Deploying Certificates with Cisco pxGrid

Using Self-Signed Certificates Updates to Cisco ISE 2.0/2.1/2.2

Author: John Eppich

Table of Contents

About this Document

This document covers Self-Signed Certificate 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: https://communities.cisco.com/docs/DOC-68291

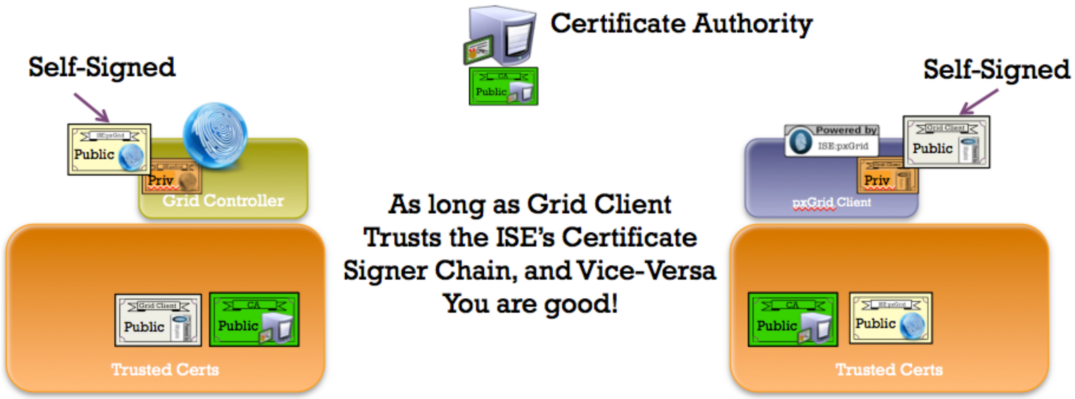
To obtain the Cisco ISE images and appropriate SDKs, please sign up for Devnet: https://developer.cisco.com/site/pxgrid/

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 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

Deploying pxGrid using self-signed certificates for both the ISE pxGrid node and the pxGrid client is an alternative for testing instead of using the sample certificates in the pxGrid SDK. This is used in a Proof of Concept (POC) Environment. Self-signed certificates do not originate from a trusted source and are less secure than using Certificate Authority (CA). However, in this document ISE trusts the public key of the pxGrid client by importing the pxGrid client's public key into the ISE trusted certificate store. The pxGrid client trusts the ISE public certificate in the pxGrid client's trusted keystore.



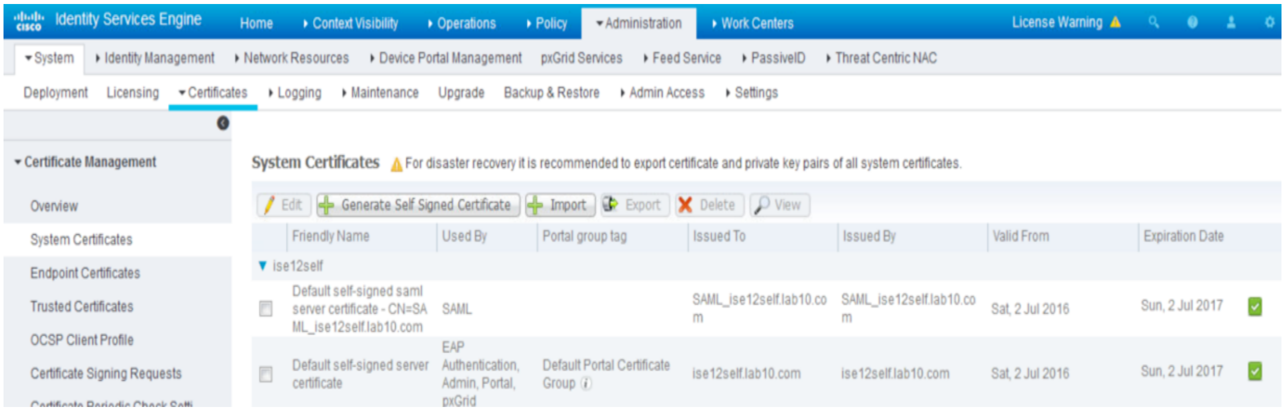
As long as Grid Client Trusts the ISE's Certificate Signer Chain, and Vice-Versa You are good!

ISE 2.0/2.1 Self-Signed ISE pxGrid Node Configuration

Self-Signed ISE pxGrid node certificate & pxGrid persona configuration

There is no need to export the ISE Identity self-signed certificate into the ISE trusted certificate store as in ISE versions 1.3 and I.4. You can just enable the pxGrid node.

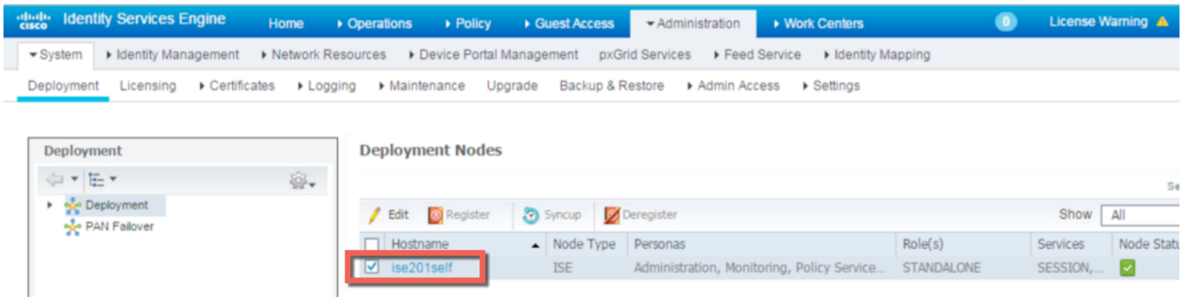
Step 1 Select **Administration->System->Certificates->System Certificates**
Note, the Identity Certificate certificate is specifically used by admin and pxGrid



System Certificates ⚠ For disaster recovery it is recommended to export certificate and private key pairs of all system certificates.

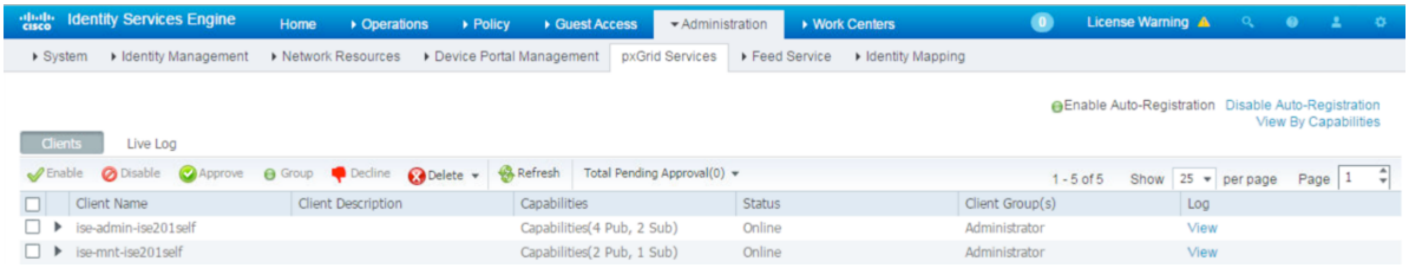
	Friendly Name	Used By	Portal group tag	Issued To	Issued By	Valid From	Expiration Date	
▼ ise12self								
□	Default self-signed saml server certificate - CN=SAML_ise12self.lab10.com	SAML		SAML_ise12self.lab10.com	SAML_ise12self.lab10.com	Sat, 2 Jul 2016	Sun, 2 Jul 2017	✓
□	Default self-signed server certificate	EAP Authentication, Admin, Portal, pxGrid	Default Portal Certificate Group ⓘ	ise12self.lab10.com	ise12self.lab10.com	Sat, 2 Jul 2016	Sun, 2 Jul 2017	✓

