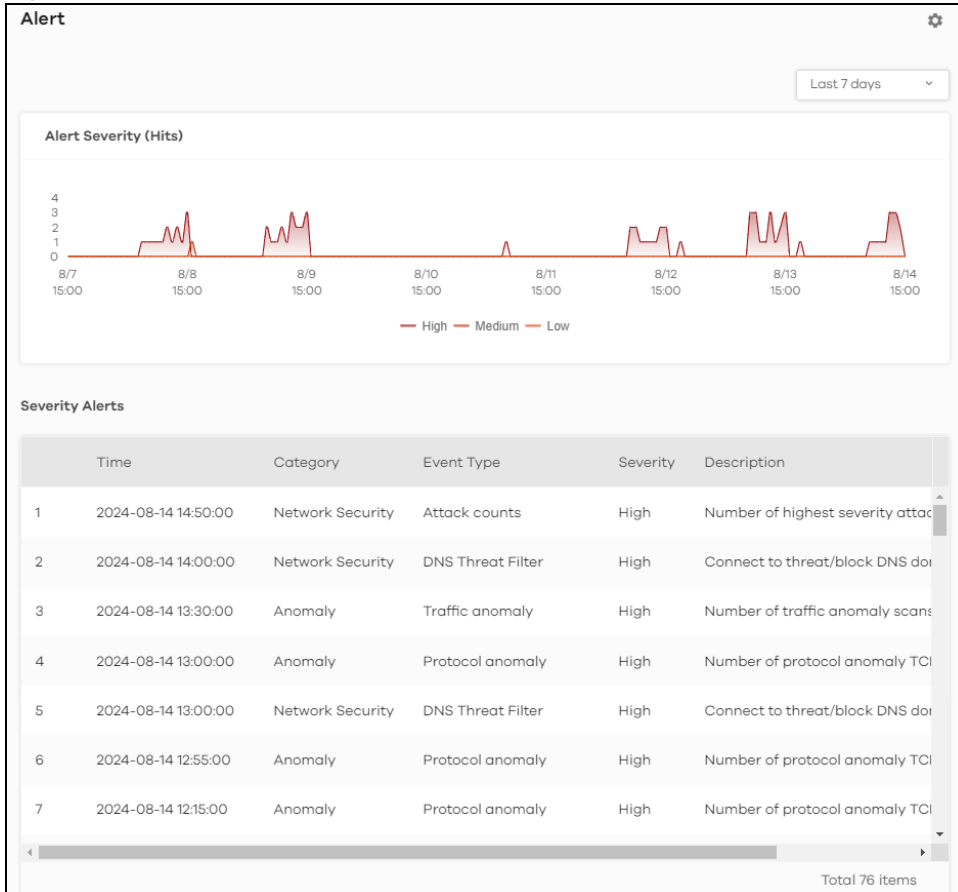
Table 35 Event Categories, Types and Criteria

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 35 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 46 History > Alert



The following table describes the labels on this screen.

Table 36 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 10 on page 22 .
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 47 History > Alert > Alert Settings > Email Notification

The following table describes the labels in this screen.

Table 37 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. <ul style="list-style-type: none"> 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 37 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 48 History > Alert > Alert Settings > View/Edit Alert Definition > Network Security

View / Edit Alert Definition

Network Security Device Anomaly

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

High Number of attacks is over times within 5 minutes.

