Cisco pxGrid로 인증서 배포

***ISE pxGrid** 노드 및 **pxGrid** 클라이언트에 자체 서명 인증서 사용*

목차

이 문서 정보

이 문서에서는 자체 서명 인증서를 사용하여 pxGrid 클라이언트 및 ISE pxGrid 노드를 구성하는 데 필요한 컨피그레이션 단계에 대해 설명합니다. 이 문서는 Cisco pxGrid를 구축하는 Cisco 현장 엔지니어, 기술 마케팅 엔지니어, 파트너 및 고객을 대상으로 합니다. 또한 pxGrid에 대해 잘 알고 있어야 합니다.

pxGrid에 대해 잘 모르는 사용자는 다음을 참조하십시오.

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

Cisco 어카운트 팀에서 pxGrid SDK를 받습니다.

Cisco ISE(Identity Services Engine) 1.3이 설치된 것을 전제로 합니다. OSX 10.8.5를 실행 중인 Mac은 pxGrid 클라이언트로 사용됩니다. Linux OS도 사용할 수 있습니다. pxGrid 클라이언트에는 Oracle Java Development Kit 7 또는 8이 필요합니다.

Deploying pxGrid with Certificates 시리즈에는 다음과 같은 두 가지의 다른 문서가 있습니다.

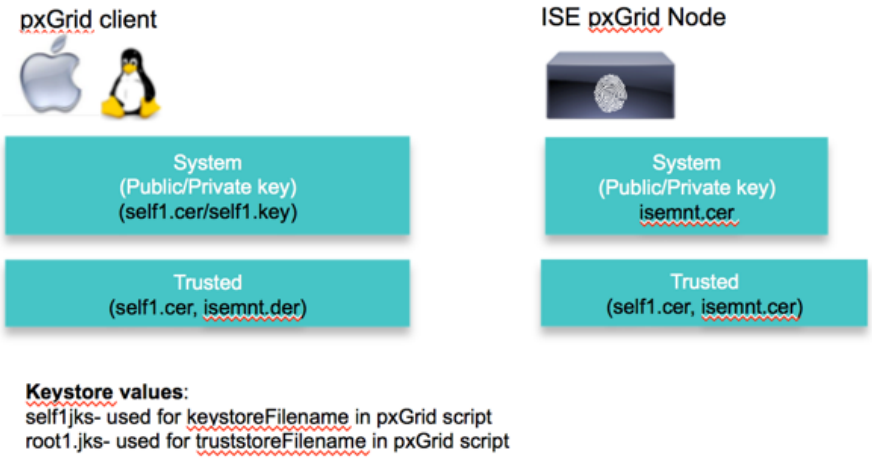
- CA(Certificate Authority) 서명 ISE pxGrid 노드 인증서 및 pxGrid 클라이언트 사용
- CA(Certificate Authority) 서명 pxGrid 클라이언트 및 ISE 자체 서명 pxGrid 노드 사용

서론

ISE pxGrid 노드 및 pxGrid 클라이언트에 모두 자체 서명 인증서를 사용하여 pxGrid를 구축하는 것은 pxGrid SDK의 샘플 인증서를 사용하지 않고 테스트하기 위한 대체적인 방법입니다. 자체 서명 인증서는 트러스트된 소스에서 생성되지 않으며 CA(Certificate Authority)를 사용하는 것보다 보안성이 낮습니다. 그러나 이 문서에서 ISE는 pxGrid 클라이언트의 퍼블릭 키를 ISE 트러스트된 인증서 저장소로 가져와 pxGrid 클라이언트의 퍼블릭 키를 트러스트합니다. pxGrid 클라이언트는 pxGrid 클라이언트의 트러스트된 저장소에 있는 ISE 퍼블릭 인증서를 트러스트합니다. 이는 일반적으로 자체 서명 인증서를 사용하는 것보다 더 높은 보안성을 제공합니다.

