LIONIC
Security Solution Provider

Web GUI User Manual

LionFilter 200

Version 1.0
Released on May 2025

Lionic Corp. www.lionic.com

LionFilter 200 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.

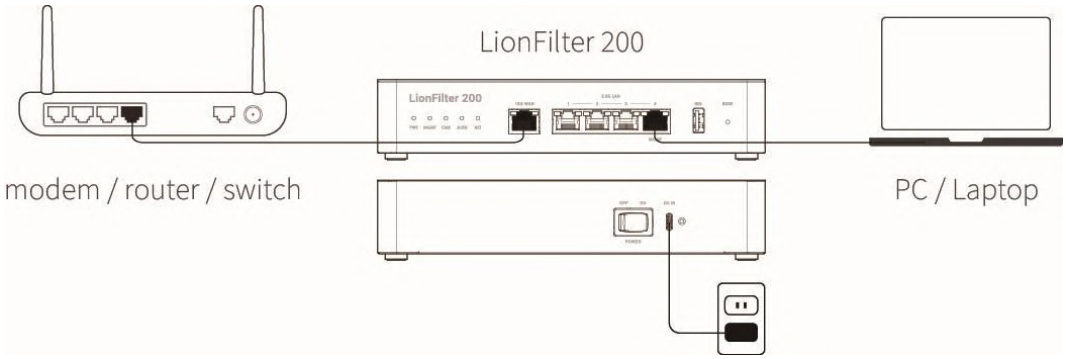
Technical Support Lionic Corporation

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

Content

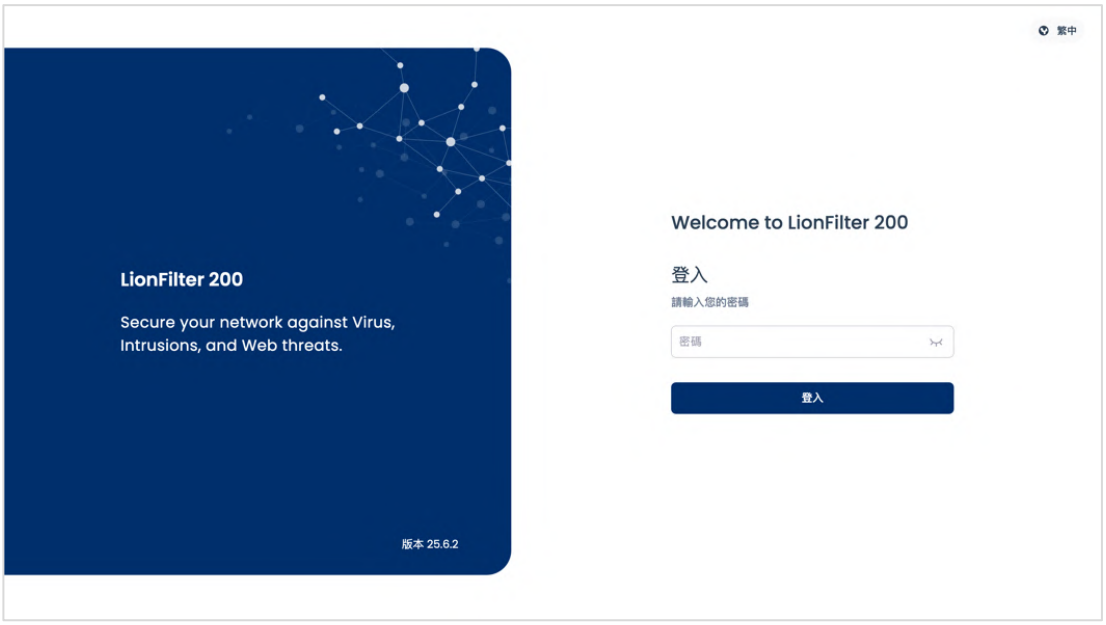
Access Web GUI and Connect to the Network

1. Plug the power cable into LionFilter 200. Turn on the power switch.
2. Connect the WAN port of LionFilter 200 to the LAN port of a modem / router / switch provided by the ISP or the IT administrator with an Ethernet cable.
3. Connect the MGMT port of LionFilter 200 to your PC/Laptop with another Ethernet cable. It will automatically assign an IP to your PC/Laptop via DHCP.



Network cable connection method

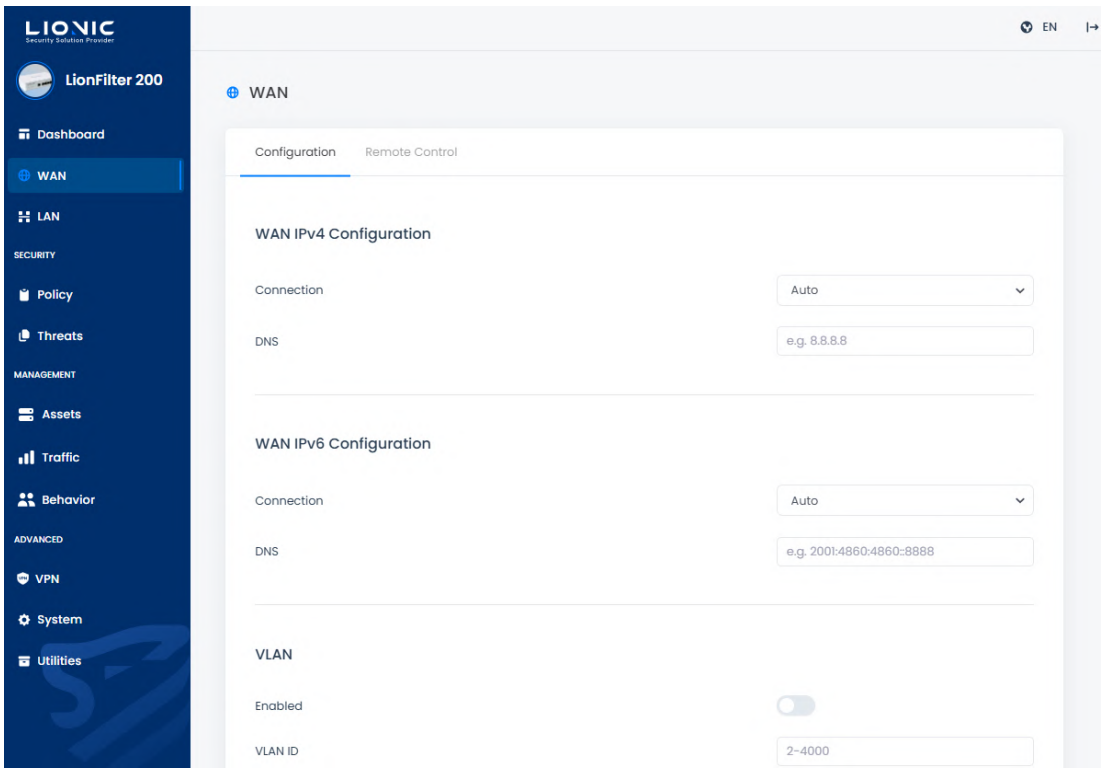
4. After getting the IP, open your PC/Laptop browser and go to https://myfilter.lionic.com/. Here you will see the LionFilter Login page.



Login page

5. The default password for login is the Serial Number shown at the bottom of the product.

6. After logging in, set the network configuration of LionFilter 200 in [WAN] page.



WAN

* Note: you can configure the MGMT port to be used as a regular LAN port. Todo this, go to [System] > [Device] page and disable the MGMT port

7. To keep the latest virus/intrusion/phishing/fraud detection and prevention, please buy the license key i.e. activation code and enter it in [System] >[Device] > [Activation Code] field. Then, click the 'Activate' button while the device is connected to the Internet to make the activation take effect.

   * Note : The activation code consists of 20 English letters and numbers. It can activate the license after applied successfully. Then the License Status will be displayed as Activated. If you do not receive the activation code when you purchase LionFilter 200 or the activation code is not working, please contact local sales representatives in your region

Overview

Dashboard:

[Dashboard] shows operating status and device information of LionFilter 200, including Inspection History, threat statics, network traffic monitoring and system resource usage.

WAN:

WAN settings of LionFilter 200 could be configured in [WAN], such as IPv4/IPv6 configurations and [Remote Control] settings.

LAN:

LAN settings of LionFilter 200 could be configured in [LAN]. After switching the connection mode from [Bridge Mode] (default) to [Router Mode], DHCP reservations, port forwarding and static route 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:

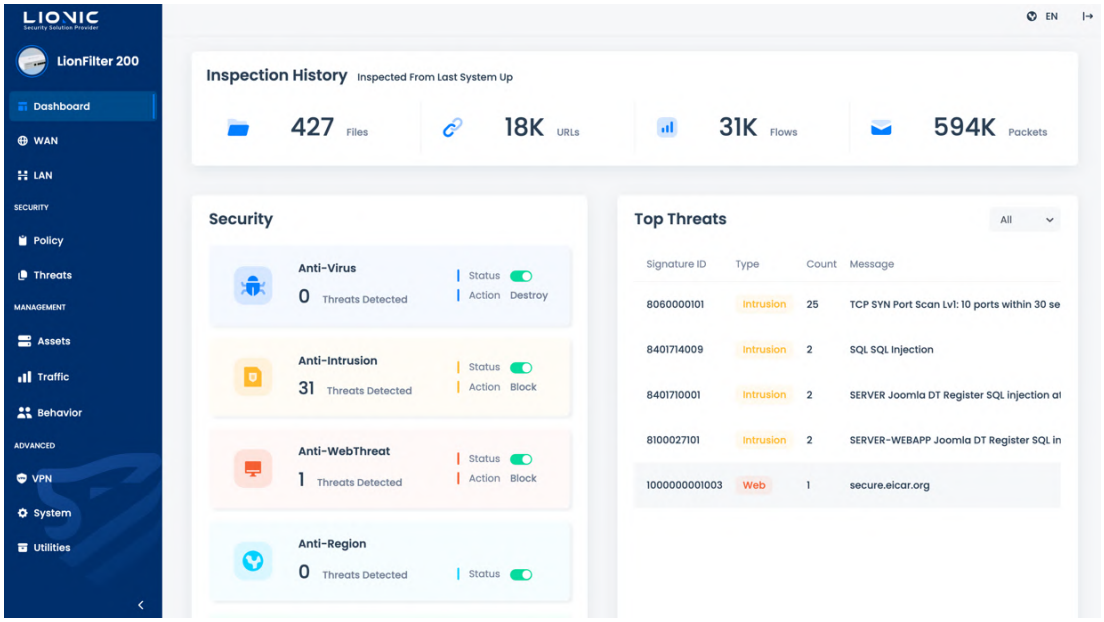
- **Assets:** The asset management feature can list the identified LAN devices and block or allow specific assets to connect to the network.
- **Traffic:** Traffic management can list the current connection usage of each LAN device and perform bandwidth management.
- Behavior Management: The behavior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

Advanced:

- **High Availability:** Adding 2 or more LionFilter 200 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 LionFilter 200 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 LionFilter 200.

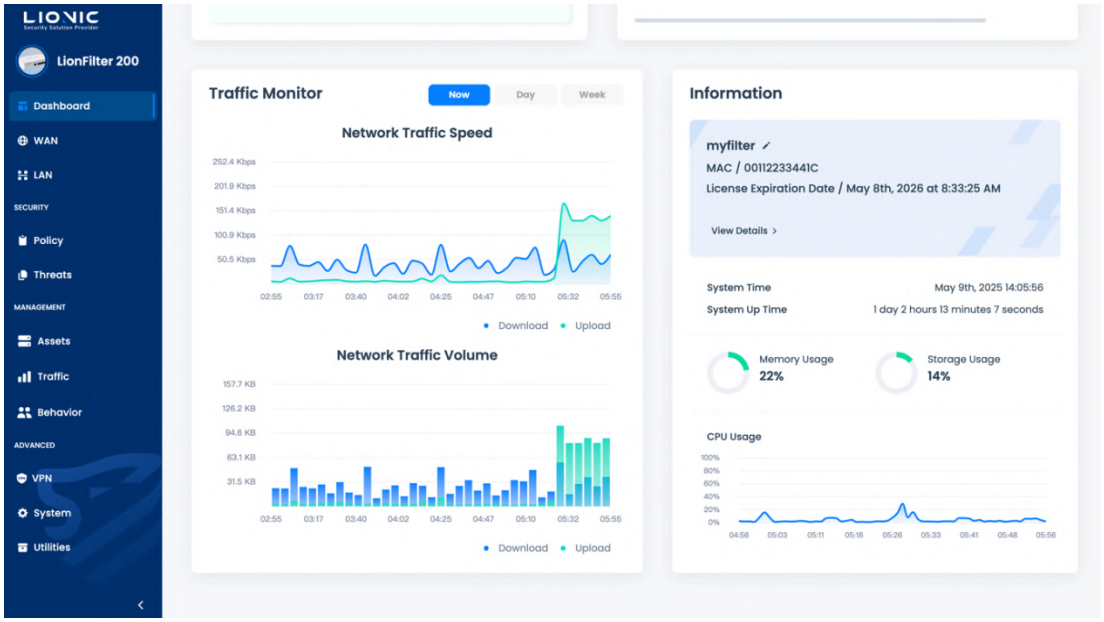


Dashboard

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

Security: Showing the threat number detected by LionFilter 200, enabling status and actions of each security feature. By clicking the threat number or the “Action” button, you can access the threat log page or the policy page of the corresponding feature.

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



Dashboard

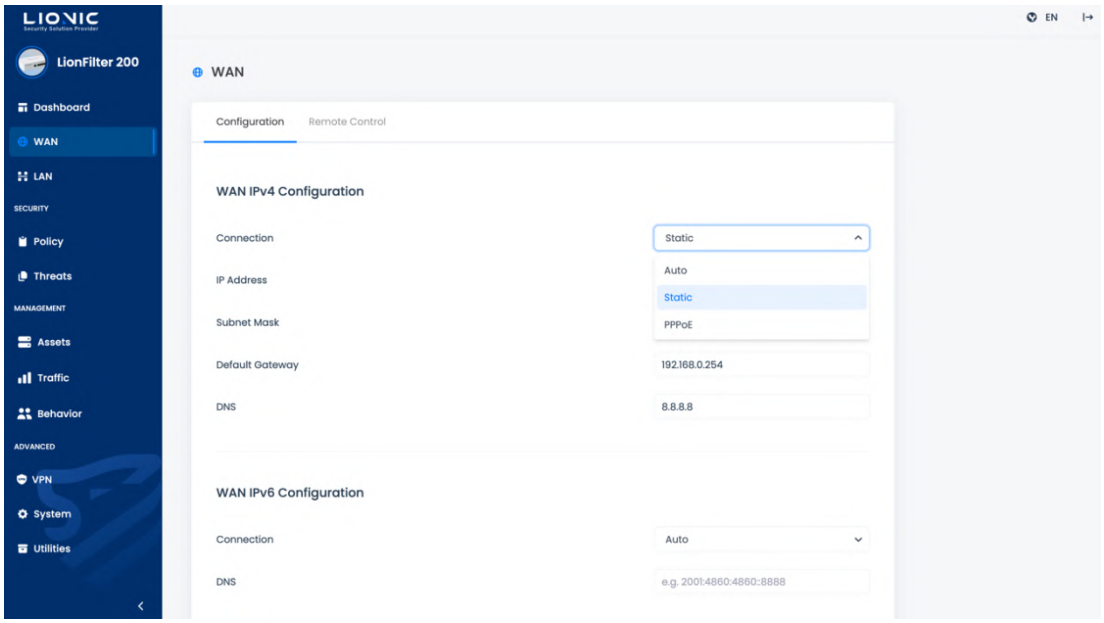
Traffic Monitor: Showing the download and upload traffic via LionFilter 200.

