

# Web GUI User Manual LionFilter 200

Version 1.0 Released on May 2025





# LionFilter 200 User Manual

Copyright © 2025, Lionic Corp.; all rights reserved.

## Trademarks

Lionic is trademarks of Lionic Corp.

WireGuard is registered trademark of Jason A. Donenfeld.

No-IP is registered trademark of Vitalwerks Internet Solutions, LLC.

# Disclaimer

Lionic provides this manual 'as is' without any warranties, either expressed or implied, including but not limited to the implied warranties or merchantability and fitness for a particular purpose. Lionic may make improvements and/or changes to the product(s), firmware(s) and/or the program(s) described in this publication at any time without notice. This publication could contain technical inaccuracies or typographical errors. Changes are periodically made to the information in this publication; these changes are merged into new editions of this publication.

# Technical Support Lionic Corporation

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

1



# Content

Access Web GUI and Connect to the Network	4
Overview	6
Dashboard	8
WAN	10
Configuration	
Remote Control	
LAN	13
Connection Mode	
LAN	14
DHCP	15
Port Forwarding	16
Static Route	16
Policy	17
General	
Anti-Virus, Anti-Intrusion, Anti-WebTheat	
Anti-Region	21
Anti-Spam	21
Firewall	23
Exceptional Websites	24
SSL / TLS Inspection	25
Threats	27
Assets	29
Traffic	30
Monitor	
QoS	
Behavior	22
Policy	

Events	36
VPN Server	37
WireGuard VPN	37
IPSec Site-to-Site VPN	39
System	41
Device	41
Server	43
Notifications	46
Firmware Upgrade	47
Backup / Restore	48
Change Password	49
User Activities	50
Summary Report	51
Utilities	52



# 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.

	Welcome to LionFilter 200	<b>⊘</b> ≌⇔
LionFilter 200 Secure your network against Virus,	<b>登入</b> 請輸入您的密碼	
intrasions, and web threats.	£λ	
版本 25.6.2		

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.

			S EN
LionFilter 200	WAN		
Dashboard	Configuration - Remote Control		
wan	Configuration Remote Control		
# LAN	WAN IPv4 Configuration		
SECURITY	-		
🎽 Policy	Connection	Auto	~
🕒 Threats	DNS	e.g. 8.8.8.8	
MANAGEMENT			
Assets			
II Traffic	WAN IPv6 Configuration		
Behavior	Connection	Auto	~
ADVANCED	DNS	e.g. 2001:4860:4860::8888	
VPN			
🗘 System			
Utilities	VLAN		
2/1	Enabled		

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

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.

curity Solution Provider								© EN
LionFilter 200	Inspection	n History Inspected Fro	m Last Systen	n Up				
Dashboard								
WAN	-	42/ Files	C	ISK URLS	at	3IK Flows	1	594K Packets
AN								
ſΓY	Security				Top Threat	s		All 🗸
Policy	,							
hreats		Anti-Virus	Statu	is 💽	Signature ID	Туре	Count	Message
GEMENT		0 Threats Detected	Actic	n Destroy	8060000101	Intrusion	25	TCP SYN Port Scan Lv1: 10 ports within 30 s
Assets					8401714009	Intrusion	2	SQL SQL Injection
Traffic		Anti-Intrusion	Statu	n Block				
Behavior		OI Imedia perecied			8401710001	Intrusion	2	SERVER Joomla DT Register SQL injection of
ICED		Anti-WebThreat	Law		8100027101	Intrusion	2	SERVER-WEBAPP Joomla DT Register SQL i
PN	-	1 Threats Detected	Actic	n Block	1000000001003	Web	1	secure.elcar.org
ystem								
Itilities		Anti-Region						
	•	0 Threats Detected	Statu	is 💽				

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.



	Traffic Monitor Now Day Week	Information
snboara	Network Traffic Speed	
IN	252.4 Kine	myfilter /
C. I	202.4 Nopa	MAC / 00112233441C
	201.9 Rops	License Expiration Date / May 8th, 2026 at 8:33:25 AM
	ют. ч Кора	View Details >
cy		
ats	50.5 Kbps	
	02:55 03:17 03:40 04:02 04:25 04:47 05:10 05:32 05:55	System Time May 9th, 2025 14:05:50
IENT	Download     Upload	System Up Time 1 day 2 hours 13 minutes 7 second
sets	Natural Traffic Volume	
offic	Network Inditic Volume	Memory Usage Storage Usage
	157.7 KB	
navior	126.2 KB	
<b>b</b>	94.6 KB	CPU Usage
	63.1 KB	100% 80%
	31.5 KB	60% 40%
tem	02:55 03:17 03:40 04:02 04:25 04:47 05:10 05:32 05:55	20%
		04:56 05:03 05:11 05:18 05:28 05:33 05:41 05:48 0



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.

