

# User Manual Central Management System

Version 2.0 Released on Jul 2024

Lionic Corp. www.lionic.com



# **CMS User Manual**

Copyright © 2024, Lionic Corp.; all rights reserved.

#### 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

1



# Content

| Setup Steps             | 3  |
|-------------------------|----|
| Installation Steps      | 3  |
| Upgrade steps           | 7  |
| Overview                | 8  |
| Dashboard               | 9  |
| Devices                 | 11 |
| Groups                  | 14 |
| Groups                  | 14 |
| Policy Template         | 16 |
| Whitelist               | 17 |
| Threats                 | 19 |
| System                  | 21 |
| Users                   | 21 |
| User Activities         | 21 |
| Notification            | 22 |
| Signatures              | 23 |
| Portal Users            | 23 |
| Feature Setting         | 26 |
| NTP Configuration       | 26 |
| Firewall Configuration  | 26 |
| Time Zone Configuration | 27 |
| HTTPS Web UI            | 28 |
| Enlarge Storage         | 29 |
| Account Locked          |    |
| Forget Dessword         | 30 |



# **Setup Steps**

## Installation Steps:

1. Download CMS VM installer

| •O• cms-2.0.0        | <b>F</b> 2/6422 ··· |
|----------------------|---------------------|
| (*)                  |                     |
| CI 288 -             | 大小 经回归期             |
| Ca Consint           |                     |
| CMS60                |                     |
| CMS-disk001.mitk     | 17 GB 3 days ago    |
| 3 Gan                |                     |
| LIONIC Share service |                     |

2. Select the CMS VM installer format

| CMS-2.0.0      | × +                  |                           |                   |         |           | ш    |
|----------------|----------------------|---------------------------|-------------------|---------|-----------|------|
| < → ↑ 0        | $\Box \rightarrow z$ | に微 > DATA (D:) > Server > | СМ5-2.0.0         | 搜尋 CMS  | -2.0.0    | Q    |
| 🕀 15 16 - 🕺 🧔  | 0 0                  | 🙆 🖞 14 #R · 🚍             | 信視 ◇ ・・・          |         | CB        | 詳細宮料 |
| ☆ 常用           |                      | 「宮境」へ                     | 修改日期              | 湖린      | 大小        |      |
|                |                      | CMS.mf                    | 2024/7/4 下午 01:53 | MF檔素    | 1 KB      |      |
|                |                      | G CM5.ovf                 | 2024/7/4下午 01:53  | OVF 標案  | 5 KB      |      |
| 調 ± T          | *                    | 😚 CMS-disk001.vmdk        | 2024/7/4下午 01:53  | VMDK 信里 | 1,815,271 |      |
| 🛓 টাহা         | *                    |                           |                   |         |           |      |
| 🔛 文件           | *                    |                           |                   |         |           |      |
| 🔁 🗄 H          |                      |                           |                   |         |           |      |
| (1) 214        | ,                    |                           |                   |         |           |      |
| 12 18月         |                      |                           |                   |         |           |      |
| Server         |                      |                           |                   |         |           |      |
| Production-2.5 |                      |                           |                   |         |           |      |
| (23E)          |                      |                           |                   |         |           | =    |



#### 3. Create a VM name and import



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



5. Choose connection mode, select network card

| Virtual Machine Settings   | :  |   |   |
|--|--|---|---|
| Hardware Options   |  |   |   |
| Device<br>Memory<br>Arad Dek (SCSI)<br>S CD(DP (DE)<br>Atwork Adapter<br>Display | Summery<br>2 GB<br>2<br>100 GB<br>Using unknown backend<br>Using clives A1<br>Bridged (Automatic)<br>Limonitor | Dekto statu:<br>Connecta z powr en<br>Rebsek connecton<br>Biologic Connected directly to the physical individual<br>Replicate physical rebucks correction state<br>Configure Adapters |   |
|  |  | HAT: Used to share the host's IP address     Host-only: A prior when network shared with the host     Outron: Specific wheat network      mean  | Automatic Bridging Settings   |
|  |  | LAN Segment:  | Select the host network adapter(s) you want to<br>automatically bridge: |
|  |  |   | Intel(R) Ethernet Connection I217-V                                     |
|  | Add Renove   | OC Carcal Hup   | OK Cancel Help  |



# 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

Ø



8. After setup is complete, open <u>http://CMS\_IP:4221</u> in a web browser to log in. Default credentials: cmsadmin / cmssecretpass



| Welcome to C         | MS  |
|----------------------|-----|
| Log In               |     |
| Usemame              |     |
|                      |     |
| Usernama             |     |
| Password             |     |
| Password<br>Password | 244 |
| Password<br>Password | 244 |