Information: Showing the device information of the LionFilter 200, such as the device name (editable), MAC address, license expiration date, firmware version, signature versions, WAN IP address, system time, system up time and system resource usage.

WAN

Configuration

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



WAN- Configuration

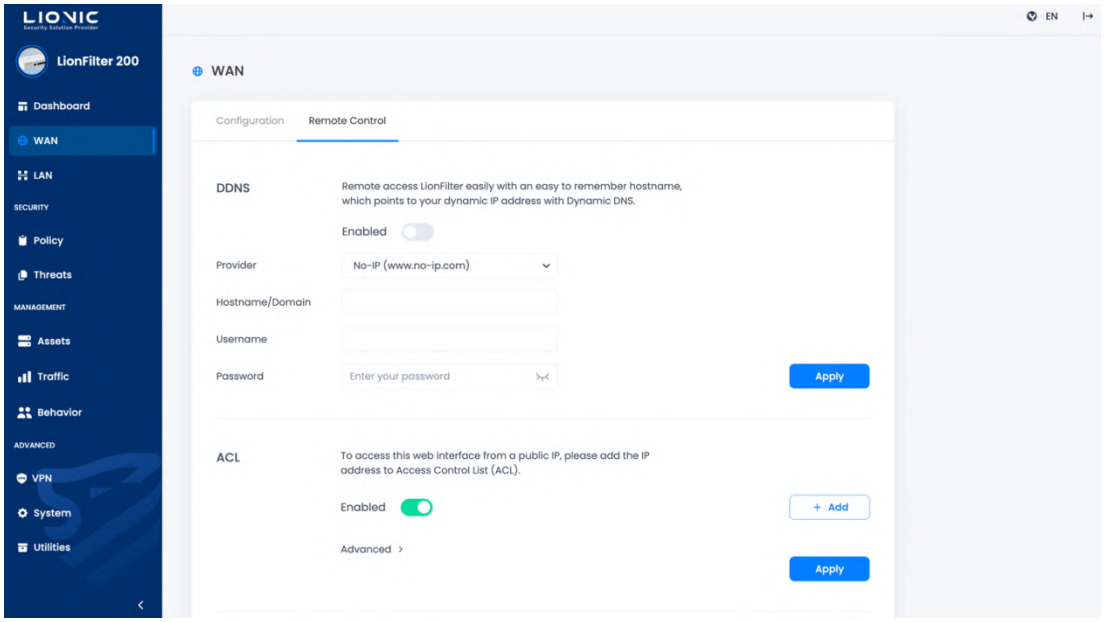
- **Auto:** LionFilter 200 obtains DHCP IP address from the router placed at the WAN side of the LionFilter 200.
- **Static:** For user to fills the correct IP address in manual.
- **PPPoE:** For user to fills the correct username and password in manual.
- **VLAN**：When LionFilter 200 is deployed in a VLAN environment, you can enter the VLAN ID of the domain to which LionFilter 200 belongs here.

* Remark: When using PPPoE connection, you may not be able to access the web GUI of LionFilter 200 due to the restriction of the access control list (ACL). Please see [Remote Control] for more details of ACL.

Remote Control

To prevent LionFilter 200 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 LionFilter 200 connects Internet using a public IP address, please configure settings in [Remote Control].



WAN- Remote Control

DDNS

When the LionFilter 200 is using a dynamic public IP address, you could use a static domain name to access the LionFilter 200.

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 LionFilter 200 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 LionFilter 200 is using a private IP address to connect Internet, please set DDNS and port forwarding on the router at the WAN side of LionFilter 200.

Access Control List (ACL)

To prevent LionFilter 200 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 LionFilter 200 connects Internet using a public IP address, the IP address that would be used to access LionFilter 200 should be added into the Access Control List (ACL).

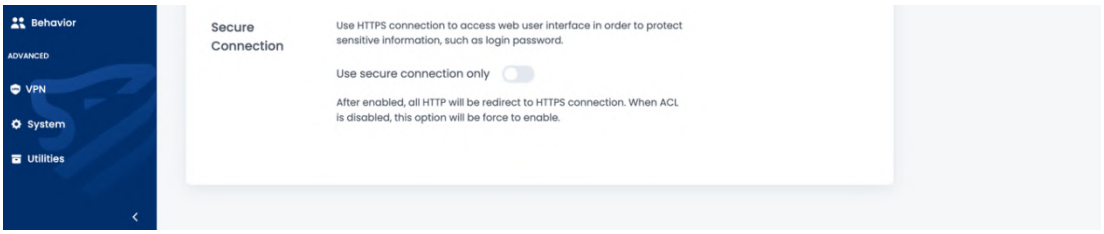
Step 1: Click [+ Add].
Step 2: Enter the public IP address of the external network device or the IP address of a specific internal domain into the input field.
Step 3: Click [Apply].

- **Restrict access from a from a private IP**
  After enabled, please add private IP addresses to ACL in order to access this web interface.

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 LionFilter 200.

* Remark:

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



WAN- Secure Connection

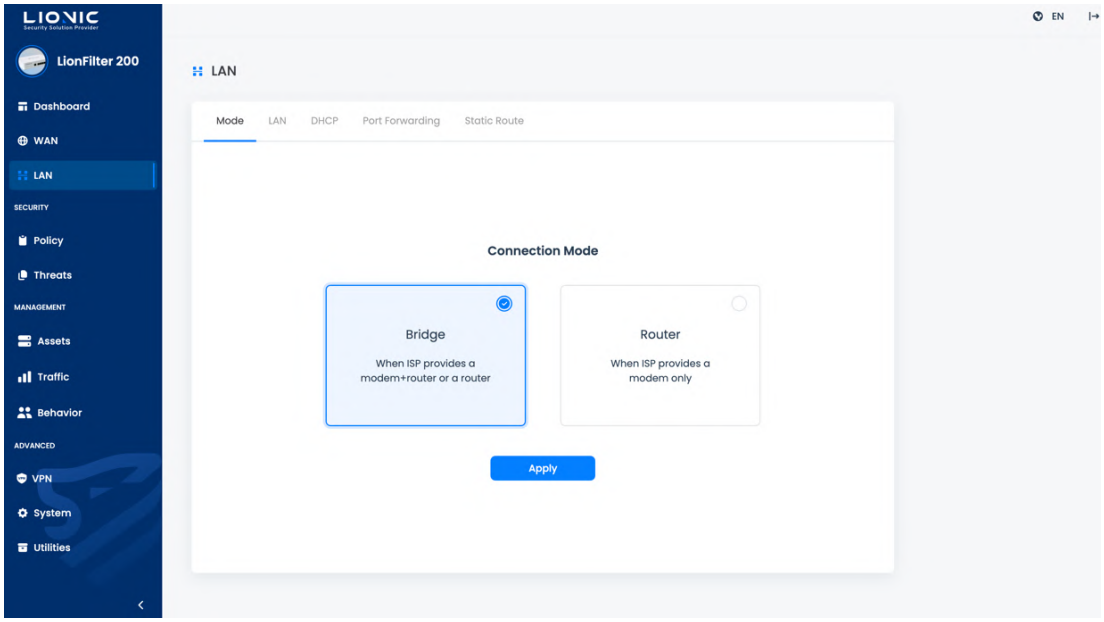
Secure Connection

After [Secure Connection] is enabled, all HTTP connections accessing the web GUI of LionFilter 200 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

LionFilter 200 supports 2 connection modes. Select a suitable connection mode based on your network environment.



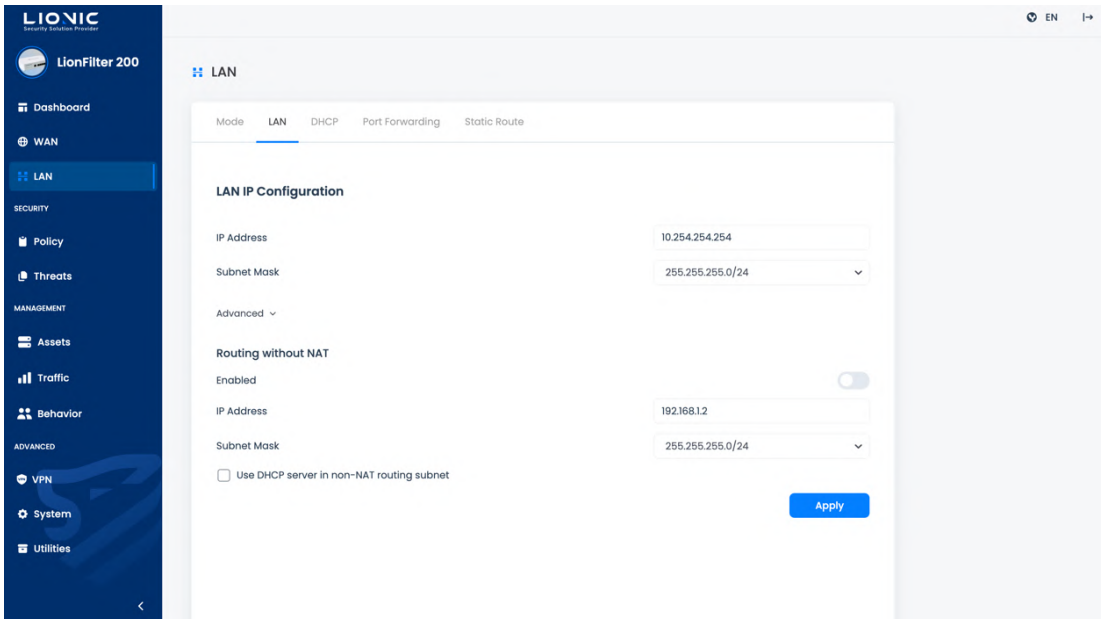
LAN-Connection Mode

- **Bridge mode (default):**
  DHCP is disable to LAN devices in [Bridge] mode. Please connect LionFilter 200 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 LionFilter 200 and its LAN devices.

After you selected the suitable connection mode and clicked [Apply], LionFilter 200 would start configuring the network function. The Internet connection would be interrupted during the configuring, and you may need to login again to access the web GUI.

LAN

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

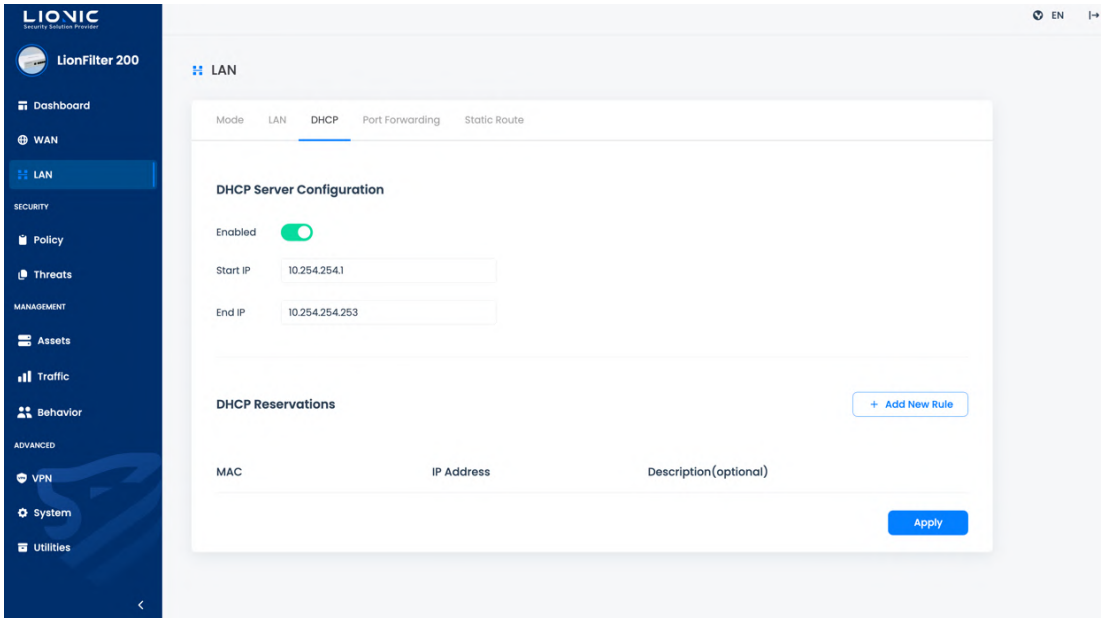


LAN-LAN IP

- **Routing without NAT**
  In [Router Mode], users can independently set the IP subnet for non-NAT routing. When there is no need for NAT translation between the external network and the internal network, enter the designated subnet into the input box and click [Apply] to enable this feature.

DHCP

In [Router] mode, LionFilter 200 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 LionFilter 200, you can use DHCP to assign private IP addresses to LAN devices.



