

使用 Cisco pxGrid 部署证书

将自签名证书与 ISE pxGrid 节点和 pxGrid 客户端配合使用

目录

关于本文档	3
简介	4
证书配置示例	5
自签名 ISE pxGrid 节点证书和 pxGrid 角色配置	5
自签名 pxGrid 客户端证书	8
测试 pxGrid 客户端和 ISE pxGrid 节点	12
查看密钥库条目	14
故障排除	16

关于本文档

本文档说明使用自签名证书配置 pxGrid 客户端和 ISE pxGrid 节点所需的配置步骤。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：

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。

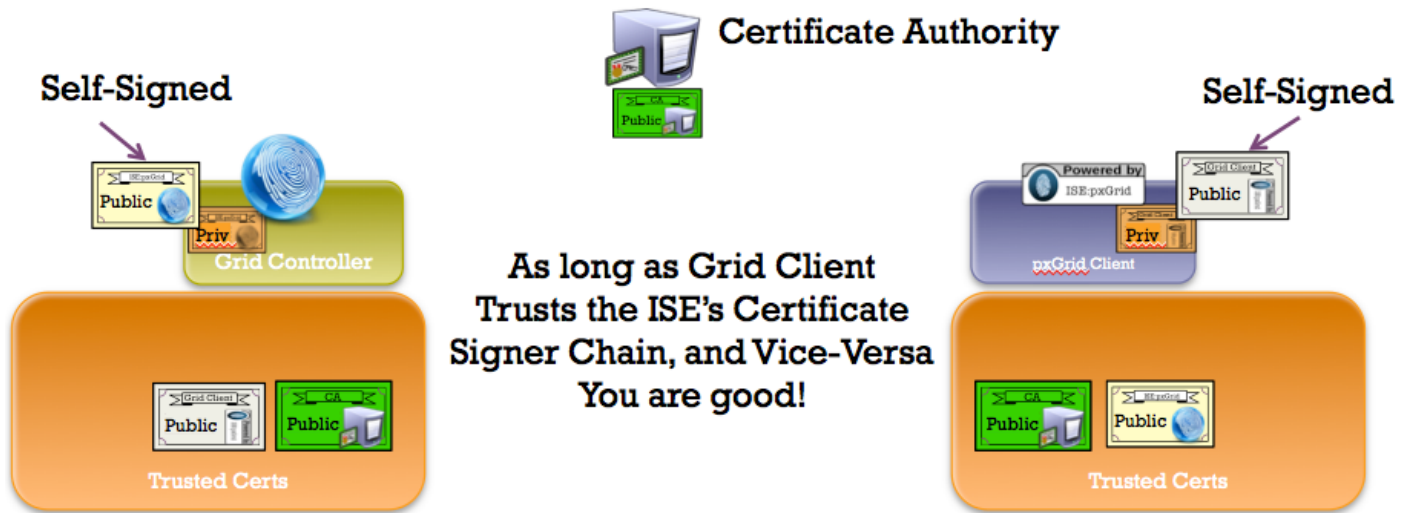
本文档假设已安装思科身份服务引擎 (ISE) 1.3。对于 pxGrid 客户端，可以使用运行 OSX 10.8.5 的 Mac，或者 Linux 操作系统。此外，pxGrid 客户端必需具备 Oracle Java Development Kit 7 或 8。

在《*使用证书部署 pxGrid*》系列中有其他两个文档：

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

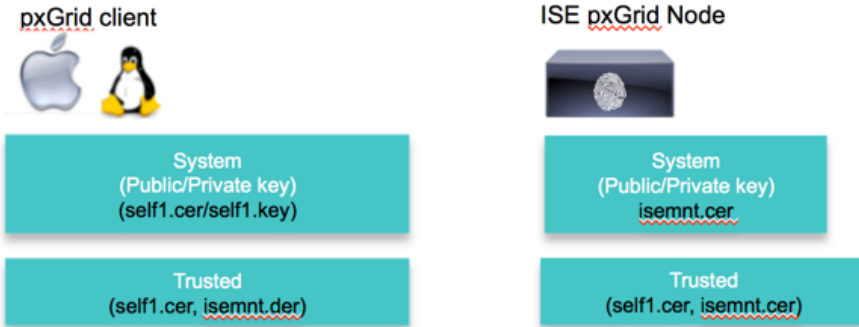
简介

使用 ISE pxGrid 节点和 pxGrid 客户端的自签名证书部署 pxGrid 是一种用于测试的替代方法，可取代使用 pxGrid SDK 中的样本证书。自签名证书不是源于可信来源，与使用证书颁发机构 (CA) 相比不够安全。但是，在本文档中，ISE 通过将 pxGrid 客户端的公钥导入到 ISE 受信任证书库中来信任 pxGrid 客户端的公钥。pxGrid 客户端信任 pxGrid 客户端的受信任密钥库中的 ISE 公共证书。一般来说，这比使用自签名证书更安全。



