Configurar o ISE 2.4 e a integração do FMC 6.2.3 pxGrid

Contents

Introduction **Prerequisites** Requirements **Componentes Utilizados** Configurar o ISE Etapa 1. Habilitar serviços pxGrid Etapa 2. Configurar o ISE para aprovar todas as contas baseadas em certificado do pxGrid Etapa 3. Exportar Certificado Admin MNT do ISE e Certificados CA pxGrid **Configurar o FMC** Etapa 4. Adicionar um novo território ao FMC Etapa 5. Gerar Certificado de CA do FMC Etapa 6. Extraia o certificado e a chave privada do certificado gerado com o uso do OpenSSL Passo 7. Instalar certificado no FMC Etapa 8. Importar o certificado FMC para o ISE Etapa 9. Configurar a conexão do pxGrid no FMC Verificar Verificação no ISE Verificação no CVP Troubleshoot

Introduction

Este documento descreve o processo de configuração para integração do ISE pxGrid versão 2.4 e do FMC versão 6.2.3.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- ISE 2.4
- CVP 6.2.3
- Ative Diretory/Lightweight Diretory Access Protocol (LDAP)

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- ISE 2.4 independente
- FMCv 6.2.3
- Ative Diretory 2012R2
- Identity Services Engine (ISE) pxGrid versão 2.4
- Firepower Management Center (FMC) versão 6.2.3

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. Se a rede estiver ativa, certifique-se de que você entenda o impacto potencial de qualquer comando.

Configurar o ISE

Etapa 1. Habilitar serviços pxGrid

- 1. Faça login na GUI do ISE Admin e navegue até Administração > Implantação.
- 2. Selecione o nó ISE a ser usado para pxGrid persona.

10	Home Home	Context Visibility + Operations + Po	icy +Administration + Work Centers			License Warning 🔺 🔍 😑 🔿 🔿
	System Identity Management Network Res	sources	Grid Services + Feed Service + Threat Centric NAC			
	Deployment Licensing + Certificates + Loggin	g + Maintenance Upgrade + Backup	& Restore + Admin Access + Settings			
	Deployment	Deployment Nodes				
	(+ * E *					Belected 0 Total 1 😵 🎡 🖕
	Deployment PAN Fallower	🖊 Edit 🔟 Register 👩 Syncup	Deregister			Show All *
		Hostname	 Personas 	Role(s)	Services	Node Status
		tim24adm	Administration, Monitoring, Policy Service, pxGrid	STANDALONE	IDENTITY MAPPING, SESSION, PROFILER	

3. Ative o serviço pxGrid e clique em **Salvar** como mostrado na imagem.

Deployment	Deployment Nodes List > tim24adm
(□ • E •	Edit Node
Arrow Deployment PAN Failover	General Settings Profiling Configuration
	Hostname
	FQDN
	IP Address
	Node Type Identity Services Engine (ISE)
	Role STANDALONE Make Primary
	Administration
	V V Monitoring
	Role PRIMARY
	Other Monitoring Node
	✓ Velicy Service
	Enable Session Services (1)
	Include Node in Node Group None (1)
	Enable Profiling Service (i)
	Enable Threat Centric NAC Service (i)
	Enable SXP Service (i)
	Enable Device Admin Service ()
	Enable Passive Identity Service (i)
	pxGrid 🥡
	Save Reset

4. Verifique se os serviços do pxGrid são executados a partir da CLI.

Observação: o processo requer até 5 minutos para que os serviços pxGrid sejam totalmente iniciados e determinem o estado de Alta Disponibilidade (HA) se mais de um nó pxGrid estiver em uso.

5. Use SSH para acessar a CLI do nó do pxGrid do ISE e verifique o status do aplicativo.

```
# show application status ise | in pxGrid
pxGrid Infrastructure Service running 24062
pxGrid Publisher Subscriber Service running 24366
pxGrid Connection Manager running 24323
pxGrid Controller running 24404
#
```

6. Acesse a GUI do administrador do ISE e verifique se os serviços estão on-line e funcionam. Navegue até Administração > pxGrid Services.

7. Na parte inferior da página, o ISE exibe Connected to pxGrid <pxGrid node FQDN>.

-dusts Identity Services Engine Hor	me	Operations Policy Admin	istration + Work Centers				License Warning 🔺 🤍 🔍 🔿 🔿
System Hentity Management Ne	twork Resources	Portal Management pxGrid Services	Feed Service Threat Centric N	AC .			Click here to do wireless setup and visibility setup Do not show this again. $^{ imes}$
All Clients Web Clients Capabilities	Live Log Settings (Certificates Permissions					
√Enable ØDisable ØApprove	oup 🎈 Decline 🔞 Delete 🔹	Refresh Total Pending Approval(0)					1-7 of 7 Show 25 * per page Page 1 +
Client Name	Client Description	Capabilities	Status	Client Group(s)	Auth Method	Log	
ise-mnt-tim24adm		Capabilities(2 Pub, 1 Sub)	Online (XMPP)	Internal	Certificate	View	
ise-fanout-tim24adm		Capabilities(0 Pub, 0 Sub)	Online (XMPP)	Internal	Certificate	View	
Ise-pubsub-tim24adm		Capabilities(0 Pub, 0 Sub)	Online (XMPP)	Internal	Certificate	View	
ise-bridge-tim24adm		Capabilities(0 Pub, 4 Sub)	Online (XMPP)	Internal	Certificate	View	
ise-admin-tim24adm		Capabilities(4 Pub, 2 Sub)	Online (XMPP)	Internal	Certificate	View	
■ iseagent-firepower-20762a2982d		Capabilities(0 Pub, 6 Sub)	Online (XMPP)		Certificate	View	
Firesightisetest-firepower-20762a		Capabilities(0 Pub, 0 Sub)	Offline (XMPP)		Certificate	View	
Connected to exCited Em24adm stresse and							

Etapa 2. Configurar o ISE para aprovar todas as contas baseadas em certificado do pxGrid

1. Navegue até Administration > pxGrid Services > Settings.

2. Marque a caixa: "Aprovar automaticamente novas contas baseadas em certificado" e clique em **Salvar**.

cisco Iden	tity Services Eng	ine Home	▸ Context Visibility	 Operations 	▶ Policy	▼ Admin	istration	Work Centers
System	Identity Manage	ement + Network	Resources Device	e Portal Management	pxGrid S	ervices	Feed Ser	vice + Threat Centric NAC
All Clients	Web Clients	Capabilities L	ive Log Settings	Certificates Perr	nissions			
PxGri	d Settings							
Auto	matically approve n w password based a	new certificate-based account creation	d accounts					
Use D	efault Save							
Test								
Connected to	pxGrid tim24adm.r	tpaaa.net						

Observação: o administrador deve aprovar manualmente a conexão do FMC ao ISE se essa opção não estiver habilitada.

