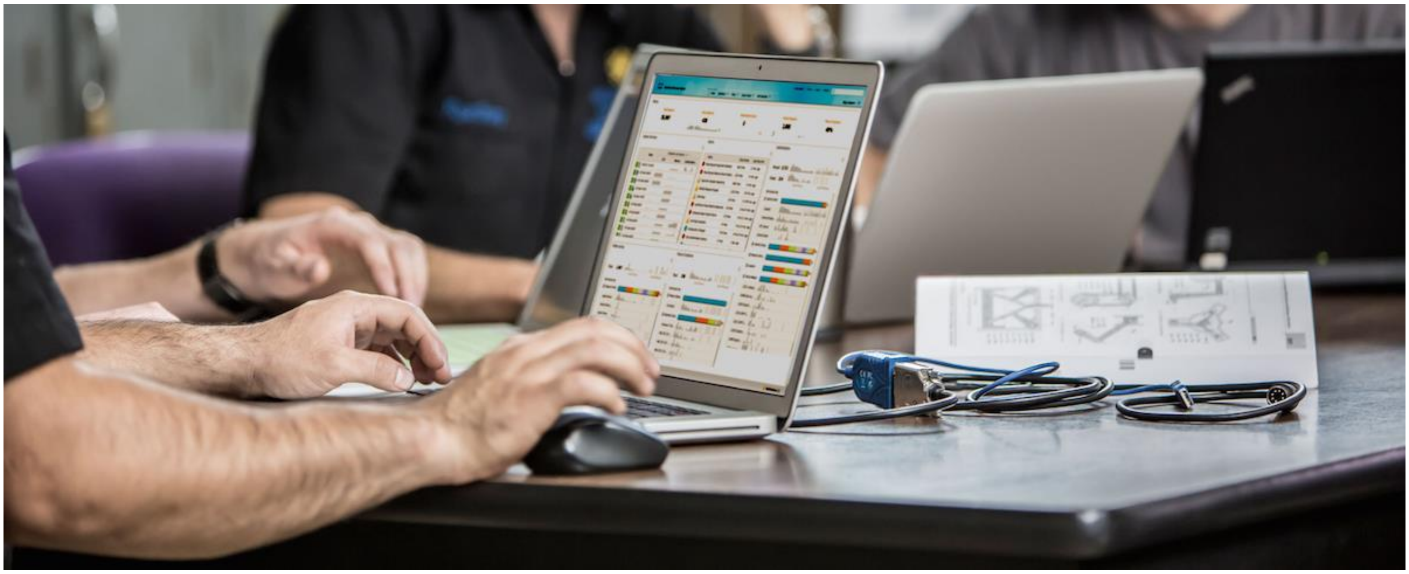


Deploying Certificates with Cisco pxGrid

Certificate Authority (CA)-signed ISE pxGrid node and CA-signed pxGrid client

Table of Contents

About this Document

This document illustrates the configuration steps required for configuring a pxGrid client and the ISE pxGrid node using a certificate authority. This document is intended for Cisco field engineers, technical marketing engineers, partners and customers deploying Cisco pxGrid. Familiarity with pxGrid is required.

If the reader is not familiar with pxGrid, please see Configure_and_Test_Integration_with_Cisco_pxGrid.pdf:

http://www.cisco.com/c/dam/en/us/td/docs/security/ise/how_to/HowTo-84-Configure_and_Test_Integration_with_Cisco_pxGrid.pdf

Obtain the pxGrid sdk from your Cisco account team.

It is assumed that Cisco Identity Services Engine (ISE) 1.3 is installed. A Mac running OSX 10.8.5 will be used as the pxGrid client. A Linux OS can also be used. The Oracle Java Development Kit 7 or 8 is required for the pxGrid client.

There are two other documents in *Deploying pxGrid with Certificates* series:

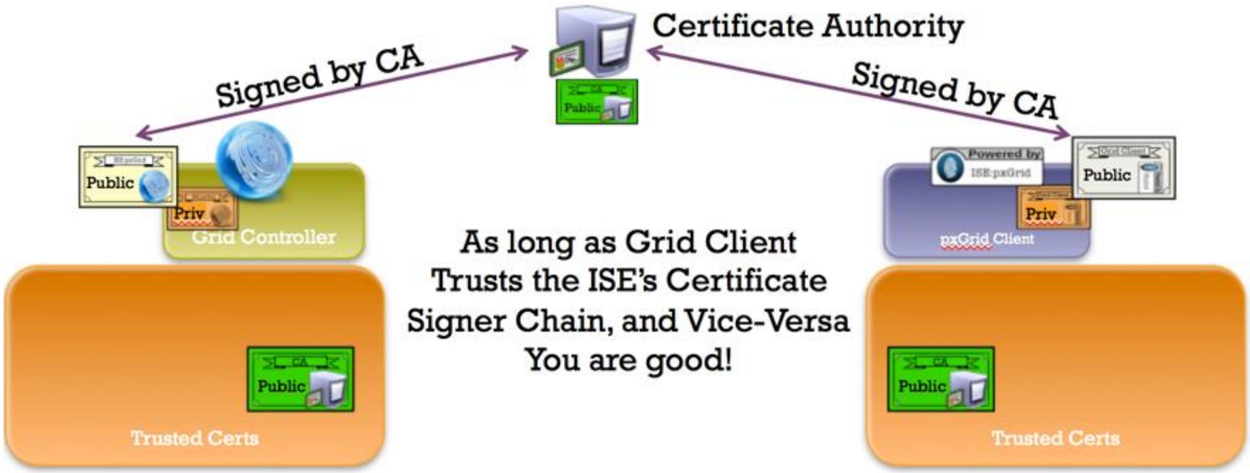
- Using Self-Signed Certificates with ISE pxGrid node and pxGrid client
- Using Certificate Authority (CA)-Signed pxGrid client and self-signed ISE pxGrid node certificate

