LIONIC
Security Solution Provider

User Manual

Central Management System

Version 2.0
Released on Jul 2024

Lionic Corp. www.lionic.com

CMS User Manual

Trademarks

Lionic and CMS are trademarks of Lionic Corp.

"WireGuard" is registered trademark of Jason A. Donenfeld.

No-IP is registered trademark of No-IP.com.

Disclaimer

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

Technical Support Lionic Corporation

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

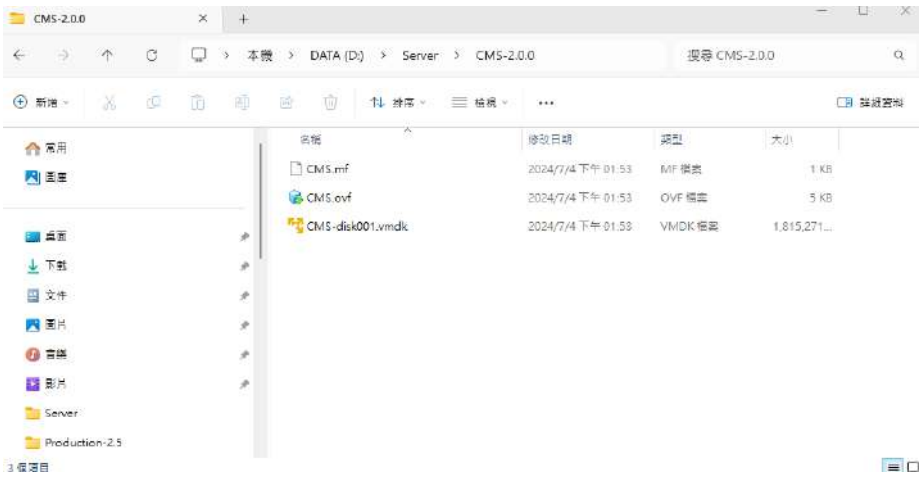
Content

Setup Steps

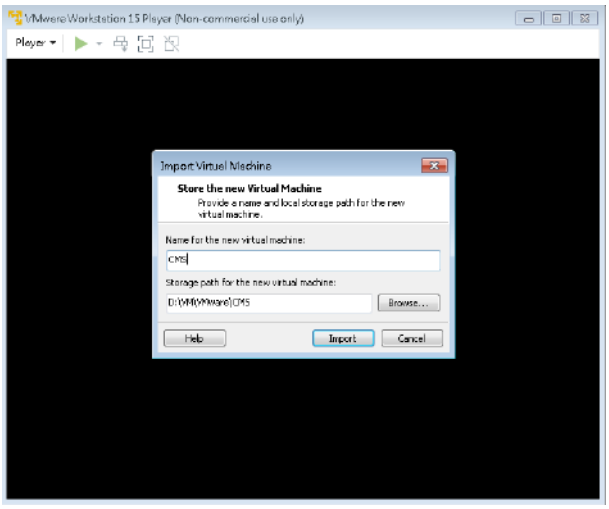
Installation Steps:

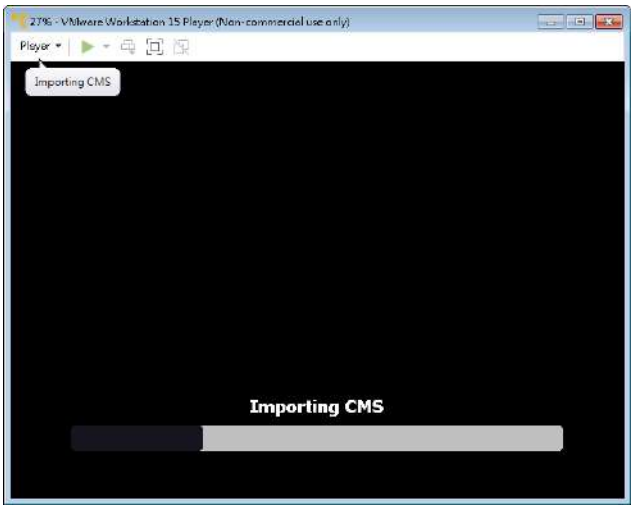
1. Download CMS VM installer

2. Select the CMS VM installer format

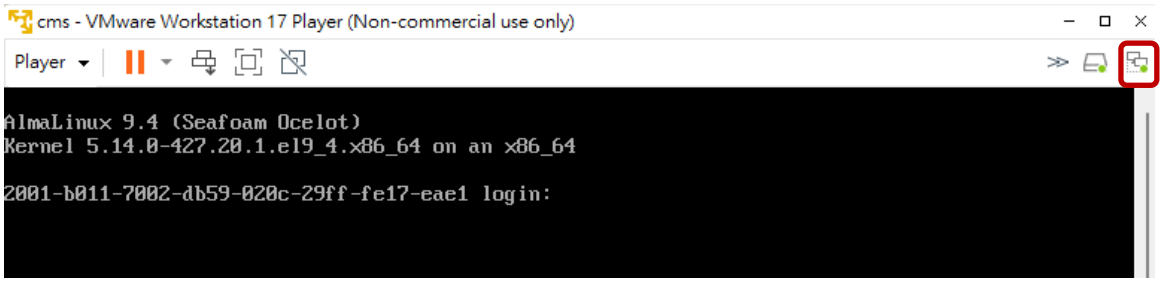


3. Create a VM name and import

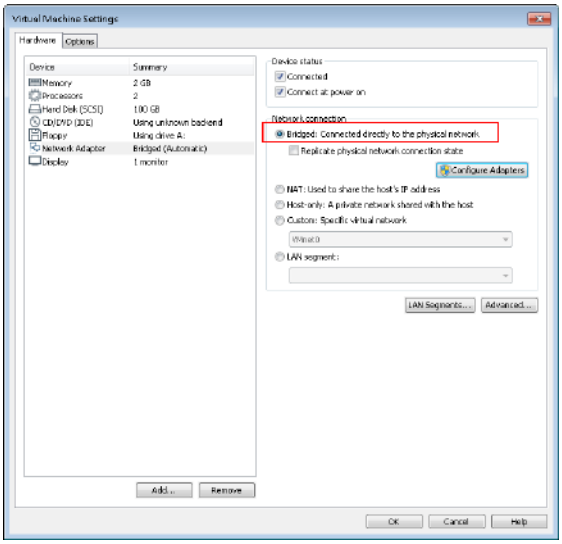


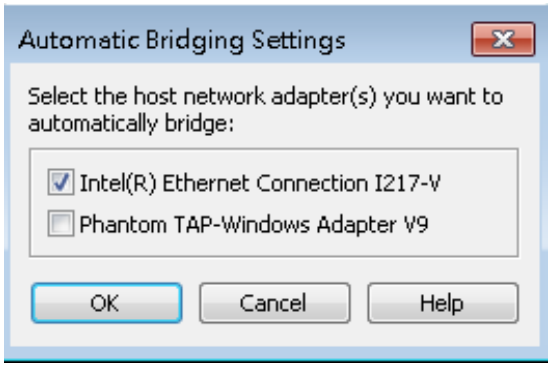


4. Right-click on the icon, select [Setting]



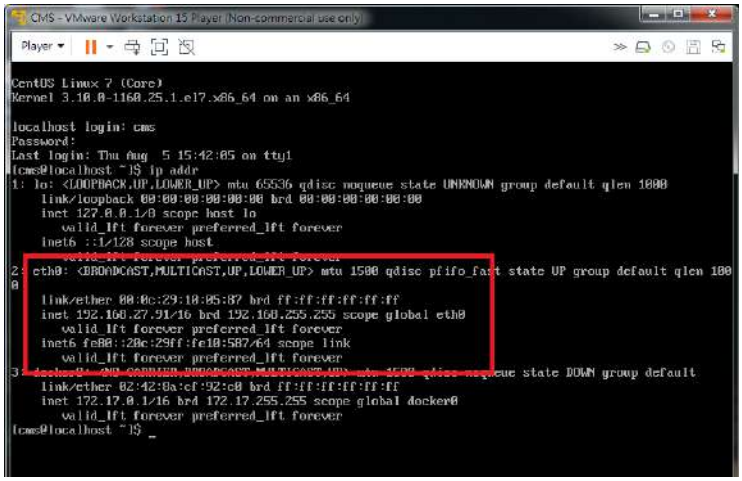
5. Choose connection mode, select network card





