Security Solution Provider

Web GUI User Manual

Pico-UTM 100

Version 2.4

Released on January 2024

Pico-UTM 100
https://www.pico-utm.com/

Lionic Corp.
https://www.lionic.com/

Pico-UTM 100 Web GUI User Manual

Trademarks

Lionic and Pico-UTM are 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.

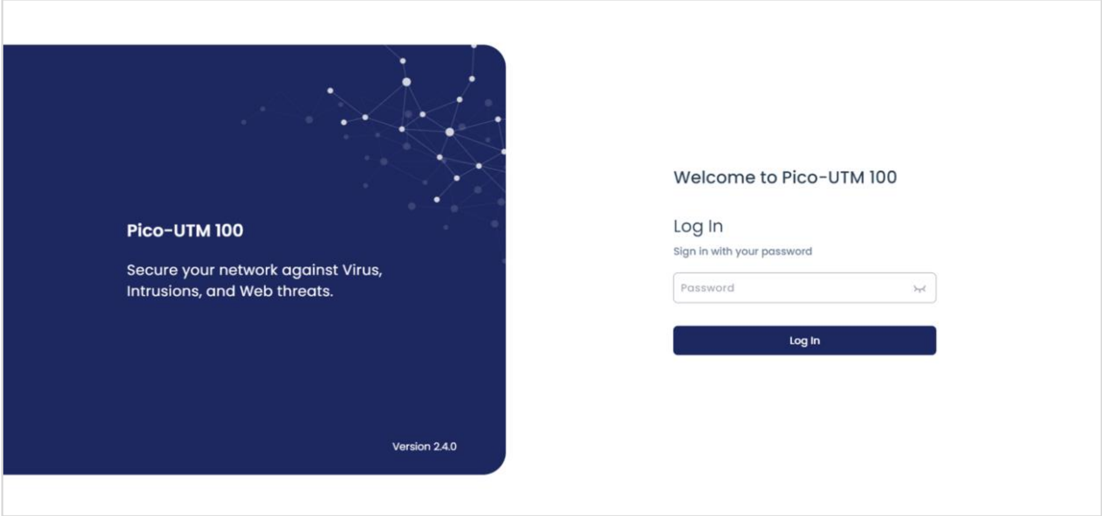
Technical Support   Lionic Corporation

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

Content

Access Web GUI and Connect to the Network

1. Plug the power cable into Pico-UTM 100.
2. Connect the WAN port of Pico-UTM 100 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 Pico-UTM 100 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 http://10.254.254.254/ with a web browser.



Pico-UTM 100

Secure your network against Virus, Intrusions, and Web threats.

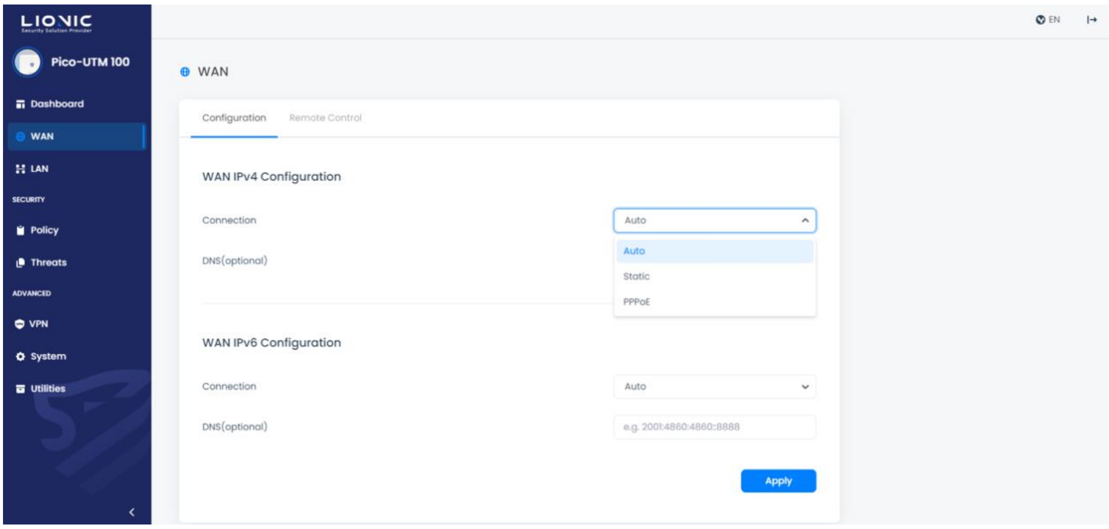
Version 2.4.0

Welcome to Pico-UTM 100

Log In

Sign in with your password

6. After the login page is shown, enter the default password to log in the web GUI. Note: The default password is the Serial Number (S/N), which is printed at the bottom of Pico-UTM 100.
7. After logged in, set the network configuration of Pico-UTM 100 in [WAN] page.



WAN

WAN IPv4 Configuration

Connection: Auto (Auto / Static / PPPoE)

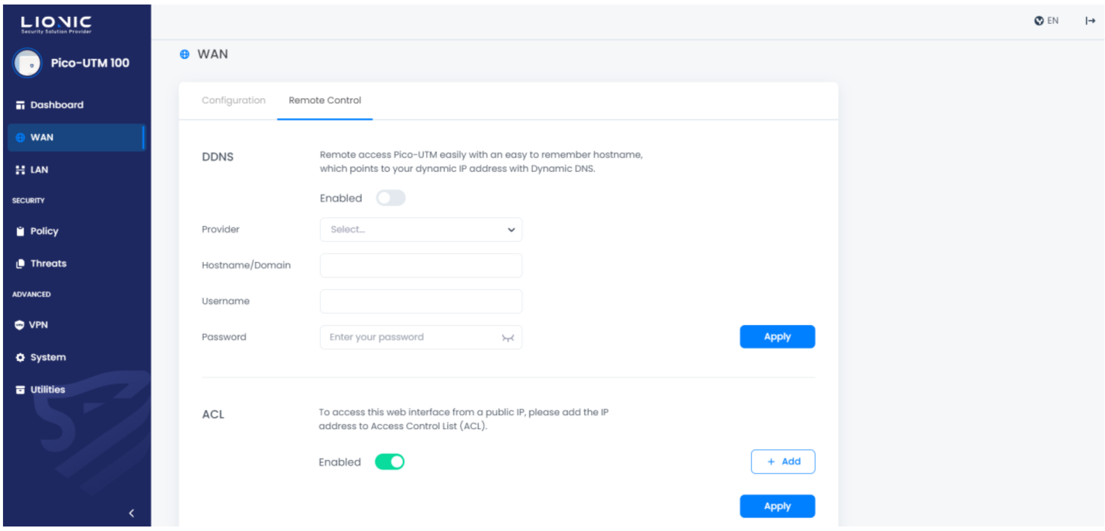
DNS(optional)

WAN IPv6 Configuration

Connection: Auto

DNS(optional): e.g. 2001:4860:4860::8888

8. After Pico-UTM 100 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 Pico-UTM 100 and your PC/laptop are using private IP addresses in the same subnet, and the PC/laptop is located at the LAN side of Pico-UTM 100, visit http://mypico.lionic.com/ to access the web GUI.
   - When Pico-UTM 100 and your PC/laptop are using different public IP addresses, and the PC/laptop is located at the LAN side of Pico-UTM 100, access the web GUI by visiting http://10.254.254.254/ as mentioned above, go to [WAN] > [Remote Contol] page and disable [ACL] (or add the IP address of the PC/laptop to the ACL). After that, visit http://mypico.lionic.com/ to access the web GUI.



WAN

DDNS

Remote access Pico-UTM easily with an easy to remember hostname, which points to your dynamic IP address with Dynamic DNS.

Enabled: off

Provider: Select...

Hostname/Domain

Username

Password: Enter your password

ACL

To access this web interface from a public IP, please add the IP address to Access Control List (ACL).

Enabled: on

Overview

Dashboard:

[Dashboard] shows operating status and device information of Pico-UTM 100, including Inspection History, threat statics, network traffic monitoring and system resource usage.

WAN:

WAN settings of Pico-UTM 100 could be configured in [WAN], such as IPv4/IPv6 configurations and [Remote Control] settings.

LAN:

LAN settings of Pico-UTM 100 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:

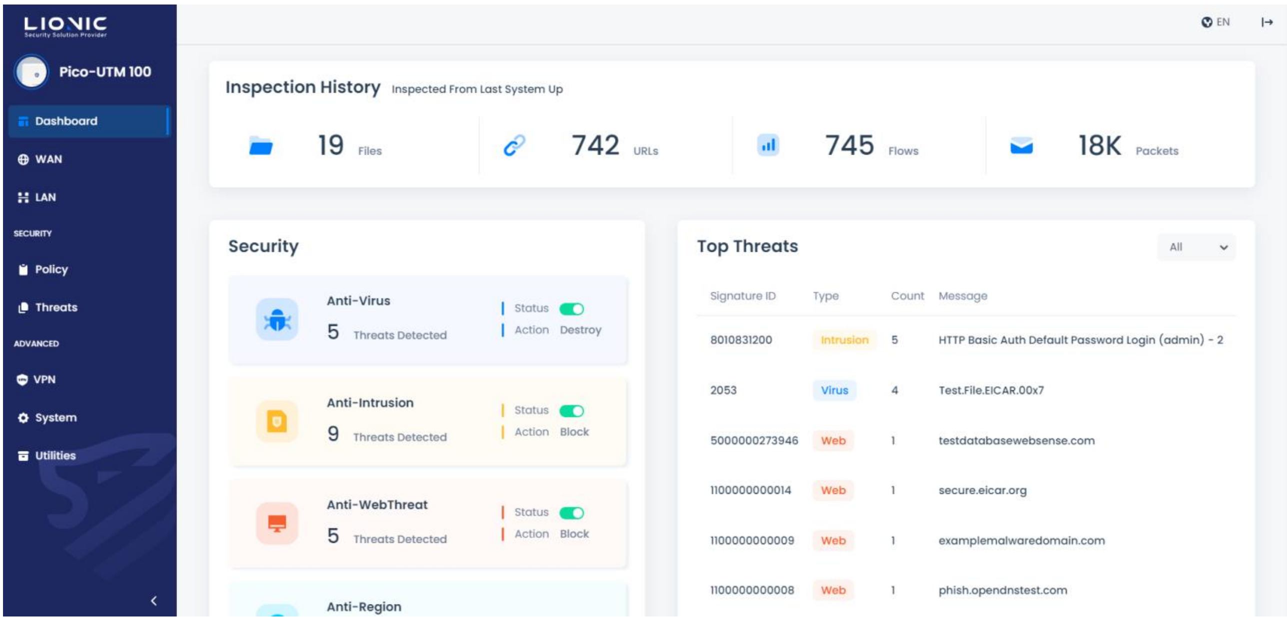
- **Policy:** Configuring protection rules for each security feature, including Anti-Virus, Anti-Intrusion, Anti-WebThreat and the firewall.
- **Threats:** Listing protection logs for each security feature.

Advanced:

- **VPN:** After the VPN server is enabled, the protecting range of Pico-UTM 100 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 Pico-UTM 100.



