Dépannage de l'intégration de Threat Grid Appliance avec FMC

Contenu

Introduction Conditions préalables **Conditions requises Components Used** Problème Scénario 1 Scénario 2 Intégration Certificats signés par l'autorité de certification interne pour l'interface Clean Admin **Nettoyer l'interface Interface Admin** Nettoyer l'interface CSR et CER vers PEM Interface administrateur CSR et CER vers PEM Format approprié du certificat pour FMC PEM SOUS Différence entre le certificat créé sous Windows et le certificat créé sous Linux Chargement de certificat sur l'appliance TG et FMC Télécharger le certificat pour une interface propre Télécharger le certificat pour une interface d'administration Télécharger le certificat vers FMC Informations connexes

Introduction

Ce document décrit en détail l'intégration de Thread Grid Appliance (TGA) avec Firepower Management Center (FMC).

Conditions préalables

Conditions requises

Cisco vous recommande de prendre connaissance des rubriques suivantes :

- Firepower Management FMC
- Configuration de base de l'appliance Threat Grid
- Créer des certificats d'autorité (CA)
- Linux/Unix

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- FMC version 6.6.1
- Threat Grid 2.12.2
- CentOS 8

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. Si votre réseau est en ligne, assurez-vous de bien comprendre l'incidence possible des commandes.

Problème

Dans ce scénario utilisé, vous pouvez voir 2 problèmes et deux codes d'erreur.

Scénario 1

L'intégration échoue avec des erreurs :

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

Lorsqu'il s'agit de ce problème, le problème est lié au certificat qui n'est pas téléchargé dans FMC en tant que chaîne complète. Puisque le certificat signé par l'autorité de certification a été utilisé, il faut utiliser l'ensemble de la chaîne de certificats regroupée en un seul fichier PEM. Dans un autre mot, vous commencez par **CA racine > Cert intermédiaire** (le cas échéant) **> Clean Int**. Veuillez consulter <u>cet article</u> du guide officiel qui décrit les exigences et la procédure.

S'il existe une chaîne de signature à plusieurs niveaux d'autorités de certification, tous les certificats intermédiaires requis et le certificat racine doivent être contenus dans un fichier unique qui est téléchargé vers le FMC.

Tous les certificats doivent être codés par PEM.

Les nouvelles lignes du fichier doivent être UNIX et non DOS.

Si l'appliance Threat Grid présente un certificat auto-signé, téléchargez le certificat que vous avez téléchargé à partir de cet appareil.

Si l'appliance Threat Grid présente un certificat signé par l'autorité de certification, téléchargez le fichier qui contient la chaîne de signature du certificat.

Scénario 2

Erreur de format de certificat non valide

Invalid Certificate format (must be PEM encoded) (code=0) Erreur de format de certificat, comme illustré dans l'image.



Cette erreur est due à la mauvaise mise en forme du certificat PEM combiné créé sur l'ordinateur Windows qui utilise OpenSSL. Il est fortement recommandé d'utiliser une machine Linux pour créer ce certificat.

Intégration

Étape 1. Configurez le TGA, comme indiqué dans les images.

cisco Threat Grid	Appliance Home Configuration Status Operations Support
Configuration 😑	Network Configuration
Authentication	CLEAN interface
CA Certificates	MAC Address: a4 Address: 172.16.2.103 (STATIC)
Clustering	IP Assignment
Date and Time	STATIC
Fmail	ID Address
Integrations	172.16.2.103
License	Subact Mask
Network	255,255,255,0
Network Exit	
NFS	172 16 2 254
Notifications	
SSH	Host Name
SSL	*
Syslog	Primary DNS Server
	Secondary DNS Server
	91

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) Se	ecurity
<u>H</u> ost (uses	parent domain if left blank):
TG-M5	
<u>F</u> ully qualifie	ed domain name (FQDN):
TC	.com
I <u>P</u> address:	
10	8.30
✓ Update	associated pointer (PTR) record

Certificats signés par l'autorité de certification interne pour l'interface Clean Admin

Étape 1. Générez la clé privée qui est utilisée à la fois pour l'administration et pour l'interface propre.

openssl ecparam -name secp521r1 -genkey -out private-ec-key.pem Étape 2. Générer CSR.