			© EN I→
LionFilter 200	WAN		
Dashboard	Configuration Remote Control		
🖶 WAN			
H LAN			
SECURITY	WAN IPv4 Configuration		
Policy	Connection	Static	
Threats	IP Address	Auto	
MANAGEMENT		Static	
🚍 Assets	Subnet Mask	PPPoE	
	Default Gateway	192.168.0.254	
** Bahmdar	DNS	8.8.8.8	
Benavior			
ADVANCED			
O VPN	WAN IPv6 Configuration		
System	Connection	Auto	
T Utilities	our notion.		
	DNS	e.g. 2001:4860:4860:8888	
<			

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].

					O EN	→
LionFilter 200	WAN					
Dashboard	Configuration Rem	ote Control				
🕀 WAN						
H LAN	DDNS	Remote access LionFilter easily with an easy to ren	ember hostname.			
SECURITY	DDNS	which points to your dynamic IP address with Dyna	mic DNS.			
🗎 Policy		Enabled				
l Threats	Provider	No-IP (www.no-ip.com)				
MANAGEMENT	Hostname/Domain					
Assets	Username					
II Traffic	Password	Enter your password		Apply		
Et Behavior						
ADVANCED	ACI	To access this web interface from a public IP, pleas	e add the IP			
VPN	ACL	address to Access Control List (ACL).				
System		Enabled		+ Add		
Utilities		Advanced >				
				Apply		
<						

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.
- 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.

Behavior ARVANCED  VPN  System  Utilities	Secure Connection	Use HTTPS connection to access web user interface in order to protect sensitive information, such as login password. Use secure connection only	
<			



## **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.

LIONIC				
Security Souties Provider	₩ LAN			
🖬 Dashboard		and a state backs		
⊕ wan	Mode LAN DHCP PORTH	orwaraing static route		
H LAN				
SECURITY				
Policy		Connection	Mode	
🕒 Threats				
MANAGEMENT		۲		
Assets		Bridge	Router	
II Traffic	Wh model	en ISP provides a m+router or a router	When ISP provides a modem only	
<b>E</b> Behavior				
ADVANCED				
VPN		Apply		
System				
🖬 Utilities				
<				



## - 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.

				♥ EN I→
LionFilter 200	H LAN			
Dashboard	Mode LAN DHCP Part Forwarding Static Rout	re		
⊕ WAN				
H LAN	LAN ID Configuration			
SECURITY	LANIF Configuration			
Policy	IP Address	10.254.254.254		
🕒 Threats	Subnet Mask	255.255.255.0/24	~	
MANAGEMENT	Advanced ~			
- Assets	Routing without NAT			
II Traffic	Enabled			
Behavior	IP Address	192.168.1.2		
ADVANCED	Subnet Mask	255.255.255.0/24	~	
VPN	Use DHCP server in non-NAT routing subnet			
System			Apply	
T Utilities				
<				

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.

		O EN I-
LionFilter 200	H LAN	
🖬 Dashboard	Mode LAN DHCP Port Forwarding Static Route	
⊕ WAN		
∺ LAN	DHCP Server Configuration	
SECURITY		
Policy	Enabled	
Threats	Stort IP 10.254.254.1	
MANAGEMENT	End IP 10.254.254.253	
Assets		
II Traffic		
Rehavior	DHCP Reservations + Add New Rule	
ADVANCED		
C VPN	MAC IP Address Description(optional)	
System	annhy	
<ul> <li>Utilities</li> </ul>		
<		

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.

LIONIC Security Solution Provider							O EN	ŀ
LionFilter 200	H LAN							
Dashboard	Mode LAN DHC	P Port Forwarding	Static Route					
⊕ wan								
H LAN	Port Forwarding					t. Add New Dule		
SECURITY						+ Add New Role		
🖆 Policy	External Port	Internal Port	Internal IP	Protocol	Description (option	al)		
le Threats	External Port	internalitort	internarie	FIOLOCOI	Description(option			
MANAGEMENT	827	109	192.168.70.215	вотн 🗸		0		
📑 Assets						Apply		
II Traffic								
Behavior								
ADVANCED								
VPN								
• System								
Utilities								
<								

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.

					© EN
LionFilter 200	H LAN				
🖬 Dashboard	Mode LAN DHCP Por	Forwarding Static Route			
Ð WAN					
t LAN	Static Route Setting View R	outing Table		+ Add New Rule	
CURITY					
Policy	Network Address	Netmask	Gateway	Interface	
Threats					
INAGEMENT	192.168.0.0	255.255.255.0	192.168.0.254	LAN 🗸 🖸	
Assets				Apply	
Traffic					
Behavior					
OVANCED					
VPN					
System					
10000					
Utilities					
<					

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.

