

_{使用者手册} 中央管理系統

版本 2.0 更新日期 2024/07

Lionic Corp. www.lionic.com



CMS 使用手册

版權聲明

© 2024 鴻璟科技股份有限公司·版權所有

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 鴻環科技股份有限公司

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



目錄

建置步驟	3
安裝步驟	3
升級步驟	7
功能概述	8
儀表板	9
裝置清單1	1
群組1	3
群組1	.3
安全規則模板1	.5
白名單1	.7
資安紀錄13	8
系統管理	0
使用者29	0
管理日誌	0
通知2	1
特徵碼	1
入口網站使用者	2
功能設定24	4
NTP 配置	24
Firewall 配置	4
時區設定2	:5
Https web ui	6
擴增儲存空間	:7
故障排除23	8
解鎖帳戶2	28



建置步驟

安裝步驟:

1. 下載 CMS VM 安裝檔

CMS-2.0.0	TM/SSR
•)	
	大小 精調時間
CMS.mf	
CMS.ovt	
CMS-dlek001.midk	L7 GB 2 days ago
3 Gidm	
LIONIC Share service	

2. 選擇 CMS VM 安裝檔格式

	-	antino antananana atawa at				1.42
⇒ ↑ U	し > 本8	ĝ > DATA (D;) > Server >	CMS-2.0.0	搜尋 CMS	-2.0.0	q
ти X 🧔	D Ø	🖄 🖞 🐴 🕸 🗧 🗄	檜硯 ◇ ・・・			詳細資料
▲ 常用	1	名稱	修改日期	羽型	大小	
- 	- 1	CMS.mf	2024/7/4 下午 01:53	MF檔素	1 KB	
		😸 CMS.ovf	2024/7/4 下午 01:53	OVF 標案	5 KB	
1 1 1	*	CMS-disk001.vmdk	2024/7/4下午01:53	VMDK檔案	1,815,271	
L Tet						
1 文件						
R III						
) = 1X	1					
28月						
Server						
Production-2.5						



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

rtual Machine Settings Hardware Options	:		
Device Monory Processors HardDisk (SCSI) Colybo (ICSI) Poppy Reference & Adapter Display	Serrerary 2 68 2 300 68 Using unknown backend Using dhra A: Bhidged (Automatic) 3 incretor	Device a data Connected Connected & prover on Retract-connection B Bridged: Connected directly in the physical motionsk. B B B B B B B B B B B B B B B B B B B	
		HAT Levit to share the hord's the address Heat-only: Approximation in Monte The Address Heat-only: Approximation of this the heat Casternis Section (Versammer Address) HAT segments LAN Segments Advanced	Automatic Bridging Settings Select the host network adapter(s) you want to automatically bridge:
			 Intel(R) Ethernet Connection I217-V Phantom TAP-Windows Adapter V9
	Add Remove	OK Canod Hep	OK Cancel Help



6. 登入 (cms / cms5678)

查看網路資訊

ip addr

CMS - VIJ/ware Workstation 15 Player (Non-commercial use only)	
Player - 👖 - 号 它 泡	* 🗗 🕤 🗒
CentOS Linux 7 (Core) Mernel 3.10.0-1160.25.1.e17.x86_64 on an x86_64	
localhost login: cms Password: Last login: The Aug 5 15:42:95 on ttyl	
<pre>fcms9lofalhost ~13 ip addr 1: lo: <loopdeck.up.lomer.up> mtu 65536 qdisc noqueue state UNKNOMM group - link/loopback 80:08:08:08:08:08 hol 08:08:08:08:08:08:08 inet 127.0.0.1/0 scope host lo valid_ift forever preferred_ift forever inet6::1/20 scope host</loopdeck.up.lomer.up></pre>	default ylen 1000
 wild 11: forever preferred 11: forever eth8: (BRONDCAST,MULTCAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fa:t state link/ether 80:80:29:10:05:87 bed ff:ff:ff:ff:ff:ff inet 192.16U.27.91/16 bed 192.16U.255.255 scope global eth8 valid_lft forever preferred_lft forever inet600:200:291f:fc10:577.64 scope link valid_lft forever preferred_lft forever 	UP group default glen 189 te DOWN group default
link/ether 02:42:0a:cf:92:c0 brd ff:ff:ff:ff:ff:ff:ff het 172.17.0.1/16 brd 172.17.255.255 scope global docker0 valid_LFt forever preferred_Ift forever tems0localhost "15 _	goog alanti