证书配置示例

本文档中使用的证书示例如下：

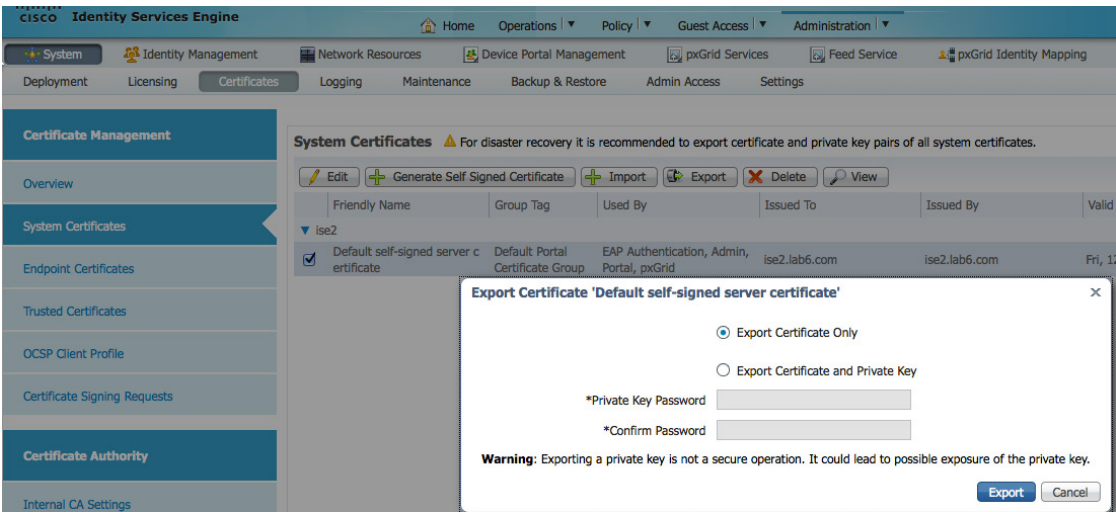


Keystore values:
 self1jks- used for keystoreFilename in pxGrid script
 root1.jks- used for truststoreFilename in pxGrid script

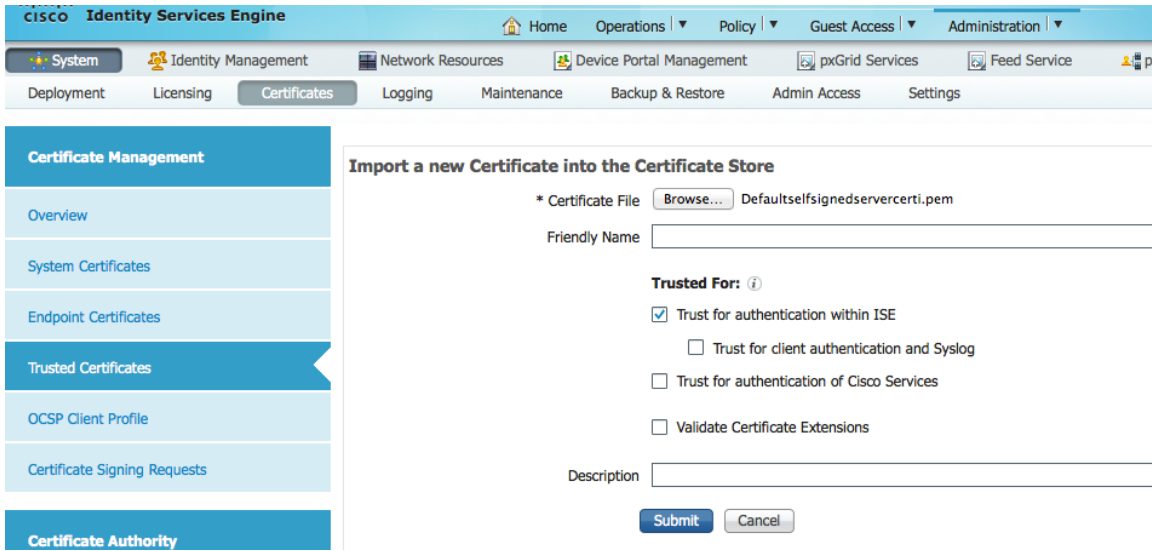
自签名 ISE pxGrid 节点证书和 pxGrid 角色配置

在本节中，我们会将 ISE 自签名证书导入到 ISE 受信任证书库中。当 ISE 身份证书导入到受信任证书库中后，ISE 节点上的 pxGrid 角色便会被启用，pxGrid ISE 节点将作为主节点。