Step 2 Select **Administration->System->Deployment->Edit the ISE pxGrid node**



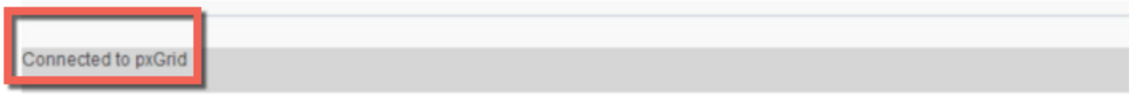
□	Hostname	Node Type	Personas	Role(s)	Services	Node Statu
☑	ise201self	ISE	Administration, Monitoring, Policy Service...	STANDALONE	SESSION,...	✓

Step 3 Enable **pxGrid**
Step 4 Select **Save**
Step 5 Select **Administration->pxGrid Services** to view the ISE published nodes
You should the ISE published nodes appear



□	Client Name	Client Description	Capabilities	Status	Client Group(s)	Log
□ ▶	ise-admin-ise201self		Capabilities(4 Pub, 2 Sub)	Online	Administrator	View
□ ▶	ise-mnt-ise201self		Capabilities(2 Pub, 1 Sub)	Online	Administrator	View

Step 6 Verify that there is connectivity to the ISE pxGrid node


Connected to pxGrid

Generating Self-Signed pxGrid Client Certificate

This section details the self-signed certificate generation process on the pxGrid client. Once the pxGrid public/private key pair is generated, a PKCS 12 file (self1.p12) will be created from the private key (i.e. self1.key).

This PKCS 12 file will be imported into the destination or identity keystore (i.e. self1.jks), which will serve as the keystoreFilename and keystorePassword for the pxGrid scripts. Both the ISE identity cert and the public certificate will be added to this keystore as well.

The ISE identity certificate will also be added to the trust keystore (i.e. root1.jks), which will serve as the truststoreFilename and truststorePassword.

Step 1 Generate a private key (i.e. self1.key) for the pxGrid client

```
openssl genrsa -out self1.key 4096

Generating RSA private key, 4096 bit long modulus
..................++
.............................++
e is 65537 (0x10001)
```

Step 2 Generate the self-signed CSR (i.e. self1.csr) request

```
openssl req -new -key self1.key -out self1.csr

You are about to be asked to enter information that will be incorporated
into your certificate request.
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.lab10.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 Generate self-signed certificate (i.e. self1.cer)

```
openssl req -x509 -days 365 -key self1.key -in self1.csr -out self1.cer
```

Step 4 A PKCS12 file (i.e. self1.p12) will be created from the private key

```
openssl pkcs12 -export -out self1.p12 -inkey self1.key -in self1.cer

Enter Export Password: cisco123
Verifying - Enter Export Password: cisco123
```

Step 5 The self1.p12 will be imported into the identity keystore (i.e. self1.jks). The keystore filename can be a random filename with a .jks extension. This will serve as the keystoreFilename and associated keystorePassword in the pxGrid scripts.

```
keytool -importkeystore -srckeystore self1.p12 -destkeystore self1.jks  -srcstoretype PKCS12

Enter destination keystore password:  cisco123
Re-enter new password: cisco123
Enter source keystore password:  cisco123
Entry for alias 1 successfully imported.
Import command completed:  1 entries successfully imported, 0 entries failed or cancelled
```

Step 6 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->System->Certificates->select the Default Signed ISE Signed Certificate and Export Certificate Only**

Step 7 Convert the .pem file to .der format.

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

Step 8 Add the ISE identity cert to the identity keystore. This will be used for securing bulk session downloads from the ISE MNT node when running the pxGrid session download scripts.

```
keytool -import -alias mnt1 -keystore self1.jks -file isemnt.der
Enter keystore password:  cisco123
Owner: CN=ise.lab6.com
Issuer: CN=ise.lab6.com
Serial number: 548502f500000000ec27e53c1dd64f46
Valid from: Sun Dec 07 17:46:29 PST 2014 until: Mon Dec 07 17:46:29 PST 2015
Certificate fingerprints:
         MD5:  04:7D:67:04:EC:D2:F5:BC:DC:79:4D:0A:FF:62:09:FD
         SHA1: 5A:7B:02:E4:07:A1:D2:0B:7D:A5:AE:83:27:3B:E7:33:33:30:1E:32
         SHA256:
C4:21:6C:6F:5B:06:F3:2C:D7:26:35:CB:BE:2B:1B:FF:0E:EE:09:91:F6:B6:54:0C:6F:63:CB:43:1F:77:F2:37
         Signature algorithm name: SHA1withRSA
         Version: 3

Extensions:
```

```
#1: ObjectId: 2.5.29.19 Criticality=false
BasicConstraints:[
  CA:true
  PathLen:2147483647
]

#2: ObjectId: 2.5.29.37 Criticality=false
ExtendedKeyUsages [
  serverAuth
  clientAuth
]

#3: ObjectId: 2.5.29.15 Criticality=false
KeyUsage [
  DigitalSignature
  Key_Encipherment
  Key_Agreement
  Key_CertSign
]

#4: ObjectId: 2.16.840.1.113730.1.1 Criticality=false
NetscapeCertType [
   SSL server
]

#5: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: C4 F3 1A 9E 7B 1B 14 4F   51 9E A4 88 33 07 7A AC  .......OQ...3.z.
0010: 75 37 36 D4                                        u76.
]
]

Trust this certificate? [no]:  yes
Certificate was added to keystore
```

Step 9 Import the pxGrid client certificate into the identity keystore.

```
keytool -import -alias pxGridclient1 -keystore self1.jks -file self1.cer

Enter keystore password:  cisco123
Certificate already exists in keystore under alias <1>
Do you still want to add it? [no]:  y
Certificate was not 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 10 Import the ISE identity cert into the trust keystore (i.e. root1.jks). This will serve as the truststore Filename and truststore Password for the pxGrid scripts.

```
keytool -import -alias root1 -keystore root1.jks -file isemnt.der
Enter keystore password:  cisco123
Re-enter new password: cisco123
Owner: CN=ise.lab6.com
Issuer: CN=ise.lab6.com
Serial number: 548502f500000000ec27e53c1dd64f46
Valid from: Sun Dec 07 17:46:29 PST 2014 until: Mon Dec 07 17:46:29 PST 2015
Certificate fingerprints:
```

```
         MD5:  04:7D:67:04:EC:D2:F5:BC:DC:79:4D:0A:FF:62:09:FD
         SHA1: 5A:7B:02:E4:07:A1:D2:0B:7D:A5:AE:83:27:3B:E7:33:33:30:1E:32
         SHA256:
C4:21:6C:6F:5B:06:F3:2C:D7:26:35:CB:BE:2B:1B:FF:0E:EE:09:91:F6:B6:54:0C:6F:63:CB:43:1F:77:F2:37
         Signature algorithm name: SHA1withRSA
         Version: 3

Extensions:

#1: ObjectId: 2.5.29.19 Criticality=false
BasicConstraints:[
  CA:true
  PathLen:2147483647
]

#2: ObjectId: 2.5.29.37 Criticality=false
ExtendedKeyUsages [
  serverAuth
  clientAuth
]

#3: ObjectId: 2.5.29.15 Criticality=false
KeyUsage [
  DigitalSignature
  Key_Encipherment
  Key_Agreement
  Key_CertSign
]

#4: ObjectId: 2.16.840.1.113730.1.1 Criticality=false
NetscapeCertType [
   SSL server
]

#5: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: C4 F3 1A 9E 7B 1B 14 4F   51 9E A4 88 33 07 7A AC  .......OQ...3.z.
0010: 75 37 36 D4                                        u76.
]
]

Trust this certificate? [no]:  yes
Certificate was added to keystore
```

Step 11 Upload the pxGrid client public certificate (self1.cer) into the ISE trusted certificate store. **Administration->System Certificates->Trusted Certificates->upload the self1.cer from the pxGrid client**

Step 12 Under **Trusted For**, enable **Trust for authentication within ISE**

Step 13 Select **Submit**

Step 14 Copy the identity keystore (self1.jks) and trust keystore (root1.jks) into the ../samples/bin/.. folder

Testing pxGrid client and ISE pxGrid node

Sample pxGrid scripts register.sh and session_download.sh will be run to ensure pxGrid client connections and pxGrid registration.