Etapa 3. Exportar Certificado Admin MNT do ISE e Certificados CA pxGrid

1. Navegue até Administração > Certificados > Certificados do Sistema.

2. Expanda o nó Monitoramento Principal (MNT) se não estiver ativado no nó Administração Principal.

3. Selecione o certificado com o campo Used-By "Admin".

Observação: este guia usa o certificado autoassinado padrão do ISE para uso do administrador. Se você usar um Certificado Admin assinado por uma Autoridade de Certificação (CA), exporte a CA raiz que assinou o certificado Admin no nó ISE MNT.

- 4. Clique em Exportar.
- 5. Escolha a opção para Exportar Certificado e Chave Privada.

- 6. Defina uma chave de criptografia.
- 7. Exportar e Salvar o arquivo como mostrado na imagem.

dentity Services Engine	Home + Context Visibility + Operations	Policy Administration	Work Centers				License Warning 🔺 🔍 😣 🔿 🔿
System Identity Management	Network Resources	pxGrid Services	Threat Centric NAC				
Deployment Licensing Certificate	s + Logging + Maintenance Upgrade + Bac	kup & Restore + Admin Access	+ Settings				
0							
Certificate Management	System Certificates 🛕 For disaster recovery i	t is recommended to expert certificat	e and private key pairs of all syster	n certificates.			
System Certificates	📝 Edit 🕂 Generate Self Signed Certificate	- Import 🕃 Export 🗶 Dele	te 🔎 Vew				
Trusted Certificates	Friendly Name	Used By Por	tal group tag	Issued To	Issued By	Valid From	Expiration Date
OCSP Client Profile	▼ 5m24adm						
Certificate Signing Requests Certificate Periodic Check Setti	OU+Certificate Services System Certificat e.CN+tim24adm.rtpaaa.net#Certificate Se rvices Endpoint Sub CA - tim24adm#0000	pxGrid				Thu, 29 Mar 2018	Thu, 30 Mar 2028
Certificate Authority	CN+SAML_tim24adm.rtpaaa.net	SAML				Fri, 30 Mar 2018	Sat, 30 Mar 2019 🕑
	Default self-signed server certificate	EAP Authentication, Admin, Defi	ault Portal Certificate Group 👔			Fri, 30 Mar 2018	Sat, 30 Mar 2019 🗾
	uncate Delaut	aen-aigne		.er en	-		^
			 Export 	Certificate	Only		
			Export	Certificate	and Private Key		
	*Private Ke	y Password					
	*Confirm	m Password	•••••				
Warning:	Exporting a private	key is not a	secure oper	ation. It co	uld lead to poss	ible exposure of	the private key.
						E	xport Cancel

- 9. Retorne à tela Certificados do Sistema ISE.
- 10. Determine o campo Emitido por no certificado com o uso de "pxGrid" na coluna Usado por.

Observação: em versões mais antigas do ISE, esse era um certificado autoassinado, mas a partir da versão 2.2 esse certificado é emitido pela Cadeia de CA interna do ISE por padrão.

11. Selecione o Certificado e clique em **Exibir** conforme mostrado na imagem.

dentity Services Engine	Home + Context Visibility + Operation	ns + Policy + Administra	tion Work Centers				License Warning 🔺 🧠 😐 🔘 🗢
* System + Identity Management	Network Resources Device Portal Manag	pement pxGrid Services + F	eed Service + Threat Centric NAC				
Deployment Licensing Certificate	es + Logging + Maintenance Upgrade	Backup & Restore Admi	n Access				
0							
* Certificate Management	System Certificates 🛕 For disaster n	ecovery it is recommended to exp	ort certificate and private is pairs of all sy	stem certificates.			
System Certificates	🕖 Edit 🛛 🕂 Generate Self Signed Certifi	kate 🕂 Import 🕼 Export	X Delete				
Trusted Certificates	Friendly Name	Used By	Portal group tag	Issued To	Issued By	Valid From	Expiration Date
OCSP Client Profile	▼ tim24adm						
Certificate Signing Requests	OU=Certificate Services System (e,CN=tim24adm.rtpaaa.net#Certil	ficate Se pxOrid				Tru, 29 Mar 2018	Thu, 30 Mar 2028
Certificate Periodic Check Set5	 Notes Endpoint Sub CA - tim24ad 1 	5780000					
Certificate Authority	 Default self-signed sami server or CN=SAML_tim24adm.rtpaaa.net 	ertificate - SAML				Fri, 30 Mar 2018	Sat, 30 Mar 2019 🛃
	 Default self-signed server certification 	the EAP AuthenScation, A Portal, RADIUS DTLS	dmin, Default Portal Certificate Group (j)			Fri, 30 Mar 2018	Sat, 30 Mar 2019 🗾

12. Determine o certificado de nível superior (Raiz). Nesse caso, é **"Certificate Services Root CA** - tim24adm".

13. Feche a janela de visualização do certificado como mostrado na imagem.

Certificate Services Root C	A - tim24adm de CA - tim24adm
Certificate Service	s Endpoint Sub CA - tim24adm
tim24adm.rtpa	aa.net
tim24adm.rtpaaa Issued By : Certi Expires : Thu, 30	.net icate Services Endpoint Sub CA - tim24adm Mar 2028 14:17:12 EDT
Certificate status is good	
Details	
Issued To	
Common Name (CN)	
Organization Unit (OU)	Certificate Services System Certificate
Organization (O)	
City (L)	
State (ST)	
State (ST)	
Country (C)	
Serial Number	58:2A:91:45:E8:23:42:74:98:53:06:94:33:9E:AD:83