Nettoyer l'interface

Étape 1. Accédez à la création CSR et utilisez la clé privée générée.

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

Note: Le nom CN doit être entré pour CSR et doit correspondre au nom d'hôte de l'interface Clean défini sous « Réseau ». Une entrée DNS doit être présente sur le serveur DNS qui résout le nom d'hôte de l'interface Clean.

Interface Admin

Étape 1. Accédez à la création CSR et utilisez la clé privée générée.

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

Note: Le nom CN doit être entré pour CSR et doit correspondre au nom d'hôte de l'interface d'administration définie sous Réseau. Une entrée DNS doit être présente sur le serveur DNS qui résout le nom d'hôte de l'interface propre.

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

Étape 2. CSR doit être signé par CA. Téléchargez le certificat au format DER avec l'extension CER.

Étape 3. Convertir CER en PEM.

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

Nettoyer l'interface CSR et CER vers PEM

Interface administrateur CSR et CER vers PEM

Format approprié du certificat pour FMC

Si vous avez déjà reçu des certificats et qu'ils sont au format CER/CRT et lisibles lorsqu'un éditeur de texte est utilisé, vous pouvez simplement changer l'extension en PEM.

Si le certificat n'est pas lisible, vous devez convertir le format DER en format PEM lisible.

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

PEIN

Exemple de format PEM lisible, comme illustré dans l'image.