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



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



歡迎使用 CMS

豆人	
使用者名稱	
使用者名稱	
密碼	
密碼	54



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。

LIONIC						e	Administrator 🔇 🌋	‡ I→
前 儀表板		使用者			12 1	2		
⊕ 裝置清單		歡迎, Administro	ator		3 線上装置總数	う 装置誘数		
11 群組		v						
● 資安紀錄		檢測歷程 近7天內已檢測			近期威脅			14
◎ 系統管理	>			a	日期	類型	訊思記錄	
		-			2024-06-18 10:53:07	Web	examplemalware	
		12 Files	737 Flows		2024-06-18 10:53:07	Web	examplemalware	
					2024-06-18 10:53:05	Web	secure.eicar.org	
		C'		-	2024-06-18 10:53:05	Web	secure.eicar.org	
		926 unts	34K Pockets		2024-06-18 10:53:02	Web	testdatabasewebs.	
		威脅摘要					2024-06-12 - 2024-00	6-18
	- ej	威脅統計			威脅排行			



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

LIONIC Security Balance Previder	威脅摘要				曲 2024-06-12	- 2024-06-18
青 儀表板	威脅統計		威脅排行			ALL 🗸
④ 裝置清單	Virus		NUM N ROM	化现代除行用的用		
i stali >	6	A.	秋節 品族紀	B-	SID	
9 資安紀錄	Interview		6 Virus	Test.File.EICAI	R 2053	
③系統管理 >	4		2 Web	secure.elcar.c	org 110000	000014
	Web	-	2 Web	testdatabase	50000	00273946
	8		2 Web	www.internet	b 110000	000004
	威脅數量		受攻擊裝置排行	ŧ.		
	• Virus • Web • Intrusion		化醋 建聚化酶	IP 位地	MAC (03)	利用法性
	20		TI myArk	10.10.0.193	A0F5090009D1	Ark-UTM 16
	15	_	7 MyPico	10.10.0.228	80029CD17B40	Pico-UTM 10

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。

						e Administrator
罰 備表板		裝置清單				
⊕ 装置清單						
H MM	>	t≘ 翔序 ~ ▽	Q			/ 助作 - 土 ④
● 資安記錄		MAC 位址	裝置名稱	群組	IP 位址	粉體版本
③ 系統管理	>	80029CD17840 已伯潮到成務	MyPico		10.10.0.228	2.5.4
		A0F5090009D1 已值源到或量 Active	myArk		10.10.0.193	1.3.3
		<u>68EC62031B0C</u> 即共進即	myTera		10.10.0.71	131
		< 1 5				10 ~ 1-3 of 3
	- C					

- 획 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
 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。
 - 删除設備: 删除管理裝置
- 🕹 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。

LIONIC Security Solution Provider			Administrator *	◎ 紫中	l→
司 儀表板	裝置清單				
₩ 群組 ● 留安記録	> A0F5090009D1 装置資訊 安全規則 資源	纪錄 統計 系統領理			
④ 系統管理	·				
	MAC 位址 A0F5090009D1 狀態 ● 已連線				
	载置名稱 my MAC 位址 A09	urk /			
	暴戰型號 Ark 群組	UTM 16			
	WAN IP 位址 10.1 公有 IP 位址 10.1	.0.207			
	< 颜本 13.	1			

- 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

						O Administrator	ø	繁中	l→
司 備 表板	群	組							
⊕ 裝置清單									
₩ 群組	~	ங #序 ∽ ▽		۹			+	0	
群組		群組名稱	設備數量	防毒系統	入侵防禦	惡意網頁阻擋			
安全規則模板					尚無資料				
白名單									
● 資安記錄		< 1 2				10 ~	0-0	of 0	
④ 系統管理	>								

2. 建立群組名稱·選取群組管理的裝置。

								e a	dministrator	◎ 繁中	l→
罰 備表板	Į	詳組									
⊕ 裝置清單											
H MA	~	建立								×	
群組		群組名稱。	Lionic								
安全規則模板		安全規則模板	選擇							~	
白名草		t≘ 排序 ~ ♡	٩							0	
● 資安記錄		MAC 位址	裝置名稱	IP 位址	版本	狀態					
◎ 系統管理	>	■ 80029CD178	40 MyPico	10.10.0.228	2.5.4	已連線	已認用	已候測對發鋒			
		A0F5090005	Dì myArk	10.10.0.193	1.3.3	已讓線	已做用	已候湖到城會	Active		
		68EC620318	DC myTera	10.10.0.71	1.3.1	Einin	已撤用	STREET.			
		< 1 >							10 ~	1-3 of 3	
										新加	



