# Configurazione dell'integrazione di ISE 2.4 e FMC 6.2.3 pxGrid

## Sommario

Introduzione **Prerequisiti** Requisiti Componenti usati **Configurare ISE** Passaggio 1. Abilita servizi PxGrid Passaggio 2. Configurazione di ISE per l'approvazione di tutti gli account basati su certificato pxGrid Passaggio 3. Esporta certificato di amministrazione ISE NT e certificati CA pxGrid Configura FMC Passaggio 4. Aggiungi un nuovo realm a FMC Passaggio 5. Genera certificato CA FMC Passaggio 6. Estrarre il certificato e la chiave privata dal certificato generato con OpenSSL Passaggio 7. Installa certificato in FMC Passaggio 8. Importazione del certificato FMC in ISE Passaggio 9. Configura connessione pxGrid in FMC Verifica Verifica ad ISE Verifica nel CCP Risoluzione dei problemi

## Introduzione

Questo documento descrive il processo di configurazione per l'integrazione di ISE pxGrid versione 2.4 e FMC versione 6.2.3.

# Prerequisiti

## Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- ISE 2.4
- CCP 6.2.3
- Active Directory/Lightweight Directory Access Protocol (LDAP)

## Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- Standalone ISE 2.4
- FMCv 6.2.3
- Active Directory 2012R2
- Identity Services Engine (ISE) pxGrid versione 2.4
- Firepower Management Center (FMC) versione 6.2.3

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

# **Configurare ISE**

### Passaggio 1. Abilita servizi PxGrid

- 1. Accedere alla GUI di ISE Admin e selezionare Amministrazione > Distribuzione.
- 2. Selezionare il nodo ISE da utilizzare per la persona pxGrid.



3. Abilitare il servizio pxGrid e fare clic su Salva come mostrato nell'immagine.

Deployment	Deployment Nodes List > tim24adm									
@ • E • &.	Edit Node									
Deployment     PAN Failover	General Settings Profiling Configuration Hostname FQDN									
	FQUN IP Address									
	Node Type Identity Services Engine (ISE)									
	Role STANDALONE Make Primary									
	Administration									
	V Monitoring									
	Role PRIMARY *									
	Other Monitoring Node									
	✓ Velicy Service									
	Enable Session Services (i)									
	Include Node in Node Group None 🦉 🕧									
	Enable Profiling Service ()									
	Enable Threat Centric NAC Service (i)									
	Enable SXP Service (i)									
	Enable Device Admin Service (i)									
	Enable Passive Identity Service (j)									
	➡ 👽 pxGrid 👔									
	Save Reset									

4. Verificare che i servizi pxGrid vengano eseguiti dalla CLI.

**Nota**: il processo richiede fino a 5 minuti per l'avvio completo dei servizi pxGrid e per determinare lo stato di elevata disponibilità (HA) se sono in uso più nodi pxGrid.

