

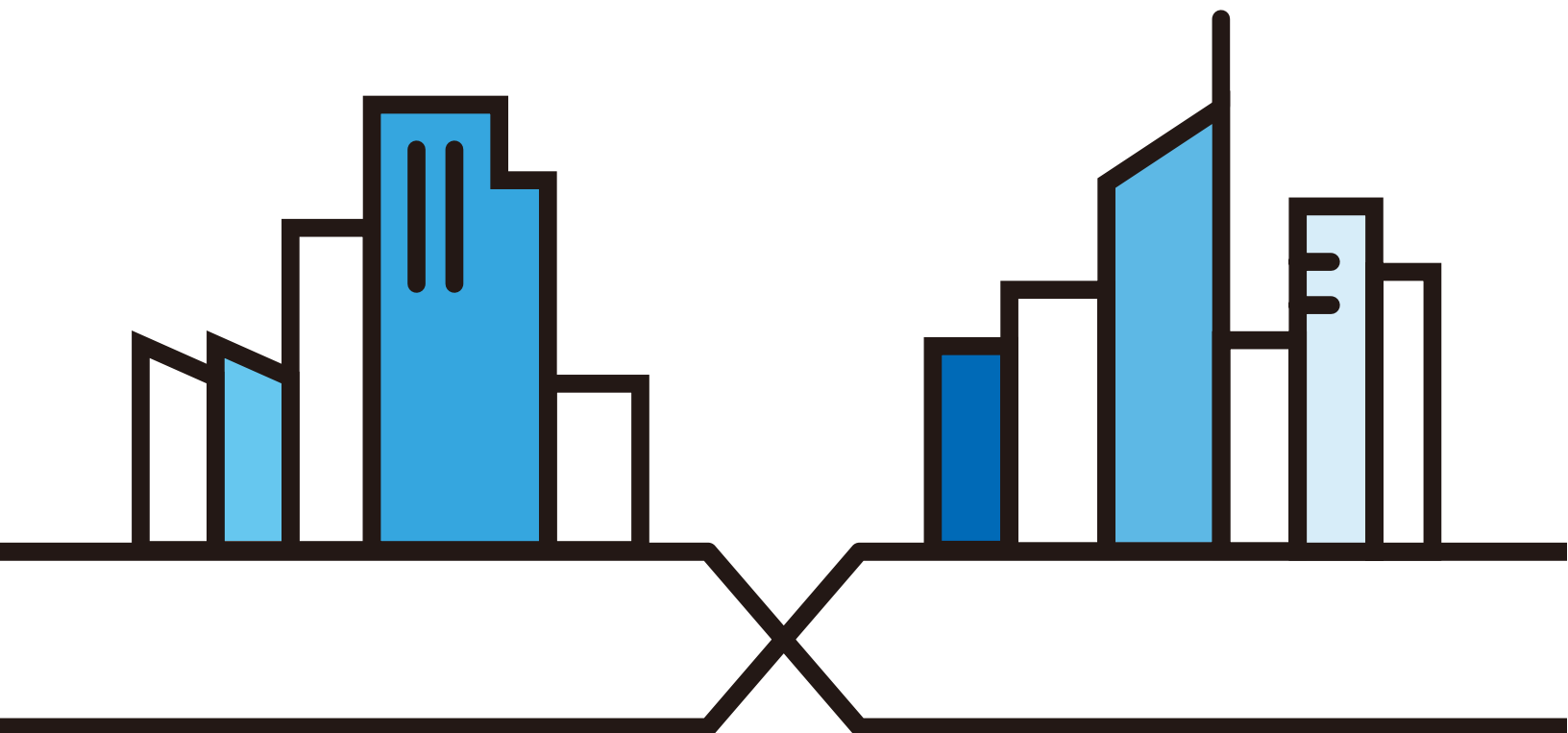
User's Guide

ZyWALL USG SecuReporter

Default Login Details

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

Version 1.4.1 12/2018



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 which you can see when you first log in to the SecuReporter on the bottom of the **Maps > Devices** screen. See [Section 1.3 on page 6](#) for details.

Related Documentation

- User's Guides

Go to support.zyxel.com to get a supported Zyxel Device User's Guide to see how to configure SecuReporter using the Web Configurator on the Zyxel Device.

Go to support.zyxel.com to get a supported Zyxel Device Command Line Interface (CLI) Reference Guide to see how to configure SecuReporter using the CLI on the Zyxel Device.

Go to support.zyxel.com 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.



Chapter 1	
Introduction	5
1.1 Overview	5
1.1.1 License Options	6
1.2 Getting Started	6
1.3 Maps > Devices	6
1.4 Map > Threat Map	7
1.4.1 Map > Threat Map > Details	8
1.5 Dashboard	10
1.6 Dashboard > Widgets	11
Chapter 2	
Analyzer.....	12
2.1 Overview	12
2.2 Analyzer Overview	13
2.3 Security Indicators	14
2.3.1 Security Indicators > Security	14
2.3.2 Security Indicators > Management	15
2.3.3 Security Indicators > Blocking	16
2.4 Users	17
2.4.1 Users > Details	18
2.5 Traffic	20
2.6 Device Details	22
Chapter 3	
Report.....	24
3.1 Overview	24
3.2 Summary Reports	24
3.3 Report Configuration	25
3.3.1 Configuration > Add Profile	27
Chapter 4	
Alerts	30
4.1 Overview	30
4.2 Alerts > Trend & Details	30
4.3 Alerts > Configuration	32
Chapter 5	
Settings.....	34
5.1 Overview	34
5.2 Organization & Devices	34
5.2.1 Add a Zyxel Device to an Organization	35
5.2.2 Claimed Device	38

5.3 User Account	38
5.4 Personal Data	39
5.4.1 User Name	39
5.4.2 E-mail Address	40
Appendix A Legal Information	41

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.

At the time of writing of this User's Guide, SecuReporter supports the following Zyxel Devices, with firmware version 4.32 and later:

- USG20-VPN
- USG20W-VPN
- USG40
- USG40W
- USG60
- USG60W
- USG110
- USG210
- ZyWALL110
- ATP200
- ATP500

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.

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.

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 1 SecuReporter Management Privileges

ROLE TYPE	SIGN IN AT MYZYXEL?	PRIVILEGES
Agent (Owner)	Yes	<ul style="list-style-type: none">• Can add/delete Zyxel Devices to/from an organization• Can add/edit organizations• Can add/edit admin/user accounts• Can configure alert notifications• Can configure dashboard widgets• Can configure analyses and reports
Admin	Yes	<ul style="list-style-type: none">• Can add/edit organizations• Can configure alert notifications• Can configure dashboard widgets• Can configure analyses and reports

Table 1 SecuReporter Management Privileges

ROLE TYPE	SIGN IN AT MYZYXEL?	PRIVILEGES
User	Yes	<ul style="list-style-type: none">• Can configure dashboard widgets• Can view analyses and report• Can configure alert notifications
None	No	<ul style="list-style-type: none">• Can receive alert notifications and reports

1.1.1 License Options

You can use SecuReporter with a free 30-day Trial license or buy a 1-year Standard license. All features are available for both licenses. 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 Getting Started

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 Device(s) 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 Device(s), follow the on-screen instructions to activate the SecuReporter license for the registered Zyxel Devices.

Once you're in the SecuReporter web portal, configure an organization with the Zyxel Device(s).

Note: See [Section 5.1 on page 34](#) for an overview of how to get started using SecuReporter.

1.3 Maps > Devices

Click **Map > Devices** to view your Zyxel Device(s) on an interactive map. The version number of your SecuReporter can be viewed at the bottom of the screen.

Figure 1 Map > Devices Screen

Click a location to display its city-level location, the device name, online status, alert status, and the IP address.

Figure 2 Click Location

Location	Device Name	Online Status	Alert	IP	✕	
Hsinchu	FT_USG110_1	●		118.163.48.108		
Hsinchu	FT_USG1900_1_New	●	!	118.163.48.108		
Hsinchu	SVD-FT-IxiaACTS-1	●		118.163.48.104		

Click this screen to open up the **Dashboard**, which displays data sent from the Zyxel Device. (Refer to [Section 1.5 on page 10](#) for information about the **Dashboard**.) An alert is a notification about a potential security problem.

On the **Devices** map, pin color indicates the status of the Zyxel Device:

Table 2 Network Sites Color Table

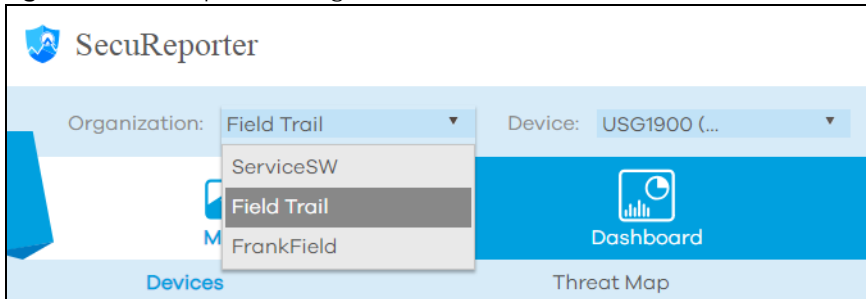
PIN COLOR	STATUS
Blue	Online
Gray	Offline

Pins also display notifications if events or alarms are triggered by a Zyxel Device at the location. To view the latest status of the Zyxel Device(s) in the network, manually refresh the page.

When there is more than one Zyxel Device in a single location, a list of Zyxel Devices will be available to choose from.

For MSSPs that manage multiple organizations, a drop-down list of organizations will be present at the top left corner of the menu bar. When an organization is selected, the Zyxel Device(s) under that organization will appear to the right.