Close

14. Expanda o menu ISE Certificate Authority.

15. Selecione Certificados da Autoridade de Certificação.

16. Selecione o Certificado Raiz identificado e clique em **Exportar.** Em seguida, salve o certificado CA raiz do pxGrid como mostrado na imagem.

dentity Services Engine	Home	Context Visibility Operation	ns + Policy - Ar	dministration + Work Centers					License Warning 🔺 👘	
System + Identity Management +	Network	Resources + Device Portal Manag	ement pxGrid Service	s + Feed Service + Threat Cent	ric NAC					
Deployment Licensing Certificated	s + Lo	gging Maintenance Upgrade	 Backup & Restore 	Admin Access Settings						
0										
Certificate Management	CAC	ertificates								
- Certificate Authority	1	idit 🕂 Import 🕃 Export 🗶	Delete 🔎 View 📢	Refresh						
Outoites		Friendly Name	Status	Trusted For	Serial Number	Issued To	Issued By	Valid From	Expiration Date	Expiration Status
Otertea	T tim	24adm								
Issued Certificates	0	Certificate Services Endpoint Sub CA - tim24adm#00003	Enabled	Infrastructure,Endpoints	32 D2 72 55 A9 7D 40 13 8F 2A EF CF 0D 1C 41 AB	Certificate Services Endpoint Sub	Certificate Services Node CA -	Thu, 29 Mar 2018	Thu, 30 Mar 2028	2
Certificate Authority Certificates		Certificate Services Root CA - tim24adm#00001	Enabled	Infrastructure,Endpoints	36 67 74 15 A6 A8 4F EB B7 46 1 E7 37 1A AB 88	Certificate Services Root CA - tim24adm	Certificate Services Root CA - tim24adm	Thu, 29 Mar 2018	Thu, 30 Mar 2028	
Certificate Templates		Certificate Services Node CA - tim24adm#00002	Enabled	Infrastructure,Endpoints	30 1A 22 E7 AA E5 45 35 8C 65 7B EE 53 09 34 3E	tim24adm	tim24adm	Thu, 29 Mar 2018	Thu, 30 Mar 2028	
External CA Settings		Certificate Services OCSP Responder - tim24adm#00004	Enabled	Infrastructure,Endpoints	74 C2 35 B8 32 6A 40 0F AC C8 D0 B9 51 DC 07 7D	Certificate Services OCSP Responder - tim24adm	Certificate Services Node CA - tim24adm	Thu, 29 Mar 2018	Thu, 30 Mar 2023	

Configurar o FMC

Etapa 4. Adicionar um novo território ao FMC

- 1. Acesse a GUI do FMC e navegue para **System > Integration > Realms**.
- 2. Clique em New Realm como mostrado na imagem.

Overview	Analysis	Policies	Devices	Objects	AMP	Intelligence			Ū						Deploy	0 s	ystem Help v	• admin •
										Configuration	Users	Domains	Integration	Updates	Licenses v	V alth 🔻	Monitoring	 Tools •
Cisco CST	Pealme	Identit	v Sources	eStreame	e He	ast Input Client	Smart Software Satellite					/						
0.000 0.01	/	- Automation	,	Contentine		or input chem	Single Solenite									V Com	nare realms	New realm
																30.00		

3. Preencha o formulário e clique no botão Testar associação do Ative Diretory (AD).

Observação: o nome de usuário de associação ao AD deve estar no formato UPN ou o teste falhará.

4. Se Testar Ingresso do AD for bem-sucedido, clique em OK.

Add New Realm			? ×	
Name *	ISEpxGrid			
Description	Realm for use with pxGrid			
Туре *	AD			
AD Primary Domain *		ex: domain.com		
AD Join Username		ex: user@domain		
AD Join Password	•••••	Test AD Join		
Directory Username *	admin	ex: user@domain		
Directory Password *	•••••			
Base DN *	CN=Users,DN=rtpaaa,DN=net	ex: ou=user,dc=cisco,dc=com		
Group DN *	DN=rtpaaa,DN=net	ex: ou=group,dc=cisco,dc=com		
Group Attribute	Member 💙]		
Dequired Field				
* Required Field				
		OK Cancel		

5. Clique na guia **Diretório** e, em seguida, clique em **Adicionar diretório** conforme mostrado na imagem.



6. Configurar IP/Nome do Host e Testar Conexão.

Observação: Se o Teste falhar, verifique as credenciais na guia Configuração do Realm.

7. Clique em OK.

Edit directory		?	×
Hostname / IP Address			
Port	389		
Encryption	◯ STARTTLS ◯ LDAPS . One		
SSL Certificate	▼ ③		
	OK Test Cance	el	
Status			

(Test connection succeeded	
	ОК	

8. Clique na guia Download do Usuário.

Overview Analysis Policies Devices Objects AMP Intelligence						Deploy	ं 🔍 Syr	stem Help v	admin v
	Configuration	Users	Domains	Integration	Updates	Licenses •	Health +	Monitoring •	Tools •
LAB E								Save (Cancel
Directory Realm Configuration User Download									

- 9. Se ainda não estiver selecionado, habilite o download de usuários e grupos
- 10. Clique em Baixar Agora

LAB Enter Descri	iption		
Directory	Realm Configuration	User Download	
Downloa Begin autor	ad users and groups matic download at 8 🔹	PM Y America/New York	Repeat Every 24 V Hours

