

Web GUI User Manual

Tera-UTM 12

Version 1.0

Released on July 2023



Tera-UTM 12 Web GUI User Manual

Copyright © 2023, Lionic Corp.; all rights reserved.

Trademarks

Lionic is trademarks of Lionic Corp.

"WireGuard" is registered trademark of Jason A. Donenfeld.

No-IP is registered trademark of No-IP.com.

Disclaimer

Lionic provides this manual 'as is' without any warranties, either expressed or implied, including but not limited to the implied warranties or merchantability and fitness for a particular purpose. Lionic may make improvements and/or changes to the product(s), firmware(s) and/or the program(s) described in this publication at any time without notice.

This publication could contain technical inaccuracies or typographical errors. Changes are periodically made to the information in this publication; these changes are merged into new editions of this publication.

Technical Support Lionic Corporation

Email: support@lionic.com Tel: +886-3-5789399 Fax: +886-3-5789595

Content

Overview	3
Dashboard.....	4
WAN.....	6
Configuration	6
Remote Control	7
LAN	9
Mode.....	9
DHCP	10
Port Forwarding	11
Policy	12
Anti-Virus, Anti-Intrusion, Anti-WebTheat.....	12
Firewall.....	14
Exceptional Websites	15
SSL/TSL Inspection.....	16
Threats	18
VPN.....	19
System	21
Device	21
Server.....	23
Notifications.....	24
Firmware Upgrade.....	26
Backup / Restore	27
Change Password	28
User Activities	29
Utilities	30

Overview

Dashboard:

[Dashboard] shows operating status and device information of Tera-UTM 12, including Inspection History, threat statics, network traffic monitoring and system resource usage.

WAN:

WAN settings of Tera-UTM 12 could be configured in [WAN], such as IPv4/IPv6 configurations and [Remote Control] settings.

LAN:

LAN settings of Tera-UTM 12 could be configured in [LAN]. After switching the connection mode from [Bridge Mode] (default) to [Router Mode], DHCP reservations and port forwarding are available.

Security:

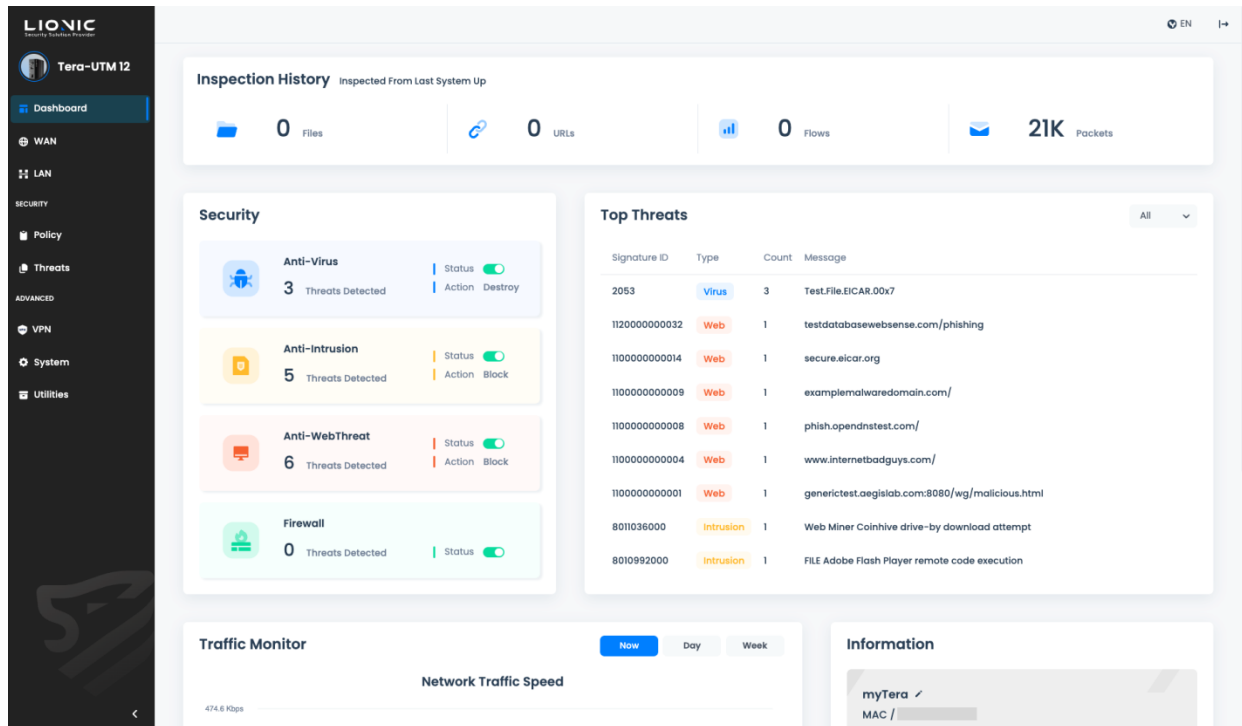
- **Policy:** Configuring protection rules for each security feature, including Anti-Virus, Anti-Intrusion, Anti-WebThreat and the firewall.
- **Threats:** Listing protection logs for each security feature.

Advanced:

- **VPN:** After the VPN server is enabled, the protecting range of Tera-UTM 12 could be expanded to your mobile devices when using cellular network or public Wi-Fi.
- **System:** Configuring system settings, including license management, server connection setting, firmware upgrade, backup and restore, etc.
- **Utilities:** Providing tools for troubleshooting, such as network tools, command-line tool and exporting system log.

Dashboard

Operating status and device information are displayed on [Dashboard] of Tera-UTM 12.

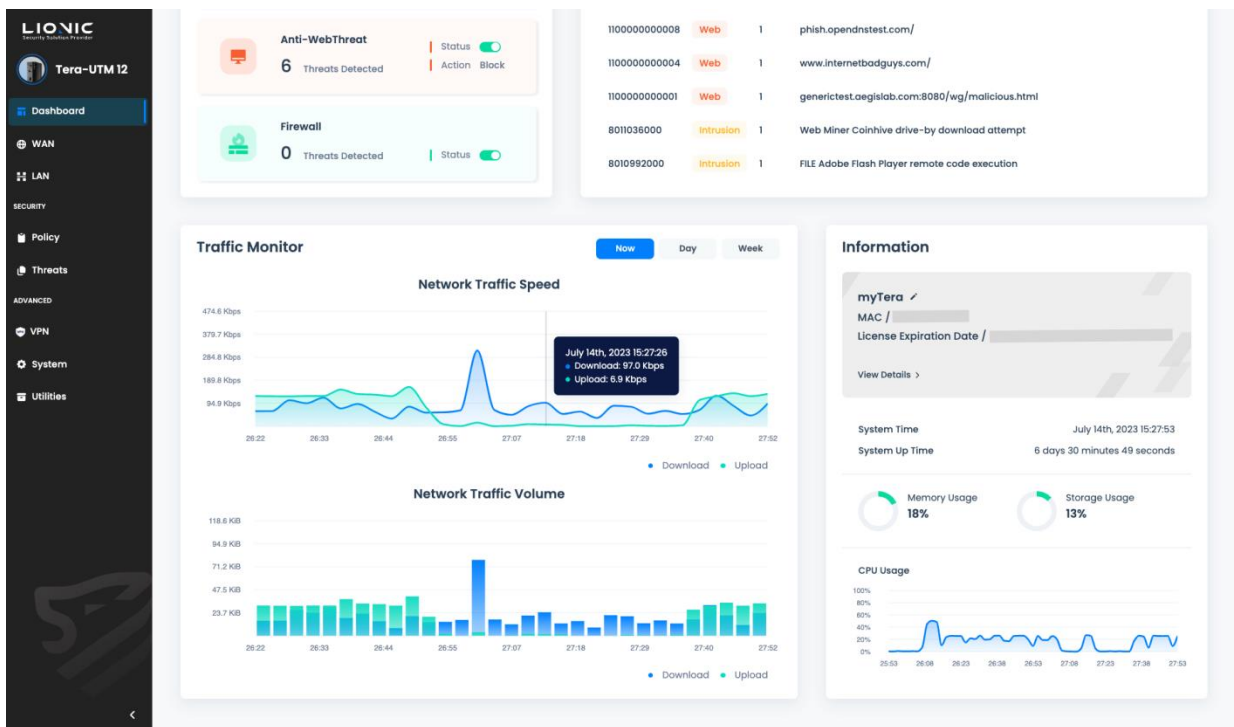


Dashboard

Inspection History: Showing the inspected number of files, URLs, flows and packets from the last system up.

Security: Showing the threat number detected by Tera-UTM 12, enabling status and actions of each security feature. By clicking the threat number or the “Action” button, you can access the threat log page or the policy page of the corresponding feature.

Top Threats: Summarizing detected threat logs of each security feature, and sorting by detected counts in all features or each feature.



Dashboard

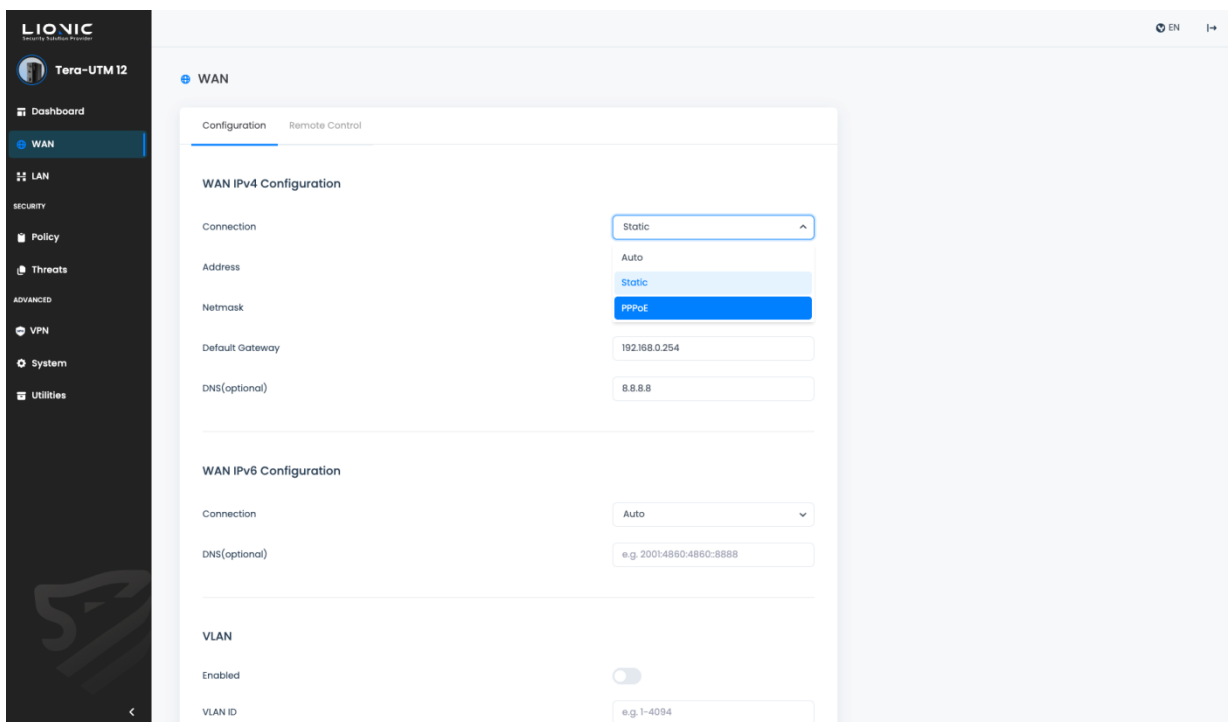
Traffic Monitor: Showing the download and upload traffic via Tera-UTM 12.

