与FMC集成的Threat Grid设备故障排除

目录

简介 先决条件 要求 使用的组件 问题 场景 1 场景 2 集成 Clean Admin接口的内部CA签名证书 干净的接口 管理界面 <u>CSR和CER到PEM的干净接口</u> 管理接口CSR和CER到PEM FMC证书的正确格式 PEM DER 在Windows中创建的证书与在Linux中创建的证书之间的差异 证书上传到TG设备和FMC 上传安全接口的证书 <u>上传管理员接口的证书</u> 将证书上传到FMC 相关信息

简介

本文档详细介绍与Firepower管理中心(FMC)的线程网格设备(TGA)集成。

先决条件

要求

Cisco 建议您了解以下主题:

- Firepower管理FMC
- Threat Grid设备基本配置
- 创建授权证书(CA)
- Linux/Unix

使用的组件

本文档中的信息基于以下软件和硬件版本:

- FMC版本6.6.1
- Threat Grid 2.12.2
- CentOS 8

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原 始(默认)配置。如果您的网络处于活动状态,请确保您了解所有命令的潜在影响。

问题

在此使用的案例场景中,您可以看到2个问题和2个错误代码。

场景 1

集成失败,但出现错误:

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

在此问题中,问题与未作为完整链上传到FMC的证书有关。由于使用了CA签名的证书,因此需要将 整个证书链合并到一个PEM文件中。换句话说,您以根CA >**中间证书**(如果适用)> Clean Int开头 。请参阅<u>官方指</u>南中介绍要求和程序的本文。

如果存在多级CA签名链,则所有必需的中间证书和根证书必须包含在上传到FMC的单个文件中。

所有证书都必须采用PEM编码。

文件的新行必须是UNIX,而不是DOS。

如果Threat Grid设备提供自签名证书,请上传您从该设备下载的证书。

如果Threat Grid设备提供CA签名的证书,请上传包含证书签名链的文件。

场景 2

证书格式错误无效

Invalid Certificate format (must be PEM encoded) (code=0) 证书格式错误,如图所示。



此错误是由于在使用OpenSSL的Windows计算机上创建的组合PEM证书的格式错误所致。强烈建议 使用Linux计算机创建此证书。

集成

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

步骤1.配置TGA,如图所示。

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							
<u>H</u> ost (use	es parent domain if left blank):							
TG-M5	TG-M5							
<u>F</u> ully qual	<u>Fully qualified domain name (FQDN):</u>							
TO	.com							
I <u>P</u> addres	ss:							
10	18.30							
√ <u>U</u> pdat	te associated pointer (PTR) record							

Clean Admin接口的内部CA签名证书

步骤1.生成用于管理界面和干净界面的私钥。

openssl ecparam -name secp521r1 -genkey -out private-ec-key.pem 步骤2.生成CSR。

干净的接口

步骤1.导航至CSR创建并使用生成的私钥。

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

注意:必须为CSR输入CN名称,并且必须与"Network"下定义的Clean接口的主机名匹配。 DNS服务器上必须存在DNS条目,该条目解析了Clean接口主机名。

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

管理界面

步骤1.导航至CSR创建并使用生成的私钥。

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

注意:必须为CSR输入CN名称,并且必须与"Network"下定义的"admin interface"的 "hostname"匹配。DNS服务器上必须存在DNS条目,该条目解析了干净的接口主机名。

ADMIN interface
MAC Address: 40: 80 IP Address: 10 8.30 (STATIC)
IP Assignment STATIC ~
IP Address
Subnet Mask 255.255.192
Gateway
Host Name TG-M5
Save Activate

步骤2. CSR由CA签署。以DER格式下载证书,其中包含CER扩展名。

步骤3.将CER转换为PEM。

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

CSR和CER到PEM的干净接口

管理接口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 Organizational Unit 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_D ER_PEM.pem

