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

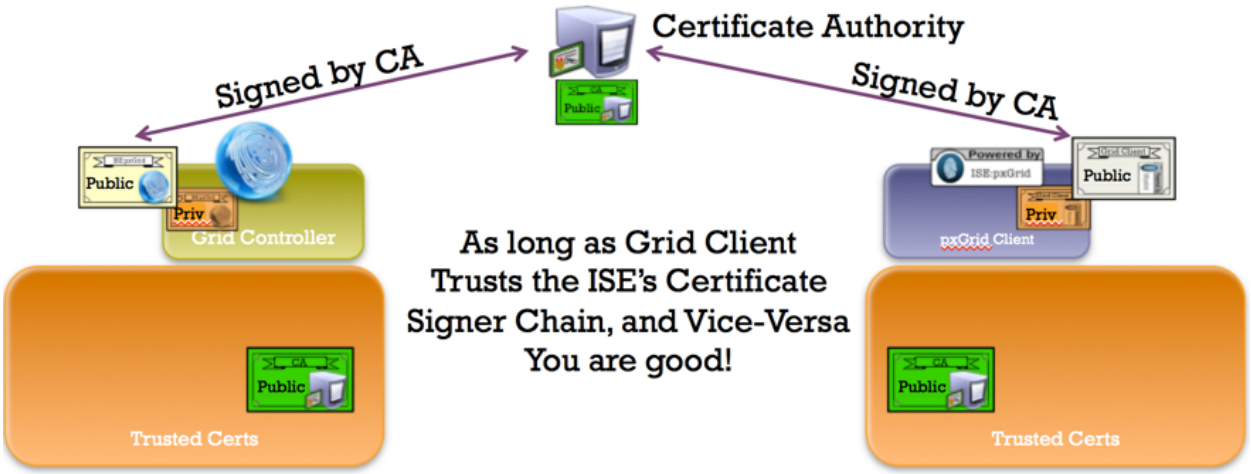
This document does not cover using the ISE 2.1/ISE 2.2 Internal Certificate Authority (CA) for deploying pxGrid client certificates which are included in the reference section.

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.

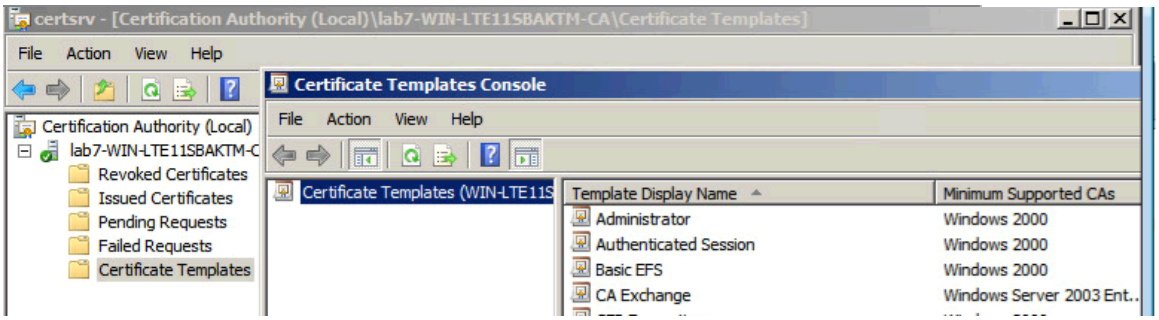


Using an External Certificate Authority (CA) Server

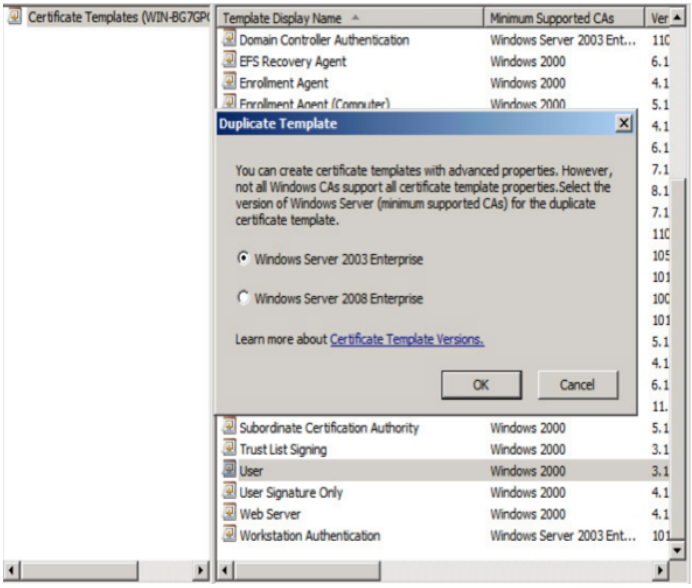
Using an external CA server to generate pxGrid certificate, a customized template with an EKU of both client and server authentication must be configured. In this example, Microsoft 2008 Enterprise CA R2 Server was used.

Customized Template

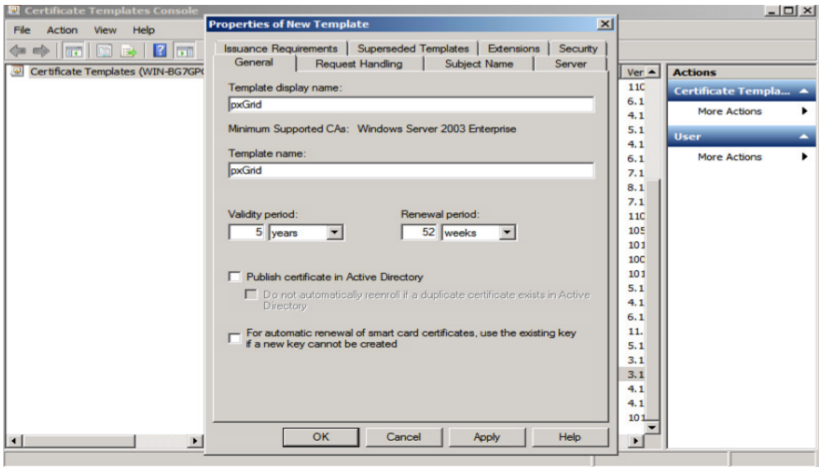
Step 1 Select **Administrative Tools->Certificate Authority-> "+" dropdown next to CA server->Right-Click on Certificate Templates->Manage**



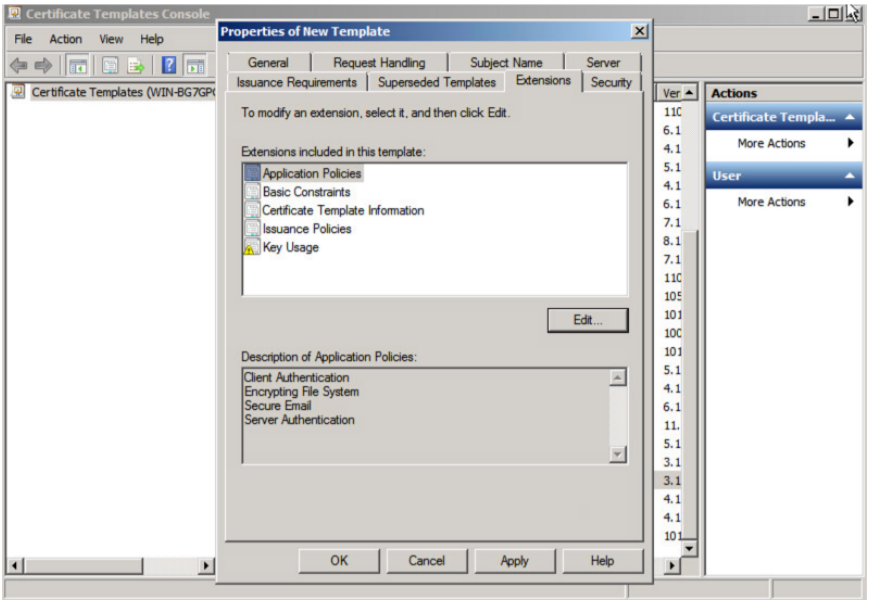
Step 2 **Right-Click** and **Duplicate User template->Select Windows 2003 Enterprise->OK**