Inspection History Inspected From Last System Up

19 Files | 742 URLs | 745 Flows | 18K Packets

Security

Anti-Virus
5 Threats Detected
Status
Action Destroy

Anti-Intrusion
9 Threats Detected
Status
Action Block

Anti-WebThreat
5 Threats Detected
Status
Action Block

Anti-Region

Top Threats

All

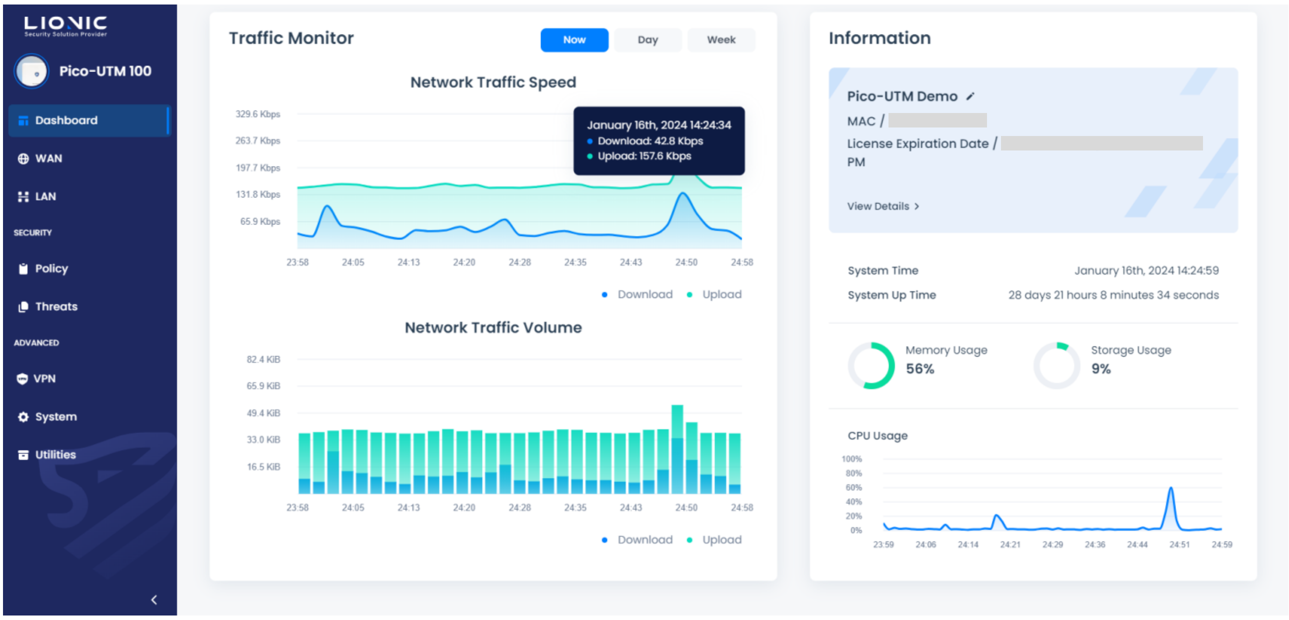
Signature ID	Type	Count	Message
8010831200	Intrusion	5	HTTP Basic Auth Default Password Login (admin) - 2
2053	Virus	4	Test.File.EICAR.00x7
5000000273946	Web	1	testdatabasewebsense.com
1100000000014	Web	1	secure.eicar.org
1100000000009	Web	1	examplemalwaredomain.com
1100000000008	Web	1	phish.opendnstest.com

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 Pico-UTM 100, 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.



January 16th, 2024 14:24:34
● Download: 42.8 Kbps
● Upload: 157.6 Kbps

Pico-UTM Demo
MAC / [redacted]
License Expiration Date / [redacted]
PM

System Time January 16th, 2024 14:24:59
System Up Time 28 days 21 hours 8 minutes 34 seconds

Memory Usage 56%
Storage Usage 9%

Dashboard

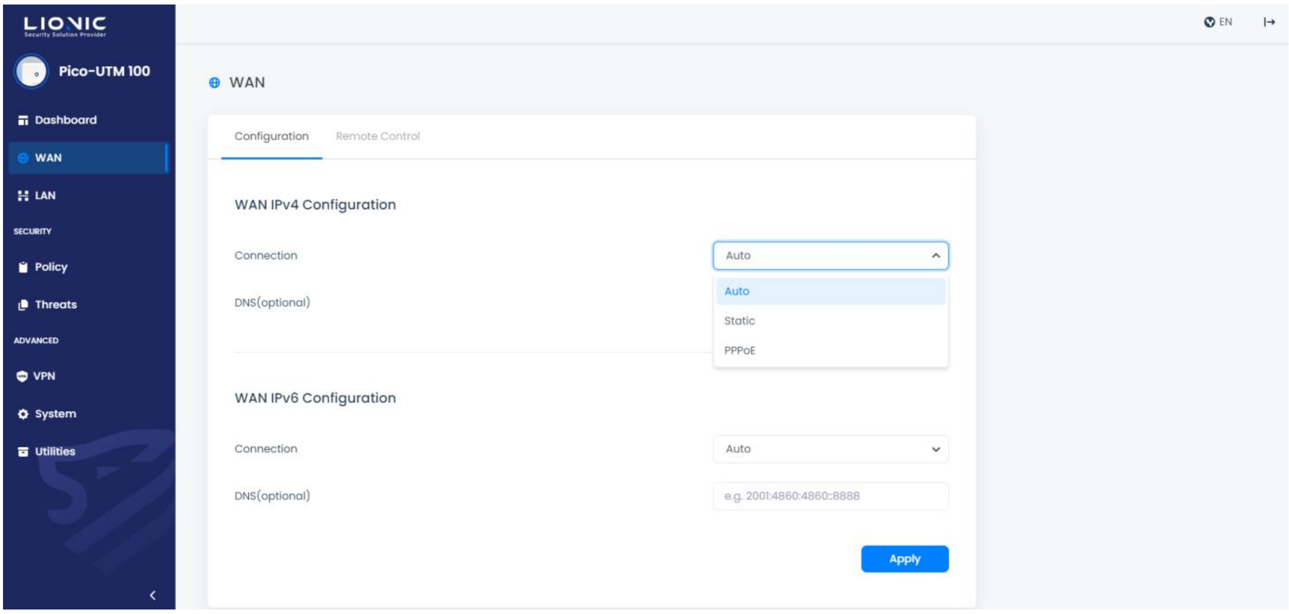
Traffic Monitor: Showing the download and upload traffic via Pico-UTM 100.

Information: Showing the device information of the Pico-UTM 100, 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 Remote Control

WAN IPv4 Configuration

Connection: Auto

DNS(optional)

WAN IPv6 Configuration

Connection: Auto

DNS(optional): e.g. 2001:4860:4860::8888

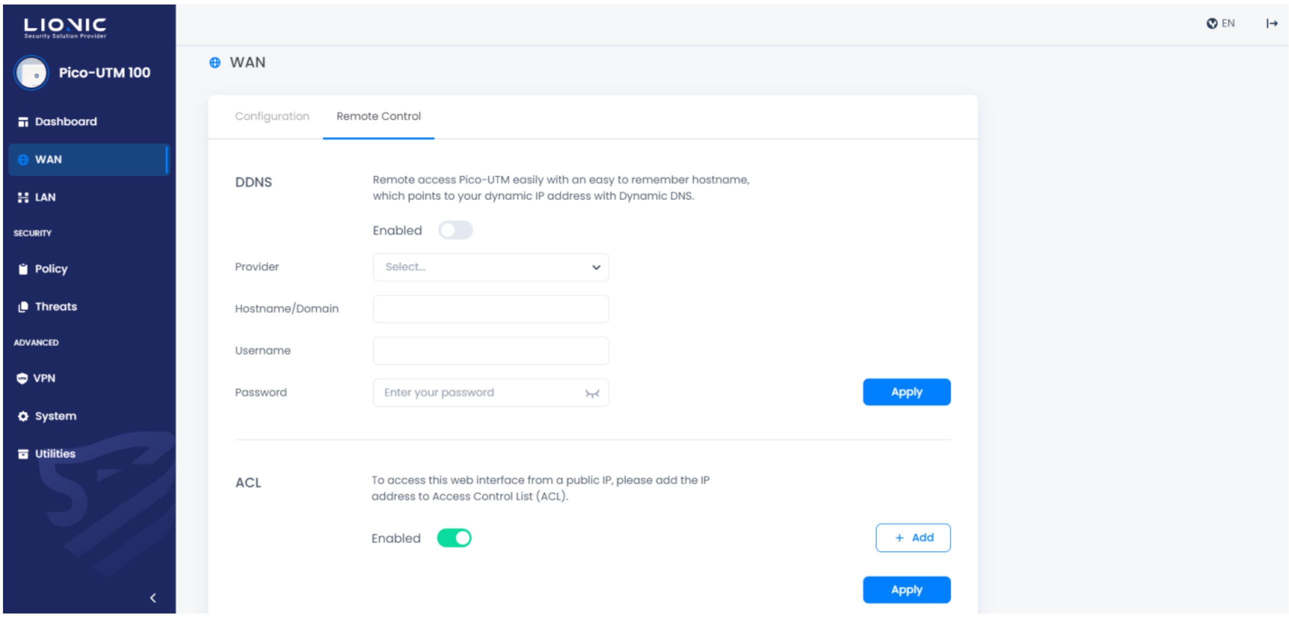
WAN- Configuration

- **Auto:** Pico-UTM obtains DHCP IP address from the router placed at the WAN side of the Pico-UTM 100.
- **Static:** For user to fills the correct IP address in manual.
- **PPPoE:** For user to fills the correct username and password in manual.

* Remark: When using PPPoE connection, you may not be able to access the web GUI of Pico-UTM 100 due to the restriction of the access control list (ACL). Please see [Remote Control] for more details of ACL.

Remote Control:

To prevent Pico-UTM 100 fromintrusion, 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 Pico-UTM 100 connects Internet using a public IP address, please configure settings in [Remote Control].



DDNS

Remote access Pico-UTM easily with an easy to remember hostname, which points to your dynamic IP address with Dynamic DNS.

Enabled ○

Provider: Select...

Hostname/Domain:

Username:

Password: Enter your password

ACL

To access this web interface from a public IP, please add the IP address to Access Control List (ACL).

Enabled ●

WAN- DDNS/Access Control (ACL)

DDNS

When the Pico-UTM 100 is using a dynamic public IP address, you could use a static domain name to access the Pico-UTM 100.

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 Pico-UTM 100 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 Pico-UTM 100 is using a private IP address to connect Internet, please set DDNS and port forwarding on the router at the WAN side of Pico-UTM 100.

Access Control List (ACL)

To prevent Pico-UTM 100 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 Pico-UTM 100 connects Internet using a public IP address, the IP address that would be used to access Pico-UTM 100 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 Pico-UTM 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 Pico-UTM 100.

* Remark:

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

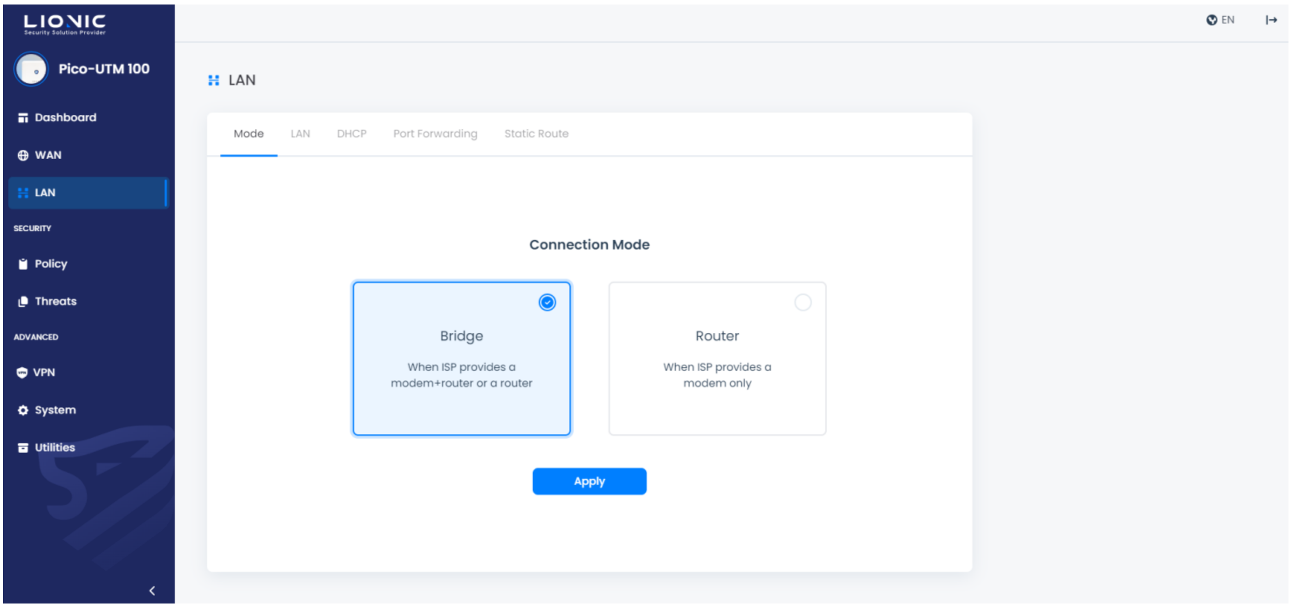
Secure Connection

After [Secure Connection] is enabled, all HTTP connections accessing the web GUI of Pico-UTM 100 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:

Pico-UTM 100 supports 2 connection modes. Select a suitable connection mode based on your network environment.



