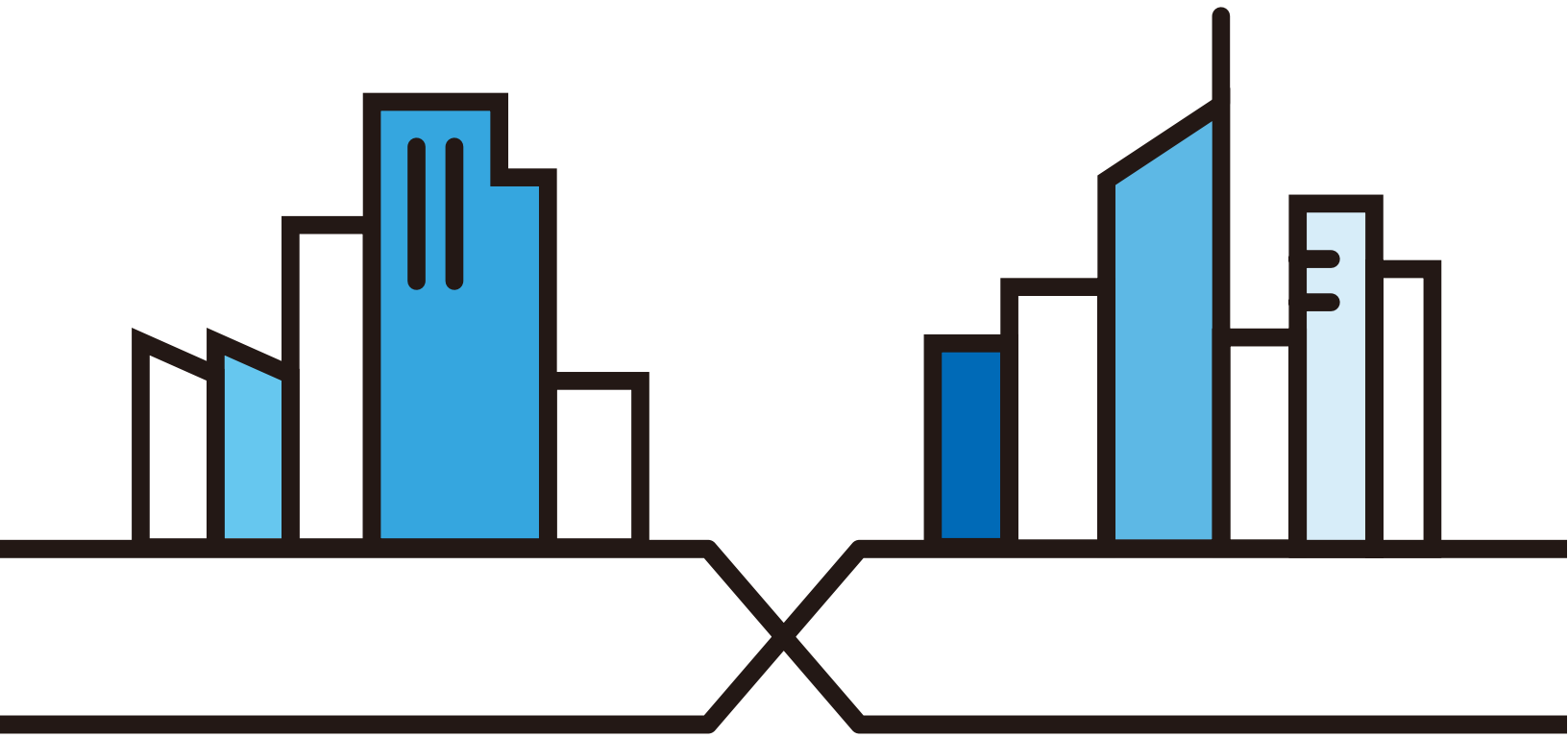
ZYXEL

User's Guide

SecuReporter

Default Login Details	
Login URL	https://secureporter.cloudcnm.zyxel.com
User Name	myZyxel.com User Name
Password	myZyxel.com Password

Version 2.5 Edition 1, 03/2021



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 download library of the Zyxel website to get a myZyxel.com User's Guide to see how to register your Zyxel Device and activate a license.

- More Information

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

Document Conventions

Warnings and Notes

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

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

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

Syntax Conventions

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

Table of Contents

CHAPTER 1
Introduction

1.1 Overview

SecuReporter is a cloud-based analytics tool that is part of the Cloud CNM suite developed by Zyxel. It aggregates logs of supported Zyxel Device across distributed locations, giving network administrators a centralized view of security events and flow data.

SecuReporter can collect data from different types of Zyxel Device models, including the Zyxel Security Gateway/AP/Switch series, with up to 40,000 units supported simultaneously.

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 Version

SUPPORTED VERSION	SUPPORTED MODELS
Version 4.32 and above	USG20
	USG20W-VPN
	USG40
	USG40W
	USG60
	USG60W
	USG110
	USG210
	ZyWALL110
	ATP200
	ATP500
	ATP800
Version 4.33 and above	USG310
	USG1100
	USG1900
	USG2200
	ZyWALL310
	ZyWALL1100
Version 4.35 and above	ATP100

Table 1 Supported Zyxel Devices and Firmware Version (continued)

SUPPORTED VERSION	SUPPORTED MODELS
Version 4.50 and above	USG FLEX 100
	USG FLEX 200
	USG FLEX 500
Version 4.60 and above	USG FLEX 100W
	USG FLEX 700

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

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 ZyWALL VPN series, ZyWALL USG series, ZyWALL ATP series and ZyWALL USG FLEX series at the time of writing.

Table 2 Features Supported on the Zyxel Devices

	ZYWALL VPN SERIES	USG SERIES	ATP SERIES	USG FLEX SERIES
Anti Virus / Anti Malware	Yes	Yes	Yes	Yes
IDP	Yes	Yes	Yes	Yes
ADP	Yes	Yes	Yes	Yes
Mail Protection	Yes	Yes	Yes	Yes
Web Security	Yes	Yes	Yes	Yes
Application Patrol	Yes	Yes	Yes	Yes
Sandboxing Statistics	No	No	Yes	No
URL Threat Filter	No	No	Yes	Yes
IP Reputation	No	No	Yes	No
DNS Filter	No	No	Yes	No

1.1.2 SecuReporter Management Privileges

A Zyxel Device owner can register a Zyxel Device at myZyxel. 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 TYPE	SIGN IN AT MYZYXEL?	PRIVILEGES
Agent (Owner)	Yes	• Can add/delete Zyxel Devices to/from an organization • Can add/edit organizations • Can add/edit admin/user accounts • Can configure alert notifications • Can configure dashboard widgets • Can configure analyses and reports • Can create request for transfer of analytics and logs • Can import analytics and logs • Can create log download request and download archived logs
Admin	Yes	• Can add/edit organizations • Can configure alert notifications • Can configure dashboard widgets • Can configure analyses and reports • Can import analytics and logs • Can download archived logs
User	Yes	• Can configure dashboard widgets • Can view analyses and report • Can configure alert notifications • Can import analytics and logs

1.1.3 License Options

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

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

1.2 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:

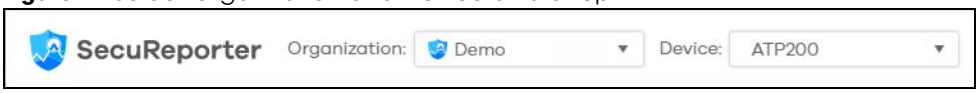
- You must enable SecuReporter on a supported Zyxel Device. Refer to the User's Guide of the supported Zyxel Device for instructions.
- Register the Zyxel Devices using the same myZyxel account. To open an account at myZyxel, go to https://portal.myzyxel.com and click **Sign Up**.
- After you register the Zyxel Devices, follow the on-screen instructions to activate the SecuReporter license for the registered Zyxel Devices.

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

Note: See Section 6.1 on page 70 for an overview of how to get started using SecuReporter.

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

Figure 1 Select Organization and Device on Startup



1.3 Title Bar

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

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

Table 4 NCC management Levels

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

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.

Figure 2 Title Bar

The icons provide the following functions.

Table 5 Title Bar: Web Configurator Icons

LABEL	DESCRIPTION
	Click this to open the help page for the current screen or go to the Forum.
	Click this to set up the following: • Organization & Device – you see all organizations that you have already created and the Zyxel Devices (Model, Device and License Status). • Members – to assign an administrator or user for organizations or Zyxel Devices within organizations that you created.
	Click this to turn on or off SecuReporter's Dark Mode display. Note: This feature is not available at the time of writing of this User's Guide.
	Click this to show a list of apps provided by Zyxel available at the time of writing.

Table 5 Title Bar: Web Configurator Icons (continued)

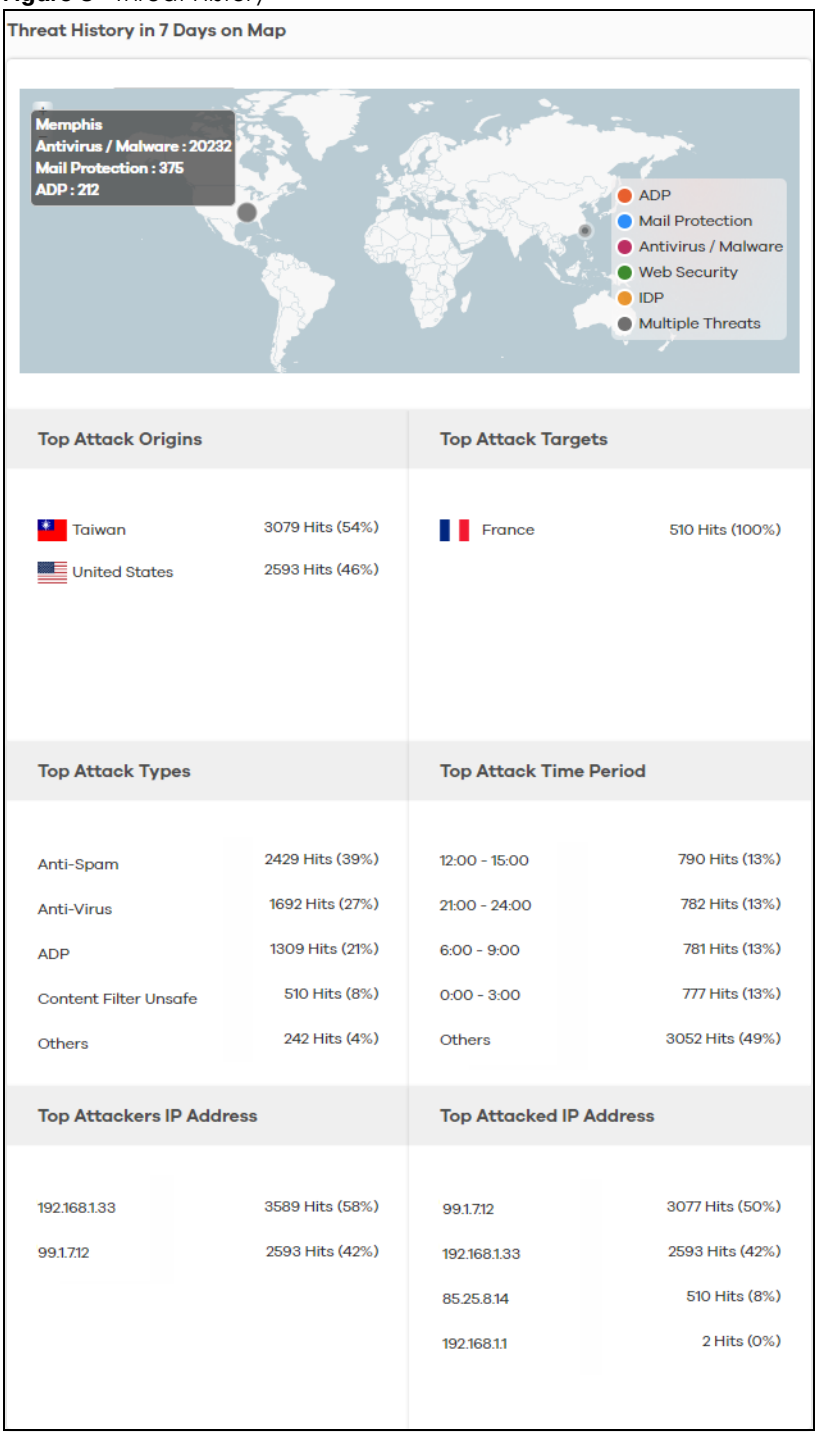
LABEL	DESCRIPTION
myZyxel	Click this to open the myZyxel web site login page in a new tab or window.
Nebula	Click this to open the NCC web site login page in a new tab or window.
SecuReporter	Click this to open the SecuReporter web site login page in a new tab or window.
CNC	Click this to open the CNC web site login page in a new tab or window.
Circle	Click this to open the Circle web site login page in a new tab or window.
Marketplace	Click this to open the myZyxel web site login page in a new tab or window. You will be redirected to the Marketplace after you log in.
Forum	Click this to go to Zyxel Biz Forum, where you can get the latest Zyxel Device information and have conversations with other people by posting your messages.
H	Click this to view your account name, manage your account information (edit Profile, change Password, set up Two-Factor Authentication), or to log out.

1.4 Threat History

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

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

Figure 3 Threat History



1.4.1 Details

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

The following table describes the labels on this screen.

Table 6 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, IDP, Malware (Anti Virus), spam, content filter, and mixed.
Hits	This displays the number of times a single threat was sent from a site and blocked by the Zyxel Device. Click the arrow to arrange the threats by the number of hits.
Top Attack Origins	This displays the percentage of the threat's source country.
Top Attack Targets	This displays the percentage of the threat's destination country.
Top Attack Types	This displays the percentage of the type of attack.
Top Attack Time Period	This displays the percentage of the 3-hour time frame when the attacks occur.
Top Attackers IP Address	This displays each threat's source IP.
Top Attacked IP Address	This displays each threat's destination IP.

1.5 Dashboard

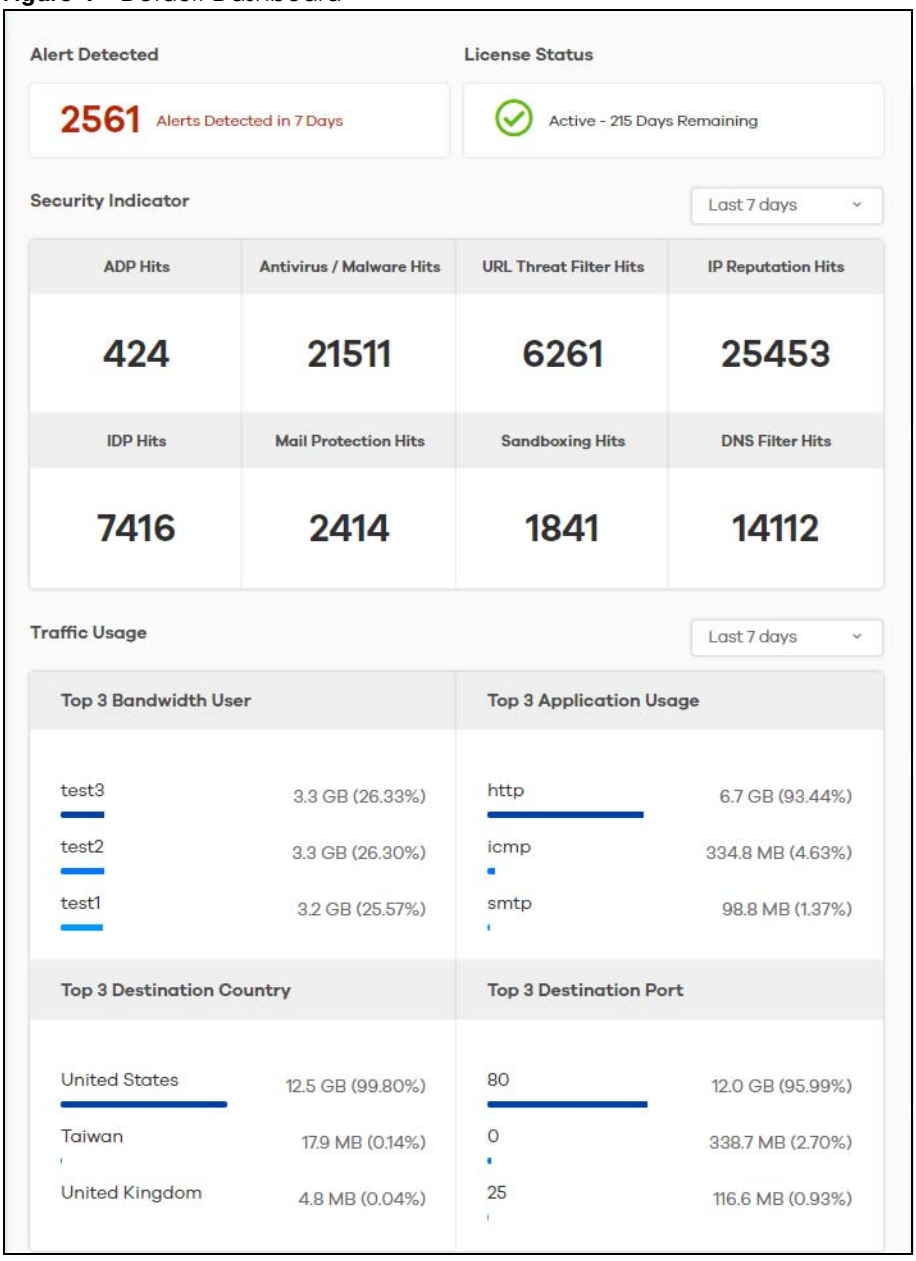
The **Dashboard** shows the key facts about your network's security environment that were collected by SecuReporter in the last 30 days, 7 days, 24 hours, one hour, or custom range.

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

By default, the dashboard will have the **Alert Detected**, **License Status**, **Security Indicator**, and **Traffic Usage** widgets. See Section 2.1.2 on page 18 and Section 2.1.3 on page 20 for more information about sandboxing.

Widgets are miniature views of SecuReporter's data visualizations, the full versions of which are available under the **Security Indicator** and **Application / Website** screens.

Figure 4 Default Dashboard



The following table describes the widgets on the default dashboard:

Table 7 Default Dashboard

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

Table 7 Default Dashboard (continued)

LABEL	DESCRIPTION
	Select the time frame to show your network's security environment collected by SecuReporter. • Last hour • Last 24 hours • Last 7 days • Last 30 days (for SecuReporter Premium only) • Custom Range (last 30 days custom range for SecuReporter Premium only) – 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.
IDP Hits	This displays the total number of malicious or suspicious packets detected by IDP in the Zyxel Devices. IDP (Intrusion, Detection and Prevention) uses signatures to detect malicious or suspicious packets to protect against network-based intrusions.
Mail Protection Hits	This displays the total number of the most common traffic classified as spam received by the Zyxel Devices.
Sandboxing Alerts	This displays the total number of files that have been scanned through the sandboxing function.
DNS Filter Hits	This displays the total number of URLs of FQDNs classified as a security threat to network devices behind the Zyxel Device.
Traffic Usage	
	Select the time frame to show your network traffic collected by SecuReporter. • Last hour • Last 24 hours • Last 7 days • Custom Range – click an allowed start and end day, select the time frame, and then click **Apply**.
Top 3 Bandwidth User	This displays the top three users of bandwidth on the network including percentage over a selected time frame, which is 7 days by default.
Top 3 Application Usage	This displays the network applications with the greatest bandwidth usage including percentage over a selected time frame, which is 7 days by default.
Top 3 Destination Country	This displays the top three countries that received the most data traffic from Zyxel Devices including percentage, over a selected time frame.
Top 3 Destination Port	This displays the top three destination ports by bandwidth usage including percentage, over a specified time frame, which is 7 days by default.

