

^{ューザーガイド} CMS 中央管理システム

バージョン 2.0 更新日付 2024/07

Lionic Corp. www.lionic.com



CMS ユーザーガイド

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

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	
更新	7
機能紹介	8
ダッシュボード	9
デバイスリスト	11
グループリスト	13
グループリスト	13
ポリシーテンプレート	15
ホワイトリスト(グローバル)	17
脅威ログ	18
システム	20
アカウント管理	20
管理履歴	20
通知	21
シグネチャ	21
ポータルユーザー管理	22
各機能の設定	24
NTP の設定	24
Firewall の設定	24
タイムゾーンの設定	25
HTTPS WEB UI	26
ストレージの追加	27
トラブルシューティング	28
アカウントロックの解除	28
パスワードを忘れた場合	28



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。

0 O 0	CMS-2.0.0	(下載所有檔案 …
•>			
É.	名稱 ~		修改時間
0	CMS.ml		
	CNS.ov/		21 cays ago
0	CMS-disk001.umdk	··· 17 GB	3 days ago
	3 鐵檔案		
	LIONIC Share service		

2. CMS VM インストーラでフォーマットを選択します。

← → ↓ Q	口 > 本8	ŧ → DATA (D:) → Server → CMS-2.	0.0	授尋 CMS	-2.0,0	۹
① 新培 · 🄏 🕐	(i)	🖄 🔟 🛝 排序 🗸 🗮 檢視 -			α	詳細資料
☆ 堂用	ĩ	名瑞	修改日期	類型	大小	
		CMS.mf	2024/7/4 下午 01:53	MF 福寨	1 KB	
		😹 CMS.ovf	2024/7/4 下午 01:53	OVF 相案	5 KB	
三 桌面	*	😼 CMS-disk001.vmdk	2024/7/4 下午 01:53	VMDK 檔案	1,815,271	
連 市 世						
□ 文件						
🛃 国片	*					
⑦ 音樂	*					
N	*					
Server						
Production-2.5						
復項目						=



3. VM の名前を設定し、インポートします。

💱 VMware Workstation 15 Player (Non-commercial use only)	27% - VMware Workstation 15 Player (Non-commercial use only)
Player 🕶 🕨 🗸 🕞 🔯	Playar +
	Importing CMS
	mileorang cina
Import Virtual Mashina	
Store the new Virtual Machine Provide a none and kind storage path for the new without modifier.	
Name for the new virtual machine:	
CPIE	
Storage path for the new virtual machine:	
D:\vM\vMware\CMS Browse	
Help Import Cencel	
	Importing CMS

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。

ual Mechine Settings		
rdware Options		
Device Summary IIII Memory 2:08 Phorosson 2: Intel dok (SC3) 100 GB CoCDPN (DC) Using unknown badend Using unknown badend Using unknown badend Vision badend Picker Picker Picker Picker Display I monbor	Denice status Connected Connected Connected Product: Connected denicity to the physical network Replicate physical network connection state Replicate physical network connection state Configure Adapters Network J. physical network Configure Adapters Network J. physical network Weither Weither Configure Adapters Network J. physical network Weither Configure Adapters Network J. Specific visibuli network Weither Configure Adapters Network J. Specific visibuli network Weither Configure Adapters Network J. Specific visibuli network Method Segments CAM Segments CA	Automatic Bridging Settings
Add.,. Remov	5	Intel(R) Ethernet Connection I217-V Phantom TAP-Windows Adapter V9 OK Cancel Help



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 <u>http://CMS_IP:4221</u>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。



	o
CMSへようこそ	
ログイン	
ユーザー名	
ユーザー名	
パスワード	
パスワード	74
ログイン	



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。

			e	Administrat	or € ♥ 日本語 I→
 ■ ダッシュボード ● デバイスリスト 	^{ューザー} ようこそ、Admini	strator	5 オンラインデバイスの数	7	の教
計 グループリスト					
● 脅威ログ	検査統計情報 7日間の検査情報		最近の脅威		
@ Э л 74			⊟ ⁴ t 2024-07-30 11:23:16	est Intrusion	メッセージ UDP Port scan LVI: _
	339 Files	96K Flaws	2024-07-29 22:28:32	Firewall	нттр
			2024-07-29 22:28:31	Firewall	нттр
			2024-07-29 22:28:31	Firewall	HTTP
	54K URLa	6M Packets	2024-07-29 22:28:29	Firewall	нттр
	脅威事件のサマリー			82	2024-07-24 - 2024-07-30
	脅威事件の統計		脅威事件ランキング		