Connection Mode

● Bridge
When ISP provides a modem+router or a router

○ Router
When ISP provides a modem only

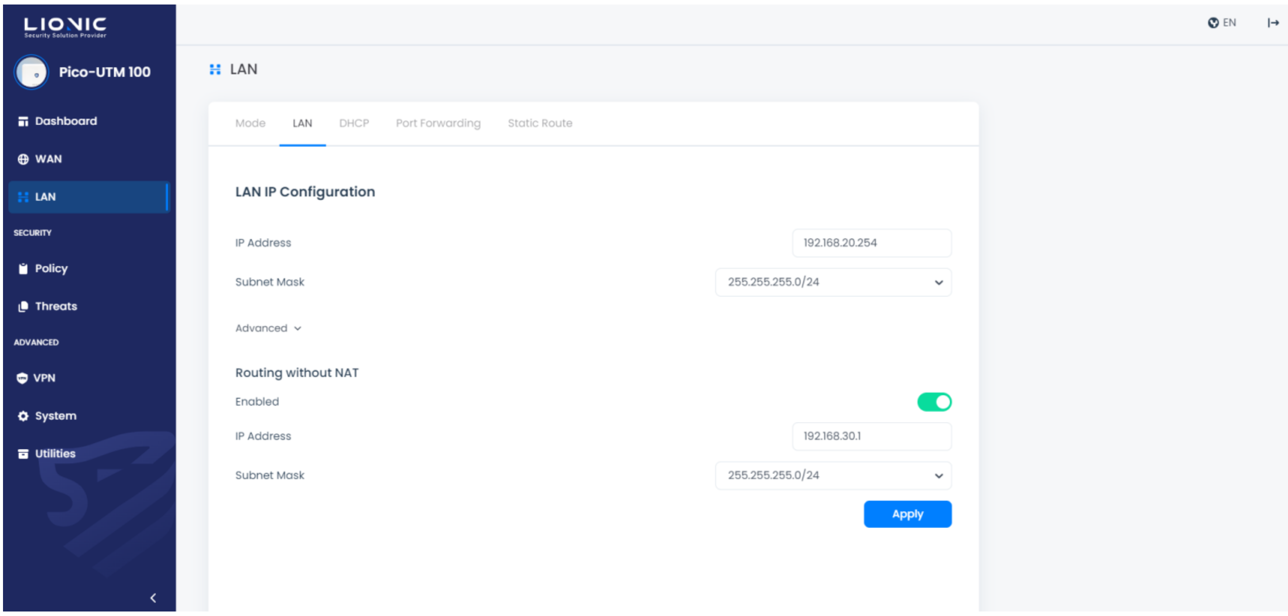
LAN-Connection Mode

- **Bridge mode (default):**
  DHCP is disable to LAN devices in [Bridge] mode. Please connect Pico-UTM 100 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 Pico-UTM 100 and its LAN devices.

After you selected the suitable connection mode and clicked [Apply], Pico-UTM 100 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 will automatically assign IP addresses within the configured range.



LAN IP Configuration

IP Address: 192.168.20.254

Subnet Mask: 255.255.255.0/24

Routing without NAT

Enabled

IP Address: 192.168.30.1

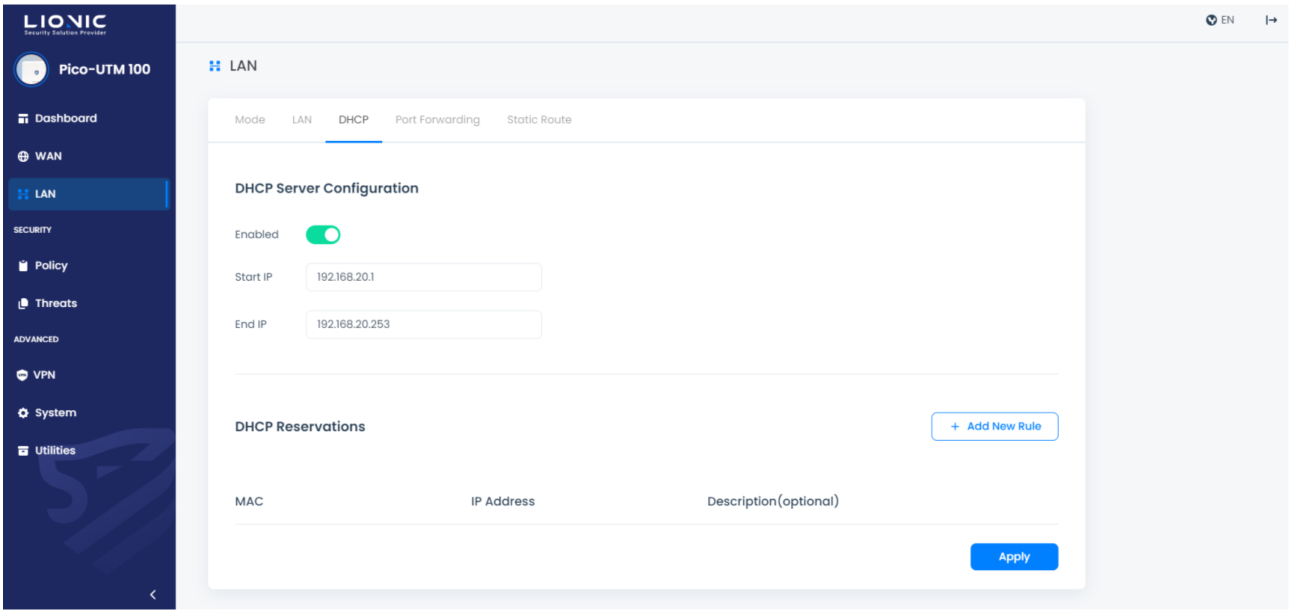
Subnet Mask: 255.255.255.0/24

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], Pico-UTM 100 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 Pico-UTM 100, you can use DHCP to assign private IP addresses to LAN devices.



DHCP Server Configuration

Enabled

Start IP 192.168.20.1

End IP 192.168.20.253

DHCP Reservations

MAC	IP Address	Description(optional)

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

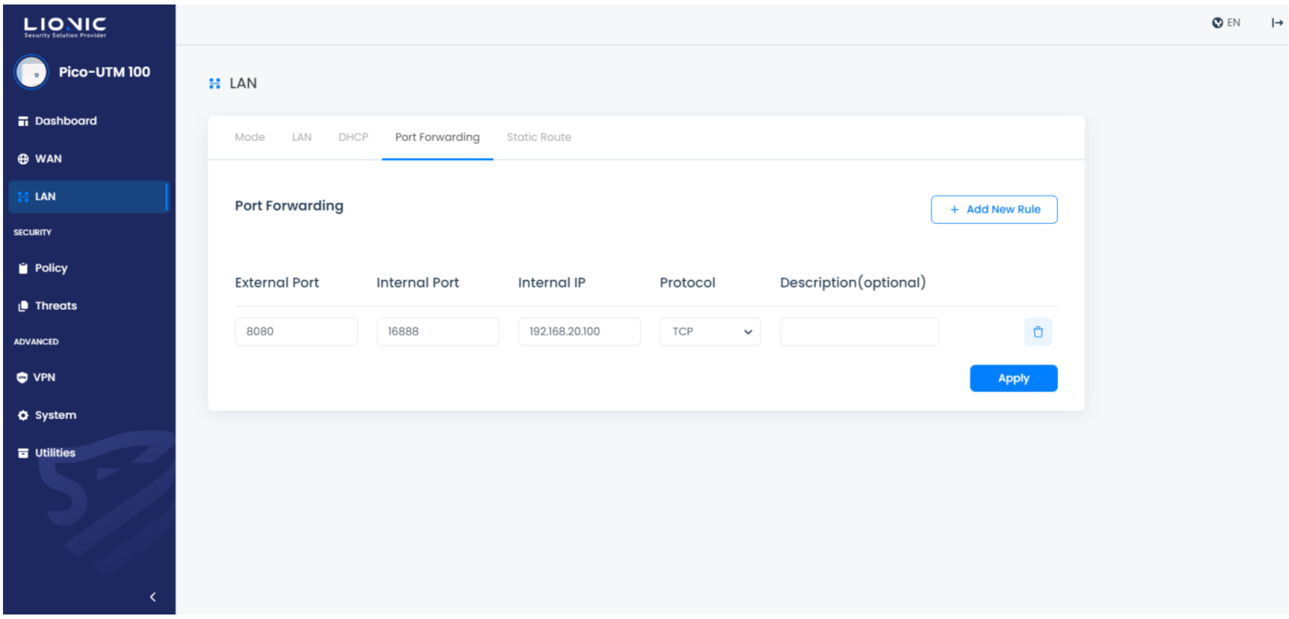
DHCP Reservations

- 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], Pico-UTM 100 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.



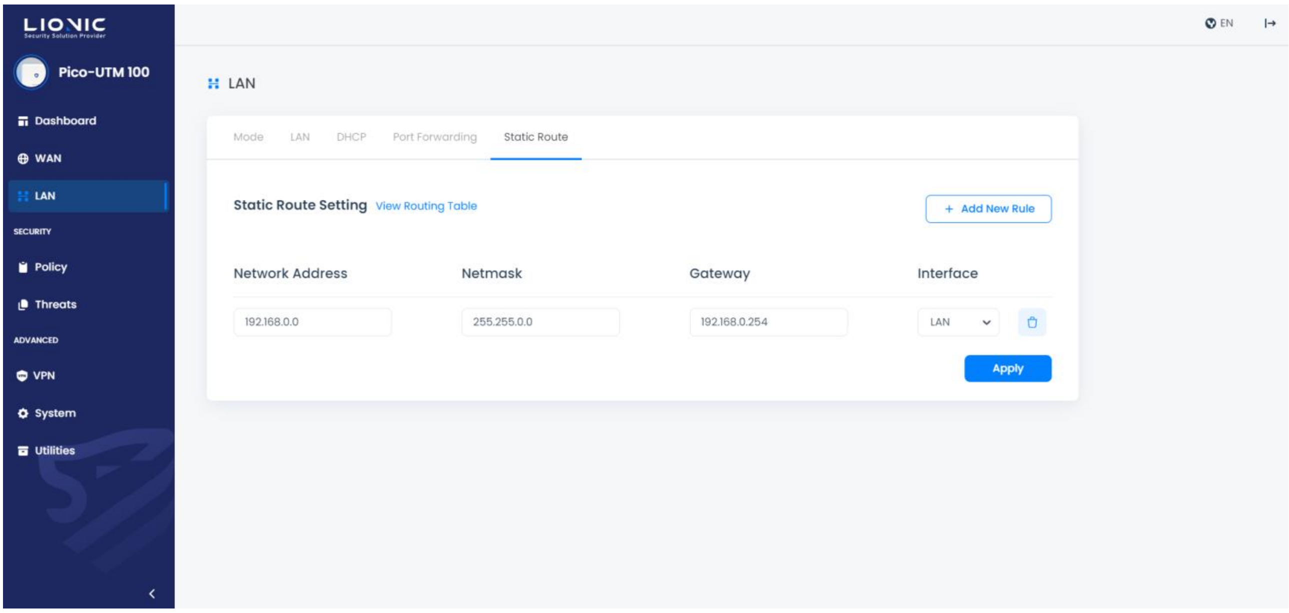
Port Forwarding

External Port	Internal Port	Internal IP	Protocol	Description(optional)
8080	16888	192.168.20.100	TCP	

LAN-Port Forwarding

Static Route:

In [Router Mode], the Pico-UTM 100 can provide static routing functionality. This feature can be used when there is a need to connect different network segments.



