Threat Grid裝置與FMC整合的故障排除

目錄

簡介 必要條件 需求 採用元件 問題 案例 1 案例 2 整合 用於Clean Admin介面的內部CA簽名證書 清潔介面 管理員介面 清除將CSR和CER連線到PEM的介面 管理介面CSR和CER到PEM FMC證書的正確格式 PEM DER 在Windows和Linux中建立的證書之間的差異 證書上傳到TG裝置和FMC 上傳乾淨介面的證書 上傳管理員介面的證書 <u>將證書上傳到FMC</u> 相關資訊

簡介

本文檔詳細介紹執行緒網格裝置(TGA)與Firepower管理中心(FMC)的整合。

必要條件

需求

思科建議您瞭解以下主題:

- Firepower管理FMC
- Threat Grid裝置基本配置
- 建立授權憑證(CA)
- Linux/Unix

採用元件

本文中的資訊係根據以下軟體和硬體版本:

- FMC版本6.6.1
- Threat Grid 2.12.2
- CentOS 8

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除(預設))的組態來啟動。如果您的網路運作中,請確保您瞭解任何指令可能造成的影響。

問題

在此用例場景中,您可以看到2個問題和兩個錯誤代碼。

案例 1

整合失敗,但有錯誤:

Sandbox registration failed: Peer certificate cannot be authenticated with given CA certificates (code = 60)

在此問題方面,問題與未以完整鏈結形式上傳到FMC的憑證相關。由於使用了CA簽名的證書,因此 需要使用合併到單個PEM檔案中的整個證書鏈。換句話說,您應該從Root CA > Intermediate Cert(如果適用) > Clean Int開始。請參考<u>官方指</u>南中介紹要求和程式的文章。

如果CA有多個簽名鏈,則所有必需的中間證書和根證書必須包含在上傳到FMC的單個檔案中。

所有證書都必須採用PEM編碼。

檔案的新行必須是UNIX,而不是DOS。

如果Threat Grid裝置提供自簽名證書,請上傳您從該裝置下載的證書。

如果Threat Grid裝置顯示CA簽名的證書,請上傳包含證書簽名鏈的檔案。

案例 2

無效的證書格式錯誤

Invalid Certificate format (must be PEM encoded) (code=0) 憑證格式錯誤,如下圖所示。



此錯誤是由於在使用OpenSSL的Windows機器上建立的組合PEM憑證的格式錯誤所致。強烈建議使用Linux電腦建立此證書。

整合

ululu cisco Threat Grid Appliance Home Configuration Status Operations Support Configuration Network Configuration e Authentication **CLEAN** interface **CA Certificates** MAC Address: a4 IP Address: 172.16.2.103 (STATIC) **Change Password IP** Assignment Clustering STATIC \sim Date and Time Email **IP Address** 172.16.2.103 Integrations License Subnet Mask Network 255.255.255.0 Network Exit Gateway NFS 172.16.2.254 Notifications Host Name W 4 SSL Primary DNS Server Syslog 172.16.2.5 Secondary DNS Server IP

步驟1.配置TGA,如下圖所示。

ADMIN interface MAC Address: 40. 20 IP Address: 10 8.30 (STATIC) IP Assignment STATIC IP Address 10 30 Subnet Mask 255.255.192 Gateway 10 1 Host Name TG-M5
Save Activate
Host (A) Security
Host (uses parent domain if left blank):
W M4
Fully qualified domain name (EQDN):
Were com
IP address:
1/2.10.2.103
 Update associated pointer (PTR) record

Host (A) Security						
Host (uses parent domain if left blank):						
TG-M5						
Fully qualified domain name (FQDN):						
TC .com						
I <u>P</u> address:						
10 18.30						
✓ Update associated pointer (PTR) record						