5. SSH nella CLI del nodo ISE pxGrid e controllare lo stato dell'applicazione.

```
# 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. Accedere all'interfaccia utente di ISE Admin e verificare che i servizi siano online e funzionino. Selezionare **Amministrazione > pxGrid Services**.

7. Nella parte inferiore della pagina, ISE visualizza Connected to pxGrid <FQDN nodo pxGrid>.

-dwite Identity Services Engine Home + Context V	sibility + Operations + Policy + Admir	istration + Work Centers				License Warning 🔺 🔍 🔍 🔿 🔿
System      Identity Management      Network Resources	Device Portal Management pxGrid Services	Feed Service     Threat Centric	NAC			Click here to do wireless setup and visibility setup Do not show this again. $ imes$
All Clients Web Clients Capabilities Live Log Set	tings Certificates Permissions					
🖋 Enable 🥝 Disable 🙄 Approve 😝 Group 👎 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 an Oxid Employee shares and						

# Passaggio 2. Configurazione di ISE per l'approvazione di tutti gli account basati su certificato pxGrid

1. Passare ad Amministrazione > pxGrid Services > Impostazioni.

2. Selezionare la casella "Approva automaticamente i nuovi account basati sui certificati" e fare clic su **Salva**.

cisco Identi	ty Services Engi	ne Home	▸ Context Visibility	<ul> <li>Operations</li> </ul>	Policy	<del>▼</del> Admi	inistration	► Wo	ork Centers
System	Identity Manage	ment	k Resources + Devic	ce Portal Management	pxGrid S	Services	Feed Ser	rvice	Threat Centric NAC
All Clients	Web Clients	Capabilities	Live Log Settings	Certificates Perr	missions				
PxGrid	Settings								
Auton Allow	natically approve ne password based a	ew certificate-base ccount creation	ed accounts						
Use De	fault Save								
Test									
Connected to p	xGrid tim24adm.rt	paaa.net							

**Nota**: se questa opzione non è attivata, l'amministratore deve approvare manualmente la connessione FMC ad ISE.

### Passaggio 3. Esporta certificato di amministrazione ISE NT e certificati CA pxGrid

1. Passare ad Amministrazione > Certificati > Certificati di sistema.

2. Espandere il nodo Monitoraggio primario (MNT) se non è abilitato nel nodo Amministrazione primaria.

3. Selezionare il certificato con il campo Utilizzato da "Amministratore".

**Nota**: questa guida utilizza il certificato autofirmato ISE predefinito per l'utilizzo da parte dell'amministratore. Se si utilizza un certificato di amministrazione firmato da un'Autorità di certificazione (CA), esportare la CA radice che ha firmato il certificato di amministrazione sul nodo ISE NT.

4. Fare clic su Esporta.

- 5. Scegliere l'opzione Esporta certificato e chiave privata.
- 6. Impostare una chiave di crittografia.
- 7. Esportare e salvare il file come mostrato nell'immagine.



9. Tornare alla schermata ISE System Certificates (Certificati di sistema ISE).

10. Determinare il campo Rilasciato da nel certificato con l'uso "pxGrid" nella colonna Utilizzato da.

**Nota**: nelle versioni precedenti di ISE, si trattava di un certificato autofirmato, ma a partire dalla versione 2.2 in poi questo certificato viene emesso dalla catena interna di CA ISE per impostazione predefinita.

11. Selezionare il certificato e fare clic su Visualizza come mostrato nell'immagine.

dentity Services Engine	Home  + Context Visibility  + Operations	Policy      Administration	Work Centers			Lie	nse Warning 🔺 🔍 🔍 🔍 🔍		
System + Identity Management + Network Resources + Device Portal Management pxOrld Services + Feed Service + Treat Centric NAC									
Deployment Licensing Certificate	+ Logging + Maintenance Upgrade + 8	ackup & Restore + Admin Acces	is Settings						