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 (1.3.6.5.5.7.3.2) 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.

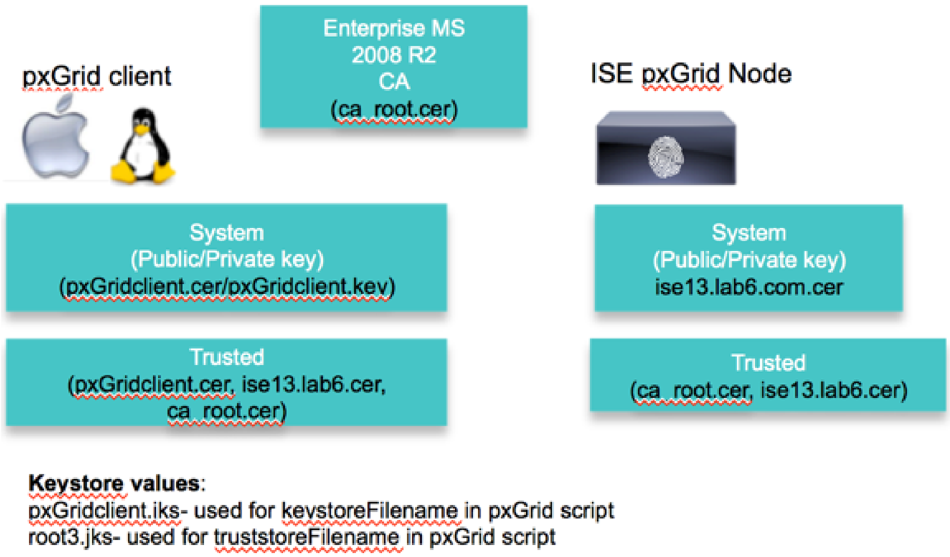
When the pxGrid client connects to the ISE pxGrid node both public certificates will be trusted for Simple Authentication and Security Layer (SASL) for a successful pxGrid connection.

The following diagram represents the certificate flow of information.



Example Certificate Configuration

This represents the certificate example used in this document

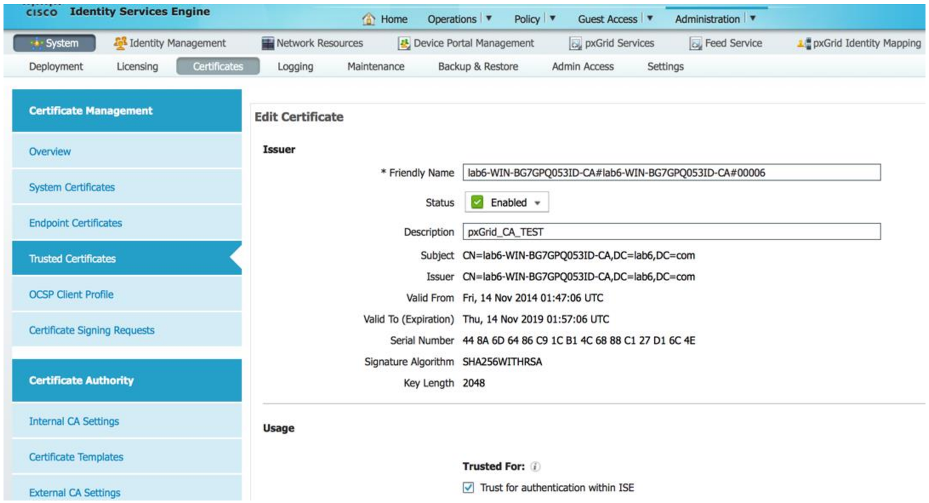

pxGrid client
Enterprise MS 2008 R2 CA (ca_root.cer)
ISE pxGrid Node
System (Public/Private key) (pxGridclient.cer/pxGridclient.key)
System (Public/Private key) ise13.lab6.com.cer
Trusted (pxGridclient.cer, ise13.lab6.cer, ca_root.cer)
Trusted (ca_root.cer, ise13.lab6.cer)

Keystore values:
pxGridclient.jks- used for keystoreFilename in pxGrid script
root3.jks- used for truststoreFilename in pxGrid script

CA-signed ISE pxGrid node certificate and pxGrid persona Configuration

This section details the CA-signed ISE pxGrid certificate process and importing of the CA root certificate into the ISE trusted certificate store. Once the CA certificate has been uploaded into the trusted store and the ISE certificate bound to the CSR request, the pxGrid persona can be enabled on the ISE node and made primary.

