

# Web GUI User Manual

# Tera-UTM 12

Version 1.4.1

Released on Feb 2025



---

# Tera-UTM 12 User Manual

Copyright © 2025, 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 Vitalwerks Internet Solutions, LLC..

## 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](mailto:support@lionic.com)    Tel: +886-3-5789399    Fax: +886-3-5789595

## Content

|                                                        |           |
|--------------------------------------------------------|-----------|
| <b>Access Web GUI and Connect to the Network .....</b> | <b>4</b>  |
| <b>Overview.....</b>                                   | <b>6</b>  |
| <b>Dashboard.....</b>                                  | <b>8</b>  |
| <b>WAN.....</b>                                        | <b>10</b> |
| Configuration .....                                    | 10        |
| Remote Control.....                                    | 11        |
| <b>LAN .....</b>                                       | <b>13</b> |
| Connection Mode .....                                  | 13        |
| LAN .....                                              | 14        |
| DHCP.....                                              | 15        |
| Port Forwarding .....                                  | 16        |
| Static Route.....                                      | 16        |
| <b>Policy .....</b>                                    | <b>17</b> |
| Anti-Virus, Anti-Intrusion, Anti-WebTheat .....        | 17        |
| Anti-Region .....                                      | 21        |
| Firewall .....                                         | 22        |
| Exceptional Websites .....                             | 23        |
| SSL / TLS Inspection .....                             | 24        |
| <b>Threats .....</b>                                   | <b>26</b> |
| <b>ICS ACL .....</b>                                   | <b>28</b> |
| Policy .....                                           | 28        |
| Events .....                                           | 29        |
| <b>Assets.....</b>                                     | <b>30</b> |
| <b>Traffic.....</b>                                    | <b>31</b> |
| Monitor .....                                          | 31        |
| QoS.....                                               | 32        |

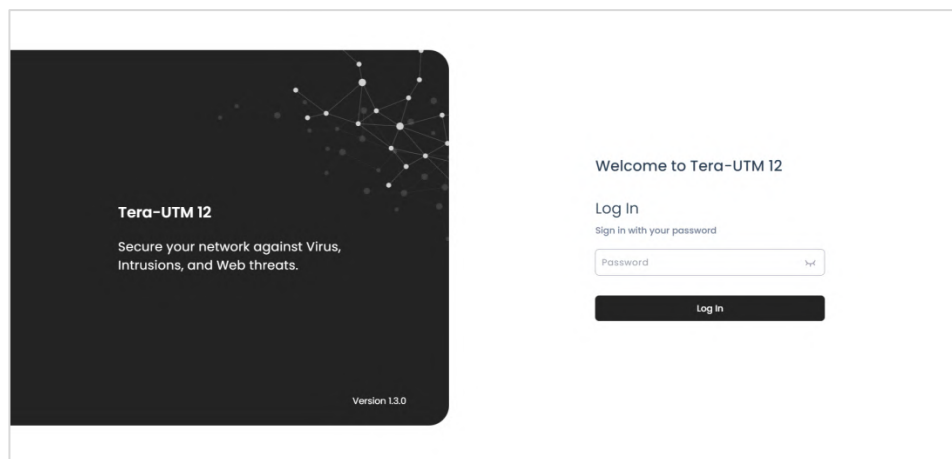
---

|                         |           |
|-------------------------|-----------|
| <b>Behavior.....</b>    | <b>34</b> |
| Policy .....            | 34        |
| Events .....            | 35        |
| <b>VPN Server .....</b> | <b>36</b> |
| <b>System .....</b>     | <b>38</b> |
| Device .....            | 38        |
| Server .....            | 40        |
| Notifications .....     | 42        |
| Firmware Upgrade .....  | 44        |
| Backup / Restore .....  | 45        |
| Change Password .....   | 46        |
| User Activities .....   | 47        |
| Summary Report .....    | 48        |
| <b>Utilities .....</b>  | <b>49</b> |



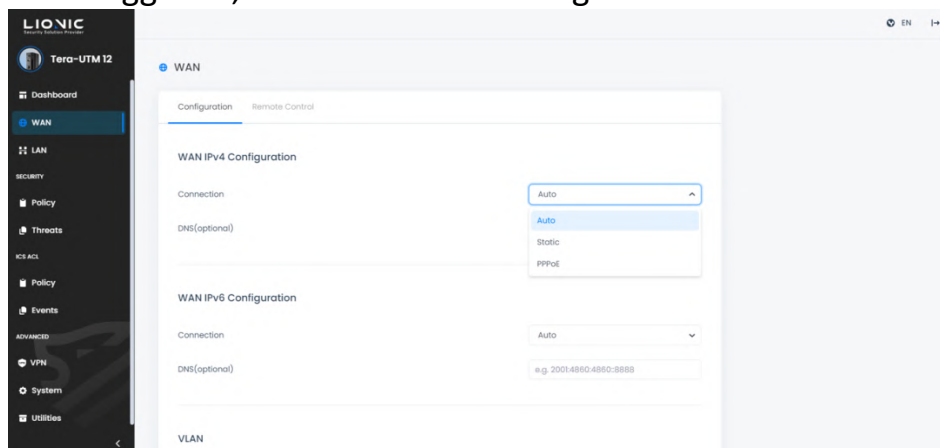
## Access Web GUI and Connect to the Network

1. Plug the power cable into Tera-UTM 12.
2. Connect the WAN port of Tera-UTM 12 to the LAN port of a modem / router / switch provided by the ISP or the IT administrator with an Ethernet cable.
3. Connect the LAN port of Tera-UTM 12 to your PC/Laptop with another Ethernet cable.
4. Set the network configuration of your PC/Laptop as below:
  - IP address: 10.254.254.50
  - Subnet mask: 255.255.255.0
5. After the configuration is set, visit <https://10.254.254.254/> with a web browser.



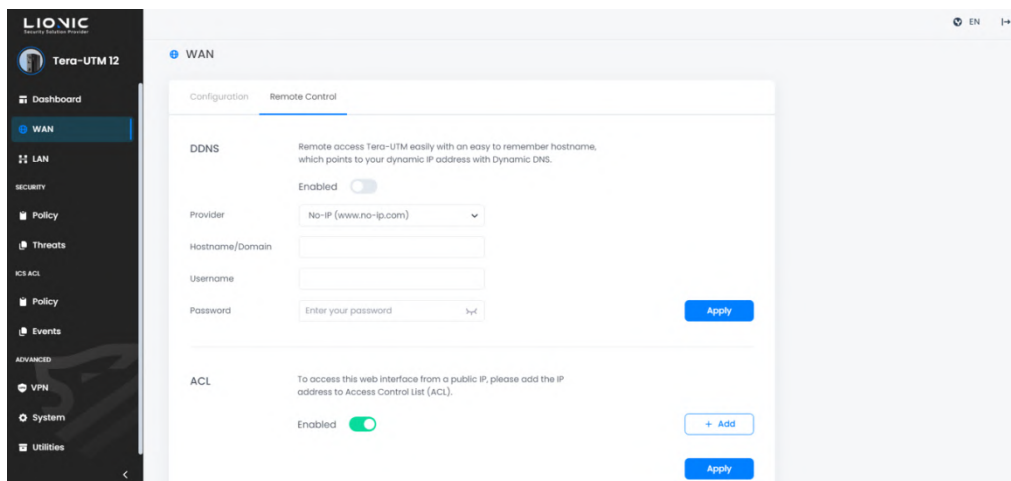
Login page

6. The default password for login is the Serial Number (S/N) shown at the bottom of the product.
7. After logged in, set the network configuration of Tera-UTM 12 in [WAN] page.



WAN-WAN IP

8. After Tera-UTM 12 obtained a valid IP address, resume the network configuration of your PC/Laptop. Thereafter, you can access the web GUI by the following method:
- When both Tera-UTM 12 and your PC/Laptop are using private IP addresses in the same subnet, and the PC/Laptop is located at the LAN side of Tera-UTM 12, visit <https://mytera.lionic.com/> to access the web GUI.
  - When Tera-UTM 12 and your PC/Laptop are using different public IP addresses, and the PC/Laptop is located at the LAN side of Tera-UTM 12, access the web GUI by visiting <https://10.254.254.254/> as mentioned above, go to [WAN] > [Remote Control] page and disable [ACL] (or add the IP address of the PC/Laptop to the ACL). After that, visit <https://mytera.lionic.com/> to access the web GUI.



WAN-Remote Control

## 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.

### ICS ACL:

- **Policy:** Detect commonly used communication protocol packets for industrial control systems and customize security rules to enable or disable functions during device communication.
- **Events:** Display the protection logs of industrial control security features.

### Management:

- **Assets:** The asset management feature can list the identified LAN devices and block or allow specific assets to connect to the network.
- **Traffic:** Traffic management can list the current connection usage of each LAN

device and perform bandwidth management.

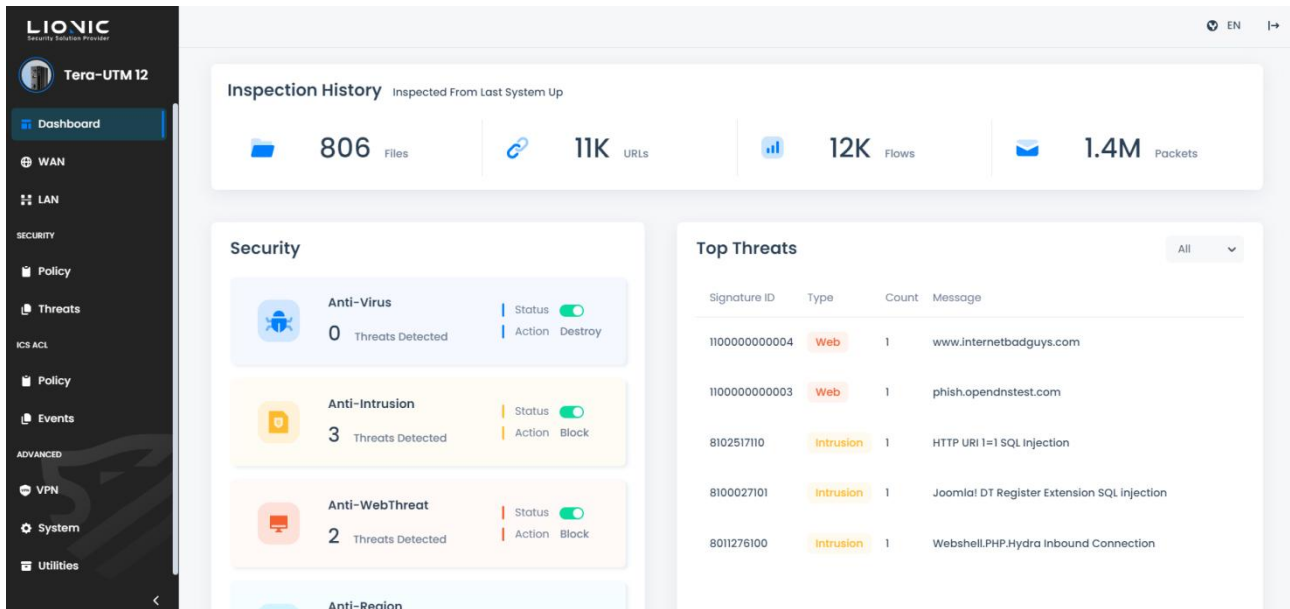
- **Behavior Management:** The behavior management feature allows you to manage specific content categories or applications.

### 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.

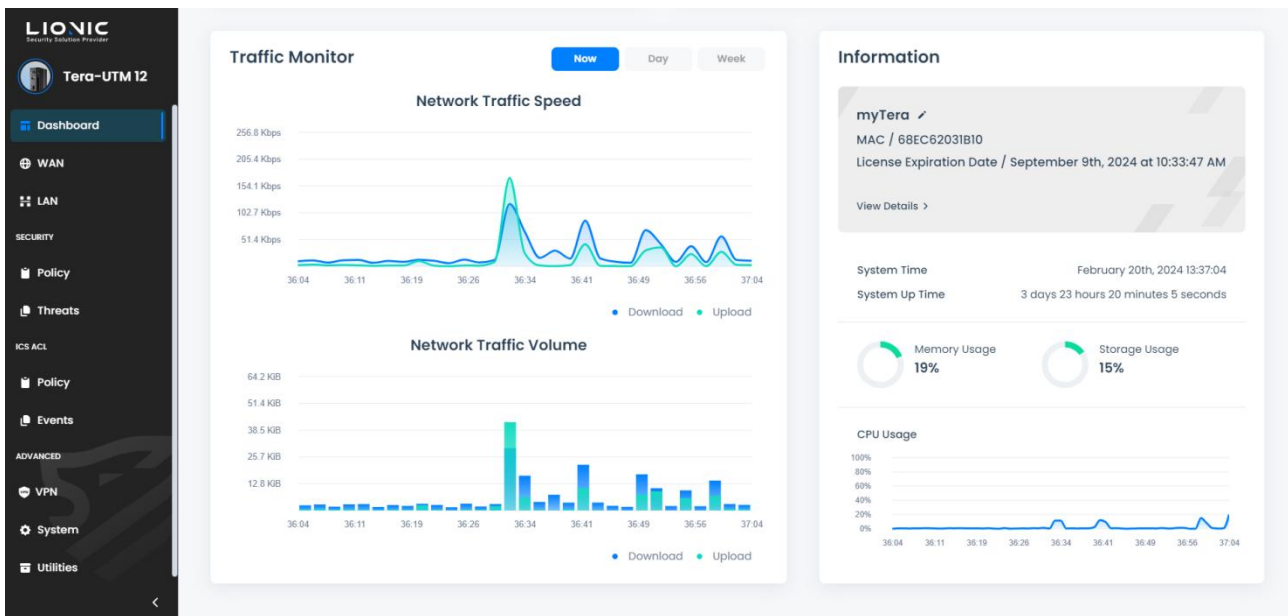


Dashboard

**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

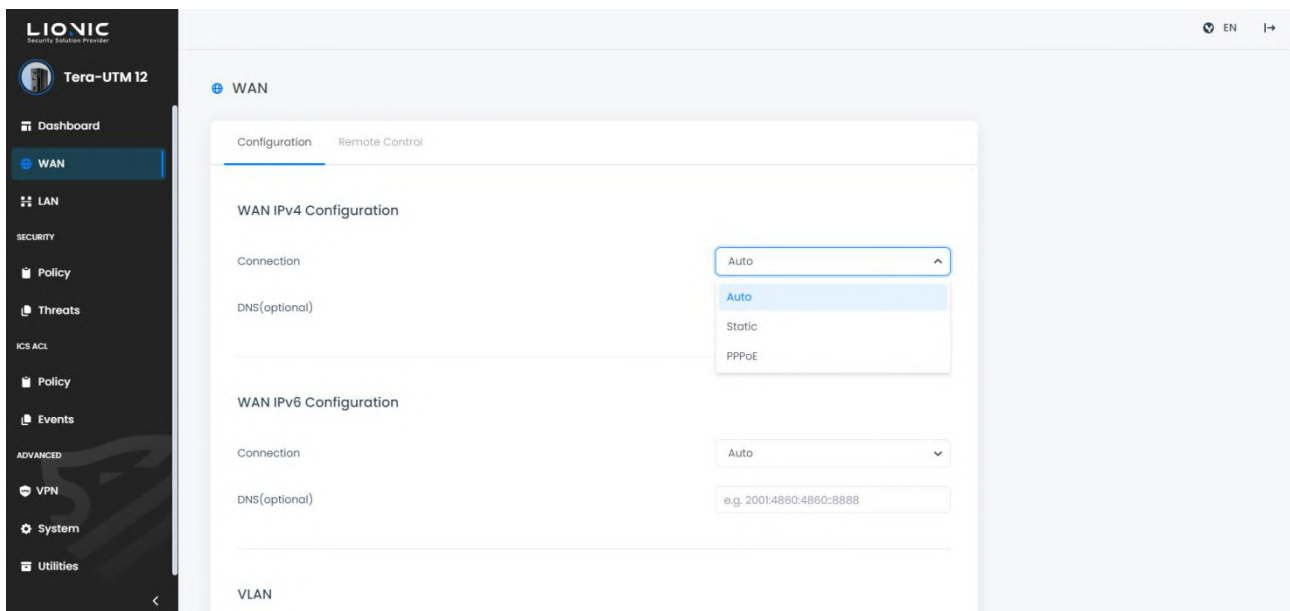
**Traffic Monitor:** Showing the download and upload traffic via Tera-UTM 12.

