# Configurazione dell'integrazione di ISE 2.4 pxGrid IND 1.6.1

# Sommario

Introduzione **Prerequisiti** Requisiti Componenti usati Configurazione Diagramma di flusso ad alto livello Configurazioni Passaggio 1. Configurazione degli attributi personalizzati dell'endpoint su ISE Passaggio 2. Configurare i criteri del profiler utilizzando gli attributi personalizzati Passaggio 3. Abilitazione degli attributi personalizzati per l'applicazione della profilatura Passaggio 4. Esportare il certificato di identità IND Passaggio 5. Carica il certificato di identità IND nell'archivio di fiducia ISE Passaggio 6. Genera certificato per IND Passaggio 7. Scaricare la catena di certificati in formato PKCS12 Passaggio 8. Caricare la catena di certificati in IND Passaggio 9. Configurare Policy Server su IND Passaggio 10. Configurare l'integrazione pxGrid su IND Passaggio 11. Approvazione di IND su ISE Passaggio 12. Attivare il servizio pxGrid su IND Verifica Verifica ISE Verifica IND Risoluzione dei problemi Stato sincronizzazione bloccato in non sincronizzato su IND Non tutti ali endpoint sono condivisi con ISE assetTag e AssetGroup non sono disponibili su ISE

# Introduzione

In questo documento viene descritto come configurare Identity Services Engine (ISE) 2.4 e l'integrazione di Industrial Network Director 1.6.1-4 su pxGrid (Platform Exchange Grid) e come risolvere i problemi. Cisco IND è registrato con pxGrid come publisher e pubblica informazioni sugli attributi degli endpoint su ISE per il dizionario IOTASSET.

# Prerequisiti

Requisiti

Cisco raccomanda la conoscenza di base dei seguenti argomenti:

- Cisco Identity Service Engine
- Cisco Industrial Network Director

#### Componenti usati

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

- Cisco Identity Service Engine versione 2.4 p6
- Industrial Network Director 1.6.1-4

### Configurazione

#### Diagramma di flusso ad alto livello



# 1. IND si registra con ISE tramite pxGrid versione 2 sul nodo ISE pxGrid. Log corrispondenti da IND (application.log):

```
2019-05-22 14:31:17,770:INF0:qtp281049997-52711:PxgridPublisher:: Connect start
2019-05-22 14:31:17,770:INF0:qtp281049997-52711:PxgridPublisher:: Hostname:WIN2012-AAA
IpAddress:10.62.145.130
2019-05-22 14:31:17,770:INF0:qtp281049997-52711:PxgridPublisher:: pxGrid
RestBaseUrl:https://WIN2012-AAA:8910/pxgrid/ind/asset/
2019-05-22 14:31:17,770:INF0:qtp281049997-52711:PxgridController:: Send Request ServiceRegister
invoked with pxGridServer(s) [ISE24-1ek.example.com]
2019-05-22 14:31:17,770:INF0:qtp281049997-52711:PxgridController:: Sending ServiceRegister
request to pxGridServer ISE24-1ek.example.com
2019-05-22 14:31:17,786:INF0:qtp281049997-52711:PxgridController::
Request={"name":"com.cisco.endpoint.asset","properties":{"wsPubsubService":"com.cisco.ise.pubsub
","restBaseUrl":"https://WIN2012-
AAA:8910/pxgrid/ind/asset/","assetTopic":"/topic/com.cisco.endpoint.asset"}}
```

2019-05-22 14:31:17,911:INFO:gtp281049997-52711:PxgridController:: Response={"id":"76d4abaf-9efd-4c68-a046-79e049564902", "reregisterTimeMillis": "300000"} 2019-05-22 14:31:17,911:INF0:qtp281049997-52711:PxgridController:: Send Request ServiceLookup invoked with pxGridServer(s) [ISE24-lek.example.com] 2019-05-22 14:31:17,911:INFO:qtp281049997-52711:PxgridController:: Sending ServiceLookup request to pxGridServer ISE24-1ek.example.com 2019-05-22 14:31:17,911:INFO:gtp281049997-52711:PxgridController:: Request={"name":"com.cisco.ise.pubsub"} 2019-05-22 14:31:17,911:INFO:qtp281049997-52711:PxgridController:: Response={"services":[{"name":"com.cisco.ise.pubsub", "nodeName":"ise-pubsub-ise24lek", "properties": {"wsurl": "wss://ISE24-1ek.example.com:8910/pxgrid/ise/pubsub" }}] 2019-05-22 14:31:17,911:INFO:qtp281049997-52711:PxgridPublisher:: wsUrl=wss://ISE24-1ek.example.com:8910/pxgrid/ise/pubsub 2019-05-22 14:31:17,911:INFO:qtp281049997-52711:PxgridController:: Send Request AccessSecret invoked with pxGridServer(s) [ISE24-1ek.example.com] 2019-05-22 14:31:17,911:INFO:qtp281049997-52711:PxgridController:: Sending AccessSecret request to pxGridServer ISE24-1ek.example.com 2019-05-22 14:31:17,926:INFO:qtp281049997-52711:PxgridController:: Request={"peerNodeName":"isepubsub-ise24-1ek"} 2019-05-22 14:31:17,926:INF0:qtp281049997-52711:PxgridController:: Access Secret recieved 2019-05-22 14:31:17,926:INFO:qtp281049997-52711:PxgridPublisher:: Client created Come mostrato nei log, IND è stato registrato per assetTopic