#### **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.

| LIONIC      |                             |               |                     | Administre        | ator <b>L ⊘</b> EN I→   |
|-------------|-----------------------------|---------------|---------------------|-------------------|-------------------------|
| 🖬 Dashboard | liter Name                  |               |                     | 2                 |                         |
| Devices     | Welcome, Admin              | istrator      | Online Devices      | 3<br>Total Device | 99                      |
| H Groups    |                             |               |                     |                   |                         |
| 🕒 Threats   | Inspection History Inspecte | d From 7 Days | Recent Threats      |                   |                         |
| System      |                             |               | Date                | Туре              | Message                 |
|             |                             |               | 2024-07-11 11:10:10 | Intrusion         | Webshell.PHP.Hyd        |
|             | 705 Files                   | 173K Rows     | 2024-07-11 11:09:18 | Web               | testdatabaseweb         |
|             |                             |               | 2024-07-11 11:08:54 | Web               | secure.eicar.org        |
|             |                             |               | 2024-07-11 11:08:53 | Web               | secure.elcar.org        |
|             | 117K URLS                   | 1M Packets    | 2024-07-1111:08:45  | Web               | www.internetbod         |
|             | Summary                     |               |                     | 8                 | 2024-07-05 - 2024-07-11 |
|             | Threat Statistics           |               | Top Threats         |                   | All                     |

**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.



|             | Summary                     |   |                                 | 2024-07-05 - 2024-07-11                         |
|-------------|-----------------------------|---|---------------------------------|---|
| 🖬 Dashboard | Threat Statistics           |   | Top Threats                     |   |
| Devices     | Virus                       |   | By Count By Device              | ALL   |
| Ħ Groups    | 0                           |   | Count Message                   |   |
| Threats     | Intrusion                   |   | 1 Intrusion Atlas               | islan 8011319000                                |
| Ø System    | 6                           | ۵ | 1 Intrusion SQL                 | SQL L. 8401714009                               |
|             | wab<br>4                    |   | UDP<br>can<br>intrusion<br>n 30 | Ports<br>Lvt:10<br>withi 8060000301<br>seco     |
|             | Threat Counts               |   | Top Devices                     |   |
|             | 🖉 🔍 Virus 🔶 Web 🔮 Intrusion |   |                                 | dress MAC Mod                                   |
|             | 12                          |   | 5 myTera 192.1                  | 68.8.123 68EC62031B0C Terr                      |
|             |                             |   | 4 myArk 192.1                   | 68.8.107 A0F5090009D1 Ark-                      |
|             |                             |   |                                 | A VALUE AND |

**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.

|  |                                 |             | Ĩ       | Intrusion | Atlassian     | 8011319000    |      |
|--|---------------------------------|-------------|---------|-----------|---------------|---------------|------|
| a Dashboard  | 6                               |             |         | Intrusion | SQL SQL L.    | 8401714009    |      |
| Devices  |                                 |             |         |           |               |               |      |
| # Groups   | Web                             |             |         | Intrusion | UDP Port      | 8060000301    |      |
| Threats  | 4                               |             |         | Web se    | ecure.eicar   | 1000000001003 |      |
| System     Sys |                                 |             |         |           |               |               |      |
|  | Threat Counts                   |             | Top Dev | vices     |               |               |      |
|  | Virus • Web • Intrusion         |             |         |           | IP Address    | MAC           |      |
|  | 12                              |             |         | myTera    | 192.168.8.123 | 68EC6203180C  | Terc |
|  |                                 |             |         | myArk     | 192.168.8.107 | A0F5090009D1  | Ark- |
|  |                                 | -           |         | MyPico    | 192.168.8.91  | 5813D32966F1  | Picc |
|  | 3                               |             |         |           |               |               |      |
|  | 0 07-05 07-06 07-07 07-08 07-09 | 07-10 07-11 |         |           |               |               |      |
|  |                                 |             |         |           |               |               |      |



# Devices

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

|             |   |   |             |       |               | Administrator    |
|-------------|---|---|-------------|-------|---------------|------------------|
| 🖬 Dashboard | I | Devices                                 |             |       |               |                  |
| Devices     |   |   |             |       |               |                  |
| H Groups    |   | î≞ Sort ~ 🖓                             | ٩           |       |               | 🖌 Actions 🛩 🛓 🕲  |
| 🜔 Threats   |   | MAC                                     | Device Name | Group | IP Address    | Firmware Version |
| System      |   | AOF5090009D1<br>(Thesis Security)       | myArk       |       | 192.168.8.107 | 1.3.3            |
|             |   | 68EC62031B0C<br>(Unnetivoted) (Threat D | myTera      |       | 192.168.8.123 | 1.3.1            |
|             |   | 5813D32966F1<br>(Threat Detected)       | MyPico      |       | 192.168.8.91  | 2.6.0            |
|             |   |   |             |       |               | 10 🛩 1-3 of 3    |
|             |   |   |             |       |               |                  |

