LIONIC
Security Solution Provider

使用者手冊

中央管理系統

版本 2.0

更新日期 2024/07

Lionic Corp. www.lionic.com

CMS 使用手冊

版權聲明

商標

鴻璟科技之商標已註冊使用

免責聲明

鴻璟科技保留對本手冊中所描述的產品/程序進行新增/更改的權利並旨在提供準確的訊息。本手冊可能包含意外的印刷錯誤，因此將定期針對此類訊息進行更改已修正此類錯誤。

技術支援聯絡資訊 鴻璟科技股份有限公司

信箱: sales@lionic.com 電話: +886-3-5789399 傳真: +886-3-5789595

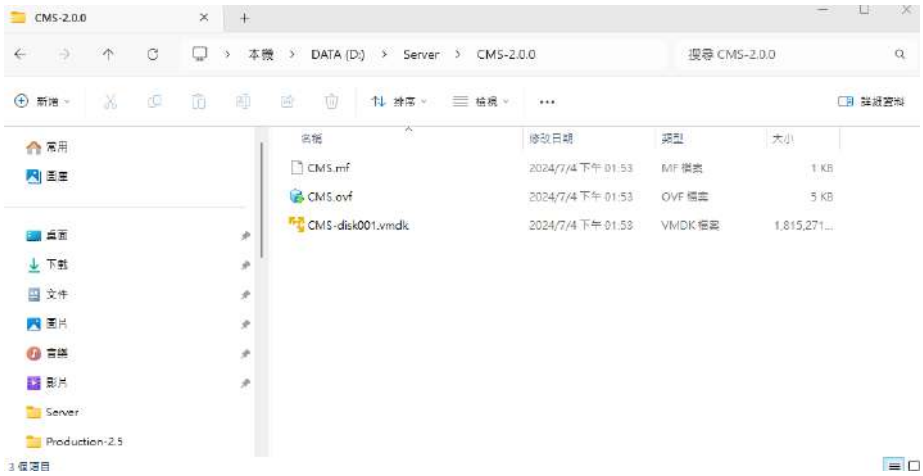
目錄

建置步驟

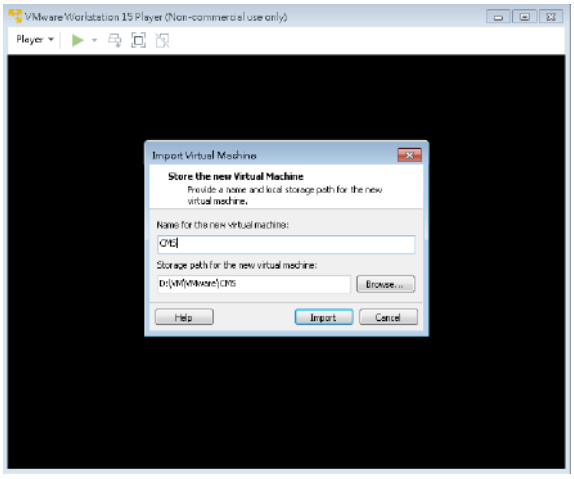
安裝步驟：

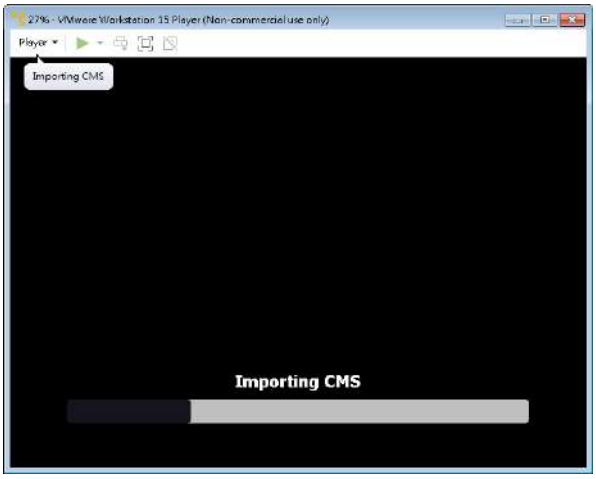
1. 下載 CMS VM 安裝檔

2. 選擇 CMS VM 安裝檔格式

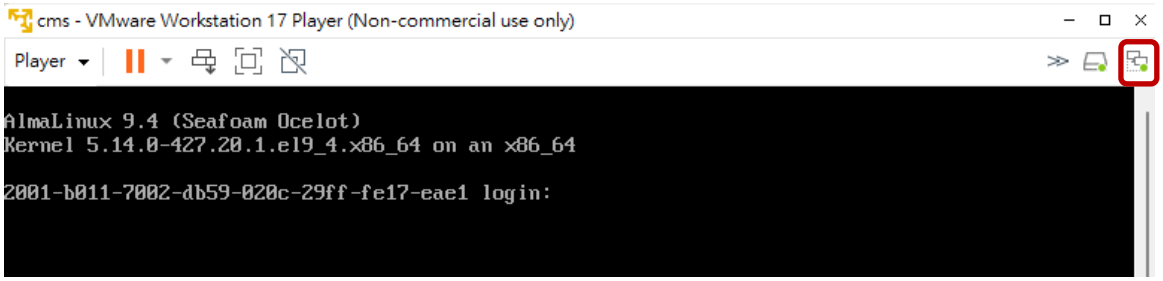


3. 建立 VM 名稱並匯入

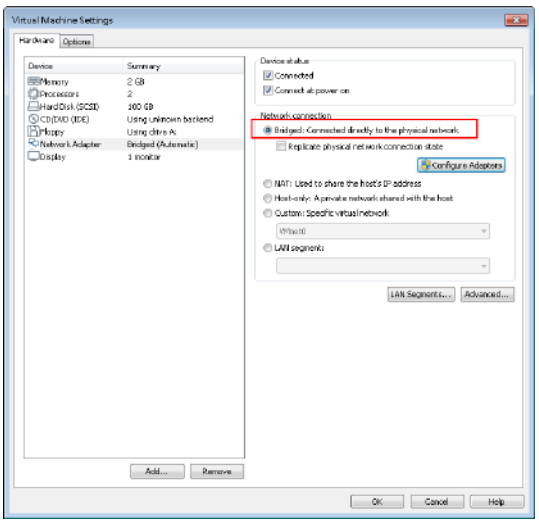


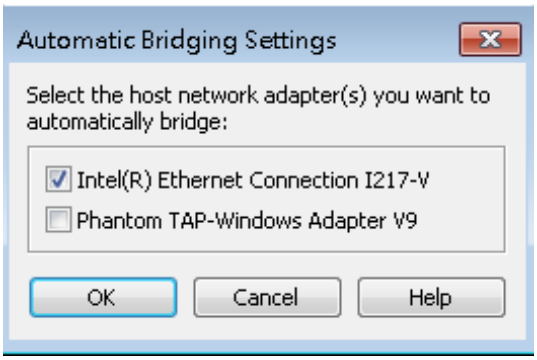


4. 點擊圖示右鍵，選擇 [Setting]



5. 選擇連線模式，選擇網卡

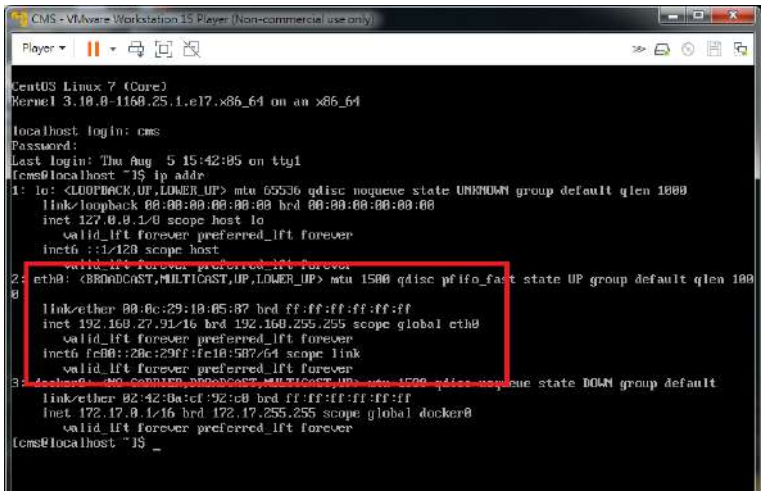




6. 登入 (cms / cms5678)

