



Deploying Certificates with Cisco pxGrid

Using External Certificate Authority (CA)-Signed Certificates Updates to Cisco ISE 2.0/2.1/2.2

Author: John Eppich



Table of Contents

About this D	ocument	3
Introduction	4	
Using an Ex	ternal Certificate Authority (CA) Server	5
	Customized Template	5
	Configuring ISE pxGrid node	9
	Generating Certificate Signing Request (CSR)	9
	Importing CA root certificate into ISE Trusted Certificate Store	11
	Bind ISE certificate to Certificate Signing Request (CSR)	11
	Enabling pxGrid	14
	pxGrid Client Certificate Configuration	16
	Testing pxGrid client and the ISE pxGrid node	22
	Viewing Keystore Entries	25
	Troubleshooting	31
References	32	

About this Document

This document covers Certificate Authority (CA)- Signed pxGrid client deployments using Java Keystores with Cisco Identity Services Engine versions ISE 2.0/2.1/2.2. This document is intended for Cisco field engineers, technical marketing engineers, partners and customers deploying Cisco pxGrid.

If the reader is not familiar with pxGrid, please see: How To: Configure and Test Integration with Cisco pxGrid using ISE 2.0: <u>https://communities.cisco.com/docs/DOC-68291</u>

To obtain the Cisco ISE images and appropriate SDKs, please sign up for Devnet: <u>https://developer.cisco.com/site/pxgrid/</u>

It is assumed that Cisco Identity Services Engine (ISE) is installed. A Mac running OSX 10.8.5 using Oracle Java Development Kit 8 will be used as the pxGrid client. A Linux OS can also be used. The Oracle Java Development Kit 8 is required for the pxGrid client for running keytools.

This document uses ISE 2.2 as the default configuration, and points out ISE 2.0 and ISE 2.1 where applicable.

This document does not cover using the ISE 2.1/ISE 2.2 Internal Certificate Authority (CA) for deploying pxGrid client certificates which are included in the reference section.

Introduction

This section details the Certificate Authority (CA) signed certificate configuration for a pxGrid client and an ISE pxGrid node in an ISE Stand-alone deployment. The ISE pxGrid node and pxGrid client will obtain a signed certificate from the Microsoft Enterprise CA 2008 R2 Authority. Please note that a customized pxGrid template having an Enhanced Key Usage (EKU) ISO- defined object identifier (OID) for both client authentication (1.3.6.1.5.5.7.3.2) and server authentication (1.3.6.1.5.5.7.3.1) must be created. The ISE pxGrid node will download the CA root certificate to its trusted certificate store and the pxGrid client will download the root certificate the trusted keystore.

When the pxGrid client connects to the ISE pxGrid node both public certificates will be trusted for Simple Authentication and Security Layer (SASL) for a successful pxGrid connection.

The following diagram represents the certificate flow of information.



Using an External Certificate Authority (CA) Server

Using an external CA server to generate pxGrid certificate, a customized template with an EKU of both client and server authentication must be configured. In this example, Microsoft 2008 Enterprise CA R2 Server was used.

Customized Template

Step 1 Select Administrative Tools->Certificate Authority-> "+" dropdown next to CA server->Right-Click on Certificate Templates->Manage



Step 2 Right-Click and Duplicate User template->Select Windows 2003 Enterprise->OK



Step 3 Enter name of certificate template, uncheck "Publish certificate in Active Directory", and provide validity period and renewal period.

Certificate Templates Console			_ [] ×
File Action View Help	Properties of New Template	×1	
Certificate Templates (WIN-BG7GP)	Issuance Requirements Superseded Templates Extensions Security General Request Handling Subject Name Server Template display name:	Ver ▲ 110	Actions Certificate Templa A
	joxGnd Minimum Supported CAs: Windows Server 2003 Enterprise Template name:	6.1 4.1 5.1 4.1	More Actions
	pxGrid	7.1 8.1 7.1	
	Validity penda: Prenewa penda:	11C 105 101 10C	
	Publish certificate in Active Directory Do not automatically reenrol if a duplicate certificate exists in Active Directory	101 5.1 4.1 6.1	
	For automatic renewal of smart card certificates, use the existing key if a new key cannot be created	11. 5.1 3.1 3.1 4.1	
×	OK Cancel Apply Help	4.1 101	

Step 4 Click Extensions->Add->Server Authentication->Ok->Apply

File Action View Help Properties of Hew Template Image: Stress of Hew Template Image: Stress of Hew Template Image: Stress of Hew Template Image: Stress of Hew Template Image: Stress of Hew Template Image: Stress of Hew Template Image: Stress of Hew Template Image: Stress of Hew Template Image: Stress of Hew Template Image: Stress of Hew Templates Image: Stress of Hew Template Image: Stress of Hew Template Image: Stress of Hew Templates Image: Stress of Hew Template Image: Stress of Hew Template Image: Stress of Hew Templates Image: Stress of Hew Template Image: Stress of Hew Template Image: Stress of Hew Templates Image: Stress of Hew Template Image: Stress of Hew Template Image: Stress of Hew Templates Image: Stress of Hew Template Image: Stress of Hew Template Image: Stress of Hew Template Image: Stress of Hew Template Image: Stress of Hew Template
General Request Handling Subject Name Server Certificate Templates (WIN-B67GP To modify an extension, select it, and then click Edit. Extensions included in this template:
Q Certificate Templates (WIN-BG7GP) Actions To modify an extension, select it, and then click Edit. 10 6.1 Extensions included in this template: Actions
To modify an extension, select it, and then click Edit. To modify an extension, select it, and then click Edit. Extensions included in this template: A1 Certificate Templa More Actions
Extensions included in this template: 6.1 4.1 More Actions
Extensions included in this template: 4.1
Application Policies
Basic Constraints
Certificate Template Information 7.1
Sket laane 8.1
7.1
110
105
Edit 101
101
Description or Application Policies: 5.1
Client Authentication
Secure Email 6.1
Server Authentication 11.
5.1
3.1
3.1
4.1
101
OK Cancel Anny Help .

Step 5 Click Subject Name, Enable Supply in the request



Step 6 Click Extensions->Issuance Policies->Edit->All Issuance Policies

Certificate Templates Console		_ _ _ _ _ _ / ×
File Action View Help	erties of New Template	1
	General Request Handling Subject Name Server	
Certificate Templates (WIN+TE115 Iss	uance Requirements Superseded Templates Extensions Security	Ver A Actions
Tr	modifier an avtancion realact it and than click Edit	4.1
	Edit Issuance Policies Extension	110
Б	ten: An issuance policy describes the conditions under which	6.1 More Actions
	Ac a certificate is issued.	4.1 User 🔺
	B	5.1 Mara Actions
	Issuance policies:	6.1
	All issuance policies	7.1
		8.1
		7.1
		110
	-	105
		101
	iscn	5.1
		4.1
	Add Edit Remove	6.1
	Make this extension critical	11.
	OK Canad V	5.1
		3.1
		4.1
		4.1
		101
•	OK Cancel Apply Help	

Step 7 Leave the defaults for request handling



- **Step 8** Right-click on Certificate Templates
- **Step 9** Select New Template to issue and select pxGrid

🙀 certsrv - [Certification Authority	(Local)\lab7-WIN-LTE115	BAKTM-CA\Cert	ificate Templates]		_ 🗆 🗙
File Action View Help					
🗢 🔿 🖄 🙆 🔂			A		
Certification Authority (Local)	Name		Intended Purpose		
🖃 🚽 lab7-WIN-LTE11SBAKTM-CA	CEP Encryption		Certificate Request Agent		
Revoked Certificates	🚇 Exchange Enrollment Ag	ent (Offline req	Certificate Request Agent		
Issued Certificates	IPSec (Offline request)		IP security IKE intermediate		
Pending Requests	able Certificate Template	~			V
Certificate Templates	lable certificate relipiat			and the second second second	-
info All c For	mation about this template ha of the certificate templates in the more information, see <u>Certifica</u>	s been replicated to the organization may the Template Conce	all domain controllers. not be available to your CA. pts.		
N	ame	Intended Purpose			-
	Exchange User	Secure Email			
	IPSec	If security INE Intermediate			
	Kerberos Authentication	Client Authenticat	ion, Server Authentication, Sma	art Card Logon, KDC Authe	int I
		OCCE Signing	eni		
	ovGrid	Server Authentica	tion Secure Email Encounting	File System Client Authent	ic:
	BAS and IAS Server	Client Authenticat	ion Server Authentication	The System, Giene Addrene	
	Router (Offline request)	Client Authenticat	ion		
	Smartcard Logon	Client Authenticat	ion, Smart Card Logon		
I I I I I I I I I I I I I I I I I I I	Smartcard User	Secure Email. Clie	ent Authentication. Smart Card L	oaon	_
					<u>></u>
				OK Can	cel