- Sort : Click to change the order (ascending/descending) <sup>↑</sup>= · Click [Sort] to select a category.
- $\nabla$  **Filter** : Click the input box to filter devices.
- Actions: Click O 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.

|             |  | Administrator | L | 🛇 EN | l→ |
|-------------|--|---------------|---|------|----|
| 🖬 Dashboard | Devices                                      |               |   |      |    |
| Devices     |  |               |   |      |    |
| ₩ Groups    | A0F5090009D1                                 |               |   |      |    |
| Threats     | Information Policy Threats Statistics System |               |   |      |    |
| System      |  |               |   |      |    |
|             | MAC A0F5050009D1<br>Status Connected         |               |   |      |    |
|             | Device Name myArk 🖌                          |               |   |      |    |
|             | MAC A0F5090009DI                             |               |   |      |    |
|             | Model Ark-UTM 16                             |               |   |      |    |
|             | Group Default Group                          |               |   |      |    |
|             | WAN IP Address 192.168.8.107                 |               |   |      |    |
|             | Public IP Address 192.168.8.107              |               |   |      |    |
|             | Version 133                                  |               |   |      |    |

- 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.

|                 |           |         |            |                | Administrator  | L    | 🗢 EN     | l+ |
|-----------------|-----------|---------|------------|----------------|----------------|------|----------|----|
| 🖬 Dashboard     | Groups    |         |            |                |                |      |          |    |
| Devices         |           |         |            |                |                |      |          |    |
| <b>∷</b> Groups | î≣ Sort ~ | 7       | ٩          |                |                |      | + @      |    |
| Groups          | Name      | Devices | Anti-Virus | Anti-Intrusion | Anti-WebThreat |      |          |    |
| Policy Template |           |         |            | 0              |                |      |          |    |
| Whitelist       |           |         |            |                |                |      |          |    |
| Threats         |           |         |            |                |                | 10 🗸 | 0-0 of 0 |    |
| @ System        |           |         |            |                |                |      |          |    |
|                 |           |         |            |                |                |      |          |    |
|                 |           |         |            |                |                |      |          |    |
|                 |           |         |            |                |                |      |          |    |
|                 |           |         |            |                |                |      |          |    |
|                 |           |         |            |                |                |      |          |    |

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

|                 |                 |             |               |         | Administrator | L OEN I      | l+ |
|-----------------|-----------------|-------------|---------------|---------|---------------|--------------|----|
| 🖬 Dashboard     | Groups          |             |               |         |               |              |    |
| Devices         |                 |             |               |         |               |              |    |
| ₩ Groups        | Create          |             |               |         |               | ×            |    |
| Groups          | Name            | Lionic      |               |         |               |              |    |
| Policy Template | Policy Template | Select      |               |         |               |              |    |
| Whitelist       | t≞ Sort ~ 🖓     | ٩           |               |         |               | ٢            |    |
| Integents       | MAC             | Device Name | IP Address    | Version | Status        |              |    |
| ම System        | S A0F509000     | 9DI myArk   | 192.168.8.107 | 1.3.3   |               |              |    |
|                 | 68EC62031       | 30C myTera  | 192.168.8.123 | 1.3.1   |               |              |    |
|                 | 5813D3296       | SFI MyPico  | 192.168.8.91  | 2.6.0   |               |              |    |
|                 |                 |             |               |         | 10            | 2 🗸 1-3 of 3 |    |
|                 |                 |             |               |         |               |              |    |



#### 3. After confirmation, [Apply].

|                 |   |                  |             |               |         | e Admir | nistrator 6 | 🛛 EN        |
|-----------------|---|------------------|-------------|---------------|---------|---------|-------------|-------------|
| 🖬 Dashboard     | G | roups            |             |               |         |         |             |             |
| Devices         |   |                  |             |               |         |         |             |             |
| ₩ Groups        |   | Lionic 🖌         |             |               |         |         |             |             |
| Groups          |   | Devices Anti-Vin |             |               |         |         |             | al Websites |
| Policy Template |   | t⊫ Sort ⊻ 🔽      | Q           |               |         |         |             |             |
| Whitelist       |   | MAC              | Device Name | IP Address    | Version | Status  |             |             |
| 🖡 Threats       |   | A0F5090009D1     | myArk       | 192.168.8.107 | 1.3.3   |         |             |             |
| ම System        |   | 68EC6203180C     | myTera      | 192.168.8.123 | 1.3.1   |         |             |             |
|                 |   | 5813D32966F1     | МуРісо      | 192.168.8.91  | 2.6.0   |         |             |             |
|                 |   |                  |             |               |         |         | 10 🛩        | 1-3 of 3    |
|                 |   |                  |             |               |         |         | Concel      | Apply       |
|                 |   |                  |             |               |         |         |             |             |
|                 |   |                  |             |               |         |         |             |             |