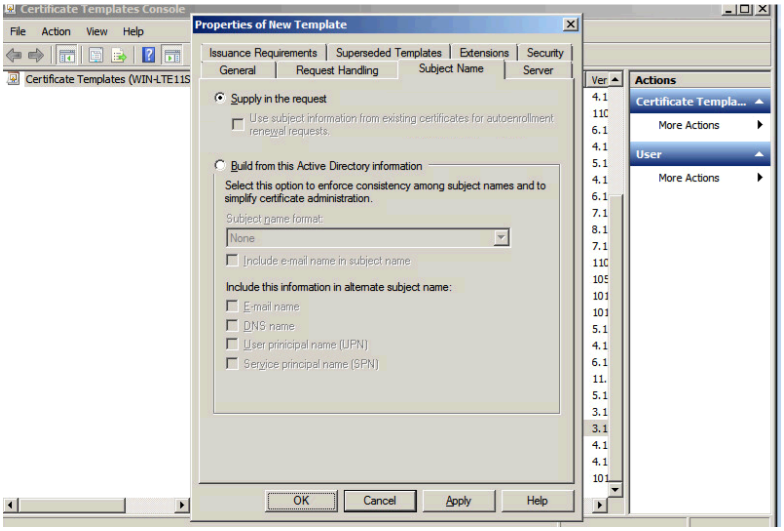
Step 3 Enter name of certificate template, uncheck "Publish certificate in Active Directory", and provide validity period and renewal period.



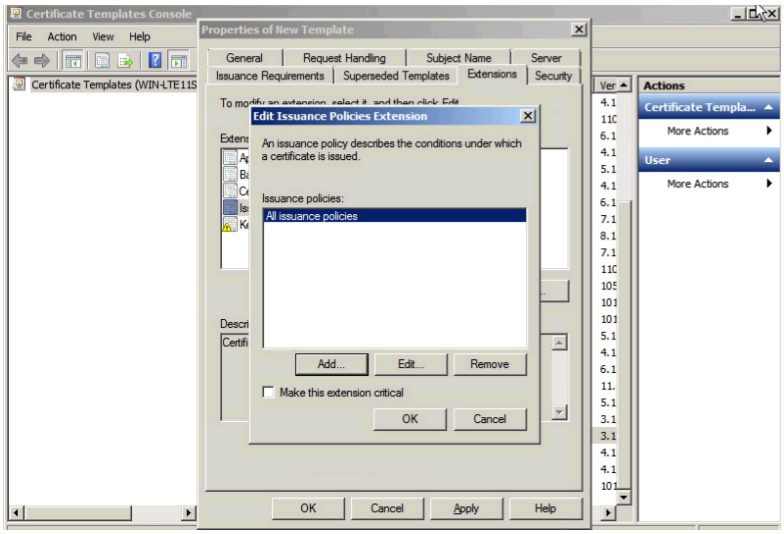
Step 4 Click **Extensions->Add->Server Authentication->Ok->Apply**



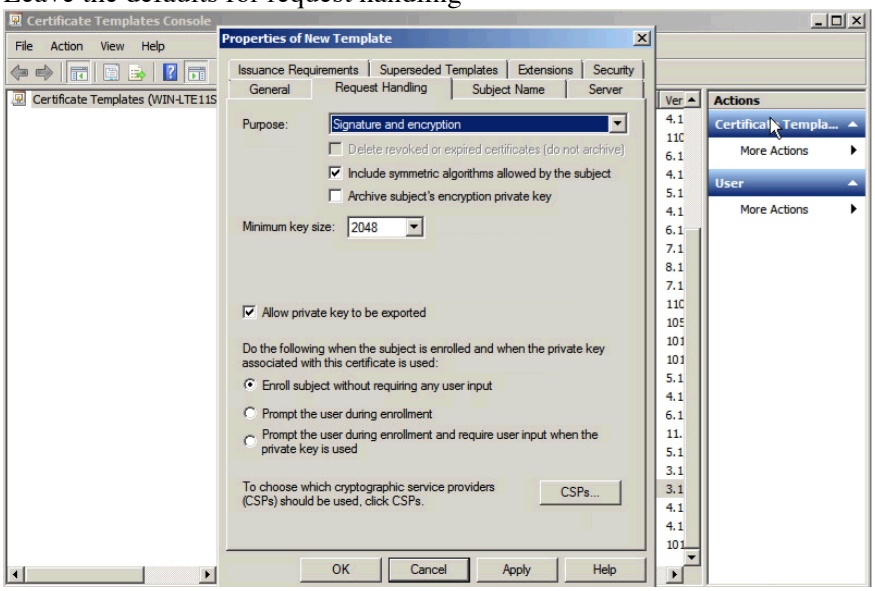
Step 5 Click Subject Name, Enable Supply in the request