인증서 컨피그레이션 예

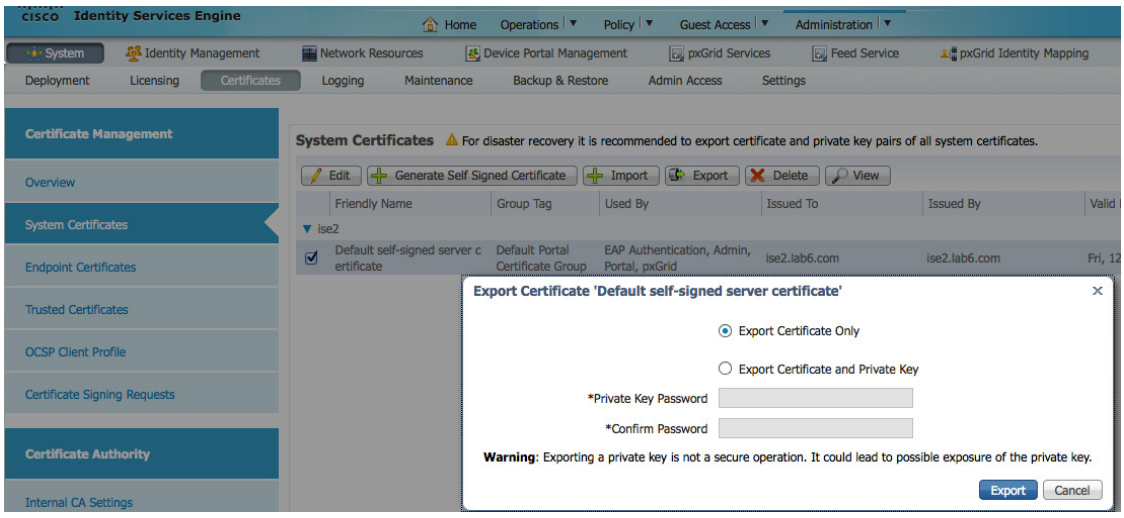
다음은 이 문서에 사용된 인증서의 예를 나타냅니다.



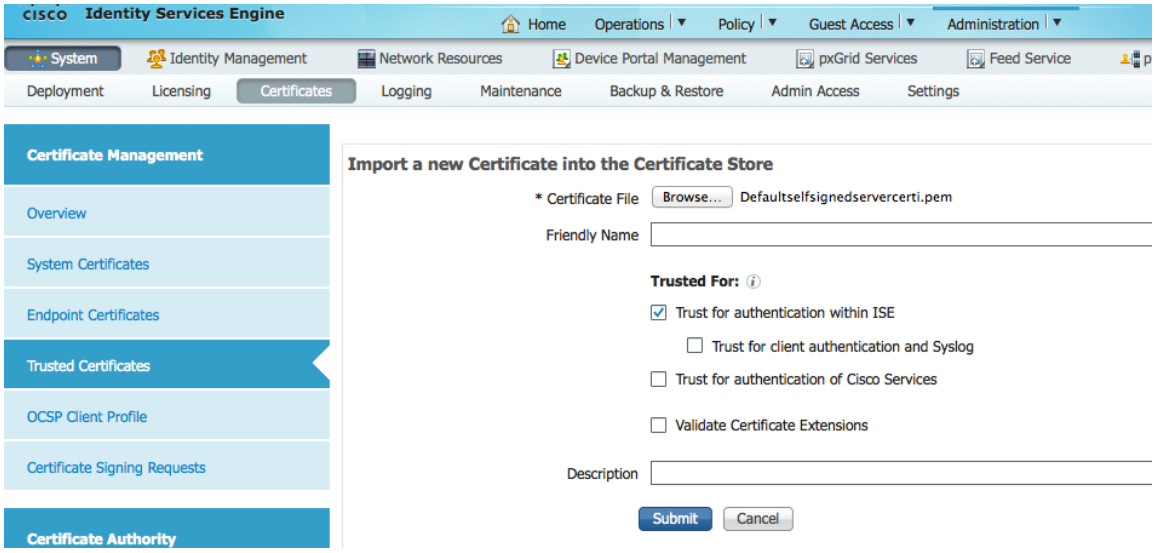
자체 서명 ISE pxGrid 노드 인증서 및 pxGrid 페르소나 컨피그레이션

