Security Solution Provider

Web GUI User Manual

Dual Ark-UTM 16

Version 1.4.1

Released on Feb 2025

Lionic Corp. www.lionic.com

Dual Ark-UTM 16 User Manual

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.

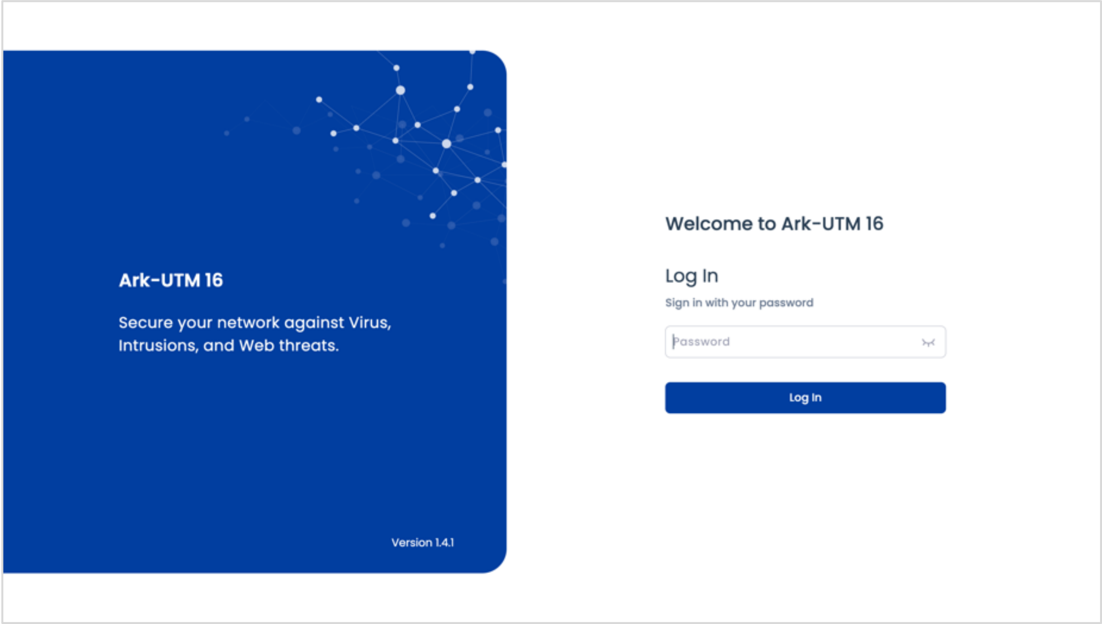
Technical Support Lionic Corporation

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

Content

Access Web GUI and Connect to the Network

1. Plug the power cable into Ark-UTM 16.
2. Connect the WAN port of Ark-UTM 16 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 Ark-UTM 16 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.



Ark-UTM 16

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

Version 1.4.1

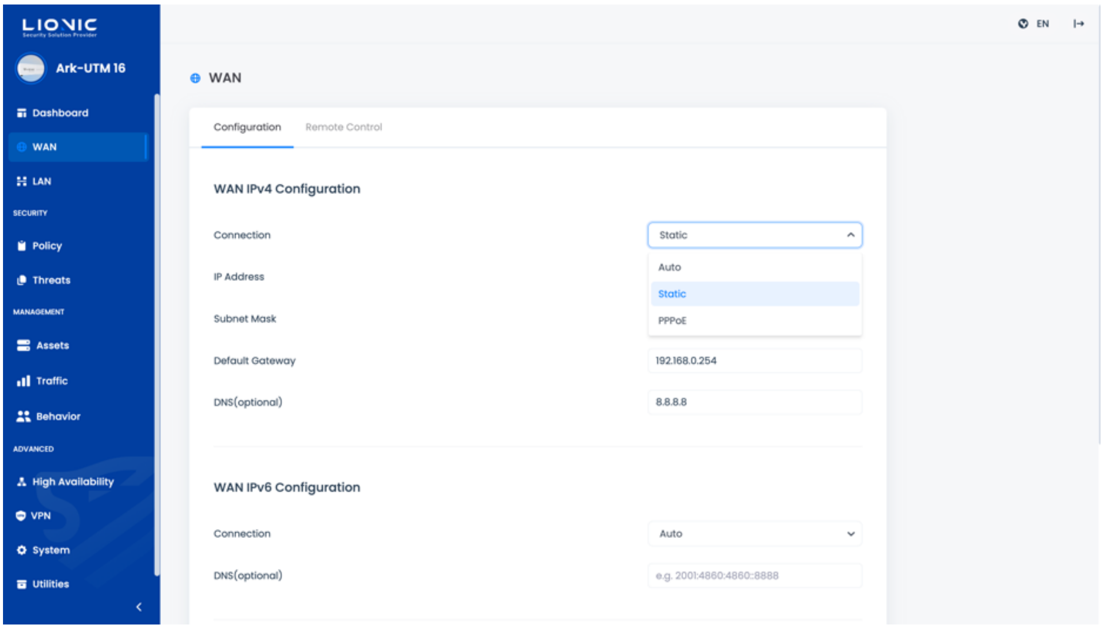
Welcome to Ark-UTM 16

Log In

Sign in with your password

Login page

6. The default password for login is the Serial Number shown at the bottom of the product.
7. After logged in, set the network configuration of Ark-UTM 16 in [WAN] page.



WAN IPv4 Configuration

Connection: Static (Auto / Static / PPPoE)

IP Address

Subnet Mask

Default Gateway: 192.168.0.254

DNS(optional): 8.8.8.8

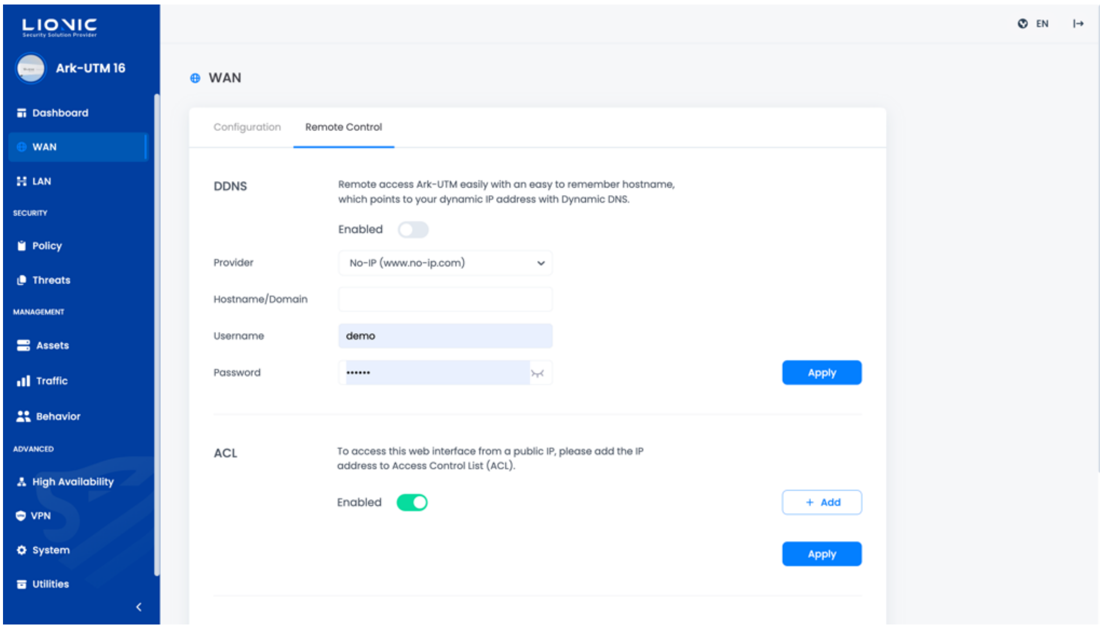
WAN IPv6 Configuration

Connection: Auto

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

WAN-WAN IP

8. After Ark-UTM 16 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 Ark-UTM 16 and your PC/Laptop are using private IP addresses in the same subnet, and the PC/Laptop is located at the LAN side of Ark-UTM 16, visit https://myark.lionic.com/ to access the web GUI.
   - When Ark-UTM 16 and your PC/Laptop are using different public IP addresses, and the PC/Laptop is located at the LAN side of Ark-UTM 16, 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://myark.lionic.com/ to access the web GUI.



DDNS

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

Enabled

Provider: No-IP (www.no-ip.com)

Hostname/Domain:

Username: demo

Password: ••••••

ACL

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

Enabled

WAN-Remote Control

Overview

Dashboard:

[Dashboard] shows operating status and device information of Ark-UTM 16, including Inspection History, threat statics, network traffic monitoring and system resource usage.

WAN:

WAN settings of Ark-UTM 16 could be configured in [WAN], such as IPv4/IPv6 configurations and [Remote Control] settings.

LAN:

LAN settings of Ark-UTM 16 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.

Management:

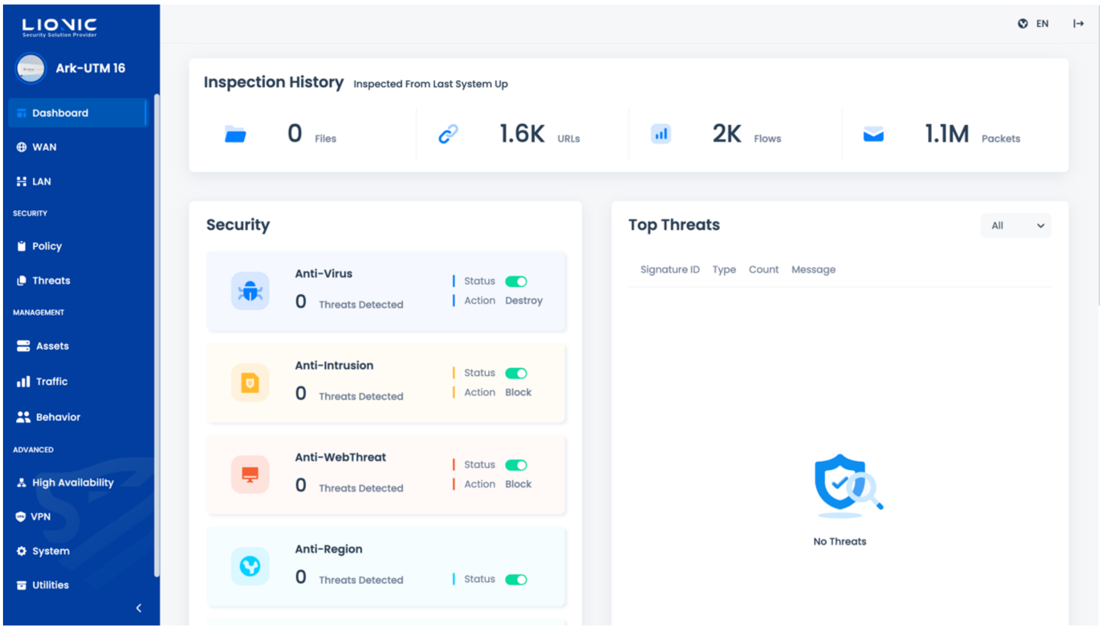
- **Assets:** The asset management feature can list the identified LAN devices and block or allow specific assets to connect to the network.
- **Traffic:** Traffic management can list the current connection usage of each LAN device and perform bandwidth management.
- Behavior Management: The behavior management feature allows you to manage specific content categories or applications.

Advanced:

- **High Availability:** Adding 2 or more Ark-UTM 16 into an HA group can maintain network connectivity without interruption by switching automatically in case of abnormalities.
- **VPN:** After the VPN server is enabled, the protecting range of Ark-UTM 16 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 Ark-UTM 16.



Inspection History Inspected From Last System Up

0 Files | 1.6K URLs | 2K Flows | 1.1M Packets

Security

Anti-Virus	0 Threats Detected	Status Action Destroy
Anti-Intrusion	0 Threats Detected	Status Action Block
Anti-WebThreat	0 Threats Detected	Status Action Block
Anti-Region	0 Threats Detected	Status

Top Threats

Signature ID	Type	Count	Message

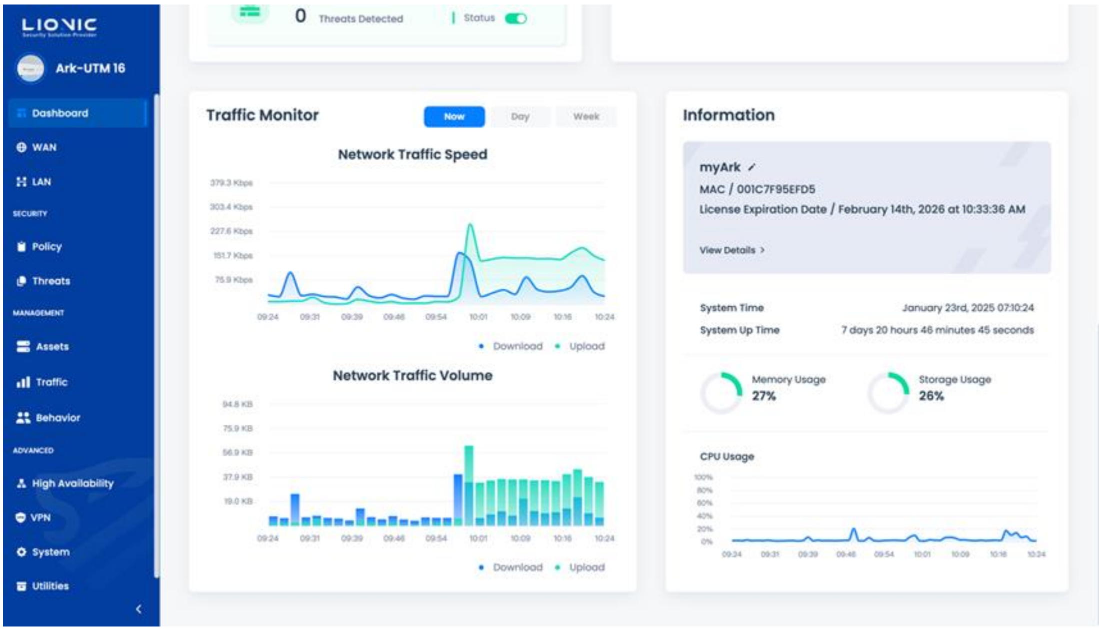
No Threats

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 Ark-UTM 16, 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.