Step 1 Register the pxGrid client

Note: The “Exception in thread…” is a known bug with pxGrid SDK 1.0.4.19. This only affects the sample script. The pxGrid client should successfully register to the ISE pxGrid node.

```
./multigroupclient.sh -a 10.0.0.96 -u pxGridclient -k self1.jks -p cisco123 -t root1.jks -q cisco123 -g
Session -d pxGrid Client
------- properties -------
  version=1.0.4.19
  hostnames=192.168.1.158
  username=MAC01
  password=
  group=Session,ANC,Session
  description=pxGrid
  keystoreFilename=self1.jks
  keystorePassword=Cisco123
  truststoreFilename=ise22root.jks
  truststorePassword=Cisco123
--------------------------
17:56:53.649 [Thread-1] INFO  com.cisco.pxgrid.ReconnectionManager - Started
Connecting...
17:56:53.667 [Thread-1] INFO  com.cisco.pxgrid.Configuration - Connecting to host 192.168.1.158
17:56:53.896 [Thread-1] INFO  com.cisco.pxgrid.Configuration - Connected OK to host 192.168.1.158
17:56:53.896 [Thread-1] INFO  com.cisco.pxgrid.Configuration - Client Login to host 192.168.1.158
17:56:53.932 [Thread-1] INFO  com.cisco.pxgrid.Configuration - Client Login OK to host 192.168.1.158
Connected
17:56:54.950 [Thread-1] INFO  com.cisco.pxgrid.ReconnectionManager - Connected
Create ANC Policy: ANC1488927412914 Result - com.cisco.pxgrid.model.anc.ANCResult@71a794e5[
  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)
```

Step 2 Run Session Download

```
./session_download.sh -keystoreFilename self1.jks -keystorePassword cisco123 -truststoreFilename root1.jks -
truststorePassword cisco123 -username pxGridclient -hostname 10.0.0.96

------- properties -------
version=1.0.0
hostnames=10.0.0.96
username=pxGridclient
keystoreFilename=self1.jks
keystorePassword=cisco123
truststoreFilename=root1.jks
truststorePassword=cisco123
filter=null
start=null
end=null
--------------------------
connecting...
connected.
starting at Wed Dec 10 11:16:04 PST 2014...

session (ip=10.0.0.18, Audit Session Id=0A0000020000000B006E1086, User Name=jeppich, AD User DNS
Domain=lab6.com, AD Host DNS Domain=null, AD User NetBIOS Name=LAB6, AD Host NETBIOS Name=null, Calling
station id=00:0C:29:D1:8D:90, Session state= STARTED, Epsstatus=null, Security Group=null, Endpoint
Profile=VMWare-Device, NAS IP=10.0.0.2, NAS Port=GigabitEthernet1/0/15, RADIUSAVPairs=[ Acct-Session-
Id=00000002], Posture Status=null, Posture Timestamp=, Session Last Update Time=Wed Dec 10 08:27:59 PST 2014
)... ending at: Wed Dec 10 11:16:04 PST 2014

---------------------------------------------------
downloaded 1 sessions in 74 milliseconds
---------------------------------------------------
```

```
connection closed
```

Viewing keystore Entries

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

```
keytool -list -v -keystore self1.jks
Enter keystore password:  cisco123

Keystore type: JKS
Keystore provider: SUN

Your keystore contains 2 entries

Alias name: 1
Creation date: Dec 10, 2014
Entry type: PrivateKeyEntry
Certificate chain length: 1
Certificate[1]:
Owner: O=Internet Widgits Pty Ltd, ST=Some-State, C=AU
Issuer: O=Internet Widgits Pty Ltd, ST=Some-State, C=AU
Serial number: e44965db7b264e4e
Valid from: Wed Dec 10 10:18:47 PST 2014 until: Thu Dec 10 10:18:47 PST 2015
Certificate fingerprints:
         MD5:  62:81:21:DF:44:DF:83:44:04:47:36:5B:B0:C0:8A:DD
         SHA1: B5:E6:6A:CE:B2:49:1E:35:46:E1:12:63:0A:73:DA:DD:F9:53:9F:6F
         SHA256:
C4:62:A3:A3:F7:2F:C7:2E:26:0E:06:88:AE:09:18:E9:00:DC:05:3C:E4:1D:EC:50:7E:C5:99:1F:80:DC:AC:12
         Signature algorithm name: SHA1withRSA
         Version: 3

Extensions:

#1: ObjectId: 2.5.29.35 Criticality=false
AuthorityKeyIdentifier [
KeyIdentifier [
0000: 35 04 62 FF 50 78 C2 1C   7E AD 57 6D 05 72 E1 46  5.b.Px....Wm.r.F
0010: 20 6B 08 21                                          k.!
]
[O=Internet Widgits Pty Ltd, ST=Some-State, C=AU]
SerialNumber: [    e44965db 7b264e4e]
]

#2: ObjectId: 2.5.29.19 Criticality=false
BasicConstraints:[
  CA:true
  PathLen:2147483647
]

#3: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: 35 04 62 FF 50 78 C2 1C   7E AD 57 6D 05 72 E1 46  5.b.Px....Wm.r.F
0010: 20 6B 08 21                                          k.!
]
]



*******************************************
*******************************************


Alias name: mnt1
Creation date: Dec 10, 2014
Entry type: trustedCertEntry

Owner: CN=ise.lab6.com
```

```
Issuer: CN=ise.lab6.com
Serial number: 548502f500000000ec27e53c1dd64f46
Valid from: Sun Dec 07 17:46:29 PST 2014 until: Mon Dec 07 17:46:29 PST 2015
Certificate fingerprints:
        MD5:  04:7D:67:04:EC:D2:F5:BC:DC:79:4D:0A:FF:62:09:FD
        SHA1: 5A:7B:02:E4:07:A1:D2:0B:7D:A5:AE:83:27:3B:E7:33:33:30:1E:32
        SHA256:
C4:21:6C:6F:5B:06:F3:2C:D7:26:35:CB:BE:2B:1B:FF:0E:EE:09:91:F6:B6:54:0C:6F:63:CB:43:1F:77:F2:37
        Signature algorithm name: SHA1withRSA
        Version: 3

Extensions:

#1: ObjectId: 2.5.29.19 Criticality=false
BasicConstraints:[
  CA:true
  PathLen:2147483647
]

#2: ObjectId: 2.5.29.37 Criticality=false
ExtendedKeyUsages [
  serverAuth
  clientAuth
]

#3: ObjectId: 2.5.29.15 Criticality=false
KeyUsage [
  DigitalSignature
  Key_Encipherment
  Key_Agreement
  Key_CertSign
]

#4: ObjectId: 2.16.840.1.113730.1.1 Criticality=false
NetscapeCertType [
   SSL server
]

#5: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: C4 F3 1A 9E 7B 1B 14 4F   51 9E A4 88 33 07 7A AC  .......OQ...3.z.
0010: 75 37 36 D4                                        u76.
]
]

keytool -list -v -keystore root1.jks
Enter keystore password:  cisco123

Keystore type: JKS
Keystore provider: SUN

Your keystore contains 1 entry

Alias name: root1
Creation date: Dec 10, 2014
Entry type: trustedCertEntry

Owner: CN=ise.lab6.com
Issuer: CN=ise.lab6.com
Serial number: 548502f500000000ec27e53c1dd64f46
Valid from: Sun Dec 07 17:46:29 PST 2014 until: Mon Dec 07 17:46:29 PST 2015
Certificate fingerprints:
        MD5:  04:7D:67:04:EC:D2:F5:BC:DC:79:4D:0A:FF:62:09:FD
        SHA1: 5A:7B:02:E4:07:A1:D2:0B:7D:A5:AE:83:27:3B:E7:33:33:30:1E:32
        SHA256:
C4:21:6C:6F:5B:06:F3:2C:D7:26:35:CB:BE:2B:1B:FF:0E:EE:09:91:F6:B6:54:0C:6F:63:CB:43:1F:77:F2:37
        Signature algorithm name: SHA1withRSA
        Version: 3

Extensions:
```

```
#1: ObjectId: 2.5.29.19 Criticality=false
BasicConstraints:[
  CA:true
  PathLen:2147483647
]

#2: ObjectId: 2.5.29.37 Criticality=false
ExtendedKeyUsages [
  serverAuth
  clientAuth
]

#3: ObjectId: 2.5.29.15 Criticality=false
KeyUsage [
  DigitalSignature
  Key_Encipherment
  Key_Agreement
  Key_CertSign
]

#4: ObjectId: 2.16.840.1.113730.1.1 Criticality=false
NetscapeCertType [
   SSL server
]

#5: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: C4 F3 1A 9E 7B 1B 14 4F   51 9E A4 88 33 07 7A AC  .......OQ...3.z.
0010: 75 37 36 D4                                        u76.
]
]
```