**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.



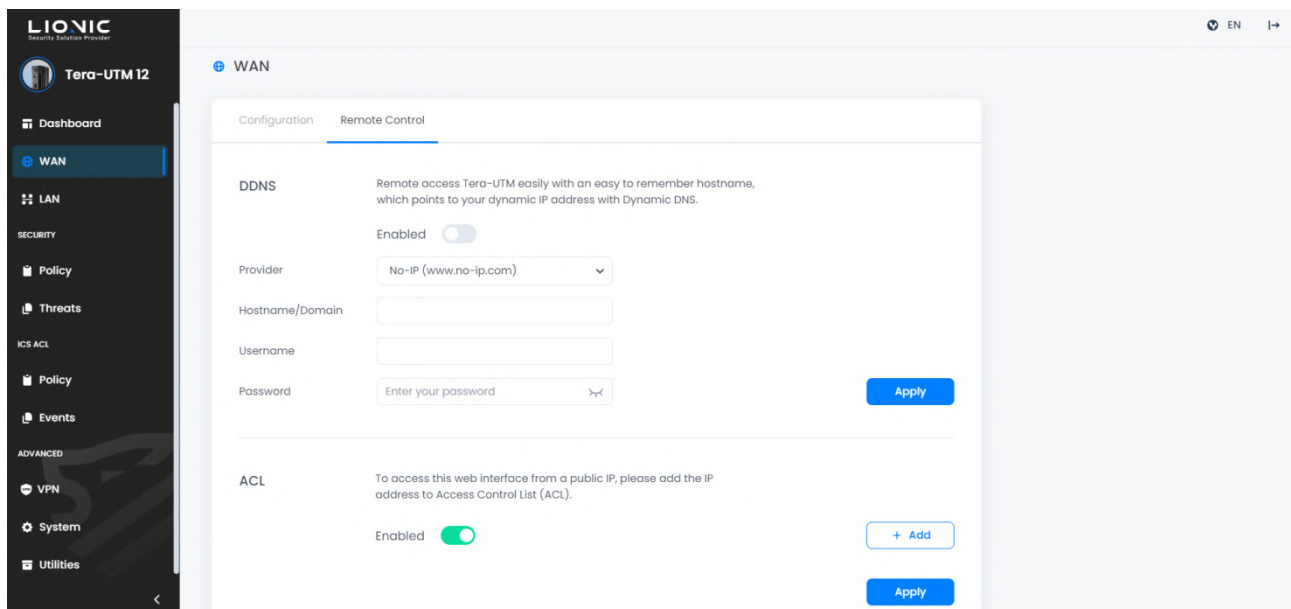
WAN- Configuration

- **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.
- **VLAN :** When Tera-UTM 12 is deployed in a VLAN environment, you can enter the VLAN ID of the domain to which Tera-UTM 12 belongs here.

\* 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].

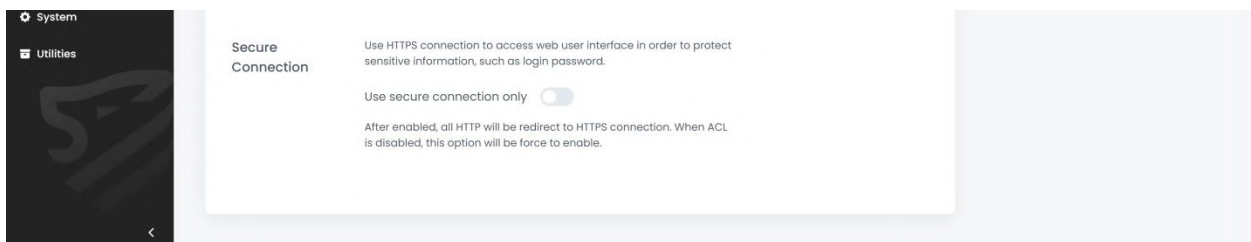
**Step 2:** Enter the IP address that would be used to access Tera-UTM 12 in the input field.

**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

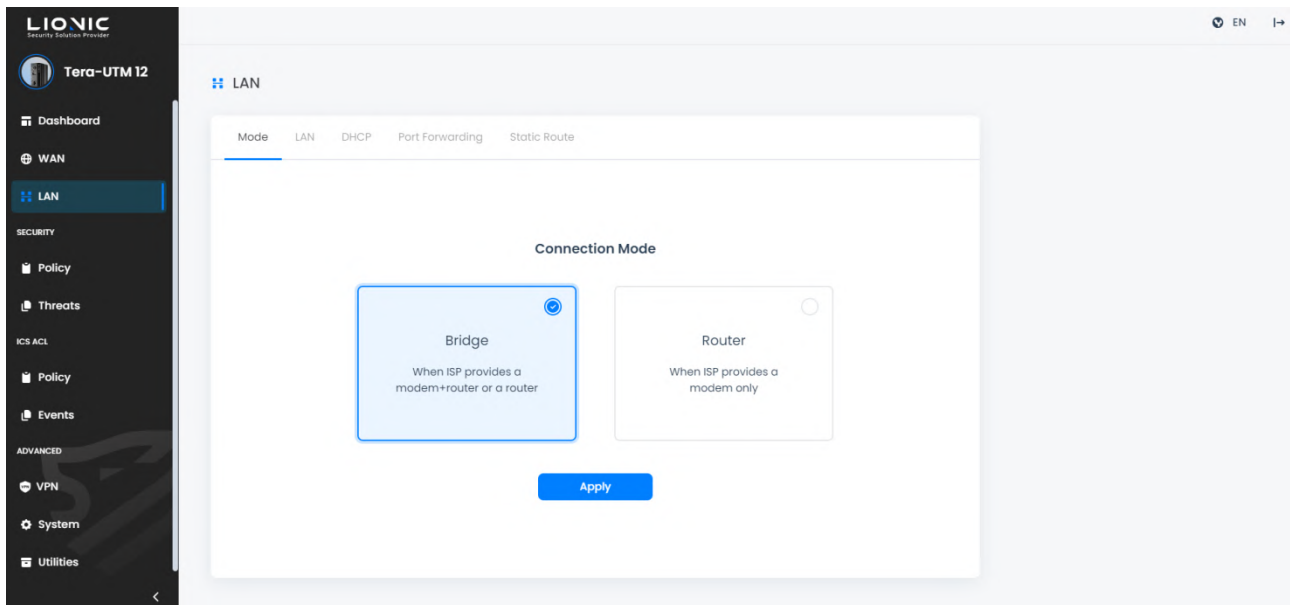
### Secure Connection

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 forced to enable.

## LAN

### Connection Mode

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



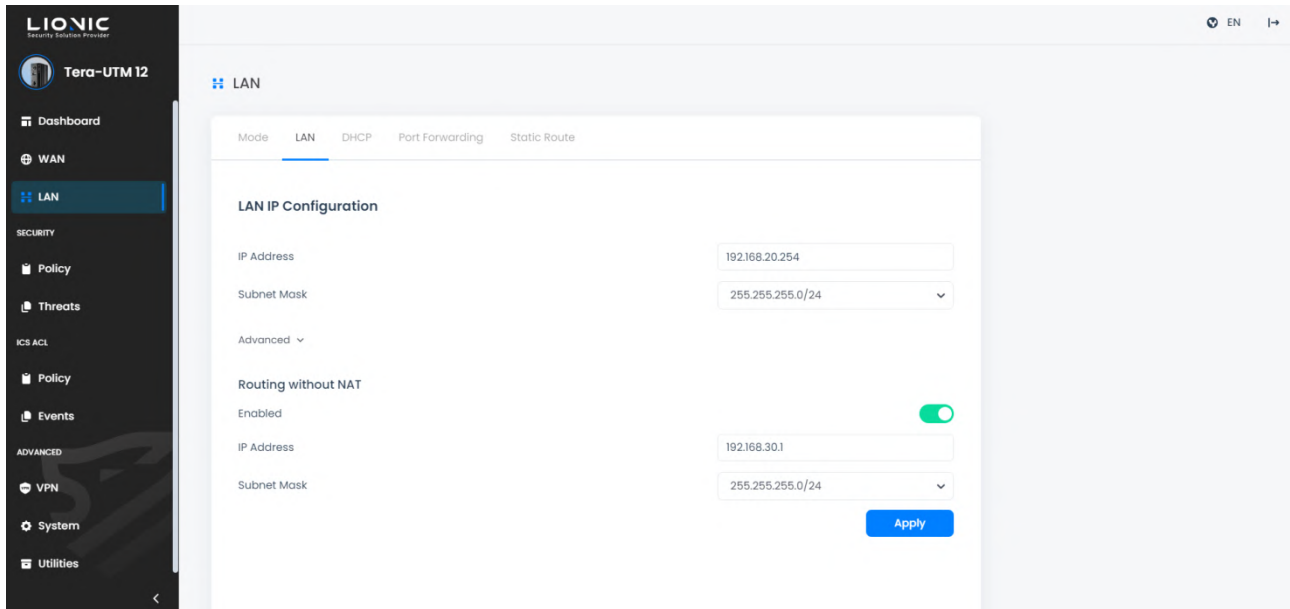
LAN-Connection Mode

- **Bridge mode (default):**  
DHCP is disabled to LAN devices in [Bridge] mode. Please connect Tera-UTM 12 to the LAN side of a router.
- **Router mode:**  
DHCP is enabled 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.

## LAN

In [Router Mode], users can independently set the local network IP subnet. After entering the designated subnet into the input box, click [Apply], and DHCP Server will automatically assign IP addresses within the configured range.



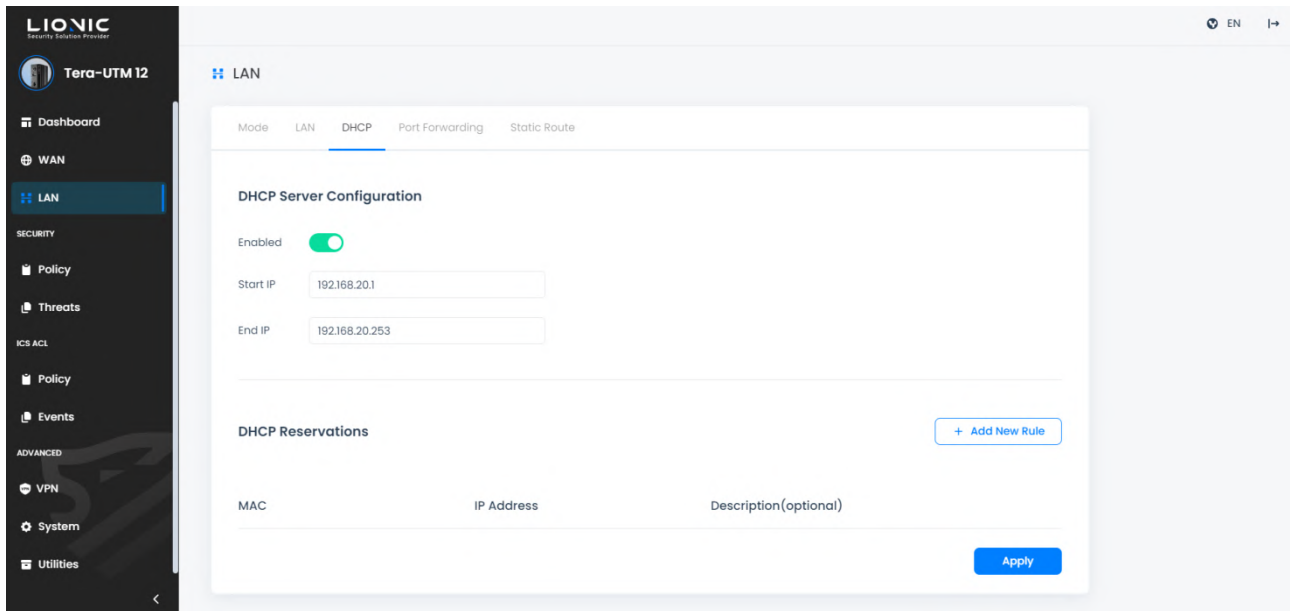
LAN-LAN IP

### - Routing without NAT

In [Router Mode], users can independently set the IP subnet for non-NAT routing. When there is no need for NAT translation between the external network and the internal network, enter the designated subnet into the input box and click [Apply] to enable this feature.

