Using ISE 2.2 Internal Certificate Authority (CA) to Deploy Certificates to Cisco Platform Exchange Grid (pxGrid) Clients

Author: John Eppich

Table of Contents

About this Document

This document is intended for Cisco Engineers, partners and customers using Cisco Identity Services Engine (ISE) 2.2 internal Certificate Authority (CA) for deploying Cisco platform Exchange Grid (pxGrid) certificates to pxGrid clients. Using the ISE internal CA authority for deploying pxGrid client certificates eases certificate deployment by using ISE as the internal CA authority and not requiring an external CA server.

The ISE 2.2 internal CA generates certificates with or without certificate signing requests (CSR) and downloaded in Privacy Enhanced Mail (PEM) format or Public-Key Cryptography Standards (PKCS12) or Privacy Enhanced Mail (PEM) format. Bulk download certificates can also be generated.

This document describes the procedure for configuring the ISE certificate provisioning portal and provides use-case examples for generating and issuing the pxGrid certificates for the following pxGrid clients:

- Security solutions using java keystores (can be used for Splunk)
- Cisco Firepower 6.2, 6.1
- Stealthwatch 6.9
- Cisco Web Security Appliance 9.0.1 build 162

Using ISE 2.2 Internal Certificate Authority (CA) to deploy certificates to pxGrid clients

The ISE 2.2 Internal CA eases pxGrid certificate by generating certificates with or without Certificate Signing Requests (CSR) in either PEM or PKCS12 format. By default, the ISE pxGrid certificate has been signed by the ISE internal CA. Using the ISE internal CA provides pxGrid client certificate generation options to generate certificates with or without providing the Certificate Signing Requests (CSR) and in different download formats Privacy Enhanced Mail (PEM) and PKCS12 file formats. Please note that you are limited to a key size of 2048, if you are providing CSR requests for generating certificates. This is a known issue.

Cisco partners and Cisco Security Solutions that have implemented Java Key Stores

Generating pxGrid client certificates in PEM format without CSR request

Step 1 Select **Administration->pxGrid Services->Certificates,** and select **Generate a single certificate (without signing request)** from the I want to drop-down menu

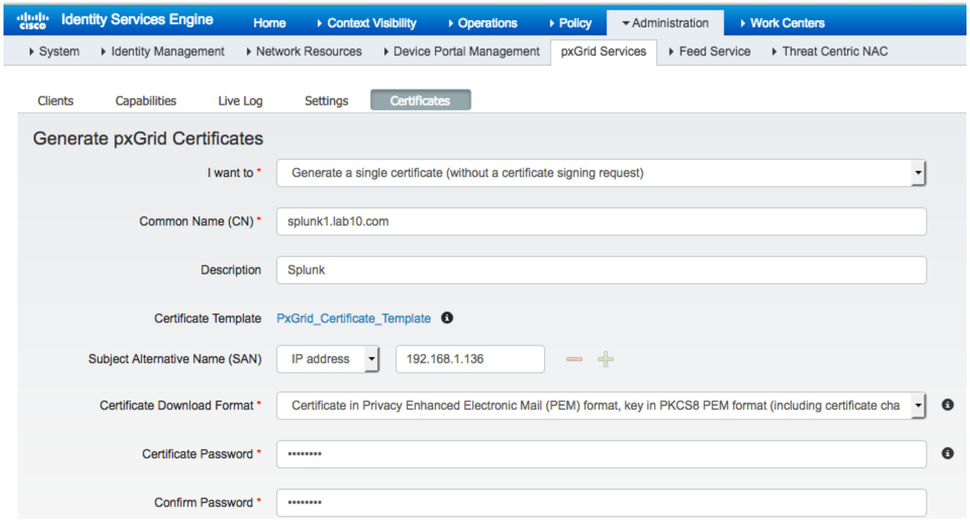
Step 2 Enter the FQDN for the **Common Name (CN)**

Step 3 Enter the certificate **Description**

Step 4 Enter the IP address or FQDN for the **Subject Alternative Name**

Step 5 Select the Certificate Download format, choose **Certificate in Privacy Enhanced Electronic Mail (PEM) format, key in PKCS8 PEM format (including certificate chain**)

Step 6 Enter and confirm the certificate password

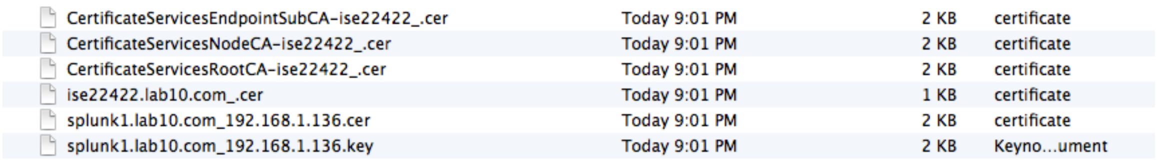


Generate pxGrid Certificates

I want to *	Generate a single certificate (without a certificate signing request)
Common Name (CN) *	splunk1.lab10.com
Description	Splunk
Certificate Template	PxGrid_Certificate_Template
Subject Alternative Name (SAN)	IP address 192.168.1.136
Certificate Download Format *	Certificate in Privacy Enhanced Electronic Mail (PEM) format, key in PKCS8 PEM format (including certificate cha
Certificate Password *	••••••••
Confirm Password *	••••••••

Step 7 Select **Create**

Step 8 Download and save the zipped file locally. The zipped file contains the following:



CertificateServicesEndpointSubCA-ise22422_.cer	Today 9:01 PM	2 KB	certificate
CertificateServicesNodeCA-ise22422_.cer	Today 9:01 PM	2 KB	certificate
CertificateServicesRootCA-ise22422_.cer	Today 9:01 PM	2 KB	certificate
ise22422.lab10.com_.cer	Today 9:01 PM	1 KB	certificate
splunk1.lab10.com_192.168.1.136.cer	Today 9:01 PM	2 KB	certificate
splunk1.lab10.com_192.168.1.136.key	Today 9:01 PM	2 KB	Keyno...ument

Note: The CertificateServicesEndpointSubCA-ise22422_.cer file is the sub CA file that gets assigned to the endpoints. The CertificateServicesNodeCA-ise22422_.cer file is used for downloading active bulk sessions from the ISE MnT node or the CertificatesServicesRootCA-ise22422_.cer file can be used in distributed ISE deployments. Ise2242.lab10.com_cer public certificate file from the ISE node containing the ISE internal CA,

Importing pxGrid client certificates into Java Key Store with PEM format

Step 1 Concatenate files into one certificates

```
cat CertificateServicesEndpointSubCA-ise22422_.cer CertificateServicesRootCA-ise22422_.cer
CertificateServicesNodeCA-ise22422_.cer ise22422.lab10.com_.cer > CA1.cer
```

Step 2 Create PKCS12 file

```
openssl pkcs12 -export -out splunk1.p12 -inkey splunk1.lab10.com_192.168.1.136.key -in
splunk1.lab10.com_192.168.1.136.cer -chain -CAfile CA1.cer
```

Step 3 Import PKCS12 file into keystore

```
keytool -importkeystore -srckeystore splunk1.p12 -destkeystore splunk1.jks -srcstoretype PKCS12
```

Step 4 Export CA root certificate from the ISE trusted certificate store PEM file converted to DER format

```
openssl x509 -outform der -in CA1.cer -out CA1.der
```

Step 5 Import the converted CA root certificate in DER format to trusted root keystore

```
keytool -import -alias mnt1 -keystore rootiseCA.jks -file CA1.der
```

Step 6 Import the pxGrid client certificate into the trusted file keystore

```
keytool -import -alias pxGridclient -keystore splunk1.jks -file splunk1.lab10.com_192.168.1.136.cer
```

Step 7 Import the CA root certificate to trusted root keystore

```
keytool -import -alias -keystore rootiseCA.jks -file CA1.cer
```

Step 8 Import the CertificateServicesRoot certificate into trusted root keystore

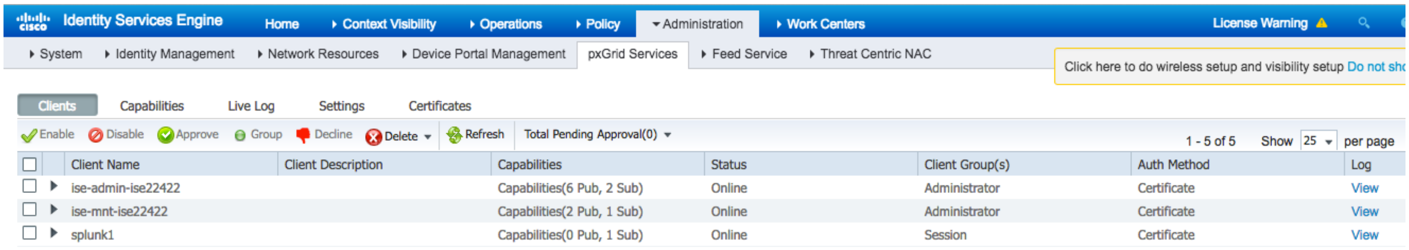
```
keytool -import -alias ise230 -keystore rootiseCA.jks -file CertificateServicesRootCA-ise22422_.cer
```

Testing using pxGrid sample session script

Step 1 Run the following session script to successfully register as a pxGrid client and subscribe to the session directory topic.

```
./session_subscribe.sh -a 192.168.1.230 -u splunk1 -k splunk1.jks -p Cisco123 -t rootiseCA.jks -q Cisco123
------- properties -------
  version=1.0.4.17
  hostnames=192.168.1.230
  username=splunk1
  password=
  group=Session
  description=null
  keystoreFilename=splunk1.jks
  keystorePassword=Cisco123
  truststoreFilename=rootiseCA.jks
  truststorePassword=Cisco123
--------------------------
18:48:39.467 [Thread-1] INFO  com.cisco.pxgrid.ReconnectionManager - Started
Connecting...
18:48:39.486 [Thread-1] INFO  com.cisco.pxgrid.Configuration - Connecting to host 192.168.1.230
18:48:39.795 [Thread-1] INFO  com.cisco.pxgrid.Configuration - Connected OK to host 192.168.1.230
18:48:39.795 [Thread-1] INFO  com.cisco.pxgrid.Configuration - Client Login to host 192.168.1.230
18:48:39.956 [Thread-1] INFO  com.cisco.pxgrid.Configuration - Client Login OK to host 192.168.1.230
Connected
Filters (ex. '1.0.0.0/255.0.0.0,1234::/16,...' or <enter> for no filter): 18:48:41.110 [Thread-1] INFO
com.cisco.pxgrid.ReconnectionManager - Connected
```

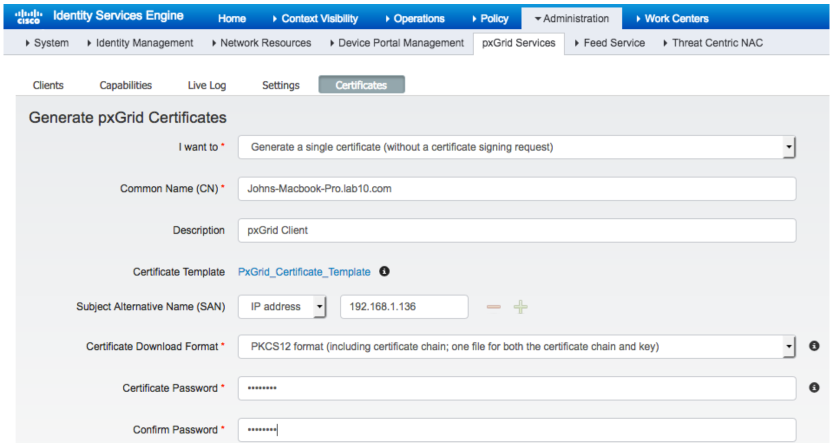
Step 2 Select **Administration->pxGrid Services** to view the registered pxGrid client.



□	Client Name	Client Description	Capabilities	Status	Client Group(s)	Auth Method	Log
□	ise-admin-ise22422		Capabilities(6 Pub, 2 Sub)	Online	Administrator	Certificate	View
□	ise-mnt-ise22422		Capabilities(2 Pub, 1 Sub)	Online	Administrator	Certificate	View
□	splunk1		Capabilities(0 Pub, 1 Sub)	Online	Session	Certificate	View

Generating pxGrid client certificates in PKCS12 format

Step 1 Select **Administration->pxGrid client->Certificates**



Generate pxGrid Certificates

I want to * Generate a single certificate (without a certificate signing request)

Common Name (CN) * Johns-Macbook-Pro.lab10.com

Description pxGrid Client

Certificate Template PxGrid_Certificate_Template

Subject Alternative Name (SAN) IP address 192.168.1.136

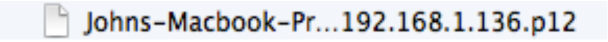
Certificate Download Format * PKCS12 format (including certificate chain; one file for both the certificate chain and key)

Certificate Password * ••••••••

Confirm Password * ••••••••

Step 2 Select **Create**

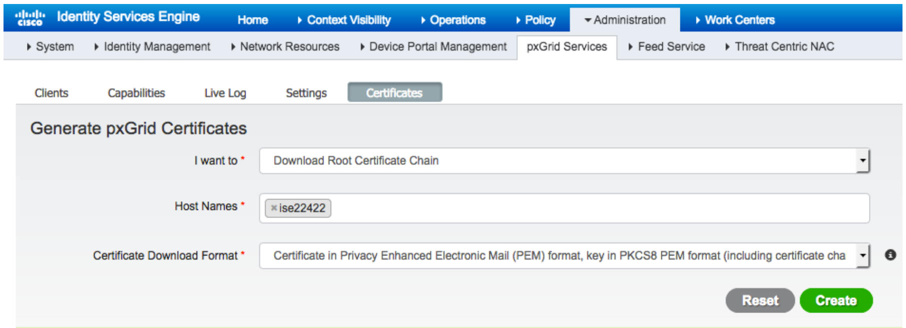
Step 3 Save the PKS12 file locally, the zipped file contains



Johns-Macbook-Pr...192.168.1.136.p12

Step 4 Download the certificate chain

Select **Administration->pxGrid certificates**



Generate pxGrid Certificates

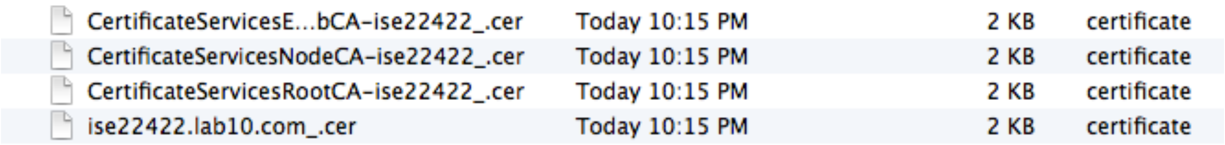
I want to * Download Root Certificate Chain

Host Names * ise22422

Certificate Download Format * Certificate in Privacy Enhanced Electronic Mail (PEM) format, key in PKCS8 PEM format (including certificate cha

Step 5 Select **Create**

Step 6 Download and save the file locally



CertificateServicesE...bCA-ise22422_.cer	Today 10:15 PM	2 KB	certificate
CertificateServicesNodeCA-ise22422_.cer	Today 10:15 PM	2 KB	certificate
CertificateServicesRootCA-ise22422_.cer	Today 10:15 PM	2 KB	certificate
ise22422.lab10.com_.cer	Today 10:15 PM	2 KB	certificate

Importing pxGrid client certificates into Java Key Store with PKS12 format

Step 1 Create keystore from PKCS12 file

```
keytool -importkeystore -srckeystore Johns-Macbook-Pro.lab10.com_192.168.1.136.p12 -destkeystore mac22.jks -
srcstoretype PKCS12
Enter destination keystore password:  Cisco123
Re-enter new password: Cisco123
Enter source keystore password:  Cisco123
Entry for alias johns-macbook-pro.lab10.com_192.168.1.136 successfully imported.
Import command completed:  1 entries successfully imported, 0 entries failed or cancelled
```

Step 2 Concatenate files

```
cat CertificateServicesEndpointSubCA-ise22422_.cer CertificateServicesRootCA-ise22422_.cer
CertificateServicesNodeCA-ise22422_.cer ise22422.lab10.com_.cer > CA1.cer
```

Step 3 Export CA root certificate from the ISE trusted certificate store PEM file converted to DER format

```
openssl x509 -outform der -in CA1.cer -out CA1.der
```

Step 4 Add the ISE root certificate into the global trust store

```
keytool -import -alias mac111 -keystore rootiseCA.jks -file CA1.der
Enter keystore password:  Cisco123
Re-enter new password: Cisco123
Owner: CN=Certificate Services Endpoint Sub CA - ise22422
Issuer: CN=Certificate Services Node CA - ise22422
Serial number: 7186cb58e5fb423a958b740f71d5e396
Valid from: Tue Dec 20 16:17:30 EST 2016 until: Tue Dec 21 16:17:28 EST 2021
Certificate fingerprints:
	 MD5:  CB:57:CA:43:EA:5B:82:ED:F8:E6:65:74:64:41:64:9E
	 SHA1: B2:31:D2:A0:39:35:49:F3:8D:B0:1C:69:66:56:C3:E7:12:E6:D4:6E
	 SHA256:
7F:82:E7:54:1C:BC:7C:64:7D:DE:CF:0E:C8:B3:F7:A9:0A:76:EB:E7:62:4D:17:A1:D9:5F:BD:4D:BF:32:B1:43
	 Signature algorithm name: SHA256withRSA
	 Version: 3

Extensions:

#1: ObjectId: 2.5.29.35 Criticality=false
AuthorityKeyIdentifier [
KeyIdentifier [
0000: 0A A3 EC 73 AC C3 0F A2   D8 40 EC D1 60 8F DB AA  ...s.....@..`...
0010: AD BC 8D 85                                        ....
]
[CN=Certificate Services Root CA - ise22422]
SerialNumber: [    86f78e30 1147c38f 62d790f1 50a172]
]

#2: ObjectId: 2.5.29.19 Criticality=true
BasicConstraints:[
  CA:true
  PathLen:2147483647
]

#3: ObjectId: 2.5.29.15 Criticality=true
KeyUsage [
  Key_CertSign
]
```

```
#4: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: B5 3A 92 CE 4B EF 93 D2   18 6B D2 59 A0 C8 80 24  .:..K....k.Y...$
0010: 6E 67 52 6C                                        ngRl
]
]

Trust this certificate? [no]:  yes
Certificate was added to keystore
```