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

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

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

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

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

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

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

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

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

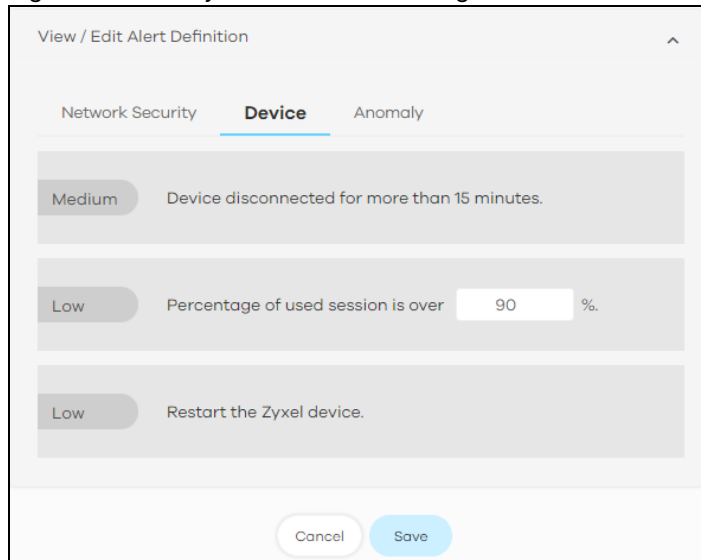
The following table describes the labels in this screen.

Table 38 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 49 History > Alert > Alert Settings > View/Edit Alert Definition > Device



The following table describes the labels in this screen.

Table 39 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 50 History > Alert > Alert Settings > View/Edit Alert Definition > Anomaly

The screenshot shows the 'View / Edit Alert Definition' interface for 'Anomaly' alerts. It features three tabs: 'Network Security', 'Device', and 'Anomaly' (which is selected). Below the tabs, there are three alert rule entries, each with a severity level and a description:

- High**: Number of traffic anomaly scans/floods detected is over times within 5 minutes.
- High**: Number of protocol anomaly TCP/UDP/ICMP/IP decoders is over times within 5 minutes.
- Medium**: Number of login failures is over times within 1 minute.

At the bottom of the screen, there are two buttons: 'Cancel' and 'Save'.

The following table describes the labels in this screen.

Table 40 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.

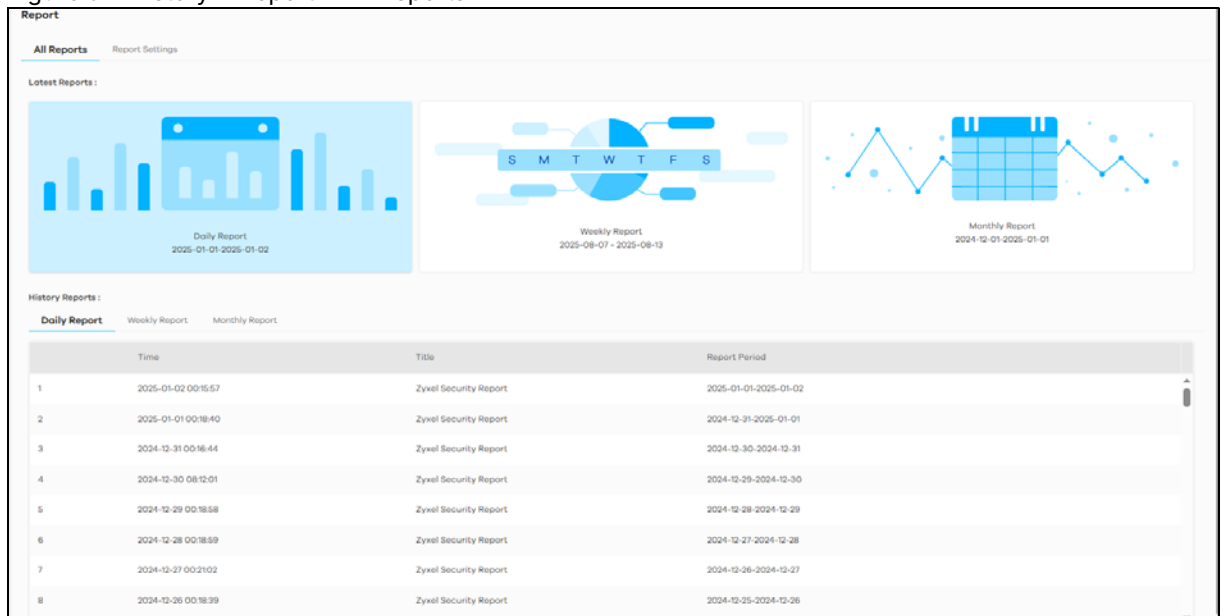
You can choose to generate reports of analyzed data collected over one of three time frames:

- 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 51 History > Report > All Reports



The following table describes the labels on this screen.

