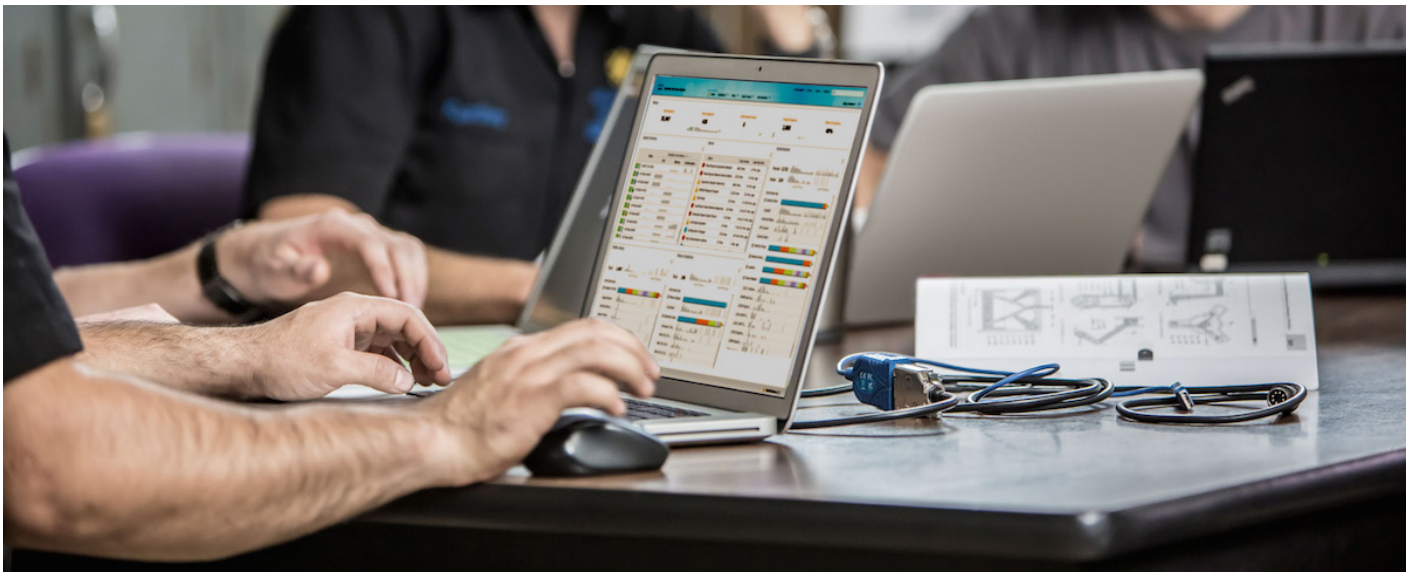


使用 Cisco pxGrid 部署证书

证书颁发机构 (CA) 签名的 pxGrid 客户端和自签名的 ISE pxGrid 节点证书

目录

关于本文档

本文档说明使用 CA 机构签名的证书和适用于 ISE pxGrid 节点的 ISE 中 ISE 自签名证书，配置 pxGrid 客户端所需执行的配置步骤。本文档面向部署 Cisco pxGrid 的思科现场工程师、技术营销工程师、合作伙伴和客户。读者需要熟悉 pxGrid。如果读者不熟悉 pxGrid，请参阅 Configure_and_Test_Integration_with_Cisco_pxGrid.pdf：http://www.cisco.com/c/dam/en/us/td/docs/security/ise/how_to/HowTo-84-Configure_and_Test_Integration_with_Cisco_pxGrid.pdf

pxGrid sdk 可从思科客户团队获取。

本文档假设已安装思科身份服务引擎 (ISE) 1.3。对于 pxGrid 客户端，可以使用运行 OSX 10.8.5 的 MAC，或者 Linux 操作系统。此外，pxGrid 客户端需要具备 Oracle Java Development Kit 7 或 8。

在《*使用证书部署 pxGrid*》系列中还有两个文档：

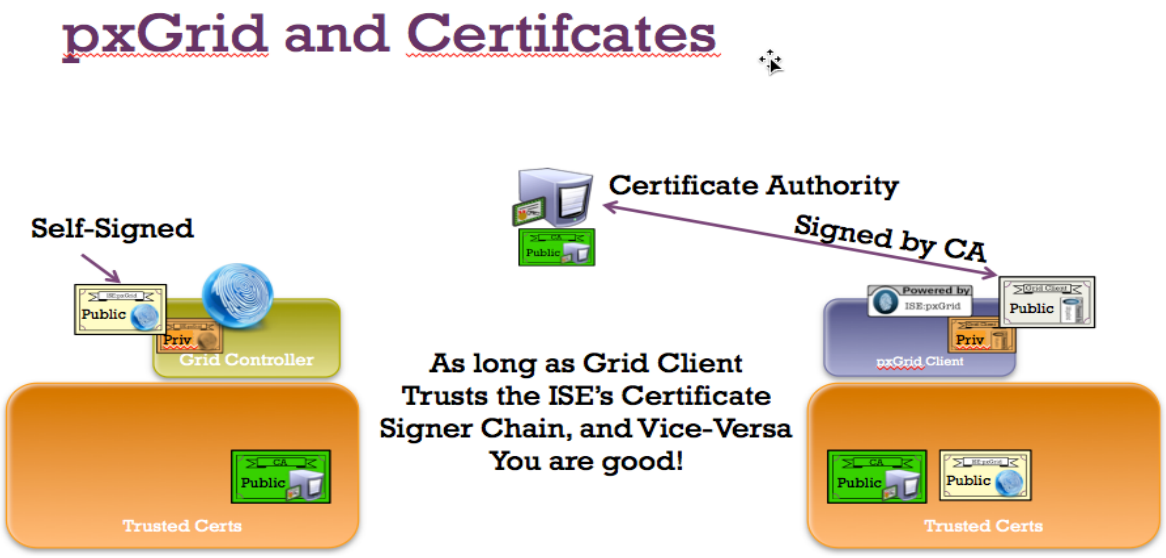
- 将 CA 签名的证书与 ISE pxGrid 节点和 pxGrid 客户端配合使用
- 将自签名证书与 ISE pxGrid 节点和 ISE pxGrid 客户端配合使用

简介

本节详细说明在 ISE 独立部署中为 pxGrid 客户端和 ISE pxGrid 节点配置 CA 签名证书的过程。在这种情况下，pxGrid 客户端可能包含 Entrust 等公共 CA 签名的证书。请注意，必须创建具有同时用于客户端身份验证 (1.3.6.5.5.7.3.2) 和服务器身份验证 (1.3.6.1.5.5.7.3.1) 的增强型密钥使用 (EKU) ISO 定义的对象标识符 (OID) 的自定义 pxGrid 模板。ISE pxGrid 节点包含 ISE 受信任证书库中的自签名 ISE 身份证书。Microsoft Enterprise CA 2008 R2 将用作签署 pxGrid 客户端证书的 CA 机构。Microsoft CA 提供的 CA root 证书将添加至 ISE 受信任证书库中。ISE 公用证书将添加至 pxGrid 客户端的密钥库。