查看網路資訊

```
ip addr
```

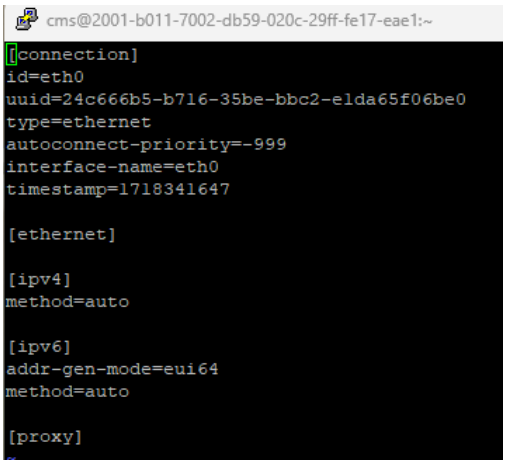


7. 更改網路設置

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

變更後重啟網路設定

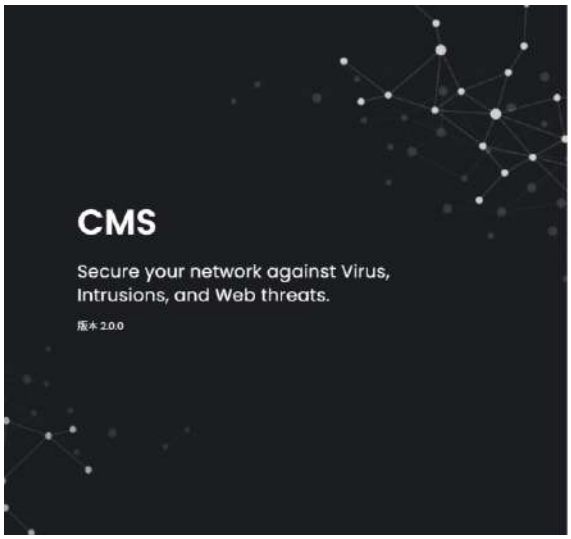
```
sudo nmcli c reload

sudo nmcli d reapply eth0
```



DHCP

Static IP

8. 設定完成後，請使用網頁瀏覽器開啟 http://CMS_IP:4221，即可登入
   預設帳密：cmsadmin / cmssecretpass



升級步驟

1. 指向至檔案夾

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

2. 將 CMS-2.0.0.tar 放至檔案夾

3. 將檔案引入

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

4. 將檔案版本更改

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

```
```

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

```
```

5. 重啟 Docker 即可完成

```
docker compose up -d
```

備份資料庫

1. 備份 Database 資料至 /home/cms/mongodb/backup/data.gz

```
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. 還原 Database 資料