Step 1 Download and upload the CA root certificate into the ISE Trusted Certificate Store and "enable trust for ISE communication



Edit Certificate

Issuer

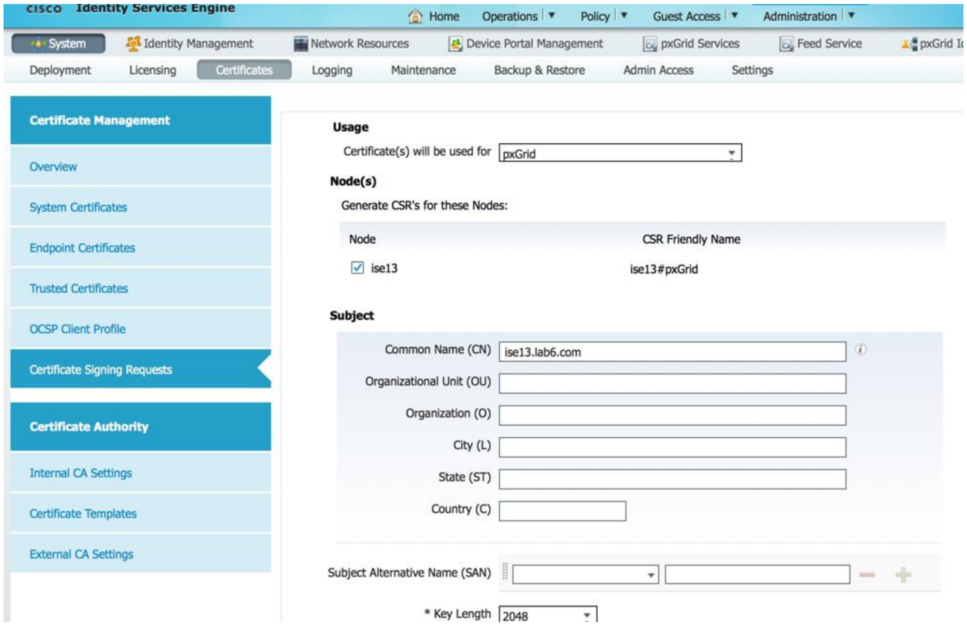
* Friendly Name	lab6-WIN-BG7GPQ053ID-CA#lab6-WIN-BG7GPQ053ID-CA#00006
Status	☑ Enabled
Description	pxGrid_CA_TEST
Subject	CN=lab6-WIN-BG7GPQ053ID-CA,DC=lab6,DC=com
Issuer	CN=lab6-WIN-BG7GPQ053ID-CA,DC=lab6,DC=com
Valid From	Fri, 14 Nov 2014 01:47:06 UTC
Valid To (Expiration)	Thu, 14 Nov 2019 01:57:06 UTC
Serial Number	44 8A 6D 64 86 C9 1C B1 4C 68 88 C1 27 D1 6C 4E
Signature Algorithm	SHA256WITHRSA
Key Length	2048

Usage

Trusted For:

☑ Trust for authentication within ISE

Step 2 Generate an ISE CSR request to the CA Authority for pxGrid usage. A pxGrid template needs to be configured for EKUs of both client authentication and server authentication to service the user certificate request.
Administration->System->Certificates->Certificate Signing Requests->Generate CSR with ISE FQDN and set for pxGrid Usage



Usage

Certificate(s) will be used for: pxGrid

Node(s)

Generate CSR's for these Nodes:

Node	CSR Friendly Name
☑ ise13	ise13#pxGrid

Subject

Common Name (CN): ise13.lab6.com

Organizational Unit (OU):

Organization (O):

City (L):

State (ST):

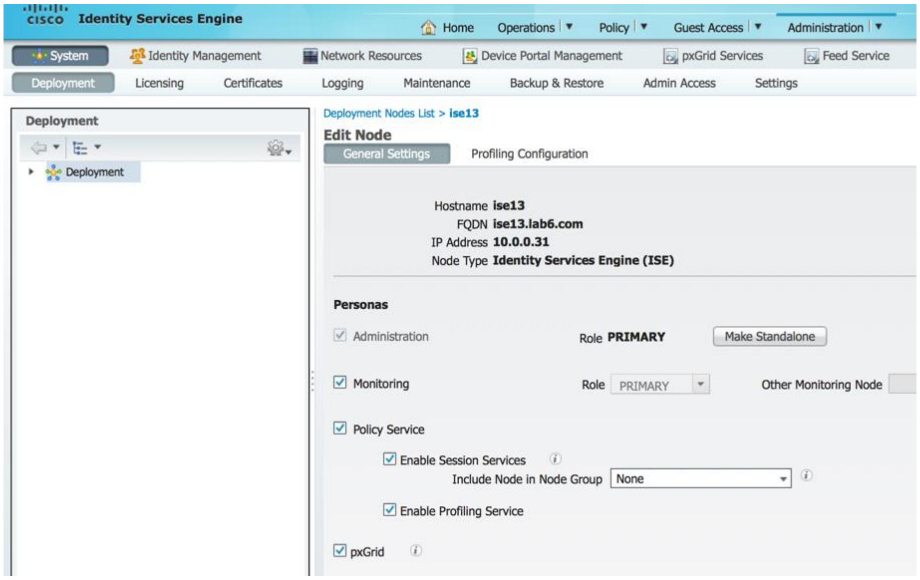
Country (C):