Static Route Setting

Network Address	Netmask	Gateway	Interface
192.168.0.0	255.255.0.0	192.168.0.254	LAN

LAN-Static Route

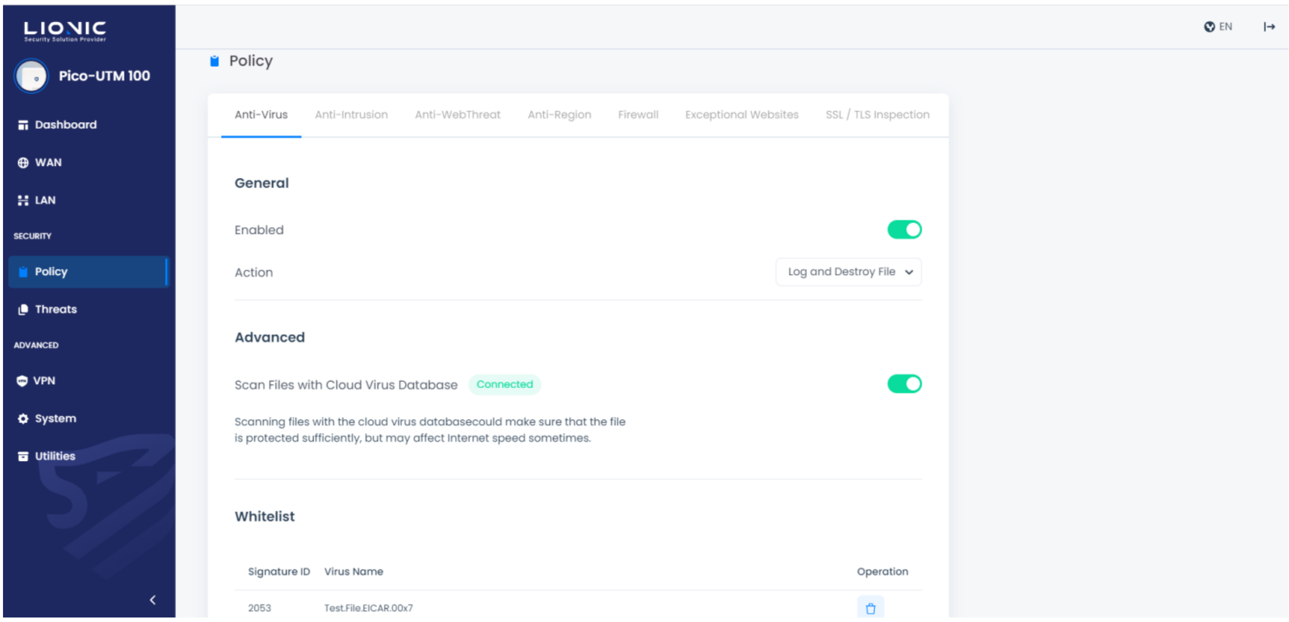
Policy

Pico-UTM 100 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, Keep PCAP when a threat is detected	---
Whitelist	View and remove whitelist rule	View and remove whitelist rule	View and remove whitelist rule



General

Enabled

Action: Log and Destroy File

Advanced

Scan Files with Cloud Virus Database Connected

Scanning files with the cloud virus databasecould make sure that the file is protected sufficiently, but may affect Internet speed sometimes.

Whitelist

Signature ID	Virus Name	Operation
2053	Test.File.EICAR.00x7	

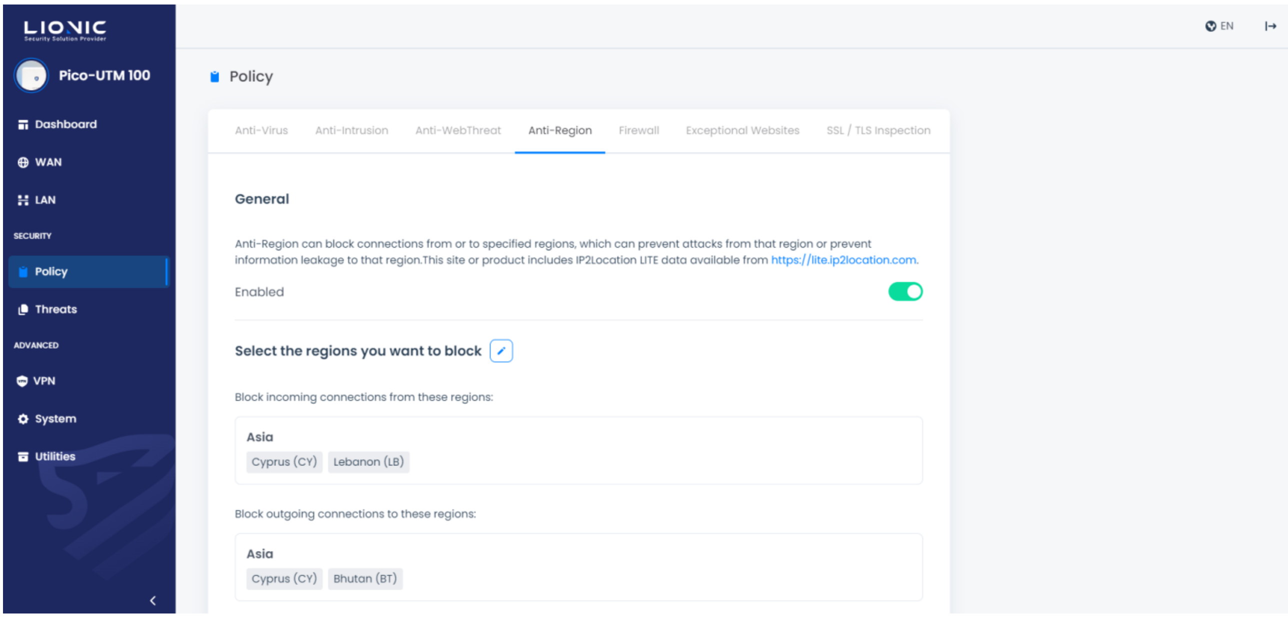
Policy

- **Enabled:** Enable or disable each security feature separately. The default setting is ENABLE.
- **Action:** The action that Pico-UTM 100 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, Pico-UTM 100 features the scan with LIONIC cloud virus database. To obtain the full protection of Anti-Virus, please make sure your Pico-UTM 100 is activated with a valid license code, and connected to the Internet.
- **Block Brute-force attacks:** After this function is enabled, Pico-UTM 100 can detect frequent login failures in a short period. Once the occurrence frequency is higher than the threshold, Pico-UTM 100 will record or block the attempting attack based on the frequency.
- **Block Protocol Anomaly:**After enabling this feature, Pico-UTM 100'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, Pico-UTM 100 will save packets considered as threats when detected in [Anti-Intrusion], allowing for subsequent analysis.
- **Whitelist:** To correct a trusted file or connection destroyed/blocked by Pico-UTM 100 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.



General

Anti-Region can block connections from or to specified regions, which can prevent attacks from that region or prevent information leakage to that region.This site or product includes IP2Location LITE data available from https://lite.ip2location.com.

Enabled

Select the regions you want to block

Block incoming connections from these regions:

Asia
Cyprus (CY) Lebanon (LB)

Block outgoing connections to these regions:

Asia
Cyprus (CY) Bhutan (BT)

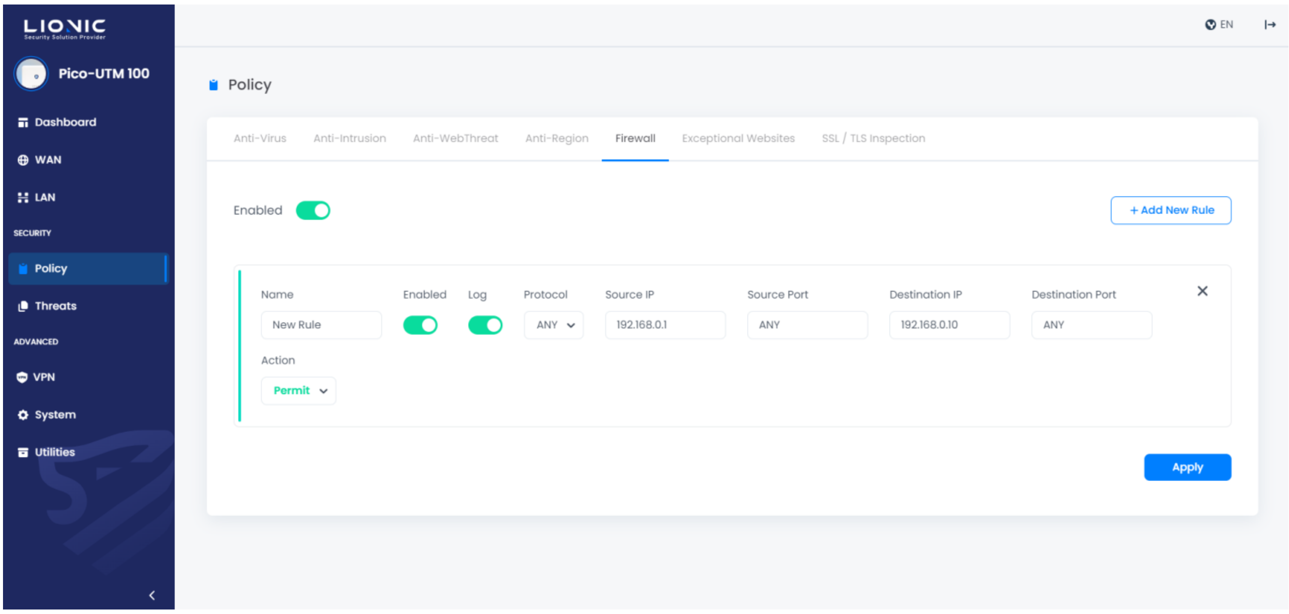
Policy-Anti-Region

- 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, Pico-UTM 100 also provide a basic firewall.



