# ISE 2.4 pxGrid IND 1.6.1統合の設定

## 内容

概要 前提条件 要件 使用するコンポーネント 設定 高レベル フロー図 設定 ステップ1:ISEでのエンドポイントカスタム属性の設定 ステップ2:カスタム属性を使用したプロファイラポリシーの設定 ステップ3:プロファイル適用のカスタム属性の有効化 ステップ4:IND ID証明書のエクスポート <u>ステップ5:ISE信頼ストアへのIND ID証明書のアップ</u>ロード ステップ6:INDの証明書の生成 ステップ7:PKCS12形式で<u>証明書チェーンをダウンロードする</u> ステップ8:INDでの証明書チェーンのアップロード ステップ9:INDでのポリシーサーバの設定 ステップ10:INDでのpxGrid統合の設定 ステップ11:ISEでのINDの承認 ステップ12:INDでpxGridサービスをアクティブにする 確認 ISEの検証 INDの検証 トラブルシュート INDで同期ステータスがOut of Syncのままになる すべてのエンドポイントがISEと共有されているわけではありません assetTagおよびAssetGroupはISEでは使用できません

## 概要

このドキュメントでは、pxGrid(Platform Exchange Grid)を介したIdentity Services Engine(ISE)2.4およびIndustrial Network Director 1.6.1-4統合の設定とトラブルシューティングの 方法について説明します。 Cisco INDはpxGridにパブリッシャとして登録され、エンドポイント 属性に関する情報をISEに公開してIOTASSET Dictionaryを作成します。

## 前提条件

### 要件

次の項目に関する基本的な知識が推奨されます。

- Cisco Identity Service Engine
- Cisco Industrial Network Director

## 使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- Cisco Identity Service Engineバージョン2.4 p6
- Industrial Network Director 1.6.1-4

## 設定

## 高レベル フロー図



#### 1. ISE pxGridノードのpxGridバージョン2を介してINDがISEに登録されます。 IND(application.log)からの対応するログ:

```
2019-05-22 14:31:17,770:INFO:qtp281049997-52711:PxgridPublisher:: Connect start
2019-05-22 14:31:17,770:INFO:qtp281049997-52711:PxgridPublisher:: Hostname:WIN2012-AAA
IpAddress:10.62.145.130
2019-05-22 14:31:17,770:INFO:qtp281049997-52711:PxgridPublisher:: pxGrid
RestBaseUrl:https://WIN2012-AAA:8910/pxgrid/ind/asset/
2019-05-22 14:31:17,770:INFO:qtp281049997-52711:PxgridController:: Send Request ServiceRegister
invoked with pxGridServer(s) [ISE24-lek.example.com]
2019-05-22 14:31:17,770:INFO:qtp281049997-52711:PxgridController:: Sending ServiceRegister
request to pxGridServer ISE24-lek.example.com
2019-05-22 14:31:17,786:INFO: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:qtp281049997-52711:PxgridController:: Response={"id":"76d4abaf-
9efd-4c68-a046-79e049564902", "reregisterTimeMillis": "300000"}
2019-05-22 14:31:17,911:INFO:qtp281049997-52711:PxgridController:: Send Request ServiceLookup
invoked with pxGridServer(s) [ISE24-1ek.example.com]
```

2019-05-22 14:31:17,911:INFO:qtp281049997-52711:PxqridController:: Sending ServiceLookup request to pxGridServer ISE24-1ek.example.com 2019-05-22 14:31:17,911:INFO:qtp281049997-52711: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-lek.example.com:8910/pxgrid/ise/pubsub"}}] 2019-05-22 14:31:17,911:INFO:qtp281049997-52711:PxqridPublisher:: wsUrl=wss://ISE24lek.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-lek.example.com] 2019-05-22 14:31:17,911:INFO:qtp281049997-52711:PxgridController:: Sending AccessSecret request to pxGridServer ISE24-lek.example.com 2019-05-22 14:31:17,926:INFO:qtp281049997-52711:PxgridController:: Request={"peerNodeName":"isepubsub-ise24-lek"} 2019-05-22 14:31:17,926:INFO:qtp281049997-52711:PxgridController:: Access Secret recieved 2019-05-22 14:31:17,926:INFO:qtp281049997-52711:PxgridPublisher:: Client created ログに示されているように、INDはassetTopicに登録されています