Figure 3 SecuReporter > Organizations/Devices



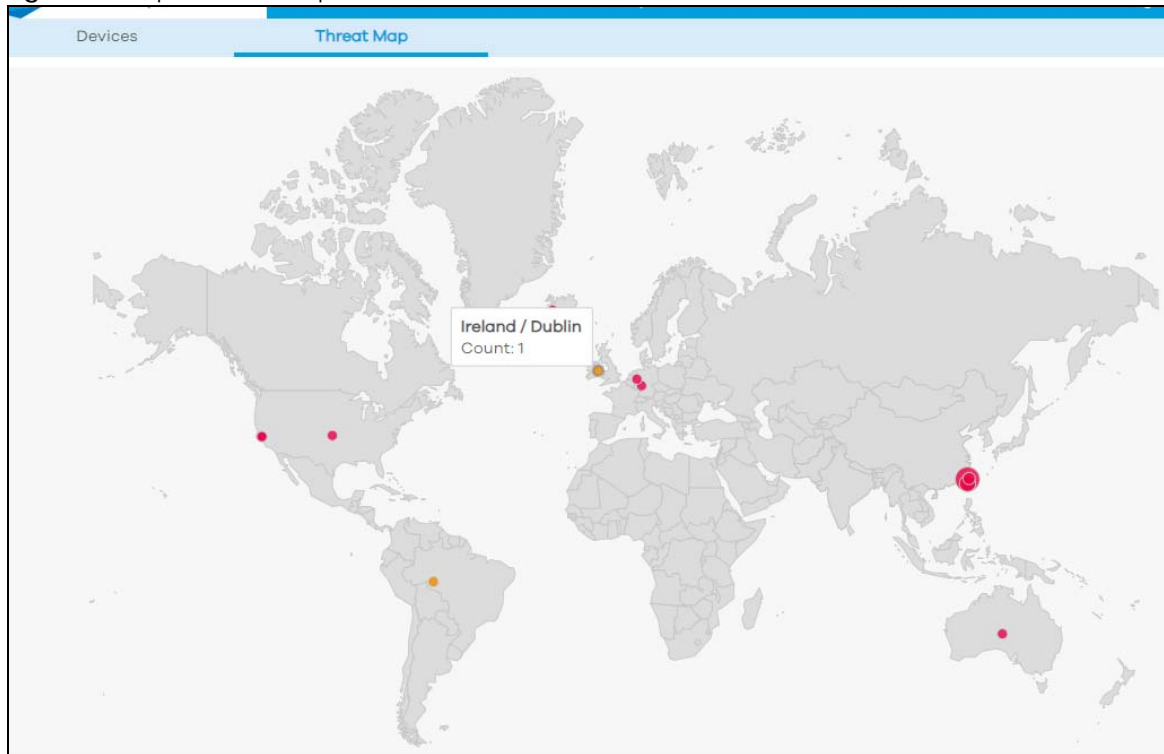
1.4 Map > Threat Map

Click **Map > Threat Map** 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 frequency of the attacks. A bigger pin means more threats.

Table 3 Threat Map Color Table

PIN COLOR	FREQUENCY
Red	Top 10 in attack frequency over the last 7 days
Orange	Other origins of threats over the last 7 days

Figure 4 Map > Threat Map

1.4.1 Map > Threat Map > Details

Click on a pin on the **Threat Map** to view more information about the threat(s) detected from that location.

Figure 5 Map > Threat Map > Details

Timestamp	Attack Type	Severity	Hits	Attack IP
2018.08.10 12:25:17	ADP	2	1	2404:6800:4008:802::2001
2018.08.10 12:23:30	ADP	2	1	2404:6800:4008:802::2003
2018.08.10 12:23:30	ADP	2	1	2404:6800:4008:802::2002
2018.08.10 12:18:00	ADP	2	1	2404:6800:4008::7
2018.08.10 12:17:59	ADP	2	1	2404:6800:4008:800::2002
2018.08.10 12:17:59	ADP	2	1	2404:6800:4008::7
2018.08.10 12:17:58	ADP	2	2	2404:6800:4008:800::2002
2018.08.10 12:17:58	ADP	2	1	2404:6800:4008::7
2018.08.10 12:17:58	ADP	2	1	2404:6800:4008:802::2006
2018.08.10 10:30:53	ADP	2	1	2404:6800:4008:802::200e
2018.08.10 08:59:46	ADP	2	1	2404:6800:4008:802::200e
2018.08.10 08:59:45	ADP	2	1	2404:6800:4008:802::200e
2018.08.09 16:39:47	ADP	2	1	2404:6800:4008:803::2016
2018.08.09 16:39:44	ADP	2	1	2404:6800:4008:802::2003
2018.08.09 16:39:44	ADP	2	2	2404:6800:4008:801::2002

Page 1 of 2

The following table describes the labels on this screen.

Table 4 Map > Threat Map > Details

LABEL	DESCRIPTION
Timestamp	This displays the year-month-date hour : minute that the threat was detected. Click to sort the table in order of the date and time that the threats were detected.
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), and spam. Click the arrow to arrange the threats by the alphabetical order of their attack type.
Severity	<p>This displays each threat's severity as represented by a number from 1 to 5 (1 = least severe, 5 = most severe). Click to order the list of threats based on their severity level.</p> <p>These are the severities as defined by the Zyxel Device.</p> <ul style="list-style-type: none"> Severe (5): These denote attacks that try to run arbitrary code or gain system privileges. High (4): These denote known serious vulnerabilities or attacks that are probably not false alarms. For example, botnets, compromised, malware, phishing & fraud sites. Botnet means the Botnet Command and Control (C&C) Server only and not the group of infected Botnet clients. Medium (3): These denote medium threats, access control attacks or attacks that could be false alarms. For example, spam sites. Low (2): These denote mild threats or attacks that could be false alarms. For example, anonymizers (a tool that attempts to make activity on the Internet untraceable). Very Low (1): These denote possible attacks caused by traffic such as Ping, trace route, ICMP queries, network errors and so on.
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.
Attack IP	This displays each threat's source IP. Click the arrow to order the threats by their source IP.

1.5 Dashboard

The **Dashboard** shows widgets with key facts about your network's security environment that were collected by SecuReporter in the last seven days, 24 hours or one hour. To change the time frame, click the drop-down list on the top right of the screen and select **Last 7 Days**, **Last Hour** or **Last 24 hours**.

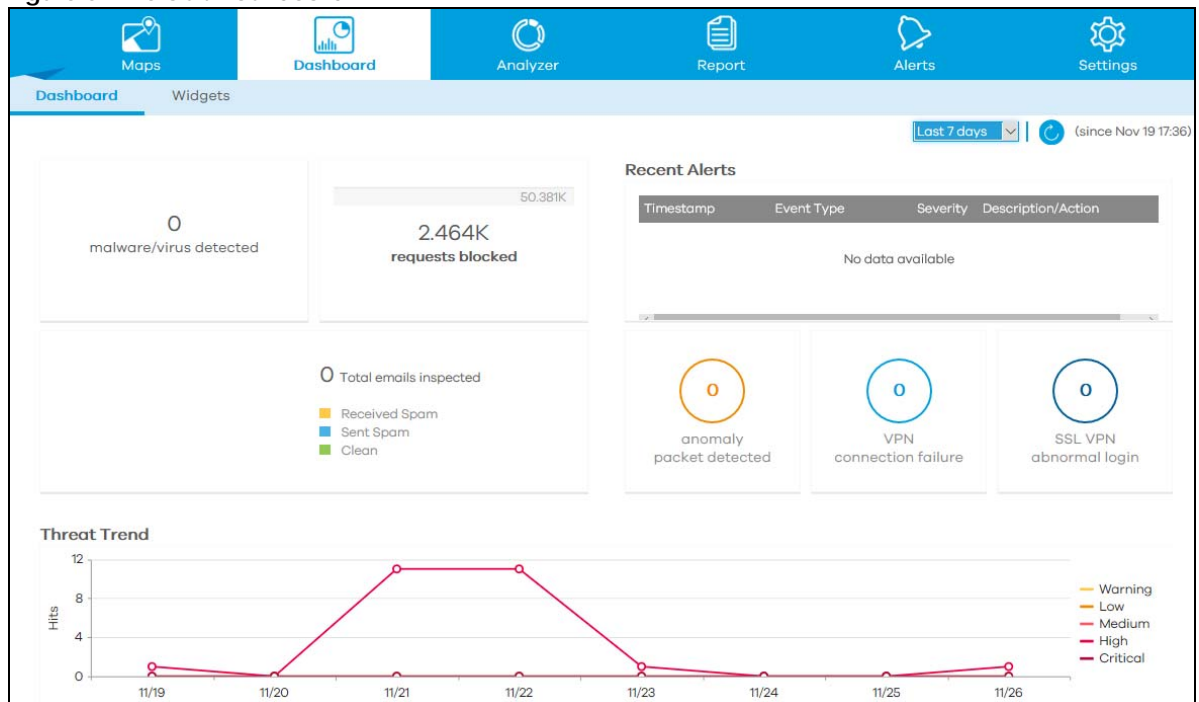
You need to create an organization with at least one Zyxel Device for information to display in the Dashboard - go to **Settings > Organization & Devices > Add Organization**.

By default, the dashboard will have the **Recent Alerts**, **Threat Trend**, and a widget showing total malware/viruses detected, requests blocked and e-mail inspection details. Go to **Dashboard > Widgets** if you want to display other widgets here.

Widgets are miniature views of SecuReporter's data visualizations, the full versions of which are available under the **Analyzer** tab. For descriptions of each widget, see [Section 1.6 on page 11](#).

Drag and drop widgets to rearrange them on the screen.

Figure 6 Default Dashboard



The following table describes the widgets on the default dashboard:

Table 5 Default Dashboard

LABEL	DESCRIPTION
Recent Alerts	This is an overview of the latest alerts sent to administrators of a network. A table provides an at-a-glance overview of the most recent alerts. Circle counters show the number of anomaly packets detected, VPN connection failures, and SSL VPN abnormal logins over a specified interval.

Table 5 Default Dashboard

LABEL	DESCRIPTION
Threat Trend	This graph shows changes in the number of threats that a network encounters over a selected time frame. Each line represents the trend in threats of a specific severity level. All lines show by default. Click on a color block to hide its corresponding trend line.
Malware/virus detected, requests blocked and total emails inspected	This widget shows the total malware/viruses detected, requests blocked and e-mail inspection details. Click on individual statistics in the widget to drill down to information generated by the SecuReporter Analyzer .

1.6 Dashboard > Widgets

To customize the information on your dashboard, click **Dashboard > Widgets** and select from the list of widgets to suit your needs.

Figure 7 Dashboard > Widgets

Security Services	Traffic
<input type="checkbox"/> Most Popular Websites	<input type="checkbox"/> Top Users with Most Bandwidth
<input type="checkbox"/> Most Popular Website Categories	<input type="checkbox"/> Top Destination Countries
<input type="checkbox"/> Top Blocked Websites	<input checked="" type="checkbox"/> Top Applications
<input checked="" type="checkbox"/> Top Blocked Destination Countries	<input checked="" type="checkbox"/> Top Destination Ports
<input type="checkbox"/> Top Malware/Virus Detected	
<input type="checkbox"/> Anomaly Packet Trend	
<input checked="" type="checkbox"/> IDP	
<input type="checkbox"/> Top Spam Received	
<input type="checkbox"/> Top Spam Sent	
<input type="checkbox"/> Top Blocked Applications	
<input type="checkbox"/> APP Patrol	
<input type="checkbox"/> Most Popular Applications	

Save Cancel

CHAPTER 2

Analyzer

2.1 Overview

Analyzer is a set of charts, tables, and other visualizations of data collected from Zyxel Device(s). Analyzer provides a big-picture overview of network activity, while making it easy to “drill down” into granular detail on what users are doing.

In the **Analyzer** section, the charts can be clicked to reveal event records, which are clickable to display more details. Charts can also be connected to the Dashboard as widgets (see [Section 1.6 on page 11](#)).