用於Clean Admin介面的內部CA簽名證書

步驟1.生成用於管理介面和乾淨介面的私鑰。

openssl ecparam -name secp521r1 -genkey -out private-ec-key.pem 步驟2.產生CSR。

清潔介面

步驟1.導航到CSR建立並使用生成的私鑰。

openssl req -new -key private-ec-key.pem -out MYCSR.csr

附註:必須為CSR輸入CN名稱,並且必須與在「Network」下定義的清理介面的主機名匹配 。DNS伺服器上必須存在DNS條目,該條目將解析Clean介面主機名。

cisco Threat Grid	Appliance Home Configuration Status Operations Support
Configuration Authentication CA Certificates Change Password Clustering Date and Time Email Integrations License Network Network Exit NFS Notifications SSH SSL Syslog	Network Configuration CLEAN interface MAC Address: a4 da IP Assignment STATIC IP Address 172.16.2.103 Subnet Mask 255.255.255.0 Gateway 172.16.2.54 Host Name W4 Primary DNS Server 172.16.2.5

管理員介面

步驟1。導覽至CSR建立並使用產生的私密金鑰。

openssl req -new -key private-ec-key.pem -out MYCSR.csr

附註:必須為CSR輸入CN名稱,並且必須與「Network」下定義的「admin interface」的「 hostname」匹配。DNS伺服器上必須存在DNS條目,該條目將解析乾淨介面主機名。

ADMIN interface
MAC Address: 40: 80 IP Address: 10 8.30 (STATIC)
IP Assignment V
IP Address 10 30
Subnet Mask 255.255.255.192
Gateway
Host Name TG-M5
Save Activate

步驟2.由CA簽署CSR。下載帶有CER擴展的DER格式的證書。

步驟3.將CER轉換為PEM。

openssl x509 -inform DER -outform PEM -in xxxx.cer -out yyyy.pem

清除將CSR和CER連線到PEM的介面

管理介面CSR和CER到PEM

C:\Users\Administrator\Downloads\TG\FMC>openssl req -new -key step7-1-private-ec -key.pem -out Admin-interface_CSR.csr You are about to be asked to enter information that will be incorporated into your certificate request. What you are about to enter is what is called a Distinguished Name or a DN. There are quite a few fields but you can leave some blank For some fields there will be a default value, If you enter '.', the field will be left blank. -----Country Name (2 letter code) [AU]: State or Province Name (full name) [Some-State]: Locality Name (eg, city) []: Organization Name (eg, company) [Internet Widgits Pty Ltd]:PPJ Organization Name (eg, section) []:IT Common Name (e.g. server FQDN or YOUR name) []:TG-Email Address []: Please enter the following 'extra' attributes to be sent with your certificate request A challenge password []:Cisco@123 An optional company name []:PPJ C:\Users\Administrator\Downloads\TG\FMC>openssl x509 -inform DER -outform PEM -i n Admin-interface_CSR_CA-signed_DER_CER.cer -out Admin-interface_CSR_CA-signed_DER_C