LAN-DHCP

DHCP Server Configuration

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

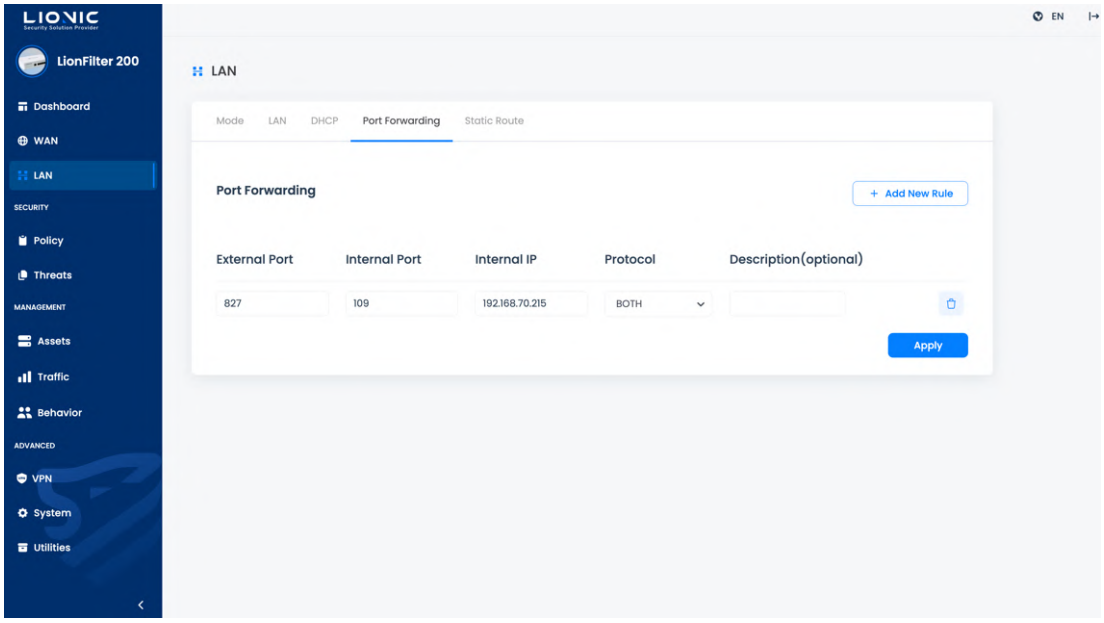
DHCP Reservations

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

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

Port Forwarding

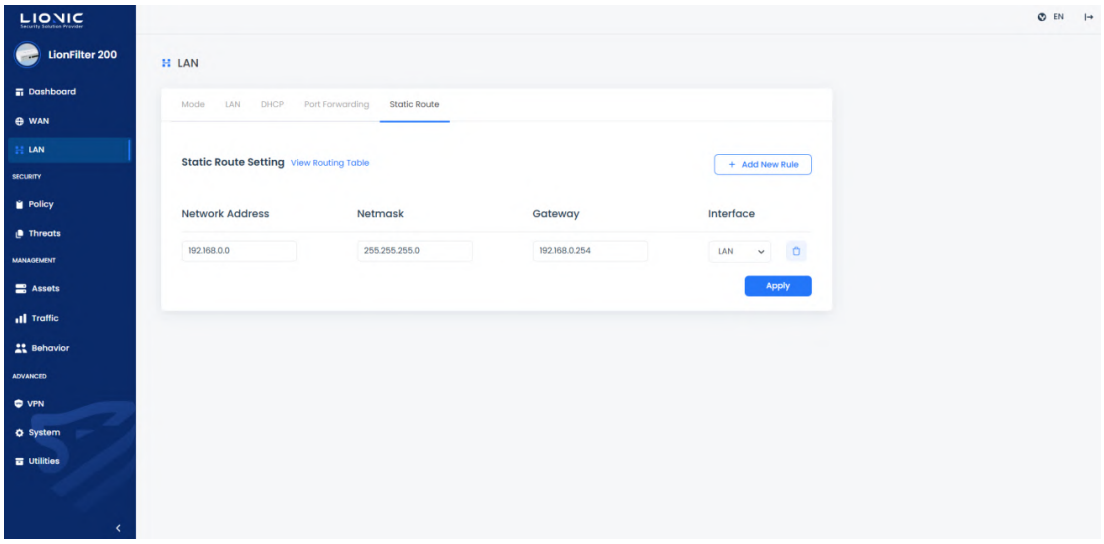
In [Router] mode, LionFilter 200 supports [Port Forwarding]. If you need to access a LAN device from Internet, set the internal port and internal IP address to access the LAN device through a specific external port.



LAN-Port Forwarding

Static Route

In [Router Mode], the LionFilter 200 can provide static routing functionality. This feature can be used when there is a need to connect different network segments.



LAN-Static Route

Policy

安全規則中提供所有資安防護功能的設定，可根據使用需求調整防護的內容。

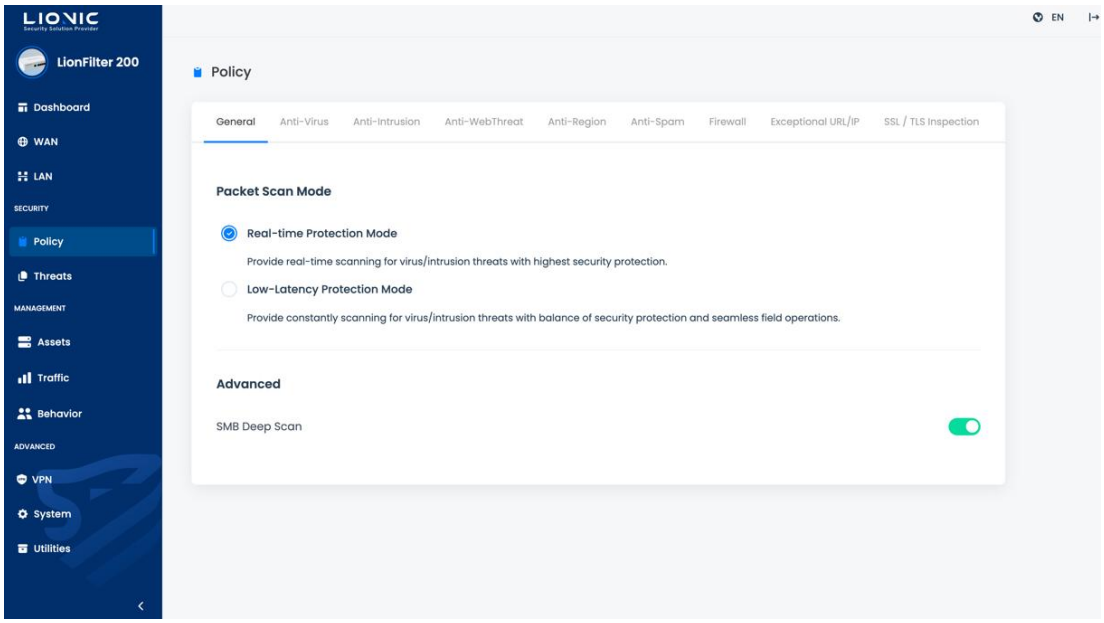
General

Packet Scan Mode

- **Real-time Protection Mode**：Inline intercept packets for scan, stop virus or intrusion immediately for network security. Suitable in high security fields, like Enterprises, Financial Bank, Healthcare institutions.
- **Low-Latency Protection Mode**：Copy packets for scan, let original packets pass through immediately for network stability. Suitable in latency sensitive fields, like Smart Factory or Automated Production Line.

SMB Deep Scan

Perform a full scan on files transmitted via the SMB protocol or for intrusions.
* Note: Disabling [SMB Deep Scan] can reduce the time required for scanning, but it will lower the protection level of the antivirus system and intrusion prevention.



Policy-General

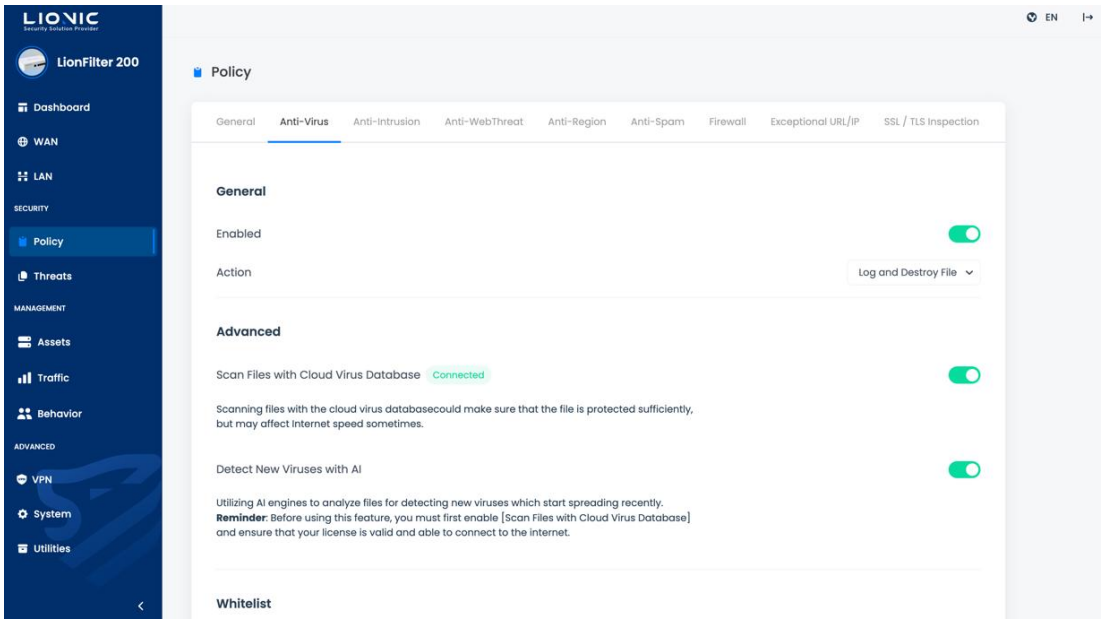
Anti-Virus, Anti-Intrusion, Anti-WebTheat

LionFilter 200 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



Policy

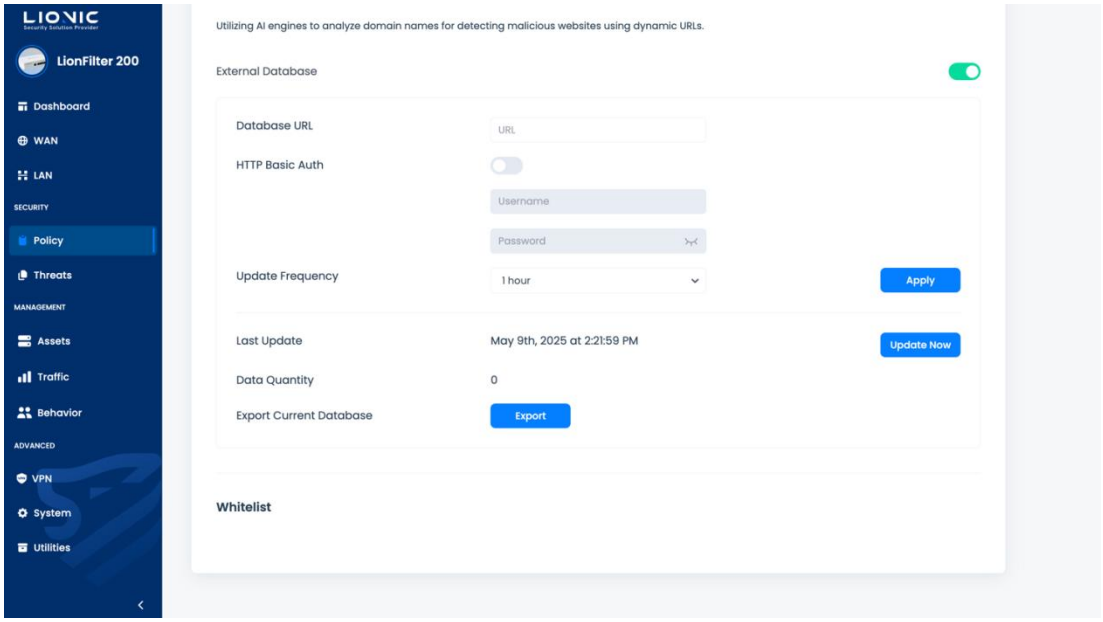
- **Enabled:** Enable or disable each security feature separately. The default setting is ENABLE.
- **Action:** The action that LionFilter 200 takes after the threat is detected.
  - Log Only: Only shows the threat event in [Threats] page.
  - Log and Destroy File: Shows the threat event in [Threats] 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, LionFilter 200 features the scan with LIONIC cloud virus database. To obtain the full protection of Anti-Virus, please make sure your LionFilter 200 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, LionFilter 200 can detect frequent login failures in a short period. Once the occurrence frequency is higher than the threshold, LionFilter 200 will record or block the attempting attack based on the frequency.
- **Block Protocol Anomaly:** After enabling this feature, LionFilter 200 '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, LionFilter 200 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 LionFilter 200 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.

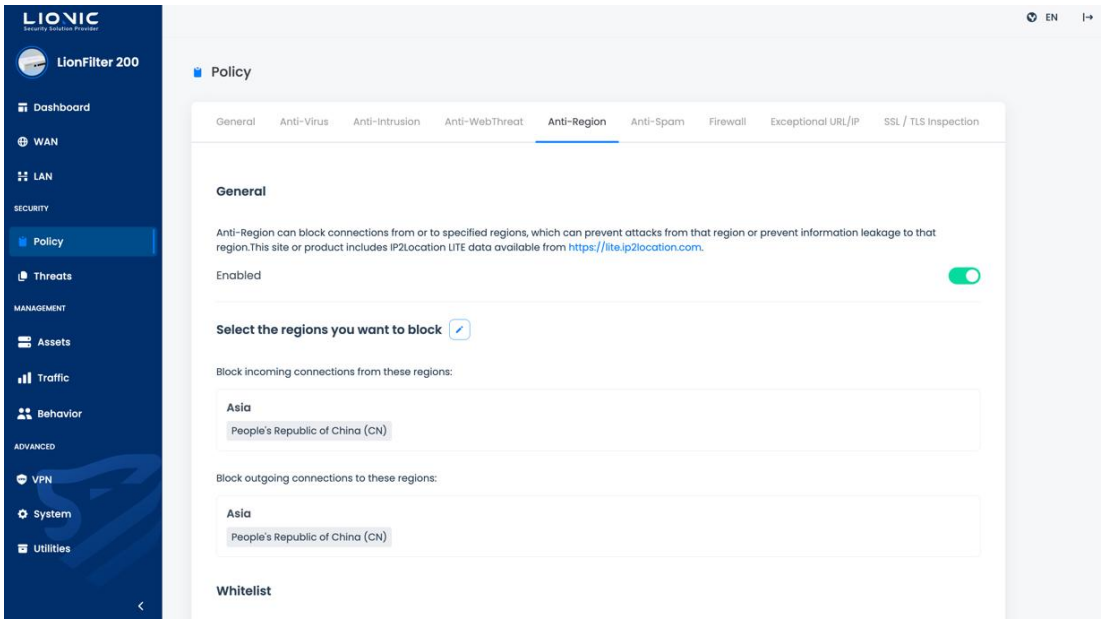


Policy-Advanced

- **Whitelist:** To correct a trusted file or connection destroyed/blocked by LionFilter 200 by adding the threat to the whitelist.
  - Add to whitelist: Find the threat event in [Threats] page, and then click [+] to add it into the whitelist.
  - View and remove whitelist rule: View the whitelist rule in [Policy] page, and remove the rule if needed.