CHAPTER 2
Analysis

2.1 Overview

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

2.1.1 Tutorial

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

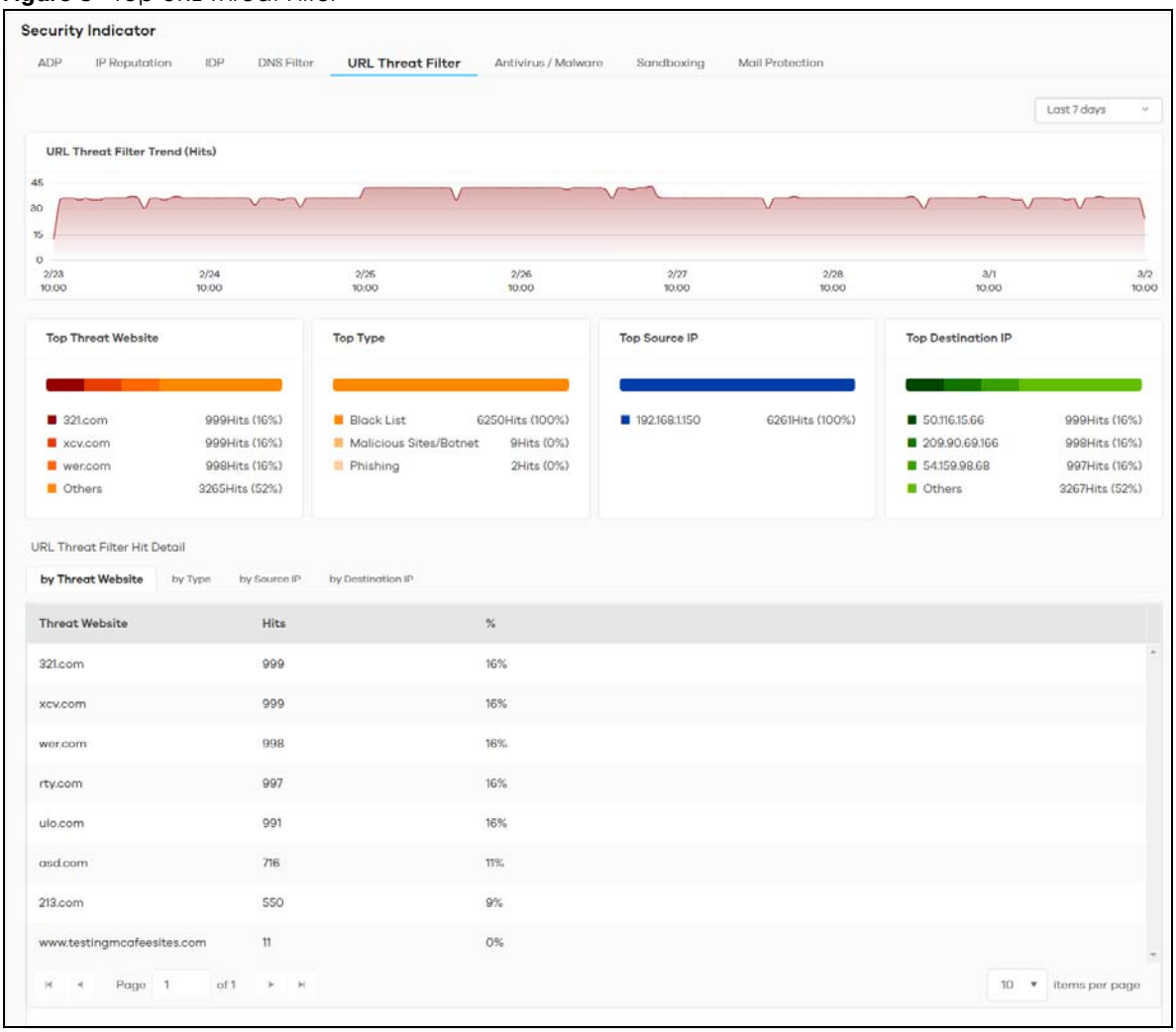
In most cases, you can choose to analyze data collected over one of five time frames (see Section 1.5 on page 12):

- Last hour
- Last 24 hours
- Last 7 days
- Last 30 days (for SecuReporter Premium only)
- Custom Range (last 30 days custom range for SecuReporter Premium only) – click an allowed start and end day, select the time frame, and then click **Apply**.

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

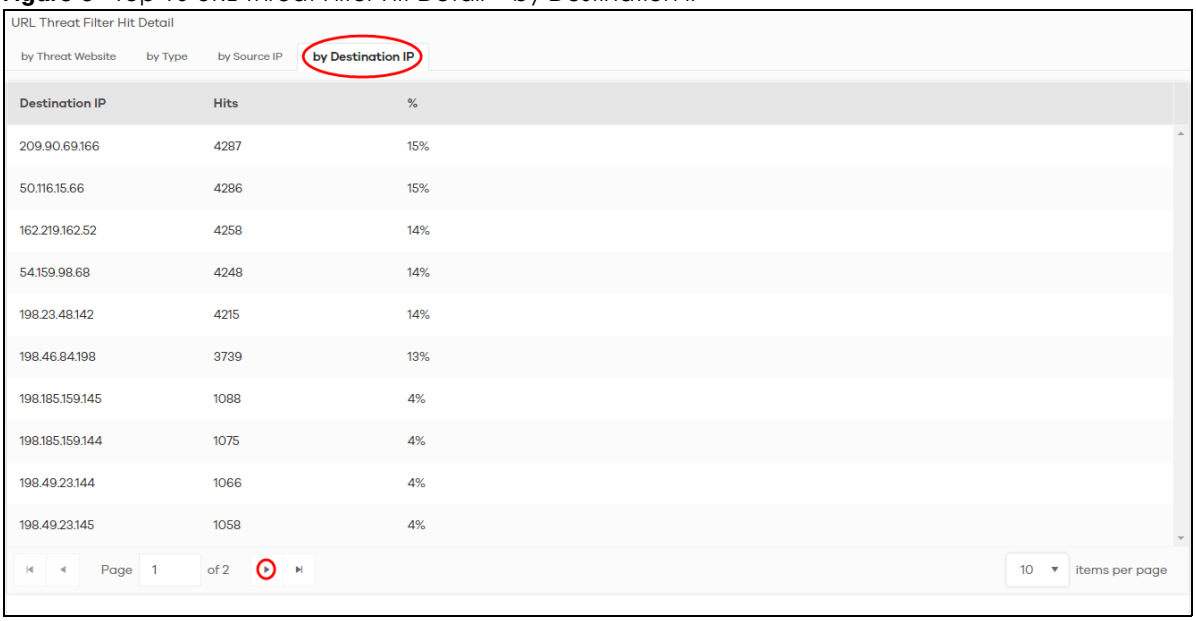
1 Click **Analysis** > **Security Indicator** > **URL Threat Filter**.

Figure 5 Top URL Threat Filter



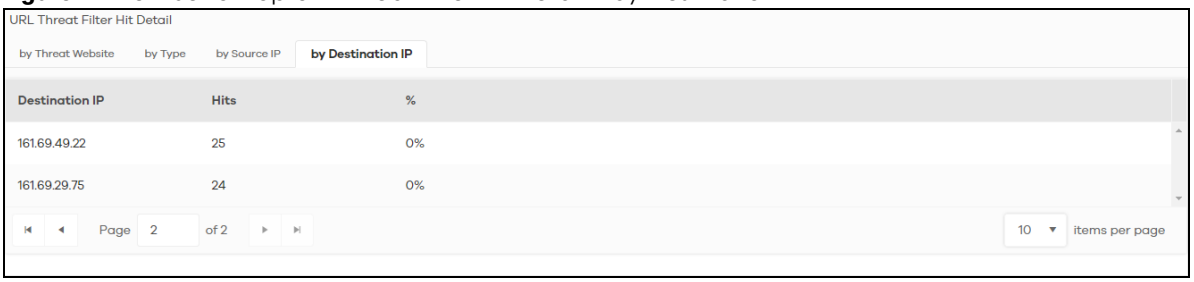
2 Click the **by Destination IP** tab. To display the next set of malware or viruses, click the arrow on the lower left of the screen.

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



The following screen appears.

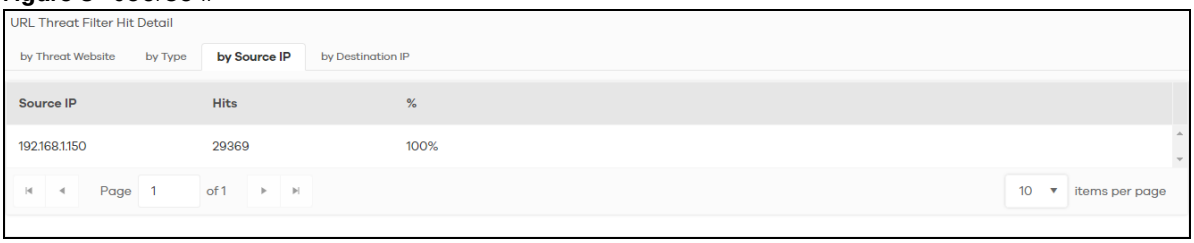
Figure 7 Next Set of Top URL Threat Filter Hit Detail > by Destination IP



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

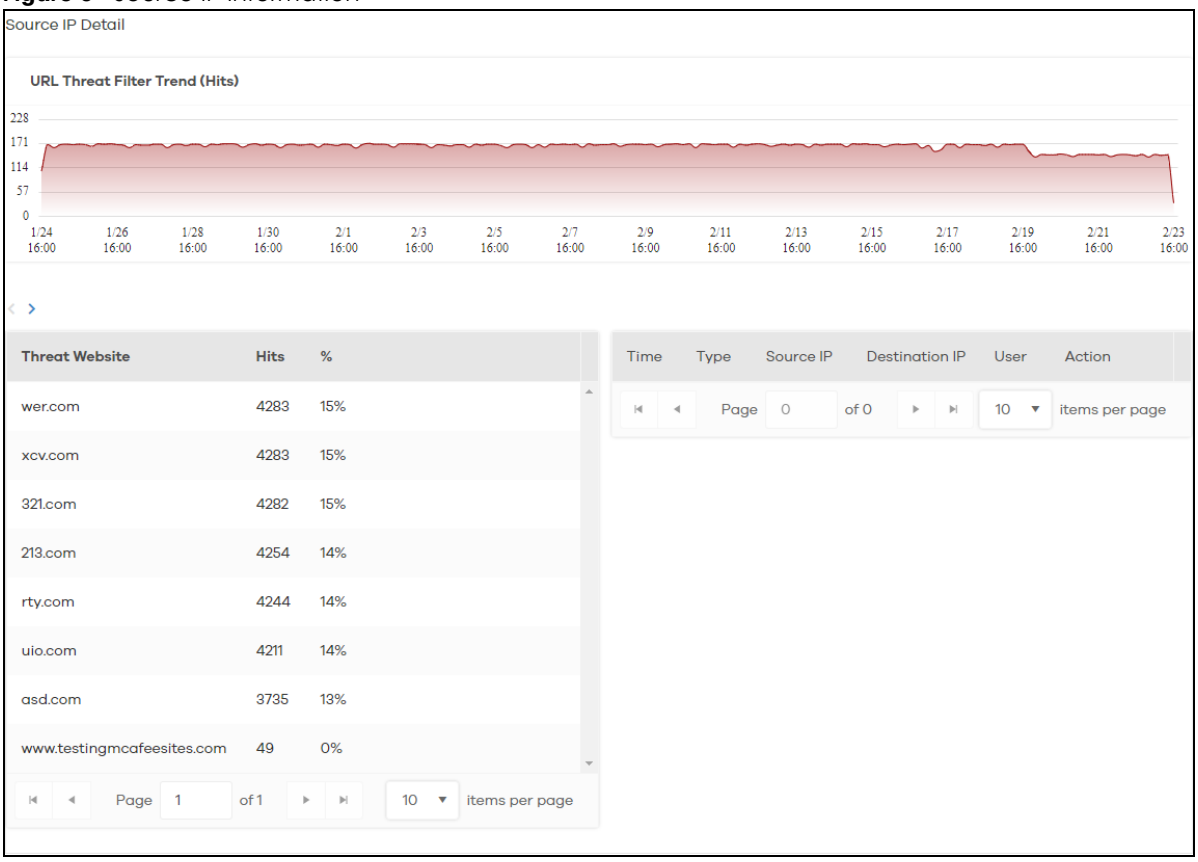
Note: You could select different metrics by clicking a tab to view the information of the selected metric.

Figure 8 Source IP



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

Figure 9 Source IP Information



2.1.2 Sandboxing

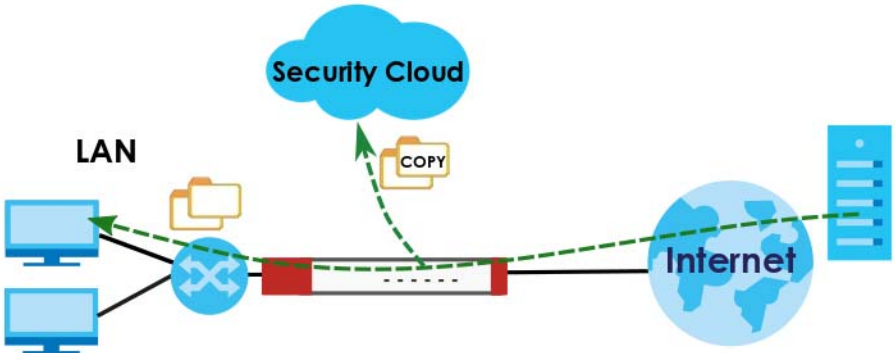
Zyxel cloud sandboxing is a security mechanism which provides a safe environment to separate running programs from your network and host devices. Unknown or untrusted programs or codes are uploaded to a cloud server and executed within an isolated virtual machine (VM) to monitor and analyze the zero-day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

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

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

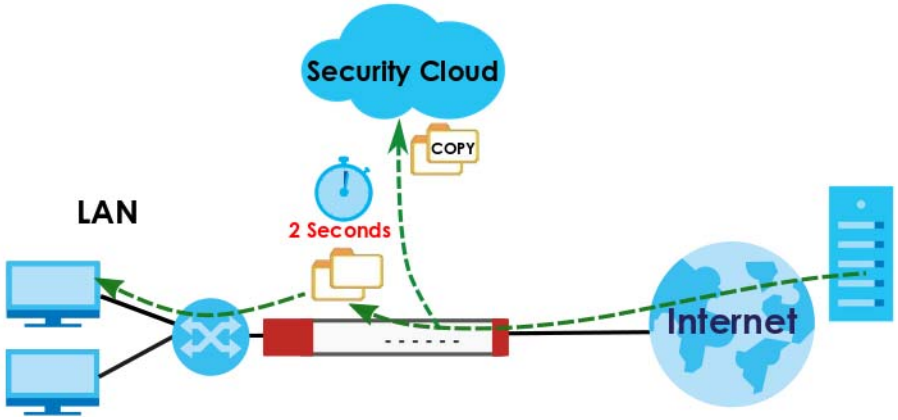
Note: The scan result is removed from the Zyxel Device cache after the Zyxel Device restarts, so all files are once again 'unknown'.

Figure 10 General Zyxel Sandbox Inspection



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

Figure 11 Advanced Zyxel Sandbox Inspection



Supported File Types for Sandboxing Inspection

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

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

Note: Configure this setting on your Zyxel Device.

Turning on Sandboxing on Your Zyxel Device

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

2.1.3 Sandboxing Alerts

SecuReporter sends sandboxing alerts to Zyxel Device administrators when:

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

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

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

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

2.2 Analysis Overview

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

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

Table 8 Analysis Overview

LABEL	TYPE	DESCRIPTION
Security Indicator	ADP	ADP Trend (Hits)
		Top Signature Type
		Top Event Severity Type
		Top Source IP
		Top Destination IP
	IP Reputation	IP Reputation Trend (Hits)
		Top Risk IP
		Top Type
		Top Source IP
		Top Destination IP
	IDP	IDP Trend (Hits)
		Top Signature Type
		Top Event Severity Type
		Top Source IP
		Top Destination IP
	DNS Filter	DNS Filter Trend (Hits)
		Top DNS Filter Domain
		Top Threat Category
		Top Source IP
		Top Query Type

Table 8 Analysis Overview (continued)

LABEL	TYPE	DESCRIPTION
Security Indicator	URL Threat Filter	URL Threat Filter Trend (Hits)
		Top Threat Website
		Top Type
		Top Source IP
		Top Destination IP
	Antivirus / Malware	Antivirus / Malware Trend (Hits)
		Top Virus / Malware
		Top Source IP
		Top Destination IP
	Sandboxing	Sandboxing Trend (Hits)
		Top File Type
		Top File Name
		Top File Hash
		Top User
		Top Source IP
		Top Destination IP
	Mail Protection	Mail Protection Trend (Hits)
		Top Spam Email Subject
		Top Spam Sender Email
		Top Spam Received IP
		Top Spam Sender IP
Application / Website	Web Security	Blocked Website Access Trend (Hits)
		Allowed Website Access Trend (Hits)
		Top Accessed Blocked Website
		Top Accessed Blocked Website Type
		Top Accessed Allowed Website
		Top Accessed Allowed Website Type
		Top Source IP (to Blocked Website)
		Top Destination IP (to Blocked Website)
		Top Source IP (to Allowed Website)
		Top Destination IP (to Allowed Website)
	App Patrol	Blocked Application Access Trend (Hits)
		Allowed Application Access Trend (Hits)
		Top Accessed Blocked Application
		Top Accessed Blocked Application Type
		Top Accessed Allowed Application
		Top Accessed Allowed Application Type

2.3 Security Indicators

Security Indicators data visualizations are categorized as:

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

2.3.1 ADP

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

Traffic Anomalies

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

Protocol Anomalies

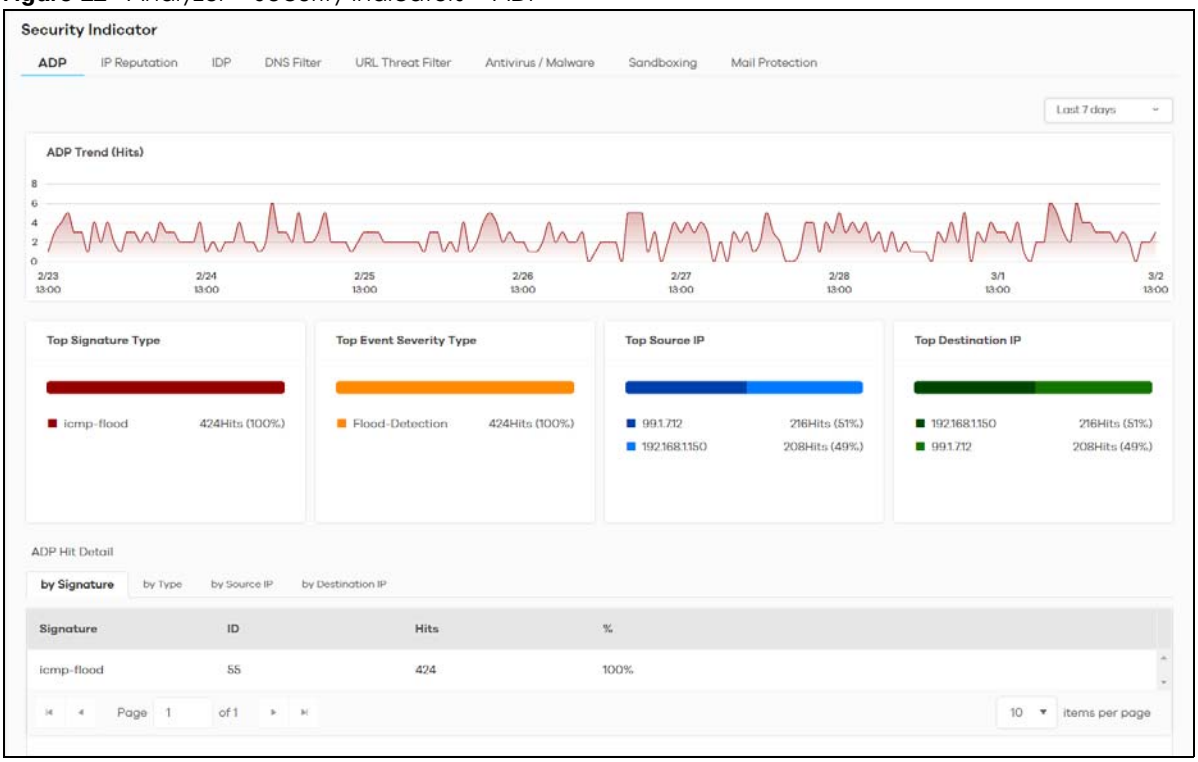
Protocol anomalies are packets that do not comply with the relevant RFC (Request For Comments). Protocol anomaly detection includes:

- TCP Decoder
- UDP Decoder
- ICMP Decoder

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

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

Figure 12 Analyzer > Security Indicators > ADP



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

Table 9 Analysis > Security Indicator > ADP

LABEL	DESCRIPTION
ADP Trend (Hits)	This chart displays patterns in 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. Move your cursor over a trend line to display the number of threats encountered over time.
Top Signature Type	This chart displays the top 3 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 Event Severity Type	This chart displays the top 3 anomaly severity 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 source IP addresses of the top 3 incoming anomalies. 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 destination IP addresses of the top 3 incoming anomalies. Scroll down to **ADP Hit Detail** and click the **by Destination IP** tab to display details about the anomalies that were detected.