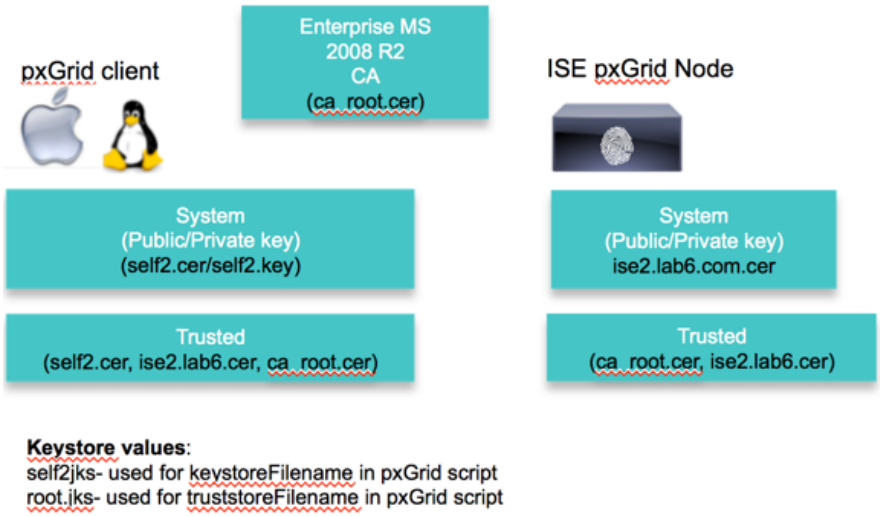
当 pxGrid 客户端连接到 ISE pxGrid 节点时，为使 pxGrid 连接成功，两个公共证书对于简单身份验证和安全层 (SASL) 而言都将是受信任的。

下图显示证书信息流。



证书配置示例

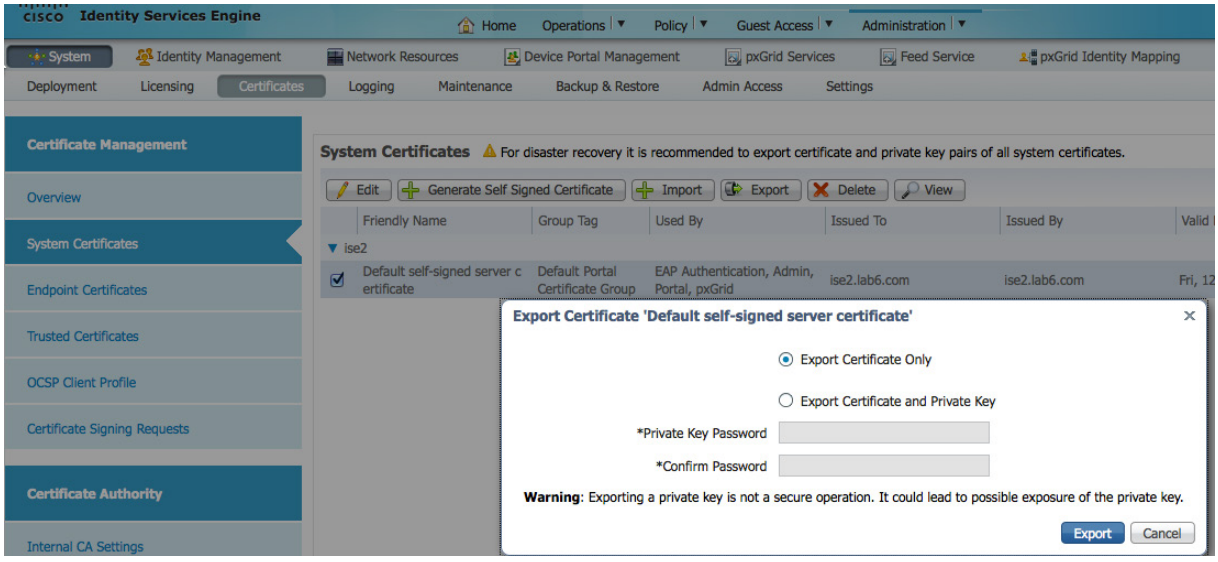
下图显示本文档中使用的证书示例。



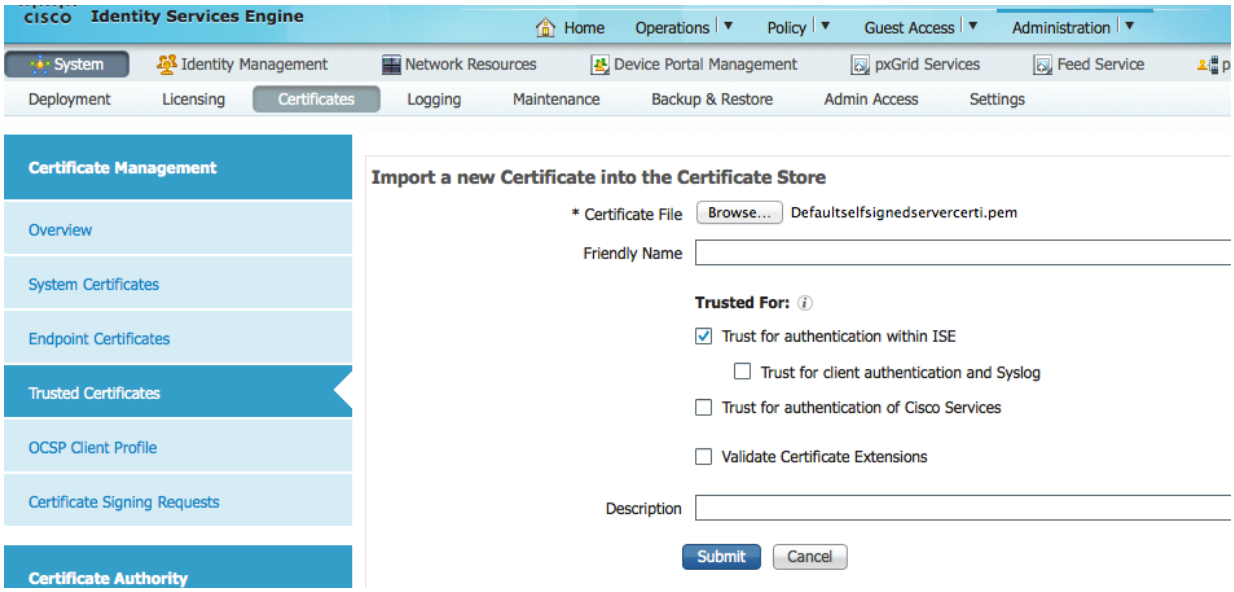
自签名 ISE pxGrid 节点证书和 pxGrid 角色配置

此处，我们将 ISE 自签名证书导入到 ISE 受信任证书库中。将 ISE 身份证书导入到受信任证书库中后，可以在 ISE 节点上启用 pxGrid 角色，并使其成为主节点。发布的节点将显示在 pxGrid Services View 中。