## 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 Server Configuration

- **Enable:** Enable/Disable DHCP Server Function
- **Start IP Address and End IP Address:** The IP range that the DHCP server will assign based on the customized IP address settings in [LAN] > [LAN] > [LAN IP Configuration]

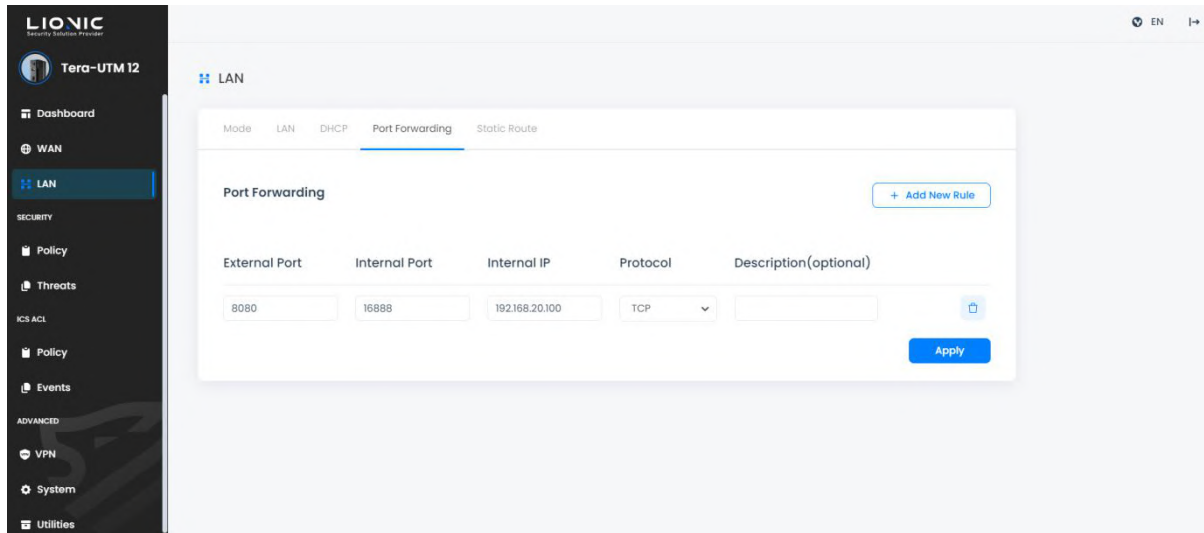
### DHCP Reservations

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

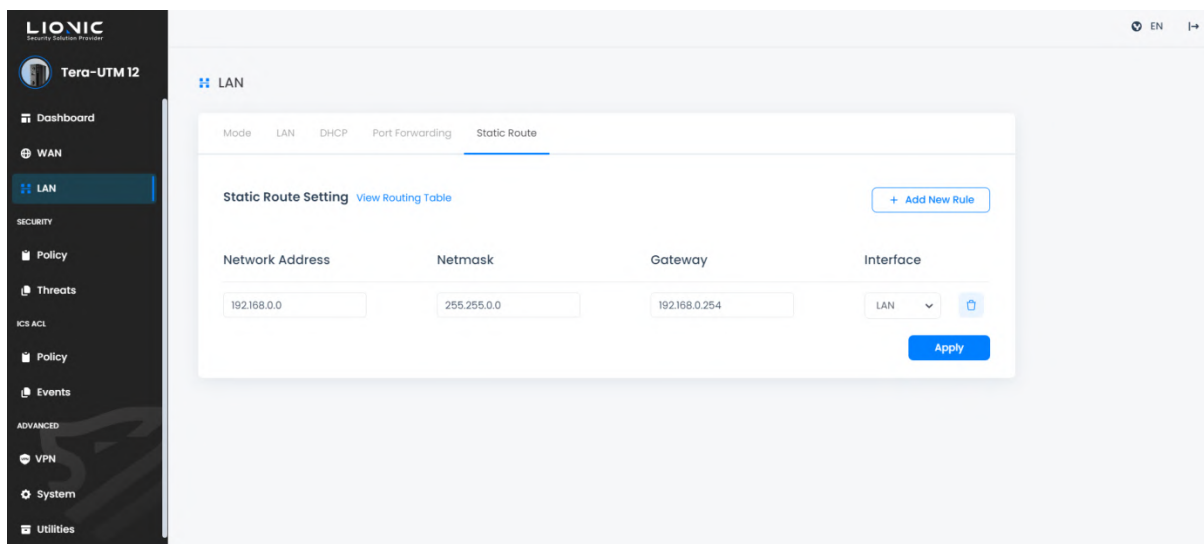
In [Router] mode, Tera-UTM 12 supports [Port Forwarding]. If you need to access a LAN device from Internet, set the internal port and internal IP address to access the LAN device through a specific external port.



LAN-Port Forwarding

## Static Route

In [Router Mode], the Tera-UTM 12 can provide static routing functionality. This feature can be used when there is a need to connect different network segments.



LAN-Static Route

## Policy

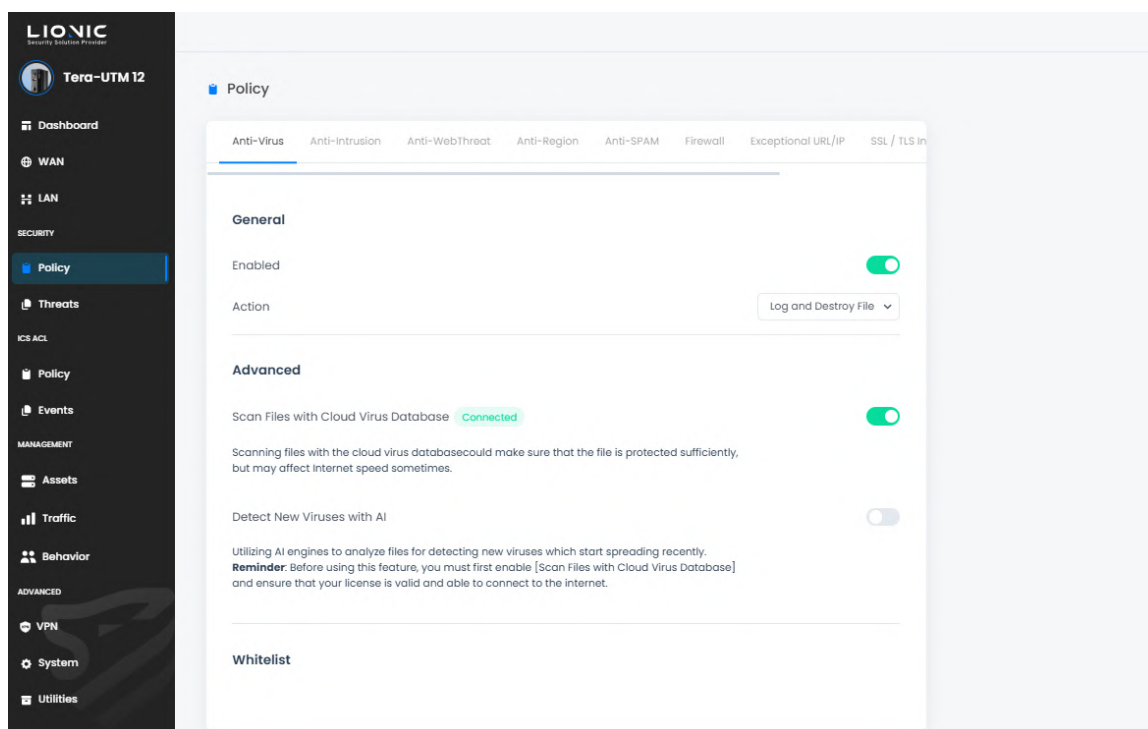
### Anti-Virus, Anti-Intrusion, Anti-WebTheat

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 /<br>Log and Destroy File                                                                                             | Log Only /<br>Log and Block                                                                                                                                                                                 | Log Only /<br>Log and Block                                                                                                         |
| Advanced  | <ul style="list-style-type: none"> <li>- Scan Files with Cloud Virus Database</li> <li>- Detect New Viruses with AI</li> </ul> | <ul style="list-style-type: none"> <li>- Block Brute-force attacks</li> <li>- Block Protocol Anomaly,</li> <li>- Block Port Scan and DoS Attacks,</li> <li>- Keep PCAP when a threat is detected</li> </ul> | <ul style="list-style-type: none"> <li>- Configure External Database for Malicious Webpages</li> <li>- External Database</li> </ul> |
| Whitelist | View and remove whitelist rule                                                                                                 | View and remove whitelist rule                                                                                                                                                                              | View and remove whitelist rule                                                                                                      |

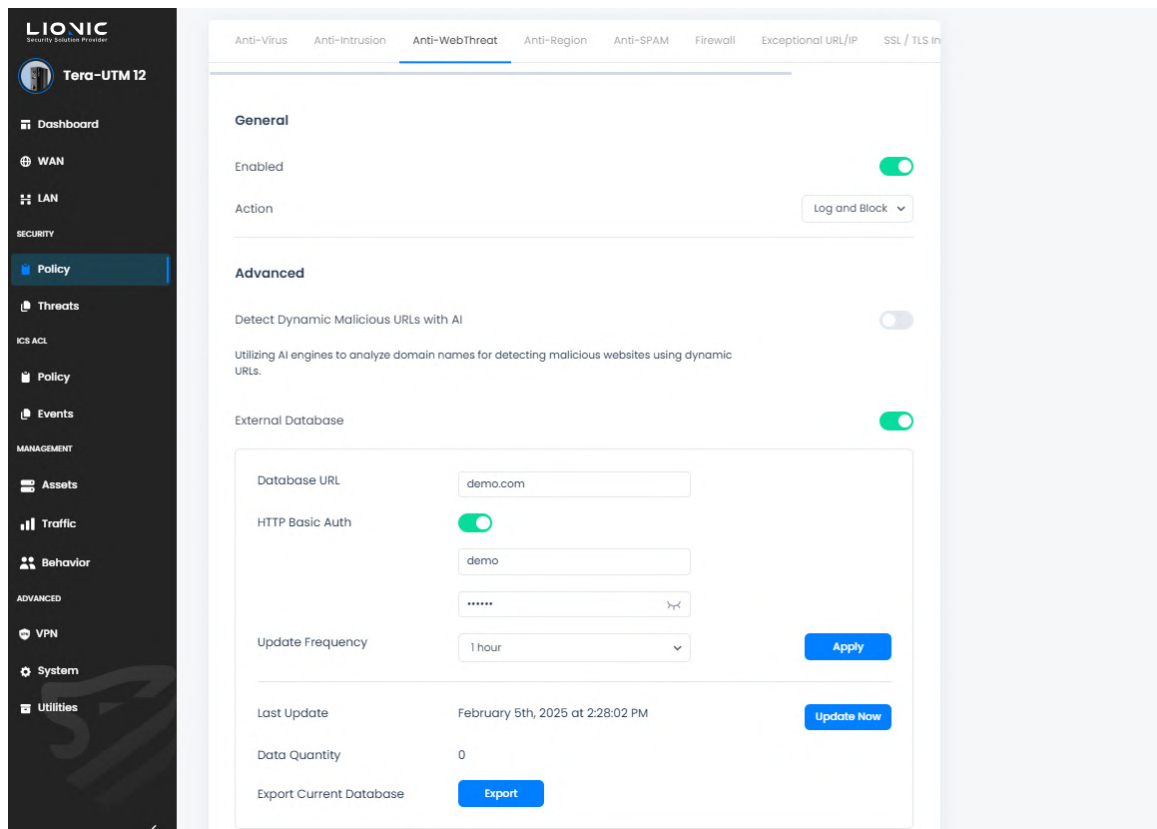


Policy

- **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.
- **Detect New Viruses with AI:** The AI Anti-Virus engine is integrated into the Lionic Anti-Virus Query Cloud. When this feature is enabled, the AI-powered engine enhances the detection of Zero-Day viruses.
- **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 enabling this feature, Tera-UTM 12 's

[Anti-Intrusion] can detect abnormal packets that do not comply with communication protocol specifications and block them.

- **Block Port Scan and Dos Attacks:**
  - Prevent DoS attacks that involve a rapid increase in connections for TCP, TCP half-open, UDP, ICMP, SCTP, and IP protocols in a short period.
  - Block devices that send a large number of packets in abnormal formats.
  - Block communication port scanning attempts such as TCP SYN scan, TCP RST scan, and UDP scan.
- **Keep PCAP when a threat is detected:** After enabling this feature, Tera-UTM 12 will save packets considered as threats when detected in [Anti-Intrusion], allowing for subsequent analysis.
- **Detect Dynamic Malicious URLs with AI:** After enabling this feature, the Tera-UTM 12 will compare the connected URLs with the cloud database and use the AI Anti-WebThreat DGA Detection Model to determine if it is a DGA domain.
- **External Database:** Allow users to configure external data sources to meet advanced protection requirements.



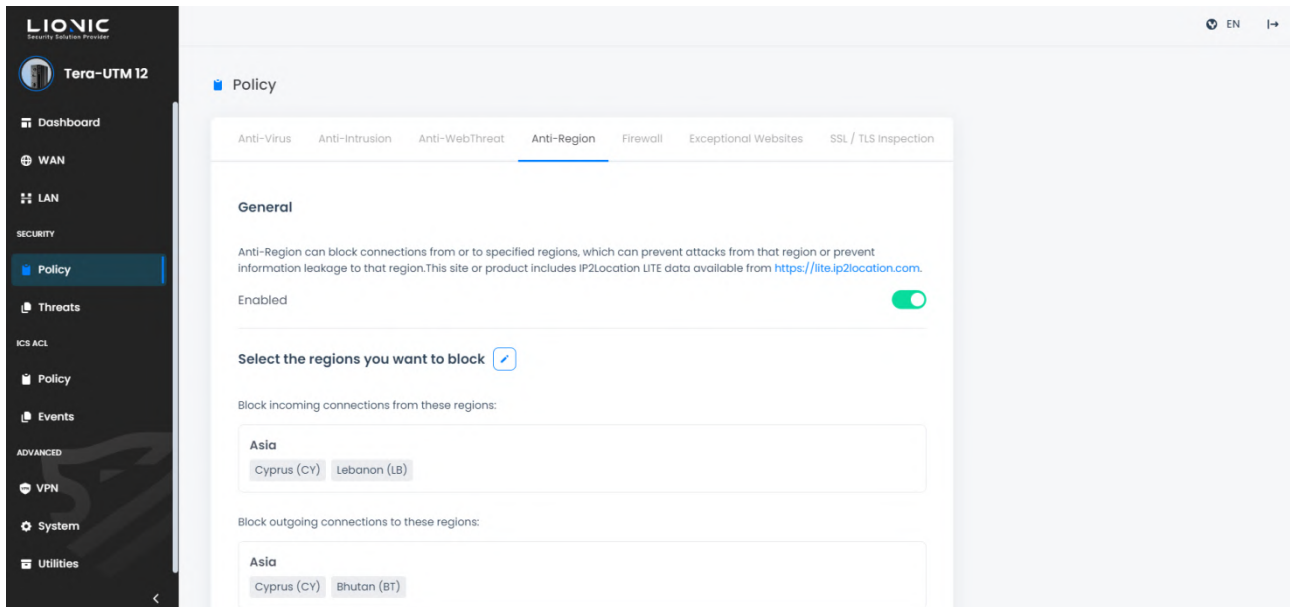
Anti-WebThreat- External Database



- 
- **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.

## Anti-Region

Based on the user-configured country/region, block attacks from that region or prevent information leakage to that region by blocking IP addresses.