```
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
```

功能概述

儀表板：

[儀表板] 會顯示 CMS 管理裝置的運行狀態與裝置資訊，包含檢測歷程、近期威脅、威脅統計或排行、威脅數量、受攻擊裝置排行等。

裝置清單：

[裝置清單] 會顯示設定連線至 CMS 管理的裝置。

群組：

- **群組：**[群組] 功能可以將不同裝置編成群組。
- **安全規則模板：**制定各項安全防護功能的執行規則模板，包含防毒系統、入侵防禦、惡意網頁阻擋、防火牆等。
- **白名單：**當 CMS 管理裝置的資安防護功能破壞了安全的檔案或阻擋了受信任的連線時，可以透過白名單功能恢復正常使用。

資安紀錄：

顯示各項安全防護功能的執行紀錄。

系統管理：

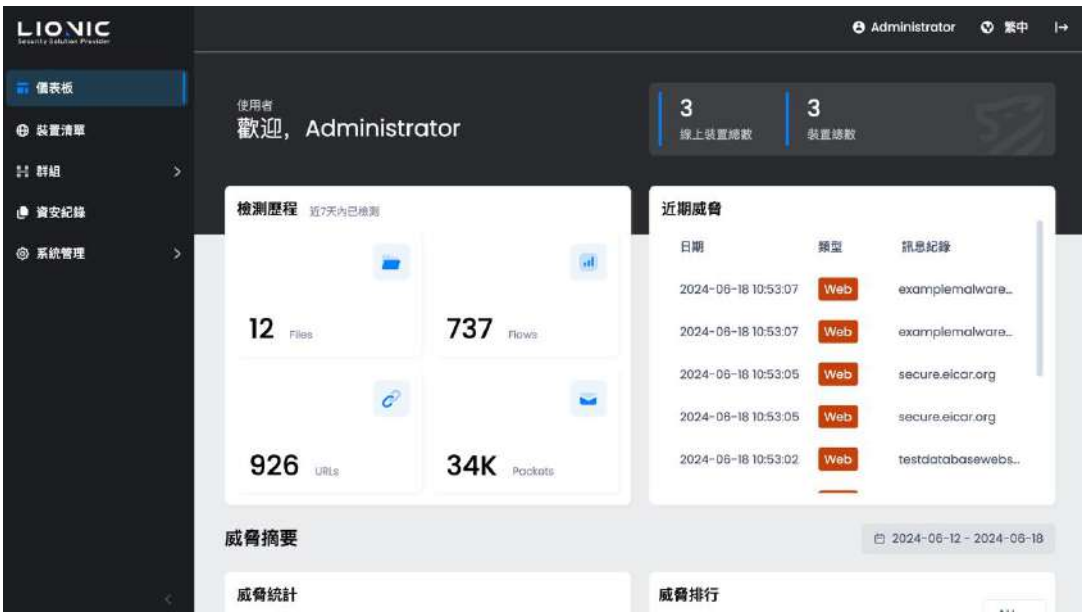
- **使用者：**[使用者] 頁面可以新增使用者並建立帳密＆權限控管。
- **管理日誌：**[管理日誌] 頁面會列出 CMS 管理員在網頁控制介面上所做的各項設定變更。
- **通知：**[通知] 功能可以在 CMS 管理裝置偵測到資安威脅時，將威脅資訊以電子郵件寄到指定信箱。除此之外，也能定時將檢測歷程、威脅統計、系統異常紀錄等資訊，寄送到指定信箱。
- **特徵碼：**當使用者因網路連線限制需要使用 CMS 當韌體及特徵碼更新伺服器，可透過此頁面上傳與管理韌體與特徵碼更新。
- **入口網站使用者：**管理者可以新增入口網站的使用者，並為其分配特定裝置，使其能夠使用 CMS 進行管理

儀表板

