Deploying pxGrid in ISE Productional Environments

(version 2.0)

Author: John Eppich

Table of Contents

About this Document

This document is for Cisco System Engineers, partners and customers deploying Cisco Platform Exchange Grid (pxGrid) across all versions of Cisco Identity Service Engine (ISE) in productional environments. An external Certificate Authority) Server is used for all ISE deployments. Starting with ISE 2.1 and above, there is an internal ISE CA server that can be used for pxGrid operation and pxGrid client certificate generation. In ISE 2.1 this optional, for ISE 2.2 releases and above the ISE internal CA is enabled for pxGrid operation and pxGrid client certificate generation by default. All ISE nodes are dedicated nodes, including the pxGrid primary and pxGrid secondary nodes. pxGrid failover is also covered in some of the examples, however all configurations encompass pxGrid failover.

This guide also addresses early ISE 1.3 and ISE 1.4 deployments.

The pxGrid client examples are covered mainly Cisco Stealthwatch 6.9+, Cisco Firepower 6.2, Cisco Web Security (WSA) Appliance (IOS 9.0+) and pxGrid clients using java keystores, which is mainly used by pxGrid ecosystem partners.

This document does not cover self-signed certificates, it also does not cover configurations using the ISE internal and ISE identity certificate only. If providing proof of concept for these configurations, please consult the appropriate How-to guides in the References section.

Deploy pxGrid using ISE 2.2+

This section describes the details for deploying pxGrid using the ISE Internal Certificate Authority (CA) and using an external CA server for ISE node deployments. This covers ISE versions 2.2 and above.

The pxGrid certificate is signed by the ISE internal CA by default.

In the following example, dedicates nodes were used for the primary and secondary pxGrid nodes. In addition, dedicated nodes were used for the primary admin node, secondary admin node, primary MNT, secondary MNT and PSN node.

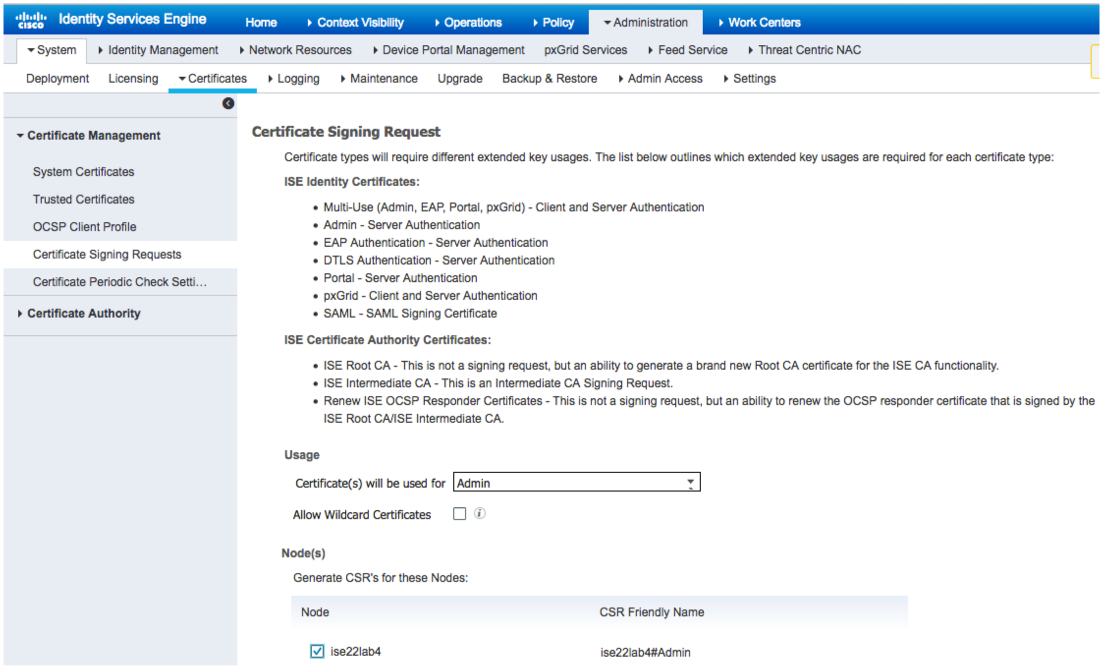
Note: If you upgraded from an earlier of ISE 1.3 or later to ISE 2.2. The ISE 2.2 Internal CA will not sign the pxGrid certificates; the pxGrid certificate will be signed by the external CA.

Generating CSR requests for ISE nodes

The desired ISE nodes: Primary Admin, Secondary Admin, Primary MNT, Secondary MNT, Policy Services Node(s) and the primary pxGrid and secondary pxGrid nodes will be signed by the External CA server using the Web Server template if using Microsoft 2008 Enterprise CA server. The Certificate Signing Request (CSR) request will use the "admin" usage for creating the certificate request.

Note: A customized pxGrid template is no longer required for the pxGrid nodes if the ISE internal CA is used in ISE 2.2+.

Step 1 Generate the Certificate Signing Request (CSR) for the desired ISE nodes. Below is an example for generating the CSR request for the desired ISE admin node.
Select **Administration->System->Certificate->Generate Certificate Signing Requests (CSR)->admin** for usage



Certificate Signing Request

Certificate types will require different extended key usages. The list below outlines which extended key usages are required for each certificate type:

ISE Identity Certificates:

- Multi-Use (Admin, EAP, Portal, pxGrid) - Client and Server Authentication
- Admin - Server Authentication
- EAP Authentication - Server Authentication
- DTLS Authentication - Server Authentication
- Portal - Server Authentication
- pxGrid - Client and Server Authentication
- SAML - SAML Signing Certificate

ISE Certificate Authority Certificates:

- ISE Root CA - This is not a signing request, but an ability to generate a brand new Root CA certificate for the ISE CA functionality.
- ISE Intermediate CA - This is an Intermediate CA Signing Request.
- Renew ISE OCSP Responder Certificates - This is not a signing request, but an ability to renew the OCSP responder certificate that is signed by the ISE Root CA/ISE Intermediate CA.

Usage

Certificate(s) will be used for: Admin

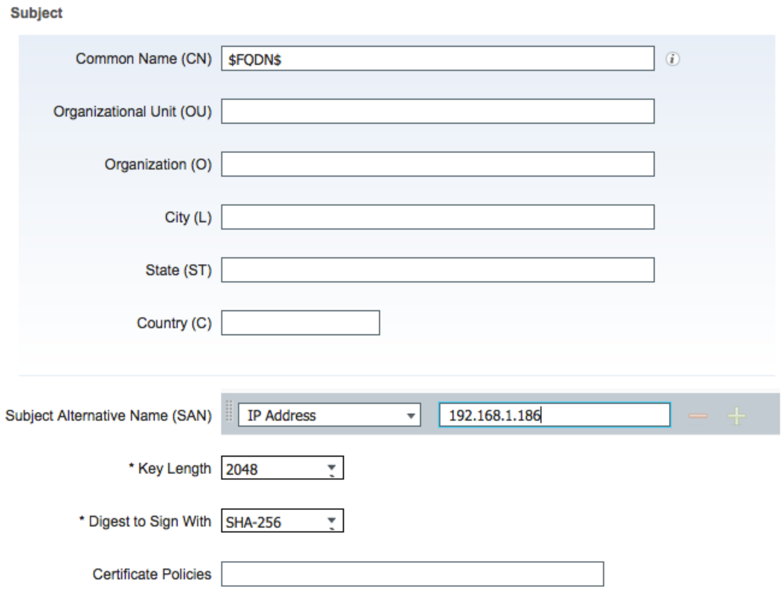
Allow Wildcard Certificates ☐

Node(s)

Generate CSR's for these Nodes:

Node	CSR Friendly Name
☑ ise22lab4	ise22lab4#Admin

Step 2 Enter the Fully Qualified Domain Name (FQDN) for DNS or enter the IP address



Subject

Common Name (CN): $FQDN$

Organizational Unit (OU):

Organization (O):

City (L):

State (ST):

Country (C):

Subject Alternative Name (SAN): IP Address 192.168.1.186

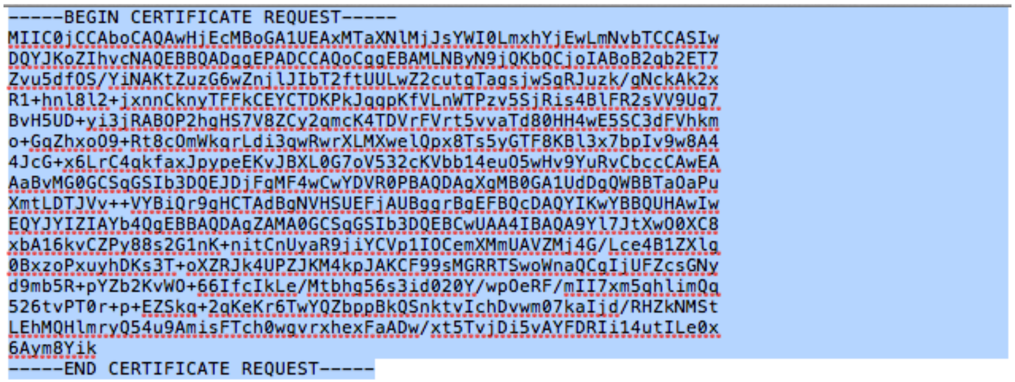
* Key Length: 2048

* Digest to Sign With: SHA-256

Certificate Policies:

Step 3 Select **Generate**

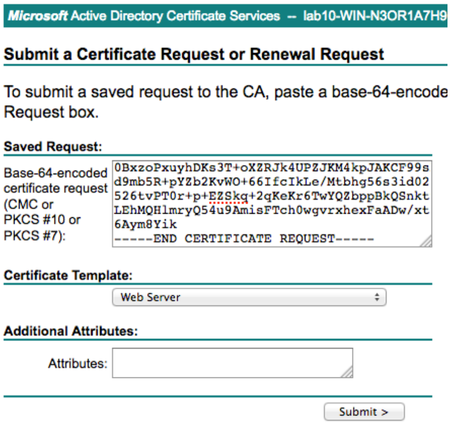
Step 4 Save the file locally, export and open the PEM file using text editor **copy** the text from the "-----BEGIN" to the end of "REQUEST-----"



```
-----BEGIN CERTIFICATE REQUEST-----
MIIC0jCCAboCAQAwHjEcMBoGA1UEAxMTaXNlMjJsYWI0LmxhYjEwLmNvbTCCASIw
DQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAMLNByN9jQKbQCjoIABoB2qb2ET7
Zvu5dfOS/YiNAKtZuzG6wZnjlJIbT2ftUULwZ2cutgTagsjwSgRJuzk/gNckAk2x
R1+hnl8l2+jxnnCknyTFFkCEYCTDKPkJqqpKfVLnWTPzv5SjRis4BlFR2sVV9Ug7
BvH5UD+yi3jRABOP2hgHS7V8ZCy2qmcK4TDVrFVrt5vvaTd80HH4wE5SC3dFVhkm
o+GqZhxoO9+Rt8cOmWkqrLdi3qwRwrXLMXwelQpx8Ts5yGTF8KBl3x7bpIv9w8A4
4JcG+x6LrC4qkfaxJpypeEKvJBXL0G7oV532cKVbb14euO5wHv9YuRvCbccCAwEA
AaBvMG0GCSqGSIb3DQEJDjFgMF4wCwYDVR0PBAQDAgXgMB0GA1UdDgQWBBTaOaPu
XmtLDTJVv++VYBiQr9gHCTAdBgNVHSUEFjAUBggrBgEFBQcDAQYIKwYBBQUHAwIw
EQYJYIZIAYb4QgEBBAQDAgZAMA0GCSqGSIb3DQEBCwUAA4IBAQA9Yl7JtXwO0XC8
xbA16kvCZPy88s2G1nK+nitCnUyaR9jiYCVp1IOCemXMmUAVZMj4G/Lce4B1ZXlg
0BxzoPxuyhDKs3T+oXZRJk4UPZJKM4kpJAKCF99sMGRRTSwoWnaQCgIjUFZcsGNy
d9mb5R+pYZb2KvWO+66IfcIkLe/Mtbhg56s3id020Y/wpOeRF/mII7xm5qhlimQq
526tvPT0r+p+EZSkq+2qKeKr6TwYQZbppBkQSnktvIchDvwm07kaIjd/RHZkNMSt
LEhMQHlmryQ54u9AmisFTch0wgvrxhexFaADw/xt5TvjDi5vAYFDRIi14utILe0x
6Aym8Yik
-----END CERTIFICATE REQUEST-----
```

Step 5 Paste into Advanced Request

Select **Request a Certificate->Advanced Certificate Request**



Microsoft Active Directory Certificate Services -- lab10-WIN-N3OR1A7H9

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encode
Request box.

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

```
0BxzoPxuyhDKs3T+oXZRJk4UPZJKM4kpJAKCF99s
d9mb5R+pYZb2KvWO+66IfcIkLe/Mtbhg56s3id02
526tvPT0r+p+EZSkq+2qKeKr6TwYQZbppBkQSnkt
LEhMQHlmryQ54u9AmisFTch0wgvrxhexFaADw/xt
6Aym8Yik
-----END CERTIFICATE REQUEST-----
```

Certificate Template:

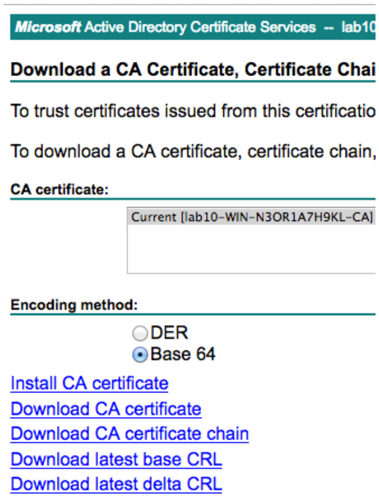
Web Server

Additional Attributes:

Attributes:

Step 6 Select **Submit** and download in 64-base encoded format

Step 7 Select **Download CA root certificate** in 64-base encoded format



Microsoft Active Directory Certificate Services -- lab10

Download a CA Certificate, Certificate Chai

To trust certificates issued from this certificatio

To download a CA certificate, certificate chain,

CA certificate:

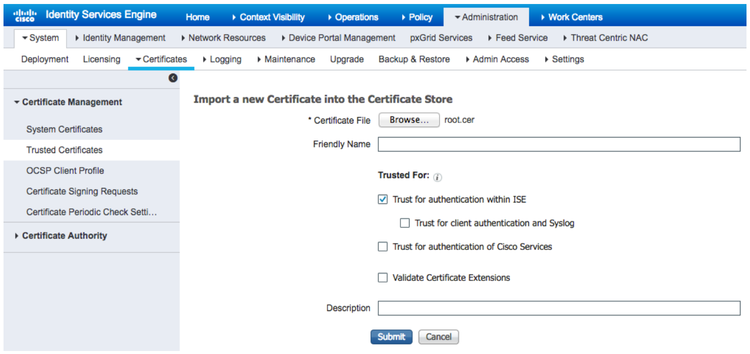
Current [lab10-WIN-N3OR1A7H9KL-CA]

Encoding method:

○ DER
● Base 64

Step 8 Upload the CA root certificate into the ISE trusted certificate store
Select **Administration->System->Certificates->Certificate Management->Trusted Certificates** and import the trusted CA root certificate

Note: Ensure trust for authentication within ISE is selected



Import a new Certificate into the Certificate Store

* Certificate File: Browse... root.cer

Friendly Name:

Trusted For:

☑ Trust for authentication within ISE

☐ Trust for client authentication and Syslog

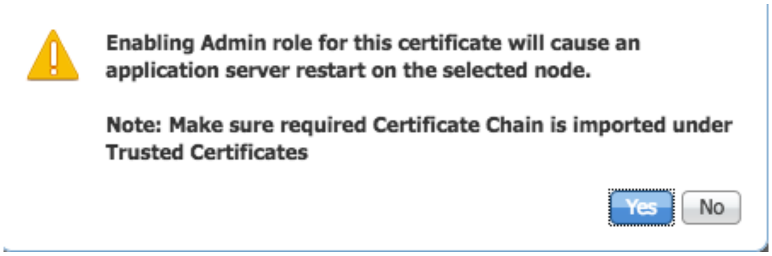
☐ Trust for authentication of Cisco Services

☐ Validate Certificate Extensions

Description:

Step 9 Select **Submit**

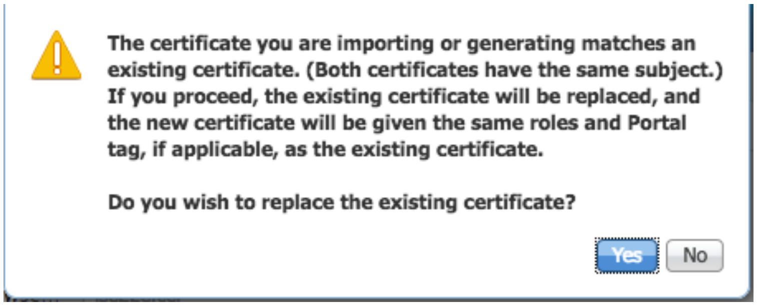
Step 10 Select **Yes**



Enabling Admin role for this certificate will cause an application server restart on the selected node.

Note: Make sure required Certificate Chain is imported under Trusted Certificates

Step 11 Select **Yes**



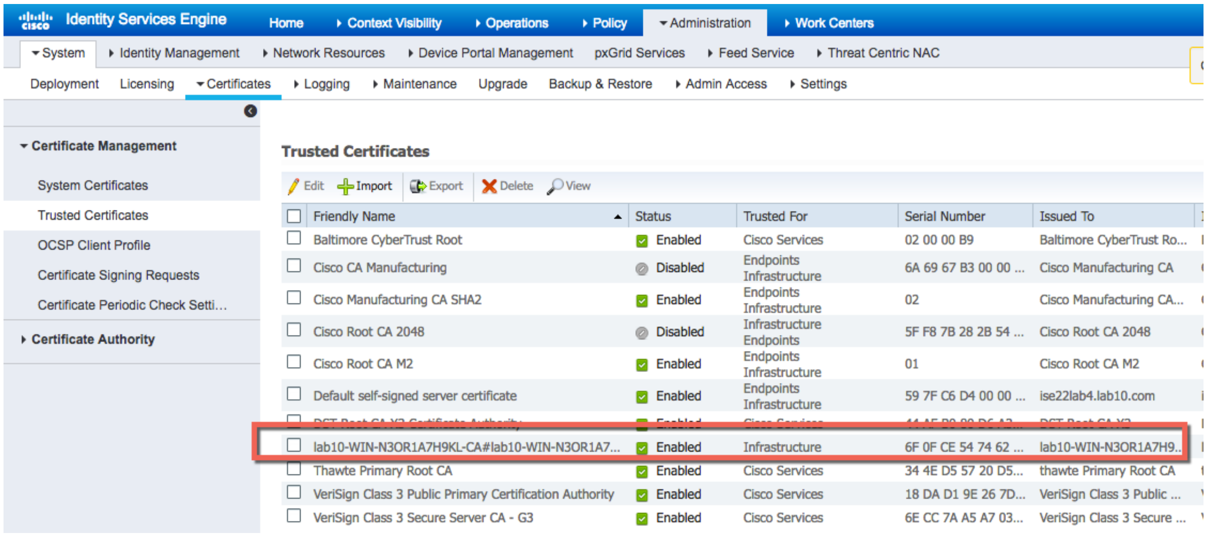
The certificate you are importing or generating matches an existing certificate. (Both certificates have the same subject.) If you proceed, the existing certificate will be replaced, and the new certificate will be given the same roles and Portal tag, if applicable, as the existing certificate.