이 섹션에서는 ISE 자체 서명 인증서를 ISE 트러스트된 인증서 저장소로 가져옵니다. ISE ID 인증서가 트러스트된 인증서 저장소에 있으면 ISE 노드의 pxGrid 페르소나가 활성화됩니다. pxGrid ISE 노드가 Primary로 변경됩니다.

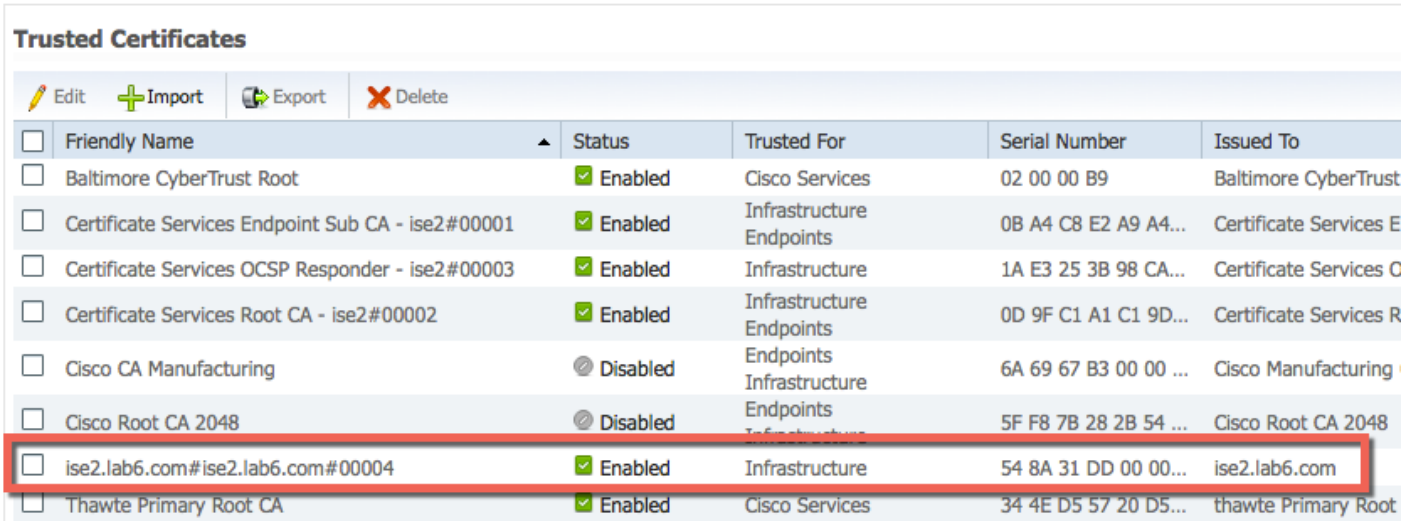
1단계 자체 서명 ISE ID 인증서를 내보내고 .pem 파일로 저장합니다. **Administration->System->Certificates를 차례로 누른 다음 ISE identity cert->Export**(퍼블릭 키만)를 선택합니다.