6. Log in (cms / cms5678)
   check network information

```
ip addr
```

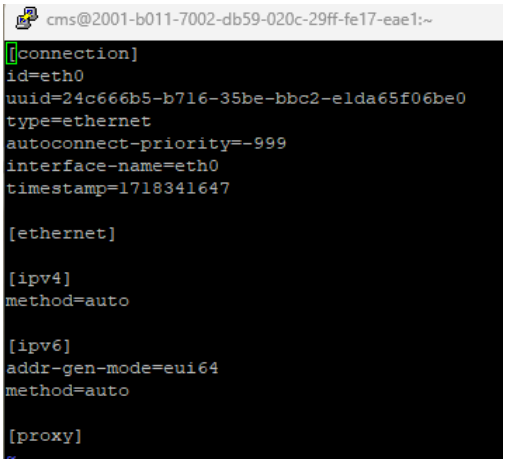


7. Change network settings

```
sudo vi /etc/NetworkManager/system-connections/eth0.nmconnection
```

   Restart network settings after changes

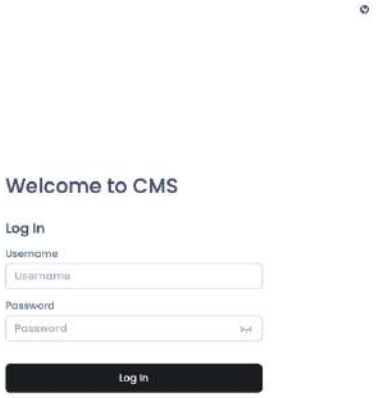
```
sudo nmcli c reload
sudo nmcli d reapply eth0
```



DHCP

Static IP

8. After setup is complete, open http://CMS_IP:4221 in a web browser to log in. Default credentials: cmsadmin / cmssecretpass



Upgrade steps

1. Navigate to the folder

```
cd /home/cms/cms
```

2. Put CMS-2.0.0.tar in VM
3. Import the file

```
docker load --input cms-2.0.0.tar
```

4. Change the file version

```
vi docker-compose.yml
```

```
```
image: cms:1.5.1 --> image: cms:2.0.0
```
```

5. Restart Docker to complete the process

```
docker compose up -d
```

Database backup and restore

1. Create database backup file/home/cms/mongodb/backup/data.gz by below commands.

```
cd mongodb
mkdir -m 777 backup
docker run --rm --network host -v $PWD/backup:/backup  mongo:3.6 mongodump
--authenticationDatabase cms -u cmsuser -p cmspass --archive=/backup/data.gz
--gzip --host localhost:27017 --db cms
```

2. Prepare backup file/home/cms/mongodb/backup/data.gz and use below command to restore database.

```
docker run --rm --network host -v $PWD/backup:/backup
mongo:3.6 mongorestore --authenticationDatabase cms -u
cmsuser -p cmspass --archive=/backup/data.gz --drop --gzip --host
localhost:27017 --db cms
```

Overview

Dashboard:

[Dashboard] displays the operational status and device information of the CMS management devices, including detection history, recent threats, threat statistics or rankings, threats counts , ranking of attacked devices.

Devices:

[Devices] displays the devices configured to connect to CMS management.

Groups:

- **Groups:** [Groups] feature allows grouping of different devices.
- **Policy Template:** Create execution rule templates for various security protection features, including antivirus systems, intrusion prevention, malicious website blocking, and firewalls.
- **Whitelist:** When the security protection features of the CMS management device compromise safe files or block trusted connections, the whitelist feature can be used to restore normal operation.

Threats:

Display execution records of various security protection features.

System:

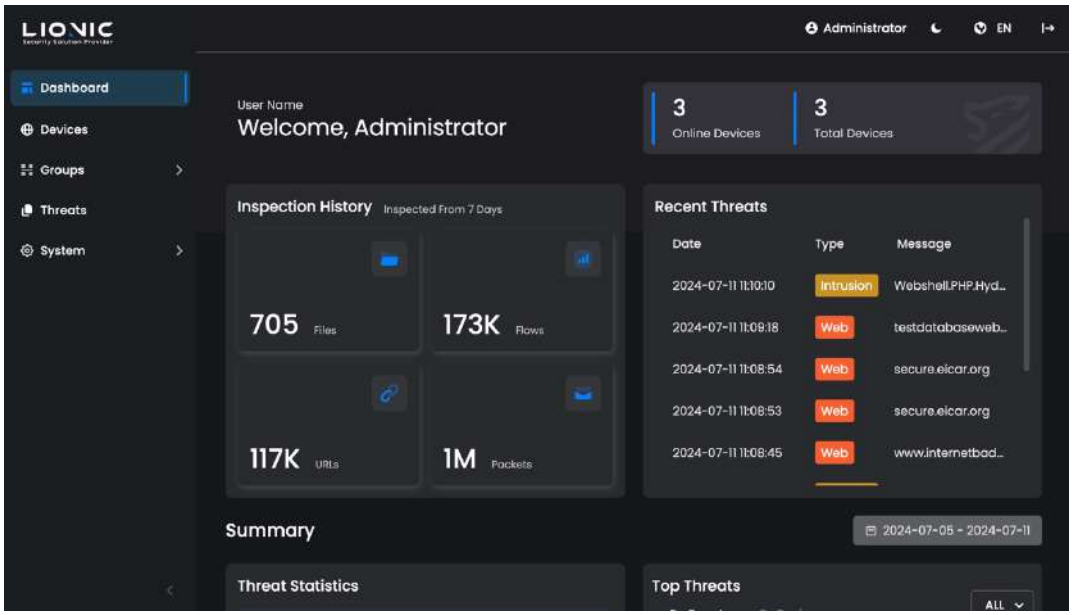
- **Users:** [Users] page allows adding users and establishing account passwords and permissions control.
- **User Activities:** [User Activities] page lists all configuration changes made by CMS administrators in the web control interface.
- **Notification:** [Notification] Function can send threat information via email to the designated mailbox when the CMS detects a cybersecurity threat on the managed devices. Additionally, it can periodically send information on inspection history, threat statistics, system anomaly records, etc, to the designated mailbox.
- **Signatures:** When users require access to the CMS firmware and feature code update server due to network connection restrictions, they can upload and manage firmware and feature code updates through this page.
- **Portal Users:** Administrators can add users to the portal and assign specific devices, enabling them to manage CMS functionalities.

Dashboard

The operational status and device information of the CMS management devices will be displayed here, including detection history, recent threats, threat statistics or rankings, threats counts , ranking of attacked devices.

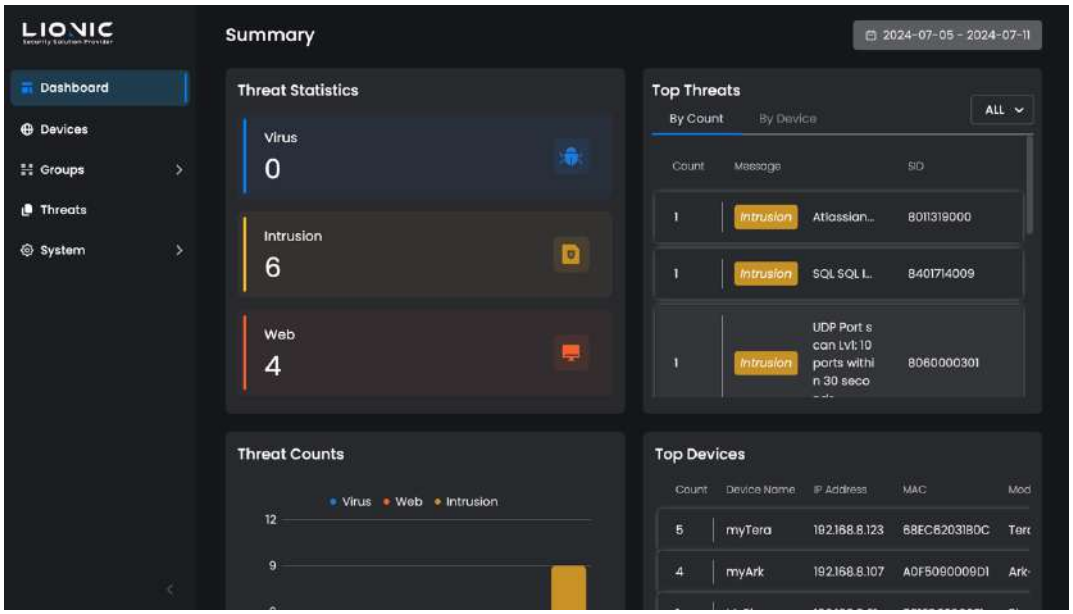
Inspection History：Displays the number of files, connections, packet flows, and packets detected by the CMS management device.

Recent Threats：Displays the latest threat data of the CMS management device.