Step 5 Generate the public certificate from the PKCS12 file

```
openssl pkcs12 -nokeys -clcerts -in Johns-Macbook-Pro.lab10.com_192.168.1.136.p12 -out Johns-Macbook-
Pro.lab10.com_192.168.1.136.cer
Enter Import Password: Cisco123
MAC verified OK
```

Step 6 Generate private Key

```
openssl pkcs12 -nocerts -in Johns-Macbook-Pro.lab10.com_192.168.1.136.p12 -out Johns-Macbook-
Pro.lab10.com_192.168.1.136.key
Enter Import Password: Cisco123
MAC verified OK
Enter PEM pass phrase: Cisco123
Verifying - Enter PEM pass phrase: Cisco123
```

Step 7 Add public certificate to trustfile keystore

```
keytool -import -alias mac111 -keystore mac22.jks -file Johns-Macbook-Pro.lab10.com_192.168.1.136.cer
Enter keystore password:  Cisco123
Certificate already exists in keystore under alias <johns-macbook-pro.lab10.com_192.168.1.136>
Do you still want to add it? [no]:  yes
Certificate was added to keystore
```

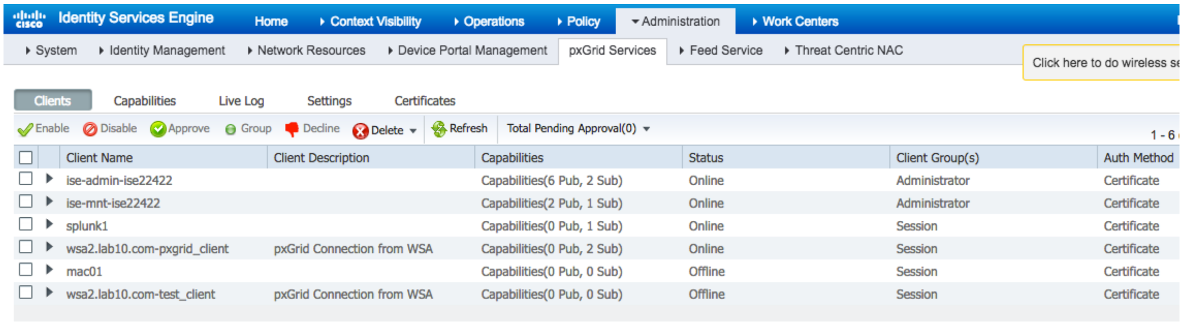
Testing using pxGrid sample session script

Step 1 Run the following session script to successfully register as a pxGrid client and subscribe to the session directory topic.

```
./session_subscribe.sh -a 192.168.1.230 -u MAC01 -k mac22.jks -p Cisco123 -t rootiseCA.jks -q Cisco123
------- properties -------
  version=1.0.4.17
  hostnames=192.168.1.230
  username=MAC01
  password=
  group=Session
  description=null
  keystoreFilename=mac22.jks
  keystorePassword=Cisco123
  truststoreFilename=rootiseCA.jks
  truststorePassword=Cisco123
--------------------------
18:20:29.348 [Thread-1] INFO  com.cisco.pxgrid.ReconnectionManager - Started
```

```
Connecting...
18:20:29.546 [Thread-1] INFO  com.cisco.pxgrid.Configuration - Connecting to host 192.168.1.230

18:20:30.806 [Thread-1] INFO  com.cisco.pxgrid.Configuration - Connected OK to host 192.168.1.230

18:20:30.806 [Thread-1] INFO  com.cisco.pxgrid.Configuration - Client Login to host 192.168.1.230
18:20:31.390 [Thread-1] INFO  com.cisco.pxgrid.Configuration - Client Login OK to host 192.168.1.230
Connected
Filters (ex. '1.0.0.0/255.0.0.0,1234::/16,...' or <enter> for no filter): 18:20:33.670 [Thread-1] INFO
com.cisco.pxgrid.ReconnectionManager - Connected
```

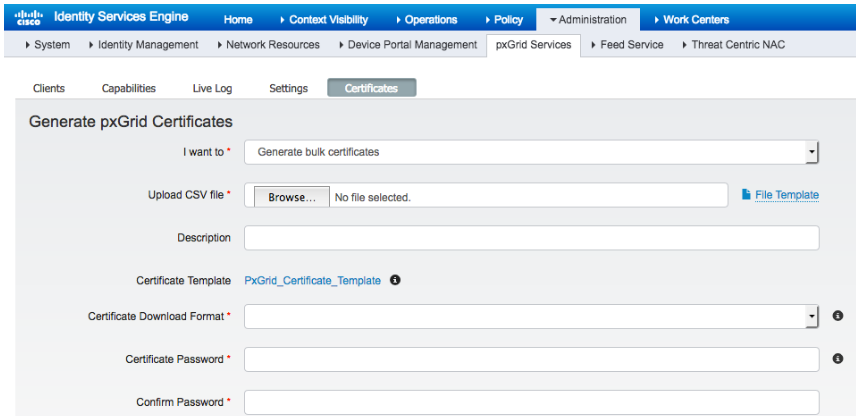
Step 2 Select **Administration->pxGrid Services**



□	Client Name	Client Description	Capabilities	Status	Client Group(s)	Auth Method
□	ise-admin-ise22422		Capabilities(6 Pub, 2 Sub)	Online	Administrator	Certificate
□	ise-mnt-ise22422		Capabilities(2 Pub, 1 Sub)	Online	Administrator	Certificate
□	splunk1		Capabilities(0 Pub, 1 Sub)	Online	Session	Certificate
□	wsa2.lab10.com-pxgrid_client	pxGrid Connection from WSA	Capabilities(0 Pub, 2 Sub)	Online	Session	Certificate
□	mac01		Capabilities(0 Pub, 0 Sub)	Offline	Session	Certificate
□	wsa2.lab10.com-test_client	pxGrid Connection from WSA	Capabilities(0 Pub, 0 Sub)	Offline	Session	Certificate

Generating Bulk Certificates

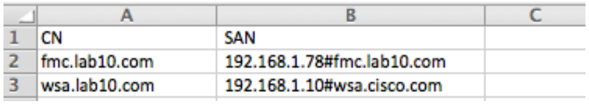
Step 1 Select **Administration->pxGrid Services->Certificates**



Generate pxGrid Certificates

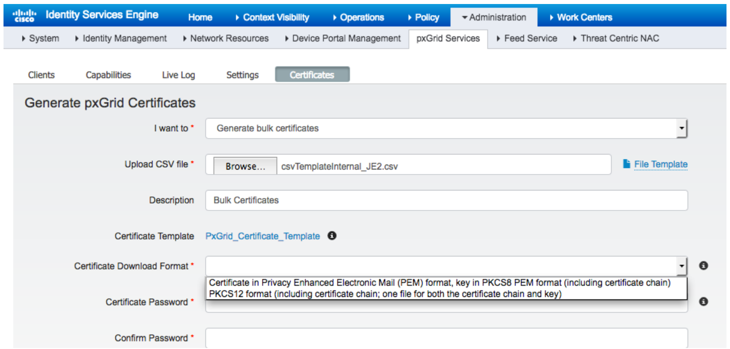
I want to *	Generate bulk certificates
Upload CSV file *	No file selected.
Description	
Certificate Template	PxGrid_Certificate_Template
Certificate Download Format *	
Certificate Password *	
Confirm Password *	

Step 2 Select and download the **File Template** and fill in the pxGrid client FQDN names and IP addresses



	A	B	C
1	CN	SAN	
2	fmc.lab10.com	192.168.1.78#fmc.lab10.com	
3	wsa.lab10.com	192.168.1.10#wsa.cisco.com	

Step 3 Upload the certificate CSV file, and select the certificate format



Generate pxGrid Certificates

I want to * Generate bulk certificates

Upload CSV file * Browse... csvTemplateInternal_JE2.csv File Template

Description Bulk Certificates

Certificate Template PxGrid_Certificate_Template

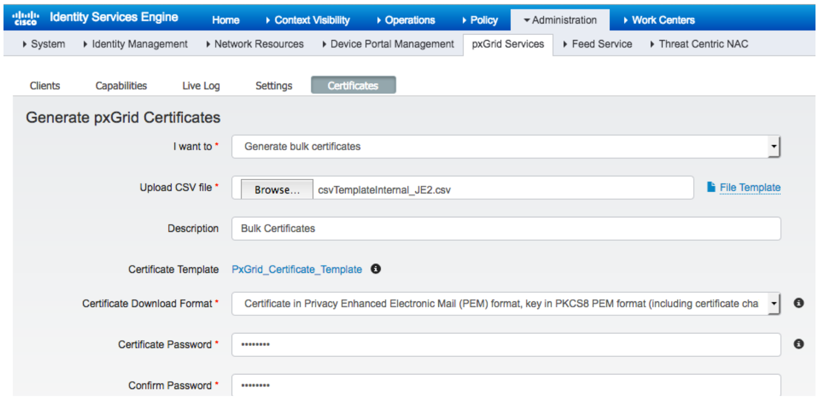
Certificate Download Format *

Certificate in Privacy Enhanced Electronic Mail (PEM) format, key in PKCS8 PEM format (including certificate chain)
PKCS12 format (including certificate chain; one file for both the certificate chain and key)

Certificate Password *

Confirm Password *

Step 4 If selecting PEM format, please refer to **"Importing pxGrid client certificates using JAVA in PEM"** format



Generate pxGrid Certificates

I want to * Generate bulk certificates

Upload CSV file * Browse... csvTemplateInternal_JE2.csv File Template

Description Bulk Certificates

Certificate Template PxGrid_Certificate_Template

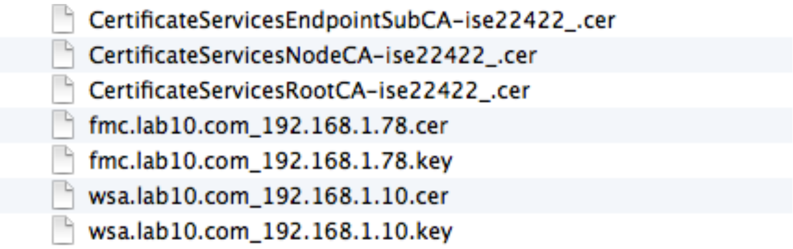
Certificate Download Format * Certificate in Privacy Enhanced Electronic Mail (PEM) format, key in PKCS8 PEM format (including certificate cha

Certificate Password * ••••••••

Confirm Password * ••••••••

Step 5 Select **Create**

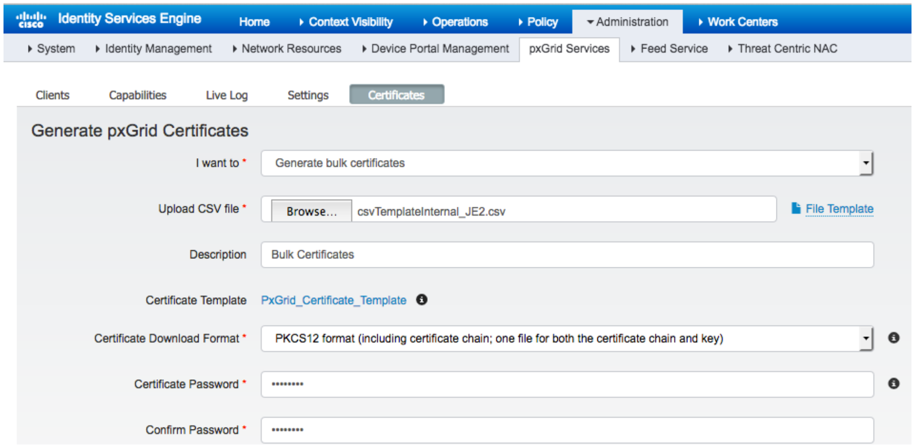
Step 6 Download the file locally, you will see the public private key-pairs for each of the pxGrid clients.



CertificateServicesEndpointSubCA-ise22422_.cer
CertificateServicesNodeCA-ise22422_.cer
CertificateServicesRootCA-ise22422_.cer
fmc.lab10.com_192.168.1.78.cer
fmc.lab10.com_192.168.1.78.key
wsa.lab10.com_192.168.1.10.cer
wsa.lab10.com_192.168.1.10.key

Step 7 You can then upload the certificates into the solutions trusted store.

Step 8 If you select PKCS12 format, please refer to **Importing pxGrid client certificates in java using PKCS 12 format**



Generate pxGrid Certificates

I want to * Generate bulk certificates

Upload CSV file * csvTemplateInternal_JE2.csv

Description Bulk Certificates

Certificate Template PxGrid_Certificate_Template

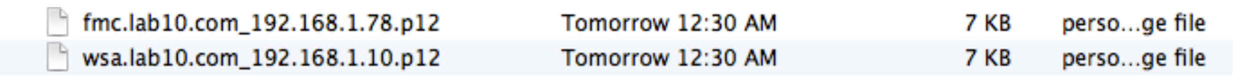
Certificate Download Format * PKCS12 format (including certificate chain; one file for both the certificate chain and key)

Certificate Password * ••••••••

Confirm Password * ••••••••

Step 9 Select **Create**

Step 10 Download file locally



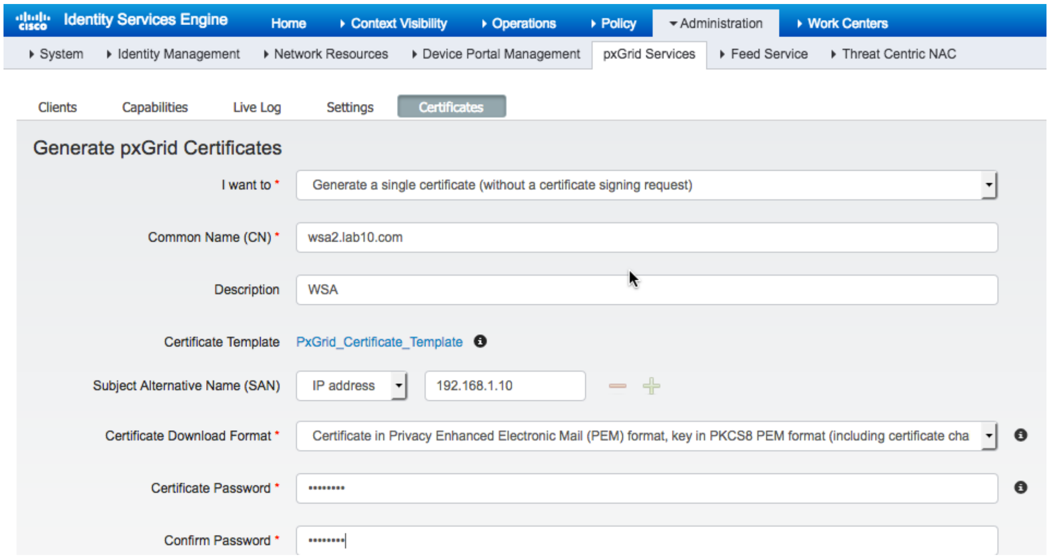
```
fmc.lab10.com_192.168.1.78.p12    Tomorrow 12:30 AM    7 KB    perso…ge file
wsa.lab10.com_192.168.1.10.p12    Tomorrow 12:30 AM    7 KB    perso…ge file
```

Cisco WSA

Below is an example of how Cisco's Web Security Appliance (WSA) implements ISE internal 2.2 certificates.