LIONIC Becurity Selution Provider		O EN	→
LionFilter 200	Policy		
Dashboard WAN UN LAN LAN COURTY Policy Threats MUMADURIT	General       Anti-Virus       Anti-Intrusion       Anti-WebThreat       Anti-Region       Anti-Spam       Firewall       Exceptional URL/IP       SSL / TLS Inspection         Packet Scan Mode                                    SSL / TLS Inspection          Packet Scan Mode                  Secondary Se		
Assets  III Traffic  Behavior  Advanced  VPN	Advanced SMB Deep Scan		
System       Utilities			

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 Only /	Log Only /
ACTION	Log and Destroy File	Log and Block	Log and Block
	- Scan Files with Cloud	- Block Brute-force attacks	- Configure External
	Virus Database	- Block Protocol Anomaly,	Database for
Advanced	- Detect New Viruses	- Block Port Scan and DoS Attacks,	Malicious Webpages
	with Al	- Keep PCAP when a threat is	- External Database
		detected	
Whitelict	View and remove	View and remove whitelist rule	View and remove
whitenst	whitelist rule	view and remove whitehst fule	whitelist rule

LIONIC Security Solution Provider		O EN
LionFilter 200	Policy	
🖬 Dashboard	General Anti-Virus Anti-Intrusion Anti-WebThreat Anti-Region Anti-Spam Firewall Exceptional URI //P SSI / TIS Inspection	
⊕ wan		
Ħ LAN	General	
SECURITY	General	
Policy	Enabled	
🕒 Threats	Action Log and Destroy File 🗸	
MANAGEMENT		
📑 Assets	Advanced	
II Traffic	Scan Files with Cloud Virus Database Connected	
L Behavior	Scanning files with the cloud virus databasecould make sure that the file is protected sufficiently, but may affect interact speed sometimes	
ADVANCED	our may anoun meaner apout aonainnea.	
VPN	Detect New Viruses with Al	
System	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]	
Utilities	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 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.

	Utilizing AI engines to analyze domain name	es for detecting malicious websites usi	ng dynamic URLs.	
LionFilter 200	External Database			
a Dashboard				
€ WAN	Database URL	URL		
E LAN	HTTP Basic Auth			
CURITY		Username		
Policy		Password	**	
Threats	Update Frequency	1 hour	~	Apply
ANAGEMENT				
Assets	Last Update	May 9th, 2025 at 2:21:59	PM	Update Now
I Traffic	Data Quantity	0		
Behavior	Export Current Database	Export		
WANCED				
VPN				
System	Whitelist			
Utilities				
<				

#### 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.

		O EN	I→
LionFilter 200	Policy		
🖬 Dashboard	General Anti-Virus Anti-Intrusion Anti-WebThreat Anti-Region Anti-Spam Firewall Exceptional URI //P SSI / TIS inspection		
⊕ wan	annen one nee neenen one neenen one neenen geve		
# LAN			
SECURITY	General		
Policy	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 UTE data available from https://ite.jp2location.com.		
🕒 Threats	Enabled		
MANAGEMENT			
Resets	Select the regions you want to block		
II Traffic	Block incoming connections from these regions:		
Le Behavior	Asia		
ADVANCED	People's Republic of China (CN)		
C VPN	Block outgoing connections to these regions:		
Ø System	Asia		
T Utilities	People's Republic of China (CN)		
<	Whitelist		

**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.
- [III-URL] : The email content contains a malicious URL.
- [Virus] : The email attachment contains a virus.



		O EN I→
LionFilter 200	Policy	
🖬 Dashboard	General Anti-Virus Anti-Intrusion Anti-WebThreat Anti-Region Anti-Spam Firewall Exceptional URL/IP SSL/TLS Inspection	
⊕ WAN		
🕂 LAN	Canadra	
SECURITY	General	
Policy	When [Anti-Spam] is enabled, the emails "Subject" field will be labeled according to the scan results:	
Threats	[spam] : Spam content     [iii-uru] : Malicious URL detected in content	
MANAGEMENT	[Virus] : Virus detected in attachment	
Assets		
II Traffic	ciuured	
Behavior	Filtering Level	
ADVANCED	Standard	
VPN	Use balanced criteria to filter out spam emails while ensuring legitimate emails are not misjudged.	
Ö System	Strict	
	Use more aggressive ways to filter out spam emails, including suspicious ones.	
- ounties		
<	Trusted Sender	
<	Trusted Sender	

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.