In most cases, you can choose to analyze data collected over one of three time frames:

- Last hour
- Last 24 hours
- Last 7 days

Analyzer contains the following tabs:

- Security Indicators
- Traffic
- Users
- Device Details

2.2 Analyzer Overview

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

Table 6 Analyzer Overview

TAB	DATA
Security Indicators	<ul style="list-style-type: none"> • Security <ul style="list-style-type: none"> • Threat Trend • Anomaly Packet Trend (ADP) • Top Malware/Virus Detected • IDP • Top Spam Received • Top Spam Sent • Top Security Threat Website Categories (for ZyWALL USG series only at the time of writing of this manual) • Top Security Threat Websites (for ZyWALL USG series only at the time of writing of this manual) • Management <ul style="list-style-type: none"> • Most Popular Website Categories • Most Popular Websites • Most Popular Applications • APP Patrol • Blocking <ul style="list-style-type: none"> • Top Blocked Applications • Top Blocked Websites • Top Blocked Destination Countries
Traffic	<ul style="list-style-type: none"> • Top Users with Most Bandwidth • Top Destination Countries • Top Applications • Top Destination Ports

Table 6 Analyzer Overview

TAB	DATA
Users	<ul style="list-style-type: none"> • Username Search • Security Events • Application Usage • Website Usage • Top Destination Countries • Login/Logout History • Traffic Upload/Download Usage Trend
Device Details	<ul style="list-style-type: none"> • Device Information • Security Service Licenses • CPU/Memory Usage Trend • Concurrent Sessions • GE1-8 Traffic Usage Trend • VLAN14-20 Traffic Usage Trend

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

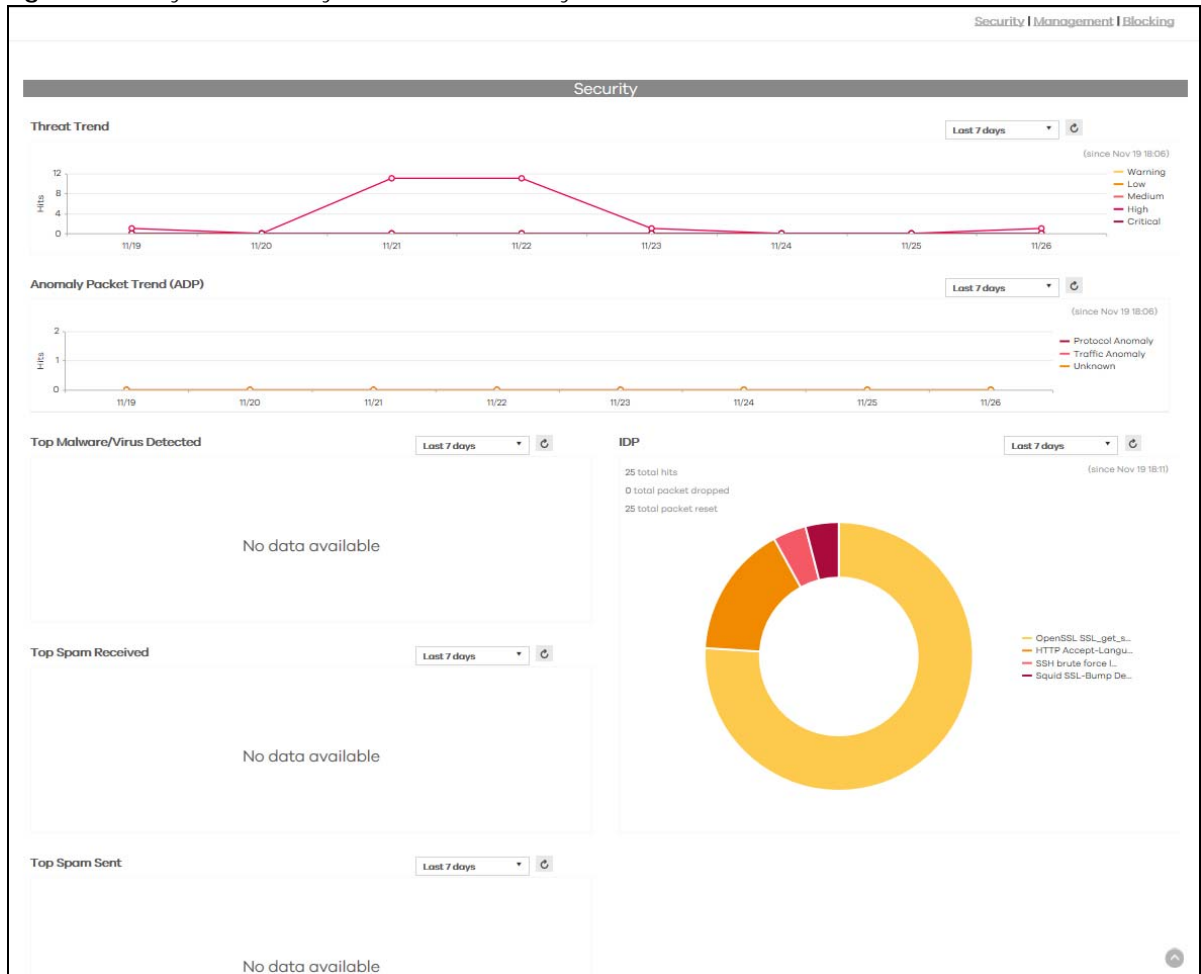
2.3 Security Indicators

Security Indicators data visualizations are categorized as:

- Security
- Management
- Blocking

2.3.1 Security Indicators > Security

The following figure shows the **Analyzer > Security Indicators > Security** data visualizations.

Figure 7 Analyzer > Security Indicators > Security

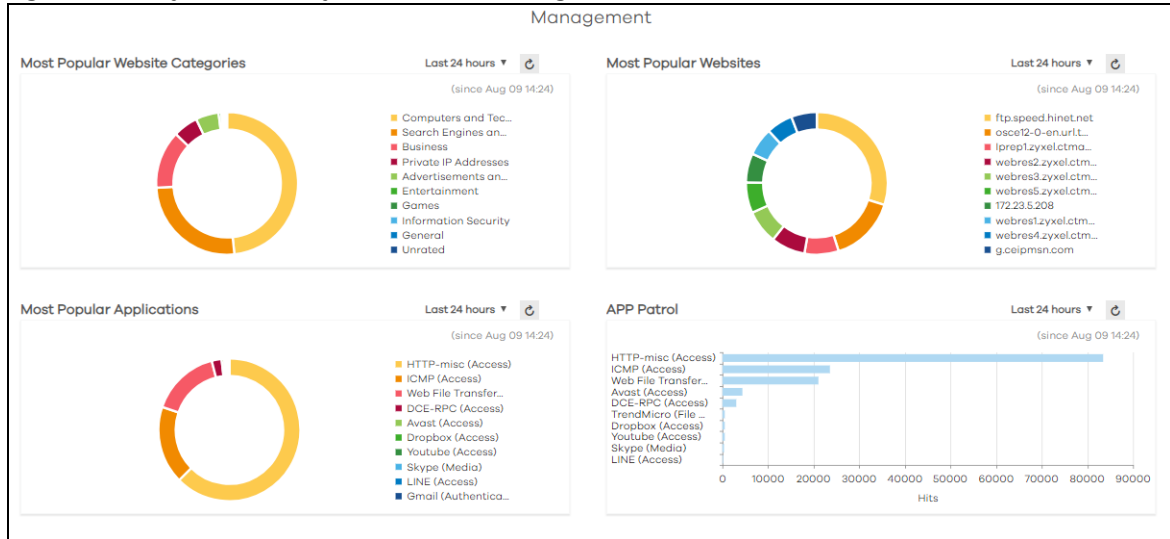
The following table describes the labels on the **Analyzer > Security Indicators > Security** screen.

Table 7 Analyzer > Security Indicators > Security

LABEL	DESCRIPTION
Threat Trend	<p>This chart displays patterns in threats by severity level.</p> <p>Move your cursor over a trend line to display the number of threats encountered over time, and click on any line to display details. To hide the trend line for a severity level, click on its corresponding color block on the right of the chart.</p> <p>These are the severities as defined by the Zyxel Device.</p> <ul style="list-style-type: none"> Severe (5): These denote attacks that try to run arbitrary code or gain system privileges. High (4): These denote known serious vulnerabilities or attacks that are probably not false alarms. For example, botnets, compromised, malware, phishing & fraud sites. Medium (3): These denote medium threats, access control attacks or attacks that could be false alarms. For example, spam sites. Low (2): These denote mild threats or attacks that could be false alarms. For example, anonymizers (a tool that attempts to make activity on the Internet untraceable). Very Low (1): These denote possible attacks caused by traffic such as Ping, trace route, ICMP queries, network errors and so on.
Anomaly Packet Trend (ADP)	<p>This chart displays patterns in anomalies detected by the Zyxel Device(s). Anomalies are based on violations of protocol standards (RFCs – Requests for Comments) or abnormal flows such as port scans.</p> <p>Click to display details about the traffic anomalies, including when they were detected, their source IP, user, and type.</p>
Top Malware/Virus Detected	<p>This chart displays the most common malware and viruses detected and blocked by the Zyxel Device.</p> <p>Click to display details about the specific websites that were blocked.</p>
IDP	<p>This chart displays malicious or suspicious packets detected by IDP in the Zyxel Device(s). IDP (Intrusion, Detection and Prevention) uses signatures to detect malicious or suspicious packets to protect against network-based intrusions.</p> <p>Click to display details about the intrusions, including the top 10 users affected.</p>
Top Spam Received	<p>This chart displays the most common traffic classified as spam received by the Zyxel Device(s).</p> <p>Click to display details about the spam, including their top 10 recipients.</p>
Top Spam Sent	<p>This chart displays the most common traffic classified as spam sent from the Zyxel Device(s).</p> <p>Click to display details about the spam traffic source.</p>
Top Security Threat Website Categories	<p>This chart displays the most common types of threats posed by websites blocked by the Zyxel Device(s). Threat categories include Malware, Spam Sites, Anonymizers, Phishing and Fraud, Botnets, and Parked Domains. Botnet means the Botnet Command and Control (C&C) Server only and not the group of infected Botnet clients.</p> <p>Click to display details about the specific websites that were blocked.</p>
Top Security Threat Websites	<p>This chart displays the most common types of threats posed by websites blocked by the Zyxel Device.</p> <p>Click to display details about the specific websites that were blocked.</p>

2.3.2 Security Indicators > Management

The following figure shows the **Analyzer > Security Indicators > Management** data visualizations.

Figure 8 Analyzer > Security Indicators > Management

The following table describes the labels on the **Analyzer > Security Indicators > Management** screen.

Table 8 Analyzer > Security Indicators > Management

LABEL	DESCRIPTION
Most Popular Website Categories	This chart displays the most common website categories accessed via the Zyxel Device(s). Click to display details about the specific websites that were blocked.
Most Popular Websites	This chart displays the most common websites accessed via the Zyxel Device(s). Click to display details about the websites accessed and the users logged in at the time of access.
Most Popular Applications	This chart displays the most commonly used applications accessed via the Zyxel Device(s). Click to display details about the applications accessed and the users logged in at the time of access.
APP Patrol	This chart displays the most frequently visited applications 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). Click to display details about the traffic detected by APP Patrol .

2.3.3 Security Indicators > Blocking

The following figure shows the **Analyzer > Security Indicators > Blocking** data visualizations.

Figure 9 Analyzer > Security Indicators > Blocking

The following table describes the labels on the **Analyzer > Security Indicators > Blocking** screen.