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

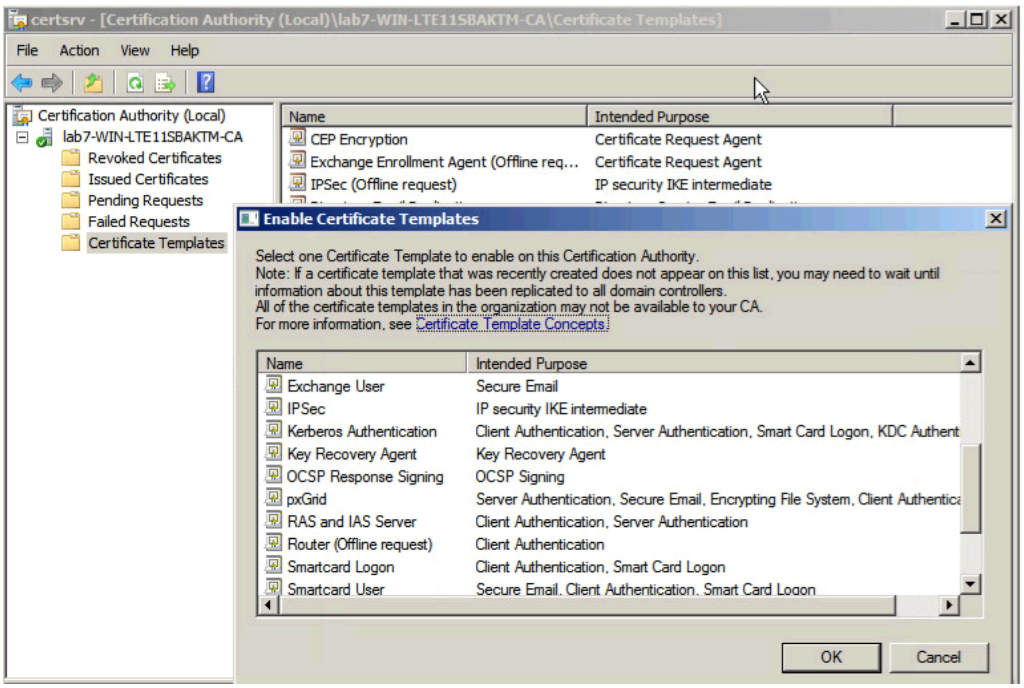


Step 7 Leave the defaults for request handling

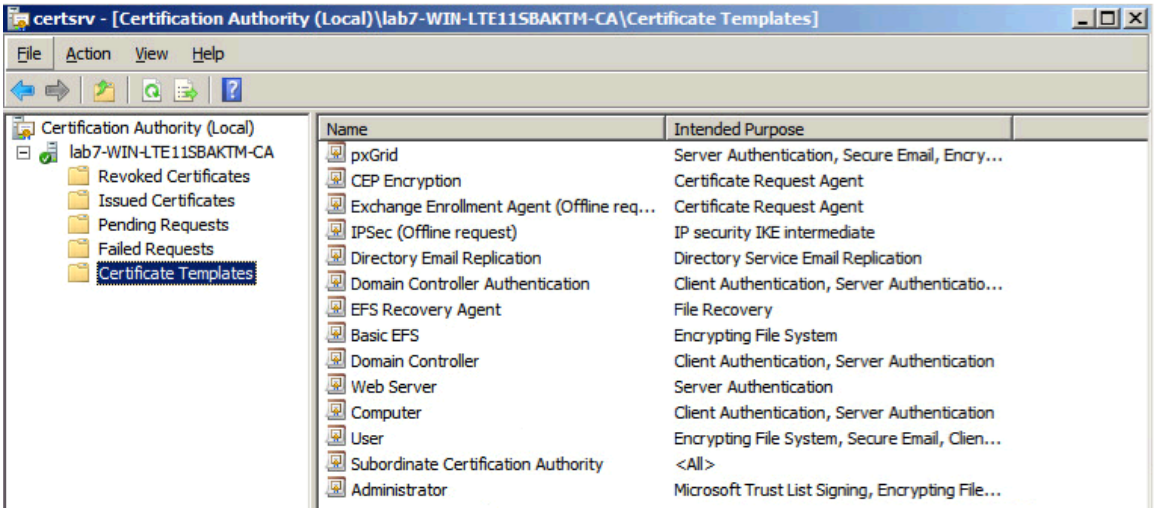


Step 8 Right-click on Certificate Templates

Step 9 Select New Template to issue and select pxGrid



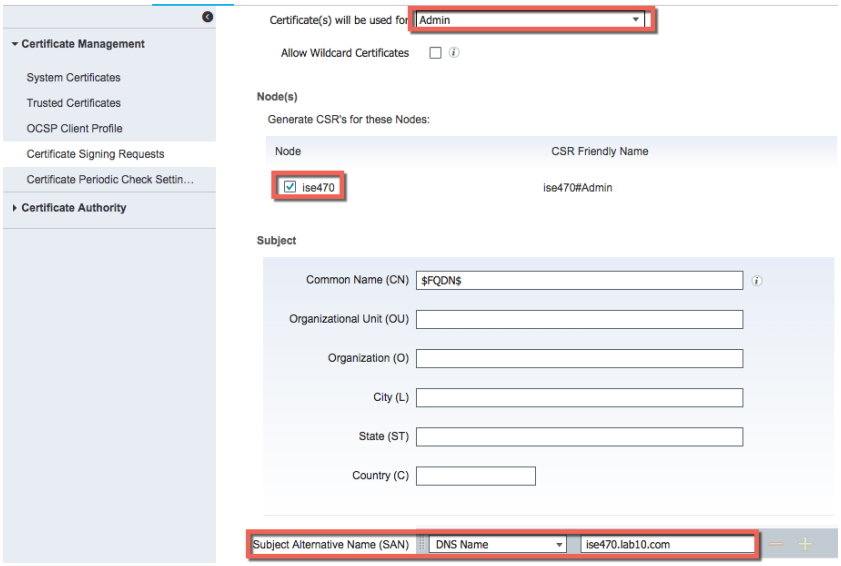
Step 10 You should see the pxGrid template



Configuring ISE pxGrid node

Generating Certificate Signing Request (CSR)