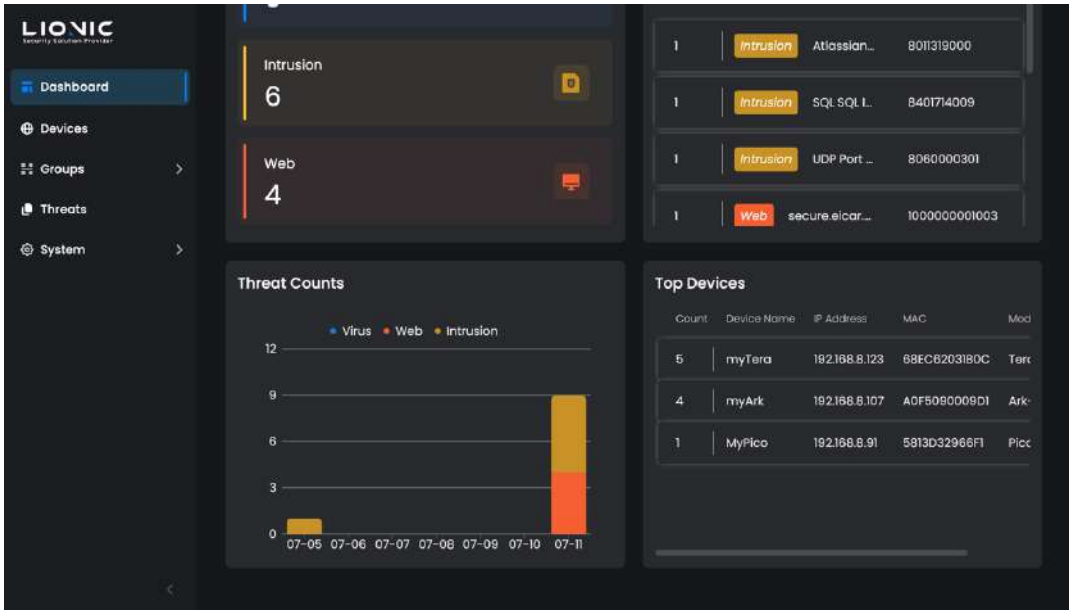
Threat Statistics：Display the recent number of threat events detected by the CMS management device.

Top Threats：Compile security logs detected by various security protection features of the CMS management device, list all or various threat rankings based on detection frequency, and rank devices by the number of attacks.



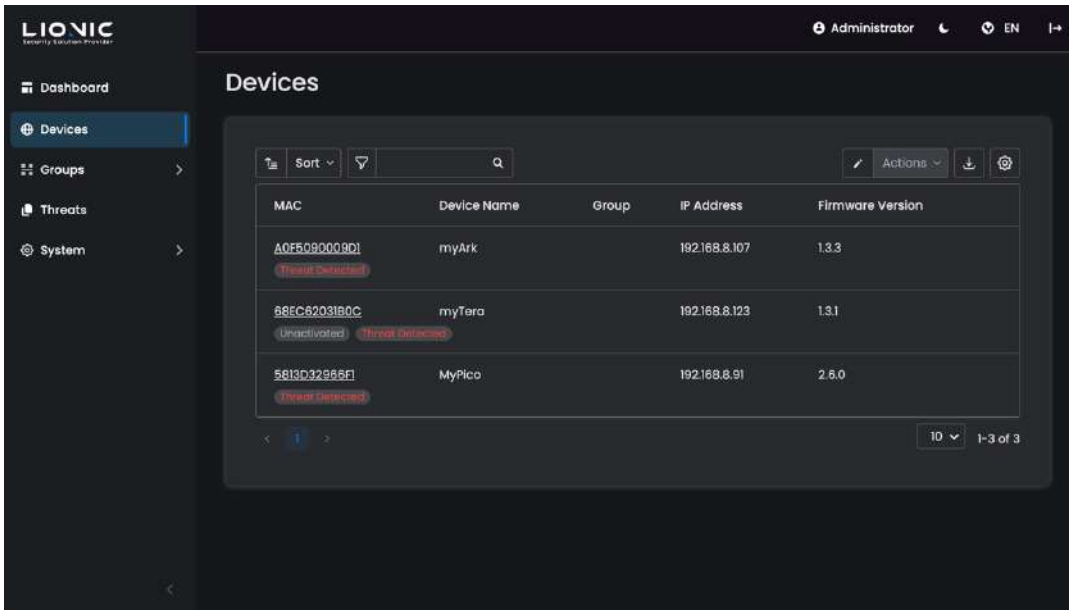
Threat Counts：Aggregate the daily count of security logs detected by each security protection feature.

Top Devices：Aggregate security logs detected by each security protection feature and list the top ten devices ranked by the number of attacks.



Devices

On the [Devices] page, display devices connected to the CMS, allowing users to remotely manage them through CMS.

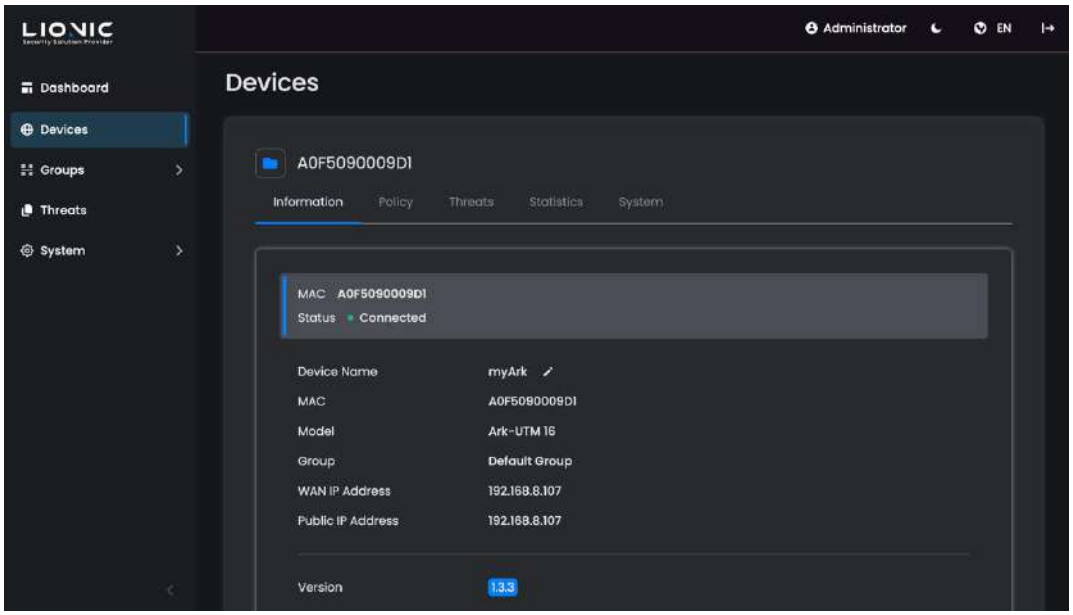


- **Sort**：Click to change the order (ascending/descending) ，Click [Sort] to select a category.
- **Filter**：Click the input box to filter devices.
- **Actions**：Click Select devices, then click [Actions] to choose an operation.
- **Sync Group Policies**（You can select devices or perform a synchronized action if changes are configured across all devices）：After setting up group functionality, this feature needs to synchronize group devices.
- **Activate License**：When using the device for the first time, ensure it's connected to the internet environment. Enter the authorization activation code and extension code to activate the license, ensuring the device provides complete security protection functionality.
- **Renewal License**：The CMS management device will display a reminder 30 days before the license expires. Please promptly complete the subscription renewal to obtain the extension code. After entering the extension code, the license period can be extended.
-
-

- **Upgrade Firmware** (You can perform a synchronized action across all devices that have not been updated to the latest version without selecting individual devices)：Update the devices to the latest version.
- **Update Signature** (Without selecting devices, perform synchronized action on devices that have not been updated to the latest version) : Devices will immediately check and download the latest signatures from the signature server.
- **Delete Device**：Delete management device.
- **Export as CSV**：Export the device list as a CSV file.

Device information :

In the [Devices], clicking on a device's MAC address allows you to access the device, where you can view device information, adjust protection settings, and more.



- **Whitelist**：When the security protection features of the CMS management device disrupt secure files or block trusted connections, you can restore normal usage through the whitelist functionality.
  - Add whitelist rule：Please search for the disrupted or blocked event records on the [Threats] page, then click [+] to add to the whitelist.
  - Delete whitelist rule：Navigate to the [Policy] page and delete the specified whitelist rule.

  ※ This whitelist is configured for individual device settings and is not a global whitelist.