2.3.2 IP Reputation

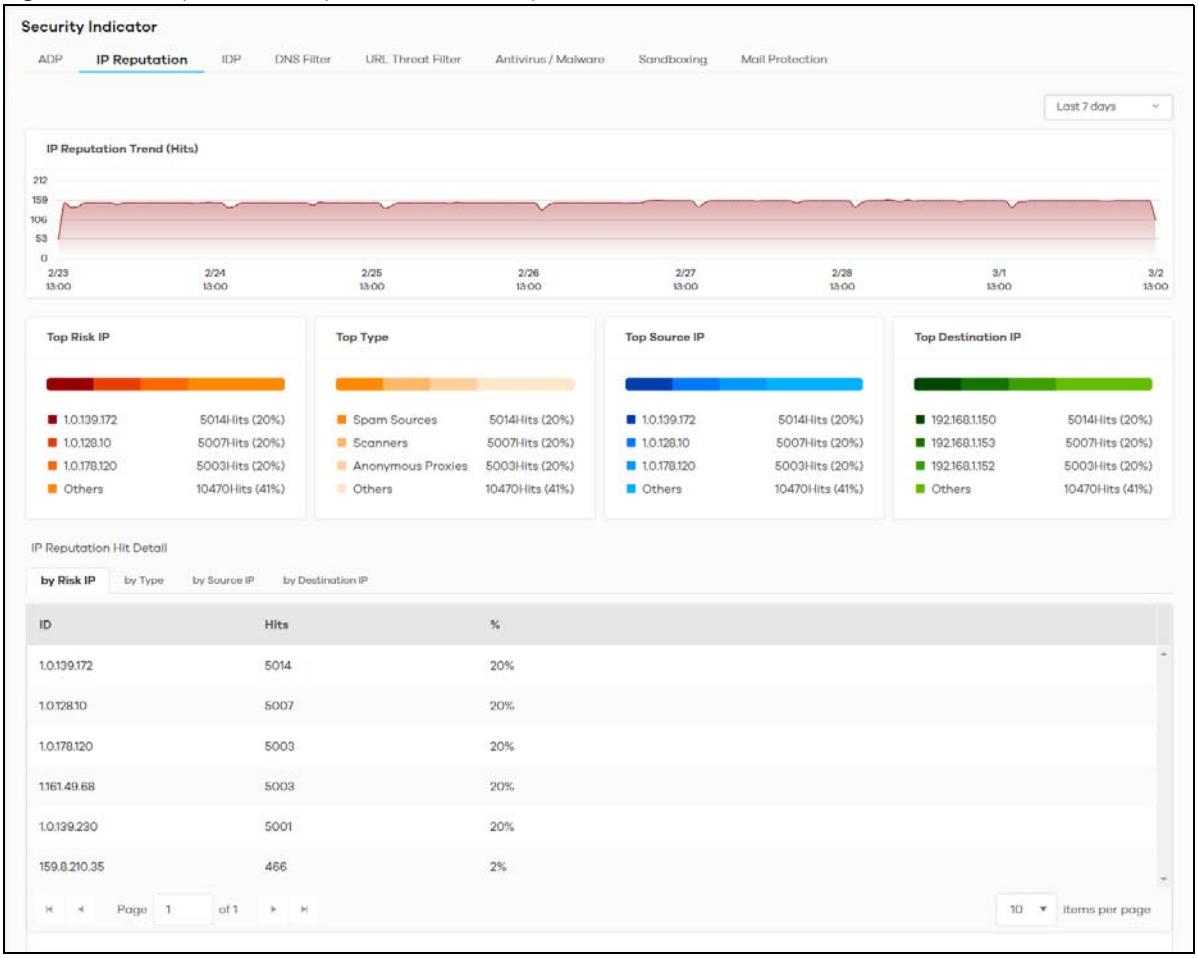
When you register for and enable the IP reputation service, your Zyxel Device downloads signature files that identifies reputation of IPv4 addresses. You can have the Zyxel Device forward, block, and/or log packets from IPv4 addresses based on these signatures and categories.

The priority for IP Reputation checking is as below:

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

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

Figure 13 Analysis > Security Indicator > IP Reputation



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

Table 10 Analysis > Security Indicator > IP Reputation

LABEL	DESCRIPTION
IP Reputation Trend (Hits)	This chart displays the number of threats posed by IPs as detected by the Zyxel Devices. Move your cursor over a trend line to display the number of threats encountered over time.
Top Risk IP	This chart displays the top 3 IP addresses detected by the Zyxel Device as detected by IP Reputation. 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 top 3 types of 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 ATP User's Guides.
Top Source IP	This chart displays the source IP addresses of the top 3 IP addresses detected by the Zyxel Device as detected by IP 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 destination IP addresses of the top 3 IP addresses detected by the Zyxel Device as detected by IP 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.

2.3.3 IDP

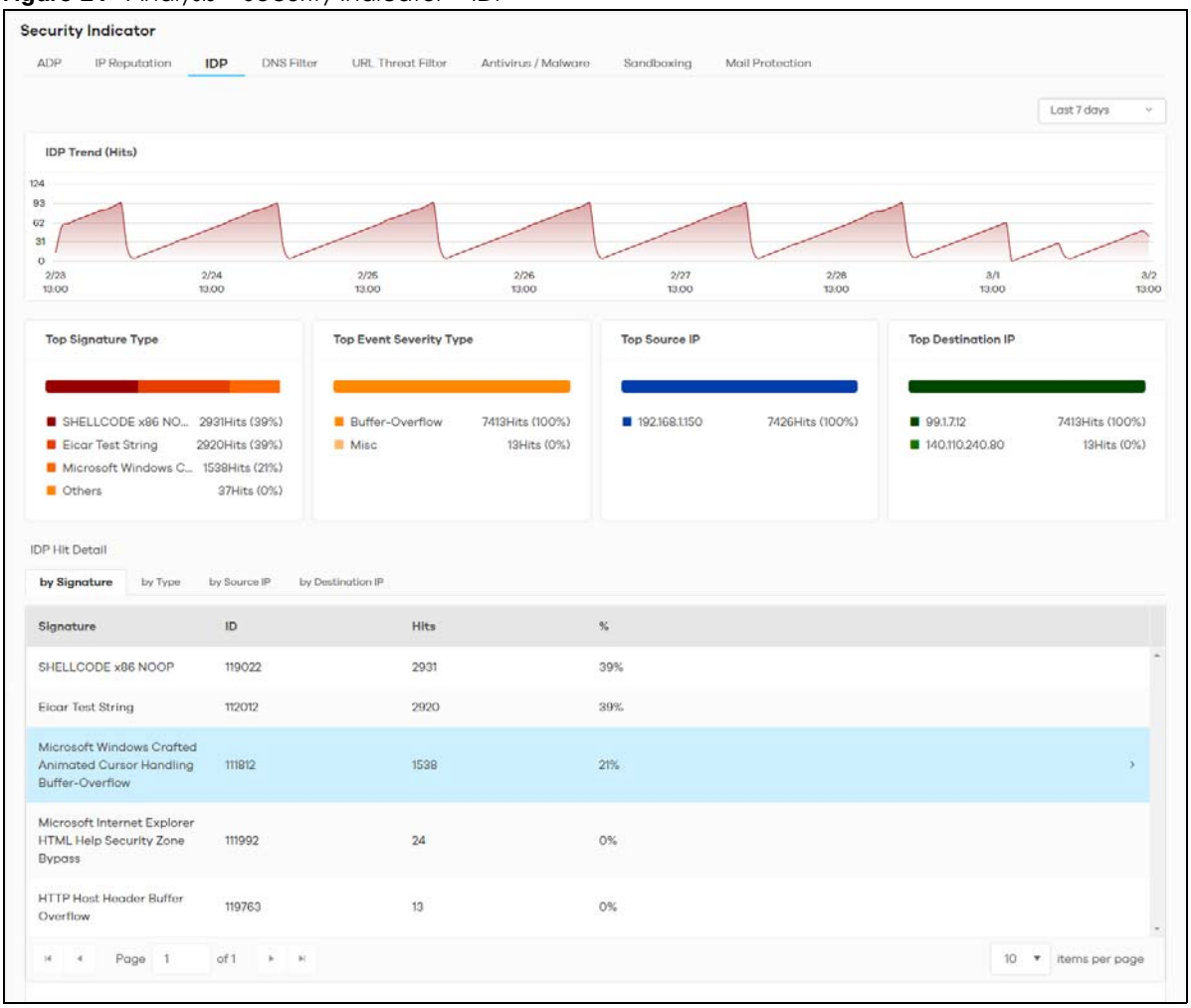
An IDP profile is a set of packet inspection signatures.

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 IDP 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** > **IDP** data visualizations.

Figure 14 Analysis > Security Indicator > IDP



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

Table 11 Analysis > Security Indicator > IDP

LABEL	DESCRIPTION
IDP Trend (Hits)	This chart displays malicious or suspicious packets detected by IDP in the Zyxel Devices. IDP (Intrusion, Detection and Prevention) 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 Signature Type	This chart displays the top 3 malicious or suspicious packets detected by IDP in the Zyxel Devices. Scroll down to **IDP Hit Detail** and click the **by Signature** tab to display details about the intrusions that were detected.
Top Event Severity Type	This chart displays the top 3 malicious or suspicious packet types detected by IDP in the Zyxel Devices. Scroll down to **IDP Hit Detail** and click the **by Type** tab to display details about the intrusions that were detected.

Table 11 Analysis > Security Indicator > IDP (continued)

LABEL	DESCRIPTION
Top Source IP	This chart displays the source IP addresses of the top 3 incoming malicious or suspicious packets detected by IDP in the Zyxel Devices. Scroll down to **IDP 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 3 incoming malicious or suspicious packets detected by IDP in the Zyxel Devices. Scroll down to **IDP Hit Detail** and click the **by Destination IP** tab to display details about the destination IP addresses of the incoming malicious or suspicious packets.

2.3.3.1 Threat Intelligence

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

Figure 15 Top Signature Details

2.3.4 DNS Filter

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

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

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

The Zyxel Device DNS 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:

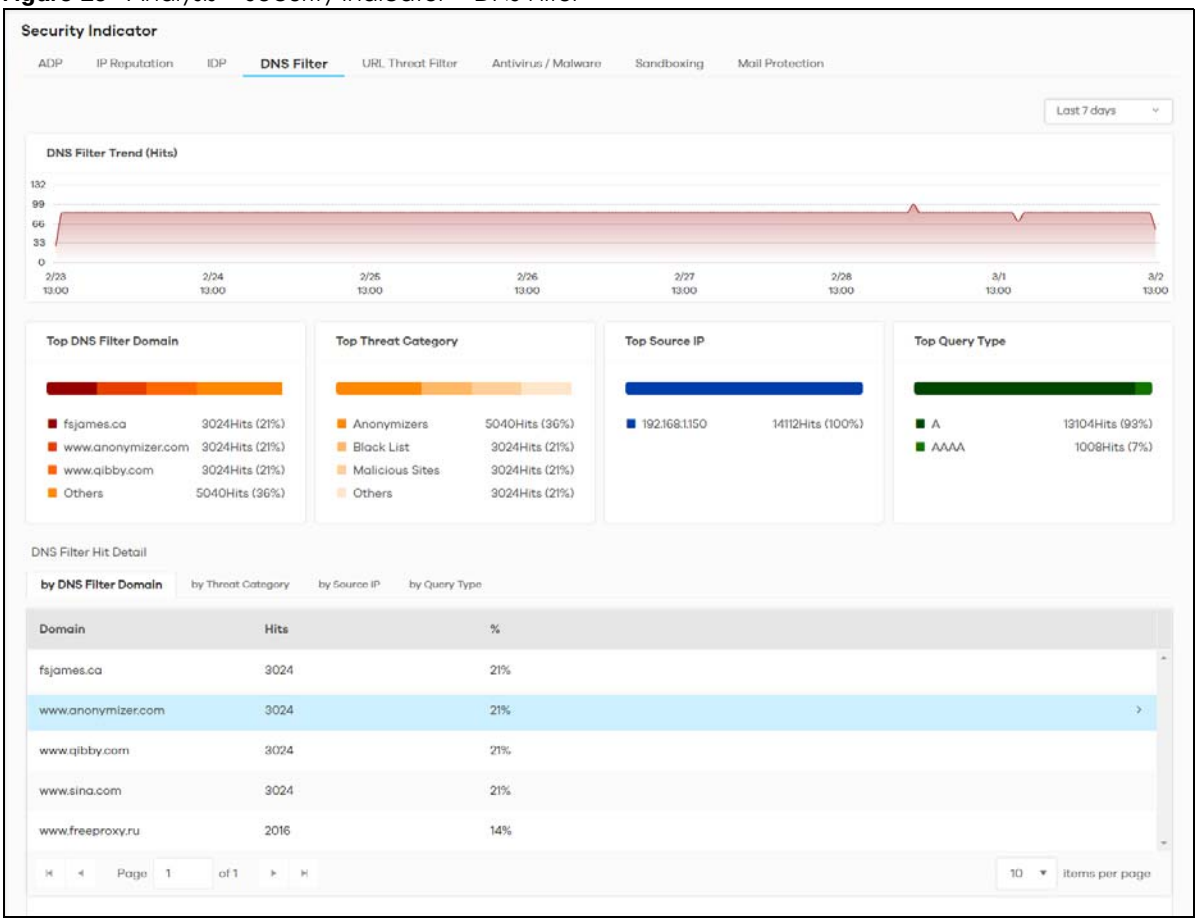
- Type "A" for IPv4 addresses

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 Filter** to display the configuration screen as shown next.

Figure 16 Analysis > Security Indicator > DNS Filter



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

Table 12 Analysis > Security Indicator > DNS Filter

LABEL	DESCRIPTION
DNS 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 DNS Filter Domain	This chart displays the 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 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 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 types of DNS (Domain Name System) record of the security threat to network devices behind the Zyxel Device. Scroll down to **DNS Filter Hit Detail** and click the **by Query Type** tab to display details about the DNS (Domain Name System) record type.

2.3.5 URL Threat Filter

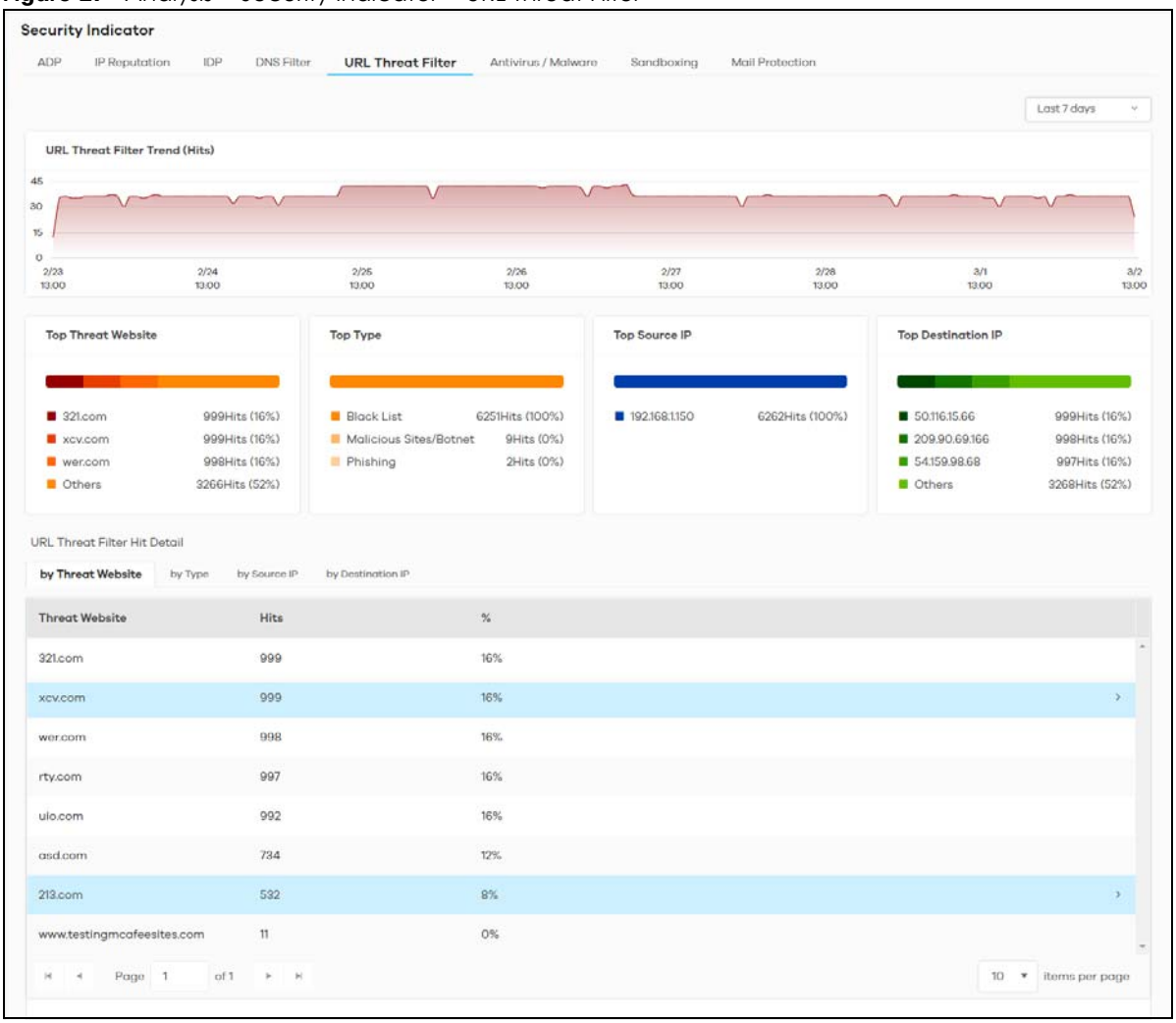
When you enable the URL Threat filtering service, your Zyxel Device downloads signature files that contain known URL Threat domain names and IP addresses. The Zyxel Device will also access an external database that has millions of web sites categorized based on content. You can have the Zyxel Device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

The priority for URL Threat checking is as below:

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

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

Figure 17 Analysis > Security Indicator > URL Threat Filter



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

Table 13 Analysis > Security Indicator > URL Threat Filter

LABEL	DESCRIPTION
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 Threat Website	This chart displays the top 3 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 3 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 ATP User's Guides.