Do you wish to replace the existing certificate?

Step 12 The system will restart

Step 13 You should see the uploaded root certificate

Select **Administration->System->Certificates->Certificate Management->Trusted Certificates**



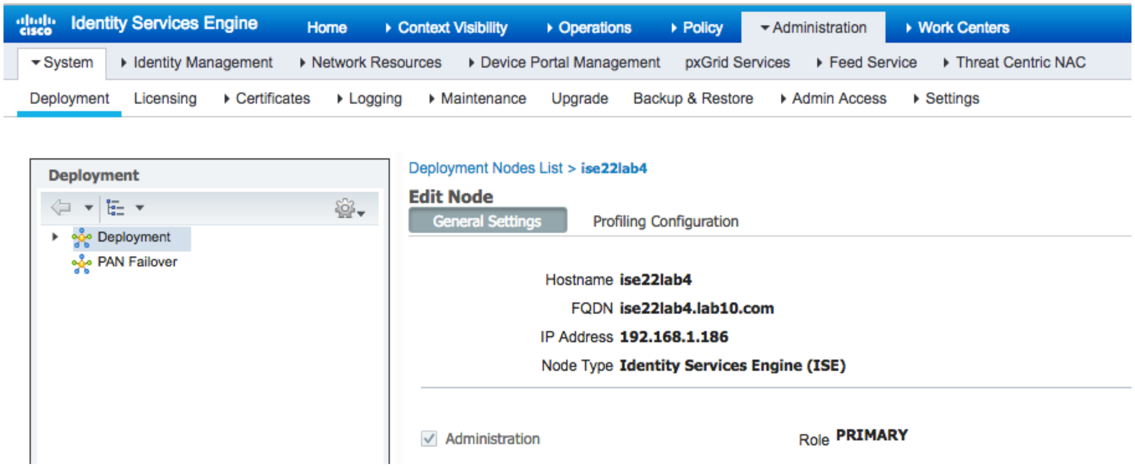
Trusted Certificates

□	Friendly Name	Status	Trusted For	Serial Number	Issued To
□	Baltimore CyberTrust Root	✓ Enabled	Cisco Services	02 00 00 B9	Baltimore CyberTrust Ro...
□	Cisco CA Manufacturing	⊘ Disabled	Endpoints Infrastructure	6A 69 67 B3 00 00 ...	Cisco Manufacturing CA
□	Cisco Manufacturing CA SHA2	✓ Enabled	Endpoints Infrastructure	02	Cisco Manufacturing CA...
□	Cisco Root CA 2048	⊘ Disabled	Infrastructure Endpoints	5F F8 7B 28 2B 54 ...	Cisco Root CA 2048
□	Cisco Root CA M2	✓ Enabled	Endpoints Infrastructure	01	Cisco Root CA M2
□	Default self-signed server certificate	✓ Enabled	Endpoints Infrastructure	59 7F C6 D4 00 00 ...	ise22lab4.lab10.com
□	DST Root CA X3 Certificate Authority	✓ Enabled	Cisco Services	44 AF B0 80 D6 A3 ...	DST Root CA X3
□	lab10-WIN-N3OR1A7H9KL-CA#lab10-WIN-N3OR1A7...	✓ Enabled	Infrastructure	6F 0F CE 54 74 62 ...	lab10-WIN-N3OR1A7H9...
□	Thawte Primary Root CA	✓ Enabled	Cisco Services	34 4E D5 57 20 D5...	thawte Primary Root CA
□	VeriSign Class 3 Public Primary Certification Authority	✓ Enabled	Cisco Services	18 DA D1 9E 26 7D...	VeriSign Class 3 Public ...
□	VeriSign Class 3 Secure Server CA - G3	✓ Enabled	Cisco Services	6E CC 7A A5 A7 03...	VeriSign Class 3 Secure ...

Step 14 Repeat steps 1-14 for all the ISE nodes including the pxGrid primary and pxGrid secondary nodes.

Registering ISE nodes

Step 1 Select the desired node designated for the primary admin node and promote to primary
Select **Administration->System->Deployment->select the node->Make primary**



Deployment Nodes List > ise22lab4

Edit Node

General Settings | Profiling Configuration

Hostname ise22lab4
FQDN ise22lab4.lab10.com
IP Address 192.168.1.186
Node Type Identity Services Engine (ISE)

☑ Administration Role PRIMARY

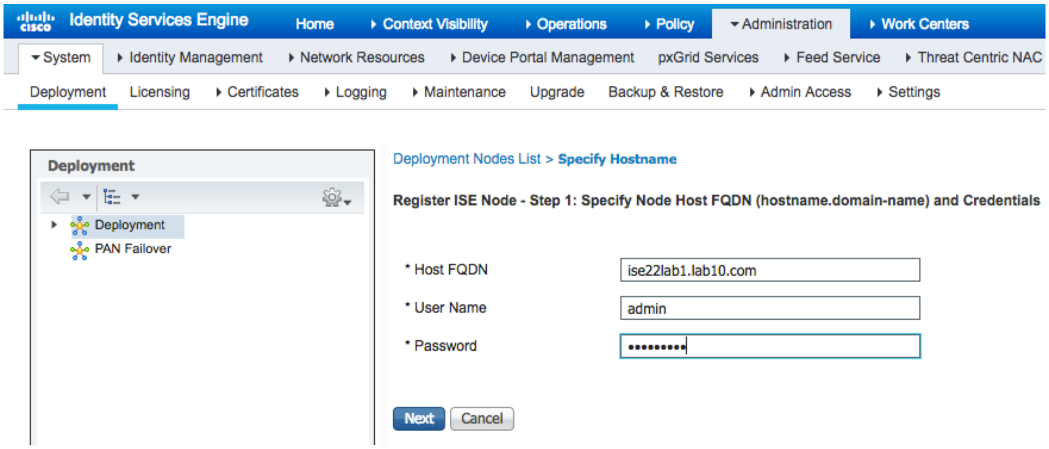
Step 2 **Uncheck** all the nodes, except for Administration and Monitoring (primary Role). This will become the primary admin node

Step 3 Select **Save.**
The node will be updated.

Note: Use “application status ise” from the ISE VM CLI to see the status of Application Server.

Step 4 Register the rest of the ISE nodes, and enable the appropriate personas.

Step 5 Below is an example of registering the primary MNT node.
Select **Administration->System->Deployment->Register->Register an ISE node**, select **Next**



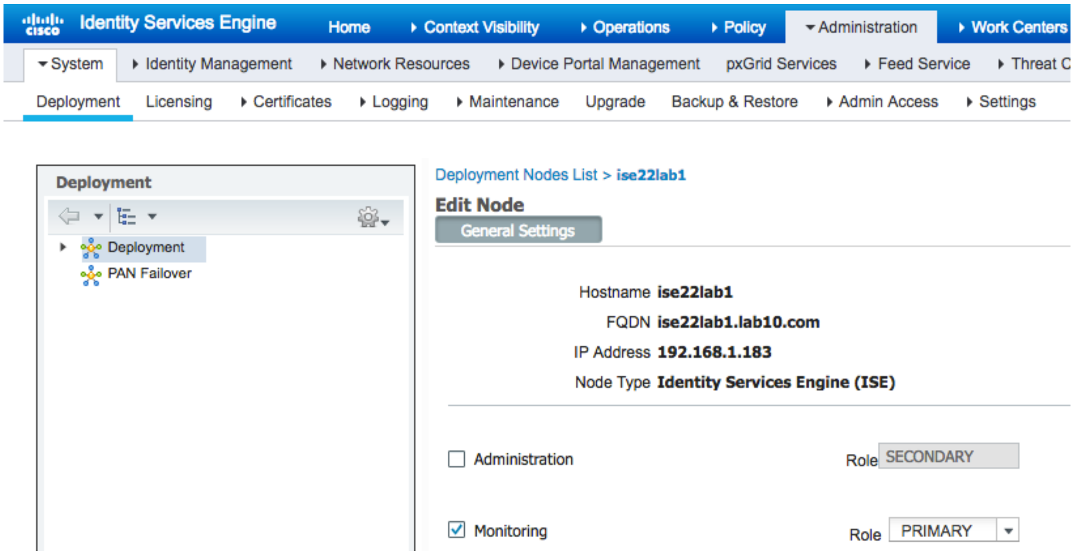
Deployment Nodes List > Specify Hostname

Register ISE Node - Step 1: Specify Node Host FQDN (hostname.domain-name) and Credentials

* Host FQDN ise22lab1.lab10.com
* User Name admin
* Password •••••••••

Step 6 Enable the **Monitoring** Persona and select the **Primary** Role

Note: When the Primary role is selected, the monitoring persona on the primary admin role will automatically change to the Secondary role.



Deployment Nodes List > ise22lab1

Edit Node

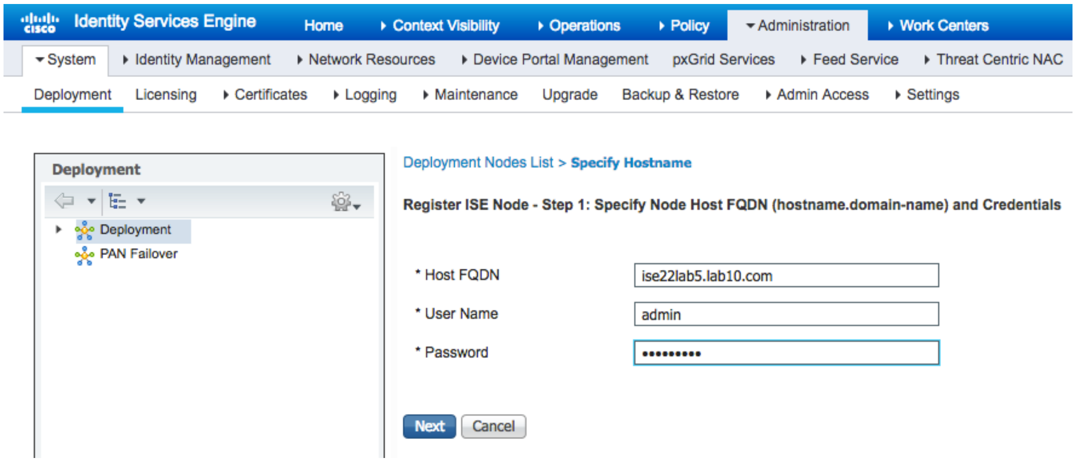
Hostname **ise22lab1**
FQDN **ise22lab1.lab10.com**
IP Address **192.168.1.183**
Node Type **Identity Services Engine (ISE)**

□ Administration Role SECONDARY

☑ Monitoring Role PRIMARY

Step 7 Select **Save**

Step 8 Below is an example of registering the primary pxGrid node.
Select **Administration->System->Deployment->Register->Register an ISE node**, select **Next**

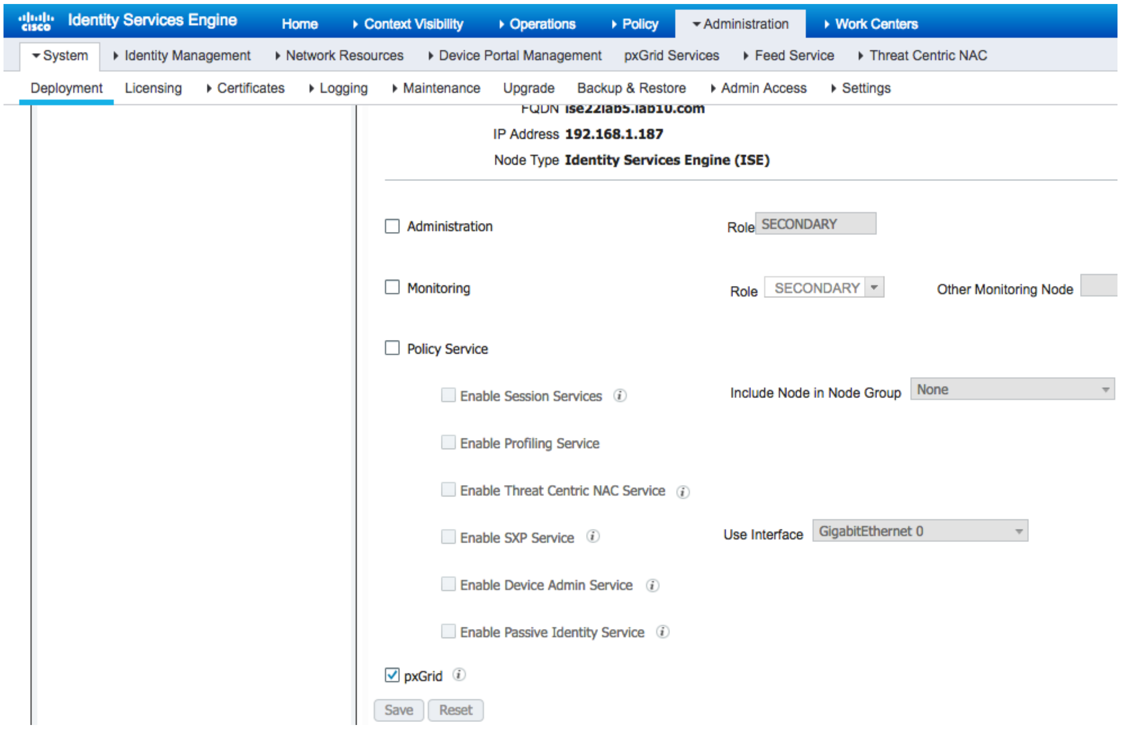


Deployment Nodes List > **Specify Hostname**

Register ISE Node - Step 1: Specify Node Host FQDN (hostname.domain-name) and Credentials

* Host FQDN ise22lab5.lab10.com
* User Name admin
* Password •••••••••

Step 9 Enable the **pxGrid** Persona



FQDN **ise22lab5.lab10.com**

IP Address **192.168.1.187**

Node Type **Identity Services Engine (ISE)**

□ Administration — Role SECONDARY

□ Monitoring — Role SECONDARY — Other Monitoring Node

□ Policy Service

- □ Enable Session Services — Include Node in Node Group None
- □ Enable Profiling Service
- □ Enable Threat Centric NAC Service
- □ Enable SXP Service — Use Interface GigabitEthernet 0
- □ Enable Device Admin Service
- □ Enable Passive Identity Service

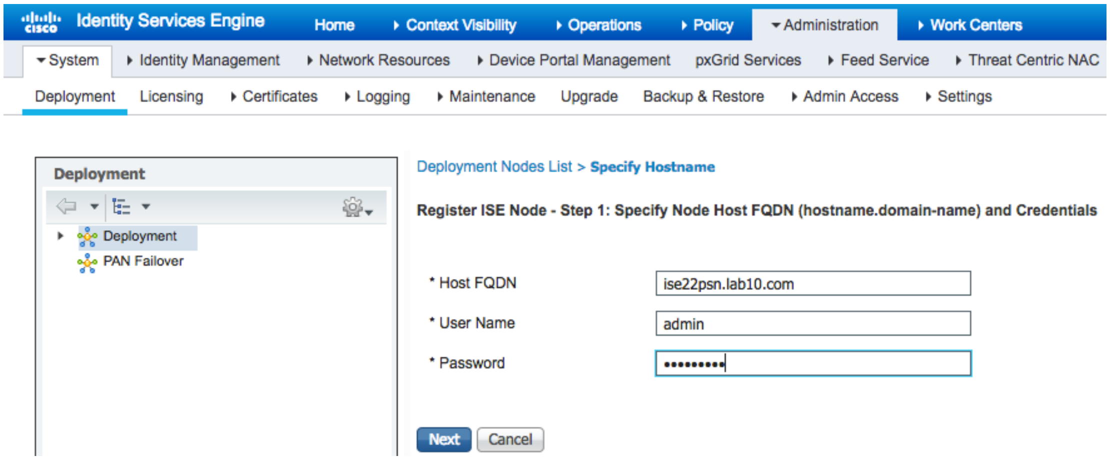
☑ pxGrid

Save Reset

Step 10 Select **Save**

Note: Verify that the published pxGrid nodes appear and there is pxGrid node connectivity. Select **Administration->pxGrid Services**

Step 11 Below is an example of registering the Policy Service Node (PSN) node.
Select **Administration->System->Deployment->Register->Register an ISE node**, select **Next**



Deployment Nodes List > **Specify Hostname**

Register ISE Node - Step 1: Specify Node Host FQDN (hostname.domain-name) and Credentials

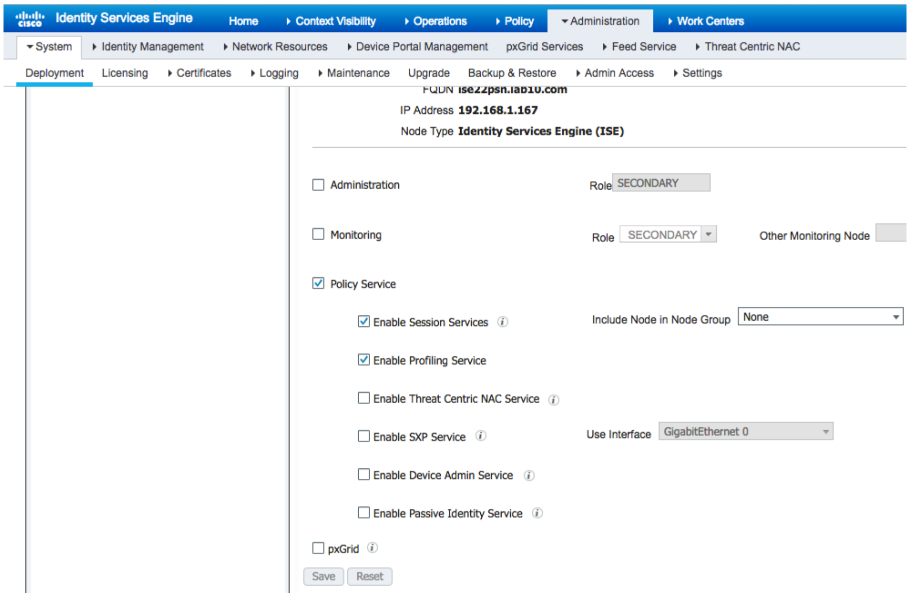
* Host FQDN ise22psn.lab10.com

* User Name admin

* Password •••••••••

Next Cancel

Step 12 Select **Police Service** persona



FQDN **ise22psn.lab10.com**
IP Address **192.168.1.167**
Node Type **Identity Services Engine (ISE)**