Information: Showing the device information of the Tera-UTM 12, such as the device name (editable), MAC address, license expiration date, firmware version, signature versions, WAN IP address, system time, system up time and system resource usage.

WAN

Configuration:

In [Configuration], you could set the IPv4 or IPv6 connection as [Auto] (default), [Static], or [PPPoE] based on your network environment. If you need to use [Static] or [PPPoE], please contact your ISP or IT administrator for detailed configuration.



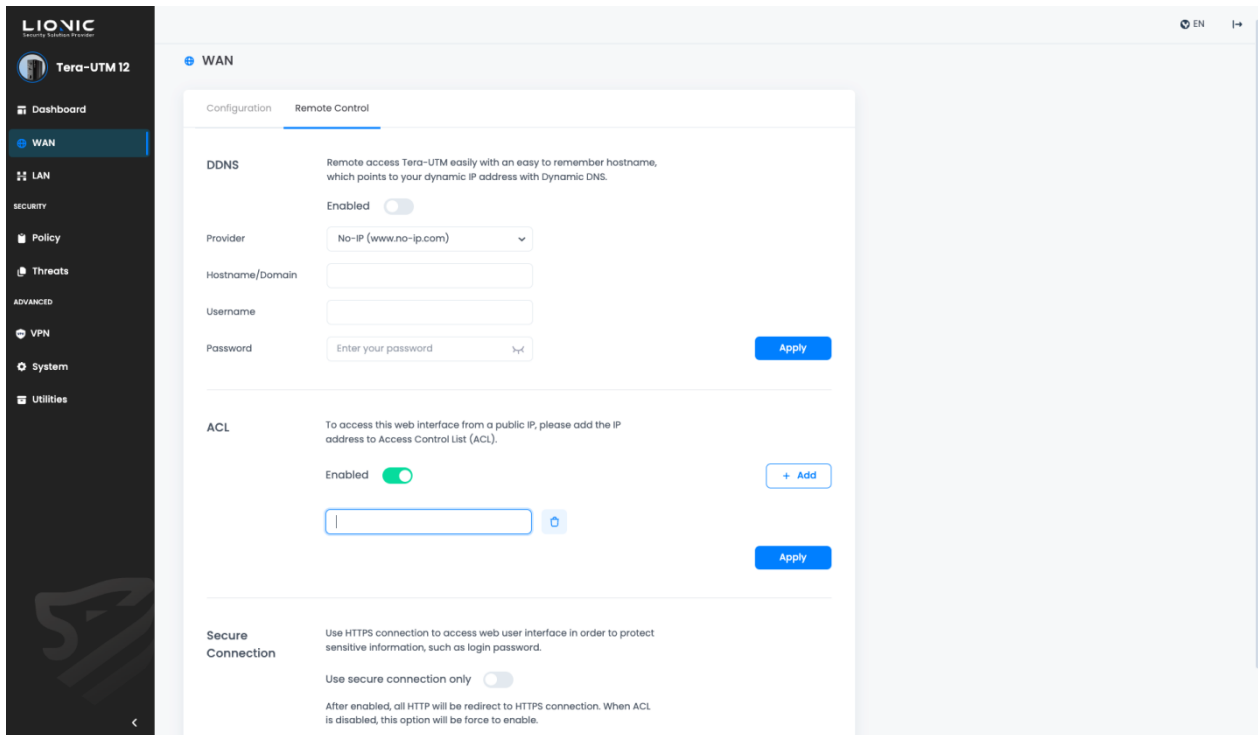
WAN- Configuration

- **Auto:** Tera-UTM 12 obtains DHCP IP address from the router placed at the WAN side of the Tera-UTM 12.
- **Static:** For user to fill the correct IP address in manual.
- **PPPoE:** For user to fill the correct username and password in manual.

* Remark: When using PPPoE connection, you may not be able to access the web GUI of Tera-UTM 12 due to the restriction of the access control list (ACL). Please see [Remote Control] for more details of ACL.

Remote Control:

To prevent Tera-UTM 12 from intrusion, only devices with private IP address in the same LAN network are allowed to access the web GUI. If it is necessary to access the web GUI remotely through Internet, or if the Tera-UTM 12 connects Internet using a public IP address, please configure settings in [Remote Control].



WAN- Remote Control

DDNS

When the Tera-UTM 12 is using a dynamic public IP address, you could use a static domain name to access the Tera-UTM 12.

Fill the following settings after you applied a domain name from the DDNS service provider:

- Provider: Choose the DDNS service provider (Remark 1).
- Hostname/Domain: Fill the domain name you applied.
- Username: Fill your username for the DDNS service.
- Password: Fill your password for the DDNS service.

After you clicked [Apply] and then enabled [DDNS], you could access the web GUI of Tera-UTM 12 in remote with the domain name you applied (Remark 2).

* Remark:

1. Only No-IP DDNS service is currently supported.
2. After a new configuration is applied or the IP address is changed, it may take a moment for the DDNS service provider to update the domain name. If you are not able to access the web GUI with the domain name during the DDNS is updating, please try again later.
3. If the Tera-UTM 12 is using a private IP address to connect Internet, please set DDNS and port forwarding on the router at the WAN side of Tera-UTM 12.

Access Control List (ACL)

To prevent Tera-UTM 12 from intrusion, only devices with private IP address in the same LAN network are allowed to access the web GUI. If it is necessary to access the web GUI remotely through Internet, or if the Tera-UTM 12 connects Internet using a public IP address, the IP address that would be used to access Tera-UTM 12 should be added into the Access Control List (ACL).

Step 1: Click [+ Add].

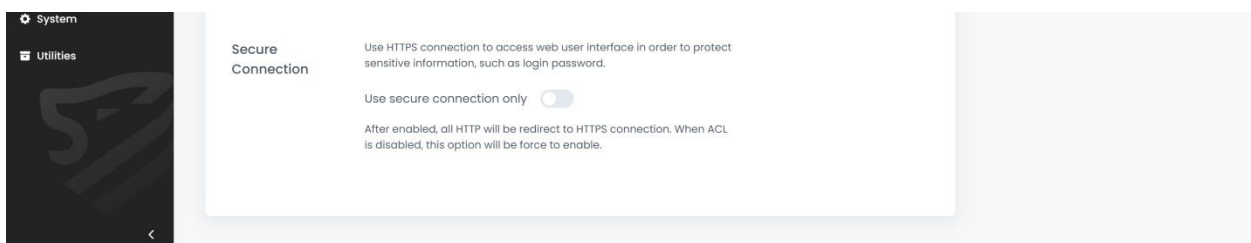
Step 2: Enter the IP address that would be used to access Tera-UTM 12 in the input field.

Step 3: Click [Apply].

If the IP address is not fixed (for example, the device is using dynamic IP addresses) (Remark 1), disable ACL so that all devices are allowed to access Tera-UTM 12.

* Remark:

1. To keep the connection secure, [Secure Connection] will be enabled automatically and cannot be disabled while [ACL] is disabled.



WAN- Secure Connection

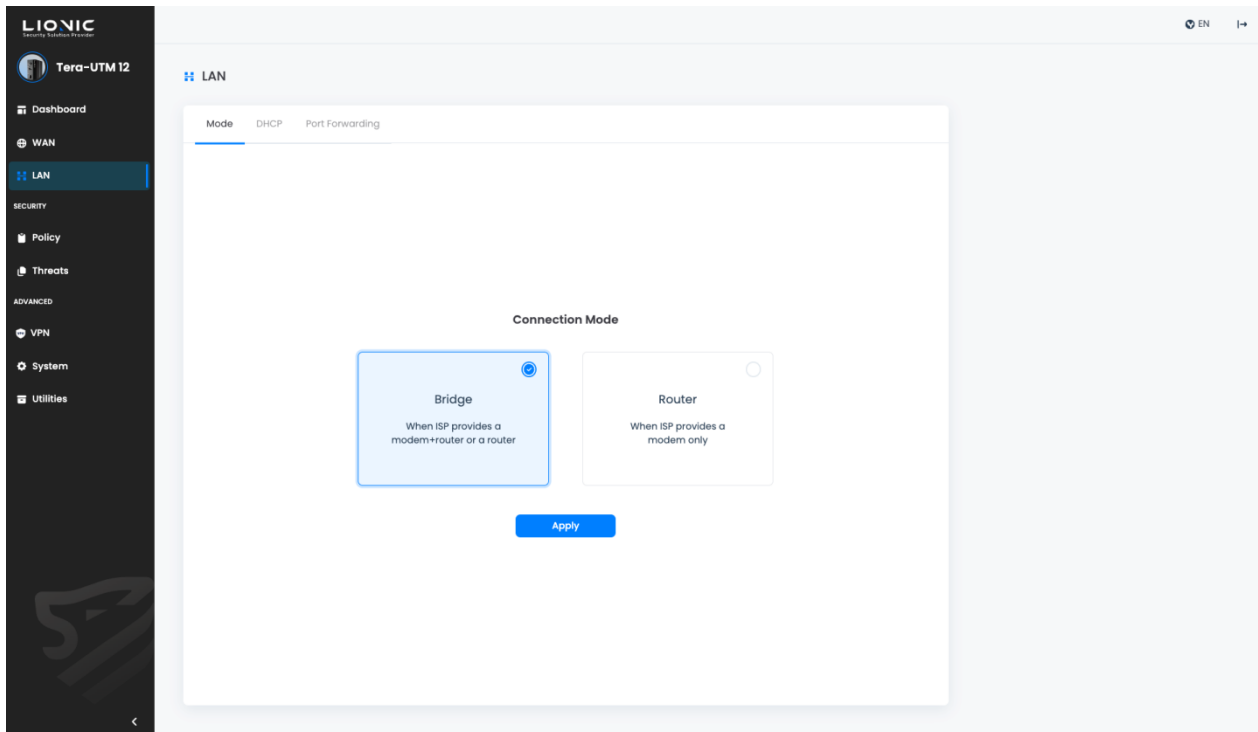
Secure Connection

After [Secure Connection] is enabled, all HTTP connections accessing the web GUI of Tera-UTM 12 will be redirected to HTTPS connections, so that sensitive information like login password can be protected. While [ACL] is disabled, [Secure Connection] will be force to enable.