# 2. ISE PSN con probe pxgrid abilitato esegue un download in blocco delle risorse pxGrid esistenti (profiler.log):

```
2019-05-22 14:39:25,817 INFO [ProfilerINDSubscriberPoller-56-thread-1][]
cisco.profiler.infrastructure.probemgr.INDSubscriber -::- New services are: [Service
[name=com.cisco.endpoint.asset, nodeName=ind2, properties={wsPubsubService=com.cisco.ise.pubsub,
restBaseUrl=https://WIN2012-AAA:8910/pxgrid/ind/asset/,
assetTopic=/topic/com.cisco.endpoint.asset}]]
2019-05-22 14:39:26,011 INFO [ProfilerINDSubscriberPoller-56-thread-1][]
cisco.profiler.infrastructure.probemgr.INDSubscriber -::- NODENAME:ind2
2019-05-22 14:39:26,011 INFO [ProfilerINDSubscriberPoller-56-thread-1][]
cisco.profiler.infrastructure.probemgr.INDSubscriber -:- REQUEST
BODY{"offset":"0","limit":"500"}
2019-05-22 14:39:26,046 INFO [ProfilerINDSubscriberPoller-56-thread-1][]
cisco.profiler.infrastructure.probemgr.INDSubscriber -::- Response status={}200
2019-05-22 14:39:26,046 INFO [ProfilerINDSubscriberPoller-56-thread-1][]
cisco.profiler.infrastructure.probemgr.INDSubscriber -::- Content: "OUT_OF_SYNC"
2019-05-22 14:39:26,047 INFO [ProfilerINDSubscriberPoller-56-thread-1][]
cisco.profiler.infrastructure.probemgr.INDSubscriber -::- Status is :"OUT_OF_SYNC"
2019-05-22 14:39:26,047 DEBUG [ProfilerINDSubscriberPoller-56-thread-1][]
cisco.profiler.infrastructure.probemgr.INDSubscriber -::- Static set after adding new services:
[Service [name=com.cisco.endpoint.asset, nodeName=ind,
properties={wsPubsubService=com.cisco.ise.pubsub, restBaseUrl=https://WIN2012-
AAA:8910/pxgrid/ind/asset/, assetTopic=/topic/com.cisco.endpoint.asset}], Service
[name=com.cisco.endpoint.asset, nodeName=ind2, properties={wsPubsubService=com.cisco.ise.pubsub,
restBaseUrl=https://WIN2012-AAA:8910/pxgrid/ind/asset/,
assetTopic=/topic/com.cisco.endpoint.asset}]]
2019-05-22 14:39:26,052 INFO [ProfilerINDSubscriberBulkRequestPool-80-thread-1][]
cisco.profiler.infrastructure.probemgr.INDSubscriber -::- NODENAME:ind2
2019-05-22 14:39:26,052 INFO [ProfilerINDSubscriberBulkRequestPool-80-thread-1][]
cisco.profiler.infrastructure.probemgr.INDSubscriber -::- REQUEST
BODY{"offset":"0","limit":"500"}
2019-05-22 14:39:26,111 INFO [ProfilerINDSubscriberBulkRequestPool-80-thread-1][]
cisco.profiler.infrastructure.probemgr.INDSubscriber -::- Response status={}200
2019-05-22 14:39:26,111 INFO [ProfilerINDSubscriberBulkRequestPool-80-thread-1][]
cisco.profiler.infrastructure.probemgr.INDSubscriber -::- Content:
{"assets":[{"assetId":"100","assetName":"WIN2012-
CHILD", "assetIpAddress": "10.62.145.131", "assetMacAddress": "00:50:56:b6:46:87", "assetVendor": "VMw
```

```
are", "assetProductId": "Unknown", "assetSerialNumber": "", "assetDeviceType": "Server", "assetSwRevisi
on":"", "assetHwRevision":"", "assetProtocol":"NetBIOS", "assetConnectedLinks":[], "assetCustomAttri
butes":[{"key":"assetGroup","value":"Root"}, {"key":"assetTag","value":"SEC_TAG2"}]}, {"assetId":"
101", "assetName": "win2012.example.com", "assetIpAddress": "10.62.145.72", "assetMacAddress": "00:50:
56:9c:3f:92", "assetVendor": "VMware", "assetProductId": "Unknown", "assetSerialNumber": "", "assetDevi
ceType":"Server", "assetSwRevision":"", "assetHwRevision":"", "assetProtocol":"NetBIOS", "assetConne
ctedLinks":[],"assetCustomAttributes":[{"key":"assetGroup","value":"Root"},{"key":"assetTag","va
lue":""}]}]
2019-05-22 14:39:26,111 DEBUG [ProfilerINDSubscriberBulkRequestPool-80-thread-1][]
cisco.profiler.infrastructure.probemgr.INDSubscriber -::- Parsing bulk response
{"assets":[{"assetId":"100","assetName":"WIN2012-
CHILD", "assetIpAddress": "10.62.145.131", "assetMacAddress": "00:50:56:b6:46:87", "assetVendor": "VMw
are", "assetProductId": "Unknown", "assetSerialNumber": "", "assetDeviceType": "Server", "assetSwRevisi
on":"", "assetHwRevision":"", "assetProtocol": "NetBIOS", "assetConnectedLinks":[], "assetCustomAttri
butes":[{"key":"assetGroup","value":"Root"}, {"key":"assetTag","value":"SEC_TAG2"}]}, {"assetId":"
101", "assetName": "win2012.example.com", "assetIpAddress": "10.62.145.72", "assetMacAddress": "00:50:
56:9c:3f:92", "assetVendor": "VMware", "assetProductId": "Unknown", "assetSerialNumber": "", "assetDevi
ceType":"Server", "assetSwRevision":"", "assetHwRevision":"", "assetProtocol":"NetBIOS", "assetConne
ctedLinks":[],"assetCustomAttributes":[{"key":"assetGroup","value":"Root"},{"key":"assetTag","va
lue":""}]}]
```

3. Il nuovo endpoint viene individuato su IND (deve essere individuato con un protocollo, altrimenti l'endpoint non viene identificato come PxGrid Asset e non viene condiviso tramite PxGrid con ISE).