FMC证书的正确格式

如果您已经获得证书,并且证书为CER/CRT格式,并且使用文本编辑器时可读,您只需将扩展更改 为PEM。

如果证书不可读,您需要将DER格式转换为PEM可读格式。

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

PEM

PEM可读格式示例,如图所示。

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	$\verb+BhdyONMrZxmQeYgFPUmd2o3x+lyq1406hIF7LLGFAoDdqi3R31D9OPb7+Dm2ezv0$
11	OKkbCHdjl3inB3D1tg1L8mZeIEte+07RvlQXr33umO6zeYi4okbaHZLvAgMBAAGj
12	$\verb"ggGwMIIBrDAQBgkrBgEEAYI3FQEEAwIBADAdBgNVHQ4EFgQU0+wPInpDnoqnuIlx"$
13	${\tt BtUbIGLdS1UwgYsGA1UdIASBgzCBgDB+BgorBgEEAYKdZwEBMHAwPgYIKwYBBQUH}$
14	${\tt Agiwh4wAFQAbwBtAEQAZQBtAG8AIABQAG8AbABpAGMAeQAgAFMAdABhAHQAZQBt}$
15	AGUAbgB0MC4GCCsGAQUFBwIBFiJodHRw0i8vcGtpLnRvbWR1bW8uc2UvcGtpL2Nw
16	$\verb"cy5odG0AMBkGCSsGAQQBgjcUAgQMHgoAUwB1AGIAQwBBMAsGA1UdDwQEAwIBhjAP"$
17	$\verb"BgNVHRMBAf8EBTADAQH/MB8GA1UdIwQYMBaAFL00e0rG2ExZ1dmboIuLwgGgPr5e"$
18	MEIGA1UdH y5zZS9wa2kvVG9t
19	RGVtbyUyMFJvb3Q1MjBDQS5jcmwwTQYIKwYBBQUHAQEEQTA/MD0GCCsGAQUFBzAC
20	hjFodHRwOi8vcGtpLnRvbWR1bW8uc2UvcGtpL1RvbUR1bW81MjBSb290JTIwQ0Eu
21	Y3J0MA0GCSqGSIb3DQEBBQUAA4ICAQBBkNHa1bX3kkpOXCV3nQ9R4CyG61WI90gL
22	57 u GRcpulSqUu790J5s4xlW8rhm32db7qvHDPaYED23gudpOSHyUywZTFbwzm92c
23	e1wZpyJH6nsuqNFDTYQTdWAq8zwCrldcUFRW301mkPuhENjttqCIJ9KeLrwCaM/p
24	QVy7qWoTU14/BY+OsLXDGURXrGejcVs8ZQy4bqhmh0TfelTcAOAX47pVt8XdnWFe
25	Vnu/rwuOnfvlyiWW62cknAATaagnLXdbFWIxnVSlbooZmYXXQqelFxJVlbhNdWM9
26	tgdq3t2qBXj3P7XiD+OWfzkABGMJrmki55LNpl0/oV+Kw3DuyGYLurq6TWWlJi8J
27	94GJm9VQBX1Py1FQn0hILcxgr+LAIKX0PqXTyRCp1/UGH1ih05S1F4GvPEj0s1BA
28	ebRkDrN2vU+9kq8UXOhzxierQDmJkCOpSUWV6Pk6/OP72vxIuAQQNdY++cJRwzi+
29	adWp6cZBzW5h3OdKlyEDdjNB75rzQcwMlerYTABSIaK6KCTNb7OF4kTW1B5R1WqD
30	VXyboYEbf0ym5CiNmDKUXqQMI45FIztDhYjJqn1NeroJUZnUYa9y63zujy2uyQeG
31	EVWpXscPOfrcrCfSuvx0KsMiLxuclfVJyCAJqBMG++LgWxhb247CvhSDK2wZrq0+
32	Q70p0WaYww==