- **After modifying individual device security rules, the changes take effect immediately without the need to [Sync Group Policies] settings.**

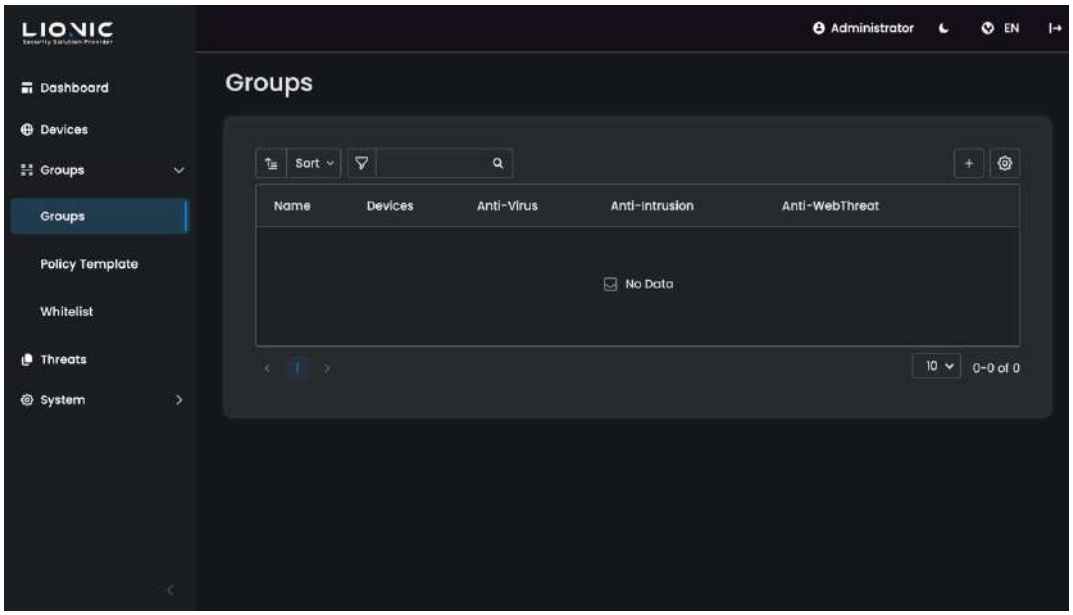
- **Please refer to the device user manual for detailed explanations on Policy and Threats.**

Groups

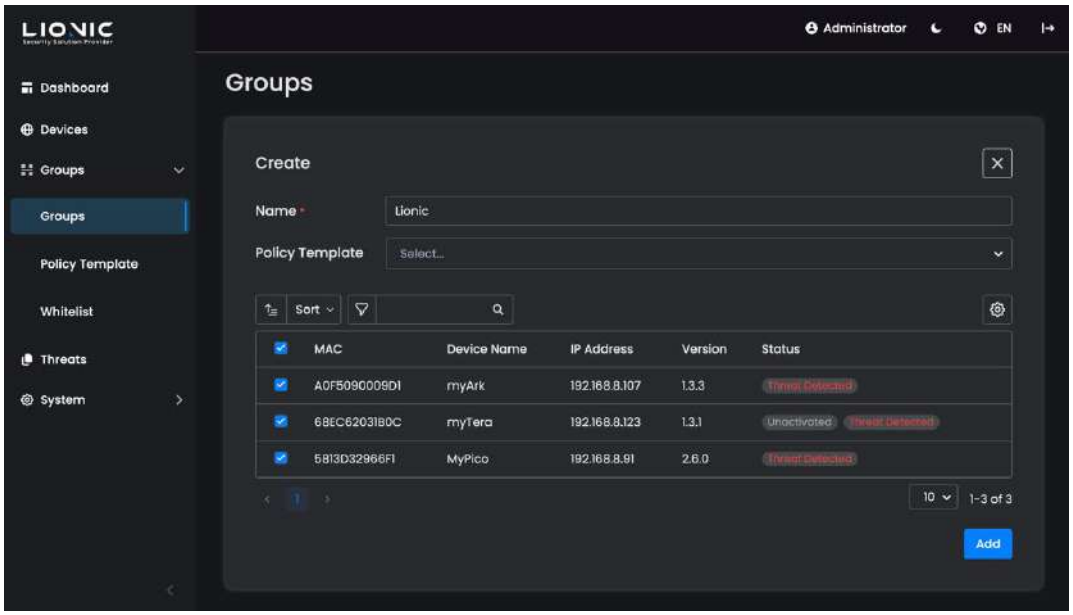
[Groups] feature allows you to group different devices together and configure various security protection functionalities for each group.

Groups

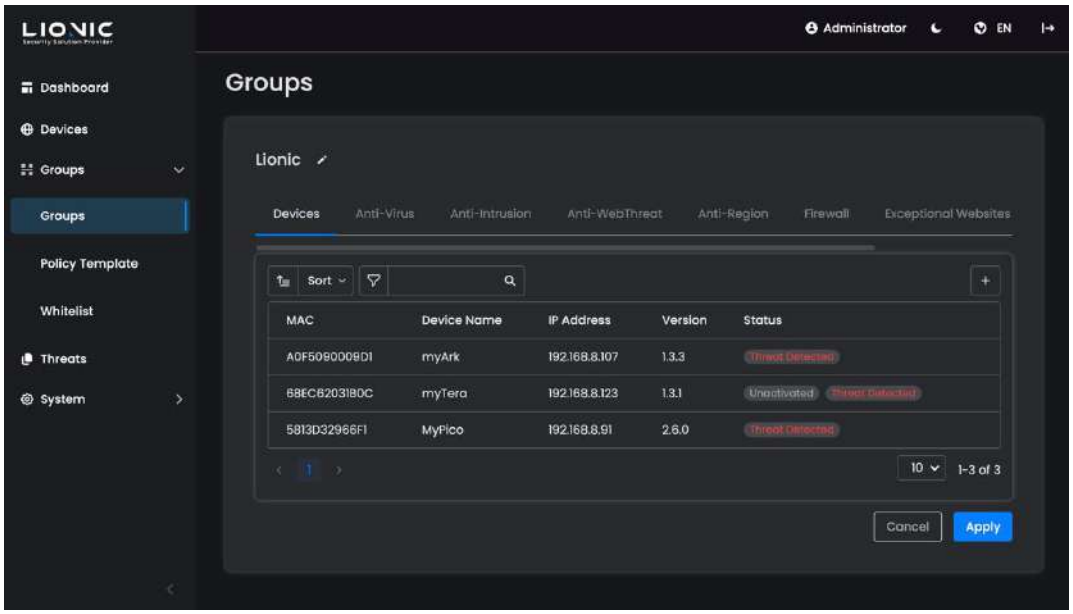
1. In the [Groups] page, users can select [+] to add devices for collective management within the group.



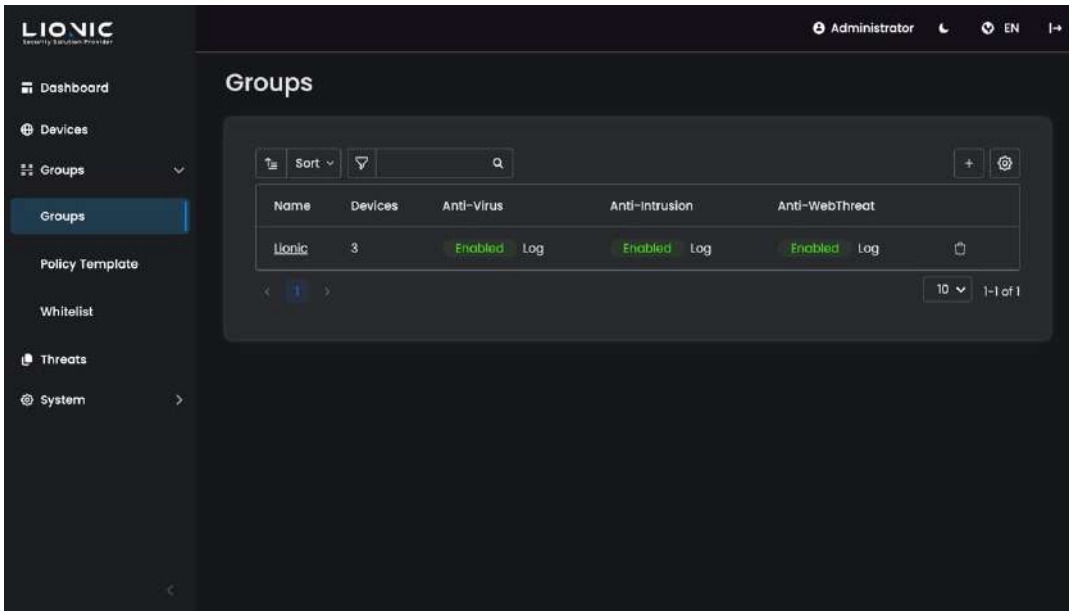
2. Create a group name and select the devices for group management.



3. After confirmation, [Apply].



4. New creation successful.

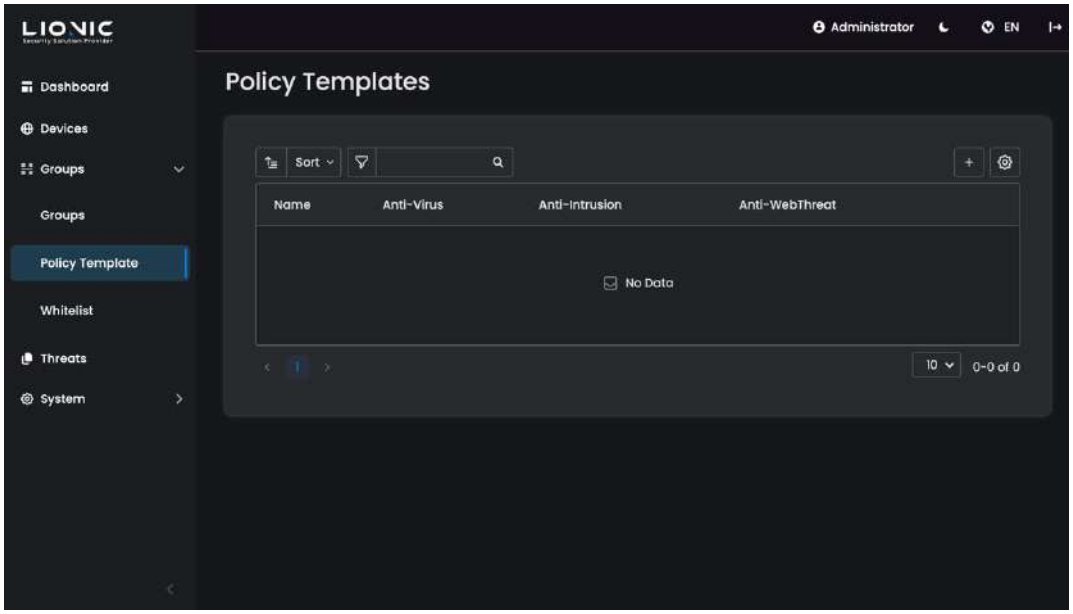


※ After creation, navigate to the device list, click , select [Actions], and choose [Sync Group Policies].