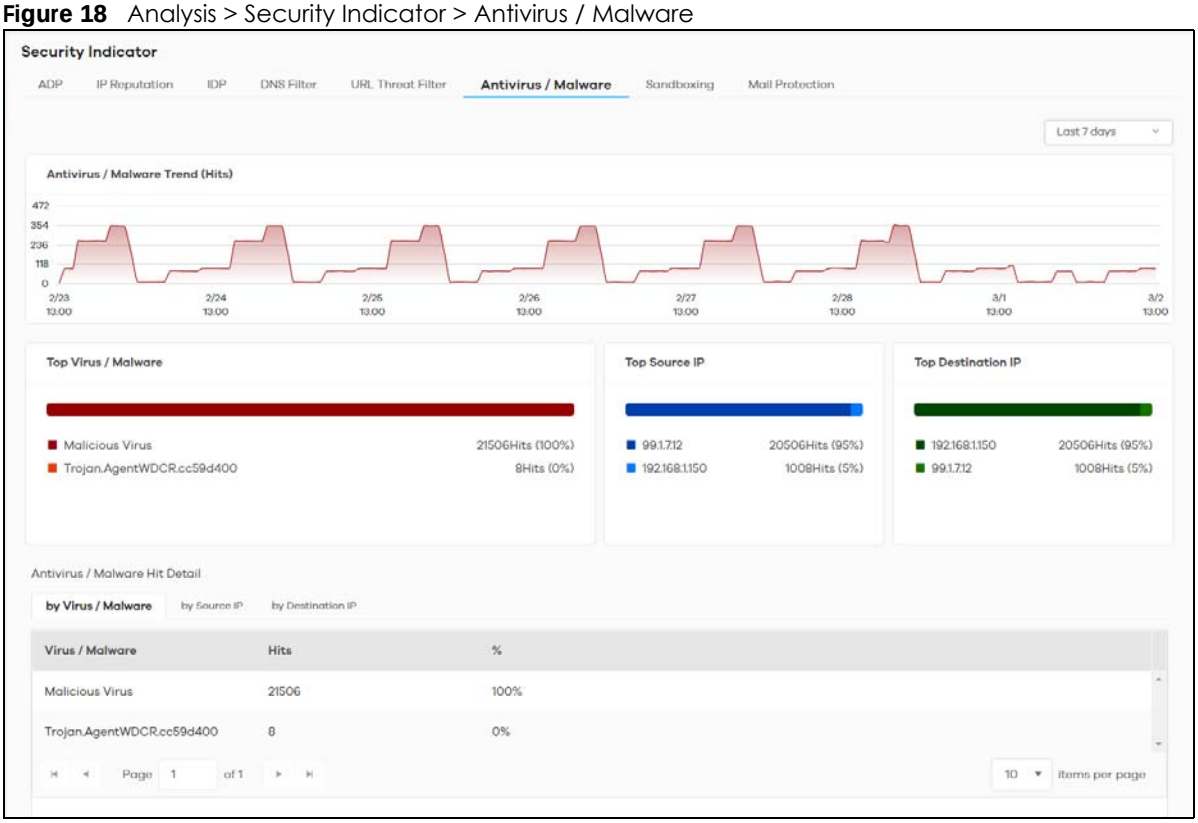
Table 13 Analysis > Security Indicator > URL Threat Filter (continued)

LABEL	DESCRIPTION
Top Source IP	This chart displays the source IP addresses of the top 3 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 top 3 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.

2.3.6 Antivirus / Malware

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

Figure 18 Analysis > Security Indicator > Antivirus / Malware



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

Table 14 Analysis > Security Indicator > Antivirus / Malware

LABEL	DESCRIPTION
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 Virus / Malware	This chart displays the top 3 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 top 3 incoming malicious and/or suspicious files. 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 top 3 incoming malicious and/or suspicious files. 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.

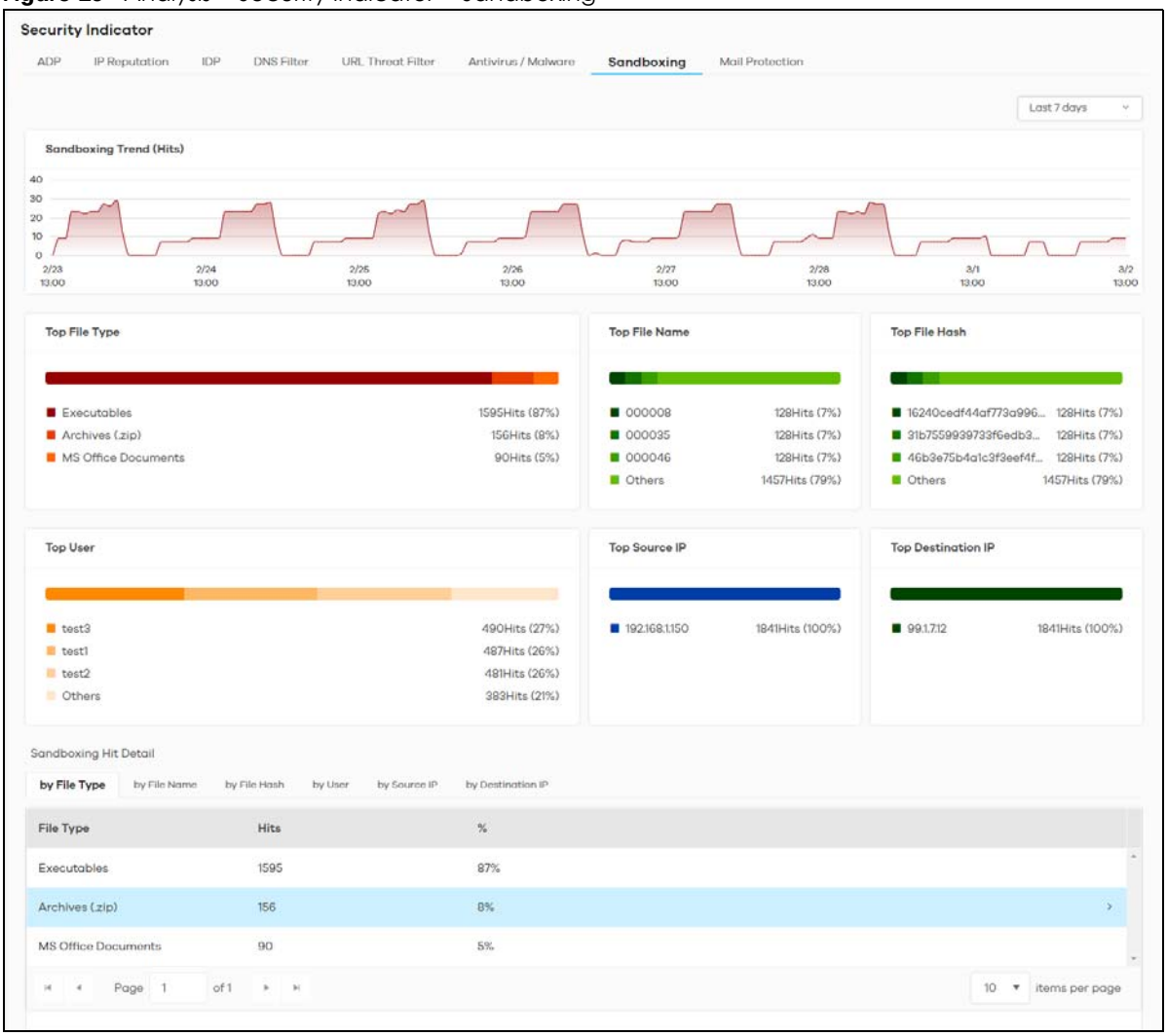
2.3.7 Sandboxing

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

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

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

Figure 19 Analysis > Security Indicator > Sandboxing



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

Table 15 Analysis > Security Indicator > Sandboxing

LABEL	DESCRIPTION
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 top 3 types of the 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 top 3 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.

Table 15 Analysis > Security Indicator > Sandboxing (continued)

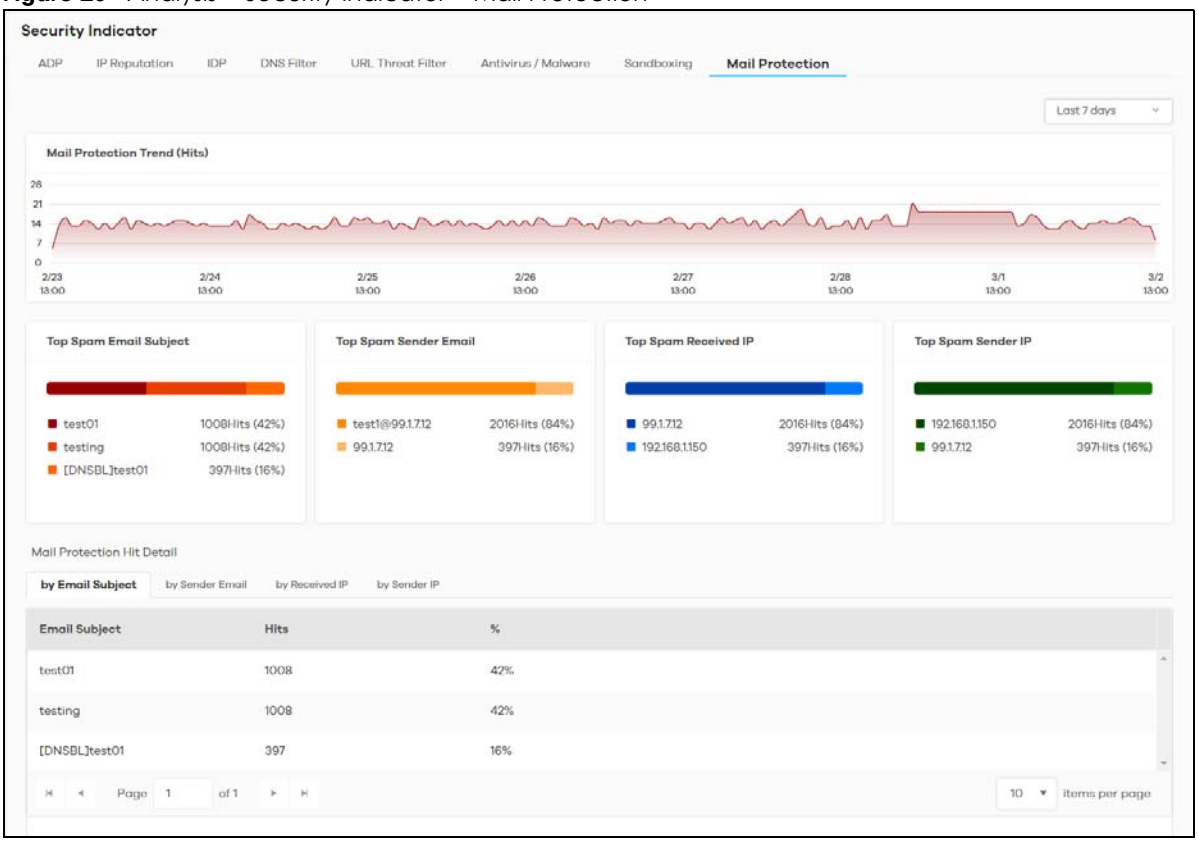
LABEL	DESCRIPTION
Top File Hash	This chart displays the hash values of the top 3 incoming malicious and/or suspicious files. Scroll down to **Sandboxing Hit Detail** and click the **by File Hash** tab to display details about the hash values of the incoming malicious and/or suspicious files.
Top User	This table displays the top 3 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 table displays the source IP addresses of the top 3 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 table displays the destination IP addresses of the top 3 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.

2.3.8 Mail Protection

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

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

Figure 20 Analysis > Security Indicator > Mail Protection



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

Table 16 Analysis > Security Indicator > Mail Protection

LABEL	DESCRIPTION
Mail Protection Trend (Hits)	This chart displays the number of spam mails detected by the Zyxel Devices. Move your cursor over a trend line to display the number of threats encountered over time.
Top Spam Email Subject	This chart displays the top 3 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 top 3 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 top 3 traffic classified as spam received by the internal users of the Zyxel Devices. 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 top 3 traffic classified as spam sent from the internal users of the Zyxel Devices. 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.

2.4 Application / Website

The following figure shows the **Analysis** > **Application / Website** data visualizations.

Application / Website 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 / Website 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.

Application Profiles and Policies

An Application / Website profile is a group of categories of application patrol signatures. For each profile, you can specify the default action the Zyxel Device takes once a packet matches a signature (forward, drop, or reject a service's connections and/or create a log alert).

Classification of Applications

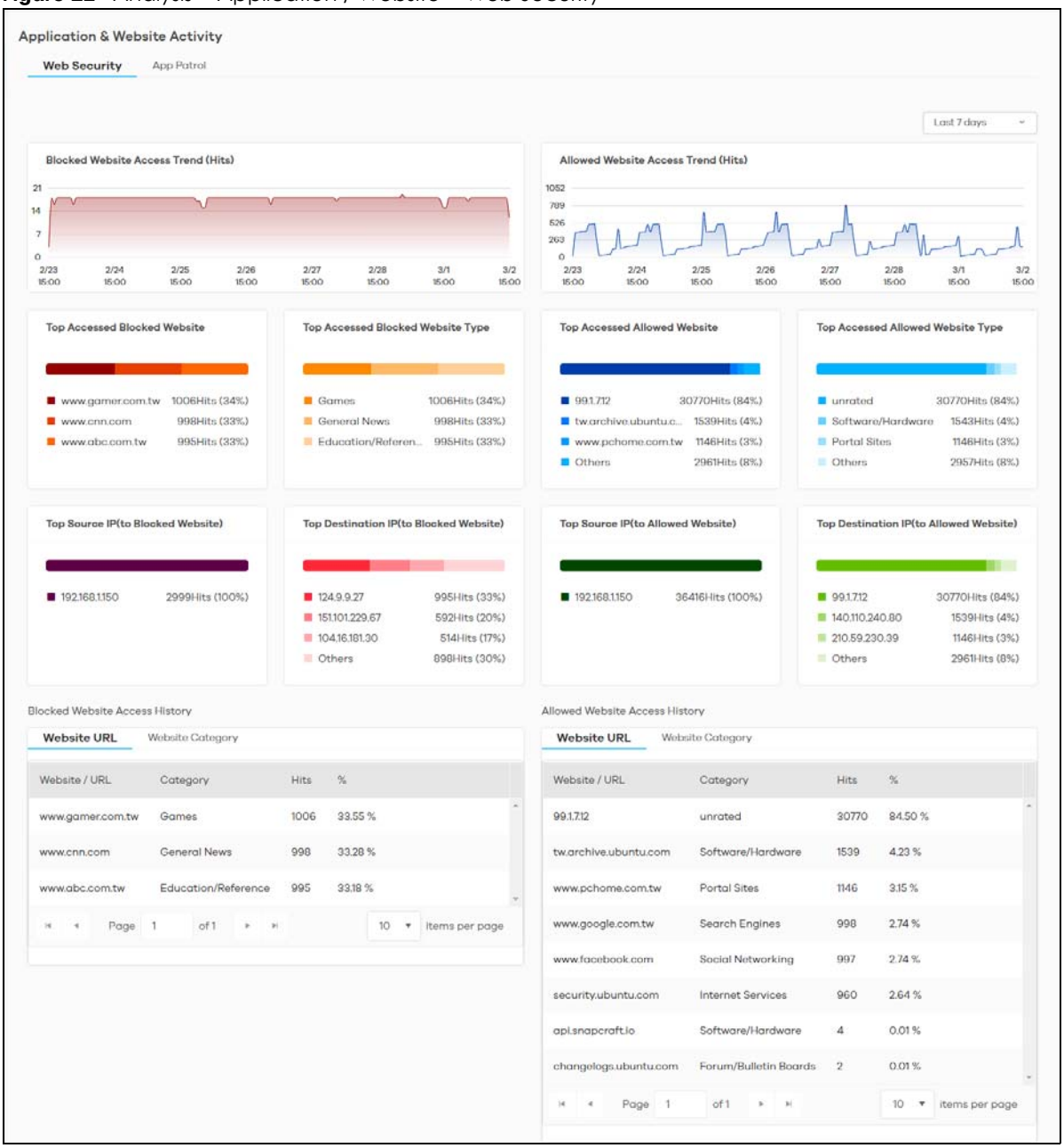
There are two ways the Zyxel Device can identify the application. The first is called auto. The Zyxel Device looks at the IP payload (OSI level-7 inspection) and attempts to match it with known patterns for specific applications. Usually, this occurs at the beginning of a connection, when the payload is more consistent across connections, and the Zyxel Device examines several packets to make sure the match is correct. Before confirmation, packets are forwarded by App Patrol with no action taken. The number of packets inspected before confirmation varies by signature.

Note: The Zyxel Device allows the first eight packets to go through the security policy, regardless of the application patrol policy for the application. The Zyxel Device examines these first eight packets to identify the application.

The second approach is called service ports. The Zyxel Device uses only OSI level-4 information, such as ports, to identify what application is using the connection. This approach is available in case the Zyxel Device identifies a lot of "false positives" for a particular application.

The following figure shows the **Analysis** > **Application / Website** > **Web Security** data visualizations.

Figure 21 Analysis > Application / Website > Web Security



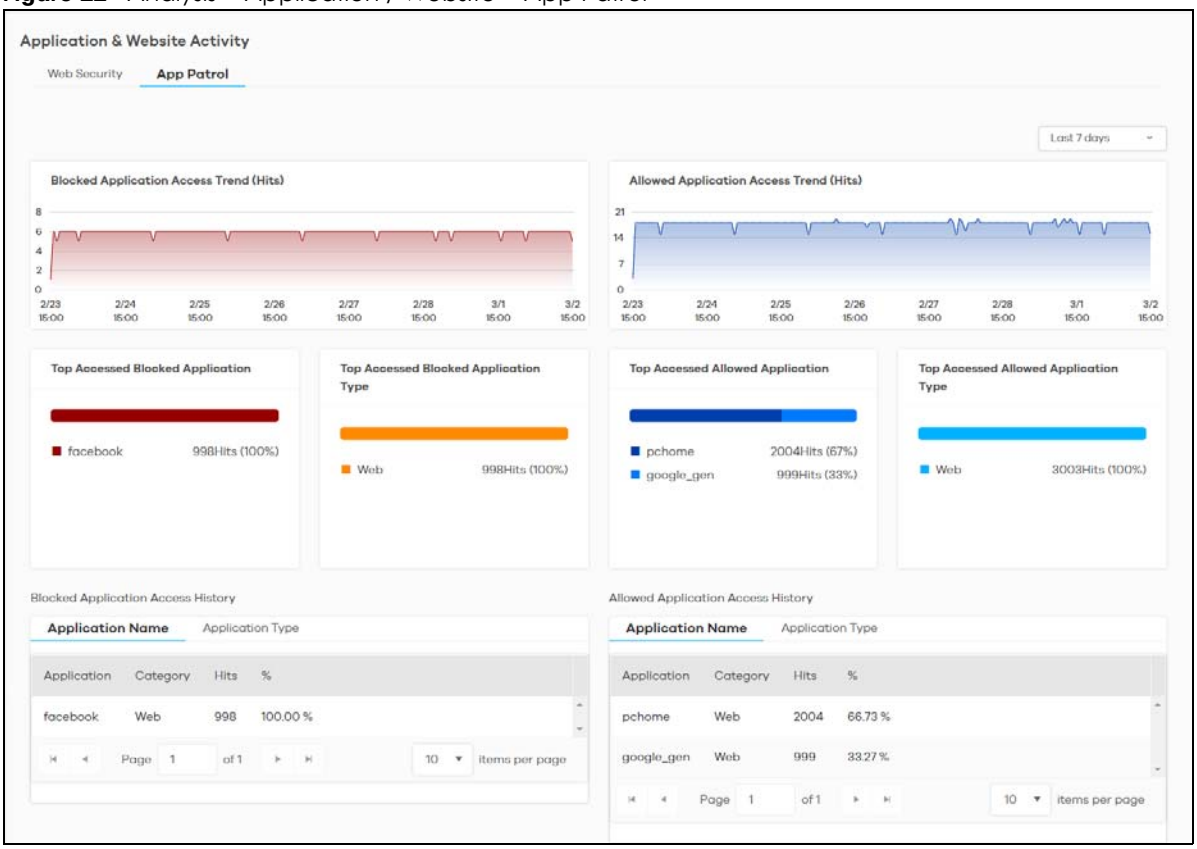
The following table describes the labels on the **Analysis** > **Application / Website** > **Web Security** screen.