□ Administration Role SECONDARY

□ Monitoring Role SECONDARY Other Monitoring Node

☑ Policy Service

☑ Enable Session Services Include Node in Node Group None

☑ Enable Profiling Service

□ Enable Threat Centric NAC Service

□ Enable SXP Service Use Interface GigabitEthernet 0

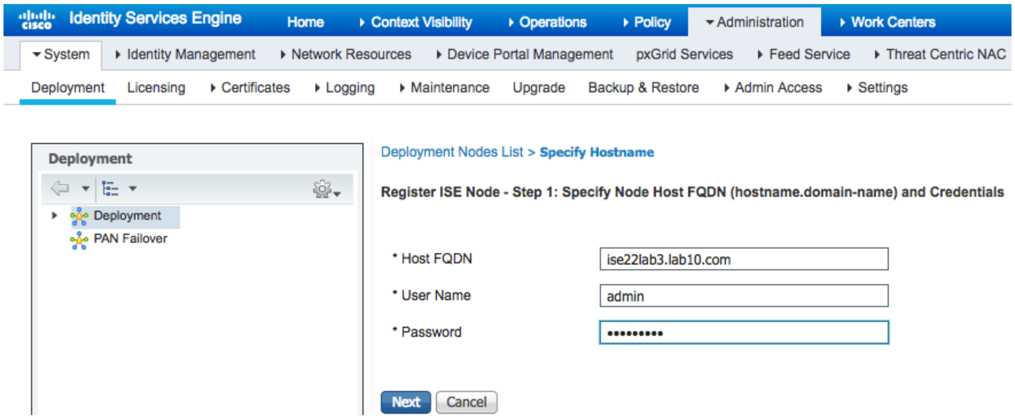
□ Enable Device Admin Service

□ Enable Passive Identity Service

□ pxGrid

Step 13 Select **Save**

Step 14 Below is an example of registering the secondary admin node.
Select **Administration->System->Deployment->Register->Register an ISE node**, select **Next**

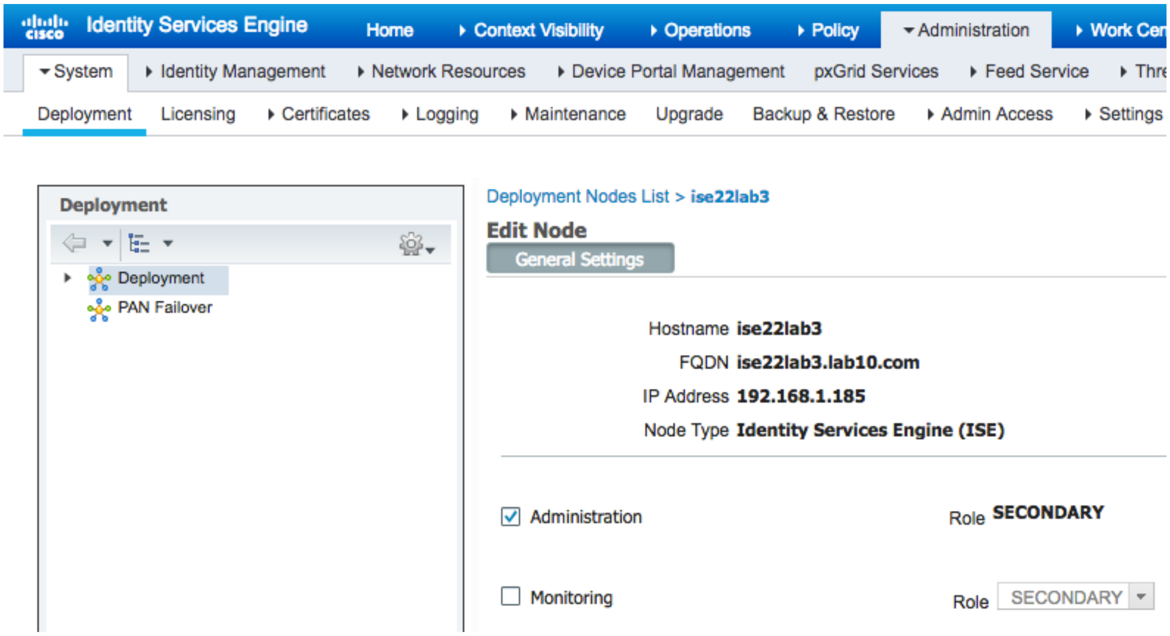


Deployment Nodes List > **Specify Hostname**

Register ISE Node - Step 1: Specify Node Host FQDN (hostname.domain-name) and Credentials

* Host FQDN ise22lab3.lab10.com
* User Name admin
* Password •••••••••

Step 15 Select **Administration** persona and the **Secondary** Role



Hostname ise22lab3
FQDN ise22lab3.lab10.com
IP Address 192.168.1.185
Node Type Identity Services Engine (ISE)

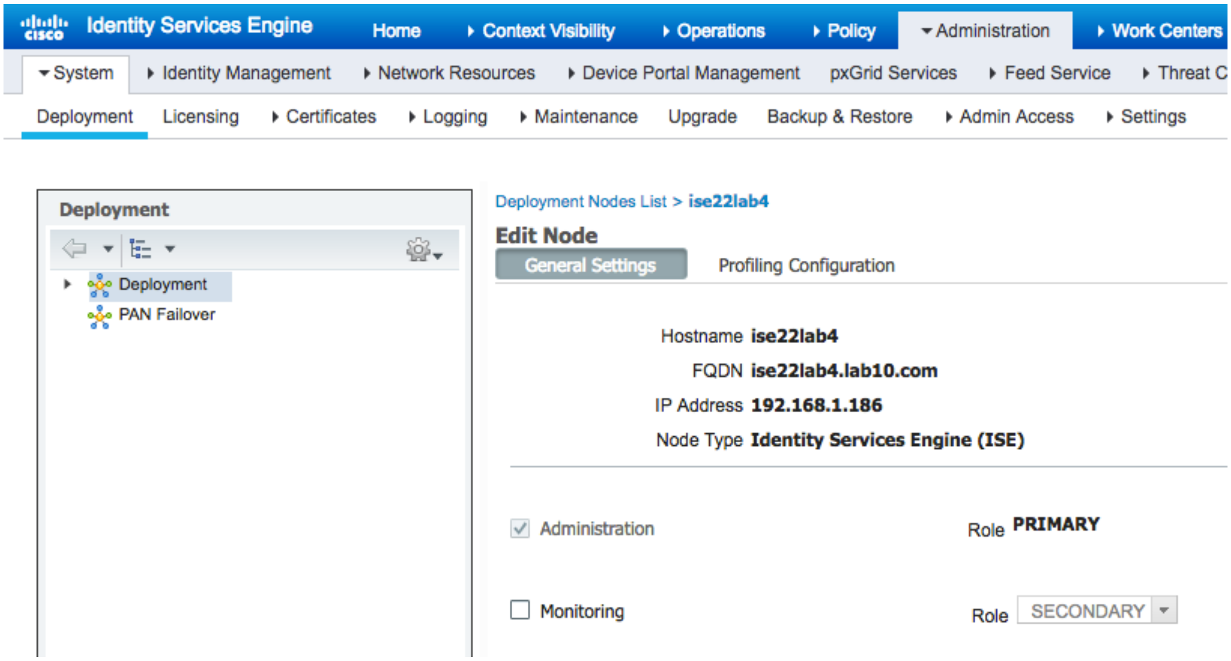
☑ Administration Role SECONDARY

□ Monitoring Role SECONDARY

Step 16 Select **Save**

Step 17 Disable the Secondary Monitoring role on the primary admin role

Select **Administration->System->Deployment->edit the primary admin role->uncheck Monitoring**



Hostname ise22lab4
FQDN ise22lab4.lab10.com
IP Address 192.168.1.186
Node Type Identity Services Engine (ISE)

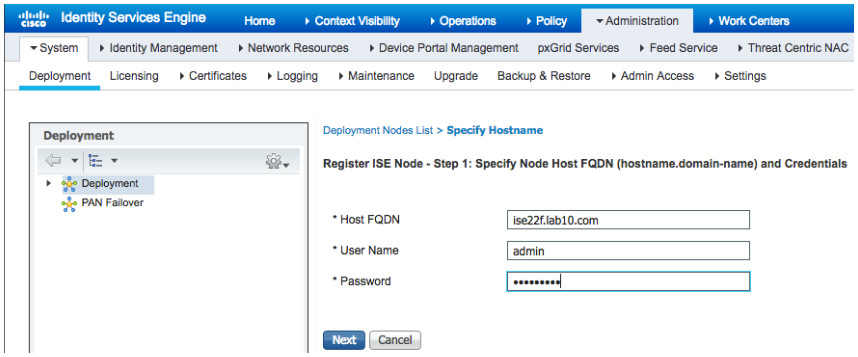
☑ Administration Role PRIMARY

□ Monitoring Role SECONDARY

Step 18 Select **Save.**

The primary admin role will restart.

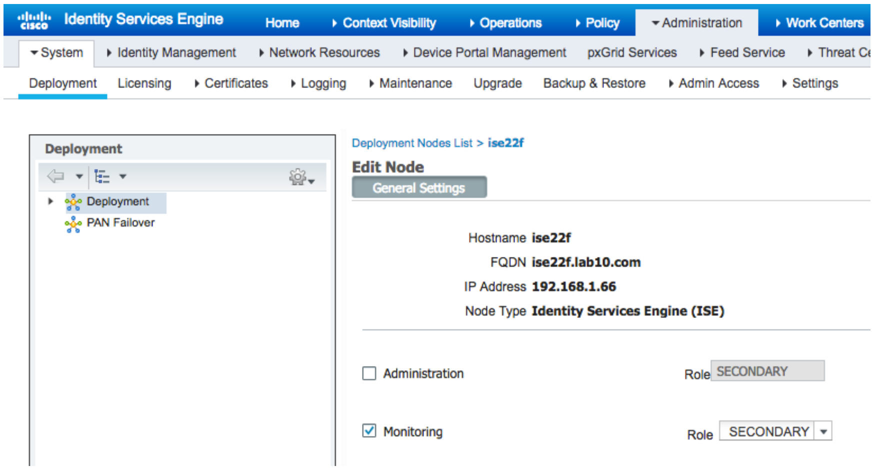
Step 19 Below is an example of registering the secondary MNT node.
Select **Administration->System->Deployment->Register->Register an ISE node**, select **Next**



Register ISE Node - Step 1: Specify Node Host FQDN (hostname.domain-name) and Credentials

* Host FQDN: ise22f.lab10.com
* User Name: admin
* Password: •••••••••

Step 20 Select **Monitoring** Persona and **Secondary** role

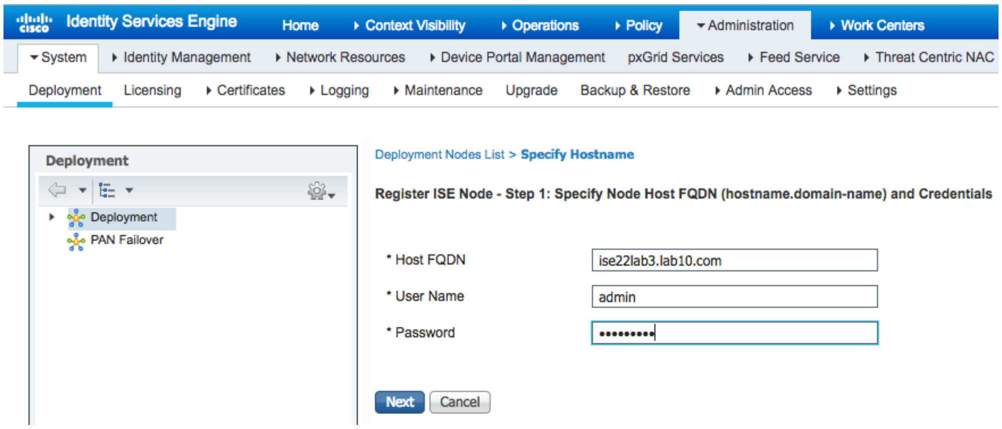


Edit Node

Hostname ise22f
FQDN ise22f.lab10.com
IP Address 192.168.1.66
Node Type Identity Services Engine (ISE)

☐ Administration Role SECONDARY
☑ Monitoring Role SECONDARY

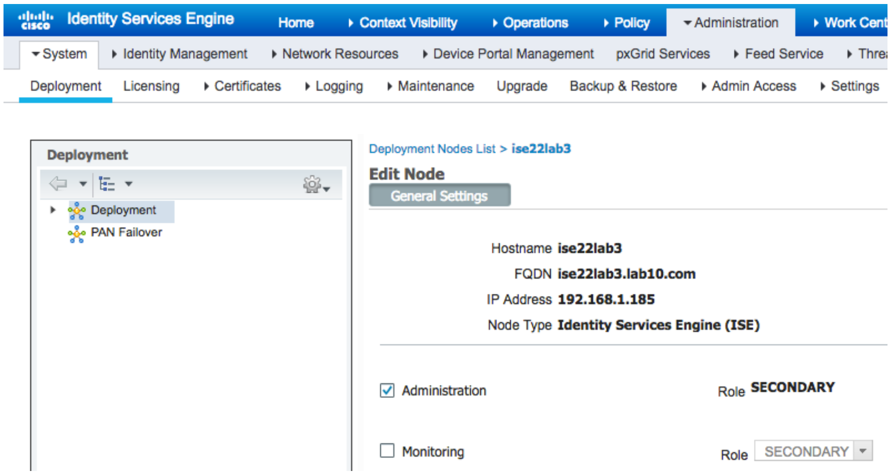
Step 21 Select **Save**
Step 22 Below is an example of registering the secondary admin node.
Select **Administration->System->Deployment->Register->Register an ISE node**, select **Next**



Register ISE Node - Step 1: Specify Node Host FQDN (hostname.domain-name) and Credentials

* Host FQDN: ise22lab3.lab10.com
* User Name: admin
* Password: •••••••••

Step 23 **Enable** the Administration Persona and ensure that the role is secondary.



Deployment Nodes List > **ise22lab3**

Edit Node

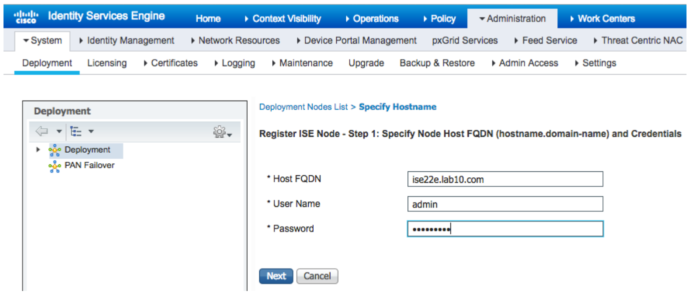
Hostname **ise22lab3**
FQDN **ise22lab3.lab10.com**
IP Address **192.168.1.185**
Node Type **Identity Services Engine (ISE)**

☑ Administration Role **SECONDARY**

□ Monitoring Role SECONDARY

Step 24 Select **Save**

Step 25 Below is an example of registering the secondary pxGrid node.
Select **Administration->System->Deployment->Register->Register an ISE node**, select **Next**

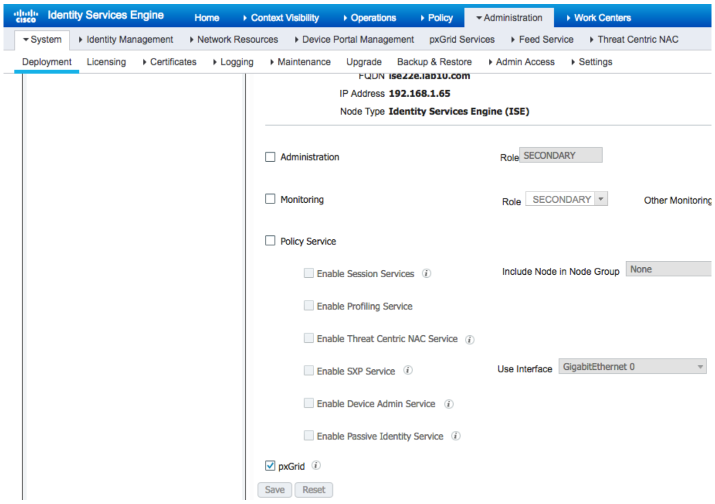


Deployment Nodes List > **Specify Hostname**

Register ISE Node - Step 1: Specify Node Host FQDN (hostname.domain-name) and Credentials

* Host FQDN ise22e.lab10.com
* User Name admin
* Password •••••••••

Step 26 **Enable** pxGrid persona



FQDN **ise22e.lab10.com**
IP Address **192.168.1.65**
Node Type **Identity Services Engine (ISE)**