Generating WSA client certificate in PEM format without CSR request

Step 1 On ISE, select **Administration->pxGrid Services->Certificates**



Generate pxGrid Certificates

I want to * Generate a single certificate (without a certificate signing request)

Common Name (CN) * wsa2.lab10.com

Description WSA

Certificate Template PxGrid_Certificate_Template

Subject Alternative Name (SAN) IP address 192.168.1.10

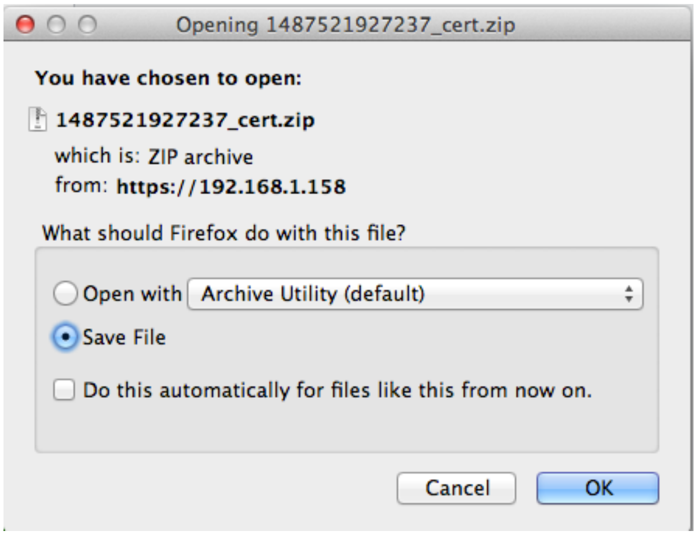
Certificate Download Format * Certificate in Privacy Enhanced Electronic Mail (PEM) format, key in PKCS8 PEM format (including certificate cha

Certificate Password * ••••••••

Confirm Password * ••••••••

Step 2 Select **Create**

Step 3 Save the file locally



Opening 1487521927237_cert.zip

You have chosen to open:

1487521927237_cert.zip

which is: ZIP archive

from: **https://192.168.1.158**

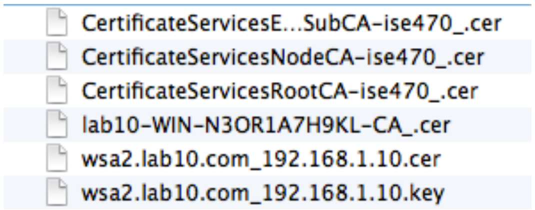
What should Firefox do with this file?

○ Open with Archive Utility (default)

● Save File

□ Do this automatically for files like this from now on.

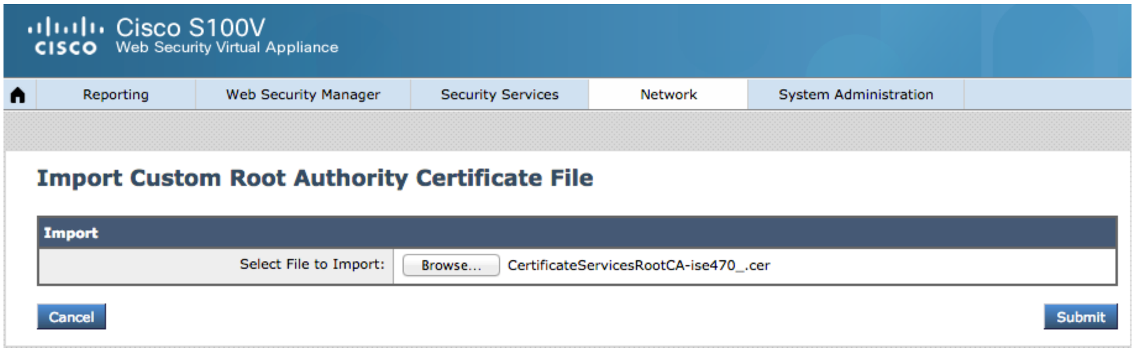
Step 4 You should see the following files



CertificateServicesE…SubCA-ise470_.cer
CertificateServicesNodeCA-ise470_.cer
CertificateServicesRootCA-ise470_.cer
lab10-WIN-N3OR1A7H9KL-CA_.cer
wsa2.lab10.com_192.168.1.10.cer
wsa2.lab10.com_192.168.1.10.key

Importing ISE Certificate Root Services CA into WSA Managed Trust Root Certificate Store

Step 1 Select **Network->System Management->Manage Trusted Root Certificates->Import->Browse->CertificateServicesRootCA….**



Import Custom Root Authority Certificate File

Import

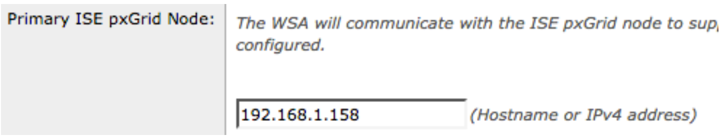
Select File to Import: Browse… CertificateServicesRootCA-ise470_.cer

Step 2 Select **Submit->Commit Changes->Commit Changes**

Uploading the ISE Root Certificate and WSA client certificates into WSA

Step 1 Select **Network->Identification Service->Identity Services Engine->Edit Settings**

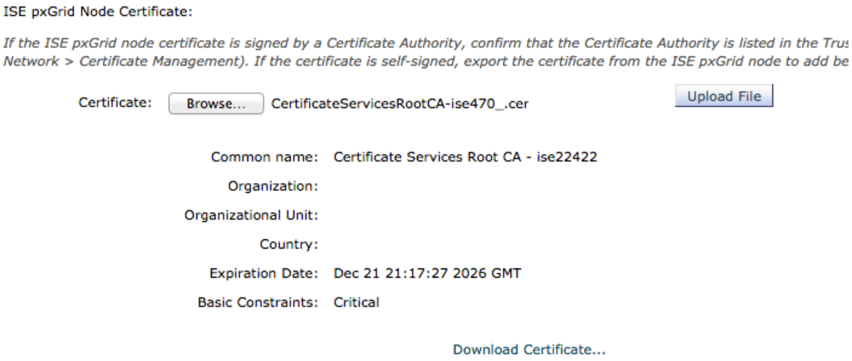
Step 2 Enter the IP Address of the ISE primary pxGrid node



Primary ISE pxGrid Node: *The WSA will communicate with the ISE pxGrid node to sup, configured.*

192.168.1.158 *(Hostname or IPv4 address)*

Step 3 Under **ISE pxGrid node certificate**, select **Browse->CSArootServiceCertifcate file->Upload**



ISE pxGrid Node Certificate:

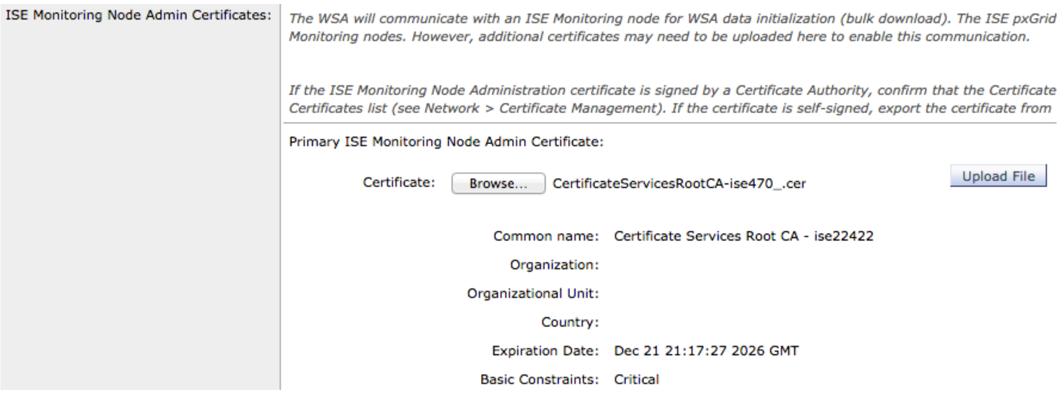
If the ISE pxGrid node certificate is signed by a Certificate Authority, confirm that the Certificate Authority is listed in the Trus Network > Certificate Management). If the certificate is self-signed, export the certificate from the ISE pxGrid node to add be

Certificate: Browse... CertificateServicesRootCA-ise470_.cer Upload File

Common name:	Certificate Services Root CA - ise22422
Organization:	
Organizational Unit:	
Country:	
Expiration Date:	Dec 21 21:17:27 2026 GMT
Basic Constraints:	Critical

Download Certificate...

Step 4 Under **ISE Monitoring Node Admin Certificate**, select **browse->CARootservice->upload**



ISE Monitoring Node Admin Certificates:

The WSA will communicate with an ISE Monitoring node for WSA data initialization (bulk download). The ISE pxGrid Monitoring nodes. However, additional certificates may need to be uploaded here to enable this communication.

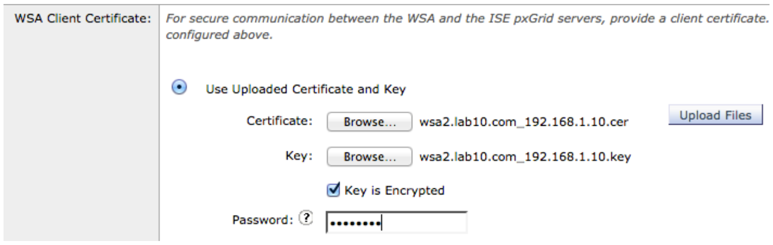
If the ISE Monitoring Node Administration certificate is signed by a Certificate Authority, confirm that the Certificate Certificates list (see Network > Certificate Management). If the certificate is self-signed, export the certificate from

Primary ISE Monitoring Node Admin Certificate:

Certificate: Browse... CertificateServicesRootCA-ise470_.cer Upload File

Common name:	Certificate Services Root CA - ise22422
Organization:	
Organizational Unit:	
Country:	
Expiration Date:	Dec 21 21:17:27 2026 GMT
Basic Constraints:	Critical

Step 5 Under **WSA Client Certificate->Use Uploaded certificate and key->browse to the files and enter encryption key password**



WSA Client Certificate: *For secure communication between the WSA and the ISE pxGrid servers, provide a client certificate. configured above.*

● Use Uploaded Certificate and Key

Certificate: Browse... wsa2.lab10.com_192.168.1.10.cer Upload Files

Key: Browse... wsa2.lab10.com_192.168.1.10.key

☑ Key is Encrypted

Password: ? ••••••••

Step 6 Select **Upload files**

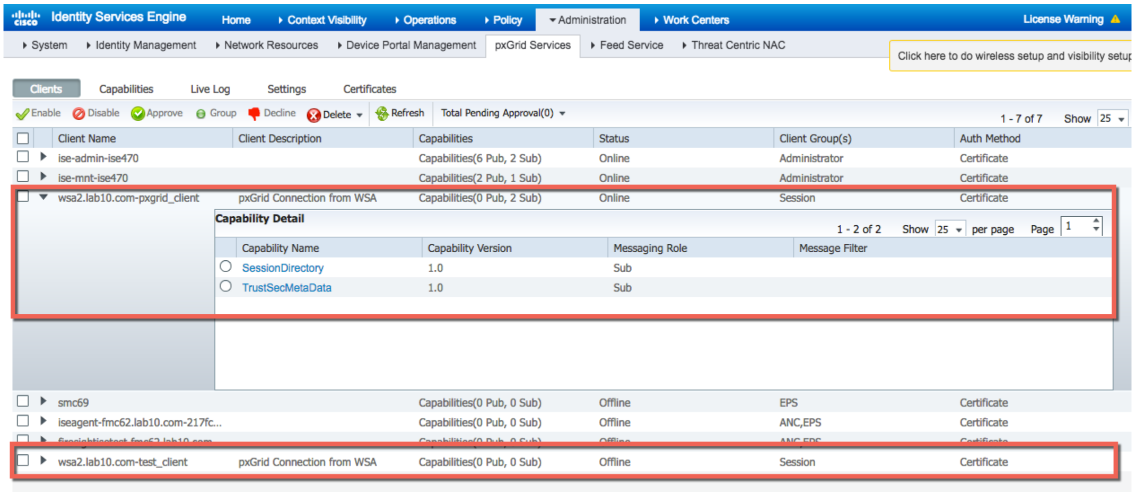
Step 7 Select **Start Test**, you should see

```
Checking DNS resolution of ISE pxGrid Node hostname(s) ...
Success: Resolved '192.168.1.158' address: 192.168.1.158

Validating WSA client certificate ...
Success: Certificate validation successful

Validating ISE pxGrid Node certificate(s) ...
Success: Certificate validation successful

Validating ISE Monitorting Node Admin certificate(s) ...
Success: Certificate validation successful

Checking connection to ISE pxGrid Node(s) ...
Success: Connection to ISE pxGrid Node was successful.
Retrieved 17 SGTs from: 192.168.1.158

Checking connection to ISE Monitorting Node (REST server(s)) ...
Success: Connection to ISE Monitorting Node was successful.
REST Host contacted: ise470.lab10.com

Test completed successfully.
```

Step 8 Select **Submit->Commit Changes->Commit Changes**

Testing Verifying the ISE published nodes appear

Step 1 Select **Administration->pxGrid Services**



☐	Client Name	Client Description	Capabilities	Status	Client Group(s)	Auth Method
☐	ise-admin-ise470		Capabilities(6 Pub, 2 Sub)	Online	Administrator	Certificate
☐	ise-mnt-ise470		Capabilities(2 Pub, 1 Sub)	Online	Administrator	Certificate
☐	wsa2.lab10.com-pxgrid_client	pxGrid Connection from WSA	Capabilities(0 Pub, 2 Sub)	Online	Session	Certificate
☐	smc69		Capabilities(0 Pub, 0 Sub)	Offline	EPS	Certificate
☐	iseagent-fmc62.lab10.com-217fc...		Capabilities(0 Pub, 0 Sub)	Offline	ANC,EPS	Certificate
☐	firesightisetest-fmc62.lab10.com		Capabilities(0 Pub, 0 Sub)	Offline	ANC,EPS	Certificate
☐	wsa2.lab10.com-test_client	pxGrid Connection from WSA	Capabilities(0 Pub, 0 Sub)	Offline	Session	Certificate

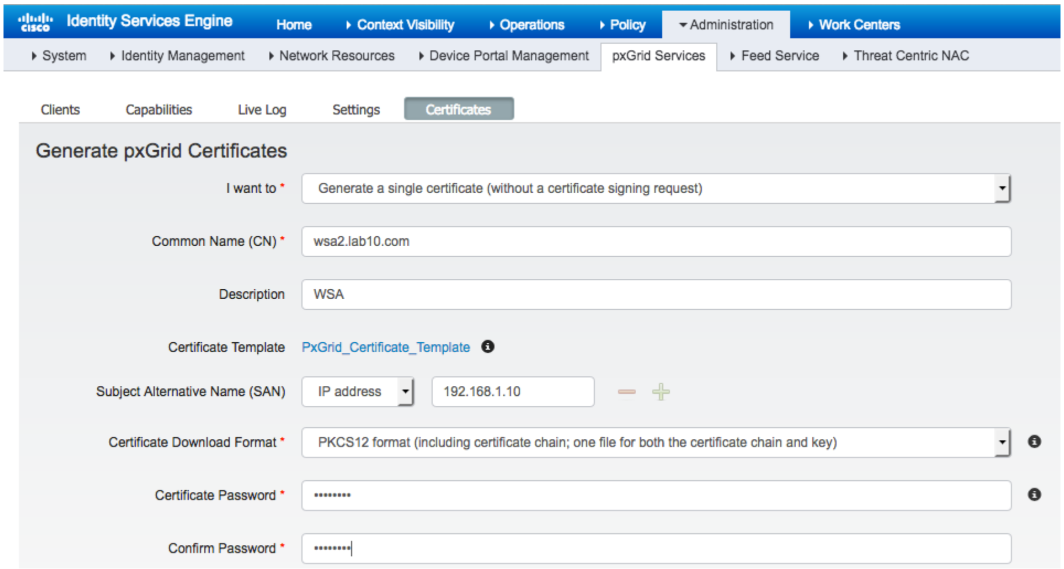
Capability Detail

1 - 2 of 2 Show 25 per page Page 1

	Capability Name	Capability Version	Messaging Role	Message Filter
○	SessionDirectory	1.0	Sub	
○	TrustSecMetaData	1.0	Sub	

Generating WSA Certificate Signing Request (CSR) using PKCS12 format

Step 1 On ISE, select **Administration -> pxGrid certificates**



Generate pxGrid Certificates

I want to * Generate a single certificate (without a certificate signing request)

Common Name (CN) * wsa2.lab10.com

Description WSA

Certificate Template PxGrid_Certificate_Template

Subject Alternative Name (SAN) IP address 192.168.1.10

Certificate Download Format * PKCS12 format (including certificate chain; one file for both the certificate chain and key)

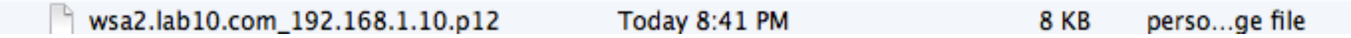
Certificate Password * ••••••••

Confirm Password * ••••••••

Step 2 Select **Create**

Step 3 Download the file locally

Step 4 You should see

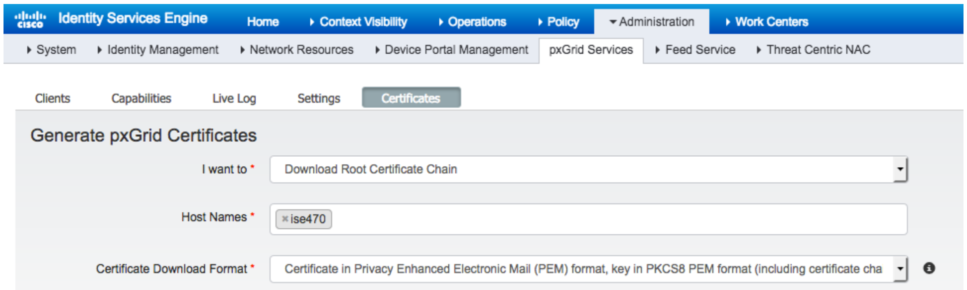


wsa2.lab10.com_192.168.1.10.p12 Today 8:41 PM 8 KB perso...ge file

Step 5 You will need to convert the files to the public private key-pair

```
sudo openssl pkcs12 -nokeys -clcerts -in wsa2.lab10.p12.com_192.168.1.10.p12 -out wsa2.cer
Enter Import Password: Cisco123
MAC verified OK
admin@sd:~$
sudo openssl pkcs12 -nocerts -in wsa2.lab10.p12 -out wsa2.key
Enter Import Password: Cisco123
MAC verified OK
Enter PEM pass phrase: Cisco123
Verifying - Enter PEM pass phrase: Cisco123
```

Step 6 You will also want to download the PKCS12 file certificate chain
Select **Administration->pxGrid Certificates**



Generate pxGrid Certificates

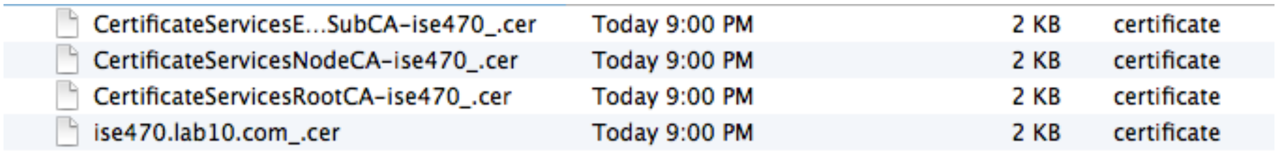
I want to * Download Root Certificate Chain

Host Names * ise470

Certificate Download Format * Certificate in Privacy Enhanced Electronic Mail (PEM) format, key in PKCS8 PEM format (including certificate cha

Step 7 Select **Create**

Step 8 Download and save the files locally.
You should see the following:



CertificateServicesE...SubCA-ise470_.cer	Today 9:00 PM	2 KB	certificate
CertificateServicesNodeCA-ise470_.cer	Today 9:00 PM	2 KB	certificate
CertificateServicesRootCA-ise470_.cer	Today 9:00 PM	2 KB	certificate
ise470.lab10.com_.cer	Today 9:00 PM	2 KB	certificate

Step 9 Use the CertificateServiceRootCA-ise470_.cer and upload into the WSA Managed Trust Root Certificate Store.