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。

		O Administrator も O 日本語 -
ダッシュボード	脅威事件のサマリー	2024-07-24 - 2024-07-30
 ⊕ デバイスリスト 詳 グループリスト ● 発成ログ ● スコート 	育威事件の統計 アンチウィルス 0	骨威事件ランキング ALL マ 検出数 証言歌 ALL マ 教量 メッセージ SID
9771	不正侵入防止 1	I Intrusion UDP Part sca 8060000301 I Web www.internetbad 1100000000004
	Web 脅威防止 2	1 phish.opendnstes 110000000008 t.com/
	脅威事件の数 ● アンチウィルス ● Web 脅威防止 ● 不正侵入防止	攻撃されたデバイスランキング 数重 デバイス名 F アドレス MACアドレス モデル
	2	

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。

Security Infatian Pranider	不正侵入防止	1 Intrusion UDP Port sca 8060000301
🖬 ダッシュボード	1	1 Web www.internetbad 110000000004
⊕ <i>デ</i> バイスリスト		
目 グループリスト >	Web 脅威防止	1 Web phish.opendnste 110000000008
● 脅威ログ	2	
@ システム >		
	脅威事件の数	攻撃されたデバイスランキング
	 アンチウィルス ● Web 脅威防止 ● 不正侵入防止 	数量 デバイス名 ドアドレス MACアドレス モデル
		3 myTera 10.10.0.144 68EC62032C6E Tera-UTM
	15	
	0.5	
	0 07-24 07-25 07-26 07-27 07-28 07-29 07-30	



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。

LIONIC								O Administrator ℃ 〇 日本通	8 (+
≣ ダッシュポード	デバイスリスト	-							
● 7/172921									
目 グループリスト								🖌 Actions : 🕹 🕲	
● 脅減□グ	MACPFLZ	FILTZE	モデル		P7F62	90-Kilip7FLA	77-49:78-93>	シグネチャパージョン	
@ 2274	80029CD37840	MyPico	Pico-UTM 100		192.168.8.56		2.53	1 3.0.1525 • 5.1272 • 2.0.1529	
	DDIB7DEEDABA	myArk	Ark-UTM 16		172.163.66	220,130,53,5	140	10.1054 6 181 20.1670	
	80029CC535M	мурісо	Pico-UTM 100		172363.44		260	* 30.1654 • 51.288 • 2.01558	
	ODIB70FFDABB	myArk.	Ark-UTM 16		17236155	220 130.53.5		30.054 5181 20.1570	
	80029CD17A34	Wilson Yu	Pice-UTM 100		192168.8.340	220 130.53.5	260	**************************************	
	80029C00344F	MyPico	Pice-UTM 100	cs-group-test-2	10.10.0,109	18185.248.5	28.0	· 3.0.1568 · 51.295 · 2.0.1570	
	BBEC62032CBE	myTera	Tera-UTM 12	Test-Wrong-Group	10:10.0.144	18.165.248.5	14.0	0 \$ 3.0.3054 51.81 \$ 2.03570	
								10 v 1⊨7 or7	

- - ・ 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。

		8 Administrator	♀ 日本語	l+
■ ダッシュポード	デバイスリスト			
● <i>デバ</i> イスリスト				
₩ グループリスト >	00187DFFDAB8			
● 脅威ログ	装置情報 セキュリティ機能 脅威ログ 統計 ライセンスの管理			
اجمد المحمد المحمد ومحمد المحمد المحم المحمد المحمد المحمد المحمد المحمد المحم المحمد المحمد محمد محمد محمد محمد محمد محمد محمد				
	MACアドレス 001870FFDAB8			
	ステーダス オンライン HA 衣服 Active			
	デバイス名 myArk /			
	MACアドレス 00187DFFDAB8			
	モデル Ark-UTM 16			
	グループ Default Group			
	WAN IPアドレス 172.16.1.55			
	グローバルPアドレス 220.130.53.5			
c	パージョン			

- **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。

					9	Administrator 🧲	S I	本語
∎ ダッシュポード	グループリスト	•						
<i>ヺ゚゚゚゙゙゙</i> パイスリスト								
〒 グループリスト 🗸 🗸	t≘		٩					٢
グループリスト	グループ名	デバイスの数	アンチウ	イルス	不正侵2	入防止	Web 脅	威防
ポリシーテンプレート	grouptest]			ログとウィルスを無効化する(Destroy)		ログとブロックする		
	grouptest2			u٧		D7		D:
ホワイトリスト	Wilson's Group			D7		nø		
● 脅威ログ	cs-group			¤Ø		D7		
9 システム >	cs-group-test-1			ロ グ		00		•
	cs-group-test-2			ログとウィルスを無効化する(Destroy)		ログとブロックする		
	cs-group-test-3			D17		D7		•
	cs-group-test-4			DØ		ロ //		
	cs-group-test-5			Dグ		ログ		