□ Administration Role SECONDARY

□ Monitoring Role SECONDARY

□ Policy Service

□ Enable Session Services Include Node in Node Group None

□ Enable Profiling Service

□ Enable Threat Centric NAC Service

□ Enable SXP Service Use Interface GigabitEthernet 0

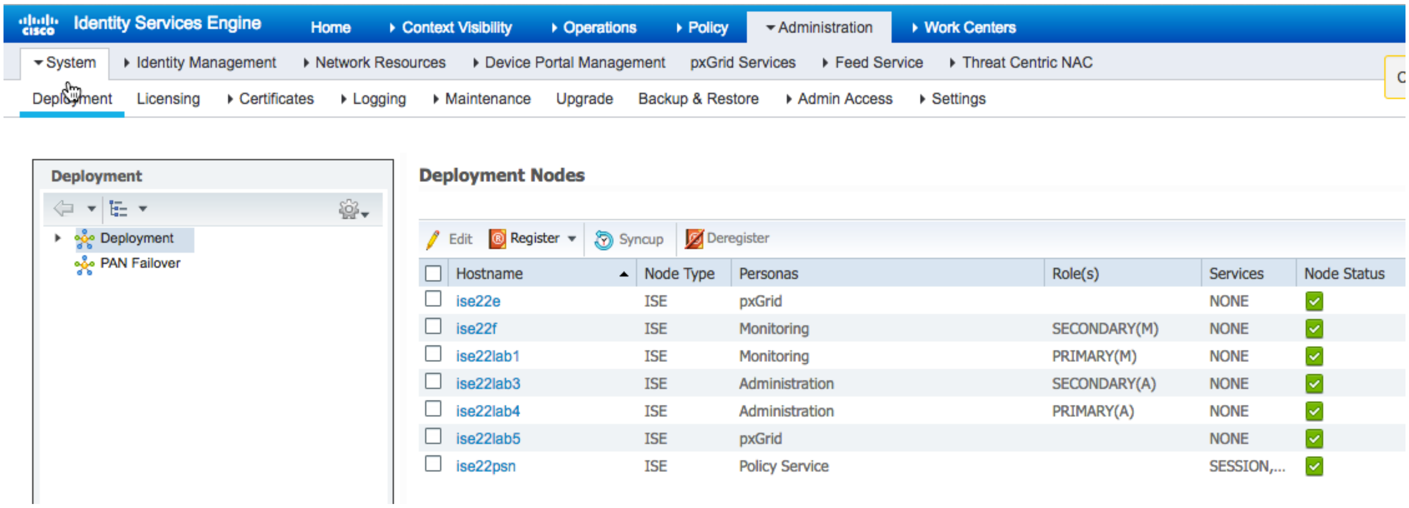
□ Enable Device Admin Service

□ Enable Passive Identity Service

☑ pxGrid

Step 27 Select **Save**

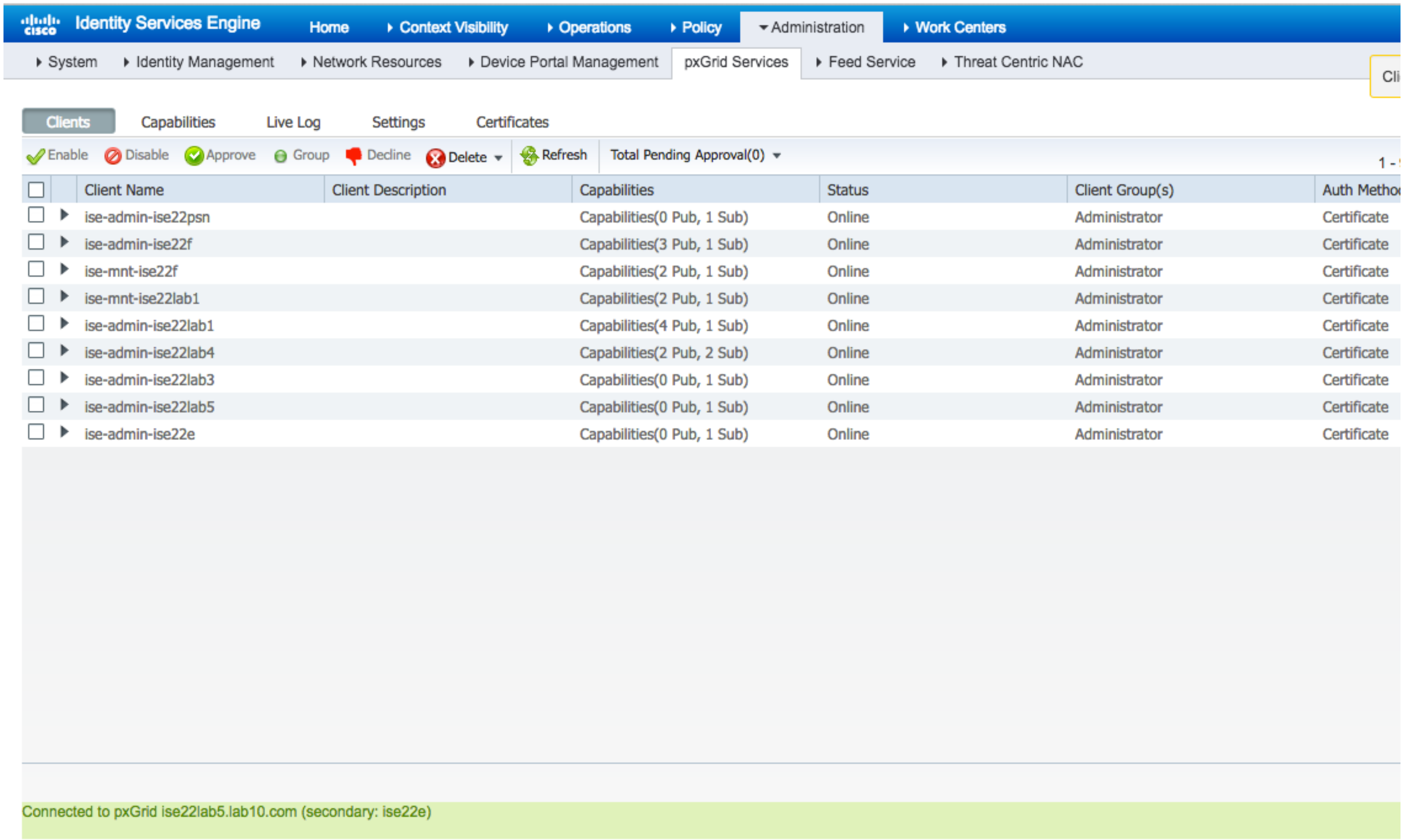
Step 28 Select **Administration->System->Deployment**, you should the following:



Deployment Nodes

Hostname	Node Type	Personas	Role(s)	Services	Node Status
ise22e	ISE	pxGrid		NONE	✓
ise22f	ISE	Monitoring	SECONDARY(M)	NONE	✓
ise22lab1	ISE	Monitoring	PRIMARY(M)	NONE	✓
ise22lab3	ISE	Administration	SECONDARY(A)	NONE	✓
ise22lab4	ISE	Administration	PRIMARY(A)	NONE	✓
ise22lab5	ISE	pxGrid		NONE	✓
ise22psn	ISE	Policy Service		SESSION,...	✓

Step 29 Select **Administration->pxGrid services**



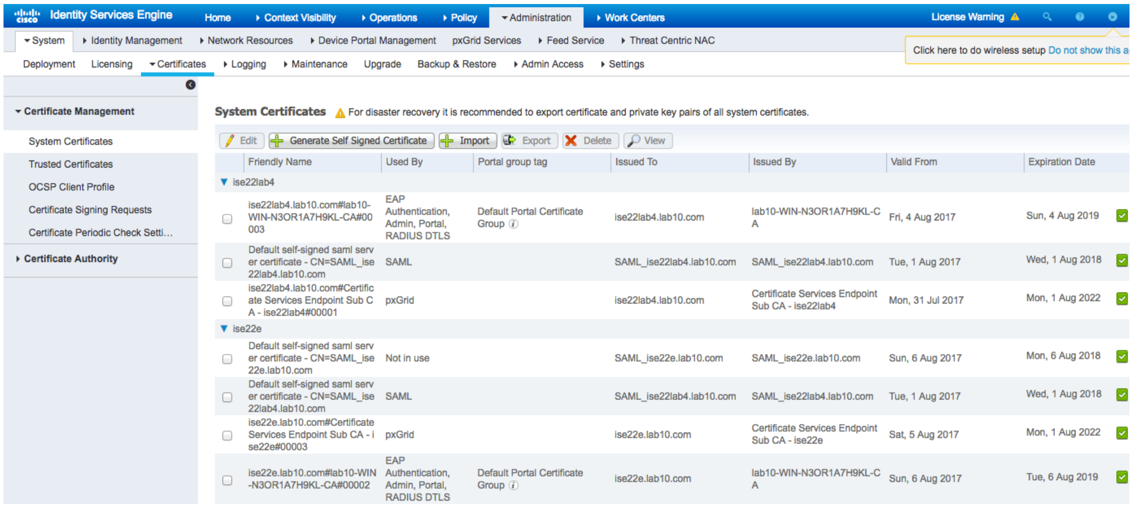
Client Name	Client Description	Capabilities	Status	Client Group(s)	Auth Metho
ise-admin-ise22psn		Capabilities(0 Pub, 1 Sub)	Online	Administrator	Certificate
ise-admin-ise22f		Capabilities(3 Pub, 1 Sub)	Online	Administrator	Certificate
ise-mnt-ise22f		Capabilities(2 Pub, 1 Sub)	Online	Administrator	Certificate
ise-mnt-ise22lab1		Capabilities(2 Pub, 1 Sub)	Online	Administrator	Certificate
ise-admin-ise22lab1		Capabilities(4 Pub, 1 Sub)	Online	Administrator	Certificate
ise-admin-ise22lab4		Capabilities(2 Pub, 2 Sub)	Online	Administrator	Certificate
ise-admin-ise22lab3		Capabilities(0 Pub, 1 Sub)	Online	Administrator	Certificate
ise-admin-ise22lab5		Capabilities(0 Pub, 1 Sub)	Online	Administrator	Certificate
ise-admin-ise22e		Capabilities(0 Pub, 1 Sub)	Online	Administrator	Certificate

Connected to pxGrid ise22lab5.lab10.com (secondary: ise22e)

Step 30 To view the certificates
Select **Administration->System->Certificates->Certificate Management->System Certificates**

The below screenshot represents the primary admin node (ise22lab4) and the secondary admin node (ise22a). Note the admin certificates (ise22lab4..) and (ise22a..) have been signed by the external CA server. The pxGrid certificates have been signed by the ISE internal CA server.

You will also see this on the Primary and Secondary nodes, the dedicated primary pxGrid and secondary pxGrid nodes, and the PSN node.



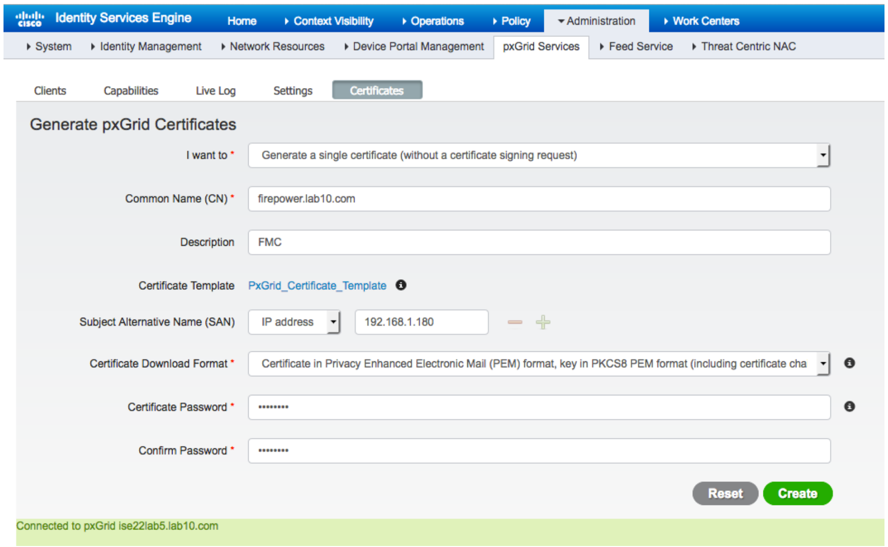
System Certificates ⚠ For disaster recovery it is recommended to export certificate and private key pairs of all system certificates.

	Friendly Name	Used By	Portal group tag	Issued To	Issued By	Valid From	Expiration Date	
▼ ise22lab4								
☐	ise22lab4.lab10.com#lab10-WIN-N3OR1A7H9KL-CA#00003	EAP Authentication, Admin, Portal, RADIUS DTLS	Default Portal Certificate Group ⓘ	ise22lab4.lab10.com	lab10-WIN-N3OR1A7H9KL-CA	Fri, 4 Aug 2017	Sun, 4 Aug 2019	✓
☐	Default self-signed saml server certificate - CN=SAML_ise22lab4.lab10.com	SAML		SAML_ise22lab4.lab10.com	SAML_ise22lab4.lab10.com	Tue, 1 Aug 2017	Wed, 1 Aug 2018	✓
☐	ise22lab4.lab10.com#Certificate Services Endpoint Sub CA - ise22lab4#00001	pxGrid		ise22lab4.lab10.com	Certificate Services Endpoint Sub CA - ise22lab4	Mon, 31 Jul 2017	Mon, 1 Aug 2022	✓
▼ ise22e								
☐	Default self-signed saml server certificate - CN=SAML_ise22e.lab10.com	Not in use		SAML_ise22e.lab10.com	SAML_ise22e.lab10.com	Sun, 6 Aug 2017	Mon, 6 Aug 2018	✓
☐	Default self-signed saml server certificate - CN=SAML_ise22lab4.lab10.com	SAML		SAML_ise22lab4.lab10.com	SAML_ise22lab4.lab10.com	Tue, 1 Aug 2017	Wed, 1 Aug 2018	✓
☐	ise22e.lab10.com#Certificate Services Endpoint Sub CA - ise22e#00003	pxGrid		ise22e.lab10.com	Certificate Services Endpoint Sub CA - ise22e	Sat, 5 Aug 2017	Mon, 1 Aug 2022	✓
☐	ise22e.lab10.com#lab10-WIN-N3OR1A7H9KL-CA#00002	EAP Authentication, Admin, Portal, RADIUS DTLS	Default Portal Certificate Group ⓘ	ise22e.lab10.com	lab10-WIN-N3OR1A7H9KL-CA	Sun, 6 Aug 2017	Tue, 6 Aug 2019	✓

Testing pxGrid Integration with Firepower Management Center 6.2+

This section details the procedure for configuring the Cisco Firepower Management Center (FMC) 6.2 with ISE 2.2 with pxGrid using the Internal CA for pxGrid operation. The Firepower certificates will be generated by the ISE internal CA.

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

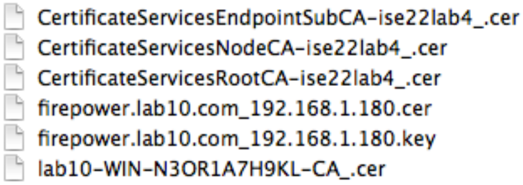


Generate pxGrid Certificates

I want to *	Generate a single certificate (without a certificate signing request)
Common Name (CN) *	firepower.lab10.com
Description	FMC
Certificate Template	PxGrid_Certificate_Template
Subject Alternative Name (SAN)	IP address 192.168.1.180
Certificate Download Format *	Certificate in Privacy Enhanced Electronic Mail (PEM) format, key in PKCS8 PEM format (including certificate cha
Certificate Password *	••••••••
Confirm Password *	••••••••

Connected to pxGrid ise22lab5.lab10.com

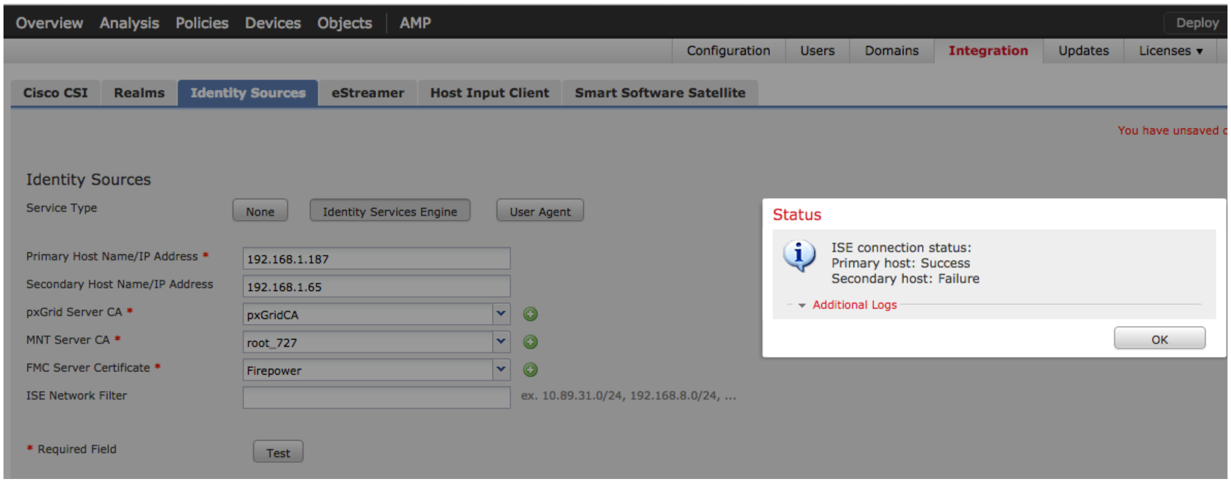
Step 2 Select **Generate** and save the file locally. You should see the following:



CertificateServicesEndpointSubCA-ise22lab4_.cer
CertificateServicesNodeCA-ise22lab4_.cer
CertificateServicesRootCA-ise22lab4_.cer
firepower.lab10.com_192.168.1.180.cer
firepower.lab10.com_192.168.1.180.key
lab10-WIN-N3OR1A7H9KL-CA_.cer

Step 3 Select **System->Integration->Identity Sources->Identity Services Engine->**

Enter the primary pxGrid host name or IP address for the **Primary Host Name/IP Address** field
Enter the secondary pxGrid host name or IP address for the **Secondary Host Name/IP Address** field
Upload the **CertificateServicesRootCA** certificate for the **pxGrid Server CA**
Upload the **CA root certificate**, in this case, lab10-WIN-N3OR1A7H9KL, for the **MNT Server CA**
Upload the **FMC Server Certificate** (public private key-pair) for **FMC Server Certificate**



Identity Sources

Service Type: None | Identity Services Engine | User Agent

Primary Host Name/IP Address *: 192.168.1.187
Secondary Host Name/IP Address: 192.168.1.65
pxGrid Server CA *: pxGridCA
MNT Server CA *: root_727
FMC Server Certificate *: Firepower
ISE Network Filter: ex. 10.89.31.0/24, 192.168.8.0/24, ...

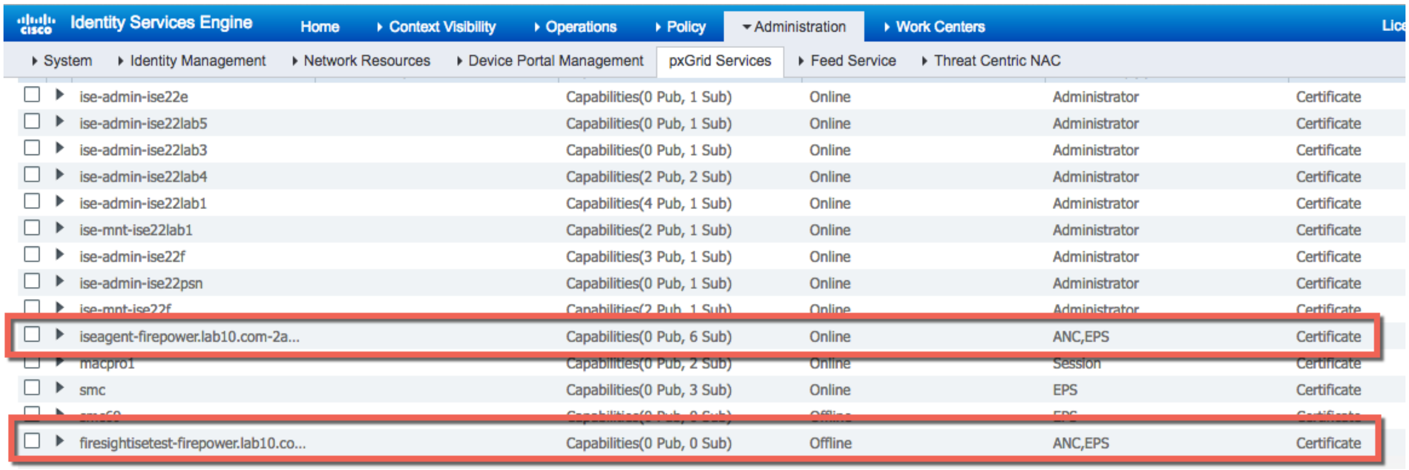
* Required Field

Status

ISE connection status:
Primary host: Success
Secondary host: Failure

Step 4 Select **Test,** you should see a **Primary host: Success message**

Step 5 Select **Administration->pxGrid** service to verify Firepower has successfully registered as the pxGrid client.