Enabled

Name	Enabled	Log	Protocol	Source IP	Source Port	Destination IP	Destination Port
New Rule	●	●	ANY	192.168.0.1	ANY	192.168.0.10	ANY

Action: Permit

Policy-Firewall

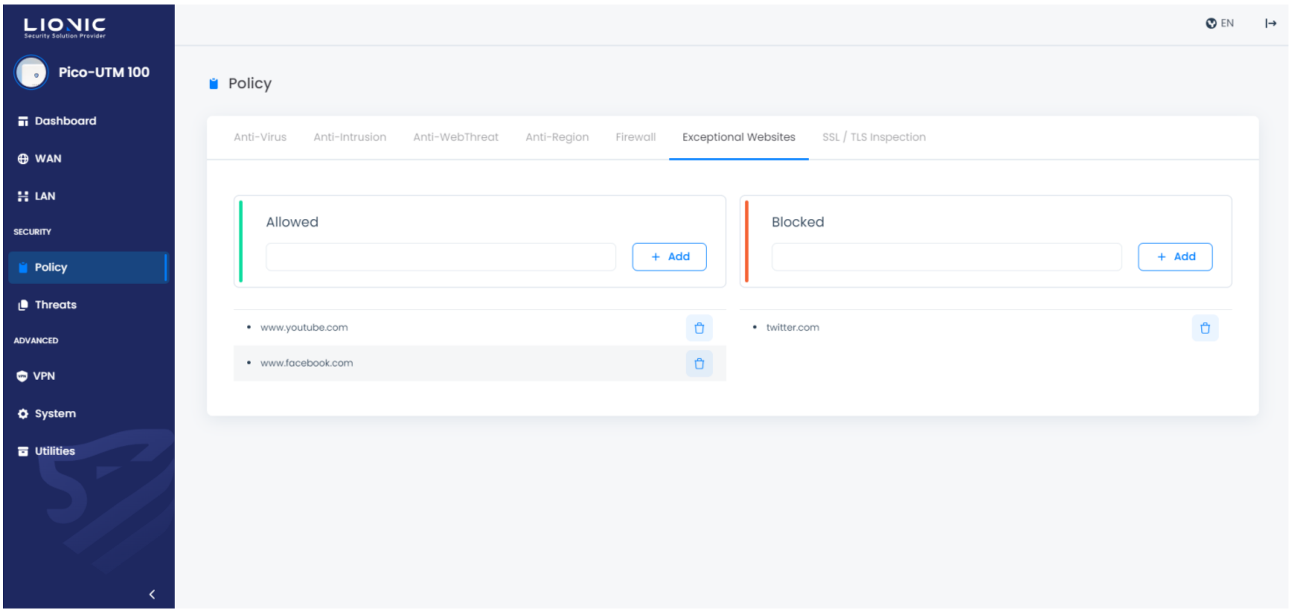
- Step 1: Enable the firewall (default is enabled).
- Step 2: Click [+Add New Rule].
- Step 3: Fill each configuration.
- Step 4: Click [Apply] to take effect.

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.



Allowed:
- www.youtube.com
- www.facebook.com

Blocked:
- twitter.com

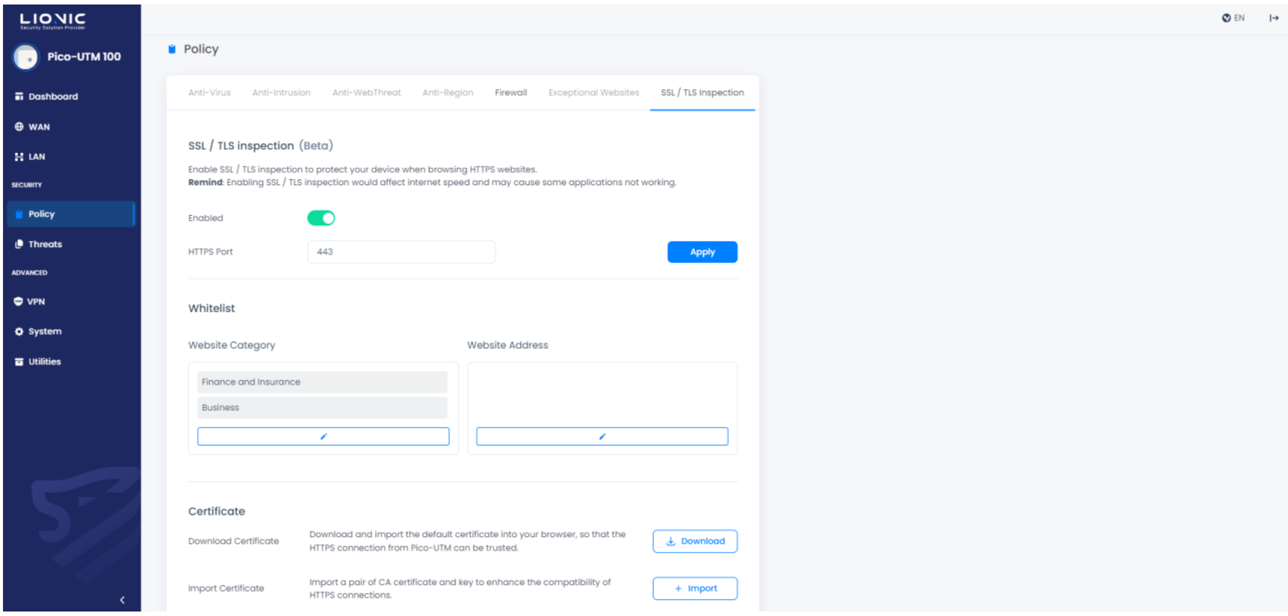
Policy-Exceptional Websites

- 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, Pico-UTM 100 will inspect packets encrypted with SSL or TLS, in order to protect your device when browsing HTTPS websites.



SSL / TLS inspection (Beta)

Enable SSL / TLS inspection to protect your device when browsing HTTPS websites.
Remind: Enabling SSL / TLS inspection would affect internet speed and may cause some applications not working.

Enabled: on

HTTPS Port: 443

Whitelist

Website Category: Finance and Insurance; Business

Website Address

Certificate

Download Certificate: Download and import the default certificate into your browser, so that the HTTPS connection from Pico-UTM can be trusted.

Import Certificate: Import a pair of CA certificate and key to enhance the compatibility of HTTPS connections.

Policy-SSL/TLS Inspection

- **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.

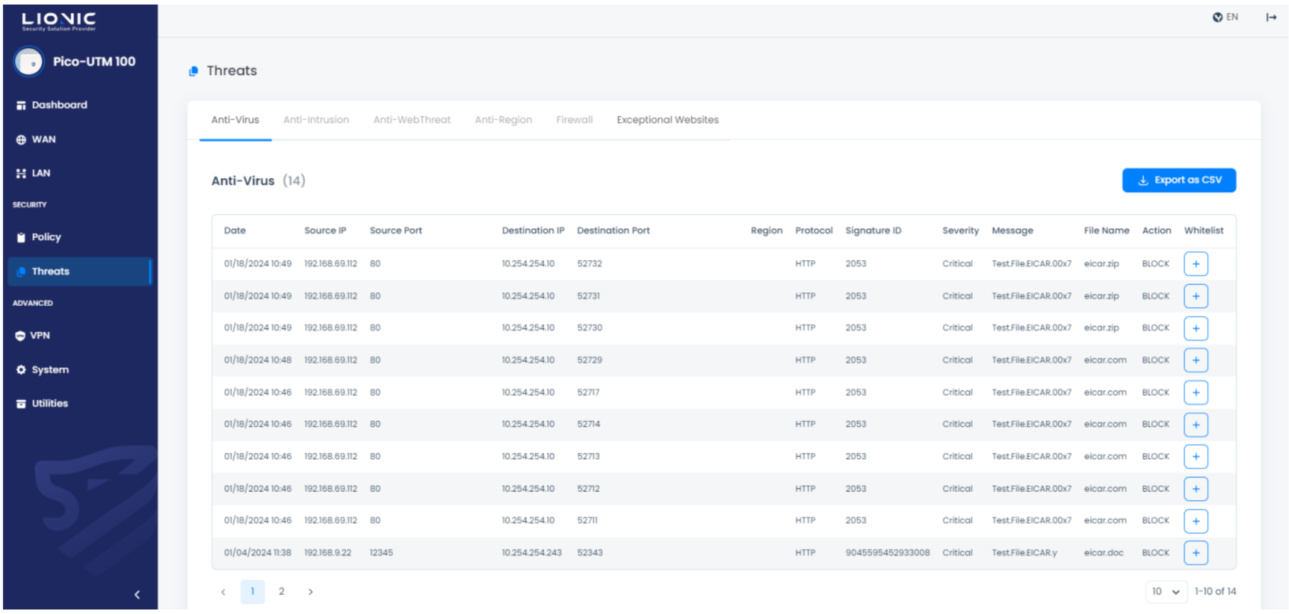
- **Whitelist:** After a website is added into the whitelist, Pico-UTM 100 will not inspect encrypted packets from / to the website. If you would like to keep the SSL / TLS packet encrypted due to the compatibility or the privacy, please add the trusted website into the whitelist.
- **Website Category:** Pico-UTM 100 provides various website categories as options for whitelisting. After adding a specified website category to the whitelist, connections to websites that meet the classification criteria will not be subject to encrypted packet inspection.

  - Website Address: Pico-UTM 100 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 Pico-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 compatibilty 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 Pico-UTM 100, the detailed threat information would be shown on the corresponding tab of each security feature in [Threats] page.



Anti-Virus (14)

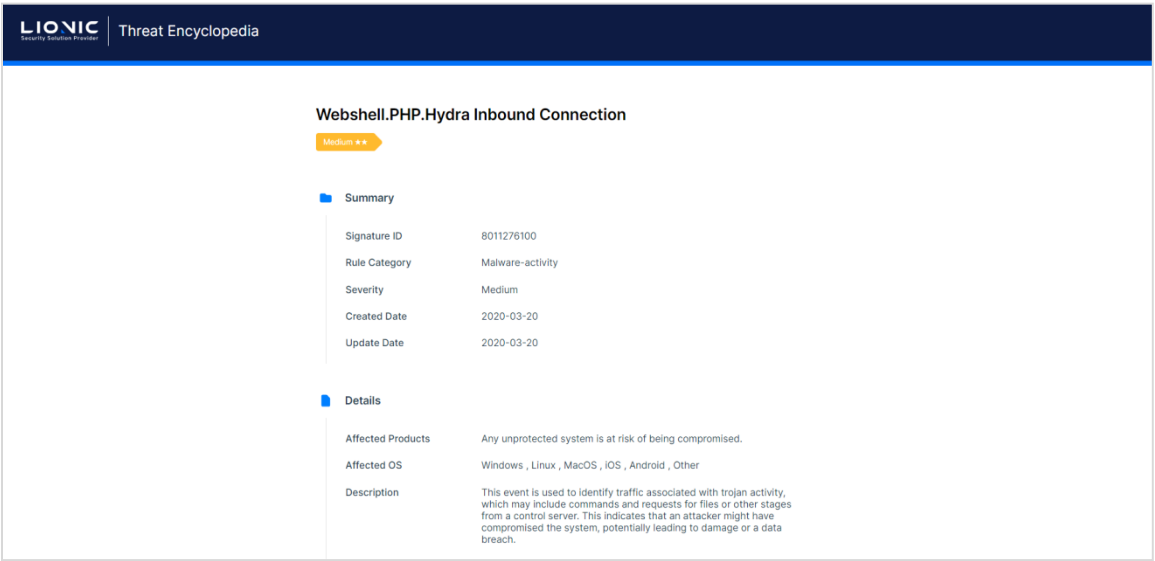
Date	Source IP	Source Port	Destination IP	Destination Port	Region	Protocol	Signature ID	Severity	Message	File Name	Action	Whitelist
01/18/2024 10:49	192.168.69.112	80	10.254.254.10	52732		HTTP	2053	Critical	Test.File.EICAR.00x7	eicar.zip	BLOCK	+
01/18/2024 10:49	192.168.69.112	80	10.254.254.10	52731		HTTP	2053	Critical	Test.File.EICAR.00x7	eicar.zip	BLOCK	+
01/18/2024 10:49	192.168.69.112	80	10.254.254.10	52730		HTTP	2053	Critical	Test.File.EICAR.00x7	eicar.zip	BLOCK	+
01/18/2024 10:48	192.168.69.112	80	10.254.254.10	52729		HTTP	2053	Critical	Test.File.EICAR.00x7	eicar.com	BLOCK	+
01/18/2024 10:46	192.168.69.112	80	10.254.254.10	52717		HTTP	2053	Critical	Test.File.EICAR.00x7	eicar.com	BLOCK	+
01/18/2024 10:46	192.168.69.112	80	10.254.254.10	52714		HTTP	2053	Critical	Test.File.EICAR.00x7	eicar.com	BLOCK	+
01/18/2024 10:46	192.168.69.112	80	10.254.254.10	52713		HTTP	2053	Critical	Test.File.EICAR.00x7	eicar.com	BLOCK	+
01/18/2024 10:46	192.168.69.112	80	10.254.254.10	52712		HTTP	2053	Critical	Test.File.EICAR.00x7	eicar.com	BLOCK	+
01/18/2024 10:46	192.168.69.112	80	10.254.254.10	52711		HTTP	2053	Critical	Test.File.EICAR.00x7	eicar.com	BLOCK	+
01/04/2024 11:38	192.168.9.22	12345	10.254.254.243	52343		HTTP	9045595452933008	Critical	Test.File.EICAR.y	eicar.doc	BLOCK	+