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

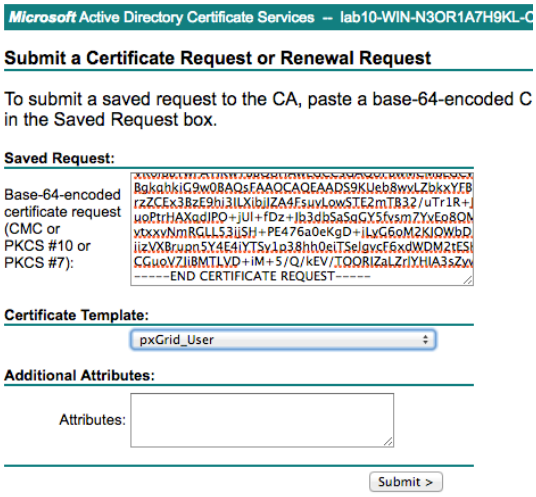


Step 2 Select **Generate**

Step 3 Select Export and open the PEM file copy


```
-----BEGIN CERTIFICATE REQUEST-----
MIIC7jCCAdYCAQAwGzEZMBcGA1UEAxMQaXNlNDcwLmxhYjEwLmNvbTCCASIwDQYJ
KoZIhvcNAQEBBQADggEPADCCAQoCggEBAJSM1PM6t1crlvZxEe584Y/dnrrEdE7j
qKiS0RWLXmbEDHXl5F0rIhcn7rAR0e9h8V1oeA4v9+Sj1I0slsfTETUoWbWpqgyo
J5DEj5YxS2vH+cAhKj5Xp4ls7ziqBaUyw9OnaRTjUp40gyOY3O2/8NCWWXvt4r0w
gFYuIbi8emMRuNPn+448f3Rx3mHs2cdARosjtUC/OmAfysl7uPDCahjGqapy/l0E
TuW0MAjdvUaibimDl+WmsWnFvmiSVuoFh5/JYGh3pXdw5MK9tt5hltP0dZMkbANJ
1jwyYmOeVz9Zal51nuWpJJ5bZJjZE88/dA8pQJFOXE/jqTmfZzwhztsCAwEAAaCB
jTCBigYJKoZIhvcNAQkOMX0wezAbBgNVHREEFDASghBpc2U0NzAubGFiMTAuY29t
MAsGA1UdDwQEAwIF4DAdBgNVHQ4EFgQU2jmj7l5rSw0yVb/vlWAYkK/YBwkwHQYD
VR0lBBYwFAYIKwYBBQUHAwEGCCsGAQUFBwMCMBEGCWCGSAGG+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



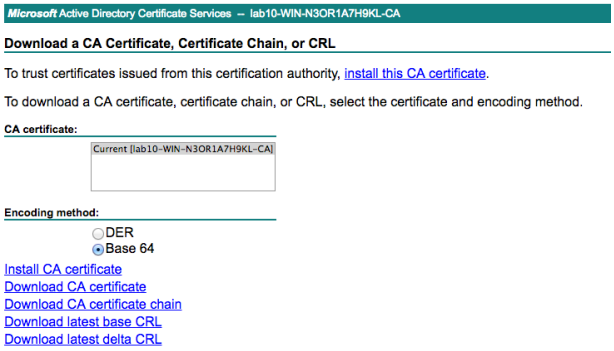
Step 5 Select **Submit**

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

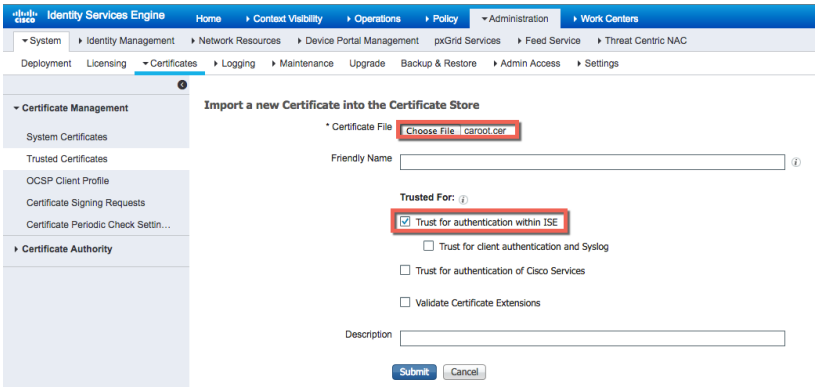
Select **Download Certificate->Base 64->Download CA certificate**