Subject Alternative Name (SAN):

* Key Length: 2048

Step 3 Download certificate from CA and bind certificate
Administration->Certificates->Certificate Signing Requests->Bind certificate

Step 4 Enable pxGrid on ISE
Administration->System->Deployment->enable pxGrid and make primary



Deployment Nodes List > ise13

Edit Node

Hostname **ise13**
FQDN **ise13.lab6.com**
IP Address **10.0.0.31**
Node Type **Identity Services Engine (ISE)**

Personas

☑ Administration — Role **PRIMARY**

☑ Monitoring — Role PRIMARY — Other Monitoring Node

☑ Policy Service

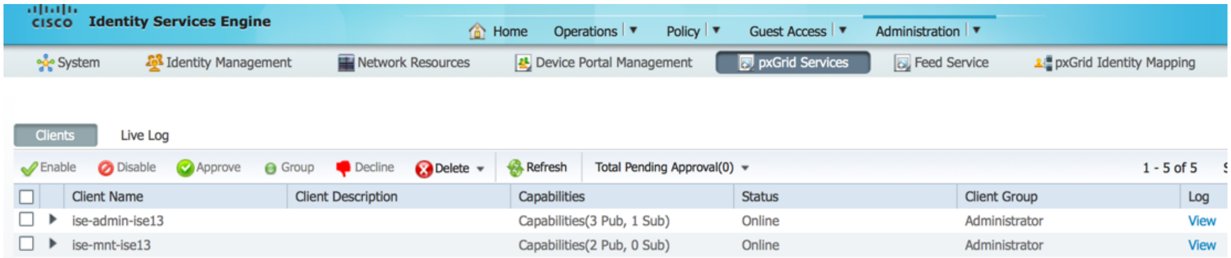
☑ Enable Session Services

Include Node in Node Group: None

☑ Enable Profiling Service

☑ pxGrid

Step 5 You should see the pxGrid services have started
Administration->pxGrid Services



□	Client Name	Client Description	Capabilities	Status	Client Group	Log
□	ise-admin-ise13		Capabilities(3 Pub, 1 Sub)	Online	Administrator	View
□	ise-mnt-ise13		Capabilities(2 Pub, 0 Sub)	Online	Administrator	View

Note: There may be a delay before the ISE publishing nodes appear. The certificates must be installed before the pxGrid persona is enabled.

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.

```
openssl genrsa -out pxGridClient.key 4096

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

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

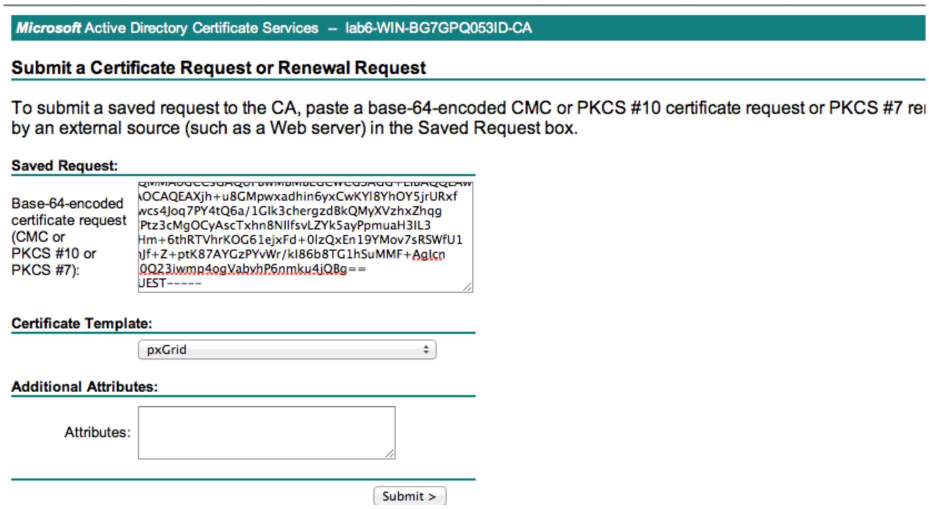
```
openssl req -new -key pxGridClient.key -out pxGridClient.csr

You are about to be asked to enter information that will be incorporated
into your certificate request.
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]:
State or Province Name (full name) [Some-State]:
Locality Name (eg, city) []:
Organization Name (eg, company) [Internet Widgits Pty Ltd]:
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:
Email Address []:
```

```
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:cisco123
An optional company name []:Eppich, Inc
```

Note: Keep the same password throughout this docunment, 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 -- lab6-WIN-BG7GPQ053ID-CA

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request or PKCS #7 re
by an external source (such as a Web server) in the Saved Request box.

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