Table 41 History > Report > All Reports

LABEL	DESCRIPTION
Latest Reports	<p>Get a summary report of activities in HTML or PDF format.</p> <p>Latest Reports are classified according to the following:</p> <ul style="list-style-type: none"> • Daily Report • Weekly Report • Monthly Report <p>Clicking any of the above will allow you to view the report online. You can then download it in PDF format or print it.</p>
History Reports	<p>This displays the type of report by clicking on the tab.</p> <ul style="list-style-type: none"> • Daily Report • Weekly Report • Monthly Report
Time	<p>This displays the reports in order of the date and time they were created, starting with the most recent one.</p>
Title	<p>This displays the title of each report as configured in Report Settings.</p>
Report Period	<p>This displays the date that the report covers.</p> <p>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.</p>
Action	<p>Click a row to display the report online. You can then download it in PDF format or print it.</p> <p>Click  to send a report in PDF format to the designated email recipients. Enter an email address and press Enter.</p> <p>Note: You can configure up to 30 email addresses.</p> <p>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.</p>

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

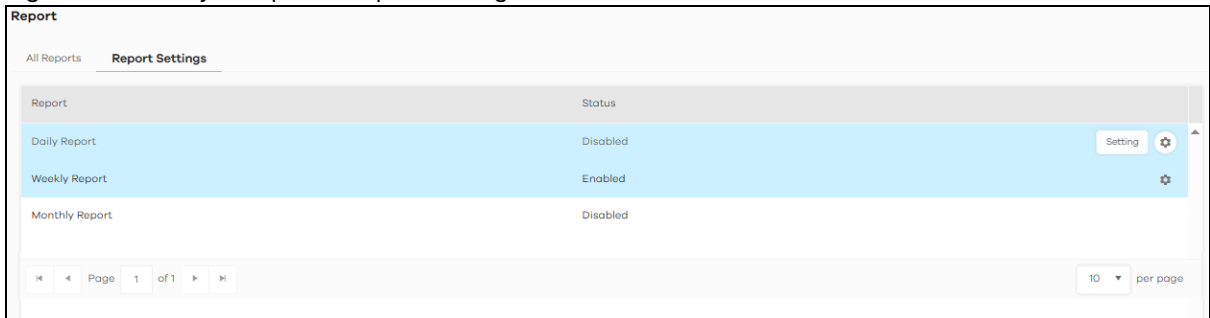
AI generates smart summaries based on the (raw) data collected from the weekly report. Created summaries allow you to identify key insights quickly and act promptly if need be.

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 52 History > Report > Report Settings



The following table describes the labels on this screen.

Table 42 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 53 History > Report > Report Settings > Weekly Report Settings