Step 9 Rename the certificate to caroot.cer

Importing CA root certificate into ISE Trusted Certificate Store

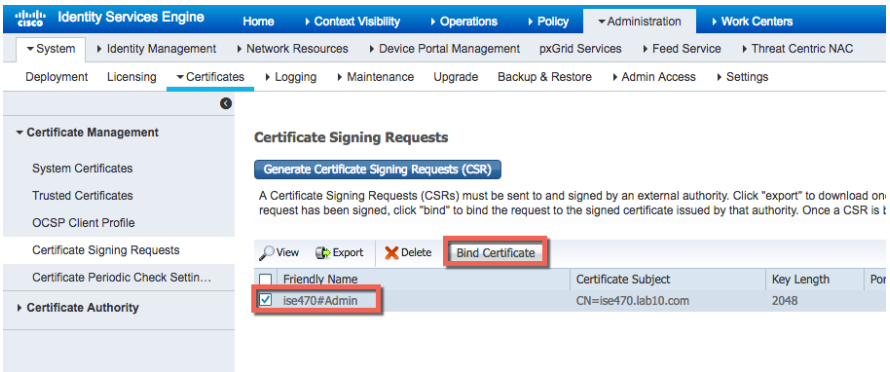
Step 1 Select **Administration->System->Certificates->Certificate Management->Trusted Certificates->Import->Certificate file and import the root certificate**



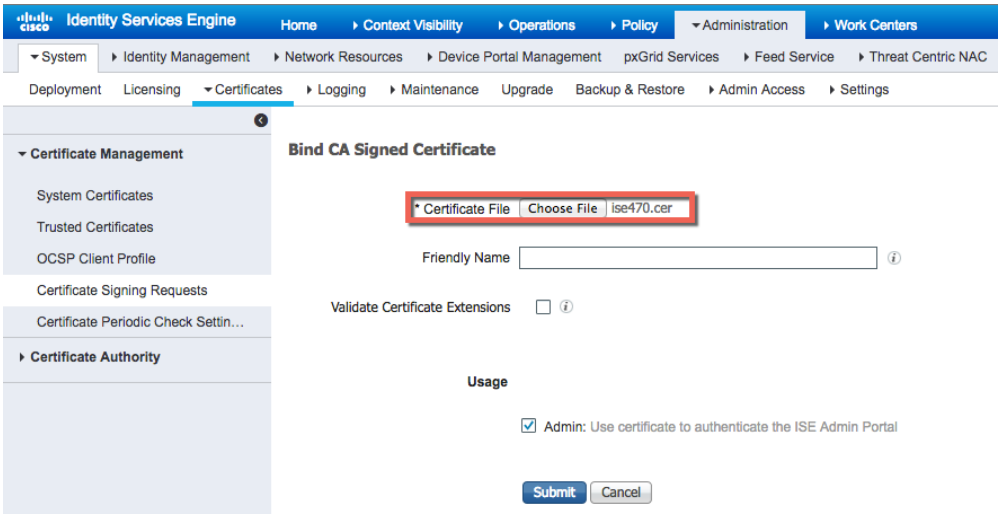
Step 2 Select **Submit**

Bind ISE certificate to Certificate Signing Request (CSR)

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



Step 2 Select ISE certificate file and upload the root certificate



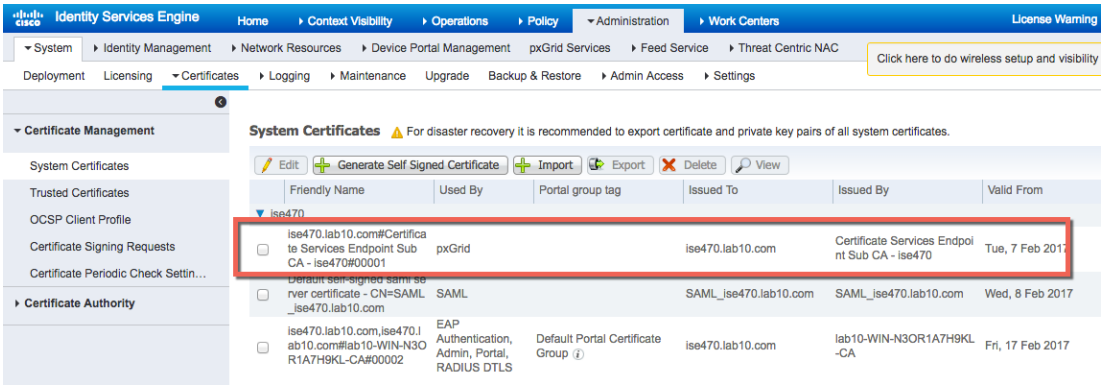
Step 3 Select **Submit**

Step 4 Select **Yes** for an application restart

Step 5 Select **Yes** to replace the existing certificate. The system will restart

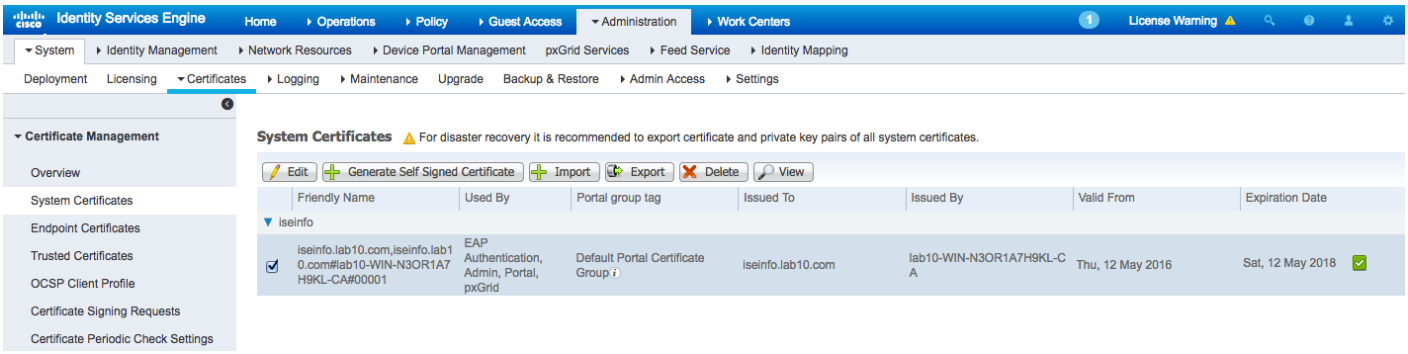
Step 6 Select **Administration->System->Certificates->System Certificates**

You should see the default pxGrid certificate signed by the internal ISE CA

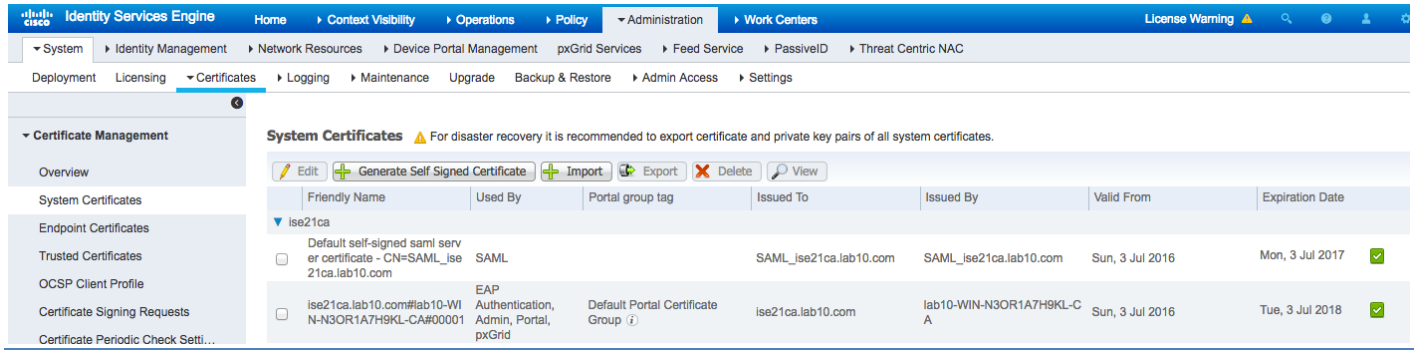


Note: For ISE 2.0 and ISE 2.1, the "admin" certificate should be valid for pxGrid also. Modify the certificate and verify that the certificate is used by pxGrid also.