Step 10 Also use the CertificateServicesRootCA-ise470_.cer and upload as the ISE pxGrid node certificate and the ISE Monitoring Admin node certificate.

Step 11 Upload the WSA public private-key pair into WSA public private-pairs as in the WSA client certificate

Step 12 Run the connection test

Generating WSA Certificate Signing Request CSR (with certificate signing request)

Step 1 Generate the private key from a Linux server.

```
openssl genrsa -des3 -out wsa2.key 2048
Generating RSA private key, 2048 bit long modulus
.....................................................+++
.............................................................................................................
......................+++
e is 65537 (0x10001)
Enter pass phrase for smc69.key: Cisco123
Verifying - Enter pass phrase for wsa2.key: Cisco123
```

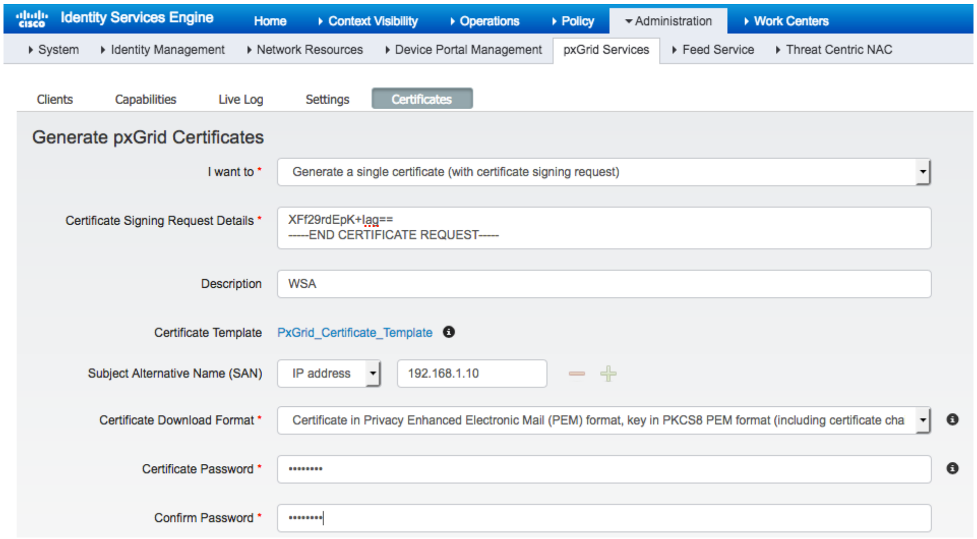
Step 2 Generate the Certificate Signing Request (CSR) from a Linux server.

```
openssl req -new -key wsa2.key -out wsa2.csr
Enter pass phrase for smc69.key: Cisco123
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:US
State or Province Name (full name) [Some-State]:Maryland
Locality Name (eg, city) []:Germantown
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Cisco
Organizational Unit Name (eg, section) []:Engineering
Common Name (e.g. server FQDN or YOUR name) []:wsa2.lab10.com
Email Address []:j@cisco.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
```

ISE Generating WSA Certificate based on CSR request in PEM format

Step 1 On ISE, select **Administration->pxGrid services,** and enter the following:

Note: You can only generate a key size of 2096; there is a bug in the pxGrid template

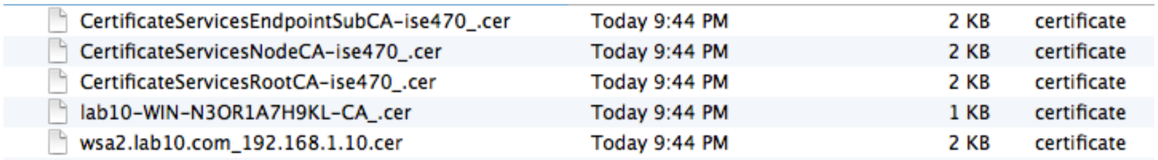


Generate pxGrid Certificates

I want to *	Generate a single certificate (with certificate signing request)
Certificate Signing Request Details *	XFf29rdEpK+lag== -----END CERTIFICATE REQUEST-----
Description	WSA
Certificate Template	PxGrid_Certificate_Template
Subject Alternative Name (SAN)	IP address 192.168.1.10
Certificate Download Format *	Certificate in Privacy Enhanced Electronic Mail (PEM) format, key in PKCS8 PEM format (including certificate cha
Certificate Password *	••••••••
Confirm Password *	••••••••

Step 2 Select **Create**

Step 3 Download the zipped file locally, you should see the following files



CertificateServicesEndpointSubCA-ise470_.cer	Today 9:44 PM	2 KB	certificate
CertificateServicesNodeCA-ise470_.cer	Today 9:44 PM	2 KB	certificate
CertificateServicesRootCA-ise470_.cer	Today 9:44 PM	2 KB	certificate
lab10-WIN-N3OR1A7H9KL-CA_.cer	Today 9:44 PM	1 KB	certificate
wsa2.lab10.com_192.168.1.10.cer	Today 9:44 PM	2 KB	certificate

Step 4 Upload the CertificateServicesRootCA-ise470_.cer into the WSA Managed Trust Root Certificate Store

Step 5 Upload the CertfifiacteServicesRootCA-ise470_.cer as the ISE pxGrid node certificate and the ISE admin node certificate.

Step 6 Upload the wsa2.lab10.com_192.168.1.10.cer as the public certificate in WSA client certificate configuration

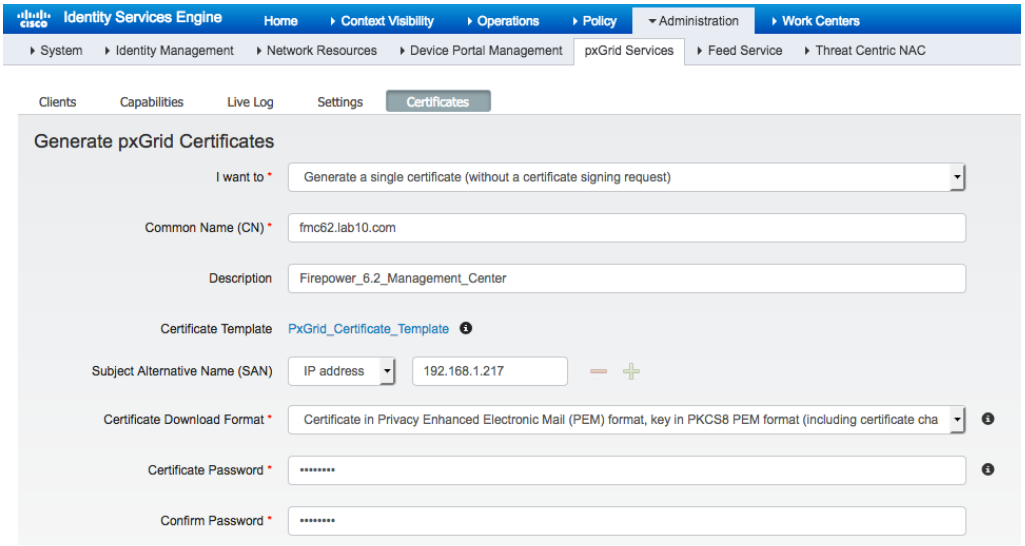
Step 7 Upload the wsa2.lab10.com_192.168.1.10.key file as the private key in WSA client certificate configuration

Step 8 Run the connection test.

Firepower 6.1, 6.2

Generating Firepower Management Client certificate in PEM format without CSR request

Step 1 Select **Administration->pxGrid Services->Certificates**



Generate pxGrid Certificates

I want to * Generate a single certificate (without a certificate signing request)

Common Name (CN) * fmc62.lab10.com

Description Firepower_6.2_Management_Center

Certificate Template PxGrid_Certificate_Template

Subject Alternative Name (SAN) IP address 192.168.1.217

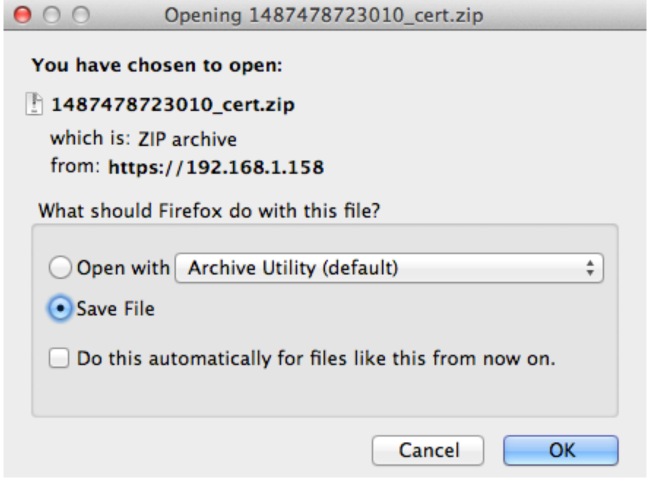
Certificate Download Format * Certificate in Privacy Enhanced Electronic Mail (PEM) format, key in PKCS8 PEM format (including certificate cha

Certificate Password * ••••••••

Confirm Password * ••••••••

Step 2 Select **Create**

Step 3 Save the file locally


Opening 1487478723010_cert.zip

You have chosen to open:

1487478723010_cert.zip

which is: ZIP archive

from: https://192.168.1.158

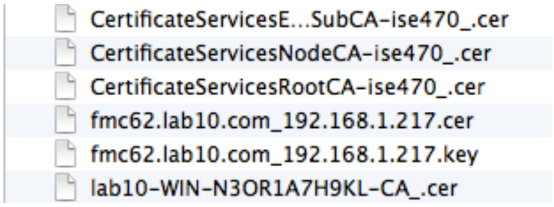
What should Firefox do with this file?

○ Open with Archive Utility (default)

● Save File

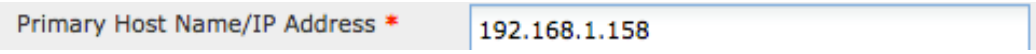
□ Do this automatically for files like this from now on.

Step 4 You should see the following


CertificateServicesE...SubCA-ise470_.cer
CertificateServicesNodeCA-ise470_.cer
CertificateServicesRootCA-ise470_.cer
fmc62.lab10.com_192.168.1.217.cer
fmc62.lab10.com_192.168.1.217.key
lab10-WIN-N3OR1A7H9KL-CA_.cer

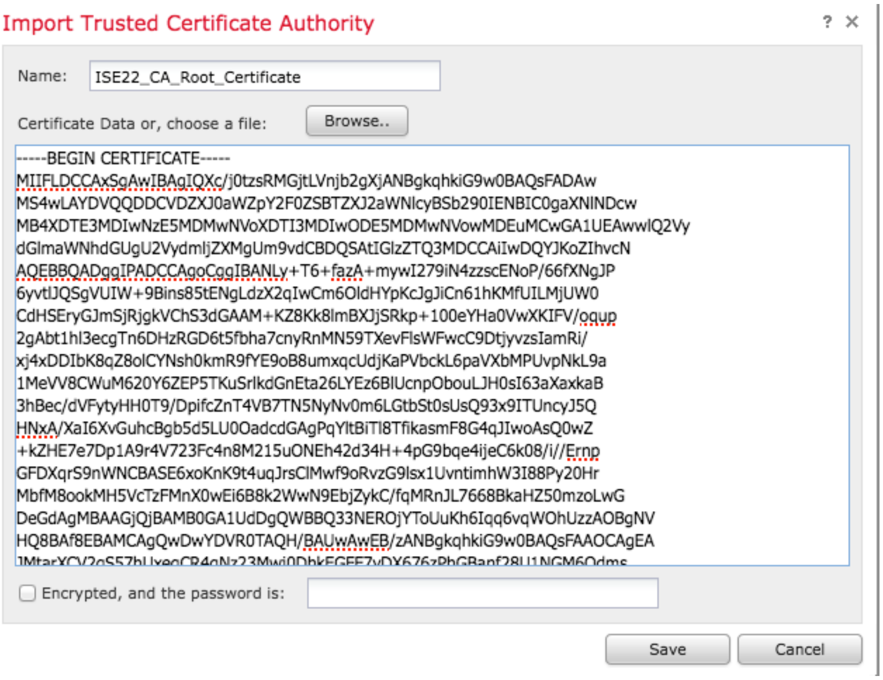
Importing ISE Root certificates into Managed CA Store

Step 1 On FMC 6.2, select **System->Integration->Identity Sources->Identity Services Engine enter the IP or the FQDN of the ISE pxGrid node**



Primary Host Name/IP Address * 192.168.1.158

Step 2 Under **pxGrid Server CA**, select ⊕, enter **ISE22_CA_Root_Certificate** browse and upload the **CertificateServicesRootCA-ise470_.cer** file into the Trusted Certificate Authority



Import Trusted Certificate Authority

Name: ISE22_CA_Root_Certificate

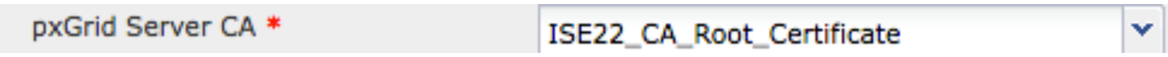
Certificate Data or, choose a file:

```
-----BEGIN CERTIFICATE-----
MIIFLDCCAxSgAwIBAgIQXc/j0tzsRMGjtLVnjb2gXjANBgkqhkiG9w0BAQsFADAw
MS4wLAYDVQQDDCVDZXJ0aWZpY2F0ZSBTZXJ2aWNlcyBSb290IENBIC0gaXNlNDcw
MB4XDTE3MDIwNzE5MDMwNVoXDTI3MDIwODE5MDMwNVowMDEuMCwGA1UEAwwlQ2Vy
dGlmaWNhdGUgU2VydmljZXMgUm9vdCBDQSAtIGlzZTQ3MDCCAiIwDQYJKoZIhvcN
AQEBBQADggIPADCCAgoCggIBANLy+T6+fazA+mywI279iN4zzscENoP/66fXNgJP
6yvtlJQSgVUIW+9Bins85tENgLdzX2qIwCm6OldHYpKcJgJiCn61hKMfUILMjUW0
CdHSEryGJmSjRjgkVChS3dGAAM+KZ8Kk8lmBXJjSRkp+100eYHa0VwXKIFV/oqup
2gAbt1hl3ecgTn6DHzRGD6t5fbha7cnyRnMN59TXevFlsWFwcC9DtjyvzsIamRi/
xj4xDDIbK8qZ8olCYNsh0kmR9fYE9oB8umxqcUdjKaPVbckL6paVXbMPUvpNkL9a
1MeVV8CWuM620Y6ZEP5TKuSrlkdGnEta26LYEz6BlUcnpObouLJH0sI63aXaxkaB
3hBec/dVFytyHH0T9/DpifcZnT4VB7TN5NyNv0m6LGtbSt0sUsQ93x9ITUncyJ5Q
HNxA/XaI6XvGuhcBgb5d5LU0OadcdGAgPqYltBiTl8TfikasmF8G4qJIwoAsQ0wZ
+kZHE7e7Dp1A9r4V723Fc4n8M215uONEh42d34H+4pG9bqe4ijeC6k08/i//Ernp
GFDXqrS9nWNCBASE6xoKnK9t4uqJrsClMwf9oRvzG9lsx1UvntimhW3I88Py20Hr
MbfM8ookMH5VcTzFMnX0wEi6B8k2WwN9EbjZykC/fqMRnJL7668BkaHZ50mzoLwG
DeGdAgMBAAGjQjBAMB0GA1UdDgQWBBQ33NEROjYToUuKh6Iqq6vqWOhUzzAOBgNV
HQ8BAf8EBAMCAgQwDwYDVR0TAQH/BAUwAwEB/zANBgkqhkiG9w0BAQsFAAOCAgEA
JMtarXCV2qS57hUxeqCR4qNz23Mwi0DhkEGEE7vDX676zPhGBanf28U1NGM6Odms
```