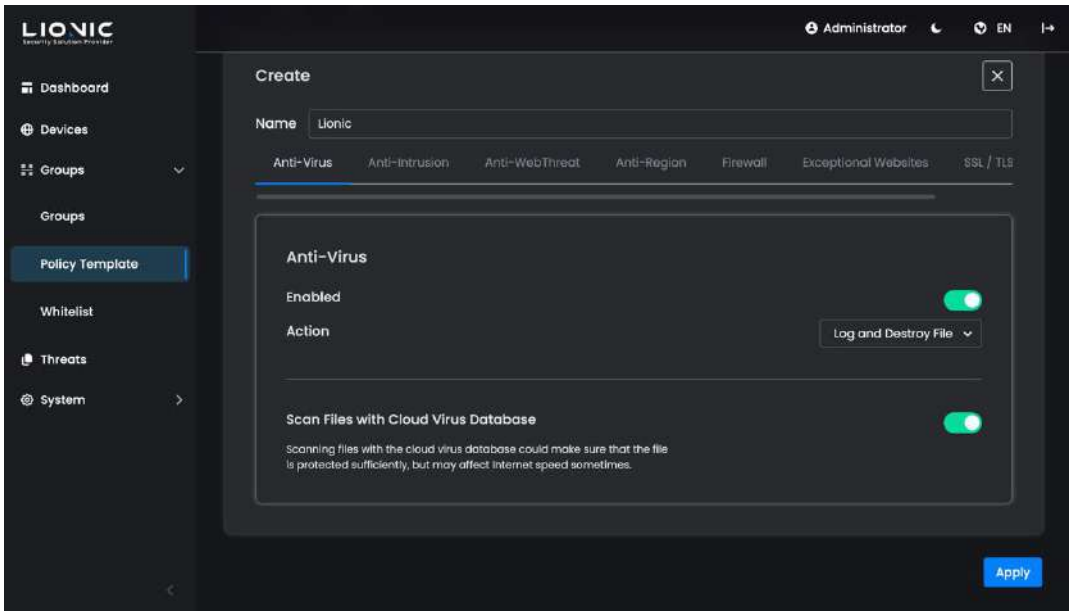
Policy Template

Create a security rule template that can be quickly applied when creating a new group to maintain consistent security rules.

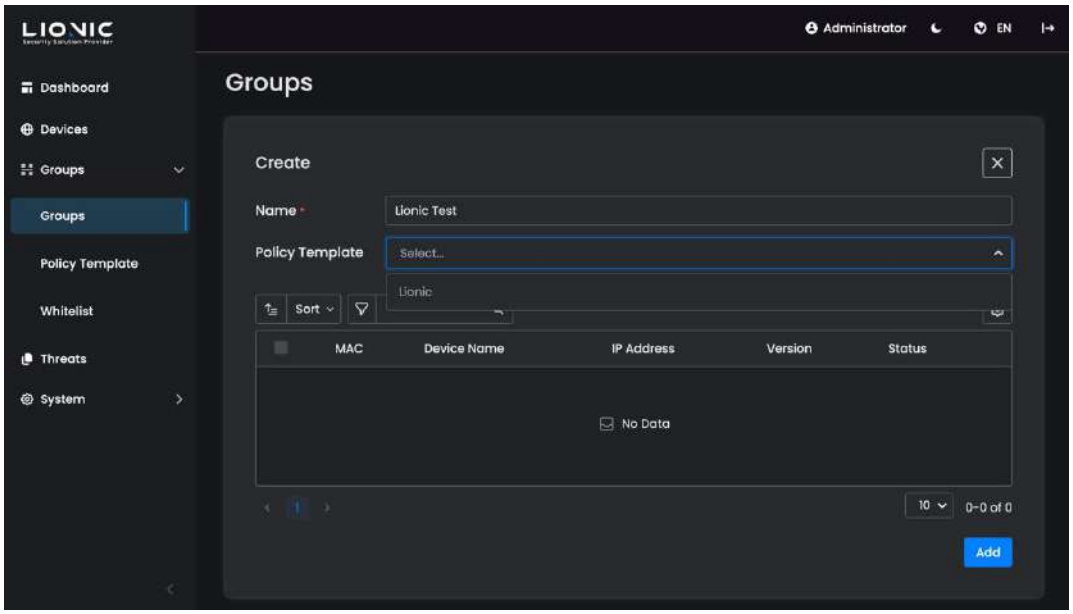
1. In the [Policy Templates] page, users can select [+] to add a template.



2. Create template name, adjust rule settings, after confirmation [Apply].



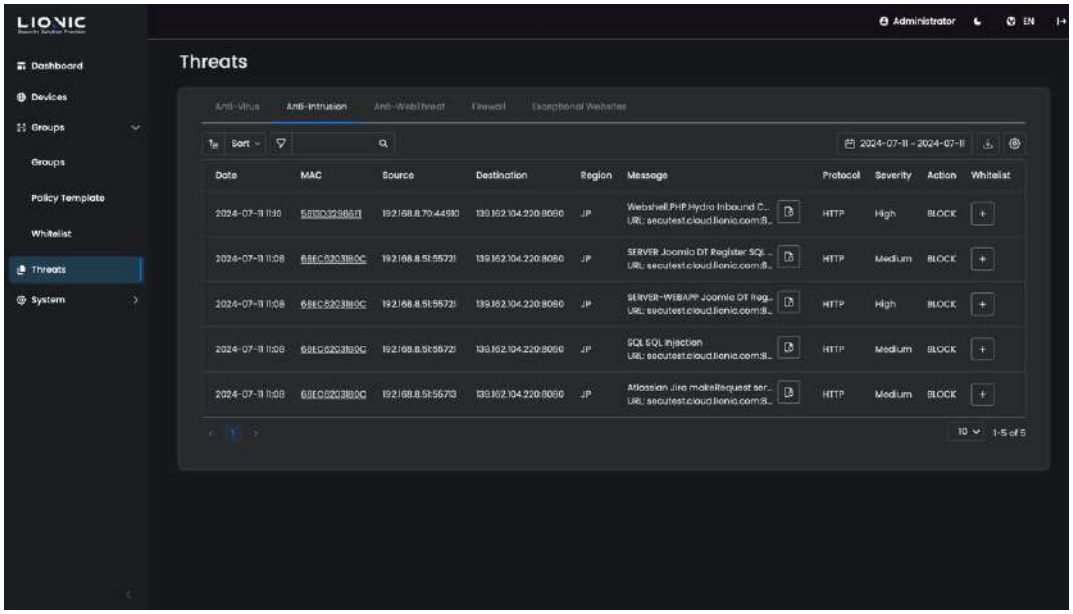
3. After completion, when creating a new group, you can apply the security rule template.



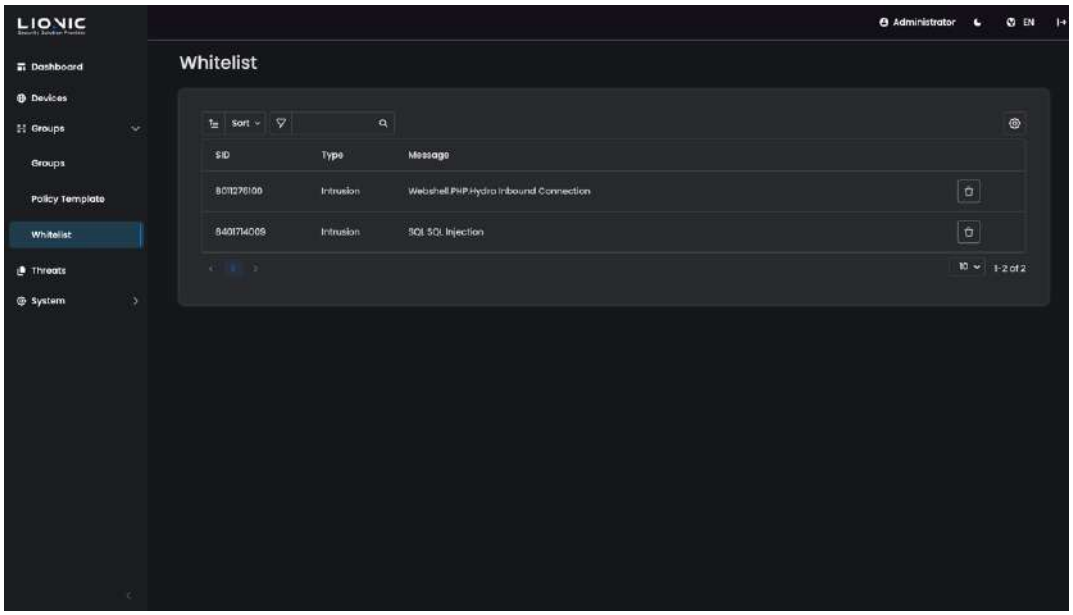
Whitelist（Global Whitelist）：

When CMS security measures disrupt legitimate files or block trusted connections, the whitelist function can be used to restore normal operation.

