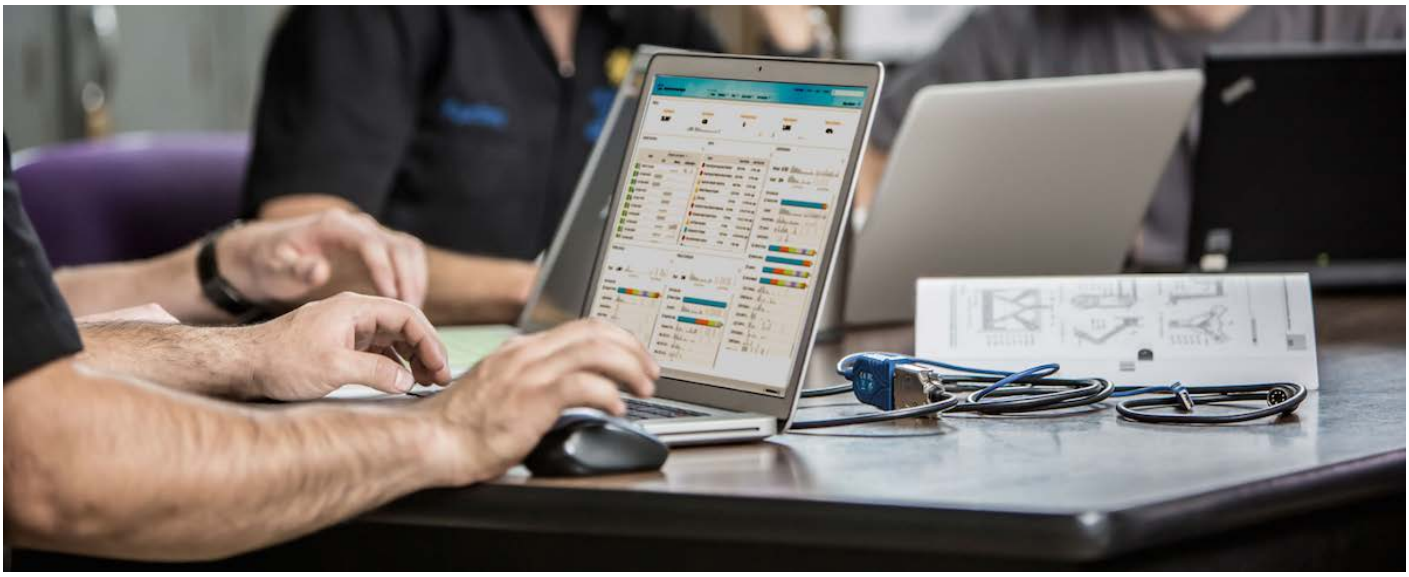


Cisco pxGrid로 인증서 배포

CA(Certificate Authority) 서명 ISE pxGrid 노드 및 CA 서명 pxGrid 클라이언트

목차

이 문서 정보

이 문서에서는 CA(Certificate Authority)를 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 아래의 Configure_and_Test_Integration_with_Cisco_pxGrid.pdf를 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 같이 두 가지의 다른 문서가 있습니다.