0	0								
* Certificate Management	System Certificates 🛕 For disaster recover	y it is recommended to export certif	fcate and private ky pairs of all system ce	rtificates.					
System Certificates	📝 Edit.) 🖶 Generate Self Signed Certificate	🖊 Edit   🖕 Generate Self Signed Certificate.   📥 Import. ) 🔂 Export. 🔀 Delete.   💭 Verv.							
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 Certific e,CN=tim24adm.rtpaaa.net#Certificate	Se pxOrid				Inu, 29 Mar 2018	Thu, 30 Mar 2028 🛃		
Certificate Periodic Check Set5	<ul> <li>Nices Endpoint Sub CA - tim24admilloc</li> <li>1</li> </ul>	00					-		
Certificate Authority	<ul> <li>Default self-signed sami server certifical CN=SAML_tim24adm.rtpaaa.net</li> </ul>	<sup>10</sup> SAML				Fri, 30 Mar 2018	Sat, 30 Mar 2019 🛃		
	<ul> <li>Default self-signed server certificate</li> </ul>	EAP Authentication, Admin, Portal, RADIUS DTLS	Default Portal Certificate Group (j)			Fri, 30 Mar 2018	Sat, 30 Mar 2019 🗾		

12. Determinare il certificato di livello superiore (radice). In questo caso si tratta di **"CA radice Servizi certificati - tim24adm".** 

13. Chiudere la finestra di visualizzazione del certificato come illustrato nell'immagine.

Certificate Services Root C/	A - tim24adm	
Certificate Services No	de CA - tim24adm	
Certificate Service	s Endpoint Sub CA - tim24adm	
tim24adm.rtpa	aa.net	
tim24adm.rtpaaa Issued By : Certit 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)		
City (L)		
State (ST)		
Country (C)		
Serial Number	58:2A:91:45:E8:23:42:74:98:53:06:94:33:9E:AD:83	

Close

14. Espandere il menu ISE Certificate Authority.

#### 15. Selezionare Certificati Autorità di certificazione.

16. Selezionare il certificato radice identificato e fare clic su **Esporta**. Quindi salvare il certificato CA radice pxGrid come mostrato nell'immagine.

dentity Services Engine	Home	Context Visibility      Operatio	ns + Policy + Ad	Iministration + Work Centers					License Warning 🔺	ι e	• •
System      Identity Management	Network	Resources + Device Portal Manag	ement pxGrid Services	s + Feed Service + Threat Cent	ric NAC						
Deployment Licensing Certification	es + Lo	gging + Maintenance Upgrade	Backup & Restore	Admin Access      Settings							
0											
Certifiate Management	CAC	ertificates									
- Certificate Authority		Edit 👍 Import 🕼 Export 🗙	Delete 🔎 View 👰	Refresh							
Omerican		Friendly Name	Status	Trusted For	Serial Number	Issued To	Issued By	Valid From	Expiration Date	Expiratio	on Status
Onernew	V Sr	n24adm									
Issued Certificates	0	Certificate Services Endpoint Sub C& . tim24arim#000003	Enabled	Infrastructure,Endpoints	32 D2 72 55 A9 7D 40 13 8F 2A EF	Certificate Services Endpoint Sub	Certificate Services Node CA -	Thu, 29 Mar 2018	Thu, 30 Mar 2028	<b>.</b>	
Certificate Authority Certificates	-	Certificate Services Root CA -	- Factoria	Index stores for the state	36 67 74 15 A6 A8 4F EB B7 46 1	Certificate Services Root CA -	Certificate Services Root CA -	The 00 May 2018	Thu: 00 Mar 0000	-	
Internal CA Settings	•	5m24adm#00001	Enabled	intrastructure, Enopoints	E7 37 1A AB 88	tim24adm	tim24adm	Thu, 29 Mar 2016	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 78 EE 53 09 34 3E	tim24adm	tim24adm	Thu, 29 Mar 2018	Thu, 30 Mar 2028	<b>*</b>	
External CA Settings		Certificate Services OCSP Responder - tim24adm#00004	Enabled	Infrastructure,Endpoints	74 C2 35 BB 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		

# **Configura FMC**

## Passaggio 4. Aggiungi un nuovo realm a FMC

- 1. Accedere alla GUI di FMC e selezionare **Sistema > Integrazione > Realm**.
- 2. Fate clic su Nuovo realm (New Realm) come mostrato nell'immagine.