CMS 管理裝置的運行狀態與裝置資訊皆會於此顯示，包含檢測歷程、近期威脅、威脅統計或排行、威脅數量、受攻擊裝置排行等。

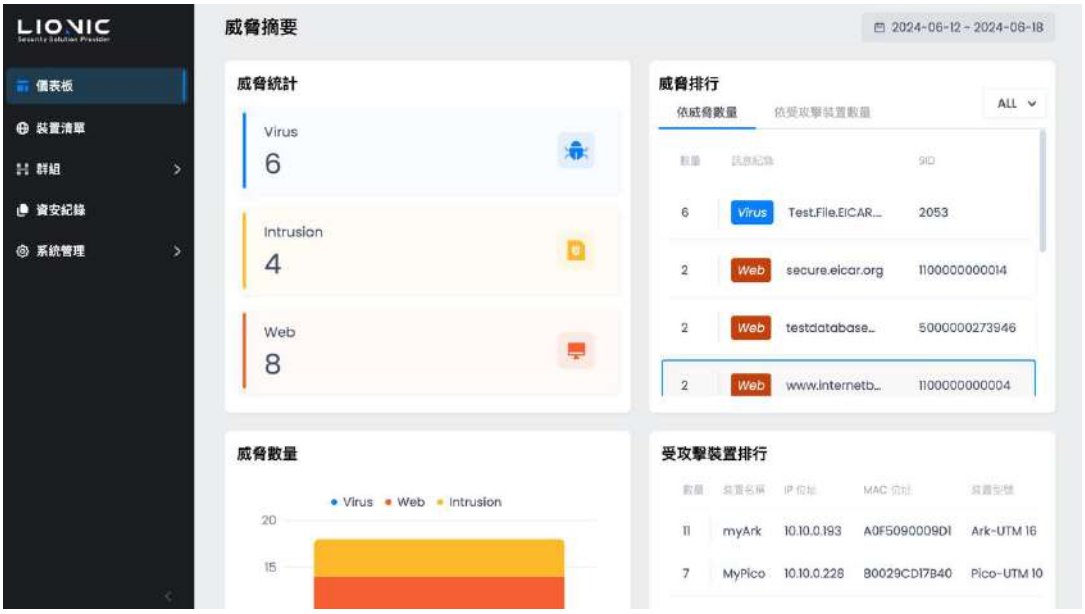
檢測歷程：顯示 CMS 管理裝置完成檢測的檔案數量、連結數量、封包流數量及封包數量。

近期威脅：顯示 CMS 管理裝置的威脅最新資料。



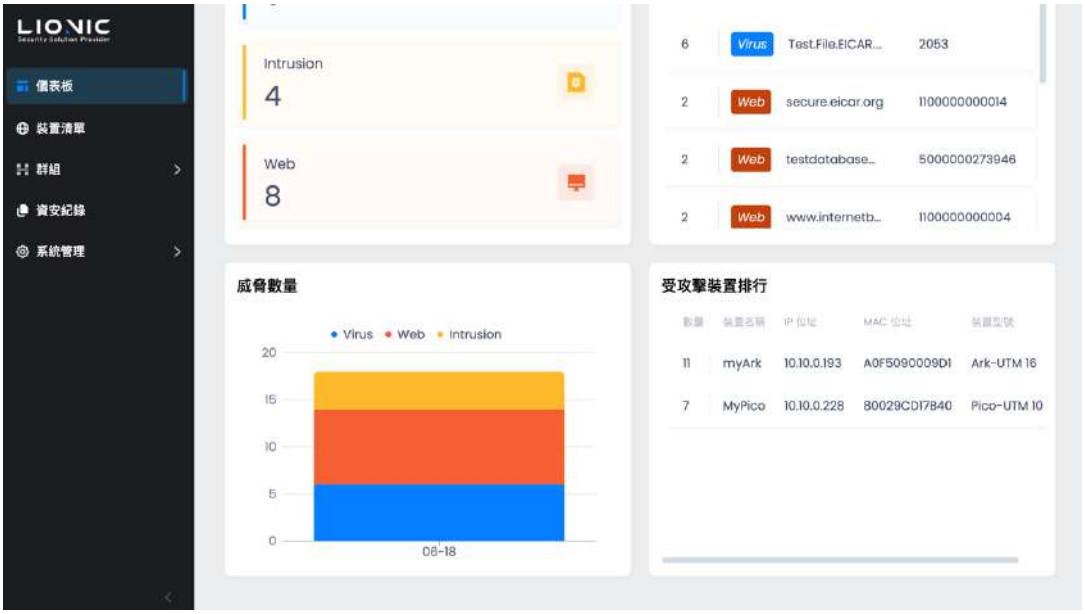
威脅統計：顯示 CMS 管理裝置的近期偵測到的威脅事件數量。

威脅排行：統計 CMS 管理裝置各項安全防護功能偵測到的資安紀錄，依照偵測次數多寡列出全部或各類威脅排行，以及依照裝置受攻擊次數排行。



威脅數量：統計每日各項安全防護功能偵測到的資安紀錄數量。

受攻擊裝置排行：統計各項安全防護功能偵測到的資安紀錄，依照受攻擊次數多寡列出前十名裝置排行。



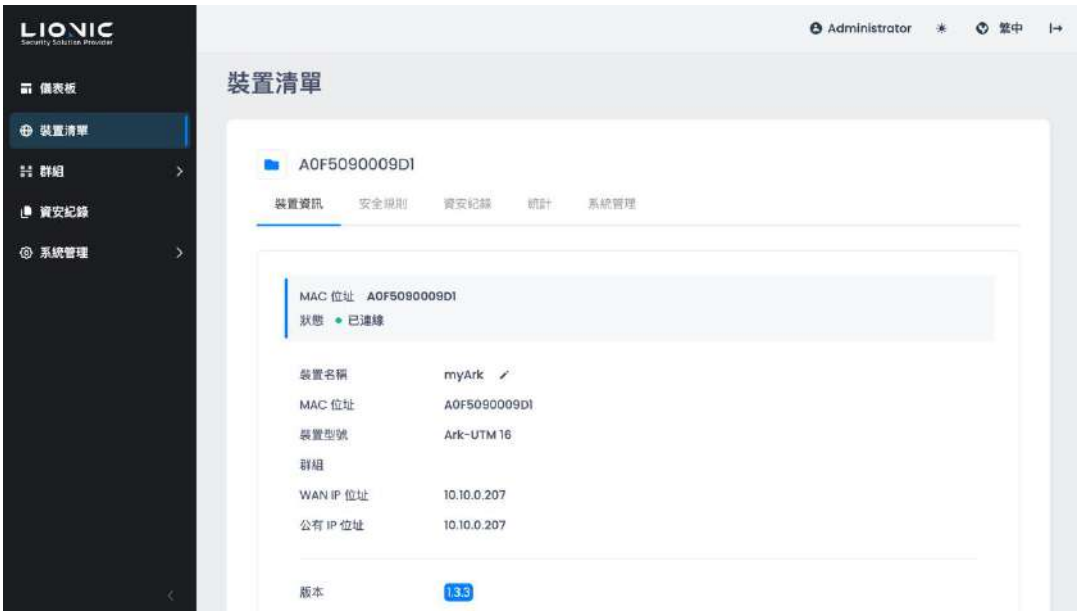
裝置清單

在 [裝置清單] 頁面裡，顯示已連線至 CMS 的裝置，使用者可透過 CMS 遠端管理裝置。

- **排序**：點擊 [排序] 選擇類別，點擊可更改順逆序 。
- **篩選**：點擊輸入框篩選裝置。
- **動作**：點擊 選取設備，選取後點擊 [動作] 選擇操作。
  - **同步群組設定 (可不選取裝置，如有設定異動裝置，全同步動作):** 群組功能設定後，需此功能同步群組裝置。
  - **啟用授權：**當第一次使用裝置時，請在裝置可連接至網際網路的環境下將授權啟用碼填入將延展碼填入後，即可啟用授權，以確保裝置能提供完整的資安防護功能。
  - **延展授權：**CMS 管理裝置會在授權到期前 30 天顯示提醒，請儘速完成授權訂閱以取得延展碼，將延展碼填入後，即可延展授權期限。