Table 17 Analyzer > Application / Website > Website

LABEL	DESCRIPTION
Blocked Websites Access Trend (Hits)	This chart displays the most frequently visited websites through the Zyxel Devices as detected and blocked by Web Security. Move your cursor over a trend line to display the number of threats encountered over time.
Allowed Website Access Trend (Hits)	This chart displays the most frequently visited websites through the Zyxel Devices as detected by Web Security. Move your cursor over a trend line to display the number of threats encountered over time.
Top Accessed Blocked Website	This chart displays the top 3 websites blocked by the Zyxel Devices. Scroll down to **Blocked Website Access History** and click the **Website URL** tab to display details about the specific websites that were blocked.
Top Accessed Blocked Website Type	This chart displays the top 3 website types blocked by the Zyxel Devices. Scroll down to **Blocked Website Access History** and click the **Website Category** tab to display details about the specific website types that were blocked.
Top Accessed Allowed Websites	This chart displays the top 3 websites accessed through the Zyxel Devices. Scroll down to **Allowed Website Access History** and click the **Website URL** tab to display details about the specific websites that were accessed.
Top Accessed Allowed Website Type	This chart displays the top 3 website types accessed through the Zyxel Devices. Scroll down to **Allowed Website Access History** and click the **Website Category** tab to display details about the specific website types that were accessed.
Top Source IP (to Blocked Website)	This chart displays the source IP addresses of the top 3 incoming blocked IP addresses.
Top Destination IP (to Blocked Website)	This chart displays the destination IP addresses of the top 3 incoming blocked IP addresses.
Top Source IP (to Allowed Website)	This chart displays the source IP addresses of the top 3 incoming accessed websites.
Top Destination IP (to Allowed Website)	This chart displays the destination IP addresses of the top 3 incoming accessed websites.

The following figure shows the **Analysis** > **Application / Website** > **App Patrol** data visualizations.

Figure 22 Analysis > Application / Website > App Patrol



The following table describes the labels on the **Analysis** > **Application / Website** > **App Patrol** screen.

Table 18 Analysis > Application / Website > App Patrol

LABEL	DESCRIPTION
Blocked Application Access Trend (Hits)	This chart displays the most commonly used applications accessed through the Zyxel Devices 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 Devices as detected by 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). Move your cursor over a trend line to display the number of threats encountered over time.
Top Accessed Blocked Application	This chart displays the top 3 applications that were blocked the most frequently by the Zyxel Devices. 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 top 3 types of application that were blocked the most frequently by the Zyxel Devices. Scroll down to **Blocked Application Access History** and click the **Application Type** tab to display details about the specific application types that were blocked.

Table 18 Analysis > Application / Website > App Patrol (continued)

LABEL	DESCRIPTION
Top Access Allowed Application	This chart displays the top 3 applications that were accessed the most frequently by the Zyxel Devices. 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 top 3 applications that were accessed the most frequently by the Zyxel Devices. Scroll down to **Allowed Application Access History** and click the **Application Type** tab to display details about the specific application types that were accessed.

CHAPTER 3
Logs

3.1 Overview

Saving Logs on SecuReporter

SecuReporter saves logs of your Zyxel Device every 5 minutes.

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

- See Section 1.1.1 on page 6 for more information on the Zyxel Devices that support sandboxing.
- Your Zyxel Devices need to have firmware version 4.35 or later.
- Make sure sandboxing is selected in the **Categories** field of the **Configuration** > **Cloud CNM** > **SecuReporter** screen.

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

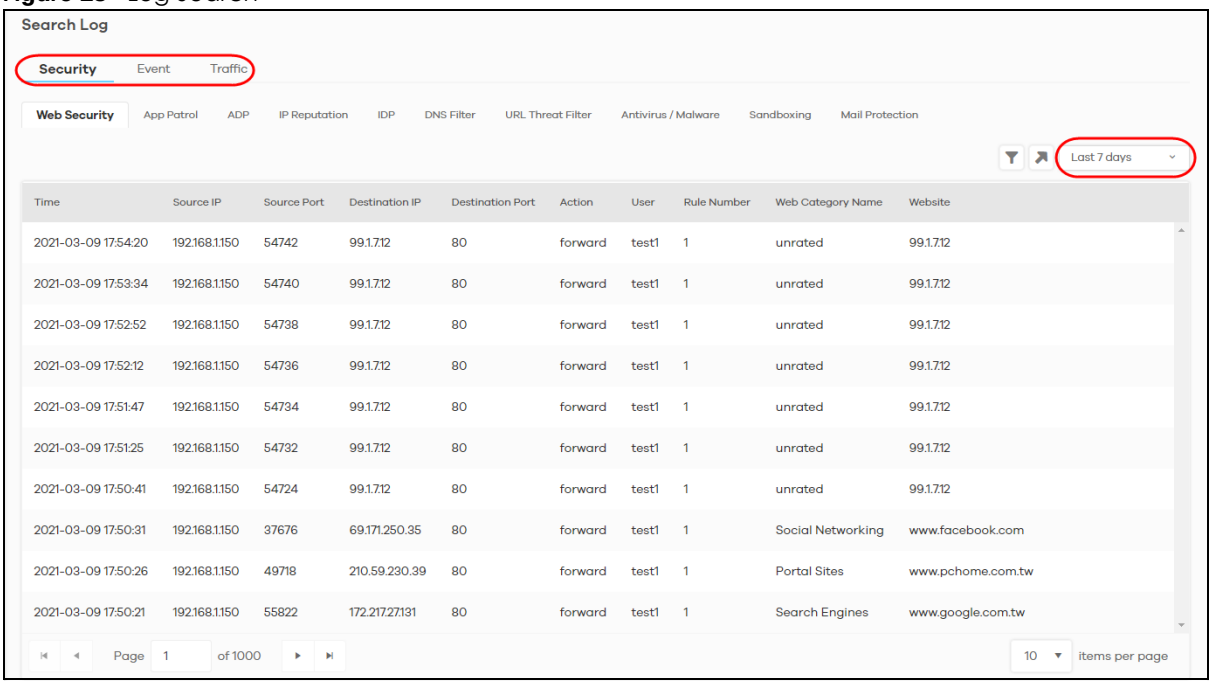
Note: Sandboxing logs will be removed after you reboot the Zyxel Device.

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

3.2 Log Search

Log search allows you to display Zyxel Device logs based on a time frame and also export them in CSV format for further analysis. You can select **Security**, **Event**, and **Traffic** 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 20 on page 44 for details.

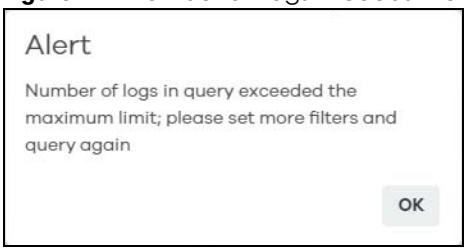
Figure 23 Log Search



You can set the log search criteria by clicking , see Table 20 on page 44 for details.

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

Figure 24 Number of Logs Exceeds the Limit



3.2.1 Log Search Privileges

SecuReporter comes with a different set of log search privileges depending on your license type.

This table summarizes SecuReporter log search privileges for each license type:

Table 19 SecuReporter Log Search Privileges

TYPE	SECUREPORTER	SECUREPORTER PREMIUM
Security Logs Date Range	Past 7 days	Past 30 days
Traffic Logs Date Range	Past 7 days	Past 7 days
Custom Range	Yes	Yes
Filters	Yes	Yes

Table 19 SecuReporter Log Search Privileges (continued)

TYPE	SECUREPORTER	SECUREPORTER PREMIUM
Frequency	No limitation	No limitation
CSV file download	No	Yes

3.2.2 Security Log Categories

Security logs are categorized as follows:

- Web Security
- App Patrol
- ADP
- IP Reputation (only available for the ZyWALL ATP series with firmware version 4.35 and above at the time of writing)
- IDP
- DNS Filter
- URL Threat Filter (only available for the ZyWALL ATP series with firmware version 4.35 and above at the time of writing)
- Antivirus / Malware
- Sandboxing (only available for the ZyWALL ATP series with firmware version 4.35 and above at the time of writing)
- Mail Protection

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

Table 20 Search > Log > Security Screens

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

Table 20 Search > Log > Security Screens (continued)

LABEL	DESCRIPTION
Action Security > Web Security	Enter how the Zyxel Device handle threats posed by websites (**forward**, **block**, **warning**). When adding this as a filter rule, enter the first letter to enable SecuReporter auto suggestion. More than one action can be entered after the first filter rule by entering another action and pressing **Enter**. Multiple action filters are entered one at a time.
Action Security > App Patrol	Enter how the Zyxel Device handle threats posed by applications (**forward**, **reject**). 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 **forward** and **reject** can be entered as a filter rule by entering **forward** and pressing **Enter**, and then entering **reject** and pressing **Enter**.
Action Security > IDP/ADP	Enter the response the Zyxel Device takes when a packet matches a signature. A signature is a pattern of malicious or suspicious packet activity. This is defined in the profile screen of your Zyxel Device's Web Configurator. The Zyxel Device checks all signatures and continues searching even after a match is found. If two or more rules have conflicting actions for the same packet, then the Zyxel Device applies the more restrictive action (**Reject Both**, **Reject Receiver** or **Reject Sender**, **Drop Packet**, **No Action** in this order). If a packet matches a rule for **Reject Receiver** and it also matches a rule for **Reject Sender**, then the Zyxel Device will **Reject Both**. When adding this as a filter rule, enter the first letter to enable SecuReporter auto suggestion. More than one action can be entered after the first filter rule by entering another action and pressing **Enter**. Multiple action filters are entered one at a time.
Action Security > IP Reputation	IP Reputation checks the reputation of an IP address from a database. An IP address with bad reputation associates with suspicious activities, such as spam, virus, and/or phishing. Enter how the Zyxel Device will respond when there are packets coming from an IPv4 address with bad reputation (**ACCESS BLOCK** and **ACCESS FORWARD**). When adding this as a filter rule, enter the action or part of the action you want to find to enable SecuReporter auto suggestion. Both **ACCESS BLOCK** and **ACCESS FORWARD** can be entered as a filter rule by entering **ACCESS BLOCK** and pressing **Enter**, and then entering **ACCESS FORWARD** and pressing **Enter**.
Action Security > DNS Filter	Enter how the Zyxel Device handle threats posed by FQDNs (**Block**, **Redirect**). When adding this as a filter rule, enter the first letter to enable SecuReporter auto suggestion. More than one action can be entered after the first filter rule by entering another action and pressing **Enter**. Multiple action filters are entered one at a time.
Action Security > URL Threat Filter	Enter how the Zyxel Device handle threats posed by URLs (Uniform Resource Locators) (**ACCESS BLOCK**, **ACCESS WARNING**, **ACCESS PASS**). When adding this as a filter rule, enter the first letter to enable SecuReporter auto suggestion. More than one action can be entered after the first filter rule by entering another action and pressing **Enter**. Multiple action filters are entered one at a time.
Action Security > Antivirus / Malware	Enter **ACCESS FORWARD** when a service can be used to access the Zyxel Device. Otherwise, it is **ACCESS BLOCK**. Enter **FILE FORWARD** when a file is allowed. Otherwise, it is **FILE DESTROY**. When adding this as a filter rule, enter the first letter to enable SecuReporter auto suggestion. More than one action can be entered after the first filter rule by entering another action and pressing **Enter**. Multiple action filters are entered one at a time.
Action Security > Sandboxing	The Zyxel Device sandbox checks all received files against its local cache for known malicious or suspicious codes. Enter how the Zyxel Device handle sandboxing (**Pass**, **Detected, Destroy**). When adding this as a filter rule, enter the first letter to enable SecuReporter auto suggestion. More than one action can be entered after the first filter rule by entering another action and pressing **Enter**. Multiple action filters are entered one at a time.

Table 20 Search > Log > Security Screens (continued)

LABEL	DESCRIPTION
Action Security > Mail Protection	Enter how the Zyxel Device handle spam SMTP/POP3 email (**MAIL FORWARD**, **MAIL DROP**). When adding this as a filter rule, enter the action or part of the action you want to find to enable SecuReporter auto suggestion. Both **MAIL FORWARD** and **MAIL DROP** can be entered as a filter rule by entering **MAIL FORWARD** and pressing **Enter**, and then entering **MAIL DROP** and pressing **Enter**.
User	Depending on the data protection policy (see Section 6.2.1 on page 71 for details), the following will be displayed: • For **Partially Anonymous** users, the user name is displayed but log search is disabled. • For **Fully Anonymous** users, copy a Hash value to search for logs. For example, USER-698a9b31-cea4-523c-8955-ffad47db967e. • For **Non-Anonymous** users, enter plain text (unlimited number of characters, case sensitive) for log search.
Signature Name	Enter the name (case sensitive, a wildcard is allowed) of a signature. When adding this as a filter rule, enter the name or part of the name of the signature you want to find to enable SecuReporter auto suggestion.
Signature ID	Enter the identification number of the signature. When adding this as a filter rule, enter the ID or part of the ID of the signature you want to find to enable SecuReporter auto suggestion.
Threat Type	Enter the signature (case sensitive) by threat type. When adding this as a filter rule, enter the threat type or part of the threat type you want to find to enable SecuReporter auto suggestion. More than one threat type can be entered after the first filter rule by entering another threat type and pressing **Enter**. Multiple threat type filters are entered one at a time.
Mail From	Depending on the data protection policy (see Section 6.2.1 on page 71 for details), the following will be displayed: • For **Partially Anonymous** users, the sender is displayed but log search is disabled. • For **Fully Anonymous** users, copy a Hash value to search for logs. For example, MAIL-108cef2d-b591-5460-af79-71994d126cc7. • For **Non-Anonymous** users, enter plain text (unlimited number of characters, case sensitive) for log search.
Mail To	Depending on the data protection policy (see Section 6.2.1 on page 71 for details), the following will be displayed: • For **Partially Anonymous** users, the recipient is displayed but log search is disabled. • For **Fully Anonymous** users, copy a Hash value to search for logs. For example, MAIL-108cef2d-b591-5460-af79-71994d126cc7. • For **Non-Anonymous** users, enter plain text (unlimited number of characters, case sensitive) for log search.
Mail Subject	This is the title header of the incoming email.
Protocol Security > Sandboxing	Enter the method email is sent or received through the Zyxel Device (**SMTP**, **POP3**, **HTTP**, **FTP**, and **Unknown**). When adding this as a filter rule, enter the protocol or part of the protocol you want to find to enable SecuReporter auto suggestion. More than one protocol can be entered after the first filter rule by entering another protocol and pressing **Enter**. Multiple protocol filters are entered one at a time.
Protocol Security > Mail Protection	Enter the method email is sent or received through the Zyxel Device (**SMTP** and **POP3**). When adding this as a filter rule, enter the protocol or part of the protocol you want to find to enable SecuReporter auto suggestion. Both **SMTP** and **POP3** can be entered as a filter rule by entering **SMTP** and pressing **Enter**, and then entering **POP3** and pressing **Enter**.

Table 20 Search > Log > Security Screens (continued)

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

Table 20 Search > Log > Security Screens (continued)

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

Table 20 Search > Log > Security Screens (continued)

LABEL	DESCRIPTION
Website	Enter the name of the website (a wildcard is allowed) tasked with screening for the most common types of threats posed by websites blocked by the Zyxel Devices. When adding this as a filter rule, enter the website or part of the website you want to find to enable SecuReporter auto suggestion.
Query Type	Enter the type of IP address that may pose a security threat to network devices behind the Zyxel Device. When adding this as a filter rule, select from the drop-down list. More than one query type can be entered after the first filter rule by entering another query type and pressing **Enter**. Multiple query type filters are entered one at a time.
Domain	Enter the URL of FQDNs that may pose a security threat to network devices behind the Zyxel Device. When adding this as a filter rule, select from the drop-down list. More than one domain can be entered after the first filter rule by entering another domain and pressing **Enter**. Multiple domain filters are entered one at a time.
Page	Select the page number to be displayed in case of multiple page reports.
item per page	Select the number of reports to be displayed in a page. You may need to scroll down the page to view when selecting **10**/**20**/**50**/**100** items per page.

3.2.3 Event Log Categories

Event logs are categorized as follows:

- User Login
- Device Event
- DHCP

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

Table 21 Search > Log > Event Screens

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

Table 21 Search > Log > Event Screens (continued)

LABEL	DESCRIPTION
Action Event > DHCP	Enter the action of assigning an IP address to a device by the DNS server or release (**assigned** and **release**). When adding this as a filter rule, enter the action or part of the action you want to find to enable SecuReporter auto suggestion. Both **assigned** and **release** can be entered as a filter rule by entering **assigned** and pressing **Enter**, and then entering **release** and pressing **Enter**.
Assign IP	This is the IPv4 or IPv6 address currently assigned to a DHCP client or reserved for a specific MAC address. When adding this as a filter rule, enter the complete IP address or enter a wildcard such as 192.168.221.* (it will search for logs with any IP within 192.168.221.0 – 192.168.221.255)
User	Depending on the data protection policy (see Section 6.2.1 on page 71 for details), the following will be displayed: • For **Partially Anonymous** users, the user name is displayed but log search is disabled. • For **Fully Anonymous** users, copy a Hash value to search for logs. For example, USER-698a9b31-cea4-523c-8955-ffad47db967e. • For **Non-Anonymous** users, enter plain text (unlimited number of characters, case sensitive) for log search.
Type	Enter the role type (a wildcard is allowed) of the event's login attempt (**Administrator**, **Limited-Admin**, **User**). When adding this as a filter rule, enter the role type or part of the role type you want to find to enable SecuReporter auto suggestion.
MAC Address Event > User Login	Enter the Zyxel Device's MAC address (case sensitive) during the event's login attempt. Depending on the data protection policy (see Section 6.2.1 on page 71 for details), the following will be displayed: • For **Partially Anonymous** users, the MAC address is displayed but log search is disabled. • For **Fully Anonymous** users, copy a Hash value to search for logs. For example, MAC-5ba49d8a-d027-5c76-bf28-a45857f780bc. • For **Non-Anonymous** users, enter plain text (unlimited number of characters, case sensitive) for log search.
MAC Address Event > DHCP	Enter the MAC address (case sensitive) to which the IP address is currently assigned or for which the IP address is reserved. Depending on the data protection policy (see Section 6.2.1 on page 71 for details), the following will be displayed: • For **Partially Anonymous** users, the MAC address is displayed but log search is disabled. • For **Fully Anonymous** users, copy a Hash value to search for logs. For example, MAC-5ba49d8a-d027-5c76-bf28-a45857f780bc. • For **Non-Anonymous** users, enter plain text (unlimited number of characters, case sensitive) for log search.
Device Event	This displays **boot-up** as the Zyxel Device event.
Host Name	Enter the unique name (case sensitive) by which a device is known on a network. The Zyxel Device learns these from the DHCP client requests. Depending on the data protection policy (see Section 6.2.1 on page 71 for details), the following will be displayed: • For **Partially Anonymous** users, the host name is displayed but log search is disabled. • For **Fully Anonymous** users, copy a Hash value to search for logs. For example, HOST-8c9f2269-c7fa-55e5-b36f-d8987efd11ee. • For **Non-Anonymous** users, enter plain text (unlimited number of characters, case sensitive) for log search.