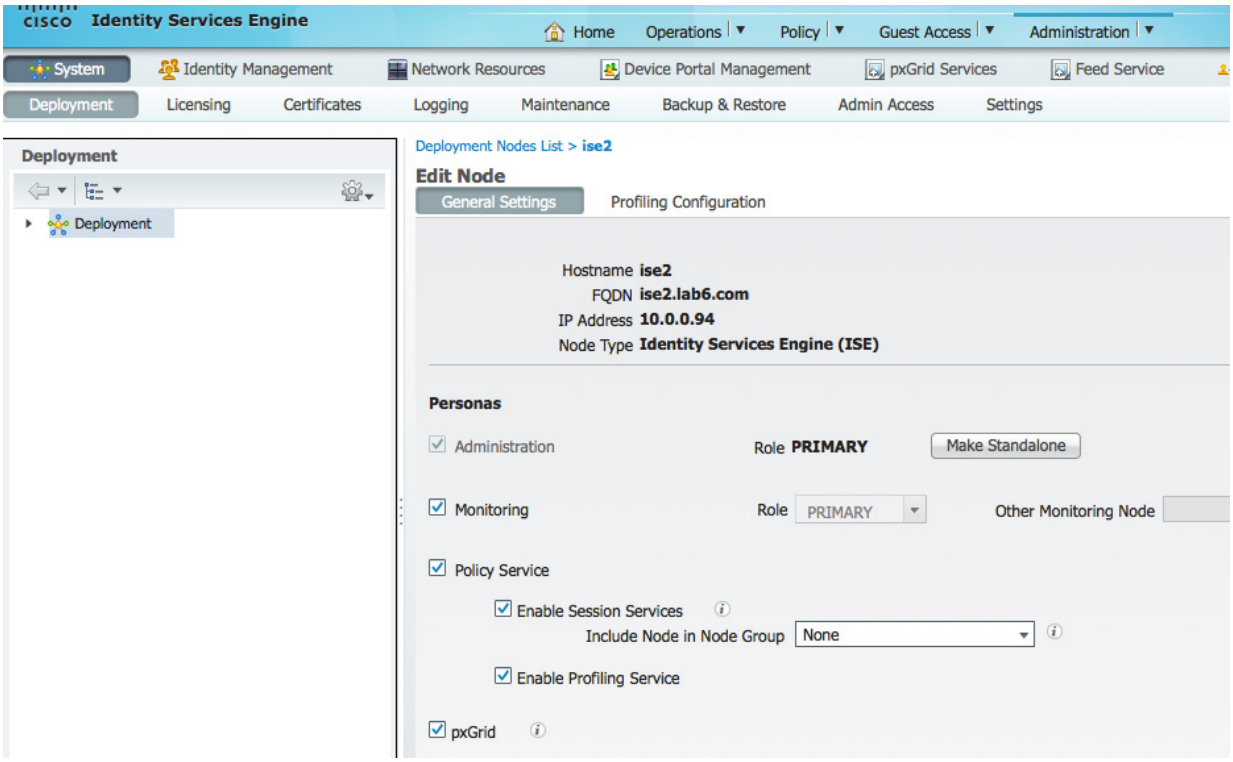
2단계 저장된 ISE .pem 파일을 ISE 트러스트된 인증서 저장소로 가져옵니다. **Administration->System->Certificates->Trusted Certificates->Browse를 차례로 누른 다음 파일을 업로드하고 Submit을 누릅니다**. "trust for authentication within ISE"를 활성화합니다.



ISE 트러스트된 인증서 가져오기가 표시됩니다.