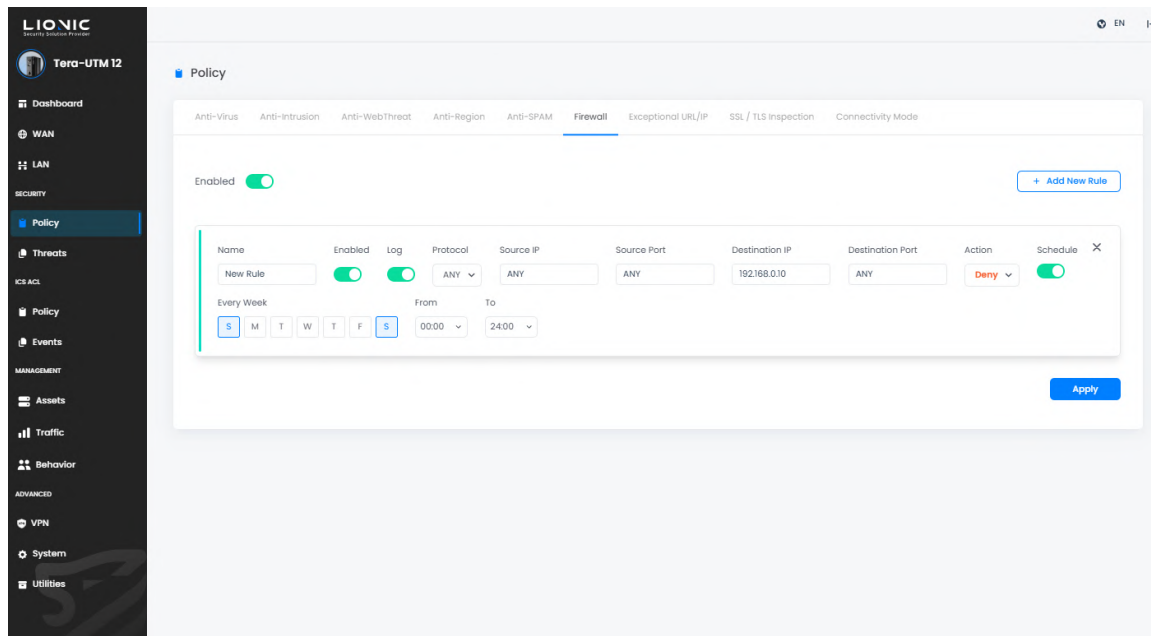


Policy- Anti-Region

- **Step 1:** Enable Geographical Blocking.
  - **Step 2:** Click Select Allow/Block Region.
  - **Step 3:** Enter the respective configuration values.
  - **Step 4 :** After clicking [Yes], the changes will take effect.
- 
- **Whitelist:** Whitelist exceptions can be configured based on the countries/regions that have been set.

## Firewall

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



Policy-Firewall

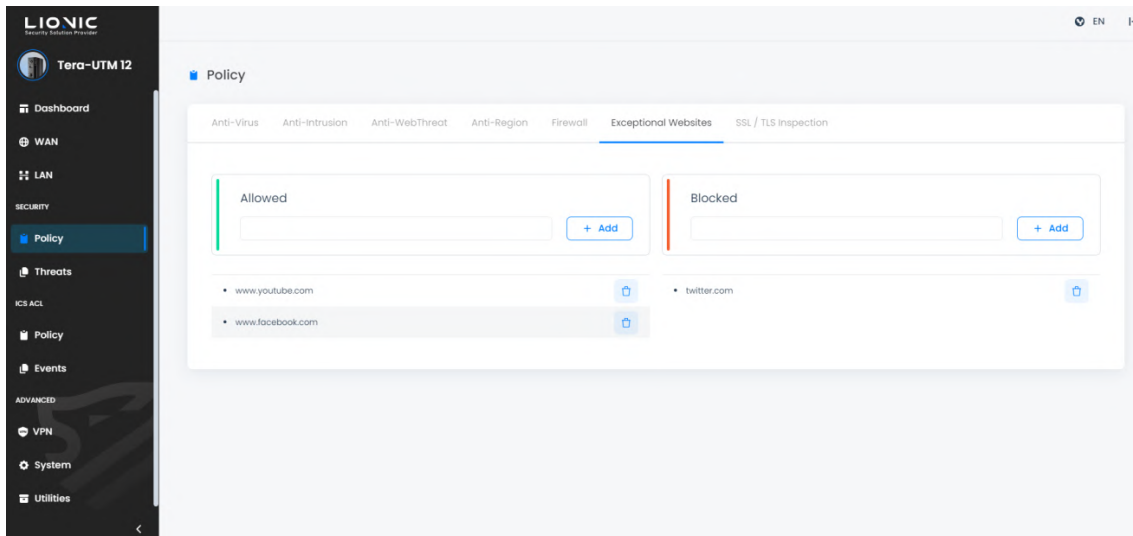
- **Step 1:** Enable the firewall (default is enabled).
- **Step 2:** Click [+Add New Rule].
- **Step 3:** Fill each configuration.
- **Step 4:** Click [Apply] to take effect.

### 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.
- **Schedule:** Schedule the effective time for firewall rules.

## Exceptional Websites

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



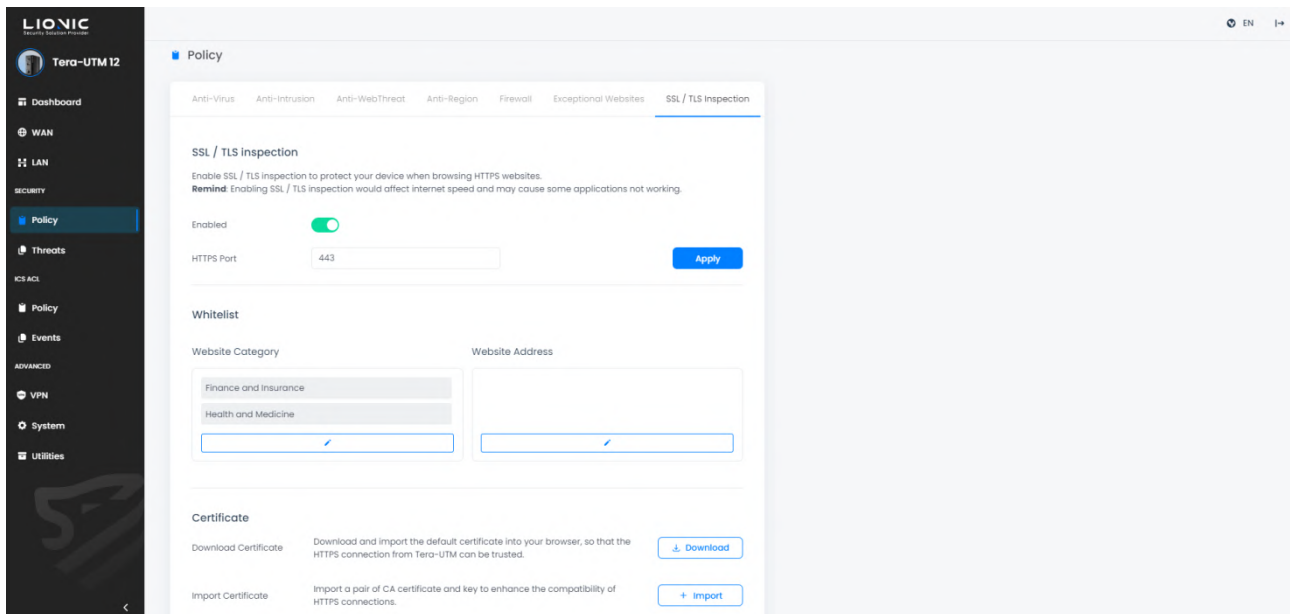
Policy-Exceptional Websites

- **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:

1. Enabling [SSL / TLS Inspection] would affect internet speed and may cause some applications not working.
2. 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

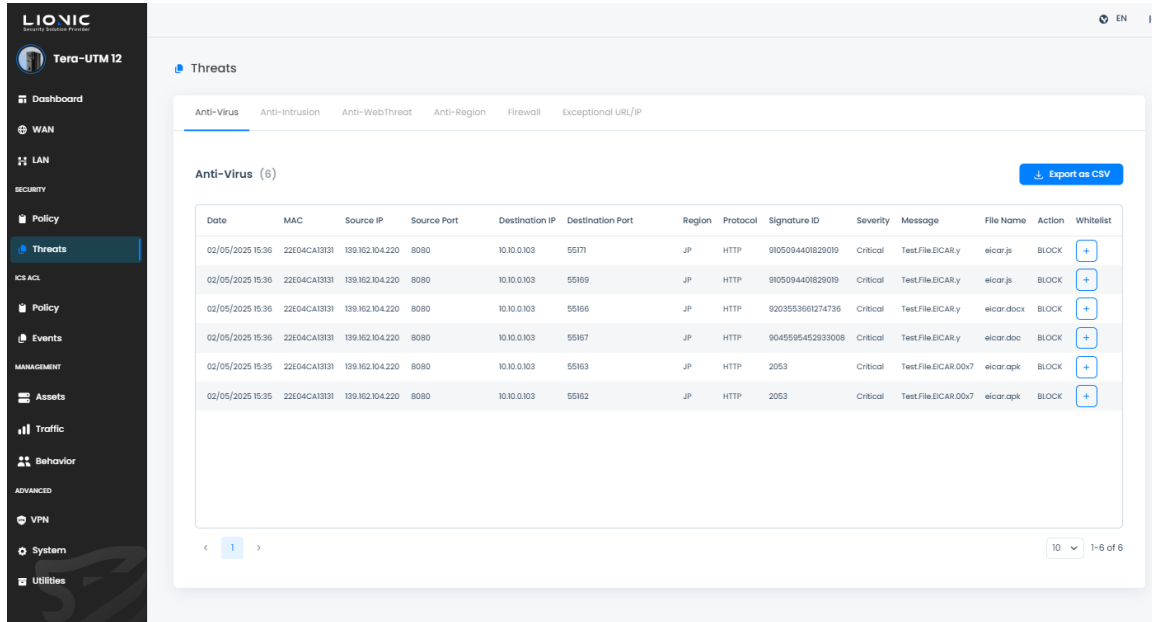
whitelist options. The categories in the default whitelist are “Finance and Insurance” and “Health and Medicine”. After a category is added into the whitelist, the website that classified as the category will not be inspected.

- **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.
- **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.
- 

\*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.

## 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.



The screenshot shows the Tera-UTM 12 interface with the 'Threats' page selected. The 'Anti-Virus' tab is active, displaying a table of 6 detected threats. The table includes columns for Date, MAC, Source IP, Source Port, Destination IP, Destination Port, Region, Protocol, Signature ID, Severity, Message, File Name, Action, and Whitelist. Each row represents a threat event, and a '+ ' button is available for each entry to add it to the whitelist.

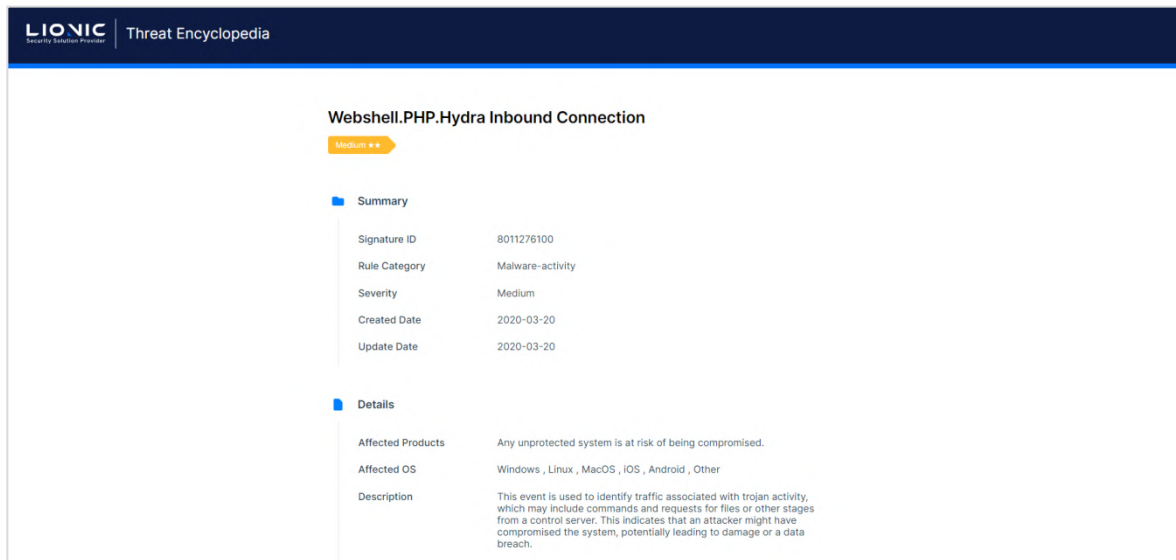
| Date             | MAC          | Source IP       | Source Port | Destination IP | Destination Port | Region | Protocol | Signature ID     | Severity | Message             | File Name  | Action | Whitelist |
|------------------|--------------|-----------------|-------------|----------------|------------------|--------|----------|------------------|----------|---------------------|------------|--------|-----------|
| 02/05/2025 15:36 | 22E04CA13331 | 139.162.104.220 | 8080        | 10.10.0.103    | 55171            | JP     | HTTP     | 9105094401829019 | Critical | TestFile.EICAR.y    | eicar.js   | BLOCK  | +         |
| 02/05/2025 15:36 | 22E04CA13331 | 139.162.104.220 | 8080        | 10.10.0.103    | 55169            | JP     | HTTP     | 9105094401829019 | Critical | TestFile.EICAR.y    | eicar.js   | BLOCK  | +         |
| 02/05/2025 15:36 | 22E04CA13331 | 139.162.104.220 | 8080        | 10.10.0.103    | 55166            | JP     | HTTP     | 9203553601274736 | Critical | TestFile.EICAR.y    | eicar.docx | BLOCK  | +         |
| 02/05/2025 15:36 | 22E04CA13331 | 139.162.104.220 | 8080        | 10.10.0.103    | 55167            | JP     | HTTP     | 9045595452933008 | Critical | TestFile.EICAR.y    | eicar.doc  | BLOCK  | +         |
| 02/05/2025 15:35 | 22E04CA13331 | 139.162.104.220 | 8080        | 10.10.0.103    | 55163            | JP     | HTTP     | 2053             | Critical | TestFile.EICAR.00x7 | eicar.apk  | BLOCK  | +         |
| 02/05/2025 15:35 | 22E04CA13331 | 139.162.104.220 | 8080        | 10.10.0.103    | 55162            | JP     | HTTP     | 2053             | Critical | TestFile.EICAR.00x7 | eicar.apk  | BLOCK  | +         |

### 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.

## Threat Encyclopedia:

In the security logs of [Intrusion Prevention], clicking on the Signature ID allows you to access the analysis and solutions for the corresponding attack.