☐ Encrypted, and the password is:

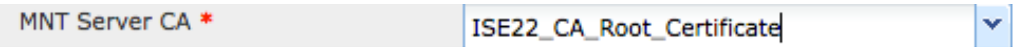
Step 3 Select **Save**

Step 4 You should see



pxGrid Server CA * ISE22_CA_Root_Certificate

Step 5 For the MNT Server CA select the ISE22_CA_Root_Certificate from the drop-down menu

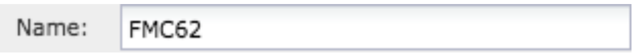


MNT Server CA * ISE22_CA_Root_Certificate

Importing FMC Client certificates into Internal Store

Step 1 For the FMC Server Certificate, select ⊕

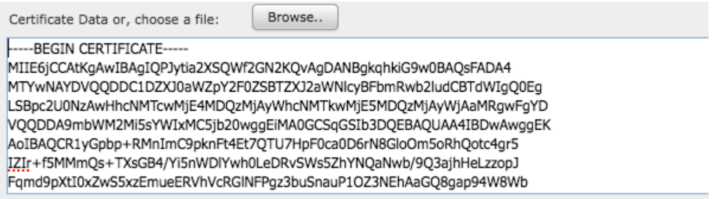
Step 2 Enter certificate name



Name: FMC62

Cisco Systems © 2017

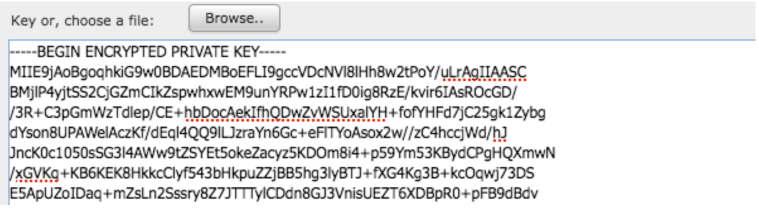
Step 3 For "**Certificate data or choose a file**" select and upload the **fmc62.lab10.com_192.168.1.217. cer** file



Certificate Data or, choose a file:

```
-----BEGIN CERTIFICATE-----
MIIE6jCCAtKgAwIBAgIQPJytia2XSQWf2GN2KQvAgDANBgkqhkiG9w0BAQsFADA4
MTYwNAYDVQQDDC1DZXJ0aWZpY2F0ZSBTZXJ2aWNlcyBFbmRwb2ludCBTdWIgQ0Eg
LSBpc2U0NzAwHhcNMTcwMjE4MDQzMjAyWhcNMTkwMjE5MDQzMjAyWjAaMRgwFgYD
VQQDDA9mbWM2Mi5sYWIxMC5jb20wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEK
AoIBAQCR1yGpbp+RMnImC9pknFt4Et7QTU7HpF0ca0D6rN8GloOm5oRhQotc4gr5
IZIr+f5MMmQs+TXsGB4/Yi5nWDlYwh0LeDRvSWs5ZhYNQaNwb/9Q3ajhHeLzzopJ
Fqmd9pXtI0xZwS5xzEmueERVhVcRGlNFPgz3buSnauP1OZ3NEhAaGQ8gap94W8Wb
```

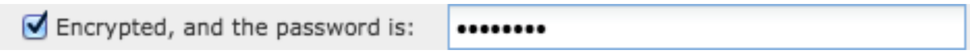
Step 4 For "**Key, or choose a file**" select and upload the **fmc62.lab10.com_192.168.1.217.key** file



Key or, choose a file:

```
-----BEGIN ENCRYPTED PRIVATE KEY-----
MIIE9jAoBgoqhkiG9w0BDAEDMBoEFLI9gccVDcNVl8lHh8w2tPoY/uLrAgIIAASC
BMjlP4yjtSS2CjGZmCIkZspwhxwEM9unYRPw1zI1fD0ig8RzE/kvir6IAsROcGD/
/3R+C3pGmWzTdlep/CE+hbDocAekIfhQDwZvWSUxalYH+fofYHFd7jC25gk1Zybg
dYson8UPAWelAczKf/dEql4QQ9lLJzraYn6Gc+eFlTYoAsox2w//zC4hccjWd/hJ
JncK0c1050sSG3l4AWw9tZSYEt5okeZacyz5KDOm8i4+p59Ym53KBydCPgHQXmwN
/xGVKg+KB6KEK8HkkcClyf543bHkpuZZjBB5hg3lyBTJ+fXG4Kg3B+kcOqwj73DS
E5ApUZoIDaq+mZsLn2Sssry8Z7JTTTylCDdn8GJ3VnisUEZT6XDBpR0+pFB9dBdv
```

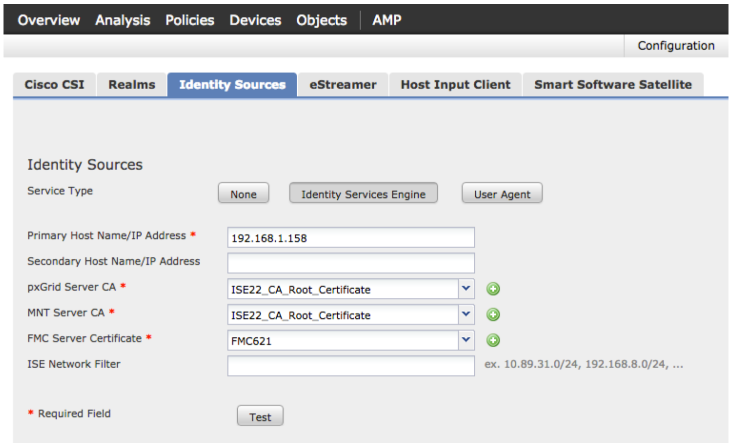
Step 5 Select **Encrypted,** and enter the password **Cisco123** as the password defined when generating the certificate



☑ Encrypted, and the password is: •••••••••

Step 6 Select **Save**

Step 7 You should see:



Identity Sources

Service Type:

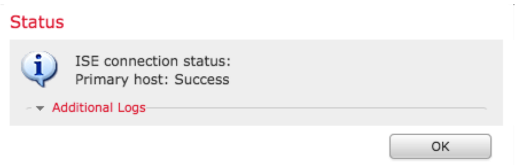
Primary Host Name/IP Address *	192.168.1.158
Secondary Host Name/IP Address	
pxGrid Server CA *	ISE22_CA_Root_Certificate
MNT Server CA *	ISE22_CA_Root_Certificate
FMC Server Certificate *	FMC621
ISE Network Filter	ex. 10.89.31.0/24, 192.168.8.0/24, ...

* Required Field

Testing Verifying the ISE published nodes appear

Step 1 Select **Test**

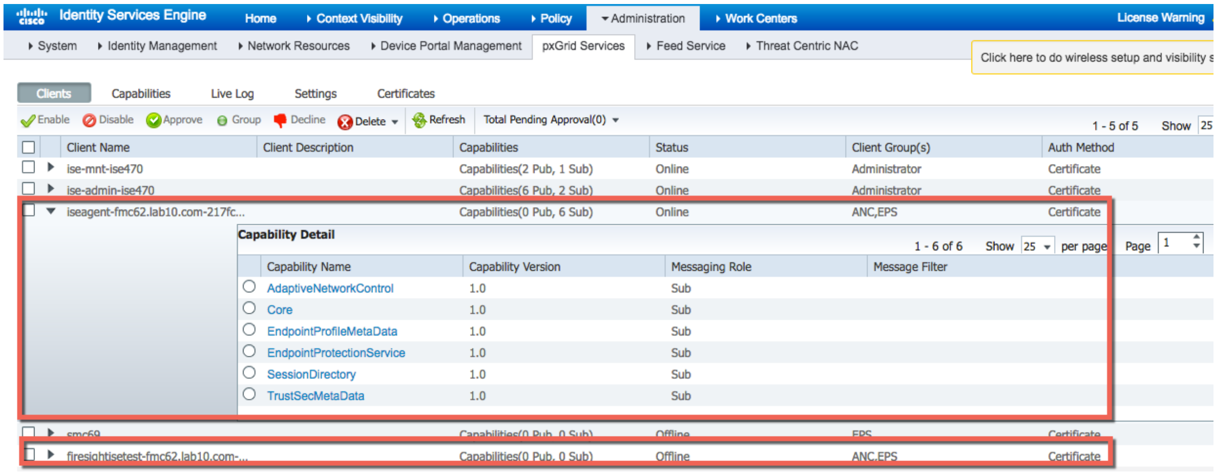
Step 2 You should see



Status

ISE connection status:
Primary host: Success

Step 3 On ISE, select **Administration->pxGrid Services** you should see:



	Client Name	Client Description	Capabilities	Status	Client Group(s)	Auth Method
□	ise-mnt-ise470		Capabilities(2 Pub, 1 Sub)	Online	Administrator	Certificate
□	ise-admin-ise470		Capabilities(6 Pub, 2 Sub)	Online	Administrator	Certificate
□	iseagent-fmc62.lab10.com-217fc...		Capabilities(0 Pub, 6 Sub)	Online	ANC,EPS	Certificate
□	smc69		Capabilities(0 Pub, 0 Sub)	Offline	EPS	Certificate
□	firesightisetest-fmc62.lab10.com-...		Capabilities(0 Pub, 0 Sub)	Offline	ANC,EPS	Certificate

Capability Detail

1 - 6 of 6 Show 25 per page Page 1

	Capability Name	Capability Version	Messaging Role	Message Filter
○	AdaptiveNetworkControl	1.0	Sub	
○	Core	1.0	Sub	
○	EndpointProfileMetaData	1.0	Sub	
○	EndpointProtectionService	1.0	Sub	
○	SessionDirectory	1.0	Sub	
○	TrustSecMetaData	1.0	Sub	

Generating FMC 6.1, 6.2 Certificate Signing Request CSR (with certificate signing request)

Step 1 Generate the private key from a Linux server.

```
openssl genrsa -des3 -out fmc621.key 2048
Generating RSA private key, 2048 bit long modulus
.....................................................+++
.............................................................................................................
......................+++
e is 65537 (0x10001)
Enter pass phrase for fmc621.key: Cisco123
Verifying - Enter pass phrase for fmc621.key: Cisco123
```

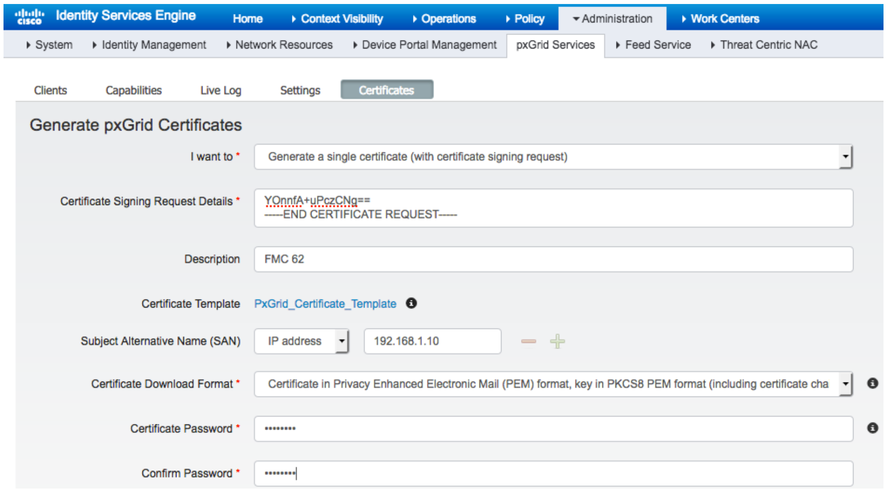
Step 2 Generate the Certificate Signing Request (CSR) from a Linux server.

```
openssl req -new -key fmc621.key -out fmc621.csr
Enter pass phrase for smc69.key: Cisco123
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:US
State or Province Name (full name) [Some-State]:Maryland
Locality Name (eg, city) []:Germantown
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Cisco
Organizational Unit Name (eg, section) []:Engineering
Common Name []:fmc62.lab10.com
Email Address []:j@cisco.com
```

ISE Generating FMC 6.1, 6.2 Certificate based on CSR request in PEM format

Step 1 On ISE, select **Administration->pxGrid services,** and enter the following:

<u>Note:</u> You can only generate a key size of 2096; there is a bug in the pxGrid template



Generate pxGrid Certificates

I want to *: Generate a single certificate (with certificate signing request)

Certificate Signing Request Details *: YOnnfA+uPczCNg==
-----END CERTIFICATE REQUEST-----

Description: FMC 62

Certificate Template: PxGrid_Certificate_Template

Subject Alternative Name (SAN): IP address 192.168.1.10

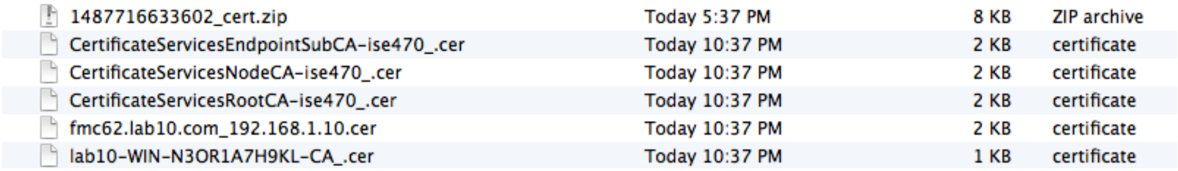
Certificate Download Format *: Certificate in Privacy Enhanced Electronic Mail (PEM) format, key in PKCS8 PEM format (including certificate cha

Certificate Password *: ••••••••

Confirm Password *: ••••••••

Step 2 Select **Create**

Step 3 Download the zipped file locally, you should see the following files



1487716633602_cert.zip	Today 5:37 PM	8 KB	ZIP archive
CertificateServicesEndpointSubCA-ise470_.cer	Today 10:37 PM	2 KB	certificate
CertificateServicesNodeCA-ise470_.cer	Today 10:37 PM	2 KB	certificate
CertificateServicesRootCA-ise470_.cer	Today 10:37 PM	2 KB	certificate
fmc62.lab10.com_192.168.1.10.cer	Today 10:37 PM	2 KB	certificate
lab10-WIN-N3OR1A7H9KL-CA_.cer	Today 10:37 PM	1 KB	certificate

Step 4 Upload the CertfifiacteServicesRootCA-ise470_.cer for the pxGrid Server CA

Step 5 Upload the CertfifiacteServicesRootCA-ise470_.cer for the MNT Server CA

Step 6 Upload the fmc2.lab10.com_192.168.1.10.cer for the FMC Server Certificate Store for the Certificate Data File

Step 7 Upload the fmc2.lab10.key for the FMC Server Certificate for the private key file

Step 8 Select encrypted and enter the password, (i.e. Cisco123 was used in this example)).

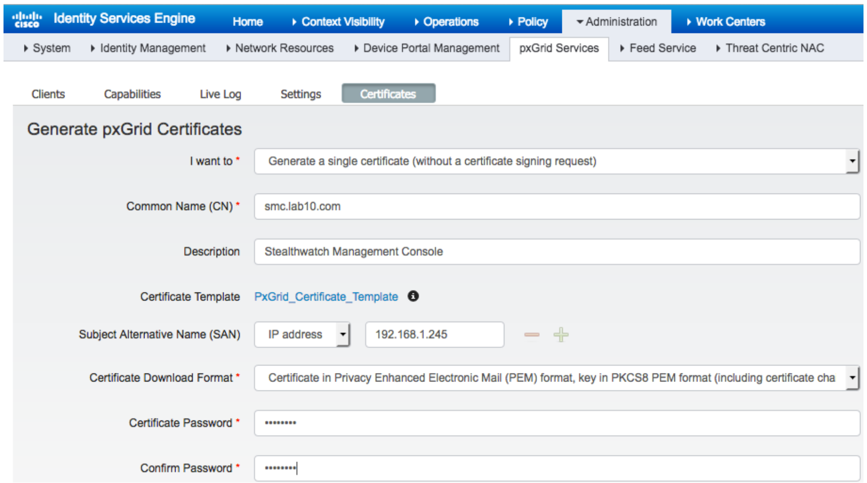
Step 9 Test the configuration

Stealthwatch 6.9

Generating Stealthwatch client certificate in PEM format without CSR request

Step 1 Select **Administration->pxGrid Services->Certificates,** and enter the information below:

Note: You can only generate a key size of 2096 due to a bug in the pxGrid certificate template

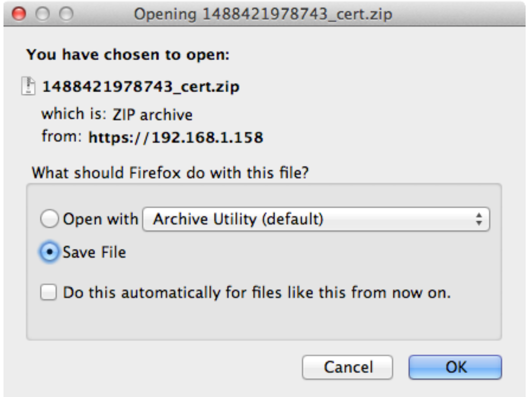


Generate pxGrid Certificates

I want to *	Generate a single certificate (without a certificate signing request)
Common Name (CN) *	smc.lab10.com
Description	Stealthwatch Management Console
Certificate Template	PxGrid_Certificate_Template
Subject Alternative Name (SAN)	IP address 192.168.1.245
Certificate Download Format *	Certificate in Privacy Enhanced Electronic Mail (PEM) format, key in PKCS8 PEM format (including certificate cha
Certificate Password *	••••••••
Confirm Password *	••••••••

Step 2 Select **Create**

Step 3 Download the zipped file locally, select **OK**



Opening 1488421978743_cert.zip

You have chosen to open:

1488421978743_cert.zip

which is: ZIP archive

from: https://192.168.1.158

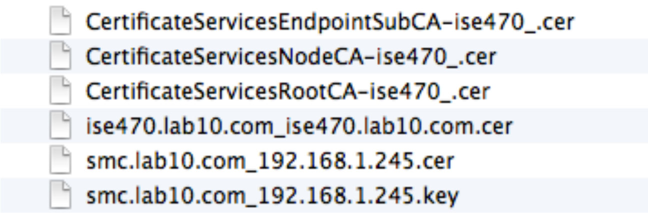
What should Firefox do with this file?