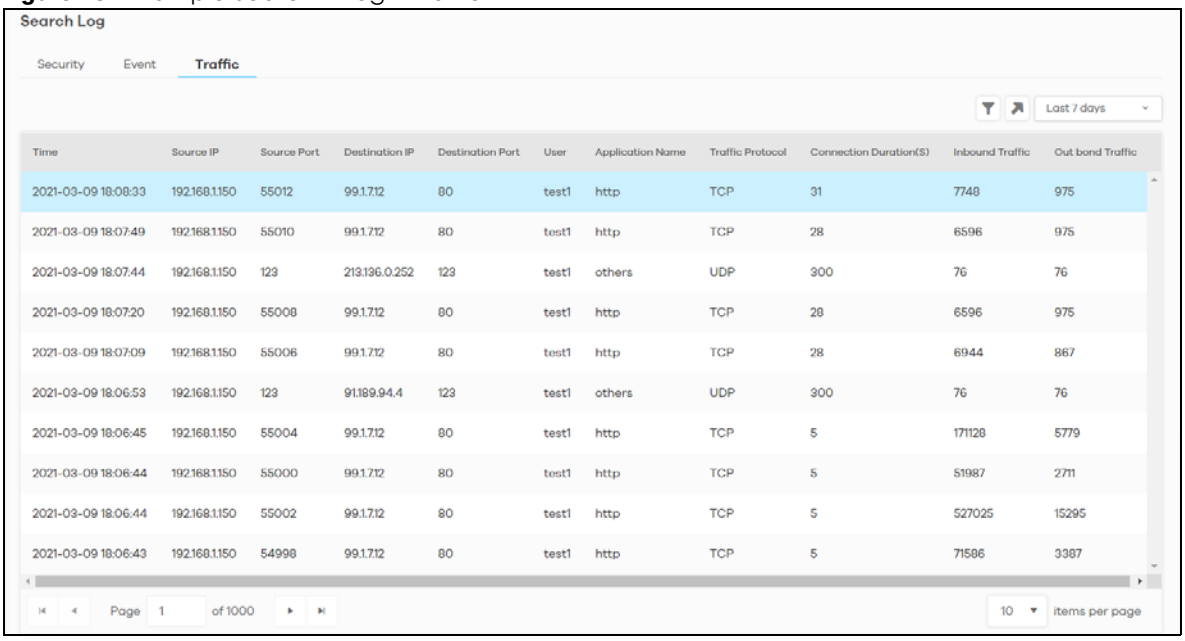
Table 21 Search > Log > Event Screens (continued)

LABEL	DESCRIPTION
Page	Select the page number to be displayed in case of multiple page reports.
item per page	Select the number of reports to be displayed in a page. You may need to scroll down the page to view when selecting **10**/**20**/**50**/**100** items per page.

3.2.4 Traffic Log Categories

The following figure shows an example **Search** > **Log** > **Traffic** result.

Figure 25 Example Search > Log > Traffic



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

Table 22 Search > Log > Traffic

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

Table 22 Search > Log > Traffic (continued)

LABEL	DESCRIPTION
User	Depending on the data protection policy (see Section 6.2.1 on page 71 for details), the following will be displayed: • For **Partially Anonymous** users, the user name is displayed but log search is disabled. • For **Fully Anonymous** users, copy a Hash value to search for logs. For example, USER-698a9b31-cea4-523c-8955-ffad47db967e. • For **Non-Anonymous** users, enter plain text (unlimited number of characters, case sensitive) for log search.
Application 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.
Page	Select the page number to be displayed in case of multiple page reports.
item per page	Select the number of reports to be displayed in a page. You may need to scroll down the page to view when selecting **10**/**20**/**50**/**100** items per page.

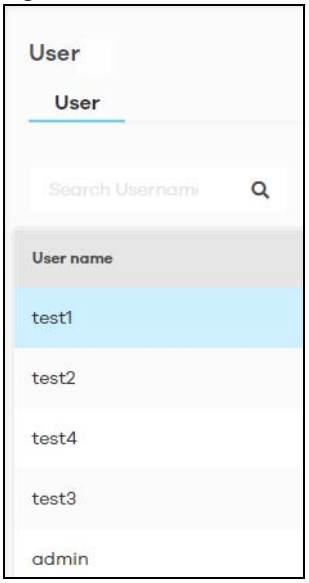
3.3 User

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

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

In the field at the top-left of the screen, enter a **User name** and press (search). You may also enter a partial term to generate a list of matching results.

Figure 26 Search > User



3.3.1 Details

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

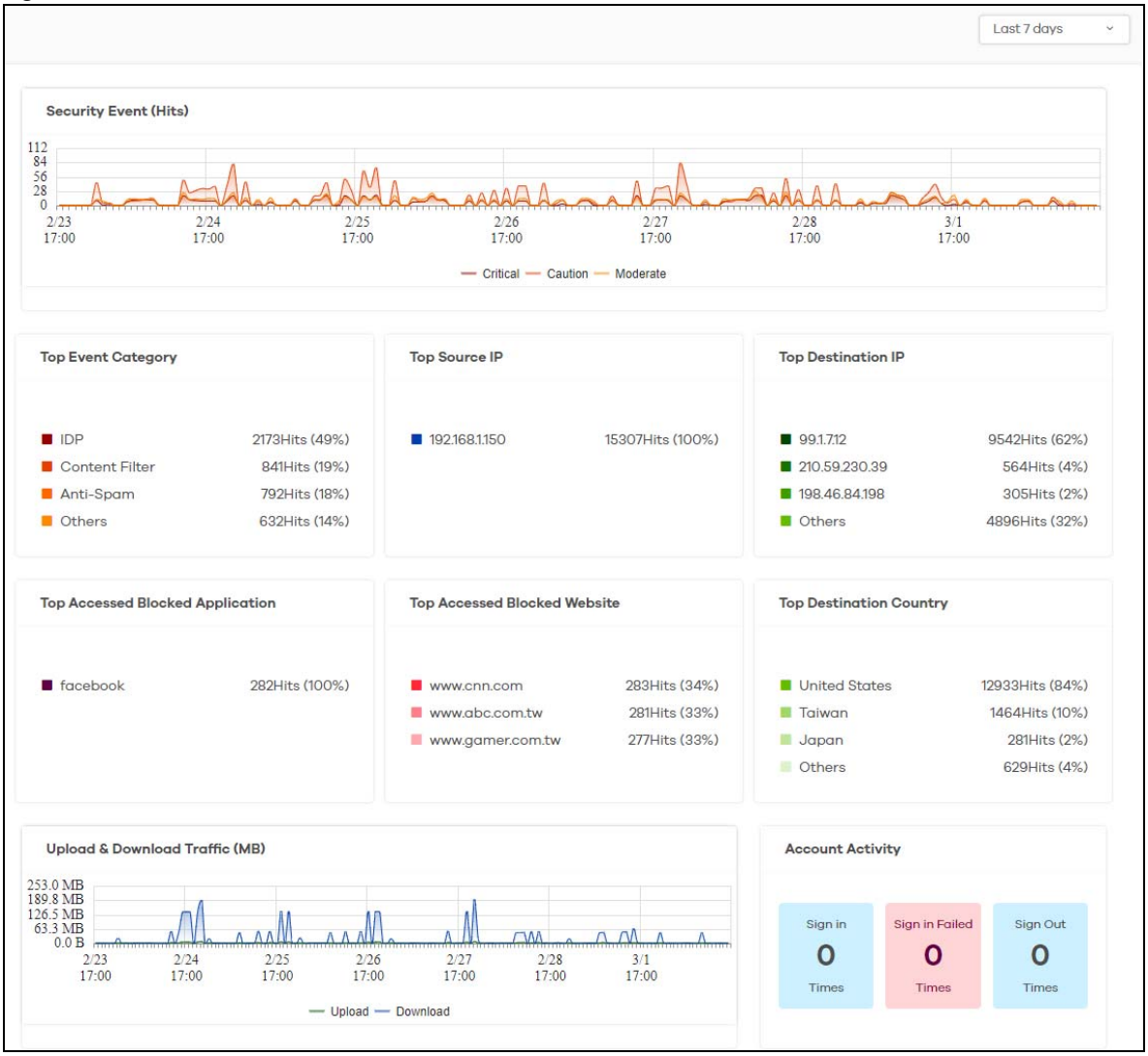
Security events include anomalies, app patrol, malware, spam, threats (IDP), unsafe websites, and web protection (websites blocked by web security policies). The following table shows severity levels for security events.

Table 23 Security Events Severity Levels

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

Select a **User name** in **Search** > **User** to display the following figure.

Figure 27 Search > User > Details



Click a graph to see further usage details for this user. For example, the following figure shows details on Internet usage per application through the selected Zyxel Device for this user.

Figure 28 Search > User > Details > Top Accessed Blocked Application

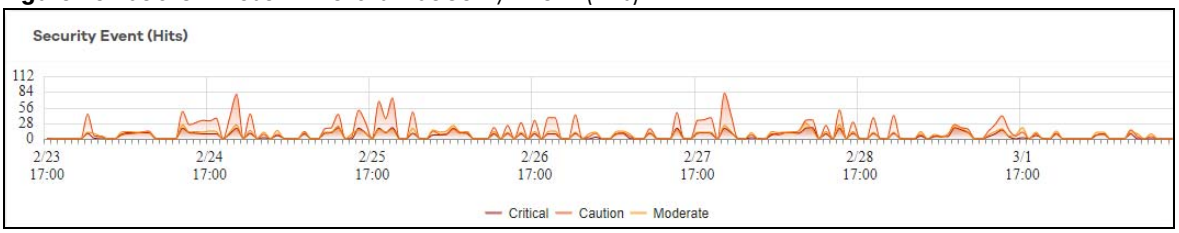
Accessed Blocked Application Detail

Time	Application Category	Application name	Firewall Action	Rule Number
2021-03-09 18:10:31	Web	facebook	reject	1
2021-03-09 18:00:31	Web	facebook	reject	1
2021-03-09 17:50:31	Web	facebook	reject	1
2021-03-09 17:40:32	Web	facebook	reject	1
2021-03-09 17:30:32	Web	facebook	reject	1
2021-03-09 15:50:31	Web	facebook	reject	1
2021-03-09 15:40:31	Web	facebook	reject	1
2021-03-09 15:30:31	Web	facebook	reject	1
2021-03-09 09:20:31	Web	facebook	reject	1
2021-03-09 09:10:31	Web	facebook	reject	1

Page 1 of 26 10 items per page

The following figure shows details on security events through the selected Zyxel Device for this user.

Figure 29 Search > User > Details > Security Event (Hits)



CHAPTER 4
Alerts

4.1 Overview

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

4.2 Trend & Details

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

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

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

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

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

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

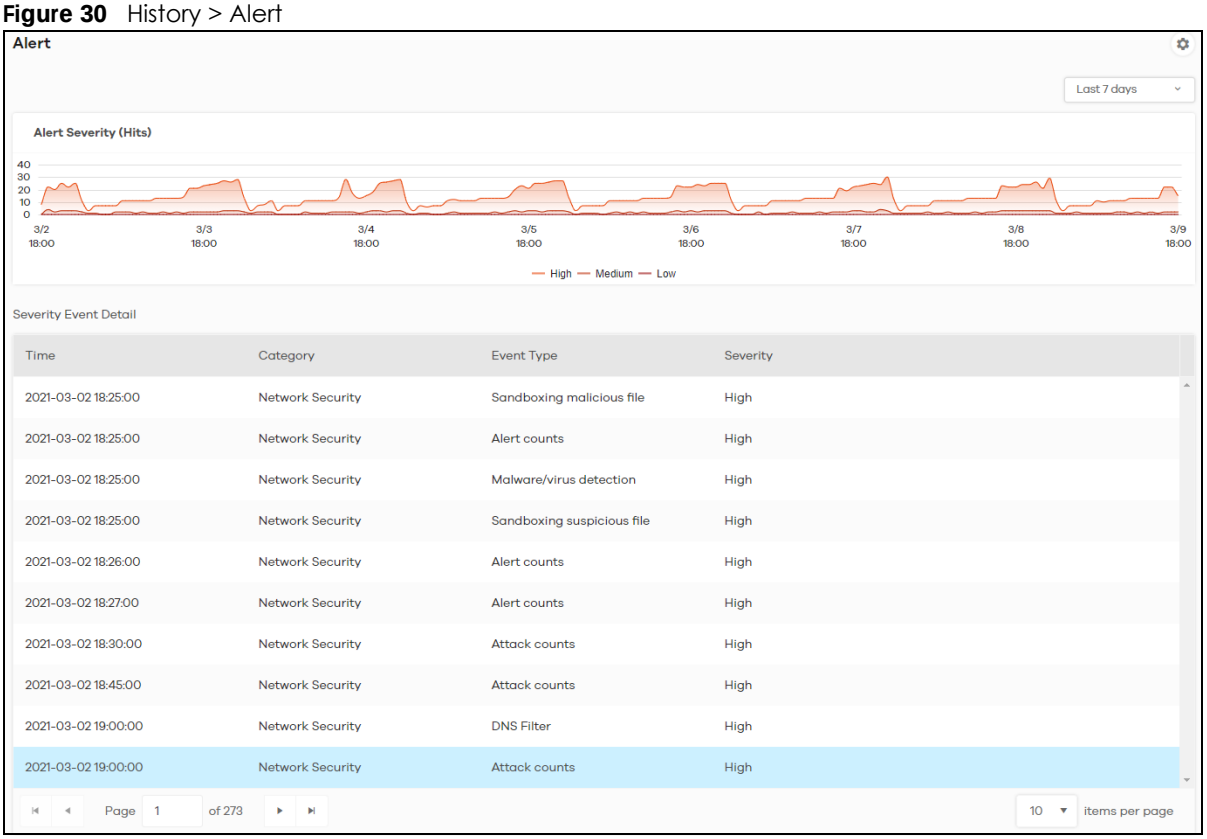
Table 24 Event Categories, Types and Criteria

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 24 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 30 History > Alert



The following table describes the labels on this screen.

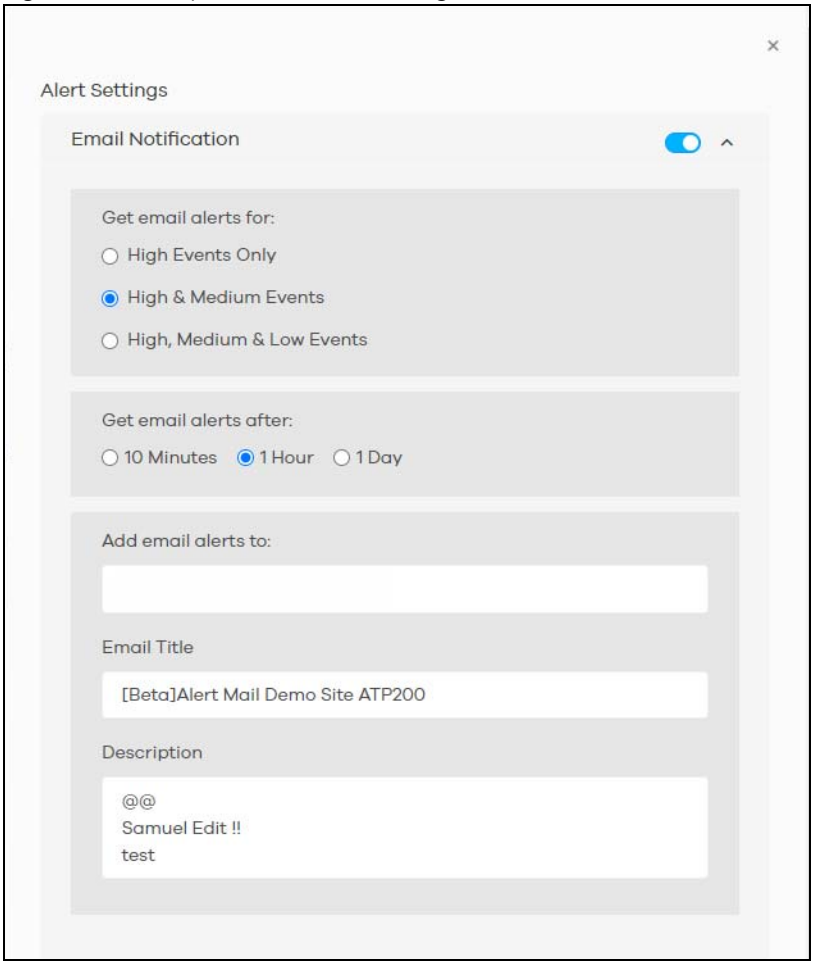
Table 25 History > Alert

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 Event Detail	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 IDP, Spam, Virus and Web.
Severity	This displays the severity level as outlined in Table 6 on page 12.

4.3 Configuration

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 31 History > Alert > Alert Settings > Email Notification

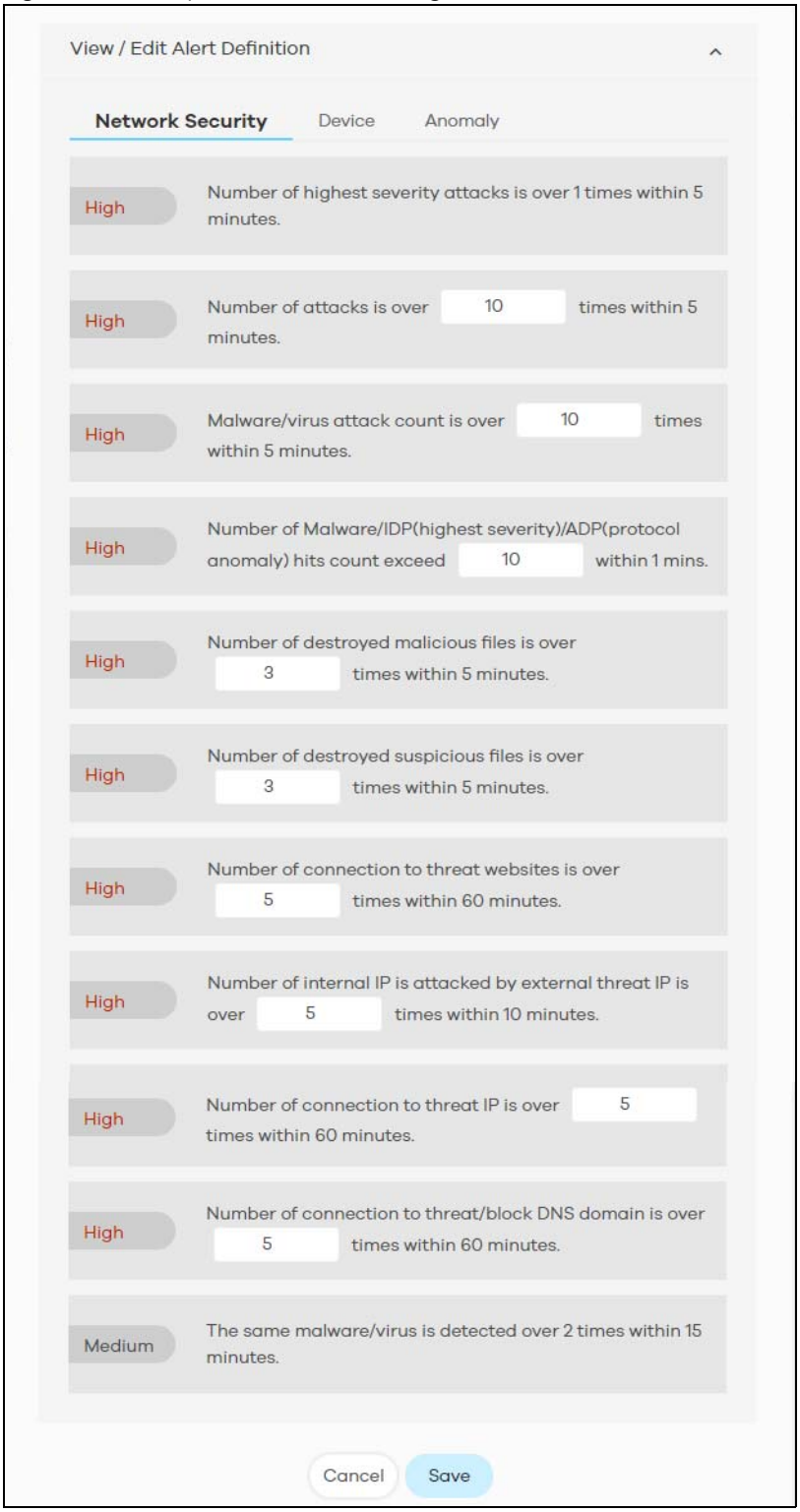


The following table describes the labels in this screen.