LAN

Connection Mode:

Tera-UTM 12 supports 2 connection modes. Select a suitable connection mode based on your network environment.



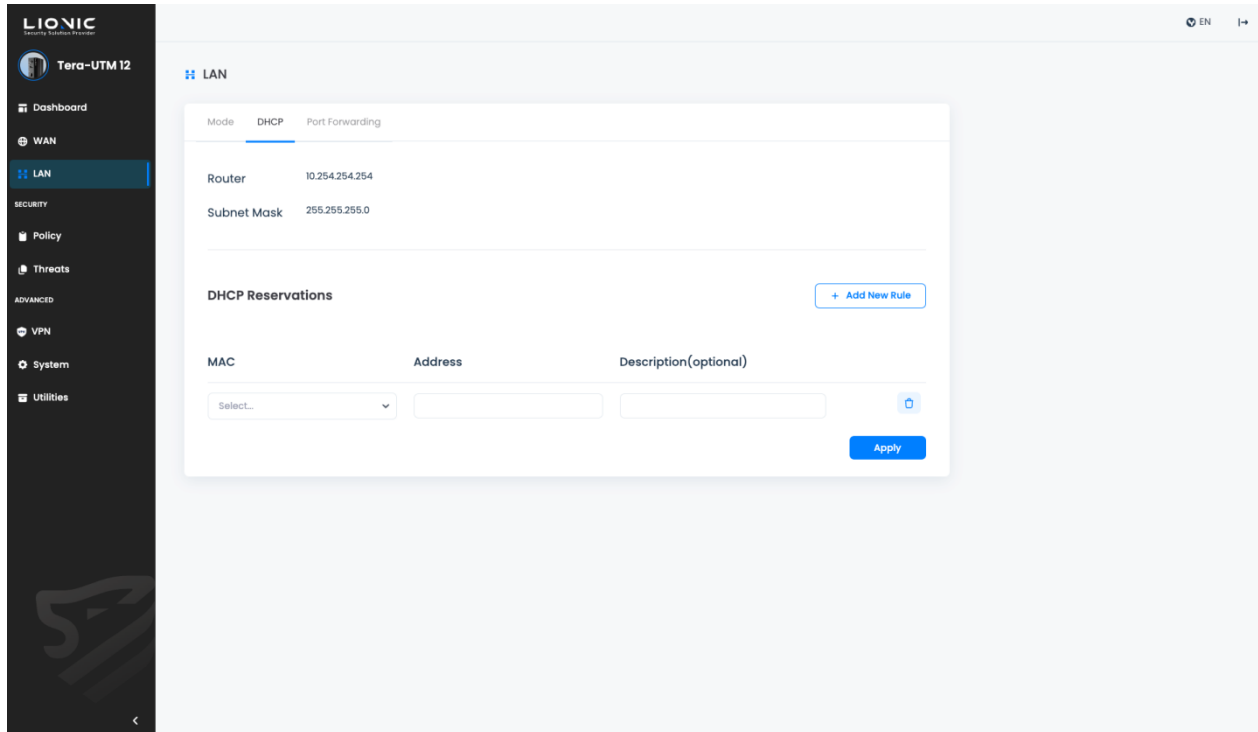
LAN-Connection Mode

- **Bridge mode (default):**
DHCP is disable to LAN devices in [Bridge] mode. Please connect Tera-UTM 12 to the LAN side of a router.
- **Router mode:**
DHCP is enable to LAN devices in [Router] mode. Please make sure only 1 IP address is assigned to Tera-UTM 12 and its LAN devices.

After you selected the suitable connection mode and clicked [Apply], Tera-UTM 12 would start configuring the network function. The Internet connection would be interrupted during the configuring, and you may need to login again to access the web GUI.

DHCP

In [Router] mode, Tera-UTM 12 is able to assign DHCP IP addresses to devices deployed at its LAN side (LAN devices). When there is only 1 WAN IP address assigned to Tera-UTM 12, you can use DHCP to assign private IP addresses to LAN devices.



LAN-DHCP

- **DHCP IP address range:** 10.254.254.100~249
- **Router IP address:** 10.254.254.254 (LAN devices can access the web GUI with this IP address)
- **Subnet Mask:** 255.255.255.0

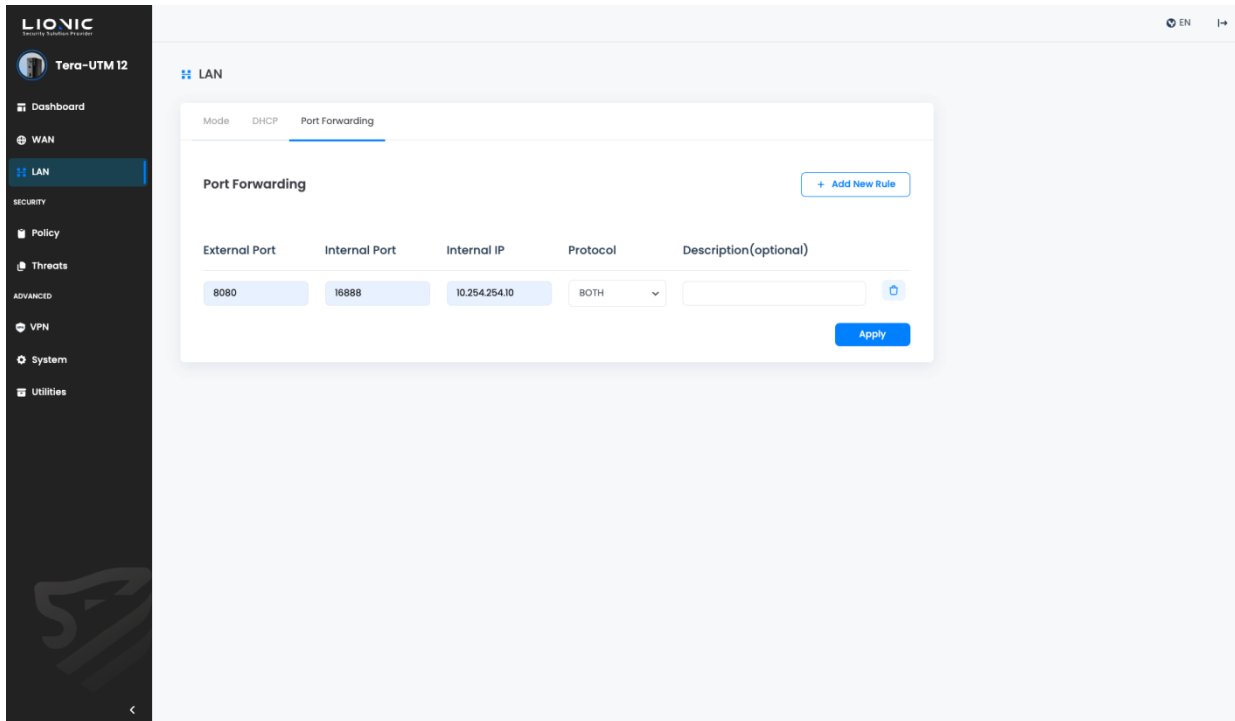
DHCP Reservations

If you need to reserve a static IP address for a specific LAN device, enter the MAC address of the LAN device and the IP address you would like to reserve, then click [Apply].

*Remark: You may need to update the network configuration of the LAN device to get the reserved IP address.

Port Forwarding

In [Router] mode, Tera-UTM 12 supports [Port Forwarding]. If you need to access a LAN device from Internet, set the internal port and internal IP address to access the LAN device through a specific external port.



LAN-Port Forwarding

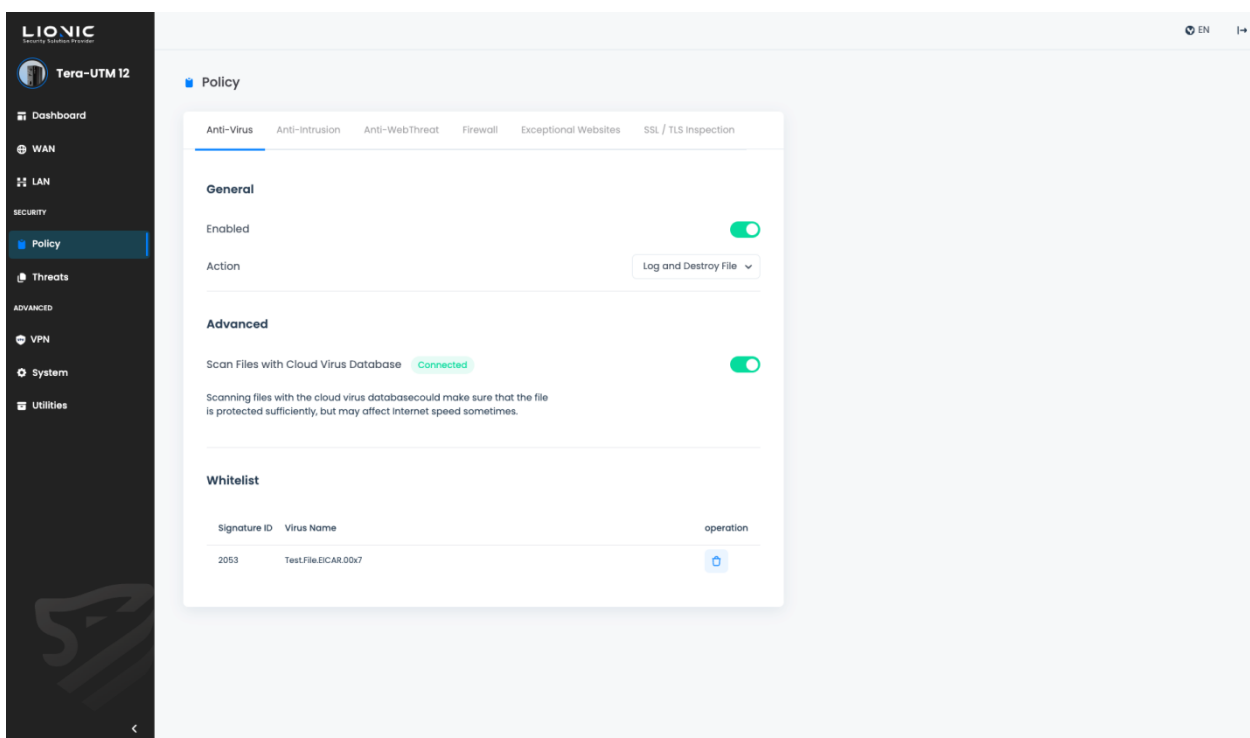
Policy

Tera-UTM 12 provides 3 cyber-security features based on the Deep Packet Inspection (DPI) technology:

- **Anti-Virus:** Inspect virus from packets and then destroy it.
- **Anti-Intrusion:** Detect intrusion from packets and then block the attack.
- **Anti-WebThreat:** Detect malicious websites connection from packets and disconnect.

