LIONIC
Security Solution Provider

ユーザーガイド

# CMS 中央管理システム

バージョン 2.0
更新日付 2024/07

# CMS ユーザーガイド



## 商標

Lionic は Lionic Corp. の商標です。

## Disclaimer

本マニュアルには技術的な誤りや誤植の可能性があるが、定期的に更新されます。このような変更は本マニュアルの新版に組み込まれます。

## Technical Support Lionic Corporation

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

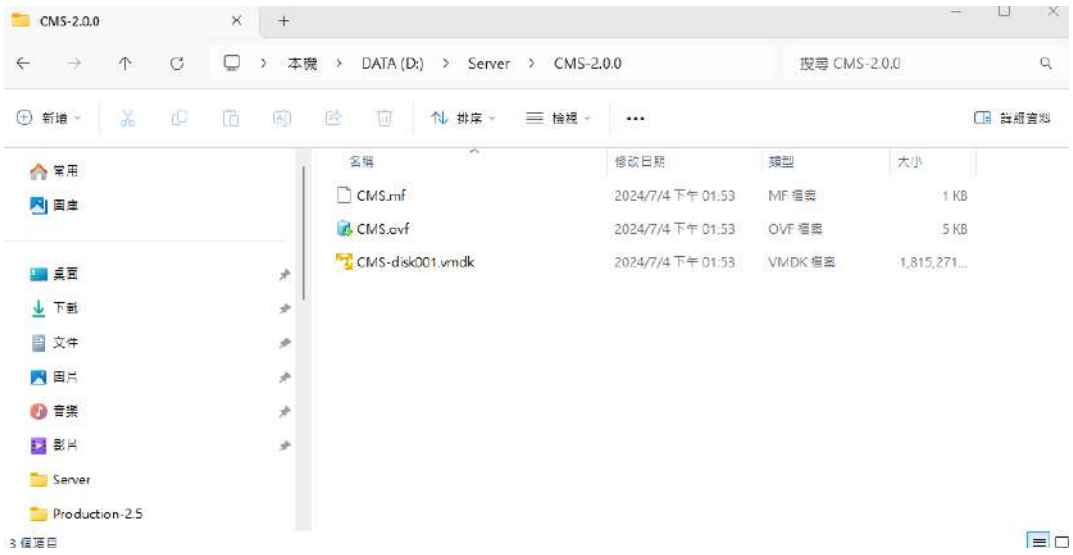
# 目次

# インストールと更新

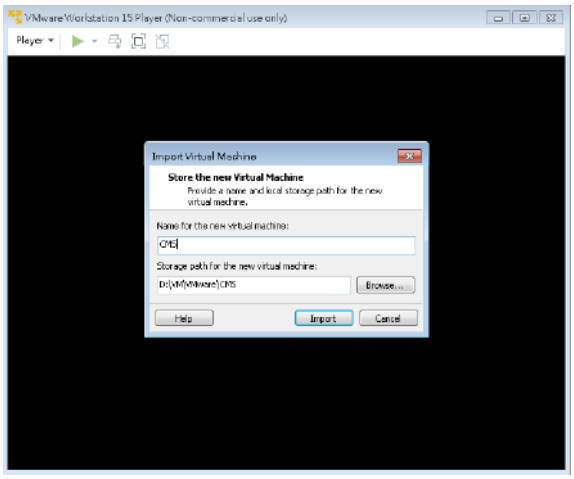
## インストール

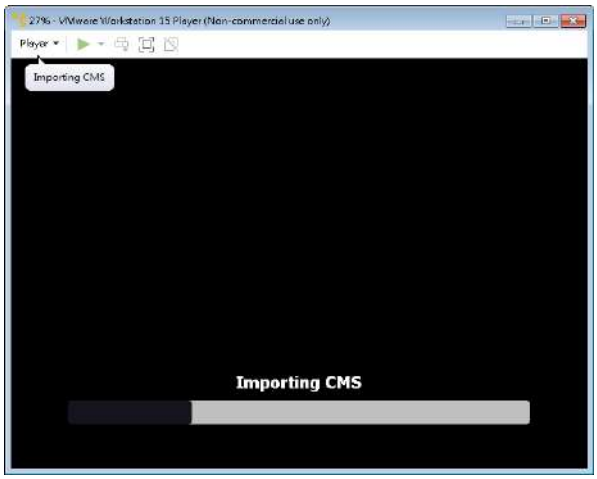
1. CMS VM をダウンロードします。