Anti-Region

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



Policy- Anti-Region

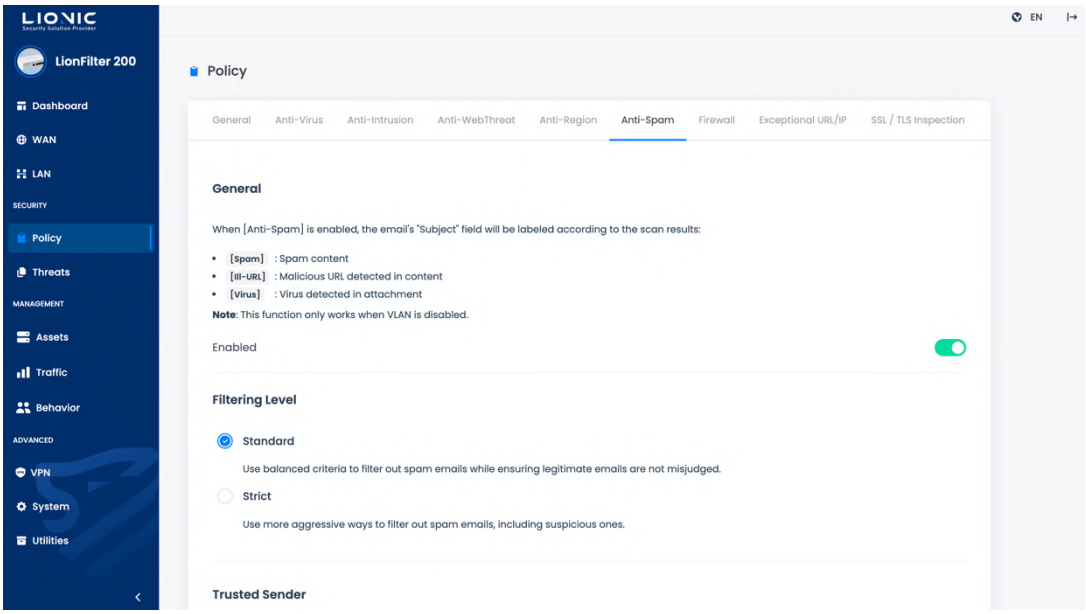
- **Step 1:** Enable Geographical Blocking.
- **Step 2:** Click Select Allow/Block Region.
- **Step 3:** Enter the respective configuration values.
- **Step 4 :** After clicking [Yes], the changes will take effect.

- **Whitelist**: Whitelist exceptions can be configured based on the countries/regions that have been set.

Anti-Spam

When [Anti-Spam] is enabled, the email's "Subject" field will be labeled according to the scan results:

- [Spam] : The email content is classified as spam.
- [Ill-URL] : The email content contains a malicious URL.
- [Virus] : The email attachment contains a virus.



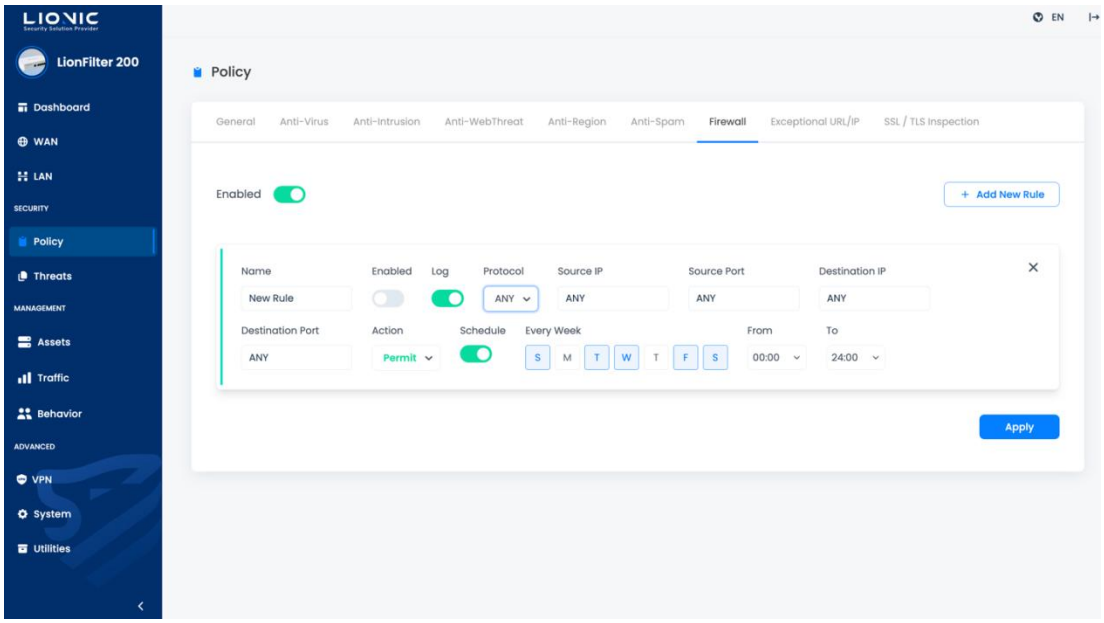
Policy- Anti-Spam

- **Filtering Level :** Select the filtering condition sensitivity.
- **Trusted Sender :** Enter the full email address or domain name. For example: demo@lionic.com or *@lionic.com.

* Note: This function only operates normally when VLAN is disabled.

Firewall

Besides the 3 cyber-security features, LionFilter 200 also provide a basic firewall.



Policy-Firewall

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

Firewall Configuration:

- **Name:** A user-defined firewall rule name.
- **Enabled:** Enable / disable the firewall rule.
- **Log:** Show / Hidden the firewall event in [Threats] page.

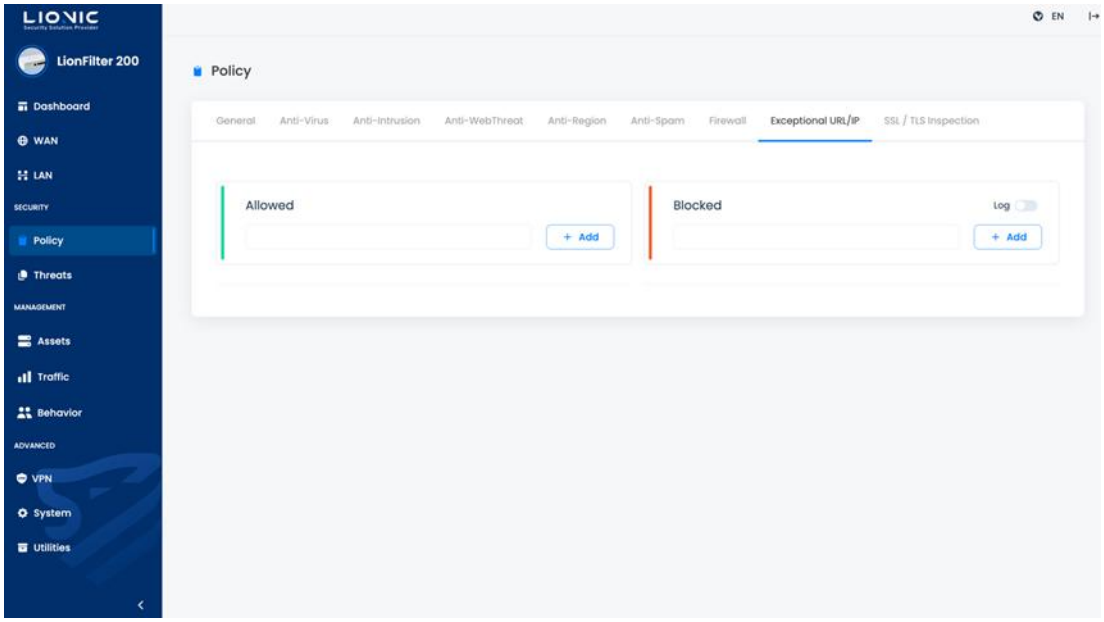
Protocol: TCP / UDP / ICMP/ IPv6-ICMP or ANY (all protocols).

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.

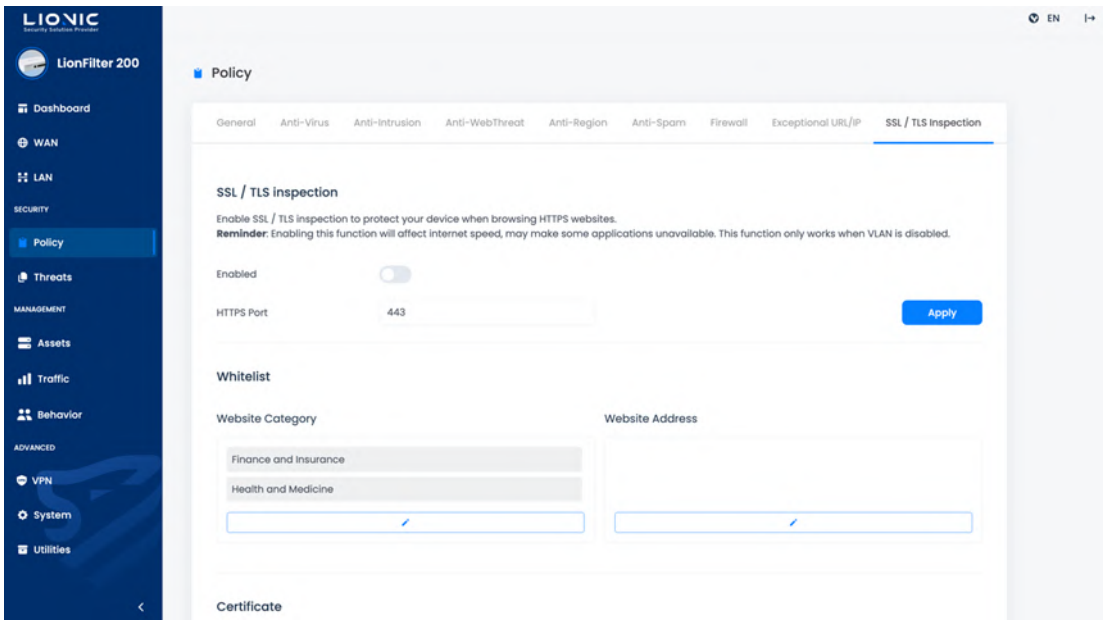
- **Log**: When enabled, if a connection is made to a prohibited website or IP, it will be recorded and displayed in the [Threats].

* Remark:

1. If a keyword is entered, all domains containing that keyword will be allowed or blocked. For example, entering "abc" will allow or block domains like www.abc.com and demo.abcdef.com. To block all files under a specific path, you must include the domain name and path. For example, entering "www.abc.com/path/" will block all paths and files under "www.abc.com/path/".
2. 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, LionFilter 200 will inspect packets encrypted with SSL or TLS, in order to protect your device when browsing HTTPS websites.



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:

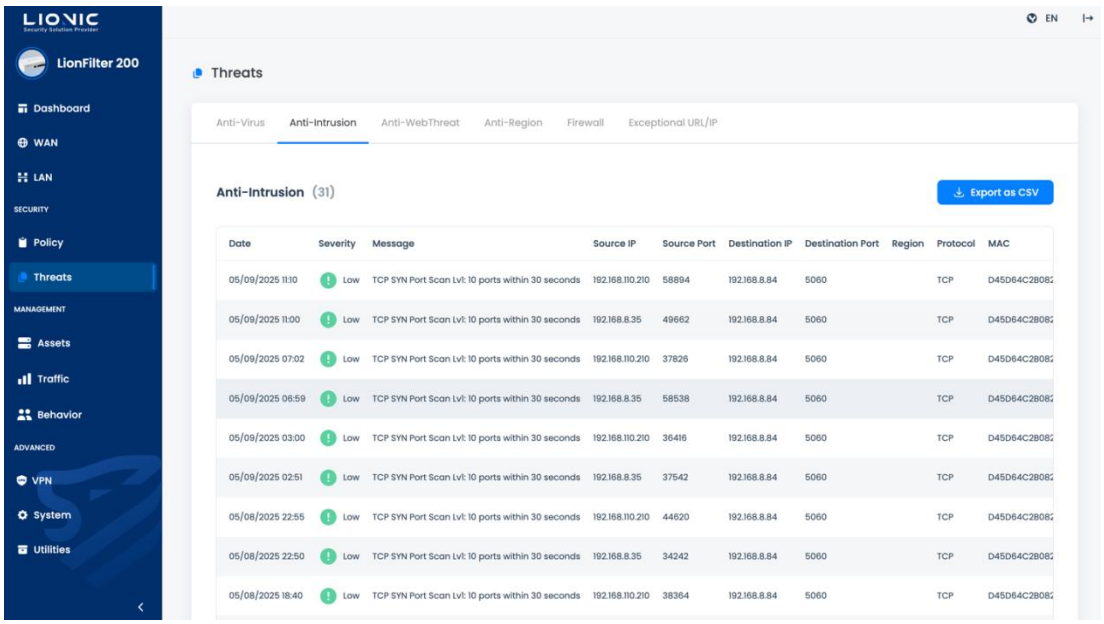
1. Enabling [SSL / TLS Inspection] would affect internet speed and may cause some applications not working.
2. When setting the HTTPS port, please avoid common ports used by other network services, such as Port 20, 21 for FTP, Port 25 for SMTP, etc., in order to prevent port conflict issues.

- **Whitelist:** After a website is added into the whitelist, LionFilter 200 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: LionFilter 200 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: LionFilter 200 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 LionFilter 200 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 LionFilter 200, the detailed threat information would be shown on the corresponding tab of each security feature in [Threats] page.