FMC證書的正確格式

如果您已經獲得證書,並且證書採用CER/CRT格式,在使用文本編輯器時是可讀的,則只需將副檔 名更改為PEM即可。

如果證書不可讀,您需要將DER格式轉換為PEM可讀格式。

openssl x509 -inform DER -outform PEM -in xxxx.cer -out yyyy.pem

PEM

PEM可讀格式示例,如圖所示。

1	BEGIN CERTIFICATE 🔫
2	MIIFozCCA4ugAwIBAgITGQAAAALex/EgACaWIAAAAAAAAjANBgkqhkiG9w0BAQUF
3	ADAaMRgwFgYDVQQDEw9Ub21EZW1vIFJvb3QgQ0EwHhcNMTQwMjA3MTQwMTU3WhcN
4	MjQwMjA3MTQxMTU3WjBKMRIwEAYKCZImiZPyLGQBGRYCc2UxFzAVBgoJkiaJk/Is
5	ZAEZFgd0b21kZW1vMRswGQYDVQQDExJUb21EZW1vIE1zc3VpbmcgQ0EwggEiMA0G
6	CSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDC8XmXxLHo0M/521CFtI4DSN6qVNAN
7	8jxujS4PSSRnQtaqpbjbcAZpvbYysNt2uwA40urkxY2nyn4SMy/21S4L9x10u8su
8	W+/4T2dcFgQKzFiNyqVkLop9vRKnCKjceD+FRKXbPCSZyy4Hhz/XCgwPRfaobx+q
9	aV1fSnW0F a2MHx60jf
10	BhdyONMrZxmQeYgFPUmd2o3x+lyq1406hIF7LLGFAoDdqi3R31D9OPb7+Dm2ezv0
11	OKkbCHdjl3inB3D1tg1L8mZeIEte+07RvlQXr33umO6zeYi4okbaHZLvAgMBAAGj
12	$\verb"ggGwMIIBrDAQBgkrBgEEAYI3FQEEAwIBADAdBgNVHQ4EFgQU0+wPInpDnoqnuIlx"$
13	BtUbIGLdS1UwgYsGA1UdIASBgzCBgDB+BgorBgEEAYKdZwEBMHAwPgYIKwYBBQUH
14	${\tt Agiwh4wAFQAbwBtAEQAZQBtAG8AIABQAG8AbABpAGMAeQAgAFMAdABhAHQAZQBt}$
15	AGUAbgB0MC4GCCsGAQUFBwIBFiJodHRwOi8vcGtpLnRvbWR1bW8uc2UvcGtpL2Nw
16	$\verb"cy5odG0AMBkGCSsGAQQBgjcUAgQMHgoAUwB1AGIAQwBBMAsGA1UdDwQEAwIBhjAP"$
17	$\verb+BgNVHRMBAf8EBTADAQH/MB8GA1UdIwQYMBaAFL00e0rG2ExZ1dmboIuLwgGgPr5e$
18	MEIGA1UdH y5zZS9wa2kvVG9t
19	${\tt RGVtbyUyMFJvb3Q1MjBDQS5jcmwwTQYIKwYBBQUHAQEEQTA/MD0GCCsGAQUFBzAC}$
20	hjFodHRwOi8vcGtpLnRvbWRlbW8uc2UvcGtpL1RvbURlbW8lMjBSb290JTIwQ0Eu
21	Y3J0MA0GCSqGSIb3DQEBBQUAA4ICAQBBkNHalbX3kkpOXCV3nQ9R4CyG61WI90gL
22	57 u GRcpulSqUu790J5s4xlW8rhm32db7qvHDPaYED23gudpOSHyUywZTFbwzm92c
23	e1wZpyJH6nsuqNFDTYQTdWAq8zwCrldcUFRW301mkPuhENjttqCIJ9KeLrwCaM/p
24	QVy7qWoTU14/BY+OsLXDGURXrGejcVs8ZQy4bqhmh0TfelTcAOAX47pVt8XdnWFe
25	Vnu/rwuOnfvlyiWW62cknAATaagnLXdbFWIxnVSlbooZmYXXQqelFxJVlbhNdWM9
26	tgdq3t2qBXj3P7XiD+OWfzkABGMJrmki55LNp10/oV+Kw3DuyGYLurq6TWWlJi8J
27	94GJm9VQBX1Py1FQn0hILcxgr+LAIKX0PqXTyRCp1/UGH1ih05S1F4GvPEj0s1BA
28	ebRkDrN2vU+9kq8UXOhzxierQDmJkCOpSUWV6Pk6/OP72vxIuAQQNdY++cJRwzi+
29	adWp6cZBzW5h3OdKlyEDdjNB75rzQcwMlerYTABSIaK6KCTNb70F4kTW1B5R1WqD
30	VXyboYEbf0ym5CiNmDKUXqQMI45FIztDhYjJqn1NeroJUZnUYa9y63zujy2uyQeG
31	EVWpXscPOfrcrCfSuvx0KsMiLxuclfVJyCAJqBMG++LgWxhb247CvhSDK2wZrq0+
32	Q70p0WaYww==