4. New creation successful.

| LIONIC          |   |                   |         |            |     |                | Administrator  | c    | 🕑 EN     | 1-+ |
|-----------------|---|-------------------|---------|------------|-----|----------------|----------------|------|----------|-----|
| 🖬 Dashboard     | ¢ | Groups            |         |            |     |                |                |      |          |     |
| Devices         |   |                   |         |            |     |                |                |      |          |     |
| ₩ Groups        |   | î <u>≡</u> Sort ~ | 7       | ٩          |     |                |                |      | + @      |     |
| Groups          |   | Name              | Devices | Anti-Virus |     | Anti-Intrusion | Anti-WebThreat |      |          |     |
| Policy Template |   | Lionic            |         |            | Log | Enabled Log    | Enabled Log    | đ    |          |     |
| Whitelist       |   |                   |         |            |     |                |                | 10 🗸 | 1-1 of 1 |     |
| 🧶 Threats       |   |                   |         |            |     |                |                |      |          |     |
| @ System        |   |                   |         |            |     |                |                |      |          |     |
|                 |   |                   |         |            |     |                |                |      |          |     |
|                 |   |                   |         |            |     |                |                |      |          |     |
|                 |   |                   |         |            |     |                |                |      |          |     |
|                 |   |                   |         |            |     |                |                |      |          |     |
|                 |   |                   |         |            |     |                |                |      |          |     |

After creation, navigate to the device list, click 2, 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.

|                 |             |            |                | e Adm          | inistrator <b>L</b> | ٥   | EN   | l+ |
|-----------------|-------------|------------|----------------|----------------|---------------------|-----|------|----|
| 🖬 Dashboard     | Policy Terr | nplates    |                |                |                     |     |      |    |
| Devices         |             |            |                |                |                     |     |      |    |
| ₩ Groups        | 1≝ Sort ~   | 7          | ٩              |                |                     |     | 0    |    |
| Groups          | Name        | Anti-Virus | Anti-Intrusion | Anti-WebThreat |                     |     |      |    |
| Policy Template |             |            | 🖂 No D         | ata            |                     |     |      |    |
| Whitelist       |             |            |                |                |                     |     |      |    |
| 🔮 Threats       |             |            |                |                | 10 ~                | 0-0 | of 0 |    |
| @ System        |             |            |                |                |                     |     |      |    |
|                 |             |            |                |                |                     |     |      |    |
|                 |             |            |                |                |                     |     |      |    |
|                 |             |            |                |                |                     |     |      |    |
|                 |             |            |                |                |                     |     |      |    |
|                 |             |            |                |                |                     |     |      |    |

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

|                 |   | O Administrator C    | ♥ EN I→ |
|-----------------|---|----------------------|---------|
| Dashboard       | Create  |                      | ×       |
| Devices         | Name Lionic   |                      |         |
| # Groups        | Anti-Virus Anti-Intrusion Anti-WebThreat Anti-Region Firewall   |                      |         |
| Groups          |   |                      |         |
| Policy Template | Anti-Virus  |                      |         |
| Whitelist       | Enabled   |                      |         |
| B Threats       | Action  | Log and Destroy File |         |
|                 |   |                      |         |
| @ System        | Scan Files with Cloud Virus Database  |                      |         |
|                 | Scanning files with the cloud virus database could make sure that the file<br>is protected sufficiently, but may affect internet speed sometimes. |                      |         |
|                 |   |                      |         |
|                 |   |                      |         |
|                 |   |                      | Apply   |
|                 |   |                      |         |



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

|                 |                         |             |            | e Adm   | inistrator C | 🕏 EN     | l→ |
|-----------------|-------------------------|-------------|------------|---------|--------------|----------|----|
| 🖬 Dashboard     | Groups                  |             |            |         |              |          |    |
| Devices         |                         |             |            |         |              |          |    |
| 밝 Groups 🗸 🗸    | Create                  |             |            |         |              | ×        |    |
| Groups          | Name®                   | Lionic Test |            |         |              |          |    |
| Policy Template | Policy Template         | Select      |            |         |              |          |    |
| Whitelist       | 1 <sub>Ξ</sub> Sort ~ 🖓 |             |            |         |              | ÷        |    |
| Threats         | MAC                     | Device Name | IP Address | Version | Status       |          |    |
| @ System >      |                         |             |            |         |              |          |    |
|                 |                         |             | 🖓 No Data  |         |              |          |    |
|                 |                         |             |            |         | 10 ~         | 0-0 of 0 |    |
|                 |                         |             |            |         |              | Add      |    |