11. Quando a lista for preenchida, adicione os grupos desejados e selecione Adicionar à Inclusão.

12. Salve a Configuração do Realm.

Overview Analysis Policies Devices Objects	AMP Intelligence							Deploy ©	System Help v admin
			Configuration	Users	Domains	Integration	Updates	Licenses • Health	 Monitoring Tool
LAB	=							You have unsaved cha	nges_ 🔚 Save 🛛 🙆 Cano
Enter Description									
								_	
Directory Realm Configuration User Download									
Download users and groups									
Basis automatic doublead at a M say M America/New Yor	k Repeat Eveny Da W Mours								
when Described New	a militar cruit 24 - monta								
Available Groups C		Groups to Include (35)			Groups to Ex	clude (0)			
Search by name		📌 NetOps		81	None				
A NetOne		SQLServer2005SQLBrowserUserSRTPAAA-DC2		8					
COL Concer20055501 Resulted InterEDTRALL.002		A WSUS Administrators		8					
WEINS Administrators		A Enterprise Read-only Domain Controllers		8					
Enterprise Read-only Domain Controllers		A DnsUpdateProxy		8					
ConsidedateProvy		🝰 jhoehn-group		8					
Onabytante (M)		A Denied RODC Password Replication Group		8					
Design BODC Research Replication Cours		📌 Domain Admins		8					
Comain Admine		📌 Child		8					
A CM		A DnsAdmins		8					
Participa Contra		A Lester\Made\Me\Do\Jt		8					
A Lastarilla da Malfrel P		A Group Policy Creator Owners		a					
A Denue Bolley Craster Dunary		🝰 INE		a					
a no		n 📥 Domain Users		8					
Pomain Hearr		A ChadTest		ā.					
A Contrat		A Read-only Domain Controllers		8					
Read-only Pompin Controllers	Includ	ARAS and IAS Servers		äll					
A RAE and IAE Senser		A Cert Publishers		a					
Cart Publishers	Add 5 Exclud	A Schema Admins		a					
Champ Links		A WSUS Reporters		8					
A WEIS Reporters		📌 Parent		8					
A Parent		💤 ISE Admins		8					
A ISE Admine		A WinRMRemoteWMIUsers		8					
WinBMRemoteWMUsers		Allowed RODC Password Replication Group		8					
Allowed RODC Password Replication Group		A TimSponsors		8					
TimSponsors		AllowedVPN		8					
Allowed VPN		🝰 Enterprise Admins		8					
A Enterorise Admins		🝰 test-users		8					
A test-users		🝰 sponsors		8					
A sponsors		A HelpLibraryUpdaters		8					
A HelpLibraryUpdaters		💤 Protected Users		8					
A Protected Users		💤 Domain Guests		8					
Domain Guests		🝰 Domain Computers		8					
Domain Computers		Pomain Controllers		8 U					
Domain Controllers		A.M							
A Chanadala Danasia Cantentine		Enter User Inclusion		Add	Enter User E	clusion			Add

13. Ative o Estado do Realm.

Overview	Analysis	Policies	Devices	Objects	AMP	Intelligence									Deploy	ି 🗢 🌖	rstem Help	v admin v
										Configuration	Users	Domains	Integration	Updates	Licenses *	Health •	Monitoring	g • Tools •
01	Bustess	T.d				and to and fillent	Count College Columb											
CISCO USI	Realms	Identit	y sources	estream	er n	lost Input Client	Smart Software Satellite											0
																. om	pare realms	New realm
Name								Description	Domain	Туре		Base DN	Group	DN	Group Atte	ibute	State	
LAB									Global	AD		DC=rtpaaa,DC=	net CN+U	sers,DC=rtpaaa,	DC+ member			± 🥒 🐚 🖯

Etapa 5. Gerar Certificado de CA do FMC

1. Navegue até **Objetos > Gerenciamento de Objetos > CAs Internas** conforme mostrado na imagem.

Overview Analysis Polic	les Devices Objects AMP Intelligence		Deple	y 🔺 System Help v	admin +
Object Management Intr	usion Rules				
			O Add N	etwork • . Fiter	
2 Network	Name	Value	Туре	Override	
Port S Interface	any		Group	×	9.8
Cunnel Zone	any-ipv4		Network	×	
🛞 VLAN Tag	any-ipv6		Host	×	
URL Geolocation	IPv4-Benchmark-Tests		Network	×	
Time Range	Pv4-Link-Local		Network	×	
\$ Variable Set	IPv4-Multicast		Network	×	
Security Intelligence Network Lists and Feeds	IPv4-Private-10.0.0.0-8		Network	×	
DNS Lists and Feeds	IPv4-Private-172.16.0.0-12		Network	×	
URL Lists and Feeds	IPv4-Private-192.168.0.0-16		Network	×	
File List	IPv4-Pnate-Al-AFC1918		Group	×	
Distinguished Name Individual Objects	IPv6-IPv4-Mapped		Network	×	
Cibject Groups	IPv6-Link-Local		Network	×	
A PKI	IPv6-Private-Unique-Local-Addresses		Network	×	
Trusted CAs	IPv6-to-IPv4-Relay-Anycast		Network	×	
External Certs Internal Certs Cert Enrolment Internal CA Groups Internal CA Groups Internal Cert Groups Internal Cert Groups External Cert Groups					

- 2. Clique em Gerar CA.
- 3. Preencha o formulário e clique em Gerar CA autoassinada.

Overview Analysis	Policies Devices	Objects AMP Intelligence				Deploy 🗛 System Help + admin +
Object Management	Intrusion Rules					
					Generate	CA Dimport CA G Filter
Network	Name				Value	
					1	
		Generate Internal Certificate	Authority	? ×		
		Name:	LabEP623	B		
				_		
		Country Name (two-letter code):	US			
			05			
		State or Province:	NC			
		Locality or City:	070			
		Eduarity of City.	RIP			
		Organization:	Cisco			
				-		
		Organizational Unit (Department):	TAC			
		Common Name:				
		Concepto CCD	Concepto colf signed CA	Canad		
		Generate CSK	Generate self-signed CA	Cancel		

4. Quando a geração terminar, clique no lápis à direita do Certificado CA gerado, conforme mostrado na imagem.

Overview A	inalysis	Policies Devic	es Objects	AMP Intelligence		Deploy	🔺 System Help	v admin v
Object Manag	ement	Intrusion Rules						
						Generate CA Generate CA	rt CA	
Network		Name			Value	lue		
Port Interface		LabFP623			CN+L	+LabFP623.rtpaaa.net, ORG+Cisco, OU+TAC, C+US		/ 8