Troubleshooting

This section describes some troubleshooting tips:

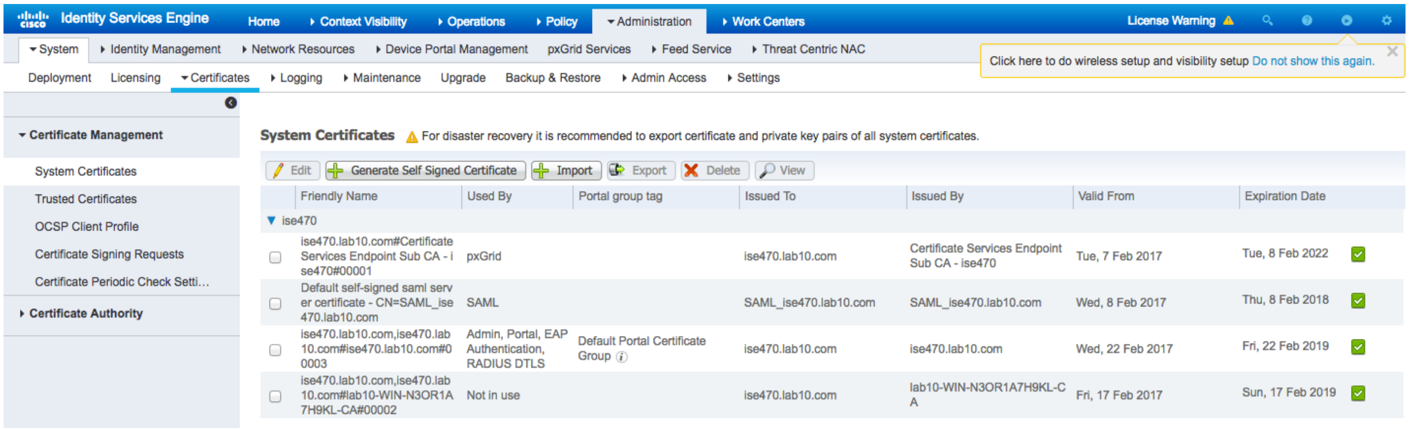
- Avoid pxGrid scripting error messages by verifying that the pxGrid client hostname and ISE pxGrid are resolvable via DNS.

Using Self-Signed Certs without ISE 2.2 Internal 2.2 CA Authority

Self-Signed ISE pxGrid node certificate & pxGrid persona configuration

Step 1 Select **Administration->System->Certificates**

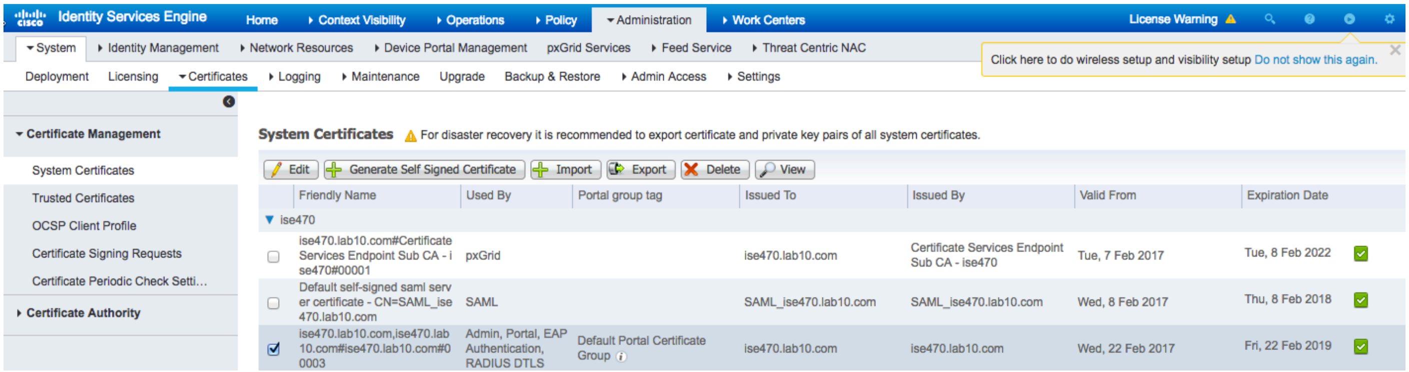
Note the pxGrid certificate (ise470.lab10.com#Certificate is signed by the internal 2.2 certificate store and the ISE identity certificate is signed by the ISE identity certificate



System Certificates ⚠ For disaster recovery it is recommended to export certificate and private key pairs of all system certificates.

	Friendly Name	Used By	Portal group tag	Issued To	Issued By	Valid From	Expiration Date	
▼ ise470								
☐	ise470.lab10.com#Certificate Services Endpoint Sub CA - ise470#00001	pxGrid		ise470.lab10.com	Certificate Services Endpoint Sub CA - ise470	Tue, 7 Feb 2017	Tue, 8 Feb 2022	✓
☐	Default self-signed saml server certificate - CN=SAML_ise470.lab10.com	SAML		SAML_ise470.lab10.com	SAML_ise470.lab10.com	Wed, 8 Feb 2017	Thu, 8 Feb 2018	✓
☐	ise470.lab10.com,ise470.lab10.com#ise470.lab10.com#00003	Admin, Portal, EAP Authentication, RADIUS DTLS	Default Portal Certificate Group ⓘ	ise470.lab10.com	ise470.lab10.com	Wed, 22 Feb 2017	Fri, 22 Feb 2019	✓
☐	ise470.lab10.com,ise470.lab10.com#lab10-WIN-N3OR1A7H9KL-CA#00002	Not in use		ise470.lab10.com	lab10-WIN-N3OR1A7H9KL-CA	Fri, 17 Feb 2017	Sun, 17 Feb 2019	✓

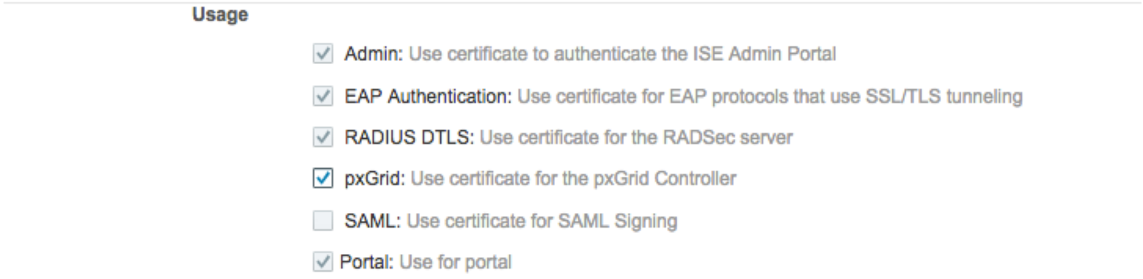
Step 2 Select **Administration->System->Certificates->System Certificates->**select **ISE Identity Cert admin** (ise470.lab10.com#ise470.lab10.com)->**Edit**



System Certificates ⚠ For disaster recovery it is recommended to export certificate and private key pairs of all system certificates.