Step 10 You should see the pxGrid template

🚋 certsrv - [Certification Authority	(Local)\lab7-WIN-LTE11SBAKTM-CA\Cert	ificate Templates]	
<u>File Action View Help</u>			
🗢 🔿 🙎 🧟 🗟 🛛			
🙀 Certification Authority (Local)	Name	Intended Purpose	
🖃 🚽 lab7-WIN-LTE11SBAKTM-CA	🚇 pxGrid	Server Authentication, Secure Email, Encry	
Revoked Certificates	CEP Encryption	Certificate Request Agent	
Issued Certificates	Rechange Enrollment Agent (Offline req	Certificate Request Agent	
Pending Requests	IPSec (Offline request)	IP security IKE intermediate	
Failed Requests	Directory Email Replication	Directory Service Email Replication	
Certificate Templates	Domain Controller Authentication	Client Authentication, Server Authenticatio	
	EFS Recovery Agent	File Recovery	
	Basic EFS	Encrypting File System	
	🗟 Domain Controller	Client Authentication, Server Authentication	
	🚇 Web Server	Server Authentication	
	Computer	Client Authentication, Server Authentication	
	🖳 User	Encrypting File System, Secure Email, Clien	
	B Subordinate Certification Authority	<all></all>	
	Administrator	Microsoft Trust List Signing, Encrypting File	

Configuring ISE pxGrid node

Generating Certificate Signing Request (CSR)

Step 1Select Administration->System->Certificates->Certificate Management->Certificate Signing
Requests->Generate Certificate Signing Request (CSR)

0	Certificate(s) will be used for	Admin
✓ Certificate Management	Allow Wildcard Certificates	
System Certificates Trusted Certificates OCSP Client Profile	Node(s) Generate CSR's for these Node	es:
Certificate Signing Requests	Node	CSR Friendly Name
Certificate Periodic Check Settin	ise470	ise470#Admin
Certificate Authority		
	Subject	
	Common Name (CN)	\$FQDN\$
	Organizational Unit (OU)	
	Organization (O)	
	City (L)	
	State (ST)	
	Country (C)	
	Subject Alternative Name (SAN)	DNS Name 🔹 ise470.lab10.com 📃 😑 🕂

Step 2 Select Generate



Step 3 Select Export and open the PEM file copy

----BEGIN CERTIFICATE REQUEST----

MIIC7jCCAdYCAQAwGzEZMBcGA1UEAxMQaXN1NDcwLmxhYjEwLmNvbTCCASIwDQYJ
KoZIhvcNAQEBBQADggEPADCCAQoCggEBAJSM1PM6t1crlvZxEe584Y/dnrrEdE7j
qKiS0RWLXmbEDHX15F0rIhcn7rAR0e9h8V1oeA4v9+Sj1I0slsfTETUoWbWpqgyo
J5DEj5YxS2vH+cAhKj5Xp4ls7ziqBaUyw9OnaRTjUp40gyOY3O2/8NCWWXvt4r0w
gFYuIbi8emMRuNPn+448f3Rx3mHs2cdARosjtUC/OmAfys17uPDCahjGqapy/10E
TuW0MAjdvUaibimDl+WmsWnFvmiSVuoFh5/JYGh3pXdw5MK9tt5hltP0dZMkbANJ
1jwyYmOeVz9Zal51nuWpJJ5bZJjZE88/dA8pQJFOXE/jqTmfZzwhztsCAwEAAaCB
jTCBigYJKoZIhvcNAQkOMX0wezAbBgNVHREEFDASghBpc2U0NzAubGFiMTAuY29t
MAsGA1UdDwQEAwIF4DAdBgNVHQ4EFgQU2jmj7l5rSw0yVb/vlWAYkK/YBwkwHQYD
VR01BBYwFAYIKwYBBQUHAwEGCCsGAQUFBwMCMBEGCWCGSAGG+EIBAQQEAwIGQDAN
BgkqhkiG9w0BAQsFAAOCAQEAADS9KUeb8wvLZbkxYFB/ecsfGM2kIGhPDtn9/0de
rzZCEx3BzE9hi3ILXibjIZA4FsuvLowSTE2mTB32/uTr1R+JEobS0foc9oLUOTgW
uoPtrHAXqdIPO+jUl+fDz+Ib3dbSaSqGY5fvsm7YvEo8OMvlbM23mTWzHoYgjk3G
vtxxvNmRGLL53ijSH+PE476a0eKgD+iLyG6oM2KJOWbDrBEwHUPDhmiIWal1uP0Y
iizVXBrupn5Y4E4iYTSy1p38hh0eiTSelgvcF6xdWDM2tESKaK6jJRDJNS6QJTR0
CGuoV7JiBMTLVD+iM+5/Q/kEV/TOORIZaLZrlYHIA3sZyw==
END CERTIFICATE REQUEST

Step 4 Paste into CSR request



- Step 5 Select Submit
- Step 6 Select Base64 encoded
- Step 7 Select Download certificate and save file locally. This file was renamed to ise470.cer
- **Step 8** Download the CA root certificate

Select Download Certificate->Base 64->Download CA certificate

Microsoft Active Directory Certificate Services lab10-WIN-N3OR1A7H9KL-CA						
Download a CA Certificate, Certificate Chain, or CRL						
To trust certificates issued from this certification authority, install this CA certificate.						
To download a CA certificate, certificate chain, or CRL, select the certificate and encoding method.						
CA certificate:						
Current [lab10-WIN-N3OR1A7H9KL-CA]						
Encoding method:						
ODER						
 Base 64 						
Install CA certificate						
Download CA certificate						
Download CA certificate chain						
Download latest base CRL						
Download latest delta CRL						

Step 9 Rename the certificate to caroot.cer

Importing CA root certificate into ISE Trusted Certificate Store

Step 1 Select Administration->System->Certificates->Certificate Management->Trusted Certificates->Import->Certificate file and import the root certificate



Step 2 Select Submit

Bind ISE certificate to Certificate Signing Request (CSR)

Step 1Select Administration->System->Certificates->Certificate management->Certificate Signing
Requests->select ISE node->Bind Certificate

dentity Services Engine	Home	erations Policy Administration	Work Centers		
System Identity Management	Network Resources Device Portal N	Aanagement pxGrid Services + Feed Serv	rice + Threat Centric NAC		
Deployment Licensing - Certificate	es + Logging + Maintenance Upg	rade Backup & Restore + Admin Access	 Settings 		
0					
- Certificate Management	Certificate Signing Requests				
System Certificates	Generate Certificate Signing Requests (CSR)				
Trusted Certificates	A Certificate Signing Requests (CSRs) must be sent to and signed by an external authority. Click "export" to download on				
OCSP Client Profile	request has been signed, click bind t	o bind the request to the signed certificate issued	b by that authonity. Once a CSR is t		
Certificate Signing Requests	🔎 View 🚯 Export 🗙 Delete	Bind Certificate			
Certificate Periodic Check Settin	Friendly Name	Certificate Subject	Key Length Por		
Certificate Authority	✓ ise470#Admin	CN=ise470.lab10.com	2048		

Step 2 Select ISE certificate file and upload the root certificate

dentity Services Engine	Home → Context Visibility → C	perations Policy	- Administration	Work Centers
System Identity Management	Network Resources Device Portal	Management pxGrid Se	ervices Feed Serv	vice
Deployment Licensing - Certificate	s I Logging I Maintenance Up	grade Backup & Restore	Admin Access	 Settings
G				
✓ Certificate Management	Bind CA Signed Certificate			
System Certificates	* Certificate File	Choose File ise470.cer		
Trusted Certificates			-	
OCSP Client Profile	Friendly Name			١
Certificate Signing Requests	Validate Certificate Extensions			
Certificate Periodic Check Settin	Valuate Certificate Extensions			
Certificate Authority	lisane			
		Admin: Use certificate	to authenticate the ISE	Admin Portal
		Submit Cancel		

Step 3 Select Submit

- **Step 4** Select **Yes** for an application restart
- **Step 5** Select **Yes** to replace the existing certificate. The system will restart
- **Step 6** Select Administration->System->Certificates->System Certificates You should see the default pxGrid certificate signed by the internal ISE CA

dentity Services Engine	Home	Context Visibility	Operations I	Policy Administration	Work Centers		License Warning
▼System → Identity Management	Network	Resources	al Management	pxGrid Services Feed Se	Prvice	Click here to do wire	eless setup and visibilit
Deployment Licensing - Certificate	s ⊧Lo	gging ► Maintenance U	Jpgrade Backup	& Restore + Admin Access	s Settings 		
Certificate Management	Syste	em Certificates 🛕 For d	disaster recovery it i	is recommended to export cer	tificate and private key pairs o	of all system certificates.	
System Certificates	1	Edit 🛛 🕂 Generate Self Sign	ed Certificate	Import 💽 Export 🔀	Delete View		
Trusted Certificates		Friendly Name	Used By	Portal group tag	Issued To	Issued By	Valid From
OCSP Client Profile	V ise	2 470					
Certificate Signing Requests		ise470.lab10.com#Certifica te Services Endpoint Sub CA - ise470#00001	pxGrid		ise470.lab10.com	Certificate Services Endpoi nt Sub CA - ise470	Tue, 7 Feb 2017
Certificate Periodic Check Settin	_	Derault self-signed sami se					
Certificate Authority		rver certificate - CN=SAML _ise470.lab10.com	SAML		SAML_ise470.lab10.com	SAML_ise470.lab10.com	Wed, 8 Feb 2017
		ise470.lab10.com,ise470.l ab10.com#lab10-WIN-N3O R1A7H9KL-CA#00002	EAP Authentication, Admin, Portal, RADIUS DTLS	Default Portal Certificate Group (j)	ise470.lab10.com	lab10-WIN-N3OR1A7H9KL -CA	Fri, 17 Feb 2017