  - **更新韌體 (可不選取裝置，未更新最新版本裝置，全同步動作):** 將裝置更新至最新版本。
  - **更新特徵碼 (可不選取裝置，未更新最新版本裝置，全同步動作):** 裝置將立刻至特徵碼伺服器檢查並下載最新特徵碼。
  - **刪除設備：**刪除管理裝置
- **匯出至 CSV：**將裝置清單批次匯出成 CSV 檔。

裝置資訊 ：

在 [裝置清單] 中，點擊裝置 MAC，可以進到裝置，並可查看裝置資訊、調整防護設定等。



- **白名單**：當 CMS 管理裝置的資安防護功能破壞了安全的檔案或阻擋了受信任的連線時，可以透過白名單功能恢復正常使用。
    - 新增白名單規則：請在 [資安紀錄] 頁面中搜尋被破壞或被阻擋的事件紀錄後，點擊 [+] 加入白名單。
    - 刪除白名單規則：在 [安全規則] 頁面中可刪除指定白名單規則。

    ※ 此白名單為個別裝置設定，不為全域白名單。

➢ **個別裝置安全規則修改後是立即生效，不需再「同步群組設定」**

➢ **安全規則、資安紀錄細節說明請參考裝置使用手冊**

群組

[群組] 功能可以將不同裝置編成群組，制定各項安全防護功能。

群組

1. 在 [群組] 頁面裡，使用者可以選擇 [+] 以加入裝置交由群組共同管理

2. 建立群組名稱，選取群組管理的裝置。

3. 確認後 [套用]

4. 新建成功

※ 建立完成後，需至裝置清單點擊 ，選取後點擊 [動作] 選擇 [同步群組設定]。

安全規則範本

建立安全規則模板，在新建群組時可快速套用，保持一致的安全規則。