myArk

MAC / 001C7F95EFD5

License Expiration Date / February 14th, 2026 at 10:33:36 AM

System Time January 23rd, 2025 07:10:24

System Up Time 7 days 20 hours 46 minutes 45 seconds

Dashboard

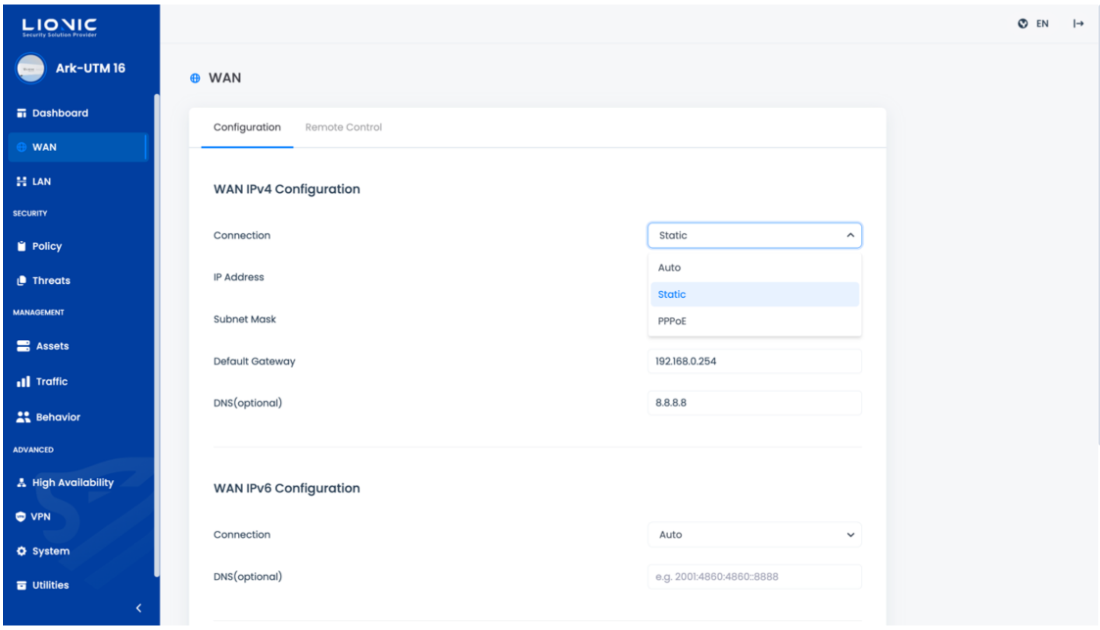
Traffic Monitor: Showing the download and upload traffic via Ark-UTM 16.

Information: Showing the device information of the Ark-UTM 16, 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 IPv4 Configuration

Connection: Static (Auto / Static / PPPoE)

IP Address

Subnet Mask

Default Gateway: 192.168.0.254

DNS(optional): 8.8.8.8

WAN IPv6 Configuration

Connection: Auto

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

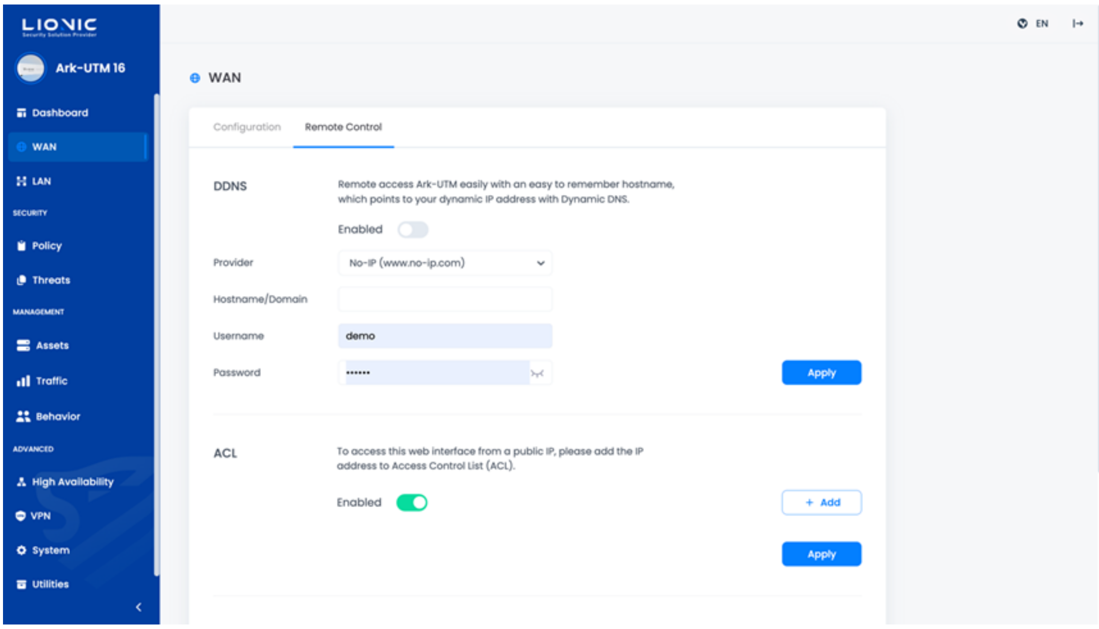
WAN- Configuration

- **Auto:** Ark-UTM 16 obtains DHCP IP address from the router placed at the WAN side of the Ark-UTM 16.
- **Static:** For user to fills the correct IP address in manual.
- **PPPoE:** For user to fills the correct username and password in manual.
- **VLAN**：When Ark-UTM 16 is deployed in a VLAN environment, you can enter the VLAN ID of the domain to which Ark-UTM 16 belongs here.

* Remark: When using PPPoE connection, you may not be able to access the web GUI of Ark-UTM 16 due to the restriction of the access control list (ACL). Please see [Remote Control] for more details of ACL.

Remote Control

To prevent Ark-UTM 16 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 Ark-UTM 16 connects Internet using a public IP address, please configure settings in [Remote Control].



DDNS

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

Enabled: off

Provider: No-IP (www.no-ip.com)

Hostname/Domain:

Username: demo

Password: ••••••

ACL

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

Enabled: on

WAN- Remote Control

DDNS

When the Ark-UTM 16 is using a dynamic public IP address, you could use a static domain name to access the Ark-UTM 16.

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 Ark-UTM 16 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 Ark-UTM 16 is using a private IP address to connect Internet, please set DDNS and port forwarding on the router at the WAN side of Ark-UTM 16.

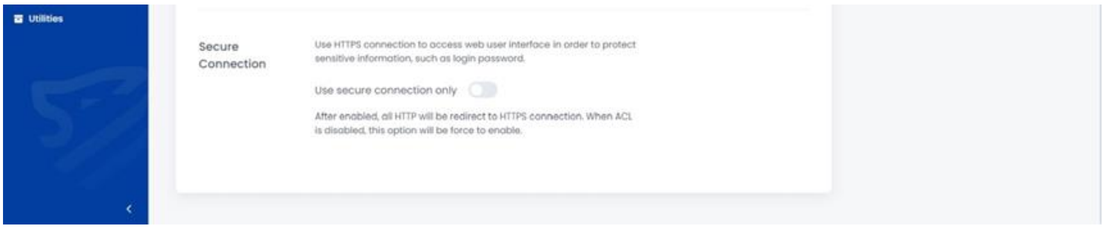
Access Control List (ACL)

To prevent Ark-UTM 16 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 Ark-UTM 16 connects Internet using a public IP address, the IP address that would be used to access Ark-UTM 16 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 Ark-UTM 16 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 Ark-UTM 16.

* Remark:

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



Secure Connection

Use HTTPS connection to access web user interface in order to protect sensitive information, such as login password.

Use secure connection only ○

After enabled, all HTTP will be redirect to HTTPS connection. When ACL is disabled, this option will be force to enable.

WAN- Secure Connection

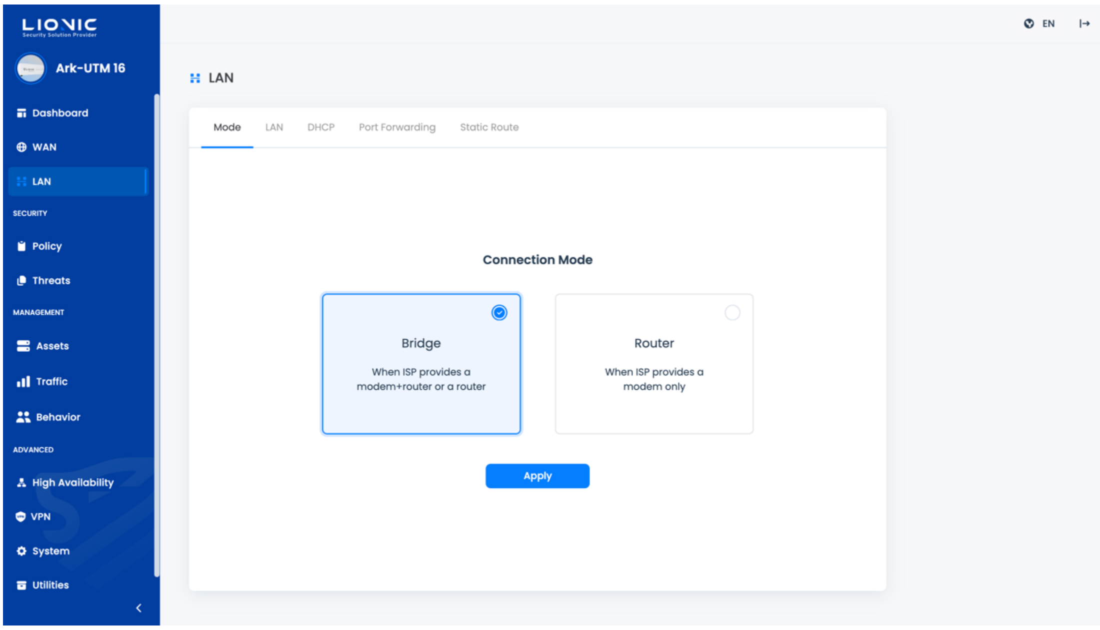
Secure Connection

After [Secure Connection] is enabled, all HTTP connections accessing the web GUI of Ark-UTM 16 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

Ark-UTM 16 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

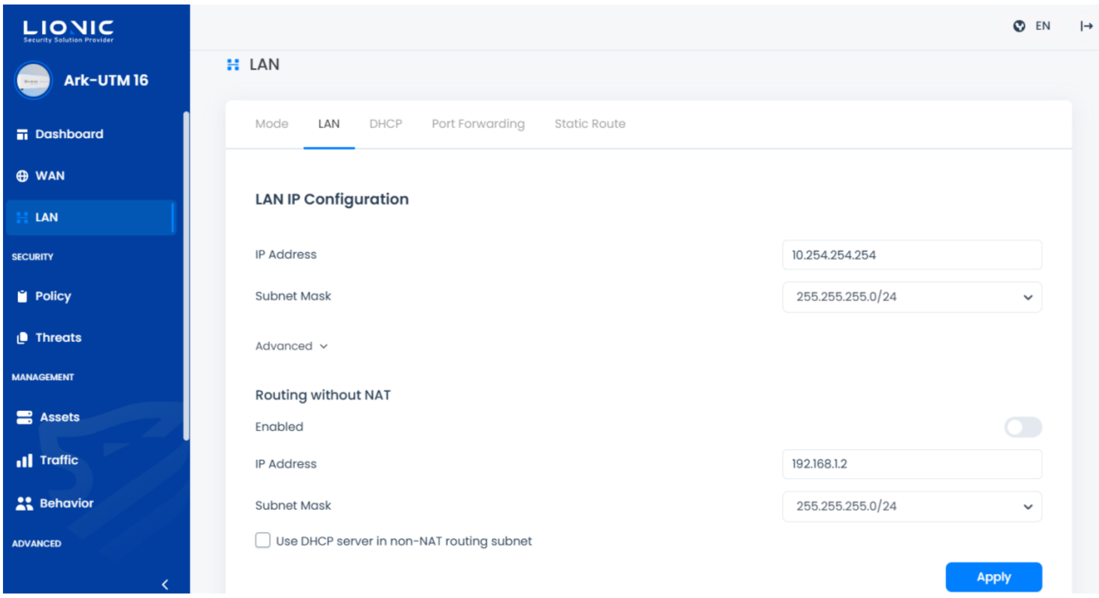
LAN-Connection Mode

- **Bridge mode (default):**
  DHCP is disable to LAN devices in [Bridge] mode. Please connect Ark-UTM 16 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 Ark-UTM 16 and its LAN devices.

After you selected the suitable connection mode and clicked [Apply], Ark-UTM 16 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 IP Configuration

IP Address 10.254.254.254

Subnet Mask 255.255.255.0/24

Routing without NAT

Enabled

IP Address 192.168.1.2

Subnet Mask 255.255.255.0/24

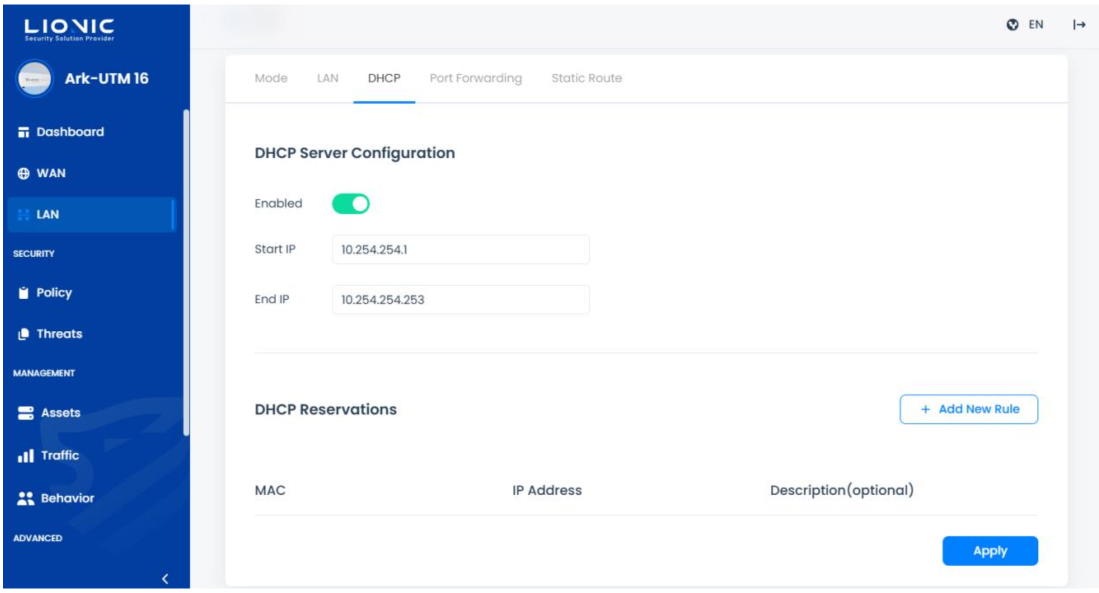
□ Use DHCP server in non-NAT routing subnet

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, Ark-UTM 16 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 Ark-UTM 16, you can use DHCP to assign private IP addresses to LAN devices.