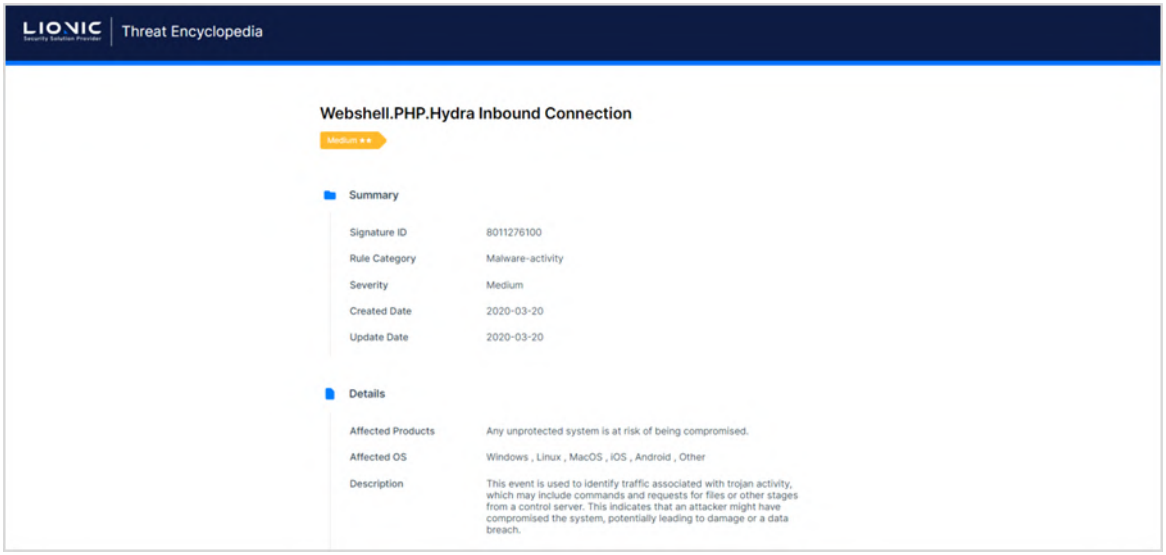


Threats

- **Export as CSV:** Export and download the log in a CSV file.
- **Whitelist:** If LionFilter 200 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:

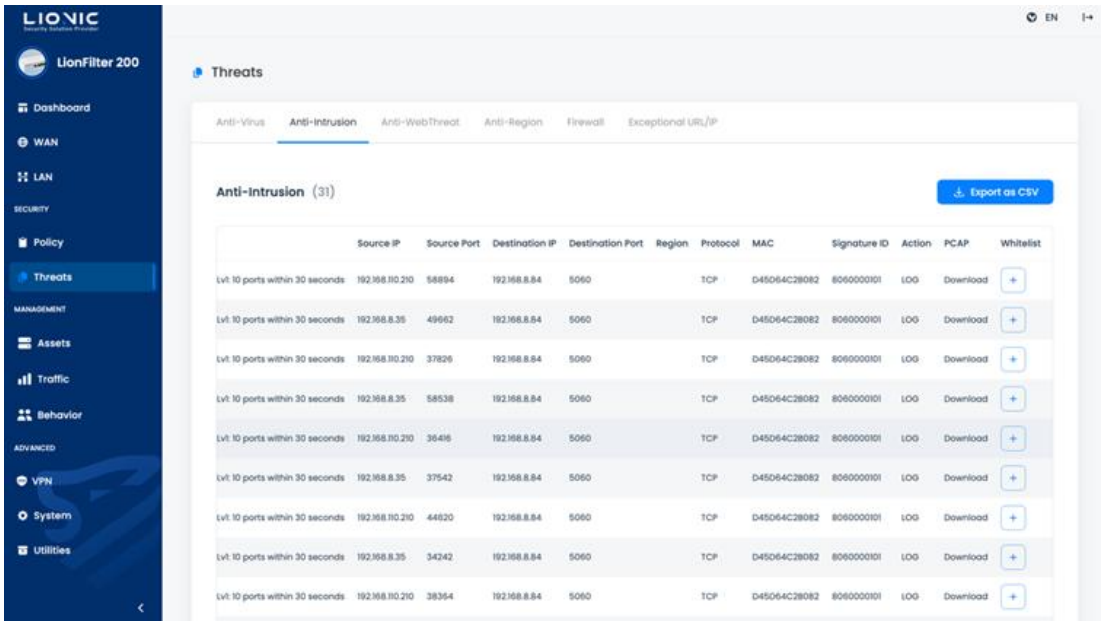
In the threat logs of [Anti-Intrusion], clicking on the Signature ID allows you to access the analysis and solutions for the corresponding attack.



Threats-Threats Encyclopedia

PCAP Packet Download:

When events of compromise or blockage occur on LionFilter 200, clicking [PCAP] > [Download] allows for packet download for further analysis.



Threats-PCAP Download

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

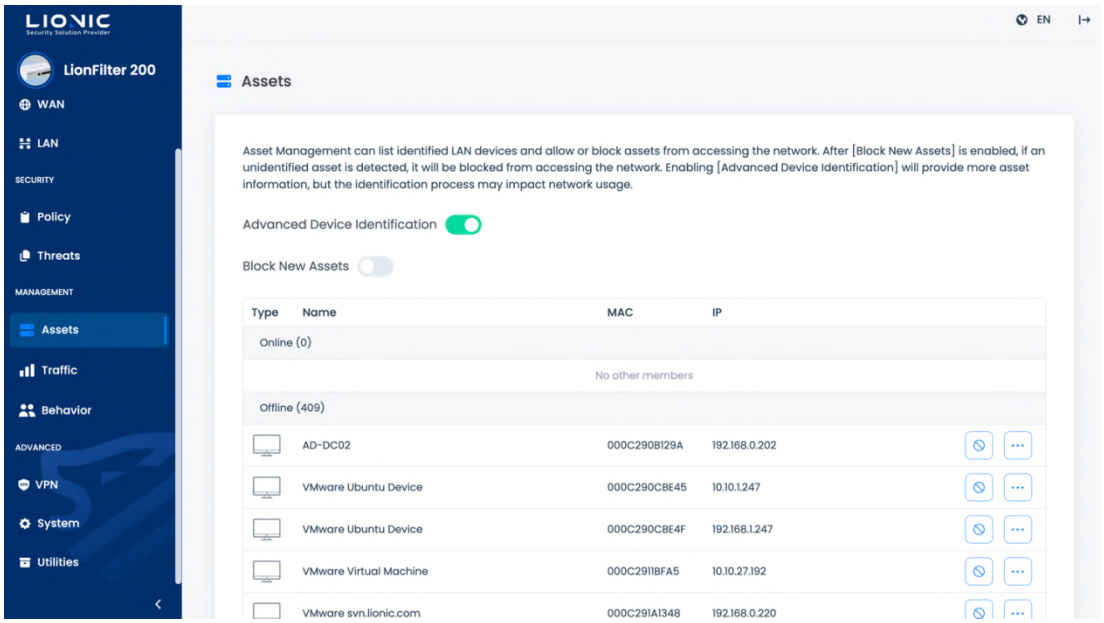
Assets

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.
-



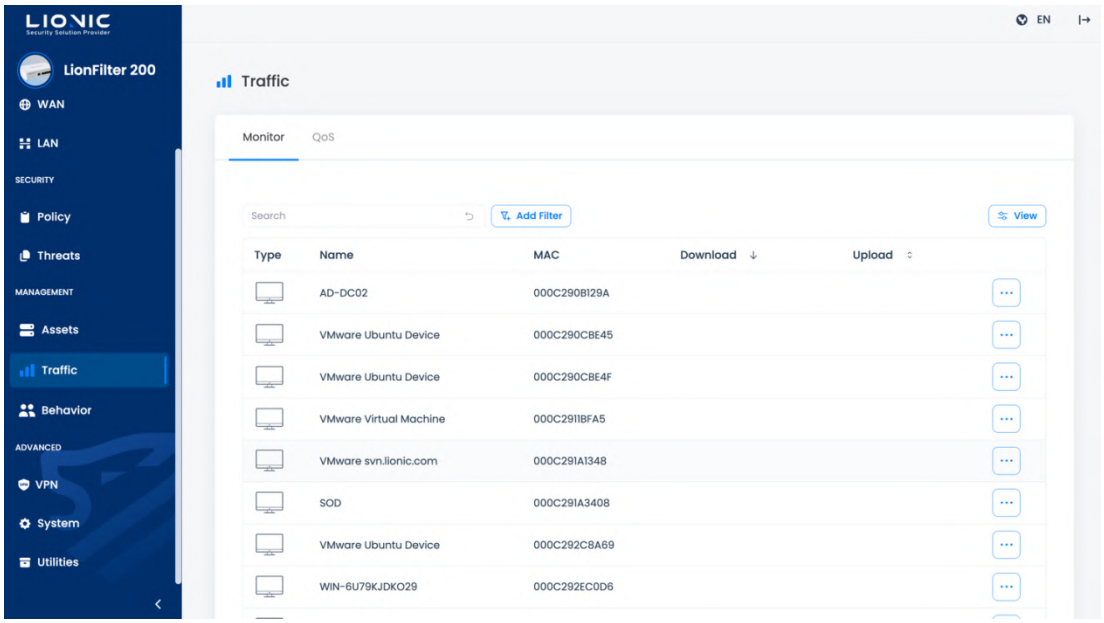
Assets

Traffic

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

Monitor

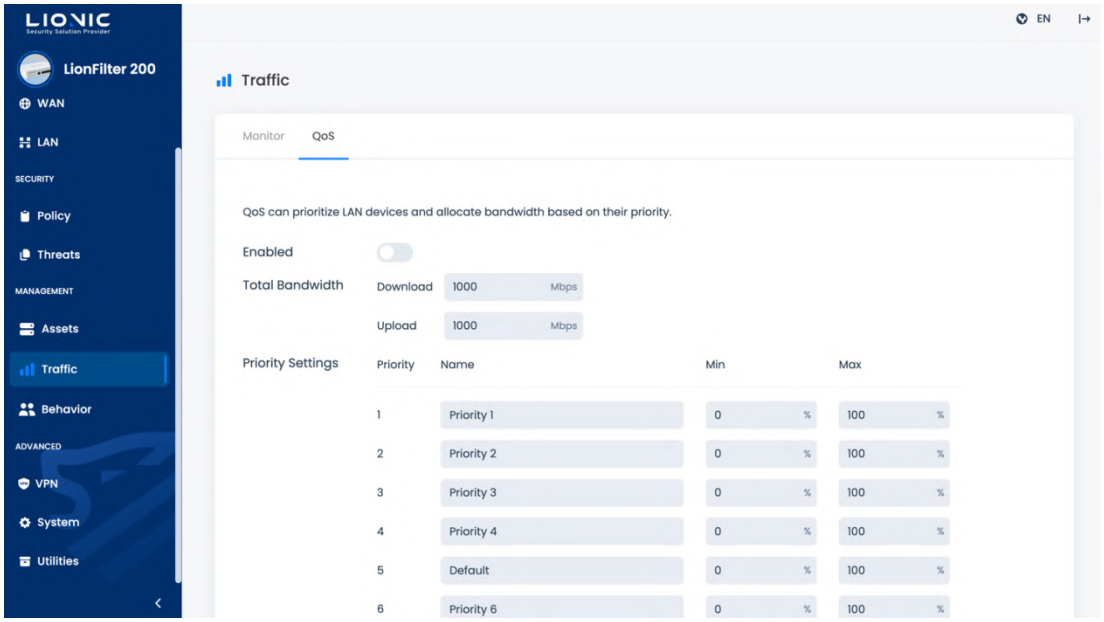
Displays the real-time download and upload traffic of LAN devices, which can be sorted by volume.



Traffic-Monitor

QoS

LionFilter 200 can perform bandwidth management for specific source IPs, destination IPs, or destination ports, allowing their traffic to receive higher priority service.

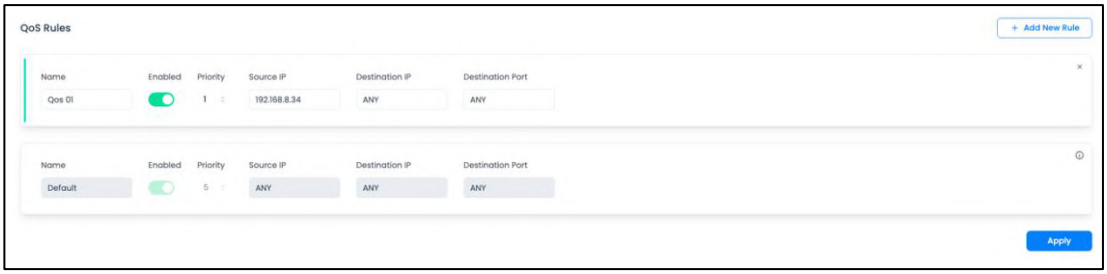


Traffic-QoS

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.

Traffic- Priority Settings

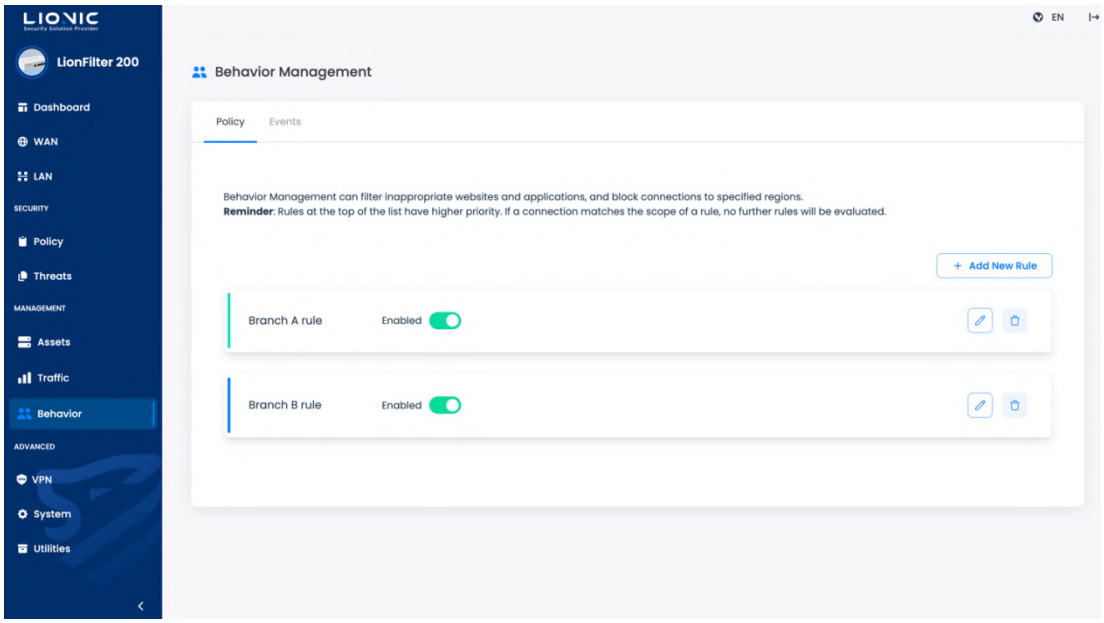
Step 5: Click [+ Add New Rule]
Step 6: Enter the setting values for each item.
Step 7: Click [Apply] to take effect.