2. CMS VM インストーラでフォーマットを選択します。

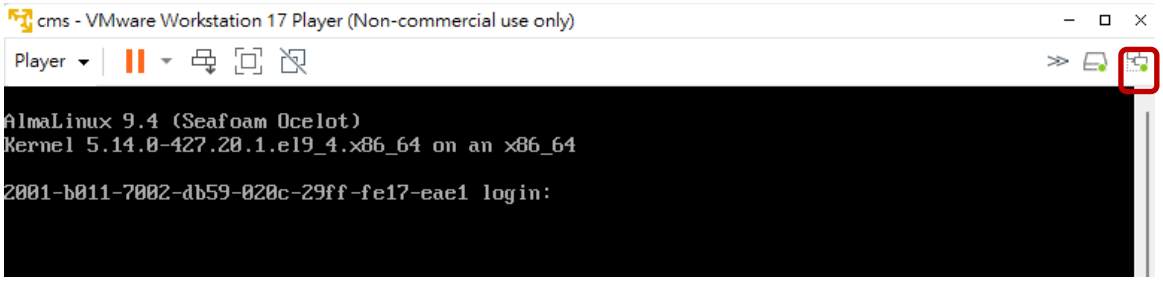


3. VM の名前を設定し、インポートします。

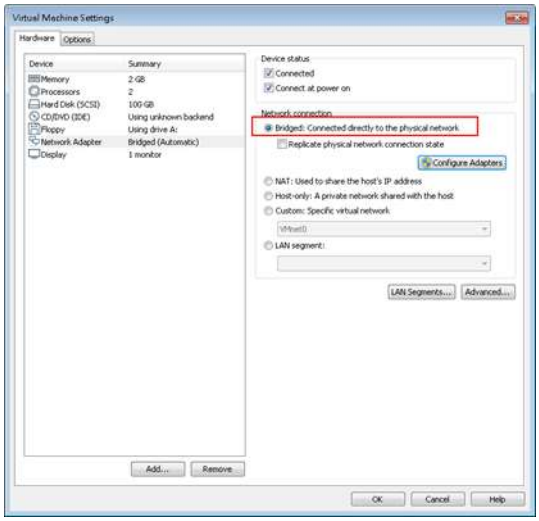



4. 下記の赤枠のアイコンを右クリックし、[Setting] を選択します。



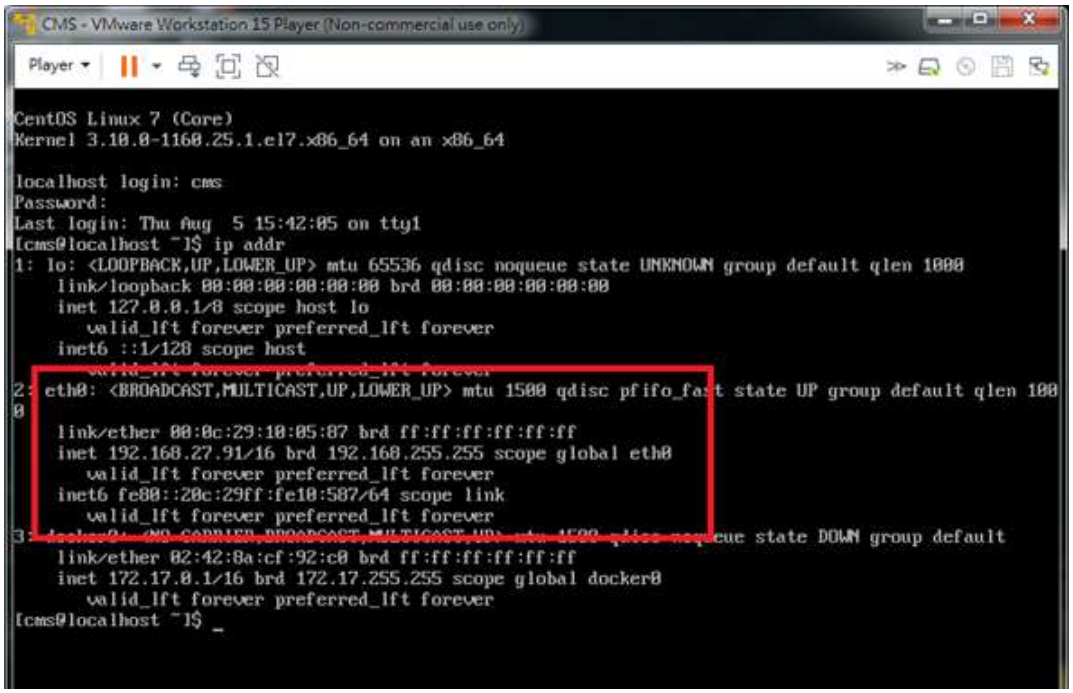

5. ネットワーク接続タイプを選択し、ネットワークカードを選択します。




6. ログイン ( cms / cms5678 )

ネットワーク情報の確認します。

```
ip addr
```

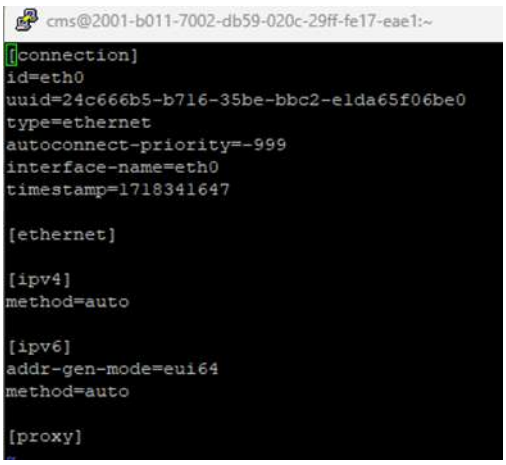



7. ネットワーク設定の変更します。

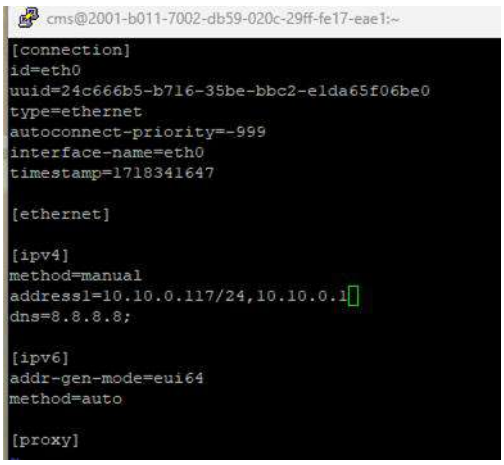
```
sudo vi /etc/NetworkManager/system-connections/eth0.nmconnection
```