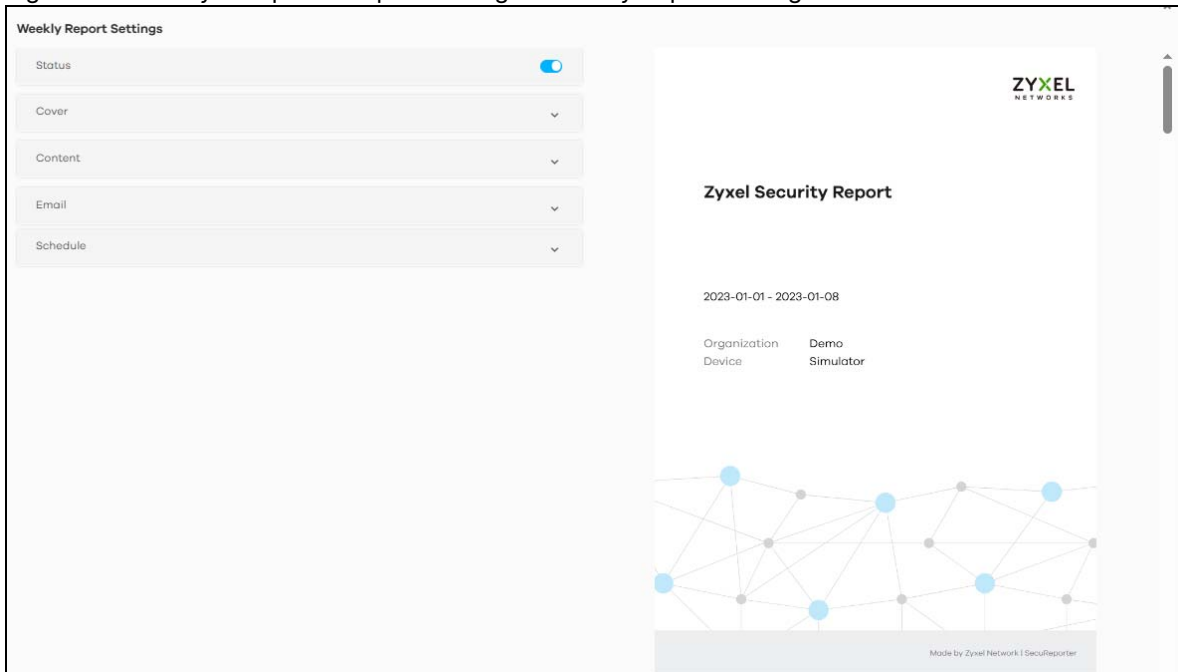


Figure 54 History > Report > Report Settings > Weekly Report Settings

Weekly Report Settings

Status

Cover

Cover Design

Classic Security Simplicity

Customized Logo

Choose file

Report Title

Zyxel Security Report

Content

Security Indicator

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

Network Activity

- DNS Content Filter
- Web Content Filter
- App Patrol

Traffic

Email

Email Title

SecuReporter Schedule Report

Always receive report for device agent and admin?

Yes No

Additionally, send email reports to :

Schedule

Report Schedule

Thursday

The following table describes the labels on this screen.

Table 43 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://securereporter.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://securereporter.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.

I've registered a passkey, but I cannot log in to the portal with it.

- Log into the same device where you registered your passkey:
Passkeys are stored locally on the device they were created on. To sign in using Passkey A, you must use the same device (computer A) where it was registered. It won't work from another computer or mobile device, unless you're using a cloud-synchronized passkey.
- Log into a different device within the same operating system:
If you are using cloud-synchronized passkeys, such as iCloud Keychain or Google Password Manager, you can log in on another device within the same operating system. For example, logging in on a Mac after registering a passkey with an iPhone.
Make sure to sync the passkeys on your devices.
For iOS operating systems: go to Settings > Apple ID > iCloud > Passwords and Keychain > Sync this iPhone.
For Android operating systems: go to Settings > Google > Password Manager > Passwords > Sync.

How many passkeys can a Zyxel Account have?

See [Passkey Limit](#) for the maximum number of Passkeys for each account. If you have reached the limit, the system will prompt you to remove an existing passkey before adding a new one.

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 26](#) 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 am getting too many anomalies.

If you are receiving a high number of anomalies, it may be due to the following reasons:

- Previous week had many anomalies

If last week had many anomalies (for example, due to the device being offline), current anomalies may simply reflect differences from last week's baseline.


- Sensitivity level is set too high

Higher sensitivity detects shorter-durations anomalies. You can go to Analysis > Device > AI Analysis > Advanced Settings, and lower the sensitivity level, for example, from High to Medium. For details on each level, see [Section Table 27 on page 80](#).