Note: For ISE 2.0 and ISE 2.1, the "admin" certificate should be valid for pxGrid also. Modify the certificate and verify that the certificate is used by pxGrid also.



dentity Services Engine	Iome	Guest Access	✓ Administration > W	ork Centers		1	License Warning 🔺	Q,	0	4 Ø
System Identity Management	System + Identity Management + Network Resources + Device Portal Management pxGrid Services + Feed Service + Identity Mapping									
Deployment Licensing	Deployment Licensing -Certificates + Logging + Maintenance Upgrade Backup & Restore + Admin Access + Settings									
0										
- Certificate Management System Certificates 🛕 For disaster recovery it is recommended to export certificate and private key pairs of all system certificates.										
Overview	📝 Edit 🕂 Generate Self Signe	d Certificate 🛛 🕂 Im	port 🔀 Export 🗶 Dele	te 🔎 View						
System Certificates	Friendly Name	Used By	Portal group tag	Issued To	Issued By	Valid Fre	m	Expiration	Date	
Endpoint Certificates	▼ iseinfo									
Trusted Certificates	iseinfo.lab10.com,iseinfo.lab1	EAP Authentication, Admin_Bortal	Default Portal Certificate	iseinfo.lab10.com	lab10-WIN-N3OR1A7H9KL-C	Thu, 12	May 2016	Sat, 12 Ma	ay 2018	
OCSP Client Profile	H9KL-CA#00001	pxGrid	Group		A					
Certificate Signing Requests										
Certificate Periodic Check Settings										



ISE 2.1								
dentity Services Engine	Home	sibility	Administration	Work Centers		License Warning 🔺	<u>୍</u> ଡ	± 0
System Identity Management	Network Resources	Device Portal Management pa	Grid Services Feed Serv	rice + PassiveID + Threat C	entric NAC			
Deployment Licensing - Certificates	Deployment Licensing → Certificates → Logging → Maintenance Upgrade Backup & Restore → Admin Access → Settings							
G								
- Certificate Management	Certificate Management System Certificates ▲ For disaster recovery it is recommended to export certificate and private key pairs of all system certificates.							
Overview	🖊 Edit 🕂 Gene	erate Self Signed Certificate	Import 😨 Export 🔀 De	elete 🔎 View				
System Certificates	Friendly Name	Used By	Portal group tag	Issued To	Issued By	Valid From	Expiration Date	
Endpoint Certificates	▼ ise21ca							
Trusted Certificates	Default self-sig er certificate - 21ca.lab10.co	gned saml serv CN=SAML_ise SAML m		SAML_ise21ca.lab10.com	SAML_ise21ca.lab10.com	Sun, 3 Jul 2016	Mon, 3 Jul 2017	
OCSP Client Profile		EAP						
Certificate Signing Requests	N-N3OR1A7H	9KL-CA#00001 Admin, Portal,	Group (i)	ise21ca.lab10.com	A	Sun, 3 Jul 2016	Tue, 3 Jul 2018	
Certificate Periodic Check Setti		pxGrid						

Step 7 Edit the admin certificate

dentity Services Engine	Home	Context Visibility	Operations I	Policy - Administration	Work Centers		License Warning
	Networl	k Resources	al Management Ipgrade Backup	pxGrid Services	ervice	Click here to do wire	eless setup and visibilit
 Certificate Management System Certificates ▲ For disaster recovery it is recommended to export certificate and private key pairs of all system certificates. 							
System Certificates	1	Edit 🛛 🕂 Generate Self Sign	ed Certificate	Import 💽 Export 🔀	Delete View		
Trusted Certificates		Friendly Name	Used By	Portal group tag	Issued To	Issued By	Valid From
OCSP Client Profile	▼ is	e470					
Certificate Signing Requests		ise470.lab10.com#Certifica te Services Endpoint Sub CA - ise470#00001	pxGrid		ise470.lab10.com	Certificate Services Endpoi nt Sub CA - ise470	Tue, 7 Feb 2017
Certificate Periodic Check Settin	_	Default self-signed saml se					
Certificate Authority		ise470.lab10.com	SAML		SAML_ISe470.lab10.com	SAML_ISe470.lab10.com	Wed, 8 Feb 2017
	ø	ise470.lab10.com,ise470.l ab10.com#lab10-WIN-N3O R1A7H9KL-CA#00002	EAP Authentication, Admin, Portal, RADIUS DTLS	Default Portal Certificate Group (i)	ise470.lab10.com	lab10-WIN-N3OR1A7H9KL -CA	Fri, 17 Feb 2017

Step 8 Select pxGrid



Step 9 Select Save

You should see the pxGrid purpose assigned to the admin certificate

 $\underline{\textbf{Note}}:$ This is required for security solutions that require bulk session downloads

dentity Services Engine	Home Context Visibility	Operations	Policy Administration	Work Centers		License Warning 🔺	<u> २</u>	ò
System Identity Management	Network Resources Device F	ortal Management	pxGrid Services Feed S	ervice Threat Centric NA	Click here to do wire	eless setup and visibility setu	p Do not show this a	gain. ×
Deployment Licensing +Cartificates +Logging + Maintenance Upgrade Backup & Restore + Admin Access + Settings								
Certificate Management System Certificates ▲ For disaster recovery it is recommended to export certificate and private key pairs of all system certificates.								
System Certificates	📝 Edit 🕂 Generate Self S	igned Certificate 🛛 🕂	Import 🔛 Export 🗙	Delete 🔎 View				
Trusted Certificates	Friendly Name	Used By	Portal group tag	Issued To	Issued By	Valid From	Expiration Date	
OCSP Client Profile	▼ ise470							
Certificate Signing Requests	ise470.lab10.com#Certifi te Services Endpoint Sub CA - ise470#00001	Not in use		ise470.lab10.com	Certificate Services Endpoi nt Sub CA - ise470	Tue, 7 Feb 2017	Tue, 8 Feb 2022	<u>~</u>
Certificate Periodic Check Settin Certificate Authority	Default self-signed saml rver certificate - CN=SAN	60 IL SAML		SAML_ise470.lab10.com	SAML_ise470.lab10.com	Wed, 8 Feb 2017	Thu, 8 Feb 2018	
	ise470.lab10.com,ise470 ab10.com#lab10-WIN-N3 R1A7H9KL-CA#00002	Admin, Portal, I EAP O Authentication, pxGrid, RADIUS DTLS	Default Portal Certificate Group (j)	ise470.lab10.com	lab10-WIN-N3OR1A7H9KL -CA	Fri, 17 Feb 2017	Sun, 17 Feb 2019	

Enabling pxGrid

Step 1 Select Administration->System->Deployment->edit ise node->enable pxGrid

dentity Services Engine	Home → Co	ntext Visibility	ns ► Policy ▼A	dministration	Work Centers	License War
- System Identity Management	 Network Resource 	rces	ement pxGrid Service	IS Feed Service	Threat Centric NAC	Click here to do wireless setup and visi
Deployment Licensing + Certifi	cates + Logging	 Maintenance Upgrade 	Backup & Restore	Admin Access	Settings	
		IP Address	192.168.1.158			
		Node Type	Identity Services Eng	ine (ISE)		
		Administration		Role STANDALO	NE Make Primary	
		Monitoring		Role PRIMARY	The Monitor	ing Node
		Policy Service				
		CENTRAL Enable Session Se	ervices (j)	Include Node in N	lode Group None	* (1)
		Enable Profiling S	ervice			
		C Enable Threat Ce	ntric NAC Service (i)			
		Enable SXP Servio	e (i)	Use Interface Gig	gabitEthernet 0	r
		Enable Device Ad	min Service (j)			
		Enable Passive Id	entity Service (i)			
		pxGrid				
		Save Reset				

- Step 2 Select Save
- Step 3 Run "sh application status ise" to verify the pxGrid services are running
- Step 4 Select Administration->pxGrid Services, you should see the published nodes appear and pxGrid node connectivity



dentity Services Engine	Home Contex	kt Visibility	Policy A	Administration V	fork Centers	License Warning 🔺
System Identity Management	 Network Resources 	Device Portal Manager	nent pxGrid Service	Feed Service	Threat Centric NAC	Click here to do wireless setup and visibility setu
Cliente Capabilities Liv	alog Cottings	Cortificatos				
Calends Capabilities Capabi	Group Decline	Pelete - & Refresh	Total Pending Approva	al(0) 👻		1.0 of 0. Show 25 -
Client Name	Client Description	n Capabili	ties	Status	Client	Group(s) Auth Method
□ ► ise-admin-ise470		Capabili	ties(6 Pub, 2 Sub)	Online	Admini	istrator Certificate
ise-mnt-ise470		Capabili	ties(2 Pub, 1 Sub)	Online	Admini	strator Certificate
Connected to pxGrid ise470.lab10.com						

Note: Here's what you would see on the ISE 2.0 Also enable Auto-Registration

entropy dentity Services Engine Home	y → Guest Access → Adminis	tration		1 Lice	ise Warning 🔺	ৎ 🙂	4 o
System Identity Management Network Resources Device Port	al Management pxGrid Services	Feed Service Fldentity Mapping	9				
				⊖Enable	Auto-Registration	Disable Auto-Reg View By Ca	gistration pabilities
Clients Live Log						ŝ	
✓ Enable Ø Disable Ø Approve	fresh Total Pending Approval(0) -			1 - 2 of 2	Show 25 + pe	erpage Page	1 ‡
Client Name Client Description	Capabilities	Status	Client Group(s)	Log			
□ ► ise-mnt-iseinfo	Capabilities(2 Pub, 1 Sub)	Online	Administrator	View			
□ ► ise-admin-iseinfo	Capabilities(4 Pub, 2 Sub)	Online	Administrator	View			
Connected to pxGrid							