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

서론

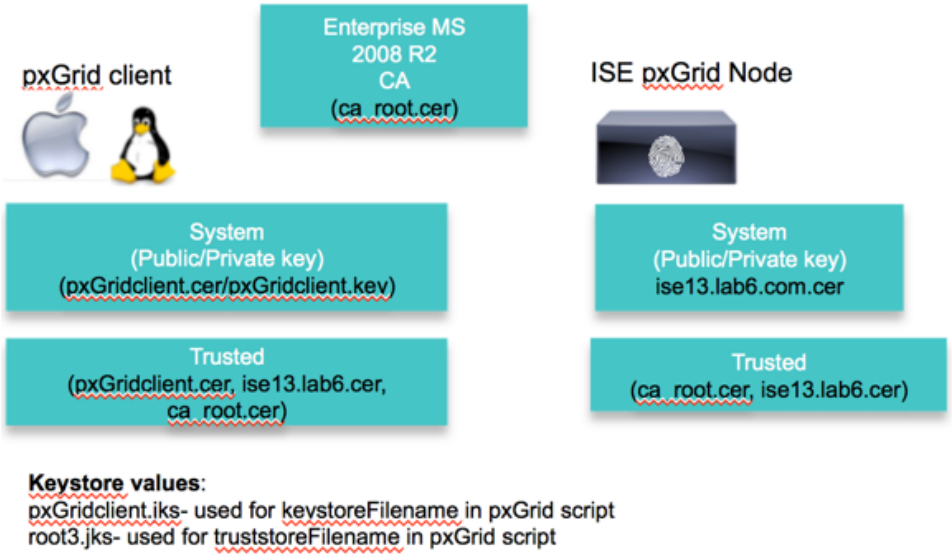
이 섹션에서는 ISE 독립형 구축 시 pxGrid 클라이언트 및 ISE pxGrid 노드의 CA(Certificate Authority) 서명 인증서 컨피그레이션에 대해 자세히 다룹니다. ISE pxGrid 노드 및 pxGrid 클라이언트는 Microsoft Enterprise CA 2008 R2 Authority에서 서명 인증서를 가져옵니다. 사용자 지정 pxGrid 템플릿은 클라이언트 인증(1.3.6.5.5.7.3.2) 및 서버 인증(1.3.6.1.5.5.7.3.1)에 모두 EKU(Enhanced Key Usage) ISO 정의 OID (object identifier)가 수반됩니다. ISE pxGrid 노드에서는 CA 루트 인증서를 신뢰할 수 있는 인증서 저장소에 다운로드하며, pxGrid 클라이언트에서는 루트 인증서를 신뢰할 수 있는 키 저장소에 다운로드합니다.

pxGrid 클라이언트가 ISE pxGrid 노드에 연결할 경우 두 공개 인증서 모두 올바른 pxGrid 연결을 위해 SASL(Simple Authentication and Security Layer)에 트러스트됩니다.

다음 다이어그램에는 정보의 인증서 플로우가 나와 있습니다.

인증서 컨피그레이션 예

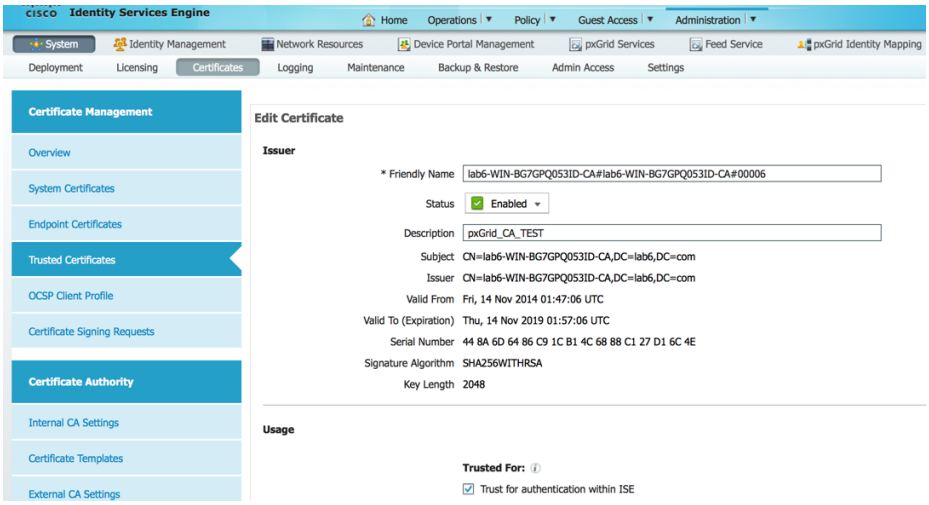
다음은 이 문서에 사용된 인증서의 예를 나타냅니다.