- 第 1 步** 导出自签名 ISE 身份证书并另存为 .pem 文件。
Administration -> System -> Certificates -> 选择 ISE 身份证书 -> Export (仅公钥)。



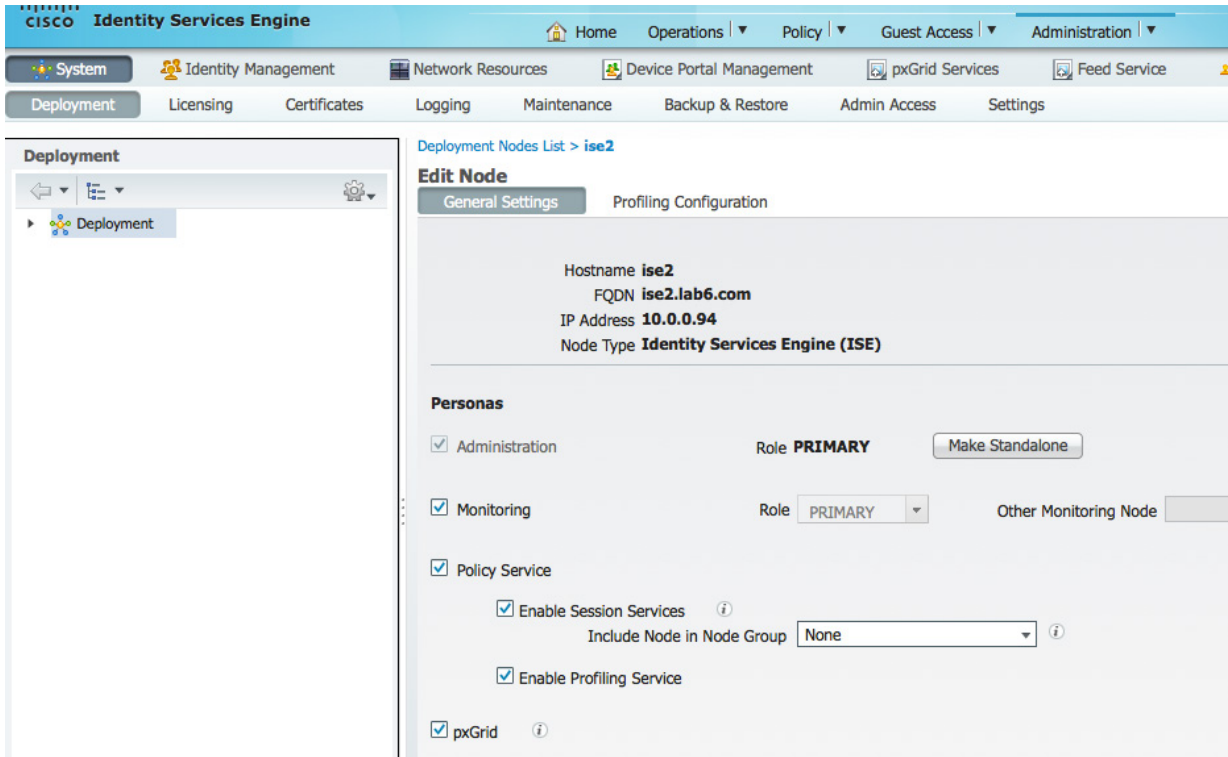
第 2 步 将已保存的 ISE .pem 文件导入到 ISE 受信任证书库中。
Administration -> System -> Certificates -> Trusted Certificates -> 浏览并上传文件 -> Submit。
启用“trust for authentication within ISE”。