DER

DER可读格式示例,如图所示

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	ACK * + H + ÷
9	SOH SOH SOH ENONULETX, SOH SINULO, SOH
10	STX, SOHSOHNULÂñy—ıèÐÏùÛP…´ŽETXHÞªTÐ
11	ò <n.sdi\$gbö°¥,ûpacki¾12°ûv»nud8òêäŧê~dc23 th="" öõ.vd÷cst»ë.[ïøog\syneod<=""></n.sdi\$gbö°¥,ûpacki¾12°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©ESCBSwc—x§BEDpõ¶
14	Kòf^
	K^ûNѾTETB }î1°y^, ¢FÚGS'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 nue nue nue to . Ack BS + Ack Sofien O Eno BEE STX Sofi
	SYN'
	+ACKSOHEOTSOH, 7 DC4 STX EOT FFRS
16	NULS NULUNULD NULC NULA 0 VT ACK ETXUGS STEOT EOT ETX STX SOH † 0 ST ACK ETXUGS

DC3SOHSOHÿEOTENO0ETXSOHSOHÿ0USACKETXUCS‡EOT(CAN0SYN€DC4№4{JÆØLYÕÙ> //ÂSOH_>%^0BNCKETXUCSUSEOT•0907-5-3+1

在Windows中创建的证书与在Linux中创建的证书之间的差异

您可以在记事本++中使用**Compare** 插件对两个证书进行简单的并排比较,#68行中的编码区别被删除。在左侧,您可以看到在Windows中创建的证书,在右侧,您可以找到在Linux计算机上生成的证书。左侧的回车符返回,使该证书PEM对FMC无效。但是,除记事本++中的一行外,无法区分文本编辑器中的区别。



将新创建/转换的RootCA和CLEAN接口的PEM证书复制到Linux计算机,并从PEM文件中删除回车

0

sed -i 's/\r//'

示例, sed -i 's/\r//' OPADMIN.pem。

验证回车是否存在。

od -c

仍显示回车的证书,如图所示。

[admin@	local	host	Des	ktop]\$ 00	d-c	MRJ	CA.c	er							
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	А	А	Р	n	р	ι	У	n	В	0	h	j
0000100	Z	а	W	Α	Е	А	Α	А	A	+	Т	Α	Ν	в	g	k
0000120	q	h	k	i	G	9	w	0	В	Α	Q	s	F	١٢	\n	Α
0000140	D	В	0	М	R	U	w	E	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	Α	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	Е	х	N	Ρ	с	2	9	j	L	W	р	v	L	U	Ν
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	×	\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	о	W	J	j	Е	k	М
0000400	С	I	G	Α	1	U	E	А	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	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	١٢	\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	o	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

在通过Linux计算机运行证书之后。

[admin@	local	host	Des	ktop]]\$ od	l - c	MRJ	CA.pe	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	Р	n	р	ι	у	n	В	0	h	j	Z
0000100	а	W	А	Е	А	А	А	А	+	Т	Α	Ν	В	g	k	q
0000120	h	k	i	G	9	W	0	В	А	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	0	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	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	А	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	Y	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	0	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	V	7	Z	l	У	а	J	Х

对于FMC,在Linux计算机上将Root_CA和无回车证书组合使用下一个命令。

cat

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

或者,您也可以在Linux计算机中打开新的文本编辑器,将Clean证书和回车合并到一个文件中,并 使用.PEM扩展名保存。您的CA证书必须位于顶部,而Clean Interface证书位于底部。



这必须是您稍后上传到FMC的证书,以便与TG设备集成。

证书上传到TG设备和FMC

上传安全接口的证书

导航至Configuration > SSL > PANDEM - Actions Upload New Certificate > Add Certificate,如图 所示。