**Webshell.PHP.Hydra Inbound Connection**  
Medium ++

**Summary**

|               |                  |
|---------------|------------------|
| Signature ID  | 8011276100       |
| Rule Category | Malware-activity |
| Severity      | Medium           |
| Created Date  | 2020-03-20       |
| Update Date   | 2020-03-20       |

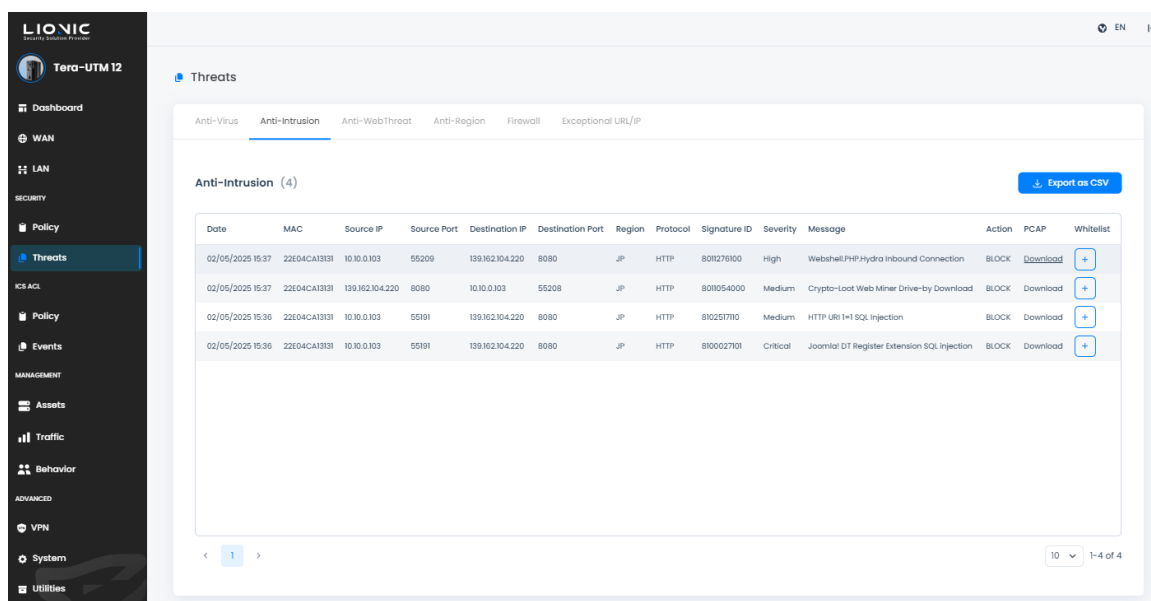
**Details**

|                   |                                                                                                                                                                                                                                                                                     |
|-------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| Affected Products | Any unprotected system is at risk of being compromised.                                                                                                                                                                                                                             |
| Affected OS       | Windows , Linux , MacOS , iOS , Android , Other                                                                                                                                                                                                                                     |
| Description       | This event is used to identify traffic associated with trojan activity, which may include commands and requests for files or other stages from a control server. This indicates that an attacker might have compromised the system, potentially leading to damage or a data breach. |

Threats-Threats Encyclopedia

## PCAP Packet Download:

When events of compromise or blockage occur on Tera-UTM 12, clicking [PCAP] > [Download] allows for packet download for further analysis.



**Threats**

Anti-Virus Anti-Intrusion Anti-WebThreat Anti-Region Firewall Exceptional URL/IP

**Anti-Intrusion (4)** [Export as CSV](#)

| Date             | MAC          | Source IP       | Source Port | Destination IP  | Destination Port | Region | Protocol | Signature ID | Severity | Message                                     | Action | PCAP                     | Whitelist         |
|------------------|--------------|-----------------|-------------|-----------------|------------------|--------|----------|--------------|----------|---------------------------------------------|--------|--------------------------|-------------------|
| 02/05/2025 15:37 | 22E04CA13B31 | 10.10.0.103     | 55209       | 139.162.104.220 | 8080             | JP     | HTTP     | 8011276100   | High     | Webshell.PHP.Hydra Inbound Connection       | BLOCK  | <a href="#">Download</a> | <a href="#">+</a> |
| 02/05/2025 15:37 | 22E04CA13B31 | 139.162.104.220 | 8080        | 10.10.0.103     | 55208            | JP     | HTTP     | 801054000    | Medium   | Crypto-Loot Web Miner Drive-by Download     | BLOCK  | <a href="#">Download</a> | <a href="#">+</a> |
| 02/05/2025 15:36 | 22E04CA13B31 | 10.10.0.103     | 55191       | 139.162.104.220 | 8080             | JP     | HTTP     | 810251710    | Medium   | HTTP URI 1+1 SQL Injection                  | BLOCK  | <a href="#">Download</a> | <a href="#">+</a> |
| 02/05/2025 15:36 | 22E04CA13B31 | 10.10.0.103     | 55191       | 139.162.104.220 | 8080             | JP     | HTTP     | 8100027101   | Critical | Joomla! DT Register Extension SQL Injection | BLOCK  | <a href="#">Download</a> | <a href="#">+</a> |

1 1-4 of 4

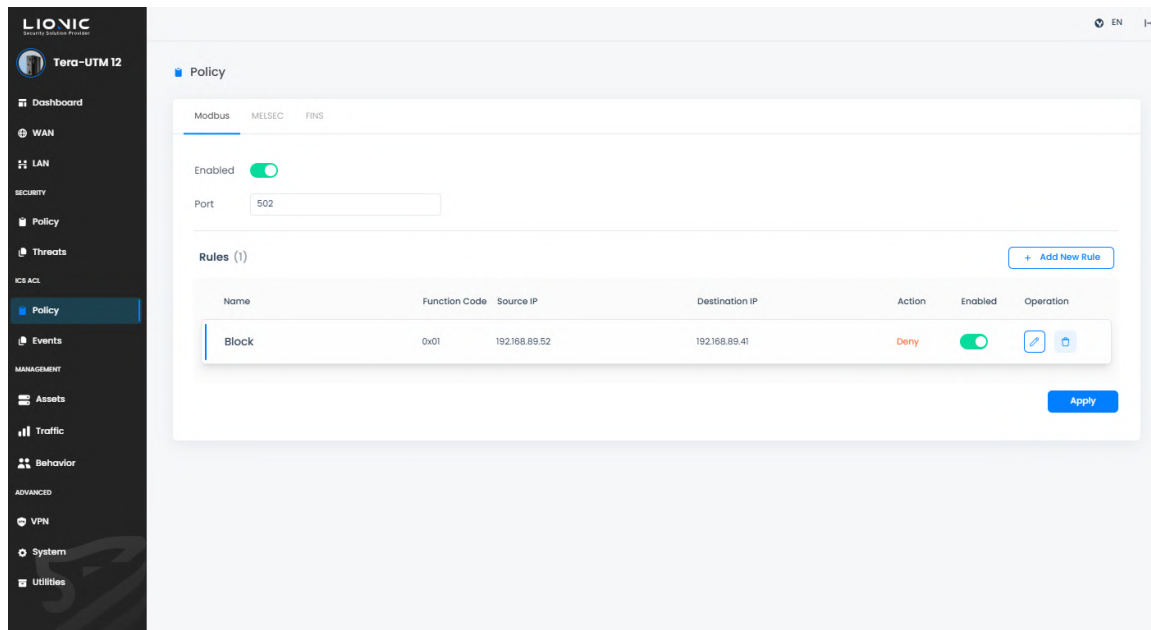
Threats-PCAP Download

\* Remark: [Policy] > [Anti-Intrusion] > [Keep PCAP when a threat is detected] function needs to be enabled.



## ICS ACL

Tera-UTM 12 can inspect packets in commonly used Industrial Control System protocols (ICS protocols). Users can customize access control rules allowing / blocking commands between ICS devices.



Policy

## Policy

Tera-UTM 12 can detect three industrial control system communication protocols: Modbus, MELSEC, and FINS.

- **Step 1:** Enable the access control (default: disabled).
- **Step 2:** Click [+Add New Rule].
- **Step 3:** Fill each configuration.
- **Step 4:** Click [Apply] to take effect.

### Rule Settings:

- **Enabled:** Enabled / disable the selected access control rule.
- **Name:** Customize rule name.
- **Source IP, Destination IP, Unit ID:** Detecting criteria of the access control rule.
- **Log:** Control whether the event that match this rule should be displayed in

[Events].

- **Action:** Allow or block the action that would be taken if the rule is hit.
- **Direction:** Set the command sending or request detection for the rule.
- **Function Code / Command / Command Code:** Set the parameter for the rule.

## Events

When Tera-UTM 12 detects configured events, it will display detailed information in the corresponding tab on the [Threats] page. Click [Export as CSV] to export the records as a CSV file.

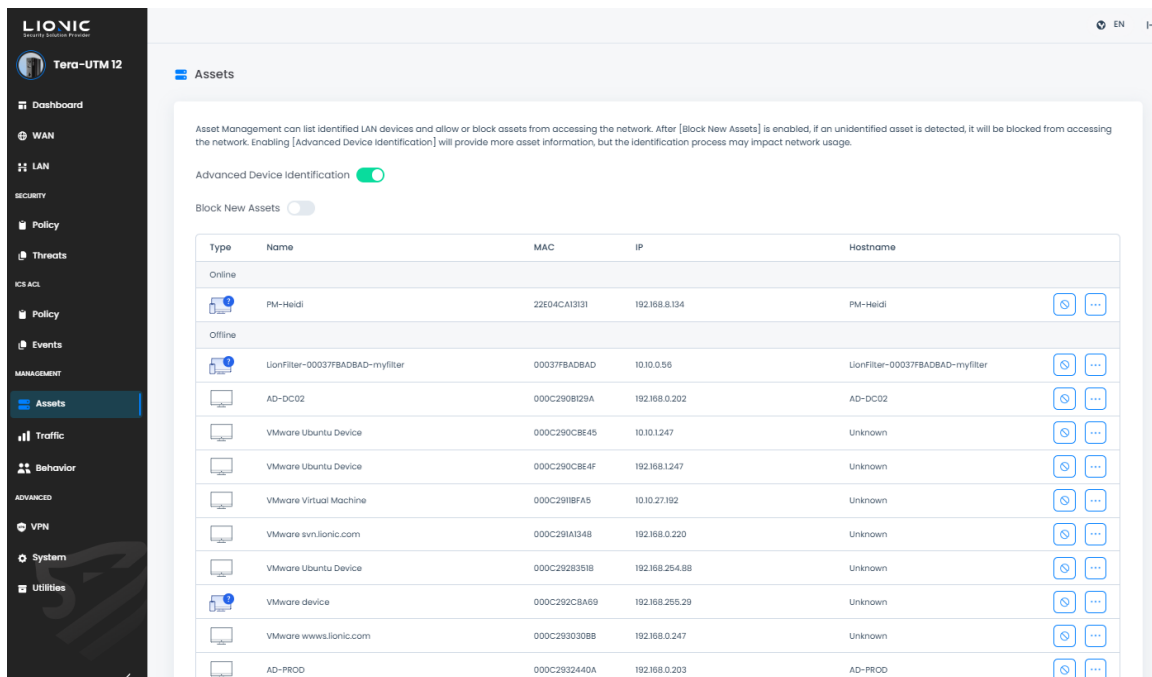
## Assets

The asset management feature can list the identified LAN devices and block or allow specific assets to connect to the network.

- **Advanced Device Identification:** Provide more asset information.

\*Remark: The identification process may affect network usage.

- **Block New Assets:** Block the unidentified devices that have not been identified.



**Assets**

Asset Management can list identified LAN devices and allow or block assets from accessing the network. After [Block New Assets] is enabled, if an unidentified asset is detected, it will be blocked from accessing the network. Enabling [Advanced Device Identification] will provide more asset information, but the identification process may impact network usage.

Advanced Device Identification ☒

Block New Assets ☐

| Type           | Name                             | MAC          | IP             | Hostname                         |
|----------------|----------------------------------|--------------|----------------|----------------------------------|
| <b>Online</b>  |                                  |              |                |                                  |
|                | PM-Heidi                         | 22E04CA13131 | 192.168.8.134  | PM-Heidi                         |
| <b>Offline</b> |                                  |              |                |                                  |
|                | LionFilter-00037FBADBAD-myfilter | 00037FBADBAD | 10.10.0.56     | LionFilter-00037FBADBAD-myfilter |
|                | AD-DC02                          | 000C290B20A  | 192.168.0.202  | AD-DC02                          |
|                | VMware Ubuntu Device             | 000C290CBE45 | 10.10.1.247    | Unknown                          |
|                | VMware Ubuntu Device             | 000C290CBE4F | 192.168.1.247  | Unknown                          |
|                | VMware Virtual Machine           | 000C291BFA5  | 10.10.27.192   | Unknown                          |
|                | VMware svn.lionic.com            | 000C291A1348 | 192.168.0.220  | Unknown                          |
|                | VMware Ubuntu Device             | 000C29283518 | 192.168.254.88 | Unknown                          |
|                | VMware device                    | 000C292C8A69 | 192.168.255.29 | Unknown                          |
|                | VMware www.lionic.com            | 000C2930308B | 192.168.0.247  | Unknown                          |
|                | AD-PROD                          | 000C2932440A | 192.168.0.203  | AD-PROD                          |

## Assets

## Traffic

Traffic management can list the current connection usage of each LAN device and perform bandwidth management.

### Monitor

Displays the real-time download and upload traffic of LAN devices, which can be sorted by volume.

| Type                   | Name                             | MAC          | Download ↓ | Upload ↗  |     |
|------------------------|----------------------------------|--------------|------------|-----------|-----|
| PM-Heldi               | PM-Heldi                         | 22E04CA13131 | 21 Kbps    | 724 bit/s | ... |
| LionFilter             | LionFilter-00037FBADBAD-myfilter | 00037FBADBAD |            |           | ... |
| AD-DC02                | AD-DC02                          | 000C2908129A |            |           | ... |
| VMware Ubuntu Device   | VMware Ubuntu Device             | 000C290C8E45 |            |           | ... |
| VMware Ubuntu Device   | VMware Ubuntu Device             | 000C290C8E4F |            |           | ... |
| VMware Virtual Machine | VMware Virtual Machine           | 000C2918FA5  |            |           | ... |
| VMware svn.lionic.com  | VMware svn.lionic.com            | 000C291A1348 |            |           | ... |
| VMware Ubuntu Device   | VMware Ubuntu Device             | 000C292B3518 |            |           | ... |
| VMware device          | VMware device                    | 000C292C8A59 |            |           | ... |
| VMware www.lionic.com  | VMware www.lionic.com            | 000C29303088 |            |           | ... |

10 1 / 50 Count: 499

Traffic-Monitor

## QoS

Tera-UTM 12 can perform bandwidth management for specific source IPs, destination IPs, or destination ports, allowing their traffic to receive higher priority service.

**QoS**

QoS can prioritize LAN devices and allocate bandwidth based on their priority.