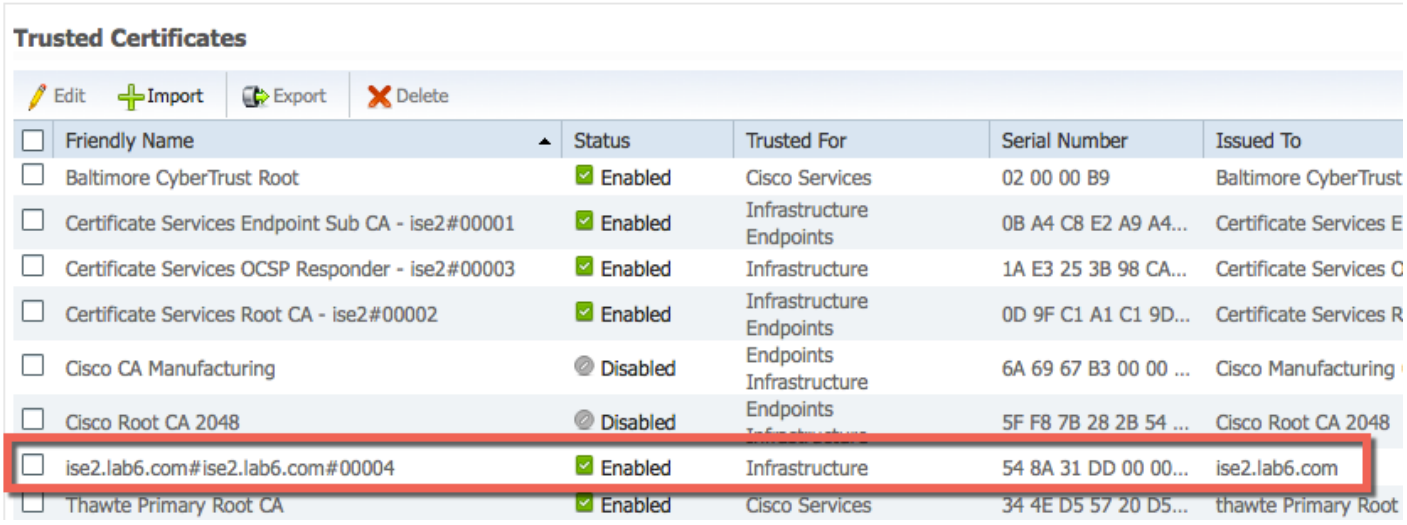
步骤 1 导出自签名 ISE 身份证书并另存为 .pem 文件。
Administration -> System -> Certificates -> select ISE identity cert -> Export（仅公钥）。



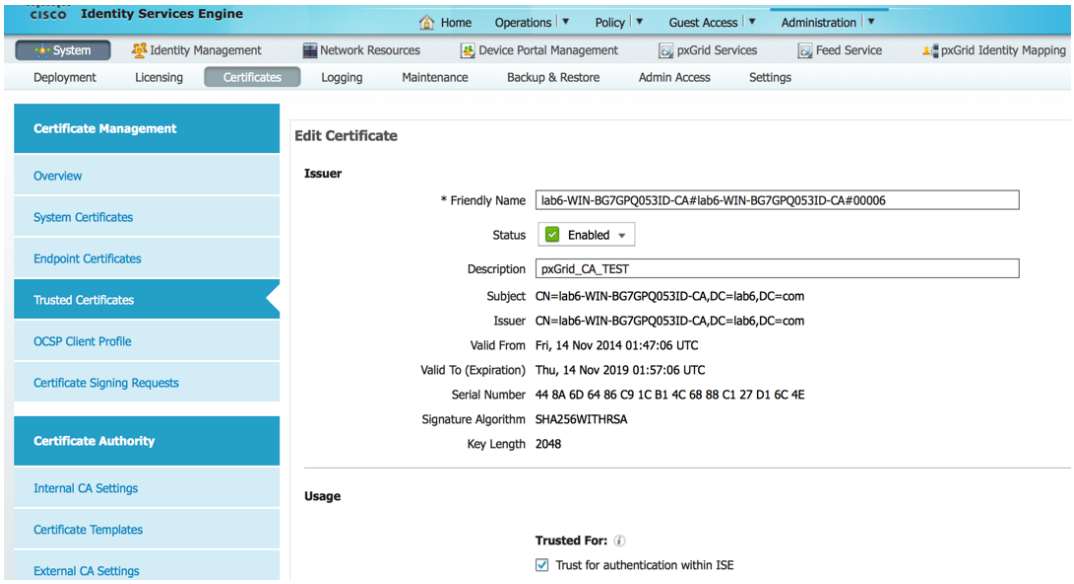
步骤 2 将已保存的 ISE .pem 文件导入到 ISE 受信任证书库中。
Administration -> System -> Certificates -> Trusted Certificates -> Browse and upload file -> Submit。