		O EN	1-
LionFilter 200	Policy		
Dashboard	General Anti-Virus Anti-Intrusion Anti-WebThreat Anti-Region Anti-Sparm <b>Frewall</b> Exceptional URI/IP SSI/TISInspection		
⊕ wan			
H LAN			
SECURITY		W RUIE	
Policy			
📮 Threats	Name Enabled Log Protocol Source IP Source Port Destination IP	×	
MANAGEMENT	New Rule ANY ANY ANY ANY		
Assets	Destination Port Action Schedule Every Week From To		
Behavior		vlag	
ADVANCED			
VPN			
System			
T Utilities			
<			

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.

LIONIC	© EN	→
ionFilter 200	Policy	
a Dashboard	General Anti-Mine Anti-Julianice Anti-MohThront Anti-Banice Anti-Score Einsteil Scorehionet 100/10 001 / 110 Inspection	
wan	орници, илистикия илистикивния илистикали илистикули илистикуран платиян <b>скорлонов илуте</b> ексутся наризнол	
H LAN	· · · · · · · · · · · · · · · · · · ·	
SECURITY	Allowed Blocked tog 🕥	
Policy	+ Add + Add	
Threats		
MANAGEMENT		
na Assets		
II Traffic		
LL Behavior		
ADVANCED		
• VPN		
O System		
🖬 Utilities		
<	1	

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:

- 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.

LIONIC		© EN I→
ConFilter 200	Policy	
Dashboard	General Anti-Virus Anti-Intrusion Anti-WebThreat Anti-Region Anti-Spam Firewall Exceptional URI/IP SSL/TLS Inspection	
⊕ wan		
H LAN	SSI / TIS instantion	
SECURITY	Enable SSL / TLS inspection to protect your device when browsing HTTPS websites.	
Policy	Reminder: Enabling this function will affect internet speed, may make some applications unavailable. This function only works when VLAN is disabled.	
Threats	Enabled	
MANAGEMENT	HTTPS Port 443 Apply	
assets		
II Traffic	Whitelist	
22 Behavior	Website Category Website Address	
ADVANCED	Finance and Insurance	
VPN	Health and Medicine	
• System		
To Utilities		
<	Certificate	

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.

							O
ConFilter 200	Threats						
🖬 Dashboard	Anti-Vinus Anti-Intrusion	Anti-WehThreat Anti-Peason Fire	wall Exceptional UP	/ip			
€ WAN		-	nai exceptional en				
å LAN	Anti-Intrusion (31)					J. Ex	port as CSV
CURITY						_	
Policy	Date Severity	Message	Source IP Source P	ort Destination IP	Destination Port Region	Protocol	MAC
Threats	05/09/2025 11:10 🕕 Low	TCP SYN Port Scan LvI: 10 ports within 30 seconds	192.168.110.210 58894	192.168.8.84	5060	TCP	D45D64C2B0
AGEMENT	05/09/2025 11:00 (] Low	TCP SYN Port Scan LvI: 10 ports within 30 seconds	192.168.8.35 49662	192.168.8.84	5060	TCP	D45D64C2B0
Assets	05/09/2025 07:02 🕕 Low	TCP SYN Port Scan Lv1: 10 ports within 30 seconds	192.168.110.210 37826	192.168.8.84	5060	TCP	D45D64C2B08
Traffic	05/09/2025 08:59 🕕 Low	TCP SYN Port Scan LvI: 10 ports within 30 seconds	192.168.8.35 58538	192.168.8.84	5060	TCP	D45D64C2B08
Behavior	05/09/2025 03:00 (]) Low	TCP SYN Port Scan Lvl: 10 ports within 30 seconds	192.168.110.210 36416	192.168.8.84	5060	TCP	D45D64C2B08
NNCED	05/09/2025 02:51 0 low	TCP SVN Port Scan Lvi: 10 ports within 30 seconds	192 168 8 35 37542	192 168 8 84	5060	TCP	D45D64C2808
Svetem		TOD CALIFIC Care 1 & 10 and a within To	100180 10000 44000	100.000.0.0	5050	100	DAEDEAGOS
Itilities	09/08/2029 22:55 (1) Low	וטר אזא אטוז Scan LVI: וע ports within 30 seconds	182.188.110.210 44620	192.168.8.84	5000	ICP	045064C2B08
Junites -	05/08/2025 22:50 () Low	TCP SYN Port Scan Lvl: 10 ports within 30 seconds	192.168.8.35 34242	192.168.8.84	5060	TCP	D45D64C2808
<	05/08/2025 18:40 🕕 Low	TCP SYN Port Scan LvI: 10 ports within 30 seconds	192.168.110.210 38364	192.168.8.84	5060	TCP	D45D64C2B08



- **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.

LIONIC Threat Encyclopedia	
	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 LionFilter 200, clicking [PCAP] > [Download] allows for packet download for further analysis.