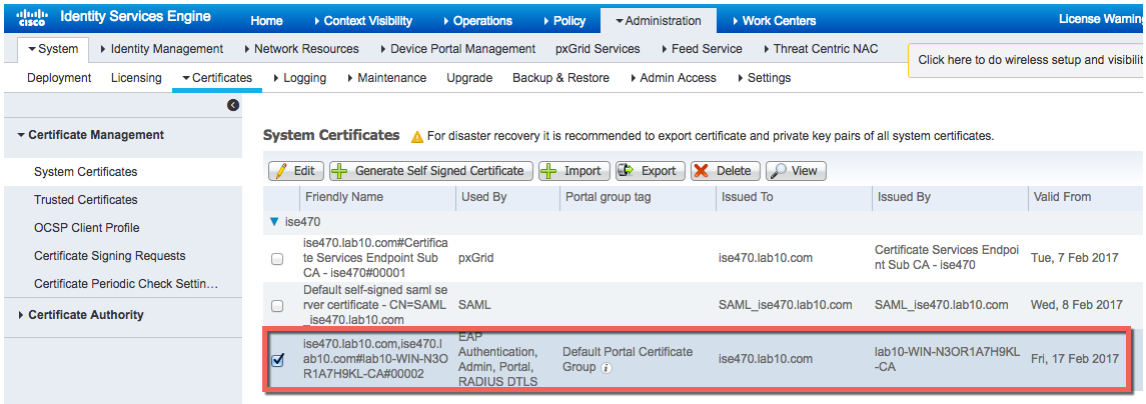
ISE 2.0



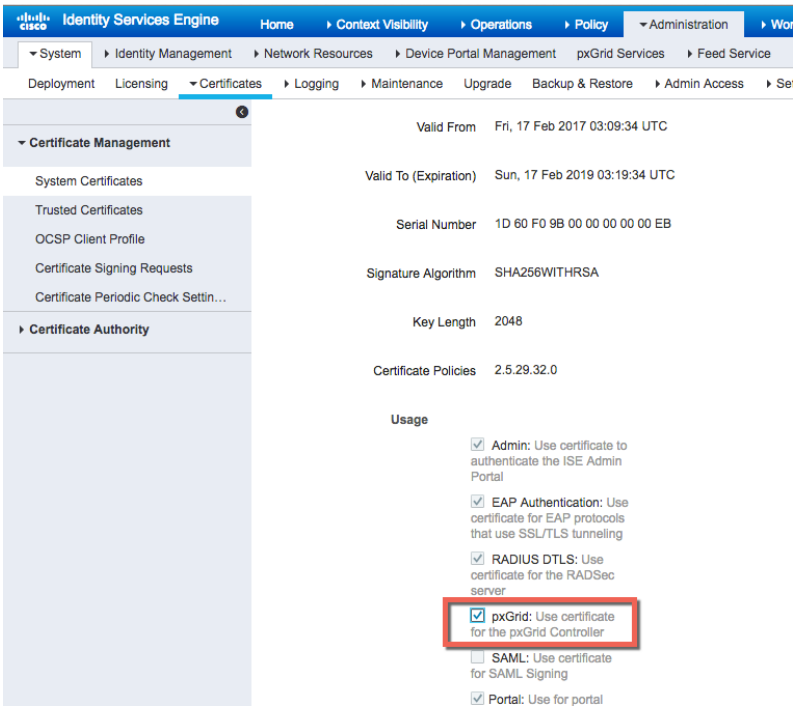
ISE 2.1



Step 7 Edit the admin certificate

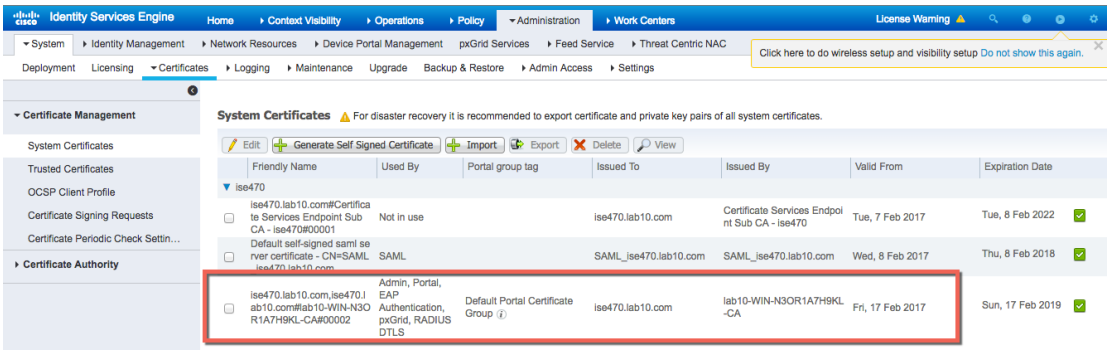


Step 8 Select **pxGrid**



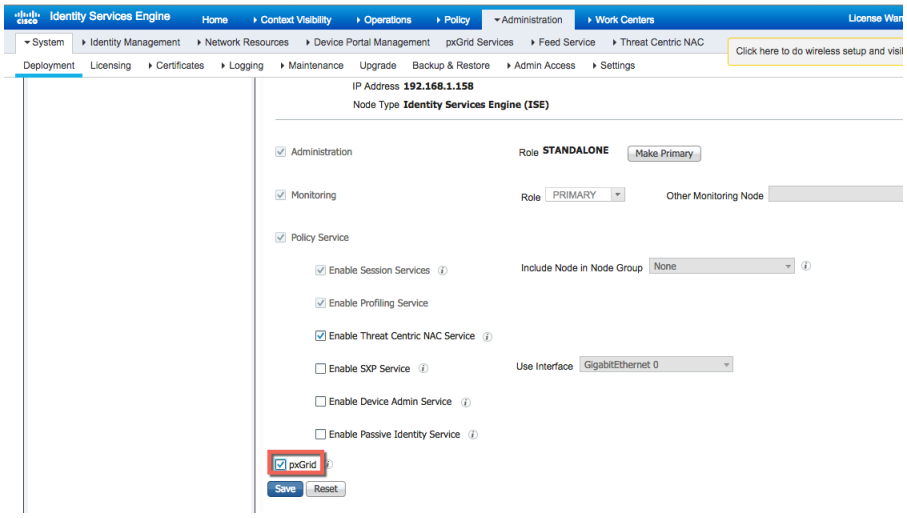
Step 9 Select **Save**
You should see the pxGrid purpose assigned to the admin certificate

Note: This is required for security solutions that require bulk session downloads

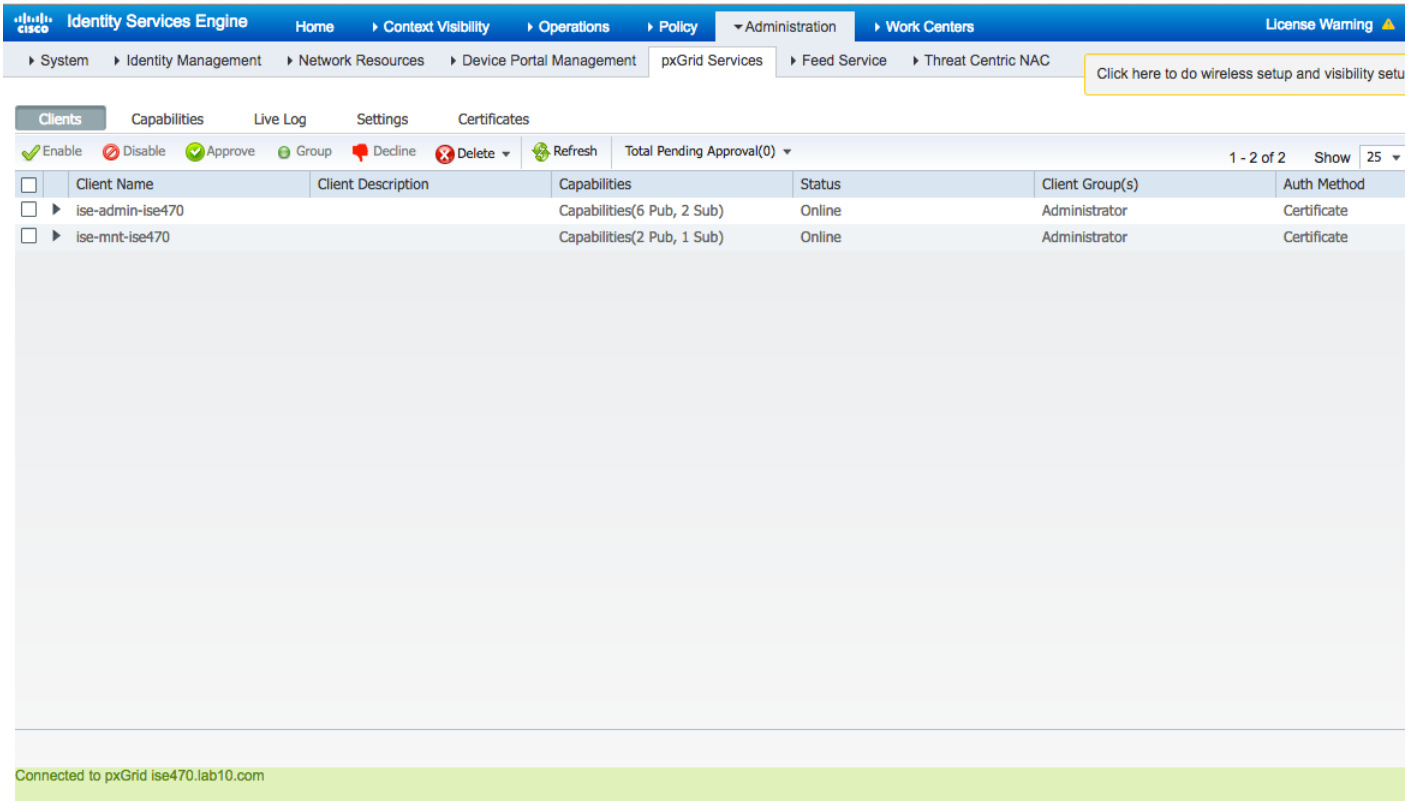


Enabling pxGrid

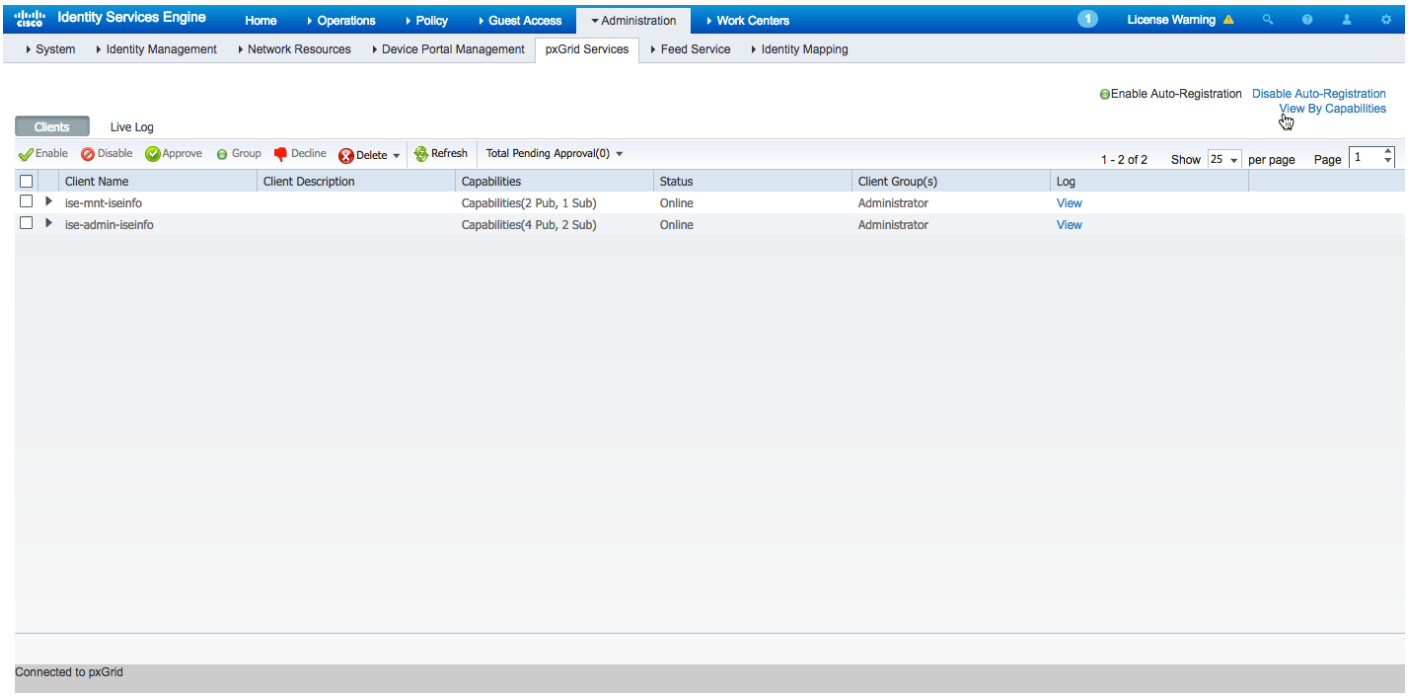
Step 1 Select **Administration->System->Deployment->edit ise node->enable pxGrid**



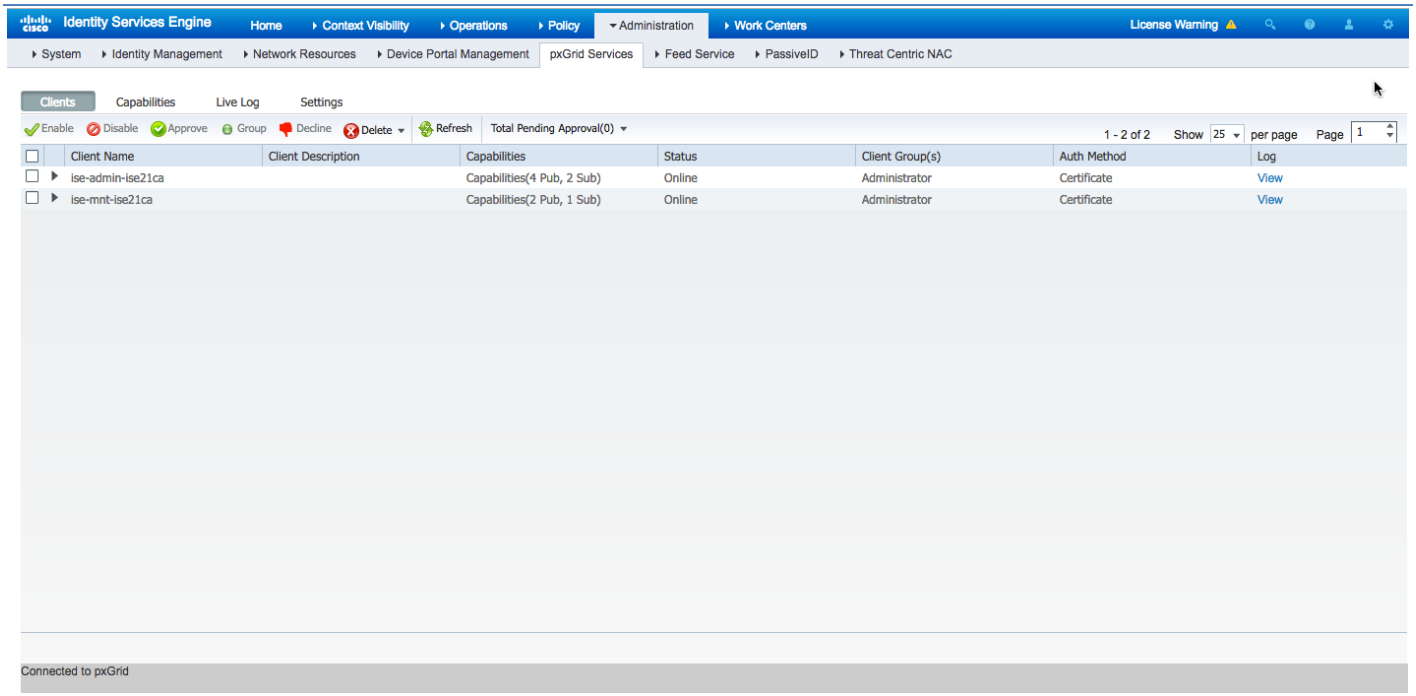
Step 2 Select **Save**
Step 3 Run "**sh application status ise**" to verify the pxGrid services are running
Step 4 Select **Administration->pxGrid Services, you should see the published nodes appear and pxGrid node connectivity**



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



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



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)

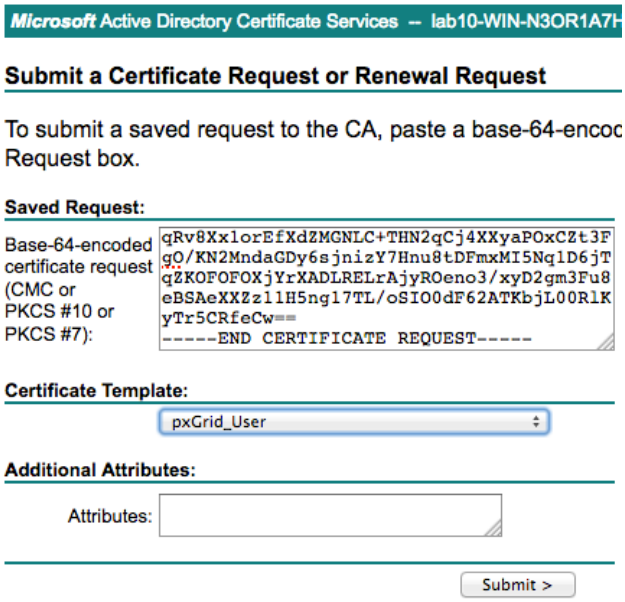
```
openssl req -new -key pxGridClient.key -out pxGridClient.csr