5. Clique em Download.

Name:	LabFP623		
Subje	ect:		
Co	ommon Name:		
Or	rganization: Cisco		
Or	rganization Unit: TAC		
Issue	r:		
Co	ommon Name:		
Or	rganization: Cisco		
Or	rganization Unit: TAC		
Not V	alid Before:		
Ma	ay 15 18:13:52 2018 GMT		
Not V	'alid After:		
Ma	ay 12 18:13:52 2028 GMT		
Serial	Number:		
a	2:1e:98:52:be:2f:b8:98		
Certif	icate Fingerprint:		
C7	7:D7:99:F3:EE:41:5C:7B:36:91:40:04:F7:1D:22:4C:60:C2:3C:9C		
Public	c Key Fingerprint:		
b5	1aabcb2cb25e922fdf6c0088771fca794897a1		
Dow	nload	OK	Cancel

6. Configure e confirme a senha de criptografia e clique em OK.

7. Salve o arquivo Public-Key Cryptography Standards (PKCS) p12 no sistema de arquivos local.

Etapa 6. Extraia o certificado e a chave privada do certificado gerado com o uso do OpenSSL

Isso é feito na raiz do FMC ou em qualquer cliente capaz de comandos OpenSSL. Este exemplo usa um shell padrão do Linux.

1. Use openssI para extrair o certificado (CER) e a chave privada (PVK) do arquivo p12.

2. Extraia o arquivo CER e configure a chave de exportação do certificado a partir da geração do certificado no FMC.

~\$ openssl pkcs12 -nokeys -clcerts -in <filename.p12> -out <filename.cer> Password: Last login: Tue May 15 18:46:41 UTC 2018 Enter Import Password: MAC verified OK

3. Extraia o arquivo PVK, configure a chave de exportação do certificado, defina uma nova senha

~\$ openssl pkcs12 -nocerts -in <filename.p12> -out <filename.pvk>
Password: Last login: Tue May 15 18:46:41 UTC 2018 Enter Import Password: MAC verified OK
4. Esta frase PEM é necessária na próxima etapa.

Passo 7. Instalar certificado no FMC

- 1. Navegue até Objetos > Gerenciamento de Objetos > PKI > Certificados Internos.
- 2. Clique em Add Internal Cert conforme mostrado na imagem.

overview Analysis	Policies Devices Objects AMP Intelligence	Deploy System Help + admin
Object Management	Intrusion Rules	
		Add Internal Cert
Retwork	Name	Value
JP Port		
4 Interface	TimPP623	CN=TimPP623.rtpaaa.net, DRG=Cisco, OU=TAC, C=US
annel Zone		
Application Filters		
🛞 VLAN Tag		
🙆 URL		
🕎 Geolocation		
🚰 Time Range		
\$ Variable Set		
 Security Intelligence 		
Network Lists and I	eeds	
ONS Lists and Feed		
URL Lists and Feed		
Sinkhole		
C File List		
Opher Suite List		
Distinguished Name		
Individual Objects		
Cobject Groups		
🔑 PKI		
Internal CAs		
Trusted CAs		
External Certs		
Internal Certs		
Cert Enrollment		
Internal CA Groups		
Trusted CA Groups		
Internal Cert Group		
External Cert Grou	5	

3. Configure um nome para o Certificado Interno.

4. Navegue até o local do arquivo CER e selecione-o. Quando os Dados do certificado forem preenchidos, selecione o segundo.

5. Navegue até Opção e selecione o arquivo PVK.

6. Exclua todos os "atributos de saco" à esquerda e todos os valores à direita na seção PVK. O PVK começa com -----BEGIN ENCRYPTED PRIVATE KEY— e termina com -----END ENCRYPTED PRIVATE KEY—.

Observação: você não poderá clicar em **OK** se o texto PVK tiver caracteres fora dos hífens à esquerda e à direita.

- 7. Marque a caixa Encrypted e configure a senha criada quando o PVK foi exportado na Etapa 6.
- 8. Clique em **OK**.

Add Known Internal Certificate

Name:	TZfpcert			
Certificat	e Data or, choose a file:	Browse		
BEGI MIIDFTC0 BAYTAIV bzEMMA0 DTE4MD BgNVBA0 DANUQU DQEBAQ D7Gm/c6	IN CERTIFICATE CAmWgAwIBAgIJAKIemFK+ TMQswCQYDVQQIDAJOQZE oGA1UECwwDVEFDMRwwG UxNTE4MTM1MloXDTI4MD0 MAk5DMQwwCgYDVQQHD MxHDAaBgNVBAMME0xhYH UAA4IBDwAwggEKAoIBAQI S9CXw/VfIPWnSBzhEkiRTysp hoose a file:	-L7iYMA0GCSqGSIb3DQEBCwUAMGQxCz/ MMAoGA1UEBwwDUIRQMQ4wDAYDVQQI gYDVQQDDBNMYWJGUDYyMy5ydHBhYW JxMjE4MTM1MlowZDELMAkGA1UEBhMCV ANSVFAxDjAMBgNVBAoMBUNpc2NvMQw cZQNjIzLnJ0cGFhYS5uZXQwggEiMA0GCSc DMjtS5IUIFiZkZK/TSGtkOCmuivTK5kk1Wz/ omTMdyf/4TJvUmUH60h108/8dZeqJOzbjc	AJBgNV KDAVDaXNj /EubmV0MB4X /VMxCzAJ wCgYDVQQL qGSIb3 Ay6 on	
Bag Attri localKi Key Attri MIIFDjB/ MBQGCC xL0qjESt 74POu/O fXvNZ94	butes eyID: C7 D7 99 F3 EE 41 50 butes: <no attributes=""> IN ENCRYPTED PRIVATE KE ABgkqhkiG9w0BBQ0wMzAbl QGSIb3DQMHBAhgGVm1+: mwuyExVp+TWC3AyIJN1D 2Vy99iFoVgW2q9DyXyL/h6 NG4HrEcFmnnij0EwJ0QT8Jr</no>	C 7B 36 91 40 04 F7 1D 22 4C 60 C2 3C 9 BgkqhkiG9w0BBQwwDgQI5uV3MsiHZsICA KHLIASCBMjjJxkffXUNUcdB22smybvWotwb E7/rRssjRAqsnSOxIvDGmg0dVsvnbbqZwji 4TH9CZtwLKIOGOeEunNKpamDnpfyN8QQ n5gAUj+AIPMe32zPqwoccRNYrRXMVM9+	AggA bcRrt FP C4DC Jwp	
C Encry	oted, and the password is:		•••	
			ОК	Cancel
cfCJU2QC acCICUAs O/g= 	5I4jT0SorN4u2Lk+S+Qd1s7 ecVrYY081GKTVVJ3bWgWfl ENCRYPTED PRIVATE KEY DELETE	Ii2wIQMWKPI2R9UGv1tyM6HTPCGoCo6VI PtR3OH12YCA2whcCKcG50MByB4tjhHN03	DI 6q	
Encryp	ted, and the password is:	•••••		
			ок	Cancel