変更完了後、ネットワークを再起動します。

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




DHCP




Static IP

8. 設定完了後、ブラウザーで http://CMS_IP:4221 にアクセスし、CMS 管理画面をログインします。
   デフォールトのユーザー名は「cmsadmin」、パスワードは「cmssecretpass」です。


## 更新

1. ディレクトリに移動します。

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

2. CMS-2.0.0.tar のファイルを上記のディレクトリにコピーします。

3. ファイルをインポートします。

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

4. バージョン情報を変更します。

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

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

5. Docker を再起動し、更新完了です。

```
docker compose up -d
```

## データーベースのバックアップ

1. Database を /home/cms/mongodb/backup/data.gz にバックアップします。

```
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. Database を復元します。

```
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
```

# 機能紹介

## ダッシュボード：

本 CMS が管理されているデバイスの情報や稼働状況を表示します。各統計情報や脅威事件の数、統計、ランキングなどの情報が含まれます。

## デバイスリスト：

デバイスの設定は本 CMS に接続されているものをリストします。

## グループリスト：

- **グループリスト：**この機能はデバイスをグループにして、管理します。
- **ポリシーテンプレート：**セキュリティポリシー( ンチウィルス、不正侵入防止、Web 脅威防止、ファイアウォールなど ) のテンプレートを作成できます。
- **ホワイトリスト：** 本 CMS で管理されるデバイスが誤検知された場合、この機能でバイパスにします。

## 脅威ログ：

各セキュリティ機能の検出記録を表示します。