○ Open with Archive Utility (default)

● Save File

□ Do this automatically for files like this from now on.

Step 4 You should see the following files

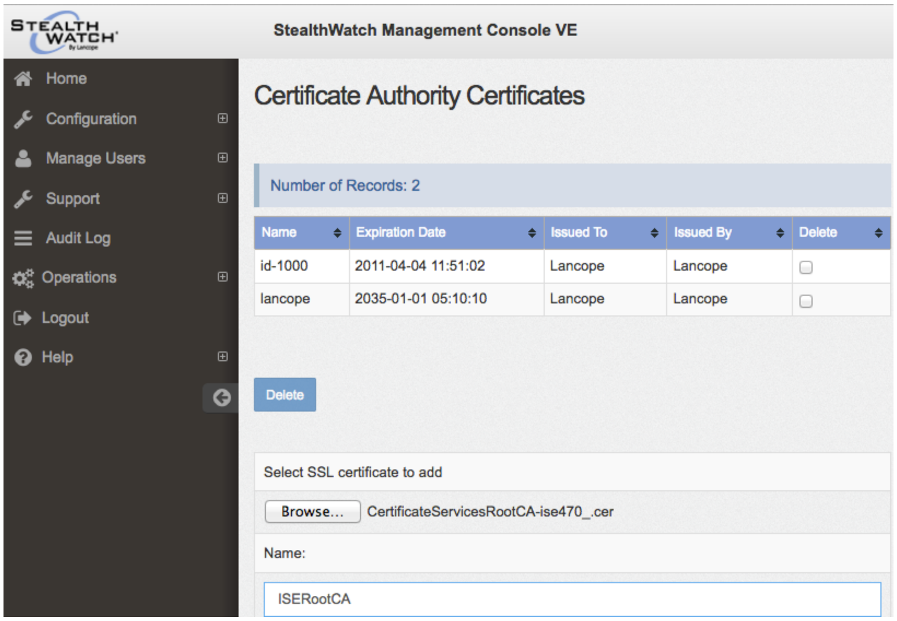


CertificateServicesEndpointSubCA-ise470_.cer
CertificateServicesNodeCA-ise470_.cer
CertificateServicesRootCA-ise470_.cer
ise470.lab10.com_ise470.lab10.com.cer
smc.lab10.com_192.168.1.245.cer
smc.lab10.com_192.168.1.245.key

Exporting ISE CertificateServicesRootCA into SMC Certificate Authority (CA) Store

Step 1 On the SMC, upload the CertificateServcicesRootCA-ise470.cer to the SMC CA Authority

Step 2 Select Gear ⚙ **->Administer Appliance->Configuration->Certificate Authority Certificates->Browse and upload the ISE certificate and provide a friendly name**



StealthWatch Management Console VE

Certificate Authority Certificates

Number of Records: 2

Name	Expiration Date	Issued To	Issued By	Delete
id-1000	2011-04-04 11:51:02	Lancope	Lancope	□
lancope	2035-01-01 05:10:10	Lancope	Lancope	□

Delete

Select SSL certificate to add

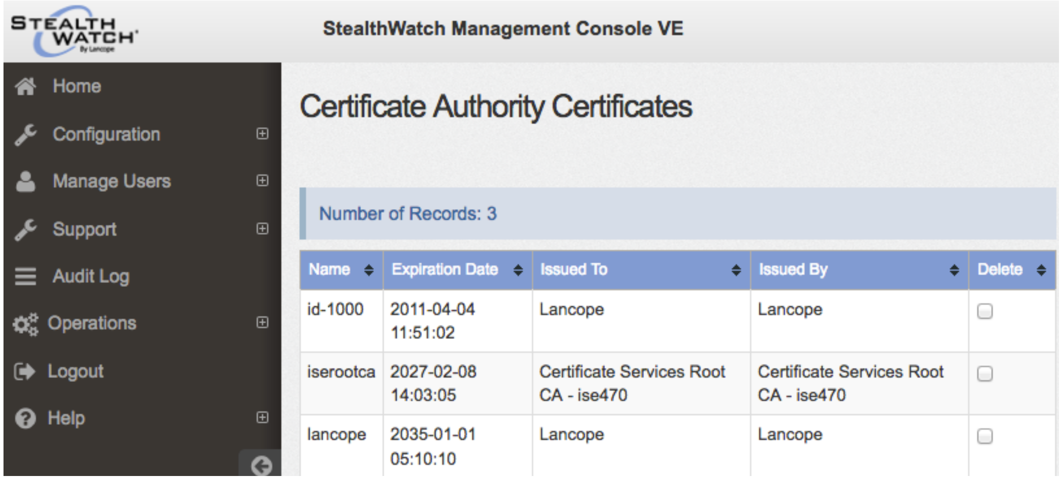
Browse... CertificateServicesRootCA-ise470_.cer

Name:

ISERootCA

Step 3 Select **Add Certificate** and confirm

Step 4 You should see that the ISE CA root certificate was successfully uploaded.



StealthWatch Management Console VE

Certificate Authority Certificates

Number of Records: 3

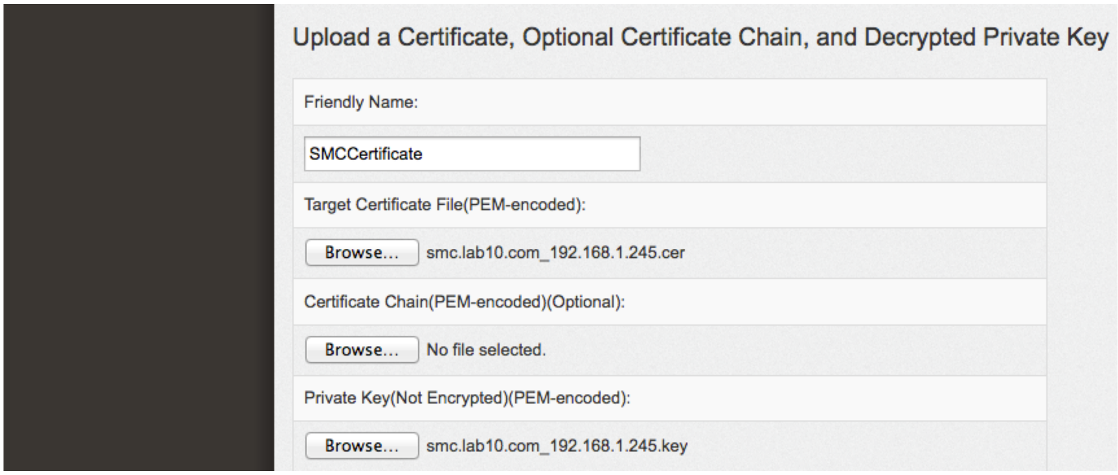
Name	Expiration Date	Issued To	Issued By	Delete
id-1000	2011-04-04 11:51:02	Lancope	Lancope	□
iserootca	2027-02-08 14:03:05	Certificate Services Root CA - ise470	Certificate Services Root CA - ise470	□
lancope	2035-01-01 05:10:10	Lancope	Lancope	□

Adding Stealthwatch certificate to SSL Client Identities Store

Step 1 Decrypt passphrase

```
cp smc.lab10.com_192.168.1.245.key smc.lab10.com_192.168.1.245.key.org
openssl rsa -in smc.lab10.com_192.168.1.245.key.org -out smc.lab10.com_192.168.1.245.key
Enter pass phrase for smc69.lab10.com_192.168.1.244.key.org: Cisco123
writing RSA key Cisco123
```

Step 2 Under SSL Client Identities, Upload a certificate, Optional certificate chain, and decrypted private key



Upload a Certificate, Optional Certificate Chain, and Decrypted Private Key

Friendly Name: SMCCertificate

Target Certificate File(PEM-encoded): Browse... smc.lab10.com_192.168.1.245.cer

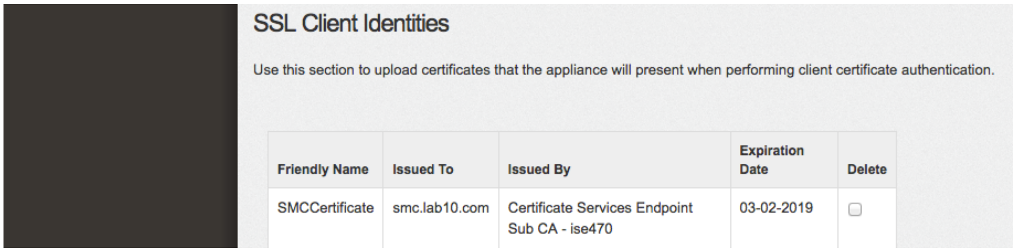
Certificate Chain(PEM-encoded)(Optional): Browse... No file selected.

Private Key(Not Encrypted)(PEM-encoded): Browse... smc.lab10.com_192.168.1.245.key

Step 3 Select **Upload Certificate** and confirm

Note: You may get an error message after you confirm, re-enter the values. This was tested on RC2 and may not be there In the productional release.

Step 4 You should see the following under SSL Client Identities

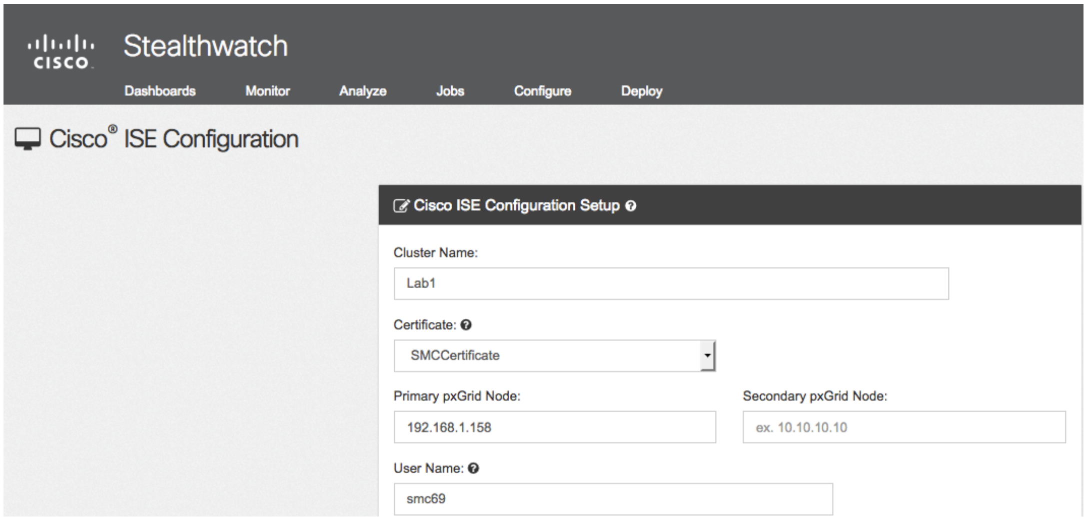


SSL Client Identities

Use this section to upload certificates that the appliance will present when performing client certificate authentication.

Friendly Name	Issued To	Issued By	Expiration Date	Delete
SMCCertificate	smc.lab10.com	Certificate Services Endpoint Sub CA - ise470	03-02-2019	□

Step 5 On the SMC Dashboard, select **Deploy->Cisco ISE Configuration**, and enter the following:



Cluster Name: Lab1

Certificate: SMCCertificate

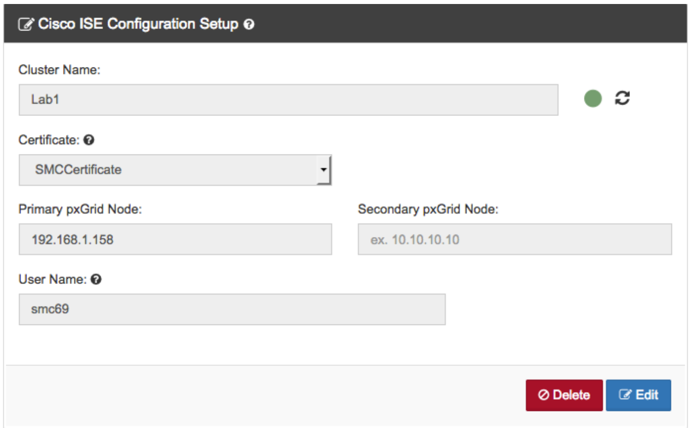
Primary pxGrid Node: 192.168.1.158

Secondary pxGrid Node: ex. 10.10.10.10

User Name: smc69

Step 6 Select **Save**

Step 7 You should see the configuration saved successfully and the status updated successfully by the green dot



Cluster Name: Lab1 ●

Certificate: SMCCertificate

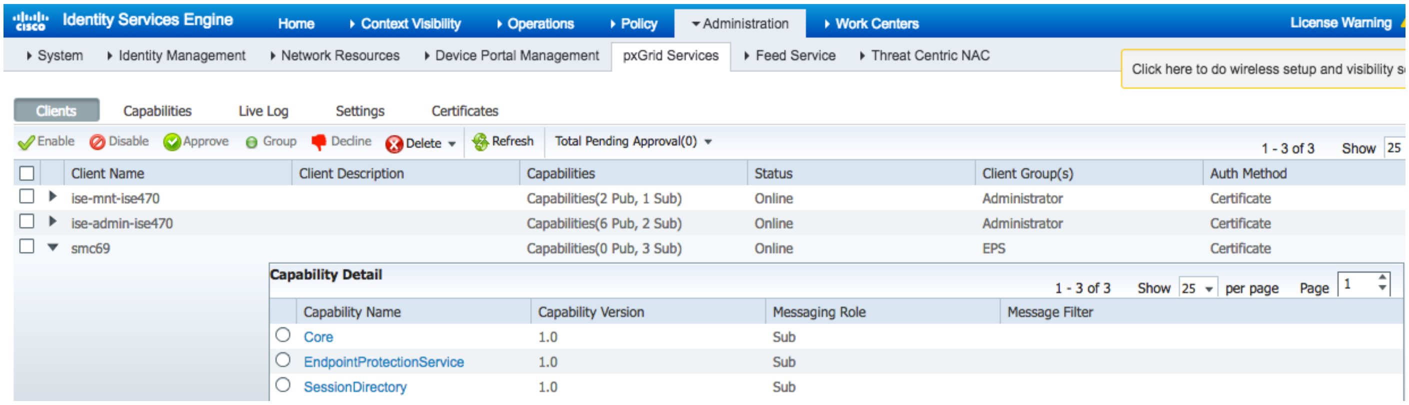
Primary pxGrid Node: 192.168.1.158

Secondary pxGrid Node: ex. 10.10.10.10

User Name: smc69

Testing Verifying the ISE published nodes appear

Step 1 In ISE, select **Administration->pxGrid Services**



	Client Name	Client Description	Capabilities	Status	Client Group(s)	Auth Method
□	ise-mnt-ise470		Capabilities(2 Pub, 1 Sub)	Online	Administrator	Certificate
□	ise-admin-ise470		Capabilities(6 Pub, 2 Sub)	Online	Administrator	Certificate
□	smc69		Capabilities(0 Pub, 3 Sub)	Online	EPS	Certificate

Capability Detail

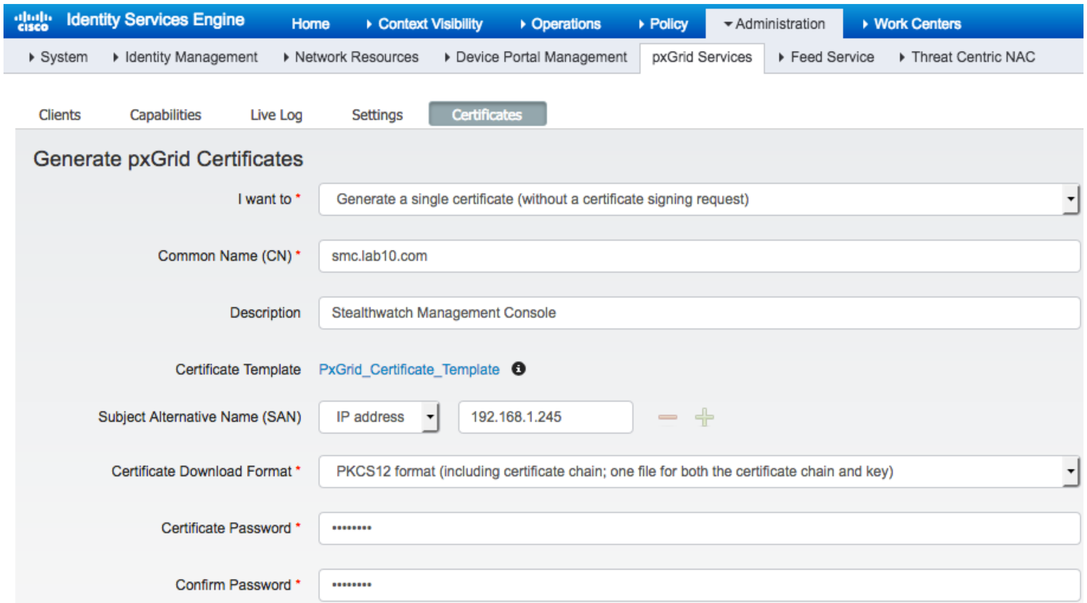
1 - 3 of 3 Show 25 per page Page 1

	Capability Name	Capability Version	Messaging Role	Message Filter
○	Core	1.0	Sub	
○	EndpointProtectionService	1.0	Sub	
○	SessionDirectory	1.0	Sub	