Overview	Analysis	Policies De	vices	Objects	AMP	Intelligence								Deploy	🛛 🔍 Sy	stem Help v	admin v
									Configuration	Users	Domains	Integration	Updates	Licenses v	Haith 🔻	Monitoring •	Tools •
Cisco CSI	Realms	Identity S	urces	eStream	er H	ost Input Client	Smart Software Satellite										
	/														Comp	are realms 🔎	New realm
-																	
																•	

3. Compilare il modulo e fare clic sul pulsante Verifica l'aggiunta ad Active Directory (AD).

**Nota**: il nome utente per l'aggiunta ad Active Directory deve essere in formato UPN (User Principal Name). In caso contrario, il test non riesce.

4. Se il test di partecipazione ad Active Directory ha esito positivo, fare clic su 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 🗸	]		
Descripted Field				
* Required Field				
		OK Cancel		

5. Fare clic sulla scheda **Directory**, quindi fare clic su **Add directory** (Aggiungi directory), come mostrato nell'immagine.



6. Configurare IP/Nome host e verificare la connessione.

Nota: se il test ha esito negativo, verificare le credenziali nella scheda Configurazione realm.

7. Fare clic su **OK**.

Edit directory		? :	×
Hostname / IP Address	••••		
Port	389		
Encryption	◯ STARTTLS ◯ LDAPS 💿 None		
SSL Certificate	▼ ()		
	Сапсе Сапсе	1	
Status			

•	Test connection succeeded	
	ок	

8. Fare clic sulla scheda Download utente.

Overview Analysis Policies Devices Objects AMP Intelligence						Deploy	/ 🗢 Sy	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 non è già selezionato, abilitare il download per utenti e gruppi
- 10. Fare clic su Download

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

11. Una volta completata la lista, aggiungere i gruppi desiderati e selezionare **Aggiungi a inclusione**.

12. Salvare la configurazione del realm.

Overview Analysis Policies Devices Objects	AMP Intelligence								Deploy 0	ystem Help v admin
				Configuration	Users	Domains	Integration	Updates	Licenses • Health •	Monitoring • Tool
LAB	=								You have unsaved chang	es_ 🔚 Save 🛛 🚨 Cano
Enter Description										
Directory Realm Configuration User Download										
Download users and groups										
Begin automatic download at 8 Y PM Y America/New Yo	k Repeat Every 24 ¥ Hours									
L Download Now										
Available Groups C			Groups to Include (35)			Groups to Ex	clude (0)			
G Search by name			# NetOps		8	None				
A NetOps			SQLServer2005SQLBrowserUserSRTPAAA-DC2		8					
SQLServer2005SQLBrowserUserSRTPAAA-OC2			WSUS Administrators							
A WSUS Administrators			Enterprise Read-only Domain Controllers		8					
A Enterprise Read-only Domain Controllers			DnsUpdateProxy		8					
PosUpdateProxy			2 jhoehn-group		8					
🝰 jhoehn-group			Ponied RODC Password Replication Group		8					
A Denied RODC Password Replication Group			💤 Domain Admins		8					
🝰 Domain Admins			A Child		8					
📌 Child			A DnsAdmins		8					
A DasAdmins			A Lester\Made\Me\Do\It		8					
A Lester/Made/Me\Do\Jt			A Group Policy Creator Owners		8					
A Group Policy Creator Owners			🝰 INE		8					
A INE			🝰 Domain Users		8					
A Domain Users			🝰 ChadTest		8					
A ChadTest			Acad-only Domain Controllers		8					
A Read-only Domain Controllers			AS and IAS Servers		8					
A RAS and IAS Servers			🝰 Cert Publishers		8					
A Cert Publishers		Exclude	🝰 Schema Admins		8					
률 Schema Admins			A WSUS Reporters		8					
A WSUS Reporters			💤 Parent		8					
A Parent			💤 ISE Admins		8					
A ISE Admins			A WinRMRemoteWMIUsers		8					
A WinRMRemoteWHIUsers			Allowed RODC Password Replication Group		8					
Allowed RODC Paspword Replication Group			A TimSponsors		8					