Etapa 8. Importar o certificado FMC para o ISE

1. Acesse a GUI do ISE e navegue para Administração > Sistema > Certificados > Certificados de Confiabilidade.

2. Clique em Importar.

dentity Services Engine	Home	Administrat	tion Vork Centers							License Warning 🔺	۹.	0 0	0
System + Identity Management +	Network Resources	id Services + Fe	ed Service + Threat Cen	tric NAC									
Deployment Licensing - Certificates	Logging + Maintenance Upgrade + Backup & F	Restore + Admir	Access + Settings										
0													
Certificate Management	Trusted Certificat												
System Certificates	/Edit 🕂 Import 🚱 Export 🗙 Delete 🔎 View									Show All		•	8
Trusted Certificates	Friendly Name	Status	Trusted For	Serial Number	Issued To	Issued By	Valid From	Expiration Date	Expiration Status				
OCSP Client Profile	Baltimore CyberTrust Root	Enabled	Cisco Services	02 00 00 89	Baltimore CyberTrust Ro	Baltimore CyberTrust Ro	Fri, 12 May 2000	Mon, 12 May 2025	•				
Certificate Signing Requests	Cisco CA Manufacturing	Disabled	Endpoints Infrastructure	6A 69 67 B3 00 00	Cisco Manufacturing CA	Cisco Root CA 2048	Fri, 10 Jun 2005	Mon, 14 May 2029	1				
Certificate Periodic Check Setti	Cisco Manufacturing CA SHA2	Enabled	Endpoints Infrastructure	02	Cisco Manufacturing CA	Cisco Root CA M2	Mon, 12 Nov 2012	Thu, 12 Nov 2037	2				
Certificate Authority	Cisco Root CA 2048	Disabled	Infrastructure Endpoints	SF F8 78 28 28 54	Cisco Root CA 2048	Cisco Root CA 2048	Fri, 14 May 2004	Mon, 14 May 2029					
	Cisco Root CA M2	Enabled	Endpoints Infrastructure	01	Cisco Root CA M2	Cisco Root CA M2	Mon, 12 Nov 2012	Thu, 12 Nov 2037	2				
	Default self-signed server certificate	Enabled	Endpoints Infrastructure	5A BE 7E D8 00 00	tim24adm.rtpaaa.net	tim24adm.rtpaaa.net	Frl, 30 Mar 2018	Sat, 30 Mar 2019					
	DigiCert root CA	Enabled	Endpoints Infrastructure	02 AC 5C 26 6A 08	DigiCert High Assurance	DigiCert High Assurance	Thu, 9 Nov 2006	Sun, 9 Nov 2031	2				
	DigiCert SHA2 High Assurance Server CA	Enabled	Endpoints Infrastructure	04 E1 E7 A4 DC SC	DigiCert SHA2 High Ass	DigiCert High Assurance.	Tue, 22 Oct 2013	Sun, 22 Oct 2028					
	DST Root CA X3 Certificate Authority	Enabled	Cisco Services	44 AF 80 80 D6 A3	DST Root CA X3	DST Root CA X3	Sat, 30 Sep 2000	Thu, 30 Sep 2021	2				
	HydrantID SSL ICA G2	Enabled	Cisco Services	75 17 16 77 83 D0	HydrantID SSL ICA G2	QuoVadis Root CA 2	Tue, 17 Dec 2013	Sun, 17 Dec 2023	1				
	QuoVadis Root CA 2	Enabled	Cisco Services	05 09	QuoVadis Root CA 2	QuoVadis Root CA 2	Fri, 24 Nov 2006	Mon, 24 Nov 2031	1				
	Thawte Primary Root CA	Enabled	Cisco Services	34 4E D5 57 20 D5	thawte Primary Root CA	thawte Primary Root CA	Thu, 16 Nov 2006	Wed, 16 Jul 2036	2				
	TimFP623	Enabled	Endpoints	BE F9 42 3D 25 AS	TimFP623.rtpaaa.net	TimFP623.rtpaaa.net	Tue, 15 May 2018	Fri, 12 May 2028	1				
	VertSign Class 3 Public Primary Certification Authority	Enabled	Cisco Services	18 DA D1 9E 26 7D	VeriSign Class 3 Public	VeriSign Class 3 Public	Tue, 7 Nov 2006	Wed, 16 Jul 2036	2				
	VeriSign Class 3 Secure Server CA - G3	Enabled	Cisco Services	6E CC 7A A5 A7 03	VeriSign Class 3 Secure	VeriSign Class 3 Public	Sun, 7 Feb 2010	Fri, 7 Feb 2020	1				

3. Clique em **Escolher arquivo** e selecione o arquivo CER do FMC do seu sistema local.

Opcional: Configure um Nome Amigável.

4. Verifique a Confiança para a autenticação no ISE.

Opcional: Configure uma Descrição.

5. Clique em Enviar conforme mostrado na imagem.

Import a new Certificate into the C	ertificate Store	
* Certificate File	Choose File TZfpcert.cer	
Friendly Name		i
	Trusted For: (j)	
	✓ Trust for authentication within ISE	
	Trust for client authentication and Syslog	
	Trust for authentication of Cisco Services	
	Validate Certificate Extensions	
Description		
<u>}</u>	Submit Cancel	

Etapa 9. Configurar a conexão do pxGrid no FMC

1. Navegue até System > Integration > Identity Sources conforme mostrado na imagem.



- 3. Configure o endereço IP ou o nome de host do nó pxGrid do ISE.
- 4. Selecione o + à direita de CA do pxGrid Server.