CA 서명 ISE pxGrid 노드 인증서 및 pxGrid 페르소나 컨피그레이션

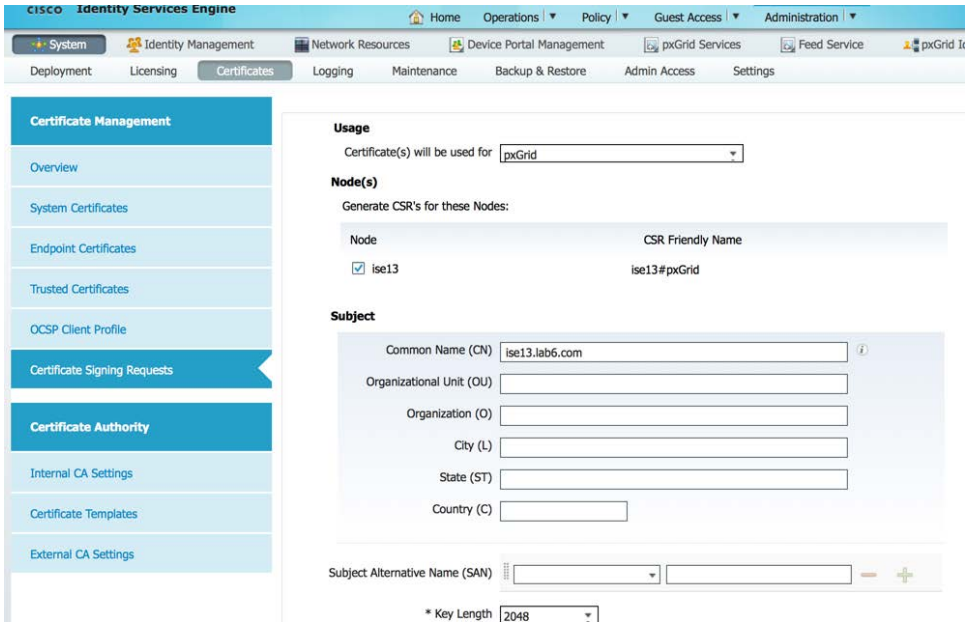
이 섹션에서는 CA 서명 ISE pxGrid 인증서 프로세스 및 CA 루트 인증서를 ISE 트러스트된 인증서 저장소에 가져오는 방법을 자세히 살펴봅니다. CA 인증서가 트러스트된 저장소에 업로드되고 ISE 인증서가 CSR 요청에 바인딩되면, ISE 노드의 pxGrid 페르소나가 활성화될 수 있으며 Primary로 변경됩니다.

1단계 CA 루트 인증서를 다운로드하고 ISE 트러스트된 인증서 저장소에 업로드한 다음 ISE 커뮤니케이션에 트러스트 활성화를 선택합니다.



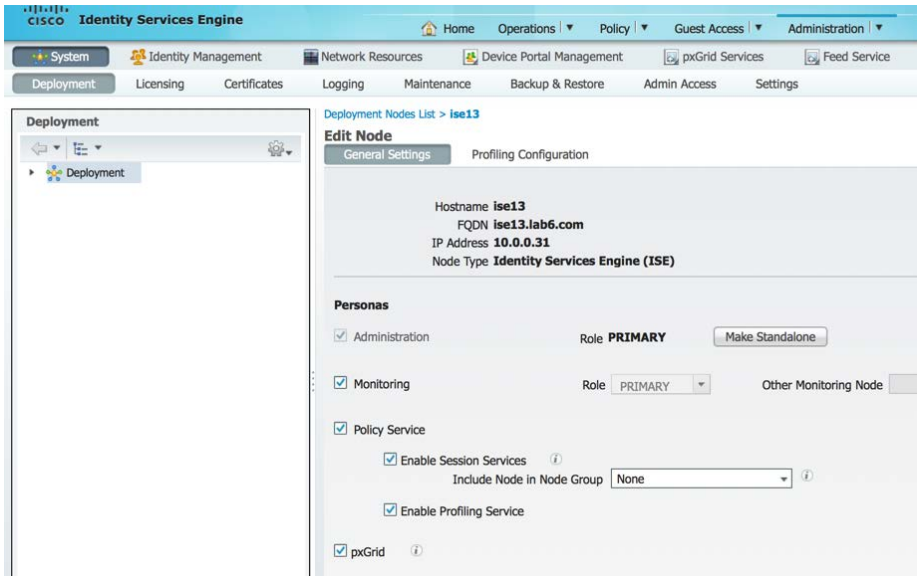
2단계 pxGrid 사용을 위해 CA 권한에 대한 ISE CSR 요청을 생성합니다. 사용자 인증서 요청을 지원하려면 pxGrid 템플릿은 클라이언트 인증 및 서버 인증 모두에 대해 EKU를 구성해야 합니다.