	Friendly Name	Used By	Portal group tag	Issued To	Issued By	Valid From	Expiration Date	
▼ ise470								
☐	ise470.lab10.com#Certificate Services Endpoint Sub CA - ise470#00001	pxGrid		ise470.lab10.com	Certificate Services Endpoint Sub CA - ise470	Tue, 7 Feb 2017	Tue, 8 Feb 2022	✓
☐	Default self-signed saml server certificate - CN=SAML_ise470.lab10.com	SAML		SAML_ise470.lab10.com	SAML_ise470.lab10.com	Wed, 8 Feb 2017	Thu, 8 Feb 2018	✓
☑	ise470.lab10.com,ise470.lab10.com#ise470.lab10.com#00003	Admin, Portal, EAP Authentication, RADIUS DTLS	Default Portal Certificate Group ⓘ	ise470.lab10.com	ise470.lab10.com	Wed, 22 Feb 2017	Fri, 22 Feb 2019	✓

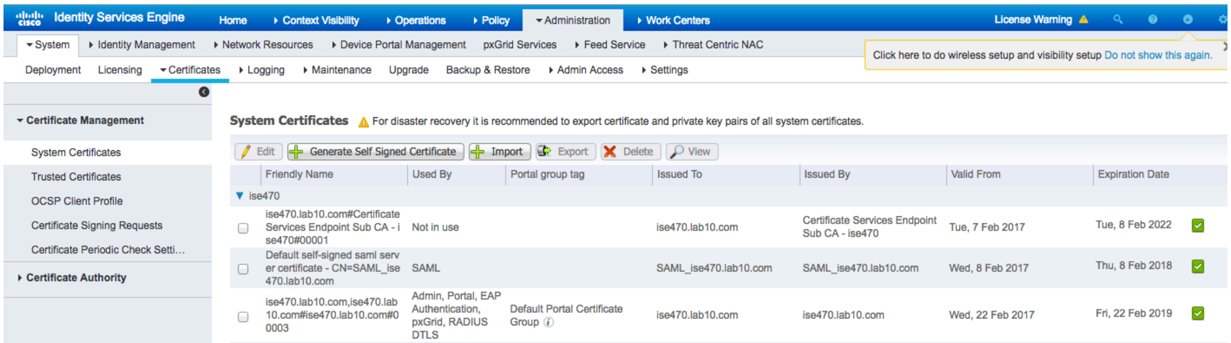
Step 3 Under usage, select “**pxGrid**”



Usage

- ☑ Admin: Use certificate to authenticate the ISE Admin Portal
- ☑ EAP Authentication: Use certificate for EAP protocols that use SSL/TLS tunneling
- ☑ RADIUS DTLS: Use certificate for the RADSec server
- ☑ pxGrid: Use certificate for the pxGrid Controller
- ☐ SAML: Use certificate for SAML Signing
- ☑ Portal: Use for portal

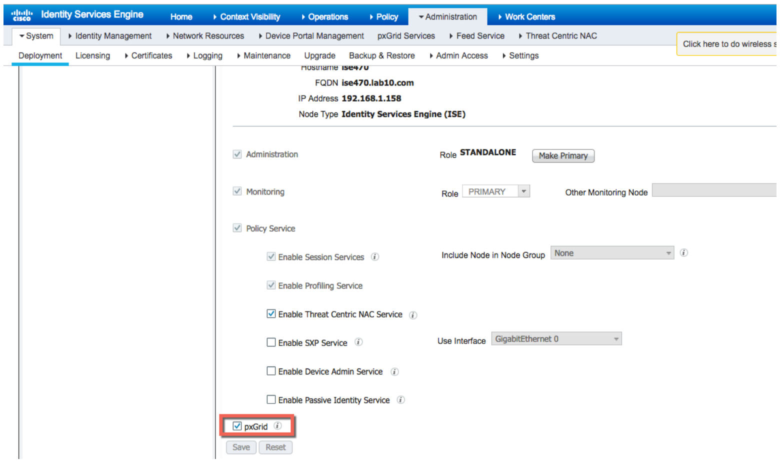
Step 4 Select **Save**
You should see:



System Certificates For disaster recovery it is recommended to export certificate and private key pairs of all system certificates.

	Friendly Name	Used By	Portal group tag	Issued To	Issued By	Valid From	Expiration Date	
▼ ise470								
☐	ise470.lab10.com#Certificate Services Endpoint Sub CA - ise470#00001	Not in use		ise470.lab10.com	Certificate Services Endpoint Sub CA - ise470	Tue, 7 Feb 2017	Tue, 8 Feb 2022	✓
☐	Default self-signed saml server certificate - CN=SAML_ise470.lab10.com	SAML		SAML_ise470.lab10.com	SAML_ise470.lab10.com	Wed, 8 Feb 2017	Thu, 8 Feb 2018	✓
☐	ise470.lab10.com,ise470.lab10.com#ise470.lab10.com#00003	Admin, Portal, EAP Authentication, pxGrid, RADIUS DTLS	Default Portal Certificate Group	ise470.lab10.com	ise470.lab10.com	Wed, 22 Feb 2017	Fri, 22 Feb 2019	✓

Step 5 Select **Administration->System->Deployment->select node->Edit->enable pxGrid**



Hostname **ise470**
FQDN **ise470.lab10.com**
IP Address **192.168.1.158**
Node Type **Identity Services Engine (ISE)**