Threats

- **Export as CSV:** Export and download the log in a CSV file.
- **Whitelist:** If Pico-UTM 100 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 threat logs of [Anti-Intrusion], clicking on the Signature ID allows you to access the analysis and solutions for the corresponding attack。



Webshell.PHP.Hydra Inbound Connection

Summary

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

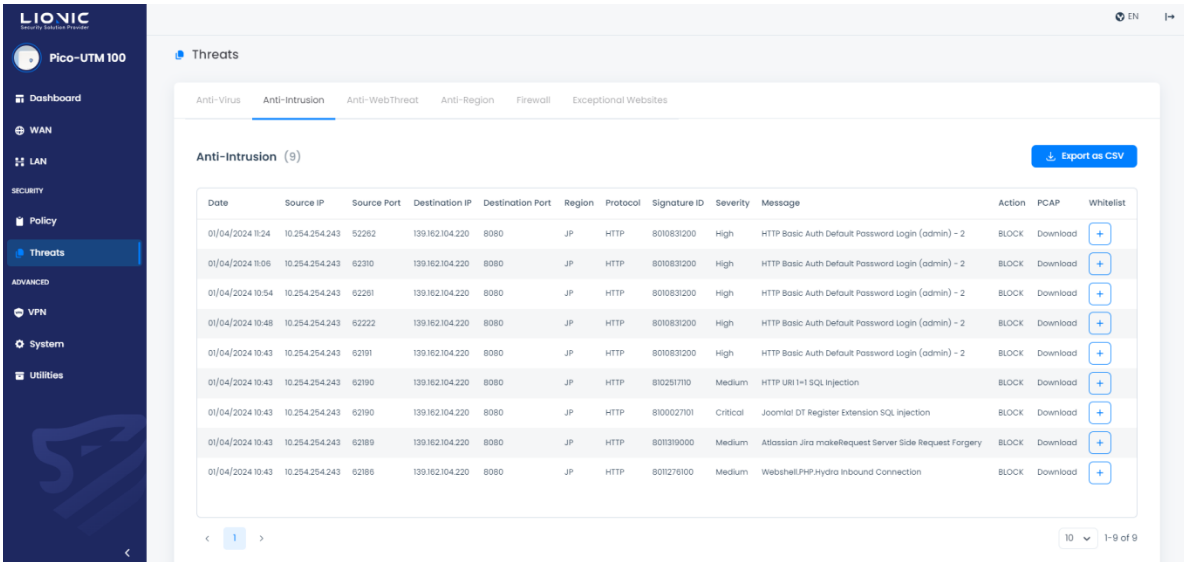
Details

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-Threat Encyclopedia

PCAP Packet Download:

When events of compromise or blockage occur on Pico-UTM 100, clicking [PCAP] > [Download] allows for packet download for further analysis.



Anti-Intrusion (9)

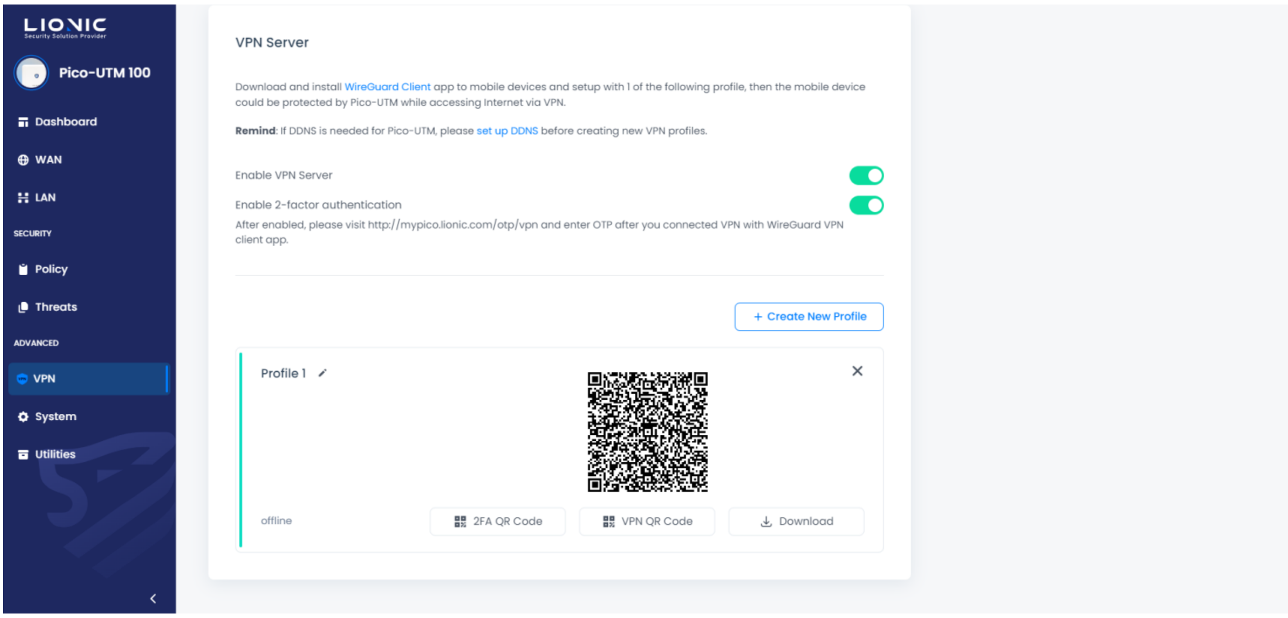
Date	Source IP	Source Port	Destination IP	Destination Port	Region	Protocol	Signature ID	Severity	Message	Action	PCAP	Whitelist
01/04/2024 11:24	10.254.254.243	52262	139.162.104.220	8080	JP	HTTP	8010831200	High	HTTP Basic Auth Default Password Login (admin) - 2	BLOCK	Download	+
01/04/2024 11:06	10.254.254.243	62310	139.162.104.220	8080	JP	HTTP	8010831200	High	HTTP Basic Auth Default Password Login (admin) - 2	BLOCK	Download	+
01/04/2024 10:54	10.254.254.243	62261	139.162.104.220	8080	JP	HTTP	8010831200	High	HTTP Basic Auth Default Password Login (admin) - 2	BLOCK	Download	+
01/04/2024 10:48	10.254.254.243	62222	139.162.104.220	8080	JP	HTTP	8010831200	High	HTTP Basic Auth Default Password Login (admin) - 2	BLOCK	Download	+
01/04/2024 10:43	10.254.254.243	62191	139.162.104.220	8080	JP	HTTP	8010831200	High	HTTP Basic Auth Default Password Login (admin) - 2	BLOCK	Download	+
01/04/2024 10:43	10.254.254.243	62190	139.162.104.220	8080	JP	HTTP	8102517110	Medium	HTTP URI 1=1 SQL Injection	BLOCK	Download	+
01/04/2024 10:43	10.254.254.243	62190	139.162.104.220	8080	JP	HTTP	8100027101	Critical	Joomla! DT Register Extension SQL injection	BLOCK	Download	+
01/04/2024 10:43	10.254.254.243	62189	139.162.104.220	8080	JP	HTTP	8011319000	Medium	Atlassian Jira makeRequest Server Side Request Forgery	BLOCK	Download	+
01/04/2024 10:43	10.254.254.243	62186	139.162.104.220	8080	JP	HTTP	8011276100	Medium	Webshell.PHP.Hydra Inbound Connection	BLOCK	Download	+

Threats -PCAP Download

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

VPN Server

Enable the VPN server to expand the protecting range of Pico-UTM 100 to devices using cellular network or public Wi-Fi. Mobile devices could be protected by Pico-UTM 100 while accessing Internet via VPN.



VPN Server

Download and install WireGuard Client app to mobile devices and setup with 1 of the following profile, then the mobile device could be protected by Pico-UTM while accessing Internet via VPN.

Remind: If DDNS is needed for Pico-UTM, please set up DDNS before creating new VPN profiles.

Enable VPN Server ●

Enable 2-factor authentication ●

After enabled, please visit http://mypico.lionic.com/otp/vpn and enter OTP after you connected VPN with WireGuard VPN client app.

VPN Server

Preparation:
Download and install WireGuard Client app to the device which needs the protection of Pico-UTM 100.

Setup:

- Step 1: Click [Enabled].
- 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 Pico-UTM 100 via VPN with WireGuard Client app whenever the protection of Pico-UTM 100 is needed.

* Remark:

1. If you would like to set DDNS for Pico-UTM 100, please setup before enabling the VPN server.
2. If there is a router at the WAN side of Pico-UTM 100, please set port forwarding on the router, so that the connection could be redirected to Port 51820 of Pico-UTM 100. 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 Pico-UTM 100.
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.
- Stpe 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.

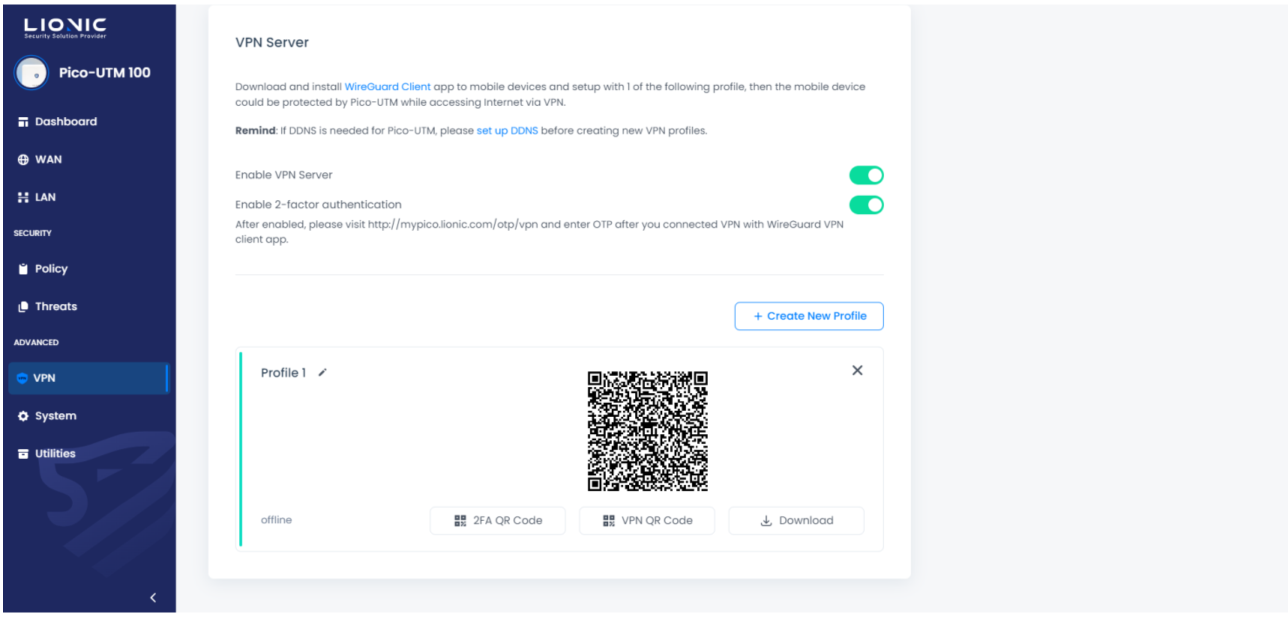
Start Accessing Internet via VPN:

- Step 1: Connect Pico-UTM 100 via VPN with WireGuard Client app.
- Step 2: Obtain the OTP from the OTP app.
- Step 3: Visit http://mypico.lionic.com/otp/vpn and enter the OTP.