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。

LIONIC				8	Administrator 6	♥ 日本語	1
〒 ダッシュボード	グループリスト						
● デバイスリスト							
<i>∉グループリスト</i> >	作成					×	
■ 脅威ログ	グループ名 Lionic					-	
) D DZFL >	ポリシーテンプレート 重択	ž				~	
	Do Davido de Alexander					1	
		۹				٩	
	MAC7FL2	デバイス名	IPアドレス	パージョン	ステータス		
	80029CC53518	MyPico	172.16.1.41	2.6.0			
	80029CD17A34	Wilson Yu	192.168.8.140	2.6.0	同志なく期間切れ		
	80029CD17840	MyPico	192.168.8.56	2.5.1	(17.57(2)		
	00187DFFDABA	myArk	172.16.1.56	14.0			
	00187DFFDAB8	myArk	172.16.1.55	14.0			
					10	1-5 of 5	



3. 確認後、 [適用] をクリックします。

					8 A	dministrator 🌜	♥ 日本語	I+
コ ダッシュボード	グリ	ループリスト						
<i>⊕ デパイス</i> リスト								
目 グループリスト >		Lionic 🖌						
● 脅威ログ		デバイスリスト アンチ		防止 Web 脅威防止				
@ >274 >								
		1= ソート ~ 🗸	٩					
		MACTFLZ	デバイス名	IPアドレス	パージョン	ステータス		
		80029CC53518	MyPico	172.16.1.41	2.6.0			
		80029CD17B40	MyPico	192.168.8.56	2.5.1			
		00187DFFDABA	myArk	172.16.1.56	14.0			
		00187DFFDAB8	myArk	172.16.1.55	1.4.0			
						10 🛩	1-4 of 4	
							瀬用	

4. 新しいグループを作成されました。

グループリスト							
t≘	c	x I					٢
グループ名	デバイスの数	アンチウ	イルス	不正侵2	、防止		Web
Wilson Test	0		nø		ログ		
Wilson test 2			П 7		ログ		
Wilson Test 3			D#		ログ		
Wilson Test.3			ロ グ		ログ		
Wilson Test 5			۵Ő		ログ		
TestFromErrorTemplate			¤#		口グ		
Test-Wrong-Group			ログとウィルスを無効化する(Destroy)		ログとプロ	ックする	
Lionic			ログとウィルスを無効化する(Destroy)		ログとプロ	ックする	
	グループ名 Wilson Test Wilson Test 2 Wilson Test 3 Wilson Test 3 Wilson Test 5 TestFromErrorTemplate TestFromErrorTemplate TestFromErrorTemplate	グループ名 デパイスの数 Wilson.Test 0 Wilson.test.2 0 Wilson.test.3 0 Wilson.Test.3 0 Wilson.Test.5 0 Test.FromErrorTemplate 0 Test.Wrong-Group 1 Lionic 4	グループ名 デパイスの数 アンチウ Wilson Test 0 和効 Wilson Test 2 0 有効 Wilson Test 3 0 有効 Wilson Test 5 0 有効 TestFromErrorTemplate 0 利効 Lionic 4 有効	グループ名 デパイスの数 アンチウィルス Wilson Test 0 有効 ログ Wilson Test 2 0 有効 ログ Wilson Test 3 0 有効 ログ Wilson Test 5 0 有効 ログ Wilson Test 5 0 有効 ログ TestFromErrorTempkate 0 有効 ログ Lonic 4 有効 ログとウィルスを集効化する(Destroy)	グループ名 デバイスの数 アンチウィルス 不正保ノ Wilson Test 0 有効 ログ 有効 Wilson Test 2 0 有効 ログ 有効 Wilson Test 3 0 有効 ログ 有効 Wilson Test 5 0 有効 ログ 有効 TestEromErrorTemplate 0 有効 ログ 有効 Test=Wrong-Group 1 有効 ログとウィルスを集効化する(Destroy) 有効 Lionic 4 有効 ログとウィルスを集効化する(Destroy) 有効	グルーブ名 デパイスの数 アンチウィルス 不正禄入助止 Wilson Iest 0 有効 ログ 有効 ログ Wilson Iest 2 0 有効 ログ 有効 ログ Wilson Iest 3 0 有効 ログ 有効 ログ Wilson Iest 5 0 有効 ログ 有効 ログ IestFromErrorTemplate 0 有効 ログ 有効 ログ IestFromErrorTemplate 1 有効 ログとウィルスを無効化する(Destroy) 有効 ログとウr	グルーブ名 デパイスの数 アンチウィルス 不正礎入防止 Wilson Iest 0 有効 ログ 有効 ログ Wilson Iest 2 0 有効 ログ 有効 ログ Wilson Iest 3 0 有効 ログ 有効 ログ Wilson Iest 5 0 有効 ログ 有効 ログ IestFromErrorIemplate 0 有効 ログ 有効 ログ IestFromErrorIemplate 1 有効 ログとウィルスを集効化する(Destroy) 有効 ログとブロックする Lionic 4 市効 ログとウィルスを集効化する(Destroy) 有効 ログとブロックする