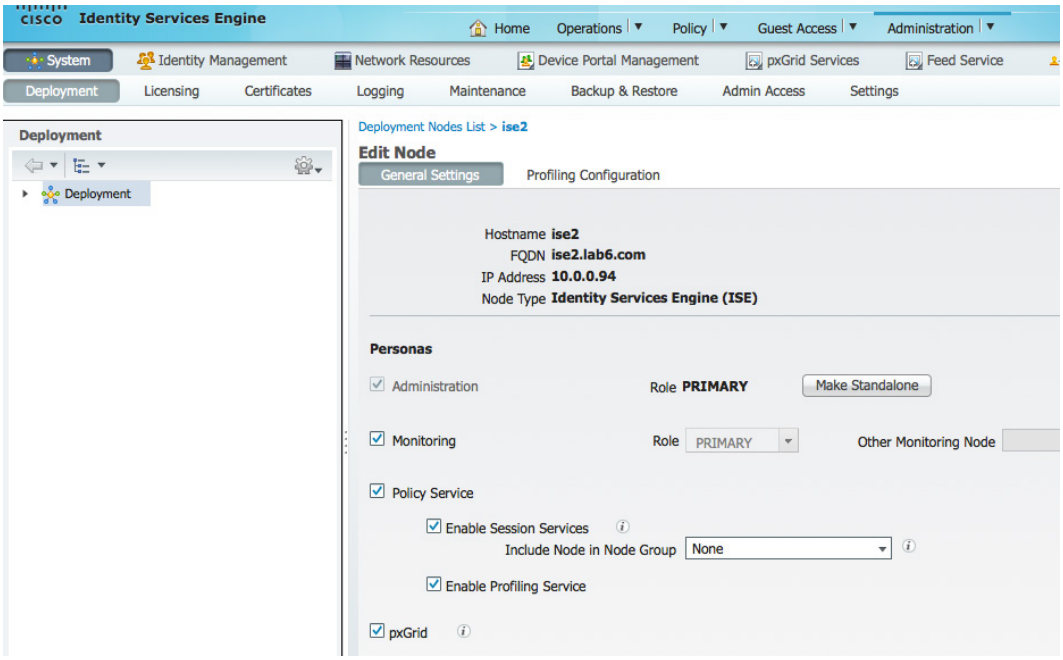
您将看到已导入的 ISE 受信任证书。



步骤 3 下载 CA root 证书并将其上传至 ISE 受信任证书库中，然后启用 Trust for ISE communication。**Administration -> System -> Certificates -> Trusted Certificates -> Import & Upload the CA root certificate。**

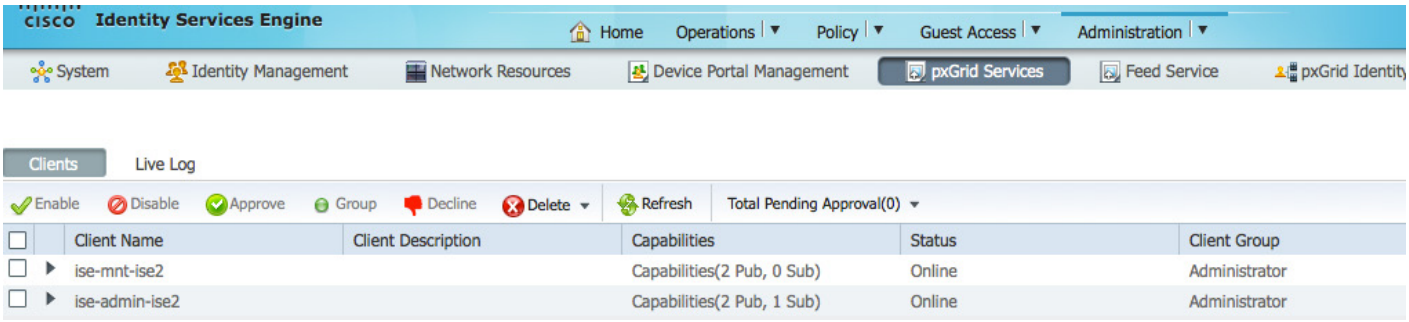


步骤 4 在 ISE 中启用 pxGrid 角色。**Administration -> System -> Deployment -> Enable pxGrid -> Change role to Primary -> Save。**



注：无需将角色改为主用。

步骤 5　验证发布的服务是否已启动。
Administration -> pxGrid Services。



Note：在 ISE 发布节点出现之前，可能会有延迟。在启用 pxGrid 角色之前，必须安装证书。

pxGrid 客户端证书配置

本节逐步介绍 pxGrid 客户端自签名证书的生成过程。生成证书公钥/私钥对之后，系统将根据私钥 self2.key 创建 PKCS12 文件。

该 PKCS12 文件将导入到身份密钥库 self1.jks 中。此身份密钥库和关联的密码将用作 pxGrid 脚本中的 keystoreFilename 和 keystorePassword。pxGrid 客户端证书 self2.cer 也将被添加至身份密钥库。

批量会话下载所需的 ISE 身份证书 isemnt 和 CA root 证书都将添加至信任密钥库 root.jks 中。此信任密钥库和关联的密码将用作 pxGrid 脚本中的 truststoreFilename 和 truststorePassword。

步骤 1　为 pxGrid 客户端生成私钥（例如 self2.key）。

```
openssl genrsa -out self2.key 4096
Generating RSA private key, 4096 bit long modulus
........++
.....................................................................................................................
..............++
e is 65537 (0x10001)
```

步骤 2　生成需要向 CA 机构提出的 CSR（例如 self2.csr）请求。提供质询密码（例如 cisco123）。

```
openssl req -new -key self2.key -out self2.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) []:
```

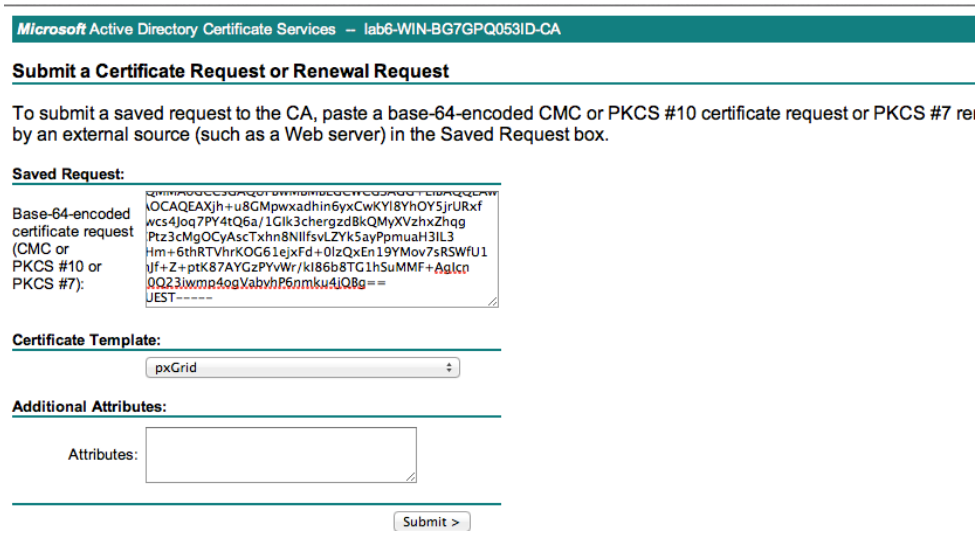
```
Common Name (e.g. server FQDN or YOUR name) []:
Email Address []:

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

注：在本文档各处使用相同的密码可便于维护，并减少错误。

步骤 3 CA 机构必须使用包含增强型密钥使用 (EKU) ISO 定义的对象标识符 (OID) 的自定义模板（例如 pxGrid）来为用户证书提供服务，其中一个对象标识符用于客户端身份验证，另一个对象标识符用于服务器身份验证。

注：已在 CA 机构中创建 pxGrid 模板。这是一个重复的用户模板，采用 Windows 2003 格式，显示于 Certificate Template 下拉列表中。EKU 客户端身份验证和服务器身份验证都已添加至模板中。



步骤 4 根据 pxGrid 客户端证书（例如 self2.cer）中的私钥创建一个 pxGrid 客户端 .pkcs12 文件（例如 self2.p12）。此文件将用于密钥库管理。其中包括 CA root 文件（例如 ca_root.cer）。