-ili-ili- cisco	INDUSTRIAL NETWORK DIRECTOR	Operate	> Inventory			
©: Overview	< Back					win2012.example.com
						DEVICE OVERVIEW
				Name	win2012.example.com	Device Type Server
				IP Address	10.62.145.72	Protocol NetBIOS
				MAC Address	00:50:56:9c:3f:92	Group Root
				Vendor	VMware	Connected to
				pxGrid Asset	Yes	Tag(s) +

4. IND pubblica queste informazioni sul nodo ISE pxGrid

#### 5. Il PSN tramite il probe pxGrid riceve i seguenti dati (profiler.log):

```
2019-05-22 15:20:40,616 DEBUG [Grizzly(2)][]
cisco.profiler.infrastructure.probemgr.INDSubscriber -::- Parsing push notification response:
{"asset":{"assetId":"101","assetName":"win2012.example.com","assetIpAddress":"10.62.145.72","ass
etMacAddress":"00:50:56:9c:3f:92", "assetVendor":"VMware", "assetProductId":"Unknown", "assetSerial
Number":"", "assetDeviceType": "Server", "assetSwRevision":"", "assetHwRevision":"", "assetProtocol":
"NetBIOS", "assetConnectedLinks": [], "assetCustomAttributes": [{ "key": "assetGroup", "value": "Root" },
{"key":"assetTag","value":"SEC_TAG2"}]},"opType":"UPDATE"}
2019-05-22 15:20:40,616 DEBUG [Grizzly(2)][]
cisco.profiler.infrastructure.probemgr.INDSubscriber -::- sending endpoint to
forwarder{"assetId":"101","assetName":"win2012.example.com","assetIpAddress":"10.62.145.72","ass
etMacAddress":"00:50:56:9c:3f:92","assetVendor":"VMware","assetProductId":"Unknown","assetSerial
Number":"", "assetDeviceType": "Server", "assetSwRevision":"", "assetHwRevision":"", "assetProtocol":
"NetBIOS", "assetConnectedLinks": [], "assetCustomAttributes": [{ "key": "assetGroup", "value": "Root" },
{"key":"assetTag","value":"SEC_TAG2"}]}
2019-05-22 15:20:40,617 INFO [Grizzly(2)][] cisco.profiler.infrastructure.probemgr.Forwarder -
::- Forwarder Mac 00:50:56:9C:3F:92 MessageCode null epSource PXGRIDPROBE
2019-05-22 15:20:40,617 DEBUG [forwarder-2][]
```

cisco.profiler.infrastructure.probemgr.ForwarderHelper -: ProfilerCollection: - sequencing Radius message for mac = 00:50:56:9C:3F:922019-05-22 15:20:40,617 DEBUG [forwarder-2][] cisco.profiler.infrastructure.probemgr.Forwarder -:ProfilerCollection:- Processing endpoint:00:50:56:9C:3F:92 2019-05-22 15:20:40,618 DEBUG [forwarder-2][] com.cisco.profiler.im.EndPoint -:ProfilerCollection:- filtered custom attributes are:{assetGroup=Root, assetTag=SEC\_TAG2} 2019-05-22 15:20:40,618 DEBUG [forwarder-2][] cisco.profiler.infrastructure.probemgr.Forwarder -:ProfilerCollection:- Filtering:00:50:56:9C:3F:92 2019-05-22 15:20:40,618 DEBUG [forwarder-2][] cisco.profiler.infrastructure.probemgr.Forwarder -:ProfilerCollection: - Endpoint Attributes: EndPoint[id=<null>, name=<null>] MAC: 00:50:56:9C:3F:92 Attribute:BYODRegistration value:Unknown Attribute:DeviceRegistrationStatus value:NotRegistered Attribute:EndPointProfilerServer value:ISE24-1ek.example.com Attribute:EndPointSource value:PXGRIDPROBE Attribute:MACAddress value:00:50:56:9C:3F:92 Attribute:NmapSubnetScanID value:0 Attribute:OUI value:VMware, Inc. Attribute:PolicyVersion value:0 Attribute:PortalUser value: Attribute:PostureApplicable value:Yes Attribute:assetDeviceType value:Server Attribute:assetGroup value:Root Attribute:assetHwRevision value: Attribute:assetId value:101 Attribute:assetIpAddress value:10.62.145.72 Attribute:assetMacAddress value:00:50:56:9c:3f:92 Attribute:assetName value:win2012.example.com Attribute:assetProductId value:Unknown Attribute:assetProtocol value:NetBIOS Attribute:assetSerialNumber value: Attribute:assetSwRevision value: Attribute:assetTag value:SEC\_TAG2 Attribute:assetVendor value:VMware Attribute:b310a420-78a5-11e9-a189-9ac8f4107843 value:Root Attribute:b8e73d50-78a5-11e9-a189-9ac8f4107843 value:SEC\_TAG2 Attribute: ip value: 10.62.145.72 Attribute:SkipProfiling value:false La visibilità del contesto viene aggiornata con i dati corretti

le Iden	ntity Services En	igine I	Home		<ul> <li>Operations</li> </ul>	Policy	<ul> <li>Administration</li> </ul>	<ul> <li>Work Centers</li> </ul>
ndpoints	Users Netwo	ork Devices	Applicat	tion				
00:50	:56:9C:3F:92 MAC Addr Username	2 🖸 ress: 00:50:56	6:9C:3F:9	2				
<b></b> @	Applications	Profile: IOT_D Address: 10.	62.145.72	2 uthentication Ti	nreats Vuln	erabilities		
General	Attributes							
Descripti	ion							
Static As	signment	false						
Endpoint	t Policy	IOT_DEVI	CE2					
Static Gr	roup Assignment	false						
Identity (	Group Assignment	Profiled						
Custom	Attributes							
							7	Filter - 🌣 -
	Attribute Name	9		Attribute Valu	e			
×	Attribute Name			Attribute Value	3			
	assetGroup			Root				
	LogicalProfile							
	assetTag			SEC_TAG2				
Other At	ttributes							

#### Configurazioni

**Nota:** I passi da 1 a 3 sono obbligatori anche se si desidera avere solo la visibilità di assetGroup e assetTag in Context Visibility