DER

DER可讀格式示例,如圖所示

1	0, ENQ£0, ETX< ETXISTX SOHISTX ISTX DC3 EMNULNUL NUL STX ÞÇÃ NUL 4-
	NUL NUL NUL NUL STX 0
2	NOM * † H † ÷
3	SOHISOHIENQIENQINULO SUB1 CANO SYNACKIETXUEOTIETXIDCSIST. CAO RSIETB
4	1402071401572
5	240207141157Z0J1 DC20 DLE ACK
6	'&%"````````````````````````````````````
7	'&%"````````````````````````````````````
	Issuing CAO, SOH"O
8	NOK * + H + ÷
9	SOH SOH SOH ENONULETX, SOH SINULO, SOH
10	STX, SOHSOHNULÂñy-ıèÐÏùÛP´ŽETXHÞªTÐ
11	ò <n.sdi\$gbö°¥,ůpacki¾12°ûv»nud8òêäŧê~dc23 th="" öõ.vd÷cst»ë.[ïøog\syneod<=""></n.sdi\$gbö°¥,ůpacki¾12°ûv»nud8òêäŧê~dc23>
12	ÌXÊ¥d.Š}%DC2SBS¨Üx?…D¥Û<\$™Ë.BDD‡?×
13	GRSDEö¨oUS *i]_Ju´?£lUmUS ^BÆòFÁ…≫EDŰÖ;)EODÒcoúONAK;Á·'ôÁ¨ZØÁñëHBACKEDE
	r8Ó+g⊠My^⊡NO=IÚñú\ª×:"{,±…STX€Ýª-ÑßPý8öûø9¶{;ô8©BSCBSwc-x§BDDpõ¶
14	Kòf^
	K^ûNѾTETE }îî³y^, ¢FÚES'ïSTXETXSOHNULSOH£, SOH°0, SOH¬0DLEACK
	+ACKSOHEOTSOH, 7 NAKSOHEOTETXSTXSOHNUL0GSACKETXUGSSOEOTSYNEOTDC4Ó1
	ST"zCžŠ§,‰qACKÕESC bÝKU0 <acketxugs eotf0€0~ack<="" th=""></acketxugs>
15	+ACKSOHEOTSOH, gSOHSOH0p0>ACKBS+ACKSOHENOENOBELSTXSTX02RS0NULTNULO
	NULMNULDNULeNULMNULONUL NULPNULONULINULINULCNULYNUL
	NUES NUET NUE a NUET NUE a NUE MUE MUE NUED NUET 0. ACK BS+ACK SOH ENQENQBEE STASOH
	SYN' .htmNUL0EMACK
	+ACKSOHEOTSOH, 7 DC4 STX EOT FFIRS
16	NUES NUE & NUE & NUE & OVERCKIETXUGS STIEOTIETX STX SOH † 0 STACKIETXUGS

DC3SOHSOHÿEOTENO0ETXSOHSOHÿ0USACKETXUGS‡EOTCAN0SYN€DC43%4{JEØLYÕÙ> //ÂSOH_>%^0BMCKETXUGSUSEOT•0907_5_3+1

在Windows和Linux中建立的證書之間的差異

您可以在記事本++中使用**Compare**外掛來將兩個證書並排進行簡單比較,並詳細描述行#68中的編 碼差異。在左側,您可以看到在Windows中建立的證書,在右側,您可以看到在Linux電腦上生成的 證書。左側的憑證有回車符,因此該憑證PEM對FMC無效。但是,除了記事本頁面中的那一行之外 ,您無法區分文本編輯器中的++同。



將新建立/轉換的RootCA和CLEAN介面的PEM證書複製到Linux電腦,並從PEM檔案中刪除回車。

sed -i 's/\r//'