```
openssl pkcs12 -export -out self2.p12 -inkey self2.key -in self2.cer -chain -CAfile ca_root.cer

Enter Export Password: cisco123
Verifying - Enter Export Password: cisco123
Johns-MacBook-Pro:pxGridsdk jeppich$
```

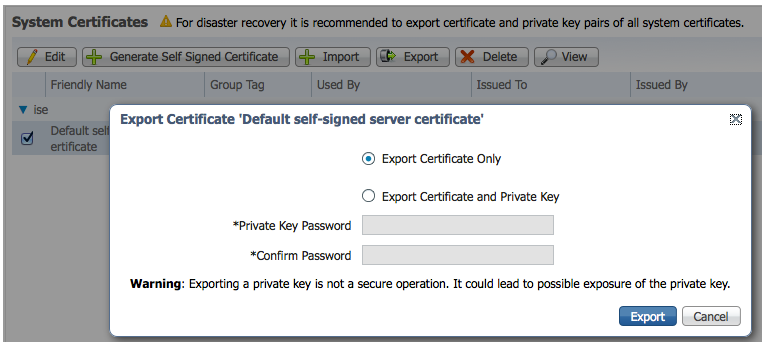
注：cisco123 是本文档中使用的密码

步骤 5 创建 pxGrid 客户端身份密钥库（例如 self2.jks），它将用作 pxGrid 脚本示例的 keystoreFilename 和关联 keystorePassword 。

```
keytool -importkeystore -srckeystore self2.p12 -destkeystore self2.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
```

步骤 6 仅将公共 ISE 身份证书导出到 pxGrid 客户端中，请注意导出文件将采用 .pem 格式。您可以重命名扩展名为 .pem 的文件，使其更易于读取。在本示例中，该文件已重命名为 isemnt.pem。



步骤 7 将 .pem 文件转换为 .der 格式。

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

步骤 8 将 ISE 身份证书添加至信任密钥库（例如 root.jks）中，它将成为 pxGrid 脚本中使用的 truststoreFilename 和关联的 truststorePassword。

```
keytool -import -alias mnt -keystore root.jks -file isemnt.der

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

Extensions:

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

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

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

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

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

Trust this certificate? [no]: yes
Certificate was added to keystore
Johns-MacBook-Pro:pxGridsdk jeppich$
```

步骤 9　将 pxGrid 客户端证书导入到身份密钥库中。

```
keytool -import -alias pxGridclient -keystore self2.jks -file self2.cer

Enter keystore password: cisco123
Certificate already exists in keystore under alias <1>
Do you still want to add it? [no]: no
Certificate was not added to keystroke
```

步骤 10　将 CA Root 证书添加至信任密钥库中。两个证书都需要驻留在信任密钥库中。

```
keytool -import -alias root -keystore root.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 17:47:06 PST 2014 until: Wed Nov 13 17:57:06 PST 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
```

步骤 11　将身份密钥库（例如 self2.jks）和信任密钥库（例如 root.jks）复制至 …/samples/bin 文件夹。

测试 pxGrid 客户端和 ISE pxGrid 节点

系统将运行样本 pxGrid 脚本 register.sh 和 session_download.sh 来确保 pxGrid 客户端连接和 pxGrid 注册。会话下载将确保 ISE MNT 证书和 pxGrid 客户端没有问题。

步骤 1　注册 pxGrid 客户端。

```
./register.sh -keystoreFilename self2.jks -keystorePassword cisco123 -truststoreFilename root.jks -
truststorePassword cisco123 -group Session -description test -hostname 10.0.0.96 -username JohnMACbook

------- properties -------
version=1.0.0
hostnames=10.0.0.96
username=JohnMACbook
descriptipon=test
keystoreFilename=self2.jks
keystorePassword=cisco123
truststoreFilename=root.jks
truststorePassword=cisco123
--------------------------
registering...
connecting...
connected.
done registering.
connection closed
```

步骤 2 运行会话下载。

```
./session_download.sh -keystoreFilename self2.jks -keystorePassword cisco123 -truststoreFilename root.jks -
truststorePassword cisco123 -hostname 10.0.0.96 -username JohnMACbook

------- properties -------
version=1.0.0
hostnames=10.0.0.96
username=JohnMACbook
keystoreFilename=self2.jks
keystorePassword=cisco123
truststoreFilename=root.jks
truststorePassword=cisco123
filter=null
start=null
end=null
--------------------------
connecting...
connected.
starting at Wed Dec 10 09:55:36 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 09:55:36 PST 2014

-------------------------------------------------
downloaded 1 sessions in 100 milliseconds
-------------------------------------------------

connection closed
```

查看密钥库条目

通过查看密钥库条目，可以查看身份和信任密钥库的受信任证书条目。

```
keytool -list -v -keystore self2.jks
Enter keystore password:

Keystore type: JKS
Keystore provider: SUN

Your keystore contains 2 entries

Alias name: isecert
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.
]
]



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


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: 6105dce600000000000a
Valid from: Wed Dec 10 09:01:44 PST 2014 until: Sat Dec 10 09:11:44 PST 2016
Certificate fingerprints:
         MD5: 76:3E:43:48:A7:FD:2C:5B:A3:FD:76:3F:6E:DF:2D:B8
         SHA1: A9:E4:66:D9:34:C6:62:67:2B:C0:AF:E1:68:83:EA:36:3D:2A:23:CC
         SHA256:
0E:D8:04:30:39:3E:0B:06:D5:3E:29:94:ED:C7:76:7A:5E:27:1C:14:CF:CD:1E:4D:10:AF:22:A7:54:E5:52:7B
         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: 36 E2 1A 09 D1 51 72 4D  C3 6A 18 C1 C4 EB AE B5 6....QrM.j......
0010: E4 48 39 4E                                       .H9N
]
]

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 17:47:06 PST 2014 until: Wed Nov 13 17:57:06 PST 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,
]
]



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

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

Keystore type: JKS
Keystore provider: SUN

Your keystore contains 2 entries

Alias name: root
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 17:47:06 PST 2014 until: Wed Nov 13 17:57:06 PST 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: mnt
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.
]
]



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

故障排除

本节介绍一些故障排除提示：

- 通过验证 pxGrid 客户端主机名和 ISE pxGrid 是否可通过 DNS 进行解析，避免出现 pxGrid 脚本错误消息。
- 如果信任库有更改，并且收到类似的错误消息，请从 ISE VM 停止并重新启动 ISE 应用。

```
./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
```