```
OCAQEAXjh+u8GMpwxadhin6yxCwKYI8YhOY5jrURxf
wcs4Joq7PY4tQ6a/1GIk3chergzdBkQMyXVzhxZhqg
Ptz3cMgOCyAscTxhn8NIlfsvLZYk5ayPpmuaH3IL3
Hm+6thRTVhrKOG61ejxFd+0lzQxEn19YMov7sRSWfU1
Jf+Z+ptK87AYGzPYvWr/kI86b8TG1hSuMMF+AgIcn
0Q23iwmp4ogVabvhP6nmku4jQBg==
UEST-----
```

Certificate Template: pxGrid

Additional Attributes:

Attributes:

Step 4 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).

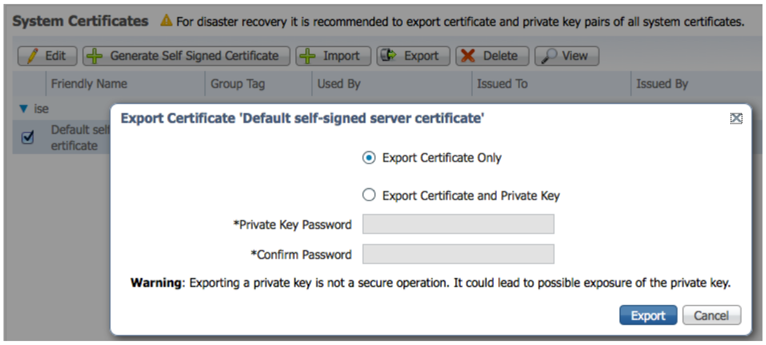
```
openssl pkcs12 -export -out pxGridClient.p12 -inkey pxGridClient.key -in pxGridClient.cer -chain -CAfile
ca_root.cer

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

Step 5 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:  cisco123
Re-enter new password: cisco123
```

```
Enter source keystore password:
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.



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

Export Certificate 'Default self-signed server certificate'

● 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 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 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.

```
keytool -import -alias isemnt -keystore root3.jks -file isemnt.der

Enter keystore password:  cisco123
Re-enter new password: cisco123

Owner: CN=ise.lab6.com
Issuer: CN=lab6-WIN-BG7GPQ053ID-CA, DC=lab6, DC=com
Serial number: 61262d7600000000000d
Valid from: Wed Dec 10 16:39:24 EST 2014 until: Sat Dec 10 16:49:24 EST 2016
Certificate fingerprints:
         MD5:  2B:3D:24:04:D3:FF:1F:1E:7E:57:8E:44:4A:AF:6D:51
         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  ..0...+....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...+.......0.
0010: 06 08 2B 06 01 05 05 07   03 02 30 0A 06 08 2B 06  ..+.......0...+.
0020: 01 05 05 07 03 04 30 0C   06 0A 2B 06 01 04 01 82  ......0...+.....
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.....
0010: 87 CB EB 79 81 89 9D 2D   86 E6 FC 53 86 82 A1 38  ...y...-...S...8
0020: 5E 86 D1 B8 23 85 FC EF   40 02 01 64 02 01 03     ^...#...@..d...


#4: ObjectId: 1.3.6.1.5.5.7.1.1 Criticality=false
AuthorityInfoAccess [
  [
   accessMethod: caIssuers
   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
]
]

#5: ObjectId: 2.5.29.35 Criticality=false
AuthorityKeyIdentifier [
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,
]
]

#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
]

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

```
keytool -import -alias pxGridMAC -keystore pxGridClient.jks -file
pxGridClient.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 10 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 11 Copy the identity keystore (pxGridClient.jks) and trust keystore (root3.jks) into the ../samples/bin/..folder.

Testing pxGrid client and the ISE pxGrid node

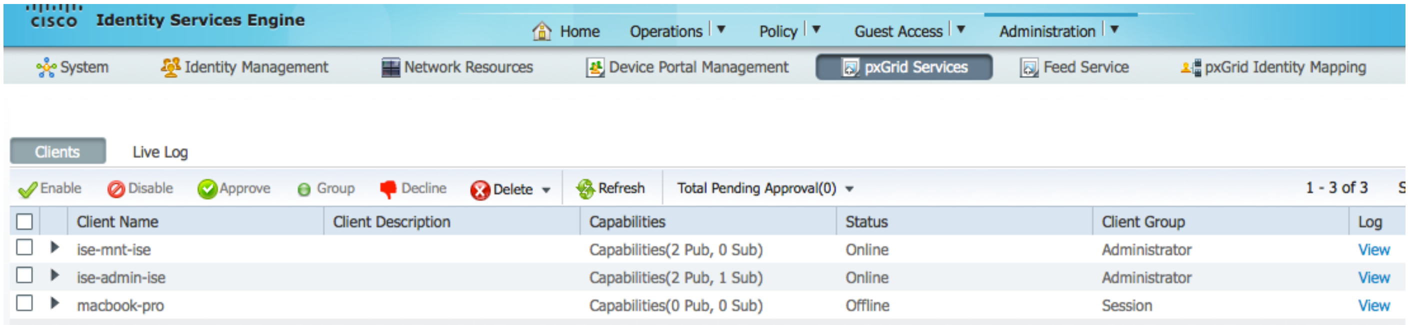
The pxGrid scripts: register.sh and session download.sh will be run to ensure pxGrid client connection and pxGrid registration. Session downloads will ensure that there are no issues with the ISE MNT certificate and the pxGrid client.