您将看到已导入的 ISE 受信任证书。

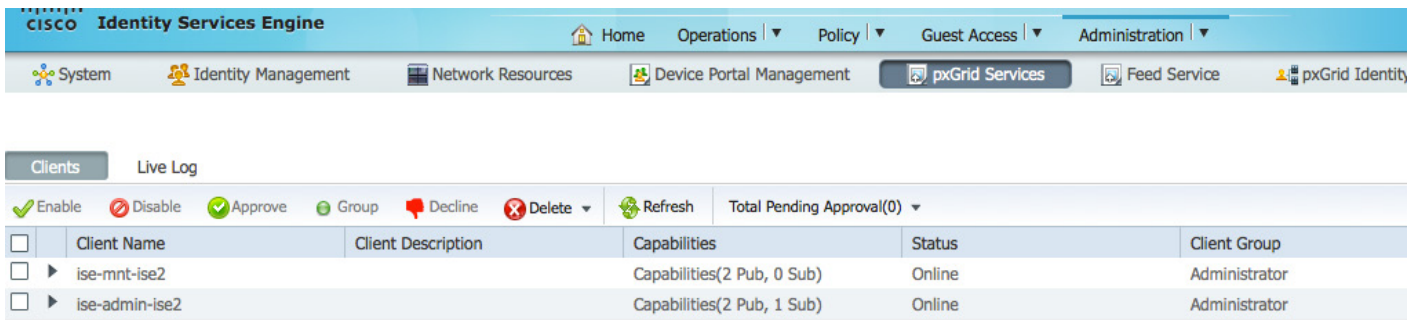
<input type="checkbox"/>	Friendly Name	Status	Trusted For	Serial Number	Issued To
<input type="checkbox"/>	Baltimore CyberTrust Root	Enabled	Cisco Services	02 00 00 B9	Baltimore CyberTrust
<input type="checkbox"/>	Certificate Services Endpoint Sub CA - ise2#00001	Enabled	Infrastructure Endpoints	0B A4 C8 E2 A9 A4...	Certificate Services E
<input type="checkbox"/>	Certificate Services OCSP Responder - ise2#00003	Enabled	Infrastructure	1A E3 25 3B 98 CA...	Certificate Services C
<input type="checkbox"/>	Certificate Services Root CA - ise2#00002	Enabled	Infrastructure Endpoints	0D 9F C1 A1 C1 9D...	Certificate Services R
<input type="checkbox"/>	Cisco CA Manufacturing	Disabled	Endpoints Infrastructure	6A 69 67 B3 00 00 ...	Cisco Manufacturing
<input type="checkbox"/>	Cisco Root CA 2048	Disabled	Endpoints Infrastructure	5F F8 7B 28 2B 54 ...	Cisco Root CA 2048
<input type="checkbox"/>	ise2.lab6.com#ise2.lab6.com#00004	Enabled	Infrastructure	54 8A 31 DD 00 00...	ise2.lab6.com
<input type="checkbox"/>	Thawte Primary Root CA	Enabled	Cisco Services	34 4E D5 57 20 D5...	thawte Primary Root

第 3 步 在 ISE 中启用 pxGrid 角色。
Administration -> System -> Deployment -> 启用 pxGrid -> 将角色更改为 Primary -> Save。



注： 无需将角色更改为 Primary

第 4 步 验证发布的服务是否已启动。
Administration -> pxGrid Services。



注： 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。

自签名 pxGrid 客户端证书

本节详细介绍 pxGrid 客户端上的自签名证书生成过程。生成 pxGrid 公钥/私钥对后，将根据私钥（例如 self1.key）创建 PKCS 12 文件（self1.p12）。

此 PKCS 12 文件将导入到充当 pxGrid 脚本的信任库文件名和信任库密码的目标或身份密钥库（例如 self1.jks）中。ISE 身份证书和公共证书也都将添加到此密钥库。

ISE 身份证书还将添加到充当信任库文件名和信任库密码的信任密钥库（例如 root1.jks）中。

第 1 步 为 pxGrid 客户端生成私钥（例如 self1.key）。

```
openssl genrsa -out self1.key 4096

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

第 2 步 生成自签名 CSR (self1.csr) 请求并提供质询密码。

```
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
```

注：在本文档各处使用相同的密码可便于维护，并减少错误

第 3 步 生成自签名证书/公钥对证书（例如 self1.cer）。

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


第 4 步 系统将根据私钥创建 PKCS12 文件（例如 self1.p12）。

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

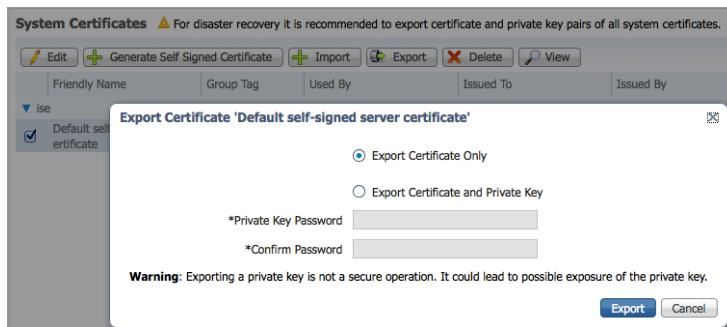
```
Enter Export Password: cisco123
Verifying - Enter Export Password: cisco123
```

第 5 步 self1.p12 将导入到身份密钥库（例如 self1.jks）中。密钥库文件名可以是扩展名为 .jks 的随机文件名。这将在 pxGrid 脚本中充当信任库文件名和关联信任库密码。