A TimSconsors			AllowedVPN		8					
Allowed VPN			💤 Enterprise Admins		8					
A Enterorise Admins			🝰 test-users		8					
A test-users			🝰 sponsors		8					
A scorsors			A HelpLibraryUpdaters		8					
A HelpLibraryUpdaters			AP Protected Users		8					
Protected Users			🝰 Domain Guests		8					
Domain Guests			🝰 Domain Computers		8					
Domain Computers			Domain Controllers		- äll					
Bonais Costrollers			A							
A Canadala Demaia Cantallan			Enter User Inclusion		Add	Enter User Ex	clusion			Add

13. Abilitare lo stato del realm.

Overview	Analysis I	Policies Devi	es Objects	AMP	Intelligence									Deploy	/ 🗢 s	rstem Help	v admin v
									Configuration	Users	Domains	Integration	Updates	Licenses +	Health +	Monitoring	<ul> <li>Tools •</li> </ul>
Cisco CSI	Realms	Identity Sou	ces eStrea	mer I	Host Input Client	Smart Software Satellite											
															Corr	pare realms	New realm
Name							Description	Domain	Туре		Base DN	Group	DN	Group Att	ribute	State	
LAB								Global	AD		DC=rtpaaa,DC=n	et CN+U	sers, DC=rtpaaa,	,DC+ member			± 🥒 🐚 🗄

Passaggio 5. Genera certificato CA FMC

1. Passare a **Oggetti > Gestione oggetti > CA interne** come mostrato nell'immagine.

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. Fare clic su Genera CA.
- 3. Compilare il modulo e fare clic su Genera CA autofirmata.

Overview Analysis	Policies Devices	Objects AMP Intelligence			Deploy 🗛 System Help v admin v
Object Management	Intrusion Rules				
Retwork	Name				Value
		Generate Internal Certificate	Authority	? ×	
		Name:	LabFP623		
		Country Name (two-letter code):	US		
		State or Province:	NC		
		Locality or City:	RTP		
		Organization:	Cisco		
		Organizational Unit (Department):	TAC		
		Common Name:			
		Generate CSR	Generate self-signed CA	Cancel	

4. Al termine della generazione, fare clic sulla matita a destra del certificato CA generato, come mostrato nell'immagine.

Overview Analysis	Policies Devices Objects	AMP Intelligence	Dep	loy 🔺 System H	elp + admin +
Object Management	Intrusion Rules				
			Generate CA	Import CA	
Retwork	Name		Value		
Port Interface	LabFP623		CN+LabFP623.rtpaaa.net, ORG+Cisco, OU+TAC,	C=US	/ 8

5. Fare clic su **Download**.

Name:	LabFP623		
Subje	ect:		
Co	ommon Name:		
Or	rganization: Cisco		
Or	ganization Unit: TAC		
Issue	r:		
Co	ommon Name:		
Or	rganization: Cisco		
Or	ganization 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	2:D7:99:F3:EE:41:5C:7B:36:91:40:04:F7:1D:22:4C:60:C2:3C:9C		
Public	: Key Fingerprint:		
b5	1aabcb2cb25e922fdf6c0088771fca794897a1		
Dow	nload	ок	Cancel

6. Configurare e confermare la password di crittografia e fare clic su OK.

7. Salvare il file PKCS (Public-Key Cryptography Standards) p12 nel file system locale.

# Passaggio 6. Estrarre il certificato e la chiave privata dal certificato generato con OpenSSL

Questa operazione viene eseguita nella directory principale della console Gestione configurazione di Microsoft o in qualsiasi client in grado di utilizzare i comandi OpenSSL. Questo esempio utilizza una shell Linux standard.

1. Utilizzare **openssi** per estrarre il certificato (CER) e la chiave privata (PVK) dal file p12.

2. Estrarre il file CER, quindi configurare la chiave di esportazione del certificato dalla generazione del certificato in 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. Estrarre il file PVK, configurare la chiave di esportazione del certificato, quindi impostare una nuova passphrase PEM e confermare.

~\$ 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. Questa frase PEM è necessaria nella fase successiva.

### Passaggio 7. Installa certificato in FMC

- 1. Passare a Oggetti > Gestione oggetti > PKI > Certificati interni.