#### Passaggio 1. Configurazione degli attributi personalizzati dell'endpoint su ISE

Passare a **Amministrazione > Gestione identità > Impostazioni > Attributi personalizzati endpoint**. Configurare gli attributi personalizzati (assetGroup e assetTag) in base all'immagine seguente.

dentity Services Engine	Home	Visibility	Policy	- Administration	Work Centers
▶ System	<ul> <li>Network Resources</li> </ul>	Device Portal Management	pxGrid S	ervices + Feed Se	rvice
Identities Groups External Ide	entity Sources Identity S	Source Sequences - Settings			
	9				
User Custom Attributes	Endpoint Cust	tom Attributes			
User Authentication Settings					
Endpoint Purge	Endpoint Attr	ibutes (for reference)			
Endpoint Custom Attributes	Mandatory	Attribute Name		Data	Гуре
		PostureApplicable		STRIN	G
		EndPointPolicy		STRIN	G
		AnomalousBehaviour		STRIN	G
		OperatingSystem		STRIN	G
		BYODRegistration		STRIN	G
		PortalUser		STRIN	G
		LastAUPAcceptanceHours		INT	
		LogicalProfile		STRIN	G
	Endpoint Cust	tom Attributes			
		Attribute name		Туре	
	assetGroup			String	-
	assetTag			String	- •
				Reset	Save

#### Passaggio 2. Configurare i criteri del profiler utilizzando gli attributi personalizzati

Passare a **Centri di lavoro > Profiler > Criteri di profilatura**. Fare clic su **Add**. Configurare i criteri del profiler in modo simile all'immagine seguente.

-that Identity Services Engine Home	Context Visibility     Operations	Policy Administration	ork Centers		
Network Access     Guest Access     TrustSec	BYOD      ▼Profiler      Posture	Device Administration			
Overview Ext Id Sources Network Devices Ends	oint Classification Node Config Feeds	Manual Scans Policy Elements	Profiling Policies Policy Sets	Troubleshoot Reports	Settings Dictionaries
Profiling ← ▼ 1 = ▼ ↔ → Profiling Policies → Logical Profiles	Profiler Policy List > IOT_DEVICE1 Profiler Policy * Name Policy Enabled * Minimum Certainty Factor * Exception Action * Network Scan (NMAP) Action Create an Identity Group for the policy * Parent Policy * Associated CoA Type System Type Rules	IOT DEVICE1	Description (Valid Range 1 to 65535) up erarchy		<i>li</i> i
	If Condition CUSTOMATTRIBUTE	_assetTag_EQUALS	Certainty Factor Increases	▼ 20	
	Save Rese	e Expression CUSTOMATTRIB	EQUALS V SEC_TA	G1	<u>•</u>

Passaggio 3. Abilitazione degli attributi personalizzati per l'applicazione della profilatura

Passare a Centri di lavoro > Profiler > Impostazioni > Impostazioni profiler. Garantire Abilita attributo personalizzato per applicazione profilatura è selezionata.

dentity Services Engine	Home  Context Visibility  Operations  Policy  Administration  Work Centers
Network Access     Guest Access	TrustSec     BYOD     Profiler     Posture     Device Administration     PassiveID
Overview Ext Id Sources Network Dev	vices Endpoint Classification Node Config Feeds + Manual Scans + Policy Elements Profiling Policies Policy Sets + Troubleshoot Reports - Settings Dictionaries
C Profiler Settings	Profiler Configuration
Promer Settings	
NMAP Scan Subnet Exclusions	* CoA Type: Reauth *
	Current custom SNMP community strings: •••••• Show
	Change custom SNMP community strings: (For NMAP, comma separated. Field will be cleared on successful saved change.)
	Confirm changed custom SNMP community strings: (For NMAP, comma separated. Field will be cleared on successful saved change.)
	EndPoint Attribute Filter: Enabled ()
	Enable Anomalous Behaviour Detection:   Enabled ()
	Enable Anomalous Behaviour Enforcement: 🔲 Enabled
	Enable Custom Attribute for Profiling Enforcement: 🥑 Enabled
	Save Reset

Passaggio 4. Esportare il certificato di identità IND

Passare a **Impostazioni > pxGrid**. Fare clic su **Download del certificato .pem IND**. Questo certificato è utilizzato durante la registrazione di pxGrid, quindi ISE deve considerarlo attendibile.

-ili-ili- cisco	NETWO	RIAL RK DIRECTOR		Settings	>	pxGrid	d																												۰ 🌲		Û	e	- 1	1	·
i⊟ Settings																					pxG	Grid																			
Trusted Certificates		Cisco Platform E Services Engine	Exchange (ISE) px0	Grid (pxGi Brid contro	rid) is an lier. This	open, scala information	lable data- on can ther	a-sharin en be lev	ng and th everaged	threat con id by upst	ntrol platf tream se	form that icurity sys	it allows r ystems to	i seamles to monito	as integ or secur	igration urity, di	on betw Setect th	veen mul threats, a	itivendor and set n	r identity network	ity, netwo k policy. I	iork, secu I. Learn m	rity and a ore here.	asset m	nanageme	nent syst	Aems. E	inabiling th	he feature	below ac	tivates t	he sharin	ig of endpo	oint assets	discovere	d by thi	is system	with a C	isco Iden	ntity	
		Download .p	em IND c	ertificate																																					

#### Passaggio 5. Carica il certificato di identità IND nell'archivio di fiducia ISE

Selezionare Amministrazione > Certificati > Gestione certificati > Certificati attendibili. Fare clic su Import. Fare clic su Sfoglia e selezionare il certificato IND dal passo 3. Fare clic su Invia.

ululu Identity Services Engine	Home  → Context Visibility  → Operations  → Policy  → Administration  → Work Centers
▼ System → Identity Management	Network Resources   Device Portal Management pxGrid Services   Feed Service   Threat Centric NAC
Deployment Licensing - Certificate	s ► Logging ► Maintenance Upgrade ► Backup & Restore ► Admin Access ► Settings
0	
- Certificate Management	Import a new Certificate into the Certificate Store
System Certificates	* Certificate File Browse ind(1).pem
Trusted Certificates	Friendly Name
OCSP Client Profile	
Certificate Signing Requests	Trusted For: 🕧
Certificate Periodic Check Setti	✓ Trust for authentication within ISE
Certificate Authority	Trust for client authentication and Syslog
	Trust for authentication of Cisco Services
	Validate Certificate Extensions
	Description
	Submit Cancel

#### Passaggio 6. Genera certificato per IND

IND non utilizza il certificato client emesso da ISE CA. L'obiettivo è invece quello di popolare l'archivio attendibile IND, in modo che quando ISE invia il proprio certificato pxGrid (durante lo scambio TLS), esso sia considerato attendibile da IND.