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

System

Device:



VPN Server

Download and install WireGuard Client app to mobile devices and setup with 1 of the following profile, then the mobile device could be protected by Pico-UTM while accessing Internet via VPN.

Remind: If DDNS is needed for Pico-UTM, please set up DDNS before creating new VPN profiles.

Enable VPN Server

Enable 2-factor authentication

After enabled, please visit http://mypico.lionic.com/otp/vpn and enter OTP after you connected VPN with WireGuard VPN client app.

System-Device

License Management

View the license status, activate or renew the license for Pico-UTM 100.

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 Pico-UTM 100, enter the activation code (Remark 1) into the input field and click [Activate] while connecting Internet.
- **Renew license:** Pico-UTM 100 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.

Date & Time

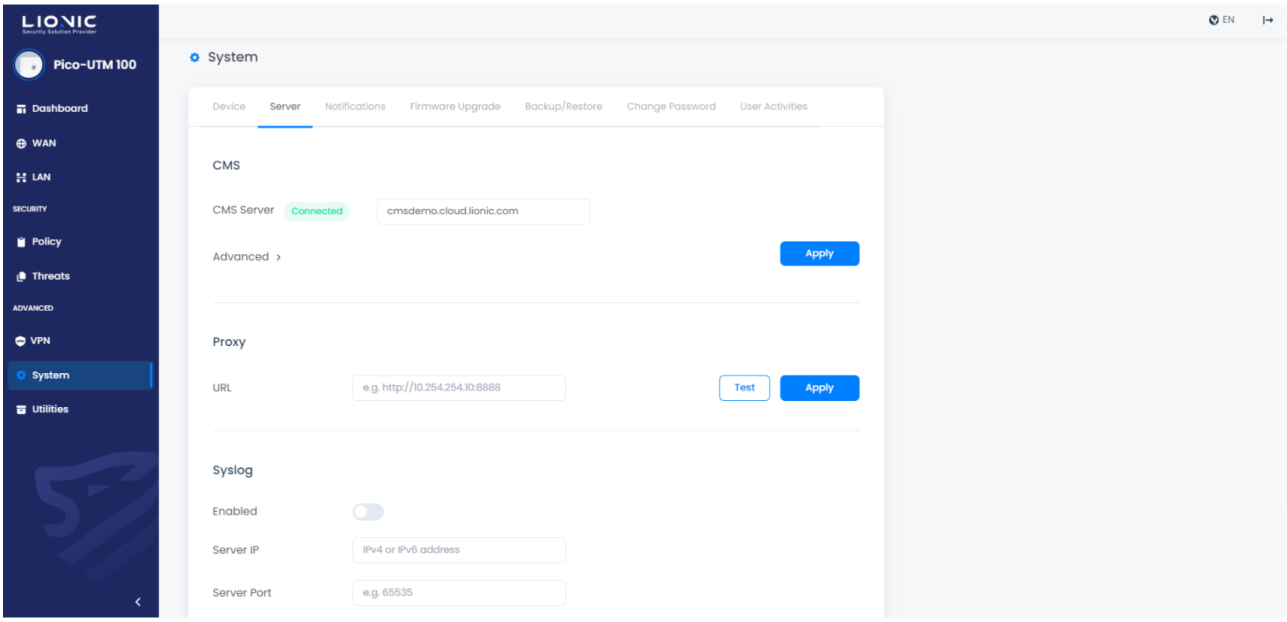
Display and configure the system time of Pico-UTM 100.

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

* 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 Pico-UTM 100 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.

Server:



CMS

CMS Server Connected cmsdemo.cloud.lionic.com

Advanced ›

Proxy

URL e.g. http://10.254.254.10:8888

Syslog

Enabled

Server IP IPv4 or IPv6 address

Server Port e.g. 65535

System-Server

CMS

Central Management System (CMS) can monitor and control multiple Pico-UTM 100 in 1 portal. After the CMS is built, enter the address of CMS into the input field and click [Apply] to connect Pico-UTM 100 with the CMS. Please contact Pico-UTM 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, Pico-UTM 100, 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

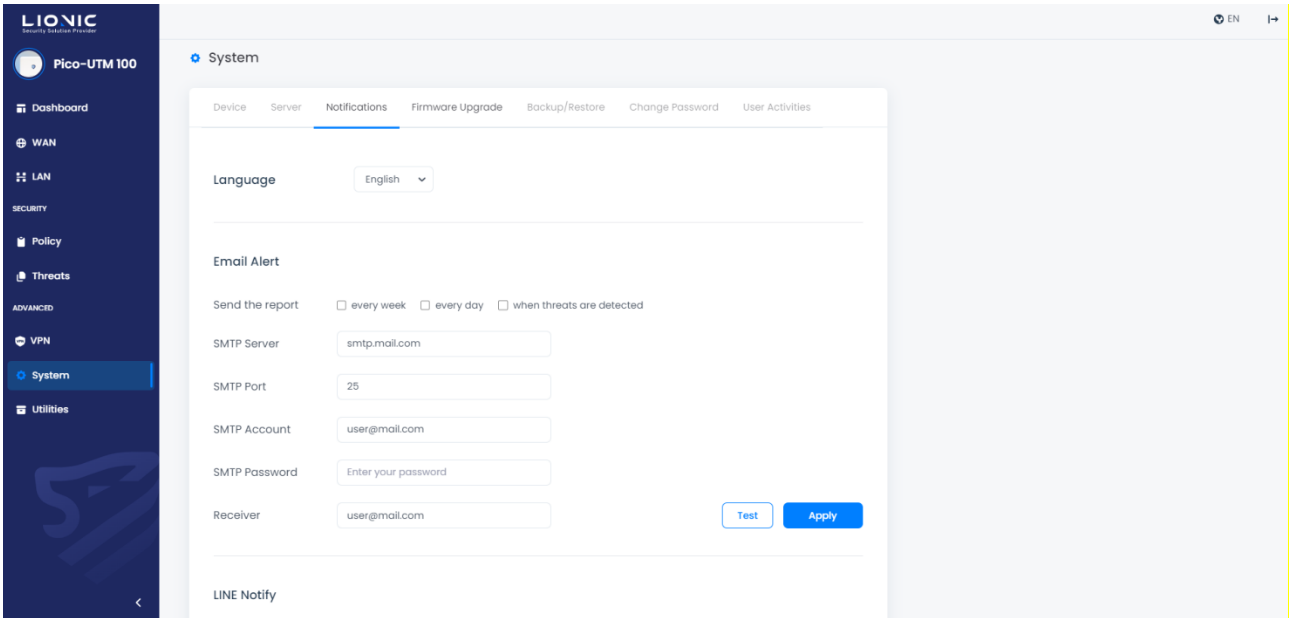
To obtain the full protection from Pico-UTM 100, the proxy server can help Pico-UTM 100 deployed in an intranet access LIONIC cloud services. After the proxy server is built, enter the server address into the input field and click [Apply] to access LIONIC cloud services via the proxy server. Please contact your IT administrator for more information.

Syslog

A syslog server can collect operating history of Pico-UTM 100. If you have your own syslog server, enter the configuration into the input field and click [Apply].

Notifications:

The [Notification] feature allows Pico-UTM 100 to send threat information via email to a specified mailbox or as LINE messages to a designated LINE account when a cybersecurity threat is detected. In addition, it can compile information such as detection history, threat statistics, system abnormal records, etc., into weekly or daily reports and send them to a specified email address.



Language: English

Email Alert

Send the report: □ every week □ every day □ when threats are detected

SMTP Server: smtp.mail.com

SMTP Port: 25

SMTP Account: user@mail.com

SMTP Password: Enter your password

Receiver: user@mail.com

LINE Notify

System-Email Alert

- **Language:** Choose the language for notification emails, statistical reports, and LINE message content (Chinese/English/Japanese).
- **Sending Frequency**:
  - Weekly: Weekly reports are sent every Sunday at 00:00.
  - Daily: Daily reports are sent every day at 00:00.
  - When threats are detected: Threat information is sent immediately upon detection.
- **SMTP Server, Port, Account, and Password:** Sending settings for notification emails and statistical reports.
- **Recipient:** Email address of the recipient.

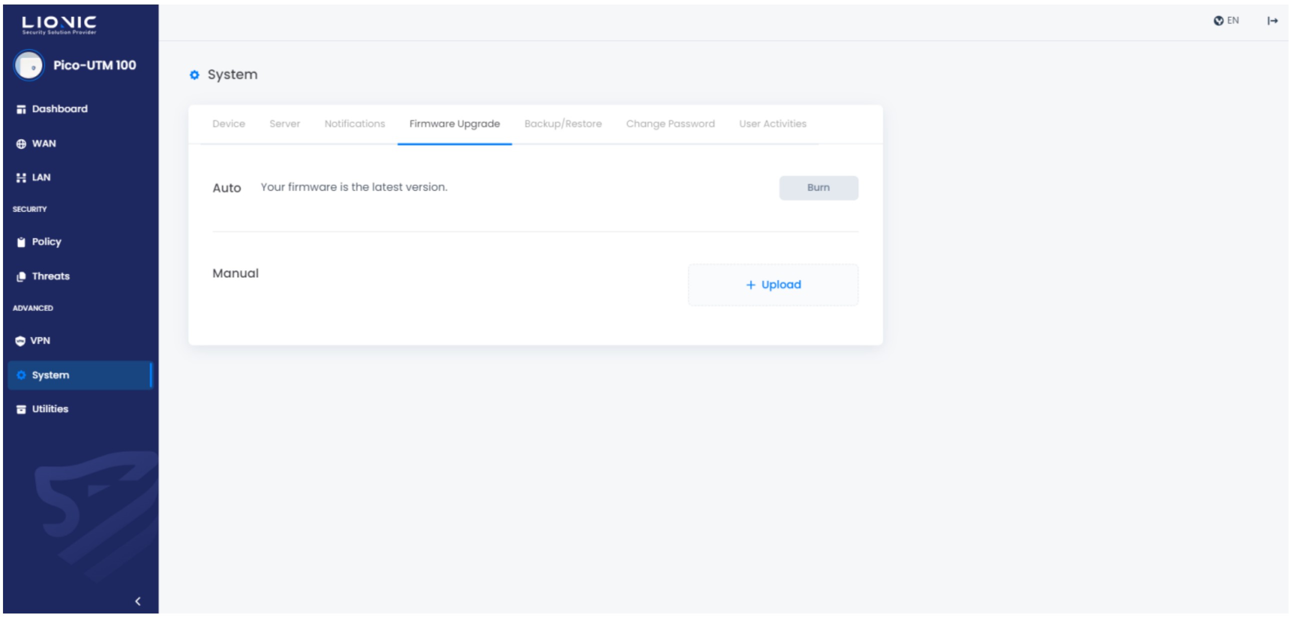
Please enter the correct settings in the input box and click [Apply] to complete the configuration. Click [Test] to have Pico-UTM 100 send a test email to confirm the settings.

* 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.
2. To use the LINE message notification feature, please follow the instructions on the LINE Notify official website to obtain a LINE Token. Then, enter the token in the input box and click [Add] to 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.



Your firmware is the latest version.