1. In the [Threats] page, users can select [+] to add to the whitelist.



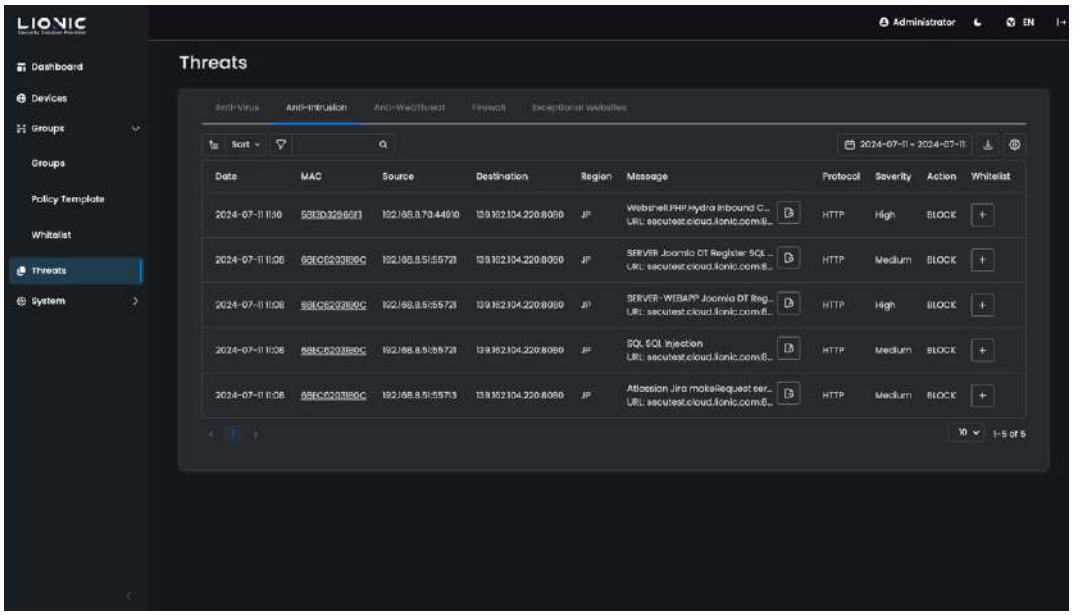
2. After successfully adding, users can view it on the [Whitelist] page



※ After creation, navigate to the device list, click , select [Actions], and choose [Sync Group Policies].

Threats

When CMS detects cybersecurity threats on managed devices, the relevant threat information will be uploaded to CMS and displayed in corresponding sections of the [Threats] page based on different security protection features.



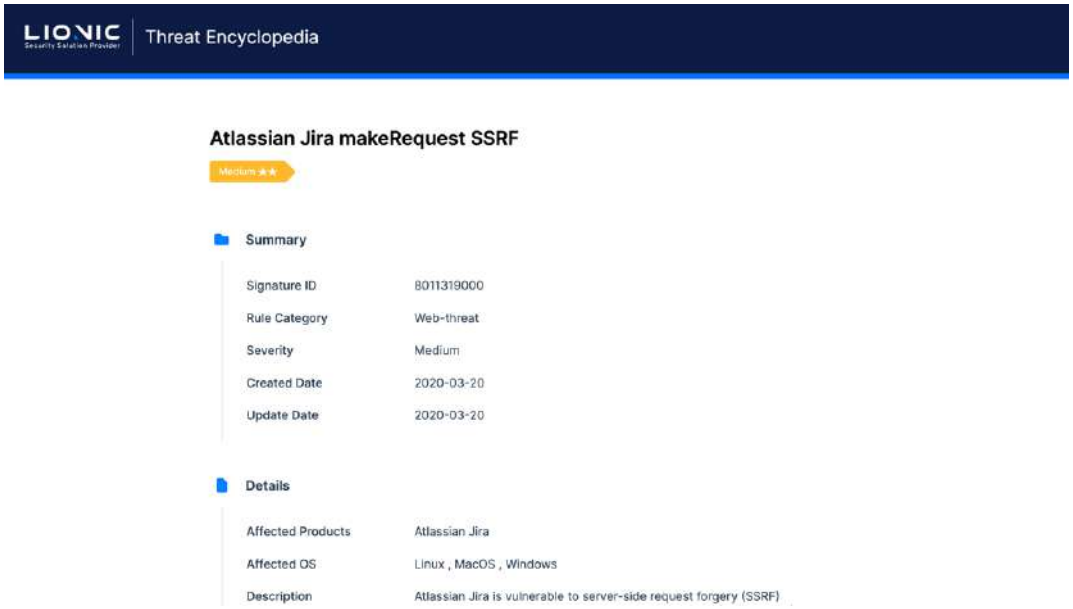
- **Sort**：Click to change the order (ascending/descending) , Click [Sort] to select a category.
- **Filter**：Click the input box to filter devices.
- **Date range filtering**：Filter records by date range
- **Export as CSV**：Export the device list as a CSV file.
- **Whitelist**：When the security protection features of the CMS management device disrupt secure files or block trusted connections, you can restore normal usage through the whitelist functionality.

  - Add whitelist rule：Please search for the disrupted or blocked event records on the [Threats] page, then click [+] to add to the whitelist.

  ※ After creation, navigate to the device list, click , select [Actions], and choose [Sync Group Policies].

  - Delete whitelist rule：Navigate to the [Whitelist] page and delete the specified whitelist rule.

- **Threat Encyclopedia:** In the threat logs of [Anti-Intrusion], clicking on allows you to access the analysis and solutions for the corresponding attack。