Step 1 Register the pxGrid client

```
./register.sh -keystoreFilename pxGridClient.jks -keystoreFilename cisco123 -truststoreFilename root3.jks -
truststorePassword cisco123 -group Session -description test -username MacBook-Pro -hostname 10.0.0.96

------- properties -------
version=1.0.0
hostnames=10.0.0.96
username=MacBook-Pro
descriptipon=test
keystoreFilename=pxGridClient.jks
keystorePassword=cisco123
truststoreFilename=root3.jks
truststorePassword=cisco123
--------------------------
registering...
connecting...
account enabled
connected.
done registering.
connection closed
```

Note: “Account enabled” means the account was enabled by the pxGrid admin

Verify the pxGrid client has registered to the pxGrid controller



□		Client Name	Client Description	Capabilities	Status	Client Group	Log
□	▸	ise-mnt-ise		Capabilities(2 Pub, 0 Sub)	Online	Administrator	View
□	▸	ise-admin-ise		Capabilities(2 Pub, 1 Sub)	Online	Administrator	View
□	▸	macbook-pro		Capabilities(0 Pub, 0 Sub)	Offline	Session	View

Step 2 Run the Session download

```
./session_download.sh -keystoreFilename pxGridClient.jks -keystoreFilename cisco123 -truststoreFilename
root3.jks -truststorePassword cisco123 -username MacBook-Pro -hostname 10.0.0.96

------- properties -------
version=1.0.0
hostnames=10.0.0.96
username=MacBook-Pro
keystoreFilename=pxGridClient.jks
keystorePassword=cisco123
truststoreFilename=root3.jks
truststorePassword=cisco123
filter=null
```

```
start=null
end=null
--------------------------
connecting...
connected.
starting at Wed Dec 10 18:44:49 EST 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 16:41:48 EST 2014
)... ending at: Wed Dec 10 18:44:49 EST 2014

---------------------------------------------------
downloaded 1 sessions in 26 milliseconds
---------------------------------------------------

connection closed
```

Viewing Keystore Entries

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

Step 1 Verify root3.jks, trust keystore.

```
keytool -list -v -keystore root3.jks
Enter keystore password:  cisco123

Keystore type: JKS
Keystore provider: SUN

Your keystore contains 3 entries

Alias name: ca_root1
Creation date: Dec 10, 2014
Entry type: trustedCertEntry

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,
]
]



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


Alias name: isemnt1
Creation date: Dec 10, 2014
Entry type: trustedCertEntry

Owner: CN=ise.lab6.com
Issuer: CN=lab6-WIN-BG7GPQ053ID-CA, DC=lab6, DC=com
Serial number: 61262d760000000000d
Valid from: Wed Dec 10 16:39:24 EST 2014 until: Sat Dec 10 16:49:24 EST 2016
Certificate fingerprints:
         MD5:  2B:3D:24:04:D3:FF:1F:1E:7E:57:8E:44:4A:AF:6D:51
         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  ..0...+....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...+.......0.
0010: 06 08 2B 06 01 05 05 07   03 02 30 0A 06 08 2B 06  ..+.......0...+.
0020: 01 05 05 07 03 04 30 0C   06 0A 2B 06 01 04 01 82  ......0...+.....
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.....
0010: 87 CB EB 79 81 89 9D 2D   86 E6 FC 53 86 82 A1 38  ...y...-...S...8
0020: 5E 86 D1 B8 23 85 FC EF   40 02 01 64 02 01 03     ^...#...@..d...


#4: ObjectId: 1.3.6.1.5.5.7.1.1 Criticality=false
AuthorityInfoAccess [
  [
   accessMethod: caIssuers
   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
]
]

#5: ObjectId: 2.5.29.35 Criticality=false
AuthorityKeyIdentifier [
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,
]
]

#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
]

#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                                        ....
]
]



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


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

Owner: CN=ise.lab6.com
Issuer: CN=lab6-WIN-BG7GPQ053ID-CA, DC=lab6, DC=com
Serial number: 61262d7600000000000d
Valid from: Wed Dec 10 16:39:24 EST 2014 until: Sat Dec 10 16:49:24 EST 2016
Certificate fingerprints:
         MD5:  2B:3D:24:04:D3:FF:1F:1E:7E:57:8E:44:4A:AF:6D:51
         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  ..0...+....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...+.......0.
0010: 06 08 2B 06 01 05 05 07   03 02 30 0A 06 08 2B 06  ..+.......0...+.
0020: 01 05 05 07 03 04 30 0C   06 0A 2B 06 01 04 01 82  ......0...+.....
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.....
0010: 87 CB EB 79 81 89 9D 2D   86 E6 FC 53 86 82 A1 38  ...y...-...S...8
0020: 5E 86 D1 B8 23 85 FC EF   40 02 01 64 02 01 03     ^...#...@..d...


#4: ObjectId: 1.3.6.1.5.5.7.1.1 Criticality=false
AuthorityInfoAccess [
  [
   accessMethod: caIssuers
   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
]
]

#5: ObjectId: 2.5.29.35 Criticality=false
AuthorityKeyIdentifier [
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,
]
]

#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
]

#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                                        ....
]
]



*******************************************
*******************************************
```

```
Johns-MacBook-Pro:bin jeppich$
```