- 重新启动 ISE 服务。

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

- 验证 pxGrid 进程是否正在初始化。

```
sh application status ise
```

- 如果您看到类似的错误消息，则需要将 root 证书添加至 truststoreFilename 密钥库中，在本示例中例如添加至 root3.jks。

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

------- properties -------
version=1.0.0
hostnames=10.0.0.96
username=Macbook_PRO
descriptipon=MACBOOK
keystoreFilename=pxGridClient.jks
keystorePassword=cisco123
truststoreFilename=root3.jks
truststorePassword=cisco123
--------------------------
registering...
connecting...
javax.net.ssl.SSLHandshakeException: java.security.cert.CertificateException: root certificate not trusted of
[ise.lab6.com]
        at sun.security.ssl.Alerts.getSSLException(Alerts.java:192)
        at sun.security.ssl.SSLSocketImpl.fatal(SSLSocketImpl.java:1917)
        at sun.security.ssl.Handshaker.fatalSE(Handshaker.java:301)
        at sun.security.ssl.Handshaker.fatalSE(Handshaker.java:295)
        at sun.security.ssl.ClientHandshaker.serverCertificate(ClientHandshaker.java:1471)
        at sun.security.ssl.ClientHandshaker.processMessage(ClientHandshaker.java:212)
        at sun.security.ssl.Handshaker.processLoop(Handshaker.java:936)
        at sun.security.ssl.Handshaker.process_record(Handshaker.java:871)
        at sun.security.ssl.SSLSocketImpl.readRecord(SSLSocketImpl.java:1043)
        at sun.security.ssl.SSLSocketImpl.performInitialHandshake(SSLSocketImpl.java:1343)
        at sun.security.ssl.SSLSocketImpl.startHandshake(SSLSocketImpl.java:1371)
        at sun.security.ssl.SSLSocketImpl.startHandshake(SSLSocketImpl.java:1355)
        at org.jivesoftware.smack.XMPPConnection.proceedTLSReceived(XMPPConnection.java:806)
        at org.jivesoftware.smack.PacketReader.parsePackets(PacketReader.java:267)
        at org.jivesoftware.smack.PacketReader.access$000(PacketReader.java:43)
        at org.jivesoftware.smack.PacketReader$1.run(PacketReader.java:70)
Caused by: java.security.cert.CertificateException: root certificate not trusted of [ise.lab6.com]
        at org.jivesoftware.smack.ServerTrustManager.checkServerTrusted(ServerTrustManager.java:144)
        at sun.security.ssl.AbstractTrustManagerWrapper.checkServerTrusted(SSLContextImpl.java:865)
        at sun.security.ssl.ClientHandshaker.serverCertificate(ClientHandshaker.java:1453)
        ... 11 more
```

- 如果您看到以下错误消息，请确保 pxGrid 客户端和 ISE pxGrid FQDN 名称可通过 DNS 解析。

```
./session_download.sh -keystoreFilename jeppich.jks -keystorePassword cisco123 -truststoreFilename
trust007.jks -truststorePassword cisco123 -hostname 10.0.0.96 -username mac2
------- properties -------
version=1.0.0
hostnames=10.0.0.96
username=mac2
keystoreFilename=jeppich.jks
keystorePassword=cisco123
truststoreFilename=trust007.jks
truststorePassword=cisco123
filter=null
start=null
end=null
--------------------------
connecting...
connected.
20:18:07.181 [main] WARN o.a.cxf.phase.PhaseInterceptorChain - Interceptor for
{https://ise.lab6.com/pxgrid/mnt/sd}WebClient has thrown exception, unwinding now
org.apache.cxf.interceptor.Fault: Could not send Message.
        at
org.apache.cxf.interceptor.MessageSenderInterceptor$MessageSenderEndingInterceptor.handleMessage(MessageSende
rInterceptor.java:64) ~[cxf-api-2.7.3.jar:2.7.3]
        at org.apache.cxf.phase.PhaseInterceptorChain.doIntercept(PhaseInterceptorChain.java:271) ~[cxf-api-
2.7.3.jar:2.7.3]
```