## システム：

- **アカウント管理**：このページでアカウント追加と権限変更を行います。
- **管理履歴**：このページは管理者が Web GUI で行った設定変更記録をリストします。
- **通知**：この機能は、本 CMS で管理されたデバイスが脅威を検知した際に、指定されたメールアドレスに通知します。
- **シグネチャ**：CMS が更新サーバとして運行します。
- **ポータルユーザー管理**：ポータルユーザーを追加し、特定のデバイスを指定して、ポータルユーザーも CMS で指定されたデバイスを管理できます。

# ダッシュボード

本 CMS が管理されているデバイスの情報や稼働状況を表示します。各統計情報や脅威事件の数、統計、ランキングなどの情報が含まれています。

**検査統計情報：**本 CMS 管理されるデバイスの検査情報を表示します。スキャンされたファイル数、リンク数、フロー数、パケット数が含まれます。

**最近の脅威：**最新の検出記録を表示します。

**脅威事件の統計：**各セキュリティ機能の検出統計情報を表示します。

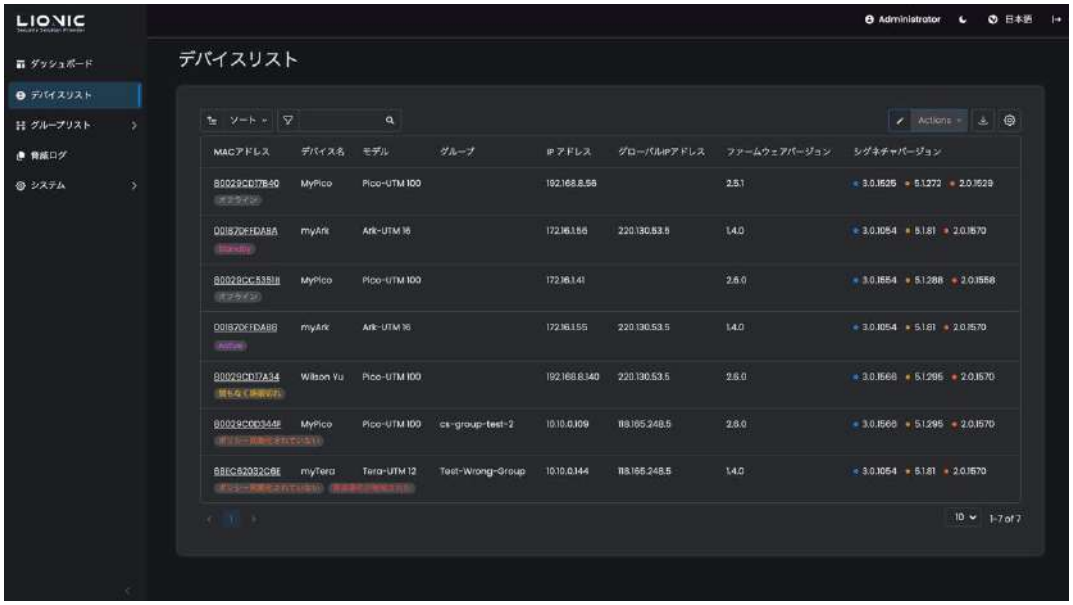
**脅威事件ランキング：**検出数の順に合計または各機能のランキングやデバイスごとの攻撃受けた回数のランキングを表示します。


**脅威事件の数：**毎日、各機能の検出数を表示します。

**攻撃されたデバイスランキング：**デバイスの検出数の前十位を表示します。

# デバイスリスト

本 CMS には、接続されているデバイスの設定がリストされます。また、デバイスの接続状況なども表示されます。さらに、デバイスのリモート管理も可能です。



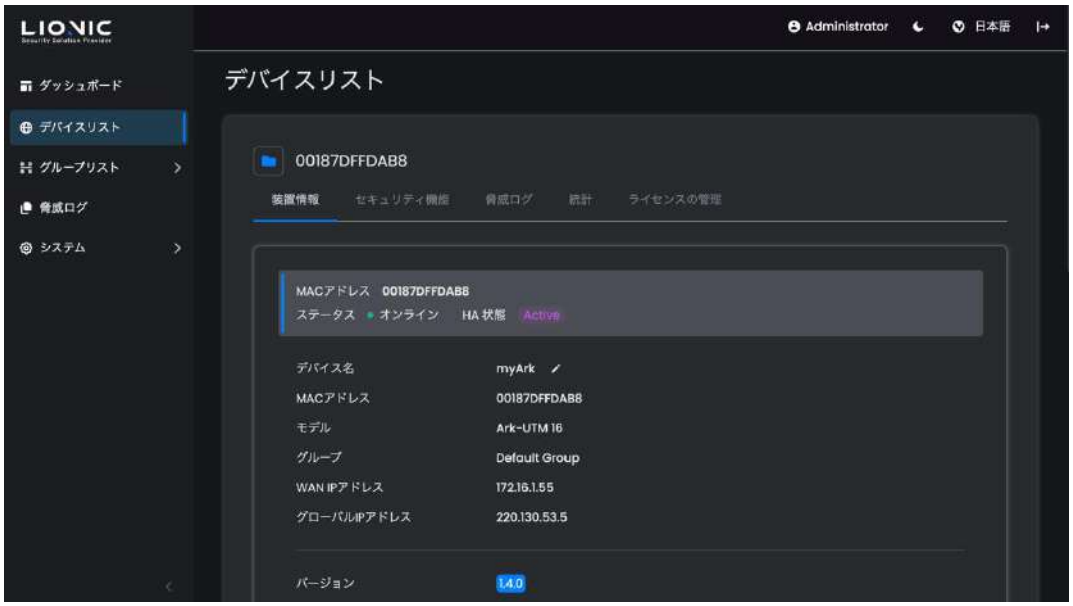

- **ソート：** [ソート] をクリックしてソートキーが選択し、並び順の昇順と降順が切り換えます。
- **フィルター：**クリックして、フィルター条件を入力します。
- **Actions：**をクリックして、デバイス選択した後、 [Actions] を選択します。
  - **グループ設定の同期化（デバイスを選択しないと、設定変更のデバイスがすべて同期されます。）：**デバイスのグループを指定された後、本機能で同期化を行います。
  - **アクティベートする：**デバイスが初めて使用する際には、デバイスがインターネットにアクセスできる環境でアクティベートコードを入力して、ライセンスをアクティベートします。
  - **ライセンス更新する：**デバイスはライセンス期限切れの 30 日前に通知を表示します。ライセンス更新コードを入力て、ライセンス有効期限を延長することができます。