1	BEGIN CERTIFICATE
2	MIIFozCCA4ugAwIBAgITGQAAAALex/EgACaWIAAAAAAAAjANBgkqhkiG9w0BAQUF
3	ADAaMRgwFgYDVQQDEw9Ub21EZW1vIFJvb3QgQ0EwHhcNMTQwMjA3MTQwMTU3WhcN
4	MjQwMjA3MTQxMTU3WjBKMRIwEAYKCZImiZPyLGQBGRYCc2UxFzAVBgoJkiaJk/Is
5	$\verb+ZAEZFgd0b21kZW1vMRswGQYDVQQDExJUb21EZW1vIE1zc3VpbmcgQ0EwggEiMA0G$
6	CSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDC8XmXxLHo0M/521CFtI4DSN6qVNAN
7	8jxujS4PSSRnQtaqpbjbcAZpvbYysNt2uwA40urkxY2nyn4SMy/21S4L9x10u8su
8	W+/4T2dcFgQKzFiNyqVkLop9vRKnCKjceD+FRKXbPCSZyy4Hhz/XCgwPRfaobx+q
9	aV1fSnW0F a2MHx60jf
10	BhdyONMrZxmQeYgFPUmd2o3x+1yq1406hIF7LLGFAoDdqi3R31D9OPb7+Dm2ezv0
11	OKkbCHdjl3inB3D1tg1L8mZeIEte+07RvlQXr33umO6zeYi4okbaHZLvAgMBAAGj
12	$\verb"ggGwMIIBrDAQBgkrBgEEAYI3FQEEAwIBADAdBgNVHQ4EFgQU0+wPInpDnoqnuIlx"$
13	$\verb BtUbIGLdS1UwgYsGA1UdIASBgzCBgDB+BgorBgEEAYKdZwEBMHAwPgYIKwYBBQUH $
14	$\verb AgiwMh4wAFQAbwBtAEQAZQBtAG8AIABQAG8AbABpAGMAeQAgAFMAdABhAHQAZQBt $
15	AGUAbgB0MC4GCCsGAQUFBwIBFiJodHRw0i8vcGtpLnRvbWRlbW8uc2UvcGtpL2Nw
16	$\verb"cy5odG0AMBkGCSsGAQQBgjcUAgQMHgoAUwB1AGIAQwBBMAsGA1UdDwQEAwIBhjAP"$
17	${\tt BgNV} H{\tt RMBAf8EBTADAQH}/{\tt MB8GA1UdIwQYMBaAFL00e0rG2ExZ1dmboIuLwgGgPr5e}$
18	MEIGA1UdH
19	${\tt RGVtbyUyMFJvb3Q1MjBDQS5jcmwwTQYIKwYBBQUHAQEEQTA/MD0GCCsGAQUFBzAC}$
20	hjFodHRwOi8vcGtpLnRvbWRlbW8uc2UvcGtpL1RvbURlbW81MjBSb290JTIwQ0Eu
21	Y3J0MA0GCSqGSIb3DQEBBQUAA4ICAQBBkNHa1bX3kkpOXCV3nQ9R4CyG61WI90gL
22	57 u GRcpulSqUu790J5s4xlW8rhm32db7qvHDPaYED23gudpOSHyUywZTFbwzm92c
23	$\verb+e1wZpyJH6nsuqNFDTYQTdWAq8zwCrldcUFRW301mkPuhENjttqCIJ9KeLrwCaM/p$
24	$\label{eq:QVy7qWoTU14/BY+OsLXDGURXrGejcVs8ZQy4bqhmh0TfelTcAOAX47pVt8XdnWFe} QVy7qWoTU14/BY+OsLXDGURXrGejcVs8ZQy4bqhmh0TfelTcAOAX47pVt8XdnWFe \\ \end{tabular}$
25	Vnu/rwuOnfvlyiWW62cknAATaagnLXdbFWIxnVSlbooZmYXXQqelFxJVlbhNdWM9
26	tgdq3t2qBXj3P7XiD+OWfzkABGMJrmki55LNp10/oV+Kw3DuyGYLurq6TWWlJi8J
27	94GJm9VQBX1Py1FQn0hILcxgr+LAIKX0PqXTyRCp1/UGH1ih05S1F4GvPEj0s1BA
28	ebRkDrN2vU+9kq8UXOhzxierQDmJkCOpSUWV6Pk6/OP72vxIuAQQNdY++cJRwzi+
29	adWp6cZBzW5h3OdKlyEDdjNB75rzQcwMlerYTABSIaK6KCTNb70F4kTWlB5RlWqD
30	VXyboYEbf0ym5CiNmDKUXqQMI45FIztDhYjJqn1NeroJUZnUYa9y63zujy2uyQeG
31	EVWpXscPOfrcrCfSuvx0KsMiLxuclfVJyCAJqBMG++LgWxhb247CvhSDK2wZrq0+
32	Q70p0WaYww==

SOUS

Exemple de format DER lisible, comme illustré dans l'image

1	0, ENQ£0, ETX< ETXISTXISOHISTXISTXIDC3EMINULINULISTXÞÇÑ NUL&-
	NULNULNULSTXO
2	ACK * tHt÷
3	SOHISOHIENQIENQINULO SUB1 CANO SYNACKIETXUEOTIETXIDC3IST. CAO RSIETB
4	140207140157Z
5	240207141157Z0J1 DC20 DLE ACK
6	'&%"````````````````````````````````````
7	'&%"````````````````````````````````````
	Issuing CAO, SOH"O
8	ACK *†H†÷
9	SOH SOH SOH ENONULETX, SOH SINULO, SOH
10	STX, SOHSOHNULÂñy-ıèÐÏùÛP…´Ž⊠TXHÞªTÐ
11	ò <n.sdi\$gbö°¥,ûpmck1¾12°ûv»nud8òêäŧê~dc23 th="" öõ.vd÷gst»ë.[ïøog\syncod<=""></n.sdi\$gbö°¥,ûpmck1¾12°ûv»nud8òêäŧê~dc23>
12	ÌXÊ¥d.Š}%DC2SBS"Üx?…D¥Û<\$™Ë.BDD‡?×
13	ERSDEö"oUS°i]_Ju´?£1UmUS^BÆòFÁ…¾EDŰÖ;)EODÒcoúONAK;Á·'ôÁ"ZØÁñëHßACKEDE
	r8ó+gDMy^DNO=IÚñú*×:"{,±…SNX€Ý°-ÑßPý8öûø9¶{;ô8©DSCBSwc—x§BDDpõ¶
14	Kòf^
	K^ûNѾTERE}îî³y^, ¢FÚES'ïSTXERXSOHNULSOH£, SOH°0, SOH¬0DLEACK
	+ ACK SOHEOT SOH, 7 NAK SOHEOT ETX STX SOHNUL 0 GS ACK ETXU GS SO EOT SYN EOT DC4 Ó 1
	SI"zCžŠ§,‰qACKIÕESC bÝKU0 <acketxugs eotf0€0~ack<="" th=""></acketxugs>
15	+ACKSOHEOTSOH, gSOHSOH0p0>ACKBS+ACKSOHENOENOBELSTXSTX02RS0NULTNUL0
	NULMNULDNULeNULMNULONUL NULPNULONUL1NULiNULCNULYNUL
	NULSNULtNULANULtNULeNULmNULeNULnNULt0.ACKBS+ACKSOHENQENQBELSTXSOH
	SYN' <u>.htm</u> NUL0EMACK
	+ACKSOHEOTSOH, 7 DC4 STXEOT FFRS
16	NULSNULDNULDNULCNULAOVTACKETXUGSSTEOTEOTETXSTXSOH†0STACKETXUGS
	DC3SOHSOHÿEOTENO0ETXSOHSOHÿ0USACKETXUGS#EOTCAN0SYN€DC43×4{JEØLYÕÙ>