Here is what you will see in ISE 2.1. Select Settings, and enable automatically approve new accounts



ulturlts Identity Services Engine Home → Cont	text Visibility → Operations → Policy → A	dministration		License Warning 🔺	Q @ 1 ¢
System Identity Management Network Resource	es Device Portal Management pxGrid Service	s + Feed Service + PassiveID	Threat Centric NAC		
					k
Clients Capabilities Live Log Settings					
✓ Enable Ø Disable Ø Approve	🐼 Delete 👻 😵 Refresh 🛛 Total Pending Approval(0) 🤜			1 - 2 of 2 Show 25 👻	per page Page 1 🗘
Client Name Client Description	ion Capabilities	Status	Client Group(s)	Auth Method	Log
□ ► ise-admin-ise21ca	Capabilities(4 Pub, 2 Sub)	Online	Administrator	Certificate	View
□ ► ise-mnt-ise21ca	Capabilities(2 Pub, 1 Sub)	Online	Administrator	Certificate	View
Connected to pxGrid					

pxGrid Client Certificate Configuration

This section steps through the pxGrid client CA signed certificate process. Once the public key/private pair is generated, a PKCS12 file will be created from the private key pxGridClient.key.

The PKCS12 file will be imported into the identity keystore, pxGridClient.jks. This identity keystore and associated password will serve as the keystoreFilename and keystorePassword for the pxGrid scripts. The pxGrid client certificate pxGridClient.cer will be added to the keystore as well.

Both the ISE identity certificate, isemnt, required for bulk download sessions, and the CA root certificate will be added to the trustkeystore, root3.jks. This trust keystore and associated password will serve as the truststoreFilename and truststorePassword for the pxGrid scripts.

Step 1 Generate a private key (i.e. pxGridClient.key) for the pxGrid client.

Step 2 Generate a CSR request (i.e. pxGridClient.csr) to the CA Authority. Provide a challenge password (i.e. cisco123)

openssl req -new -key pxGridClient.key -out pxGridClient.csr

You are about to be asked to enter information that will be incorporated into your certificate request.

cisco.

What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
----Country Name (2 letter code) [AU]: US
State or Province Name (full name) [Some-State]: Maryland
Locality Name (eg, city) []: Germantown
Organization Name (eg, company) [Internet Widgits Pty Ltd]: Cisco
Organizational Unit Name (eg, section) []: Engineering
Common Name (e.g. server FQDN or YOUR name) []: johns-macbook-pro.labl0.com
Email Address []: j@cisco.com
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []
An optional company name []

Note: Keep the same password throughout this documnent, easier to maintain, and cut down on errors

Step 3 The CA authority must service the user certificate using a pxGrid template with both EKUs for client authentication and server authentication.

Note: A CA template of Windows 2003 was selected, so it would appear in the Drop-down. A user template was duplicated wit both EKUs for client and server authentication.

Microsoft Active Directory Certificate Services -- lab10-WIN-N3OR1A7H

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoc Request box.

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):	qRv8XxlorEfXdZMGNLC+ gQ/KN2MndaGDy6sjnizY qZKOFOFOXjYrXADLRELr eBSAeXXzl1H5ng17TL/ yTr5CRfeCw== END CERTIFICATE	THN2qCj4XXyaPOxCZt3F Hnu8tDFmxMI5Nq1D6jT AjyROeno3/xyD2gm3Fu8 osIO0dF62ATKbjL00R1K REQUEST
Certificate Templ	ate:	
	pxGrid_User	\$
Additional Attribu	ites:	
Attributes:		
		Submit >

- Step 4 Select Submit
- Step 5 Select Base 64 encoded and download and rename the file to pxGridclient.cer
- Step 6 Download the CA certificate in Base 64 format and rename to caroot.cer

Microsoft Active Directory Certificate Services -- lab10-WIN-N3OR1A7H9KL-CA

Download a CA Certificate, Certificate Chain, or CRL

To trust certificates issued from this certification authority, install this CA certificate.

To download a CA certificate, certificate chain, or CRL, select the certificate and encoding method.

CA certificate:

Current [lab10-WIN-N3OR1A7H9KL-CA]

Encoding method:

DER
Base 64

Install CA certificate Download CA certificate Download CA certificate chain Download latest base CRL Download latest delta CRL

Step 7 Create a pxGrid client pkcs12 file (pxGridClient.p12) from the private key in the pxGridClient certificate (i.e. pxGridClient.cer). This will be used for keystore management and can be a random filename with a .p12 extension. Include the CA root file (i.e. ca_root).

openssl pkcs12 -export -out pxGridClient.p12 -inkey pxGridClient.key -in pxGridClient.cer -chain -CAfile ca_root.cer

Enter Export Password: Cisco123 Verifying - Enter Export Password: Cisco123

Step 8 Create the pxGrid client identity keystore (i.e.pxGridClient.jks). This will be the pxGrid client identity keystore. This can be a random filename with a .jks extension. This will serve as the keystoreFilename and associated keystorePassword in the pxGrid script examples.

```
keytool -importkeystore -srckeystore pxGridClient.p12 -destkeystore pxGridClient.jks -srcstoretype PKCS12
Enter destination keystore password: Ciscol23
Enter new password: Ciscol23
Enter source keystore password:
Entry for alias 1 successfully imported.
Import command completed: 1 entries successfully imported, 0 entries failed or cancelled
```

Step 9 Export only the public ISE Identity certificate into the pxGrid client, note that this will be in .pem format. You can rename the file with .pem extension to make it easier to read. In this example, the file was renamed to isemnt.pem.
 Select Administration->select the ISE certificate->Export



Identity Services Engine	Home > Context Visibility > Operations > Policy Administration > Work Centers	License Warning 🛕 🔍 🥥 🌀 🖒
System Identity Management	Network Resources → Device Portal Management pxGrid Services → Feed Service → Threat Centric NAC Clic	k here to do wireless setup and visibility setup Do not show this again.
Deployment Licensing - Certificates	s > Logging > Maintenance Upgrade Backup & Restore > Admin Access > Settings	
0		
✓ Certificate Management	System Certificates 🛕 For disaster recovery it is recommended to export certificate and private key pairs of all system certificates.	
System Certificates	📝 Edit] 🕂 Generate Self Signed Certificate] 🕂 Import] 🕼 Export] 🗶 Delete] 🔎 View	
Trusted Certificates	Friendly Name Used By Portal group tag Issued To Issued By	Valid From Expiration Date
OCSP Client Profile	▼ ise470	
Certificate Signing Requests	ise470.lab10.com#Certificate Services Endpoint Sub CA - i Not in use ise470.lab10.com Sub CA - ise470 Sub CA - ise470	Endpoint Tue, 7 Feb 2017 Tue, 8 Feb 2022 🗹
Certificate Periodic Check Setti	Default self-signed sami serv	_
Certificate Authority	er certificate - CN=SAML_ise SAML 470.lab10.com SAML_ise470.lab10.com	D.com Wed, 8 Feb 2017 Thu, 8 Feb 2018 🗹
	ise470.lab10.com#se470.lab □ 10.com#se470.lab10.com#0 Not in use ise470.lab10.com 0003	Wed, 22 Feb 2017 Fri, 22 Feb 2019 🔽
	Ise470.lab10.com/ise470.lab Admin, Portal, EAP ✓ 10.com/#ab10-WIN-NSOR1 Authentication, Default Portal Certificate Ise470.lab10.com Authentication, Default Portal Certificate Ise470.l	A7H9KL-C Fri, 17 Feb 2017 Sun, 17 Feb 2019 🗹

Step 10 You should see:

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 Click be
Deployment Licensing - Certificate	es	Church
0		
- Certificate Management	System Certificates 🛕 For disaster recovery it is recommended to export certificate and private key pair	rs of all system certificates.
System Certificates	🖌 Edit) 🕂 Generate Self Signed Certificate) 🕂 Import) 🕼 Export) 🗶 Delete 🔎 View	
Trusted Certificates	Friendly Name Used By Portal group tag Issued To	Issued By
OCSP Client Profile	▼ ise470	
Certificate Signing Requests	ise470.lab10.com#Certificate	Certificate Services En
Certificate Periodic Check Setti	se470#00001 Export Certificate 'ise470.lab10.com,ise470.lab10.com#lab10-WIN Default self-signed	-N3OR1A7H9KL-CA#0000X
Certificate Authority	er certificate CN= 470.lab10.com	
	Ise470.lab10.com, 10.com/lise470.lat 0003 Export Certificate and Private Key	1
	ise470.lab10.com, *Private Key Password	
	7H9KL-CA#00002 *Confirm Password	
	Warning: Exporting a private key is not a secure operation. It could lead to poss	sible exposure of the private key.
		Export Cancel

- Step 11 Select Export Certificate Only->Export and save the ise470lab10comise470lab10co.pem file locally.
- Step 12 Rename the ise470lab10comise470lab10co.pem to isemnt.pem
- **Step 13** Convert the .pem file to .der format

openssl x509 -outform der -in isemnt.pem -out isemnt.der

Step 14 Add the ISE identity cert to the trust keystore (i.e. root3.jks). this will be the trusted keystore. This can be a random filename with a .jks extension. This will become the truststoreFilename and truststorePassword used in the pxGrid scripts.