Administration->System->Certificates->Certificate Signing Requests를 차례로 누른 다음 ISE FQDN으로 CSR을 생성하고 pxGrid 사용을 설정합니다.

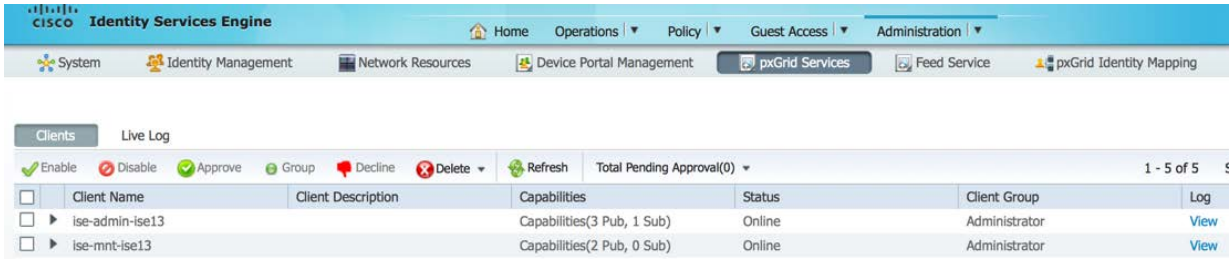


3단계 CA에서 인증서를 다운로드하고 인증서를 바인딩합니다.
Administration->Certificates->Certificate Signing Requests->Bind certificate

4단계 ISE에서 pxGrid를 활성화합니다.
Administration->System->Deployment를 차례로 누른 다음 pxGrid를 활성화하고 Primary로 변경합니다.



5단계 시작된 pxGrid 서비스가 표시되어야 합니다.
Administration->pxGrid Services



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

pxGrid 클라이언트 인증서 컨피그레이션

이 섹션에서는 pxGrid 클라이언트 CA 서명 인증서 프로세스를 단계별로 살펴봅니다. 퍼블릭 키/프라이빗 쌍이 생성되면 프라이빗 키인 pxGridClient.key에서 PKCS12 파일이 생성됩니다.

PKCS12 파일은 ID 키 저장소인 pxGridClient.jks로 가져오기됩니다. 이 ID 키 저장소 및 관련 비밀번호는 pxGrid 스크립트의 keystoreFilename 및 keystorePassword 역할을 합니다. pxGrid 클라이언트 인증서인 pxGridClient.cer도 키 저장소에 추가됩니다.

ISE ID 인증서인 isemnt는 모두 벌크 다운로드 세션에 필요하며, CA 루트 인증서는 트러스트 키 저장소인 root3.jks에 추가됩니다. 이 트러스트 키 저장소 및 관련 비밀번호는 pxGrid 스크립트의 truststoreFilename 및 truststorePassword 역할을 합니다.