※ 作成完了後、デバイスリストのページに *ℓ*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。

[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。

					🖨 Administrato	ar C	♥ 日本語	
コ ダッシュボード	ポリシーテンプレ・	- ト						
● デバイスリスト								
【 グループリスト	t≘ ソート ~ ▽		٩				+ 🕲	
グループリスト	グループ名	アンチウ	リイルス	不正侵2	、防止	Web 脅	威防止	
ポリシーテンプレート	Wilson Test		ログ		ログ		ログ	
	wilson-test-2		ログとウィルスを無効化する(Destroy)		ログとブロックする		ログとプロ	
ホワイトリスト	Iest		ログ		D7		D#	
● 脅威ログ	cs-policy		ログ		DØ		D7	
シ ステム	cs-policy-test-1		۵ %		DØ		ログ	
	cs-policy-test-2		ログとウィルスを無効化する(Destroy)		ログとブロックする		ログとブロ	
	wilson-test-template-2		ログとウィルスを無効化する(Destroy)		ログとブロックする		ログとプロ	
	test-temp		ログとウィルスを無効化する(Destroy)		ログとブロックする		ログとプロ	
	11		ログとウィルスを無効化する(Destroy)		ログとプロックする		ログとブロ	

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。

LIONIC				e Administrator	٤	♥ 日本語	l→
■ ダッシュボード	グループリスト						
⊕ デバイスリスト							
₩ グループリスト 〜	作成					×	
グループリスト	グループ名・ ロ	onic Test					
ポリシーテンプレート	ポリシーテンプレート	洪坎					
ホワイトリスト	t <u>=</u> ソート ~ ▽	wilson-test-template	3 -2				
● 脅威ログ	MACアドレス						
@ \$2754 >	80029CDI7A3	w-test-3 wilson-test-ACL wilson -tes t Lionic					

16



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。

 [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。

					Administrator	L	♥ 日4	湖 →
■ ダッシュポード	脅威ログ							
● デバイスリスト	アンチウィルス 不正優入防	L Web 香椒防止						
₩ グループリスト 〜	t= ソート -> ▽	۹		= 20	124-07-30 - 2024-0	7-30	F 6	<u>}</u>
グループリスト		送信元	宛先	国, 地域 ×	ッセージ			
ポリシーテンプレート	2024-07-30 11:23 68EC 62032	CGE 10.10.0.166:5355	10.10.0.106.59792	U	DP Port scan LvI: 10	ports wi	th [B	¥.
ホワイトリスト						10		
● 脅威ログ						1.10	¥_ 1-10	r I
 ۵.754 ٥.754 								

2. 追加した後、 [ホワイトリスト] のページで表示します。

	C Administrator 6 〇 日本語 I-	•
コ ダッシュボード	ホワイトリスト	
⊕ デバイスリスト		
目 グループリスト 🗸 🗸	t _≡	
グループリスト	SID 種類 メッセージ	
ポリシーテンプレート	110000000004 Web www.internetbadguys.com/	
ホワイトリスト	< <u>1</u> → 1-1 of 1	
● 脅威ログ		
@ \$2754 >		
15		



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。

						8 Admini	strator	L	日本語	
コ ダッシュポード	脅威ログ									
● デバイスリスト		不正侵入防止								
∄ グループリスト ∽	<u>1</u> = ソート ~ ∇		٩		e] 202 4-07-30	~ 2024-0	7-30 .	r ©	
グループリスト	日付	мас	送信元	宛先	国地域	メッセージ				
ポリシーテンプレート	2024-07-30 11:23	68EC62032C6E	10.10.0.166:5355	10.10.0.108:59792		UDP Port sco	in Lv1: 10 p	orts with	- []]	
ホワイトリスト								144222		
● 養威ログ								10 0	i-I of I	
) 927L >										

- **ヽ 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
- **ア 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 2 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 C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。

LIONIC Security Exclusion Provider	cyclopedia	
At	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)