例如sed -i 's/r/' OPADMIN.pem。

驗證是否存在回車。

^{od -c} 仍顯示有回車符的憑證,如圖所示。

[admin@	local	.host	Des	ktop]\$ od	- c	: MRJ	CA.c	er							l i
0000000						в	Е	G	I	Ν		С	Е	R	т	I
0000020	F	I	С	Α	Т	Е						١r	\n	М	I	I
0000040	G	t	D	С	С	в	Z	У	g	Α	W	I	В	Α	g	I
0000060	Т	R	Q	А	Α	А	Р	n	р	ι	У	n	В	0	h	j
0000100	Z	а	W	А	Е	А	Α	Α	Α	+	т	Α	Ν	В	g	k
0000120	q	h	k	i	G	9	w	0	В	Α	Q	s	F	\r	\n	Α
0000140	D	в	0	М	R	U	w	Е	W	Y	к	С	Z	I	m	i
0000160	Z	Р	У	L	G	Q	В	G	R	Y	F	т	G	9	j	Y
0000200	U	w	х	F	z	А	V	В	g	0	J	k	i	а	J	k
0000220	/	I	s	Z	Α	Е	Z	F	g	d	Р	с	2	9	j	\r
0000240	\n	L	W	р	v	М	R	W	W	G	g	Y	D	V	Q	Q
0000260	D	E	х	Ν	Р	с	2	9	j	L	W	р	v	L	U	N
0000300	D	т	ι	R	Е	Q	z	Α	У	L	U	Ν	В	М	В	4
0000320	х	D	т	I	х	М	D	Q	W	Ν	D	I	х	М	j	U
0000340	х	\r	\n	М	ι	о	Х	D	т	I	z	М	D	Q	W	N
0000360	D	I	х	М	j	U	х	М	ι	0	W	J	j	Е	k	М
0000400	с	I	G	А	1	U	Е	Α	х	м	b	т	V	J	К	L
0000420	U	F	Ν		С	1	U	R	У	1	Ν	Ν	s	0	w	М
0000440	S	5	q	\r	\n	d	С	5	q	d	G	d	У	b	3	V
0000460	w	м	I	ī	в	I	j	А	Ν	в	g	k	q	h	k	i
0000500	G	9	W	Θ	в	А	Q	Е	F	Α	Α	0	С	Α	Q	8
0000520	Α	м	I	I	В	c	g	К	С	Α	Q	Е	Α	s	g	4
0000540	Z	s	m	0	Y	\r	\n	W	т	2	Q	Y	0	7	h	h
0000560	z	d	8	b	+	ĸ	b	s	U	м	с	Q	Q	0	5	Θ
0000600	р	0	g	q	v	е	1	Q	5	2	G	7	т	m	w	е
0000620	+	v	m	q	+	Е	Y	н	W	b	В	т	g	D	9	9
0000640	К	D	ι	х	R	о	ι	١٢	\n	0	s	У	I	g	3	W
0000660	k	i	ι	М	р	I	ι	u	Р	i	0	Е	U	н	d	Α
0000700	с	2	т	q	А	d	w	0	r	е	Е	М	k	н	ι	F
0000720	n	Q	5	4	G	J	ι	W	Z	6	S	0	h	I	9	J
0000740	2	8	h	/	L	k	R	f	8	\r	\n	Z	3	5	В	q
0000760	q	F	0	х	р	s	8	s	0	k	р	7	1	0	7	н
0001000	А	1	b	х	q	b	4	5	t	t	U	U	Ν	n	/	i