□	ise-admin-ise22e	Capabilities(0 Pub, 1 Sub)	Online	Administrator	Certificate
□	ise-admin-ise22lab5	Capabilities(0 Pub, 1 Sub)	Online	Administrator	Certificate
□	ise-admin-ise22lab3	Capabilities(0 Pub, 1 Sub)	Online	Administrator	Certificate
□	ise-admin-ise22lab4	Capabilities(2 Pub, 2 Sub)	Online	Administrator	Certificate
□	ise-admin-ise22lab1	Capabilities(4 Pub, 1 Sub)	Online	Administrator	Certificate
□	ise-mnt-ise22lab1	Capabilities(2 Pub, 1 Sub)	Online	Administrator	Certificate
□	ise-admin-ise22f	Capabilities(3 Pub, 1 Sub)	Online	Administrator	Certificate
□	ise-admin-ise22psn	Capabilities(0 Pub, 1 Sub)	Online	Administrator	Certificate
□	ise-mnt-ise22f	Capabilities(2 Pub, 1 Sub)	Online	Administrator	Certificate
□	iseagent-firepower.lab10.com-2a...	Capabilities(0 Pub, 6 Sub)	Online	ANC,EPS	Certificate
□	macpro1	Capabilities(0 Pub, 2 Sub)	Online	Session	Certificate
□	smc	Capabilities(0 Pub, 3 Sub)	Online	EPS	Certificate
□	smc60	Capabilities(0 Pub, 0 Sub)	Offline	EPS	Certificate
□	firesightisetest-firepower.lab10.co...	Capabilities(0 Pub, 0 Sub)	Offline	ANC,EPS	Certificate

Testing pxGrid Integration with Java-based pxGrid Client

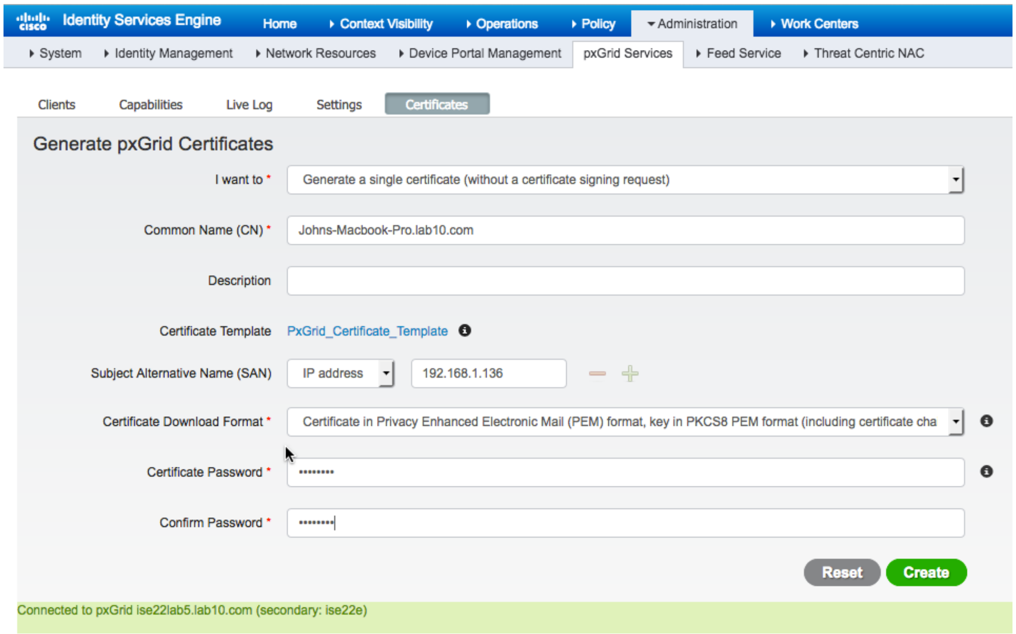
This section details the procedure for configuring java-based pxGrid solution vendors with ISE 2.2+ with pxGrid using the Internal CA for pxGrid operation. The solution vendor certificates will be generated by the ISE internal CA. In this example, a MAC Pro Laptop was used as the pxGrid client.

We will create the trust file keystore filename macpro1.jks and trust root store filename macpro1_root.jks, password for both Cisco123.

If the ecosystem security solution does not support certificate encryption, the private key must be decrypted, below is the procedure:

```
cp Johns-Macbook-Pro.lab10.com_192.168.1.136.key Johns-Macbook-Pro.lab10.com_192.168.1.136.key.org
openssl rsa -in Johns-Macbook-Pro.lab10.com_192.168.1.136.key.org -out Johns-Macbook-
Pro.lab10.com_192.168.1.136.key
```

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



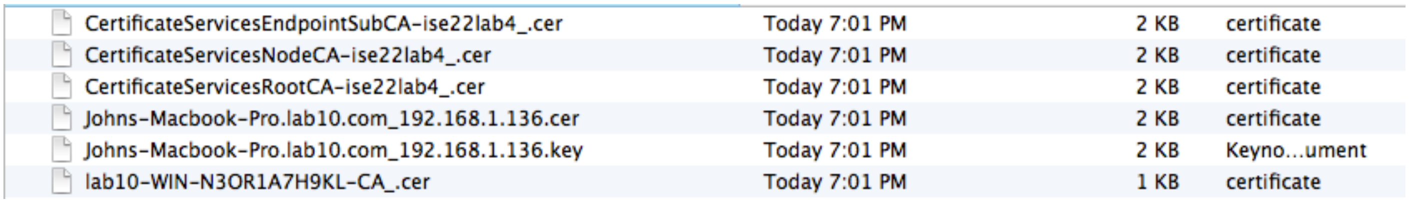
Generate pxGrid Certificates

I want to *	Generate a single certificate (without a certificate signing request)
Common Name (CN) *	Johns-Macbook-Pro.lab10.com
Description	
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 *	••••••••

Connected to pxGrid ise22lab5.lab10.com (secondary: ise22e)

Step 2 Select **Create**

Step 3 Download the file locally, and unzip the files, you should see:



CertificateServicesEndpointSubCA-ise22lab4_.cer	Today 7:01 PM	2 KB	certificate
CertificateServicesNodeCA-ise22lab4_.cer	Today 7:01 PM	2 KB	certificate
CertificateServicesRootCA-ise22lab4_.cer	Today 7:01 PM	2 KB	certificate
Johns-Macbook-Pro.lab10.com_192.168.1.136.cer	Today 7:01 PM	2 KB	certificate
Johns-Macbook-Pro.lab10.com_192.168.1.136.key	Today 7:01 PM	2 KB	Keyno...ument
lab10-WIN-N3OR1A7H9KL-CA_.cer	Today 7:01 PM	1 KB	certificate

Step 4 Concatenate files into one certificate

```
cat CertificateServicesEndpointSubCA-ise22lab4_.cer CertificateServicesRootCA-ise22lab4_.cer
CertificateServicesNodeCA-ise22lab4_.cer lab10-WIN-N3OR1A7H9KL-CA_.cer > CA1.cer
```

Step 5 Create PKCS12 file

Note: The passphrase is the password that was typed when generating the certificates from the ISE internal CA

```
openssl pkcs12 -export -out macpro1.p12 -inkey Johns-Macbook-Pro.lab10.com_192.168.1.136.key -in Johns-
Macbook-Pro.lab10.com_192.168.1.136.cer -chain -CAfile CA1.cer

Enter pass phrase for Johns-Macbook-Pro.lab10.com_192.168.1.136.key: Cisco123
Enter Export Password: Cisco123
Verifying - Enter Export Password: Cisco123
```

Step 6 Import PKCS file into keystore

```
keytool -importkeystore -srckeystore macpro1.p12 -destkeystore macpro1.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
```

Step 7 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 8 Import the converted CA root certificate in DER format to trusted keystore

```
keytool -import -alias macpro1 -keystore macpro1_root.jks -file CA1.der
Enter keystore password:  Cisco123
Re-enter new password: Cisco123
Owner: CN=Certificate Services Endpoint Sub CA - ise22lab4
Issuer: CN=Certificate Services Node CA - ise22lab4
Serial number: 109b2c4872244d9694707f48079b1446
Valid from: Sun Jul 30 20:10:30 EDT 2017 until: Sun Jul 31 20:10:26 EDT 2022
Certificate fingerprints:
         MD5:  3E:76:5C:6D:8C:26:3B:8F:5B:C4:C0:40:A4:3F:D4:B6
         SHA1: 1B:BC:2A:65:44:1D:D3:D8:97:97:90:9B:25:27:23:16:C2:8D:62:5D
         SHA256:
45:3C:E9:F7:83:25:A9:11:B9:AB:00:A8:BA:0E:B3:DC:0E:3E:40:28:C2:7C:8D:C8:78:54:8A:03:97:B9:01:74
         Signature algorithm name: SHA256withRSA
         Version: 3

Extensions:

#1: ObjectId: 2.5.29.35 Criticality=false
AuthorityKeyIdentifier [
KeyIdentifier [
0000: F4 7F 2E 7B D4 DB 5C 1A   74 09 51 EB 25 24 4E 0F  ......\.t.Q.%$N.
0010: 74 7E 50 54                                        t.PT
]
[CN=Certificate Services Root CA - ise22lab4]
SerialNumber: [    46c64293 c0d94c8c ba9d37f3 6830037d]
]

#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: 0C 67 46 A2 FA A1 90 35   0E 51 02 A5 9F 46 13 36  .gF....5.Q...F.6
0010: 1E D0 26 7F                                        ..&.
]
]

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

Step 9 Import the pxGrid client certificate into the trusted file keystore

```
keytool -import -alias macpro2 -keystore macpro1.jks -file Johns-Macbook-Pro.lab10.com_192.168.1.136.cer
Enter keystore password:  Cisco123
Certificate already exists in keystore under alias <1>
Do you still want to add it? [no]:  yes
Certificate was added to keystore
```

Step 10 Import the CA root certificate to trusted root keystore

```
keytool -import -alias macpro3 -keystore macpro1_root.jks -file CA1.cer
Enter keystore password:  Cisco123
Certificate already exists in keystore under alias <macpro1>
Do you still want to add it? [no]:  yes
Certificate was added to keystore
```

Step 11 Import the ISE CertificateServicesRoot certificate into trusted root keystore

```
keytool -import -alias macpro5 -keystore macpro1_root.jks -file CertificateServicesRootCA-ise22lab4_.cer
Enter keystore password: Cisco123
Owner: CN=Certificate Services Root CA - ise22lab4
Issuer: CN=Certificate Services Root CA - ise22lab4
Serial number: 655ffcd9c3cd4fce8462fdc6062c0ea9
Valid from: Sun Jul 30 20:10:13 EDT 2017 until: Sat Jul 31 20:10:13 EDT 2027
Certificate fingerprints:
         MD5:  E6:78:C1:87:BA:47:FE:FB:81:00:A6:40:81:28:57:1F
         SHA1: 07:6B:0D:C7:C3:4F:39:9F:42:E7:2B:9F:33:0A:0D:55:3B:2E:D5:50
         SHA256:
6F:1D:F6:81:D5:AB:CE:EB:72:A4:89:AD:70:BA:11:BD:49:48:57:16:F1:53:A5:1E:E2:34:2E:8D:FD:A5:2D:5B
         Signature algorithm name: SHA256withRSA
         Version: 3

Extensions:

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

#2: ObjectId: 2.5.29.15 Criticality=true
KeyUsage [
  Key_CertSign
]

#3: ObjectId: 2.5.29.14 Criticality=false
```

```
SubjectKeyIdentifier [
KeyIdentifier [
0000: 33 9E 4A 44 BB 04 1B B9   13 C8 F4 00 F8 DC F9 78  3.JD...........x
0010: 6C 17 6F 00                                        l.o.
]
]

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

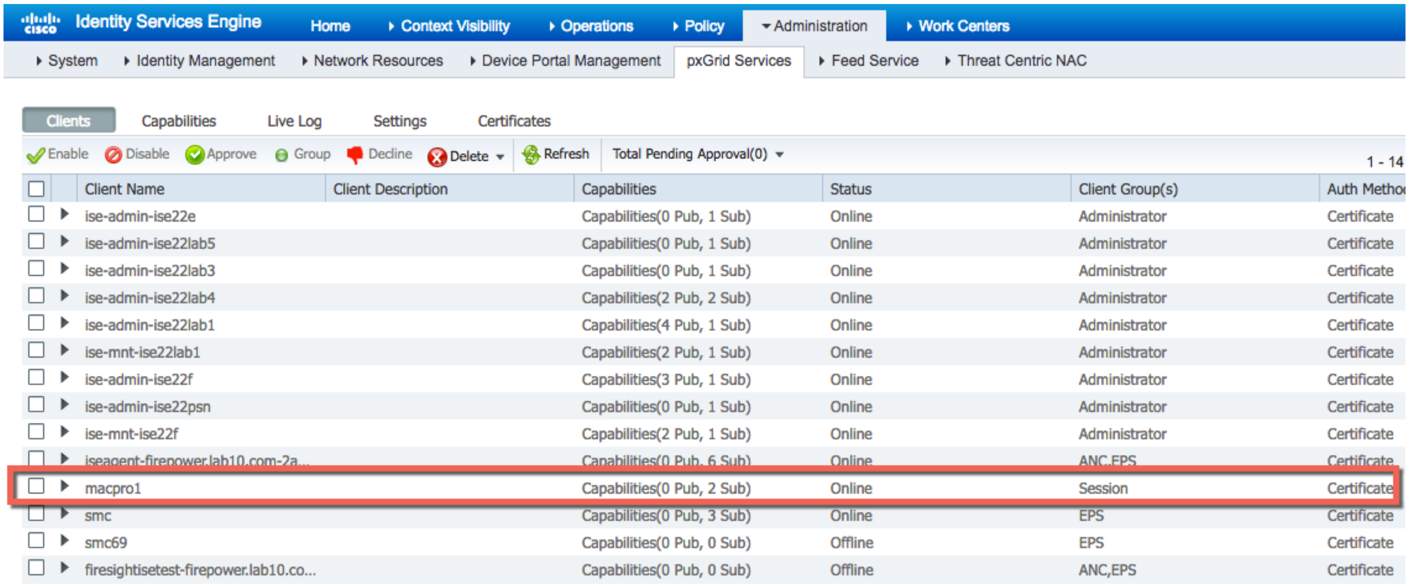
Step 12 Run Session_download script.

Note: The session_download sample script is not required for testing. The security vendor should be able to download active session information if supported in their configuration.

The session_download sample script is part of the pxGrid SDK(pxGrid 1.0) which can be downloaded from https://developer.cisco.com/site/pxgrid/. You will need to register which is no cost. For script reference, please see: https://communities.cisco.com/docs/DOC-68291

```
./session_download.sh -a 192.168.1.187,192.168.1.65 -u macpro1 -k macpro1.jks -p Cisco123 -t macpro1_root.jks
-q Cisco123
------- properties -------
  version=1.0.4.19
  hostnames=192.168.1.187,192.168.1.65
  username=macpro1
  password=
  group=Session
  description=null
  keystoreFilename=macpro1.jks
  keystorePassword=Cisco123
  truststoreFilename=macpro1_root.jks
  truststorePassword=Cisco123
--------------------------
Connecting...
15:51:30.419 [main] INFO  com.cisco.pxgrid.Configuration - Connecting to host 192.168.1.187
15:51:30.722 [main] INFO  com.cisco.pxgrid.Configuration - Connected OK to host 192.168.1.187
15:51:30.722 [main] INFO  com.cisco.pxgrid.Configuration - Client Login to host 192.168.1.187
15:51:30.754 [main] INFO  com.cisco.pxgrid.Configuration - Client Login OK to host 192.168.1.187
Connected
Filters (ex. '1.0.0.0/255.0.0.0,1234::/16...' or <enter> for no filter):
Start time (ex. '2015-01-31 13:00:00' or <enter> for no start time):
End time (ex. '2015-01-31 13:00:00' or <enter> for no end time):
pxGrid controller version=1.0.4.18
Going to url:https://ise22f.lab10.com:8910/pxgrid/mnt/sd/getSessionListByTime
Session={ip=[192.168.1.187], Audit Session Id=0A000001000000280077C9BC, UserName=00:0C:29:1D:1A:5A,
MacAddresses=[00:0C:29:1D:1A:5A], State=STARTED, EndpointProfile=ISE-Appliance, NAS IP=192.168.1.3, NAS
Port=GigabitEthernet1/0/15, RADIUSAVPairs=[ Acct-Session-Id=00000029], Posture Status=null, Posture
Timestamp=, LastUpdateTime=Mon Aug 07 15:45:12 EDT 2017, Session attributeName=Authorization_Profiles,
Session attributeValue=PermitAccess, Providers=[None], EndpointCheckResult=none, IdentitySourceFirstPort=0,
IdentitySourcePortStart=0, IdentitySourcePortEnd=0}
Session={ip=[192.168.1.186], Audit Session Id=0A000001000000270077B549, UserName=00:0C:29:21:DF:BF,
MacAddresses=[00:0C:29:21:DF:BF], State=STARTED, EndpointProfile=ISE-Appliance, NAS IP=192.168.1.3, NAS
Port=GigabitEthernet1/0/15, RADIUSAVPairs=[ Acct-Session-Id=00000028], Posture Status=null, Posture
Timestamp=, LastUpdateTime=Mon Aug 07 15:45:30 EDT 2017, Session attributeName=Authorization_Profiles,
Session attributeValue=PermitAccess, Providers=[None], EndpointCheckResult=none, IdentitySourceFirstPort=0,
IdentitySourcePortStart=0, IdentitySourcePortEnd=0}
Session={ip=[192.168.1.30], Audit Session Id=0A0000010000003700ABD28D, UserName=00:0C:29:7C:79:39,
MacAddresses=[00:0C:29:7C:79:39], State=STARTED, EndpointProfile=VMWare-Device, NAS IP=192.168.1.3, NAS
Port=GigabitEthernet1/0/15, RADIUSAVPairs=[ Acct-Session-Id=00000038], Posture Status=null, Posture
Timestamp=, LastUpdateTime=Mon Aug 07 15:45:21 EDT 2017, Session attributeName=Authorization_Profiles,
Session attributeValue=PermitAccess, Providers=[None], EndpointCheckResult=none, IdentitySourceFirstPort=0,
IdentitySourcePortStart=0, IdentitySourcePortEnd=0}
Session={ip=[192.168.1.183], Audit Session Id=0A000001000000160002C975, UserName=00:0C:29:AB:23:FF,
MacAddresses=[00:0C:29:AB:23:FF], State=STARTED, EndpointProfile=ISE-Appliance, NAS IP=192.168.1.3, NAS
Port=GigabitEthernet1/0/10, RADIUSAVPairs=[ Acct-Session-Id=00000017], Posture Status=null, Posture
Timestamp=, LastUpdateTime=Mon Aug 07 15:45:30 EDT 2017, Session attributeName=Authorization_Profiles,
Session attributeValue=PermitAccess, Providers=[None], EndpointCheckResult=none, IdentitySourceFirstPort=0,
IdentitySourcePortStart=0, IdentitySourcePortEnd=0}
Session={ip=[192.168.1.10], Audit Session Id=0A0000010000003E016FBD40, UserName=00:0C:29:C1:7B:2C,
MacAddresses=[00:0C:29:C1:7B:2C], State=STARTED, EndpointProfile=VMWare-Device, NAS IP=192.168.1.3, NAS
Port=GigabitEthernet1/0/11, RADIUSAVPairs=[ Acct-Session-Id=00000040], Posture Status=null, Posture
Timestamp=, LastUpdateTime=Mon Aug 07 15:49:02 EDT 2017, Session attributeName=Authorization_Profiles,
Session attributeValue=PermitAccess, Providers=[None], EndpointCheckResult=none, IdentitySourceFirstPort=0,
IdentitySourcePortStart=0, IdentitySourcePortEnd=0}
Session={ip=[192.168.1.185], Audit Session Id=0A000001000000260077A376, UserName=00:0C:29:E1:AD:B7,
MacAddresses=[00:0C:29:E1:AD:B7], State=STARTED, EndpointProfile=ISE-Appliance, NAS IP=192.168.1.3, NAS
Port=GigabitEthernet1/0/15, RADIUSAVPairs=[ Acct-Session-Id=00000027], Posture Status=null, Posture
Timestamp=, LastUpdateTime=Mon Aug 07 15:48:43 EDT 2017, Session attributeName=Authorization_Profiles,
Session attributeValue=PermitAccess, Providers=[None], EndpointCheckResult=none, IdentitySourceFirstPort=0,
IdentitySourcePortStart=0, IdentitySourcePortEnd=0}
Session={ip=[192.168.1.159], Audit Session Id=0A000001000000290077E32A, UserName=00:50:56:86:08:19,
MacAddresses=[00:50:56:86:08:19], State=STARTED, EndpointProfile=ISE-Appliance, NAS IP=192.168.1.3, NAS
Port=GigabitEthernet1/0/10, RADIUSAVPairs=[ Acct-Session-Id=0000002A], Posture Status=null, Posture
Timestamp=, LastUpdateTime=Mon Aug 07 15:48:33 EDT 2017, Session attributeName=Authorization_Profiles,
Session attributeValue=PermitAccess, Providers=[None], EndpointCheckResult=none, IdentitySourceFirstPort=0,
IdentitySourcePortStart=0, IdentitySourcePortEnd=0}
Session={ip=[192.168.1.9], Audit Session Id=0A0000010000003800ACA782, UserName=10:DD:B1:C9:3C:39,
MacAddresses=[10:DD:B1:C9:3C:39], State=STARTED, EndpointProfile=Workstation, NAS IP=192.168.1.3, NAS
Port=GigabitEthernet1/0/12, RADIUSAVPairs=[ Acct-Session-Id=00000039], Posture Status=null, Posture
Timestamp=, LastUpdateTime=Mon Aug 07 15:44:54 EDT 2017, Session attributeName=Authorization_Profiles,
Session attributeValue=PermitAccess, Providers=[None], EndpointCheckResult=none, IdentitySourceFirstPort=0,
IdentitySourcePortStart=0, IdentitySourcePortEnd=0}
Session={ip=[192.168.1.7], Audit Session Id=0A000001000000170002C9C0, UserName=18:E7:28:2E:29:CC,
MacAddresses=[18:E7:28:2E:29:CC], State=STARTED, EndpointProfile=Cisco-Device, NAS IP=192.168.1.3, NAS
Port=GigabitEthernet1/0/15, RADIUSAVPairs=[ Acct-Session-Id=00000018], Posture Status=null, Posture
Timestamp=, LastUpdateTime=Mon Aug 07 15:48:33 EDT 2017, Session attributeName=Authorization_Profiles,
Session attributeValue=PermitAccess, Providers=[None], EndpointCheckResult=none, IdentitySourceFirstPort=0,
IdentitySourcePortStart=0, IdentitySourcePortEnd=0}
Session={ip=[192.168.1.6], Audit Session Id=0A000001000000310094786C, UserName=74:26:AC:5A:82:24,
MacAddresses=[74:26:AC:5A:82:24], State=STARTED, EndpointProfile=Cisco-Device, NAS IP=192.168.1.3, NAS
Port=GigabitEthernet1/0/17, RADIUSAVPairs=[ Acct-Session-Id=00000032], Posture Status=null, Posture
Timestamp=, LastUpdateTime=Mon Aug 07 15:45:30 EDT 2017, Session attributeName=Authorization_Profiles,
Session attributeValue=PermitAccess, Providers=[None], EndpointCheckResult=none, IdentitySourceFirstPort=0,
IdentitySourcePortStart=0, IdentitySourcePortEnd=0}
Session={ip=[192.168.1.43], Audit Session Id=0A0000010000003000946FC5, UserName=74:26:AC:5A:82:26,
MacAddresses=[74:26:AC:5A:82:26], State=STARTED, EndpointProfile=Cisco-Device, NAS IP=192.168.1.3, NAS
Port=GigabitEthernet1/0/17, RADIUSAVPairs=[ Acct-Session-Id=00000031], Posture Status=null, Posture
Timestamp=, LastUpdateTime=Mon Aug 07 15:45:45 EDT 2017, Session attributeName=Authorization_Profiles,
Session attributeValue=PermitAccess, Providers=[None], EndpointCheckResult=none, IdentitySourceFirstPort=0,
IdentitySourcePortStart=0, IdentitySourcePortEnd=0}
Session count=11
Connection closed
Johns-MacBook-Pro:
```