Enabled ☒

Total Bandwidth Download 1000 Mbps Upload 1000 Mbps

| Priority | Name       | Min | Max   |
|----------|------------|-----|-------|
| 1        | Priority 1 | 0 % | 100 % |
| 2        | Priority 2 | 0 % | 100 % |
| 3        | Priority 3 | 0 % | 100 % |
| 4        | Priority 4 | 0 % | 100 % |
| 5        | Default    | 0 % | 100 % |
| 6        | Priority 6 | 0 % | 100 % |
| 7        | Priority 7 | 0 % | 100 % |
| 8        | Priority 8 | 0 % | 100 % |

Apply

+ Add New Rule

Traffic-QoS

**Step 1:** Enable QoS function.

**Step 2:** Set the total bandwidth of download and upload.

**Step 3:** Configure priority and bandwidth ratio.

\*Remark: Eight priority levels are provided, with priority level 1 being the highest and level 8 the lowest. Priority level 5 is the default setting.

**Step 4:** Click [Apply] to activate the settings.

| Priority | Name       | Min | Max   |
|----------|------------|-----|-------|
| 1        | Priority 1 | 0 % | 100 % |
| 2        | Priority 2 | 0 % | 100 % |
| 3        | Priority 3 | 0 % | 100 % |
| 4        | Priority 4 | 0 % | 100 % |
| 5        | Default    | 0 % | 100 % |
| 6        | Priority 6 | 0 % | 100 % |
| 7        | Priority 7 | 0 % | 100 % |
| 8        | Priority 8 | 0 % | 100 % |

Apply

Traffic- Priority Settings

**Step 5:** Click [+ Add New Rule]

**Step 6:** Enter the setting values for each item.

**Step 7:** Click [Apply] to take effect.

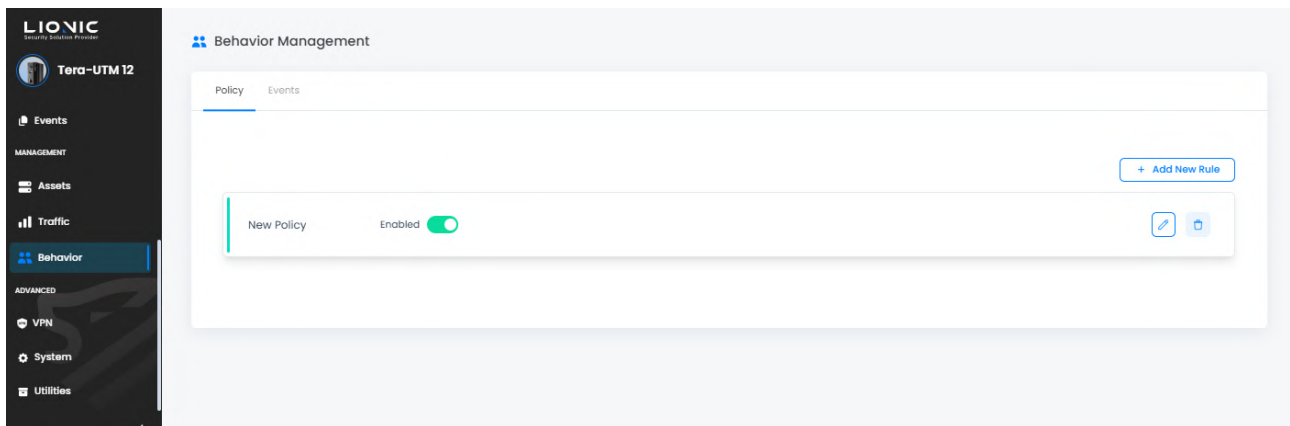
The screenshot displays the 'QoS Rules' configuration window. It features a table with columns for Name, Enabled, Priority, Source IP, Destination IP, and Destination Port. Two rules are listed: 'Qos 01' and 'Default'. The 'Qos 01' rule is enabled, has a priority of 1, and is configured for Source IP 192.168.8.34, Destination IP ANY, and Destination Port ANY. The 'Default' rule is also enabled, has a priority of 5, and is configured for Source IP ANY, Destination IP ANY, and Destination Port ANY. An '+ Add New Rule' button is in the top right, and an 'Apply' button is in the bottom right.

| Name    | Enabled                             | Priority | Source IP    | Destination IP | Destination Port |
|---------|-------------------------------------|----------|--------------|----------------|------------------|
| Qos 01  | <input checked="" type="checkbox"/> | 1        | 192.168.8.34 | ANY            | ANY              |
| Default | <input checked="" type="checkbox"/> | 5        | ANY          | ANY            | ANY              |

Traffic-QoS Rules

## Behavior

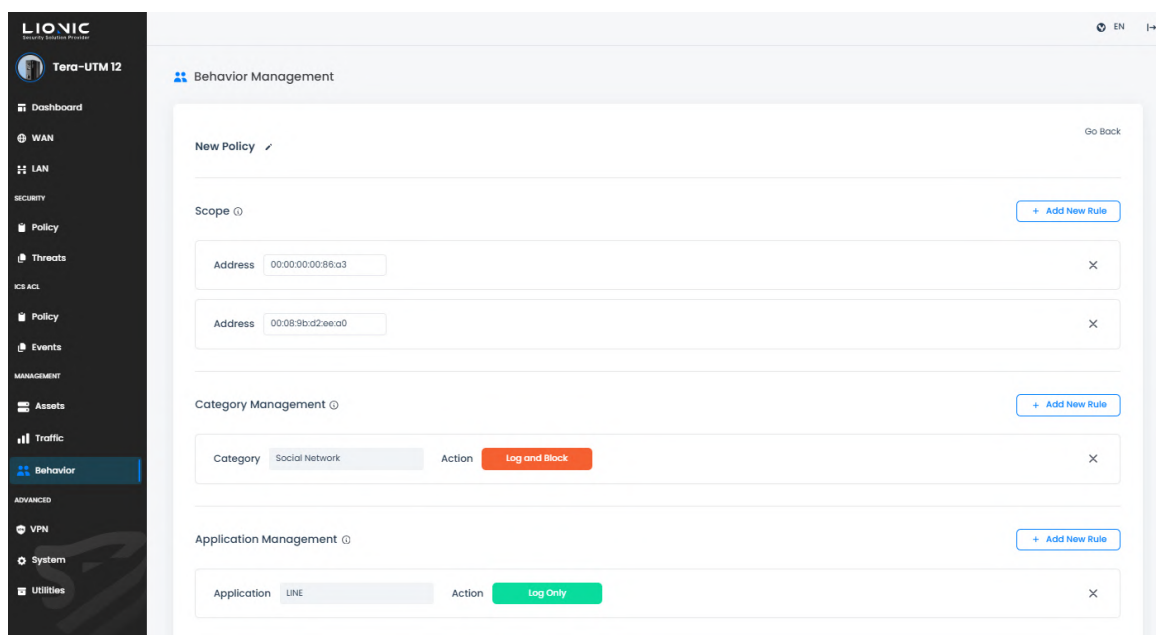
The Behavior Management feature allows you to manage specific content categories or applications. You can configure settings based on your needs to protect family members or employees from inappropriate content.



Behavior Management

## Policy

Click [+ Add New Rule] to add a new rule. You can edit or delete rules on the Policy page.



Behavior Management-Policy Rule

The rule editing page allows you to edit different types of rules:

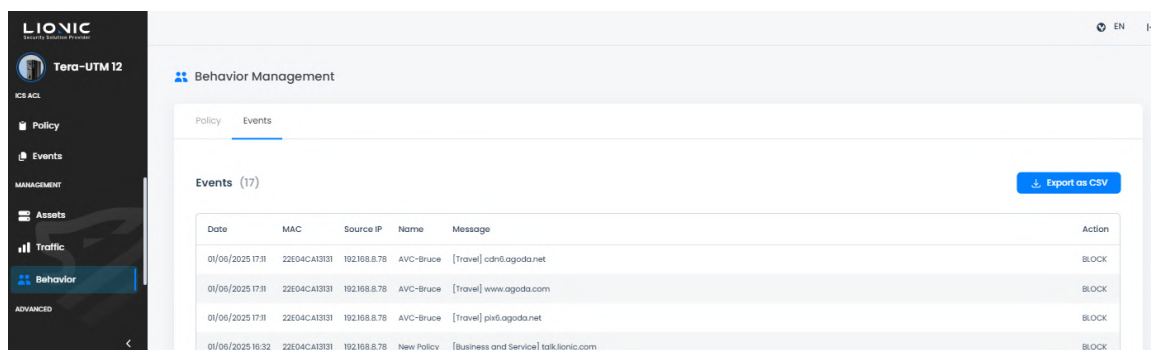
- **Step 1:** Click [+ Add New Rule] in the Scope to set the scope of the policy.
- **Step 2:** Enter the IP address or MAC address to be managed.
- **Step 3:** Choose the items to manage and click [+ Add New Rule] to configure the content and actions.
- **Step 4:** Click [Apply] to activate the settings.
- **Step 5:** Click [Go Back] to return to the Policy page.

### Rule Configuration Details:

- **Scope:** Manage the rule scope by IP addresses or MAC addresses. This is a required field.
- **Category Management:** Manage the corresponding action based on the category of the web content.
- **Application Management:** Manage the corresponding action based on the application associated with the network connection.
- **Websites:** Allow or block all connections to specified websites.

## Events

The detection results and actions of Behavior Management are displayed on the Events page. Click [Export as CSV] to export the records as a CSV file.



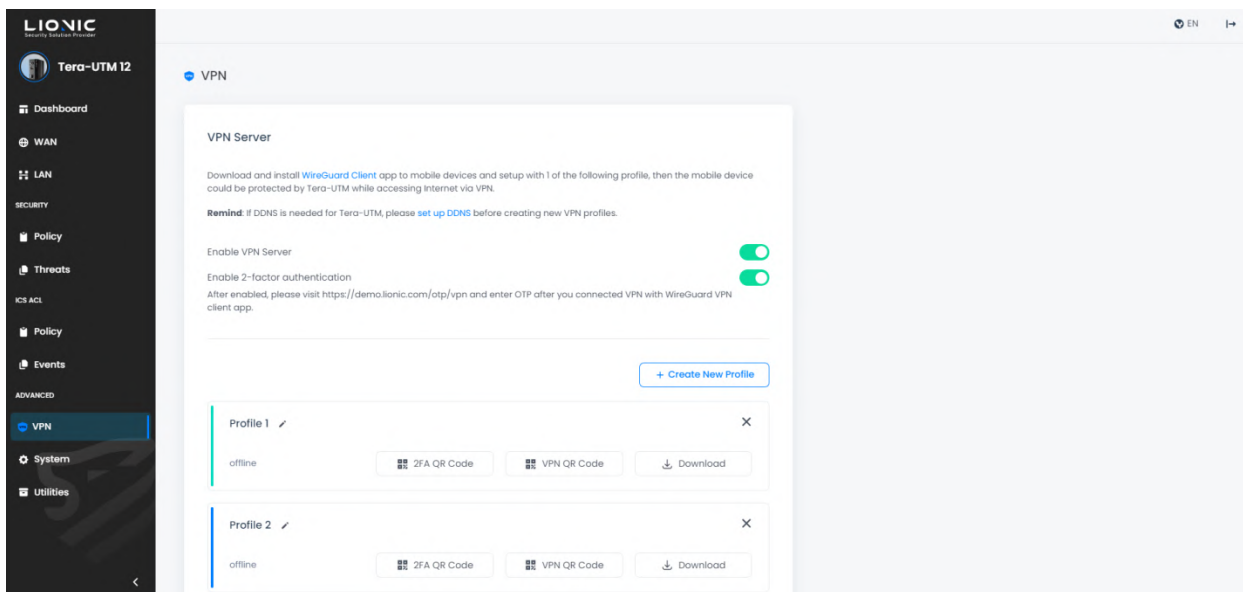
| Date             | MAC          | Source IP    | Name       | Message                                | Action |
|------------------|--------------|--------------|------------|----------------------------------------|--------|
| 01/06/2025 17:11 | 22E04CA13131 | 192.168.8.78 | AVC-Bruce  | [travel] odr6.agoda.net                | BLOCK  |
| 01/06/2025 17:11 | 22E04CA13131 | 192.168.8.78 | AVC-Bruce  | [travel] www.agoda.com                 | BLOCK  |
| 01/06/2025 17:11 | 22E04CA13131 | 192.168.8.78 | AVC-Bruce  | [travel] pin6.agoda.net                | BLOCK  |
| 01/06/2025 16:32 | 22E04CA13131 | 192.168.8.78 | New Policy | [Business and Service] talk.lionic.com | BLOCK  |

Behavior Management-Events



## 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.

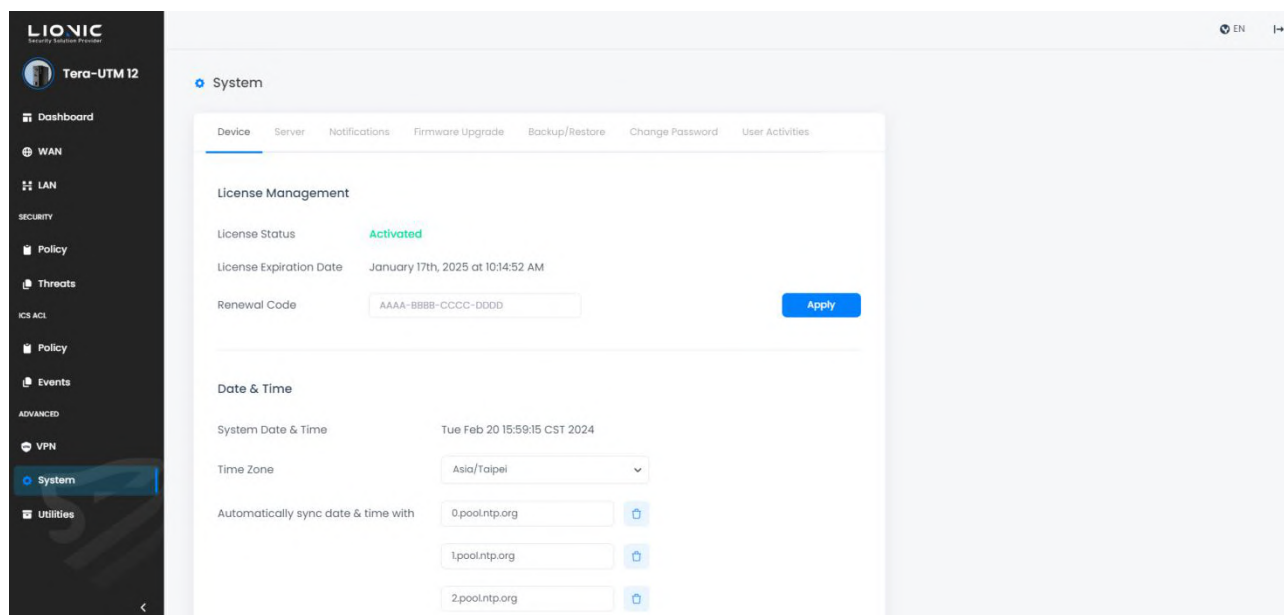
### Start Accessing Internet via VPN:

- Step 1: Connect Tera-UTM 12 via VPN with WireGuard Client app.
- Step 2: Obtain the OTP from the OTP app.
- Step 3: Visit <https://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 keep the latest virus/intrusion/phishing/fraud detection and prevention, please buy the license key i.e. activation code (Remark 1) and enter it in [Activation Code] field. Then, click the [Activate] button while the Ark-UTM 16 is connecting to the Internet to make the activation take effect.
- **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 [Renewal Code] field and click [Apply] to extend the expiration date.