DHCP Server Configuration

Enabled: on

Start IP: 10.254.254.1

End IP: 10.254.254.253

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

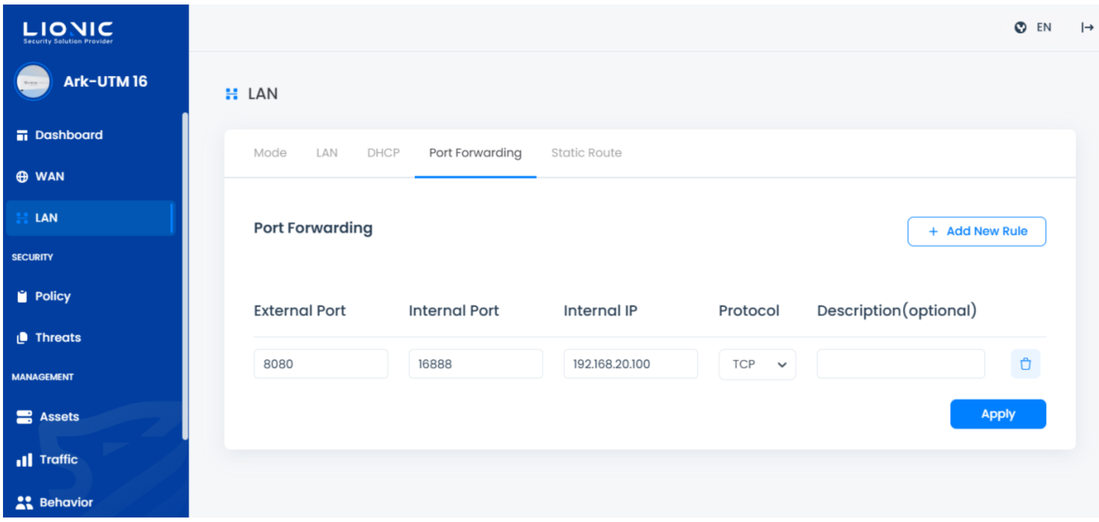
DHCP Reservations

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, Ark-UTM 16 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.



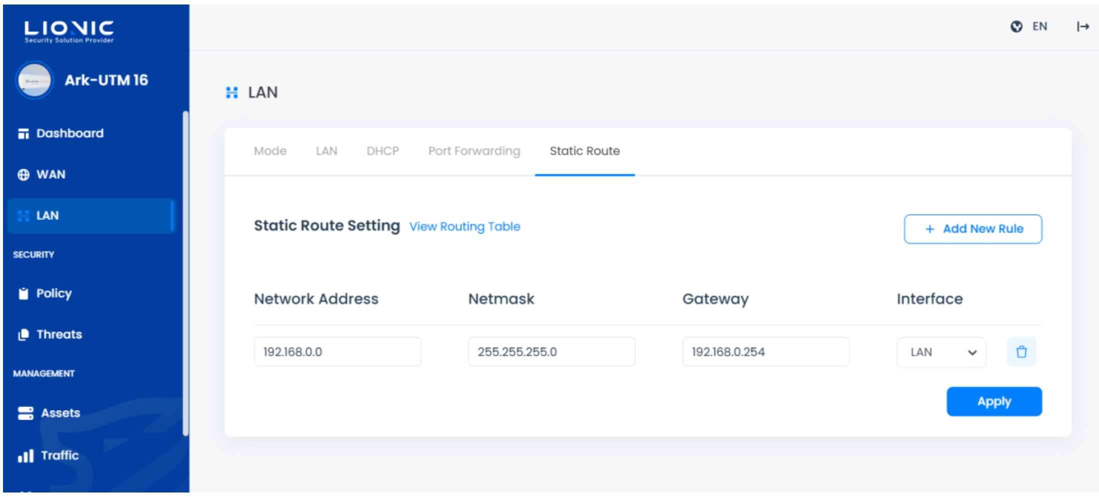
Port Forwarding

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 Ark-UTM 16 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	255.255.255.0	192.168.0.254	LAN

LAN-Static Route

Policy

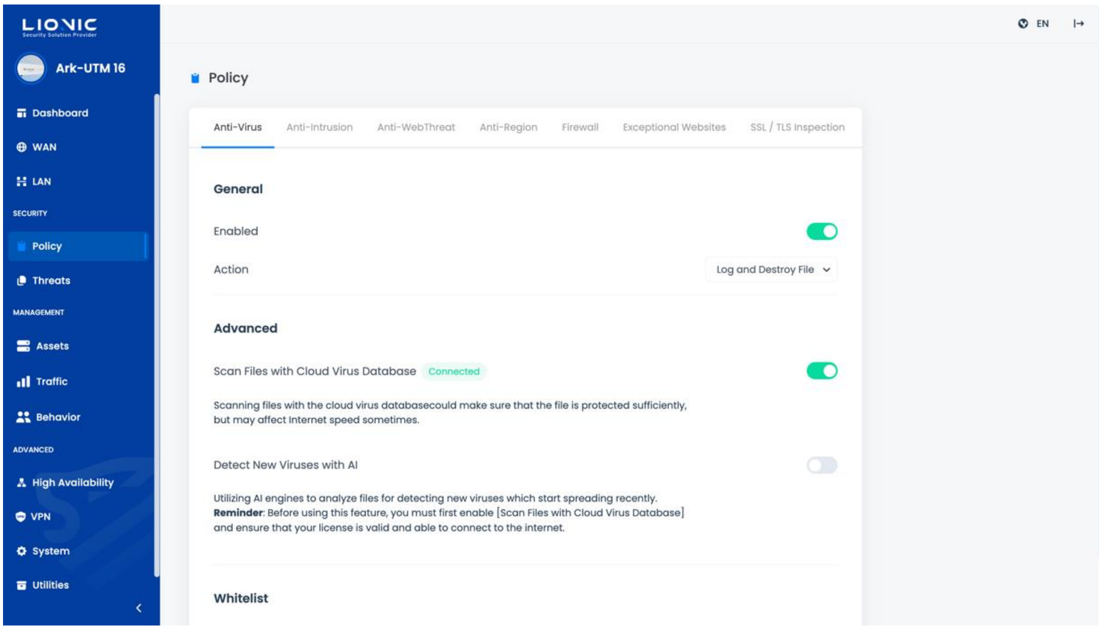
Anti-Virus, Anti-Intrusion, Anti-WebTheat

Ark-UTM 16 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 - Detect New Viruses with AI	- Block Brute-force attacks - Block Protocol Anomaly, - Block Port Scan and DoS Attacks, - Keep PCAP when a threat is detected	- Configure External Database for Malicious Webpages - External Database
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.

Detect New Viruses with AI ○

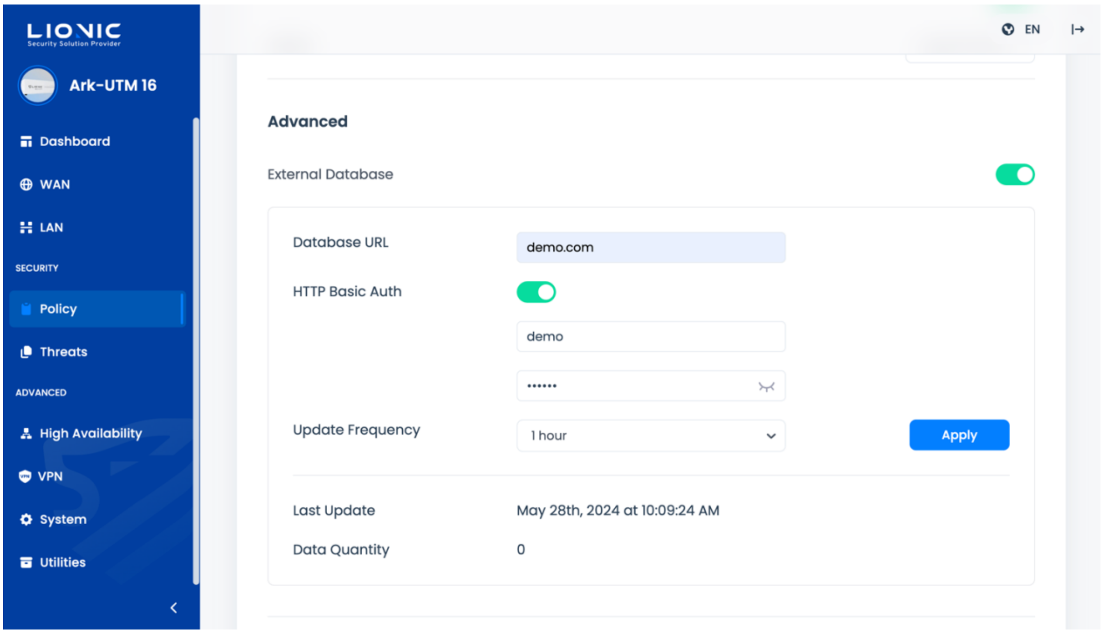
Utilizing AI engines to analyze files for detecting new viruses which start spreading recently.
Reminder: Before using this feature, you must first enable [Scan Files with Cloud Virus Database] and ensure that your license is valid and able to connect to the internet.

Whitelist

Policy

- **Enabled:** Enable or disable each security feature separately. The default setting is ENABLE.
- **Action:** The action that Ark-UTM 16 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, Ark-UTM 16 features the scan with LIONIC cloud virus database. To obtain the full protection of Anti-Virus, please make sure your Ark-UTM 16 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, Ark-UTM 16 can detect frequent login failures in a short period. Once the occurrence frequency is higher than the threshold, Ark-UTM 16 will record or block the attempting attack based on the frequency.
- **Block Protocol Anomaly:** After enabling this feature, Ark-UTM 16 '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, Ark-UTM 16 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 Ark-UTM 16 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.



Advanced

External Database

Database URL: demo.com

HTTP Basic Auth

demo

••••••

Update Frequency: 1 hour

Last Update: May 28th, 2024 at 10:09:24 AM

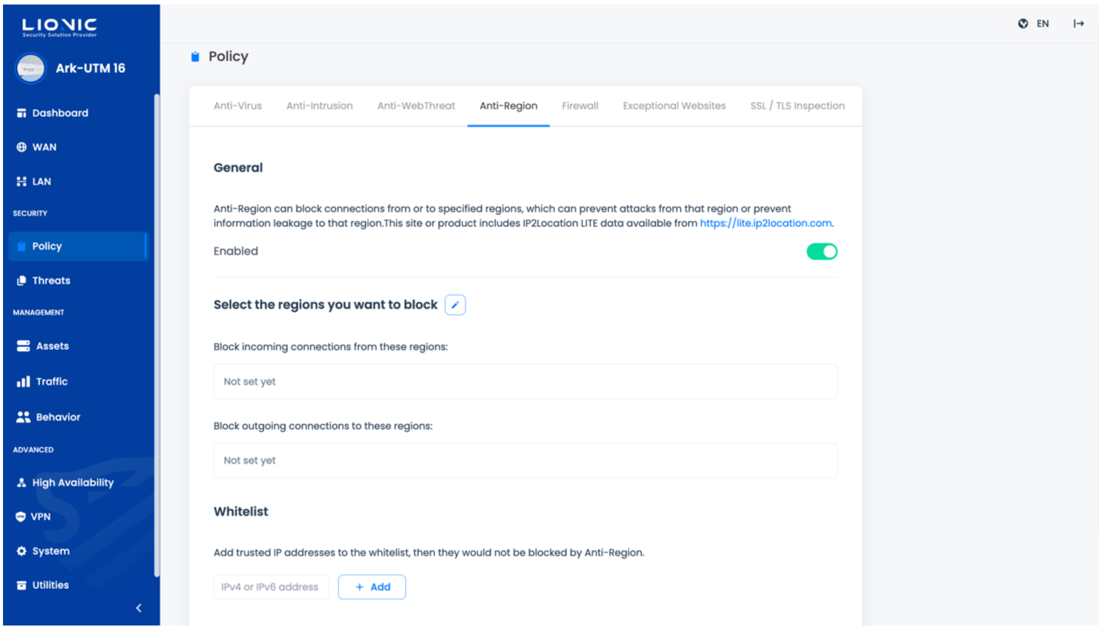
Data Quantity: 0

Policy-Advanced

- **Whitelist:** To correct a trusted file or connection destroyed/blocked by Ark-UTM 16 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

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:

Not set yet

Block outgoing connections to these regions:

Not set yet

Whitelist

Add trusted IP addresses to the whitelist, then they would not be blocked by Anti-Region.