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

```
openssl genrsa -out pxGridClient.key 4096

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

2단계 CA 권한에 대한 CSR 요청(예: pxGridClient.csr)을 생성합니다. 챌린지 비밀번호(예: cisco123)를 제공합니다.

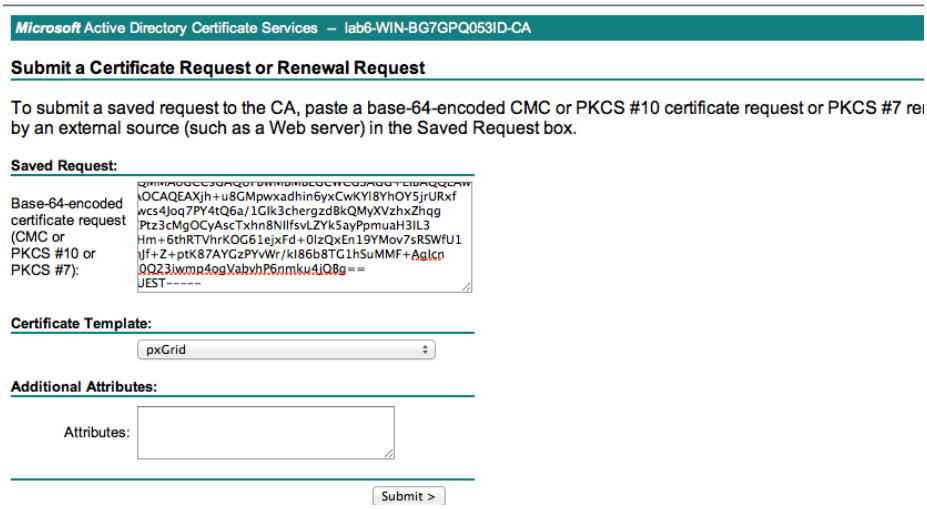
```
openssl req -new -key pxGridClient.key -out pxGridClient.csr

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
```

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

3단계 CA 인증기관은 클라이언트 인증 및 서버 인증을 위한 EKU가 모두 포함된 pxGrid 템플릿을 사용하여 사용자 인증서를 지원해야 합니다.

참고: Windows 2003의 CA 템플릿이 선택되었으므로, 이는 드롭다운 목록에 표시됩니다. 사용자 템플릿은 클라이언트 및 서버 인증을 위한 EKU를 모두 포함하여 중복되었습니다.



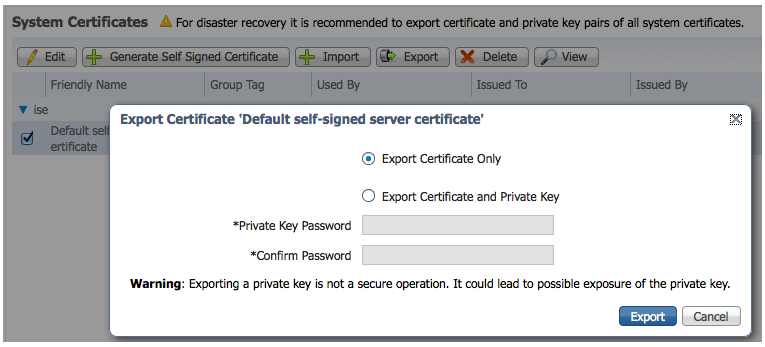
4단계 pxGridClient 인증서(예: pxGridClient.cer)의 프라이빗 키에서 pxGrid 클라이언트인.pkcs12 파일(pxGridClient.p12)을 생성합니다. 이 파일은 키 저장소 관리에 사용되며 확장자가 .p12인 임의의 파일 이름일 수 있습니다. CA 루트 파일(예: ca_root)을 포함합니다.

```
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
```

5단계 pxGrid 클라이언트 ID 키 저장소(예: pxGridClient.jks)를 생성합니다. 이는 pxGrid 클라이언트 ID 키 저장소가 되며, 확장자가.jks인 임의의 파일 이름일 수 있습니다. 또한 pxGrid 스크립트 예에서 keystoreFilename 및 관련 keystorePassword 역할을 합니다.