5. Nomeie o arquivo da CA do servidor e navegue até a CA de assinatura raiz do pxGrid coletada na Etapa 3. e clique em **Salvar**.

6. Selecione + à direita de MNT Server CA.

7. Nomeie o arquivo Server CA e navegue até o certificado Admin coletado na Etapa 3. e clique em **Salvar**.

8. Selecione o arquivo FMC CER na lista suspensa.

Identity Sources								
Service Type	None Identity Services Engine	U	User Agent					
Primary Host Name/IP Address * Secondary Host Name/IP Address	<ise address="" ip="" node="" pxgrid=""></ise>	83						
pxGrid Server CA *	ISE24InternalRoot	~	0					
MNT Server CA *	ISE24SelfSigned	~	٥					
FMC Server Certificate *	TimFP623	~	0					
ISE Network Filter			ex. 10.89.31.0/24, 192.168.8.0/24,					
* Required Field	Test							

9. Clique em Testar.

10. Se o teste for bem-sucedido, clique em **OK**, depois em **Salvar** no canto superior direito da tela.

Status



Observação: quando você executa dois nós do ISE pxGrid, é normal que um host mostre Êxito e outro mostre Falha, já que o pxGrid é executado ativamente apenas em um nó do ISE por vez. Depende da configuração se o host principal deve exibir Falha e o host secundário deve exibir Êxito. Tudo isso depende de qual nó no ISE é o nó pxGrid ativo.

Verificar

Verificação no ISE

1. Abra a GUI do ISE e navegue para Administração > serviços do pxGrid.

Se obtiver êxito, duas conexões firepower serão listadas na lista de clientes. Um para o FMC real (iseagent-hostname-33bytes) e um para o dispositivo de teste (firesightisetest-hostname-33bytes).

ystem i bietty Management i Nation Resources i Device Partal Management priori Services i Press Partal Management i Nation Resources i Device Partal Management i Device Parta	dealers Identity Services Engine	Home + Context Visibility	Operations Policy Admin	istration + Work Centers				License Warning 📥 🔍 😝 😋	
A Clerins Vaco Clerins Capabilities Live Log Settings Certings Permissions Clerins Clerins Clerins Clerins Clerins Clerins Log Clerins <	System Identity Management	nt Network Resources Device P	fortal Management pxGrid Services	Feed Service Threat Centric	NAC				
	All Clients Web Clients Cr	apabilities Live Log Settings C	Certificates Permissions						
Operation Operation Operation Status Oten Compa() Ath Method Log Carry Log </td <td>✓Enable Ø Disable Ø Approve</td> <td>e 😝 Group 👎 Decline 🚷 Delete 🕶</td> <td>Refresh Total Pending Approval(0)</td> <td>•</td> <td></td> <td></td> <td></td> <td>1 - 7 of 7 Show 25 + per page Page</td> <td>1</td>	✓Enable Ø Disable Ø Approve	e 😝 Group 👎 Decline 🚷 Delete 🕶	Refresh Total Pending Approval(0)	•				1 - 7 of 7 Show 25 + per page Page	1
Capabilite(2 Ap, 1 Sub) Online (XMPP) Internal Certificate Vew Capabilite(3 Ap, 0 Sub) Online (XMPP) Internal Certificate Vew Capabilite(3 Ap, 0 Sub) Online (XMPP) Internal Certificate Vew Capabilite(3 Ap, 0 Sub) Online (XMPP) Internal Certificate Vew Capabilite(3 Ap, 0 Sub) Online (XMPP) Internal Certificate Vew Capabilite(3 Ap, 0 Sub) Online (XMPP) Internal Certificate Vew Capabilite(3 Ap, 0 Sub) Online (XMPP) Certificate Vew Capabilite(3 Ap, 0 Sub) Online (XMPP) Certificate Vew	Client Name	Client Description	Capabilities	Status	Client Group(s)	Auth Method	Log		
Capabilities(10 PAB, 0 Sub) Online (0499) Internal Certificate View Capabilities(10 PAB, 0 Sub) Online (0499) Internal Certificate View Capabilities(10 PAB, 0 Sub) Online (0499) Internal Certificate View Capabilities(10 PAB, 0 Sub) Online (0499) Internal Certificate View Capabilities(10 PAB, 0 Sub) Online (0499) Internal Certificate View Capabilities(10 PAB, 0 Sub) Online (0499) Certificate View Capabilities(10 PAB, 0 Sub) Online (0499) Certificate View	0		Capabilities(2 Pub, 1 Sub)	Online (XMPP)	Internal	Certificate	View		
Capabilizer(0 Au, 0 Sub) Online (0949) Internal Certificate Vew Capabilizer(0 Au, 0 Sub) Online (0949) Internal Certificate Vew Capabilizer(0 Au, 0 Sub) Online (0949) Internal Certificate Vew Capabilizer(0 Au, 0 Sub) Online (0949) Internal Certificate Vew Capabilizer(0 Au, 0 Sub) Online (0949) Certificate Vew Capabilizer(0 Au, 0 Sub) Online (0949) Certificate Vew			Capabilities(0 Pub, 0 Sub)	Online (XMPP)	Internal	Certificate	View		
Copublities(0 Nu), 4 Sub) Online (0499) Internal Certificate Vew Copublities(4 Nu), 2 Sub) Online (0499) Internal Certificate Vew Copublities(0 Nu), 4 Sub) Online (0499) Internal Certificate Vew Copublities(0 Nu), 4 Sub) Online (0499) Certificate Vew Copublities(0 Nu), 6 Sub) Offline (0499) Certificate Vew			Capabilities(0 Pub, 0 Sub)	Online (XMPP)	Internal	Certificate	View		
Constitute(3 b.0.2 Sub) Celler (XOPP) Internal Cetificate Vew Copublicity(3 b.0.6 Sub) Celler (XOPP) Certificate Vew Copublicity(3 b.0.6 Sub) Celler (XOPP) Certificate Vew			Capabilities(0 Pub, 4 Sub)	Online (XMPP)	Internal	Certificate	View		
Capabilities(0 Pub, 6 Sub) Chrime (XMPP) Certificate Vew Capabilities(0 Pub, 6 Sub) Offline (XMPP) Certificate Vew	П		Casabilities(4 Pub. 2 Sub)	Online (XMPP)	Internal	Certificate	Vew		
Capabilities(2 Pub, 6 Sub) Office (2499) Cetificate View			Capabilities(0 Pub, 6 Sub)	Online (XMPP)		Certificate	View		
			Capabilities(0 Pub, 0 Sub)	Offline (XMPP)		Certificate	View		

A conexão iseagent-firepower exibe seis (6) subs e é exibida on-line.