- 2. Fare clic su Add Internal Cert (Aggiungi certificato interno) come illustrato nell'immagine.



3. Configurare un nome per il certificato interno.

4. Individuare la posizione del file CER e selezionarlo. Una volta inseriti i dati del certificato, selezionare il secondo.

5. Selezionare Option (Opzione) e selezionare il file PVK.

6. Eliminare tutti gli "attributi del sacchetto" iniziali ed eventuali valori finali nella sezione PVK. La chiave PVK inizia con —BEGIN ENCRYPTED PRIVATE KEY— e termina con —END ENCRYPTED PRIVATE KEY—.

**Nota**: non è possibile fare clic su **OK** se il testo PVK contiene caratteri non compresi nei segni meno iniziali e finali.

7. Selezionare la casella Encrypted (Crittografato) e configurare la password creata al momento dell'esportazione della chiave PVK al punto 6.

8. Fare clic su OK.

### Add Known Internal Certificate

Name: TZfpcert	
Certificate Data or, choose a file: Browse	
BEGIN CERTIFICATE MIIDFTCCAmWgAwIBAgIJAKIemFK+L7iYMA0GCSqGSIb3DQEBCwUAM BAYTAIVTMQswCQYDVQQIDAJOQzEMMAoGA1UEBwwDUIRQMQ4wDAY bzEMMAoGA1UECwwDVEFDMRwwGgYDVQQDDBNMYWJGUDYyMy5yd DTE4MDUxNTE4MTM1MloXDTI4MDUxMjE4MTM1MlowZDELMAkGA1UE BgNVBAgMAk5DMQwwCgYDVQQHDANSVFAxDjAMBgNVBAoMBUNpc2H DANUQUMxHDAaBgNVBAMME0xhYkZQNjIzLnJ0cGFhYS5uZXQwggEiM DQEBAQUAA4IBDwAwggEKAoIBAQDMjtS5IUIFiZkZK/TSGtkOCmuivTK5 D7Gm/c69cXw/VfIPWnSBzhEkiRTyspmTMdyf/4TJvUmUH60h108/8dZe Key or, choose a file: Browse	GQxCzAJBgNV YDVQQKDAVDaXNj IHBhYWEubmV0MB4X EBhMCVVMxCzAJ NvMQwwCgYDVQQL A0GCSqGSIb3 ikk1WzAy6 qJOzbjon
Bag Attributes localKeyID: C7 D7 99 F3 EE 41 5C 7B 36 91 40 04 F7 1D 22 4C 60 Key Attributes: <no attributes=""> MIIFDjBABgkqhkiG9w0BBQ0wMzAbBgkqhkiG9w0BBQwwDgQI5uV3Msi MBQGCCqGSIb3DQMHBAhgGVm1+xHLIASCBMjjJxkffXUNUcdB22smyb xL0qjEStmwuyExVp+TWC3AyIJN1DE7/rRssjRAqsnSOxIvDGmg0dVsvnl 74POu/O2Vy99iFoVgW2q9DyXyL/h64TH9CZtwLKIOGOeEunNKpamDnp fXvNZ9 NG4HrEcFmnnij0EwJ0QT8Jn5gAUj+AIPMe32zPqwoccRNYrRXN</no>	C2 3C 9C iHZsICAggA vWotwbcRrt bbqZwjFP ofyN8QC4DC MVM9+Jwp
Encrypted, and the password is:	
	OK Cancel
cfCJU2QGI4jT0SorN4u2Lk+S+Qd1s7Ii2wIQMWKPI2R9UGv1tyM6HTPCG acClCUAsecVrYY081GKTVVJ3bWgWfPtR3OH12YCA2whcCKcG50MByB4t O/g= END_ENCRYPTED_PRIVATE_KEY ← DELETE	GoCo6VDI jhHN036q
Encrypted, and the password is:	•••
	OK Cancel

## Passaggio 8. Importazione del certificato FMC in ISE

1. Accedere alla GUI di ISE e selezionare Amministrazione > Sistema > Certificati > Certificati attendibili.

2. Fare clic su Importa.

dentity Services Engine	Home + Context Visibility + Operations + Policy	- Administra	Son Vork Centers							License Warning 🔺	<u> </u>	0 0	0
System + Identity Management +	Network Resources	id Services + Fe	ed Service + Threat Cent	tric NAC									
Deployment Licensing - Certificates	Logging      Maintenance Upgrade      Backup &	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	<ul> <li>Baltimore CyberTrust Root</li> </ul>	Enabled	Cisco Services	02 00 00 89	Baltimore CyberTrust Ro	Baltimore CyberTrust Ro	Fri, 12 May 2000	Mon, 12 May 2025	<b>1</b>				
Certificate Signing Requests	Cisco CA Manufacturing	O Disabled	Endpoints Infrastructure	6A 69 67 B3 00 00	Cisco Manufacturing CA	Cisco Root CA 2048	Fri, 10 Jun 2005	Mon, 14 May 2029	<b>1</b>				
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					
Certificate Authority	Cisco Root CA 2048	Disabled	Infrastructure Endpoints	5F 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 GA M2	Cisco Root CA M2	Mon, 12 Nov 2012	Thu, 12 Nov 2037	<b>1</b>				
	Default self-signed server certificate	Enabled	Endpoints Infrastructure	SA BE 7E D8 00 00	tim24adm.rtpaaa.net	tim24adm.rtpaaa.net	Fri, 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	<b>1</b>				