Différence entre le certificat créé sous Windows et le certificat créé sous Linux

Une simple comparaison côte à côte des deux certificats à côté de l'autre vous pouvez utiliser le plug-in **Comparer** dans le Bloc-notes ++ a révélé la différence encodée dans la ligne #68. Sur la gauche, vous pouvez voir le certificat créé dans Windows, sur la droite vous pouvez trouver le certificat généré sur la machine Linux. Celui de gauche a un retour chariot qui rend ce PEM certificat non valide pour FMC. Cependant, vous ne pouvez pas faire la différence dans l'éditeur de texte sauf pour cette ligne du Bloc-notes ++.



Copiez le certificat PEM nouvellement créé/converti pour l'interface RootCA et CLEAN sur votre machine Linux et supprimez le retour chariot du fichier PEM.

sed -i 's/\r//'

Exemple, sed -i 's/\r//' OPADMIN.pem.

Vérifiez si le retour chariot est présent.

od -c

Certificats dont le retour chariot est toujours présenté, comme l'illustre l'image.

[admin@	local	host	Des	ktop]\$ od	- c	MRJ	CA.c	er							
0000000						в	Е	G	I	Ν		с	Е	R	т	I
0000020	F	I	с	Α	т	Е						١٢	\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	А	А	Р	n	р	ι	У	n	В	0	h	j
0000100	Z	а	W	Α	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	А	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	Ν
0000300	D	т	ι	R	E	Q	z	Α	У	L	U	Ν	В	М	В	4
0000320	х	D	т	I	x	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	Ν
0000360	D	I	х	М	j	U	х	М	ι	0	W	J	j	Е	k	М
0000400	С	I	G	Α	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	Α	Ν	В	g	k	q	h	k	i
0000500	G	9	W	0	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	0	ι	\r	\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	N	n	/	i

Certificat après avoir exécuté cela via une machine Linux.

[admin@	local	host	Des	ktop]]\$ od	- C	MRJ	CA.po	em							
0000000						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	Ζ	у	g	А	W	I	В	Α	g	I	Т
0000060	R	Q	А	А	А	Ρ	n	р	ι	у	n	В	0	h	j	Z
0000100	а	W	А	Е	А	А	Α	Α	+	Т	А	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	Ζ	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	۷	Q	Q	D	Е	х
0000260	N	Р	с	2	9	j	L	W	р	v	L	U	Ν	D	Т	l
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	Ι	Z	М	D	Q	W	Ν	D	I	х	М
0000360	j	U	х	М	ι	0	W	J	j	Е	k	М	С	I	G	А
0000400	1	U	Е	А	х	М	b	Т	V	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	+	K
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	+	E
0000620	Y	Н	W	b	В	Т	g	D	9	9	К	D	ι	х	R	0
0000640	ι	\n	0	S	У	Ι	g	3	W	k	i	ι	М	р	I	l
0000660	u	Р	i	0	E	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	l
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	N	n	/	i	٧	7	Ζ	ι	у	а	J	Х