1. 在 [安全規則範本] 頁面裡，使用者可以選擇 [+] 以加入範本。

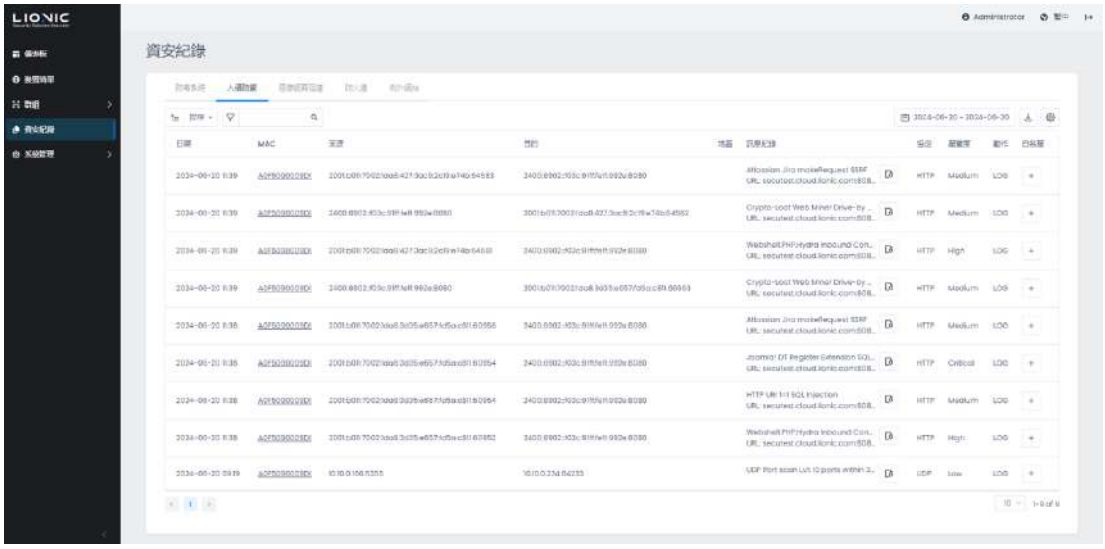
2. 建立範本名稱，調整規則設定，確認後 [套用]。

3. 完成後，在新建群組時，即可套用安全規則模板。

白名單（全域白名單）：

當 CMS 管理裝置的資安防護功能破壞了安全的檔案或阻擋了受信任的連線時，可以透過白名單功能恢復正常使用。

1. 在 [資安紀錄] 頁面裡，使用者可以選擇 [+] 以加入白名單。

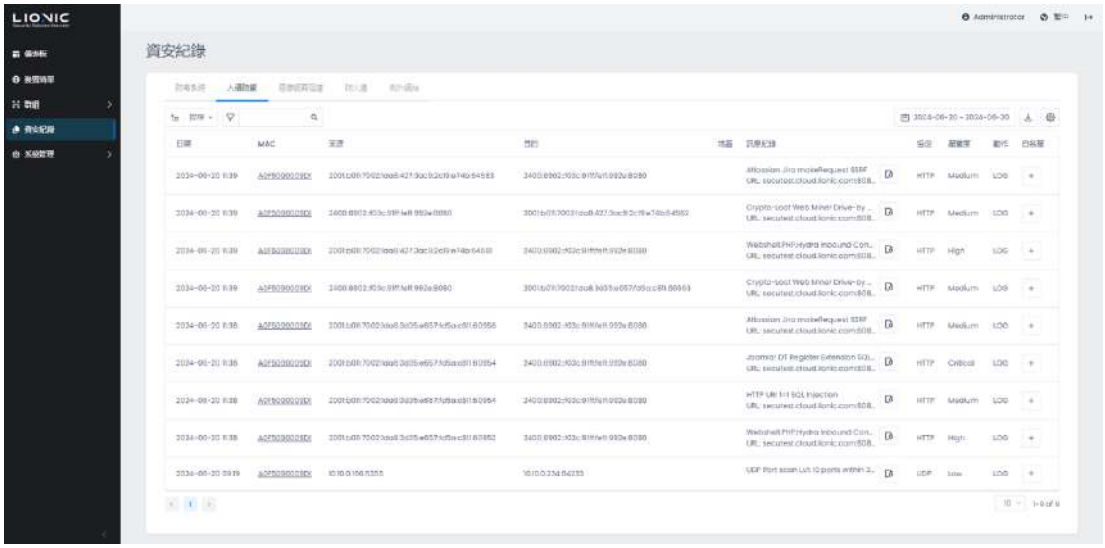


2. 加入成功後，使用者可以在 [白名單] 頁面裡顯示。

※ 資安紀錄白名單會加入全域白名單，建立完成後，需至裝置清單點擊 ，選取後點擊 [動作] 選擇 [同步群組設定]。

資安紀錄

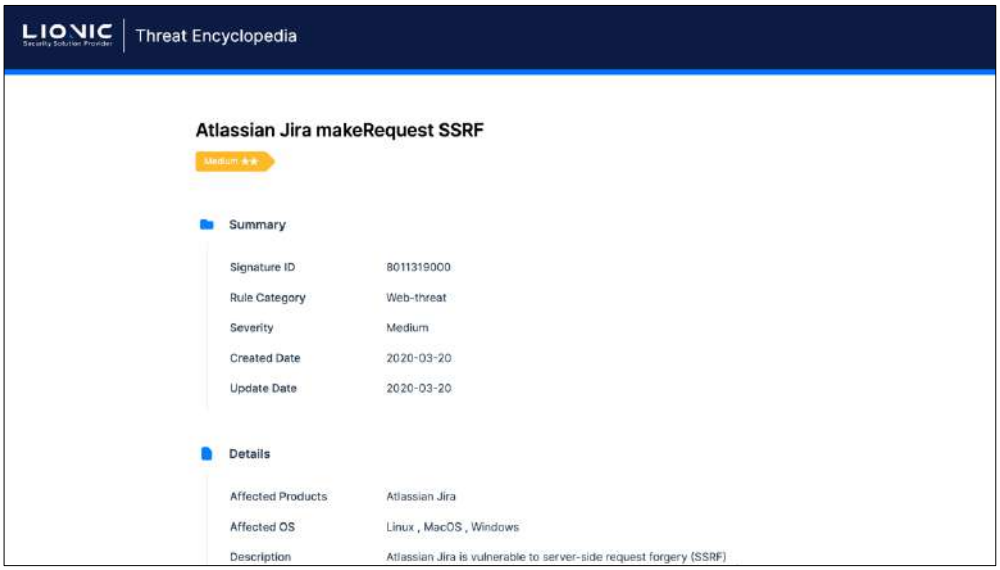
在 CMS 管理裝置偵測到資安威脅後上傳至 CMS，相關的威脅資訊會依照不同的資安防護功能顯示在對應的 [資安紀錄] 頁面裡。



- **排序**：將紀錄，選擇排序類別，點擊圖示可更改排序 。
- **篩選**：將紀錄條件篩選。
- **日期區間篩選**：將紀錄篩選日期區間資料。
- **匯出至 CSV**：將紀錄批次匯出成 CSV 檔。
- **白名單**：當 CMS 管理裝置的資安防護功能破壞了安全的檔案或阻擋了受信任的連線時，可以透過白名單功能恢復正常使用。
    - 新增白名單規則：請在 [資安紀錄] 頁面中搜尋被破壞或被阻擋的事件紀錄後，點擊 [+] 加入白名單。

    ※ 資安紀錄白名單會加入全域白名單，建立完成後，需至裝置清單點擊 ，選取後點擊 [動作] 選擇 [同步群組設定]。