In [Policy] page, you can configure protection rules for these 3 features:

Feature	Anti-Virus	Anti-Intrusion	Anti-WebThreat
Enabled	Enable / Disable	Enable / Disable	Enable / Disable
Action	Log Only / Log and Destroy File	Log Only / Log and Block	Log Only / Log and Block
Advanced	Scan Files with Cloud Virus Database	Block Brute-Force Attacks, Block Protocol Anomaly, Block Port Scan and DoS Attacks	---
Whitelist	View and remove whitelist rule	View and remove whitelist rule	View and remove whitelist rule



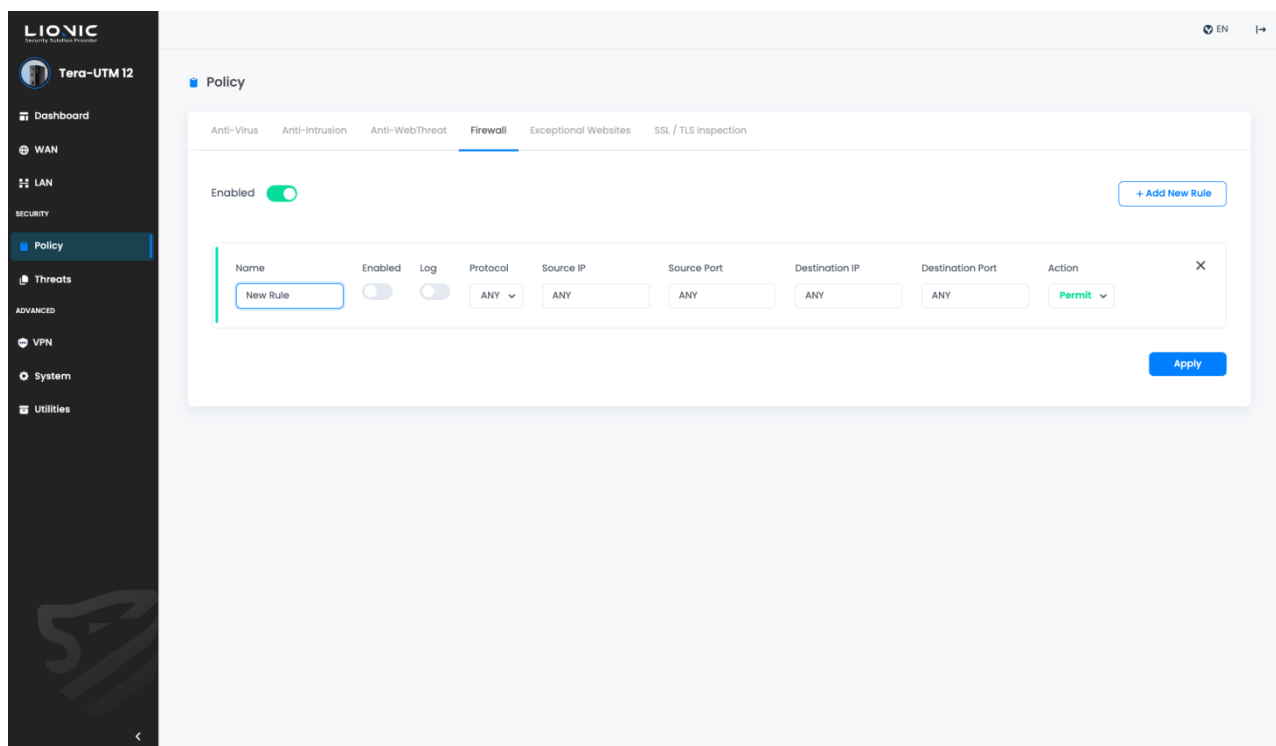
Policy

- **Enabled:** Enable or disable each security feature separately. The default setting is ENABLE.
- **Action:** The action that Tera-UTM 12 takes after the threat is detected.
 - Log Only: Only shows the threat event in [Threats] page.
 - Log and Destroy File: Shows the threat event in [Threats] page and destroys the virus file.
 - Log and Block: Shows the threat event in [Threats] page and blocks the connection.
- **Scan Files with Cloud Virus Database:** Besides the scan with the local virus signatures, Tera-UTM 12 features the scan with LIONIC cloud virus database. To obtain the full protection of Anti-Virus, please make sure your Tera-UTM 12 is activated with a valid license code, and connected to the Internet.
- **Block Brute-Force Attacks:** After this function is enabled, Tera-UTM 12 can detect frequent login failures in a short period. Once the occurrence frequency is higher than the threshold, Tera-UTM 12 will record or block the attempting attack based on the frequency.
- **Block Protocol Anomaly:** After this function is enabled, Tera-UTM 12 can detect and block abnormal packets that do not comply with protocol specifications.
- **Block Port Scan and DoS Attacks:**
 - Prevent DoS attacks using flooding burst connections within short time

- period on TCP, TCP half-open, UDP, ICMP, SCTP or IP protocols.
- Block devices which keep sending mis-formatted packets.
- Block port-scan attempting including TCP SYN scan, TCP RST scan and UDP scan.
- **Whitelist:** To correct a trusted file or connection destroyed/blocked by Tera-UTM 12 by adding the threat to the whitelist.
 - Add to whitelist: Find the threat event in [Threats] page, and then click [+] to add it into the whitelist.
 - View and remove whitelist rule: View the whitelist rule in [Policy] page, and remove the rule if needed.

Firewall:

Besides the 3 cyber-security features, Tera-UTM 12 also provide a basic firewall.



Policy-Firewall

Step 1: Enable the firewall (default is enabled).

Step 2: Click [+Add New Rule].

Step 3: Fill each configuration.

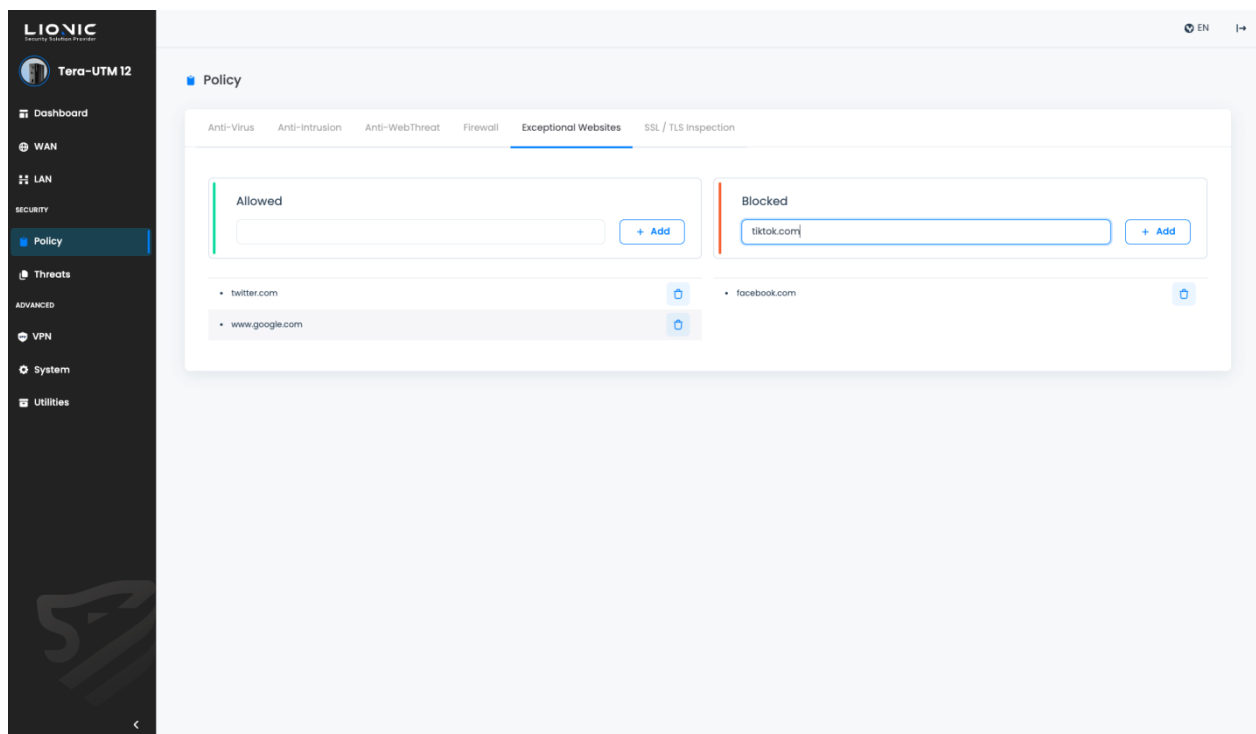
Step 4: Click [Apply] to take effect.

Firewall Configuration:

- Name: A user-defined firewall rule name.
- Enabled: Enable / disable the firewall rule.
- Log: Show / Hidden the firewall event in [Threats] page.
- Protocol: TCP / UDP / ANY.
- Source IP, Source Port, Destination IP, Destination Port: Criteria of the firewall rule.
- Action: Permit / deny the connection that matches the criteria.

Exceptional Websites:

Add a specific website into [Exceptional Websites] to allow or block all connection to the website.