2. pxgridプローブを有効にしたISE PSNは、既存のpxGridアセット(profiler.log)を一括ダウンロー ドします。

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. INDで新しいエンドポイントが検出されます(エンドポイントはプロトコルで検出する必要が あります。検出しない場合、エンドポイントはpxGrid資産として識別されず、ISEとpxGridを介し て共有されません)。

.ili.ili. cisco	INDUSTRIAL NETWORK DIRECTOR	Operate	> Inventor	,			
0verview	< 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はこの情報をISE pxGridノードに公開します

#### 5. pxGridプローブ経由のPSNは、次のデータ(profiler.log)を受信します。

```
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:92
2019-05-22 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
6.コンテキストの可視性が正しいデータで更新される
```

lle Ide	ntity Services	Engine	Home	✓ Conte	ext Visibility	<ul> <li>Operatio</li> </ul>	ns	Administration	Work Centers
ndpoints	Users N	etwork Devices	Appl	ication					
00:50	):56:9C:3F	:92 G	56-90-3	₩ F-92					
Username: Endpoint Profile: IOT_DEVICE2 Current IP Address: 10.62.145.72 Location:				5.72					
۲	Applications	Attributes	6	Authenticat	ion T	Threats	Vulnerabilities		
Genera	I Attributes								
Description									
Static Assignment false									
Endpoint Policy IOT_DEVICE2									
Static Group Assignment false									
Identity	Group Assignm	ent Profiled							
Custon	n Attributes								
								٦	Filter - 🌣 -
	Attribute Na	ame		A	ttribute Val	ue			
×	Attribute Na	me			Attribute Valu	е			
	assetGroup			R	oot				
	LogicalProfile	9							
	assetTag			S	EC_TAG2				
Other A	Attributor								
other P	-unibules								

## 設定

**注**: Context VisibilityでassetGroupとassetTagを表示したい場合でも、ステップ1 ~ 3が必要です

#### ステップ1:ISEでのエンドポイントカスタム属性の設定

[Administration] > [Identity Management] > [Settings] > [Endpoint Custom Attributes]に移動します 。次の図に従って、カスタムアトリビュート(assetGroupおよびassetTag)を設定します。

cisco Iden	tity Services Engine	Home   Contex	t Visibility	Policy	Administration	Work Centers
<ul> <li>System</li> </ul>	✓ Identity Management	<ul> <li>Network Resources</li> </ul>	Device Portal Management	t pxGrid Servic	es + Feed Ser	vice
Identities	Groups External Ide	ntity Sources Identity	Source Sequences - Settings	5		
	(	3				
User Custom	Attributes	Endpoint Cus	stom Attributes			
User Authent	ication Settings					
Endpoint Pur	ge	Endpoint Att	ributes (for reference)			
Endpoint Cus	stom Attributes	Mandatory	Attribute Name		Data T	уре
			PostureApplicable		STRING	)
			EndPointPolicy		STRING	3
			AnomalousBehaviour		STRING	3
			OperatingSystem		STRING	3
			BYODRegistration		STRING	3
			PortalUser		STRING	3
			LastAUPAcceptanceHours		INT	
			LogicalProfile		STRING	3
		Endpoint Cus	stom Attributes			
			Attribute name		Туре	
		assetGroup			String •	]-
		assetTag			String •	- •
					Reset	Save

## ステップ2:カスタム属性を使用したプロファイラポリシーの設定

[Work Centers] > [Profiler] > [Profiling Policies] に移動します。[Add] をクリックします。次の図の ようにプロファイラポリシーを設定します。

dentity Services Engine	Home >	Context Visibility	<ul> <li>Operations</li> </ul>	Policy      Ad	ministration 🗸	Vork Centers					
Network Access     Guest Access	TrustSec	► BYOD ▼ Profil	Posture	Device Administra	ation + PassiveID						
Overview Ext Id Sources Network De	vices Endpoir	nt Classification No	de Config Feeds	Manual Scans	Policy Elements	Profiling Policies	Policy Sets	Troubleshoot	Reports	<ul> <li>Settings</li> </ul>	Dictionaries