3. 確認後 [套用]

A TONIC							8	administrator	♥ 繁中
備表板 君	羊組								
裝置清單									
詳組 ~	Lionic 🖌								
\$FAB	装置清單 防毒系統	入侵防制	思意相頁险檔	地理調	JAR K	防火牆	例外網站	SSL/ILS 植现	
安全規則模板	1≝ 排序 ~ ▽		٩						+
白名單	MAC 位址	裝置名稱	IP位址	版本	狀態				
資安紀錄	80029CD17840	MyPico	10.10.0.228	2.5.4	EWW	Emm	已值測到或價		
系统管理 >	A0F5090009D1	myArk	10.10.0.193	1.3.3	已遵線	已設用	已值該倒成費	Activo	
	68EC62031B0C	myTera	10.10.0.71	1.3.1	已通線	已政用	部將油額		
	< 1 >							10 🗸	1-3 of 3
								取消	書用

4. 新建成功

LIONIC									🖯 Administr	ator	♥ 繁中	
罰 備表板		群組										
⊕ 装置清單												
计数据	~	た 御序 ~	∇	Q						+	0	
群組		群組名稱	設備數量	防毒系统		入侵防禦		惡意網頁阻	ŝ			
安全規則模板		Lionic	3	記錄	已啟用	建路	已放用	紀錄	已線用	Ó		
白名單		s 1 2								10 ~	1-1 of 1	
● 資安記錄	3											
④ 系統管理	>											
◎ 系統管理	>											
	- 4											

※ 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。

					O Administrator	ø	繁中	→
訂 備表板	安全規則範本							
⊕ 裝置清單								
H ### ~	き 脚序 ~ 🏷	Q				+	0	
群組	群組名稱	防寒系統	入侵防禦	恶意娴真阻擋				
安全規則模板			一 光報認知					
白名單								
● 資安紀錄	< 1 3				10 ~	0~0	of 0	
④ 系統管理 >								

2. 建立範本名稱,調整規則設定,確認後 [套用]。

		e Administrator ● 繁中 i→
罰 催表板	建立	×
⊕ 裝置清單	範本名稱 Lionic	
H ### ~	防毒系统 入侵防御 恐服或責阻擋 地理封譯 防火牆 例外網站	SSL/TLS 檢測
若羊 A目		
安全規則模板	防毒系統	
白名單	已飲用	
資安記錄	重为作	紀錄並且破壞 ~
 承給管理 > 	使用雲鏡病毒資料庫排指檔案 使用雪茄肉毒資料時指檔案形能確保檔案況到最先整約肉毒補指防護,但會影響 部分下載、上傳檔質時的傳輸這度。	



3. 完成後,在新建群組時,即可套用安全規則模板。

						e Administr	ator 🔹	e l	• 梁中	→
罰 儀表板	ŧ	詳組								
⊕ 裝置清單										
∺ 群組	~	建立							×	
群組		群組名稱・	LionicTest							
安全規則模板		安全規則模板	選擇						^	
白名單		惶 排序 ∽ ∽	Lionic	-					÷	
.● 資安記錄		MAC	: 位址	裝置名稱	IP 位址	版本	狀態			
③ 系統管理	>			Q	向無資料					
		3 1 3					10	•] (0-0 of 0	
	e .								and a	