Table 9 Analyzer > Security Indicators > Blocking

LABEL	DESCRIPTION
Top Blocked Applications	This chart displays the 10 applications that were blocked the most frequently by the Zyxel Device(s). Click to display details about the specific applications that were blocked.
Top Blocked Websites	This chart displays websites most often blocked by the Zyxel Device(s). Click to display details about the websites accessed and the users logged in at the time of access.
Top Blocked Destination Countries	This chart displays a list of countries to which the most Internet traffic was denied, along with the number of hits per destination country. Click to display details about the outbound traffic blocked by the Zyxel Device(s).

2.4 Users

Analyzer allows administrators to look up network activity by user. A user-aware user is a user who must log into 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 **Analyzer > Users**.

In the field at the top 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 10 Analyzer > Users

The screenshot shows the 'Users' tab in the Analyzer interface. At the top, there are three tabs: 'Traffic', 'Users' (selected), and 'Device Details'. Below the tabs is a 'Username Search' section with a text input field and a 'Search' button. Below the search bar is a table with the following data:

	Username
1	ZT02708
2	ZT01801
3	admin
4	ZT02531
5	ZT02646

At the bottom of the table, there is a pagination control showing 'Page 1 of 1' with navigation arrows.

2.4.1 Users > Details

Click on 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/logout history.

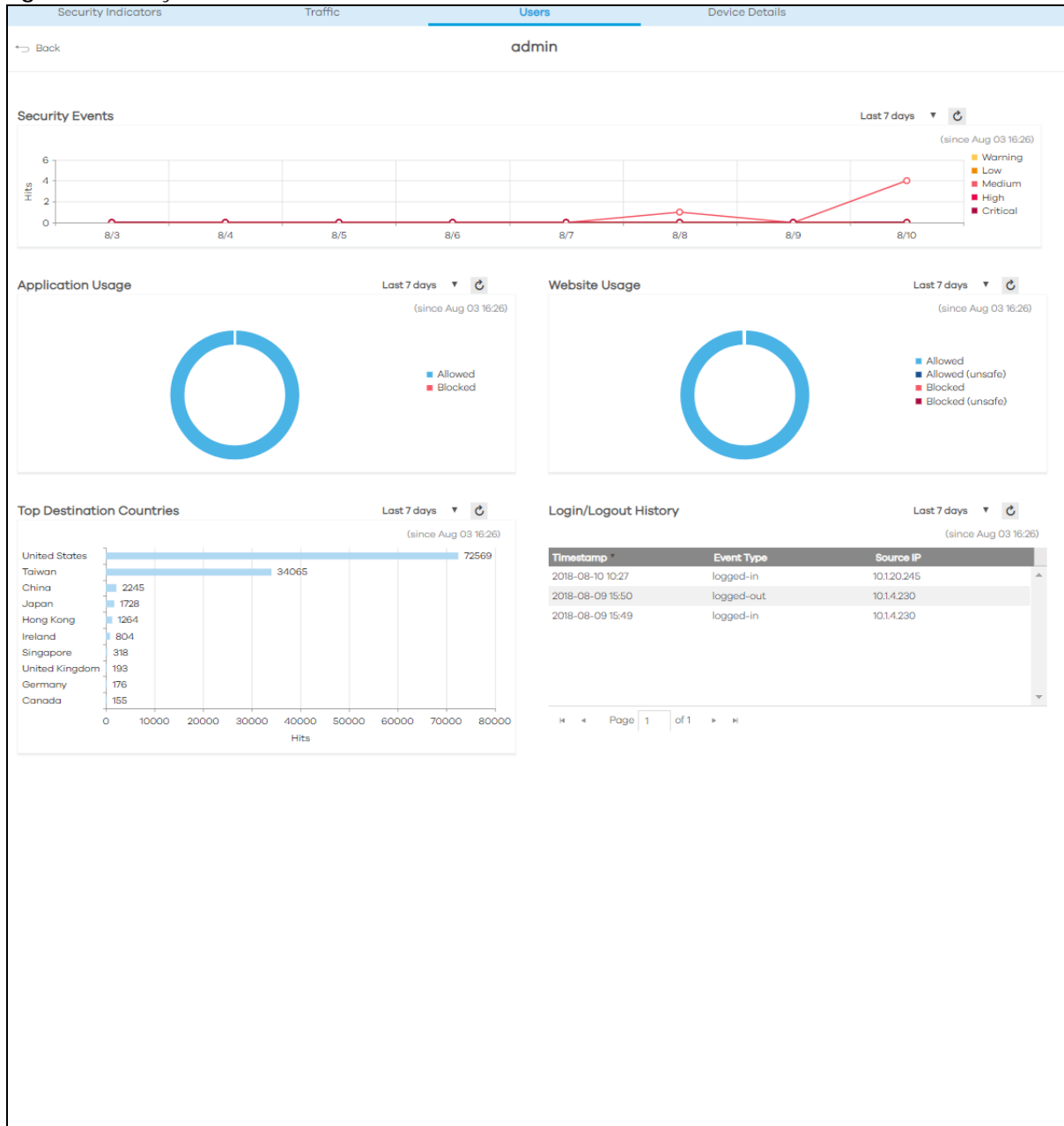
Security events include anomalies, app patrol, malware, spam, threats (IDP), unsafe websites, and web protection (websites blocked by content filter policies). The following figure shows severity levels for security events.

Figure 11 Security Events Severity Levels

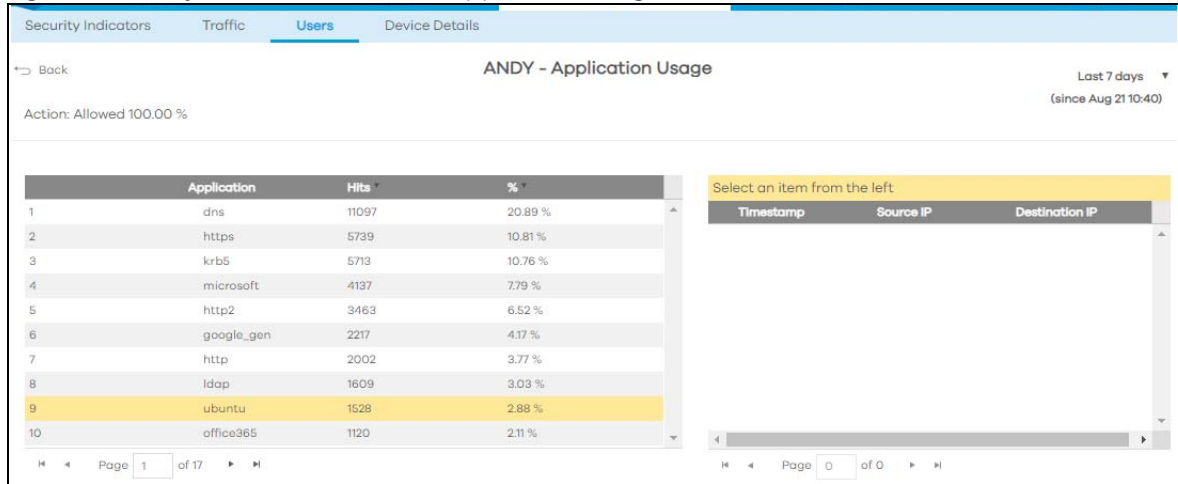
Security Event	Severity Definition
IDP	IDP: highest is 5, lowest is 1 Severity from 1~5
Malware	severity 4
Spam	Severity 3
unsafe website access	For these categories, severity is level 4 <ul style="list-style-type: none"> Botnets Compromised Malware Phishing & Fraud
	• Spam Sites : severity 3
	• Anonymizers : severity 2
	• Network Errors: severity 1
anomaly	• severity 2

Select a **Username** in **Analyzer > Users** to display the following figure.

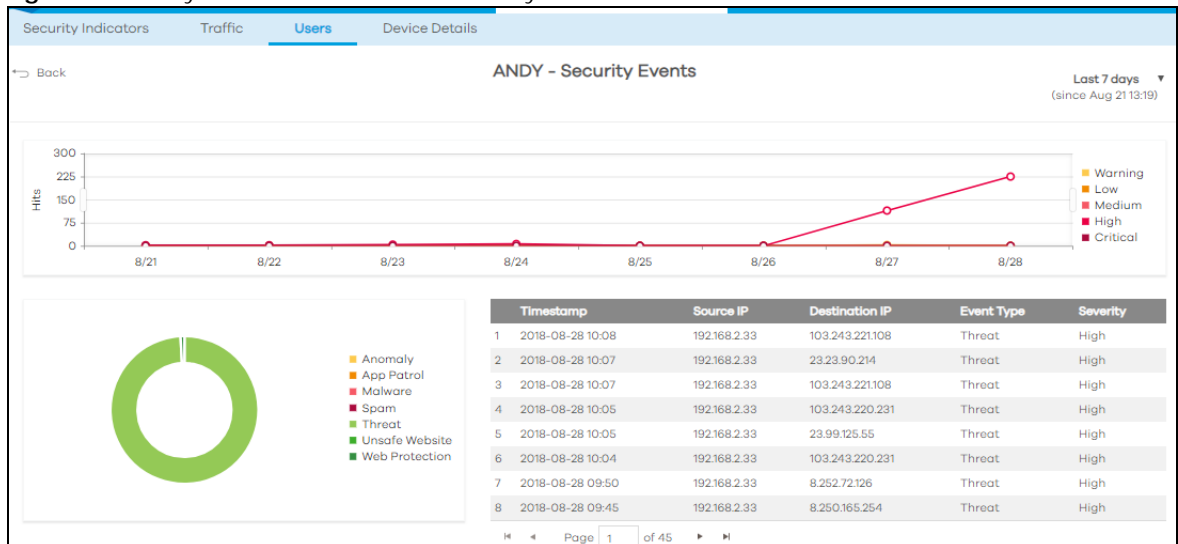
Figure 12 Analyzer > Users > Details



Click on 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 13 Analyzer > Users > Details > Application Usage