# 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.

| LIONIC          |                     |              |                   |                      |        |  |          | Administrator        | •             | Ø EN   |  |
|-----------------|---------------------|--------------|-------------------|----------------------|--------|--|----------|----------------------|---------------|--------|--|
| 🖬 Dashboard     | Threats             |              |                   |                      |        |  |          |                      |               |        |  |
| Devices         | Anti-Virus Ar       | 16-Intrusion |                   |                      |        |  |          |                      |               |        |  |
| H Groups        | t <u>⊌</u> Sort ~ ▽ |              |                   |                      |        |  | ė.       | 024-07-11 - 2024-07- | r s           | ۲      |  |
| Groups          | Date                | MAC          | Source            | Destination          | Region | Message  | Protocol | Severity Action      | White         | at     |  |
| Policy Templats | 2024-07-11 1130     | 581303298671 | 192168.870.44910  | 139 162 104 220 8080 |        | Webshell PHP3Hydra Inbound C.<br>URL secutest cloud lionia.com8,     | 5 нттр   | High BLOCK           |               |        |  |
| Threats         | 2024-07-1111:08     | 686C0203180C | 192168.8 51:55721 | 139362104.220.8080   |        | SERVER Joamia DT Register SQL<br>URL: secutest cloud filanic.com:B.  | чтн      | Medium BLOCK         |               |        |  |
| @ System        | 2024-07-11 11:08    | 68EC6203880C | 192168.8 51:55721 | 139,162,104,220,8090 |        | SERVER-WEBAPP Joomie DT Reg. G                                       | нте      | High BLOCK           |               |        |  |
|                 | 2024-07-11 11:08    | 68EC6203880G | 192169.8.51:55721 | 136.162.104.220.8080 |        | SQL SQL injection<br>URL secutest cloud lion is com 8.               | 1 ните   | Medium BLOCK         |               |        |  |
|                 | 2024-07-11 1:08     | 68EC6203880C | 192/68.8.51:567/3 | 139,162,104,220,9060 |        | Atlassian Jiro makellequest sor.<br>URL: secutest cloud bonic com/8. | НТТР     | Modium BLOCK         |               |        |  |
|                 |                     |              |                   |                      |        |  |          |                      | 10 <b>v</b> 1 | 5 of 5 |  |
|                 |                     |              |                   |                      |        |  |          |                      |               |        |  |
|                 |                     |              |                   |                      |        |  |          |                      |               |        |  |
|                 |                     |              |                   |                      |        |  |          |                      |               |        |  |



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

| m bashboard  | <pre>k bashboord bashboord</pre>  | LIONIC          |             |           |                                       | 🖯 Administrator 🖌 🛇 | EN |
|---|---|-----------------|-------------|-----------|---------------------------------------|---------------------|----|
| B Deckes   25 Groups   Broups   Broups   B01270000   Intrivusion   B  | i croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>croups<br>cro | 🖬 Dashboard     | Whitelist   |           |                                       |                     |    |
| Image: Serie of the Serie  | i choupă<br>croupă<br>Policy templotă<br>Intrusion SOL SOL Injection<br>Spatem<br>System  | 🕑 Devices       |             |           |                                       |                     |    |
| Stroups         SID         Type         Message           Policy Template         B01220000         Initiation         Weishell PriPhydra Indound Connection         Image: Connection           Whitelate         B401740066         Initiation         SOL SOL Injection         Image: Connection         Image: Connecon: Conn   | excpt<br>policy templets<br>whiteline<br>threads<br>system  | H Groups        | t≘ sort ~ 🖓 |           | <b>a</b>                              | ٢                   |    |
| Policy template         B0122800         Infrasion         Webshell Prip Hydra Information         Image: Comparison         Image: Comparison <t< td=""><td>Poticy tempions whealest wheal</td><td>Groups</td><td>SID</td><td>Туре</td><td>Message</td><td></td><td></td></t<> | Poticy tempions whealest wheal  | Groups          | SID         | Туре      | Message                               |                     |    |
| Whitelist         840174009         Intrusion         SQL SQL Injection         D           # Throats         ID ~ 1-2012         ID ~ 1-2012         ID ~ 1-2012         ID ~ 1-2012   | Multilite     94/07/24089     Intrusion     90/07/2009     Intrusion     90/07/2009       1 Threads     10 v     1-2.012  | Policy Template | 8011276100  | Intrusion | Webshell PkP Hydra Inbound Connection |                     |    |
| Threads   | Threads (10 - 1-2 of 2  | Whitelist       | 8401714009  | Intrusion | SQL 5QL Injection                     | ¢                   |    |
|   | s System  | Threats         |             |           |                                       | 10 - 1-2ot          |    |
| @ System  |   | 🕀 System        |             |           |                                       |                     |    |
|   |   |                 |             |           |                                       |                     |    |
|   |   |                 |             |           |                                       |                     |    |
|   |   |                 |             |           |                                       |                     |    |
|   |   |                 |             |           |                                       |                     |    |
|   |   |                 |             |           |                                       |                     |    |
|   |   |                 |             |           |                                       |                     |    |
|   |   |                 |             |           |                                       |                     |    |
|   |   |                 |             |           |                                       |                     |    |
|   |   |                 |             |           |                                       |                     |    |
|   |   |                 |             |           |                                       |                     |    |
|   |   |                 |             |           |                                       |                     |    |