    - 刪除白名單規則：在 [白名單] 頁面中可刪除指定白名單規則。

- **威脅百科：**在 [入侵防禦] 的資安紀錄中，點擊 ，可以查詢該項攻擊的分析與解決方案。



系統管理

使用者

[使用者] 頁面可以新增使用者並建立帳密＆權限控管。

- 管理員：擁有所有權限。
- 一般：和管理員的差別在於無法管理使用者與檢視管理日誌。
- 檢視者：只能檢視，不能任何設定。

管理日誌

[管理日誌] 頁面會列出 CMS 管理員在網頁控制介面上所做的各項設定變更。

通知

[通知] 功能可以在 CMS 管理裝置偵測到資安威脅時上傳至 CMS，將威脅資訊以電子郵件寄到指定信箱。請在輸入框內填入正確設定值後點擊 [套用] 以完成設定。

特徵碼

當使用者因網路連線限制需要使用 CMS 當韌體及特徵碼更新伺服器，可透過此頁面上傳與管理韌體與特徵碼更新。

※ 僅供完全無法連線至網際網路的場域使用，啟用前請先聯繫 LIONIC 或銷售夥伴的技術支援窗口。

入口網站使用者

若有不同權限的合作夥伴要協助管理 CMS 上的部分裝置，CMS 管理員可以透過開放入口網站（CMS Portal）、創建入口網站使用者並分配裝置，讓不同的合作夥伴以入口網站使用者身份管理各自負責的裝置。

1. 開啟 CMS Portal 功能

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

    ...

    environment:

- CMS_ADDRESS=0.0.0.0:4221

- CMS_PORTAL_ADDRESS=0.0.0.0:80
```