  - **ファームウェア更新（特定のデバイスを選択しない場合、すべてのデバイスが更新されます）：**デバイスを最新版に更新します。

- **シグネチャ更新 ( 特定のデバイスを選択しない場合、すべてのデバイスが更新されます )**: デバイスをシグネチャを確認させ、最新版に更新します。
- **デバイスを削除**：デバイスを削除します。

- **CSV を出力する**：デバイスリストを CVS ファイルを書き出します。

**デバイス情報 ：**

[デバイスリスト] で、デバイスの MAC アドレスをクリックして、デバイスの詳細情報が確認でき、セキュリティポリシーが変更できます。




- **ホワイトリスト：** 本 CMS 管理されるデバイスが誤検知された場合、この機能でバイパスにします。
  - ホワイトリストの追加： [脅威ログ] のタブでバイパスしたい事件を探して、[+] をクリックしてホワイトリストに追加します。
  - ホワイトリストの削除： [セキュリティ機能] の各機能のタブや [脅威ログ] のタブで削除します。

  **※ こちらのホワイトリストは各デバイス専属のです。グローバルではないです。**

➢ **デバイスの個別のセキュリティポリシーを変更されると、すぐに適用されます。「グループ設定の同期化」を実行する必要がありません。**

➢ **セキュリティポリシー、脅威ログの詳しい説明について、各デバイスのマニュアルをご参考ください。**

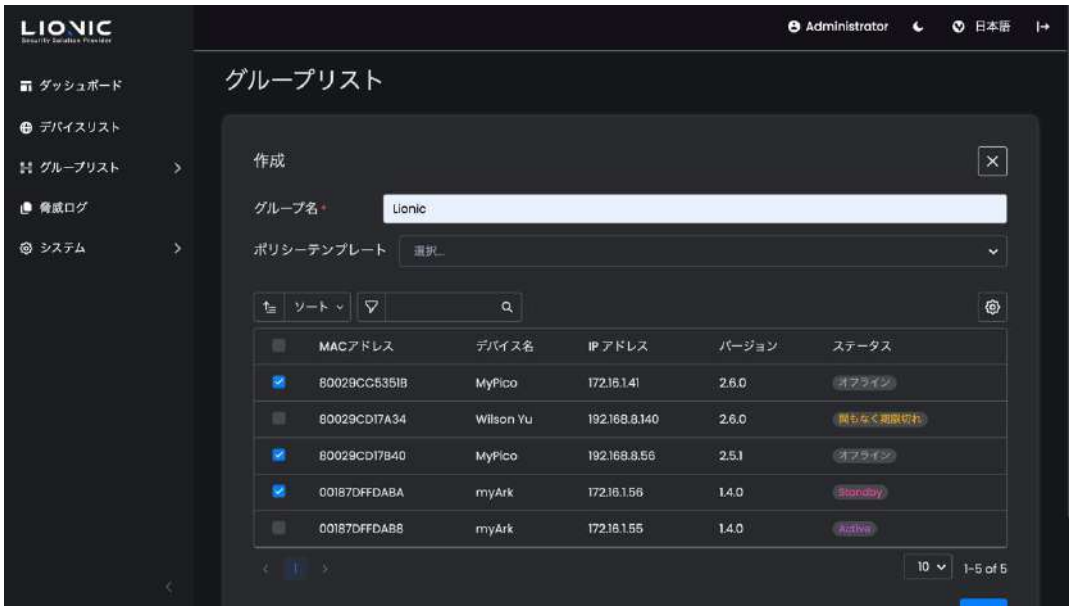
# グループリスト

この機能はデバイスをグループにして、管理します。

## グループリスト

1. [グループリスト] のページで、 [+] をクリックし、新しいグループを作成します。


2. グループ名を入力し、デバイスを選択して、グループに属します。



3. 確認後、 [適用] をクリックします。


4. 新しいグループを作成されました。


※ 作成完了後、デバイスリストのページに🖉をクリックし、[Actions] の [グループ設定の同期化] を行うことが必要です。

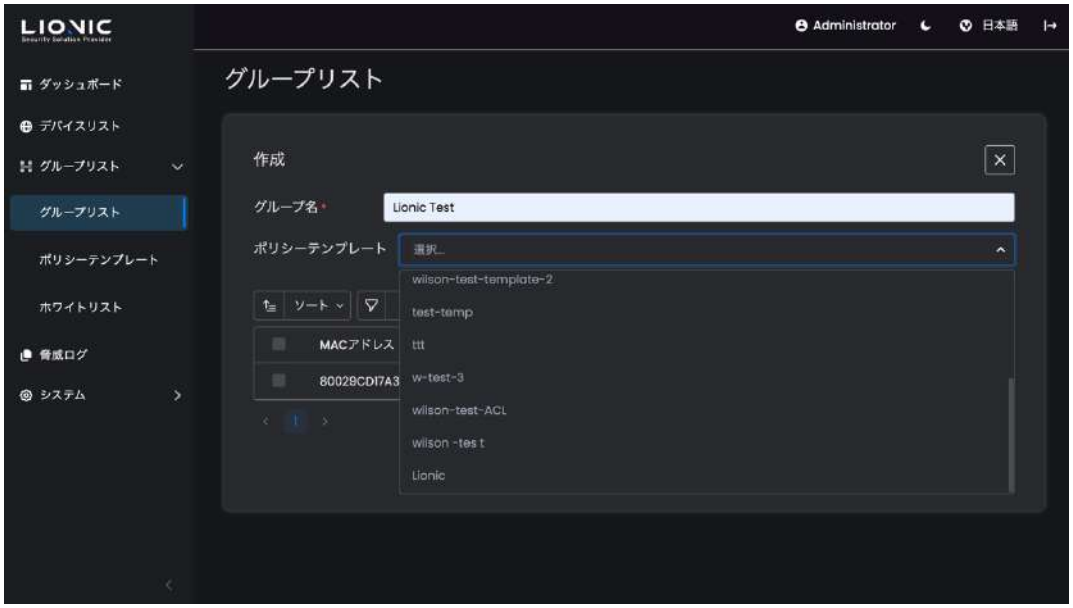
## ポリシーテンプレート

ポリシーテンプレートで、新しいグループを作成する時、適用できます。

1. [ポリシーテンプレート] のページで、 [+] をクリックし、テンプレートを作成します。


2. テンプレート名、セキュリティポリシーを設定し、[適用]をクリックします。