Selezionare Amministrazione > pxGrid Services > Certificati. Compilare i campi in base all'immagine seguente. Il campo CN è obbligatorio in quanto l'obiettivo di ISE CA è il rilascio di un certificato di identità. È consigliabile immettere il nome di dominio completo (FQDN) di IND, ma poiché il certificato di identità non viene utilizzato da IND, il valore del campo CN non è critico.

dentity Services Engine Ho	me   Context Visibility   Operations   Policy   Administration   Work Centers	
System     Identity Management     No	etwork Resources	
All Clients Web Clients Capabilities	Live Log Settings Certificates Permissions	
Generate pxGrid Certificates		
I want to *	Generate a single certificate (without a certificate signing request)	•
Common Name (CN) *	ind.example.com	
Description		
Certificate Template	PxGrid_Certificate_Template	
Subject Alternative Name (SAN)	- +	
Certificate Download Format *	PKCS12 format (including certificate chain; one file for both the certificate chain and key)	• 0
Certificate Password *		0
Confirm Password *		
	Reset Create	

Passaggio 7. Scaricare la catena di certificati in formato PKCS12

00	Opening 1558534704560_cert.zip
You have cho	sen to open:
155853470	04560_cert.zip
which is: ZI from: https	P archive ://10.62.145.140
What should	Firefox do with this file?
Open with	Archive Utility (default)
Save File	
Do this aut	omatically for files like this from now on.
	Cancel OK

#### Passaggio 8. Caricare la catena di certificati in IND

Passare a **Impostazioni > pxGrid > Certificati attendibili**. Fare clic su **Nuovo**. Immettete il nome (la catena sarà visibile con questo nome su IND). La password è quella del passaggio 1.

Upload Trusted Certificate			×
Name *	IND		
Password			
Certificate *	Browse	C:\fakepath\ind.example.com_ 3.p12	<b>×</b>
	Upload	Cancel	

#### Passaggio 9. Configurare Policy Server su IND

Selezionare **Impostazioni > Server dei criteri**, quindi fare clic su **Nuovo**. Immettere l'FQDN ISE e l'indirizzo IP di ISE pxGrid Node.

	R Settings > Policy Servers				<b>≜</b> ∘ ⊡
< Back to Servers			New Server		
	Protocols*				
	Host Name* ISE24-1ek.example.com	IP Address • 10.62.145.140		Description	0
		E	Zancel Save		

#### Passaggio 10. Configurare l'integrazione pxGrid su IND

Passare a **Impostazioni > pxGrid** e abilitare l'integrazione di pxGrid. Fare clic sull'interruttore. Immettere il Nome nodo; questo Nome host è il nome del client pxGrid su ISE. Selezionare l'ISE configurata in precedenza dal menu a discesa nel campo Server 1. Fare clic su **Register** (Registra).

uludu l cisco d	NDUSTRIAL IETWORK DIRECTOR	Settings > pxGrid						۰ 🌲	Û	? ·	۰ 🛦
i⊟ Settings				ş	xGrid						
Trusted Certificates	Enable pxGrid- Settin Download .pem I Connect Using I	ngs ND certificate the Existing Node Node									
	ISE Server Node Name* IND		0	Server 1* ISE24-1ek.example.com		• 0	Server 2 Solect a server				• 0
				Cancel	Register						

**Nota:** I passaggi da 11 a 12 possono essere ignorati se l'impostazione Approva automaticamente nuovi account basati su certificato è abilitata su ISE.

Al termine della registrazione, viene visualizzato il seguente messaggio:

V Message		×
pxGrid Node Approval Pending on	the pxGrid Server	
	ОК	

#### Passaggio 11. Approvazione di IND su ISE

Selezionare **Amministrazione > pxGrid Services > All Clients**. Aprire il menu a discesa Approvazione totale in sospeso(1). Fare clic su **Approva tutto**.

dentity Services Engine Ho	ome	Operations     Policy	- Administration	Work Centers
System      Identity Management     Netrice	etwork Resources	e Portal Management pxGrid	Services Feed Service	▶ Threat Centric NAC
All Clients Web Clients Capabilities	Live Log Settings	Certificates Permissions		
🖌 Enable 🖉 Disable 📿 Approve 😝 Group	Decline 🛞 Delete 👻	Sefresh Total Pending Approv	val(1) 🔻	
Client Name	Client Description	Capi Approve All	Status	Client Group(s)
□ ► ise-fanout-ise24-1ek		Capabilities(U Pub, U Su	Online (XMF	P) Internal
□ ► ise-pubsub-ise24-1ek		Capabilities(0 Pub, 0 Su	b) Online (XMF	P) Internal
□ ► ise-pubsub-ise24-2ek		Capabilities(0 Pub, 0 Su	b) Online (XMF	P) Internal
□ ► ise-fanout-ise24-2ek		Capabilities(0 Pub, 0 Su	b) Online (XMF	P) Internal
□ ► ise-admin-ise24-3ek		Capabilities(0 Pub, 0 Su	b) Online (XMF	P) Internal
□ ► ise-mnt-ise24-2ek		Capabilities(2 Pub, 1 Su	b) Online (XMF	P) Internal
□ ► ise-mnt-ise24-1ek		Capabilities(2 Pub, 1 Su	b) Online (XMF	P) Internal
□ ► ise-bridge-ise24-1ek		Capabilities(0 Pub, 4 Su	b) Online (XMF	P) Internal
□ ▶ ise-admin-ise24-1ek		Capabilities(5 Pub, 2 Su	b) Online (XMF	P) Internal
□ ► ise-admin-ise24-2ek		Capabilities(1 Pub, 1 Su	b) Online (XMF	P) Internal
□ ► ind		Capabilities(0 Pub, 0 Su	b) Pending	

Passaggio 12. Attivare il servizio pxGrid su IND

Passare a Impostazioni > pxGrid. Fare clic su Activate.