Step 13 Select **Administration->pxGrid Services** to verify the pxGrid client appears



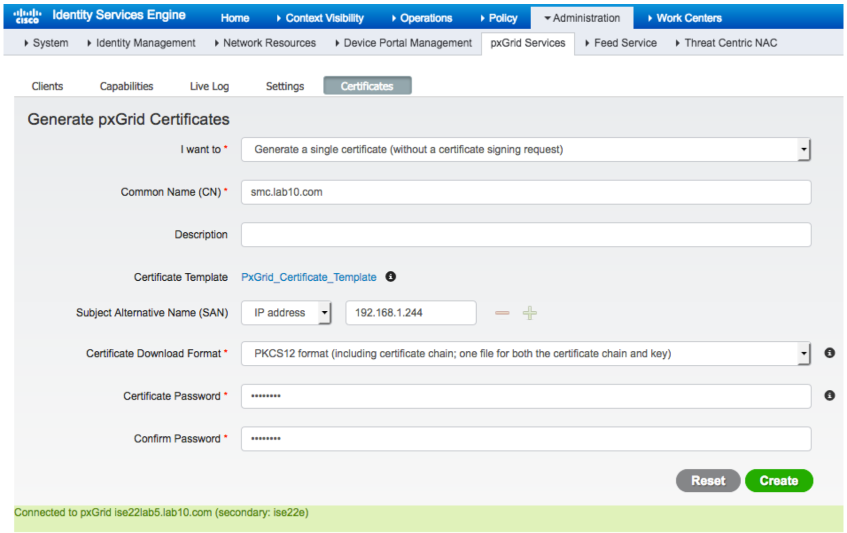
□	Client Name	Client Description	Capabilities	Status	Client Group(s)	Auth Metho
□	ise-admin-ise22e		Capabilities(0 Pub, 1 Sub)	Online	Administrator	Certificate
□	ise-admin-ise22lab5		Capabilities(0 Pub, 1 Sub)	Online	Administrator	Certificate
□	ise-admin-ise22lab3		Capabilities(0 Pub, 1 Sub)	Online	Administrator	Certificate
□	ise-admin-ise22lab4		Capabilities(2 Pub, 2 Sub)	Online	Administrator	Certificate
□	ise-admin-ise22lab1		Capabilities(4 Pub, 1 Sub)	Online	Administrator	Certificate
□	ise-mnt-ise22lab1		Capabilities(2 Pub, 1 Sub)	Online	Administrator	Certificate
□	ise-admin-ise22f		Capabilities(3 Pub, 1 Sub)	Online	Administrator	Certificate
□	ise-admin-ise22psn		Capabilities(0 Pub, 1 Sub)	Online	Administrator	Certificate
□	ise-mnt-ise22f		Capabilities(2 Pub, 1 Sub)	Online	Administrator	Certificate
□	iseagent-firepower.lab10.com-2a...		Capabilities(0 Pub, 6 Sub)	Online	ANC,EPS	Certificate
□	macpro1		Capabilities(0 Pub, 2 Sub)	Online	Session	Certificate
□	smc		Capabilities(0 Pub, 3 Sub)	Online	EPS	Certificate
□	smc69		Capabilities(0 Pub, 0 Sub)	Offline	EPS	Certificate
□	firesightisetest-firepower.lab10.co...		Capabilities(0 Pub, 0 Sub)	Offline	ANC,EPS	Certificate

Testing pxGrid Integration with Cisco Stealthwatch 6.9+

This section details the procedure for configuring Cisco Stealthwatch 6.9+ with ISE 2.2 with pxGrid using the Internal CA for pxGrid operation. The Stealthwatch pxGrid client certificates will be generated by the ISE internal CA.

Note: Please install all the Cisco Stealthwatch patches before configuring for pxGrid and certificate generation.

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) * smc.lab10.com

Description

Certificate Template PxGrid_Certificate_Template

Subject Alternative Name (SAN) IP address 192.168.1.244

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

Certificate Password * ••••••••

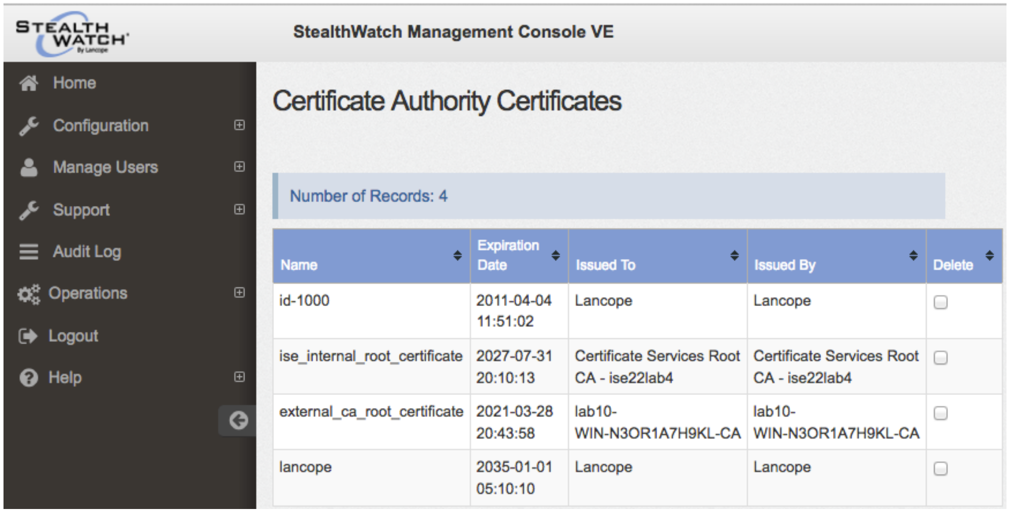
Confirm Password * ••••••••

Connected to pxGrid ise22lab5.lab10.com (secondary: ise22e)

Step 2 Select **Create,** download and unzip the files locally.

Step 3 Select **Administer Appliance->Configuration->Certificate Authority Certificates->Browse** and upload CA root certificate and **ISE CertificateServicesRootCA** certificate and provide the Name.

Step 4 Also upload the **external Root CA**, in this case, lab10-WIN-N3OR1A7H9KL-CA



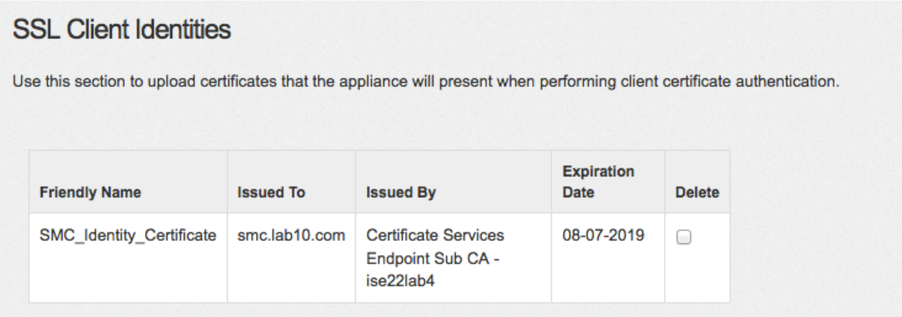
StealthWatch Management Console VE

Certificate Authority Certificates

Number of Records: 4

Name	Expiration Date	Issued To	Issued By	Delete
id-1000	2011-04-04 11:51:02	Lancope	Lancope	□
ise_internal_root_certificate	2027-07-31 20:10:13	Certificate Services Root CA - ise22lab4	Certificate Services Root CA - ise22lab4	□
external_ca_root_certificate	2021-03-28 20:43:58	lab10-WIN-N3OR1A7H9KL-CA	lab10-WIN-N3OR1A7H9KL-CA	□
lancope	2035-01-01 05:10:10	Lancope	Lancope	□

Step 5 Select **Configuration->SSL Certificates->SSL Client Identities->**upload the PKCS12 bundle file
Provide the password used for the SMC certificate generation in ISE
Provide a friendly name

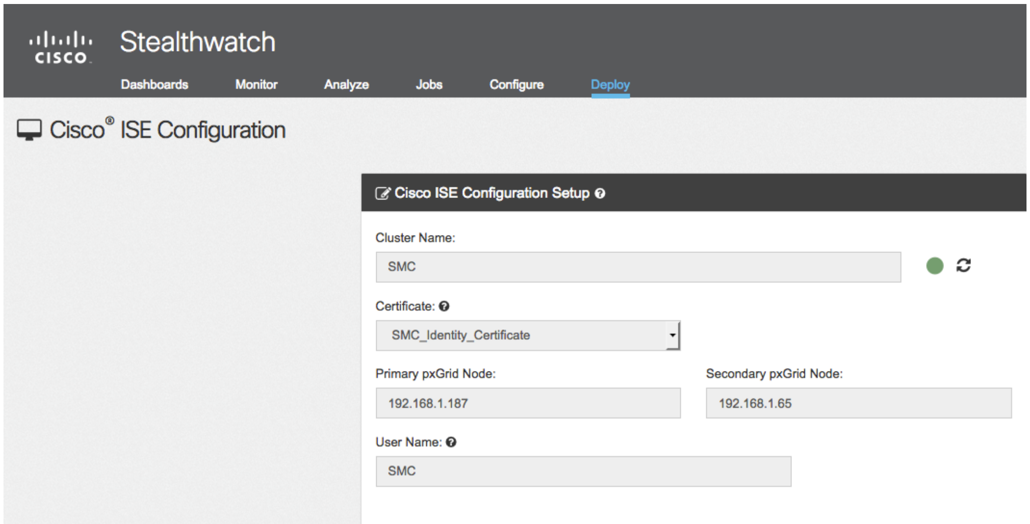


SSL Client Identities

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
SMC_Identity_Certificate	smc.lab10.com	Certificate Services Endpoint Sub CA - ise22lab4	08-07-2019	□

Step 6 Select **Deploy->Cisco ISE Configuration** and provide the following information:



Cisco® ISE Configuration

Cisco ISE Configuration Setup

Cluster Name: SMC

Certificate: SMC_Identity_Certificate

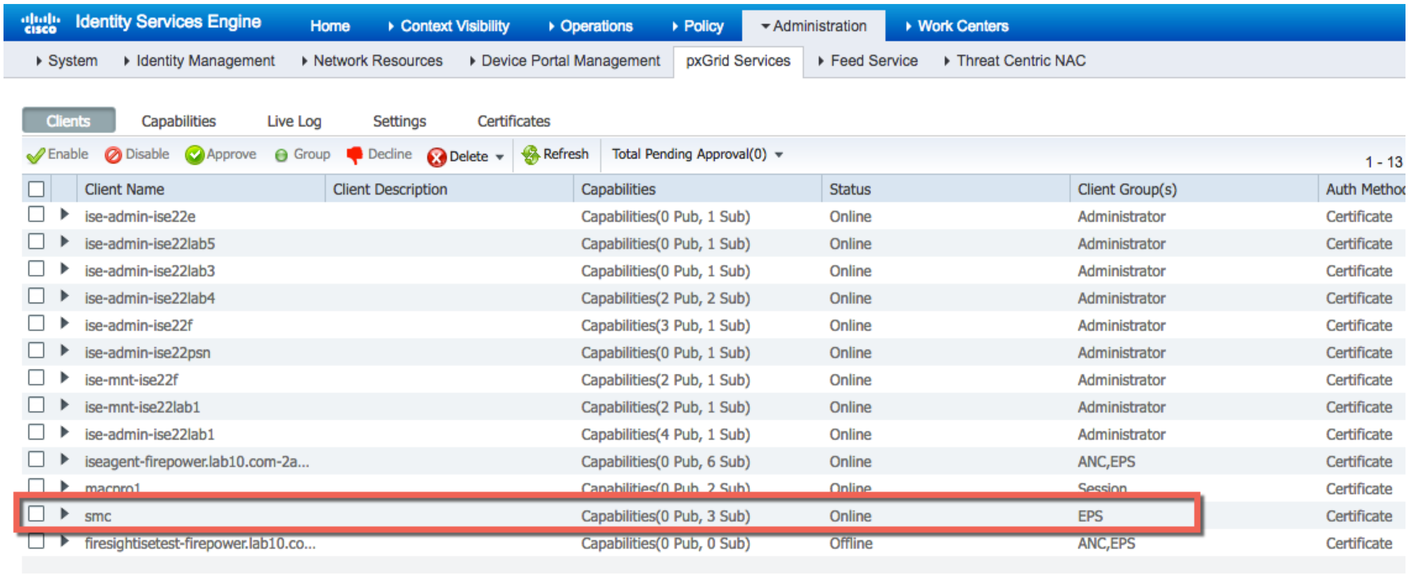
Primary pxGrid Node: 192.168.1.187

Secondary pxGrid Node: 192.168.1.65

User Name: SMC

Step 7 You should see a successful connection indicated by the green circle

Step 8 Select **Administration->pxGrid services**

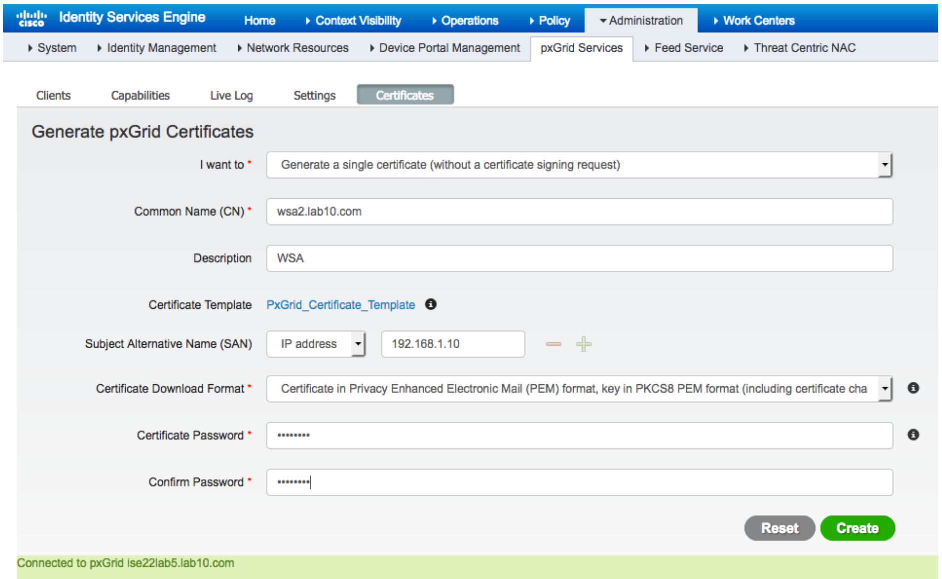


	Client Name	Client Description	Capabilities	Status	Client Group(s)	Auth Metho
□	ise-admin-ise22e		Capabilities(0 Pub, 1 Sub)	Online	Administrator	Certificate
□	ise-admin-ise22lab5		Capabilities(0 Pub, 1 Sub)	Online	Administrator	Certificate
□	ise-admin-ise22lab3		Capabilities(0 Pub, 1 Sub)	Online	Administrator	Certificate
□	ise-admin-ise22lab4		Capabilities(2 Pub, 2 Sub)	Online	Administrator	Certificate
□	ise-admin-ise22f		Capabilities(3 Pub, 1 Sub)	Online	Administrator	Certificate
□	ise-admin-ise22psn		Capabilities(0 Pub, 1 Sub)	Online	Administrator	Certificate
□	ise-mnt-ise22f		Capabilities(2 Pub, 1 Sub)	Online	Administrator	Certificate
□	ise-mnt-ise22lab1		Capabilities(2 Pub, 1 Sub)	Online	Administrator	Certificate
□	ise-admin-ise22lab1		Capabilities(4 Pub, 1 Sub)	Online	Administrator	Certificate
□	iseagent-firepower.lab10.com-2a...		Capabilities(0 Pub, 6 Sub)	Online	ANC,EPS	Certificate
□	macpro1		Capabilities(0 Pub, 2 Sub)	Online	Session	Certificate
□	smc		Capabilities(0 Pub, 3 Sub)	Online	EPS	Certificate
□	firesightisetest-firepower.lab10.co...		Capabilities(0 Pub, 0 Sub)	Offline	ANC,EPS	Certificate

Testing pxGrid Integration with Cisco Security Web Security Appliance (WSA)

This section details the procedure for configuring the Cisco WSA with ISE 2.2 with pxGrid using the Internal CA for pxGrid operation. The Cisco WSA certificates will be generated by the ISE internal CA.