- Device is offline

When a device goes offline, data collection stops. Any period without recorded data can be flagged as an anomaly. Since powering off the device may itself be considered abnormal behavior.

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

Copyright © 2025 by Zyxel and/or its affiliates.

The contents of this publication may not be reproduced in any part or as a whole, transcribed, stored in a retrieval system, translated into any language, or transmitted in any form or by any means, electronic, mechanical, magnetic, optical, chemical, photocopying, manual, or otherwise, without the prior written permission of Zyxel and/or its affiliates.

Published by Zyxel and/or its affiliates. All rights reserved.

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.

A

- account name
 - view [17](#)
- activity
 - search [102](#)
- administration privilege
 - priority [34](#)
- ADP
 - hits [24, 43](#)
- ADP data visualization [41](#)
- ADP screen [43](#)
- advanced persistent threat (APT) [38](#)
- Advanced Zyxel Sandboxing Inspection [39](#)
- alert
 - SecuReporter [107](#)
 - severity [109](#)
- alert notification
 - interval [110](#)
- Alert screen [107](#)
- Alert Settings screen [110](#)
- allowed application
 - hits [70](#)
- Analysis [35](#)
- Anomaly Detection [75](#)
- anomaly detection [47](#)
- Anomaly Detection and Prevention (ADP) [41](#)
- anti malware
 - data visualization [59](#)
 - filter rule [91](#)
- Anti Malware screen [39, 61](#)
- anti virus
 - data visualization [59](#)
- Anti Virus screen [61](#)
- anti-malware scanner
 - run [40](#)
- app list
 - view [16](#)
- app patrol data visualization [68](#)
- App Patrol screen [70](#)

- application
 - with most bandwidth usage [24, 74](#)
- application category name
 - filter rule [93, 96](#)
- application name
 - filter rule [93, 97, 99](#)
- assign IP
 - filter rule [101](#)
- Astra email [99](#)
- attack
 - destination of threat [22](#)
 - source of threat [22](#)
 - time period percentage [22](#)
- attack type [22](#)
 - percentage [22](#)

B

- blocked application
 - hits [70](#)

C

- cache
 - Zyxel Device [38](#)
- category name
 - filter rule [93](#)
- certifications
 - viewing [129](#)
- Circle web site [17](#)
- claimed Zyxel Device [30](#)
- Cloud CNM suite [7](#)
- cloud sandboxing
 - results [38](#)
- cloud-based analytics tool [7](#)
- CNAME (Canonical Name) [51](#)
- configuration
 - report [116](#)

- connection duration [99](#)
 - contact information [124](#)
 - copyright [129](#)
 - countries
 - received most data traffic from Zyxel Device [24](#),
[74](#)
 - CSV file [89](#), [95](#), [98](#), [100](#)
 - CSV format [83](#)
 - customer support [124](#)
- ## D
- Dark Mode [16](#)
 - Dashboard screen [22](#)
 - data protection
 - change level [29](#)
 - data protection policy [91](#), [96](#), [99](#), [101](#)
 - Defend Center
 - for malware characteristics [92](#)
 - destination IP
 - filter rule [90](#), [96](#), [99](#), [101](#)
 - destination IP address [37](#)
 - destination port
 - bandwidth usage [24](#), [74](#)
 - filter rule [90](#), [96](#), [99](#)
 - Device Health Anomaly Detection [75](#)
 - Device tab [27](#)
 - DHCP
 - filter rule [101](#)
 - disclaimer [129](#)
 - display
 - Dark Mode [16](#)
 - DNS (Domain Name System) [53](#)
 - DNS Filter [50](#)
 - filter rule [90](#)
 - hits [24](#)
 - DNS Filter screen [53](#), [54](#), [58](#)
 - DNS query
 - type [50](#)
 - DNS query packet [50](#)
 - DNS response
 - fake [50](#)
 - domain
 - filter rule [94](#), [97](#)
 - second-level [50](#)
 - top level [50](#)
 - Domain Name System (DNS) server [50](#)
- ## E
- EICAR test file [39](#)
 - email alert
 - description [111](#)
 - email protection
 - filter rule [91](#), [92](#)
 - email spam
 - hits [24](#)
 - email subject [111](#)
 - event
 - high [110](#)
 - low [110](#)
 - medium [110](#)
 - event category [107](#)
 - event log
 - category [99](#)
 - event notification
 - email list [110](#)
 - Event screens [100](#)
 - exceptional case
 - add [33](#)
- ## F
- features
 - supported list [7](#)
 - File Submission Options [39](#)
 - file type
 - filter rule [92](#)
 - filename
 - filter rule [93](#)
 - filter rule
 - anti malware [91](#)
 - anti virus [91](#)
 - application category name [93](#), [96](#)
 - application name [93](#), [97](#), [99](#)
 - assign IP [101](#)
 - category name [93](#)
 - destination IP [90](#), [96](#), [99](#), [101](#)