·ili·ili· cisco	INDUSTRIAL NETWORK DIRECTOR	Settings	> p	xGrid								
Settings										I	oxGrid	
Trusted Certificates	Enable pxGrid- Activate	3										
	ISE Server											
	Download .pem	IND certificate										
	Node Name*						Server 1					
	IND						ISE24	-1ek.exam	nple.com			
										Disable	e Activate	

Al termine dell'attivazione, viene visualizzato il seguente messaggio:

Message	×	
pxGrid Service is active		
ОК		

# Verifica

#### Verifica ISE

Selezionare **Amministrazione > pxGrid Services > All Clients**. Si prevede che il client IND venga visualizzato come non in linea (XMPP) in Tutti i client, IND utilizza pxGrid versione 2.

cisco	Identity Services Engine	Iome	Operations     Polic	Administration	▶ Work Centers
In System System	tem  Identity Management I	Network Resources	ce Portal Management pxG	id Services    Feed Services	vice
All C	lients Web Clients Capabilitie	es Live Log Settings	Certificates Permissions		
🖌 Enal	ble 🧭 Disable 😪 Approve 😝 Gro	up 👎 Decline  🐼 Delete 👻	🛞 Refresh Total Pending App	oroval(0) 👻	
	Client Name	Client Description	Capabilities	Status	Client Group(s)
	ise-fanout-ise24-1ek		Capabilities(0 Pub, 0	Sub) Online (X	MPP) Internal
►►	ise-pubsub-ise24-1ek Client Name:	Not Sortable	Capabilities(0 Pub, 0	Sub) Online (X	MPP) Internal
	ise-pubsub-ise24-2ek		Capabilities(0 Pub, 0	Sub) Online (X	MPP) Internal
►	ise-fanout-ise24-2ek		Capabilities(0 Pub, 0	Sub) Online (X	MPP) Internal
	ise-admin-ise24-3ek		Capabilities(0 Pub, 0	Sub) Online (X	MPP) Internal
	ise-mnt-ise24-2ek		Capabilities(2 Pub, 1	Sub) Online (X	MPP) Internal
	ise-mnt-ise24-1ek		Capabilities(2 Pub, 1	Sub) Online (X	MPP) Internal
	ise-bridge-ise24-1ek		Capabilities(0 Pub, 4	Sub) Online (X	MPP) Internal
	ise-admin-ise24-1ek		Capabilities(5 Pub, 2	Sub) Online (X	MPP) Internal
	ise-admin-ise24-2ek		Capabilities(1 Pub, 1	Sub) Online (X	MPP) Internal
	ind		Capabilities(0 Pub, 0	Sub) Offline (>	(MPP)

Fare clic su **Client Web**, verificare che il client IND abbia uno stato ON e che /topic/com.cisco.endoint.asset faccia parte di Subscription.

cise	ly Ident	ty Services Engi	ine Home	Conti	ext Visibility	<ul> <li>Operations</li> </ul>	Policy	→ Administra	ation 🕨 🔪	Vork Centers					
•	System	<ul> <li>Identity Manage</li> </ul>	ment • Netwo	ork Resource	s I Devic	e Portal Manager	nent pxGrid \$	Services + F	eed Service	<ul> <li>Threat Cent</li> </ul>	ric NAC				
,	Il Clients	Web Clients	Capabilities	Live Log	Settings	Certificates	Permissions								
												Rows/Page 25	• 1 0	/1 (	Go 12 Total Rows
2	Refresh														🔻 Filter 🕶 🗘 🗸
	Clien	t Name	Connect To	Se	ssion Id	Certificat	е	Subscripti	ions		Publications		IP Address	Status	Start time
×	Clier	it Name		•									IP Address		•
	IND		ISE24-1ek	ISE	24-1ek:181	CN=WIN2	012-AAA,						10.62.145.130	ON	2019-05-23 08:27
	ise-m	nt-ise24-1ek	ISE24-1ek	ISE	24-1ek:182	CN=ISE24	l-1ek.exa	/topic/com.o	cisco.ise.ses	ion.internal			10.62.145.140	ON	2019-05-23 08:28
	ise-fa	nout-ise24-1ek	ISE24-1ek	ISE	24-1ek:183	CN=ISE24	l-1ek.exa	/topic/distrit	buted		/topic/distributed	I.	10.62.145.140	ON	2019-05-23 08:28
	ise-ad	Imin-ise24-1ek	ISE24-1ek	ISE	24-1ek:184	CN=ISE24	l-1ek.exa	/topic/com.o	cisco.endpoir	t.asset			10.62.145.140	OFF 🕢	2019-05-23 08:28
	ise-m	nt-ise24-2ek	ISE24-1ek	ISE	24-1ek:185	No Certific	ate	/topic/com.e	cisco.ise.ses	ion.internal	/topic/com.cisco	ise.session.internal	10.62.145.141	OFF 🕢	2019-05-23 08:59
	ise-ad	Imin-ise24-2ek	ISE24-1ek	ISE	24-1ek:188	No Certific	ate						10.62.145.141	ON	2019-05-23 09:30
	ise-br	idge-ise24-1ek	ISE24-1ek	ISE	24-1ek:189	CN=ISE24	l-1ek.exa						127.0.0.1	OFF 🕢	2019-05-23 09:30
	ise-fa	nout-ise24-1ek	ISE24-1ek	ISE	24-1ek:190	CN=ISE24	l-1ek.exa	/topic/wildca	ard				127.0.0.1	ON	2019-05-23 09:30
	ise-m	nt-ise24-2ek	ISE24-1ek	ISE	24-1ek:191	No Certific	ate 💠	/topic/com.o	cisco.ise.sess	ion.internal	/topic/com.cisco	ise.session.internal	10.62.145.141	ON	2019-05-23 09:43
	ise-ad	Imin-ise24-1ek	ISE24-1ek	ISE	24-1ek:192	CN=ISE24	l-1ek.exa	/topic/com.o	cisco.endpoir	t.asset			10.62.145.140	ON	2019-05-23 09:43
	ise-br	idge-ise24-1ek	ISE24-1ek	ISE	24-1ek:193	CN=ISE24	l-1ek.exa						127.0.0.1	OFF 🕢	2019-05-23 10:04
	ise-br	idge-ise24-1ek	ISE24-1ek	ISE	24-1ek:194	CN=ISE24	l-1ek.exa						127.0.0.1	ON	2019-05-23 10:09