Generating Stealthwatch Certificate Signing Request (CSR) using PKCS12 format

Step 1 Select **Administration->pxGrid Services->Certificates,** and enter the information below:

Note: You can only generate a key size of 2096 due to a bug in the pxGrid template

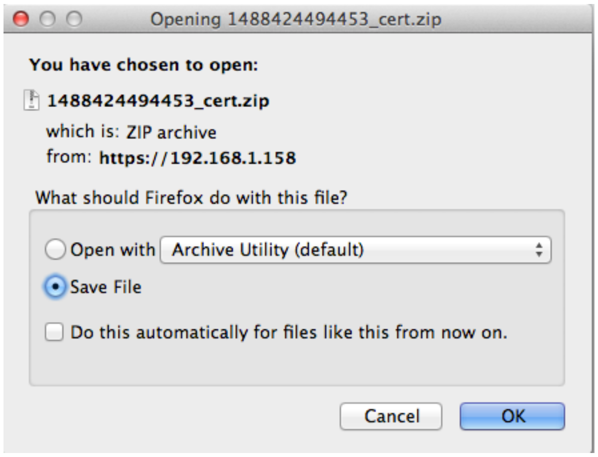


Generate pxGrid Certificates

I want to *	Generate a single certificate (without a certificate signing request)
Common Name (CN) *	smc.lab10.com
Description	Stealthwatch Management Console
Certificate Template	PxGrid_Certificate_Template
Subject Alternative Name (SAN)	IP address 192.168.1.245
Certificate Download Format *	PKCS12 format (including certificate chain; one file for both the certificate chain and key)
Certificate Password *	••••••••
Confirm Password *	••••••••

Step 2 Select **Create**

Step 3 Save the zipped file locally


Opening 1488424494453_cert.zip

You have chosen to open:

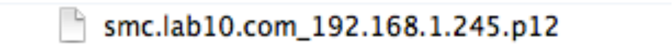
1488424494453_cert.zip

which is: ZIP archive
from: **https://192.168.1.158**

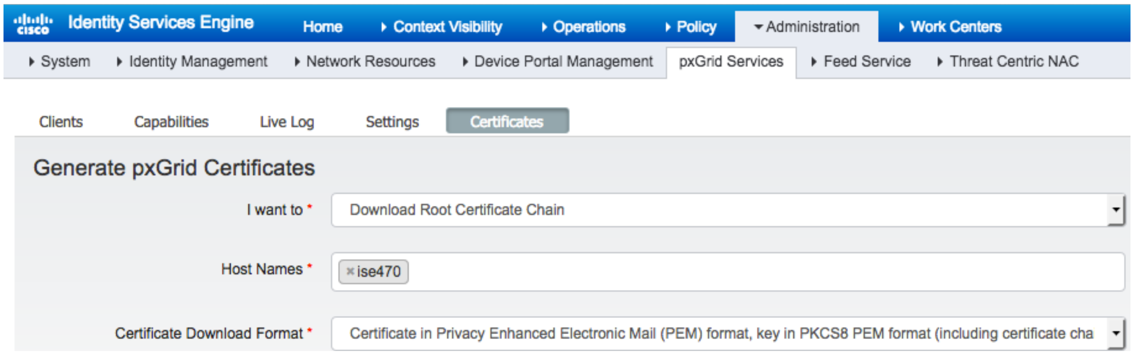
What should Firefox do with this file?

○ Open with Archive Utility (default)
● Save File
□ Do this automatically for files like this from now on.

Step 4 You should see the following


smc.lab10.com_192.168.1.245.p12

Step 5 Download the root certificate chain
Select **Administration->pxGrid Services->Certificates->select the ISE pxGrid hostname and PEM format**



Generate pxGrid Certificates

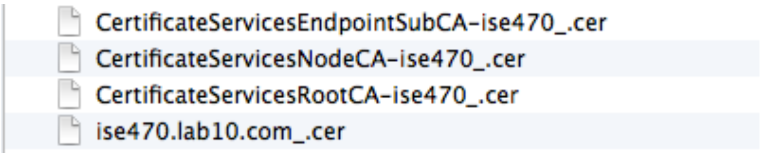
I want to * Download Root Certificate Chain

Host Names * ×ise470

Certificate Download Format * Certificate in Privacy Enhanced Electronic Mail (PEM) format, key in PKCS8 PEM format (including certificate cha

Step 6 Select **Create**

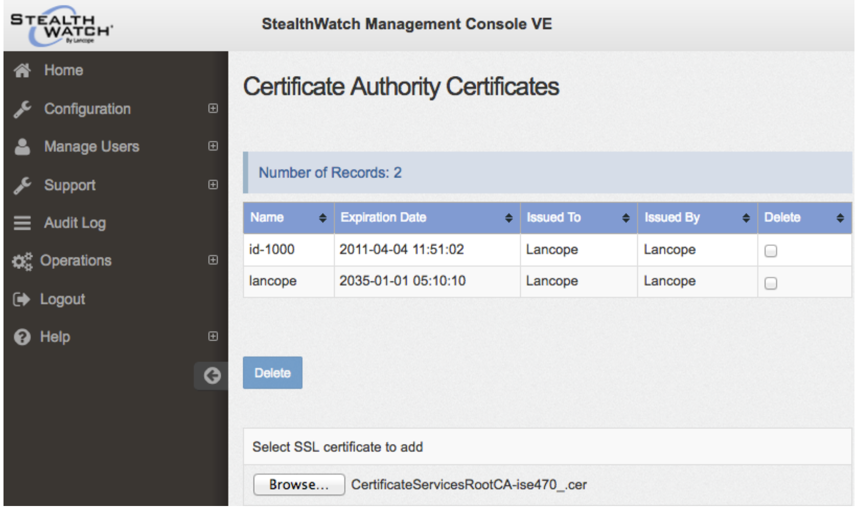
Step 7 Save the zipped file locally, you should see the following files:



CertificateServicesEndpointSubCA-ise470_.cer
CertificateServicesNodeCA-ise470_.cer
CertificateServicesRootCA-ise470_.cer
ise470.lab10.com_.cer

Importing ISE CertificateServicesRootCA into Stealthwatch CA store

Step 1 Upload the CertificatesServicesRootCA certificate to the Stealthwatch CA Authority
Select Gear ⚙ **->Administer Appliance->Configuration->Certificate Authority Certificates->Browse and upload the ISE certificate and provide a friendly name**



Certificate Authority Certificates

Number of Records: 2

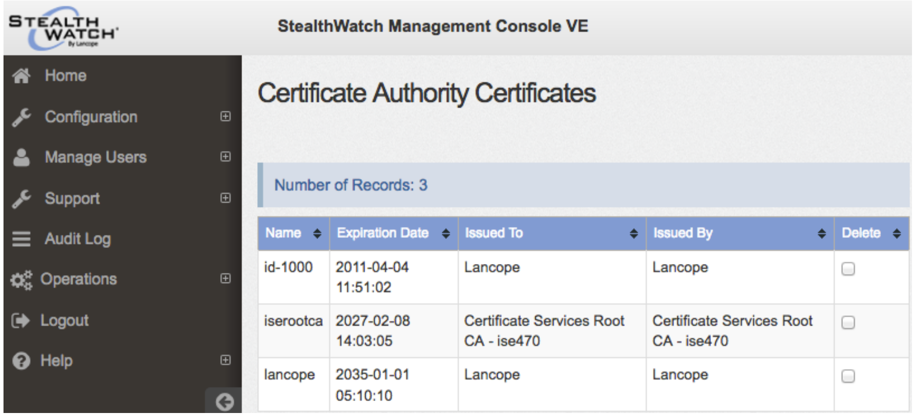
Name	Expiration Date	Issued To	Issued By	Delete
id-1000	2011-04-04 11:51:02	Lancope	Lancope	□
lancope	2035-01-01 05:10:10	Lancope	Lancope	□

Select SSL certificate to add

Browse... CertificateServicesRootCA-ise470_.cer

Step 2 Select **Add Certificate** and confirm

Step 3 You should see the following:



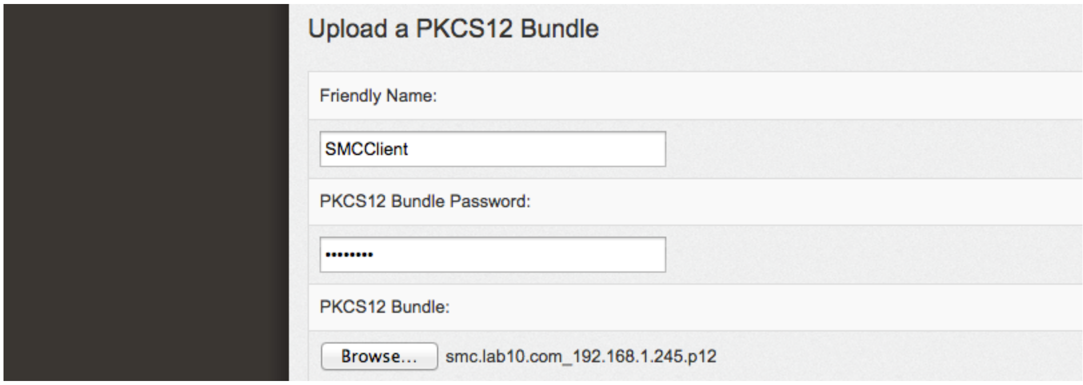
Certificate Authority Certificates

Number of Records: 3

Name	Expiration Date	Issued To	Issued By	Delete
id-1000	2011-04-04 11:51:02	Lancope	Lancope	☐
iserootca	2027-02-08 14:03:05	Certificate Services Root CA - ise470	Certificate Services Root CA - ise470	☐
lancope	2035-01-01 05:10:10	Lancope	Lancope	☐

Uploading Stealthwatch PKCS12 file

Step 1 Select **Configuration->SSL Certificate->SSL Certificates->SSL Client Identities->Upload a PKCS12 file**



Upload a PKCS12 Bundle

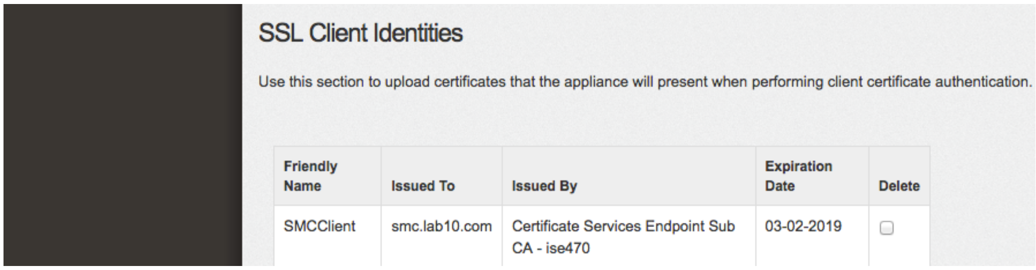
Friendly Name: SMCClient

PKCS12 Bundle Password: ••••••••

PKCS12 Bundle: Browse... smc.lab10.com_192.168.1.245.p12

Step 2 Select **Upload Bundle** and confirm

Step 3 You should see the following under SSL Client Identities

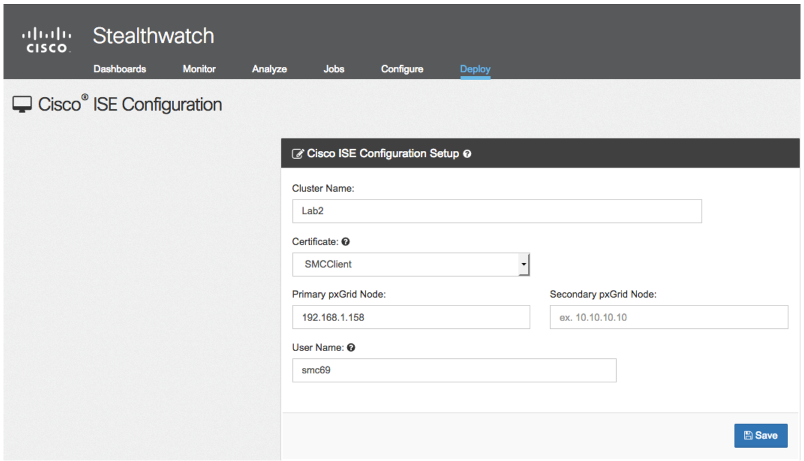


SSL Client Identities

Use this section to upload certificates that the appliance will present when performing client certificate authentication.

Friendly Name	Issued To	Issued By	Expiration Date	Delete
SMCClient	smc.lab10.com	Certificate Services Endpoint Sub CA - ise470	03-02-2019	☐

Step 4 From the Stealthwatch Management Center Dashboard, select **Deploy->Cisco ISE Configuration**



Cisco® ISE Configuration

Cisco ISE Configuration Setup

Cluster Name: Lab2

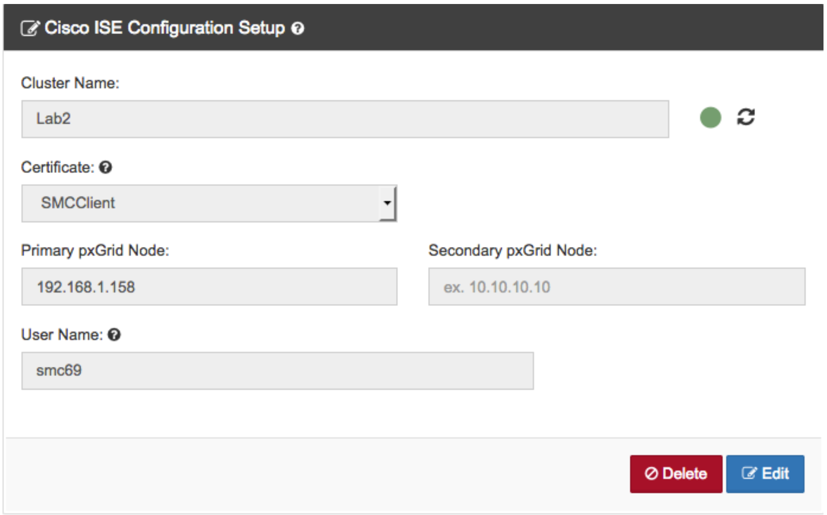
Certificate: SMCClient

Primary pxGrid Node: 192.168.1.158

Secondary pxGrid Node: ex. 10.10.10.10

User Name: smc69

Step 5 Select **Save** and **OK,** you should see a successful connection



Cisco ISE Configuration Setup

Cluster Name: Lab2

Certificate: SMCClient

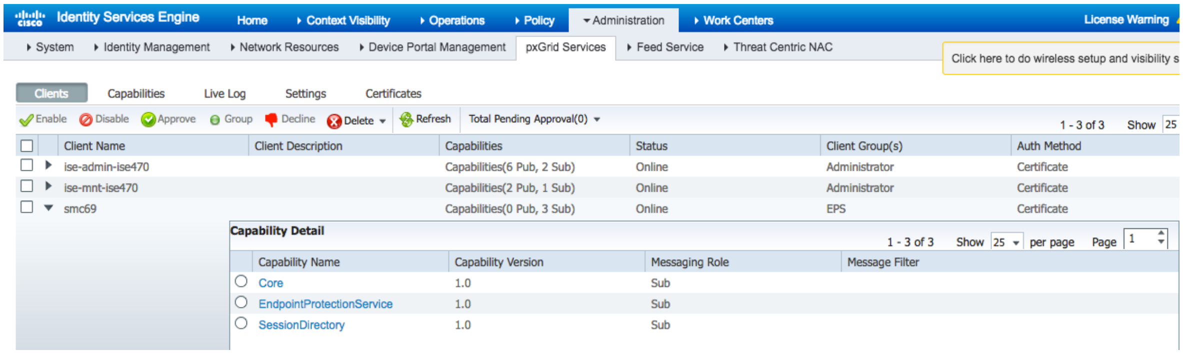
Primary pxGrid Node: 192.168.1.158

Secondary pxGrid Node: ex. 10.10.10.10

User Name: smc69

Testing Verifying the ISE published nodes appear

Step 1 On ISE, select **Administration->pxGrid Services**



Client Name	Client Description	Capabilities	Status	Client Group(s)	Auth Method
ise-admin-ise470		Capabilities(6 Pub, 2 Sub)	Online	Administrator	Certificate
ise-mnt-ise470		Capabilities(2 Pub, 1 Sub)	Online	Administrator	Certificate
smc69		Capabilities(0 Pub, 3 Sub)	Online	EPS	Certificate

Capability Detail

1 - 3 of 3 Show 25 per page Page 1

Capability Name	Capability Version	Messaging Role	Message Filter
Core	1.0	Sub	
EndpointProtectionService	1.0	Sub	
SessionDirectory	1.0	Sub	