IPv4 or IPv6 address

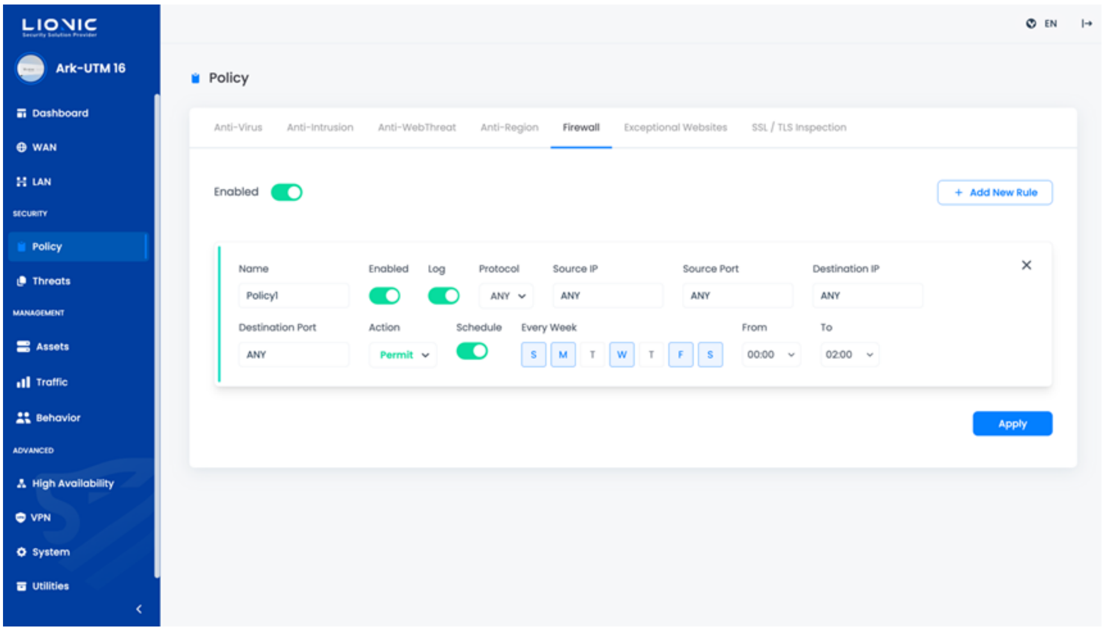
Policy- **Anti-Region**

- **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, Ark-UTM 16 also provide a basic firewall.



Enabled ●

Name	Enabled	Log	Protocol	Source IP	Source Port	Destination IP
Policy1	●	●	ANY	ANY	ANY	ANY

Destination Port	Action	Schedule	Every Week	From	To
ANY	Permit	●	S M T W T F S	00:00	02:00

Policy-Firewall

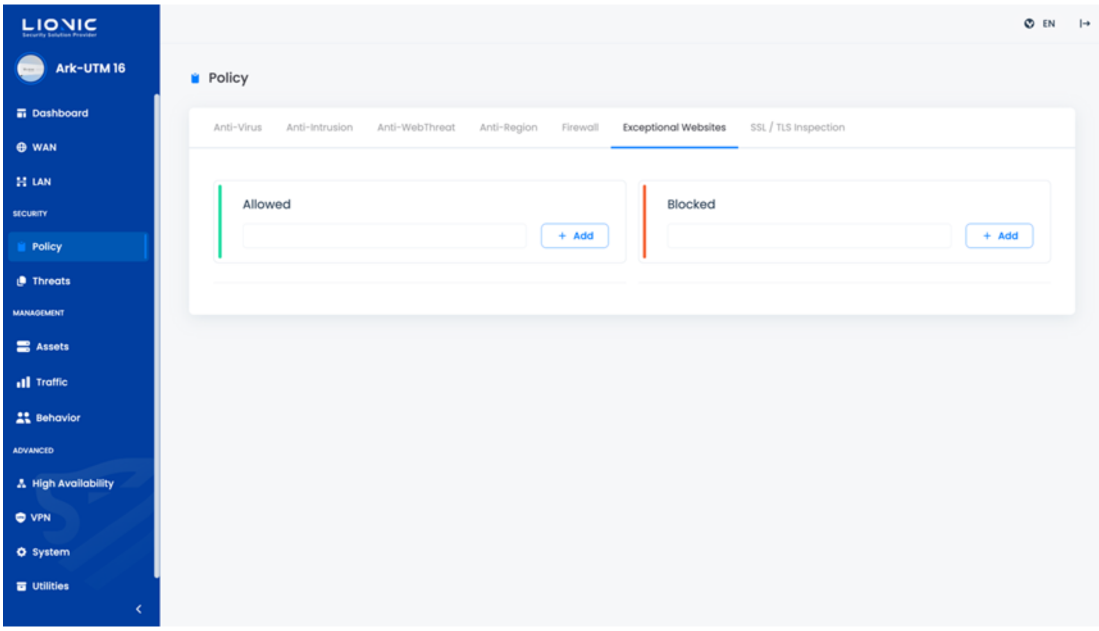
- **Step 1:** Enable the firewall (default is enabled).
- **Step 2:** Click [+Add New Rule].
- **Step 3:** Fill each configuration.
- **Step 4:** Click [Apply] to take effect.

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.



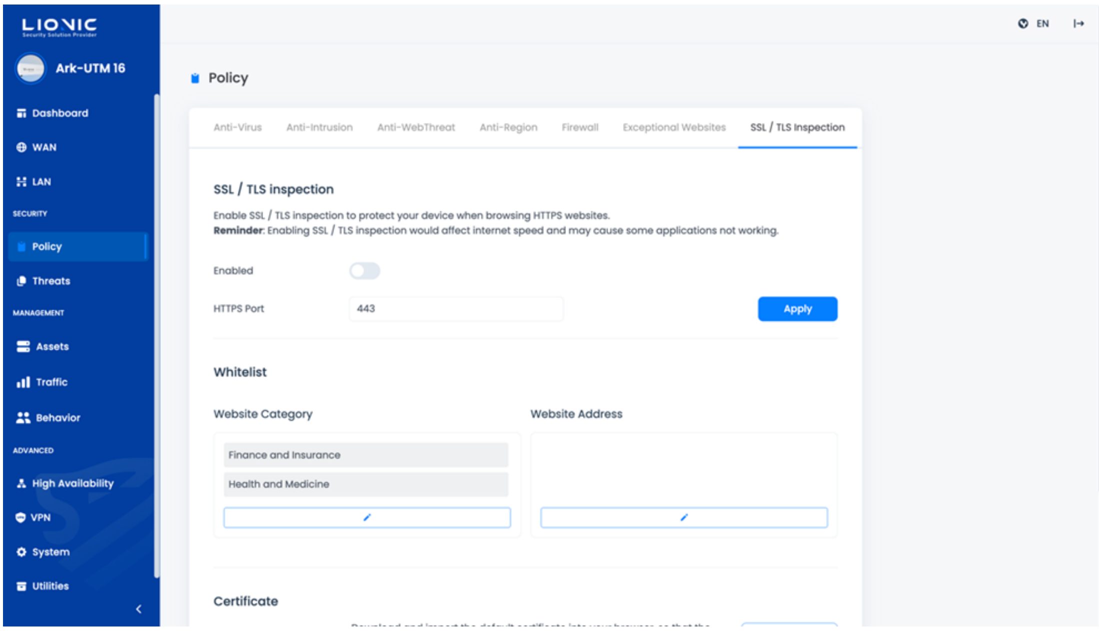
Policy-Exceptional Websites

- **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, Ark-UTM 16 will inspect packets encrypted with SSL or TLS, in order to protect your device when browsing HTTPS websites.



SSL / TLS inspection

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

Enabled

HTTPS Port: 443

Whitelist

Website Category: Finance and Insurance, Health and Medicine

Website Address

Certificate

Download and import the default certificate into your browser so that the

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:

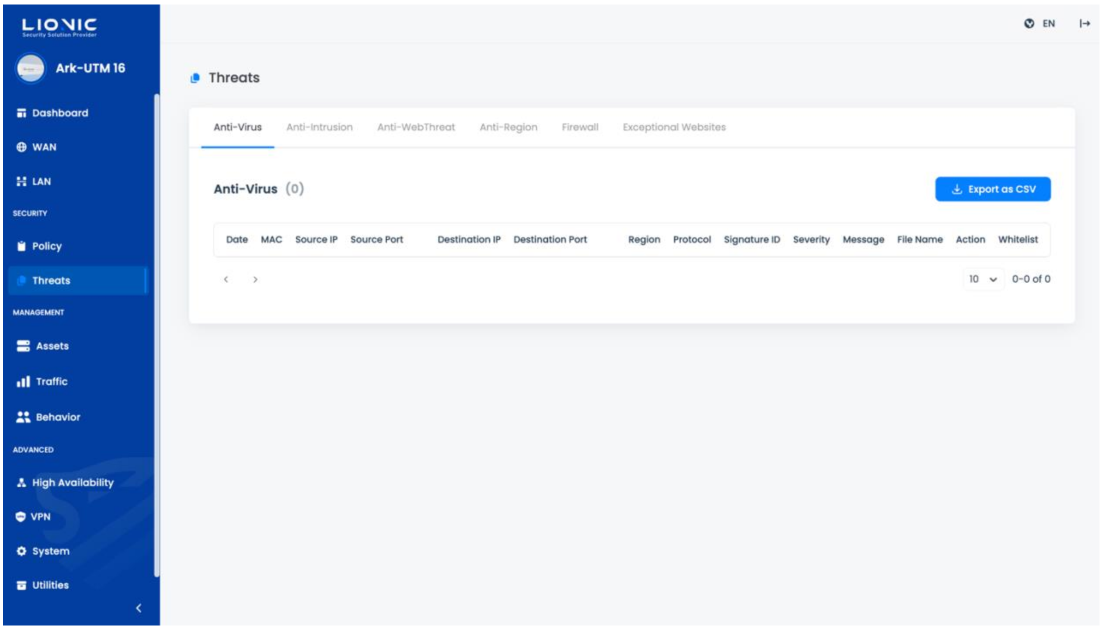
1. Enabling [SSL / TLS Inspection] would affect internet speed and may cause some applications not working.
2. When setting the HTTPS port, please avoid common ports used by other network services, such as Port 20, 21 for FTP, Port 25 for SMTP, etc., in order to prevent port conflict issues.

- **Whitelist:** After a website is added into the whitelist, Ark-UTM 16 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: Ark-UTM 16 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: Ark-UTM 16 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 Ark-UTM 16 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 Ark-UTM 16, the detailed threat information would be shown on the corresponding tab of each security feature in [Threats] page.



Anti-Virus (0)

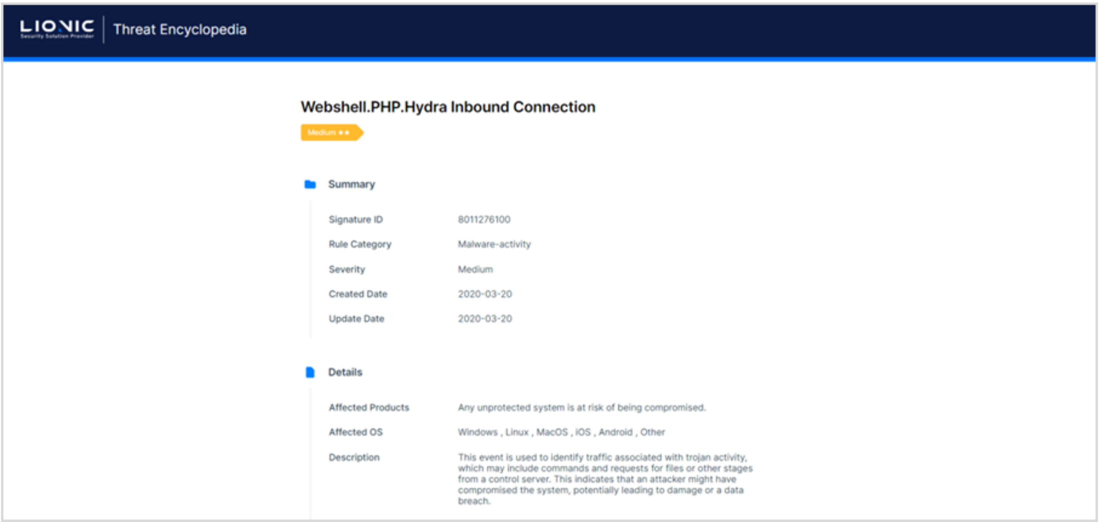
Date	MAC	Source IP	Source Port	Destination IP	Destination Port	Region	Protocol	Signature ID	Severity	Message	File Name	Action	Whitelist

Threats

- **Export as CSV:** Export and download the log in a CSV file.
- **Whitelist:** If Ark-UTM 16 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

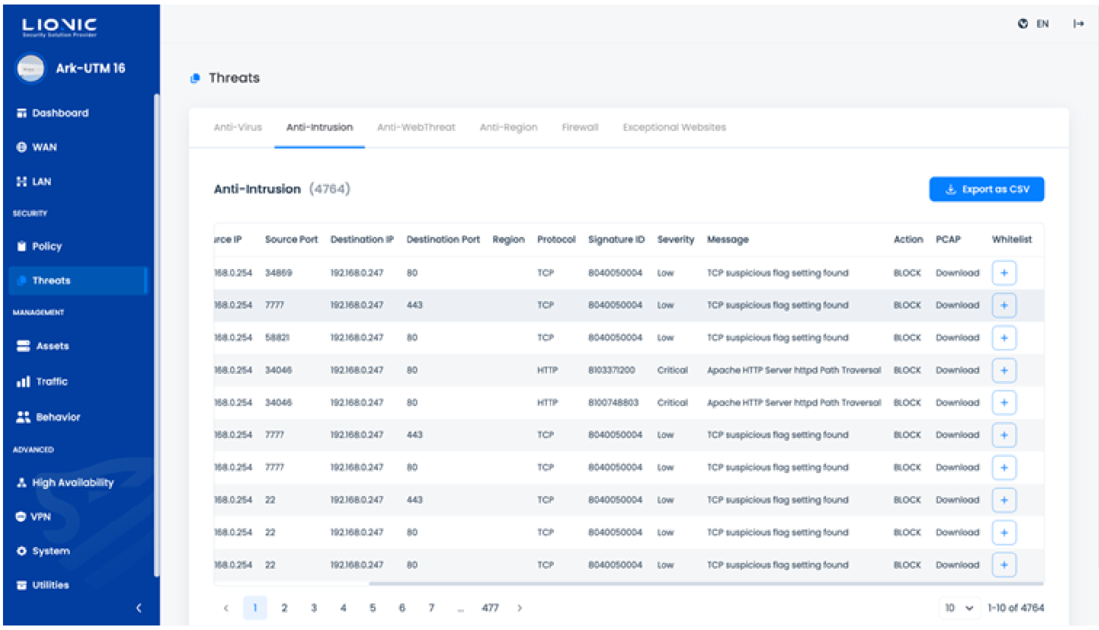
Details

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-Threats Encyclopedia

PCAP Packet Download:

When events of compromise or blockage occur on Ark-UTM 16, clicking [PCAP] > [Download] allows for packet download for further analysis.