Policy-Exceptional Websites

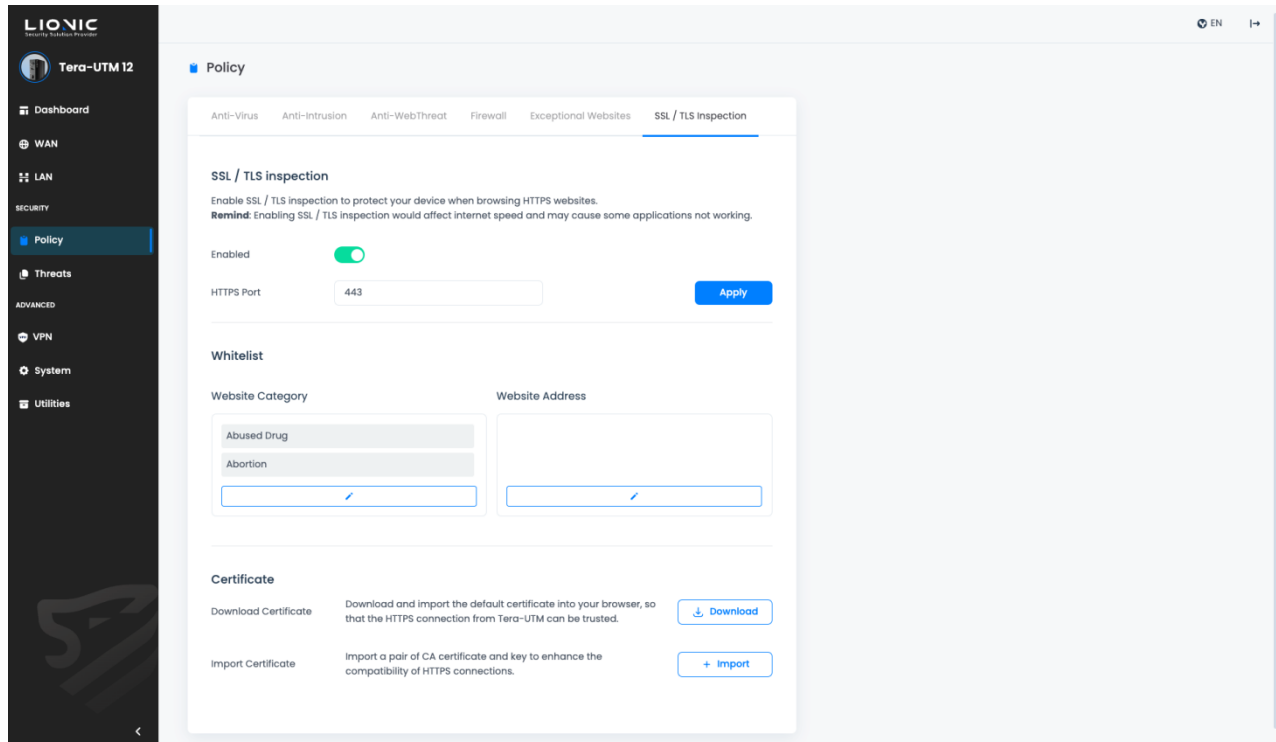
Step 1: Fill the input field with the URL or IP address of the website which you would like to allow / deny.

Step 2: Click [+ Add] to take effect.

*Remark: Some of the website or cloud service requires more than 1 domain name or IP address to access different pages. You may not completely allow or deny this kind of website until you added all URLs / IP addresses.

SSL / TLS Inspection:

After [SSL / TLS inspection] is enabled, Tera-UTM 12 will inspect packets encrypted with SSL or TLS, in order to protect your device when browsing HTTPS websites.



Policy-SSL/TLS Inspection

*Remark: Enabling [SSL / TLS Inspection] would affect internet speed and may cause some applications not working.

- **Enabled:** Enable or disable [SSL / TLS Inspection]. The default setting is DISABLE.
- **HTTPS Port:** Set the port* used by HTTPS connection. The default setting is 443. If you would like to set multiple ports, please separate them with “,”.

*Remark: When setting the HTTPS port, please avoid common ports used by other network services, such as Port 20, 21 for FTP, Port 25 for SMTP, etc., in order to prevent port conflict issues.

- **Whitelist:** After a website is added into the whitelist, Tera-UTM 12 will not inspect encrypted packets from / to the website. If you would like to keep the SSL / TLS packet encrypted due to the compatibility or the privacy, please add the trusted website into the whitelist.

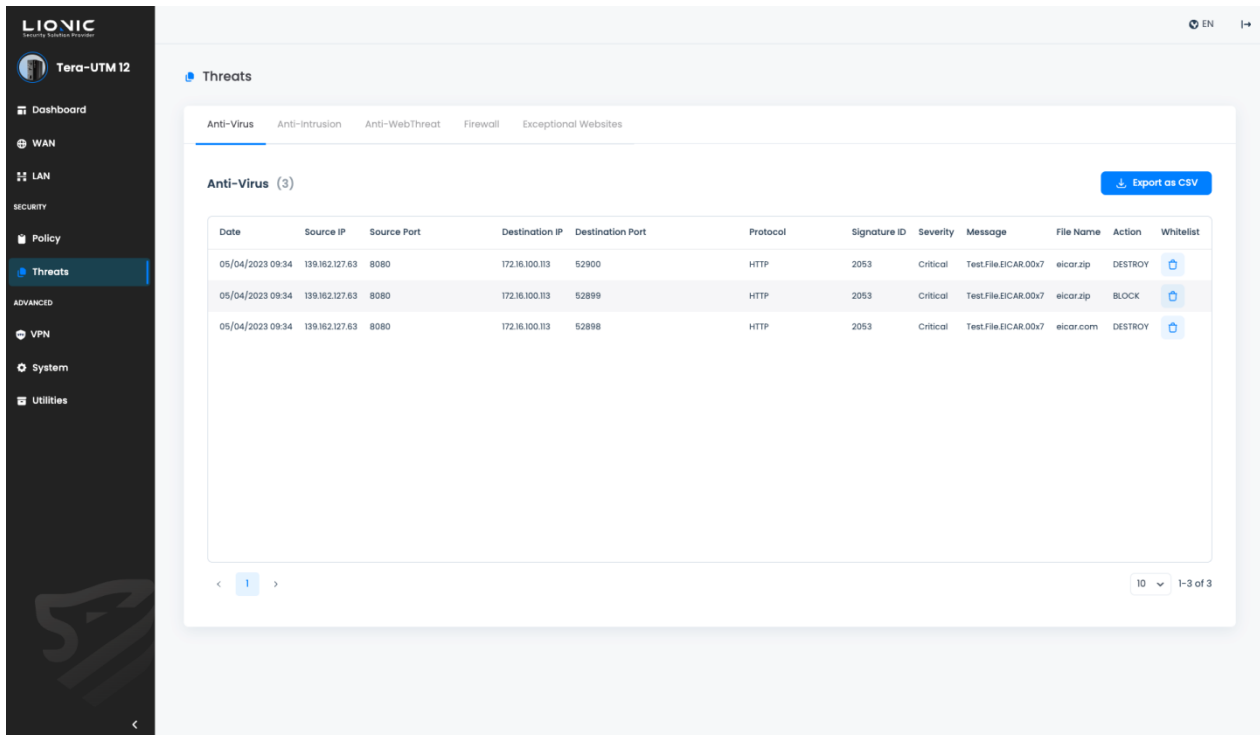
- **Website Category:** Tera-UTM 12 provides multiple website categories as whitelist options. The categories in the default whitelist are “Finance and Insurance” and “Health and Medicine”. After a category is added into the whitelist, the website that classified as the category will not be inspected.
- **Website Address:** Tera-UTM 12 provides a customizable field to add trusted website addresses into the whitelist. After adding the specified website address into the whitelist, the encrypted connection from / to the website will not be inspected.

*Remark: To enhance the compatibility after [SSL / TLS Inspection] is enabled, some trusted network services, such as Apple, Google, Microsoft, etc., have been added into the whitelist.

- **Download Certificate:** Download and import the default certificate into your browser, so that the HTTPS connection from Tera-UTM can be trusted.
- **Import Certificate:** Import a pair of CA certificate and key to enhance the compatibility of HTTPS connections.

Threats

After a threat is detected by Tera-UTM 12, the detailed threat information would be shown on the corresponding tab of each security feature in [Threats] page.



Threats

Anti-Virus Anti-Intrusion Anti-WebThreat Firewall Exceptional Websites

Anti-Virus (3) [Export as CSV](#)

Date	Source IP	Source Port	Destination IP	Destination Port	Protocol	Signature ID	Severity	Message	File Name	Action	Whitelist
05/04/2023 09:34	139.162.127.63	8080	172.16.100.113	52900	HTTP	2053	Critical	TestFile.EICAR.00x7	eicar.zip	DESTROY	+
05/04/2023 09:34	139.162.127.63	8080	172.16.100.113	52899	HTTP	2053	Critical	TestFile.EICAR.00x7	eicar.zip	BLOCK	+
05/04/2023 09:34	139.162.127.63	8080	172.16.100.113	52898	HTTP	2053	Critical	TestFile.EICAR.00x7	eicar.com	DESTROY	+

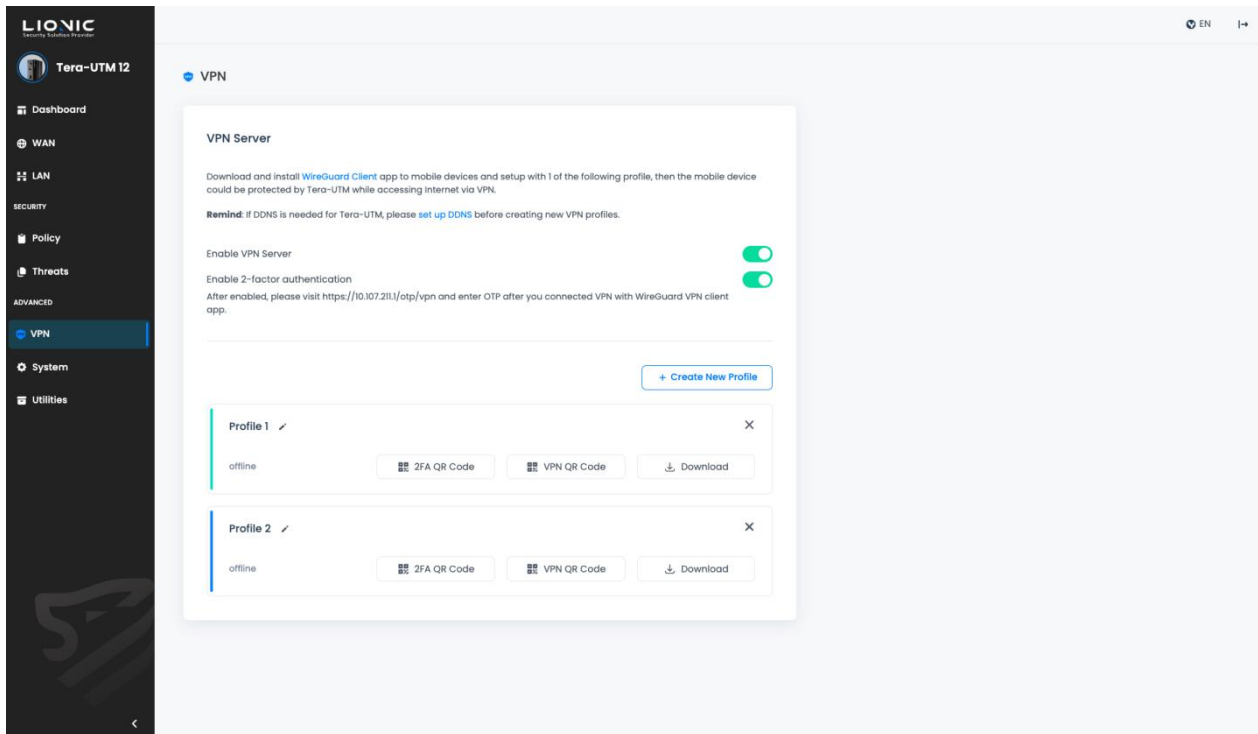
< 1 > 10 1-3 of 3

Threats

- **Export as CSV:** Export and download the log in a CSV file.
- **Whitelist:** If Tera-UTM 12 destroyed a trusted file or blocked a trusted connection, it can be corrected by adding the threat on the whitelist.
 - Add to whitelist: Find the threat event in [Threats] page, and then click [+] to add it into the whitelist.
 - View and remove whitelist rule: View the whitelist rule in [Policy] page, and remove the rule if needed.