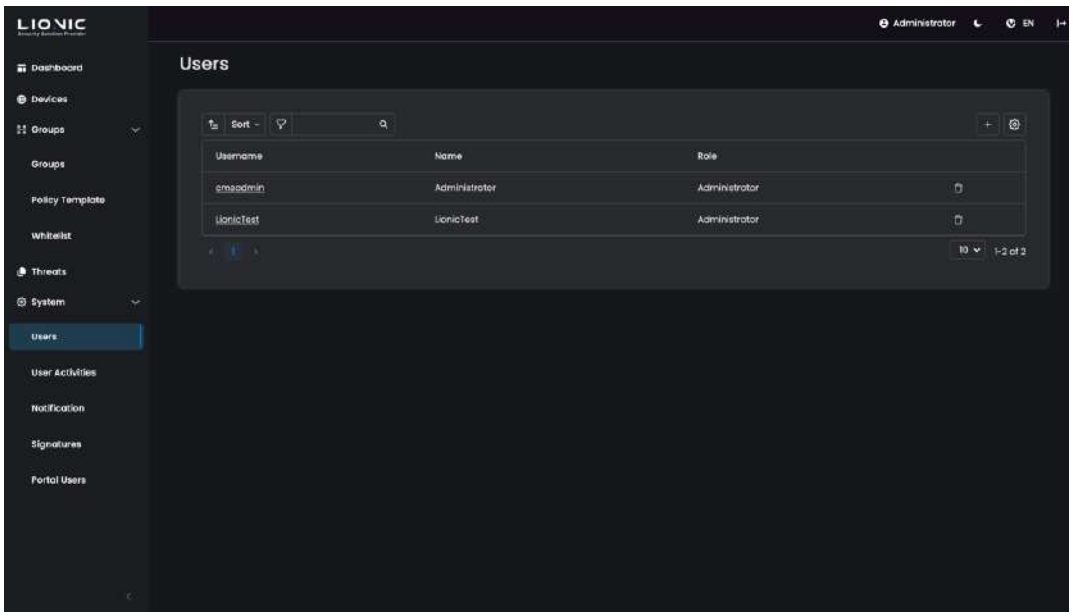


System

Users

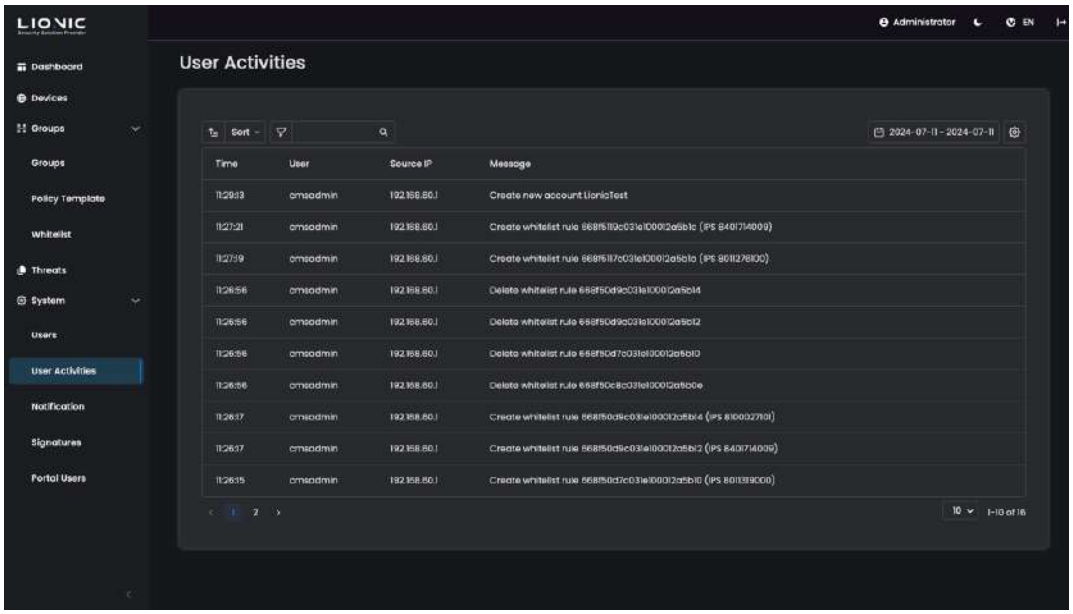
Add user page allows creation of users with account, password, and permission management.

- Administrator: Has all permissions.
- Regular User: Differs from the administrator in that they cannot manage users or view management logs.
- Viewer: Can only view and cannot perform any configurations.



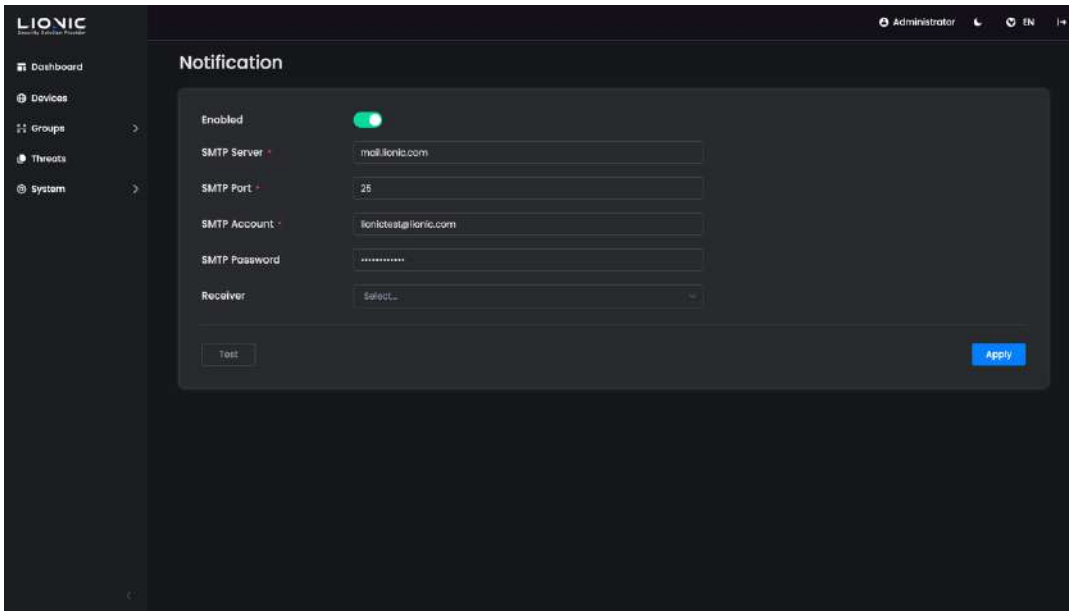
User Activities

The [User Activities] page displays all changes made by CMS administrators in the web control interface.



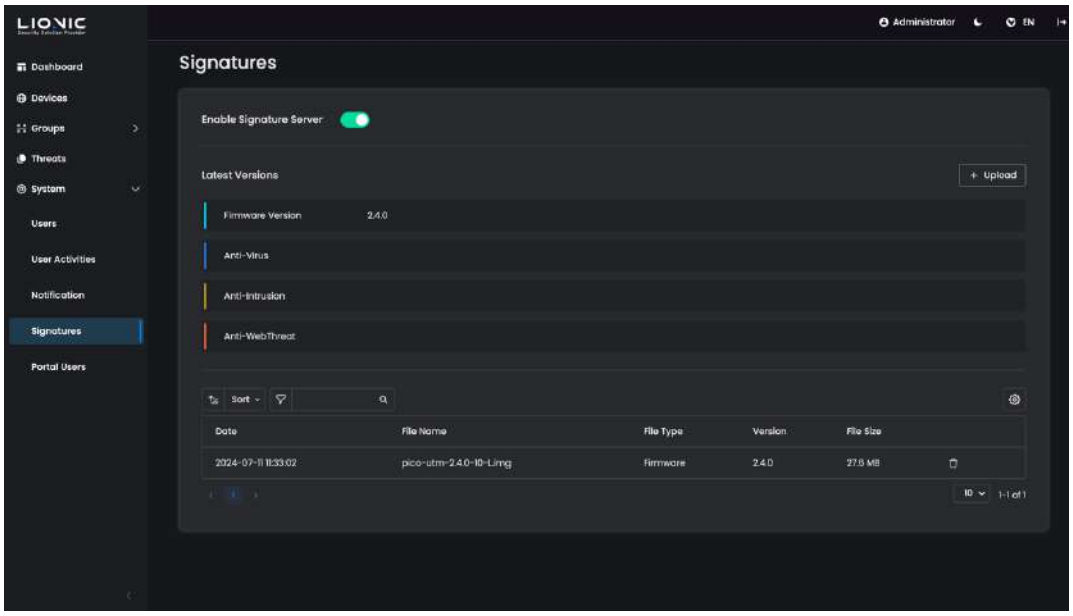
Notification

[Notification] feature detects cybersecurity threats on CMS management devices and uploads them to the CMS. Threat information is then sent via email to a designated mailbox. Please enter the correct configuration values in the input box and click [Apply] to complete the setup.



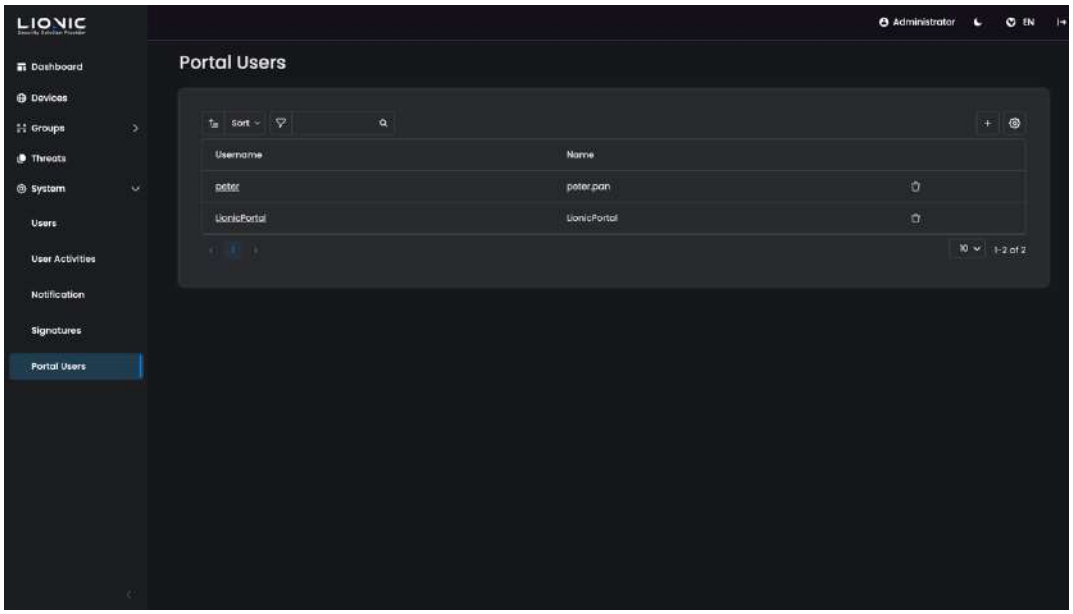
Signatures

When users require access to the CMS firmware and feature code update server due to network connection restrictions, they can upload and manage firmware and feature code updates through this page.
※ Intended for use only in environments completely disconnected from the internet. Before enabling, please contact LIONIC or your sales partner's technical support window.



Portal Users

If different partners with varying permissions need to assist in managing devices on the CMS, the CMS administrator can use the CMS Portal to create portal users and assign devices. This allows different partners to manage their assigned devices under their portal user identities.