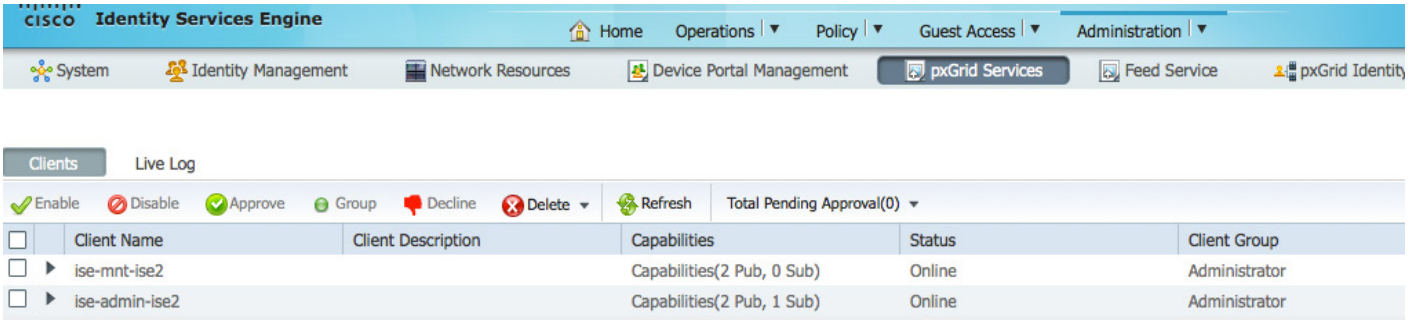


3단계 ISE에서 pxGrid 페르소나를 활성화합니다.
Administration->System->Deployment->Enable pxGrid를 차례로 누른 다음 역할을 Primary로 변경하고 Save를 누릅니다.



참고: 역할을 Primary로 반드시 변경해야 하는 것은 아닙니다.

4단계 게시된 서비스가 시작되었는지 확인합니다.
Administration->pxGrid Services



참고: ISE 게시 노드가 표시되기 전까지 지연이 발생할 수 있습니다. pxGrid 페르소나가 활성화되기 전에 인증서를 설치해야 합니다.

자체 서명 pxGrid 클라이언트 인증서

이 섹션에서는 pxGrid 클라이언트에서 자체 서명 인증서를 생성하는 프로세스를 자세히 살펴봅니다. pxGrid 퍼블릭/프라이빗 키 쌍이 생성되면 프라이빗 키(예: self1.key)에서 PKCS 12 파일(self1.p12)이 생성됩니다.

이 PKCS 12 파일은 대상 또는 ID 키 저장소(예: self1.jks)에 가져오기 되며, 이러한 저장소는 pxGrid 스크립트의 keystoreFilename 및 keystorePassword 역할을 합니다. ISE ID 인증서 및 퍼블릭 인증서도 모두 이 키 저장소에 추가됩니다.

ISE ID 인증서는 truststoreFilename 및 truststorePassword 역할을 하는 트러스트 키 저장소(예: root1.jks)에도 추가됩니다.

1단계 pxGrid 클라이언트에 대한 프라이빗 키(예: self1.key)를 생성합니다.

```
openssl genrsa -out self1.key 4096

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

2단계 자체 서명 CSR(self1.csr) 요청을 생성하고 챌린지 비밀번호를 제공합니다.

```
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]:
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 []:LAB
```

참고: 유지 관리의 용이성을 높이고 오류를 줄이려면 이 문서 전체에서 같은 비밀번호를 사용하십시오.

3단계 자체 서명 퍼블릭 키 쌍 인증서(예: self1.cer)를 생성합니다.

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

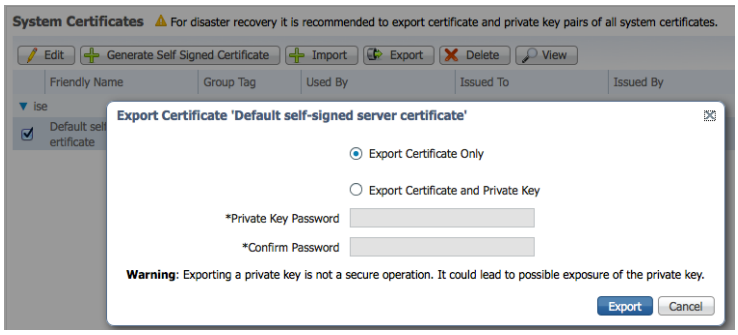
4단계 PKCS12 파일(예: self1.p12)이 프라이빗 키에서 생성됩니다.

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

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

5단계 self1.p12 파일이 ID 키 저장소(예: self1.jks)에 가져오기됩니다. 키 저장소 파일 이름은 확장자가 .jks인 임의의 이름일 수 있습니다. 이는 pxGrid 스크립트에서 keystoreFilename 및 associated keystorePassword 역할을 합니다.