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。

	資安紀錄										
	Instan Add	- CHERCH	that they								
*	A. 1999 - 17	_								20.00	1 5
	1 1 1 1 V			144	1.000	and an initial of		d anna-s	(-)) - juin		
\$4.	Die	Moc	22	50	1540	108.63		80	10.814	#211=	088
	2039-00+10 1139	A04800000000	2001000/7902/068427/3009/2019/0740/64688	3400.6902-103c p1124/1.0924/8080		Affossion Jio molefiequest 915 CRL socutors cloud Jonic com858.	D	RITE	stealum	108	٠
	2034-00-20 0:30	A17503000303	2400 0002-003: 3781 kell 9504 0.000	3001b0/0.20021co8.427.3ec/02c70w74ec04882		Crypto-soot Web Miver Drive-By URL: securiest cloud lionic contd08.	D	HETE	Medium	100	+
	2014-04-20 9.39	ALEBLINDUND	2001-00175021001142730c18249w14045468	3400-0002-403-51 404 83224 8080		WebshaltPHP-Hydra Incound Con. OIL: socurrent cloud lionic com/808.	D	4877P	High	109	+
	2034-08-20 0.89	A0F809000101	1400 8802.45% 3W MR 9624.8090	3001407170021008.8651w0657/05cc.81.80963		Crypto-soct Web time/ Drive-by - VRL secures.cloud.lonic.com/808.	63	HTTP	Notum	1/28	+
	2024-05-20 1.38	a0/502000304	1001.500.70023do8.3c05.e6574d5oxd8(.80556	3400-9902-403;: 01M/e11-912w 6080		Attonion 3ro moleflequest 8397 UR: securest cloud lonic com608.	ß	HTTP	Medium	100	+
	2024-06-20 8:36	A015030003DI	2001:00117002144483605956774d5axx81180354	2400-0802-030-0105e0-010e 6080		Joomio Of Register Extension T(s) (Rc; sincularit cloud Jonic contable.	D	6072	Critical	100	•
	202+-08-20 6:36	A07500000000	2001-501-1002/sdas 3036-a68776/dax/dit16/0164	3400.0002.H03c-01HAuti-0024-0080		HTP VM HI SQL Injection VML recurrenced advice correction.	0	HTT:	Maalum	100	+
	2024-00-30 H 38	AGEDOROOOJDA	2001:500-70023dail.3x25+65375c5a+c31167862	3400 6002-x23c 3197w1 992w 6080		Webshill Philippyshia lebound Clin. URL Securest cloud lionic com/508.	D	6772	нат	100	+
	2034-00-20 0979	ACTORNOTICS	10 10 0 106 5355	16/0.0.334 84233		UDP Port asser LVI 10 ports within 2.	D)	107	htter	100	+
	100 100 100									10	1.00

2. 加入成功後,使用者可以在 [白名單] 頁面裡顯示。

		⊕ Administrator * ♥ 繁中 I→
冒 借 表板	白名單	
⊕ 裝置清單	· · · · · · · · · · · · · · · · · · ·	
計 群組	↓ 推序 - ▽ Q	٢
群組	SID 類型 訊息紀錄	
安全規則模板	110000000009 Web examplematwaredomain.com	Û
白名單	× 1 3	10 ~ 1-1 of 1
● 資安記錄		
③ 系統管理	>	
(

※ 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 2,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。

1	質安紀錄										
	tranic - Addr	e berro	the second								
*	A. 100 - 12									20.20	1.54
	in part of			Her.	- inst	5869		da da	1000	and.	
÷.	2030-00-20 1139	ANYRORODIDE	2001.001/7902/446-427/30c3/20104746-54583	3400.8802.555c.915/wit.092wi8030		Attosion Jio molefiequest \$125 GRL socioecticud fonic consiste.	D	RITE	Madum	108	
	2024-00-20 8:39	<u>21750901080</u>	2000 0002.455-30H MR 9924-0080	30016/17/20031068-427/3ee8 2c19+34e644883		Crypto-soot Web Miner Drive-by . UR: secured cloud lonic constitut.	D	HETE	Medium	108	+
	2014-49-25 8:39	ALEBSTRUCTURE	2001-001/2002/0001/02/20010269/w140-646/8	3400-0902-502c 91499 P. 9924 80380		Webshalt PHP-rythm incound Con. CRL: recurst cloud ionic correl[08.	D	HTP	High	1.09	+
	2034-00-20 839	A0F009000101	1400.0802.03c.5W/wR.962a.8080	30010071000210083035w057/050.c89.60963		Crypto-sout Web timer brive-by VRC constructional Bank: com/808.	(A	HTF	Notium	109	+
	2034-06-20 1/38	A07532023104	2001.1:01/70.023/sio8.3x05.#8575.c5o.c8(180.955	3400.0002-H53;; 518/wH 992w B930		Attonion Dis moleitequesi 1597 UR: securet cloud lonic com808.	D	HTTP	Medium	100	+
	2024-06-20 1036	A01503900300	2001:001:002:003-3605-455-73d5a.xd0.60354	2400-0902-003c 0105e0 910e 8080		Joomio (77 Register Extension 12) GR: secularit stoud ionic constitut.	D	1177	Critical	100	•
	202+-08-20 8/28	A0100000000	2001500:100230063003-88875098001150964	340010202-903c-0195410.0026-0080		with UN 1-1 SQL Injection URL: securist cloud lionic corrolf/08.	0	itte	Malum	100	+
	2024-00-20 8.38	AGEDORODORDE	2001:s08 75023:s08 3:s25 #0573:c0a c30 67862	3400 0902-93c 819/wit 992w 0080		Violated PhPolydra lessand Can. URL securest cloud lionic com/608.	D.	HIT	High	100	•
	2034-00-20 0979	accontinue	10 10 0 108 m255	1070.0.334 84738		UDP Port asser UVI 10 ports within 3	D)	100	hite-	100	+