Step 2 Verify pxGridclient.jks, the identity keystore.

```
keytool -list -v -keystore pxGridClient.jks
Enter keystore password:

Keystore type: JKS
Keystore provider: SUN

Your keystore contains 2 entries

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

Owner: O=Internet Widgits Pty Ltd, ST=Some-State, C=AU
Issuer: CN=lab6-WIN-BG7GPQ053ID-CA, DC=lab6, DC=com
Serial number: 6101649b00000000000e
Valid from: Wed Dec 10 17:01:25 EST 2014 until: Sat Dec 10 17:11:25 EST 2016
Certificate fingerprints:
         MD5:  0F:3C:57:64:7E:BD:D9:0A:7B:C2:25:64:84:F2:E3:FA
         SHA1: 65:9C:A8:8D:52:B0:CF:C6:1B:46:7E:41:80:D3:7B:96:40:B1:E3:68
         SHA256:
3D:8A:72:6B:9D:7F:12:5A:AF:A7:CC:A6:E2:F7:E9:9A:F9:D8:BE:89:55:12:87:30:F8:17:3B:91:29:EB:6A: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  ..0...*.H.......
0020: 00 80 30 07 06 05 2B 0E   03 02 07 30 0A 06 08 2A  ..0...+....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...+.......0.
0010: 06 08 2B 06 01 05 05 07   03 02 30 0A 06 08 2B 06  ..+.......0...+.
0020: 01 05 05 07 03 04 30 0C   06 0A 2B 06 01 04 01 82  ......0...+.....
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.....
0010: 87 CB EB 79 81 89 9D 2D   86 E6 FC 53 86 82 A1 38  ...y...-...S...8
0020: 5E 86 D1 B8 23 85 FC EF   40 02 01 64 02 01 03     ^...#...@..d...


#4: ObjectId: 1.3.6.1.5.5.7.1.1 Criticality=false
AuthorityInfoAccess [
  [
   accessMethod: caIssuers
   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
]
]

#5: ObjectId: 2.5.29.35 Criticality=false
AuthorityKeyIdentifier [
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,
]
]

#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
]

#9: ObjectId: 2.5.29.15 Criticality=true
KeyUsage [
  DigitalSignature
  Key_Encipherment
]

#10: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: E6 87 7E 18 67 25 03 29   12 B4 56 F8 51 78 A1 94  ....g%.)..V.Qx..
0010: 78 88 D2 94                                        x...
]
]



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



Alias name: 1
Creation date: Dec 10, 2014
Entry type: PrivateKeyEntry
Certificate chain length: 2
Certificate[1]:
Owner: O=Internet Widgits Pty Ltd, ST=Some-State, C=AU
Issuer: CN=lab6-WIN-BG7GPQ053ID-CA, DC=lab6, DC=com
Serial number: 6101649b00000000000e
Valid from: Wed Dec 10 17:01:25 EST 2014 until: Sat Dec 10 17:11:25 EST 2016
Certificate fingerprints:
        MD5:  0F:3C:57:64:7E:BD:D9:0A:7B:C2:25:64:84:F2:E3:FA
        SHA1: 65:9C:A8:8D:52:B0:CF:C6:1B:46:7E:41:80:D3:7B:96:40:B1:E3:68
        SHA256:
3D:8A:72:6B:9D:7F:12:5A:AF:A7:CC:A6:E2:F7:E9:9A:F9:D8:BE:89:55:12:87:30:F8:17:3B:91:29:EB:6A: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  ..0...*.H.......
0020: 00 80 30 07 06 05 2B 0E   03 02 07 30 0A 06 08 2A  ..0...+....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...+.......0.
0010: 06 08 2B 06 01 05 05 07   03 02 30 0A 06 08 2B 06  ..+.......0...+.
0020: 01 05 05 07 03 04 30 0C   06 0A 2B 06 01 04 01 82  ......0...+.....
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.....
0010: 87 CB EB 79 81 89 9D 2D   86 E6 FC 53 86 82 A1 38  ...y...-...S...8
0020: 5E 86 D1 B8 23 85 FC EF   40 02 01 64 02 01 03     ^...#...@..d...


#4: ObjectId: 1.3.6.1.5.5.7.1.1 Criticality=false
AuthorityInfoAccess [
  [
   accessMethod: caIssuers
   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
]
]

#5: ObjectId: 2.5.29.35 Criticality=false
AuthorityKeyIdentifier [
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,
]
]

#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
]

#9: ObjectId: 2.5.29.15 Criticality=true
KeyUsage [
  DigitalSignature
  Key_Encipherment
]

#10: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: E6 87 7E 18 67 25 03 29   12 B4 56 F8 51 78 A1 94  ....g%.)..V.Qx..
0010: 78 88 D2 94                                        x...
]
]

Certificate[2]:
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,
]
]



*******************************************
*******************************************
```

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.