#### Verifica IND

Lo stato di transizione di IND deve essere In Sync. Questo è fatto se il download in blocco è riuscito su ISE, in caso contrario IND sarà bloccato in stato Out of Sync.

cisco	INDUSTRIAL NETWORK DIRE	CTOR Settings > pxGrid									۰ 🌲	Ċ	0 ·	1.
Eetings						px	Grid							
Trusted Centricates	Cisco Pia Services	form Exchange Grid (zxGrid) is an open, scalable ingine (ISE) pxGrid controller. This information can	data-sharing and threat then be leveraged by	control platform that all upstream security syste	ows seamless integration ms to monitor security, det	between multivendor identity, net tect threats, and set network polic	work, security and asset manageme y. Learn more here.	ent systems. Enabling t	the feature below activate	the sharing of endpoint asse	ts discovered by	this system w	vith a Cisco Ide	entity
	Downi	bad .pem IND certificate												
	ISE	Server												
	Node	Name *			Server 1*				Server 2					
	IND				ISE24-1ek.ex	ample.com								
	Stati	stics												
			Sync. Status	In Sync				Last Sy	nc. Status Probe Time	2019-05-23 10:19:16				
		Number of Assets Shared via	Last Bulk Request	2				L	ast Bulk Request Time	2019-05-23 08:29:14				
		Las	t Update Operation	Update					Last Update Time	2019-05-22 20:17:36				
		Total p	xGrid Asset Count	2										

## Risoluzione dei problemi

#### Stato sincronizzazione bloccato in non sincronizzato su IND

La transizione da Out of Sync a In Sync si verifica se il download bulk ha esito positivo su ISE. IND application.log di seguito.

```
2019-05-22 22:09:06,902:INFO:qtp281049997-53444:PxgridConfigMgr:: Pxgrid Statistics Start:: Bulk
Request : bulkReqAssetCount:2 add: false
2019-05-22 22:09:06,902:INFO:qtp281049997-53444:PxgridConfigMgr:: Pxgrid Statistics updated::
Bulk Request : AssetCount:2
2019-05-22 22:09:06,902:INFO:qtp281049997-53444:PxgridConfigMgr:: Sync Status transition to
IN_SYNC
2019-05-22 22:09:06,918:INFO:qtp281049997-53444:PxGridServiceRestController:: getAssets
Completed
```