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) * wsa2.lab10.com

Description WSA

Certificate Template PxGrid_Certificate_Template

Subject Alternative Name (SAN) IP address 192.168.1.10

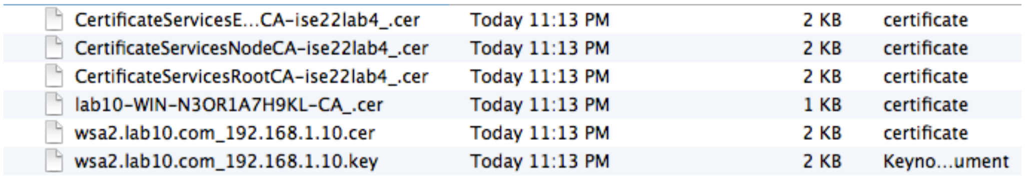
Certificate Download Format * Certificate in Privacy Enhanced Electronic Mail (PEM) format, key in PKCS8 PEM format (including certificate cha

Certificate Password * ••••••••

Confirm Password * ••••••••

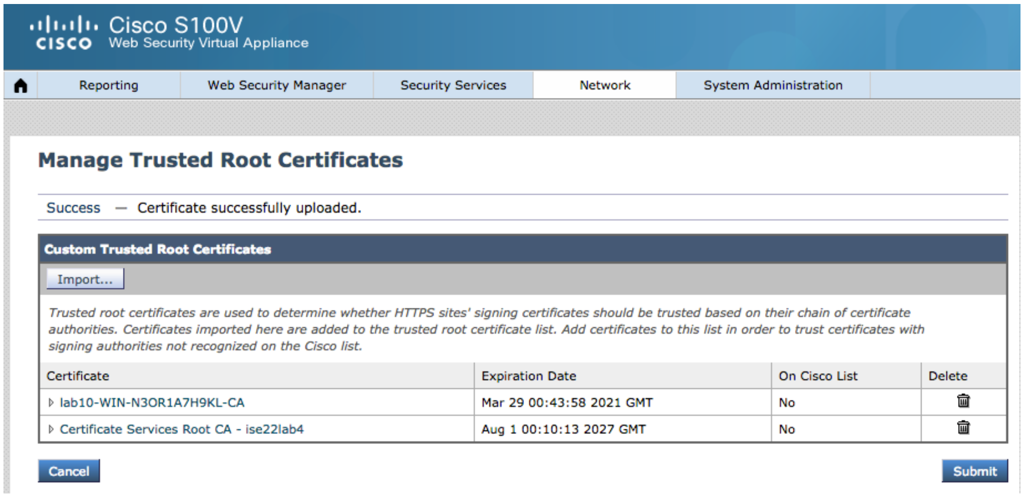
Connected to pxGrid ise22lab5.lab10.com

Step 2 Select **Create**, download and unzip the files locally



CertificateServicesE...CA-ise22lab4_.cer	Today 11:13 PM	2 KB	certificate
CertificateServicesNodeCA-ise22lab4_.cer	Today 11:13 PM	2 KB	certificate
CertificateServicesRootCA-ise22lab4_.cer	Today 11:13 PM	2 KB	certificate
lab10-WIN-N3OR1A7H9KL-CA_.cer	Today 11:13 PM	1 KB	certificate
wsa2.lab10.com_192.168.1.10.cer	Today 11:13 PM	2 KB	certificate
wsa2.lab10.com_192.168.1.10.key	Today 11:13 PM	2 KB	Keyno...ument

Step 3 Select **Network->Certificate Management->Managed Trusted Root Certificates->Import and upload the ISE CertificateServicesRootCA and the external root CA, in this case, lab10-WIN-N3OR1A7H9KL-CA**



Manage Trusted Root Certificates

Success — Certificate successfully uploaded.

Custom Trusted Root Certificates

Import...

Trusted root certificates are used to determine whether HTTPS sites' signing certificates should be trusted based on their chain of certificate authorities. Certificates imported here are added to the trusted root certificate list. Add certificates to this list in order to trust certificates with signing authorities not recognized on the Cisco list.

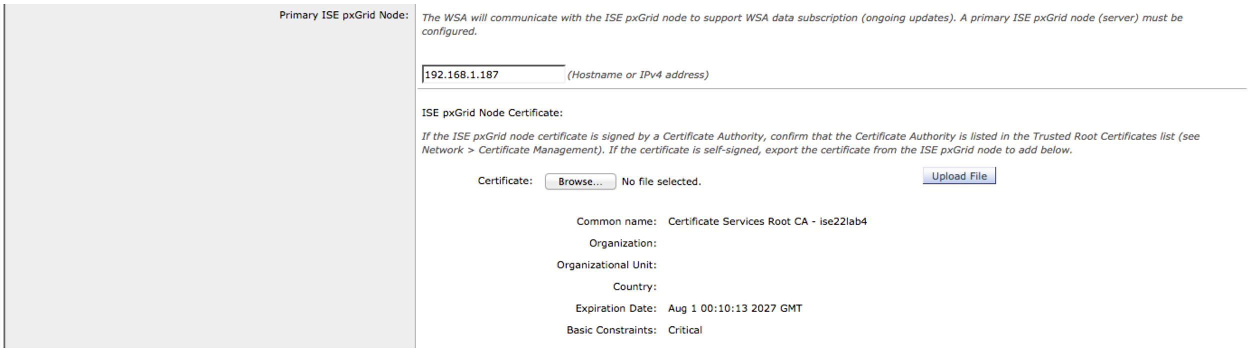
Certificate	Expiration Date	On Cisco List	Delete
▹ lab10-WIN-N3OR1A7H9KL-CA	Mar 29 00:43:58 2021 GMT	No	🗑
▹ Certificate Services Root CA - ise22lab4	Aug 1 00:10:13 2027 GMT	No	🗑

Cancel Submit

Step 4 Select **Commit Changes** twice

Step 5 Select **Network->Identification Services->Identity Services Engine** and **Enable**

Step 6 For **Primary pxGrid node,** enter the IP address of the primary pxGrid node and upload the ISE Certificate Root Services certificate



Primary ISE pxGrid Node:

The WSA will communicate with the ISE pxGrid node to support WSA data subscription (ongoing updates). A primary ISE pxGrid node (server) must be configured.

192.168.1.187 *(Hostname or IPv4 address)*

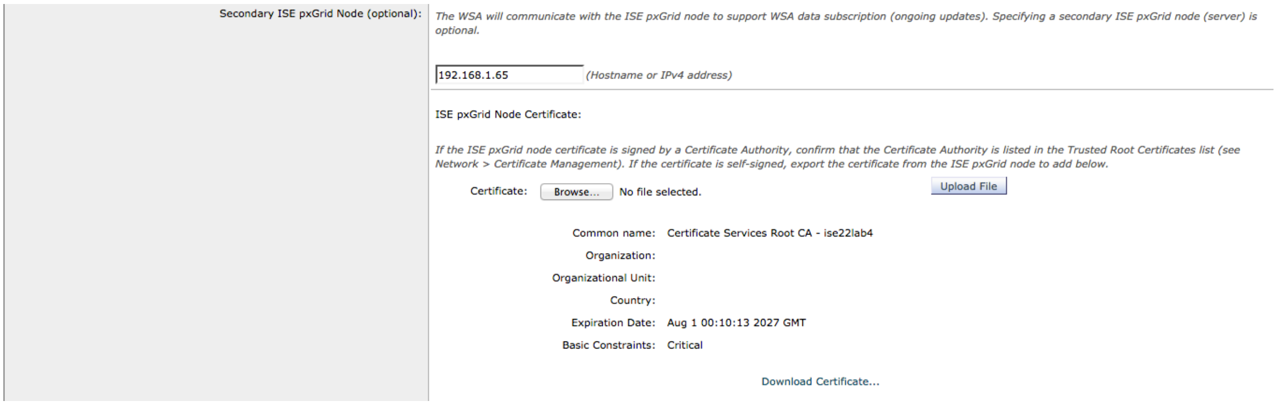
ISE pxGrid Node Certificate:

If the ISE pxGrid node certificate is signed by a Certificate Authority, confirm that the Certificate Authority is listed in the Trusted Root Certificates list (see Network > Certificate Management). If the certificate is self-signed, export the certificate from the ISE pxGrid node to add below.

Certificate: Browse... No file selected. Upload File

Common name:	Certificate Services Root CA - ise22lab4
Organization:	
Organizational Unit:	
Country:	
Expiration Date:	Aug 1 00:10:13 2027 GMT
Basic Constraints:	Critical

Step 7 For **Secondary pxGrid node,** enter the IP address of the secondary pxGrid node and upload the ISE Certificate Root Services certificate



Secondary ISE pxGrid Node (optional):

The WSA will communicate with the ISE pxGrid node to support WSA data subscription (ongoing updates). Specifying a secondary ISE pxGrid node (server) is optional.

192.168.1.65 *(Hostname or IPv4 address)*

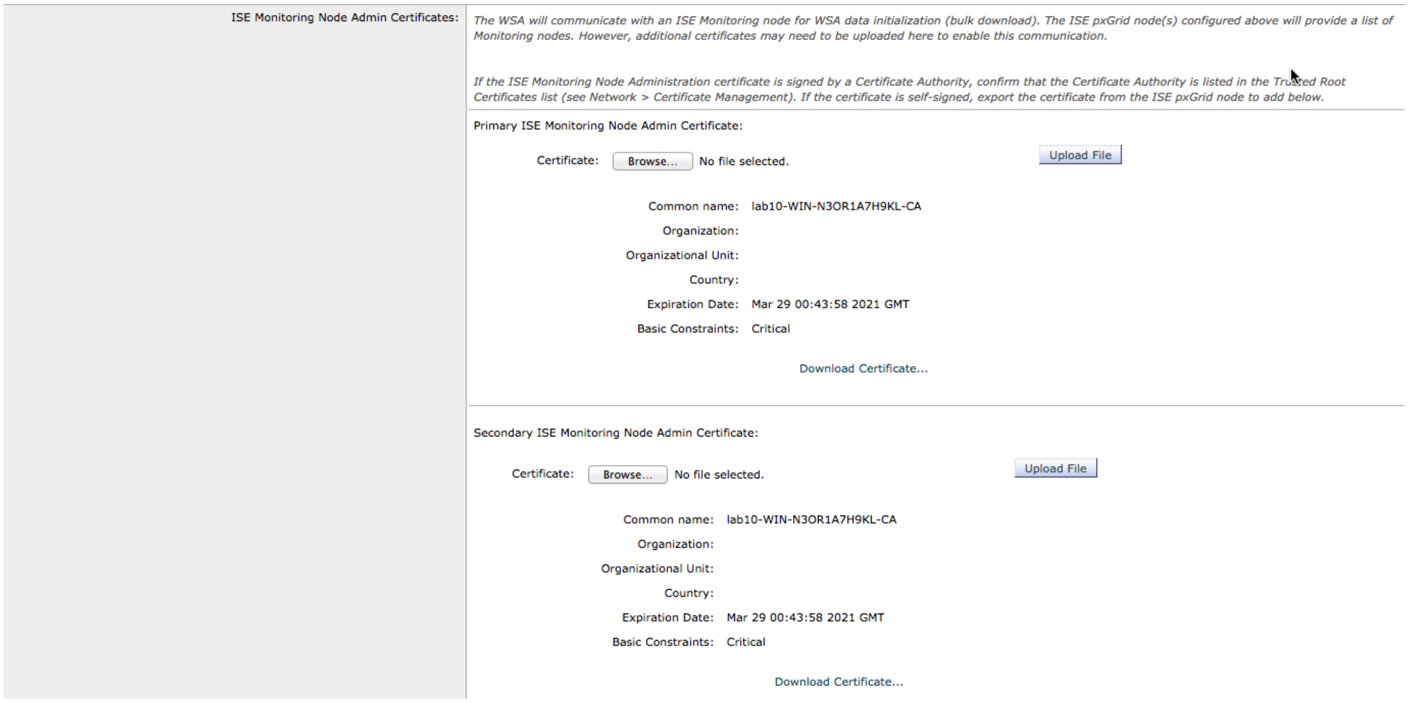
ISE pxGrid Node Certificate:

If the ISE pxGrid node certificate is signed by a Certificate Authority, confirm that the Certificate Authority is listed in the Trusted Root Certificates list (see Network > Certificate Management). If the certificate is self-signed, export the certificate from the ISE pxGrid node to add below.

Certificate: No file selected.

Common name: Certificate Services Root CA - ise22lab4
Organization:
Organizational Unit:
Country:
Expiration Date: Aug 1 00:10:13 2027 GMT
Basic Constraints: Critical

Step 8 For the ISE Monitoring Node Admin Certificate and for the primary and secondary admin node certificates, **upload the CA root certificate**, in this case, lab10-WIN-N3OR1AH9KL-CA



ISE Monitoring Node Admin Certificates:

The WSA will communicate with an ISE Monitoring node for WSA data initialization (bulk download). The ISE pxGrid node(s) configured above will provide a list of 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 Authority is listed in the Trusted Root Certificates list (see Network > Certificate Management). If the certificate is self-signed, export the certificate from the ISE pxGrid node to add below.

Primary ISE Monitoring Node Admin Certificate:

Certificate: No file selected.

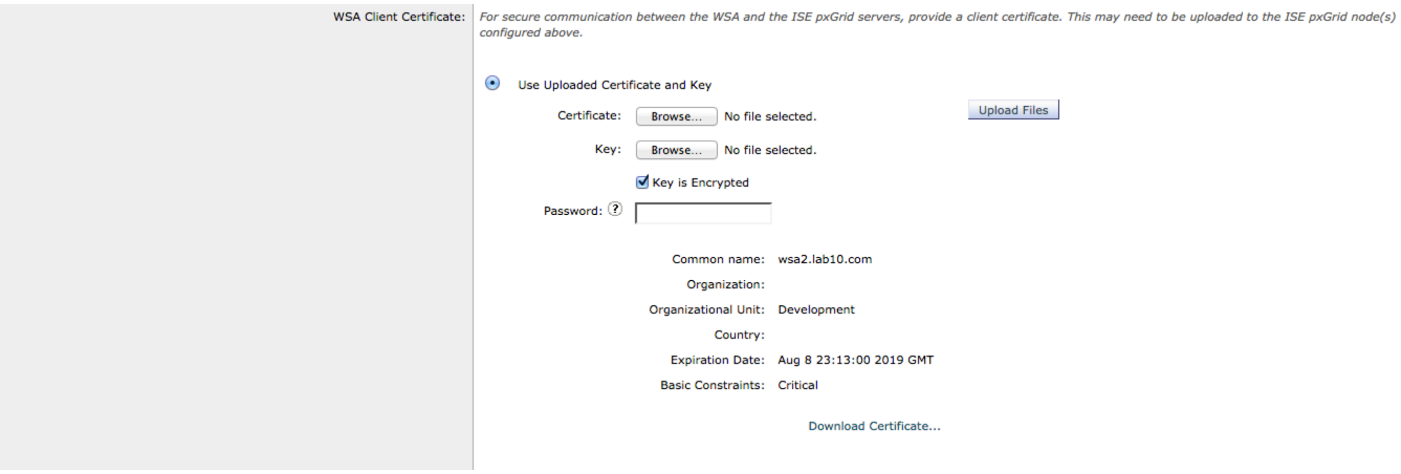
Common name: lab10-WIN-N3OR1A7H9KL-CA
Organization:
Organizational Unit:
Country:
Expiration Date: Mar 29 00:43:58 2021 GMT
Basic Constraints: Critical

Secondary ISE Monitoring Node Admin Certificate:

Certificate: No file selected.

Common name: lab10-WIN-N3OR1A7H9KL-CA
Organization:
Organizational Unit:
Country:
Expiration Date: Mar 29 00:43:58 2021 GMT
Basic Constraints: Critical

Step 9 For the WSA Client Certificate, **upload the WSA public private-key pair**, and enter the password that was entered when generating the WSA certificate from the ISE Internal CA.



WSA Client Certificate: *For secure communication between the WSA and the ISE pxGrid servers, provide a client certificate. This may need to be uploaded to the ISE pxGrid node(s) configured above.*

● Use Uploaded Certificate and Key

Certificate: Browse... No file selected. Upload Files

Key: Browse... No file selected.

☑ Key is Encrypted

Password: ?