通過Linux電腦運行證書之後。

[admin@	local	host	Des	ktop]	\$ od	- C	MRJ	CA.p	em							
00000000						в	Е	G	I	Ν		С	Е	R	Т	I
0000020	F	I	С	А	Т	Е						\n	М	I	I	G
0000040	t	D	С	С	В	Z	У	g	А	W	I	В	Α	g	I	Т
0000060	R	Q	А	А	А	Р	n	р	ι	У	n	В	0	h	j	Z
0000100	а	W	А	Е	А	А	Α	Α	+	Т	Α	Ν	В	g	k	q
0000120	h	k	i	G	9	w	0	В	Α	Q	s	F	\n	Α	D	В
0000140	0	М	R	U	w	Е	W	Y	К	С	Z	I	m	i	Z	Р
0000160	У	L	G	Q	В	G	R	Y	F	Т	G	9	j	Y	U	W
0000200	х	F	z	А	v	в	g	о	J	k	i	а	J	k	/	I
0000220	s	Z	А	Е	Z	F	g	d	Р	с	2	9	j	\n	L	W
0000240	р	v	М	R	w	W	G	g	Y	D	V	Q	Q	D	Е	х
0000260	N	Р	с	2	9	j	L	W	р	v	L	U	Ν	D	Т	ι
0000300	R	Е	Q	z	А	У	L	U	Ν	В	М	В	4	Х	D	Т
0000320	I	х	М	D	Q	W	Ν	D	I	х	М	j	U	х	\n	М
0000340	ι	0	Х	D	Т	I	Z	М	D	Q	W	Ν	D	I	х	М
0000360	j	U	х	М	ι	о	W	J	j	Е	k	М	С	I	G	А
0000400	1	U	Е	А	х	М	b	Т	٧	J	к	L	U	F	Ν	U
0000420	С	1	U	R	У	1	Ν	Ν	S	0	W	М	s	5	q	\n
0000440	d	С	5	q	d	G	d	У	b	3	V	W	М	I	I	В
0000460	I	j	А	Ν	В	g	k	q	h	k	i	G	9	W	0	В
0000500	Α	Q	Е	F	А	А	0	С	А	Q	8	Α	М	I	I	В
0000520	С	g	К	С	А	Q	Е	А	s	g	4	Z	s	m	0	Y
0000540	\n	W	Т	2	Q	Υ	0	7	h	h	z	d	8	b	+	К
0000560	b	s	U	М	с	Q	Q	0	5	0	р	0	g	q	v	е
0000600	1	Q	5	2	G	7	Т	m	W	е	+	v	m	q	+	Е
0000620	Y	Н	W	b	В	Т	g	D	9	9	к	D	ι	х	R	0
0000640	ι	\n	0	S	У	I	g	3	W	k	i	ι	М	р	I	ι
0000660	u	Р	i	0	Е	U	Н	d	А	с	2	Т	q	Α	d	W
0000700	0	r	е	Е	М	k	Н	ι	F	n	Q	5	4	G	J	ι
0000720	W	Z	6	S	о	h	I	9	J	2	8	h	/	L	k	R
0000740	f	8	\n	Z	3	5	В	q	q	F	0	х	р	s	8	s
0000760	0	k	р	7	1	0	7	Н	А	1	b	х	q	b	4	5
0001000	t	t	U	U	Ν	n	/	i	٧	7	Ζ	l	У	а	J	Х

對於FMC,在Linux電腦上結合Root_CA和無回車證書,請使用下一個命令。

cat

例如,cat Clean-interface_CSR_CA-signed_DER_CER_PEM_no-carriage.pem Root-CA.pem > combine.pem。

或者,也可以在Linux電腦中開啟一個新的文本編輯器,將刪除回車的Clean證書合併到一個檔案中,然後使用.PEM副檔名儲存該檔案。您必須將CA證書放在頂部,將Clean Interface證書放在底部 。



該證書必須是您稍後上傳到FMC以與TG裝置整合的證書。

證書上傳到TG裝置和FMC

上傳乾淨介面的證書

導覽至Configuration > SSL > PANDEM - Actions Upload New Certificate > Add Certificate,如下 圖所示。

CISCO Threat Grid	Appliance Home Configuration Status Operations Support	
Configuration	Upload SSL certificate for PANDEM	
CA Certificates	KrC8naXNCsN9D/9weTU6WKXBGI46MrJHffk1fSbFbQDkHC	×
Change Password	gkeQHT18nxjF6mJ9ekfirYNGKLCqAFNu2dMDNvTQhmVAPy File Home Share View	~ 🕜
Clustering	pgalM7rLfotadcl26KIPfuhg3TVJgreiRs38jat0FDFqKtE6kuOm $\leftarrow \rightarrow \checkmark \uparrow$ > New folder > Original > 16 \checkmark © \land Search 16	
Date and Time	c55Kk/gfNdMCliq6fAfobxGl/VjFQN+PUtSOmkvzzd0SCKxam A Name Date modified Type Size	
Email	QH/ 3/20/2021 12:44 AM Privacy Enhanced	1 KB
Integrations	MB0GA1UdDgQWBBTC42Sse9pCs/DXxHe6mXqzm3jw0DA	2 KB 1 KB
License	Private Key (PEM) Privacy Enhanced	3 KB
Network	Control Contro Control Control Control Control Control Control Control Control Co	2 KB
Network Exit	END EC PARAMETERS Lightshot	
NFS	MIH-cqEBBEIBCqBhqFBuuEEsV/fcgAdpdAyHNIZnXZ/gD/U To FMC	
Notifications	IXMRPDaticOjolic IVrgandodi/2007 0 egbw1rAcE2RC07 IXffqxkD7yLF2A2wu+HFxAnh2Kb4wV9jY3TB3xFvNovNEv7/	
SSH	7g5t9l0U2heq7eVkMQHp+Cl1CuenzXUkwYUW1HPF100Q(
SSL		
Syslog	Add Certificate Cancel	