Profiling	Profiler Policy List > IOT_DEVICE1				
م م	Profiler Policy				
⟨- + E +	* Name	IOT_DEVICE1	Description		
Profiling Policies	Policy Enabled	0			
	* Minimum Certainty Factor	20	Valid Range 1 to 6553	5)	
	* Exception Action	NONE -			
	* Network Scan (NMAP) Action	NONE *			
	Create an Identity Group for the policy	Yes, create matching Identity Gr	oup		
		No, use existing Identity Group I	hierarchy		
	* Parent Policy	NONE *			
	* Associated CoA Type	Global Settings v			
	System Type	Administrator Created			
	Rules				
	If Condition CUSTOMATTRIBUTE_	assetTag_EQUALS 🗢 The	en Certainty Factor Incre	eases v 20	\$\$ v
	Save Rese Condition Name	Expression CUSTOMATTRIB	C EQUALS -	SEC_TAG1	

#### ステップ3:プロファイル適用のカスタム属性の有効化

[ワークセン**ター] > [プロファイラ] > [設定] > [プロファイラ設定]に移動します**。確認 プロファイ ル適用のカスタム属性の有効化 チェックボックスがオンになっています。

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	rices Endpoint Classification Node Config Feeds + Manual Scans + Policy Elements Profiling Policies Policy Sets + Troubleshoot Reports - Settings Dictionaries
Profiler Settings	Profiler Configuration
Fromer Setungs	
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: Denabled
	Enable Anomalous Behaviour Detection:   Enabled ()
	Enable Anomalous Behaviour Enforcement:   Enabled
	Enable Custom Attribute for Profiling Enforcement: 🥑 Enabled
	Save Reset

#### ステップ4:IND ID証明書のエクスポート

[**Settings**] > [pxGrid]**に移動します**。[**Download .pem IND certificate]をクリックします**。この証明 書はpxGridの登録時に使用されるため、ISEはこれを信頼する必要があります。

Cisco Platform Exchange Grid (pxGirld) is an open, scalable data-sharing and threat control platform that allows seamless integration between multivendor identity, network, security and asset management systems. Enabling the feature below activates the sharing of endpoint assets discovered by this system with a services Engine (ISE) pxGirld controline. This information can then be leveraged by upsteam security systems to monitor security, detect threas, and set network policy. Learn more here.	
Cisco Platform Exchange Grid (pxGrid) is an open, scalable data-sharing and threat control platform that allows seamless integration between multivendor identity, network, security and asset management systems. Enabling the feature below activates the sharing of endpoint assets discovered by this system with a feature below. Scalar for the security, detect threats, and set network policy. Learn more here.	
	Cisco Identity
Download .pem IND certificate	

#### ステップ5:ISE信頼ストアへのIND ID証明書のアップロード

[Administration] > [Certificates] > [Certificate Management] > [Trusted Certificates]に移動します。 [インポート]をク**リックします**。[Browse]をクリックし、ステップ3から[IND certificate]を選択し ます。[Submit]をクリックします。

dentity 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	tes  ► Logging  ► Maintenance Upgrade  ► Backup & Restore  ► Admin Access  ► Settings	
Ø		
- Certificate Management	Import a new Certificate into the Certificate Store	
System Certificates	* Certificate File Browse ind(1).pem	
Trusted Certificates	Friendly Name	(i)
OCSP Client Profile		V
Certificate Signing Requests	Trusted For: (j)	
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	

#### ステップ6:INDの証明書の生成

INDは、ISE CAが発行するクライアント証明書を使用しません。代わりに、IND信頼ストアを入 力することを目標としているため、ISEがpxGrid証明書を送信すると(TLS交換中)、INDによっ て信頼されます。

[Administration] > [pxGrid Services] > [Certificates]に移動します。下の図に従ってフィールドに入 力します。ISE CAの目的はID証明書を発行することであるため、CNフィールドは必須です。 INDのFQDNを入力するのが理想的ですが、ID証明書はINDによって使用されないため、CNフィ ールドの値は重要ではありません。