Traffic-QoS Rules

Behavior

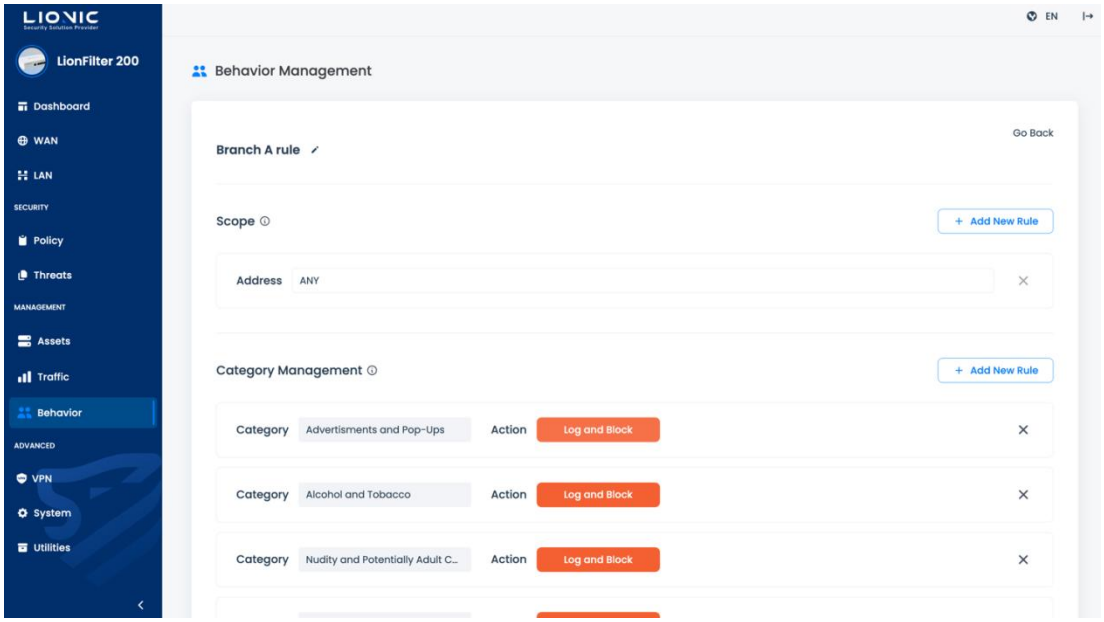
The Behavior Management feature allows you to manage specific content categories or applications. You can configure settings based on your needs to protect family members or employees from inappropriate content.



Behavior Management

Policy

Click [+ Add New Rule] to add a new rule. You can edit or delete rules on the Policy page.
Drag the left sidebar of a rule to change the order of rule checks. Rules at the top of the list have higher priority and will be evaluated from top to bottom. If a connection matches a rule's scope, the action configured for that rule is triggered, and no subsequent rules are evaluated for this connection.



Behavior Management-Policy Rule

Click  to enter the rule editing page, you can add different types of rules:

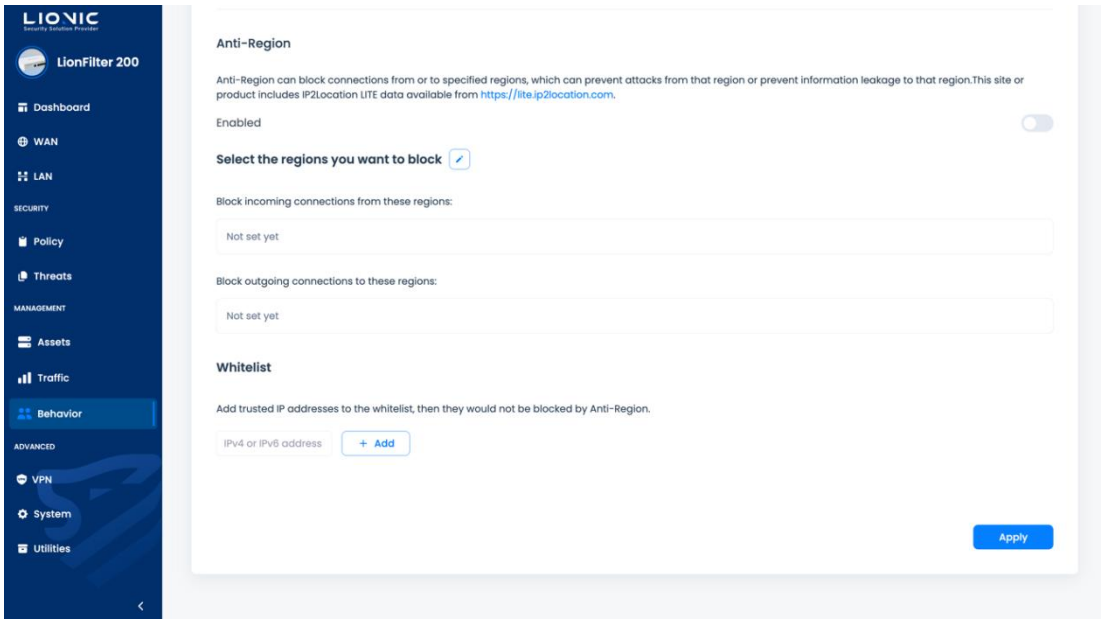
- **Step 1:** Click [+ Add New Rule] in the Scope to set the scope of the policy.
- **Step 2:** Enter the IP address or MAC address to be managed.
- **Step 3:** Choose the items to manage and click [+ Add New Rule] to configure the content and actions.
- **Step 4:** Click [Apply] to activate the settings.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

Anti-Region

Based on the country/region set by the user, block incoming connections from that region, or prevent devices from establishing connections to that country/region.



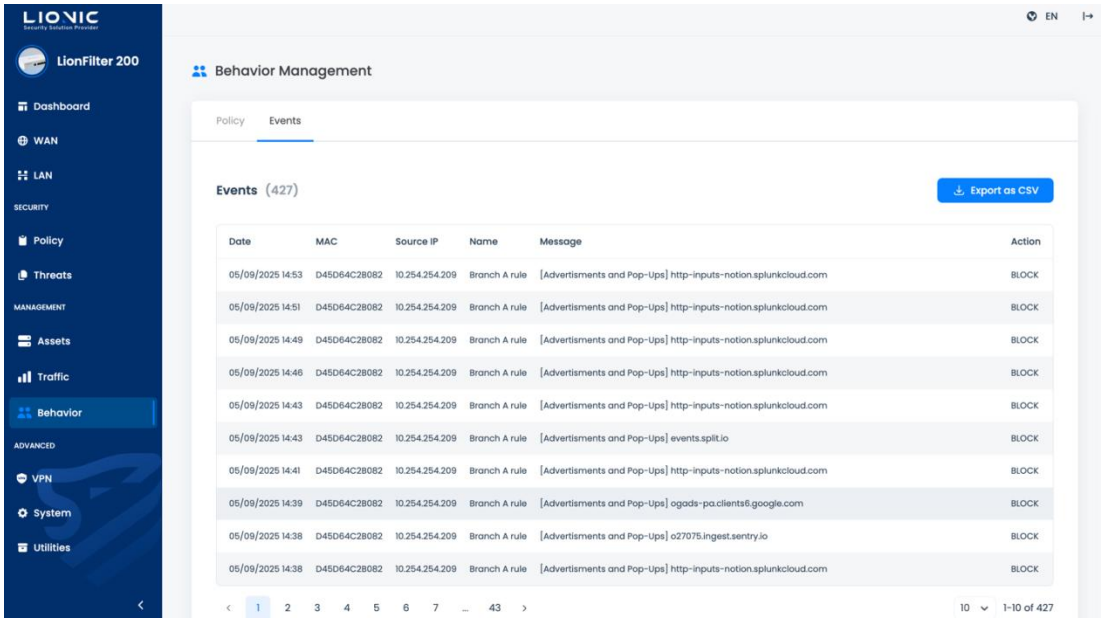
Behavior Management -Policy-Anti-Region

Step 1: Enable Anti-Region.
Step 2: Click ✎ to select the regions to allow/block.
Step 3: Enter the various configuration values.
Step 4: Click [Yes] to apply the settings.

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

Events

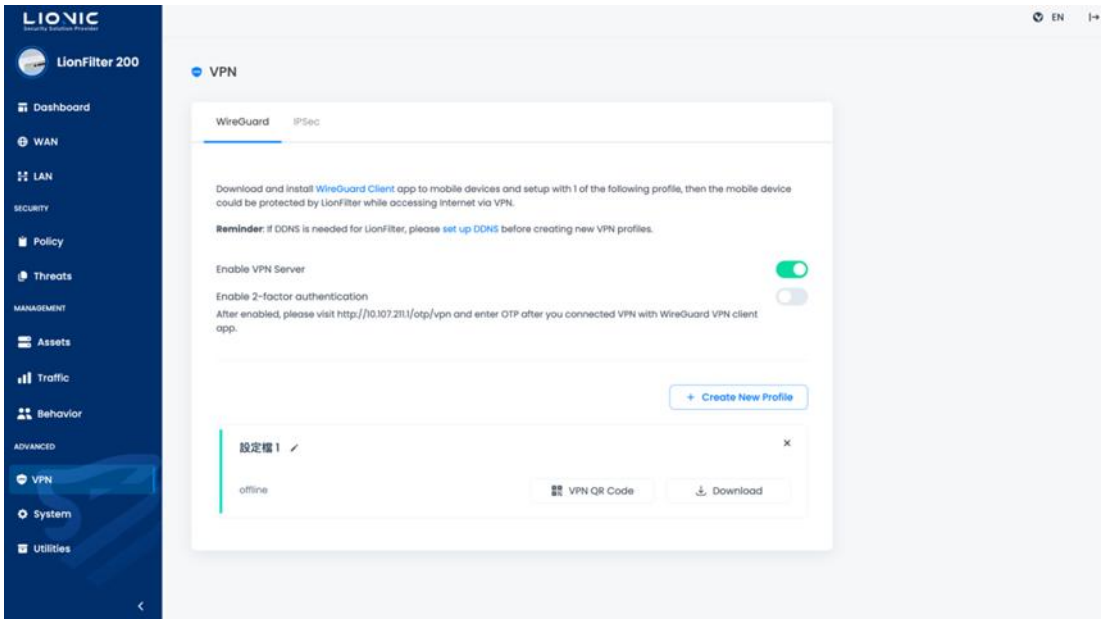
The detection results and actions of Behavior Management are displayed on the Events page. Click [Export as CSV] to export the records as a CSV file.



Behavior Management -Events

VPN Server

Enable the VPN server to expand the protecting range of LionFilter 200 to devices using cellular network or public Wi-Fi. Mobile devices could be protected by LionFilter 200 while accessing Internet via VPN.



VPN Server

WireGuard VPN

Preparation:
Download and install WireGuard Client app to the device which needs the protection of LionFilter 200.

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 LionFilter 200 via VPN with WireGuard Client app whenever the protection of LionFilter 200 is needed.

* Remark:

1. If you would like to set DDNS for LionFilter 200, please setup before enabling the VPN server.
2. If there is a router at the WAN side of LionFilter 200, please set port forwarding on the router, so that the connection could be redirected to Port 51820 of LionFilter 200. 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 LionFilter 200.
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:

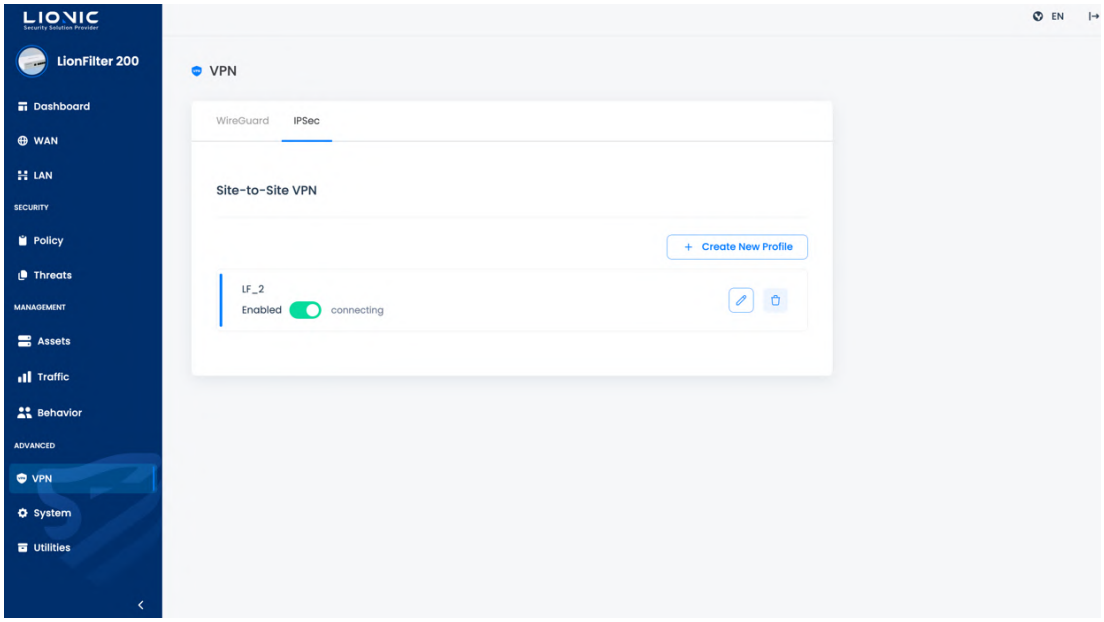
- **Step 1:** Connect LionFilter 200 via VPN with WireGuard Client app.
- **Step 2:** Obtain the OTP from the OTP app.
- **Step 3:** Visit https://myfilter.lionic.com/otp/vpn and enter the OTP.

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

· Note: After configuring the WireGuard VPN, the QoS function for PPPoE connections will be disabled.

IPSec Site-to-Site VPN

IPSec Site-to-Site VPN Used to establish a secure communication channel between networks in different geographical locations (such as a corporate headquarters and its branch offices), allowing their local area networks to safely connect with each other.



VPN -IPSec

Setup Steps:
Step 1: Click [+ Create New Profile].
Step 2: Enter the configuration values.