2. 開啟防火牆 80 Port

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

sudo firewall-cmd –reload
```

3. 重啟 CMS Server

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

4. 設定完成後完成後，即可登入 CMS Portal，請使用網頁瀏覽器開啟 http://CMS_IP，即可登入

5. 即可控管管理者分配的管理裝置

功能設定

NTP 配置

默認情況下，CMS 會連接至 2.almalinux.pool.ntp.org 進行時間同步，可以通過修改配置文件來更改為想使用的 NTP Server，具體步驟如下：

1. 編輯檔案

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

2. 將 2.almalinux.pool.ntp.org 更改為想使用的 NTP server

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

3. 重啟 chronyd 生效

```
sudo systemctl restart chronyd
```

Firewall 配置

預設 Port 皆為開啟

- 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 使用 firewalld 管理防火牆規則。如不需要 ssh 功能，可以禁用 sshd 服務 22 Port

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

允許特定 IP 才可連線 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
```

刪除 IP 連線 ssh

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

允許特定 IP 才可連線 Web GUI

```
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
```

時區設定

預設時區為 Asia/Taipei.可以修改更換時區

1. 編輯檔案

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

2. 更換時區為 Asia/Japan 做範例

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

3. 重啟 CMS Server

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

HTTPS Web UI

默認情況下，CMS 的 Web UI 訪問是未加密的。以下步驟啟用 HTTPS 加密。

1. 編輯檔案

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

2. 將 CMS_CERT 和 CMS_KEY 添加到環境設置中

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

3. 重啟 CMS Server

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

4. 現在用戶可以通過 https://CMS_IP:4221。如果您想使用自己的憑證，需要通過設置來覆蓋憑證，如下所示。

```
    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
```

擴增儲存空間

按照以下步驟增加 100GB 儲存空間

1. 關閉 CMS 並通過 VMWare/VirtualBox 將磁碟容量擴展到 200GB。

2. 開啟 CMS 並輸入以下命令。

```
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
```

故障排除

解鎖帳戶

如果在 5 分鐘內出現 10 次密碼錯誤，帳戶將被鎖定 5 分鐘。使用以下命令解鎖帳戶

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

忘記密碼

如果管理員帳戶密碼忘記，用戶可以從控制台更改密碼。以下命令將帳戶的密碼更改為 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.