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	

ステップ7:PKCS12形式で証明書チェーンをダウンロードする

• • •	Opening 1558534704560_cert.zip							
You have chosen to open:								
1558534704560_cert.zip								
which is: ZIP archive								
from: https	from: https://10.62.145.140							
What should Firefox do with this file?								
Open with	Archive Utility (default)							
OSave File								
Do this automatically for files like this from now on.								
	Cancel OK							

### ステップ8:INDでの証明書チェーンのアップロード

[**Settings**] > [pxGrid] > [**Trusted Certificates]に移動します**。[New]をクリ**ックします**。[Name]を入 力します(チェーンはINDでこの名前で表示されます)。 Passwordはステップ1のパスワードで す。

Upload Trusted Certificate		×
Name *	IND	
Password		
Certificate *	Browse C:\fakepath\ind.example.com_3.p12	×
	Upload Cancel	

#### ステップ9:INDでのポリシーサーバの設定

[**Settings**] > [**Policy Servers**]**に移動し、[New**]をクリ**ックします**。ISE pxGridノードのISE FQDNと IPアドレスを入力します。

.11.11. INDUSTRIAL cisco NETWORK DIRECTO	R Settings > Policy Servers		¢• 🗓
< Back to Servers		New Server	
	Protocols*		
	Host Name* ISE24-1ek.example.com	IP Address         Description           0         10.62.145.140	0
		Cancel Save	

#### ステップ10:INDでのpxGrid統合の設定

[**Settings**] > [pxGrid]に**移動し、pxGrid**統合を有効にします。トグルボタンをクリックします。ノ ード名を入力します。このホスト名は、ISE上のpxGridクライアントの名前です。[Server 1]フィ ールドのドロップダウンメニューから、先に設定したISEを選択します。[登録]をクリ**ックします** 。

uluulu cisco	INDUSTRIAL NETWORK DIRECTOR	Settings >	pxGrid							۰ 🌲	Û	<b>@</b> ·	٤.
i⊟ Settings						pxGrid							
Trusted Certificates	Enable pxGrid- Setti Download .pem Connect Using Register a New	IND certificate the Existing Node Node											
	ISE Server Node Name* IND			0	Server 1* ISE24-1ek.example.com	Cancel Registr	И	• 0	Server 2 Select a server				• 0

**注**: ISEで[Automatically approve new certificate-based accounts]設定が有効になっている場合、ステップ11 ~ 12は無視される場合があります。

登録が成功すると、INDに次のメッセージが表示されます。

Message		×
pxGrid Node Approval Pending	on the pxGrid Server	
	ОК	

### ステップ11:ISEでのINDの承認

[**Administration] > [pxGrid Services] > [All Clients]に移動します**。[承認待ちの合計(1)(Total Pending Approval(1))]ドロップダウンメニューを開きます。[すべて認**可]をクリックします**。

dentity Services Engine	Home	Operations     Policy	✓ Administration					
System     Identity Management	Network Resources     Dev	ice Portal Management pxGrid Se	rvices + Feed Service + Threat C	entric NAC				
All Clients Web Clients Capabilities Live Log Settings Certificates Permissions								
🖌 Enable 🖉 Disable 😪 Approve 🌘	) Group 👎 Decline  🔞 Delete 👻	Sefresh Total Pending Approval	(1) 🔻					
Client Name	Client Description	Capi Approve All	Status	Client Group(s)				
□ ► ise-fanout-ise24-1ek		Capabilities(U Pub, U Sub)	Online (XMPP)	Internal				
□ ► ise-pubsub-ise24-1ek		Capabilities(0 Pub, 0 Sub)	Online (XMPP)	Internal				
☐ ▶ ise-pubsub-ise24-2ek		Capabilities(0 Pub, 0 Sub)	Online (XMPP)	Internal				
□ ► ise-fanout-ise24-2ek		Capabilities(0 Pub, 0 Sub)	Online (XMPP)	Internal				
□ ► ise-admin-ise24-3ek		Capabilities(0 Pub, 0 Sub)	Online (XMPP)	Internal				
□ ► ise-mnt-ise24-2ek		Capabilities(2 Pub, 1 Sub)	Online (XMPP)	Internal				
□ ▶ ise-mnt-ise24-1ek		Capabilities(2 Pub, 1 Sub)	Online (XMPP)	Internal				
□ ► ise-bridge-ise24-1ek		Capabilities(0 Pub, 4 Sub)	Online (XMPP)	Internal				
□ ► ise-admin-ise24-1ek		Capabilities(5 Pub, 2 Sub)	Online (XMPP)	Internal				
□ ► ise-admin-ise24-2ek		Capabilities(1 Pub, 1 Sub)	Online (XMPP)	Internal				
□ ▶ ind		Capabilities(0 Pub, 0 Sub)	Pending					