上傳管理員介面的證書

. .

導覽至Configuration > SSL > OPADMIN - Actions Upload New Certificate > Add Certificate,如下 圖所示。

Threat Grid	Appliance Home Configuration Status 0	Operations Support				
Configuration E	Upload SSL certificate for OPADMIN Certificate (PEM) 8a2ieTLPQDTiy/62Q85+QIG2a9ws5p2+zKZpNeiEVyfrbBl0c IdeAdtEND3TYYDsEEm/e6aKRIcF2QyQDe/3laMvSJGG rRSEo1jeTUByg1yHX8FRh9CzdkRVdExue40mhpyaluQZT1y xa4F7xXBY/dZ1K8Q7IYGe-2LLeeQ6dBP/VmK6mQ4mdAlGq R6EmfDL91g54Qg/WQSLSC+ackZy+Htx2gFkY1/aeVAmC VIGwOnMyXT4K/RHOCOHHV8W35MpLVI1yqrR9i5II1bv8M 82fbaV7E7cgtLdazp6/C+zfqI80E7Jyr3GJw3RVc75KpzTDQA 5/Qh1YYg=END CERTIFICATE Private Key (PEM)BEGIN EC PRIVATE KEY MIHcAqEBEIBOQ9ndFBuuEEsV/YeqAdpfAyHNTZnNZ/gD/U 9tKmRPDahdQj8UE1VR8BRGca/Zguj7UegBWYFK4EEACO UKfmxKP2JF22Avu+HFxAnh2Kb4wV9Y3TB3Z+WNVNEV7/ 7gS19I0UZheq7eVkMQHp+CL1CuenzxUikwYUw1frPPT00Q JFOXwn1dzHKnPImN/SMJ7AVg11pDAIWDVWwjuJCSw==END EC PRIVATE KEY Site	Image: Image	higinal > 15 Name ^ Admin.Private-EC-key.pem Admin.interface_CSR_CA-signed_DER_C Clean.Private-EC-key.pem Clean.Interface_CSR_CA-signed_DER_CE Root-CA.pem	V Č Date modified 3/20/2021 12-44 AM 3/20/2021 12-44 AM 3/20/2021 12-44 AM 3/20/2021 12-44 AM 3/20/2021 12-44 AM 3/20/2021 12-44 AM 3/20/2021 12-44 AM	Search TG Type Privacy Enhanced Privacy Enhanced Privacy Enhanced Privacy Enhanced Privacy Enhanced	□ X ✓ ● Size 1 K8 2 K8 3 K8 2 K8 2 K8 2 K8
	Add Certificate					

將證書上傳到FMC

若要將憑證上傳到FMC,請導覽至AMP > Dynamic Analysis Connections > Add New Connection,然後填寫所需的資訊。

名稱:要標識的任何名稱。

主機:清潔介面FQDN,在生成清潔介面的CSR時定義

證書:ROOT_CA和clean interface_no-carriage的組合證書。

	🐝 Cisco® ISE Configuration 🛛 🗙 🔮 Privacy error	X 🗱 Cisco Firepower Management Ce X +	- 0 ×										
ĺ	Cisco® ISE Configuration 5.2.240/ddd/#Dynam 5.2.240/ddd/#Dynam	nicAnalysisConnections 🖈 🕴											
	CISCO AMP / Dynamic Analysis Connections	Q Overview Analysis Policies Devices Objects AMP Intelligence Deploy	🔅 👩 admin 🔻										
		Add New Connection	Add New Connection										
	Cloud Name		Actions										
	Cisco Sandbox API, US Cloud	Name: 75 ThreatGrid Host: WNcconstruction com Certificate Upload: C:\fakepath\PANDEM_clean-interf Browse Use Proxy When Available:	/ •										
		Cancel Register											