\* Remark:

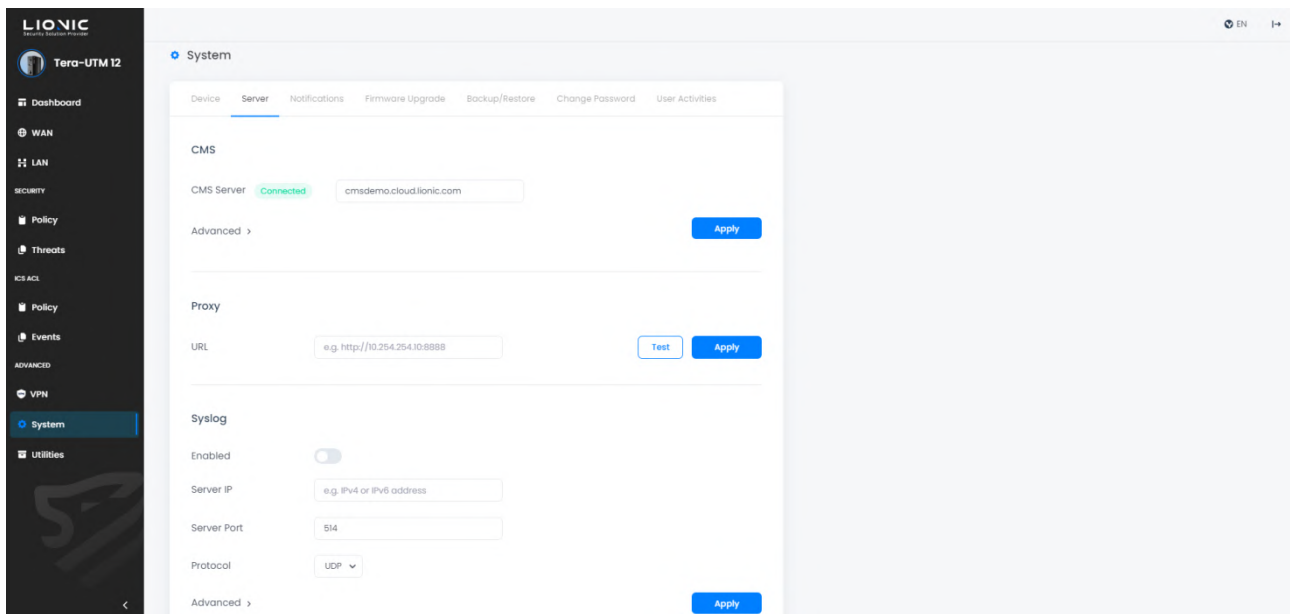
1. The activation code consists of 20 English letters and numbers. It can activate the license after applied successfully. If you do not receive the activation code when you purchase Tera-UTM 12 or if the activation code is not working, please contact local sales representatives in your region.
2. The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

- **Get Firmware or Signature Updates from CMS Server:**  
This advanced feature is used when the local network cannot connect to the internet. If you have related requirements, please contact your local dealer or sales representative. °
- **Send firewall logs and exceptional websites logs to CMS:**  
To improve the storage space efficiency of CMS, Tera-UTM 12, after setting up CMS, by default, only uploads security logs related to the three main functions: antivirus system, intrusion prevention, and malicious web page blocking. Enabling this feature will also upload firewall and exception website event logs to CMS.

## 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

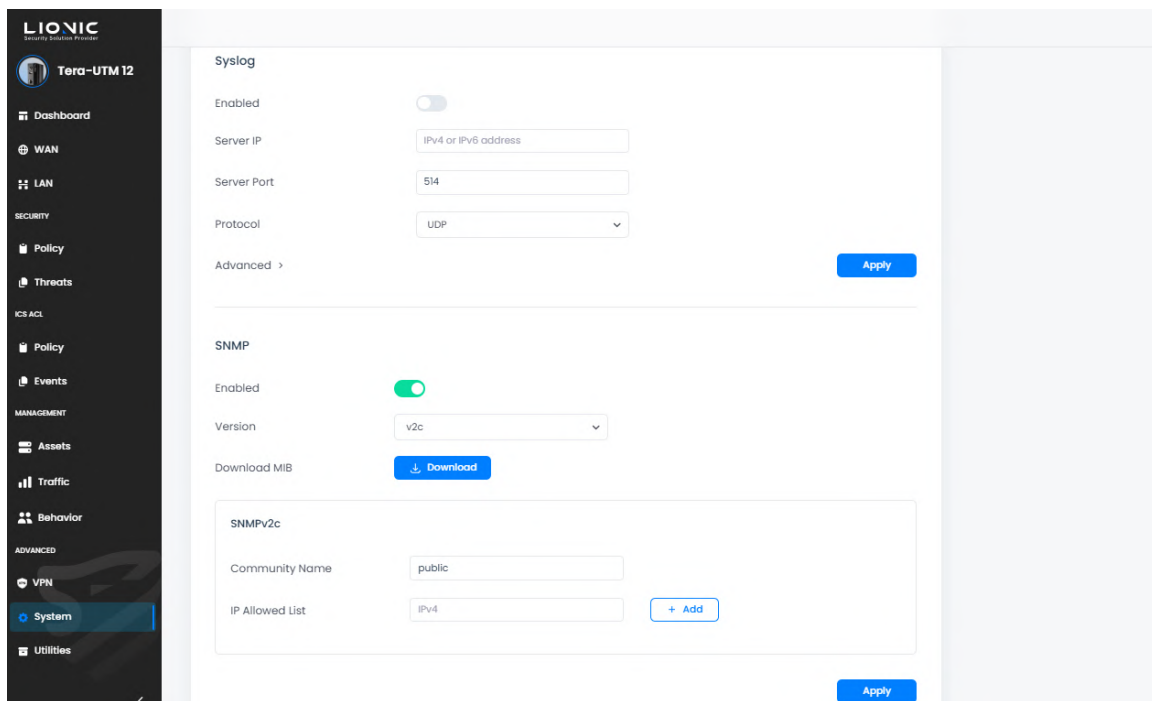
built, enter the server address into the input field and click [Apply] to access LIONIC cloud services via the proxy server. Please contact your IT administrator for more information.

## 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].

## SNMP

SNMP allows administrators to remotely monitor the system status information of the Tera-UTM 12. If you have set up your own SNMP server (v2c, v3 versions), enter the configuration into the input field and click [Apply].

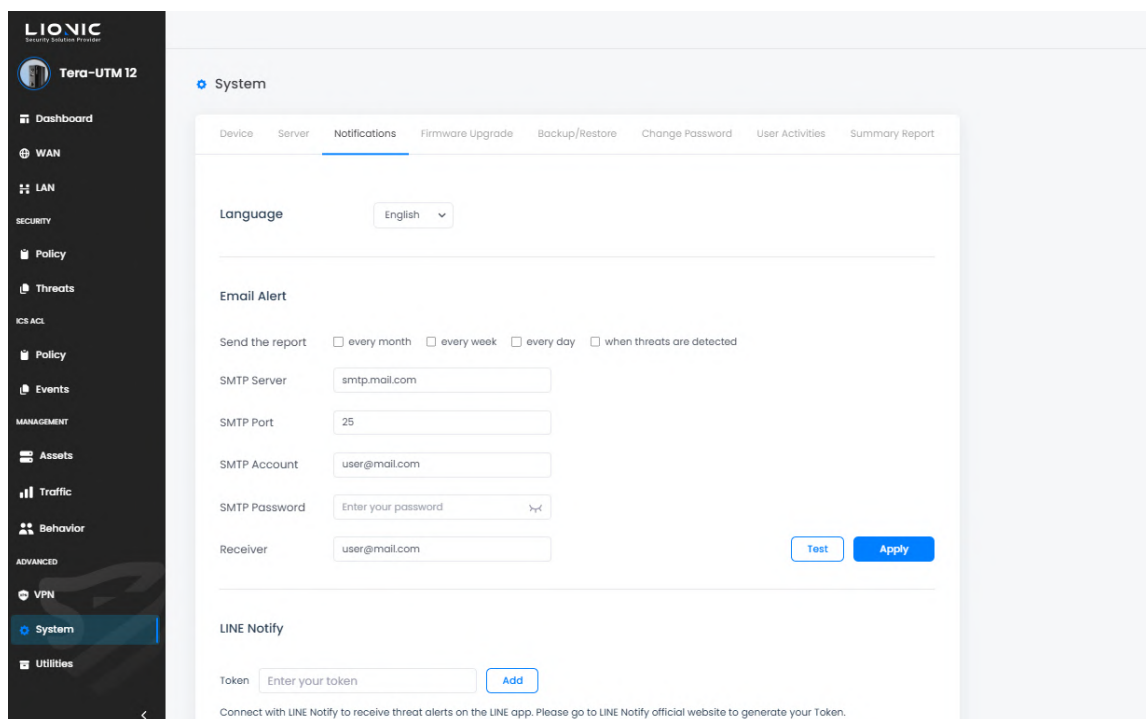


The screenshot displays the Tera-UTM 12 configuration interface. On the left is a dark sidebar with a menu including Dashboard, WAN, LAN, SECURITY (Policy, Threats), ICS ACL (Policy, Events), MANAGEMENT (Assets, Traffic), Behavior, ADVANCED (VPN, System, Utilities), and the 'System' option is currently selected. The main content area is divided into two sections: Syslog and SNMP. The Syslog section has a toggle for 'Enabled' (currently off), input fields for 'Server IP' (placeholder: IPv4 or IPv6 address), 'Server Port' (value: 514), and a 'Protocol' dropdown (value: UDP). An 'Advanced >' link and an 'Apply' button are also present. The SNMP section has a toggle for 'Enabled' (currently on), a 'Version' dropdown (value: v2c), and a 'Download MIB' button with a download icon. Below this is a table for 'SNMPv2c' with columns for 'Community Name' (value: public) and 'IP Allowed List' (value: IPv4). An '+ Add' button is next to the IP Allowed List. An 'Apply' button is at the bottom right of the SNMP section.

Server-SNMP

## 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.

## Email Alert

- **Send the report:**
  - Every month: Send the monthly report on the 1st day of each month at 00:00.
  - Every week: Send the weekly report every Sunday at 00:00.
  - Every day: Send daily report at 00:00 every day.
  - When threats are detected: Threat information is sent immediately upon detection.
- **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.

Please enter the correct settings in the input box and click [Apply] to complete the configuration. Click [Test] to have Tera-UTM 12 send a test email to confirm the settings.

\* Remark:

1. If you need to use Gmail as the sender for email notifications, please enable Gmail's 2-Step Verification and create an App Password to enter in the [SMTP Password] field.

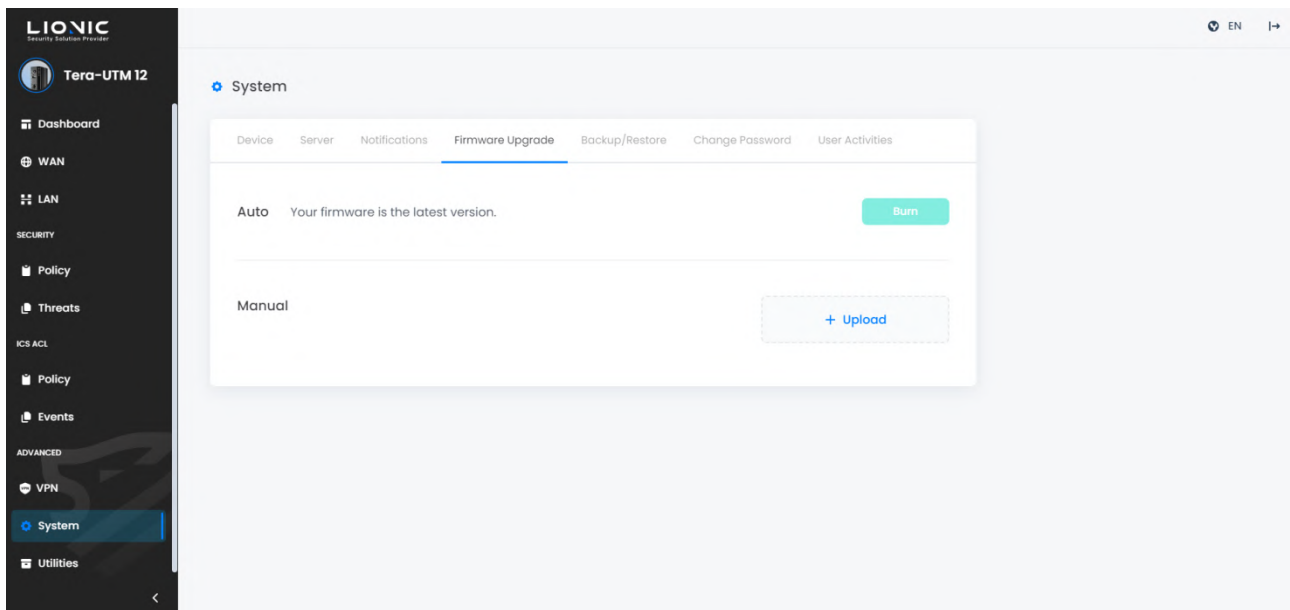
## LINE Notify

To use the LINE message notification feature, please first follow the instructions on the LINE Notify official website to obtain a LINE Token. Then, fill in the Token in the input box and click [Add]. You can then receive real-time threat detection notifications via the LINE App.