- destination port [90, 96, 99](#)
 - DHCP [101](#)
 - DNS Filter [90, 96](#)
 - domain [94, 97](#)
 - email protection [91, 92](#)
 - file type [92](#)
 - filename [93](#)
 - hash value [92](#)
 - IDP/ADP [90](#)
 - IP Reputation [90](#)
 - query type [94, 97](#)
 - risk [93](#)
 - risk IP [93](#)
 - role type [101](#)
 - rule number [92](#)
 - sandboxing [91, 92](#)
 - scan result [92](#)
 - score level [92](#)
 - service name [101](#)
 - severity [92](#)
 - signature ID [91](#)
 - signature name [91](#)
 - source IP [90, 96, 98, 101](#)
 - source port [90, 96, 99](#)
 - threat category [93](#)
 - threat name [93](#)
 - threat type [91](#)
 - time [90, 96, 98, 101](#)
 - traffic protocol [99](#)
 - URL [92](#)
 - URL threat [90](#)
 - user login [101](#)
 - virus name [93](#)
 - web category name [94, 97](#)
 - website [94, 97](#)
 - firmware version
 - supported [7](#)
 - flow data [7](#)
 - FQDN (Fully Qualified Domain Name) [50](#)
 - Fully Anonymous user [91, 96](#)
 - Fully Qualified Domain Name (FQDN) [50](#)
- ## G
- grace period
 - expired [9](#)
 - license renewal [8](#)
- ## H
- hash value
 - filter rule [92](#)
 - Help page
 - link [16](#)
 - high event [110](#)
 - high severity [107, 109](#)
 - Hits
 - number of [37, 38](#)
- ## I
- ICMP decoder [41](#)
 - icon
 - account name [17](#)
 - Circle web site [17](#)
 - Help [16](#)
 - list of apps [16](#)
 - Marketplace [17](#)
 - More [16](#)
 - myZyxel web site [16](#)
 - NCC web site [16](#)
 - SecuReporter web site login page [17](#)
 - Setting [16](#)
 - Zyxel Biz Forum [17](#)
 - IDP
 - hits [24, 49](#)
 - IDP (Intrusion, Detection and Prevention) [24, 49](#)
 - IDP data visualization [47](#)
 - IDP profile [47](#)
 - IDP screen [49](#)
 - IDP/ADP
 - filter rule [90](#)
 - inbound traffic [99](#)
 - instant messenger (IM) [68, 99](#)
 - IP
 - destination of threat [22](#)
 - source of threat [22](#)
 - IP address
 - custom [50](#)
 - destination [101](#)
 - source [53, 57, 61](#)
 - IP Reputation
 - hits [24, 45](#)