CISCO Threat Grid	Appliance Home Configuration Status Operations Support	
Configuration	Upload SSL certificate for PANDEM Certificate (PEM)	×
CA Certificates	krC8naXNCsN9D/9we1U6WKXBGi46MrJHftk11SbFbQDkHC	$\hat{}$
Change Password Clustering	Sc24CHs6kHc3Lbt779IOnsMgt0jp7VVVJINJSVQRWhn6QS pg8IM7rLfotadcl26KIPfuhg3TVJgreiRs38jat0FDFqKtE6kUOm ← → × ↑ → New folder → Original → 16 × 0 / Search 16 × 0 / Search 16	Ť
Date and Time	c55KxlgNdMCliq6fAfobxGiVpCQN+PUtSOmkvzzdOSCKxam CGSWdWExE0alAgMBAAGiUTBPNASGA1UdDwOEAwilBhiAF # Quick access Date modified Type Size	
Email	QH/ 3/20/2021 12:44 AM Privacy Enhanced 1 MB0GA1UdDqQWBBTC42Sse9pCs7DXxHe6mXqzm3jw0DA Documents # @ Admin_Private-EC-key.pem 3/20/2021 12:44 AM Privacy Enhanced 2	KB
Integrations	Downloads Private Key (PEM) Pri	KB
License	BEGIN EC PARAMETERS BSOD	KB
Network Exit	BQUIGUCAIW ¹¹ Desktop END EC PARAMETERS Lightshot	
NFS	MILCAGEBBEIBOONGANGFBUUESV/YegAdofAvHNTZNNZ/gD/U	
Notifications	9tKwRPDandOJ8IUE1VRg8RgCac/2011/UegBwYFK4EEACOI IXffqxkD7yLF2A2wu+HFxAnh2Kb4wV9)Y3TB3xFvNovNEv7/ OneDrive	
SSH	7gSt9/0UZheq7eVKMQHp+CL1CuenzxUikwYUw1frPPT00Qt — JFOXwn1dzHtknPtmN/sMj7AVg1JpD4/WDvWwjvJCSw== 5 items 1 item selected 1.90 KB	
SSL		
Syslog	Add Certificate Cancel	

上传管理员接口的证书

导航至Configuration > SSL > OPADMIN - Actions Upload New Certificate > Add Certificate,如图 所示。

cisco Thre	at Grid .	Appliance	Home	Configuration	Status	Operations	Support							
Configuration Authentication CA Certificates Change Password Clustering Date and Time Email Integrations License Network Network NFS Notifications SSH SSL		Upload SSL cc Certificate (PEM) 8a2ieTLPQDTIjy/6 JekAtleLRb03TYY rRSE01jeTUByg1V wa4F7x8KY/d2R8 R6fEmfDLI9tg540 VNGwOnMy2T4Kr 82tbaV7E7cgtLda 5rQhNYg= END CC PAR BEGIN EC PF MIHcAgEBBEIDQ 9tKwRPDahdQ8IU DRftqxkD7yLF2A2Q JFOXwn1dzHtknPI END EC PRI	ertificate f ZQ85+QIG2a9 DGsEEn/e6ak HX8FR9C2di Q7WG-22LL g7WJ-5Q1K0-24 g7WJ-5Q1K0-24 g7WJ-5Q1K0-24 GCATE RVATE-KEY RVATE-KEY ShqFBuUESV E1Vk9BRGC3 Uu-HFXAnh2K KMCHp-CL1 tmN/sMj7AVg A/TE-KEY	or OPADMIN ws5pz+zKZpNeiE RicFZQvQDe/9laf RvdExue40mhpyy godd8Pr/mK6mQ godd8Pr/mK6mQ godd8Pr/mK6mQ zwdzyktftyzaExh1 y3ShpU11 yqxP9 7/yr3GJw3Rvc75	VyfrbBf0c Wv5JGG aluQZT1y 4mdAtGq (/aeVAmC i5ll1bv8M KpzTDQA nNZ/gD/U K4EEACOI NovNEv7/ irPPT0Q4 (CSw==	File Home ← → ← ↑ ↓ Downloads ⇒ Pictures SSOD Desktop Lightshot TG to FMC ◆ OneDrive Sitems 1 item s	G Share View > New Folder # # # # # # # # # # # # # # # # # # #	> Origin	al > 16 me ^ Admin_Private-EC-key.pem Admin-interface_CSR_CA-signed_DER_CC Clean_Private-EC-key.pem Clean-interface_CSR_CA-signed_DER_CE Root-CA.pem	V Date modified 3/20/2021 12-44 AN 3/20/2021 12-44 AN 3/20/2021 12-44 AN 3/20/2021 12-44 AN	ح ۸ ۸ ۸	Search TG Type Privacy Enhanced Privacy Enhanced Privacy Enhanced Privacy Enhanced	Size	X 2 KB 1 KB 2 KB 3 KB 2 KB 2 KB
Syslog		Add Certificate	Cancel											