```
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
```

6단계 퍼블릭 ISE ID 인증서만 pxGrid 클라이언트로 내보내며, 이는 .pem 형식으로 이루어집니다. 확장자가 .pem인 파일의 이름을 더 읽기 쉽게 변경할 수 있으며, 이 예에서 해당 파일의 이름은 isemnt.pem으로 변경되었습니다.



7단계 .pem 파일을 .der 형식으로 변환합니다.

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

8단계 ISE ID 인증서를 ID 키 저장소에 추가합니다. 이는 pxGrid 세션 다운로드 스크립트를 실행할 경우 ISE MNT 노드에서 벌크 세션 다운로드의 보안을 강화하기 위해 사용됩니다.

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

Johns-MacBook-Pro:bin jeppich$ keytool -import -alias pxGridclient1 -keystore self1.jks -file self1.cer
Enter keystore password:
Certificate already exists in keystore under alias <1>
Do you still want to add it? [no]:  n
Certificate was not added to keystore
```

9단계 pxGrid 클라이언트 인증서를 ID 키 저장소로 가져옵니다.

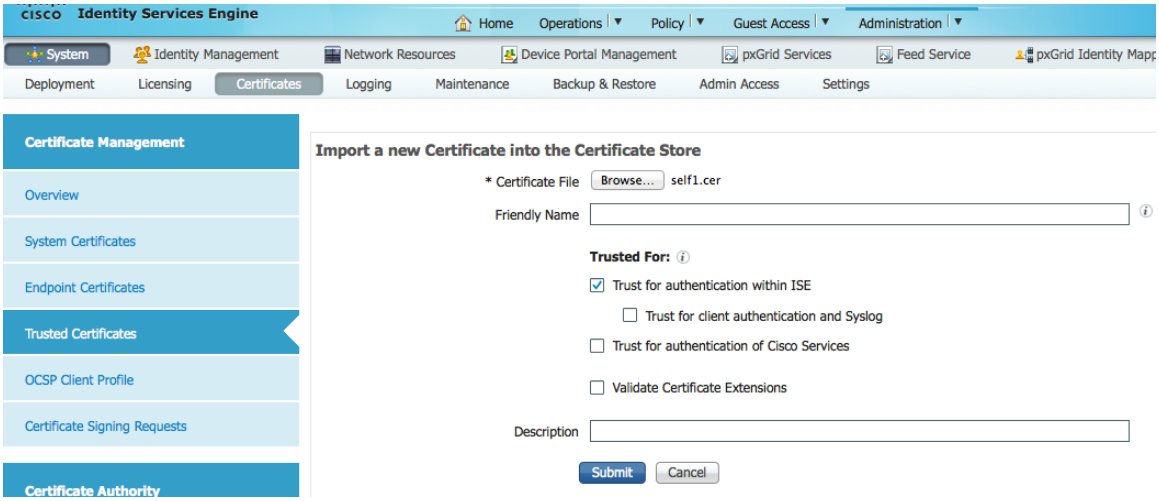
```
keytool -import -alias pxGridclient1 -keystore self1.jks -file self1.cer

Enter keystore password:
Certificate already exists in keystore under alias <1>
Do you still want to add it? [no]: n
Certificate was not added to keystore
```

참고: 다음 메시지가 표시될 경우 인증서가 이미 기존에 있는 키 저장소에 추가된 것이므로, "no"를 입력하면 그대로 유지됩니다. 여기에서는 "yes"를 선택했으므로 인증서가 나중에 추가되었음을 확인할 수 있습니다.