A conexão firesightisetest-firepower exibe zero (0) subs e aparece offline.

A visualização expandida do cliente iseagent-firepower exibe as seis assinaturas.

 iseagent-firepower-20762a2982d 	Capal	bilities(0 Pub, 6 Sub) On	line (XMPP)	(Certificate	View		
	Capab	pility Detail			1 - 6 of 6	Show 25 👻 per page	Page 1	\$
	C	Capability Name	Capability Version	Messaging Role	Message Filter			
	0 4	AdaptiveNetworkControl	1.0	Sub				
	0 0	Core	1.0	Sub				
	0 6	EndpointProfileMetaData	1.0	Sub				
	OE	EndpointProtectionService	1.0	Sub				
	0.8	SessionDirectory	1.0	Sub				
	0 1	FrustSecMetaData	1.0	Sub				
	0 s	SessionDirectory frustSecMetaData	1.0	Sub Sub				

Observação: devido ao bug da Cisco <u>IDCSCvo75376</u> há uma limitação de nome de host e o download em massa falha. O botão de teste no FMC exibe uma falha de conectividade. Isso afeta 2.3p6, 2.4p6 e 2.6. A recomendação atual é executar o 2.3 patch 5 ou o 2.4 patch 5 até que um patch oficial seja liberado.

Verificação no CVP

1. Abra a GUI do FMC e navegue para Analysis > Users > Ative Sessions.

Qualquer sessão ativa publicada através do recurso de diretório de sessão no ISE é exibida na tabela Sessões ativas no FMC.

Ov	Overview Analysis Policies Devices Objects AMP Intelligence Deploy 💩 System Help + admin											idmin v						
Con	ntext Expl	orer Connection	s Intrusions	Files • Hosts •	Users + Active Sessi	ons Vulnerabilities	Correlation •	Custom	 Lookup • 	Search								
													Bookmark This Pi	age Report De	signer Dashboa	rd View Book	marks Se	earch +
Ac	tive S	Sessions																
							Info No devices reg <u>Click here to re</u>	jistered. egister a devic	ž.	×								
Teb	de View o	Active Sessions >	Active Sessions															
• S	earch Cons	traints (Edit Search)															Disabled	Columns
3	ump to	•																
	•	Login Time ×	Last.Seen ×	User ×	Authe	ntication Type ×	Current IP ×	Realm ×	Username ×	First Name	K Last Name ×	E-Mail ×	Department ×	Phone ×	Discovery A	oplication ×	Dex	ice ×
4	0 2	018-05-15 13:26:21	2018-05-15 13:27:36	🖳 xiao yao (LAB).	iavao. LDAP1 Passive	Authentication		LAB					users (rtoaaa)		C LDAP		fireq	ower
4	0 2	018-05-15 12:35:54	2018-05-15 12:35:54	admin.admin.(L	AB\admin.LDAP) Passive	Authentication		LAB					users (rtoaaa)		LDAP		fireq	antr
4	- C 2	018-05-15 11:27:14	2018-05-15 11:27:14	tom (LAB\tom.	LDAP) Passive	Authentication		LAB					users (rtoaaa)		LDAP		fireq	ontr
4	0 2	018-05-15 11:20:30	2018-05-15 11:20:30	lark kent (LAB	superman_LDAP) Passive	Authentication		LAB					users (rtoaaa)		DAR		fireq	ante
14	< Page	1 of 1 >> Display	ring rows 1-4 of 4 rows															
	View View All	Logout																

No modo sudo da CLI do FMC, 'adi_cli session' exibe as informações de sessão do usuário enviadas do ISE para o FMC.

ssh admin@<FMC IP ADDRESS> Password: Last login: Tue May 15 19:03:01 UTC 2018 from dhcp-172-18-250-115.cisco.com on ssh Last login: Wed May 16 16:28:50 2018 from dhcp-172-18-250-115.cisco.com Copyright 2004-2018, Cisco and/or its affiliates. All rights reserved. Cisco is a registered trademark of Cisco Systems, Inc. All other trademarks are property of their respective owners. Cisco Fire Linux OS v6.2.3 (build 13) Cisco Firepower Management Center for VMWare v6.2.3 (build 83) admin@firepower:~\$ sudo -i Password: Last login: Wed May 16 16:01:01 UTC 2018 on cron root@firepower:~# adi_cli session received user session: username tom, ip ::ffff:172.18.250.148, location_ip ::ffff:10.36.150.11, realm_id 2, domain rtpaaa.net, type Add, identity Passive. received user session: username xiayao, ip ::ffff:10.36.148.98, location_ip ::, realm_id 2, domain rtpaaa.net, type Add, identity Passive. received user session: username admin, ip ::ffff:10.36.150.24, location_ip ::, realm_id 2, domain rtpaaa.net, type Add, identity Passive. received user session: username administrator, ip ::ffff:172.18.124.200, location_ip ::, realm_id 2, domain rtpaaa.net, type Add, identity Passive.

Troubleshoot

Atualmente, não existem informações disponíveis específicas sobre Troubleshooting para esta configuração.

Sobre esta tradução

A Cisco traduziu este documento com a ajuda de tecnologias de tradução automática e humana para oferecer conteúdo de suporte aos seus usuários no seu próprio idioma, independentemente da localização.

Observe que mesmo a melhor tradução automática não será tão precisa quanto as realizadas por um tradutor profissional.

A Cisco Systems, Inc. não se responsabiliza pela precisão destas traduções e recomenda que o documento original em inglês (link fornecido) seja sempre consultado.