Èfondamentale che ISE sia in grado di risolvere il nome host IND condiviso da IND. In caso contrario ISE non può eseguire il download in blocco e IND non passerà mai allo stato In sincrono. È possibile visualizzare la seguente eccezione nel file profiler.log se il download di massa non riesce (WIN2012-AAA non è stato risolvibile da ISE). Per attivare il download in blocco è possibile deselezionare e controllare il probe pxGrid su PSN.

```
2019-04-30 13:59:50,708 INFO [ProfilerINDSubscriberPoller-60-thread-1][]
cisco.profiler.infrastructure.probemgr.INDSubscriber -::- New services are: []
2019-04-30 13:59:50,714 INFO [ProfilerINDSubscriberPoller-60-thread-1][]
cisco.profiler.infrastructure.probemgr.INDSubscriberPoller-60-thread-1][]
cisco.profiler.infrastructure.probemgr.INDSubscriber -::- REQUEST
BODY{"offset":"0","limit":"500"}
2019-04-30 13:59:50,716 ERROR [ProfilerINDSubscriberPoller-60-thread-1][]
cisco.profiler.infrastructure.probemgr.INDSubscriberPoller-60-thread-1][]
cisco.profiler.infrastructure.probemgr.INDSubscriberPoller-60-thread-1][]
cisco.profiler.infrastructure.probemgr.INDSubscriber -::- Unable to get sync statusWIN2012-
AAA:WIN2012-AAA
java.net.UnknownHostException: WIN2012-AAA
at java.net.AbstractPlainSocketImpl.connect(AbstractPlainSocketImpl.java:184)
at java.net.SocksSocketImpl.connect(SocksSocketImpl.java:392)
at java.net.Socket.connect(Socket.java:589)
at sun.security.ssl.SSLSocketImpl.connect(SSLSocketImpl.java:673)
```

```
at sun.security.ssl.BaseSSLSocketImpl.connect(BaseSSLSocketImpl.java:173)
at sun.net.NetworkClient.doConnect(NetworkClient.java:180)
at sun.net.www.http.HttpClient.openServer(HttpClient.java:463)
at sun.net.www.http.HttpClient.openServer(HttpClient.java:558)
at sun.net.www.protocol.https.HttpsClient.<init>(HttpsClient.java:264)
at sun.net.www.protocol.https.HttpsClient.New(HttpsClient.java:367)
sun.net.www.protocol.https.AbstractDelegateHttpsURLConnection.getNewHttpClient(AbstractDelegateH
ttpsURLConnection.java:191)
at sun.net.www.protocol.http.HttpURLConnection.plainConnect0(HttpURLConnection.java:1156)
at sun.net.www.protocol.http.HttpURLConnection.plainConnect(HttpURLConnection.java:1050)
at
\verb+sun.net.www.protocol.https.AbstractDelegateHttpsURLConnection.connect(AbstractDelegateHttpsURLConnection.connect(AbstractDelegateHttpsURLConnection.connect(AbstractDelegateHttpsURLConnection.connect(AbstractDelegateHttpsURLConnection.connect(AbstractDelegateHttpsURLConnection.connect(AbstractDelegateHttpsURLConnection.connect(AbstractDelegateHttpsURLConnection.connect(AbstractDelegateHttpsURLConnection.connect(AbstractDelegateHttpsURLConnection.connect(AbstractDelegateHttpsURLConnection.connect(AbstractDelegateHttpsURLConnection.connect(AbstractDelegateHttpsURLConnection.connect(AbstractDelegateHttpsURLConnection.connect(AbstractDelegateHttpsURLConnection.connect(AbstractDelegateHttpsURLConnection.connect(AbstractDelegateHttpsURLConnection.connect(AbstractDelegateHttpsURLConnection.connect(AbstractDelegateHttpsURLConnection.connect(AbstractDelegateHttpsURLConnection.connect(AbstractDelegateHttpsURLConnection.connect(AbstractDelegateHttpsURLConnection.connect(AbstractDelegateHttpsURLConnection.connect(AbstractDelegateHttpsURLConnection.connect(AbstractDelegateHttpsURLConnection.connect(AbstractDelegateHttpsURLConnection.connect(AbstractDelegateHttpsURLConnection.connection.connect(AbstractDelegateHttpsURLConnection.connection.connection.connection.connection.connection.connection.connection.connection.connection.connection.connection.connection.connection.connection.connection.connection.connection.connection.connection.connection.connection.connection.connection.connection.connection.connection.connection.connection.connection.connection.connection.connection.connection.connection.connection.connection.connection.connection.connection.connection.connection.connection.connection.connection.connection.connection.connection.connection.connection.connection.connection.connection.connection.connection.connection.connection.connection.connection.connection.connection.connection.connection.connection.connection.connection.connection.connection.connection.connection.connection.connection.connection.connection.conne
nnection.java:177)
at sun.net.www.protocol.http.HttpURLConnection.getOutputStream0(HttpURLConnection.java:1334)
at sun.net.www.protocol.http.HttpURLConnection.getOutputStream(HttpURLConnection.java:1309)
at
sun.net.www.protocol.https.HttpsURLConnectionImpl.getOutputStream(HttpsURLConnectionImpl.java:25
9)
at com.cisco.profiler.infrastructure.probemgr.INDSubscriber.getRequest(INDSubscriber.java:362)
     com.cisco.profiler.infrastructure.probemgr.INDSubscriber.isInSync(INDSubscriber.java:500)
at
at
com.cisco.profiler.infrastructure.probemgr.INDSubscriber.populateIOTServiceList(INDSubscriber.ja
va:462)
at
com.cisco.profiler.infrastructure.probemgr.INDSubscriber$WorkerThread.run(INDSubscriber.java:441
)
at java.util.concurrent.Executors$RunnableAdapter.call(Executors.java:511)
at java.util.concurrent.FutureTask.runAndReset(FutureTask.java:308)
at
java.util.concurrent.ScheduledThreadPoolExecutor$ScheduledFutureTask.access$301(ScheduledThreadP
oolExecutor.java:180)
at
java.util.concurrent.ScheduledThreadPoolExecutor$ScheduledFutureTask.run(ScheduledThreadPoolExec
utor.java:294)
at java.util.concurrent.ThreadPoolExecutor.runWorker(ThreadPoolExecutor.java:1149)
at java.util.concurrent.ThreadPoolExecutor$Worker.run(ThreadPoolExecutor.java:624)
at java.lang.Thread.run(Thread.java:748)
```

#### Non tutti gli endpoint sono condivisi con ISE

Gli endpoint su IND vengono condivisi con ISE solo se il flag pxGrid Asset è Yes, anche l'indirizzo MAC dovrebbe essere disponibile, altrimenti ISE non ha dati sufficienti per creare un endpoint.

cisco	NDUSTRIAL NETWORK DIRECTOR	Operate > Inventory					٩	Û	<b>@</b> -	<b>1</b> -
ST Overview	< Back			WIN2012-CHILD						
				DEVICE OVERVIEW						
		Name	WIN2012-CHILD		Device Type	Server				
		IP Address	10.62.145.131		Protocol	NetBIOS				
		MAC Address	00:50:56:b6:46:87		Group	Root				
		Vendor	VMware		Connected to					
		pxGrid Asset	Yes		Tag(s)	SEC_TAG2				

#### assetTag e AssetGroup non sono disponibili su ISE

Se assetTag only non è disponibile, è possibile che venga utilizzato un tipo di TAG errato. Quando

si aggiorna l'endpoint, è necessario utilizzare il tag di protezione (non il tag regolare).

socialed Device Tags		×
No Tags Associated with this device		
Add Regular Tag		
Select a tag	-	
Add Security Tag Select a tag SEC_TAG1 SEC TAG2		

Se AssetTag e AssetGroup non sono disponibili, è possibile che esistano più motivi

1. Il criterio di profilatura non è configurato utilizzando gli attributi custom (vedere i passi 1-3 nella sezione Configurazioni del documento)

2. A causa del difetto <u>CSCvn66106</u> Filtro attributi EndPoint: deve essere disabilitato. In caso contrario, vengono filtrati gli attributi personalizzati dal classificatore. Il seguente registro è disponibile nel file profiler.log.

```
2019-05-22 11:20:11,796 DEBUG [PersistentWorker-8-18-thread-1][] com.cisco.profiler.im.EndPoint
-:Profiling:- filtered custom attributes are:{assetGroup=Root, assetTag=SEC_TAG2, b310a420-78a5-
11e9-a189-9ac8f4107843=Root, b8e73d50-78a5-11e9-a189-9ac8f4107843=SEC_TAG2}
```