```
        at org.apache.cxf.jaxrs.client.AbstractClient.doRunInterceptorChain(AbstractClient.java:581) [cxf-rt-
frontend-jaxrs-2.7.3.jar:2.7.3]
        at org.apache.cxf.jaxrs.client.WebClient.doChainedInvocation(WebClient.java:904) [cxf-rt-frontend-
jaxrs-2.7.3.jar:2.7.3]
        at org.apache.cxf.jaxrs.client.WebClient.doInvoke(WebClient.java:772) [cxf-rt-frontend-jaxrs-
2.7.3.jar:2.7.3]
        at org.apache.cxf.jaxrs.client.WebClient.doInvoke(WebClient.java:759) [cxf-rt-frontend-jaxrs-
2.7.3.jar:2.7.3]
        at org.apache.cxf.jaxrs.client.WebClient.invoke(WebClient.java:355) [cxf-rt-frontend-jaxrs-
2.7.3.jar:2.7.3]
        at org.apache.cxf.jaxrs.client.WebClient.post(WebClient.java:381) [cxf-rt-frontend-jaxrs-
2.7.3.jar:2.7.3]
        at com.cisco.pxgrid.stub.identity.impl.SessionIteratorImpl.open(SessionIteratorImpl.java:128)
[pxgrid-identity-client-stub-1.0.0.jar:1.0.0]
        at com.cisco.pxgrid.samples.ise.SessionDownload.main(SessionDownload.java:132) [pxgrid-sdk-
1.0.0.jar:1.0.0]
Caused by: java.net.UnknownHostException: UnknownHostException invoking
https://ise.lab6.com/pxgrid/mnt/sd/getSessionListByTime: ise.lab6.com
        at sun.reflect.NativeConstructorAccessorImpl.newInstance0(Native Method) ~[na:1.8.0_25]
        at sun.reflect.NativeConstructorAccessorImpl.newInstance(NativeConstructorAccessorImpl.java:62)
~[na:1.8.0_25]
        at
sun.reflect.DelegatingConstructorAccessorImpl.newInstance(DelegatingConstructorAccessorImpl.java:45)
~[na:1.8.0_25]
        at java.lang.reflect.Constructor.newInstance(Constructor.java:408) ~[na:1.8.0_25]
        at org.apache.cxf.transport.http.HTTPConduit$WrappedOutputStream.mapException(HTTPConduit.java:1338)
~[cxf-rt-transports-http-2.7.3.jar:2.7.3]
        at org.apache.cxf.transport.http.HTTPConduit$WrappedOutputStream.close(HTTPConduit.java:1322) ~[cxf-
rt-transports-http-2.7.3.jar:2.7.3]
        at org.apache.cxf.transport.AbstractConduit.close(AbstractConduit.java:56) ~[cxf-api-2.7.3.jar:2.7.3]
        at org.apache.cxf.transport.http.HTTPConduit.close(HTTPConduit.java:622) ~[cxf-rt-transports-http-
2.7.3.jar:2.7.3]
        at
org.apache.cxf.interceptor.MessageSenderInterceptor$MessageSenderEndingInterceptor.handleMessage(MessageSende
rInterceptor.java:62) ~[cxf-api-2.7.3.jar:2.7.3]
        ... 9 common frames omitted
Caused by: java.net.UnknownHostException: ise.lab6.com
        at java.net.AbstractPlainSocketImpl.connect(AbstractPlainSocketImpl.java:184) ~[na:1.8.0_25]
        at java.net.SocksSocketImpl.connect(SocksSocketImpl.java:392) ~[na:1.8.0_25]
        at java.net.Socket.connect(Socket.java:589) ~[na:1.8.0_25]
        at sun.security.ssl.SSLSocketImpl.connect(SSLSocketImpl.java:649) ~[na:1.8.0_25]
        at sun.net.NetworkClient.doConnect(NetworkClient.java:175) ~[na:1.8.0_25]
        at sun.net.www.http.HttpClient.openServer(HttpClient.java:432) ~[na:1.8.0_25]
        at sun.net.www.http.HttpClient.openServer(HttpClient.java:527) ~[na:1.8.0_25]
        at sun.net.www.protocol.https.HttpsClient.<init>(HttpsClient.java:275) ~[na:1.8.0_25]
        at sun.net.www.protocol.https.HttpsClient.New(HttpsClient.java:371) ~[na:1.8.0_25]
        at
sun.net.www.protocol.https.AbstractDelegateHttpsURLConnection.getNewHttpClient(AbstractDelegateHttpsURLConnec
tion.java:191) ~[na:1.8.0_25]
        at sun.net.www.protocol.http.HttpURLConnection.plainConnect0(HttpURLConnection.java:1103)
~[na:1.8.0_25]
        at sun.net.www.protocol.http.HttpURLConnection.plainConnect(HttpURLConnection.java:997)
~[na:1.8.0_25]
        at
sun.net.www.protocol.https.AbstractDelegateHttpsURLConnection.connect(AbstractDelegateHttpsURLConnection.java
:177) ~[na:1.8.0_25]
        at sun.net.www.protocol.http.HttpURLConnection.getOutputStream0(HttpURLConnection.java:1281)
~[na:1.8.0_25]
        at sun.net.www.protocol.http.HttpURLConnection.getOutputStream(HttpURLConnection.java:1256)
~[na:1.8.0_25]
        at sun.net.www.protocol.https.HttpsURLConnectionImpl.getOutputStream(HttpsURLConnectionImpl.java:250)
~[na:1.8.0_25]
        at
org.apache.cxf.transport.http.URLConnectionHTTPConduit$URLConnectionWrappedOutputStream.setupWrappedStream(UR
LConnectionHTTPConduit.java:170) ~[cxf-rt-transports-http-2.7.3.jar:2.7.3]
        at
org.apache.cxf.transport.http.HTTPConduit$WrappedOutputStream.handleHeadersTrustCaching(HTTPConduit.java:1282)
~[cxf-rt-transports-http-2.7.3.jar:2.7.3]
        at org.apache.cxf.transport.http.HTTPConduit$WrappedOutputStream.onFirstWrite(HTTPConduit.java:1233)
~[cxf-rt-transports-http-2.7.3.jar:2.7.3]
        at
org.apache.cxf.transport.http.URLConnectionHTTPConduit$URLConnectionWrappedOutputStream.onFirstWrite(URLConne
ctionHTTPConduit.java:183) ~[cxf-rt-transports-http-2.7.3.jar:2.7.3]
```