註冊新連線後,將顯示一個彈出視窗,按一下**Yes按**鈕。

🐝 Cisco 🖲 ISE Configuration 🛛 🗙 📔 🍪 Privacy error	× Sisco Firepower Management Ce × +	_ 8 X
← → C ▲ Not secure 172.16.2.240/ddd/#Dyna	micAnalysisConnections	☆ 🔒 :
Firepower Management Center AMP / Dynamic Analysis Connections	Q Overview Analysis Policies Devices Objects AMP Intelligence Deploy 🥩	🔅 🕑 admin 🔻
Cloud Name	Add New Connection	dd New Connection
Cisco Sandbox API, US Cloud	Name: DS	/ %
	ThreatGrid Host: WMP2441 Certificate U C:\fakepat Use Proxy W No Yes	
	Cancel Register	

頁面重定向至TG Clean介面和登入提示,如圖所示。



接受EULA。

← → ♂ ✿	🖸 🔒 https://wmp	.cor	m /eula.html	?next=%2Fa	ctivate_device9	63Fdevice_key%3D0500000	000 F G	2 ☆	: III\ 🗉) ® Ξ
cisco Threat Grid	Submit Sample	Dashboard	Samples	Reports	Indicators	Administration \checkmark		Q ? ()		admin 🗸
THREAT GRID SERVICE Terms of Use Agreement										
This is a legal agreement ("Agreement") between you, the party using the Threat Grid Service, and Cisco Systems, Inc., a California corporation having offices at 170 West Tasman Drive, San Jose, CA 95134 ("Cisco"). This Agreement applies to your access and use of Cisco's Threat Grid Service. By clicking accept or using the Cisco Technology, you agree that such use is governed by the Cisco End User License Agreement and the applicable Product Specific Terms (collectively, the "EULA"). You also acknowledge and agree that you have read the Cisco Privacy Statement. If you do not have authority to bind your company and its affiliates, or if you do not agree with the terms of the EULA, do not click 'accept' and do not use the Cisco Technology. If you are a Cisco channel partner accepting on behalf of an end customer ("customer"), you must inform the customer that the EULA applies to customer's use of the Cisco Technology and provide the										
customer with access to all relevant terms. BY CLICKING ON THE "I AGREE" BUTTON BELOW YOU ACKNOWLEDGE THAT YOU HAVE READ ALL OF THE TERMS AND CONDITIONS OF THIS AGREEMENT, UNDERSTAND THEM, AND AGREE TO BE LEGALLY BOUND BY THEM.						ŗ	Full Name: A Title: A	xdministrator xdministrator Agree		

成功整合將顯示活動裝置,如下圖所示。

← → ♂ ☆	0 & https://wmp.com/activate_device?device_key=0500000000000000000000000000000000000	· 🖂 🕁	⊻ ∥\ ₪ இ ≡
cisco Threat Grid	Submit Sample Dashboard Samples Reports Indicators Administration 🗸	Q ? () admin 🗸
	Active Device A device has been registered and activated with your appliance. Device Type FMC Model 42 Model ID 52 Mgmt IF 005056B95288 Current status Active	Return	

按一下「**Return**」,返回FMC,成功整合TG,如下圖所示。

Firepower Management Center AMP / Dynamic Analysis Connections	۹	Overview	Analysis	Policies	Devices	Objects	AMP	Intelligence	
Cloud Name			Host					Purpose	
ThreatGrid			W	pj.com	n	File Submissions, Private Report Lookups			
Cisco Sandbox API, US Cloud			fmc.api.t	threatgrid.com		Public Report Lookups			

相關資訊

- Firepower管理中心配置指南6.6版
- 技術支援與文件 Cisco Systems