![](_page_19_Picture_1.jpeg)

# 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.

| IONIC           |                  |               |                    |                       |        |   |          | O Administrate     | •      | Ø B      | N |
|-----------------|------------------|---------------|--------------------|-----------------------|--------|---|----------|--------------------|--------|----------|---|
| Dashboard       | Threats          |               |                    |                       |        |   |          |                    |        |          |   |
| Devices         | Anti-Vinus A     | nti-Intrusion |                    |                       |        |   |          |                    |        |          |   |
| Groups          | ts Sort - ⊽      |               |                    |                       |        |   | 82       | 024-07-11 - 2024-0 | 2-m _4 | ٢        |   |
| Groups          | Date             | MAC           | Source             | Destination           | Region | Message   | Protocol | Soverity Actio     | n Whi  | olist    |   |
| Policy Templote | 2024-07-11 11:10 | 58130.3296611 | 192/65.3 70 44910  | 139 162 104 220 8080  |        | Webshell/HPHydra Inbound C.,<br>URL securest cloud.lonic.com.B.,    |          | High BLOC          | K [+   |          |   |
| Threats         | 2024-07-1111:06  | 63EC6203180C  | 192105.8.51:55721  | 135 152 104 220 8 050 |        | SERVER Joomic DT Register SQL B<br>URL: eecutest cloud.lonic.com8   |          | Medium BLOC        | K [+   |          |   |
| iystem          | 2024-07-1111:08  | 68LC620380C   | 192.188,8.5155721  | 139,162,104,220,8060  |        | SERVER-WEBARY Joomia DT Reg.,<br>URL secutest cloud lionic.com/fl.  |          | High BLOC          | K [+   |          |   |
|                 | 2024-07-11 1606  | 68EC6203180C  | 192.168.8.51:55721 | 139.162.104.220.8080  |        | SQL SQL injection<br>URL ancutest.cloud fanic.com/8.                |          | Medium BLOC        | к [+   |          |   |
|                 | 2024-07-11 (1:08 | 65FC0203860C  | 192/68.8.51:55713  | 139 152 104 220 8090  |        | Atlassian Jira makeitequest ser.<br>URL secutest.cloud.lonic.com.8. |          | Medium BLOC        | ¢ [+   |          |   |
|                 |                  |               |                    |                       |        |   |          |                    | 10 🛩   | 1-5 of 5 |   |
|                 |                  |               |                    |                       |        |   |          |                    |        |          |   |
|                 |                  |               |                    |                       |        |   |          |                    |        |          |   |
|                 |                  |               |                    |                       |        |   |          |                    |        |          |   |
|                 |                  |               |                    |                       |        |   |          |                    |        |          |   |

- ➡ Sort : Click to change the order (ascending/descending) <sup>↑</sup>= · Click [Sort] to select a category.
- $\nabla$  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 *2*, select [Actions], and choose [Sync Group Policies].
  - Delete whitelist rule : Navigate to the [Whitelist] page and delete the specified whitelist rule.