Generating Stealthwatch Certificate Signing Request CSR (with certificate signing request)

Step 1 Generate the private key from the Stealthwatch Management Console

```
openssl genrsa -des3 -out smc.key 2048
Generating RSA private key, 2048 bit long modulus
.....................................................+++
.............................................................................................................
......................+++
e is 65537 (0x10001)
Enter pass phrase for smc69.key: Cisco123
Verifying - Enter pass phrase for smc.key: Cisco123
```

Step 2 Generate the Certificate Signing Request (CSR) from the Stealthwatch Management Console

```
openssl req -new -key smc.key -out smc.csr
Enter pass phrase for smc.key: Cisco123
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:US
State or Province Name (full name) [Some-State]:Maryland
Locality Name (eg, city) []:Germantown
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Cisco
Organizational Unit Name (eg, section) []:Engineering
Common Name (e.g. server FQDN or YOUR name) []:smc.lab10.com
Email Address []:j@cisco.com

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

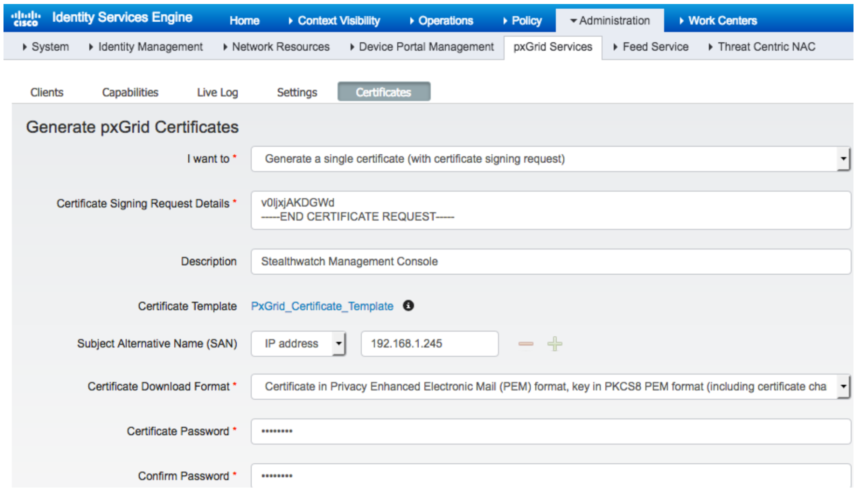
Step 3 Copy files locally

```
scp smc69.key jeppich@192.168.1.13:/Applications/smc69/smc1
RSA key fingerprint is 10:ce:54:b6:20:8b:3f:86:b1:5f:29:bb:d0:6a:a8:ab.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.1.13' (RSA) to the list of known hosts.
Password:
smc69.key                                     100% 1751     1.7KB/s   00:00
scp smc69.csr jeppich@192.168.1.13:/Applications/smc69/smc1
Password:yes
smc69.csr                                     100% 1058     1.0KB/s   00:00
```

ISE Generating Certificate based on CSR request in PEM format

Step 1 On ISE, select **Administration->pxGrid services,** and enter the following:

Note: You can only generate a key size of 2096; there is a bug in the pxGrid template

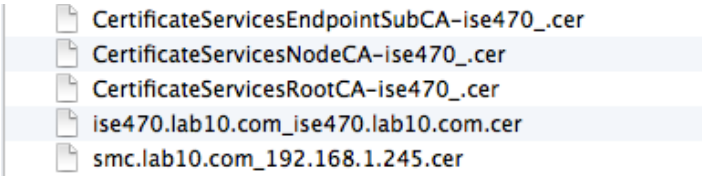


Generate pxGrid Certificates

I want to *	Generate a single certificate (with certificate signing request)
Certificate Signing Request Details *	v0ljxjAKDGWd -----END CERTIFICATE REQUEST-----
Description	Stealthwatch Management Console
Certificate Template	PxGrid_Certificate_Template
Subject Alternative Name (SAN)	IP address 192.168.1.245
Certificate Download Format *	Certificate in Privacy Enhanced Electronic Mail (PEM) format, key in PKCS8 PEM format (including certificate cha
Certificate Password *	••••••••
Confirm Password *	••••••••

Step 2 Select **Create**

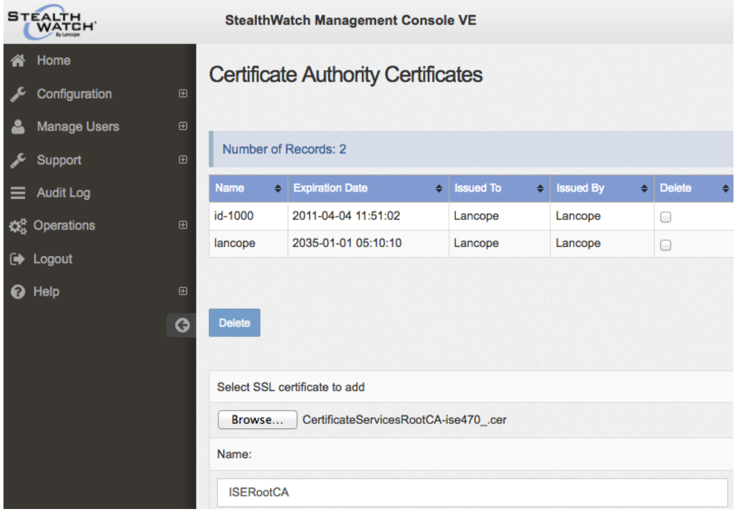
Step 3 Download the zipped file locally, you should see the following files



CertificateServicesEndpointSubCA-ise470_.cer
CertificateServicesNodeCA-ise470_.cer
CertificateServicesRootCA-ise470_.cer
ise470.lab10.com_ise470.lab10.com.cer
smc.lab10.com_192.168.1.245.cer

Import ISE CAServicesRoot certificate into Stealthwatch CA store

Step 1 On SMC, add root to CA authority



Certificate Authority Certificates

Number of Records: 2

Name	Expiration Date	Issued To	Issued By	Delete
id-1000	2011-04-04 11:51:02	Lancope	Lancope	□
lancope	2035-01-01 05:10:10	Lancope	Lancope	□

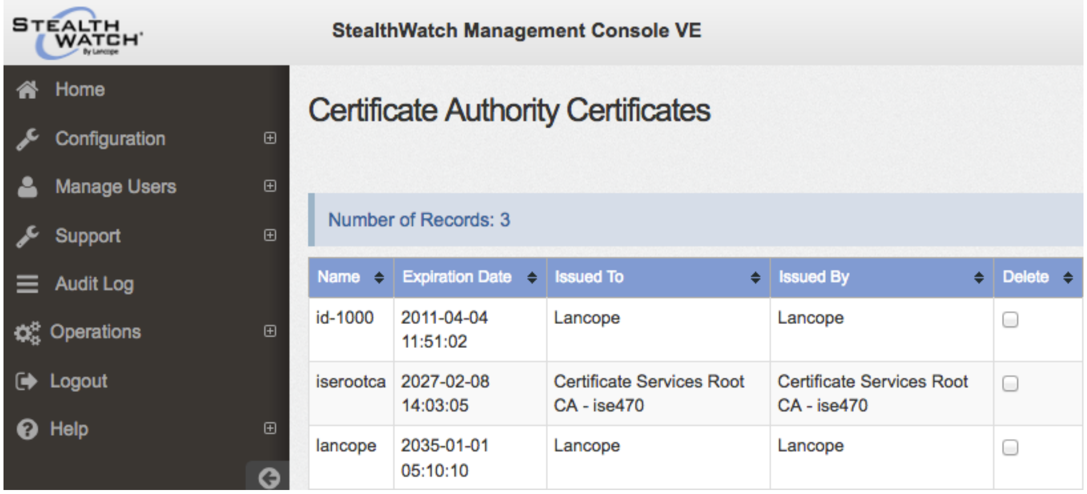
Select SSL certificate to add

Browse... CertificateServicesRootCA-ise470_.cer

Name: ISERootCA

Step 2 Select **Add Certificate and confirm**

Step 3 You should see the following:



StealthWatch Management Console VE

Certificate Authority Certificates

Number of Records: 3

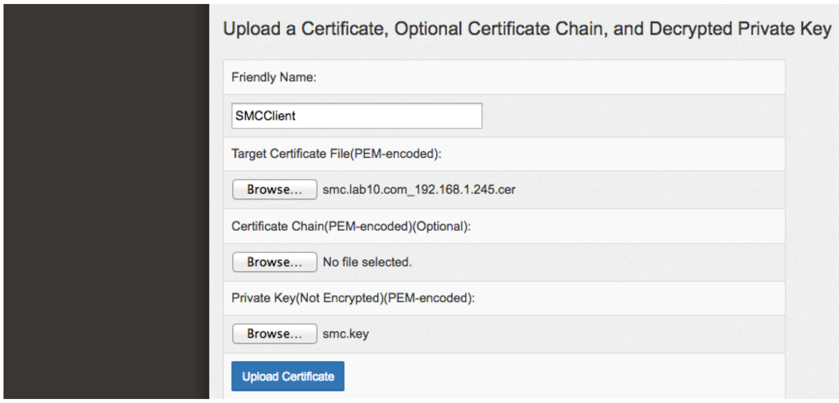
Name	Expiration Date	Issued To	Issued By	Delete
id-1000	2011-04-04 11:51:02	Lancope	Lancope	□
iserootca	2027-02-08 14:03:05	Certificate Services Root CA - ise470	Certificate Services Root CA - ise470	□
lancope	2035-01-01 05:10:10	Lancope	Lancope	□

Import Stealthwatch certificates into SSL Client Store

Step 1 Decrypt password

```
cp smc.key smc.key.org
openssl rsa -in smc.key.org -out smc.key
Enter pass phrase for smc69.key.org: Cisco123
writing RSA key
```

Step 2 Select **Configuration->SSL Certificate->SSL Client Identities->Upload the Stealthwatch public private-key pair**



Upload a Certificate, Optional Certificate Chain, and Decrypted Private Key

Friendly Name: SMCClient

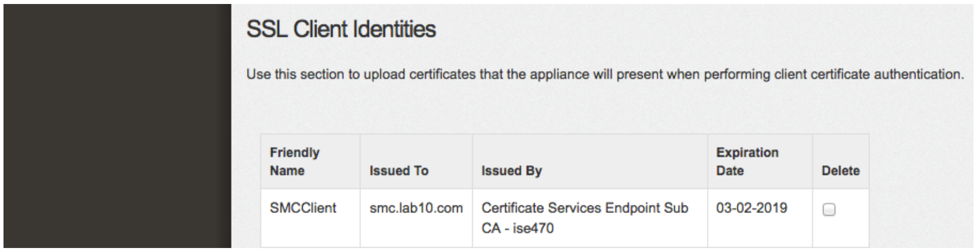
Target Certificate File(PEM-encoded): Browse... smc.lab10.com_192.168.1.245.cer

Certificate Chain(PEM-encoded)(Optional): Browse... No file selected.

Private Key(Not Encrypted)(PEM-encoded): Browse... smc.key

Step 3 Select **Upload Certificate and confirm**

Step 4 You should see the following under SSL Client Identities

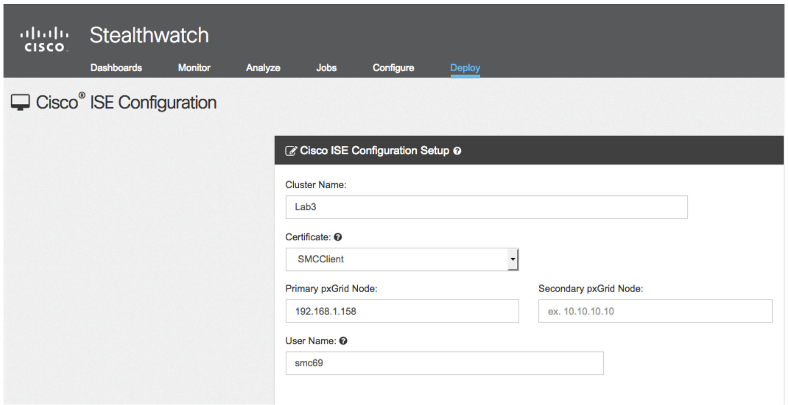


SSL Client Identities

Use this section to upload certificates that the appliance will present when performing client certificate authentication.

Friendly Name	Issued To	Issued By	Expiration Date	Delete
SMCClient	smc.lab10.com	Certificate Services Endpoint Sub CA - ise470	03-02-2019	□

Step 5 On the SMC Dashboard, select **Deploy->Cisco ISE Configuration** and configure pxGrid



Cisco® ISE Configuration

Cisco ISE Configuration Setup

Cluster Name: Lab3

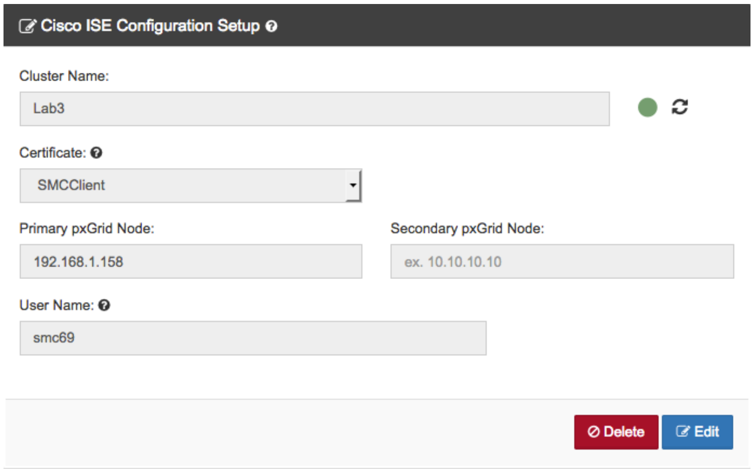
Certificate: SMCClient

Primary pxGrid Node: 192.168.1.158

Secondary pxGrid Node: ex. 10.10.10.10

User Name: smc69

Step 6 Select Save and OK, you should see a successful connection



Cisco ISE Configuration Setup

Cluster Name: Lab3 ●

Certificate: SMCClient

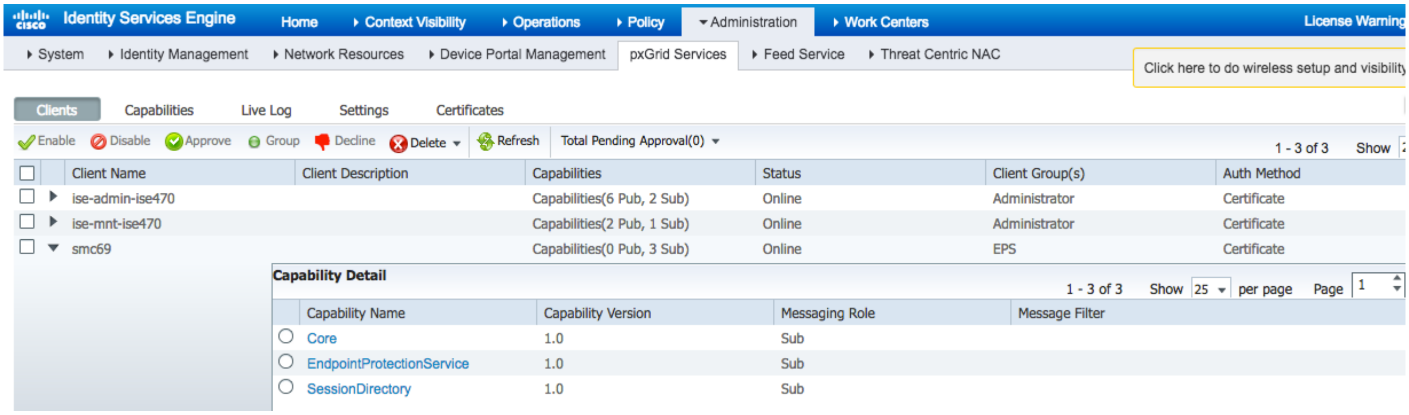
Primary pxGrid Node: 192.168.1.158

Secondary pxGrid Node: ex. 10.10.10.10

User Name: smc69

Testing Verifying the ISE published nodes appear

Step 1 In ISE, select **Administration->pxGrid services**, you should see the SMC successfully registered and subscribed to the ISE pxGrid node



□		Client Name	Client Description	Capabilities	Status	Client Group(s)	Auth Method
□	▶	ise-admin-ise470		Capabilities(6 Pub, 2 Sub)	Online	Administrator	Certificate
□	▶	ise-mnt-ise470		Capabilities(2 Pub, 1 Sub)	Online	Administrator	Certificate
□	▼	smc69		Capabilities(0 Pub, 3 Sub)	Online	EPS	Certificate

Capability Detail

1 - 3 of 3 Show 25 per page Page 1

	Capability Name	Capability Version	Messaging Role	Message Filter
○	Core	1.0	Sub	
○	EndpointProtectionService	1.0	Sub	
○	SessionDirectory	1.0	Sub	

References

How to: Splunk and ISE pxGrid Adaptive Network Control (ANC) Mitigation Workflow Actions https://communities.cisco.com/docs/DOC-68289

Deploying Cisco Stealthwatch 6.9 with Cisco Identity Services Engine (ISE) 2.2 using Cisco Platform Exchange Grid (pxGrid)

How To: Integrate Cisco WSA using ISE and TrustSec via pxGrid: https://communities.cisco.com/docs/DOC-68290