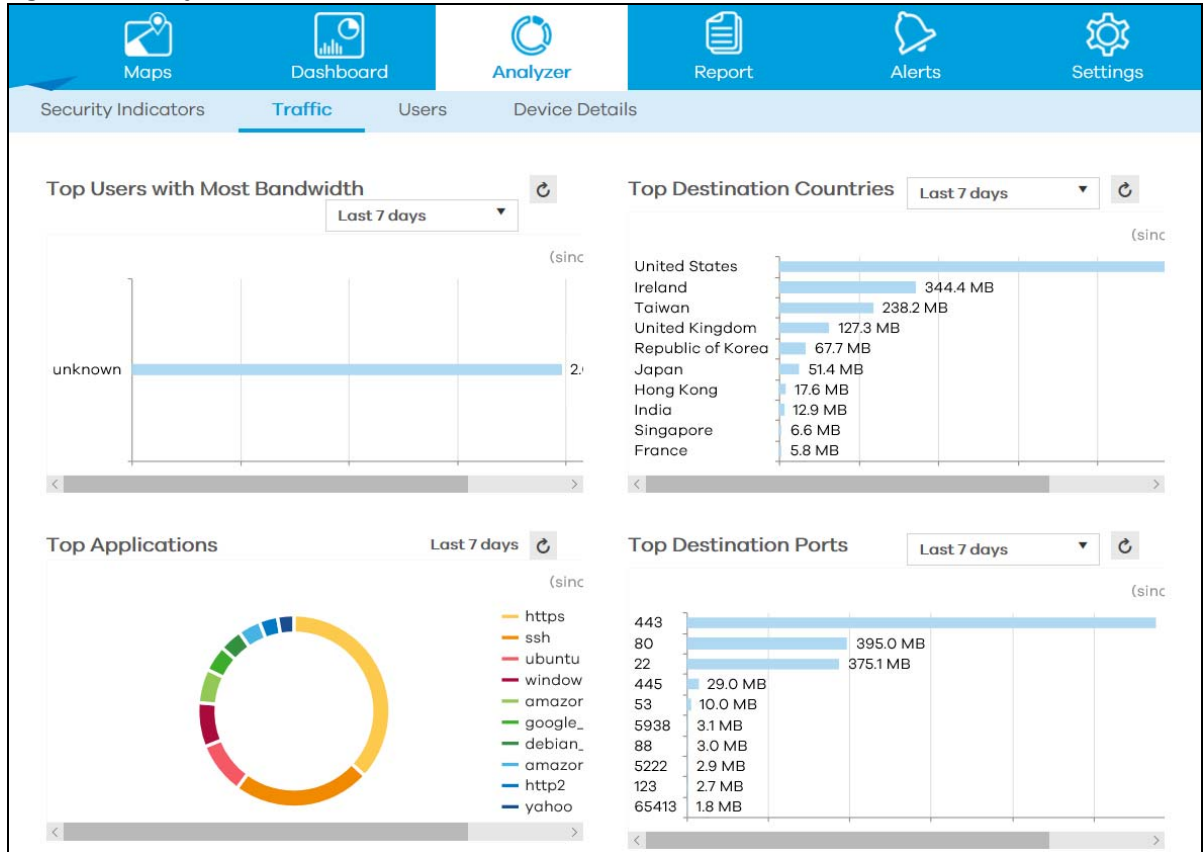
The following figure shows details on security events through the selected Zyxel Device for this user.

Figure 14 Analyzer > Users > Details > Security Events

2.5 Traffic

Click **Analyzer > Traffic** to view insights about the network's traffic flow.

Figure 15 Analyzer > Traffic



The following table describes the labels on this screen.

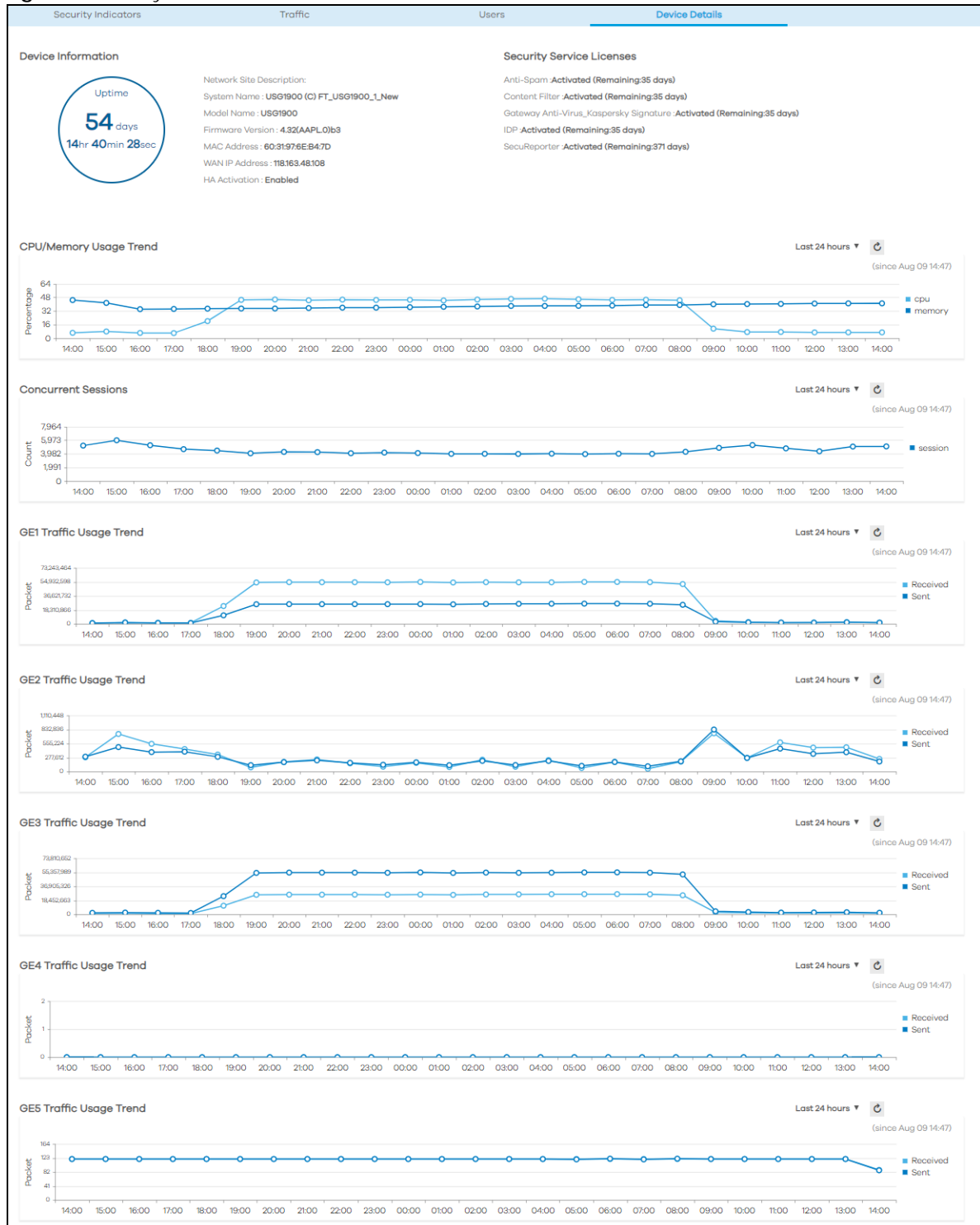
Table 10 Analyzer > Traffic

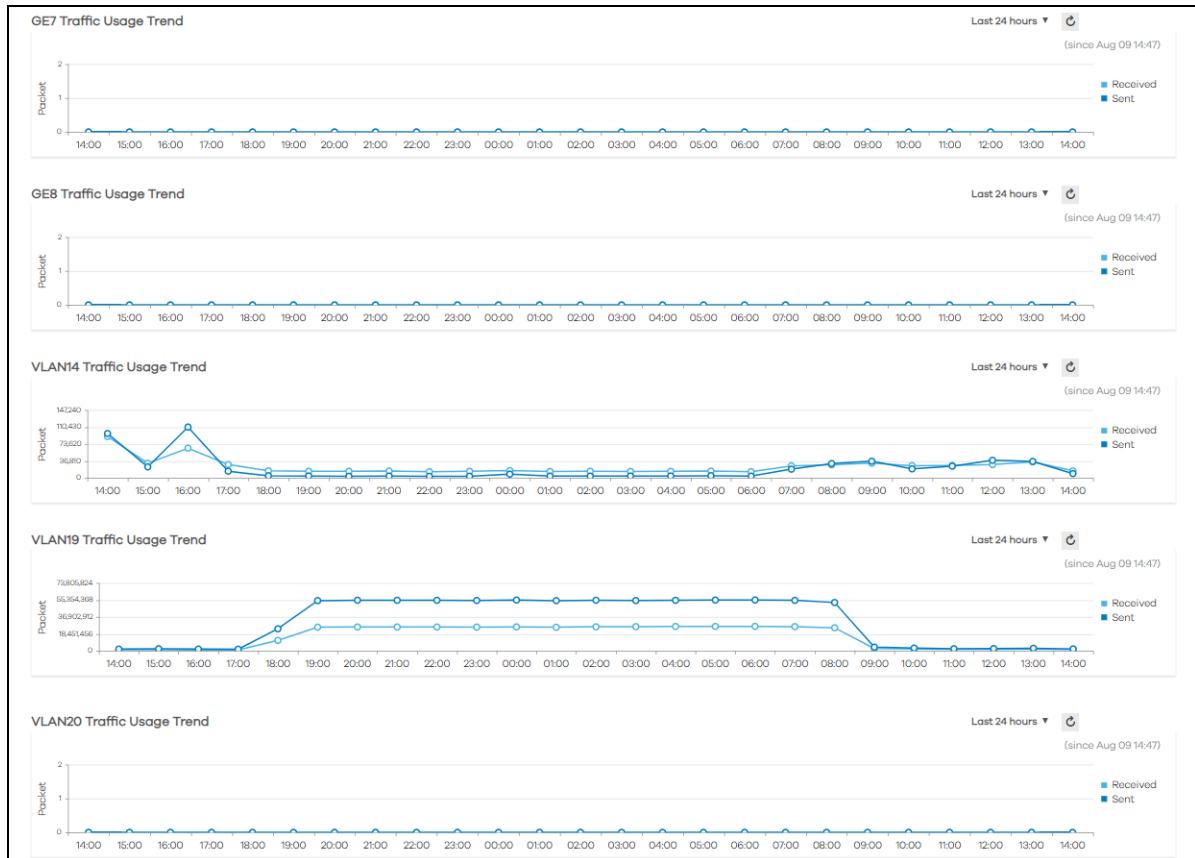
LABEL	DESCRIPTION
Top Users with Most Bandwidth	<p>This displays the top users of bandwidth on the network over a selected time frame, which is 7 days by default.</p> <p>Click to display details about a user's bandwidth usage, including upload and download volumes.</p>
Top Destination Countries	<p>This displays the countries that received the most data traffic from Zyxel Device(s) over a selected time frame.</p> <p>Click to display details about the users driving the outgoing traffic.</p>
Top Applications	<p>This displays the network applications with the greatest bandwidth usage over a selected time frame, which is 7 days by default.</p> <p>Click to display details including total forwarded data, dropped data, rejected data, and inbound/outbound kbps.</p>
Top Destination Ports	<p>This lists the top destination ports by bandwidth usage over a specified time frame, which is 7 days by default.</p> <p>Click to display details about the ports, including upload/download data volume and user information.</p>

2.6 Device Details

Click **Analyzer > Device Details** to see the status of individual Zyxel Device(s), including its connection status, activated security service licenses, and usage statistics.