VPN Server

Enable the VPN server to expand the protecting range of Tera-UTM 12 to devices using cellular network or public Wi-Fi. Mobile devices could be protected by Tera-UTM 12 while accessing Internet via VPN.



VPN Server

Preparation:

Download and install WireGuard Client app to the device which needs the protection of Tera-UTM 12.

Setup :

- Step 1: Click [Enable VPN Server].
- Step 2: Click [+ Create New Profile].
- Step 3:
 - For mobile phones or tablets: Click [Show QR Code] and scan the QR code with WireGuard Client app.
 - For laptops or PCs: Click [Download] and import the profile into WireGuard Client app.

After the setup is done, please connect Tera-UTM 12 via VPN with WireGuard Client

app whenever the protection of Tera-UTM 12 is needed.

* Remark:

1. If you would like to set DDNS for Tera-UTM 12, please setup before enabling the VPN server.
2. If there is a router at the WAN side of Tera-UTM 12, please set port forwarding on the router, so that the connection could be redirected to Port 51820 of Tera-UTM 12. Meanwhile, please edit the profile manually in WireGuard Client app, use the IP address or domain name of the router as the VPN server address.
3. If the VPN connection failed, please try to reconnect the VPN server with WireGuard Client app.

Enable 2-factor authentication for VPN server

After [2-factor authentication] (2FA) is enabled, an extra one-time-password (OTP) is required before accessing Internet via VPN. This feature is used to enhance the VPN profile security.

Preparation:

1. Download and install WireGuard Client app to the device which needs the protection of Tera-UTM 12.
2. Download and install Google Authenticator app or other OTP apps.

Setup:

- Step 1: Click [Enable VPN Server] and [Enable 2-factor authentication].
- Step 2: Click [+ Create New Profile].
- Step 3: Click [2FA QR Code] in the profile.
- Step 4: Use your OTP app to scan the 2FA QR code.
- Step 5:
 - For mobile phones or tablets: Click [Show QR Code] and scan the QR code with WireGuard Client app.
 - For laptops or PCs: Click [Download] and import the profile into WireGuard Client app.

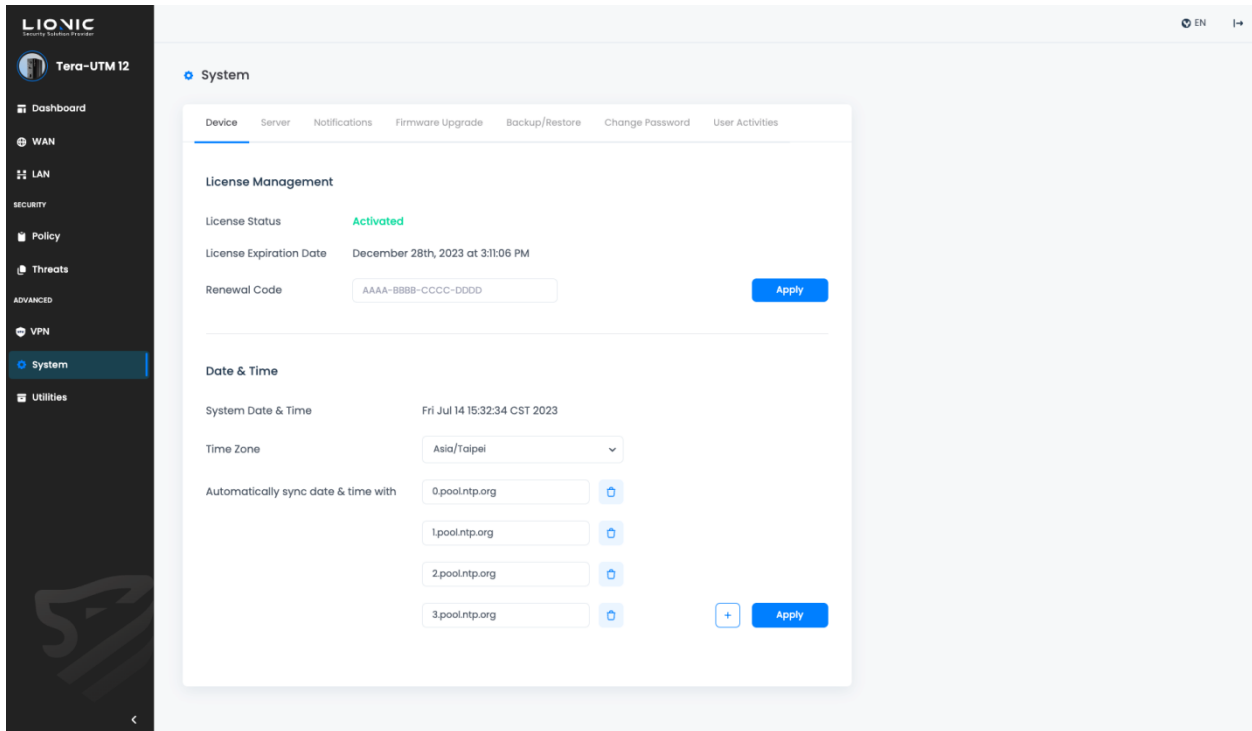
Start Accessing Internet via VPN:

- Step 1: Connect Tera-UTM 12 via VPN with WireGuard Client app.
- Step 2: Obtain the OTP from the OTP app.
- Step 3: Visit <http://mytera.lionic.com/otp/vpn> and enter the OTP.

After the 2FA is done, you can start accessing Internet via VPN.

System

Device:



System-Device

License Management

View the license status, activate or renew the license for Tera-UTM 12.

Message	License Status
Activated	License is valid
Not Activated	License has not been activated yet
Expired	License is expired
Status checking failed	Failed to connect the license server

- **Activate license:** To obtain the full cyber-security protection from Tera-UTM 12, enter the activation code (Remark 1) into the input field and click [Activate] while connecting Internet.
- **Renew license:** Tera-UTM 12 will remind you in 30 days before the license is

expired. Please purchase the renewal code (Remark 2) , enter it into the input field and click [Apply] to extend the expiration date.

* Remark:

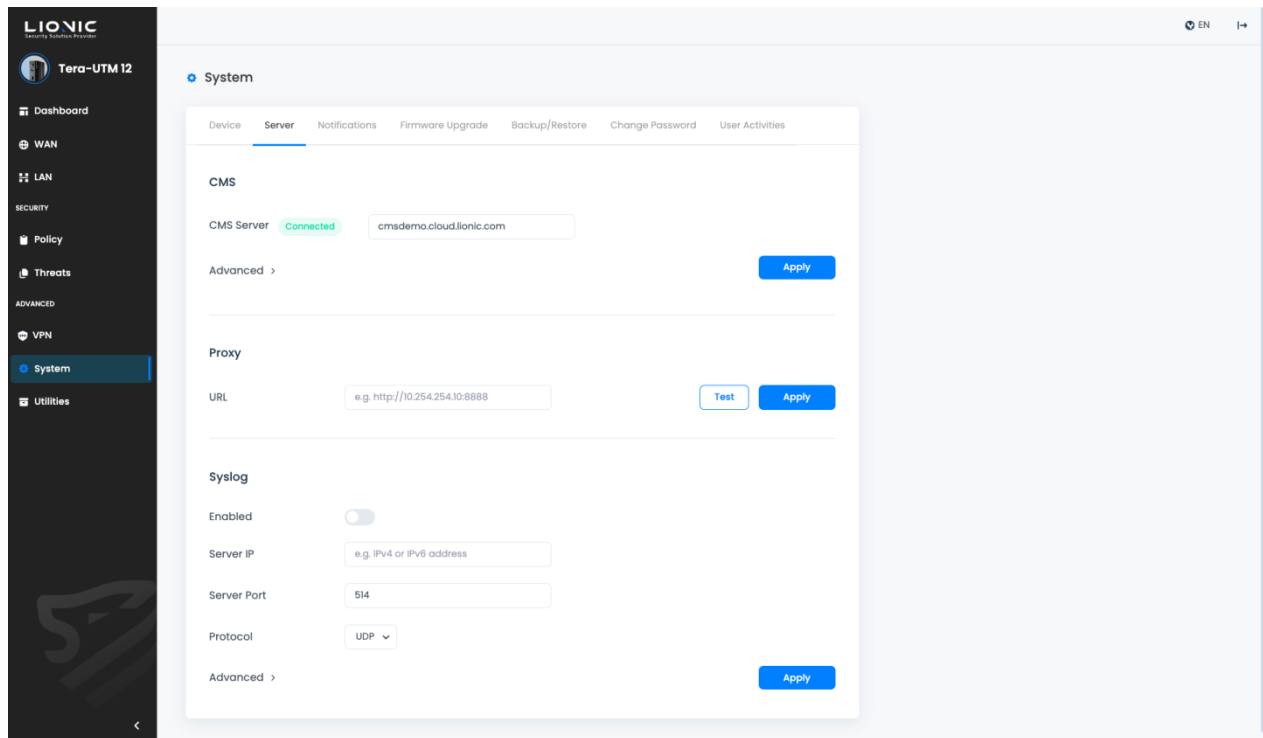
1. The activation code consists of 20 English letters and numbers. It can activate the license after applied successfully. If you did not receive the activation code when you purchase Tera-UTM 12 or if the activation code is not working, please contact local sales representatives in your region.
2. The renewal code consists of 16 English letters and numbers. It can extend the expiration date of the license after applied successfully. To purchase the renewal code, please contact local sales representatives in your region.

Date & Time

Display and configure the system time of Tera-UTM 12.

- **Time Zone:** Select your local time zone.
- **Automatically sync date & time with:** Add or remove NTP server based on your demand.

Server:



System-Server

CMS

Central Management System (CMS) can monitor and control multiple Tera-UTM 12 in 1 portal. After the CMS is built, enter the address of CMS into the input field and click [Apply] to connect Tera-UTM 12 with the CMS. Please contact Tera-UTM 12 sales representatives or resellers in your region for more information.