SHA1: BD:18:C0:DD:4D:DD:43:80:CA:CA:3B:F6:DC:1E:6E:46:93:59:FE:B7 SHA256: F9:11:FC:EC:BC:0F:0F:84:36:F1:26:BC:5A:09:B7:2B:3C:D1:1B:AC:FC:1A:F1:AB:6D:00:8D:11:F8:26:93:FF Signature algorithm name: SHA256withRSA Version: 3 Extensions: #1: ObjectId: 1.2.840.113549.1.9.15 Criticality=false 0000: 30 35 30 0E 06 08 2A 86 48 86 F7 0D 03 02 02 02 050...*.H..... 0010: 00 80 30 0E 06 08 2A 86 48 86 F7 0D 03 04 02 02 ...0...*.H..... 0020: 00 80 30 07 06 05 2B 0E 03 02 07 30 0A 06 08 2A* 0030: 86 48 86 F7 0D 03 07 . H #2: ObjectId: 1.3.6.1.4.1.311.21.10 Criticality=false 0000: 30 32 30 0A 06 08 2B 06 01 05 05 07 03 01 30 0A 020...+.....0. 0010: 06 08 2B 06 01 05 05 07 0020: 01 05 05 07 03 04 30 OC 0030: 37 0A 03 04 7... #3: ObjectId: 1.3.6.1.4.1.311.21.7 Criticality=false 0000: 30 2D 06 25 2B 06 01 04 01 82 37 15 08 DC FD 1A 0-.*+....7.... 86 E6 FC 53 86 82 A1 38 ...y...-...8 40 02 01 64 02 01 03 ^...#...@..d... 0010: 87 CB EB 79 81 89 9D 2D 0020: 5E 86 D1 B8 23 85 FC EF #4: ObjectId: 1.3.6.1.5.5.7.1.1 Criticality=false AuthorityInfoAccess [ſ accessMethod: calssuers accessLocation: URIName: ldap:///CN=lab6-WIN-BG7GPQ053ID-CA, CN=AIA, CN=Public%20Key%20Services, CN=Services, CN=Configuration, DC=lab6, DC=com?cACertificate?base?objectCla ss=certificationAuthority 1 #5: ObjectId: 2.5.29.35 Criticality=false AuthorityKeyIdentifier [KevIdentifier [0000: A9 C7 8E 26 9C F5 37 0A E6 5A 15 36 26 D4 A2 06 ... &..7..Z.6&... 0010: 6A C8 79 2C j.y, #6: ObjectId: 2.5.29.31 Criticality=false CRLDistributionPoints [[DistributionPoint: [URIName: ldap:///CN=lab6-WIN-BG7GPQ053ID-CA,CN=WIN-BG7GPQ053ID,CN=CDP,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=lab6,DC=com?certificateRevocati onList?base?objectClass=cRLDistributionPoint]]] #7: ObjectId: 2.5.29.32 Criticality=false CertificatePolicies [[CertificatePolicyId: [2.5.29.32.0] []] #8: ObjectId: 2.5.29.37 Criticality=false ExtendedKeyUsages [serverAuth clientAuth emailProtection 1.3.6.1.4.1.311.10.3.4 1 #9: ObjectId: 2.5.29.15 Criticality=true KeyUsage [DigitalSignature

Key_Encipherment
]
#10: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: DA 39 A3 EE 5E 6B 4B 0D 32 55 BF EF 95 60 18 90 .9..^kK.2U...`.
0010: AF D8 07 09
]
Trust this certificate? [no]: yes
Certificate was added to keystroke

Step 15 Import the pxGrid client certificate into the identity keystore.

```
keytool -import -alias pxGridMAC -keystore pxGridClient.jks -file
pxGridClient.cer
Enter keystore password: Ciscol23
Certificate already exists in keystore under alias <1>
Do you still want to add it? [no]: yes
Certificate was added to keystore
```

Note: If you receive the following message the certficate was already added to a pre-existing keystore, you can say "no" and still be okay. I selected "yes" so we can verify thay the certificate was added later on.

Step 16 Add the CA root certificate to trusted keystore. The CA root certificate needs to be trusted as well.

```
keytool -import -alias ca root1 -keystore root3.jks -file ca root.cer
Enter keystore password: Cisco123
Owner: CN=lab6-WIN-BG7GPQ053ID-CA, DC=lab6, DC=com
Issuer: CN=lab6-WIN-BG7GPQ053ID-CA, DC=lab6, DC=com
Serial number: 448a6d6486c91cb14c6888c127d16c4e
Valid from: Thu Nov 13 20:47:06 EST 2014 until: Wed Nov 13 20:57:06 EST 2019
Certificate fingerprints:
        MD5: 41:10:8A:F5:36:76:79:9C:2C:00:03:47:55:F8:CF:7B
        SHA1: 9D:DA:06:AF:06:3F:8F:5E:84:C7:F4:58:50:95:03:22:64:48:96:9F
        SHA256:
DB:28:50:D6:47:CA:C0:6A:E9:7B:87:B4:0E:9C:3A:C1:A2:61:EA:D1:29:8B:45:B4:76:4B:DA:2A:F1:D8:E0:A3
        Signature algorithm name: SHA256withRSA
        Version: 3
Extensions:
#1: ObjectId: 1.3.6.1.4.1.311.21.1 Criticality=false
0000: 02 01 00
                                                          . . .
#2: ObjectId: 2.5.29.19 Criticality=true
BasicConstraints:[
  CA:true
  PathLen:2147483647
#3: ObjectId: 2.5.29.15 Criticality=false
KeyUsage [
```

DigitalSignature Key_CertSign Crl_Sign] #4: ObjectId: 2.5.29.14 Criticality=false SubjectKeyIdentifier [KeyIdentifier [0000: A9 C7 8E 26 9C F5 37 0A E6 5A 15 36 26 D4 A2 06 ...&..7..Z.6&... 0010: 6A C8 79 2C j.y,]] Trust this certificate? [no]: **yes** Certificate was added to keystore

Step 17 Copy the identity keystore (pxGridClient.jks) and trust keystore (root3.jks) into the ../samples/bin/..folder.

Testing pxGrid client and the ISE pxGrid node

The pxGrid scripts: register.sh and session download.sh will be run to ensure pxGrid client connection and pxGrid registration. Session downloads will ensure that there are no issues with the ISE MNT certificate and the pxGrid client.

Step 1 Register the pxGrid client

```
./multigroupclient.sh -a 192.168.1.158 -u SIM01 -k pxGridClient.jks -p Cisco123 -t root3.jks -q Cisco123
 ----- properties
  version=1.0.4.19
  hostnames=192.168.1.158
  username=SIM01
 password=
 group=Session, ANC,
  description=null
  keystoreFilename=pxGridClient.jks
  keystorePassword=Cisco123
  truststoreFilename=root3.jks
  truststorePassword=Cisco123
00:22:10.169 [Thread-1] INFO com.cisco.pxgrid.ReconnectionManager - Started
Connecting...
00:22:10.356 [Thread-1] INFO com.cisco.pxgrid.Configuration - Connecting to host 192.168.1.158
00:22:11.330 [Thread-1] INFO com.cisco.pxgrid.Configuration - Connected OK to host 192.168.1.158
00:22:11.330 [Thread-1] INFO com.cisco.pxgrid.Configuration - Client Login to host 192.168.1.158
00:22:12.038 [Thread-1] INFO com.cisco.pxgrid.Configuration - Client Login OK to host 192.168.1.158
Connected
00:22:14.437 [Thread-1] INFO com.cisco.pxgrid.ReconnectionManager - Connected
Create ANC Policy: ANC1489551726715 Result - com.cisco.pxgrid.model.anc.ANCResult@cb0ed20[
  ancStatus=SUCCESS
  ancFailure=<null>
  failureDescription=<null>
  ancEndpoints=<null>
  ancpolicies=<null>
Exception in thread "main" java.lang.IllegalArgumentException: illegal grid configuration type. must use
TLSConfiguration.
       at.
com.cisco.pxgrid.stub.identity.SessionDirectoryFactory.createSessionDirectoryQuery(SessionDirectoryFactory.ja
va:46)
       at com.cisco.pxgrid.samples.ise.MultiGroupClient.main(MultiGroupClient.java:51)
```



Note: "Account enabled" means the account was enabled by the pxGrid admin

Step 2Verify the pxGrid client has registered to the ISE pxGrid node
Select Administration->pxGrid Services

Cisco Identity Services Engine Home	Context Visibility Operative	ations Policy Adminis	tration Vork Centers		Licer	nse Warning 🔺	୍ କ
System Identity Management Network Res	sources	nagement pxGrid Services	Feed Service	VC	Click here to do wireless setup	and visibility set	up Do not sho
Clients Capabilities Live Log Set	ttings Certificates						
🖌 Enable 🕜 Disable 😪 Approve 😝 Group 👎 Dec	line 🔞 Delete 👻 😵 Refresh	Total Pending Approval(0) 👻			1 - 3 of 3	Show 25 👻	per page
Client Name Client De	scription Ca	apabilities	Status	Client Group(s)	Auth Method		Log
□ ▶ ise-mnt-ise470	Ca	apabilities(2 Pub, 1 Sub)	Online	Administrator	Certificate		View
□ ▶ ise-admin-ise470	Ca	apabilities(6 Pub, 2 Sub)	Online	Administrator	Certificate		View
□ ▼ sim01	Ca	apabilities(0 Pub, 2 Sub)	Online	ANC,Session	Certificate		View
Capability D	etail			1 - 2 of 2	Show 25 🔻 per page Pag	je 1 🗘	
Capabilit	ty Name 0	Capability Version	Messaging Role	Message Filter			
O Adaptive	NetworkControl	1.0	Sub				
O Core	t	1.0	Sub				