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。

LIONIC Bereilly Exalise Prever			e Administr	ator 🌜 📀 日本語
目 グループリスト 🗸 🗸	アカウント管理			
グループリスト				
ポリシーテンプレート	1= ソート → ▽	٩		+ 0
ホワイトリスト	アカウント	名前		
● 愛感口グ	emsadmin	Administrator	管理者	Û
a 5250 v	wilson	Wilson Yu	管理者	Ô
	ichung	ichung	管理者	e
THUSTER	cslee	Chen-Shao Lee	問覧者	đ
管理履歴	wilsony	Wilson Viewer	開覧者	Ċ
通知	winnie	Winnie Hu	標準ユーザー	đ
シグネチャ				10 🗸 1-6 of 6
ポータルユーザー管理				

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。

LIONIC		O Administrator
₩ グループリスト 🗸 🗸	管理履歴	
グループリスト		
ポリシーテンプレート	1 y-h - V Q	🖾 2024-07-30 - 2024-07-30 🛛 👰
ホワイトリスト	日付 ユーザー 送信元PP メッセージ	
● 務戚ログ	2024-07-30 13:47:35 cmsadmin 220.130.53.5 Create policy	y template Lionic
» کټې ک	2024-07-30 13:4518 cmsadmin 220.130.53.5 Modify setting	g of group Lionic
アカウント管理	2024-07-30 13:44:18 cmsadmin 220.130.53.5 Add GateKeep	opers to group Lianic
管理度型	2024-07-30 13:44:18 cmsadmin 220.130.53.5 Create group	o Lionic
	2024-07-30 13:27:29 willson 220.130.53.5 Sign in	
	2024-07-30 13:21:08 cm:admin 192.168.8.129 Sign in	
シグネチャ	2024-07-30 11:37:23 cmsadmin 42:73.67:201 Delete group l	Lionic Test
ポータルユーザー管理	2024-07-30 11:36:52 cmsadmin 42.73.67.20 Add GateKeep	apers to group Lionic Test
19	2024-07-30 11:36:52 cm/sodmin 42.73.67.201 Create group	o Lionic Test



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。

			e Administrator	€ ♥ 8	本語	•
目 グループリスト 🗸 🗸	通知					
グループリスト						
ポリシーテンプレート	有効					
ホワイトリスト	SMTPサーバ・	maillionic.com				
● 脅威ログ	SMTPポート・	25				
@ >Z74 v	SMTPアカウント・	wilson.yu@lionic.com				
アカウント管理	SMTPパスワード・					
管理限歴	通知先	wilsonyu@lionic.com				
通知						
シグネチャ						
ポータルユーザー管理						
()						

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。

LIONIC	S Administrator 🖕 🛇 日本語 日+
₩ グループリスト ~	シグネチャ
グループリスト	
ポリシーテンプレート	シグネチャサーバを起用する
ホワイトリスト	最新パージョン + アップロード
▶ 脅威ログ	ファームウェアパージョン
@ 9756 V	
アカウント管理	72494.62
管理履歴	不正侵入防止
通知	Web 骨减防止
シグネチャ	
ポータルユーザー管理	t _a y-k · V Q
(c)	日村 ファイル名 ファイルタイプ パージョン ファイルサイズ



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。

			❸ Administrator 🖕 🔮 日本語 া→
₩ グループリスト ~	ポータルユーザー管理		
グループリスト			
ポリシーテンプレート	t <u>=</u> ν−⊦ - ⊽ Q		+ 🐵
ホワイトリスト	アカウント	名前	
• ##o#	cslee	Chen-Shao Lee	0
	cstesti	Chen-Shao Lee	Û
	cstest2	Chen-Shao Lee	Ċ
アカウント管理	cstest3		Ó
管理履歴	cstest4		Ó
通知	cstest5	cstest5	o
シグネチャ	wilson	Wilson Yu	Ċ
ポータルユーザー管理	<u>cstest6</u>	CSLee	Ċ
4			10 🗸 1-8 of 8

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

Ø



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。

				🖨 Lion	icPortal C	♥ 日本語	I I+
	デバイスのリスト						
● 脅威ログ							
♠ 通知	き シート ~ 🛛 🏹	۹			Actions -	* @	
	MACアドレス	デバイス名	IPアドレス	ファームウェアバージ	∍ ≻		
	68EC6203IB0C 1909776 (19900776)	myTera EN/E)	192.168.8.123	1.3.1			
	A0F5090009D1	myArk	192.168.8.107	1.3.3			
					10	♥ 1-2 of 2	
. 6							



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

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



© 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.