Table 26 History > Alert > Alert Settings > Email Notification

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

Figure 32 History > Alert > Alert Settings > View/Edit Alert Definition > Network Security



The following table describes the labels in this screen.

Table 27 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 33 History > Alert > Alert Settings > View/Edit Alert Definition > Device

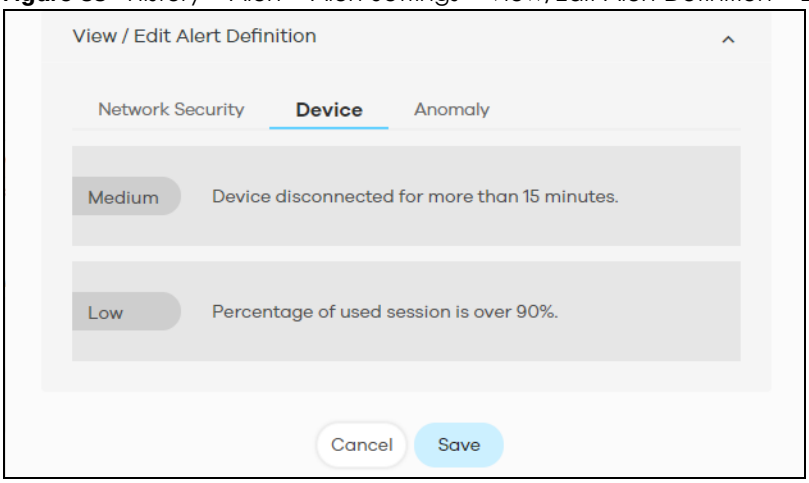
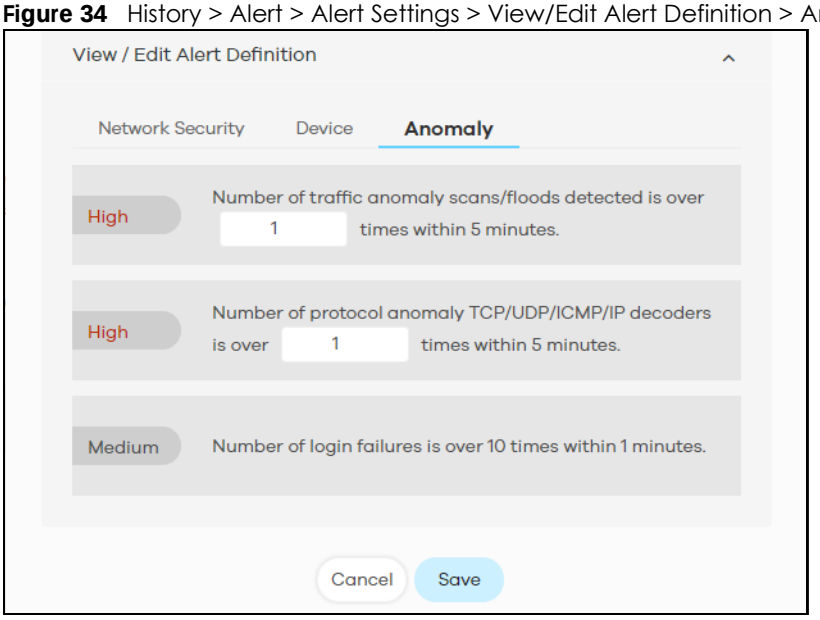


Figure 34 History > Alert > Alert Settings > View/Edit Alert Definition > Anomaly



The following table describes the labels in this screen.

Table 28 History > Alert > Alert Settings > View/Edit Alert Definition > Anomaly

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

CHAPTER 5
Report

5.1 Overview

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

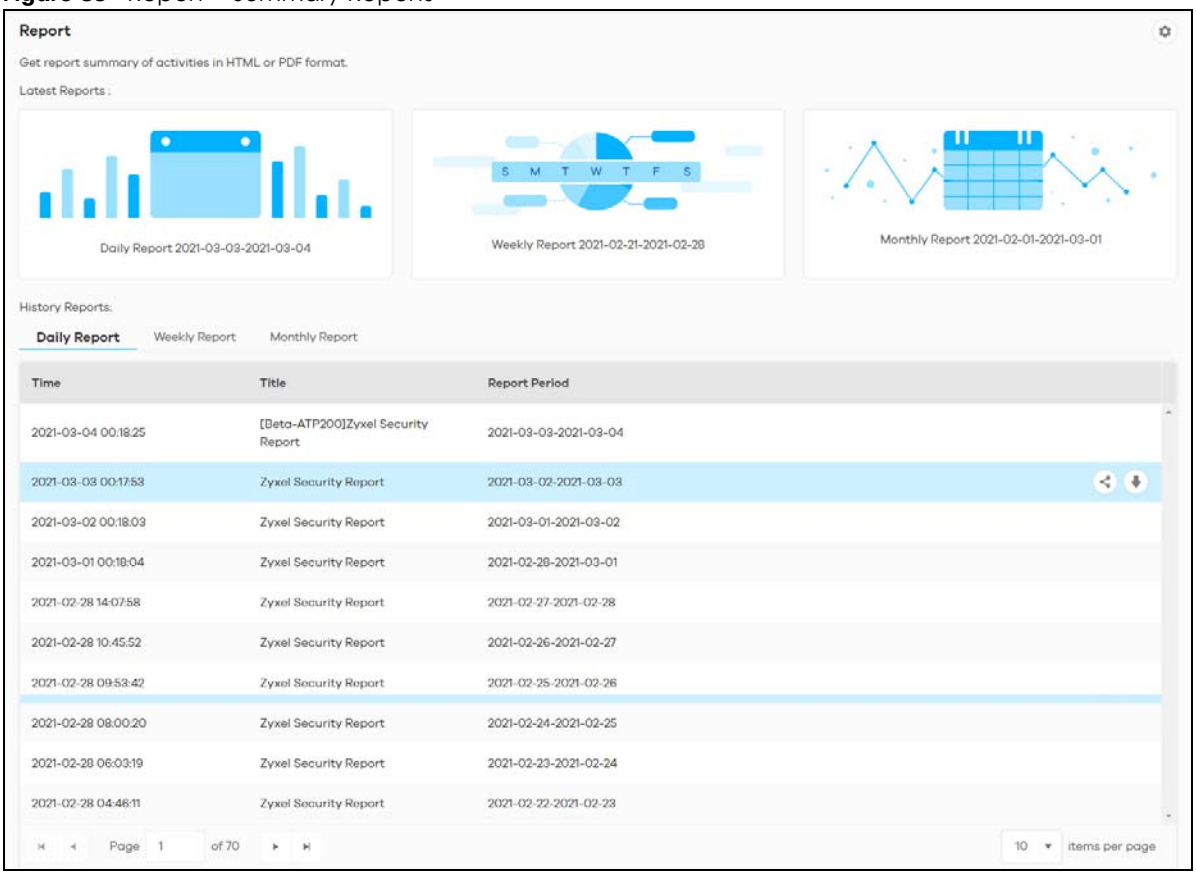
You can choose to generate reports of analyzed data collected over one of three time frames:

- Last 24 hours
- Last 7 days
- Last 30 days (for SecuReporter Premium only)

5.2 Summary Reports

Click **History** > **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 35 Report > Summary Reports



The following table describes the labels on this screen.

Table 29 Report > Summary Reports

LABEL	DESCRIPTION
Report	Get a summary report of activities in HTML or PDF format. **Latest Reports** are classified according to the following: • Daily Report • Weekly Report • Monthly Report (for SecuReporter Premium only) Clicking any of the above will allow you to view the report online. You can then download it in PDF format or print it.
History Reports	This displays the type of report by clicking on the tab. • Daily Report • Weekly Report • Monthly Report (for SecuReporter Premium only)
Time	This displays the reports in order of the date and time they were created, starting with the most recent one.
Title	This displays the title of each report as configured in **Report Settings**.
Report Period	This displays the date that the report covers. For a daily type of report a range of two consecutive dates will be displayed. For a weekly type of report a range of seven consecutive dates will be displayed. For a monthly type of report a range of 30 consecutive dates will be displayed.

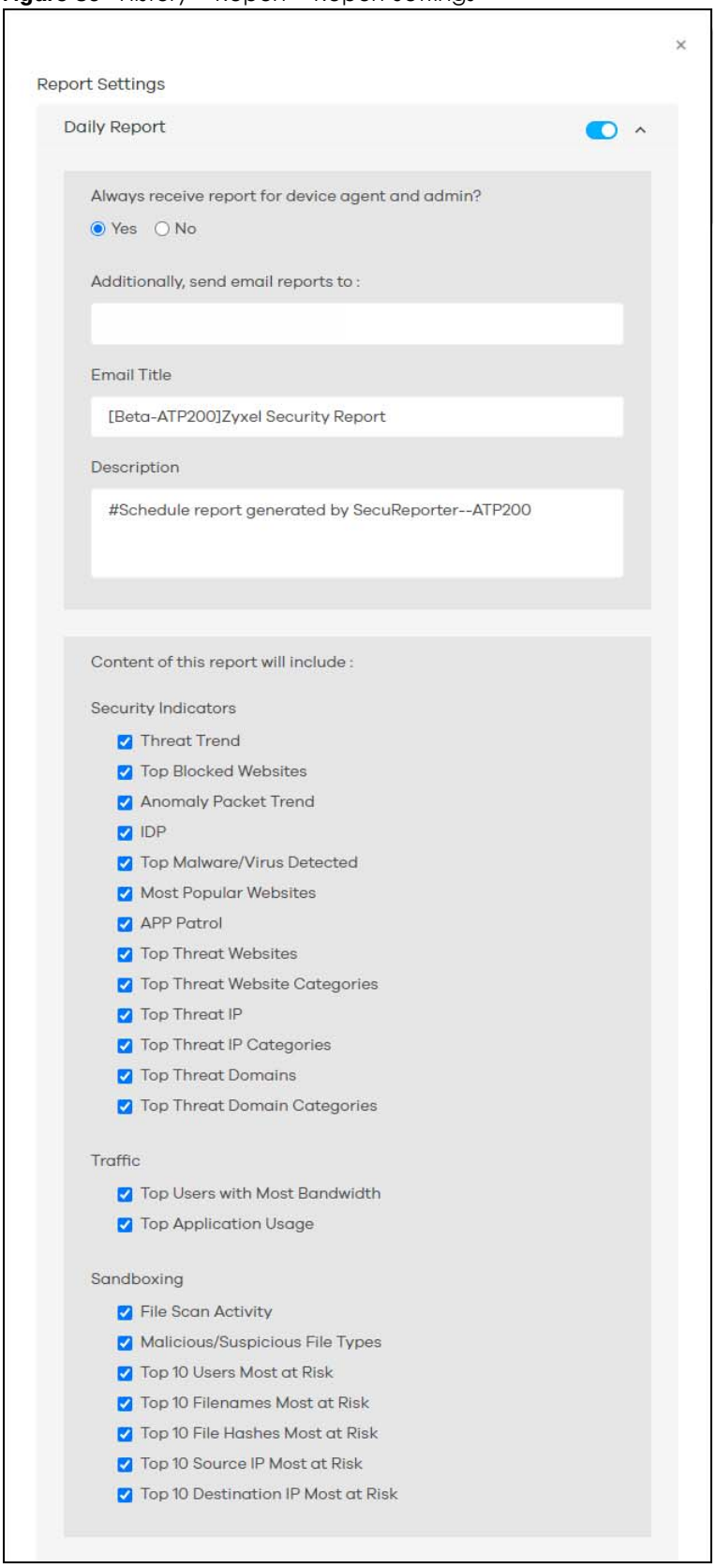
Table 29 Report > Summary Reports (continued)

LABEL	DESCRIPTION
Action	Click a row to display the report online. You can then download it in PDF format or print it. Click  to send a report in PDF format to the designated email recipients. Enter an email address and press **Enter**. Note: You can configure up to 30 email addresses. Click  to save a report in PDF format to your computer. Upon clicking (Download), you will be asked where you want to save the report in your computer.
Page	Select the page number to be displayed in case of multiple page reports.
items per page	Select the number of reports to be displayed in a page. You may need to scroll down the page to view when selecting **10**/**20**/**50**/**100** items per page.

5.3 Report Configuration

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

Figure 36 History > Report > Report Settings



The following table describes the labels on this screen.

Table 30 History > Report > Report Settings

LABEL	DESCRIPTION
Daily/Weekly/Monthly Report	Click this to enable (activate) On or disable (deactivate) Off the scheduled report.
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: email1@zyxel.com,email2@zyxel.com)
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 [~!@#$%^&*()_+{}|:"<>?-=[]\;',./].
Description	This field allows you to enter a description of the purpose of this report profile for future reference. Up to 1100 characters are allowed for the **Description** including special characters inside the square quotes [~!@#$%^&*()_+{}|:"<>?-=[]\;',./].
Content of this report will include	The widgets are the security services and traffic indicators that you can select to be included in the report profile. Refer to Chapter 2 Analysis for a description of the widgets. Click an item (with check mark) to include it in the report profile.
Save	Click **Save** to save your changes.
Cancel	Click **Cancel** to restore your previously saved settings.

CHAPTER 6
Settings

6.1 Overview

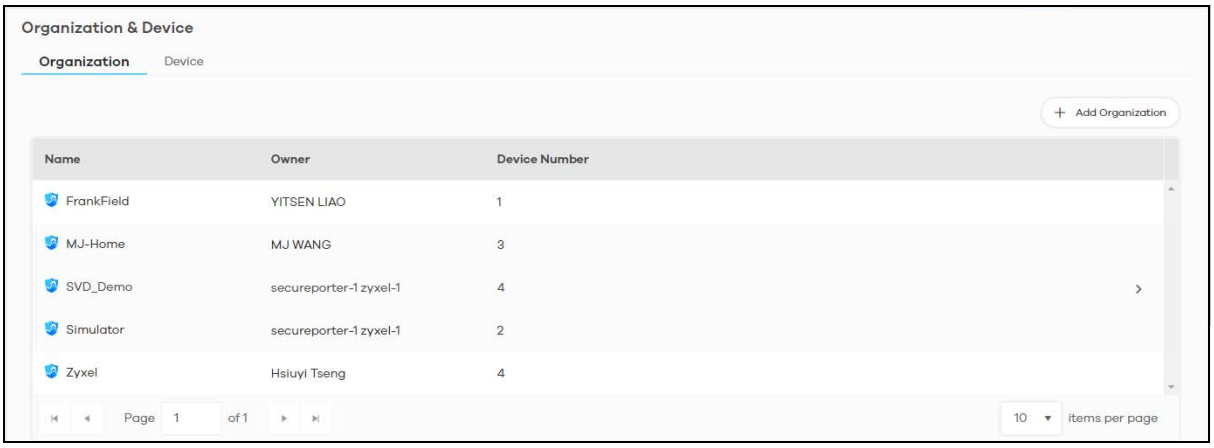
First, register your Zyxel Device at myZyxel.com, activate the SecuReporter license, and enable SecuReporter in the Zyxel Device using its Web Configurator or commands. You can then add your Zyxel Device to an organization at the SecuReporter web portal.