Anti-Intrusion (4764)

rce IP	Source Port	Destination IP	Destination Port	Region	Protocol	Signature ID	Severity	Message	Action	PCAP	Whitelist
168.0.254	34869	192.168.0.247	80		TCP	8040050004	Low	TCP suspicious flag setting found	BLOCK	Download	+
168.0.254	7777	192.168.0.247	443		TCP	8040050004	Low	TCP suspicious flag setting found	BLOCK	Download	+
168.0.254	58821	192.168.0.247	80		TCP	8040050004	Low	TCP suspicious flag setting found	BLOCK	Download	+
168.0.254	34046	192.168.0.247	80		HTTP	8103371200	Critical	Apache HTTP Server httpd Path Traversal	BLOCK	Download	+
168.0.254	34046	192.168.0.247	80		HTTP	8100748803	Critical	Apache HTTP Server httpd Path Traversal	BLOCK	Download	+
168.0.254	7777	192.168.0.247	443		TCP	8040050004	Low	TCP suspicious flag setting found	BLOCK	Download	+
168.0.254	7777	192.168.0.247	80		TCP	8040050004	Low	TCP suspicious flag setting found	BLOCK	Download	+
168.0.254	22	192.168.0.247	443		TCP	8040050004	Low	TCP suspicious flag setting found	BLOCK	Download	+
168.0.254	22	192.168.0.247	80		TCP	8040050004	Low	TCP suspicious flag setting found	BLOCK	Download	+
168.0.254	22	192.168.0.247	80		TCP	8040050004	Low	TCP suspicious flag setting found	BLOCK	Download	+

‹ 1 2 3 4 5 6 7 … 477 ›   10 ⌄   1-10 of 4764

Threats-PCAP Download

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

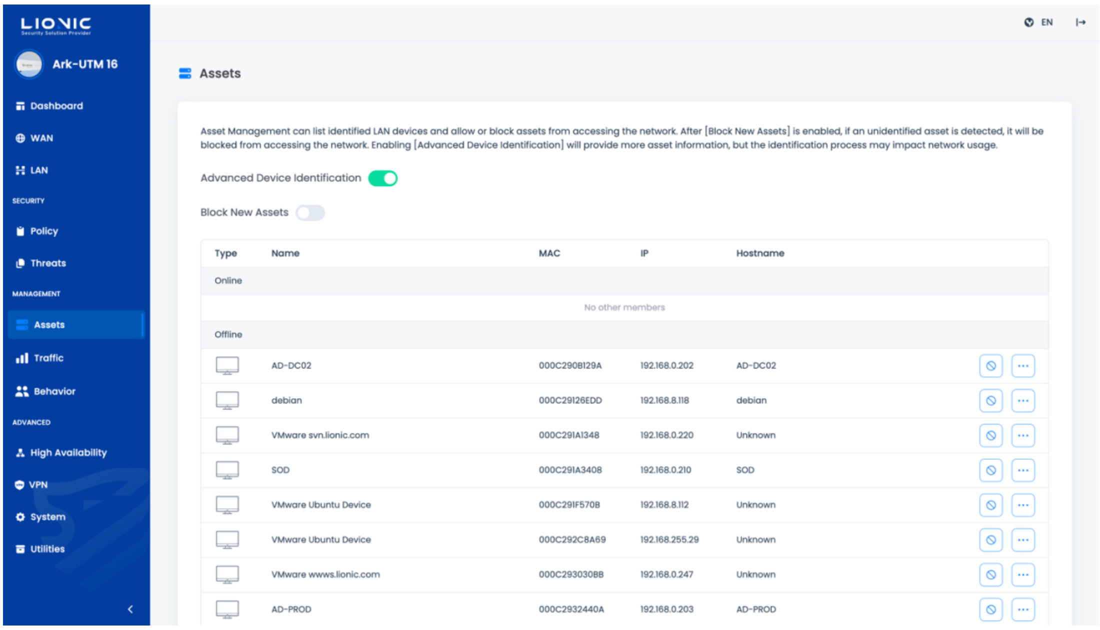
Assets

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
Online				
	No other members			
Offline				
	AD-DC02	000C290B129A	192.168.0.202	AD-DC02
	debian	000C29126EDD	192.168.8.118	debian
	VMware svn.lionic.com	000C291A1348	192.168.0.220	Unknown
	SOD	000C291A3408	192.168.0.210	SOD
	VMware Ubuntu Device	000C291F570B	192.168.8.112	Unknown
	VMware Ubuntu Device	000C292C8A69	192.168.255.29	Unknown
	VMware wwws.lionic.com	000C293030BB	192.168.0.247	Unknown
	AD-PROD	000C2932440A	192.168.0.203	AD-PROD

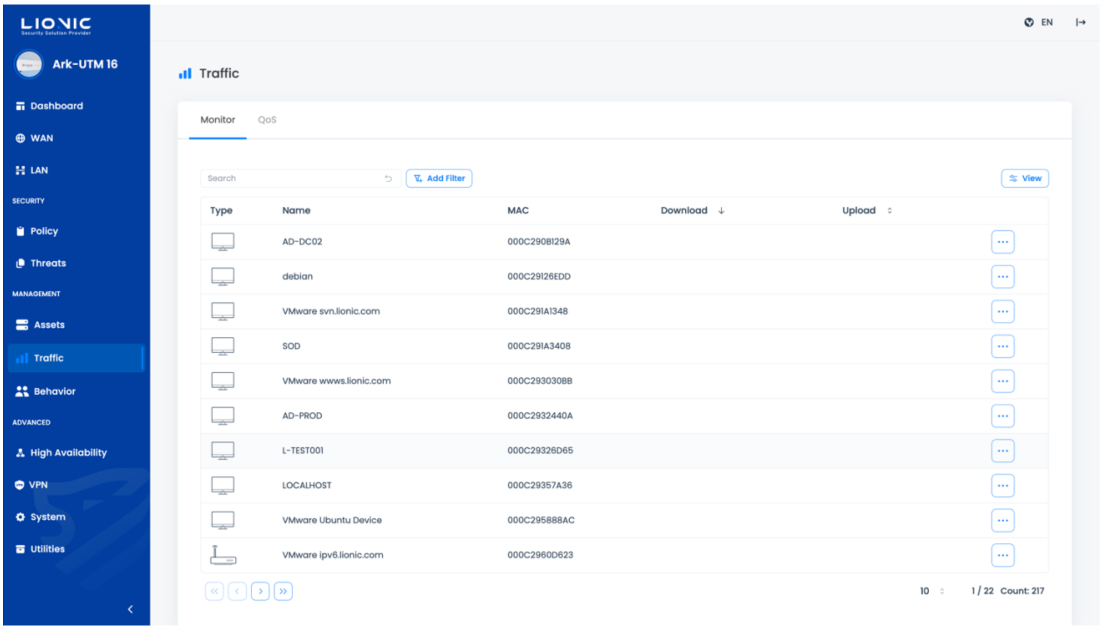
Assets

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.



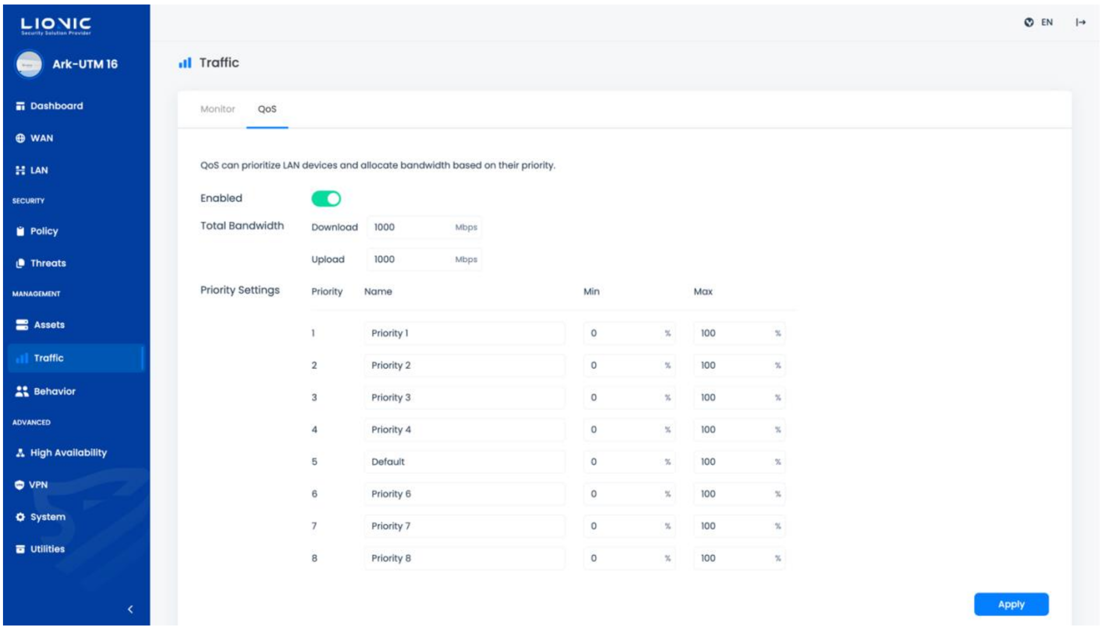
Type	Name	MAC	Download ↓	Upload ⇕	
🖥	AD-DC02	000C290B129A			···
🖥	debian	000C29126EDD			···
🖥	VMware svn.lionic.com	000C291A1348			···
🖥	SOD	000C291A3408			···
🖥	VMware wwws.lionic.com	000C293030BB			···
🖥	AD-PROD	000C2932440A			···
🖥	L-TEST001	000C29326D65			···
🖥	LOCALHOST	000C29357A36			···
🖥	VMware Ubuntu Device	000C295888AC			···
📶	VMware ipv6.lionic.com	000C2960D623			···

« ‹ › » 10 ⇕ 1 / 22 Count: 217

Traffic-Monitor

QoS

Ark-UTM 16 can perform bandwidth management for specific source IPs, destination IPs, or destination ports, allowing their traffic to receive higher priority service.



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

Enabled: ●

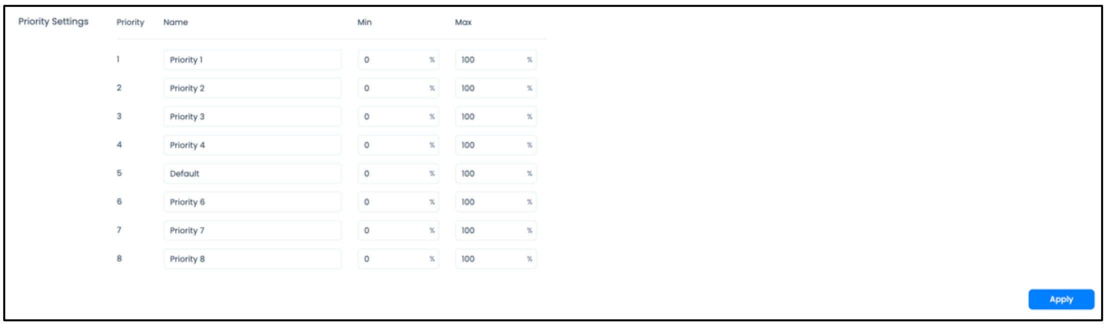
Total Bandwidth: Download 1000 Mbps; Upload 1000 Mbps

Priority 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 %

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.

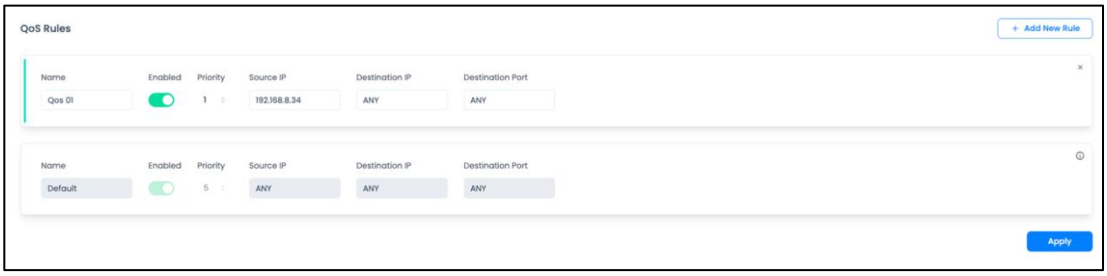


Priority Settings

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 %

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.



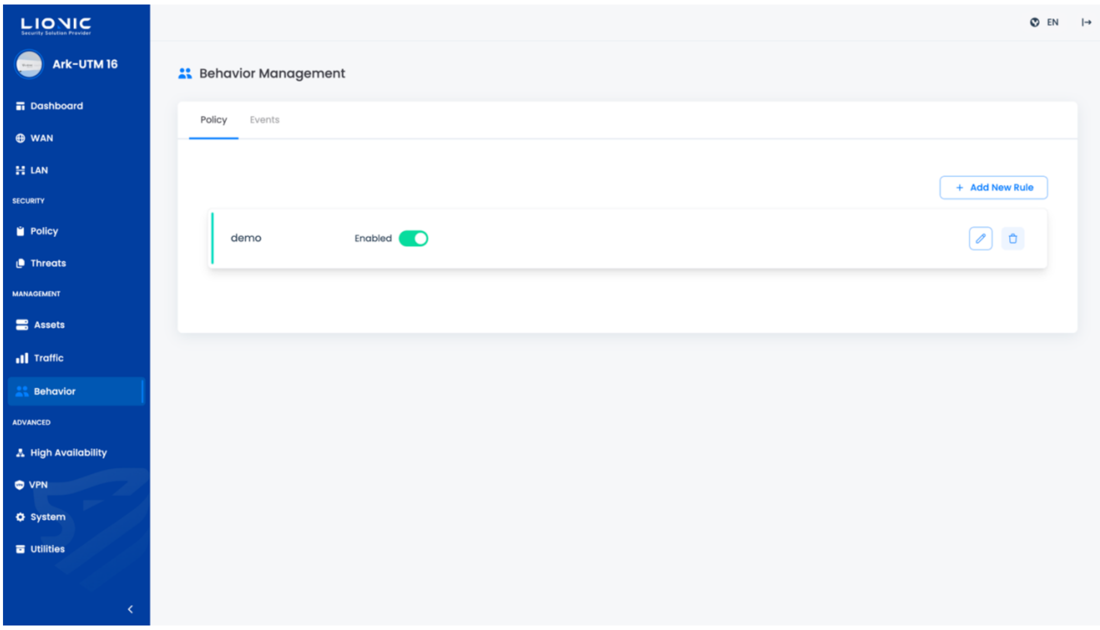
QoS Rules

Name	Enabled	Priority	Source IP	Destination IP	Destination Port
Qos 01	●	1	192.168.8.34	ANY	ANY
Default	●	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.