IONIC												ø
LionFilter 200	• Threats											
ashboard	Anti-Maria Anti-Internio		do Theorem	Lett Dealer	fraunt from	at land 11	er 14					
AN		1 100-111	ionniou.	Hard and Port	TITVITUE EALS	00011010	url n.					
N (	Anti-lotusion (21)											dian CRV
	Anti-introsion (31)										G. Depo	il dal con
licy		Source IP	Source Port	Destination IP	Destination Port	Region	Protocol	MAC	Signature ID	Action	PCAP	Whitelist
eats	Lvi: 10 ports within 30 seconds	192.168.110.210	58894	192168.8.84	5060		TOP	D45064C28082	8060000101	100	Download	+
ent -	Lvt 10 ports within 30 seconds	192.168.8.35	49662	192.168.8.64	5060		TOP	D45D64C28082	8060000101	100	Download	+
ets	Lvl: 10 ports within 30 seconds	192,168,110,210	37826	192.168.8.84	5060		TOP	D45064C28082	8060000101	100	Download	+
ffic	Lut 10 mosts within 30 seconds	102 168 8 35	54538	1021688844	5050		108	045064028082	806000000	100	Download	Ē
iavior												
¥	Lvt: 10 ports within 30 seconds	192,168,110,210	36416	192.168.8.84	5050		TOP	D45D64C28082	8060000101	100	Download	(+)
	Lvit 10 ports within 30 seconds	192,168.8.35	37542	192168.8.84	5060		TCP	D45064C28082	8060000101	100	Download	+
tem	Lvt. 10 ports within 30 seconds	192.168.110.210	44820	192168.8.84	5060		TCP	D45064C28082	8060000101	100	Download	+
ities	Lvt 10 ports within 30 seconds	192,168,8.35	34242	192168.8.84	5060		TOP	D45064C28082	101000008	100	Download	+
	LVI: 10 ports within 30 seconds	192168110.210	38364	192168.8.84	5060		TOP	D45064C28082	8060000101	100	Download	( <b>+</b> )

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 device:	s and allow or block assets from a	ccessing the network. After [Block Ne <sup>,</sup>	w Assets] is enabled, if an
unidentified asset is detected, it will be blocked fr nformation, but the identification process may ir	om accessing the network. Enabli npact network usage.	ng [Advanced Device Identification] v	vill provide more asset
SIOCK NEW ASSETS			
Type Name	MAC	IP	
Online (0)			
	No other members		
Offline (409)			
AD-DC02	000C290B129A	192.168.0.202	<b>I</b>
VMware Ubuntu Device	000C290CBE45	10.10.1.247	<b>I</b>
VMware Ubuntu Device	000C290CBE4F	192.168.1.247	<b>I</b>
VMware Virtual Machine	000C2911BFA5	10.10.27.192	(o) []
	Asset Management can list identified LAN device unidentified asset is detected, it will be blocked fr nformation, but the identification process may in Advanced Device Identification           Advanced Device Identification         Stock New Assets         Online (0)         Offline (409)         AD-DC02         VMware Ubuntu Device         VMware Ubuntu Device         VMware Virtual Machine	Asset Management can list identified LAN devices and allow or block assets from a unidentified asset is detected, it will be blocked from accessing the network. Enablis information, but the identification process may impact network usage. Advanced Device Identification C Block New Assets C Block N	Asset Management can list identified LAN devices and allow or block assets from accessing the network. After [Block New anidentified asset is detected, it will be blocked from accessing the network. Enabling [Advanced Device Identification] v nformation, but the identification process may impact network usage. Advanced Device Identification <b>MAC</b> IP Online (0) Type Name MAC IP Online (409) Children State Sta

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.

LIONIC Security Solution Provider						👁 en	1
⊖ LionFilter 200 ⊕ WAN	11 Traffic						
# LAN	Monitor QoS						
SECURITY							
Policy	Search		5 V. Add Filter			S View	
Threats	Туре Na	me	MAC	Download $\downarrow$	Upload 0		
MANAGEMENT	AD	-DC02	000C290B129A				
Assets	L VM	ware Ubuntu Device	000C290CBE45			•••	
11 Traffic	VM	ware Ubuntu Device	000C290CBE4F				
Behavior	VM	ware Virtual Machine	000C2911BFA5				
ADVANCED	UM	ware svn.lionic.com	000C291A1348				
• VPN	so	þ	000C291A3408				
System	VM	ware Ubuntu Device	000C292C8A69			····	
<b>T</b> Utilities	wir	-6U79KJDKO29	000C292EC0D6				
<	- <u></u>						

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.