```
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
```

第 6 步 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。可以重命名扩展名为 .pem 的文件以使其更易于读取，在本例中该文件重命名为 isemnt.pem。



第 7 步 将 .pem 文件转换为 .der 格式。

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

第 8 步 将 ISE 身份证书添加到身份密钥库。这将用于在运行 pxGrid 会话下载脚本时保护从 ISE MNT 节点进行的批量会话下载。

```
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   .....0Q...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
```

第 9 步 将 pxGrid 客户端证书导入到身份密钥库中。

```
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
```

注：如果您收到表明证书已添加到预先存在的密钥库的消息，则可以选择“no”，这不会有任何问题。我选择了“yes”，因此我们可以验证后来是否添加了证书。

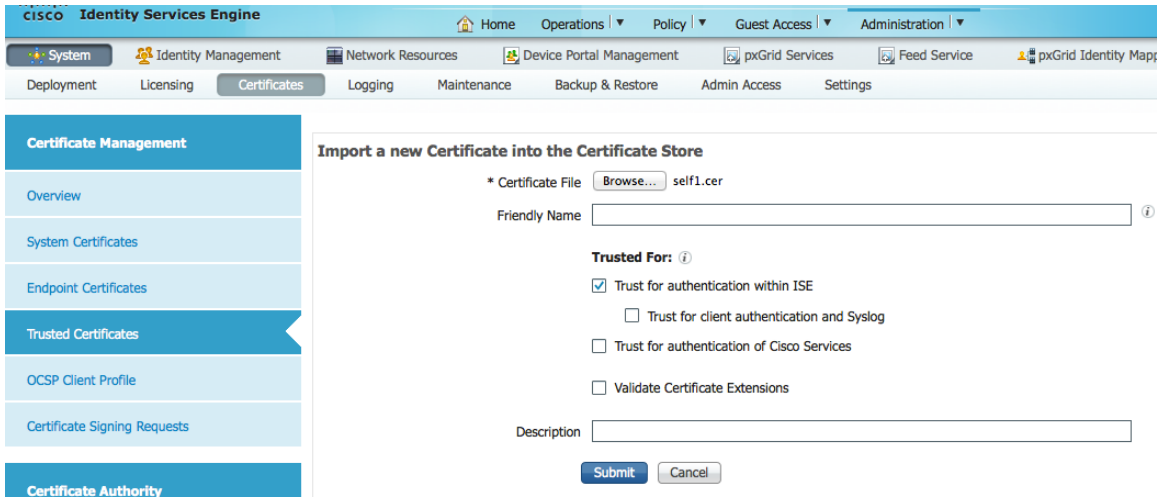
第 10 步 将 ISE 身份证证书导入到信任密钥库（例如 root1.jks）中。这将充当 pxGrid 脚本的信任库文件名和信任库密码。

```
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
```

第 11 步 将 pxGrid 客户端公共证书 (self1.cer) 上传到 ISE 受信任证书库中。
Administration -> System Certificates -> Trusted Certificates -> 从 pxGrid 客户端上传 self1.cer。



Certificate Management

- Overview
- System Certificates
- Endpoint Certificates
- Trusted Certificates**
- OCSP Client Profile
- Certificate Signing Requests

Import a new Certificate into the Certificate Store

* Certificate File

Friendly Name

Trusted For:

- Trust for authentication within ISE
- Trust for client authentication and Syslog
- Trust for authentication of Cisco Services
- Validate Certificate Extensions

Description

第 12 步 将身份密钥库 (self1.jks) 和信任密钥库 (root1.jks) 复制到 ../samples/bin/.. 文件夹中。

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。

第 1 步 注册 pxGrid 客户端。

```

./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

```

CISCO Identity Services Engine

Home Operations Policy Guest Access Administration

System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service pxGrid Identity Ma

Clients Live Log

Enable Disable Approve Group Decline Delete Refresh Total Pending Approval(0) 1 -

Client Name	Client Description	Capabilities	Status	Client Group
ise-admin-ise		Capabilities(2 Pub, 1 Sub)	Online	Administrator
ise-mnt-ise		Capabilities(2 Pub, 0 Sub)	Online	Administrator
pxgridclient	test1	Capabilities(0 Pub, 0 Sub)	Offline	Session

第 2 步 运行会话下载。

```
./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=jepich, 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
```

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 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 .....0Q...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.
]
]

```

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.GCException: 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
```