- 🔁 排序:將紀錄,選擇排序類別,點擊圖示可更改排序 气 。
- 🔽 篩選:將紀錄條件篩選。
- ᄇ 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 **b**·可以查詢該項攻擊的分析與解決方案。

Security Solution Provider Threat End	cyclopedia	
Ati	lassian Jira makef	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)



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。

LIONIC				O Adr	ninistrator © 繁中 I→
罰 儀表板	1	使用者			
H THE	~	── 相序 ~ ▽	9		+ 🕲
群編		報號	名稱	角色	
安全規則模板		cmsodmin	Administrator	被理典	Ð
白名單		1		-10	o
● 資安記録		4 1 2			10 🗁 1-2 of 2
③ 系統管理	~				
使用者	1				
管理日誌					
通知					
	3				

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。

LIONIC						O Administrator	9 繁中	-+
訂 儀表板		管理日誌						
⊕ 裝置清單								
H FFAI	*	1日 単序 ~	8	۹		2024-06-18 - 2024-06-18	0	
et all		84 (10)	使用者	來還位址	积息纪錄			
安全規則構板		14:10:30	cmsadmin	10.10.0.228	Add GateKeepers to group Lionic			
白名單		14:10:30	cmsadmin	10.10.0.228	Create group Lionic			
● 資安記錄		14:08:00	cmsadmin	10.10.0.234	Sign in			
③ 系統管理	~	13:32.16	cmsadmin	10,10,0.228	Sign in			
使用者		11:05:32	cmsadmin	10.10.0.228	Sign in			
管理日誌		10:49:42	cmsadmin	10.30.0.71	Sign in			
通知	-	10:20:53	cmsodmin	192.168.8.70	Sign in			
059005		09:54:06	cmsadmin	192.168.8.70	sign in			
	199	0 1 3				10 - 1	-8 of 8	



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。

				⊖ Administrator O 版中	I→
H RIAL	~	通知			
群組					
安全規則模板		啟用			
白名單		SMTP 伺服器			
● 資安紀錄		SMTP 通訊埠	25		
③ 系統管理	~	SMTP 帳號			
使用者		SMTP 密碼			
管理日誌		收信者	選擇	~	
通知		2014			
特徵碼		JM224,		西市	
入口網站使用者					
	1				

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。

LIONIC			🕒 Administrator 🛛 繁中 1
H 群組	~	特徵碼	
群組			
安全規則模板		敗用特徵碼伺服器	
白名單		最新版本	+ 上錦
● 資安紀錄		初體坂本	
◎ 系統管理	~		
使用者		防毒系统	
管理日誌		入侵防禦	
通知		惡意調買阻當	
特徵碼	1		
入口網站使用者		1≘ 拼揮 ~ ♡ Q	٢
	3	日期 檔案名稱 檔案類型 版本	《 檔案大小



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 。

					O Administrator	ø	繁中	l→
∺ 群組	× ,	入口網站使用者						
群組								
安全规则模板		№ 排序 ~ ▽	٩			+	0	
白名單		\$ 長號		名稱				
● 資安紀錄		portal			Ċ			
@ 系統管理	~	C 1 3			10 -	1-1	ofl	
使用者								
管理日誌								
通知								
特徵碼								
入口網站使用者	1							
	15							

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

Ø



 設定完成後:即可登入 CMS Portal,請使用網頁瀏覽器開啟 <u>http://CMS_IP</u>, 即可登入



歡迎使用 CMS Porta	L
登入	
使用者名稱	
Username	
密碼	
Password	540
登入	

5. 即可控管管理者分配的管理裝置

				⊖ peter.pan * O \$\$中 I→
● 装置清單	技置清單			
資安記錄				
▲ 通知	*≘ 排序 ~ ▽	Q		/ 動作 - 上 ③
192	MAC 位址	装置名稱	IP 位址	粉糖版本
	A0F5090009D1 Active	myArk	10.10.0.207	13.3
	< 1 >			10 😒 1-1 of 1



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 <u>https://CMS_IP:4221</u>。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



© 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.