☑ Administration — Role **STANDALONE**

☑ Monitoring — Role PRIMARY — Other Monitoring Node

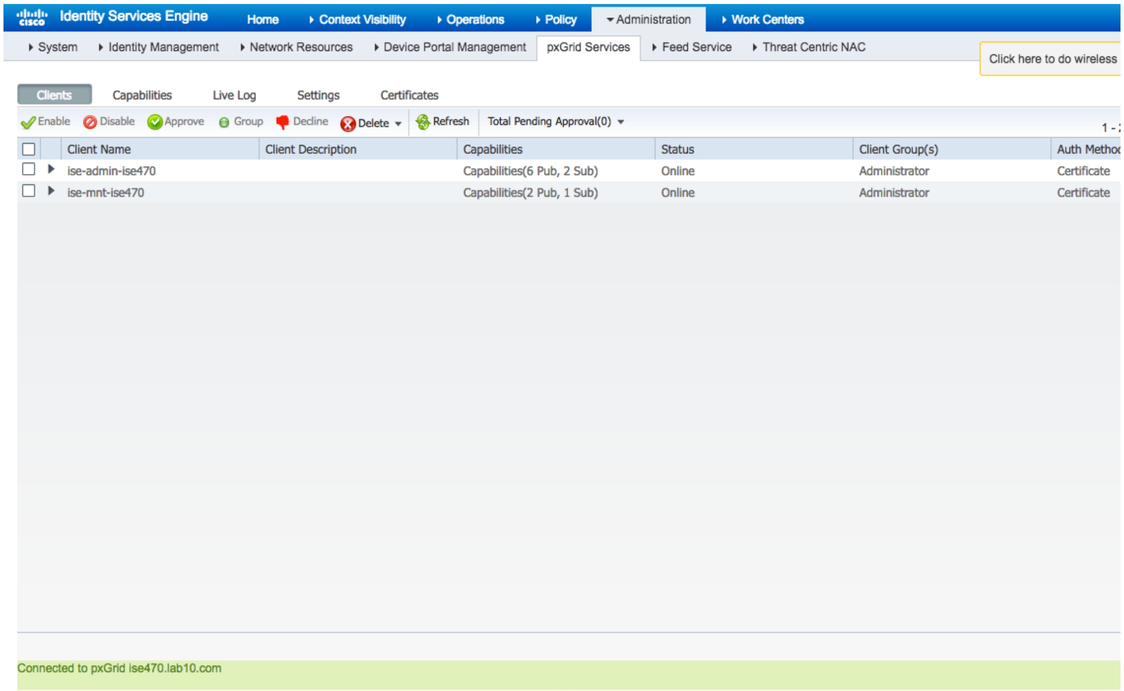
☑ Policy Service

- ☑ Enable Session Services — Include Node in Node Group None
- ☑ Enable Profiling Service
- ☑ Enable Threat Centric NAC Service
- ☐ Enable SXP Service — Use Interface GigabitEthernet 0
- ☐ Enable Device Admin Service
- ☐ Enable Passive Identity Service

☑ pxGrid

Step 6 Select **Save**

Step 7 Verify that the published node appear and that there is connectivity to the ISE pxGrid node Administration **pxGrid Services**



	Client Name	Client Description	Capabilities	Status	Client Group(s)	Auth Metho
□	ise-admin-ise470		Capabilities(6 Pub, 2 Sub)	Online	Administrator	Certificate
□	ise-mnt-ise470		Capabilities(2 Pub, 1 Sub)	Online	Administrator	Certificate

Connected to pxGrid ise470.lab10.com

Generating Self-Signed pxGrid client certificate

Step 1 Generate a private key (i.e. self1.key) for the pxGrid client

```
openssl genrsa -out self1.key 4096

Generating RSA private key, 4096 bit long modulus
..................++
.............................++
e is 65537 (0x10001)
```

Step 2 Generate the self-signed CSR (self1.csr) request and provide a challenge password.

```
openssl req -new -key self1.key -out self1.csr

You are about to be asked to enter information that will be incorporated
into your certificate request.
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.lab10.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 docunment, easier to maintain, and cut down on errors
```

Step 3 Generate self-signed cert public-key pair certificate (i.e. self1.cer)

```
openssl req -x509 -days 365 -key self1.key -in self1.csr -out self1.cer
```

Step 4 A PKCS12 file (i.e. self1.p12) will be created from the private key.

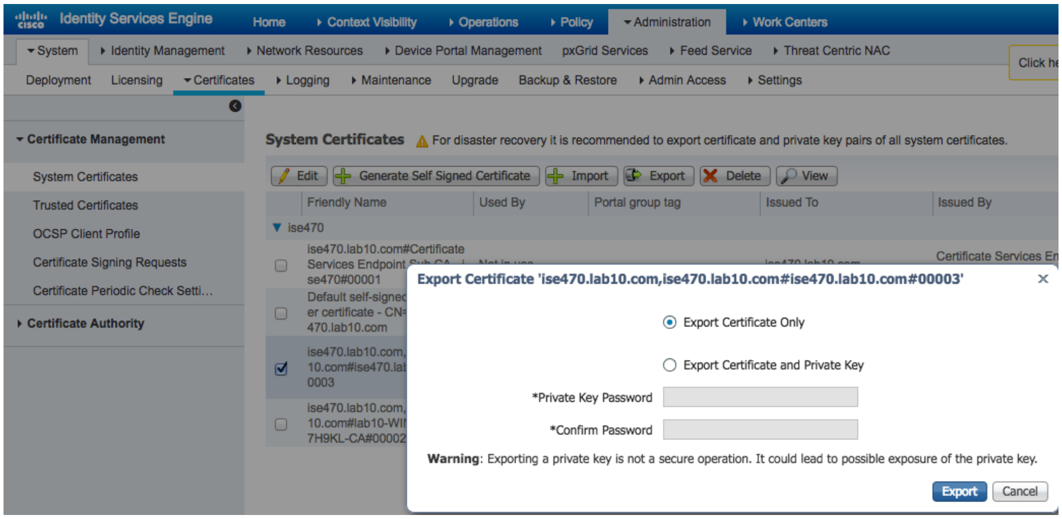
```
openssl pkcs12 -export -out self1.p12 -inkey self1.key -in self1.cer

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

Step 5 The self1.p12 will be imported into the identity keystore (i.e. self1.jks). The keystore filename can be a random filename with a .jks extension. This will serve as the keystoreFilename and associated keystorePassword in the pxGrid scripts.

```
keytool -importkeystore -srckeystore self1.p12 -destkeystore self1.jks  -srcstoretype PKCS12

Enter destination keystore password:  Cisco123
Re-enter new password: Cisco123
Enter source keystore password:  Cisco123
Entry for alias 1 successfully imported.
Import command completed:  1 entries successfully imported, 0 entries failed or cancelled
```

Step 6 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->System->Certificates->select the Default Signed ISE Signed Certificate and Export Certificate Only**



System Certificates ⚠ For disaster recovery it is recommended to export certificate and private key pairs of all system certificates.

Export Certificate 'ise470.lab10.com,ise470.lab10.com#ise470.lab10.com#00003'

● Export Certificate Only

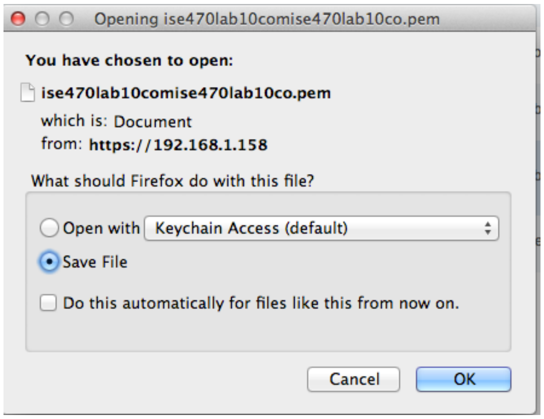
○ Export Certificate and Private Key

*Private Key Password

*Confirm Password

Warning: Exporting a private key is not a secure operation. It could lead to possible exposure of the private key.

Step 7 Save the file locally and you can rename the file to make it easier to work with.



Opening ise470lab10comise470lab10co.pem

You have chosen to open:

ise470lab10comise470lab10co.pem

which is: Document
from: **https://192.168.1.158**

What should Firefox do with this file?

○ Open with Keychain Access (default)

● Save File

□ Do this automatically for files like this from now on.

Step 8 Convert the .pem file to .der format.

```
openssl x509 -outform der -in ise470lab10comise470lab10co.pem -out ise470lab10comise470lab10co.der
```

Step 9 Add the ISE identity cert to the identity keystore. This will be used for securing bulk session downloads from the ISE MNT node when running the pxGrid session download scripts.