19

![](_page_20_Picture_1.jpeg)

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

| ELIONIC<br>esurity Estation Provider | Encyclopedia        |  |
|--------------------------------------|---------------------|--|
|                                      | Atlassian Jira make | Request SSRF   |
|                                      | Summary             |  |
|                                      | Signature ID        | 8011319000   |
|                                      | Rule Category       | Web-threat   |
|                                      | Severity            | Medium   |
|                                      | Created Date        | 2020-03-20   |
|                                      | Update Date         | 2020-03-20   |
|                                      | Details             |  |
|                                      | Affected Products   | Atlassian Jira   |
|                                      | Affected OS         | Linux , MacOS , Windows  |
|                                      | Description         | Atlassian Jira is vulnerable to server-side request forgery (SSRF) |
|                                      |                     |  |

![](_page_21_Picture_1.jpeg)

# 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.

| LIONIC          |               |               |               | e Administrator | O EN     | 1+ |
|-----------------|---------------|---------------|---------------|-----------------|----------|----|
| Doshboard       | Users         |               |               |                 |          |    |
| Devices         |               |               |               |                 |          |    |
| H Groups 🗸 🗸    | t≝ Sort - 🖓 Q |               |               |                 | ۲        |    |
| Groups          | Usemame       | Name          | Role          |                 |          |    |
| Policy Template | emeadmin      | Administrator | Administrator |                 |          |    |
| whitelist       | LionicTest    | LionicTest    | Administrator |                 |          |    |
|                 |               |               |               | 10 🕶            | 1-2 of 2 |    |
| Threats         |               |               |               |                 |          |    |
| G System 🔶      |               |               |               |                 |          |    |
| Users           |               |               |               |                 |          |    |
| User Activities |               |               |               |                 |          |    |
| Notification    |               |               |               |                 |          |    |
| Signatures      |               |               |               |                 |          |    |
| Portal Users    |               |               |               |                 |          |    |
|                 |               |               |               |                 |          |    |
|                 |               |               |               |                 |          |    |
|                 |               |               |               |                 |          |    |
| (c)             |               |               |               |                 |          |    |

#### **User Activities**

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

![](_page_22_Picture_1.jpeg)

| LIONIC          |              |          |              |   | O Administrator C    | 😻 EN       | l+ |
|-----------------|--------------|----------|--------------|---|----------------------|------------|----|
| 🖬 Dashboard     | User Activit | ies      |              |   |                      |            |    |
| Devices         |              |          |              |   |                      |            |    |
| H Groups        | ty Sort - 7  |          |              |   | 2024-07-11 - 2024-07 | -11 🐵      |    |
| Groups          | Time         | User     | Source IP    | Message   |                      |            |    |
| Policy Template | 11:29:13     | omsodmin | 192,158.80.1 | Create new account LionisTest                                   |                      |            |    |
| whitelist       | 11:27:21     | cmsodmin | 192,168,60,1 | Create whitelist rule 968/5/89c031e1000(2a/5b)c (#5 840/7/4009) |                      |            |    |
| . Thursday      | 112759       | omsodmin | 192,168,80,1 | Create whitelist rule 66675117cC3tel00012c5b1c (95 6011276100)  |                      |            |    |
| © System        | 112656       | cmsodmin | 192168.60.1  | Delate whitekist rule 666/50d/90031a100012a/5614                |                      |            |    |
| Lines.          | 11⊈6:56      | amsadmin | 192168.60.1  | Delata whitekut rule 658/50d90031a10001265012                   |                      |            |    |
| USURE           | 11:26:56     | omsodmin | 192158,60,1  | Delete whitelist rule 668/50d7c031e00012e6610                   |                      |            |    |
| User Activities | 11:26:06     | omsodmin | 192,168,60,1 | Delate whitelist rule 668/50C8c031e100012c6500e                 |                      |            |    |
| Natification    | 11:26:17     | cmiadmin | 192358.60.1  | Ствате интелят ние 668/50/39c03/e)0001205b14 (#5 8100022701)    |                      |            |    |
| Signatures      | 11:26:17     | cmadmin  | 192158.60.1  | Create whitelist rule 568/50d9c03/e)00012a56/2 (IPS 840/714009) |                      |            |    |
| Portal Users    | 11:26:15     | omeadmin | 192,158,60,1 | Create whiteest rule 5585007c031e0000120500 (IPS 8011319000)    |                      |            |    |
|                 |              |          |              |   | 10 🛩                 | 1-10 of 16 |    |
|                 |              |          |              |   |                      |            |    |
|                 |              |          |              |   |                      |            |    |
|                 |              |          |              |   |                      |            |    |