Step 3 Run the Session download

./session_download.sh -a 192.168.1.158 -u SIM01 -k pxGridClient.jks -p Cisco123 -t root3.jks -q Cisco123
properties
version=1.0.4.19
hostnames=192.168.1.158
username=SIM01
password=
aroup=Session
description=null
keystoreFilename=pxGridClient.iks
keystorePassword=Cisco123
truststoreFilename=root3 iks
truststorePassword=Cisco123
Connecting
00.26.20 356 [main] INFO, com cisco pygrid Configuration - Connecting to bost 192 168 1 158
00.26.20 647 [main] INFO commence on Figuration - Connected OK to best 192.168.1.158
00.26.20.647 [main] INFO commission particle configuration = Client Login to host 12.168.1.158
00.26.20.675 [main] INFO complete and a configuration - Client Login to host 102.160.1.150
Connected
Connecteu Filters (or 11.0.0.0/255.0.0.0.1224/16 L or (orter) for no filter).
Finters (ex. 1.0.0.0/235.0.0.0,1234:;/10) of venter/ for no finter):
Start Lime (ex. 2013-01-31 13:00:00 of center) for no start Lime):
End time (ex. 2015-01-31 13:00:00 or center/ for no end time):
pxgrid controller version=1.0.4.18
Going to uri:https://ise4/0.labi0.com:990/pxgrid/mnt/sd/getsessionListByrime
Session={1p={192.168.1.30}, Audit Session 1a=0AUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUUU
MacAddresses=[UU:UC:29:7C:79:39], State=STARTED, EndpointProfile=VMWare-Device, NAS IP=192.168.1.3, NAS
Port=GigabitEthernet1/0/15, RADIUSAVPairs=[Acct-Session-Id=00000028], Posture Status=null, Posture
Timestamp=, LastUpdateTime=Tue Mar 14 12:38:43 EDT 2017, Session attributeName=Authorization Profiles,
Session attributevalue=PermitAccess, Providers=[None], EndpointCheckResult=none, IdentitySourceFirstPort=0,
IdentitySourcePortStart=0, IdentitySourcePortEnd=0}
Session={ip=[192.168.1.158], Audit Session Id=0A0000001000000150001E814, UserName=00:0C:29:C4:54:40,
MacAddresses=[00:0C:29:C4:54:40], State=STARTED, EndpointProfile=ISE-Appliance, NAS IP=192.168.1.3, NAS
Port=GigabitEthernet1/0/10, RADIUSAVPairs=[Acct-Session-Id=00000016], Posture Status=null, Posture
Timestamp=, LastUpdateTime=Tue Mar 14 12:37:06 EDT 2017, Session attributeName=Authorization_Profiles,
Session attributeValue=PermitAccess, Providers=[None], EndpointCheckResult=none, IdentitySourceFirstPort=0,
IdentitySourcePortStart=0, IdentitySourcePortEnd=0}
Session={ip=[192.168.1.15], Audit Session Id=0A0000010000008206396712, UserName=user7@lab10.com,
ADUserDNSDomain=lab10.com, ADUserNetBIOSName=LAB10, ADUserResolvedIdentities=user7@lab10.com,
ADUserResolvedDNs=CN=user7,CN=Users,DC=lab10,DC=com, MacAddresses=[00:0C:29:CF:07:17], State=STARTED,
ANCstatus=Quarantine, SecurityGroup=Quarantined_Systems, EndpointProfile=Windows7-Workstation, NAS
IP=192.168.1.3, NAS Port=GigabitEthernet1/0/11, RADIUSAVPairs=[Acct-Session-Id=00000097], Posture
Status=null, Posture Timestamp=, LastUpdateTime=Mon Mar 13 13:34:49 EDT 2017, Session
attributeName=Authorization_Profiles, Session attributeValue=Quarantined_Systems, Providers=[None],

EndpointCheckResult=none, IdentitySourceFirstPort=0, IdentitySourcePortStart=0, IdentitySourcePortEnd=0, IsMachineAuthentication=false} Session={ip=[192.168.1.111], Audit Session Id=0A00000100000030017464A9, UserName=LAB10\user1, ADUserDNSDomain=lab10.com, ADUserNetBIOSName=LAB10, ADUserResolvedIdentities=user1@lab10.com, ADUserResolvedDNs=CN=user1, CN=Users, DC=lab10, DC=com, MacAddresses=[00:50:56:86:BC:07], State=STARTED, SecurityGroup=Employees, EndpointProfile=Windows7-Workstation, NAS IP=192.168.1.3, NAS Port=GigabitEthernet1/0/10, RADIUSAVPairs=[Acct-Session-Id=00000034], Posture Status=null, Posture Timestamp=, LastUpdateTime=Tue Mar 14 15:50:33 EDT 2017, Session attributeName=Authorization Profiles, Session attributeValue=Employees, Providers=[None], EndpointCheckResult=none, IdentitySourceFirstPort=0, IdentitySourcePortStart=0, IdentitySourcePortEnd=0, IsMachineAuthentication=false} Session={ip=[], Audit Session Id=0A00000100000077057DE2C5, UserName=00:50:56:86:DA:DE, MacAddresses=[00:50:56:86:DA:DE], State=STARTED, EndpointProfile=VMWare-Device, NAS IP=192.168.1.3, NAS Port=GigabitEthernet1/0/20, RADIUSAVPairs=[Acct-Session-Id=00000083], Posture Status=null, Posture Timestamp=, LastUpdateTime=Mon Mar 13 12:50:38 EDT 2017, Session attributeName=Authorization Profiles, Session attributeValue=PermitAccess, Providers=[None], EndpointCheckResult=none, IdentitySourceFirstPort=0, IdentitySourcePortStart=0, IdentitySourcePortEnd=0 } Session={ip=[192.168.1.136], Audit Session Id=0A00000100000032018140D4, UserName=10:DD:B1:C9:3C:39, MacAddresses=[10:DD:B1:C9:3C:39], State=STARTED, EndpointProfile=Apple-Device, NAS IP=192.168.1.3, NAS Port=GigabitEthernet1/0/12, RADIUSAVPairs=[Acct-Session-Id=00000036], Posture Status=null, Posture Timestamp=, LastUpdateTime=Tue Mar 14 15:55:50 EDT 2017, Session attributeName=Authorization Profiles, Session attributeValue=PermitAccess, Providers=[None], EndpointCheckResult=none, IdentitySourceFirstPort=0, IdentitySourcePortStart=0, IdentitySourcePortEnd=0 } Session={ip=[192.168.1.7], Audit Session Id=0A000001000000130001E5A7, UserName=18:E7:28:2E:29:CB, MacAddresses=[18:E7:28:2E:29:CB], State=STARTED, EndpointProfile=Cisco-Device, NAS IP=192.168.1.3, NAS Port=GigabitEthernet1/0/15, RADIUSAVPairs=[Acct-Session-Id=00000014], Posture Status=null, Posture Timestamp=, LastUpdateTime=Tue Mar 14 12:37:48 EDT 2017, Session attributeName=Authorization Profiles, Session attributeValue=PermitAccess, Providers=[None], EndpointCheckResult=none, IdentitySourceFirstPort=0, IdentitySourcePortStart=0, IdentitySourcePortEnd=0 } Session={ip=[192.168.1.7], Audit Session Id=0A00000100000190001FFA3, UserName=18:E7:28:2E:29:CC, MacAddresses=[18:E7:28:2E:29:CC], State=STARTED, EndpointProfile=Cisco-Device, NAS IP=192.168.1.3, NAS Port=GigabitEthernet1/0/15, RADIUSAVPairs=[Acct-Session-Id=0000001A], Posture Status=null, Posture Timestamp=, LastUpdateTime=Tue Mar 14 12:37:48 EDT 2017, Session attributeName=Authorization Profiles, Session attributeValue=PermitAccess, Providers=[None], EndpointCheckResult=none, IdentitySourceFirstPort=0, IdentitySourcePortStart=0, IdentitySourcePortEnd=0} Session={ip=[], Audit Session Id=0A0000010000003705788C2E, UserName=74:26:AC:5A:82:23, MacAddresses=[74:26:AC:5A:82:23], State=STARTED, EndpointProfile=Cisco-Device, NAS IP=192.168.1.3, NAS Port=GigabitEthernet1/0/6, RADIUSAVPairs=[Acct-Session-Id=00000043], Posture Status=null, Posture Timestamp=, LastUpdateTime=Mon Mar 13 12:40:15 EDT 2017, Session attributeName=Authorization_Profiles, Session attributeValue=PermitAccess, Providers=[None], EndpointCheckResult=none, IdentitySourceFirstPort=0, IdentitySourcePortStart=0, IdentitySourcePortEnd=0 } Session={ip=[192.168.1.6], Audit Session Id=0A000001000000240012B3C3, UserName=74:26:AC:5A:82:24, MacAddresses=[74:26:AC:5A:82:24], State=STARTED, EndpointProfile=Cisco-Device, NAS IP=192.168.1.3, NAS Port=GigabitEthernet1/0/17, RADIUSAVPairs=[Acct-Session-Id=00000025], Posture Status=null, Posture Timestamp=, LastUpdateTime=Tue Mar 14 12:37:48 EDT 2017, Session attributeName=Authorization Profiles, Session attributeValue=PermitAccess, Providers=[None], EndpointCheckResult=none, IdentitySourceFirstPort=0, IdentitySourcePortStart=0, IdentitySourcePortEnd=0 } Session={ip=[192.168.1.43], Audit Session Id=0A000001000000230012AB58, UserName=74:26:AC:5A:82:26, MacAddresses=[74:26:AC:5A:82:26], State=STARTED, EndpointProfile=Cisco-Device, NAS IP=192.168.1.3, NAS Port=GigabitEthernet1/0/17, RADIUSAVPairs=[Acct-Session-Id=00000024], Posture Status=null, Posture Timestamp=, LastUpdateTime=Tue Mar 14 12:37:48 EDT 2017, Session attributeName=Authorization_Profiles, Session attributeValue=PermitAccess, Providers=[None], EndpointCheckResult=none, IdentitySourceFirstPort=0, IdentitySourcePortStart=0, IdentitySourcePortEnd=0 } Session count=11 Connection closed