```
        at org.apache.cxf.io.AbstractWrappedOutputStream.write(AbstractWrappedOutputStream.java:47) ~[cxf-
api-2.7.3.jar:2.7.3]
        at org.apache.cxf.io.AbstractThresholdOutputStream.write(AbstractThresholdOutputStream.java:69)
~[cxf-api-2.7.3.jar:2.7.3]
        at org.apache.cxf.transport.http.HTTPConduit$WrappedOutputStream.close(HTTPConduit.java:1295) ~[cxf-
rt-transports-http-2.7.3.jar:2.7.3]
        ... 12 common frames omitted
20:18:07.185 [main] WARN c.c.p.s.i.impl.SessionIteratorImpl - unsuccessful attempt made to session directory
ise.lab6.com
javax.ws.rs.client.ClientException: javax.ws.rs.client.ClientException: org.apache.cxf.interceptor.Fault:
Could not send Message.
        at org.apache.cxf.jaxrs.client.WebClient.doResponse(WebClient.java:946) ~[cxf-rt-frontend-jaxrs-
2.7.3.jar:2.7.3]
        at org.apache.cxf.jaxrs.client.WebClient.doChainedInvocation(WebClient.java:905) ~[cxf-rt-frontend-
jaxrs-2.7.3.jar:2.7.3]
        at org.apache.cxf.jaxrs.client.WebClient.doInvoke(WebClient.java:772) ~[cxf-rt-frontend-jaxrs-
2.7.3.jar:2.7.3]
        at org.apache.cxf.jaxrs.client.WebClient.doInvoke(WebClient.java:759) ~[cxf-rt-frontend-jaxrs-
2.7.3.jar:2.7.3]
        at org.apache.cxf.jaxrs.client.WebClient.invoke(WebClient.java:355) ~[cxf-rt-frontend-jaxrs-
2.7.3.jar:2.7.3]
        at org.apache.cxf.jaxrs.client.WebClient.post(WebClient.java:381) ~[cxf-rt-frontend-jaxrs-
2.7.3.jar:2.7.3]
        at com.cisco.pxgrid.stub.identity.impl.SessionIteratorImpl.open(SessionIteratorImpl.java:128)
~[pxgrid-identity-client-stub-1.0.0.jar:1.0.0]
        at com.cisco.pxgrid.samples.ise.SessionDownload.main(SessionDownload.java:132) [pxgrid-sdk-
1.0.0.jar:1.0.0]
Caused by: javax.ws.rs.client.ClientException: org.apache.cxf.interceptor.Fault: Could not send Message.
        at org.apache.cxf.jaxrs.client.AbstractClient.checkClientException(AbstractClient.java:522) ~[cxf-rt-
frontend-jaxrs-2.7.3.jar:2.7.3]
        at org.apache.cxf.jaxrs.client.AbstractClient.preProcessResult(AbstractClient.java:508) ~[cxf-rt-
frontend-jaxrs-2.7.3.jar:2.7.3]
        at org.apache.cxf.jaxrs.client.WebClient.doResponse(WebClient.java:941) ~[cxf-rt-frontend-jaxrs-
2.7.3.jar:2.7.3]
        ... 7 common frames omitted
Caused by: org.apache.cxf.interceptor.Fault: Could not send Message.
        at
org.apache.cxf.interceptor.MessageSenderInterceptor$MessageSenderEndingInterceptor.handleMessage(MessageSende
rInterceptor.java:64) ~[cxf-api-2.7.3.jar:2.7.3]
        at org.apache.cxf.phase.PhaseInterceptorChain.doIntercept(PhaseInterceptorChain.java:271) ~[cxf-api-
2.7.3.jar:2.7.3]
        at org.apache.cxf.jaxrs.client.AbstractClient.doRunInterceptorChain(AbstractClient.java:581) ~[cxf-
rt-frontend-jaxrs-2.7.3.jar:2.7.3]
        at org.apache.cxf.jaxrs.client.WebClient.doChainedInvocation(WebClient.java:904) ~[cxf-rt-frontend-
jaxrs-2.7.3.jar:2.7.3]
        ... 6 common frames omitted
Caused by: java.net.UnknownHostException: UnknownHostException invoking
https://ise.lab6.com/pxgrid/mnt/sd/getSessionListByTime: ise.lab6.com
        at sun.reflect.NativeConstructorAccessorImpl.newInstance0(Native Method) ~[na:1.8.0_25]
        at sun.reflect.NativeConstructorAccessorImpl.newInstance(NativeConstructorAccessorImpl.java:62)
~[na:1.8.0_25]
        at
sun.reflect.DelegatingConstructorAccessorImpl.newInstance(DelegatingConstructorAccessorImpl.java:45)
~[na:1.8.0_25]
        at java.lang.reflect.Constructor.newInstance(Constructor.java:408) ~[na:1.8.0_25]
        at org.apache.cxf.transport.http.HTTPConduit$WrappedOutputStream.mapException(HTTPConduit.java:1338)
~[cxf-rt-transports-http-2.7.3.jar:2.7.3]
        at org.apache.cxf.transport.http.HTTPConduit$WrappedOutputStream.close(HTTPConduit.java:1322) ~[cxf-
rt-transports-http-2.7.3.jar:2.7.3]
        at org.apache.cxf.transport.AbstractConduit.close(AbstractConduit.java:56) ~[cxf-api-2.7.3.jar:2.7.3]
        at org.apache.cxf.transport.http.HTTPConduit.close(HTTPConduit.java:622) ~[cxf-rt-transports-http-
2.7.3.jar:2.7.3]
        at
org.apache.cxf.interceptor.MessageSenderInterceptor$MessageSenderEndingInterceptor.handleMessage(MessageSende
rInterceptor.java:62) ~[cxf-api-2.7.3.jar:2.7.3]
        ... 9 common frames omitted
Caused by: java.net.UnknownHostException: ise.lab6.com
        at java.net.AbstractPlainSocketImpl.connect(AbstractPlainSocketImpl.java:184) ~[na:1.8.0_25]
        at java.net.SocksSocketImpl.connect(SocksSocketImpl.java:392) ~[na:1.8.0_25]
        at java.net.Socket.connect(Socket.java:589) ~[na:1.8.0_25]
        at sun.security.ssl.SSLSocketImpl.connect(SSLSocketImpl.java:649) ~[na:1.8.0_25]
        at sun.net.NetworkClient.doConnect(NetworkClient.java:175) ~[na:1.8.0_25]
        at sun.net.www.http.HttpClient.openServer(HttpClient.java:432) ~[na:1.8.0_25]
```

```
        at sun.net.www.http.HttpClient.openServer(HttpClient.java:527) ~[na:1.8.0_25]
        at sun.net.www.protocol.https.HttpsClient.<init>(HttpsClient.java:275) ~[na:1.8.0_25]
        at sun.net.www.protocol.https.HttpsClient.New(HttpsClient.java:371) ~[na:1.8.0_25]
        at
sun.net.www.protocol.https.AbstractDelegateHttpsURLConnection.getNewHttpClient(AbstractDelegateHttpsURLConnec
tion.java:191) ~[na:1.8.0_25]
        at sun.net.www.protocol.http.HttpURLConnection.plainConnect0(HttpURLConnection.java:1103)
~[na:1.8.0_25]
        at sun.net.www.protocol.http.HttpURLConnection.plainConnect(HttpURLConnection.java:997)
~[na:1.8.0_25]
        at
sun.net.www.protocol.https.AbstractDelegateHttpsURLConnection.connect(AbstractDelegateHttpsURLConnection.java
:177) ~[na:1.8.0_25]
        at sun.net.www.protocol.http.HttpURLConnection.getOutputStream0(HttpURLConnection.java:1281)
~[na:1.8.0_25]
        at sun.net.www.protocol.http.HttpURLConnection.getOutputStream(HttpURLConnection.java:1256)
~[na:1.8.0_25]
        at sun.net.www.protocol.https.HttpsURLConnectionImpl.getOutputStream(HttpsURLConnectionImpl.java:250)
~[na:1.8.0_25]
        at
org.apache.cxf.transport.http.URLConnectionHTTPConduit$URLConnectionWrappedOutputStream.setupWrappedStream(UR
LConnectionHTTPConduit.java:170) ~[cxf-rt-transports-http-2.7.3.jar:2.7.3]
        at
org.apache.cxf.transport.http.HTTPConduit$WrappedOutputStream.handleHeadersTrustCaching(HTTPConduit.java:1282
) ~[cxf-rt-transports-http-2.7.3.jar:2.7.3]
        at org.apache.cxf.transport.http.HTTPConduit$WrappedOutputStream.onFirstWrite(HTTPConduit.java:1233)
~[cxf-rt-transports-http-2.7.3.jar:2.7.3]
        at
org.apache.cxf.transport.http.URLConnectionHTTPConduit$URLConnectionWrappedOutputStream.onFirstWrite(URLConne
ctionHTTPConduit.java:183) ~[cxf-rt-transports-http-2.7.3.jar:2.7.3]
        at org.apache.cxf.io.AbstractWrappedOutputStream.write(AbstractWrappedOutputStream.java:47) ~[cxf-
api-2.7.3.jar:2.7.3]
        at org.apache.cxf.io.AbstractThresholdOutputStream.write(AbstractThresholdOutputStream.java:69)
~[cxf-api-2.7.3.jar:2.7.3]
        at org.apache.cxf.transport.http.HTTPConduit$WrappedOutputStream.close(HTTPConduit.java:1295) ~[cxf-
rt-transports-http-2.7.3.jar:2.7.3]
        ... 12 common frames omitted
Exception in thread "main" java.io.IOException: unsuccessful attempts made to all session directories
        at com.cisco.pxgrid.stub.identity.impl.SessionIteratorImpl.open(SessionIteratorImpl.java:148)
        at com.cisco.pxgrid.samples.ise.SessionDownload.main(SessionDownload.java:132)
```