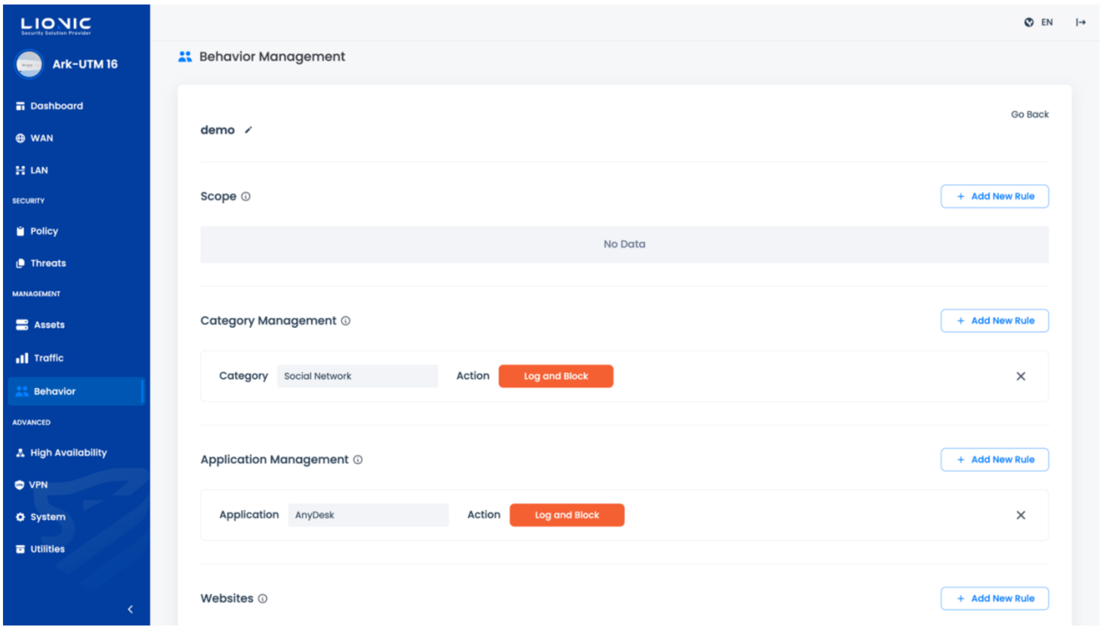


demo Enabled

Behavior Management

Policy

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



demo

Scope

Category Management

Category: Social Network · Action: Log and Block

Application Management

Application: AnyDesk · Action: Log and Block

Websites

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:

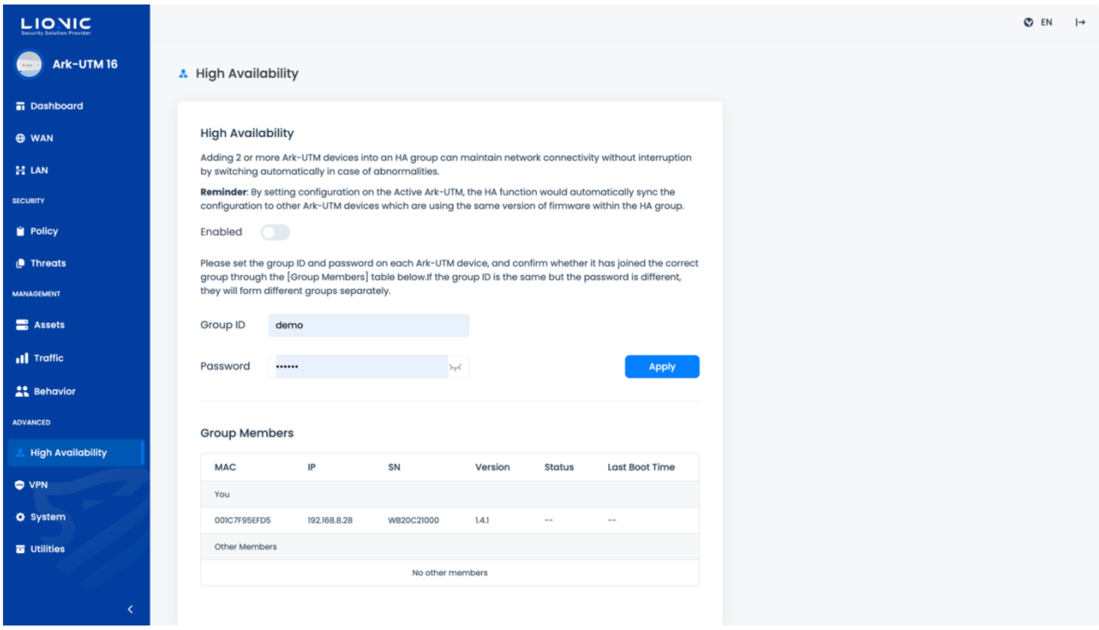
- **Scope:** Manage the rule scope by IP addresses or MAC addresses. This is a required field.
- **Category Management:** Manage the corresponding action based on the category of the web content.
- **Application Management:** Manage the corresponding action based on the application associated with the 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.

High Availability (HA)

Adding 2 or more Ark-UTM 16 into an HA group can maintain network connectivity without interruption by switching automatically in case of abnormalities.



High Availability

High Availability

Adding 2 or more Ark-UTM devices into an HA group can maintain network connectivity without interruption by switching automatically in case of abnormalities.

Reminder: By setting configuration on the Active Ark-UTM, the HA function would automatically sync the configuration to other Ark-UTM devices which are using the same version of firmware within the HA group.

Enabled ○

Please set the group ID and password on each Ark-UTM device, and confirm whether it has joined the correct group through the [Group Members] table below.If the group ID is the same but the password is different, they will form different groups separately.

Group ID: demo

Password: ••••••

Apply

Group Members

MAC	IP	SN	Version	Status	Last Boot Time
You					
001C7F95EFD5	192.168.8.28	WB20C21000	1.4.1	--	--
Other Members					
No other members					

High Availability

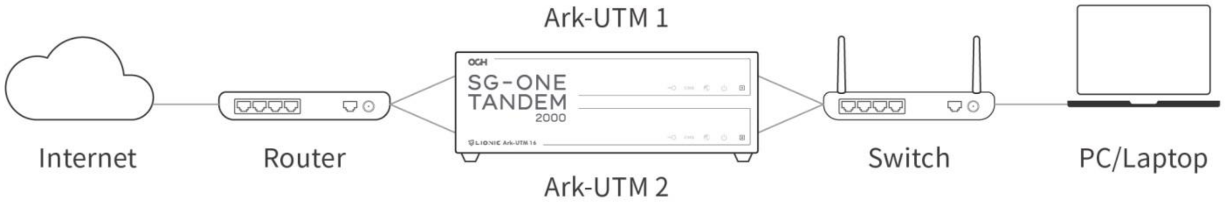
- **Enabled:** Enable or disable [High Availability]. The default setting is DISABLE.
- **Group ID:** A user-defined ID (1~255) for the HA group.
- **Password:** A user-defined password for the HA group.

Please set the group ID and password on each Ark-UTM 16, and confirm if it has joined the correct group by checking the [Group Members] table below. If both the group ID and the password are the same, other group members would be shown in the [Group Members] table; if the group ID is the same but the password is different, they will form different groups separately.

Configure High Availability:

- **Step 1:** Set up the network configuration for both Ark-UTM 16 in the 2-in-1 enclosure and make sure they are on the same subnet.
- **Step 2:** Connect the LAN port of Ark-UTM 16 (No.1) to your PC/Laptop with an Ethernet cable.
- **Step 3:** Visit https://myark.lionic.com/ with a web browser and access the web GUI.

- **Step 4:** After logged in, go to [High Availability] page.
- **Step 5:** Click [Enabled], set the group ID (1~255) and password (custom), then click [Apply].
- **Step 6:** After Ark-UTM 16 (No.1) is set, connect the LAN port of Ark-UTM 16 (No.2) to your PC/Laptop with an Ethernet cable, and repeat Step 3 and 4.
- **Step 7:** Click [Enabled], enter the group ID and password you set on Ark-UTM 16 (No.1), and then click [Apply].
- **Step 8:** After the HA of both Ark-UTM 16 are set, connect the LAN port of both Ark-UTM 16 to the same switch (as shown in the figure). The HA configuration is now completed.

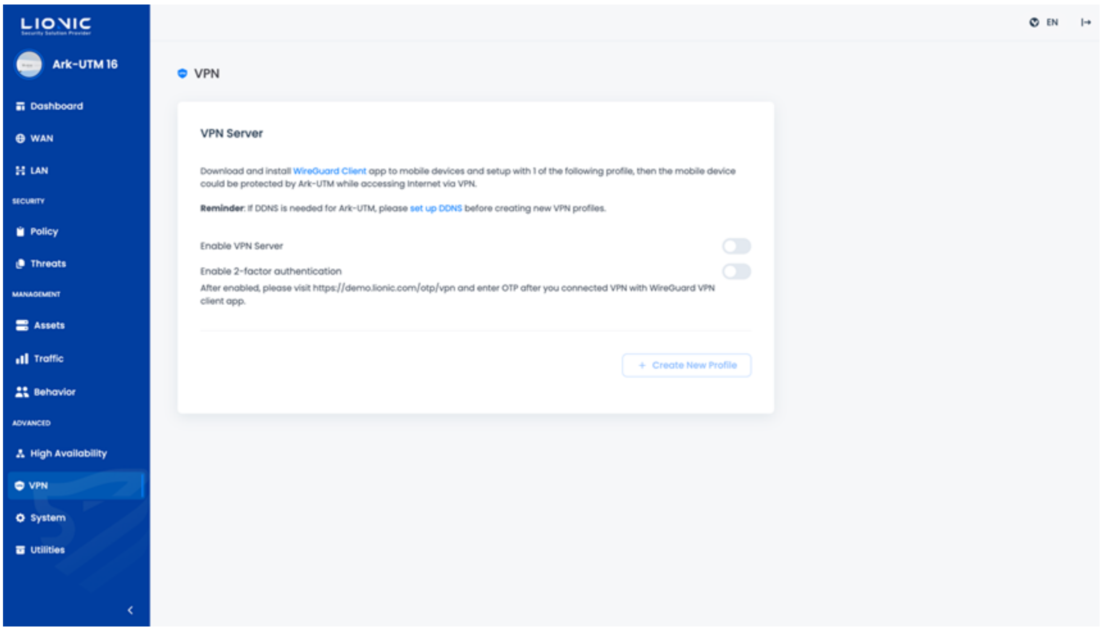


HA Topology

* Remind: By setting configuration on the Active Ark-UTM 16, the HA function would automatically sync the configuration to other Ark-UTM 16 which are using the same version of firmware within the HA group.

VPN Server

Enable the VPN server to expand the protecting range of Ark-UTM 16 to devices using cellular network or public Wi-Fi. Mobile devices could be protected by Ark-UTM 16 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 Ark-UTM while accessing Internet via VPN.

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

Enable VPN Server

Enable 2-factor authentication

After enabled, please visit https://demo.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 Ark-UTM 16.

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 Ark-UTM 16 via VPN with WireGuard Client app whenever the protection of Ark-UTM 16 is needed.

* Remark:

1. If you would like to set DDNS for Ark-UTM 16, please setup before enabling the VPN server.
2. If there is a router at the WAN side of Ark-UTM 16, please set port forwarding on the router, so that the connection could be redirected to Port 51820 of Ark-UTM 16. 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 Ark-UTM 16.
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.

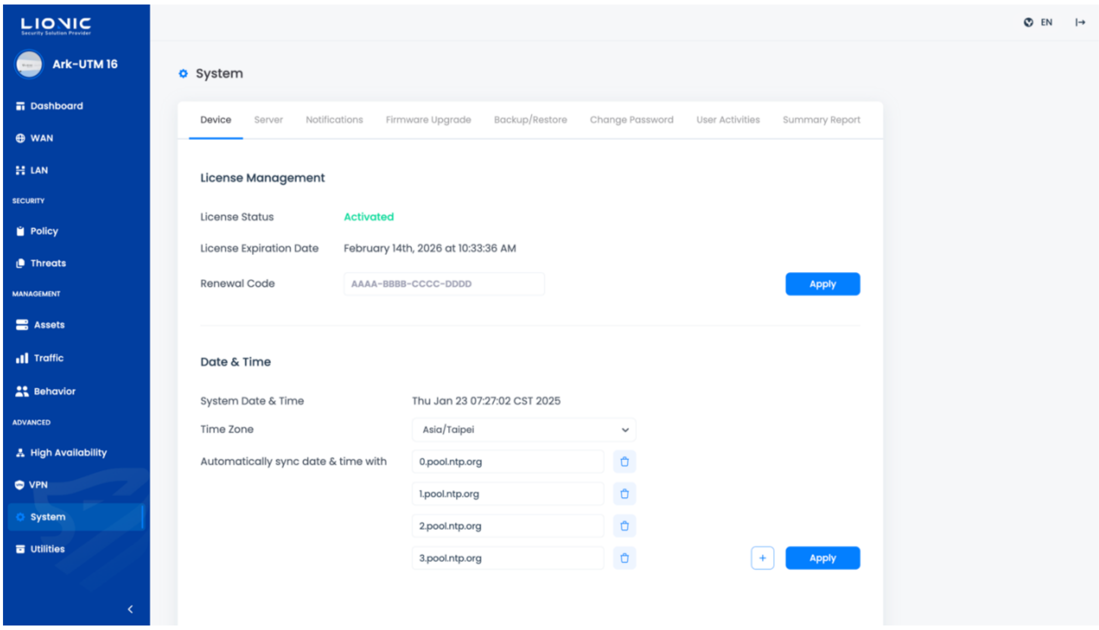
Start Accessing Internet via VPN:

- **Step 1:** Connect Ark-UTM 16 via VPN with WireGuard Client app.
- **Step 2:** Obtain the OTP from the OTP app.
- **Step 3:** Visit https://myark.lionic.com/otp/vpn and enter the OTP.