3. 作成完了後、新しいグループを作成する際に、ポリシーテンプレートを選択できます。

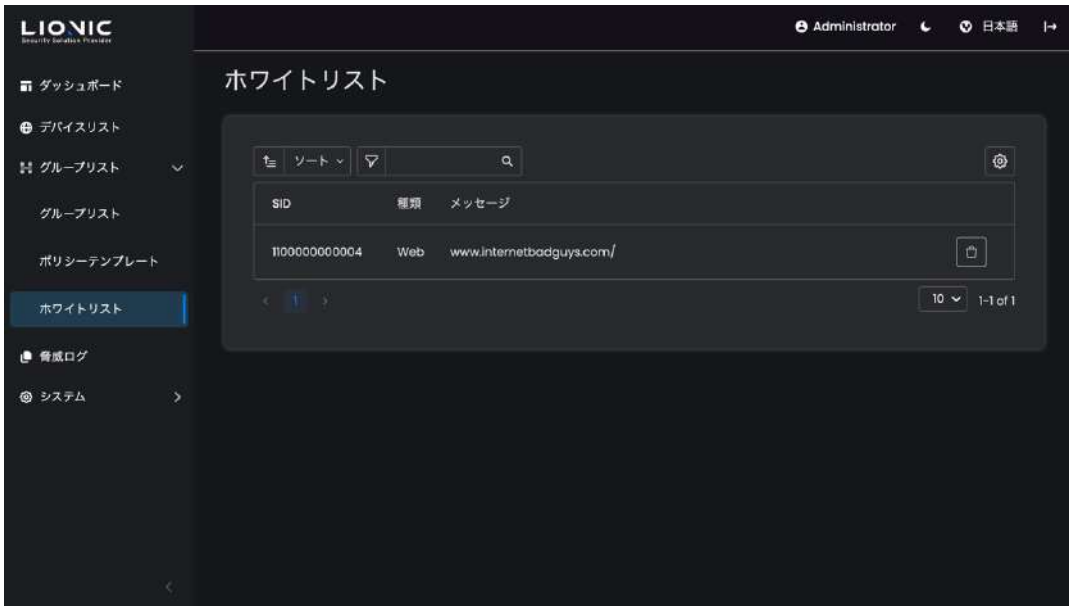


## ホワイトリスト ( グローバル )

本 CMS 管理されるデバイスが誤検知された場合、この機能でバイパスにします。

1. [脅威ログ] のページでバイパスしたい事件を探し、 [+] をクリックして、ホワイトリストに追加します。

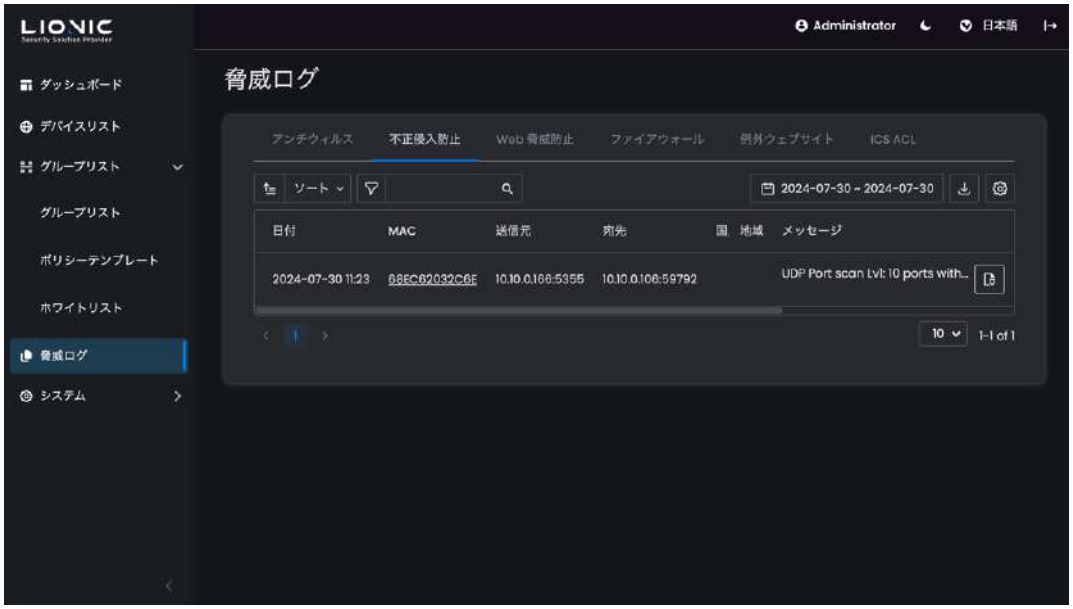

2. 追加した後、 [ホワイトリスト] のページで表示します。




※ 脅威ログのページで追加されたのはグローバルのホワイトリストになります。追加した後、デバイスリストのページに✎をクリックし、[Actions] の [グループ設定の同期化] を行うことが必要です。

# 脅威ログ

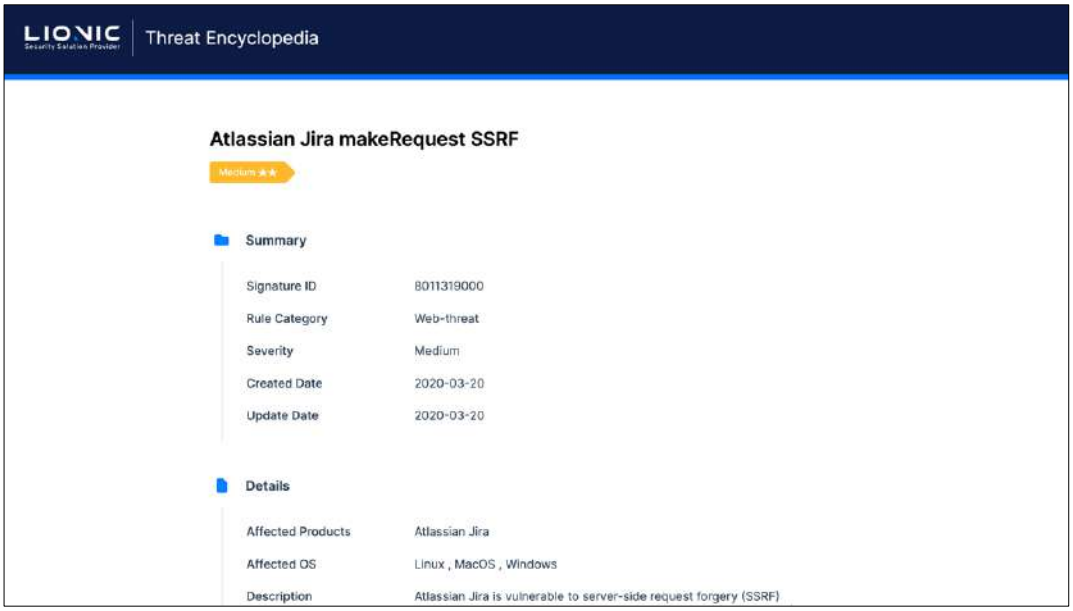
本 CMS 管理されるデバイスは脅威を検出されたあと、本 CMS にアップロードされます。各セキュリティ機能の脅威は各自のタブに表示される。




- ソート：[ソート] をクリックしてソートキーが選択し、並び順の昇順と降順が切り換えます
- **フィルター**：クリックして、フィルター条件を入力します。
- **日付でフィルター**：指定の日付範囲でのログを表示されます。
- **CSV を出力する**：脅威ログを CVS ファイルを書き出します。
- **ホワイトリスト**：誤検知された場合、この機能でバイパスにします。
    - ホワイトリストの追加： [脅威ログ] のページでバイパスしたい事件を探して、[+] をクリックしてホワイトリストに追加します。

    ※ 脅威ログのページで追加されたのはグローバルのホワイトリストになります。追加した後、デバイスリストのページにをクリックし、[Actions] の [グループ設定の同期化] を行うことが必要です。
    - ホワイトリストの削除： [ホワイトリスト] のページで削除します。

- **Threat Encyclopedia**：[脅威ログ]のページで、不正侵入防止の記録の をクリックして、- Threat Encyclopedia にアクセスし、当不正侵入の分析と対策を参考します。



# システム

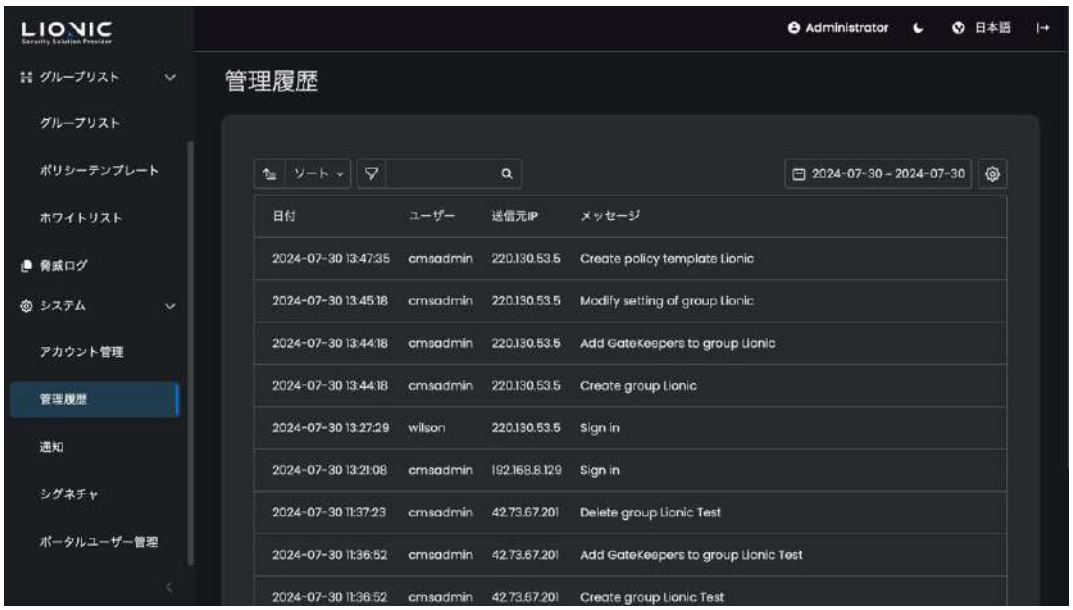
## アカウント管理

[アカウント管理] のページでアカウント追加と権限変更を行えます。

- 管理者：最高レベルの権限を持っています。
- 標準ユーザー：アカウント管理と管理履歴のページをアクセスできません。