ステップ12:INDでpxGridサービスをアクティブにする

[Settings] > [pxGrid]に移動します。[Activate]をクリックします。

INDUSTRIAL NETWORK DIRECTOR	Settings >	pxGrid									
								px0	Grid		
Enable pxGrid- Activa	e										
ISE Server											
Download .pem	IND certificate										
Node Name*						Server 1*					
IND						ISE24-1ek.	.example.com				
								Disable	Activate		
	INDUSTRIAL NETWORK DIRECTOR	INDUSTRIAL NETWORK DIRECTOR     Settings       Enable pxGrid- Activate       ISE Server       Download .pem IND certificate       Node Name*       IND	INDUSTRIAL NETWORK DIRECTOR     Settings > pxGrid       Enable pxGrid- Activate       ISE Server       Download .pem IND certificate       Node Name*       IND	INDUSTRIAL NETWORK DIRECTOR     Settings     pxGrid       Enable pxGrid- Activate     ISE Server       Download .pem IND certificate       Node Name*       IND	NDUSTRIAL NETWORK DIRECTOR     Settings > pxGrid       Enable pxGrid- Activate       ISE Server       Download .pem IND certificate       Node Name*       IND	NDUSTRIAL NETWORK DIRECTOR     Settings > pxGrid	NDUSTRIAL NETWORK DIRECTOR     Settings     pxGrid       Enable pxGrid- Activate     ISE Server       Download .pem IND certificate       Node Name*       Server 1*       IND	NUUSTRIAL NETWORK DIRECTOR     Settings > pxGrid         Enable pxGrid- Activate         ISE Server         Download .pem IND certificate   Node Name* ISE24-1ek.example.com	NUDUSTRIAL NETWORK DIRECTOR       Settings ) pxGrid         pxl         Image: setting in the pxGrid-Activate         Ise Server         Download.pem IND certificate         Node Name*         Server 1*         IND         ISE 24-1ek.example.com         Disable	NUDUSTRAL pxGrid pxGrid Enable pxGrid-Activate ISE Server Download .pem IND certificate Node Name* IND ISE24-1ek.example.com Disable Activate	NUMENTRAL NETWORK DIRECTOR       Settings > pxGrid         pxGrid       pxGrid         Enable pxGrid - Activate       ISE Server         Download .pem IND certificate       ISE 24-1ek.example.com         IND       ISE24-1ek.example.com

#### アクティブ化が成功すると、INDに次のメッセージが表示されます。

Message		×
pxGrid Service is active		
	ОК	

## 確認

## ISEの検証

[**Administration] > [pxGrid Services] > [All Clients]に移動します**。INDクライアントはAll Clientsで Offline(XMPP)と表示され、INDはpxGridバージョン2を使用します。