Proxy

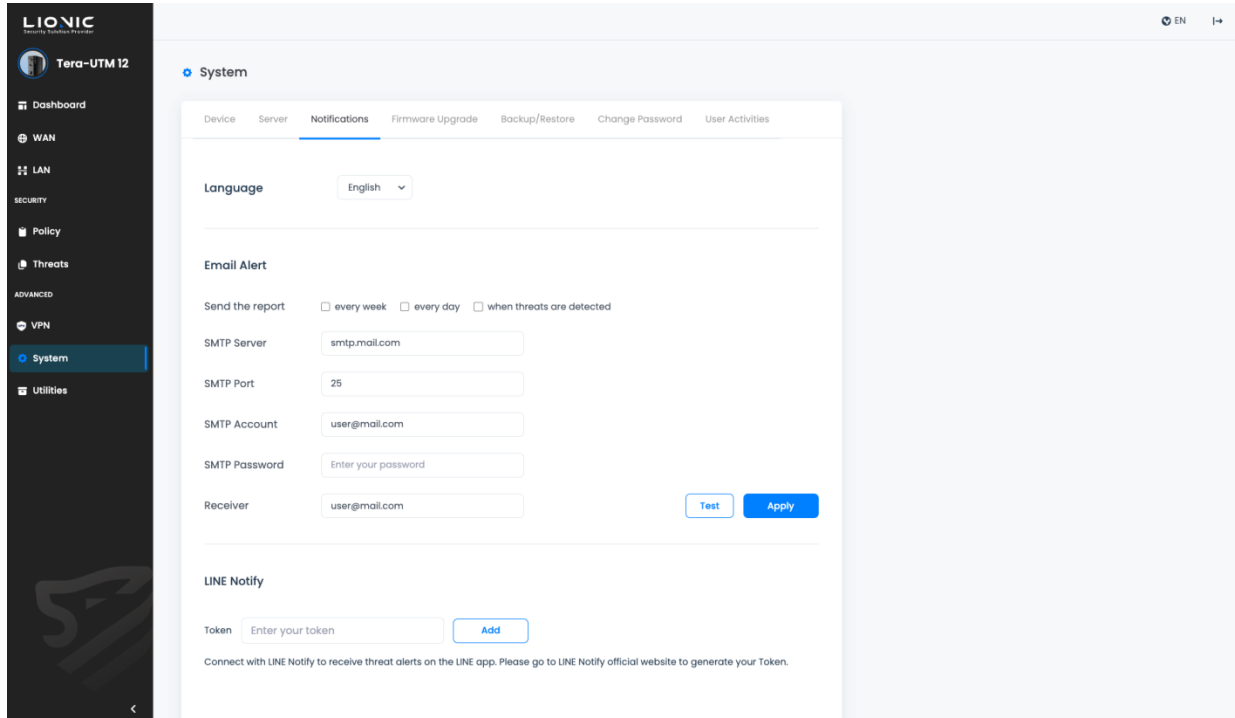
To obtain the full protection from Tera-UTM 12, the proxy server can help Tera-UTM 12 deployed in an intranet access LIONIC cloud services. After the proxy server is built, enter the server address into the input field and click [Apply] to access LIONIC cloud services via the proxy server. Please contact your IT administrator for more information.

Syslog

A syslog server can collect operating history of Tera-UTM 12. If you have your own syslog server, enter the configuration into the input field and click [Apply].

Notifications:

When a threat is detected, Tera-UTM 12 can notify the details to the mail address or LINE account you set in [Notifications] tab. Furthermore, Tera-UTM 12 can also summarize Inspection History, Threats Statics and System Notification every day or every week, and send Daily Report or Weekly Report to the mail address you set.



System-Notifications

- Language: Select the language you prefer for mails, LINE messages or reports.
- Send the report:
 - Every week: send a weekly report at 0:00 on every Sunday.
 - Every day: send a daily report at 0:00 everyday.
 - When threats are detected: send a notification mail or message whenever a threat is detected.
- SMTP Server, Port, Account and Password: SMTP settings used to send mails or reports.
- Receiver: The mail address which you would like to receive mails or reports.

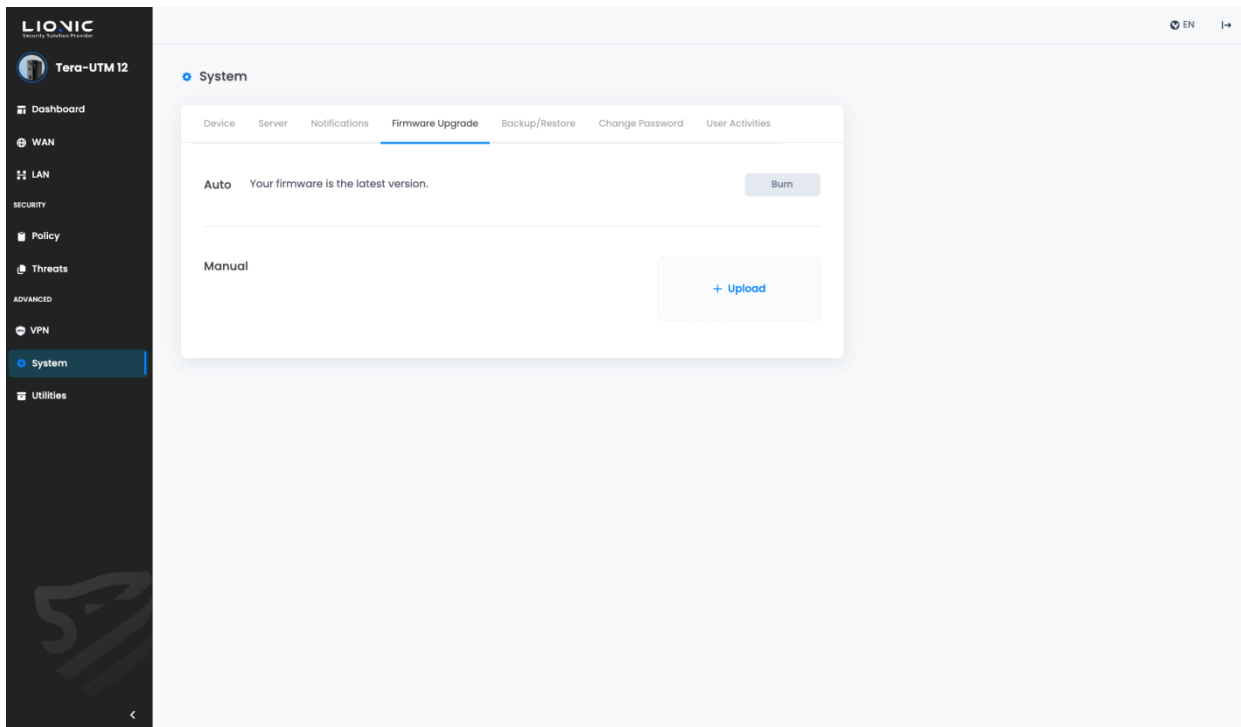
Enter the configuration into the input field and click [Apply], then click [Test] to make sure the setting is correct.

* Remark: If you would like to use Gmail account as the sender (SMTP account), please enable “2-step Verification” in Gmail and create “App Password” to fill the SMTP Password field.

Before setting up LINE Notify, please go to LINE Notify official website to generate your Token. Enter your Token to the input field and click [Add], then the threat notification will be sent to your LINE app.

Firmware Upgrade:

A notification will be shown on [Firmware Upgrade] tab when a new firmware is available. Click [Burn] to upgrade.



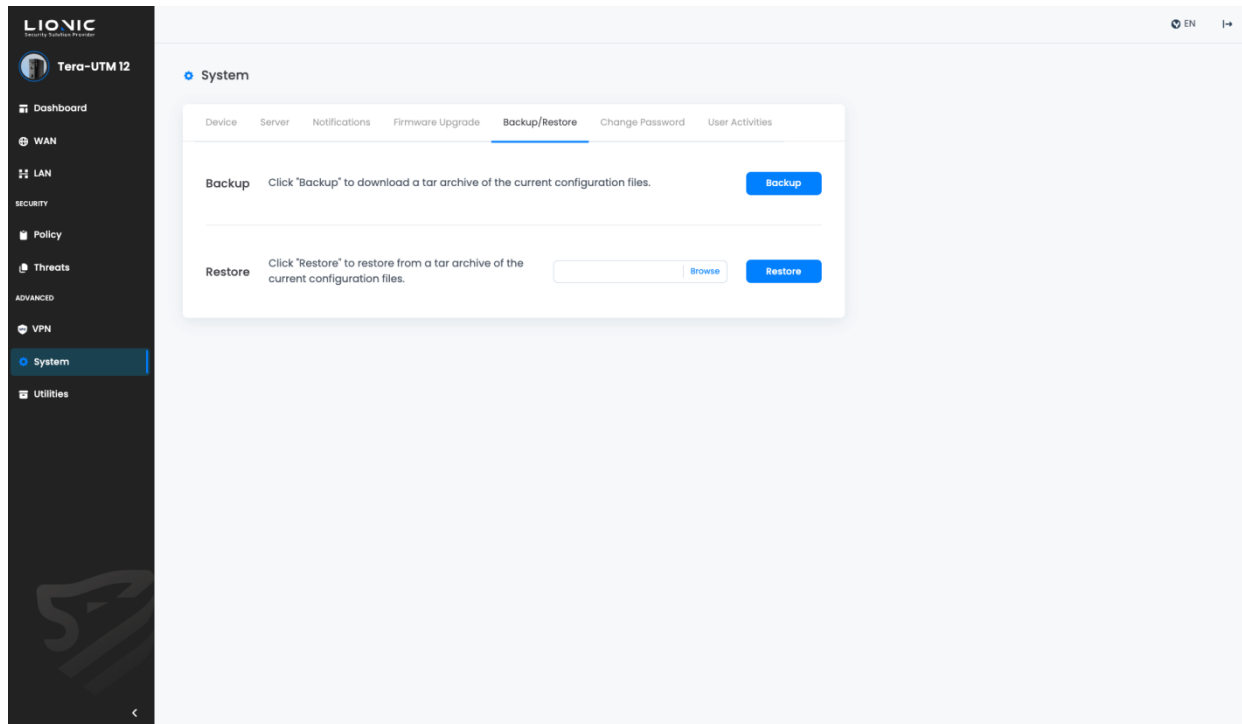
System-Firmware Upgrade

To upgrade or re-install the firmware manually during troubleshooting, click [+ Upload], select the correct firmware file and start upgrading or re-installing.

* Remark: Tera-UTM 12 would reboot during upgrading firmware. The network connection will resume after the reboot is completed.