- 閲覧者：閲覧のみ可能で、設定はできません。

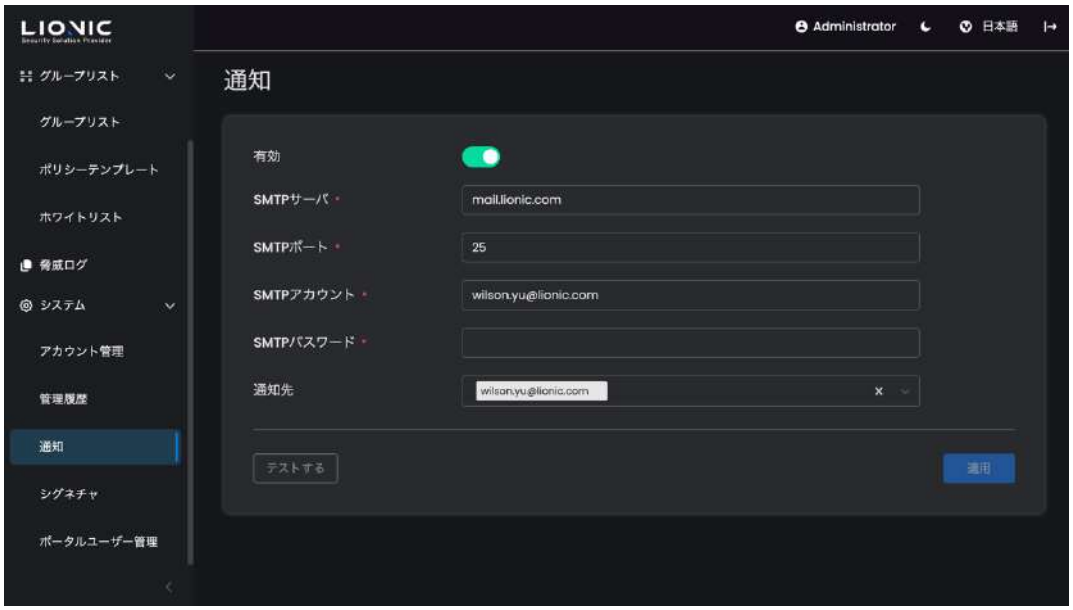

## 管理履歴

[管理履歴] このページは管理者が Web GUI での設定変更記録をリストします。



## 通知

[通知] の機能は本 CMS 管理されたデバイスが脅威を検知した時、E メールで指定のメールアドレスに送ります。設定完了後、 [適用] をクリックして本機能を起動します。




## シグネチャ

ユーザーのネットワークがインターネットにアクセスできない場合、 CMS がファームウェアとシグネチャの更新サーバとして使われます。

※ インターネットにアクセスできない環境のみ使われます。この機能が必要の場合は、Lionic や代理店のテクニカルサポート窓口にお問い合わせください。

## ポータルユーザー管理

パートナーが CMS 上の一部のデバイスを管理する必要がある場合、CMS 管理者はポータルサイト( CMS ポータル )を起動し、ポータルユーザーを作成してデバイスを割り当てで、各パートナーがそれぞれの責任範囲内のデバイスをポータルユーザーとして管理します。


1. CMS ポータル機能を起動します。

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

2. ファイアウォールの 80 Port を開きます。

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

3. CMS Server を再起動します。

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

4. 設定完了後、ブラウザーで http://CMS_IP にあくせすし、CMS Portal を使います。



5. ポータルユーザーがログインして、責任範囲のデバイスを管理します。

# 各機能の設定

## NTP の設定

デフォールトの設定で、CMS は 2.almalinux.pool.ntp.org の NTP サーバで時刻同期を行います。設定ファイルで NTP サーバを変更できます。下記は変更のプロセスです。

1. 設定ファイルを編集します。

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

2. 2.almalinux.pool.ntp.org を他の NTP サーバに変更します。

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

3. Chronyd を再起動で適用します。