Figure 16 Analyzer > Device Details





CHAPTER 3

Report

3.1 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 your own logo, title, 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 two time frames:

- Last 24 hours
- Last 7 days

Report contains the following tabs:

- Summary
- Configuration

3.2 Summary Reports

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

Figure 17 Report > Summary Reports

Timestamp	Title	Report Type	Report Period	Action
1 2018-11-27 00:26	Zyxel Security Report	Daily	2018-11-26-2018-11-27	View Download Email Delete
2 2018-11-26 00:27	Zyxel Security Report	Daily	2018-11-25-2018-11-26	View Download Email Delete
3 2018-11-25 00:28	Zyxel Security Report	Weekly	2018-11-18-2018-11-25	View Download Email Delete
4 2018-11-25 00:27	Zyxel Security Report	Daily	2018-11-24-2018-11-25	View Download Email Delete
5 2018-11-24 00:30	Zyxel Security Report	Daily	2018-11-23-2018-11-24	View Download Email Delete
6 2018-11-23 00:28	Zyxel Security Report	Daily	2018-11-22-2018-11-23	View Download Email Delete
7 2018-11-22 00:18	Zyxel Security Report	Daily	2018-11-21-2018-11-22	View Download Email Delete
8 2018-11-21 00:27	Zyxel Security Report	Daily	2018-11-20-2018-11-21	View Download Email Delete
9 2018-11-20 00:23	Zyxel Security Report	Daily	2018-11-19-2018-11-20	View Download Email Delete
10 2018-11-19 00:27	Zyxel Security Report	Daily	2018-11-18-2018-11-19	View Download Email Delete

Page 1 of 7 10 Items per page

The following table describes the labels on this screen.

Table 11 Report > Summary Reports

LABEL	DESCRIPTION
Timestamp	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 the Configuration tab > Report Profile > Report Title .
Report Type	This displays the type of report as configured in the Configuration tab > Report Profile > Type . <ul style="list-style-type: none"> Daily Weekly
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.
Action	Click View to display the Title , Organization , Device and the Report Period of a report. Click Download 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. Click Email to send a report in PDF format to the designated e-mail recipient(s). Use a comma (,) but without space after the comma to separate the e-mail addresses. Otherwise, you will get a multiple e-mail format error message. A maximum of 30 e-mail recipients only is allowed. Click Delete to remove a report from the list. Click OK to confirm the deletion when the warning window appears.
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 20/50/100 items per page.

3.3 Report Configuration

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

Figure 18 Report > Configuration



The following table describes the labels on this screen.

Table 12 Report > Configuration

LABEL	DESCRIPTION
Choose a logo for the report	
Enable a custom logo	Click to enable the display of a logo for a report profile.
Select Files	Click this button to browse for the location of the image file to be used as your report logo. <ul style="list-style-type: none"> JPG, JPEG, PNG, BMP and GIF are the allowed file formats of the image file. Maximum image file size is 100KB. Otherwise, you will get a File size too large error message.
#	This displays the index number of an existing report profile.
Status	This displays the status of a report profile, whether enabled (blue dot) or disabled (gray dot), as selected in the Enable field of the Report Profile screen. Click the Edit button under the Action column to change the status.
Profile Name	This displays the name of a report profile, as entered in the Profile Name field of the Report Profile screen. Click the Edit button under the Action column to change the name.
Title	This displays the title of a report profile, as entered in the Report Title field of the Report Profile screen. Click the Edit button under the Action column to change the title.
Type	This displays the type of report Daily or Weekly as selected in the Type field of the Report Profile screen. Click the Edit button under the Action column to change the report type.
Action	Click Edit to configure a report profile. See Section 3.3.1 on page 27 for a description of the fields. See also Section on page 12 for a description of the items in the Selected Widgets box. Click Delete to remove a report profile. When the next window appears click OK to confirm the deletion. If at present, you only have a Daily/Weekly report profile, click Duplicate to quickly create a Weekly/Daily report profile. And then just change the Type field.
Add Profile	Click Add Profile to create a new report profile. See Section 3.3.1 on page 27 for details.

3.3.1 Configuration > Add Profile

Click **Add Profile** in the **Report > Configuration** screen to create a new report profile and who to send it to.

Figure 19 Report > Configuration > Add Profile

The following table describes the labels on this screen.

Table 13 Report > Configuration





LABEL	DESCRIPTION
Enable	Click this to enable (activate)  or disable (deactivate)  the report profile.
Type	Select the frequency of the report generation. <ul style="list-style-type: none"> • Daily • Weekly
Profile Name	This field allows you to enter a descriptive name for the report profile (for example Daily Report or Weekly Report). Up to 255 characters are allowed for the Profile Name including special characters (~!@#\$\$%^&*()_+{} :~<>?-=[]\';',./).
Report 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 Report Title including special characters (~!@#\$\$%^&*()_+{} :~<>?-=[]\';',./).
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 (~!@#\$\$%^&*()_+{} :~<>?-=[]\';',./).

Table 13 Report > Configuration

LABEL	DESCRIPTION
Send report to device's agent and admin	<p>Select the check box to enable the sending of a report in PDF format to the Zyxel Device's agent and admin only. Refer to Section Table 1 on page 6 for the privileges of agent and admin.</p> <p>Note: The check box must not be selected if agent and admin do not wish to receive the report via e-mail. A summary of activities over the selected period of time is still generated.</p>
Additional recipients (separated by commas without space)	<p>This field allows you to enter the report's designated e-mail recipient(s) other than the Zyxel Device's agent and admin. Use a comma (,) to separate the e-mail addresses with no space in between two e-mail addresses. A maximum of 30 e-mail recipients is allowed. (Example: email1@zyxel.com,email2@zyxel.com)</p>
Widgets	<p>The widgets are the security services and traffic indicators that you can select to be included in the report profile. Refer to Section on page 12 for a description of the widgets in the Available Widgets box.</p> <p>Highlight an Available Widgets and click the right arrow  to move it to the Selected Widgets box. You can also double-click an item and it will automatically move over to the other side.</p> <p>Likewise, highlight a Selected Widgets and click the left arrow  to move it to the Available Widgets box. Thus, removing the item from the report profile. You can also double-click an item and it will automatically move over to the other side.</p>
Save	Click Save to save your changes.
Cancel	Click Cancel to restore your previously saved settings.

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 Alerts > Trend & Details

To see the alerts that have been raised by SecuReporter, click **Alerts > Trend & Details**.

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 right.

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 **Timestamp**, **Category**, **Event Type**, **Severity** and **Description/Action**, click on the labels of the **Alert History** table.

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

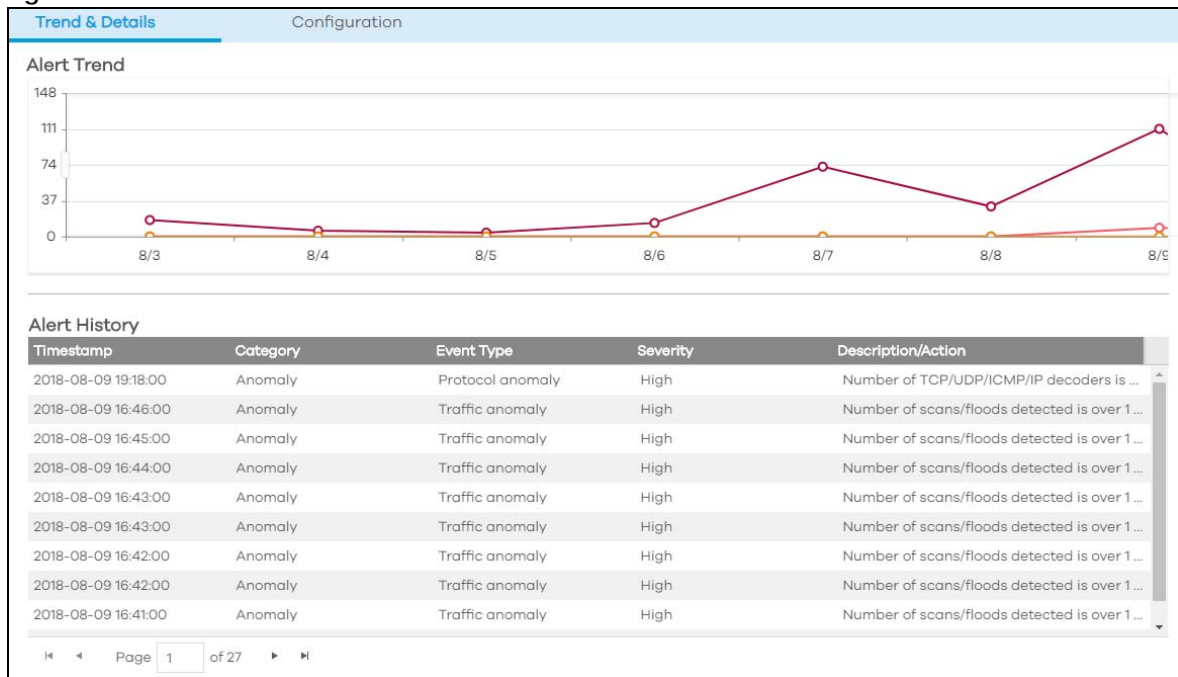
Table 14 Event Categories, Types And Criteria

CATEGORY	EVENT TYPES	CRITERIA
Network Security	Attack counts	Number of highest severity attacks greater than the threshold within {x} minutes
Network Security	Attack counts	Number of attacks greater than the threshold within {x} minutes
Network Security	Malware/virus detection	Malware/virus attack count greater than the threshold within {x} minutes
Network Security	Malware/virus detection	Number of times the same malware/virus is detected greater than the threshold within {x} minutes
Network Security	Alert counts	Number of alerts greater than the threshold

Table 14 Event Categories, Types And Criteria (continued)

CATEGORY	EVENT TYPES	CRITERIA
Device	Online status	Device offline for more than {threshold} minutes
Device	Reboot	Reboot
Device	Concurrent sessions	Session numbers greater than the {threshold}%
Anomaly	Login failure	Number of login failures over threshold within {x} minutes
Anomaly	Traffic anomaly	Number of scans/floods detected greater than the threshold within {x} minutes
Anomaly	Protocol anomaly	Number of TCP/UDP/ICMP/IP decoders greater than the threshold within {x} minutes

Figure 20 Alerts > Trend & Details



The following table describes the labels on this screen.

Table 15 Alerts > Trend & Details

LABEL	DESCRIPTION
Alert Trend	<p>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:</p> <p>High severity - Events that are exceptionally harmful, such as attacks by viruses [OR: 10 potential malware attacks within 5 minutes?]</p> <p>Medium severity - Events that could collect users' personal information or adversely affect the network [OR: 2 potential malware or virus attacks within 15 minutes?]</p> <p>Low severity - Events that usually have no adverse effect on a network.</p> <p>Trend lines for all security classifications appear on the graph by default. Click on a color block to hide its corresponding trend line.</p>
Alert History	This table shows a list of recent security events.
Timestamp	This displays the year-month-date hour:minute that the threat occurred. Click to sort the table in order of the date and time that the alerts were triggered.

Table 15 Alerts > Trend & Details

LABEL	DESCRIPTION
Category	Select to group 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. Click to order the alerts by the type of threat that occurred.
Severity	This displays the severity level as outlined in Table 4 on page 9 .
Description/Action	This displays the reason for the alert and the action taken.

4.3 Alerts > Configuration

Configure alert settings, such as recipients, e-mail subject, event severity levels to e-mail, and event triggering thresholds in the **Alerts > Configuration** screen.