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

System

Device



License Management

License Status Activated

License Expiration Date February 14th, 2026 at 10:33:36 AM

Renewal Code AAAA-BBBB-CCCC-DDDD

Date & Time

System Date & Time Thu Jan 23 07:27:02 CST 2025

Time Zone Asia/Taipei

Automatically sync date & time with 0.pool.ntp.org
1.pool.ntp.org
2.pool.ntp.org
3.pool.ntp.org

System-Device

License Management

View the license status, activate or renew the license for Ark-UTM 16.

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:** Ark-UTM 16 will remind you in 30 days before the license is expired. Please purchase the renewal code (Remark 2), enter it into the input field and click [Apply] to extend the expiration date.

* Remark:

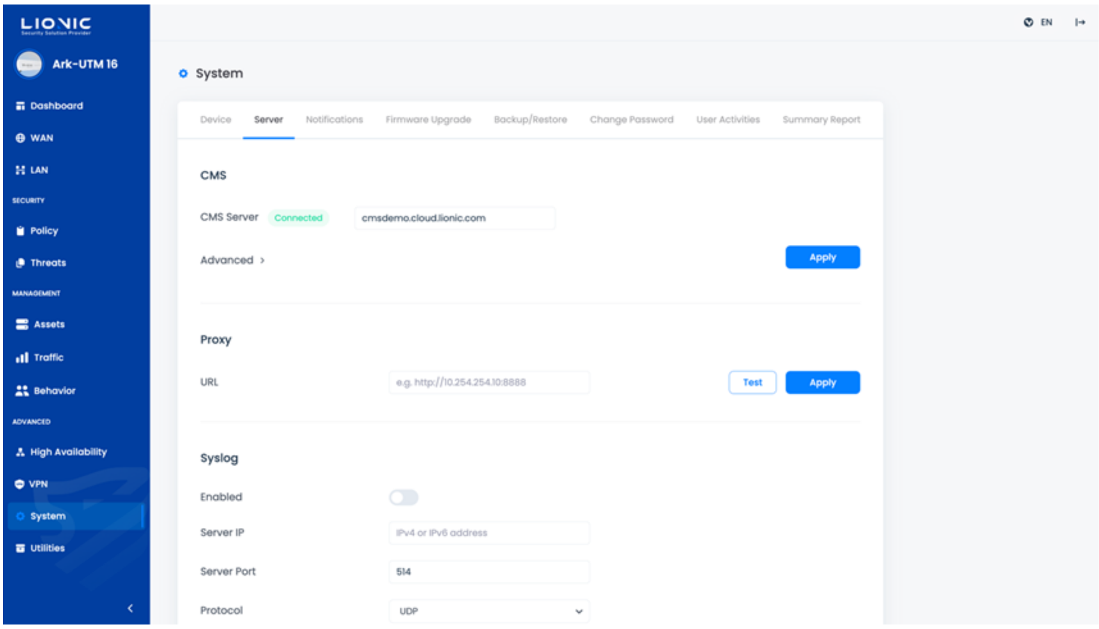
1. The activation code consists of 20 English letters and numbers. It can activate the license after applied successfully. If you do not receive the activation code when you purchase Ark-UTM 16 or the activation code is not working, please contact local sales representatives in your region.
2. The renewal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

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

Server



CMS

CMS Server Connected cmsdemo.cloud.lionic.com

Proxy

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

Syslog

Enabled

Server IP IPv4 or IPv6 address

Server Port 514

Protocol UDP

System-Server

CMS

Central Management System (CMS) can monitor and control multiple Ark-UTM 16 in 1 portal. After the CMS is built, enter the address of CMS into the input field and click [Apply] to connect Ark-UTM 16 with the CMS. Please contact Ark-UTM 16 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, Ark-UTM 16, 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

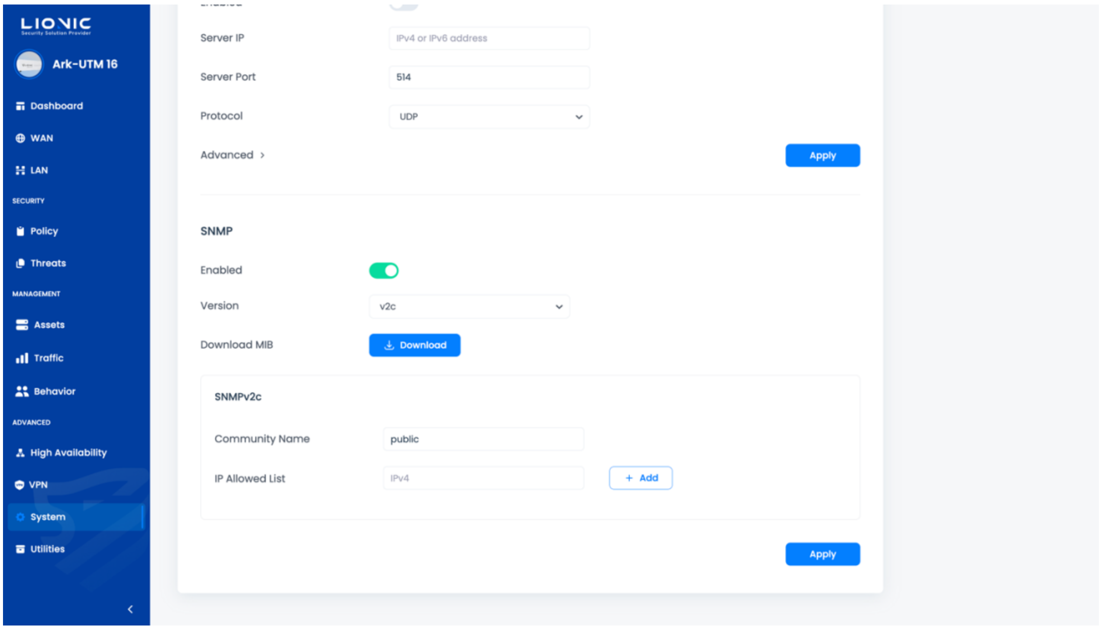
To obtain the full protection from Ark-UTM 16, the proxy server can help Ark-UTM 16 deployed in an intranet access LIONIC cloud services. After the proxy server is built, enter the server address into the input field and click [Apply] to access LIONIC cloud services via the proxy server. Please contact your IT administrator for more information.

Syslog

A syslog server can collect operating history of Ark-UTM 16. 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 Ark-UTM 16. If you have set up your own SNMP server (v2c, v3 versions),enter the configuration into the input field and click [Apply].



Server IP: IPv4 or IPv6 address

Server Port: 514

Protocol: UDP

SNMP

Enabled

Version: v2c

SNMPv2c

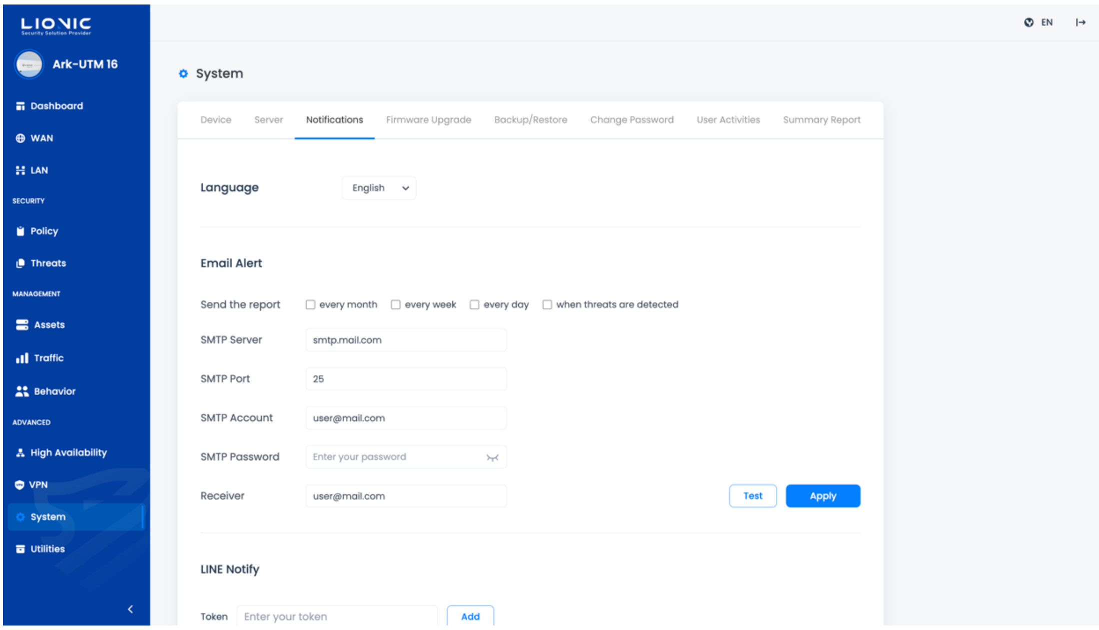
Community Name: public

IP Allowed List: IPv4

System-Server

Notifications

When a threat is detected, Ark-UTM 16 can notify the details to the mail address or LINE account you set in [Notifications] tab. Furthermore, Ark-UTM 16 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.



Language English

Email Alert

Send the report □ every month □ 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

Token Enter your token

System-Notifications

Language

Select the language you prefer for mails, LINE messages or reports.

Email Alert

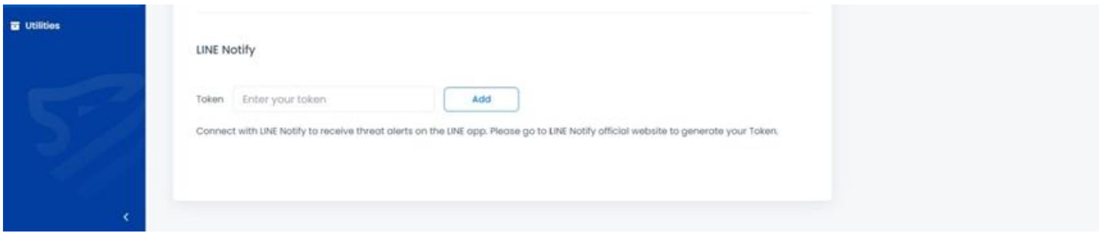
- **Send the report:**
  - Every month: Send the monthly report on the 1st day of each month at 00:00.
  - Every week: Send the weekly report every Sunday at 00:00.
  - Every day: Send daily report at 00:00 every day.
  - When threats are detected: Threat information is sent immediately upon detection.
- **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 Ark-UTM 16 send a test email to confirm the settings.

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

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.

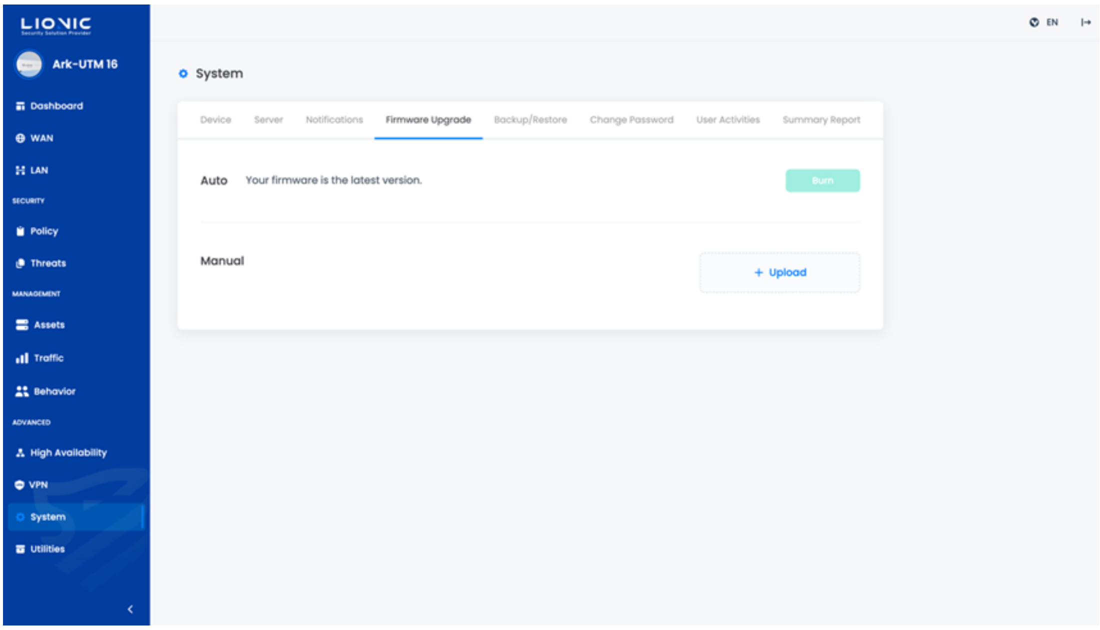


Connect with LINE Notify to receive threat alerts on the LINE app. Please go to LINE Notify official website to generate your Token.

Notify-Line Notify

Firmware Upgrade

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



Auto Your firmware is the latest version.