```
keytool -import -alias ise22mnt -keystore self1.jks -file ise470lab10comise470lab10co.der
Enter keystore password:  Cisco123
Owner: OU=engineeiring, CN=ise470.lab10.com
Issuer: OU=engineeiring, CN=ise470.lab10.com
Serial number: 58acea5200000000d178f9fbf20372e3
Valid from: Tue Feb 21 20:33:06 EST 2017 until: Thu Feb 21 20:33:06 EST 2019
Certificate fingerprints:
         MD5:  E8:D7:8C:28:C8:BC:74:9B:5C:5C:EB:C8:21:E6:BC:B8
         SHA1: 56:BE:F9:0A:96:7C:B2:08:0A:8D:F9:A7:78:88:61:0E:63:AA:1A:4E
         SHA256:
B8:32:64:2B:5A:08:E2:51:8F:BE:A4:81:7D:4E:4B:33:5C:56:62:03:E6:F0:49:8B:CA:CD:79:DD:81:D6:8E:DB
         Signature algorithm name: SHA256withRSA
         Version: 3

Extensions:
```

```
#1: ObjectId: 2.5.29.19 Criticality=false
BasicConstraints:[
  CA:true
  PathLen:2147483647
]

#2: ObjectId: 2.5.29.37 Criticality=false
ExtendedKeyUsages [
  serverAuth
  clientAuth
]

#3: ObjectId: 2.5.29.15 Criticality=false
KeyUsage [
  DigitalSignature
  Non_repudiation
  Key_Encipherment
  Key_Agreement
  Key_CertSign
]

#4: ObjectId: 2.16.840.1.113730.1.1 Criticality=false
NetscapeCertType [
   SSL server
]

#5: ObjectId: 2.5.29.17 Criticality=false
SubjectAlternativeName [
  DNSName: ise470.lab10.com
]

#6: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: 1A B4 95 E9 4C 83 05 78   FB 17 16 98 2D 21 3C 38  ....L..x....-!<8
0010: 41 05 B3 15                                        A...
]
]

Trust this certificate? [no]:  yes
Certificate was added to keystore
```

Step 10 Import the pxGrid client certificate into the identity keystore.

```
keytool -import -alias pxGridclientTest -keystore self1.jks -file self1.cer
Enter keystore password:  Cisco123
Certificate already exists in keystore under alias <1>
Do you still want to add it? [no]:  Yes
Certificate was added to keystore
```

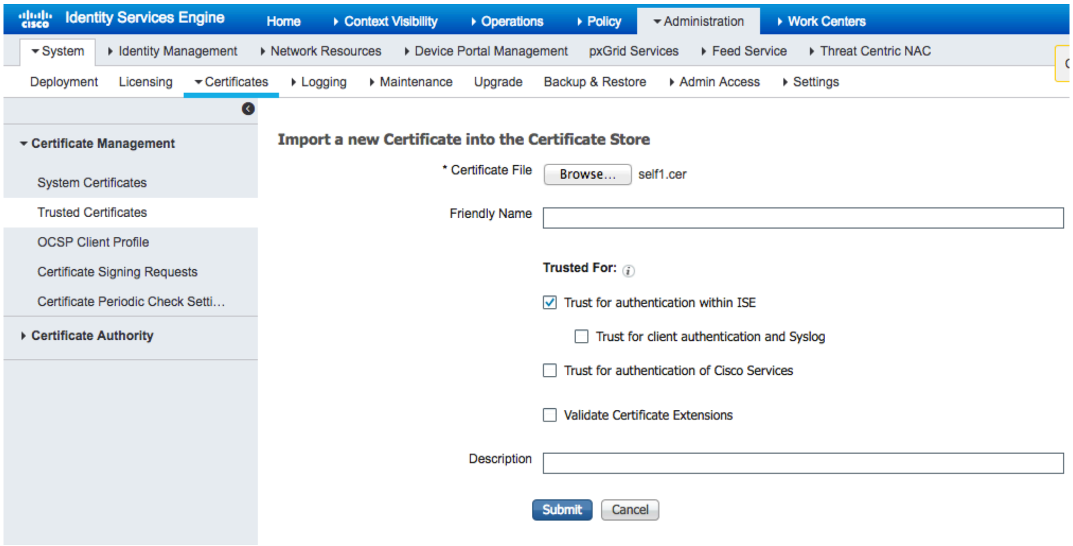
Note: If you receive the following message the certficate was already added to a pre-existing keystore, you can say "no" and still be okay. I selected "yes" so we can verify thay the certificate was added later on.

Step 11 Import the ISE identity cert into the trust keystore (i.e. root1.jks). This will serve as the truststore Filename and truststore password for the pxGrid scripts.

```
keytool -import -alias ise22root -keystore ise22root.jks -file ise470lab10comise470lab10co.der
Enter keystore password:  Cisco123
Re-enter new password: Cisco123
Owner: OU=engineeiring, CN=ise470.lab10.com
Issuer: OU=engineeiring, CN=ise470.lab10.com
Serial number: 58acea5200000000d178f9fbf20372e3
Valid from: Tue Feb 21 20:33:06 EST 2017 until: Thu Feb 21 20:33:06 EST 2019
Certificate fingerprints:
         MD5:  E8:D7:8C:28:C8:BC:74:9B:5C:5C:EB:C8:21:E6:BC:B8
         SHA1: 56:BE:F9:0A:96:7C:B2:08:0A:8D:F9:A7:78:88:61:0E:63:AA:1A:4E
         SHA256: 
B8:32:64:2B:5A:08:E2:51:8F:BE:A4:81:7D:4E:4B:33:5C:56:62:03:E6:F0:49:8B:CA:CD:79:DD:81:D6:8E:DB
         Signature algorithm name: SHA256withRSA
         Version: 3

Extensions: 

#1: ObjectId: 2.5.29.19 Criticality=false
BasicConstraints:[
  CA:true
  PathLen:2147483647
]

#2: ObjectId: 2.5.29.37 Criticality=false
ExtendedKeyUsages [
  serverAuth
  clientAuth
]

#3: ObjectId: 2.5.29.15 Criticality=false
KeyUsage [
  DigitalSignature
  Non_repudiation
  Key_Encipherment
  Key_Agreement
  Key_CertSign
]

#4: ObjectId: 2.16.840.1.113730.1.1 Criticality=false
NetscapeCertType [
   SSL server
]

#5: ObjectId: 2.5.29.17 Criticality=false
SubjectAlternativeName [
  DNSName: ise470.lab10.com
]

#6: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: 1A B4 95 E9 4C 83 05 78   FB 17 16 98 2D 21 3C 38  ....L..x....-!<8
0010: 41 05 B3 15                                        A...
]
]

Trust this certificate? [no]:  yes
Certificate was added to keystore
johns-macbook-pro:ise22_prod2 jeppich$
```

Step 12 Upload the pxGrid client public certificate (self1.cer) into the ISE trusted certificate store.

Administration->System Certificates->Trusted Certificates->Upload the self1.cer from the pxGrid client



Import a new Certificate into the Certificate Store

* Certificate File: self1.cer

Friendly Name:

Trusted For:

☑ Trust for authentication within ISE

☐ Trust for client authentication and Syslog

☐ Trust for authentication of Cisco Services

☐ Validate Certificate Extensions

Description:

Step 13 Select->**Submit**

Step 14 Select->**Yes Ok**-> for the message received

Testing pxGrid client and ISE pxGrid node

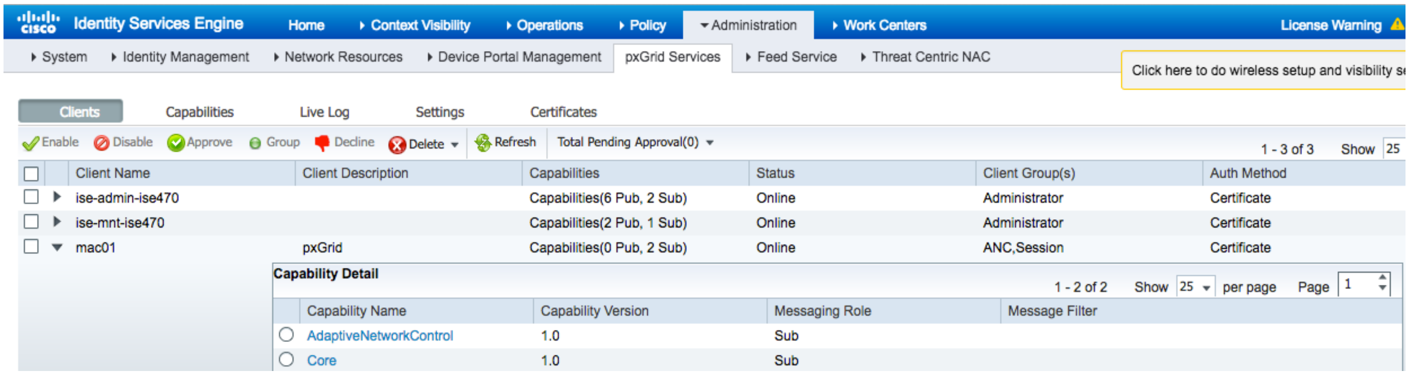
Sample pxGrid scripts register.sh and session_download.sh will be run to ensure pxGrid client connections and pxGrid registration.

Step 1 Register the pxGrid client

Note: The "Exception in thread…" is a known bug with pxGrid SDK 1.0.4.19. This only affects the sample script. The pxGrid client should successfully