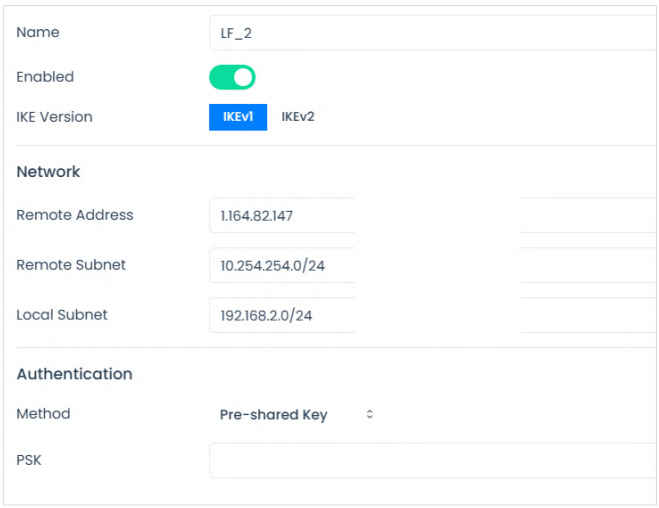
- **Name**: Profile Name
- **Enabled**: Enable/Disable
- **IKE Version**: Internet Key Exchange Version
- **Remote Address**: Remote IP Address
- **Remote Subnet**: Remote Subnet Mask
- **Local Subnet**: Local Subnet Mask

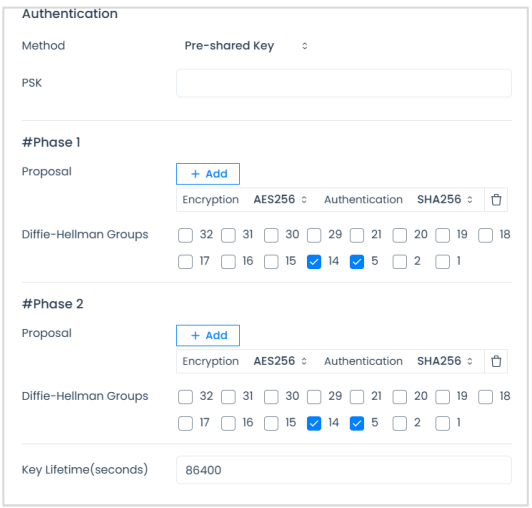
Authentication

- **Method**:
  - Pre-shared Key: A shared password set on both ends, used for mutual verification during Phase.
  - Signature: Uses public-private key certificates for authentication; requires certificate pairs on both servers.
- **PSK**: Pre-shared Key

Phase

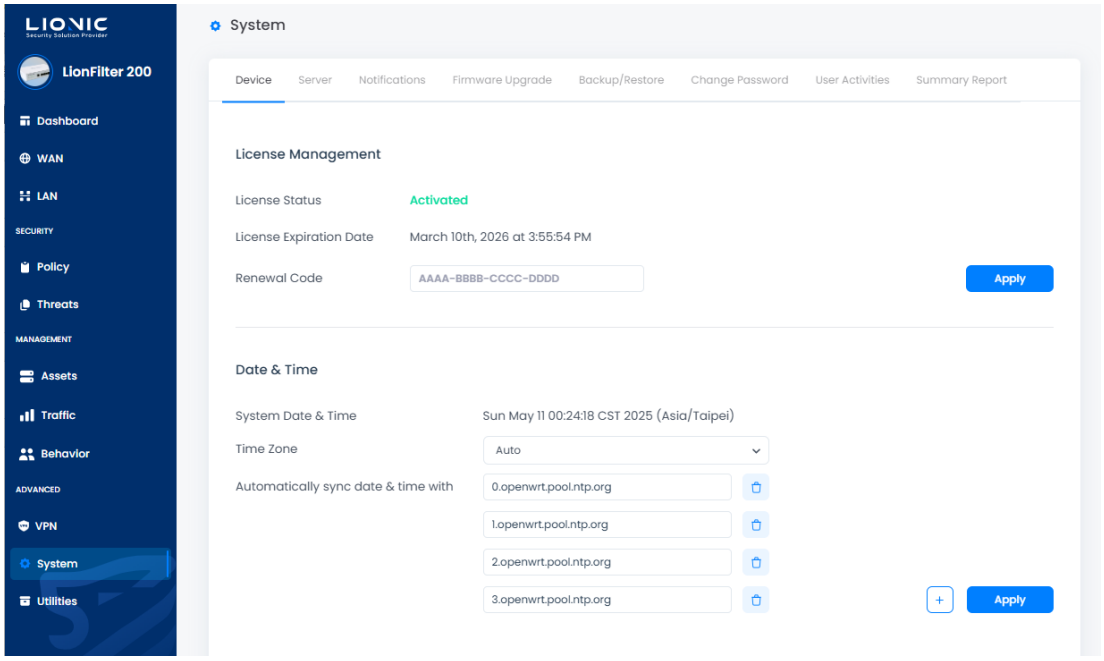
- **Method**: Encryption method for data transmission
- **Authentication**: Method used to authenticate encryption
- **Diffie-Hellman Groups**: Select the key exchange group length, used for encryption
- **Key Lifetime (seconds)**: Duration in seconds after which the AES encryption key is automatically rotated





System

Device



System-Device

License Management

View the license status, activate or renew the license for LionFilter 200.

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 LionFilter 200 is connecting to the Internet to make the activation take effect.

- **Renew license:** LionFilter 200 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 LionFilter 200 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

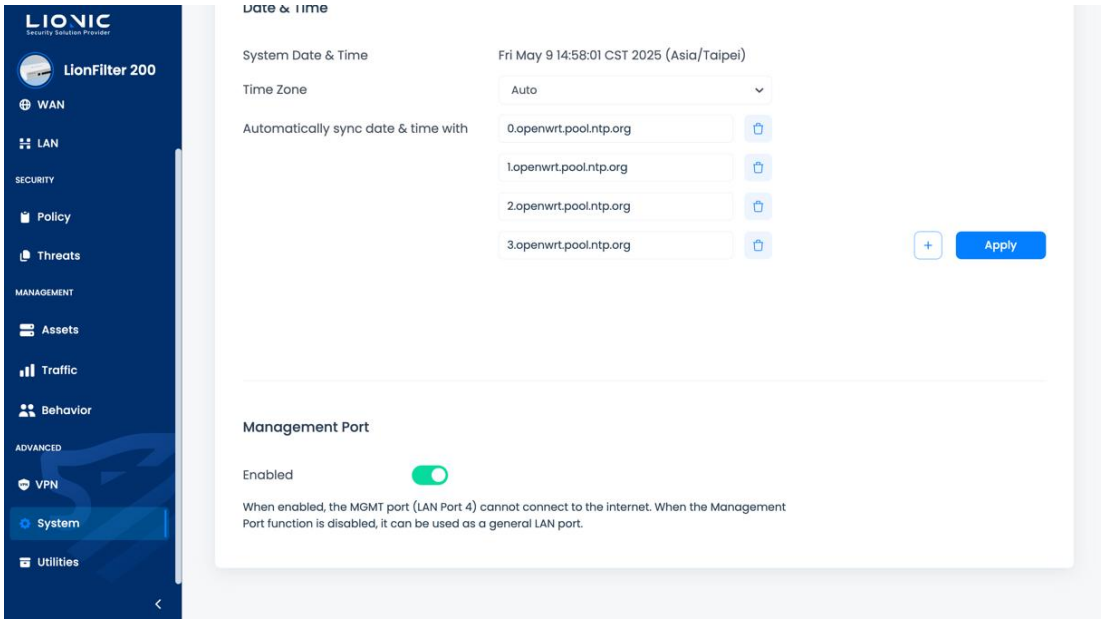
Display and configure the system time of LionFilter 200.

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

Management Port

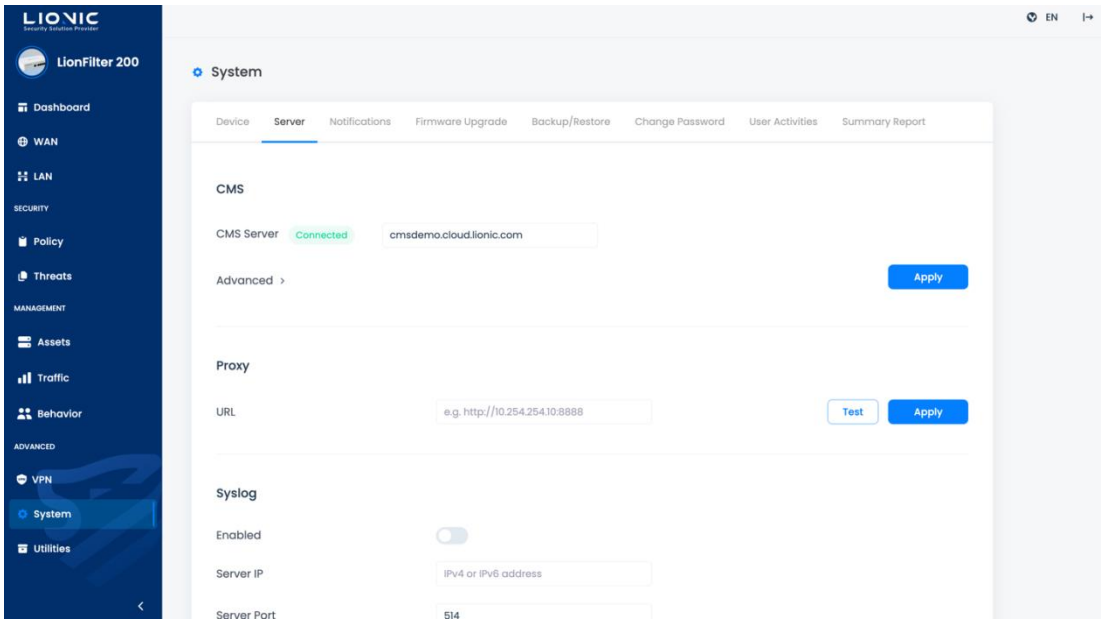
- The management port only supports in bridge mode, meaning the LionFilter 200 will assign IP addresses to connected devices via DHCP.
- When the management port is enabled, the MGMT port cannot connect to the WAN; when it is disabled, the MGMT port functions as a regular LAN port for network connections.

  *Note: The management port cannot be used simultaneously with the VLAN function. To use the VLAN feature, please disable the management port first.



System- Management Port

Server



System-Server

CMS

Central Management System (CMS) can monitor and control multiple LionFilter 200 in 1 portal. After the CMS is built, enter the address of CMS into the input field and click [Apply] to connect LionFilter 200 with the CMS. Please contact LionFilter 200 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, LionFilter 200, 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

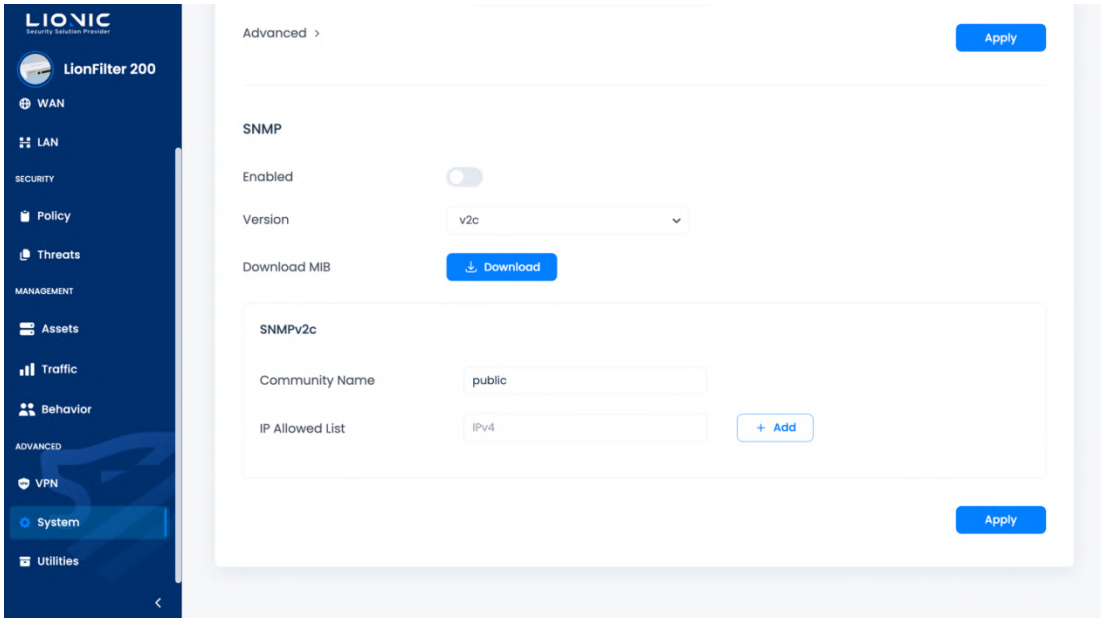
To obtain the full protection from LionFilter 200, the proxy server can help LionFilter 200 deployed in an intranet access LIONIC cloud services. After the proxy server is built, enter the server address into the input field and click [Apply] to access LIONIC cloud services via the proxy server. Please contact your IT administrator for more information.

Syslog

A syslog server can collect operating history of LionFilter 200. If you have your own syslog server, enter the configuration into the input field and click [Apply].

SNMP

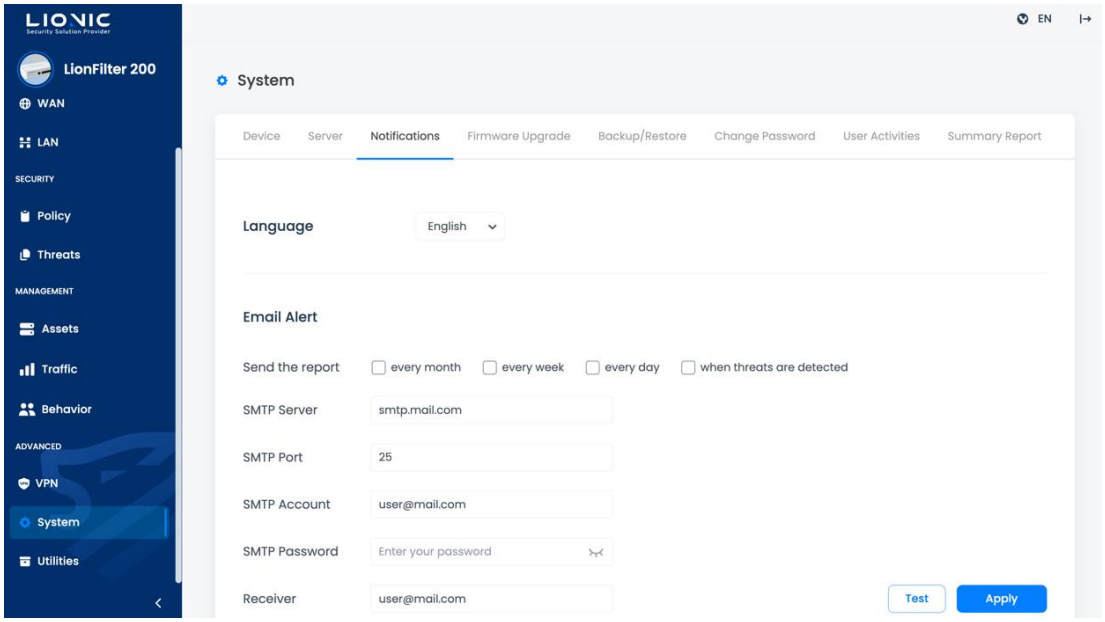
SNMP allows administrators to remotely monitor the system status information of the LionFilter 200. If you have set up your own SNMP server (v2c, v3 versions),enter the configuration into the input field and click [Apply].


LIONIC
Security Solution Provider
LionFilter 200
WAN
LAN
SECURITY
Policy
Threats
MANAGEMENT
Assets
Traffic
Behavior
ADVANCED
VPN
System
Utilities
Advanced
Apply
SNMP
Enabled
Version
v2c
Download MIB
Download
SNMPv2c
Community Name
public
IP Allowed List
IPv4
+ Add
Apply

System-SNMP

Notifications

When a threat is detected, LionFilter 200 can notify the details to the mail address you set in [Notifications] tab. Furthermore, LionFilter 200 can also summarize Inspection History, Threats Statics and System Notification every day or every week, and send Daily Report or Weekly Report to the mail address you set.



System-Notifications

Language

Select the language you prefer for mails and reports.