cisco	Identity Services Engine	Home	Operations     P	olicy - Administration	▶ Work Centers				
Is Sys	tem <ul> <li>Identity Management</li> </ul>	Network Resources	ce Portal Management	xGrid Services Feed Se	rvice				
All C	All Clients Web Clients Capabilities Live Log Settings Certificates Permissions								
🖌 Enal	ble 🧭 Disable 😪 Approve 😝 Gr	oup 👎 Decline  🐼 Delete 👻	😵 Refresh 🛛 Total Pending	Approval(0) 👻					
	Client Name	Client Description	Capabilities	Status	Client Group(s)				
	ise-fanout-ise24-1ek		Capabilities(0 Pul	b, 0 Sub) Online (X	KMPP) Internal				
	ise-pubsub-ise24-1ek Client Name	e: Not Sortable	Capabilities(0 Pul	b, 0 Sub) Online (X	KMPP) Internal				
	ise-pubsub-ise24-2ek		Capabilities(0 Pul	b, 0 Sub) Online (2	KMPP) Internal				
	ise-fanout-ise24-2ek		Capabilities(0 Pul	b, 0 Sub) Online (2	KMPP) Internal				
	ise-admin-ise24-3ek		Capabilities(0 Pul	b, 0 Sub) Online (2	KMPP) Internal				
	ise-mnt-ise24-2ek		Capabilities(2 Pul	b, 1 Sub) Online (2	KMPP) Internal				
	ise-mnt-ise24-1ek		Capabilities(2 Pul	b, 1 Sub) Online (2	XMPP) Internal				
	ise-bridge-ise24-1ek		Capabilities(0 Pul	b, 4 Sub) Online (2	XMPP) Internal				
	ise-admin-ise24-1ek		Capabilities(5 Pul	b, 2 Sub) Online (X	XMPP) Internal				
	ise-admin-ise24-2ek		Capabilities(1 Pul	b, 1 Sub) Online (2	KMPP) Internal				
►►	ind		Capabilities(0 Pul	b, 0 Sub) Offline (	XMPP)				

### [Web Clients] をクリックし、INDクライアントのステータスが[ON]であること、および /topic/com.cisco.endoint.assetが[Subscriptions]に含まれていることを確認します。

cisco	Identity Services Engi	ne Home	<ul> <li>Context Visibility</li> </ul>	<ul> <li>Operations</li> </ul>	Policy ▼A	dministration	Work Centers				
+ Sj	stem  Identity Manage	ment • Netwo	rk Resources + Devi	ice Portal Management	pxGrid Service	Feed Service	e F Threat Centric N	NAC			
All	Clients Web Clients	Capabilities	Live Log Settings	Certificates Pe	rmissions						
								Rows/Page 25	• · · · 1 0	1 = = (	Go 12 Total Rows
SI	Refresh										🔻 Filter 🕶 🗘 🗸
	Client Name	Connect To	Session Id	Certificate	Su	bscriptions	F	Publications	IP Address	Status	Start time
×	Client Name		•						IP Address		•
	IND	ISE24-1ek	ISE24-1ek:181	CN=WIN2012	-AAA,				10.62.145.130	ON	2019-05-23 08:27
	ise-mnt-ise24-1ek	ISE24-1ek	ISE24-1ek:182	CN=ISE24-1e	k.exa /top	oic/com.cisco.ise.s	ssion.internal		10.62.145.140	ON	2019-05-23 08:28
	ise-fanout-ise24-1ek	ISE24-1ek	ISE24-1ek:183	CN=ISE24-1e	k.exa /top	oic/distributed	л	topic/distributed	10.62.145.140	ON	2019-05-23 08:28
	ise-admin-ise24-1ek	ISE24-1ek	ISE24-1ek:184	CN=ISE24-1e	k.exa /top	oic/com.cisco.endp	pint.asset		10.62.145.140	OFF 🕢	2019-05-23 08:28
	ise-mnt-ise24-2ek	ISE24-1ek	ISE24-1ek:185	No Certificate	/top	oic/com.cisco.ise.s	ession.internal /	topic/com.cisco.ise.session.internal	10.62.145.141	OFF 🕢	2019-05-23 08:59
	ise-admin-ise24-2ek	ISE24-1ek	ISE24-1ek:188	No Certificate					10.62.145.141	ON	2019-05-23 09:30
	ise-bridge-ise24-1ek	ISE24-1ek	ISE24-1ek:189	CN=ISE24-1e	k.exa				127.0.0.1	OFF 🧿	2019-05-23 09:30
	ise-fanout-ise24-1ek	ISE24-1ek	ISE24-1ek:190	CN=ISE24-1e	k.exa /top	oic/wildcard			127.0.0.1	ON	2019-05-23 09:30
	ise-mnt-ise24-2ek	ISE24-1ek	ISE24-1ek:191	No Certificate	/top	ic/com.cisco.ise.s	ession.internal /	topic/com.cisco.ise.session.internal	10.62.145.141	ON	2019-05-23 09:43
	ise-admin-ise24-1ek	ISE24-1ek	ISE24-1ek:192	CN=ISE24-1e	k.exa /top	oic/com.cisco.endp	pint.asset		10.62.145.140	ON	2019-05-23 09:43
	ise-bridge-ise24-1ek	ISE24-1ek	ISE24-1ek:193	CN=ISE24-1e	k.exa				127.0.0.1	OFF 🕢	2019-05-23 10:04
	ise-bridge-ise24-1ek	ISE24-1ek	ISE24-1ek:194	CN=ISE24-1e	k.exa				127.0.0.1	ON	2019-05-23 10:09