LIONIC Security Solution Provider								O EN	l→
← WAN	I Traffic								
# LAN	Monitor QoS								
SECURITY									
Policy	QoS can prioritize LAN	devices and	allocate bandwidth based on their	priority.					
🕒 Threats	Enabled								
MANAGEMENT	Total Bandwidth	Download	1000 Mbps						
Assets		Upload	1000 Mbps						
11 Traffic	Priority Settings	Priority	Name	Min		Max			
Behavior		1	Priority 1	0	%	100	%		
ADVANCED		2	Priority 2	0	%	100	%		
VPN		3	Priority 3	0	%	100	%		
System		4	Priority 4	0	%	100	%		
T Utilities		5	Default	0	%	100	%		
<		6	Priority 6	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	%
	Б	Default	0	%	100	%
	6	Priority 6	0	×	100	x
	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.

Rules						+ Add New R
Name Qos 01	Enabled	Priority	Source IP 192.168.8.34	Destination IP	Destination Port ANY	
Name	Enabled	Priority	Source IP	Destination IP	Destination Port	
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.

		c	D EN	1
LionFilter 200	😫 Behavior Management			
Dashboard	Bolley Sunte			
⊕ wan				
# LAN				
SECURITY	Behavior Management can filter inappropriate websites and applications, and block connections to specified regions. Reminder: Rules at the top of the list have higher priority. If a connection matches the scope of a rule, no further rules will be evaluated.			
Policy				
Threats		+ Add New Rule		
MANAGEMENT	Branch A rule Enabled	00		
Assets	-			
Le Behavior	Branch B rule Enabled	0		
ADVANCED				
• VPN				
Ø System				
Utilities				
<				

**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.



acurity Solution Provider		O EN
LionFilter 200	💦 Behavior Management	
Dashboard		
WAN	Branch A rule 🖌	Go Back
LAN		
IRITY	Scope ©	+ Add New Rule
Policy		
Threats	Address ANY	×
AGEMENT		
Assets	Category Management ()	L. Add New Pute
Traffic	Cutegory management o	
Behavior	Category Advertisments and Pop-Ups Action Log and Block	
		×
+CED		×
IPN	Category Alcohol and Tobacco Action Leg and Block	×
vced IPN System	Category Alcohol and Tobacco Action tog and Block	×



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.

LIONIC	
	Anti-Region
	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
🖬 Dashboard	product includes instruction une data available from https://wei.psocduon.com.
⊕ wan	Euglied
H LAN	Select the regions you want to block 🕐
SECURITY	Block incoming connections from these regions:
🗎 Policy	Not set yet
🕒 Threats	Block outgoing connections to these regions:
MANAGEMENT	Not set yet
Resets	
II Traffic	Whitelist
21 Behavior	Add trusted IP addresses to the whitelist, then they would not be blocked by Anti-Region.
ADVANCED	IPv4 or IPv8 oddress + Add
VPN	
System	
T Utilities	Apply

Behavior Management -Policy-Anti-Region

**Step 1**: Enable Anti-Region.

**Step 2**: Click *i* 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.

						O EN
LionFilter 200	👪 Behavior Mo	nagement				
Dashboard	Policy Event					
⊕ wan						
# LAN	Events (427)					L Event as CEV
SECURITY	Events (+27)					S Export ds CSV
Policy	Date	MAC	Source IP	Name	Message	Action
📮 Threats	05/09/2025 14:5	3 D45D64C28082	10.254.254.209	Branch A rule	[Advertisments and Pop-Ups] http-inputs-notion.splunkcloud.com	BLOCK
MANAGEMENT	05/09/2025 14:5	D45D64C2B082	10.254.254.209	Branch A rule	[Advertisments and Pop-Ups] http-inputs-notion.splunkcloud.com	BLOCK
📑 Assets	05/09/2025 14:4	9 D45D64C2B082	10.254.254.209	Branch A rule	[Advertisments and Pop-Ups] http-inputs-notion.splunkcloud.com	BLOCK
II Traffic	05/09/2025 14:4	6 D45D64C28082	10.254.254.209	Branch A rule	[Advertisments and Pop-Ups] http-inputs-notion.splunkcloud.com	BLOCK
Eehavior	05/09/2025 14:4	3 D45D64C2B082	10.254.254.209	Branch A rule	[Advertisments and Pop-Ups] http-inputs-notion.splunkcloud.com	BLOCK
ADVANCED	05/09/2025 14:4	3 D45D64C2B082	10.254.254.209	Branch A rule	[Advertisments and Pop-Ups] events.split.io	BLOCK
VPN	05/09/2025 14:4	D45D64C28082	10.254.254.209	Branch A rule	[Advertisments and Pop-Ups] http-inputs-notion.splunkcloud.com	BLOCK
• System	05/09/2025 14:3	9 D45D64C2B082	10.254.254.209	Branch A rule	[Advertisments and Pop-Ups] ogads-paclients6.google.com	BLOCK
Utilities	05/09/2025 14:3	8 D45D64C2B082	10.254.254.209	Branch A rule	[Advertisments and Pop-Ups] o27075.ingest.sentry.io	BLOCK
	05/09/2025 14:3	8 D45D64C2B082	10.254.254.209	Branch A rule	[Advertisments and Pop-Ups] http-inputs-notion.splunkcloud.com	BLOCK
	< 1 2	3 4 5	6 7	43 >		10 🗸 1-10 of 427