	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	<b>.</b>				
	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	<b>2</b>				
	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	<b>1</b>				
	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	<b>.</b>				
	TimFP623	Enabled	Infrastructure Endpoints	BE F9 42 3D 25 AS	TimFP623.rtpaaa.net	TimFP623.rtpaaa.net	Tue, 15 May 2018	Fri, 12 May 2028	<b>1</b>				
	VeriSign 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					
	VeriSign Class 3 Secure Server CA - G3	Enabled	Cisco Services	6E CC 7A AS A7 03	VeriSign Class 3 Secure	VeriSign Class 3 Public	Sun, 7 Feb 2010	Fri, 7 Feb 2020	<b>1</b>				

3. Fare clic su Scegli file e selezionare il file CER FMC dal sistema locale.

Facoltativo: configurare un nome descrittivo.

4. Controllare l'attendibilità per l'autenticazione in ISE.

Facoltativo: configurare una descrizione.

5. Fare clic su Submit (Invia) come mostrato nell'immagine.

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

### Passaggio 9. Configura connessione pxGrid in FMC

1. Passare a Sistema > Integrazione > Origini identità come mostrato nell'immagine.



2. Fare clic su ISE.

Import a

- 3. Configurare l'indirizzo IP o il nome host del nodo ISE pxGrid.
- 4. Selezionare il segno + a destra di pxGrid Server CA.

5. Assegnare un nome al file CA del server, quindi individuare la CA di firma radice pxGrid raccolta nel passaggio 3 e fare clic su **Salva**.

6. Selezionare il segno + a destra di CA del server NT.

7. Assegnare un nome al file della CA del server, quindi individuare il certificato amministratore raccolto nel passaggio 3 e fare clic su **Salva**.

8. Selezionare il file FMC CER dall'elenco a discesa.

Identity Sources			
Service Type	None Identity Services Engine		lser Agent
Primary Host Name/IP Address * Secondary Host Name/IP Address	<ise address="" ip="" node="" pxgrid=""></ise>	8	
pxGrid Server CA *	ISE24InternalRoot	~	٥
MNT Server CA *	ISE24SelfSigned	~	0
FMC Server Certificate *	TimFP623	~	٥
ISE Network Filter			ex. 10.89.31.0/24, 192.168.8.0/24,
* Required Field	Test		

#### 9. Fare clic su Test.

10. Se il test ha esito positivo, fare clic su **OK**, quindi su **Salva** nella parte superiore destra della schermata.

## Status



**Nota**: quando si eseguono due nodi ISE pxGrid, è normale che un host visualizzi il risultato positivo e uno il risultato negativo, in quanto pxGrid viene eseguito attivamente su un solo nodo ISE alla volta. A seconda della configurazione, la modalità di visualizzazione degli errori dell'host primario e degli errori dell'host secondario dipende dalla configurazione. Tutto questo dipende da quale nodo in ISE è il nodo pxGrid attivo.

## Verifica

Verifica ad ISE

1. Aprire la GUI di ISE e selezionare Administration > pxGrid Services.

Se l'operazione ha esito positivo, nell'elenco dei client sono elencate due connessioni firepower. Uno per il CCP effettivo (iseagent-hostname-33bytes) e uno per il dispositivo di test (firesightisetest-hostname-33bytes).

tinde Identity Services Engine	Home + Context Visibility	Operations      Policy      Admin	istration + Work Centers				License Warning 🔺 🧠 😐 🔿 🔍
System      Identity Management	Network Resources      Device Pr	ortal Management pxGrid Services	Feed Service      Threat Centri	o NAC			
All Clients Web Clients Cap	abilities Live Log Settings C	ertificates Permissions					
√Enable Ø Disable Ø Approve	😝 Group 📫 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	
		Capabilities(2 Pub, 1 Sub)	Online (XMPP)	Internal	Certificate	Vew	