Viewing Keystore Entries

By viewing the keystore entries you can view the trusted certificate entries for the identity and trust keystores.



```
keytool -list -v -keystore root3.jks
Enter keystore password: Cisco123
Keystore type: JKS
Keystore provider: SUN
Your keystore contains 2 entries
Alias name: ca rootl
Creation date: Mar 15, 2017
Entry type: trustedCertEntry
Owner: CN=lab10-WIN-N3OR1A7H9KL-CA, DC=lab10, DC=com
Issuer: CN=lab10-WIN-N3OR1A7H9KL-CA, DC=lab10, DC=com
Serial number: 6f0fce547462b29a4e866b88536b829d
Valid from: Mon Mar 28 20:33:59 EDT 2016 until: Sun Mar 28 20:43:58 EDT 2021
Certificate fingerprints:
        MD5: 7E:6E:B2:3A:8F:00:17:19:F1:A9:23:C9:F5:C8:B8:25
        SHA1: EA:01:AB:89:F4:A7:77:75:23:0A:29:81:10:D8:AA:F9:02:79:3B:CB
        SHA256:
6A:4C:8E:76:FF:E8:8C:C5:1D:22:5B:ED:4C:E2:7E:8F:A3:55:C4:16:DA:D6:A4:4A:EA:27:47:A4:87:77:25:42
        Signature algorithm name: SHA256withRSA
        Version: 3
Extensions:
#1: ObjectId: 1.3.6.1.4.1.311.21.1 Criticality=false
0000: 02 01 00
                                                      . . .
#2: ObjectId: 2.5.29.19 Criticality=true
BasicConstraints:[
 CAttrue
  PathLen:2147483647
1
#3: ObjectId: 2.5.29.15 Criticality=false
KeyUsage [
 DigitalSignature
  Key_CertSign
 Crl Sign
1
#4: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: 16 EB 8F 72 43 0F 41 9B 68 16 F9 12 10 7E 86 73 ...rC.A.h....s
0010: 3F 01 1B E1
                                                      ?...
1
1
Alias name: isemnt
Creation date: Mar 15, 2017
Entry type: trustedCertEntry
```



Owner: CN=ise470.lab10.com Issuer: CN=lab10-WIN-N3OR1A7H9KL-CA, DC=lab10, DC=com Serial number: 1d60f09b000000000eb Valid from: Thu Feb 16 22:09:34 EST 2017 until: Sat Feb 16 22:19:34 EST 2019 Certificate fingerprints: MD5: 48:06:06:CD:06:24:12:8B:26:3C:0C:CB:55:B0:A4:E6 SHA1: F1:9F:69:D7:74:A4:3B:A7:6B:67:ED:4E:ED:35:FA:9C:CB:3F:51:E6 SHA256: A1:74:B3:DA:FB:E6:26:C7:E9:E3:10:31:A5:33:49:13:D2:2F:A4:28:E2:A4:38:51:FF:0A:32:97:00:25:4C:8E Signature algorithm name: SHA256withRSA Version: 3 Extensions: #1: ObjectId: 1.2.840.113549.1.9.15 Criticality=false 0000: 30 35 30 0E 06 08 2A 86 48 86 F7 0D 03 02 02 02 050...*.H.... 0010: 00 80 30 0E 06 08 2A 86 48 86 F7 0D 03 04 02 02*.H..... 0020: 00 80 30 07 06 05 2B 0E 03 02 07 30 0A 06 08 2A+....0....* 0030: 86 48 86 F7 0D 03 07 .H.... #2: ObjectId: 1.3.6.1.4.1.311.21.10 Criticality=false 0000: 30 32 30 0A 06 08 2B 06 01 05 05 07 03 01 30 0A 020...+..... 0020: 01 04 01 82 37 0A 03 04 30 0A 06 08 2B 06 01 057...0...+... 0030: 05 07 03 02 #3: ObjectId: 1.3.6.1.4.1.311.21.7 Criticality=false 0000: 30 2E 06 26 2B 06 01 04 01 82 37 15 08 84 E9 B3 0...&+....7.... 0010: 0A 87 92 90 6B 87 A1 89 09 84 9E CB 6A 84 C8 96k.....j... 0020: 06 55 84 E2 D7 2F 85 F6 CB 7B 02 01 64 02 01 03 .U.../....d... #4: ObjectId: 1.3.6.1.5.5.7.1.1 Criticality=false AuthorityInfoAccess [[accessMethod: calssuers accessLocation: URIName: ldap:///CN=lab10-WIN-N3OR1A7H9KL-CA, CN=AIA, CN=Public%20Key%20Services, CN=Services, CN=Configuration, DC=lab10, DC=com?cACertificate?base?objectCl ass=certificationAuthority 1 1 #5: ObjectId: 2.5.29.35 Criticality=false AuthorityKeyIdentifier [KeyIdentifier [0000: 16 EB 8F 72 43 0F 41 9B 68 16 F9 12 10 7E 86 73 ...rC.A.h....s 0010: 3F 01 1B E1 ?... 1 #6: ObjectId: 2.5.29.31 Criticality=false CRLDistributionPoints [[DistributionPoint: [URIName: ldap:///CN=lab10-WIN-N3OR1A7H9KL-CA,CN=WIN-N3OR1A7H9KL,CN=CDP,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=lab10,DC=com?certificateRevocat ionList?base?objectClass=cRLDistributionPoint]]] #7: ObjectId: 2.5.29.32 Criticality=false CertificatePolicies [[CertificatePolicyId: [2.5.29.32.0] [] 1 #8: ObjectId: 2.5.29.37 Criticality=false ExtendedKeyUsages [serverAuth emailProtection 1.3.6.1.4.1.311.10.3.4

Cisco Systems © 2017



clientAuth

```
1
#9: ObjectId: 2.5.29.15 Criticality=true
KevUsage [
 DigitalSignature
 Key Encipherment
1
#10: ObjectId: 2.5.29.17 Criticality=false
SubjectAlternativeName [
 DNSName: ise470.lab10.com
1
#11: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: DA 39 A3 EE 5E 6B 4B 0D 32 55 BF EF 95 60 18 90 .9..^kK.2U...`..
0010: AF D8 07 09
                                                . . . .
1
]
*****
```

Step 2 Verify pxGridclient.jks, the identity keystore.

```
keytool -list -v -keystore pxGridClient.jks
Enter keystore password: Cisco123
Keystore type: JKS
Keystore provider: SUN
Your keystore contains 2 entries
Alias name: pxgridmac
Creation date: Mar 15, 2017
Entry type: trustedCertEntry
Owner: EMAILADDRESS=j@cisco.com, CN=johns-macbook-pro.lab10.com, OU=Engineering, O=Cisco, L=Germantown,
ST=Marvland, C=US
Issuer: CN=lab10-WIN-N3OR1A7H9KL-CA, DC=lab10, DC=com
Serial number: 126f78a5000000000f2
Valid from: Tue Mar 14 23:42:07 EDT 2017 until: Thu Mar 14 23:52:07 EDT 2019
Certificate fingerprints:
        MD5: C9:51:9E:3F:BB:92:CC:C1:35:0C:E1:D4:7C:4C:75:23
        SHA1: 98:C5:BF:78:9A:1C:BB:54:04:36:AA:0E:B8:6F:C8:10:C3:46:FB:00
        SHA256:
E0:A4:CC:78:69:A3:95:26:97:82:BA:B1:52:70:DC:43:EF:8C:1B:2D:07:E6:35:D4:BD:AD:03:2B:49:02:1F:23
        Signature algorithm name: SHA256withRSA
        Version: 3
Extensions:
#1: ObjectId: 1.2.840.113549.1.9.15 Criticality=false
0000: 30 35 30 0E 06 08 2A 86 48 86 F7 0D 03 02 02 02 050...*.H....
0010: 00 80 30 0E 06 08 2A 86
                              48 86 F7 0D 03 04 02 02 .....*.H.....
0020: 00 80 30 07 06 05 2B 0E
                              03 02 07 30 0A 06 08 2A
                                                       0030: 86 48 86 F7 0D 03 07
                                                        .H....
#2: ObjectId: 1.3.6.1.4.1.311.21.10 Criticality=false
0000: 30 32 30 0A 06 08 2B 06 01 05 05 07 03 01 30 0A 020...+.....
```