Behavior Management - Events

Lionic Confidential 2025



# **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.

LIONIC			
LionFilter 200	• VDN		
E Dashboard	VPN		
0.000	WireGuard IPSec		
U WAN			
H LAN	Download and install WireGuard Client app to mobile device	es and setup with 1 of the following profile, then the mobile device	
SECURITY	Reminder: # DONS is needed for LionFilter, please set up DDNS	S before creating new VPN profiles.	
Policy			
P Threats	Enable VPN Server		
MANAGEMENT	After enabled, please visit http://10.107.211.1/otp/vpn and enter	er OTP after you connected VPN with WireGuard VPN client	
E Assets	- alido		
II Traffic			
L Behavior		+ Create New Profile	
ADVANCED	設定欄1 /	×	
O VPN			
• System	offune	10 VPN QR Code €. Download	
-			
- other			
ć			

**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 <u>https://myfilter.lionic.com/otp/vpn</u> 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.

		O EN
LionFilter 200	• VPN	
🖬 Dashboard	WireGuard IPSec	
⊕ wan		
# LAN		
SECURITY	216-10-216 ANM	
Policy	+ Create New Profile	
Threats	15.2	
MANAGEMENT	Enabled Connecting	
Assets	· · · · · · · · · · · · · · · · · · ·	
II Traffic		
Behavior		
DVANCED		
VPN		
System		
T Utilities		
<		

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

Name	LF_2	Authentication	Pre-shared Key o
Enabled		PSK	
IKE Version	IKEVI IKEV2		
		#Phase 1	
Network		Proposal	+ Add
Remote Address	1164 92147		Encryption AES256 $\circ$ Authentication SHA256 $\circ$ $\ddot{\Box}$
Normoto Addross	1.104.02.147	Diffie-Hellman Groups	s 32 31 30 29 21 20 19 18
Remote Subnet	10.254.254.0/24		17 16 15 ✓ 14 ✓ 5 2 1
Local Subpet	10216820/24	#Phase 2	
Local Subher	132.100.2.0/24	Proposal	+ Add
Authentication			Encryption AES256 $\circ$ Authentication SHA256 $\circ$ 🖞
Addientication		Diffie-Hellman Groups	32 31 30 29 21 20 19 18
Method	Pre-shared Key 0		
PSK		Key Lifetime(seconds)	86400



# System

## Device

	System		
LionFilter 200	Device Server Notifications Firmware Upg	rade Backup/Restore Change Password	User Activities Summary Report
Dashboard			
⊕ wan	License Management		
a LAN	License Status Activated		
ECURITY	License Expiration Date March 10th, 2026 at	3:55:54 PM	
Policy	Renewal Code	DDDD	Apply
Threats			
IANAGEMENT			
Assets	Date & Time		
Traffic	System Date & Time Sun Mo	y 11 00:24:18 CST 2025 (Asia/Taipei)	
Behavior	Time Zone Auto	~	
DVANCED	Automatically sync date & time with 0.oper	wrt.pool.ntp.org	
VPN	1.open	wrt.pool.ntp.org	
System	2.oper	wrt.pool.ntp.org	
Utilities	3.oper	wrt.pool.ntp.org	+ Apply

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:
- 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.



	Date & Time			
LionFilter 200	System Date & Time	Fri May 9 14:58:01 CST 2025 (Asi	a/Taipei)	
AN	Time Zone	Auto	~	
N	Automatically sync date & time with	0.openwrt.pool.ntp.org	Ŭ	
		1.openwrt.pool.ntp.org	Ŭ	
Y		2.openwrt.pool.ntp.org	0	
licy		3.openwrt.pool.ntp.org	n	+ Apply
ireats				
ireats IMENT				
ireats :MENT ssets				
ireats iment ssets raffic				
ireats iment ssets raffic ehavior				
reats мюл raffic ehavior	Management Port			
reats ment ssets raffic enhavior	Management Port			
reats mant ssots raffic ehavior to	Management Port Enabled	cannot connect to the internet. When	the Management	
reats ment ssots enavior to N stem	Management Port Enabled When enabled, the MGMT port (LAN Port 4) o Port function is disabled, it can be used as a	cannot connect to the internet. When	the Management	