## INDの検証

INDが[In Sync]ステータスに移行します。これは、ISEで一括ダウンロードが成功した場合に行われます。失敗した場合、INDがOut of Sync状態のままになります。

-II-II-INDUSTRIAL cisco NETWORK DIRECTOR Settings > pxGrid							۰ 🌲	Û	•	1	
Eetings					pxGrid						
Trusted Certificate	Cicco Platform Exchange Grid (pxGird) is an open, scalable data-sharing and threat control platform that allows seamless integration between multivendor identity, network, security and asset management systems. Enabling the feature below activates the sharing of endpoint as Services Engine (ISE) psGrid controller. This information can then be leveraged by updream security systems to monitor security, detect threats, and set network policy. Learn more hare.								this system v	eith a Cisco Id	ientity
	Download .pem	IND certificate									
	ISE Server										
	Node Name*			Server 1*		Server 2					
	IND			ISE24-1ek.example.com							
	Statistics										
		Sync. Status	In Sync		L	ast Sync. Status Probe Time	2019-05-23 10:19:16				
		Number of Assets Shared via Last Bulk Request	2			Last Bulk Request Time	2019-05-23 08:29:14				
		Last Update Operation	Update			Last Update Time	2019-05-22 20:17:36				
		Total pxGrid Asset Count	2								

## トラブルシュート

### INDで同期ステータスがOut of Syncのままになる

ISEでの一括ダウンロードが成功すると、Out of SyncからIn Syncへの移行が発生します。以下の IND application.log。

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 ISEがINDによって共有されるINDホスト名を解決できることが重要です。そうしないと、ISEは −括ダウンロードを実行できず、INDはIn Sync状態に移行しません。bulk downloadが失敗した場 合(WIN2012-AAAがISEで解決できなかった場合)、profiler.logに次の例外が表示されます。 -括ダウンロードをトリガーするには、PSNのpxGridプローブをオフにしてチェックします。 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.INDSubscriber -::- NODENAME:ind 2019-04-30 13:59:50,714 INFO [ProfilerINDSubscriberPoller-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.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)
at
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
sun.net.www.protocol.https.AbstractDelegateHttpsURLConnection.connect(AbstractDelegateHttpsURLCo
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)
at com.cisco.profiler.infrastructure.probemgr.INDSubscriber.isInSync(INDSubscriber.java:500)
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)
```

## すべてのエンドポイントがISEと共有されているわけではありません

IND上のエンドポイントがISEと共有されるのは、pxGridアセットフラグが[Yes, MAC address]の 場合だけです。そうでない場合、ISEはエンドポイントを作成するのに十分なデータを持ってい ません。

.ılı.ılı. cısco	INDUSTRIAL NETWORK DIRECTOR	Operate > Inventory					۰ 🌲	Û	0.	1 -
(Dverview	< 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およびAssetGroupはISEでは使用できません

assetTagのみが使用できない場合は、誤ったTAGタイプが使用されている場合が考えられます。

#### エンドポイントを更新するときは、セキュリティタグ(通常のタグではなく)を使用する必要が あります。

Associated Device Tags		×
No Tags Associated with this device		
Add Regular Tag		
Select a tag	•	
Add Security Tag		
Select a tag		
SEC_IAG2		

AssetTagとAssetGroupの両方が使用できない場合は、次の理由が考えられます

1.プロファイリングポリシーがカスタム属性を使用して設定されていない(このドキュメントの 「設定」セクションのステップ1-3を参照)

2.不具合<u>CSCvn66106</u> エンドポイント属性フィルタ: 無効にする必要があります。それ以外の場合は、分類子からカスタム属性をフィルタします。profiler.logには次のログが表示されます。

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}