- If there changes to the truststore, and receive similar error messages stop and restart ISE application from the ISE VM.

```
./register.sh -keystoreFilename pxGridClient.jks -keysrePassword cisco123 -truststoreFilename root3.jks -
truststorePassword cisco123 -username pxGridclient -hostname 10.0.0.96 -group Session -description test1
------- properties -------
version=1.0.0
hostnames=10.0.0.96
username=pxGridclient
descriptipon=test1
keystoreFilename=pxGridClient.jks
keystorePassword=cisco123
truststoreFilename=root3.jks
truststorePassword=cisco123
--------------------------
registering...
connecting...
javax.net.ssl.SSLHandshakeException: Received fatal alert: unknown_ca
        at sun.security.ssl.Alerts.getSSLException(Alerts.java:192)
        at sun.security.ssl.Alerts.getSSLException(Alerts.java:154)
        at sun.security.ssl.SSLSocketImpl.recvAlert(SSLSocketImpl.java:1991)
        at sun.security.ssl.SSLSocketImpl.readRecord(SSLSocketImpl.java:1104)
        at sun.security.ssl.SSLSocketImpl.performInitialHandshake(SSLSocketImpl.java:1343)
        at sun.security.ssl.SSLSocketImpl.startHandshake(SSLSocketImpl.java:1371)
        at sun.security.ssl.SSLSocketImpl.startHandshake(SSLSocketImpl.java:1355)
        at org.jivesoftware.smack.XMPPConnection.proceedTLSReceived(XMPPConnection.java:806)
        at org.jivesoftware.smack.PacketReader.parsePackets(PacketReader.java:267)
        at org.jivesoftware.smack.PacketReader.access$000(PacketReader.java:43)
        at org.jivesoftware.smack.PacketReader$1.run(PacketReader.java:70)
Exception in thread "main" com.cisco.pxgrid.GCLException: SASL authentication failed:
        at com.cisco.pxgrid.GridConnection.connect(GridConnection.java:197)
        at com.cisco.pxgrid.samples.ise.Register.main(Register.java:99)
Caused by: SASL authentication failed:
        at org.jivesoftware.smack.SASLAuthentication.authenticate(SASLAuthentication.java:281)
        at org.jivesoftware.smack.XMPPConnection.login(XMPPConnection.java:206)
        at com.cisco.pxgrid.Configuration.connect(Configuration.java:194)
        at com.cisco.pxgrid.GridConnection.connect(GridConnection.java:134)
        ... 1 more
```

- Restarting ISE services

```
application stop ise
application start ise
```

Step 3 If you see a similar error message, the root cert needs to be added to the truststoreFilename keystore, in this case root3.jks.

```
./register.sh -keystoreFilename pxGridClient.jks -keystorePassword cisco123 -truststoreFilename root3.jks -
truststorePassword cisco123 -group Session -description MACBOOK -username Macbook_PRO -hostname 10.0.0.96

------- properties -------
version=1.0.0
hostnames=10.0.0.96
username=Macbook_PRO
descriptipon=MACBOOK
keystoreFilename=pxGridClient.jks
keystorePassword=cisco123
```

```
truststoreFilename=root3.jks
truststorePassword=cisco123
--------------------------
registering...
connecting...
javax.net.ssl.SSLHandshakeException: java.security.cert.CertificateException: root certificate not trusted of
[ise.lab6.com]
        at sun.security.ssl.Alerts.getSSLException(Alerts.java:192)
        at sun.security.ssl.SSLSocketImpl.fatal(SSLSocketImpl.java:1917)
        at sun.security.ssl.Handshaker.fatalSE(Handshaker.java:301)
        at sun.security.ssl.Handshaker.fatalSE(Handshaker.java:295)
        at sun.security.ssl.ClientHandshaker.serverCertificate(ClientHandshaker.java:1471)
        at sun.security.ssl.ClientHandshaker.processMessage(ClientHandshaker.java:212)
        at sun.security.ssl.Handshaker.processLoop(Handshaker.java:936)
        at sun.security.ssl.Handshaker.process_record(Handshaker.java:871)
        at sun.security.ssl.SSLSocketImpl.readRecord(SSLSocketImpl.java:1043)
        at sun.security.ssl.SSLSocketImpl.performInitialHandshake(SSLSocketImpl.java:1343)
        at sun.security.ssl.SSLSocketImpl.startHandshake(SSLSocketImpl.java:1371)
        at sun.security.ssl.SSLSocketImpl.startHandshake(SSLSocketImpl.java:1355)
        at org.jivesoftware.smack.XMPPConnection.proceedTLSReceived(XMPPConnection.java:806)
        at org.jivesoftware.smack.PacketReader.parsePackets(PacketReader.java:267)
        at org.jivesoftware.smack.PacketReader.access$000(PacketReader.java:43)
        at org.jivesoftware.smack.PacketReader$1.run(PacketReader.java:70)
Caused by: java.security.cert.CertificateException: root certificate not trusted of [ise.lab6.com]
        at org.jivesoftware.smack.ServerTrustManager.checkServerTrusted(ServerTrustManager.java:144)
        at sun.security.ssl.AbstractTrustManagerWrapper.checkServerTrusted(SSLContextImpl.java:865)
        at sun.security.ssl.ClientHandshaker.serverCertificate(ClientHandshaker.java:1453)
        ... 11 more
```