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

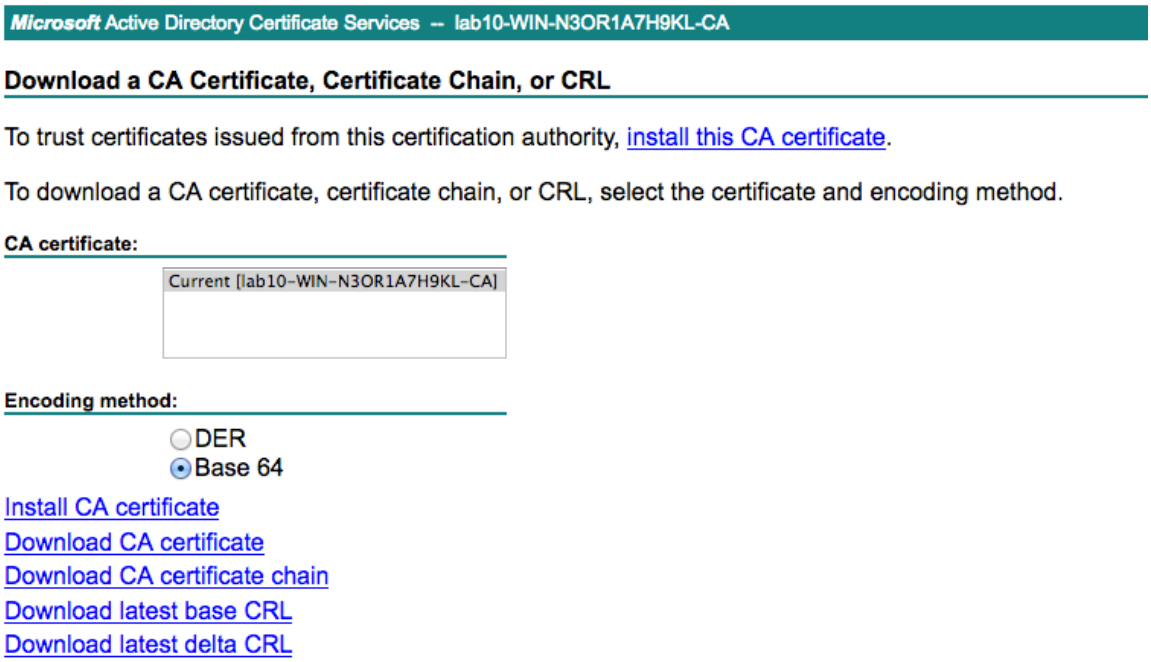
Note: A CA template of Windows 2003 was selected, so it would appear in the Drop-down. A user template was duplicated wit both EKUs for client and server authentication.