```
./multigroupclient.sh -a 192.168.1.158 -u MAC01 -k self1.jks -p Cisco123 -t ise22root.jks -q Cisco123 -g
Session -d pxGrid Client
------- properties -------
  version=1.0.4.19
  hostnames=192.168.1.158
  username=MAC01
  password=
  group=Session,ANC,Session
  description=pxGrid
  keystoreFilename=self1.jks
  keystorePassword=Cisco123
  truststoreFilename=ise22root.jks
  truststorePassword=Cisco123
--------------------------
17:56:53.649 [Thread-1] INFO  com.cisco.pxgrid.ReconnectionManager - Started
Connecting...
17:56:53.667 [Thread-1] INFO  com.cisco.pxgrid.Configuration - Connecting to host 192.168.1.158
17:56:53.896 [Thread-1] INFO  com.cisco.pxgrid.Configuration - Connected OK to host 192.168.1.158
17:56:53.896 [Thread-1] INFO  com.cisco.pxgrid.Configuration - Client Login to host 192.168.1.158
17:56:53.932 [Thread-1] INFO  com.cisco.pxgrid.Configuration - Client Login OK to host 192.168.1.158
Connected
17:56:54.950 [Thread-1] INFO  com.cisco.pxgrid.ReconnectionManager - Connected
Create ANC Policy: ANC1488927412914 Result - com.cisco.pxgrid.model.anc.ANCResult@71a794e5[
  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)
```

Step 2 You should see the pxGrid client successfully register to the ISE pxGrid node



□		Client Name	Client Description	Capabilities	Status	Client Group(s)	Auth Method
□	▶	ise-admin-ise470		Capabilities(6 Pub, 2 Sub)	Online	Administrator	Certificate
□	▶	ise-mnt-ise470		Capabilities(2 Pub, 1 Sub)	Online	Administrator	Certificate
□	▼	mac01	pxGrid	Capabilities(0 Pub, 2 Sub)	Online	ANC,Session	Certificate

Capability Detail

1 - 2 of 2 Show 25 per page Page 1

	Capability Name	Capability Version	Messaging Role	Message Filter
○	AdaptiveNetworkControl	1.0	Sub	
○	Core	1.0	Sub	

Step 3 You should see the pxGrid client successfully register to the ISE pxGrid node

```
./session_download.sh -a 192.168.1.158 -u MAC01 -k self1.jks -p Cisco123 -t ise22root.jks -q Cisco123
------- properties -------
  version=1.0.4.19
  hostnames=192.168.1.158
  username=MAC01
  password=
  group=Session
  description=null
  keystoreFilename=self1.jks
  keystorePassword=Cisco123
  truststoreFilename=ise22root.jks
  truststorePassword=Cisco123
--------------------------
Connecting...
17:44:32.600 [main] INFO  com.cisco.pxgrid.Configuration - Connecting to host 192.168.1.158
17:44:32.827 [main] INFO  com.cisco.pxgrid.Configuration - Connected OK to host 192.168.1.158
17:44:32.827 [main] INFO  com.cisco.pxgrid.Configuration - Client Login to host 192.168.1.158
17:44:32.860 [main] INFO  com.cisco.pxgrid.Configuration - Client Login OK to host 192.168.1.158
Connected
Filters (ex. '1.0.0.0/255.0.0.0,1234::/16...' or <enter> for no filter):
Start time (ex. '2015-01-31 13:00:00' or <enter> for no start time):
End time (ex. '2015-01-31 13:00:00' or <enter> for no end time):
pxGrid controller version=1.0.4.18
Going to url:https://ise470.lab10.com:8910/pxgrid/mnt/sd/getSessionListByTime
Session={ip=[192.168.1.30], Audit Session Id=0A00000100000027003482A5, UserName=00:0C:29:7C:79:39,
MacAddresses=[00:0C: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 07 10:35:03 EST 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=0A0000010000001300015C5B, 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=00000014], Posture Status=null, Posture
Timestamp=, LastUpdateTime=Tue Mar 07 10:35:04 EST 2017, Session attributeName=Authorization_Profiles,
Session attributeValue=PermitAccess, Providers=[None], EndpointCheckResult=none, IdentitySourceFirstPort=0,
IdentitySourcePortStart=0, IdentitySourcePortEnd=0}
Session={ip=[192.168.1.159], Audit Session Id=0A0000010000002A01196252, UserName=00:50:56:86:08:19,
MacAddresses=[00:50:56:86:08:19], State=STARTED, EndpointProfile=ISE-Appliance, NAS IP=192.168.1.3, NAS
Port=GigabitEthernet1/0/10, RADIUSAVPairs=[ Acct-Session-Id=0000002C], Posture Status=null, Posture
Timestamp=, LastUpdateTime=Tue Mar 07 15:20:41 EST 2017, Session attributeName=Authorization_Profiles,
Session attributeValue=PermitAccess, Providers=[None], EndpointCheckResult=none, IdentitySourceFirstPort=0,
IdentitySourcePortStart=0, IdentitySourcePortEnd=0}
Session={ip=[192.168.1.8], Audit Session Id=0A0000010000002B01ABF06F, UserName=user7@lab10.com,
ADUserDNSDomain=lab10.com, ADUserNetBIOSName=LAB10, ADUserResolvedIdentities=user7@lab10.com,
ADUserResolvedDNs=CN=user7,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=00000037], Posture Status=null, Posture
Timestamp=, LastUpdateTime=Tue Mar 07 17:41:02 EST 2017, Session attributeName=Authorization_Profiles,
Session attributeValue=Employees, Providers=[None], EndpointCheckResult=none, IdentitySourceFirstPort=0,
IdentitySourcePortStart=0, IdentitySourcePortEnd=0, IsMachineAuthentication=false}
Session={ip=[192.168.1.5], Audit Session Id=0A00000100000011000015A10, 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=00000012], Posture Status=null, Posture
Timestamp=, LastUpdateTime=Tue Mar 07 10:35:04 EST 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=0A000001000000210004B723, 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=00000022], Posture Status=null, Posture
Timestamp=, LastUpdateTime=Tue Mar 07 10:35:00 EST 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=0A000001000000200004AE7D, 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=00000021], Posture Status=null, Posture
Timestamp=, LastUpdateTime=Tue Mar 07 10:35:04 EST 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=0A000001000000220009D388, UserName=F0:DE:F1:94:65:9C,
MacAddresses=[F0:DE:F1:94:65:9C], State=STARTED, EndpointProfile=Microsoft-Workstation, NAS IP=192.168.1.3,
NAS Port=GigabitEthernet1/0/12, RADIUSAVPairs=[ Acct-Session-Id=00000023], Posture Status=null, Posture
Timestamp=, LastUpdateTime=Tue Mar 07 10:35:04 EST 2017, Session attributeName=Authorization_Profiles,
Session attributeValue=PermitAccess, Providers=[None], EndpointCheckResult=none, IdentitySourceFirstPort=0,
IdentitySourcePortStart=0, IdentitySourcePortEnd=0}
Session count=8
Connection closed
johns-macbook-pro:bin jeppich$
```

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