0010: 06 08 2B 06 01 05 05 07 03 04 30 0C 06 0A 2B 06 ...+....0...+. 0020: 01 04 01 82 37 0A 03 04 30 0A 06 08 2B 06 01 057...0...+.. 0030: 05 07 03 02 #3: ObjectId: 1.3.6.1.4.1.311.21.7 Criticality=false 0000: 30 2E 06 26 2B 06 01 04 01 82 37 15 08 84 E9 B3 0...&+....7.... 0010: 0A 87 92 90 6B 87 A1 89 09 84 9E CB 6A 84 C8 96k.....j... 0020: 06 55 84 E2 D7 2F 85 F6 CB 7B 02 01 64 02 01 03 .U.../....d... #4: ObjectId: 1.3.6.1.5.5.7.1.1 Criticality=false AuthorityInfoAccess [ſ accessMethod: calssuers accessLocation: URIName: ldap:///CN=lab10-WIN-N3OR1A7H9KL-CA, CN=AIA, CN=Public%20Key%20Services, CN=Services, CN=Configuration, DC=lab10, DC=com?cACertificate?base?objectCl ass=certificationAuthority #5: ObjectId: 2.5.29.35 Criticality=false AuthorityKeyIdentifier [KeyIdentifier [0000: 16 EB 8F 72 43 0F 41 9B 68 16 F9 12 10 7E 86 73 ...rC.A.h....s 0010: 3F 01 1B E1 ?... #6: ObjectId: 2.5.29.31 Criticality=false CRLDistributionPoints [[DistributionPoint: [URIName: ldap:///CN=lab10-WIN-N3OR1A7H9KL-CA,CN=WIN-N3OR1A7H9KL,CN=CDP,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=lab10,DC=com?certificateRevocat ionList?base?objectClass=cRLDistributionPoint]]] #7: ObjectId: 2.5.29.32 Criticality=false CertificatePolicies [[CertificatePolicyId: [2.5.29.32.0] []] #8: ObjectId: 2.5.29.37 Criticality=false ExtendedKeyUsages [serverAuth emailProtection 1.3.6.1.4.1.311.10.3.4 clientAuth #9: ObjectId: 2.5.29.15 Criticality=true KeyUsage [DigitalSignature Key_Encipherment #10: ObjectId: 2.5.29.14 Criticality=false SubjectKeyIdentifier [KeyIdentifier [0000: 92 49 28 E0 BF 23 90 7C E3 52 12 0E DF 06 75 55 .I(..#...R...uU 0010: FF C2 95 86

1

1 1

1

1

]] CISCO



Alias name: 1 Creation date: Mar 15, 2017 Entry type: PrivateKeyEntry Certificate chain length: 2 Certificate[1]: Owner: EMAILADDRESS=j@cisco.com, CN=johns-macbook-pro.lab10.com, OU=Engineering, O=Cisco, L=Germantown, ST=Maryland, C=US Issuer: CN=lab10-WIN-N3OR1A7H9KL-CA, DC=lab10, DC=com Serial number: 126f78a5000000000f2 Valid from: Tue Mar 14 23:42:07 EDT 2017 until: Thu Mar 14 23:52:07 EDT 2019 Certificate fingerprints: MD5: C9:51:9E:3F:BB:92:CC:C1:35:0C:E1:D4:7C:4C:75:23 SHA1: 98:C5:BF:78:9A:1C:BB:54:04:36:AA:0E:B8:6F:C8:10:C3:46:FB:00 SHA256: E0:A4:CC:78:69:A3:95:26:97:82:BA:B1:52:70:DC:43:EF:8C:1B:2D:07:E6:35:D4:BD:AD:03:2B:49:02:1F:23 Signature algorithm name: SHA256withRSA Version: 3 Extensions: #1: ObjectId: 1.2.840.113549.1.9.15 Criticality=false 0000: 30 35 30 0E 06 08 2A 86 48 86 F7 0D 03 02 02 02 050...*.H..... 0010: 00 80 30 0E 06 08 2A 86 48 86 F7 0D 03 04 02 02*.H..... 0030: 86 48 86 F7 0D 03 07 . H #2: ObjectId: 1.3.6.1.4.1.311.21.10 Criticality=false 0000: 30 32 30 0A 06 08 2B 06 01 05 05 07 03 01 30 0A 020...+....0. 0010: 06 08 2B 06 01 05 05 07 03 04 30 OC 06 0A 2B 06 0020: 01 04 01 82 37 0A 03 04 30 0A 06 08 2B 06 01 057...0...+... 0030: 05 07 03 02 #3: ObjectId: 1.3.6.1.4.1.311.21.7 Criticality=false 0000: 30 2E 06 26 2B 06 01 04 01 82 37 15 08 84 E9 B3 0..&+....7.... 0010: 0A 87 92 90 6B 87 A1 89 09 84 9E CB 6A 84 C8 96k.....j...k....j... 0020: 06 55 84 E2 D7 2F 85 F6 CB 7B 02 01 64 02 01 03 .U.../....d... #4: ObjectId: 1.3.6.1.5.5.7.1.1 Criticality=false AuthorityInfoAccess [ſ accessMethod: calssuers accessLocation: URIName: ldap:///CN=lab10-WIN-N3OR1A7H9KL-CA, CN=AIA, CN=Public%20Key%20Services, CN=Services, CN=Configuration, DC=lab10, DC=com?cACertificate?base?objectCl ass=certificationAuthority #5: ObjectId: 2.5.29.35 Criticality=false AuthorityKeyIdentifier [KeyIdentifier [0000: 16 EB 8F 72 43 0F 41 9B 68 16 F9 12 10 7E 86 73 ...rc.A.h....s 0010: 3F 01 1B E1 ? . . . 1 #6: ObjectId: 2.5.29.31 Criticality=false CRLDistributionPoints [[DistributionPoint: [URIName: ldap:///CN=lab10-WIN-N3OR1A7H9KL-CA, CN=WIN-N3OR1A7H9KL,CN=CDP,CN=Public%20Key%20Services,CN=Services,CN=Configuration,DC=lab10,DC=com?certificateRevocat ionList?base?objectClass=cRLDistributionPoint] 11 #7: ObjectId: 2.5.29.32 Criticality=false CertificatePolicies [[CertificatePolicyId: [2.5.29.32.0] []] 1



#8: ObjectId: 2.5.29.37 Criticality=false ExtendedKeyUsages [serverAuth emailProtection 1.3.6.1.4.1.311.10.3.4 clientAuth 1 #9: ObjectId: 2.5.29.15 Criticality=true KeyUsage [DigitalSignature Key Encipherment] #10: ObjectId: 2.5.29.14 Criticality=false SubjectKeyIdentifier [KeyIdentifier [0000: 92 49 28 E0 BF 23 90 7C E3 52 12 0E DF 06 75 55 .I(..#...R....uU 0010: FF C2 95 86] 1 Certificate[2]: Owner: CN=lab10-WIN-N3OR1A7H9KL-CA, DC=lab10, DC=com Issuer: CN=lab10-WIN-N3OR1A7H9KL-CA, DC=lab10, DC=com Serial number: 6f0fce547462b29a4e866b88536b829d Valid from: Mon Mar 28 20:33:59 EDT 2016 until: Sun Mar 28 20:43:58 EDT 2021 Certificate fingerprints: MD5: 7E:6E:B2:3A:8F:00:17:19:F1:A9:23:C9:F5:C8:B8:25 SHA1: EA:01:AB:89:F4:A7:77:75:23:0A:29:81:10:D8:AA:F9:02:79:3B:CB SHA256: 6A:4C:8E:76:FF:E8:8C:C5:1D:22:5B:ED:4C:E2:7E:8F:A3:55:C4:16:DA:D6:A4:4A:EA:27:47:A4:87:77:25:42 Signature algorithm name: SHA256withRSA Version: 3 Extensions: #1: ObjectId: 1.3.6.1.4.1.311.21.1 Criticality=false 0000: 02 01 00 . . . #2: ObjectId: 2.5.29.19 Criticality=true BasicConstraints:[CA:true PathLen:2147483647 #3: ObjectId: 2.5.29.15 Criticality=false KeyUsage [DigitalSignature Key_CertSign Crl_Sign 1 #4: ObjectId: 2.5.29.14 Criticality=false SubjectKeyIdentifier [KeyIdentifier [0000: 16 EB 8F 72 43 0F 41 9B 68 16 F9 12 10 7E 86 73 ...rC.A.h....s 0010: 3F 01 1B E1 ?... 1 1 *****

Troubleshooting

This section describes some troubleshooting tips:

• Avoid pxGrid scripting error messages by verifying that the pxGrid client hostname and ISE pxGrid node are resolvable via DNS.

References

Using ISE 2.1 Internal Certificate Authority (CA) to Deploy Certificates to Cisco Platform Exchange Grid (pxGrid) clients

Using ISE 2.2 Internal Certificate Authority (CA) to Deploy Certificates to Cisco Platform Exchange Grid (pxGrid) clients