将证书上传到FMC

要将证书上传到FMC,请导航至AMP > Dynamic Analysis Connections > Add New Connection,然后填写所需信息。

名称:任何要标识的名称。

主机:生成clean-interface的CSR时定义的clean-interface FQDN

证书:ROOT_CA和clean interface_no-carriage的组合证书。

🐖 Cisco® ISE Configuration 🛛 🗙 🔮 Privacy error	X att Cisco Firepower Management Ce X +	D X
Cisco® ISE Configuration 5.2.240/ddd/#Dynar	micAnalysisConnections	e :
CISCO AMP / Dynamic Analysis Connections	Q. Overview Analysis Policies Devices Objects AMP Intelligence Deploy 🧬 🌣 🙆 a	idmin v
	Add New Connection	nection
Cloud Name	Actions	
Cisco Sandbox API, US Cloud	Name: ThreatGrid Host: Wkeenset Com Certificate Upload: C:\fakepath\PANDEM_clean-interf Browse Use Proxy When Available:	99
	Cancel Register	

注册新连接后,将显示弹出窗口,单击"是"**按**钮。

🐝 Cisco 🖲 ISE Configuration 🛛 🗙 📔 🍪 Privacy error	× dtb Cisco Firepower Management Ce × +	_ 0 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	Add New Connection
Cisco Sandbox API, US Cloud	Name: JS	/ %
	ThreatGrid Host: WMP2441 Certificate U C:\fakepat Use Proxy W	
	Cancel Register	

页面重定向到TG Clean界面和登录提示,如图所示。



接受EULA。

← → ♂ ☆	🛛 🔒 https://wmp	.co	m /eula.html	?next=%2Fa	ctivate_device9	63Fdevice_key%3D0500000		・ 🖂 🕁	$\overline{\mathbf{A}}$	III\ 🖽) (8) =
Cisco Threat Grid	Submit Sample	Dashboard	Samples	Reports	Indicators	Administration \checkmark		Q ?	С		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											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 Full Name:						III Name:	Administrator				
HAVE READ ALL OF THE TERMS AND CONDITIONS OF THIS AGREEMENT, UNDERSTAND THEM AND AGREE TO BE LEGALLY BOUND BY THEM											
Title:						Title:	Administrator				
								I Agree			

如图所示,成功集成可显示活动设备。

← → ♂ ✿	🛛 🔒 https://wmp	com/activate_devic	ce?device_key=0500000000000000000000000000000000000	000000000000000 ···· 🗵 🏠	⊻ III/	▣ : =
cisco Threat Grid	Submit Sample Dashboa	rd Samples Reports	Indicators Administration 🗸	٩	•	admin 🗸
	Active Device A device has been register Device Type Model ID Mgmt IF Current status	ed and activated with FMC 12 52 005056B95288 Active	your appliance.	Return		

单击Return(返回),返回TG集成成功的FMC,如图所示。

Firepower Management Center	Q	Overview	Analysis	Policies	Devices	Objects	AMP	Intellige	jence	
Cloud Name			Host						Purpose	
ThreatGrid			W	pj.co	n	File Submissions, Private Report Lookups				
Cisco Sandbox API, US Cloud			fmc.api.	fmc.api.threatgrid.com					Public Report Lookups	

相关信息

- Firepower管理中心配置指南,版本6.6
- <u>技术支持和文档 Cisco Systems</u>