- IP Reputation check
 - priority [43](#)
 - IP Reputation data visualization [43](#)
 - IP Reputation screen [45, 46](#)
 - IP Reputation service [43](#)
 - IPv4 address
 - reputation [43](#)
 - source [90, 96](#)
 - IPv6 address [50](#)
 - source [90, 96](#)
- ## J
- junk email
 - mark or discard [63](#)
- ## L
- layer-4 packet content [47](#)
 - layer-7 packet content [47](#)
 - license
 - SecuReporter [10](#)
 - license option [8](#)
 - license status [23](#)
 - log
 - search [83](#)
 - search privilege [88](#)
 - log out
 - Web Configurator [17](#)
 - log search privileges [84](#)
 - login attempt
 - status [101](#)
 - logs
 - save [83](#)
 - supported Zyxel Device [7](#)
 - low event [110](#)
 - low severity [107, 109](#)
- ## M
- MAC address
 - corresponding IP address [102](#)
 - Zyxel Device [101](#)
 - mail protection [63](#)
 - hits [65](#)
 - mail protection data visualization [63](#)
 - malicious file [24](#)
 - malware
 - hits [24, 61](#)
 - malware detected
 - most common [24](#)
 - management
 - data visualization [40](#)
 - management privileges
 - SecuReporter [8](#)
 - map
 - threat [21](#)
 - Marketplace [17](#)
 - medium event [110](#)
 - medium severity [107, 109](#)
 - member
 - email address [32](#)
 - Members screen [31, 32](#)
 - MX (Mail eXchange) [51](#)
 - myZyxel
 - open account [10](#)
 - myZyxel web site [16](#)
- ## N
- NCC management level [9](#)
 - NCC mode [16](#)
 - Nebula Mobile app [9](#)
 - network activity
 - by user [102](#)
 - network flooding [41](#)
 - network security
 - data visualization [40](#)
 - network session
 - length [99](#)
 - Non-Anonymous user [91, 96](#)
 - NS (Name Server) [51](#)

O

- organization
 - add a Zyxel Device [27](#)
 - create new [26](#)
 - monitor [9](#)
- Organization tab [26](#)
- OSI (Open System Interconnection) [47](#)
- OSI layer-2 [41](#)
- OSI layer-3 [41](#)
- outbound traffic [99](#)

P

- packet
 - destination [101](#)
- packet inspection signature [47](#)
- packet match a signature
 - response [90](#)
- Partially Anonymous [29](#)
- Partially Anonymous user [91, 96](#)
- PAYG
 - pay as you go [24](#)
 - pay as you go license [23](#)
- peer-to-peer (P2P) [68, 99](#)
- percentage
 - of hits from source IP address [38](#)
 - of hits to destination IP address [37](#)
- pin color
 - frequency of attacks [21](#)
- pin size
 - threat volume [21](#)
- port scanning [41](#)
- port sweeping [41](#)
- privilege
 - full administration [33](#)
 - none administrative [33](#)
 - restricted administration [33](#)
- problems [120](#)
- protocol anomaly [114](#)
- protocol anomaly detection [41](#)
- PTR (Pointer) [51](#)

Q

- query type
 - filter rule [94, 97](#)

R

- real-time traffic analytics [7](#)
- report
 - automatic removal [115](#)
 - configuration [116](#)
 - period [116](#)
 - SecuReporter [115](#)
 - title [116, 119](#)
- Report screen [115](#)
- Report Settings screen [116](#)
- RFCs – Requests for Comments [41](#)
- risk
 - filter rule [93](#)
- risk IP
 - filter rule [93](#)
- role type
 - admin [8](#)
 - agent (owner) [8](#)
 - filter rule [101](#)
 - user [8](#)
- rule number
 - filter rule [92](#)

S

- sandboxing [38](#)
 - alerts [24](#)
 - filter rule [91, 92](#)
 - turn on [39](#)
- sandboxing alerts [39](#)
- Sandboxing data visualization [61](#)
- sandboxing inspection [39](#)
 - supported file types [39](#)
- sandboxing log
 - drop [83](#)
 - remove [83](#)
- sandboxing logs
 - save criteria [83](#)