		Capabilities(0 Pub, 0 Sub)	Online (XMPP)	Internal	Certificate	View	
		Capabilities(0 Pub, 0 Sub)	Online (XMPP)	Internal	Certificate	Vew	
		Capabilities(0 Pub, 4 Sub)	Online (XMPP)	Internal	Certificate	View	
		Canabilities(4 Pub. 2 Sub)	Online (XMPP)	Internal	Certificate	Van	
		Capabilities(0 Pub, 6 Sub)	Online (XMPP)		Certificate	View	
		Capabilities(0 Pub, 0 Sub)	Offline (XMPP)		Certificate	View	

La connessione iseagent-firepower visualizza sei (6) subs e appare online.

La connessione firesightisetest-firepower visualizza zero (0) subs e appare offline.

La visualizzazione estesa del client iseagent-firepower visualizza le sei sottoscrizioni.

Capability Detail	
1-6 of 6 Show 25 v per page Page	\$
Capability Name Capability Version Messaging Role Message Filter	
AdaptiveNetworkControl 1.0 Sub	
C Core 1.0 Sub	
C EndpointProfileMetaData 1.0 Sub	
O EndpointProtectionService 1.0 Sub	
SessionDirectory 1.0 Sub	
O TrustSecMetaData 1.0 Sub	

**Nota**: a causa del bug Cisco <u>IDCSCvo75376</u> esiste un limite per il nome host e il download bulk non riesce. Il pulsante di prova del CCP visualizza un errore di connettività. Ciò influisce su 2,3p6, 2,4p6 e 2,6. Si consiglia di eseguire la patch 2.3 5 o 2.4 5 fino al rilascio di una patch ufficiale.

### Verifica nel CCP

1. Aprire la GUI di FMC e selezionare **Analisi > Utenti > Sessioni attive**.

Tutte le sessioni di Active Directory pubblicate tramite la funzionalità Directory di sessione in ISE vengono visualizzate nella tabella Active Sessions in FMC.

Overview Analysis Policies Devices Objects AMP Intelligence																Deploy 🗢 System	Help v admin
Con	ntext Explorer	Connection	s   Intrusions	Files • Ho	sts • Users • Ac	tive Sessions	Vulnerabilities •	Correlation •	Custom	<ul> <li>Lookup •</li> </ul>	Search						
														Bookmark This P	ege Report De	signer Dashboard View Booi	kmarks Search ¥
Active Sessions																	
								O lafe			~						
								No devices rea	istered.								
								Click here to re	oister a devic	a.							
Teb	de View of Act	ive Sessions > (	Active Sessions														
Search Constraints (Edit Search)     Dis														Disabled Column			
-	* Los	in Time X	Last Seen X	User X		Authenticatio	no Type X Cu	rreat IP ×	Realm X	Username X	First Name	X Last Name X	E-Mail X	Department X	Phone X	Discovery Application X	Device X
		ILLING A	MARK PROVIDENT	Real of		Construction of the	all the second	and a contract of	Example 1	Section in the	CLAR HALIN	A REALING A	ALCOND **	Resident and a second s	Lines	RUSSESSEE	Extina -
+	2018-	25-15 13:26:21	2018-05-15 13:27:36	3 xiao xao (1	AB\xiavao, LDAP)	Passive Authen	tication		LAB					users (rtoaaa)		IDAP	fireqower
4	2018-	5-15 12:35:54	2018-05-15 12:35:54	admin adm	nin (LAB\admin, LDAP)	Passive Authen	tication		LAB					users (rtoaaa)		LDAP	fireqower
4	2018-	5-15 11:27:14	2018-05-15 11:27:14	tom (LAB)	tom, LDAP)	Passive Authen	tication		LAB					users (rtoaaa)		LDAP	firecower
4	2018-	5-15 11:20:30	2018-05-15 11:20:30	lark kent	(LAB\superman, LDAP)	Passive Authen	tication		LAB					users.(rtoaaa)		IDA2	firequier
< < Page ■ of 3 >>  Displaying rows 1=4 of 4 rows																	
	View	Logout															
	View All																

In modalità sudo CLI FMC, il comando 'adi\_cli session' visualizza le informazioni sulla sessione utente inviate dall'ISE al 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.

## Risoluzione dei problemi

Al momento non sono disponibili informazioni specifiche per la risoluzione dei problemi di questa configurazione.

#### Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l'accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).