Figure 21 Alerts > Configuration

Configuration

Email Notification ☐ Off

Email Title

Description

Event Severity
☐ High ☐ Medium ☐ Low

Email Group

User Account

- svd1.ft@gmail.com
- frank.liao@zyxel.com.tw
- email@grr.la
- vic.chen@zyxel.com.tw
- mei.chan@zyxel.com.tw
- johng@zyxel.com.tw

Email Recipients

Alerts Configuration

Category	Event Type	Alert Criteria	Severity	Threshold
Network Security	Attack counts	Number of highest severity attacks > threshold within 5 minutes	High	1 counts
Network Security	Attack counts	Number of attacks > threshold within 5 minutes	High	10 counts <input checked="" type="checkbox"/>
Network Security	Malware/virus detecti...	Malware/virus attack count > threshold within 5 minutes	High	10 counts <input checked="" type="checkbox"/>
Network Security	Malware/virus detecti...	Number of times the same malware/virus is detected > threshold within 15 minu...	Medium	2 times
Network Security	Alert counts	Number of alerts > threshold	High	10 counts <input checked="" type="checkbox"/>
Device	Online status	Device offline for more than 15 minutes	Medium	15 mins
Device	Concurrent sessions	Session numbers > 90%	Low	90 %
Anomaly	Login failure	Number of login failures over threshold within 1 minutes	Medium	10 times
Anomaly	Traffic anomaly	Number of scans/floods detected > threshold within 5 minutes	High	1 counts <input checked="" type="checkbox"/>

Page 1 of 1

Save Cancel

The following table describes the labels in this screen.

Table 16 Alerts > Configuration

LABEL	DESCRIPTION
Email Notification	Off means no alerts are e-mailed to any recipients. Select On to have alerts e-mailed to the selected recipients.
Email Title	Type an e-mail subject here.
Description	Type a description of the e-mails to be sent here. For example, maybe these emails are just for high severity events.

Table 16 Alerts > Configuration

LABEL	DESCRIPTION
Event Severity	<p>Select the severity levels of the security events for which you wish to send out e-mail notifications.</p> <ul style="list-style-type: none"> • High severity - Events that are exceptionally harmful, such as attacks by viruses or a high frequency of attacks. • Medium severity - Events that could collect users' personal information or adversely affect the network or a medium frequency of attacks. • Low severity - Events that usually have no adverse effect on a network or a low frequency of attacks.
Email Group	<p>This is where you can add users to the mailing list for event notifications. To add a user, select one or more names from the User Account box and click > to move them to the Email Recipients box.</p>
Alerts Configuration	<p>This table shows a list of recent security events.</p>
Category	<p>Select to group the alerts by category.</p>
Event type	<p>This displays the type of alert that was triggered. Examples of alert types are IDP, Spam, Virus and Web. Click to order the alerts by the type of threat that occurred.</p>
Alert Criteria	<p>Alert Criteria are the rules that trigger SecuReporter alerts. For example:</p> <ul style="list-style-type: none"> • An alert is triggered when over 10 login failures occur within one minute. • An alert is triggered when over 10 malware/virus attacks are blocked within five minutes.
Severity	<p>This displays the severity level as outlined in Table 4 on page 9.</p>
Threshold	<p>The threshold is the number that triggers an alert. If the threshold is adjustable, an icon will appear next to it. Click the icon and then set the threshold for the alert by typing in the numeric value or by pressing the up- and down-arrows. Adjustable values vary and include frequency, rate of occurrence, and the time period.</p>

CHAPTER 5

Settings

5.1 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 1 on page 6](#) for details on management privileges.

5.2 Organization & Devices

In **Settings > Organization & Devices**, you see all organizations that you have already created. You do not see organizations other people created.

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

	Organization	Claimed Device	Unclaimed Device	Action
1	[beta] ZYXEL-Headquarter	2	1	Edit Delete
2	[beta] Demo	1	1	Edit Delete

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



Organization

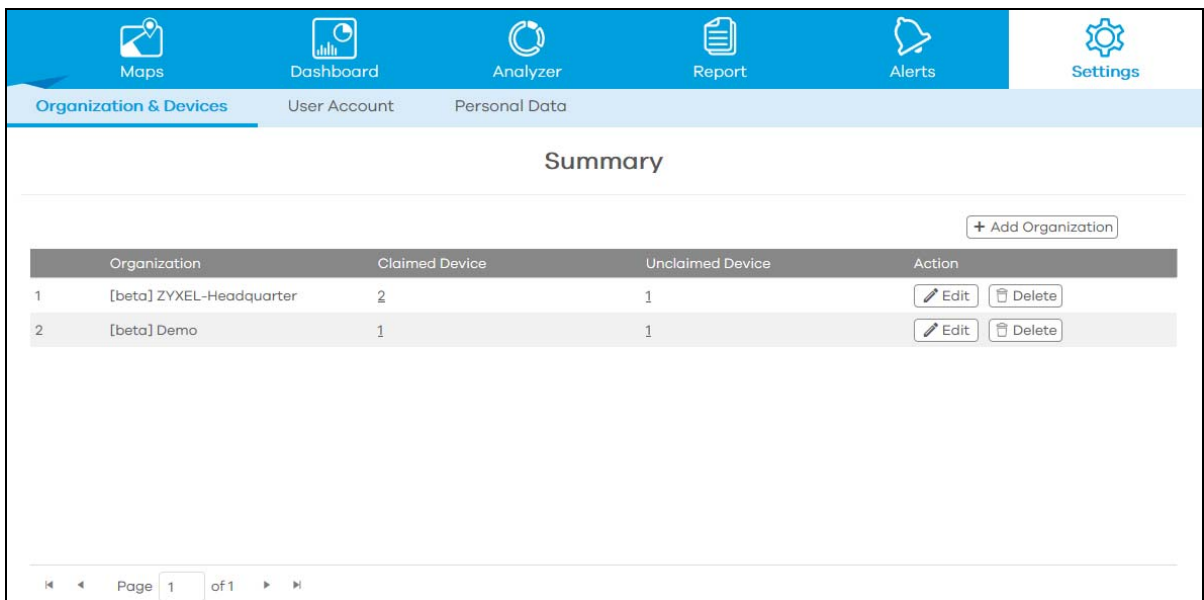
Organization Name:

Description:

After an organization has been added, you can still modify it using the **Edit** or **Delete** buttons under **Action**.

5.2.1 Add a Zyxel Device to an Organization

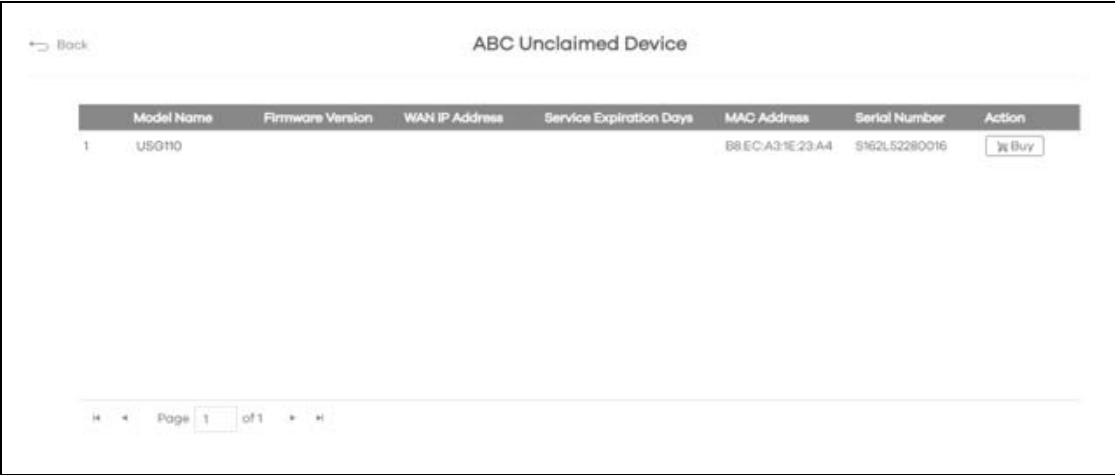
The hyper link under **Unclaimed Device** displays the number of Zyxel Device(s) that are available to be added to this organization by the Zyxel Device owner.



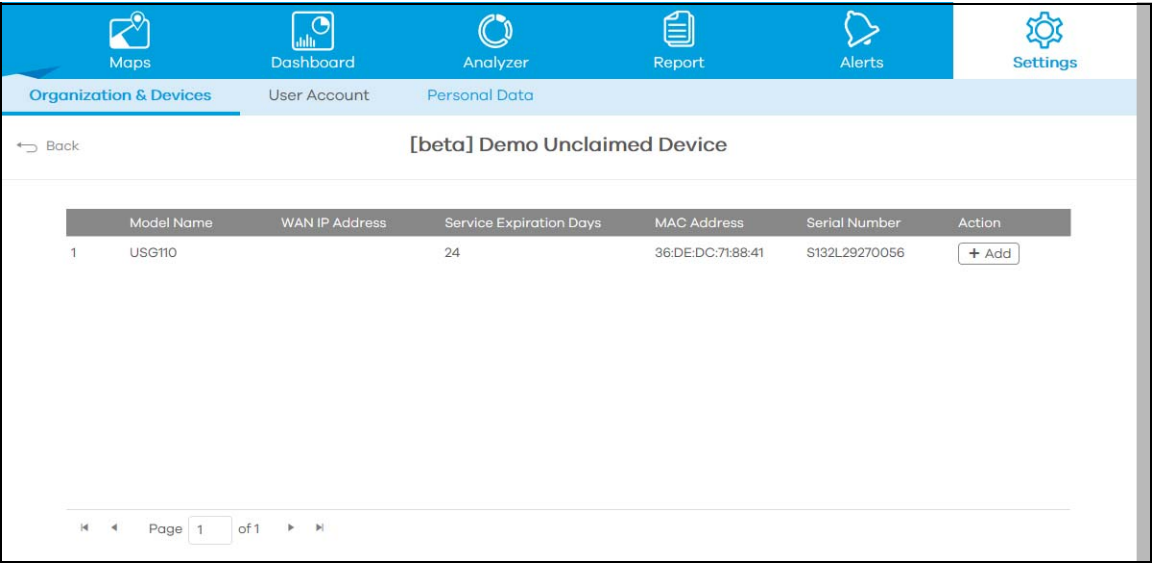
The screenshot shows the 'Summary' page under 'Organization & Devices'. It features a table with columns: Organization, Claimed Device, Unclaimed Device, and Action. There are two rows of data. The 'Action' column contains 'Edit' and 'Delete' buttons for each row. A '+ Add Organization' button is located at the top right of the table area. The page footer shows 'Page 1 of 1'.

	Organization	Claimed Device	Unclaimed Device	Action
1	[beta] ZYXEL-Headquarter	2	1	Edit Delete
2	[beta] Demo	1	1	Edit Delete

- 1 Click the hyper link under **Unclaimed Device** to add Zyxel Devices to this organization. You will see details of Zyxel Device(s) that are available to be added.
- 2 Under **Action**, you will see **Buy** for registered Zyxel Devices that do not have activated SecuReporter licenses. Click **Buy** to go to myZyxel to activate the SecuReporter license.