Backup / Restore:

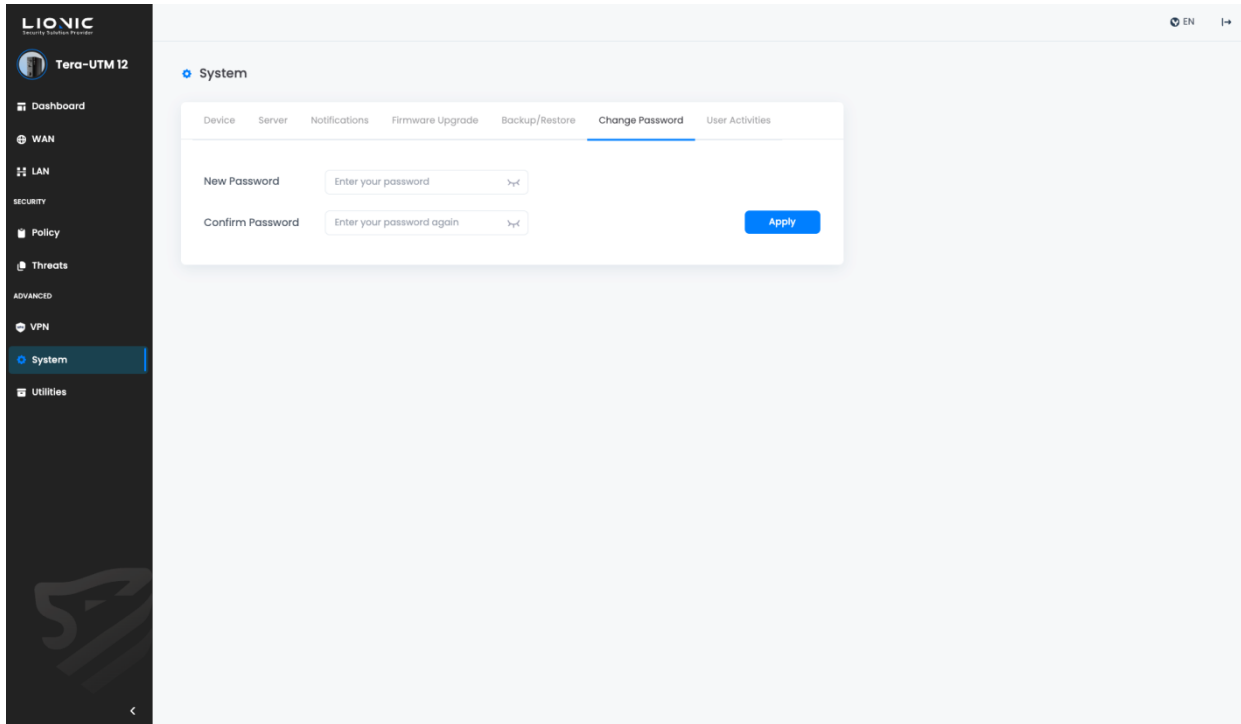
[Backup / Restore] function can backup Tera-UTM 12 configurations, such as security policies and whitelist setting, and restore on the same or other Tera-UTM 12.



System-Backup / Restore

Change Password:

To change the login password of the web GUI, enter the new password to the input field and click [Apply].

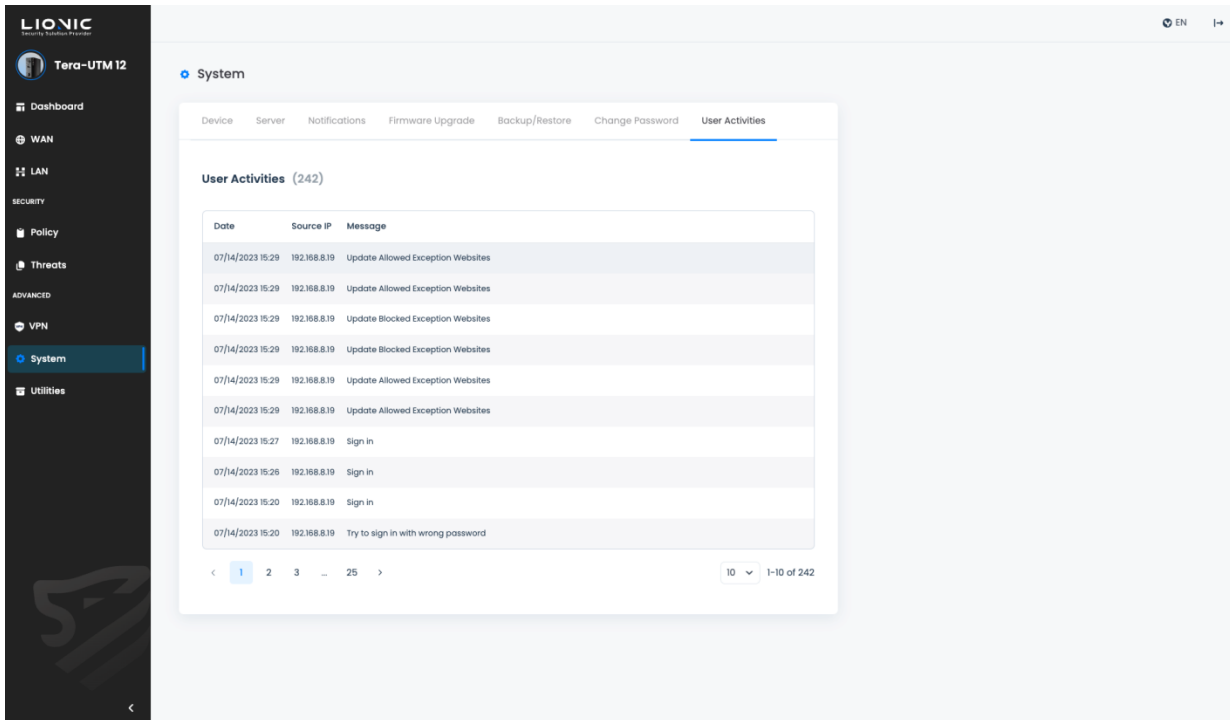


The screenshot displays the Tera-UTM 12 Web GUI interface. On the left is a dark sidebar with a menu including Dashboard, WAN, LAN, SECURITY, Policy, Threats, ADVANCED, VPN, System (highlighted), and Utilities. The main content area has a light blue header with the 'System' tab selected. Below the header, there are tabs for Device, Server, Notifications, Firmware Upgrade, Backup/Restore, Change Password (active), and User Activities. The 'Change Password' form contains two input fields: 'New Password' with the placeholder 'Enter your password' and 'Confirm Password' with the placeholder 'Enter your password again'. Both fields have a password icon (an eye with a slash) to the right. A blue 'Apply' button is located to the right of the 'Confirm Password' field.

System-Change Password

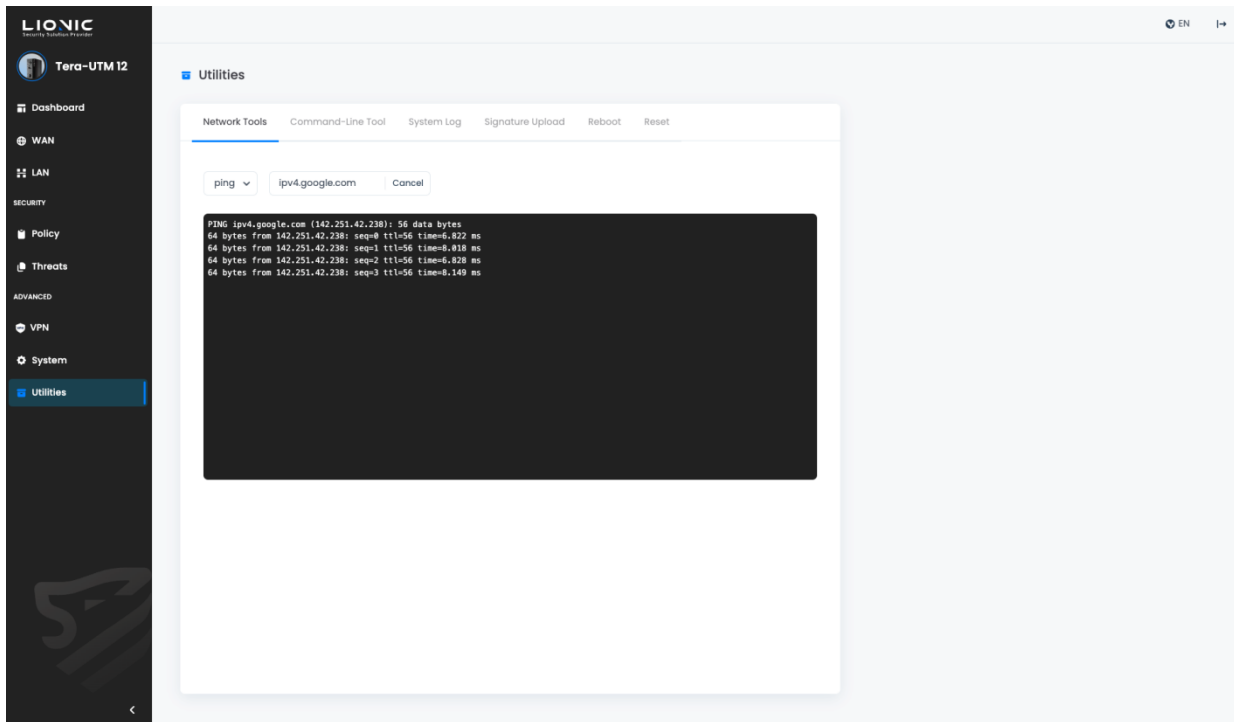
User Activities:

All configuration changes would be listed on [User Activities] tab.



System-User Activities

Utilities



Utilites

Tera-UTM 12 provides the following troubleshooting function:

- **Network Tools:** Find network connection issue with “ping”, “traceroute”, “nslookup” functions.
- **Command-Line Tool:** An advanced troubleshooting function. Contact LIONIC technical support before using this function.
- **System Log:** Export the system log for the technical support when troubleshooting.
- **Signature Upload:** Upload signatures manually when troubleshooting.
- **Reboot:** Reboot Tera-UTM 12 immediately or setup a daily reboot schedule.
- **Reset:** Reset all configuration to the factory default settings.

* Remark: While the license is valid and Internet is connected, Tera-UTM 12 would automatically download and update the signature.

Tera-UTM 12 Makes Security Simple



© Copyright 2023 Lionic Corp. All rights reserved.

Sales Contact
Tel : +886-3-5789399
Fax : +886-3-5789595
Email : sales@lionic.com

Lionic Corp.
<https://www.lionic.com/>
1F-C6, No.1, Lising 1st Rd.,
Science-Based Industrial Park,
Hsinchu City 300, Taiwan, R.O.C.