Pour FMC combiner Root_CA et le certificat no-chariot sur une machine Linux, utilisez la commande suivante.

cat

Par exemple, **cat Clean-interface_CSR_CA-signed_DER_CER_PEM_no-chariot.pem Root-CA.pem > combine.pem.**

Vous pouvez également ouvrir un nouvel éditeur de texte dans votre machine Linux et combiner les deux certificats Clean avec retour chariot supprimé dans un fichier et l'enregistrer avec l'extension .PEM. Vous devez avoir votre certificat CA en haut et le certificat Clean Interface en bas.



Il doit s'agir du certificat que vous téléchargez ultérieurement sur votre FMC pour l'intégrer à l'appareil TG.

Chargement de certificat sur l'appliance TG et FMC

Télécharger le certificat pour une interface propre

Naviguez jusqu'à Configuration > SSL > PANDEM - Actions Upload New Certificate > Add Certificate, comme indiqué dans l'image.

CISCO Threat Grid	Appliance Home Configuration Status Operations Support	
Configuration Authentication CA Certificates Observe Decement	Upload SSL certificate for PANDEM Certificate (PEM) KrC8naXNCsN9D/9weTU6WKXBGI46MrJHffk1fSbFbQDkHC I 7 15 - 0 gkeQHT18nxjF6m.J9ektfin7NGKLCqAFNu2dMDNxTQhmVAPp File Home Share View	× ~ 0
Clustering Date and Time	pgalM7rLfotadcl26KIPfuhg3TYJgraiRs38jat0FDFqKtE6kuOm VGrruqES6C6kbk0Wi28oJ0BiBinh1UGLdc/wzKz5xwaa+0e C55KxigfNMCling6/fobWi28oJ0BiBinh1UGLdc/wzKz5xwaa+0e C55KxigfNMCling6/fobWi28oJ0BiBinh1UGDc/wzKz5xwaa+0e C55KxigfNMCling6/fobWi28oJ0BiBiAh1UDwQEAwIBhjAf W Guick access QH/ QH/	1 KB
License	Image: Application of the state of the	2 KB 1 KB 3 KB 2 KB
Network Network Exit NFS	BgUrgQQAIve= DestropEND EO PARAMETERS Lightshot Lightshot MIHcAgEBBEIBOgghqFBuuEEsV/yegAdplAyHNTZnX/gD/U TG to FMC WitweDDAeDROCon (2017) InoRuNEEVEEDC0	
Notifications SSH SSL	SIXIFY Vallocitor Tryporterior (Section 1) (Section 1) (Section 1) (Section 2) (Section 1) (Section 2) (Section 2	
Syslog	Add Certificate Cancel	

Télécharger le certificat pour une interface d'administration

Accédez à Configuration > SSL > OPADMIN - Actions Upload New Certificate > Add Certificate, comme indiqué dans l'image.

Threat Grid	Appliance Home Configuration Status Operations Support	
Configuration	Upload SSL certificate for OPADMIN Certificate (PEM) BazietLPQDTijy/62Q85+QIGza9ws5pz+zKZpNeiEVyfrbBI0c = 1 2 = 1 TG JekAtleLRD03TYYD62EEm/e6aKRicFZQyQDe/9JaMW5JGG rie Home Share View	□ × ~ •
Clustering Date and Time Email Integrations	xa4+ xxky*/dz/tk8U/Ydc*zLeCQbd8Pr/vmkbmQ4mQAttod {	Size 1 KB 2 KB 1 KB 3 KB
Network Network Exit NFS Notifications SSH	END EC PARAMETERS BSOD BEGIN EC PRIVATE KEY Desktop MIHcAgEBBEIBOQ9hqFBuuEEsV/YgoAdp/AyHNTZnNZ/qD/U Desktop jttw:RPDahd0j8UE1Nq8gRGCac/Z0j/JUegBwYFK4EEACOI Lightshot XTarxkD7yLF2AZwu+HFXahn2XbdwW9y3TB3xFvNovNEv7/J To to FMC. JEOXwm1dzHtknPtmN/SMj7AVg1JpD4IWDvWwjvJCSw= OneDrive END EC PRIVATE KEY Sitems 1 item selected 1.90 KB	2 KB
SSL Syslog	Add Certificate Cancel	