Manual

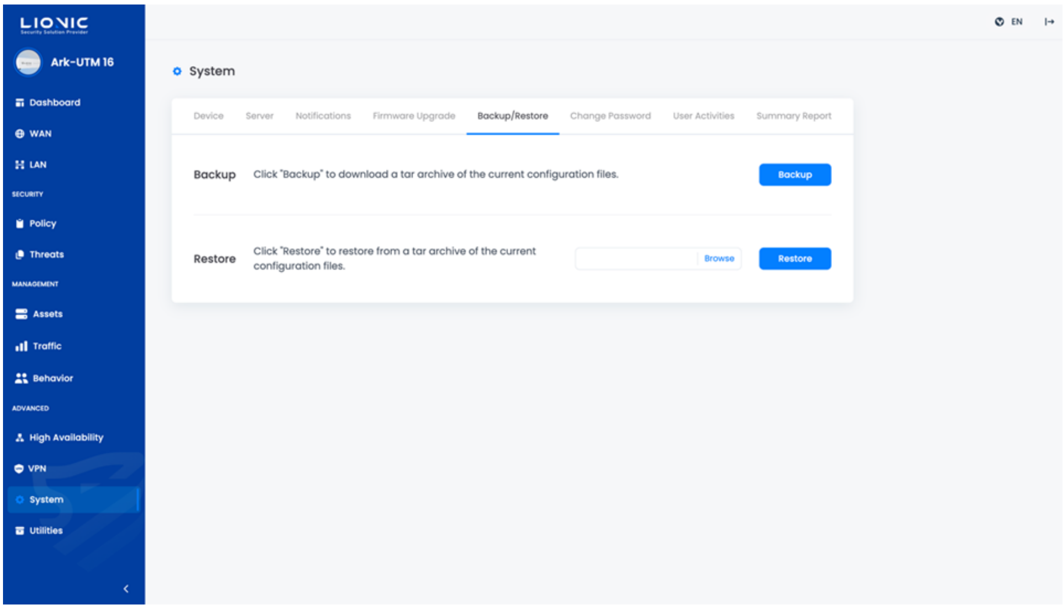
System-Firmware Upgrade

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

* Remark: Ark-UTM 16 would reboot during upgrading firmware. The network connection will resume after the reboot is completed.

Backup / Restore

[Backup / Restore] function can backup Ark-UTM 16 configurations, such as security policies and whitelist setting, and restore on the same or other Ark-UTM 16.



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

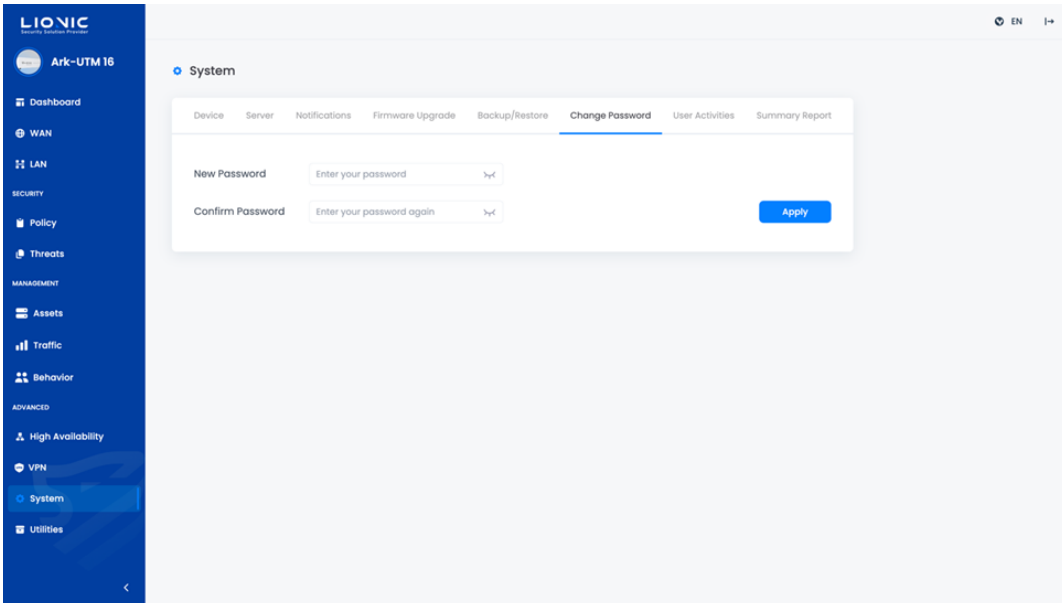
Restore Click "Restore" to restore from a tar archive of the current configuration files.

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]

.



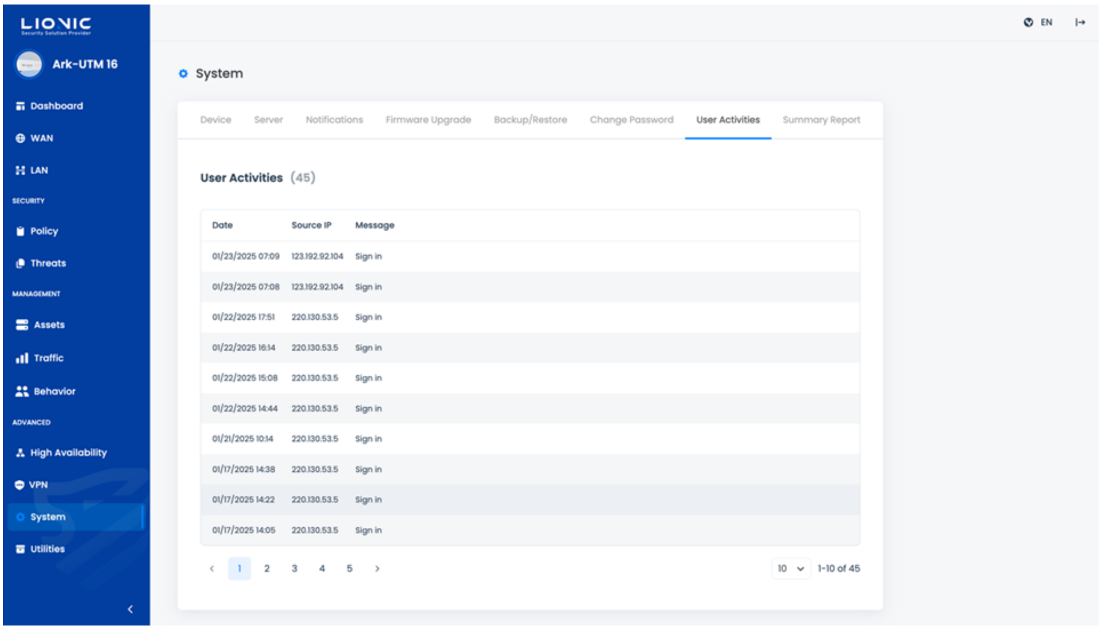
New Password: Enter your password

Confirm Password: Enter your password again

System-Change Password

User Activities

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



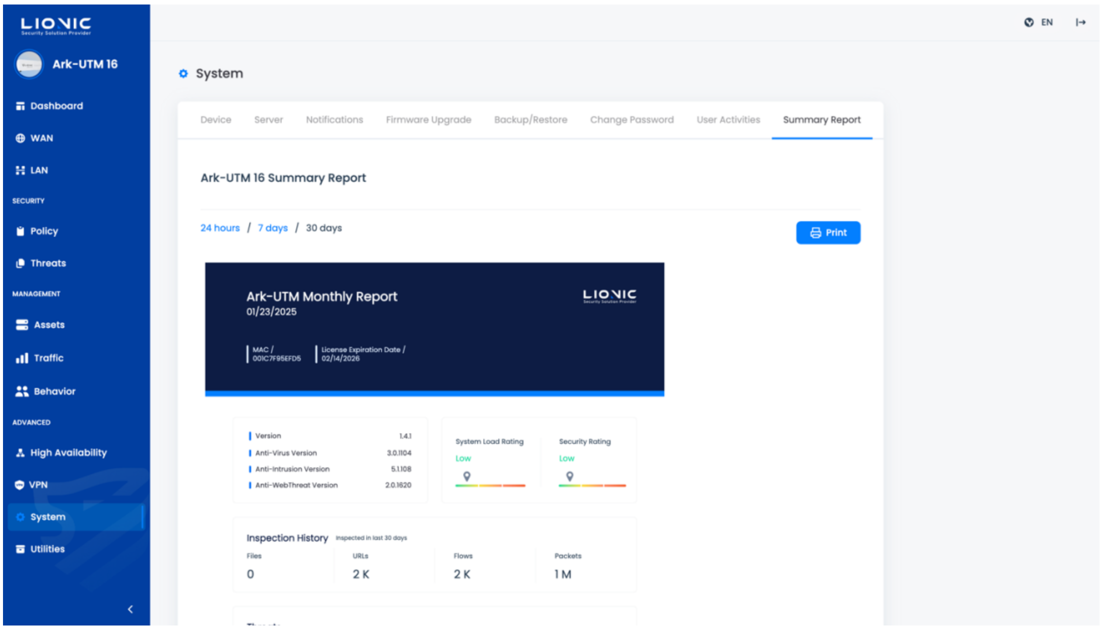
User Activities (45)

Date	Source IP	Message
01/23/2025 07:09	123.192.92.104	Sign in
01/23/2025 07:08	123.192.92.104	Sign in
01/22/2025 17:51	220.130.53.5	Sign in
01/22/2025 16:14	220.130.53.5	Sign in
01/22/2025 15:08	220.130.53.5	Sign in
01/22/2025 14:44	220.130.53.5	Sign in
01/21/2025 10:14	220.130.53.5	Sign in
01/17/2025 14:38	220.130.53.5	Sign in
01/17/2025 14:22	220.130.53.5	Sign in
01/17/2025 14:05	220.130.53.5	Sign in

System-User Activities

Summary Report

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



Ark-UTM 16 Summary Report

Ark-UTM Monthly Report
01/23/2025

MAC / 001C7F95EFD5
License Expiration Date / 02/14/2026

Version	1.4.1
Anti-Virus Version	3.0.1104
Anti-Intrusion Version	5.1.108
Anti-WebThreat Version	2.0.1620

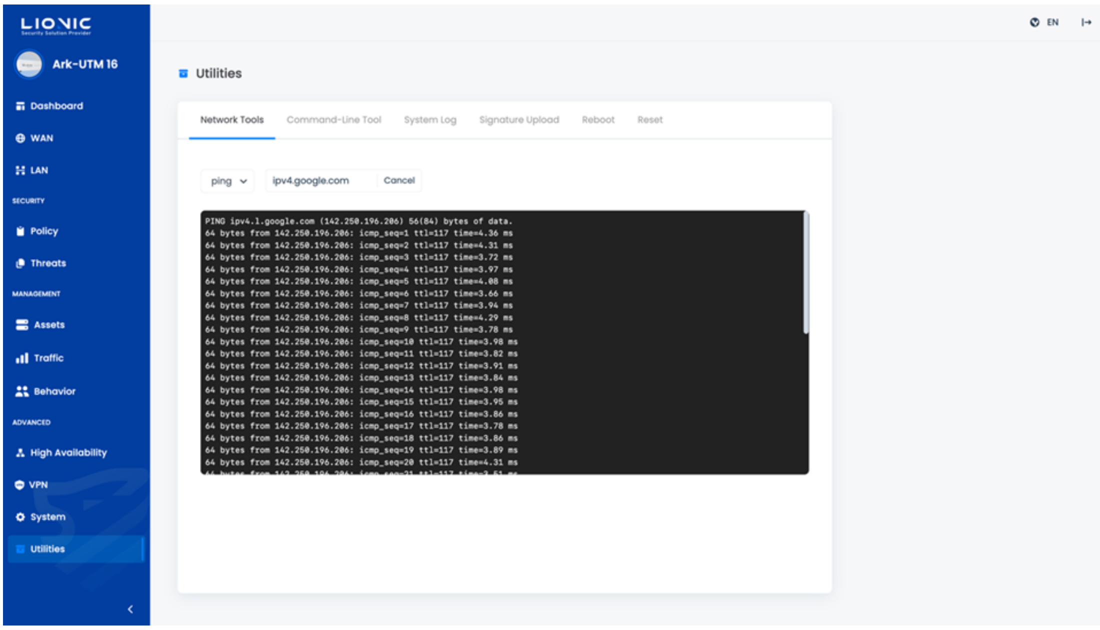
System Load Rating: Low
Security Rating: Low

Inspection History Inspected in last 30 days

Files	URLs	Flows	Packets
0	2 K	2 K	1 M

System-Summary Report

Utilities



ping ipv4.google.com

```
PING ipv4.1.google.com (142.250.196.206) 56(84) bytes of data.
64 bytes from 142.250.196.206: icmp_seq=1 ttl=117 time=4.36 ms
64 bytes from 142.250.196.206: icmp_seq=2 ttl=117 time=4.31 ms
64 bytes from 142.250.196.206: icmp_seq=3 ttl=117 time=3.72 ms
64 bytes from 142.250.196.206: icmp_seq=4 ttl=117 time=3.97 ms
64 bytes from 142.250.196.206: icmp_seq=5 ttl=117 time=4.08 ms
64 bytes from 142.250.196.206: icmp_seq=6 ttl=117 time=3.66 ms
64 bytes from 142.250.196.206: icmp_seq=7 ttl=117 time=3.94 ms
64 bytes from 142.250.196.206: icmp_seq=8 ttl=117 time=4.29 ms
64 bytes from 142.250.196.206: icmp_seq=9 ttl=117 time=3.78 ms
64 bytes from 142.250.196.206: icmp_seq=10 ttl=117 time=3.98 ms
64 bytes from 142.250.196.206: icmp_seq=11 ttl=117 time=3.82 ms
64 bytes from 142.250.196.206: icmp_seq=12 ttl=117 time=3.91 ms
64 bytes from 142.250.196.206: icmp_seq=13 ttl=117 time=3.84 ms
64 bytes from 142.250.196.206: icmp_seq=14 ttl=117 time=3.98 ms
64 bytes from 142.250.196.206: icmp_seq=15 ttl=117 time=3.95 ms
64 bytes from 142.250.196.206: icmp_seq=16 ttl=117 time=3.86 ms
64 bytes from 142.250.196.206: icmp_seq=17 ttl=117 time=3.78 ms
64 bytes from 142.250.196.206: icmp_seq=18 ttl=117 time=3.86 ms
64 bytes from 142.250.196.206: icmp_seq=19 ttl=117 time=3.89 ms
64 bytes from 142.250.196.206: icmp_seq=20 ttl=117 time=4.31 ms
64 bytes from 142.250.196.206: icmp_seq=21 ttl=117 time=3.51 ms
```

Utilities

Ark-UTM 16 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 Ark-UTM 16 immediately or setup a reboot schedule.
- **Reset:** Reset all configurations to the factory default settings.

* Remark: While the license is valid and Internet is connected, Ark-UTM 16 would automatically download and update the signature.

Dual Ark-UTM 16
Makes Security Simple

LIONIC
Security Solution Provider

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

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

1F-C6, No.1, Lising 1st Rd.,
Science-Based Industrial Park,
Hsinchu City 300, Taiwan, R.O.C.