1. Enable CMS Portal functionality.

```
vi /home/cms/cms/docker-compose.yml
    ...
    environment:
- CMS_ADDRESS=0.0.0.0:4221
- CMS_PORTAL_ADDRESS=0.0.0.0:80
```

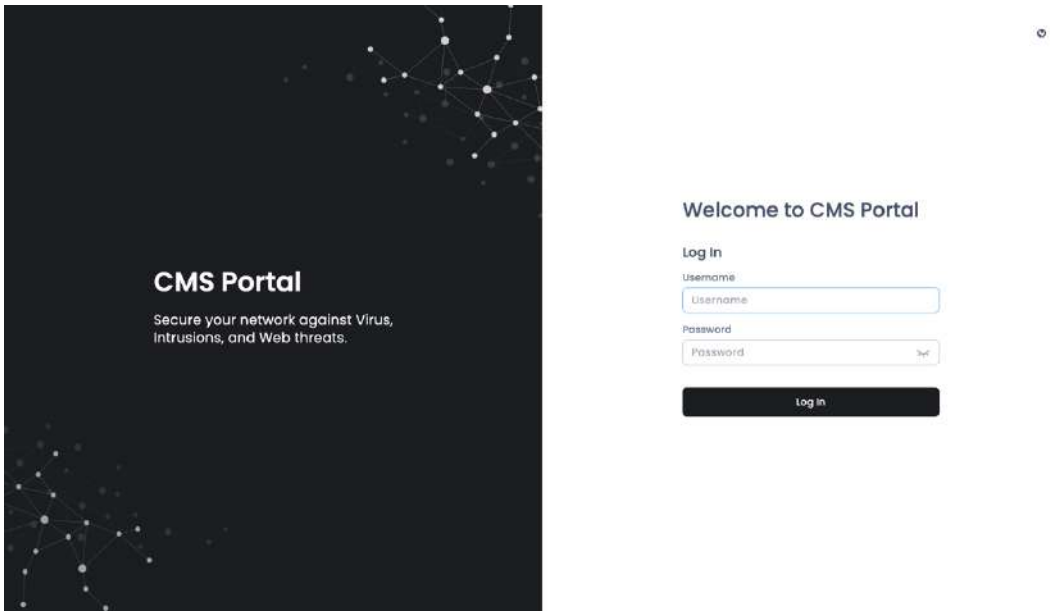
2. Open firewall port 80.

```
sudo firewall-cmd --zone=public --permanent --add-port=80/tcp
sudo firewall-cmd –reload
```

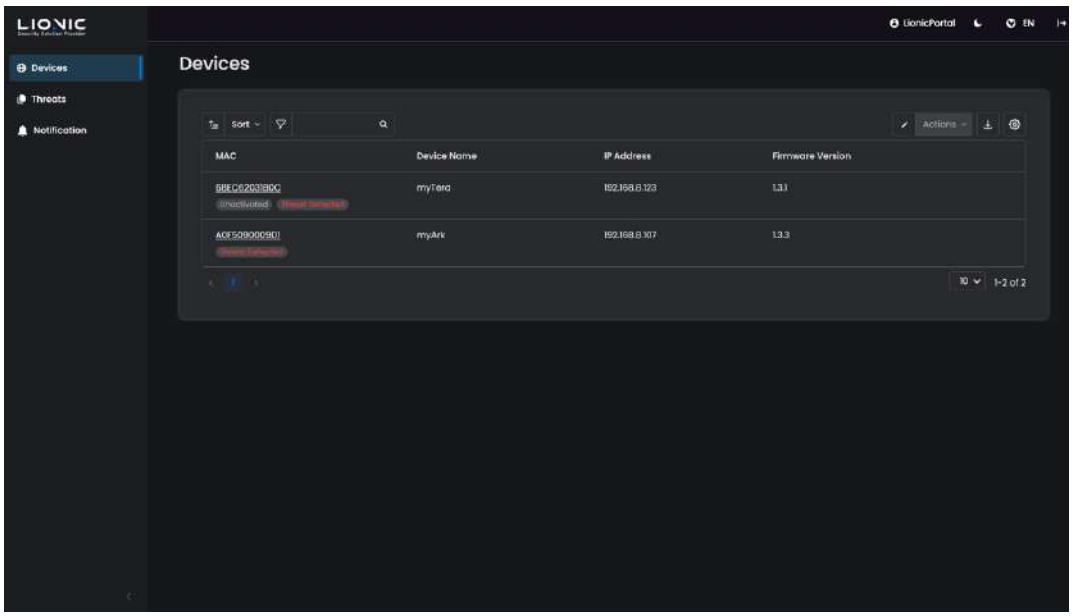
3. Restart the CMS server.

```
docker-compose -f /home/cms/cms/docker-compose.yml up -d
```

4. After completing the setup, you can log in to the CMS Portal by opening http://CMS_IP in a web browser.



5. You can now manage the devices assigned by administrators.



Feature Setting

NTP Configuration

By default, CMS connects to 2.almalinux.pool.ntp.org for time synchronization. NTP server can be changed by modifying configuration file as below.

```
sudo vi /etc/chrony.conf
```

Replace 2.almalinux.pool.ntp.org by new NTP server.

```
pool 2.almalinux.pool.ntp.org iburst
```

Restart chronyd to take effect.

```
sudo systemctl restart chronyd
```

Firewall Configuration

By default, below ports are open.

- TCP port 22: SSH service.
- UDP Port 123: NTP service
- TCP port 4221: CMS Web UI.
- TCP port 4222: Pico-UTM connects to CMS via this port.
- TCP port 4223: CMS signature update service for Pico-UTM.
- TCP port 8888: CMS proxy service for Pico-UTM.

CMS uses firewalld to manage firewall rules. If SSH service is not needed. You can disable sshd service and block TCP port 22.

```
sudo systemctl stop sshd
sudo systemctl disable sshd
sudo firewall-cmd --zone=public --permanent –-remove-service=ssh
sudo firewall-cmd --reload
```

You can also allow specific IP to access SSH.

```
sudo firewall-cmd --permanent --zone=public --add-rich-rule='rule
family="ipv4" source address="192.168.8.8" port protocol="tcp" port="22"
accept'
sudo firewall-cmd --reload
```

To remove above rule:

```
sudo firewall-cmd --permanent --zone=public --remove-rich-rule='rule
family="ipv4" source address="192.168.8.8" port protocol="tcp" port="22"
accept'
```

Similarly, you can also allow specific IP to access web UI.

```
sudo firewall-cmd --zone=public --permanent --remove-port=4221/tcp
sudo firewall-cmd --permanent --zone=public --add-rich-rule='rule
family="ipv4" source address="192.168.8.8" port protocol="tcp" port="4221"
accept'
sudo firewall-cmd --reload
```

Time Zone Configuration

By default the time zone is Asia/Taipei. You can change the time zone by editing CMS Configuration file as below.

```
vi /home/cms/cms/docker-compose.yml
```

Change the time zone to Asia/Japan for example.

```
  ...
  environment:
    ...
    - TZ=Asia/Japan
```

Restart CMS server.

```
docker-compose -f /home/cms/cms/docker-compose.yml up -d
```

HTTPS Web UI

By default, the access to CMS web UI is not encrypted. Below describes the steps to enable HTTPS encryption.

1. Edit CMS configuration file.

```
vi /home/cms/cms/docker-compose.yml
```

2. Add CMS_CERT and CMS_KEY to environment settings.

```
    environment:
      - CMS_ADDRESS=0.0.0.0:4221
      - CMS_CERT=certs/server.crt
      - CMS_KEY=certs/server.key
```

3. Restart CMS server.

```
docker-compose -f /home/cms/cms/docker-compose.yml up -d
```

4. Now users can access https://{ip}:4221.

If you want to use your own certificate, you need to overwrite certificates by setting volumes as below.

```
    environment:
      - CMS_ADDRESS=0.0.0.0:4221
      - CMS_CERT=certs/server.crt
      - CMS_KEY=certs/server.key
    volumes:
      ...
      - ./certs/server.crt:/app/certs/server.crt
- ./certs/server.key:/app/certs/server.key
```

Enlarge Storage

Follow below steps to add 100GB to storage.

1. Power off CMS and expand disk capacity to 200GB via VMWare/VirtualBox.

2. Power on CMS and enter below commands.

```
sudo parted ---pretend-input-tty /dev/sda resizepart 2 100%
sudo partx -u /dev/sda
sudo pvresize /dev/sda2
sudo lvextend -l +100%FREE -r /dev/almalinux/home
```

Trouble Shooting

Account Locked

An account will be locked for 24 hours if there are 10 password errors within 5 minutes. Use below command to unlock account bob.

```
docker exec -it cms /app/cms -cmd unlock -account bob
```

Forgot Password

If the password of admin account was forgotten, users can change the password from the console. Below command change account bob's password to 123456.

```
docker exec -it cms /app/cms -cmd password -account bob -password 123456
```

Central Management System 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.