#### 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.

| LIONIC      |               |                      | O Administrator | c  | O IN | 14 |
|-------------|---------------|----------------------|-----------------|----|------|----|
| 🖬 Dathboard | Notification  |                      |                 |    |      |    |
| Devices     |               |                      |                 |    |      |    |
| # Groups    | Enabled       |                      |                 |    |      |    |
| Threats     | SMTP Server   | mail.lionic.com      |                 |    |      |    |
| ③ System    | SMTP Port +   | 26                   |                 |    |      |    |
|             | SMTP Account  | Toniotesta Konic.com |                 |    |      |    |
|             | SMTP Password | 2                    |                 |    |      |    |
|             | Receiver      |                      |                 |    |      |    |
|             |               |                      |                 |    |      |    |
|             |               |                      |                 | Ap | ply  |    |
|             |               |                      |                 |    |      |    |
|             |               |                      |                 |    |      |    |
|             |               |                      |                 |    |      |    |
|             |               |                      |                 |    |      |    |
|             |               |                      |                 |    |      |    |
|             |               |                      |                 |    |      |    |
|             |               |                      |                 |    |      |    |
|             |               |                      |                 |    |      |    |

22

![](_page_23_Picture_1.jpeg)

#### 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.

![](_page_23_Figure_5.jpeg)

#### **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.

![](_page_24_Picture_1.jpeg)

| LIONIC          |              |   |              | Administrator | ¢   | S IN   | 14 |
|-----------------|--------------|---|--------------|---------------|-----|--------|----|
| 🖬 Dashboard     | Portal Users |   |              |               |     |        |    |
| Devices         |              |   |              |               |     |        |    |
| # Groups        | t≘ sort ~ 🖓  | ٩ |              |               |     | 0      |    |
| Threats         | Username     |   | Name         |               |     |        |    |
| ③ System        | Deter        |   | poter.pan    |               |     |        |    |
| Users.          | LionicFortal |   | LionicPortal |               |     |        |    |
| User Activities |              |   |              | ×             | • E | 2 of 2 |    |
| Notification    |              |   |              |               |     |        |    |
| Simotome        |              |   |              |               |     |        |    |
|                 |              |   |              |               |     |        |    |
| Portal Users    |              |   |              |               |     |        |    |
|                 |              |   |              |               |     |        |    |
|                 |              |   |              |               |     |        |    |
|                 |              |   |              |               |     |        |    |
|                 |              |   |              |               |     |        |    |
|                 |              |   |              |               |     |        |    |
|                 |              |   |              |               |     |        |    |
|                 |              |   |              |               |     |        |    |

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.

Ø

![](_page_25_Picture_1.jpeg)

![](_page_25_Picture_2.jpeg)

| Welcome to Cl | MS Portal |
|---------------|-----------|
| Log In        |           |
| Usemame       |           |
| Username      |           |
| Password      |           |
| Password      |           |

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

| Percenter  Devices  Devices Devices  Devices  Devices Device | LIONIC       |   |             |               |                  | 🖯 LionicPortal 🖌 🔿 EN |
|---|--------------|---|-------------|---------------|------------------|-----------------------|
| Investigation        Investigation  | Devices      | Devices                                       |             |               |                  |                       |
| Image: Solid Control        Image: Solid Control   | Threats      |   |             |               |                  |                       |
| MAC     Deside Nome     IP Address     Filmmatre Version       BEC02209000     myTerio     N02.868.8123     1.31       AGE00000001     myAri     192.868.8127     1.33  | Notification | t <u>a</u> sort ∼ 🖓                           |             |               |                  | 🖌 Actions - 土 🕲       |
| BBECDE20019BOC         my/fero         102168.8.23         1.31           ACE COBDOCRUI         my.Ark         192168.8.307         1.33  |              | MAC   | Device Name | IP Address    | Firmware Version |                       |
| 40500000001 myArk 1921618.307 1.3<br>10 - 1-2 or 2  |              | BBEC6203/BBC<br>(Inactivoted) (Theat Science) | myTera      | 192,168,8.123 |                  |                       |
| 2 μ τ τ τ<br>2 μ τ τ  |              | ACF509000901                                  | myArk       | 192.168.8 107 |                  |                       |
|   |              |   |             |               |                  | 10 v 1-2 of 2         |
|   |              |   |             |               |                  |                       |
|   |              |   |             |               |                  |                       |
|   |              |   |             |               |                  |                       |
|   |              |   |             |               |                  |                       |
|   |              |   |             |               |                  |                       |
|   |              |   |             |               |                  |                       |
|   |              |   |             |               |                  |                       |

![](_page_26_Picture_1.jpeg)

# **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

![](_page_27_Picture_1.jpeg)

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

![](_page_28_Picture_1.jpeg)

#### **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

![](_page_29_Picture_1.jpeg)

#### **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
```

![](_page_30_Picture_1.jpeg)

# **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

![](_page_31_Picture_1.jpeg)

© Copyright 2023 Lionic Corp. All rights reserved.

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

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