Under **Action**, you will see **Add** for registered Zyxel Devices that have activated SecuReporter licenses.



- 3 Click **Add** to add the Zyxel Device into this organization. Type an identifying name for this Zyxel Device in **Network Site Name** and an optional description, and then click **Next**.

Device

1. Device Setting 2. Protection Policy

Device Info

Model Name: **USG110**

MAC Address: **36:DE:DC:71:88:41**

Serial Number: **S132L29270056**

Device Name

Description

Previous 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**.

Device

1. Device Setting 2. Protection Policy

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

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

☐ **Fully Anonymous** – Personal data (user names, MAC addresses, email addresses and host names) are replaced with anonymized information in Analyzer, Reports, and downloaded Archive Logs. Data can no longer be traced back to individual people.

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

Previous Save

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 e-mail address of an existing record set as **Partially Anonymous**, go to **Settings > Personal Data** (refer to [Section 5.4 on page 39](#) for details).

5.2.2 Claimed Device

The hyper link under **Claimed Device** displays the number of Zyxel Device(s) that have been added to this organization. Click **Edit** to change the settings including the **Protection Policy**.

Organization & Devices

User Account

Personal Data

⌕ Back

[beta] Demo Claimed Devices

	Claimed Device	Model Name	Firmware Version	WAN IP Address	Service Expiration Days	Protection Policy	Action
1	ATP200	ATP200		61.222.86.79	35	Fully Anonymous	<div><div><div><div></div></div>Edit</div><div><div><div></div></div>Delete</div></div>

⏪

⏩

Page 1 of 1

⏪

⏩

5.3 User Account

To assign an administrator for this organization or Zyxel Devices within this organization, go to **Settings > User Account**.

- 1 Click **Add User**.

Maps

Dashboard

Analyzer

Report

Alerts

Settings

Organization & Devices

User Account

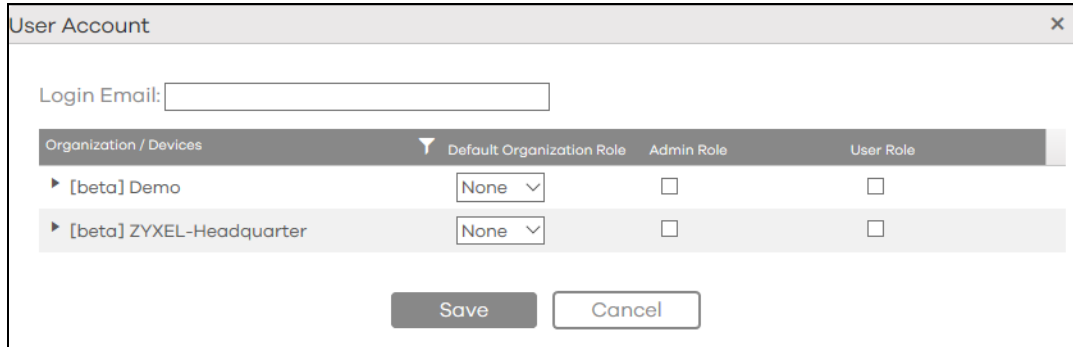
Personal Data

+ Add User

On-Line Status	User Name	Email Address	Privilege	Action
N		test@test.com	Details	<div>Edit</div> <div>Delete</div>
N	liu daikuei	daikuei.liu@zyxel.com.tw	Details	<div>Edit</div> <div>Delete</div>
N	kaochiuan teng	kaochiuan@gmail.com	Details	<div>Edit</div> <div>Delete</div>
N	John Gallagher	johng@zyxel.com.tw	Details	<div>Edit</div> <div>Delete</div>

Page 1 of 1

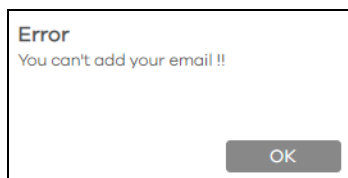
- 2 Type the e-mail address of the person that you want to be administrator in **Login Email**.



The 'User Account' window contains a 'Login Email' text field at the top. Below it is a table with columns: 'Organization / Devices', 'Default Organization Role', 'Admin Role', and 'User Role'. The table has two rows: one for '[beta] Demo' and one for '[beta] ZYXEL-Headquarter'. Both rows have a 'None' dropdown for the 'Default Organization Role' column and checkboxes for the 'Admin Role' and 'User Role' columns. At the bottom are 'Save' and 'Cancel' buttons.

Organization / Devices	Default Organization Role	Admin Role	User Role
[beta] Demo	None	<input type="checkbox"/>	<input type="checkbox"/>
[beta] ZYXEL-Headquarter	None	<input type="checkbox"/>	<input type="checkbox"/>

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. You also cannot add your own email address.



- 3 Select this user's **Default Organization Role** 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 **User** 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 don't want this user to see new Zyxel Devices added to this organization after the user account was created.

You may configure **Admin Role** and **User Role** privileges for individual Zyxel Devices within this organization. The individual Zyxel Device setting takes priority over the **Default Organization Role** setting.

Note: See [Table 1 on page 6](#) for details on management privileges.

- 4 Click **Save** when finished.

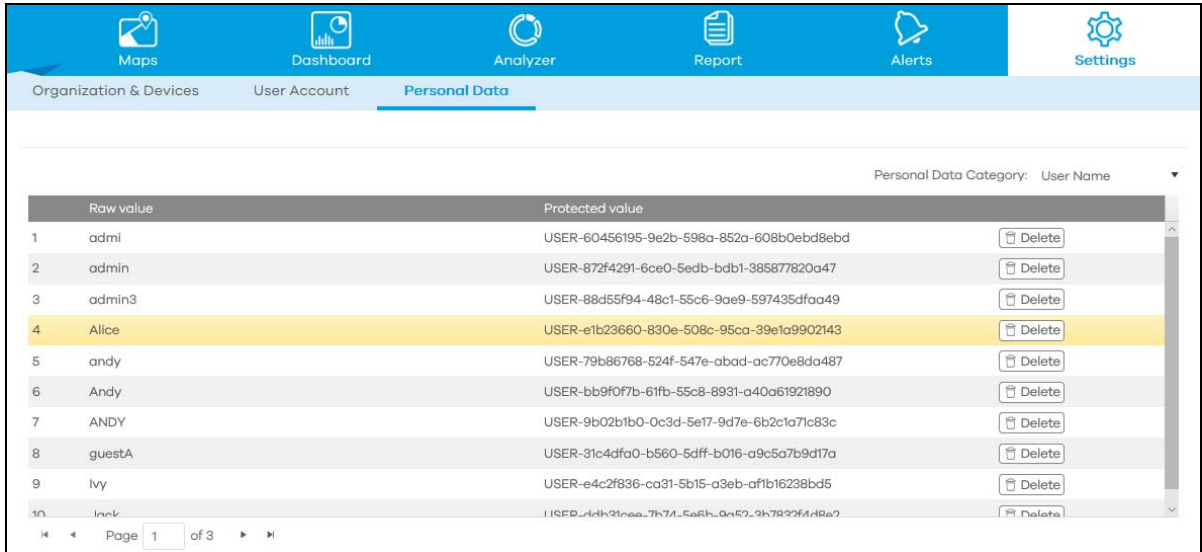
5.4 Personal Data

SecuReporter allows you to hide the user name and/or e-mail address in generated security events, traffic and analytics report.

5.4.1 User Name

To hide the user name, go to **Settings > Personal Data**.

- 1 On the **Personal Data Category** drop-down menu select **User Name**.

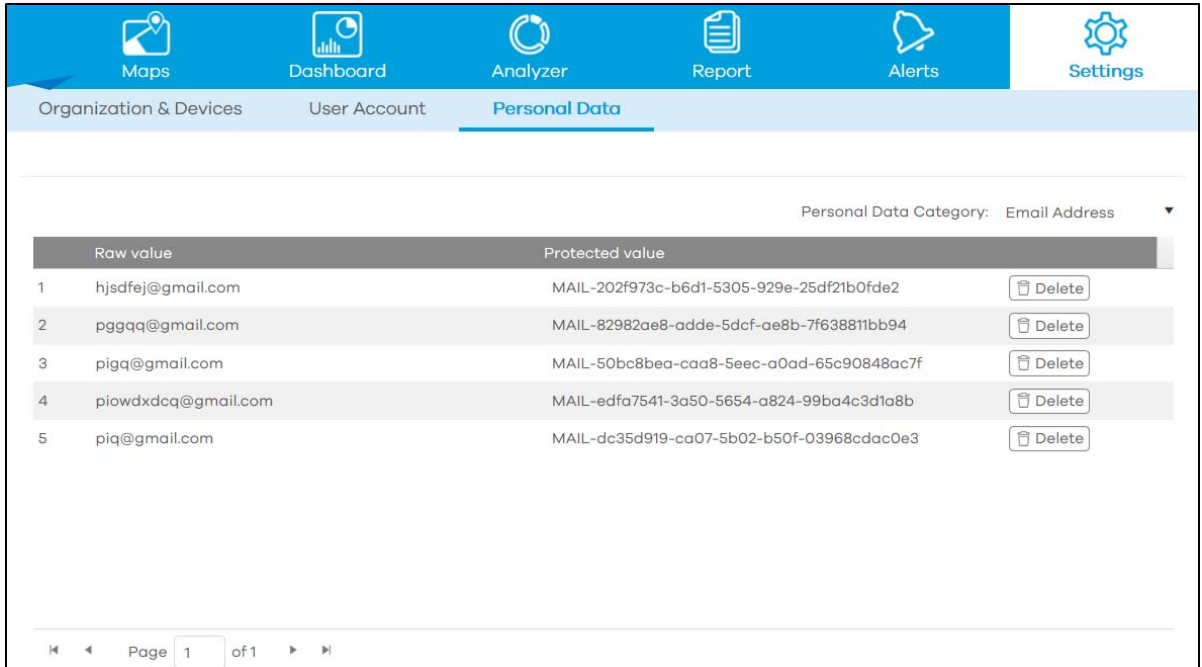


- 2 Select the user name you want hidden and click **Delete**. Then click **OK** to confirm removal.

5.4.2 E-mail Address

To hide the e-mail address, go to **Settings > Personal Data**.

- 1 On the **Personal Data Category** drop-down menu select **Email Address**.



- 2 Select the e-mail address you want hidden and click **Delete**. Then click **OK** to confirm removal.

Note: User name and e-mail address deletion is not reversible.

APPENDIX A

Legal Information

Copyright

Copyright © 2018 by Zyxel Communications Corporation.

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

Published by Zyxel Communications Corporation. All rights reserved.

Disclaimer

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

Viewing Certifications

Go to <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 e-mail notices of firmware upgrades and information at www.zyxel.com for global products, or at www.us.zyxel.com for North American products.

Open Source Licenses

This product contains in part some free software distributed under GPL license terms and/or GPL-like licenses. Open source licenses are provided with the firmware package. You can download the latest firmware at www.zyxel.com. If you cannot find it there, contact your vendor or Zyxel Technical Support at support@zyxel.com.tw.

To obtain the source code covered under those Licenses, please contact your vendor or Zyxel Technical Support at support@zyxel.com.