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**



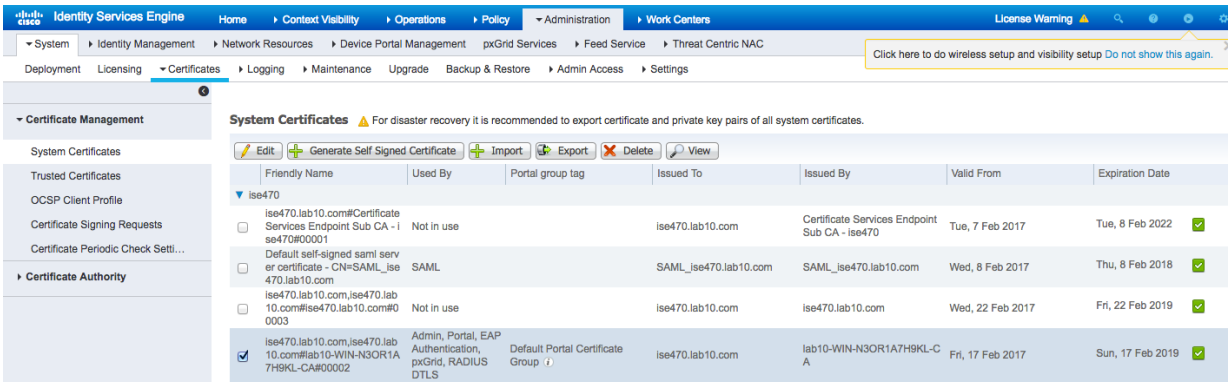
Step 7 Create a pxGrid client pkcs12 file (pxGridClient.p12) from the private key in the pxGridClient certificate (i.e. pxGridClient.cer). This will be used for keystore management and can be a random filename with a .p12 extension. Include the CA root file (i.e. ca_root).

```
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
```

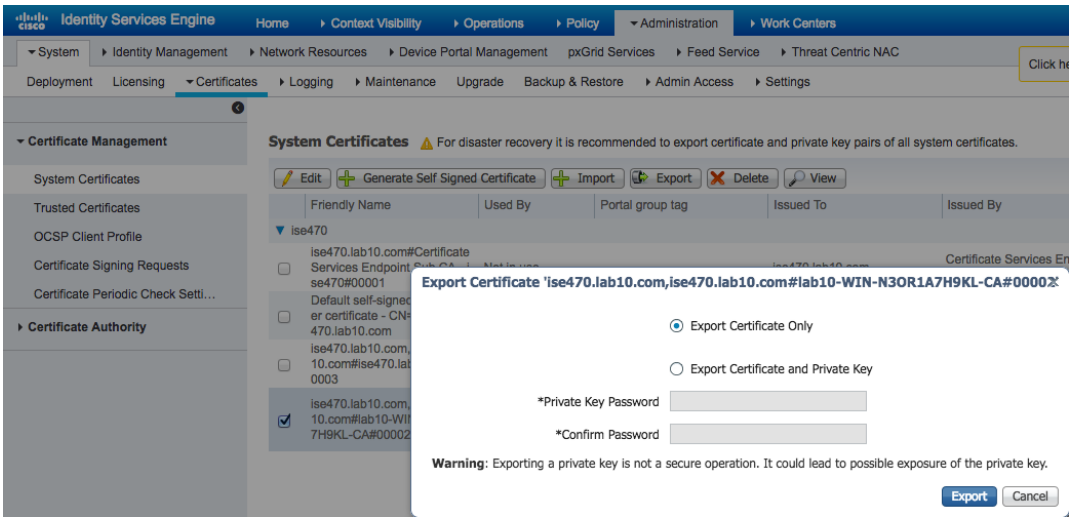
Step 8 Create the pxGrid client identity keystore (i.e.pxGridClient.jks). This will be the pxGrid client identity keystore. This can be a random filename with a .jks extension. This will serve as the keystoreFilename and associated keystorePassword in the pxGrid script examples.

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

Enter destination keystore password:  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 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



Step 10 You should see:



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.

```
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 15 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 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

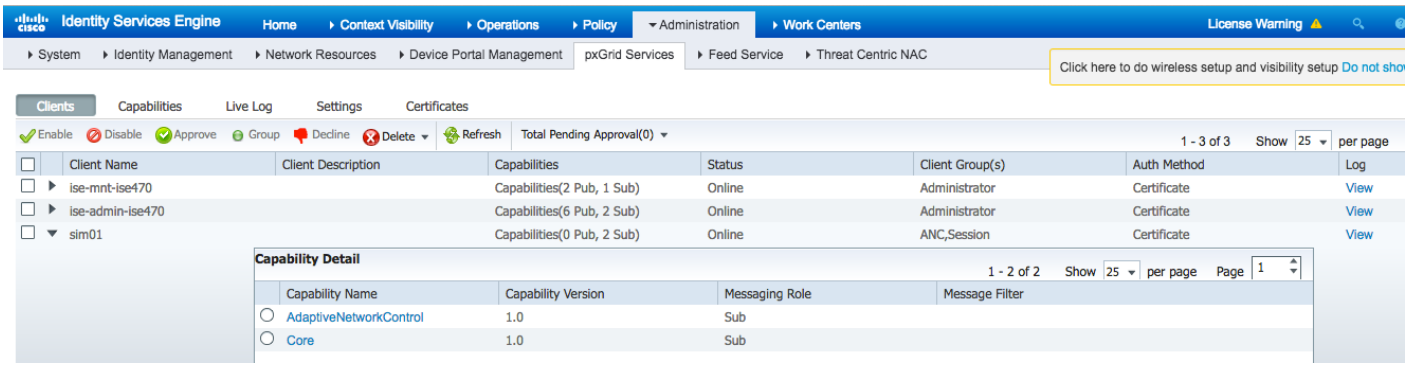
The pxGrid scripts: register.sh and session download.sh will be run to ensure pxGrid client connection and pxGrid registration. Session downloads will ensure that there are no issues with the ISE MNT certificate and the pxGrid client.

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



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=
  group=Session
  description=null
  keystoreFilename=pxGridClient.jks
  keystorePassword=Cisco123
  truststoreFilename=root3.jks
  truststorePassword=Cisco123
--------------------------
Connecting...
00:26:20.356 [main] INFO  com.cisco.pxgrid.Configuration - Connecting to host 192.168.1.158
00:26:20.647 [main] INFO  com.cisco.pxgrid.Configuration - Connected OK to host 192.168.1.158
00:26:20.648 [main] INFO  com.cisco.pxgrid.Configuration - Client Login to host 192.168.1.158
00:26:20.675 [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=0A0000010000002A00C760B6, 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=0000002B], 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=0A000001000000150001E814, 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=0A0000010000030017464A9, 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=0A000001000000032018140D4, 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=0A000001000000190001FFA3, 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.

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 2 entries

Alias name: ca_root1
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:[
  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: 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                                        ?...
]
]



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


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: 1d60f09b0000000000eb
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  ..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 04 30 0C 06 0A 2B 06  ..+.......0...+.
0020: 01 04 01 82 37 0A 03 04   30 0A 06 08 2B 06 01 05  ....7...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 96  ....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 [
  [
   accessMethod: caIssuers
   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: 2.5.29.17 Criticality=false
SubjectAlternativeName [
  DNSName: ise470.lab10.com
]

#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                                        ....
]
]



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

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=Maryland, C=US
Issuer: CN=lab10-WIN-N3OR1A7H9KL-CA, DC=lab10, DC=com
Serial number: 126f78a50000000000f2
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  ..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 04 30 0C 06 0A 2B 06  ..+.......0...+.
0020: 01 04 01 82 37 0A 03 04   30 0A 06 08 2B 06 01 05  ....7...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 96  ....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 [
  [
   accessMethod: caIssuers
   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                                        ....
]
]



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

```
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: 126f78a50000000000f2
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  ..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 04 30 0C 06 0A 2B 06  ..+.......0...+.
0020: 01 04 01 82 37 0A 03 04   30 0A 06 08 2B 06 01 05  ....7...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 96  ....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 [
  [
   accessMethod: caIssuers
   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                                        ....
]
]

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
]

#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                                        ?...
]
]



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

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