Télécharger le certificat vers FMC

Afin de télécharger le certificat sur le FMC, accédez à **AMP > Connexions d'analyse dynamique > Ajouter une nouvelle connexion**, puis renseignez les informations requises.

Name : Tout nom à identifier.

Hôte : Nom de domaine complet (FQDN) de l'interface propre tel que défini lors de la génération du CSR pour l'interface propre

Certificat: Certificat combiné de ROOT_CA et interface_no-chariot propre.

	🐝 Cisco® ISE Configuration 🛛 🗙 🧶 Privacy error	X dt Cisco Firepower Management Ce X +	
ĺ	Cisco® ISE Configuration 5.2.240/ddd/#Dynai	micAnalysisConnections	☆ 🛛 :
	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: ThreatGrid Host: When the set of th	/ *
		Cancel Register	

Une fois la nouvelle connexion enregistrée, une fenêtre contextuelle s'affiche, cliquez sur le bouton **Oui**.

💷 Cisco® ISE Configuration 🛛 🗙 📔 🍪 Privacy error	× ditte Cisco Firepower Management Ce × +	_ 0 ×
← → 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	Add New Connection
Cisco Sandbox API, US Cloud	Name: ThreatGrid Host: Creating Connection Do you want to allow redirection to another page to complete registration? C:\fakepat Use Proxy W No Yes Cancel Register	25

La page est redirigée vers l'interface TG Clean et l'invite de connexion, comme illustré dans les images.



Acceptez le CLUF.

← → ♂ ☆	🛛 🔒 https://wmp	.co	m /eula.html	?next=%2Fa	ctivate_device9	63Fdevice_key%3D050000000] … ⊠ ☆	±	lii\ 🗉) (2) =
Cisco Threat Grid	Submit Sample	Dashboard	Samples	Reports	Indicators	Administration 🗸		٩ ٢ ()		admin 🗸
			-	THREAT (Terms of	GRID SERVI Use Agreeme	CE nt				
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.						ne: Adminis	strator			
						tle: Adminis	Administrator			
						I Agree				

L'intégration réussie affiche un périphérique actif, comme l'illustre l'image.

\leftarrow \rightarrow C \textcircled{a}	🛛 🔊 https://wmp	com/activate_devi	e?device_ke	ey=0500000000000000000000000000000000000	000000000000000000000000000000000000000	$\overline{\mathbf{A}}$	II\ 🗉 🛎 🗄
cisco Threat Grid	Submit Sample Dashb	oard Samples Reports	Indicators	Administration \checkmark	٩	° ()	admin 🗸
	Active Device A device has been regist Device Type Model Model ID Mgmt IF Current status	E tered and activated with FMC 42 52 005056B95288 Active	your appli	ance.	Return		

Cliquez sur Retour, revenez à FMC avec intégration TG réussie, comme illustré dans l'image.

alialia cisco	Firepower Management Center AMP / Dynamic Analysis Connections	۹	Overview	Analysis	Policies	Devices	Objects	AMP	Intelligence
Cloud Name	3			Host					Purpose
ThreatGrid					pj.cor	n	File Submissions, Private Report Lookups		
Cisco Sandbox API, US Cloud			fmc.api.t	hreatgrid.com		Public Report Lookups			

Informations connexes

- Guide de configuration de Firepower Management Center, version 6.6
- Support et documentation techniques Cisco Systems