```
sudo systemctl restart chronyd
```

## Firewall の設定

デフォールトの設定は全ての Port が開かれています。

- 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 は firewalld でファイアウォールを管理します。ssh の機能が不要の場合は、sshd の 22 Port を禁止します。下記はコマンドです。

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

指定の IP アドレスのみで ssh を使えます。

```
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
```

上記のポリシーを削除します。

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

指定の IP アドレスのみで Web GUI にアクセスできます・

```
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
```

## タイムゾーンの設定

デフォールトのタイムゾーンは Asia/Taipei です。変更できます。

1. 設定ファイルを編集します。

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

2. 例えば、Asia/Japan に変更します。

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

3. CMS Server を再起動します。

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

## HTTPS Web UI

デフォールトの設定で CMS の Web UI は暗号化されないトラフィックです。
下記は HTTPS を使用するプロセスです。

1. 設定ファイルを編集します。

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

2. CMS_CERT と CMS_KEY を指定します。

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

3. CMS Server を再起動します。

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

4. https://CMS_IP:4221 で HTTPS を使います。ご自身の証明書を使用したい場合は、設定を通じて証明書を上書きすることが必要です。方法は下記の通りです。

```
    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
```

## ストレージの追加

下記のコマンドで 100GB のストレージを追加します。

1. CMS をシャットダウンし、VMWare/VirtualBox 通じで 200GB に変更します。

2. CMS を起動し、下記のコマンドを入力します。

```
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
```

# トラブルシューティング

## アカウントロックの解除

パスワードを 5 分内で 10 回間違った場合、アカウントは 5 分間ロックされます。
下記のコマンドでアカウントロックを解除します。

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

## パスワードを忘れた場合

管理者のパスワードを忘れた場合、下記のコマンドでパスワードを「123456」に変更します。

```
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.