Email Alert

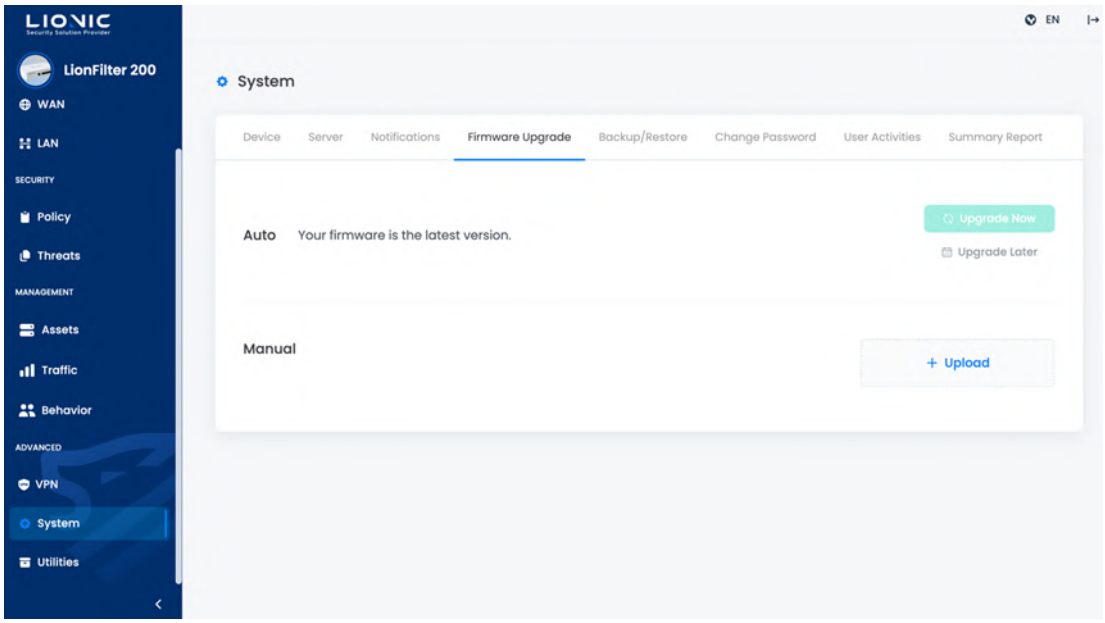
- **Send the report:**
  - Every month: Send the monthly report on the 1st day of each month at 00:00.
  - Every week: Send the weekly report every Sunday at 00:00.
  - Every day: Send daily report at 00:00 every day.
  - When threats are detected: Threat information is sent immediately upon detection.
- **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 LionFilter 200 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.

Firmware Upgrade

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



System-Firmware Upgrade

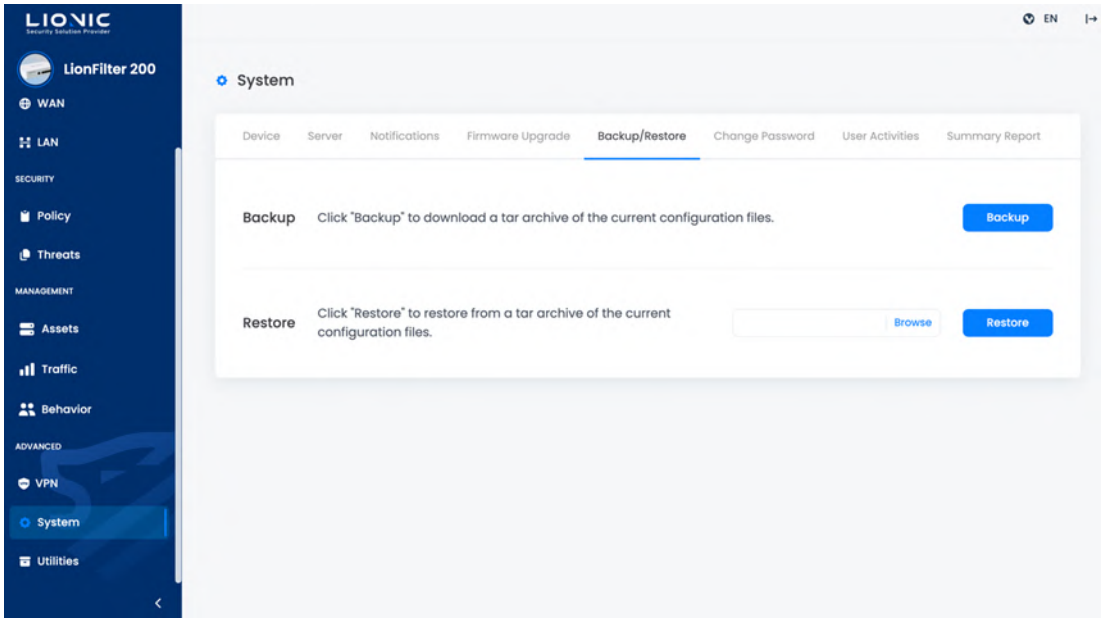
Update Later: To allow users to update the firmware during off-peak network hours, a scheduling function is available to specify the desired date and time for the firmware update.

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

* Remark: LionFilter 200 would reboot during upgrading firmware. The network connection will resume after the reboot is completed.

Backup / Restore

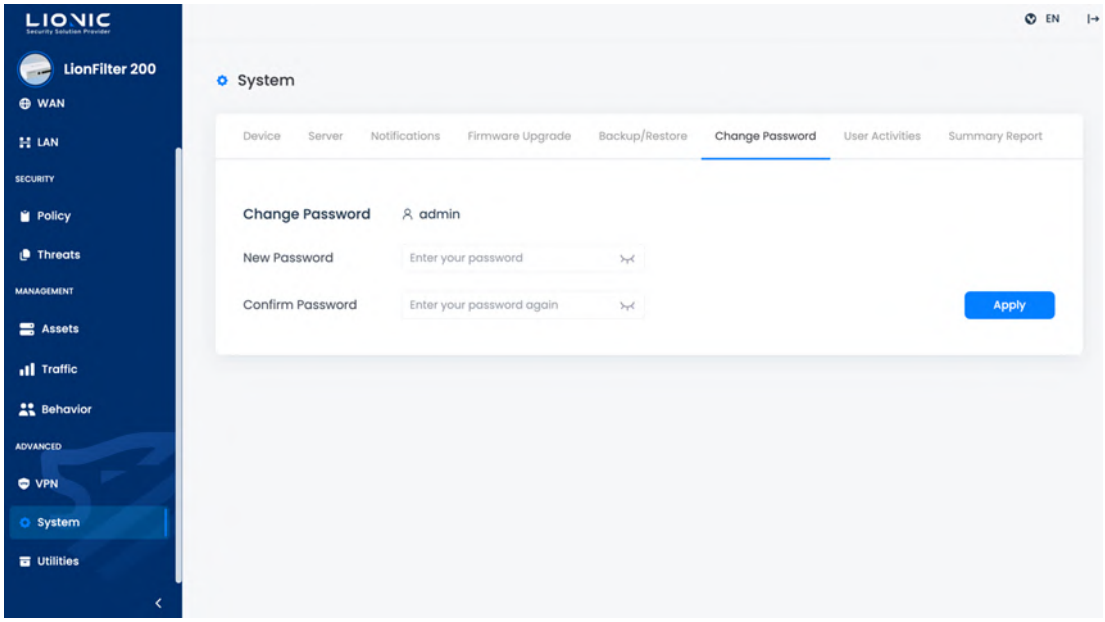
[Backup / Restore] function can backup LionFilter 200 configurations, such as security policies and whitelist setting, and restore on the same or other LionFilter 200.



System-Backup / Restore

Change Password

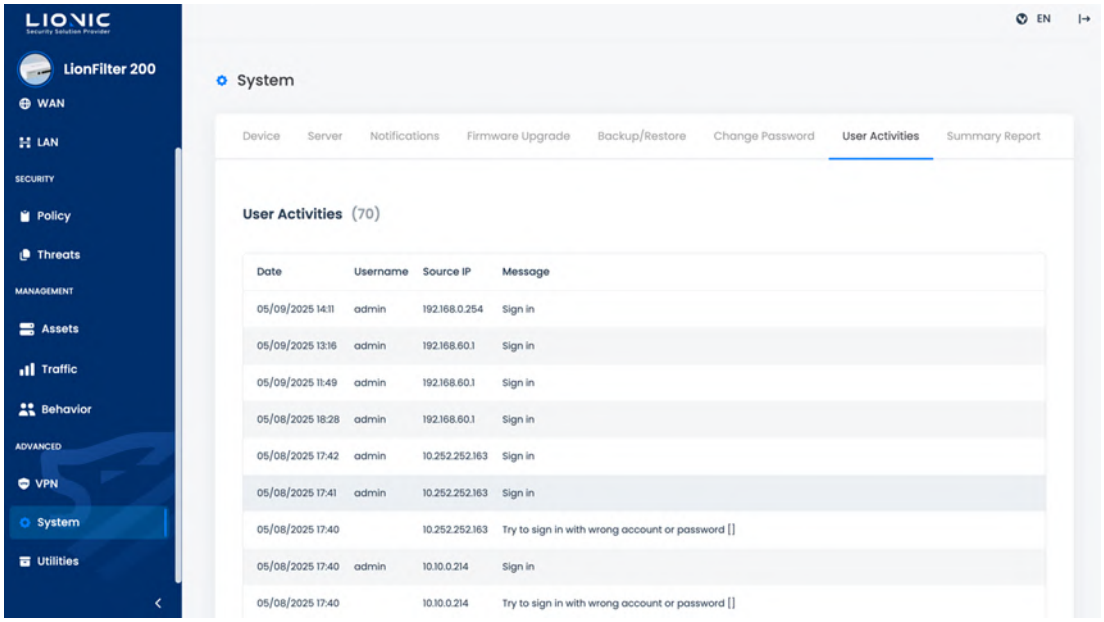
To change the login password of the web GUI, enter the new password to the input field and click [Apply].



System-Change Password

User Activities

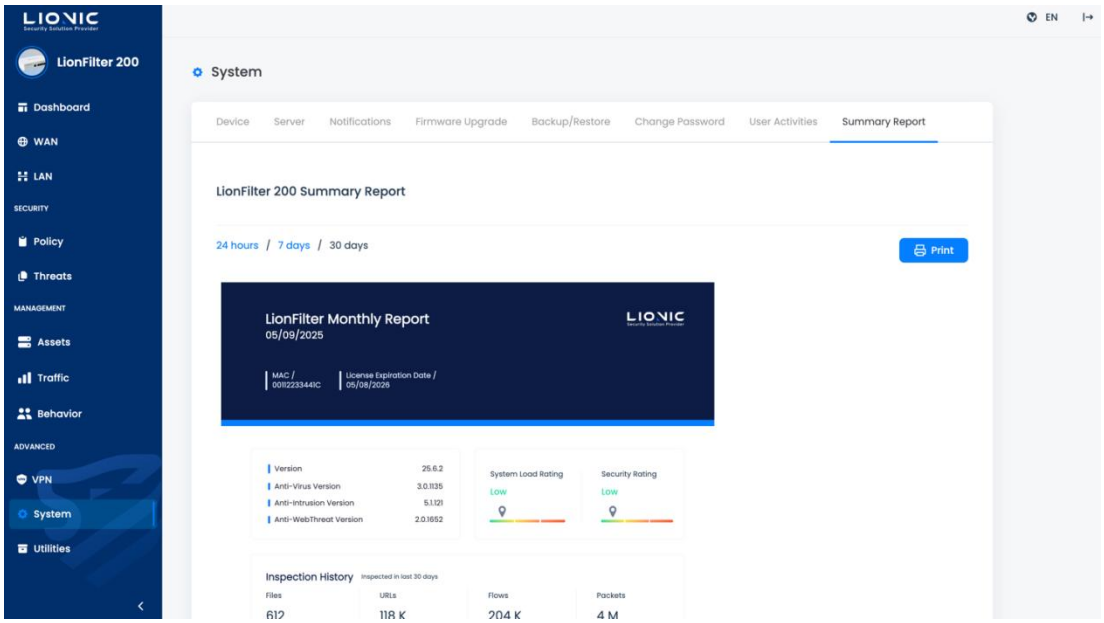
All configuration changes would be listed on [User Activities] tab.



System-User Activities

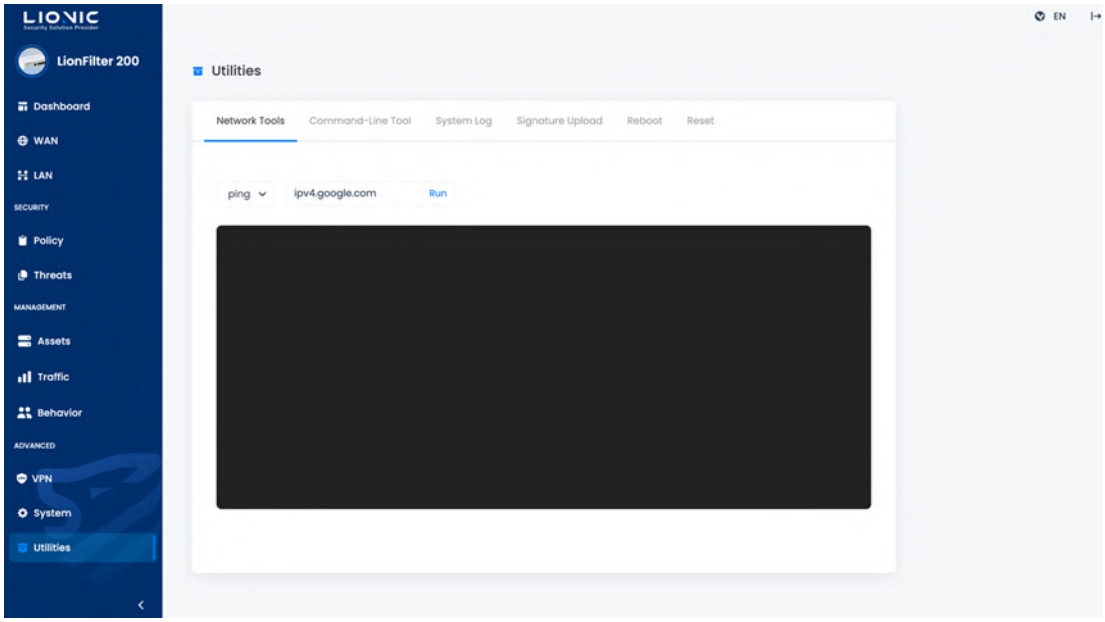
Summary Report

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



System-Summary Report

Utilities



Utilities

LionFilter 200 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.

  Enable Crash Reporter: If the system crashes unexpectedly, send a crash report to help us diagnose the problem.
- **Signature Upload:** Upload signatures manually when troubleshooting.
- **Reboot:** Reboot LionFilter 200 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, LionFilter 200 would automatically download and update the signature.

LionFilter 200
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.