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

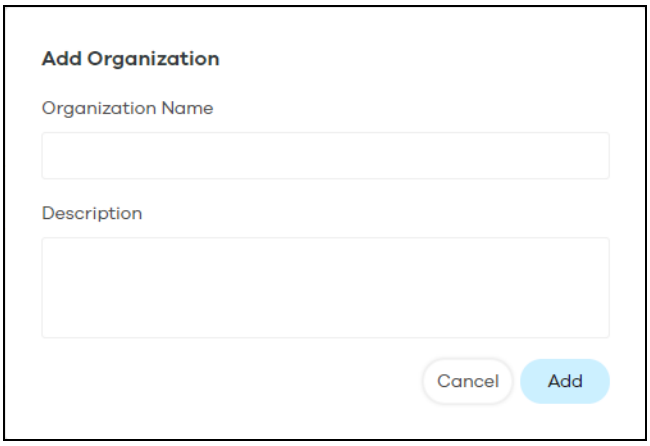
6.2 Organization & Device

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

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

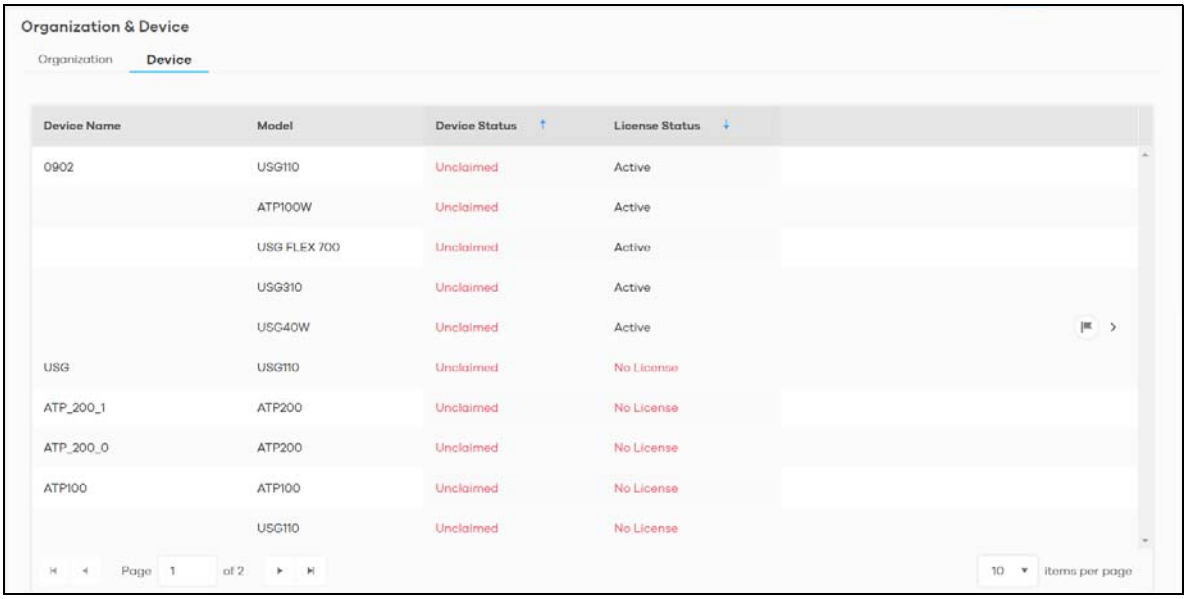


2 Enter a name of up to 255 characters and description for the organization.

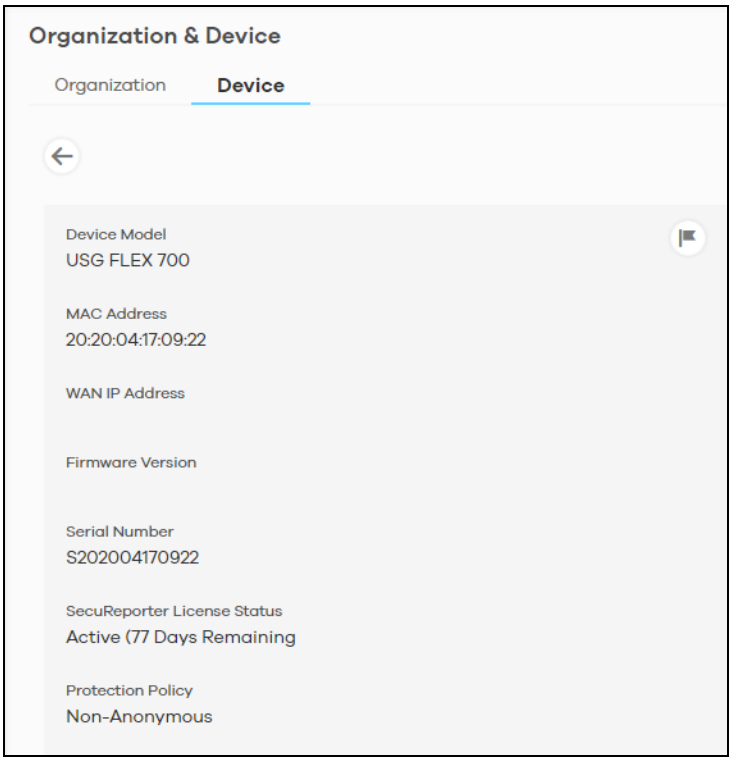


6.2.1 Add a Zyxel Device to an Organization

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

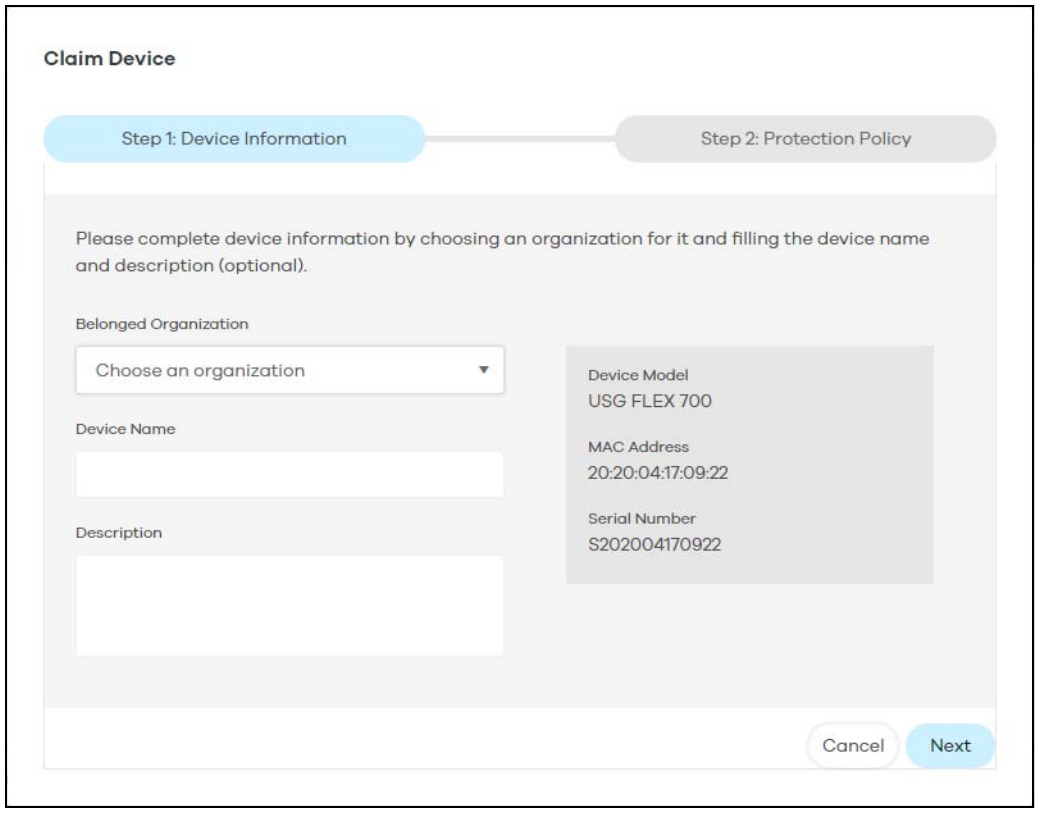


1 Click the hyperlink under **Unclaimed** to add Zyxel Devices to this organization. You will see details of Zyxel Devices that are available to be added.

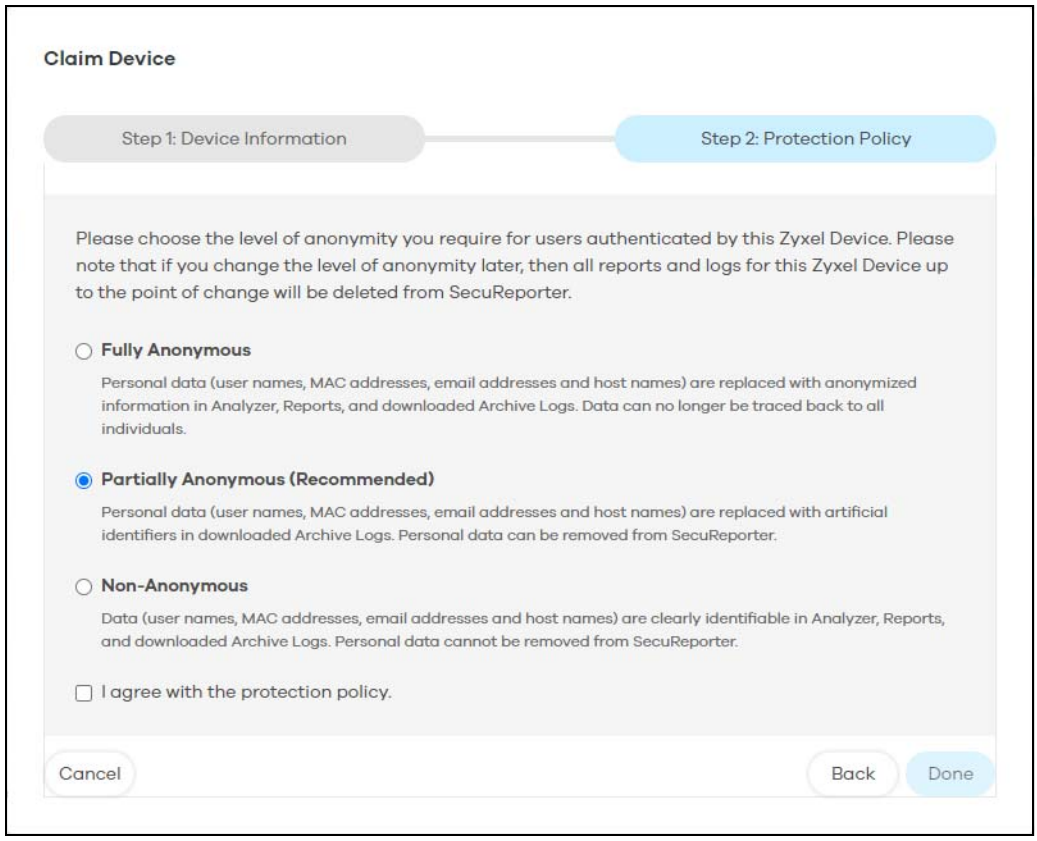


2 You will see the icon on the right when you hover the mouse on the registered Zyxel Devices that have activated SecuReporter licenses. This icon will not appear for registered Zyxel Devices that do not have activated SecuReporter license.

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



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

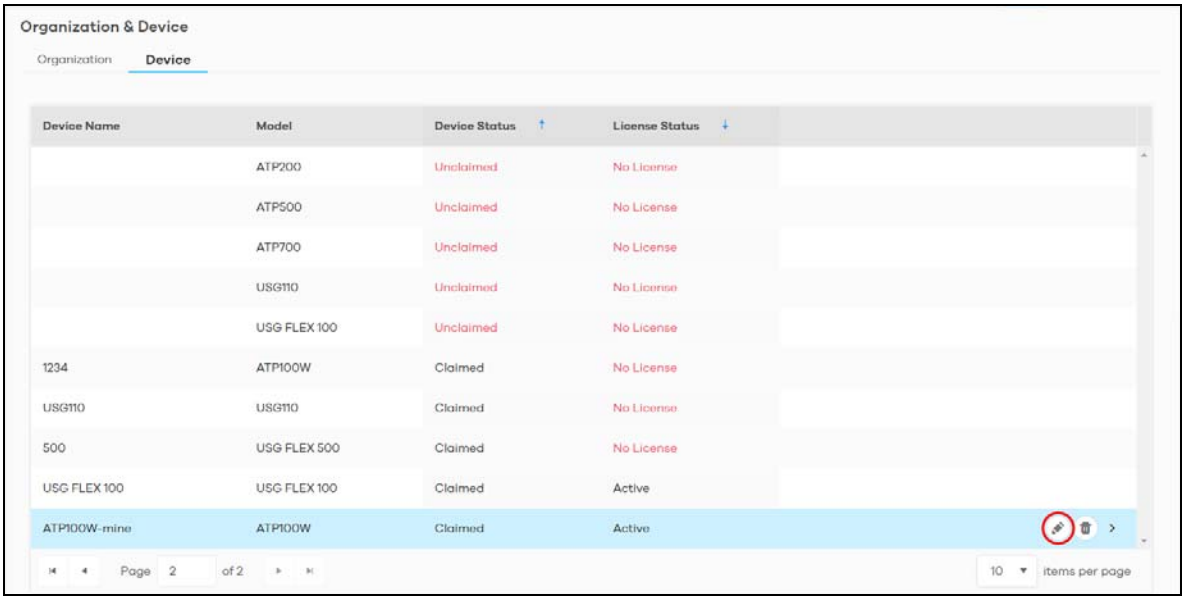


Note: You can change the level of data protection later, but all logs and reports created for the Zyxel Device up to that point will be lost.

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

6.2.2 Claimed Device

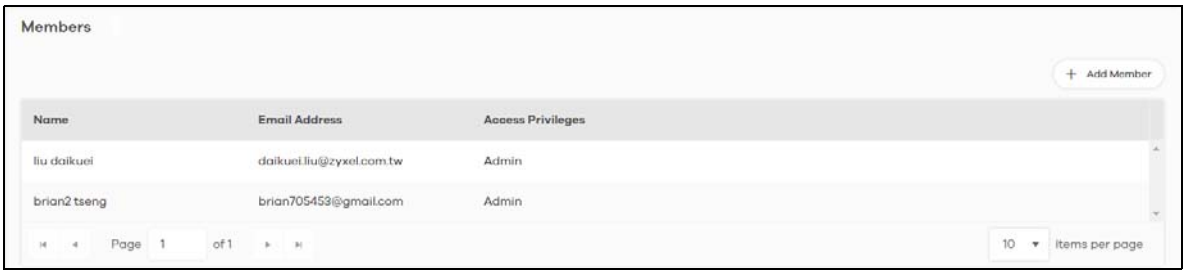
The hyperlink under **Claimed** device displays the Zyxel Devices that have been added to this organization. Click the edit icon to change the settings including the **Protection Policy**.



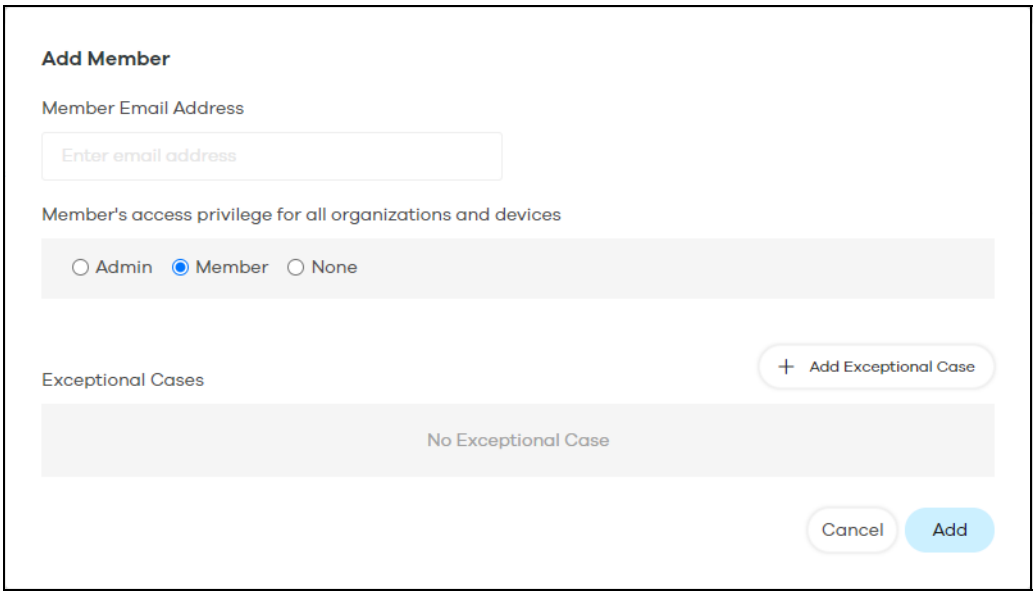
6.3 User Account

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

1 Click **Add Member**.



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



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

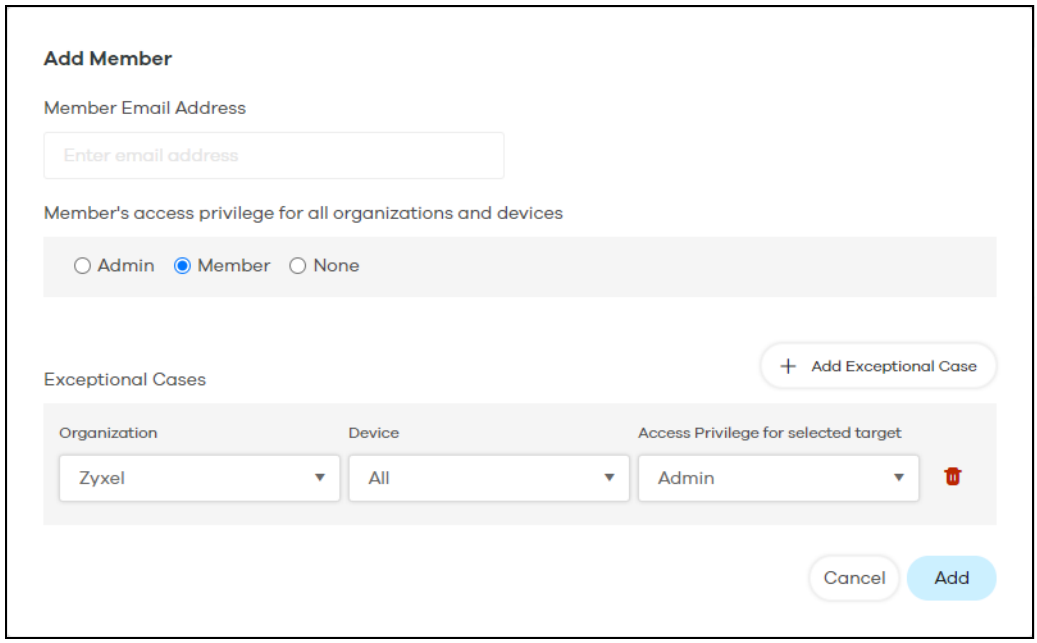
3 Select this **Member's access privilege for all organizations and devices** for all new Zyxel Devices added to this organization after the user account was created.

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

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

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

- Device
- Organization
- Access Privilege for selected target



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

4 Click **Add** when finished.

CHAPTER 7
Troubleshooting

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

I cannot access the SecuReporter portal.

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

I cannot log into the SecuReporter portal.

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

There is no data shown at SecuReporter.

- Make sure your Zyxel Device supports SecuReporter. See Section 1.1.1 on page 6 for the supported Zyxel Devices.
- Make sure the firmware version of your Zyxel Device supports SecuReporter. See Section 1.1.1 on page 6 for the supported firmware versions.
- Make sure you activated the SecuReporter license at myZyxel. See Section 1.2 on page 8 for more information.
- Make sure your license is not expired. See the User's Guide of the supported Zyxel Device for how to check your license status.
- Make sure you enabled SecuReporter on your Zyxel Device. See the User's Guide of the supported Zyxel Device for how to enable and activate SecuReporter.
- Make sure you selected the categories that you want your Zyxel Device to send to the SecuReporter portal. See the User's Guide of the supported Zyxel Device for instructions.
- Make sure you added your Zyxel Device to an organization. See Section 6.2 on page 70 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 Section 1.1 on page 6 for the Zyxel Devices that support sandboxing.

Some files types cannot be inspected through sandboxing.

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

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

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

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

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

IP Reputation does not work on IPv6 addresses.

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

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

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

I cannot add my Zyxel Device to an organization.

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

Some fields cannot be used as filters for log search.

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

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

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

Some **Security** log categories does not appear for my Zyxel Device.

URL Threat Filter, **IP Reputation**, and **Sandboxing** are only available for the ZyWALL ATP series with firmware version 4.35 and above at the time of writing.

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

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

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.

See *https://www.zyxel.com/homepage.shtml* and also *https://www.zyxel.com/about_zyxel/zyxel_worldwide.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 Corporation
- http://www.zyxel.com

Asia

China

- Zyxel Communications (Shanghai) Corp.
  Zyxel Communications (Beijing) Corp.
  Zyxel Communications (Tianjin) Corp.
- https://www.zyxel.com/cn/zh/

India

- Zyxel Technology India Pvt Ltd.
- https://www.zyxel.com/in/en/

Kazakhstan

- Zyxel Kazakhstan
- https://www.zyxel.kz

Korea

- Zyxel Korea Corp.
- http://www.zyxel.kr

Malaysia

- Zyxel Malaysia Sdn Bhd.
- http://www.zyxel.com.my

Pakistan

- Zyxel Pakistan (Pvt.) Ltd.
- http://www.zyxel.com.pk

Philippines

- Zyxel Philippines
- http://www.zyxel.com.ph

Singapore

- Zyxel Singapore Pte Ltd.
- http://www.zyxel.com.sg

Taiwan

- Zyxel Communications Corporation
- 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 BY
- https://www.zyxel.by

Belgium

- Zyxel Communications B.V.
- https://www.zyxel.com/be/nl/

- https://www.zyxel.com/be/fr/

Bulgaria

- Zyxel България
- 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/

Estonia

- Zyxel Estonia
- https://www.zyxel.com/ee/et/

Finland

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

France

- Zyxel France
- https://www.zyxel.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
- https://www.zyxel.com/it/it/

Latvia

- Zyxel Latvia
- https://www.zyxel.com/lv/lv/

Lithuania

- Zyxel Lithuania
- https://www.zyxel.com/lt/lt/

Netherlands

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

Norway

- Zyxel Communications
- 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

Russia

- Zyxel Russia
- https://www.zyxel.com/ru/ru/

Slovakia

- Zyxel Communications Czech s.r.o. organizacna zlozka
- https://www.zyxel.com/sk/sk/

Spain

- Zyxel Communications ES Ltd.
- https://www.zyxel.com/es/es/

Sweden

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

Switzerland

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

Turkey

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

UK

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

Ukraine

- Zyxel Ukraine
- http://www.ua.zyxel.com

South America

Argentina

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

Brazil

- Zyxel Communications Brasil Ltda.
- https://www.zyxel.com/br/pt/

Colombia

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

Ecuador

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

South America

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

Middle East

Israel

- Zyxel Communications Corporation
- http://il.zyxel.com/

Middle East

- Zyxel Communications Corporation
- https://www.zyxel.com/me/en/

North America

USA

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

Oceania

Australia

- Zyxel Communications Corporation
- https://www.zyxel.com/au/en/

Africa

South Africa

- Nology (Pty) Ltd.
- https://www.zyxel.com/za/en/

APPENDIX B
Legal Information

Copyright

Disclaimer

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

Viewing Certifications

Go to http://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 http://www.zyxel.com/web/support_warranty_info.php.

Registration

Register your product online to receive email notices of firmware upgrades and information at www.zyxel.com.

Open Source Licenses

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

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

Index

A

B

C

D

E

F

G

H

I

J

L

M

N

O

P

Q

R

S

T

U

V

W

Z