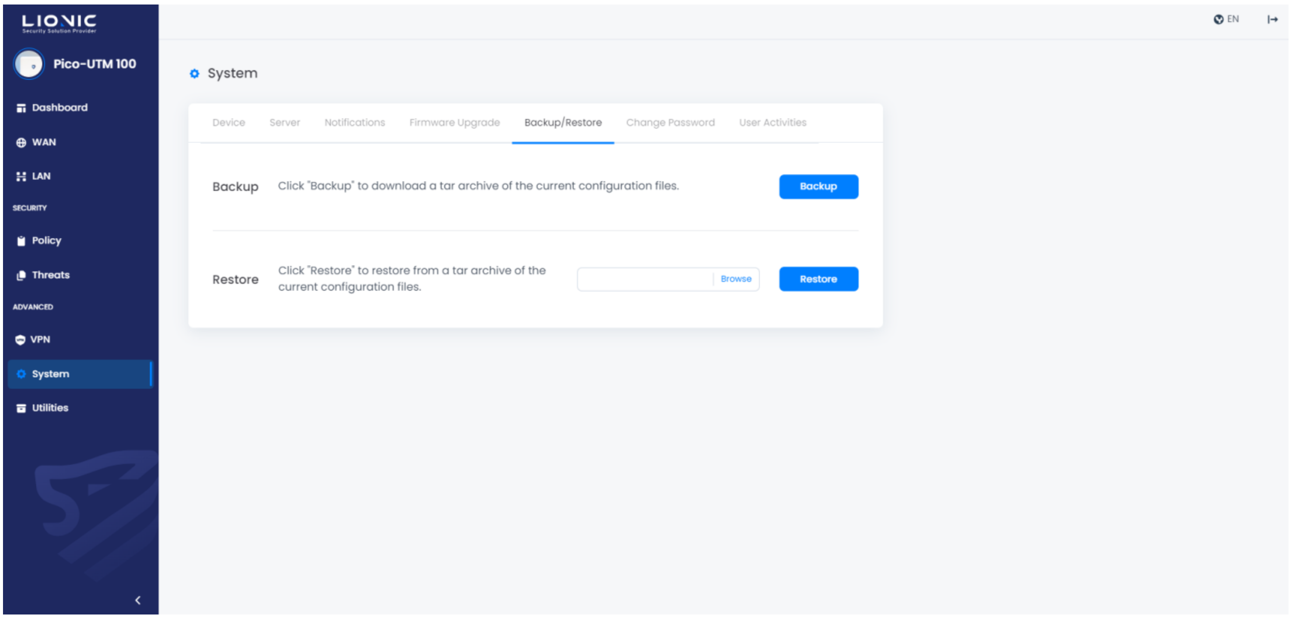
System-Firmware Upgrade

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

* Remark: Pico-UTM 100 would reboot during upgrading firmware. The network connection will resume after the reboot is completed.

Backup / Restore:

[Backup / Restore] function can backup Pico-UTM 100 configurations, such as security policies and whitelist setting, and restore on the same or other Pico-UTM 100.



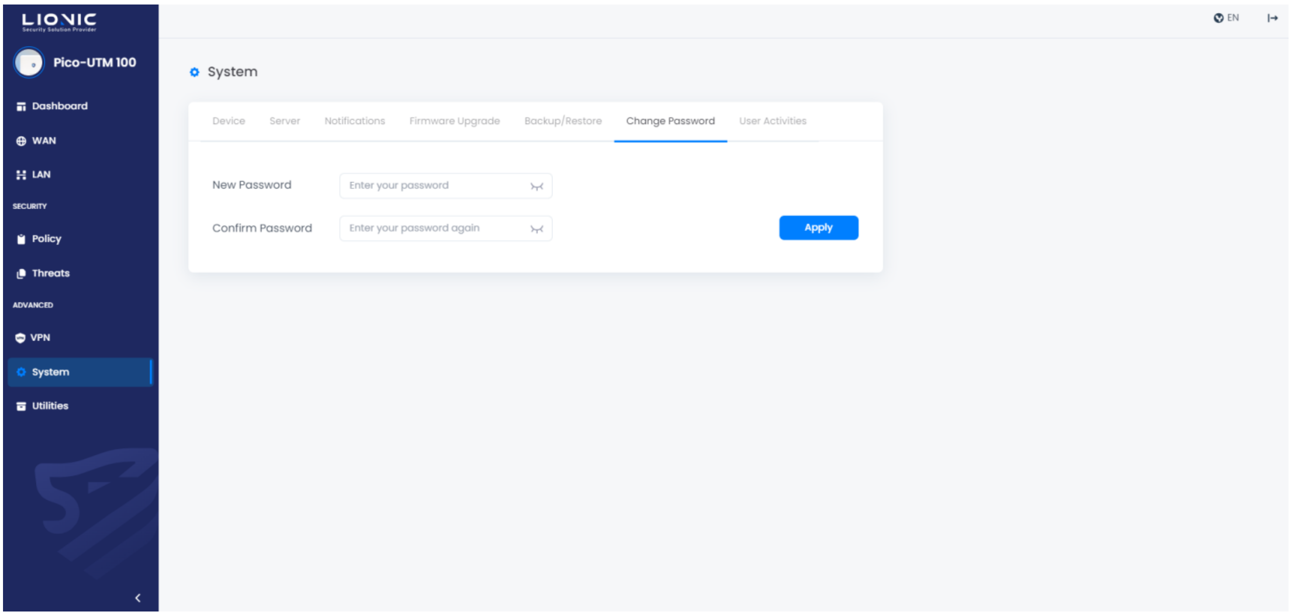
Backup — Click "Backup" to download a tar archive of the current configuration files.

Restore — Click "Restore" to restore from a tar archive of the current configuration files.

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].



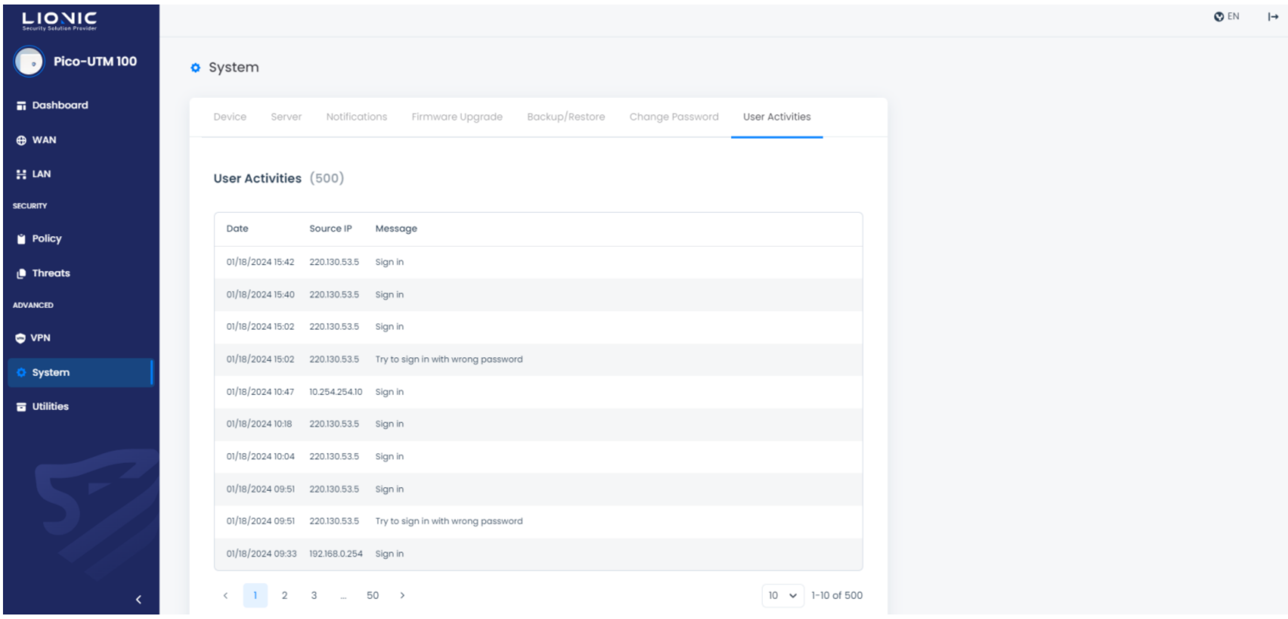
New Password: Enter your password

Confirm Password: Enter your password again

System-Change Password

User Activities:

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

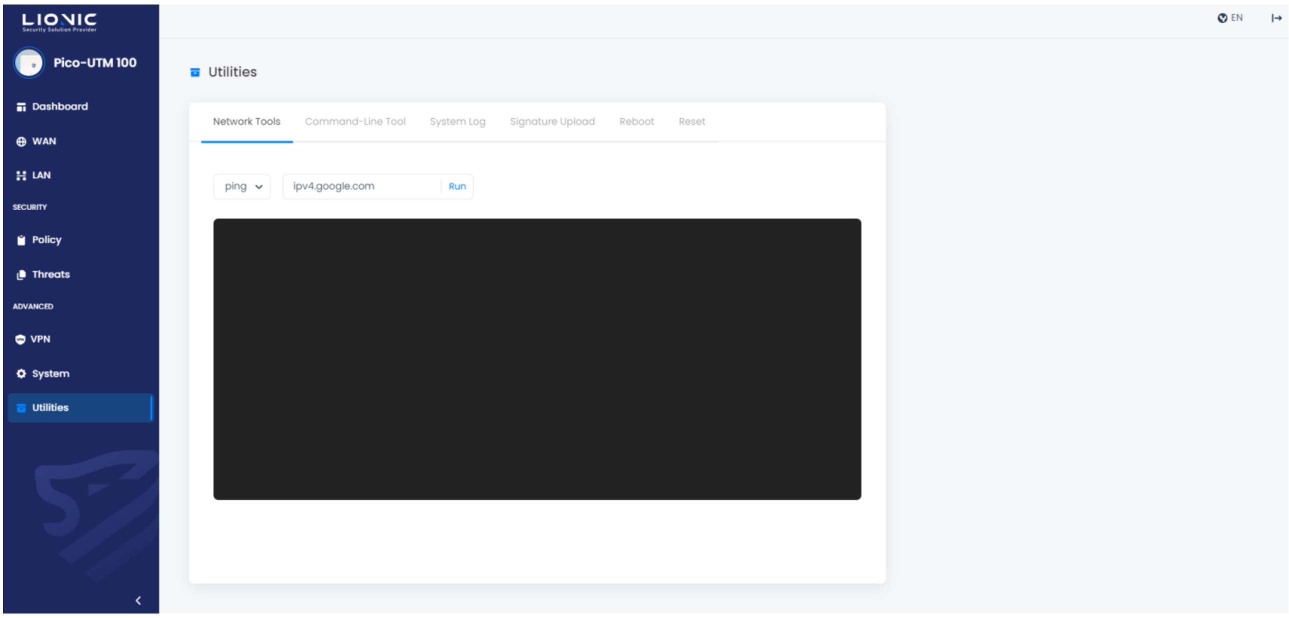


User Activities (500)

Date	Source IP	Message
01/18/2024 15:42	220.130.53.5	Sign in
01/18/2024 15:40	220.130.53.5	Sign in
01/18/2024 15:02	220.130.53.5	Sign in
01/18/2024 15:02	220.130.53.5	Try to sign in with wrong password
01/18/2024 10:47	10.254.254.10	Sign in
01/18/2024 10:18	220.130.53.5	Sign in
01/18/2024 10:04	220.130.53.5	Sign in
01/18/2024 09:51	220.130.53.5	Sign in
01/18/2024 09:51	220.130.53.5	Try to sign in with wrong password
01/18/2024 09:33	192.168.0.254	Sign in

System-User Activities

Utilities



Utilites

Pico-UTM 100 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 Pico-UTM 100.
- **Reset:** Reset all configuration to the factory default settings.

* Remark: While the license is valid and Internet is connected, Pico-UTM 100 would automatically download and update the signature.

Pico-UTM 100
Makes Security Simple

LIONIC
Security Solution Provider

Sales Contact
Tel : +886-3-5789399
Fax : +886-3-5789595
Email : sales@lionic.com
https://www.pico-utm.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.