## Firmware Upgrade

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



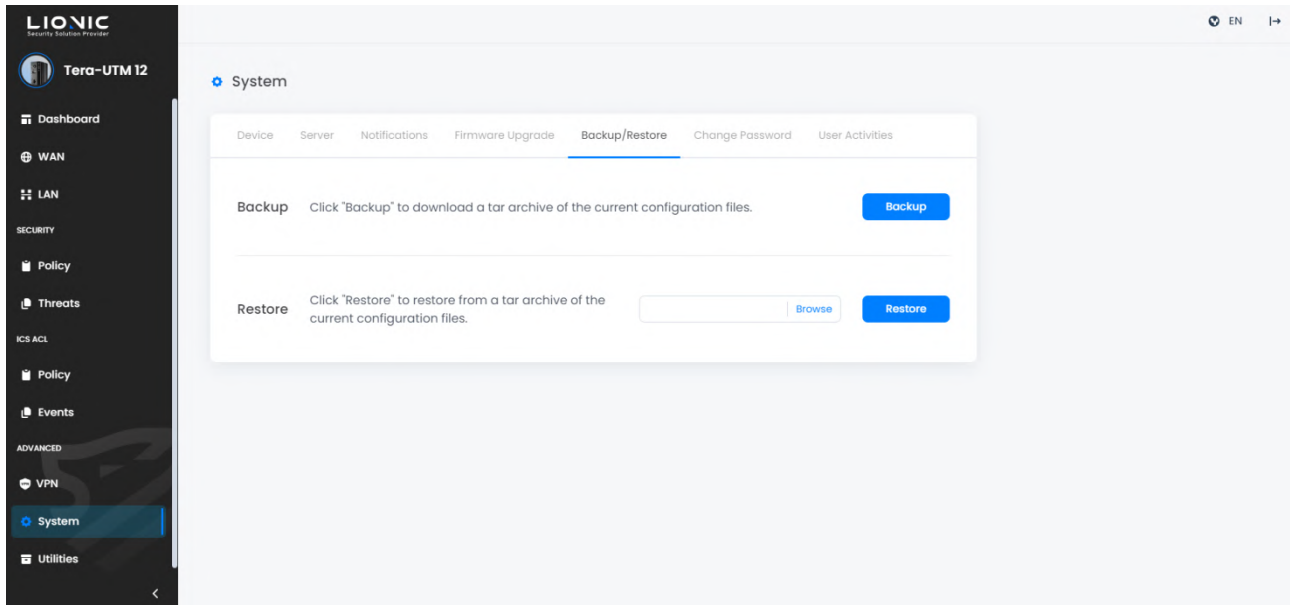
System-Firmware Upgrade

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

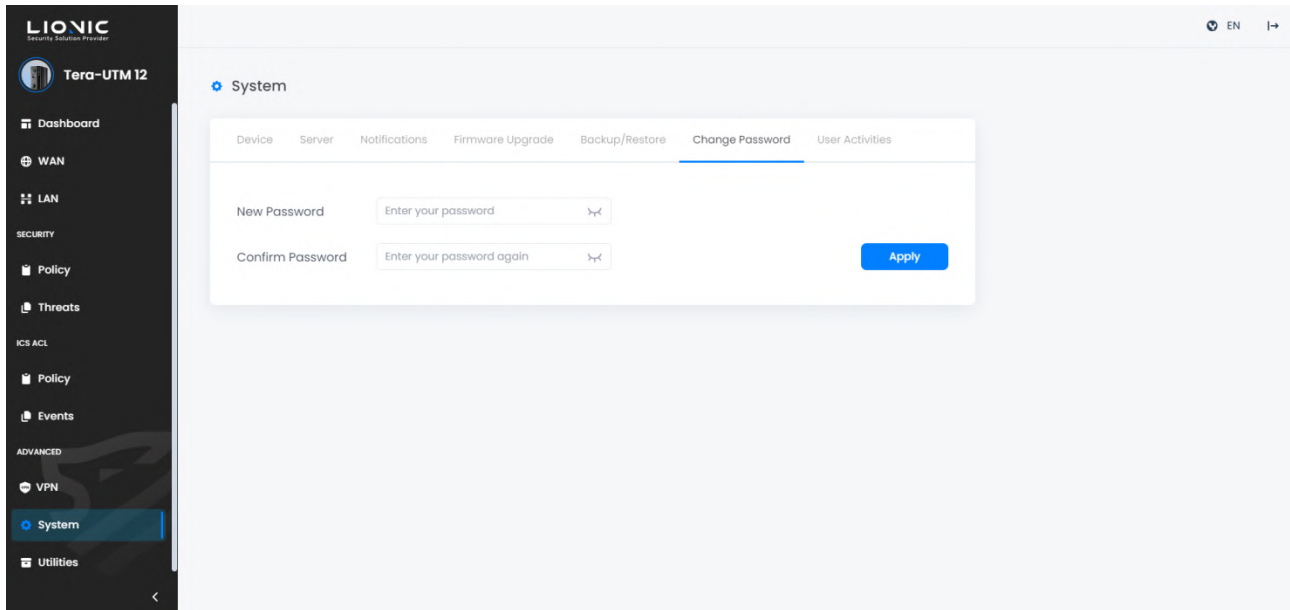
[Backup / Restore] function can backup Tera-UTM 12 configurations, such as security policies and whitelist setting, and restore on the same or other Tera-UTM 12.



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].

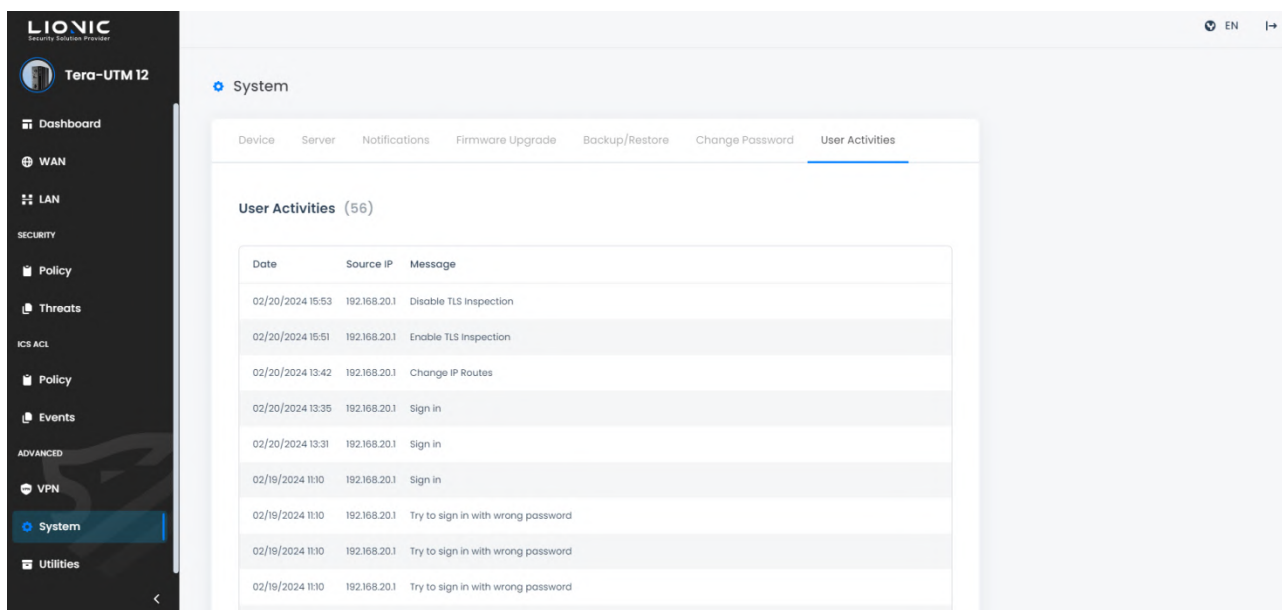


The screenshot displays the Tera-UTM 12 web interface. On the left is a dark sidebar with the 'LIONIC' logo and a menu including 'Dashboard', 'WAN', 'LAN', 'SECURITY' (with sub-items 'Policy', 'Threats'), 'ICS ACL' (with sub-items 'Policy', 'Events'), 'ADVANCED' (with sub-items 'VPN', 'System', 'Utilities'), and 'System' (which is currently selected). The main content area has a top bar with 'EN' and a language icon. Below this is a 'System' section with a sub-header containing tabs: 'Device', 'Server', 'Notifications', 'Firmware Upgrade', 'Backup/Restore', 'Change Password' (which is 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 password icons (an eye with a slash) on their right. A blue 'Apply' button is positioned to the right of the 'Confirm Password' field.

System-Change Password

## User Activities

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



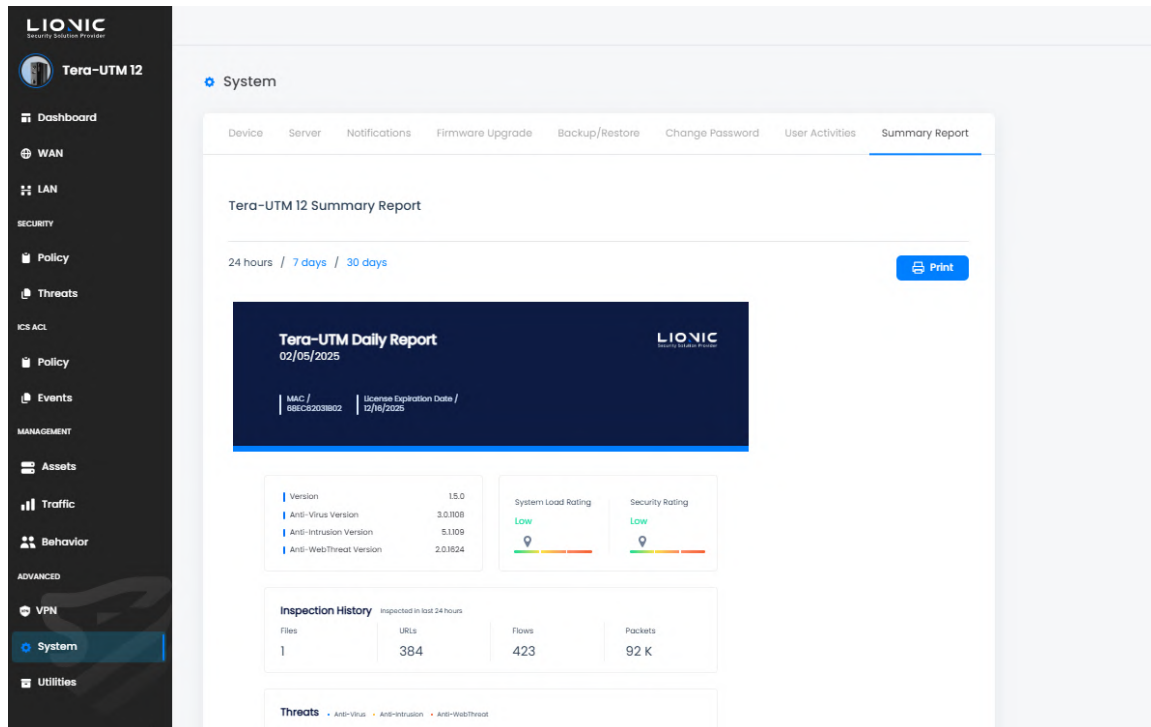
The screenshot displays the Tera-UTM 12 web interface. On the left is a dark sidebar with the 'LIONIC' logo and 'Tera-UTM 12' title. Navigation items include Dashboard, WAN, LAN, SECURITY (with sub-items Policy, Threats, ICS ACL, Policy, Events), and ADVANCED (with sub-items VPN, System, and Utilities). The 'System' item is currently selected. The main panel shows the 'System' section with tabs for Device, Server, Notifications, Firmware Upgrade, Backup/Restore, Change Password, and User Activities. The 'User Activities' tab is active, showing a list of 56 activities. The table below represents the data shown in this tab.

| Date             | Source IP    | Message                            |
|------------------|--------------|------------------------------------|
| 02/20/2024 15:53 | 192.168.20.1 | Disable TLS Inspection             |
| 02/20/2024 15:51 | 192.168.20.1 | Enable TLS Inspection              |
| 02/20/2024 13:42 | 192.168.20.1 | Change IP Routes                   |
| 02/20/2024 13:35 | 192.168.20.1 | Sign in                            |
| 02/20/2024 13:31 | 192.168.20.1 | Sign in                            |
| 02/19/2024 11:10 | 192.168.20.1 | Sign in                            |
| 02/19/2024 11:10 | 192.168.20.1 | Try to sign in with wrong password |
| 02/19/2024 11:10 | 192.168.20.1 | Try to sign in with wrong password |
| 02/19/2024 11:10 | 192.168.20.1 | Try to sign in with wrong password |

System-User Activities

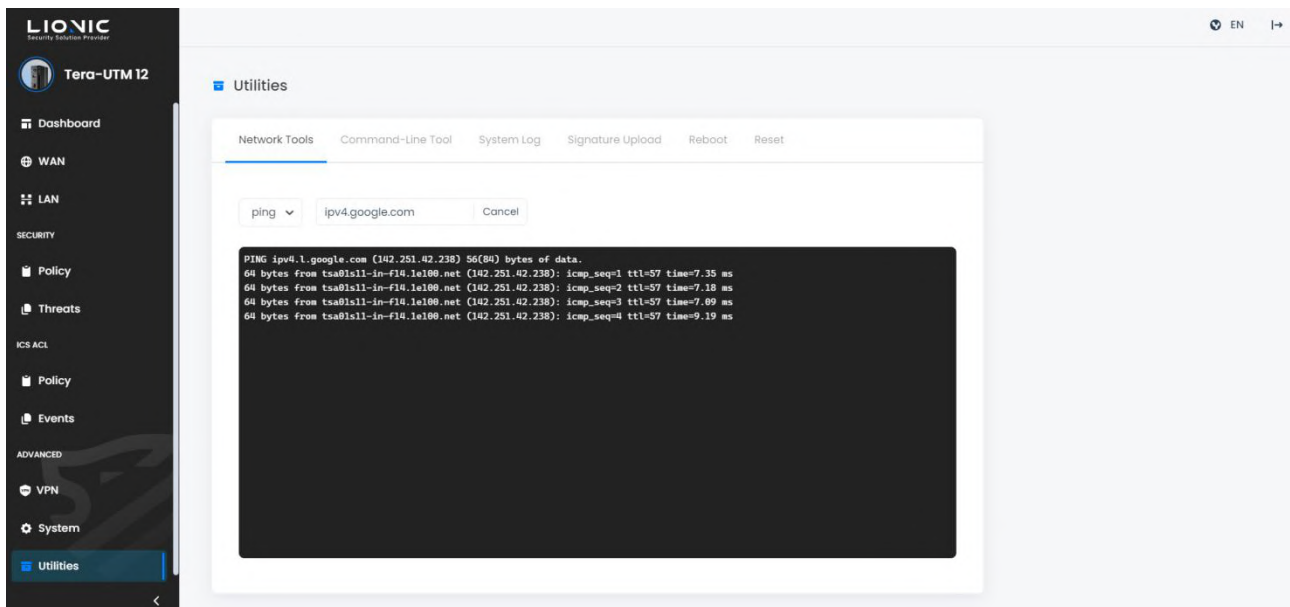
## Summary Report

Summary Report page will generate daily, weekly, and monthly reports in real time.



System-Summary Report

## Utilities



Utilities

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 configurations 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 2025 Lionic Corp. All rights reserved.

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