10단계 ISE ID 인증서를 트러스트 키 저장소(예: root1.jks)로 가져옵니다. 저장소는 pxGrid 스크립트의 truststore Filename 및 truststore Password 역할을 합니다.

```
keytool -import -alias root1 -keystore root1.jks -file isemnt.der
Enter keystore password:
Re-enter new password:
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
```

11단계 pxGrid 클라이언트 퍼블릭 인증서(self1.cer)를 ISE 트러스트된 인증서 저장소에 업로드합니다. **Administration->System Certificates->Trusted Certificates를 차례로 누른 다음 pxGrid 클라이언트에서 self1.cer를 업로드합니다.**



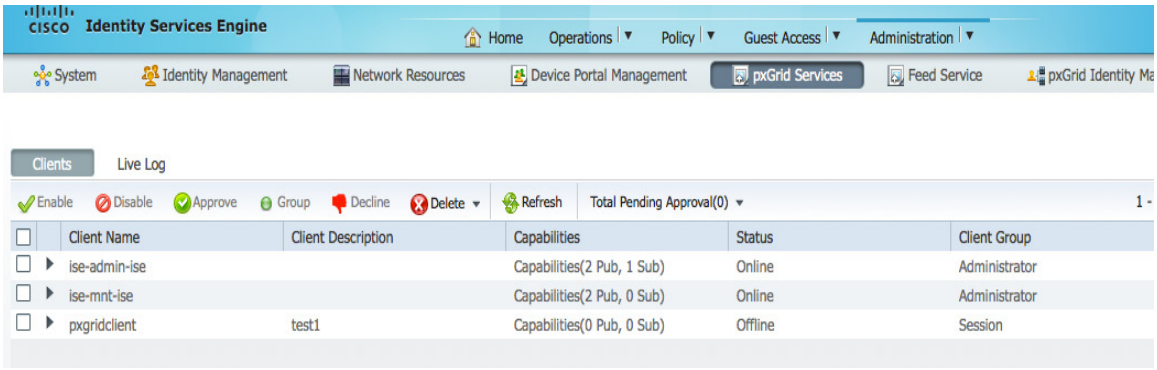
12단계 ID 키 저장소(self1.jks) 및 트러스트 키 저장소(root1.jks)를 ../samples/bin/.. 폴더에 복사합니다.

pxGrid 클라이언트 및 ISE pxGrid 노드 테스트

샘플 pxGrid 스크립트인 register.sh 및 session_download.sh는 pxGrid 클라이언트 연결 및 pxGrid 등록을 확인하기 위해 실행됩니다.

1단계 pxGrid 클라이언트 등록

```
./register.sh -keystoreFilename self1.jks -keystorePassword cisco123 -truststoreFilename root1.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=self1.jks
keystorePassword=cisco123
truststoreFilename=root1.jks
truststorePassword=cisco123
--------------------------
registering...
connecting...
connected.
done registering.
connection closed
```



2단계 세션 다운로드 실행

```
./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
```

키 저장소 항목 보기

키 저장소 항목을 확인하여 ID 및 트러스트 키 저장소의 트러스트된 인증서 항목을 볼 수 있습니다.

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

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:

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.
]
]
```

문제 해결

이 섹션에서는 트러블슈팅에 대한 정보를 제공합니다.

- pxGrid 클라이언트 호스트 이름 및 ISE pxGrid가 DNS를 통해 확인 가능한지 파악하여 pxGrid 스크립팅 오류 메시지를 방지합니다.
- 트러스트 저장소가 변경되고 유사한 오류 메시지가 표시될 경우, ISE VM에서 ISE 애플리케이션을 중지하고 다시 시작합니다.

```
./register.sh -keystoreFilename self1.jks -keysrePassword cisco123 -truststoreFilename root1.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=self1.jks
keystorePassword=cisco123
truststoreFilename=root1.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
```

- ISE 서비스 다시 시작

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