```
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
```

6단계 퍼블릭 ISE ID 인증서만 pxGrid 클라이언트로 내보내며, 이는.pem 형식으로 이루어집니다. 확장자가.pem인 파일의 이름을 더 읽기 쉽게 변경할 수 있습니다. 이 예에서 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 신뢰 키 저장소(예: root3.jks)에 추가하면 이는 신뢰할 수 있는 키 저장소가 됩니다. 확장자가.jks인 임의의 파일 이름일 수 있습니다. 이는 pxGrid 스크립트에 사용된 truststoreFilename 및 truststorePassword가 됩니다.

```
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
```

9단계 pxGrid 클라이언트 인증서를 ID 키 저장소로 가져옵니다.

```
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.

10단계 CA 루트 인증서를 트러스트된 키 저장소에 추가합니다. CA 루트 인증서도 트러스트되어야 합니다.

```
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
```

```
#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
```

11단계 ID 키 저장소(pxGridClient.jks) 및 트러스트 키 저장소(root3.jks)를../samples/bin/.. 폴더에 복사합니다.

pxGrid 클라이언트 및 ISE pxGrid 노드 테스트

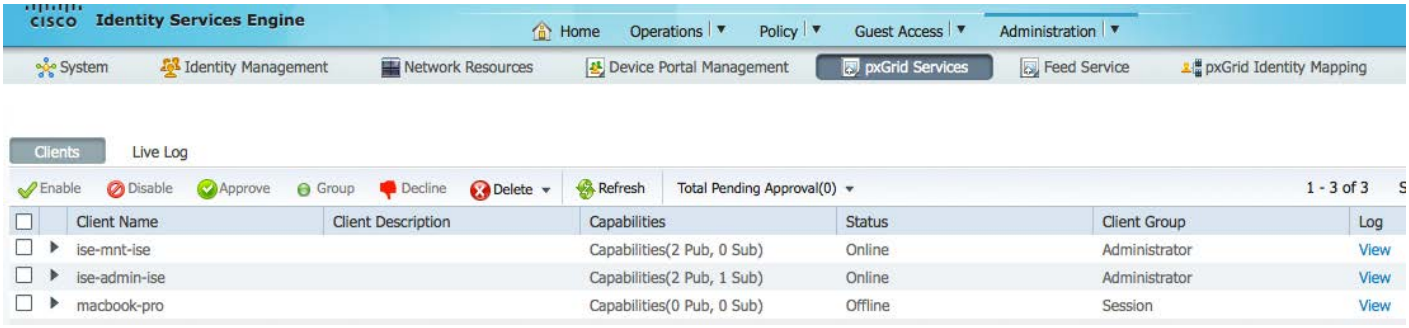
pxGrid 스크립트인 register.sh 및 session download.sh는 pxGrid 클라이언트 연결 및 pxGrid 등록을 확인하기 위해 실행됩니다. 세션 다운로드는 ISE MNT 인증서 및 pxGrid 클라이언트에 문제가 없는지 확인합니다.

1단계 pxGrid 클라이언트 등록

```
./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
```

참고: "Account enabled"는 pxGrid 관리자에 의해 어카운트가 활성화되었음을 의미합니다.

pxGrid 클라이언트가 pxGrid 컨트롤러에 등록되었는지 확인합니다.



2단계 세션 다운로드 실행

```
./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
```

키 저장소 항목 보기

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

1단계 트러스트 키 저장소인 root3.jks를 확인합니다.

```
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: 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                                        ....
]
]



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


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$
```

2단계 ID 키 저장소인 pxGridclient.jks를 확인합니다.

```
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,
]
]



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

문제 해결

이 섹션에서는 트러블슈팅에 대한 정보를 제공합니다.

- pxGrid 클라이언트 호스트 이름 및 ISE pxGrid 노드가 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 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
```

- ISE 서비스 다시 시작

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

3단계 유사한 오류 메시지가 표시되면 루트 인증서를 truststoreFilename 키 저장소(이 예에서는 root3.jks)에 추가해야 합니다.

```
./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
```