System- Management Port

## Server

C LionFilter 200 O System			
Dashboard	Server Natifications Firmware Uparade Backup/Res	ore Change Password User Activities	Summary Report
⊕ wan			
SECURITY			
Policy CMS Ser	er Connected cmsdemo.cloud.lionic.com		
Threats Advance	d >		Apply
INAGEMENT			
Assets			
I Traffic			
Behavior URL	e.g. http://10.254.254.10:8888		Test Apply
VANCED			
VPN			
System			
Enabled Enabled			
Server IP	IPv4 or IPv6 address		
< Server Po	rt 514		

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	Advanced >				Apply
LionFilter 200					
⊕ WAN	SNMP				
H LAN					
SECURITY	Enabled				
🗑 Policy	Version	v2c	~		
Threats	Download MIB	J. Download			
MANAGEMENT					
🖁 Assets	SNMPv2c				
Traffic	Community Name	public			
Behavior					
DVANCED	IP Allowed List	IPv4		+ Add	
VPN					
🔅 System					Apply
Utilities					
<					

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.

LIONIC Security Solution Provider		٥	EN I→
← LionFilter 200	o System		
∺ LAN	Device Server	Notifications Firmware Upgrade Backup/Restore Change Password User Activities Summary Repo	ort
SECURITY			
🖞 Policy	Language	English 🗸	
Threats			
MANAGEMENT			
📑 Assets	Email Alert		
II Traffic	Send the report	every month every week every day when threats are detected	
<b>E</b> Behavior	SMTP Server	smtp.mail.com	
ADVANCED	SMTP Port	25	
I VPN	SMTP Account	user@mail.com	
O System	entri Hoceant		
🗃 Utilities	SMTP Password	Enter your password	
	Receiver	user@mail.com Test Apply	

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.

© EN I→
ade Backup/Restore Change Password User Activities Summary Report
Q: Upgrade Now
🗇 Upgrade Later
+ Upload

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.

		© EN I→
LionFilter 200	o System	
H LAN	Device Server Notifications Firmware Upgrade Backup/Restore Change Password User Activities S	Summary Report
SECURITY		
🗎 Policy	Backup Click "Backup" to download a tar archive of the current configuration files.	Backup
Threats		
MANAGEMENT	Olici, "Restore" to settere from a tex archive of the surgest	
Rests	Restore configuration files. Browse	Restore
II Traffic		
Et Behavior		
ADVANCED		
O VPN		
O System		
Utilities		
<		

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].

						© EN I→
⊖ LionFilter 200 ⊕ WAN	o System					
H LAN	Device Server Not	ifications Firmware Upgrade	Backup/Restore	Change Password	User Activities	Summary Report
SECURITY						
Policy	Change Password	8 admin				
Threats	New Password	Enter your password	¥			
MANAGEMENT	Confirm Password	Enter your password again	¥			Apply
Assets						
II Traffic						
Le Behavior						
ADVANCED						
© VPN						
<ul> <li>System</li> </ul>						
T Utilities						
<						

System-Change Password



# **User Activities**

LIONIC Security Solution Provider							© EN
LionFilter 200	• System						
⊕ WAN							
H LAN	Device Server	Notificat	tions Firm	vare Upgrade Backup/Restore Chang	ge Password	User Activities	Summary Report
ECURITY							
9 Policy	User Activities	(70)					
Threats	Date	Username	Source IP	Messoge			
ANAGEMENT	05/00/0005147	adasia	100100.0054	film in			
Assets	00/00/2020 14:11	Gumin	182.106.0.2.04	aign in			
I Traffic	05/09/2025 13:16	admin	192.168.60.1	Sign in			
. Dahardar	05/09/2025 11:49	odmin	192.168.60.1	Sign in			
Benavior	05/08/2025 18:28	admin	192.168.60.1	Sign in			
WANCED	05/08/2025 17:42	admin	10.252.252.163	Sign in			
VPN	05/08/2025 17:41	admin	10.252.252.163	Sign in			
System	05/08/2025 17:40		10.252.252.163	Try to sign in with wrong account or password []			
Utilities	05/08/2025 17:40	admin	10.10.0.214	Sign in			
c i	05/08/2025 17:40		10.10.0.214	Try to sign in with wrong account or password []			

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

LIONIC		© EN I→
LionFilter 200	Utilities	
Dashboard	Natural Task Commend line Test, Datase and Constructional Delant Dest	
🕀 WAN	Network roos	
H LAN		
ECURITY	ping v ipv4.google.com Run	
Policy		
Threats		
ANAGEMENT		
Assets		
Traffic		
Behavior		
WANCED		
VPN		
System		
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



© Copyright 2025 Lionic Corp. All rights reserved.

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

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