- Sandboxing screen [39, 63](#)
 - sandboxing statistics [61](#)
 - scan result [38](#)
 - filter rule [92](#)
 - score level
 - filter rule [92](#)
 - search result
 - maximum [89, 95, 98, 100](#)
 - SecuReporter
 - activate license [10](#)
 - enable [26](#)
 - set up [9](#)
 - web portal [26](#)
 - SecuReporter license
 - activate [26, 28](#)
 - SecuReporter Premium [84](#)
 - SecuReporter web site login page
 - new tab or window [17](#)
 - Security [35](#)
 - Security Cloud [40](#)
 - security event [7](#)
 - detail [109](#)
 - security indicator [24, 35, 40](#)
 - security log
 - category [88, 94](#)
 - Security screens [89](#)
 - service license
 - activate [39](#)
 - service name
 - filter rule [101](#)
 - severity
 - filter rule [92](#)
 - high [107, 109](#)
 - low [107, 109](#)
 - medium [107, 109](#)
 - signature [47](#)
 - malicious [47](#)
 - signature ID
 - filter rule [91](#)
 - signature name
 - filter rule [91](#)
 - Smart [116](#)
 - smart summaries [116](#)
 - SOA (Start Of zone Authority) [51](#)
 - source IP
 - filter rule [98, 101](#)
 - source IP address [38](#)
 - filter rule [90, 96](#)
 - source port
 - filter rule [90, 96, 99](#)
 - Standard license [8](#)
 - streaming (RSTP) application [68](#)
 - supported firmware version [7](#)
 - supported model [7](#)
- ## T
- TCP decoder [41](#)
 - threat
 - destination IP [22](#)
 - severity [107](#)
 - source country [22](#)
 - source IP [22](#)
 - target country [22](#)
 - threat category
 - filter rule [93](#)
 - Threat Intelligence [49](#)
 - threat level
 - threshold [93](#)
 - threat map
 - details [21](#)
 - threat name
 - filter rule [93](#)
 - threat type
 - filter rule [91](#)
 - time
 - filter rule [90, 96, 98, 101](#)
 - time frame
 - data collection [35](#)
 - report generation [115](#)
 - Timestamp [116](#)
 - title bar
 - NCC mode [16](#)
 - Top Signature table [49](#)
 - top users
 - with most bandwidth [24, 74](#)
 - traffic
 - anomaly [114](#)
 - inbound [99](#)
 - outbound [99](#)
 - traffic anomaly policy [41](#)

traffic log
 categories [97](#)
traffic protocol
 filter rule [99](#)
Traffic screen [98](#)
transport packet
 type [99](#)
Trial license [8](#)
troubleshooting [120](#)

U

UDP decoder [41](#)
unclaimed Zyxel Device [27](#)
URL
 filter rule [92](#)
URL (Uniform Resource Locator) [90](#)
URL threat [93](#)
 hits [24](#)
URL threat check
 priority [55](#)
URL threat domain name [55](#)
URL threat filter [65](#)
 hits [57](#)
URL Threat Filter data visualization [55](#)
URL Threat Filter screen [35, 57](#)
URL Threat filtering [24](#)
URL threat IP address [55](#)
user login
 filter rule [101](#)

V

version number
 SecuReporter [2](#)
virtual machine (VM) [38](#)
virus
 hits [24, 61](#)
virus name
 filter rule [93](#)
viruses detected
 most common [24](#)
Voice over IP (VoIP) [68, 99](#)

W

warranty [129](#)
 note [129](#)
web category name
 filter rule [94, 97](#)
Web Page Blocked! page [50](#)
website
 filter rule [94, 97](#)
Website screen [67](#)

Z

Zyxel Biz Forum [17](#)
Zyxel Device
 add to an organization [26](#)
 register [26](#)
 register at [10](#)
 supported [7](#)
Zyxel Device cache [38](#)