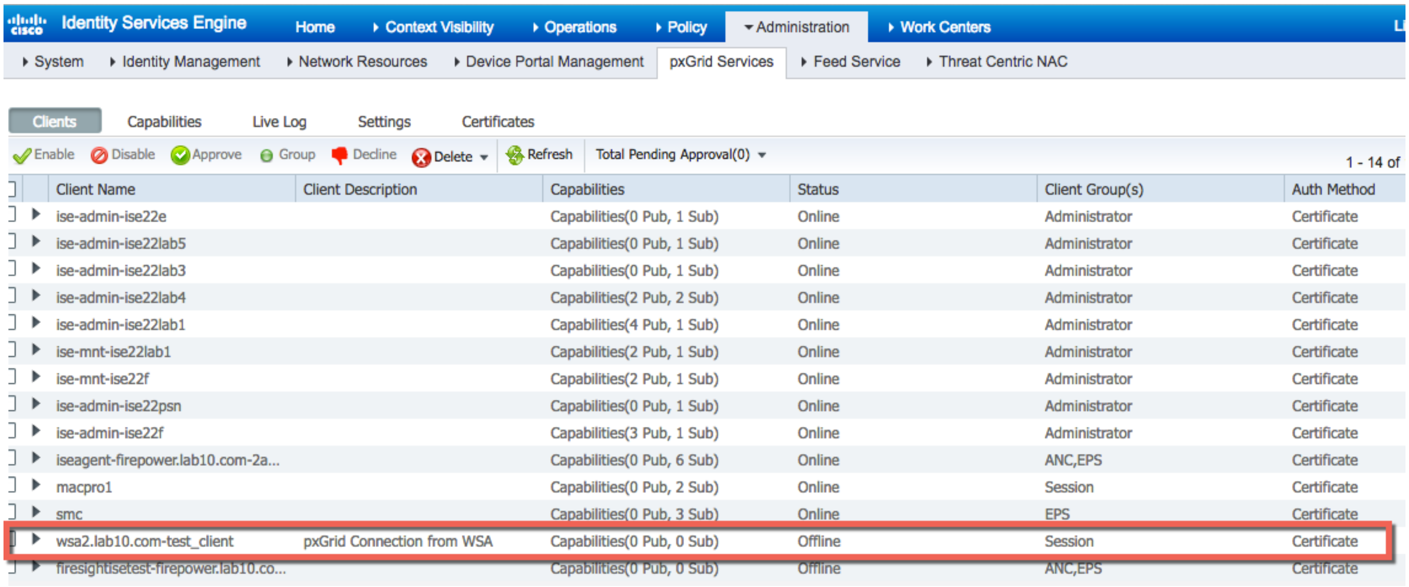
Common name: wsa2.lab10.com
Organization:
Organizational Unit: Development
Country:
Expiration Date: Aug 8 23:13:00 2019 GMT
Basic Constraints: Critical

Download Certificate...

Step 10 Select **Test**
You should see:

```
Checking DNS resolution of ISE pxGrid Node hostname(s) ...
Success: Resolved '192.168.1.187' address: 192.168.1.187
Success: Resolved '192.168.1.65' address: 192.168.1.65

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

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

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

Checking connection to ISE pxGrid Node(s) ...
Success: Connection to ISE pxGrid Node was successful.
Retrieved 17 SGTs from: 192.168.1.187

Checking connection to ISE Monitorting Node (REST server(s)) ...
Success: Connection to ISE Monitorting Node was successful.
REST Host contacted: ise22lab1.lab10.com

Test completed successfully.
```

Step 11 To verify in ISE, select **Administration->pxGrid services**



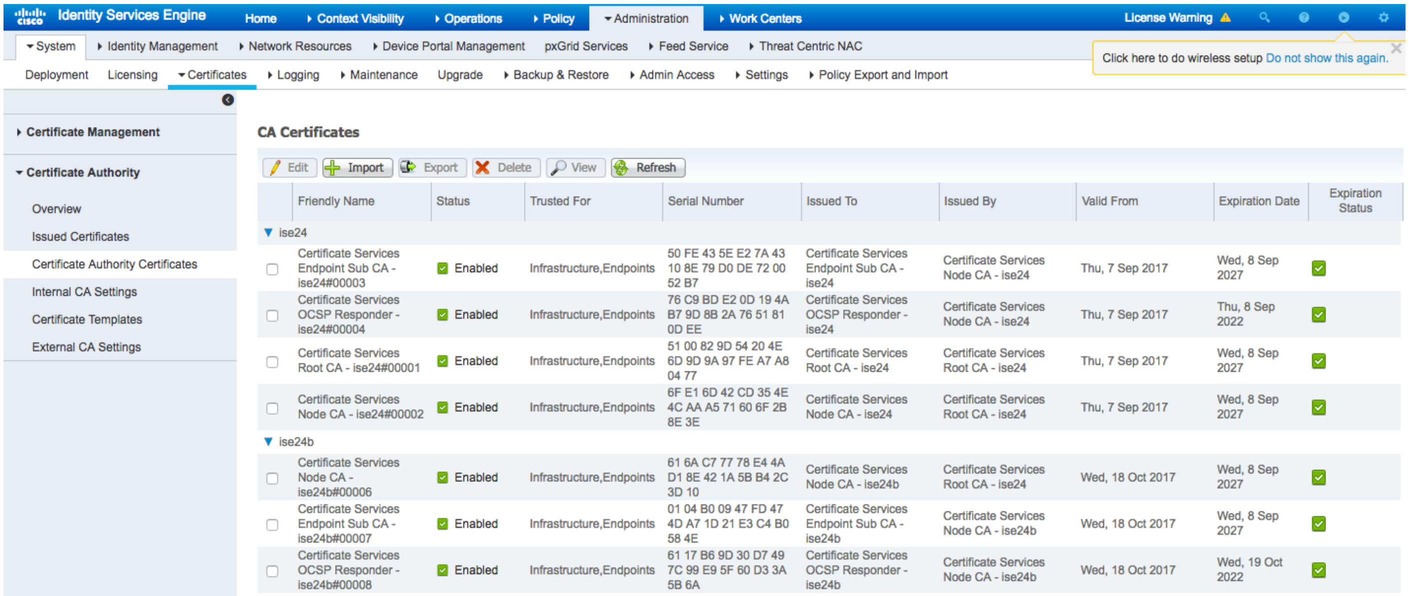
Client Name	Client Description	Capabilities	Status	Client Group(s)	Auth Method
ise-admin-ise22e		Capabilities(0 Pub, 1 Sub)	Online	Administrator	Certificate
ise-admin-ise22lab5		Capabilities(0 Pub, 1 Sub)	Online	Administrator	Certificate
ise-admin-ise22lab3		Capabilities(0 Pub, 1 Sub)	Online	Administrator	Certificate
ise-admin-ise22lab4		Capabilities(2 Pub, 2 Sub)	Online	Administrator	Certificate
ise-admin-ise22lab1		Capabilities(4 Pub, 1 Sub)	Online	Administrator	Certificate
ise-mnt-ise22lab1		Capabilities(2 Pub, 1 Sub)	Online	Administrator	Certificate
ise-mnt-ise22f		Capabilities(2 Pub, 1 Sub)	Online	Administrator	Certificate
ise-admin-ise22psn		Capabilities(0 Pub, 1 Sub)	Online	Administrator	Certificate
ise-admin-ise22f		Capabilities(3 Pub, 1 Sub)	Online	Administrator	Certificate
iseagent-firepower.lab10.com-2a...		Capabilities(0 Pub, 6 Sub)	Online	ANC,EPS	Certificate
macpro1		Capabilities(0 Pub, 2 Sub)	Online	Session	Certificate
smc		Capabilities(0 Pub, 3 Sub)	Online	EPS	Certificate
wsa2.lab10.com-test_client	pxGrid Connection from WSA	Capabilities(0 Pub, 0 Sub)	Offline	Session	Certificate
firesightisetest-firepower.lab10.co...		Capabilities(0 Pub, 0 Sub)	Offline	ANC,EPS	Certificate

pxGrid Fail-Over

There can be only 2 pxGrid nodes per ISE deployment There is a heartbeat timer between the 2 pxGrid nodes, when the primary pxGrid node goes down, the secondary pxGrid node will come up.

The primary and secondary pxGrid node contain the external CA root certificate from the initial ISE node setup. The external root certificate is required for active bulk downloads from the MNT node. In this ISE deployment all the nodes were signed by the external CA.

The ISE internal CA signs the pxGrid certificate by default, and will also sign the generated pxGrid client certificate. The ISE internal CA is trusted for all the ISE nodes.



	Friendly Name	Status	Trusted For	Serial Number	Issued To	Issued By	Valid From	Expiration Date	Expiration Status
▼ ise24									
□	Certificate Services Endpoint Sub CA - ise24#00003	☑ Enabled	Infrastructure,Endpoints	50 FE 43 5E E2 7A 43 10 8E 79 D0 DE 72 00 52 B7	Certificate Services Endpoint Sub CA - ise24	Certificate Services Node CA - ise24	Thu, 7 Sep 2017	Wed, 8 Sep 2027	☑
□	Certificate Services OCSP Responder - ise24#00004	☑ Enabled	Infrastructure,Endpoints	76 C9 BD E2 0D 19 4A B7 9D 8B 2A 76 51 81 0D EE	Certificate Services OCSP Responder - ise24	Certificate Services Node CA - ise24	Thu, 7 Sep 2017	Thu, 8 Sep 2022	☑
□	Certificate Services Root CA - ise24#00001	☑ Enabled	Infrastructure,Endpoints	51 00 82 9D 54 20 4E 6D 9D 9A 97 FE A7 A8 04 77	Certificate Services Root CA - ise24	Certificate Services Root CA - ise24	Thu, 7 Sep 2017	Wed, 8 Sep 2027	☑
□	Certificate Services Node CA - ise24#00002	☑ Enabled	Infrastructure,Endpoints	6F E1 6D 42 CD 35 4E 4C AA A5 71 60 6F 2B 8E 3E	Certificate Services Node CA - ise24	Certificate Services Root CA - ise24	Thu, 7 Sep 2017	Wed, 8 Sep 2027	☑
▼ ise24b									
□	Certificate Services Node CA - ise24b#00006	☑ Enabled	Infrastructure,Endpoints	61 6A C7 77 78 E4 4A D1 8E 42 1A 5B B4 2C 3D 10	Certificate Services Node CA - ise24b	Certificate Services Root CA - ise24	Wed, 18 Oct 2017	Wed, 8 Sep 2027	☑
□	Certificate Services Endpoint Sub CA - ise24b#00007	☑ Enabled	Infrastructure,Endpoints	01 04 B0 09 47 FD 47 4D A7 1D 21 E3 C4 B0 58 4E	Certificate Services Endpoint Sub CA - ise24b	Certificate Services Node CA - ise24b	Wed, 18 Oct 2017	Wed, 8 Sep 2027	☑
□	Certificate Services OCSP Responder - ise24b#00008	☑ Enabled	Infrastructure,Endpoints	61 17 B6 9D 30 D7 49 7C 99 E9 5F 60 D3 3A 5B 6A	Certificate Services OCSP Responder - ise24b	Certificate Services Node CA - ise24b	Wed, 18 Oct 2017	Wed, 19 Oct 2022	☑

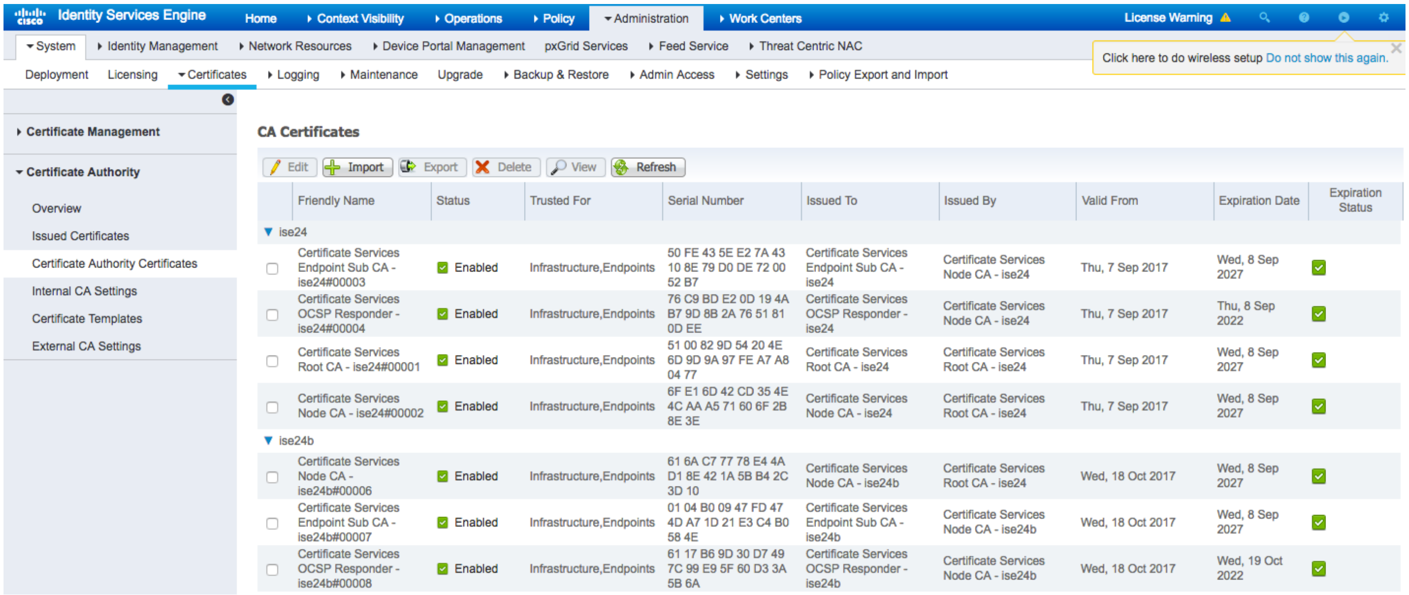
Both the external CA root certificate and internal ISE root certificate will be uploaded or imported into the trusted store.

The pxGrid client certificate public private key-pair will be uploaded or imported into the pxGrid client's trusted file store.

This can be implemented differently for each vendor but the basics still remain.

Both are in the trusted certificate store of these ISE nodes and also the rest of the ISE nodes.   The external CA root certificate will be used in the MNT configuration setting for bulk active user downloads.

The ISE internal root CA certificate will be trusted for both the primary pxGrid node and the secondary pxGrid node.

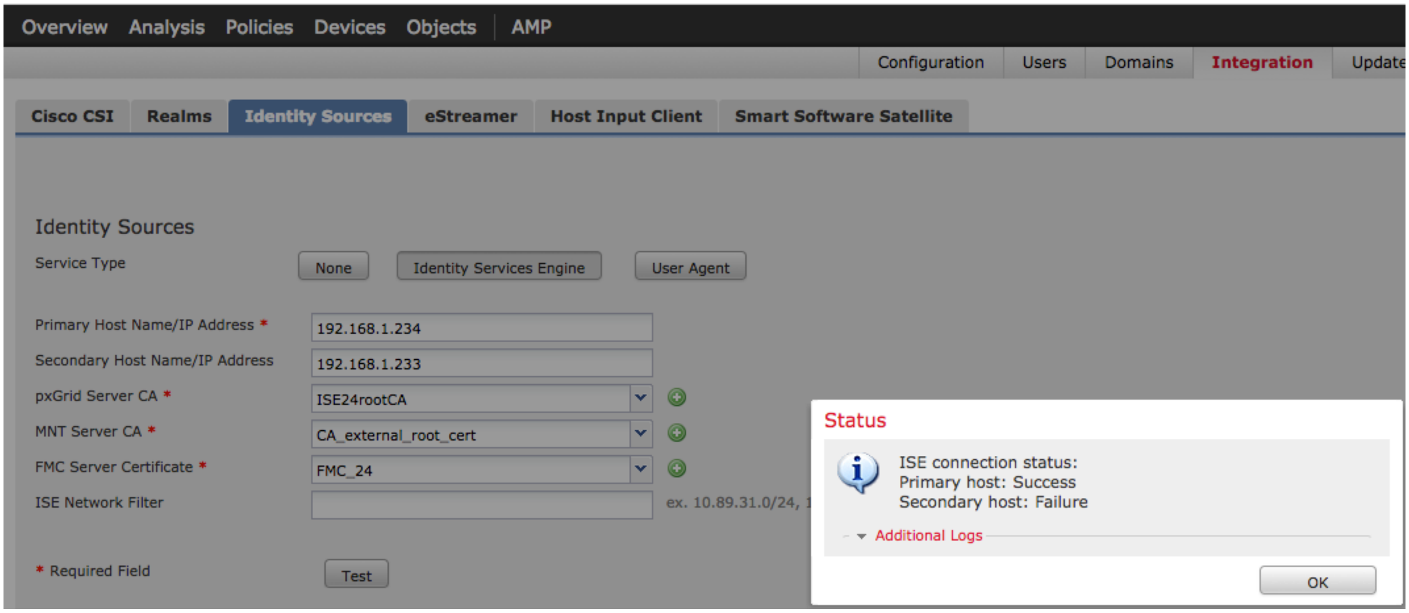


CA Certificates

	Friendly Name	Status	Trusted For	Serial Number	Issued To	Issued By	Valid From	Expiration Date	Expiration Status
▼ ise24									
□	Certificate Services Endpoint Sub CA - ise24#00003	☑ Enabled	Infrastructure,Endpoints	50 FE 43 5E E2 7A 43 10 8E 79 D0 DE 72 00 52 B7	Certificate Services Endpoint Sub CA - ise24	Certificate Services Node CA - ise24	Thu, 7 Sep 2017	Wed, 8 Sep 2027	☑
□	Certificate Services OCSP Responder - ise24#00004	☑ Enabled	Infrastructure,Endpoints	76 C9 BD E2 0D 19 4A B7 9D 8B 2A 76 51 81 0D EE	Certificate Services OCSP Responder - ise24	Certificate Services Node CA - ise24	Thu, 7 Sep 2017	Thu, 8 Sep 2022	☑
□	Certificate Services Root CA - ise24#00001	☑ Enabled	Infrastructure,Endpoints	51 00 82 9D 54 20 4E 6D 9D 9A 97 FE A7 A8 04 77	Certificate Services Root CA - ise24	Certificate Services Root CA - ise24	Thu, 7 Sep 2017	Wed, 8 Sep 2027	☑
□	Certificate Services Node CA - ise24#00002	☑ Enabled	Infrastructure,Endpoints	6F E1 6D 42 CD 35 4E 4C AA A5 71 60 6F 2B 8E 3E	Certificate Services Node CA - ise24	Certificate Services Root CA - ise24	Thu, 7 Sep 2017	Wed, 8 Sep 2027	☑
▼ ise24b									
□	Certificate Services Node CA - ise24b#00006	☑ Enabled	Infrastructure,Endpoints	61 6A C7 77 78 E4 4A D1 8E 42 1A 5B B4 2C 3D 10	Certificate Services Node CA - ise24b	Certificate Services Root CA - ise24	Wed, 18 Oct 2017	Wed, 8 Sep 2027	☑
□	Certificate Services Endpoint Sub CA - ise24b#00007	☑ Enabled	Infrastructure,Endpoints	01 04 B0 09 47 FD 47 4D A7 1D 21 E3 C4 B0 58 4E	Certificate Services Endpoint Sub CA - ise24b	Certificate Services Node CA - ise24b	Wed, 18 Oct 2017	Wed, 8 Sep 2027	☑
□	Certificate Services OCSP Responder - ise24b#00008	☑ Enabled	Infrastructure,Endpoints	61 17 B6 9D 30 D7 49 7C 99 E9 5F 60 D3 3A 5B 6A	Certificate Services OCSP Responder - ise24b	Certificate Services Node CA - ise24b	Wed, 18 Oct 2017	Wed, 19 Oct 2022	☑

Cisco Firepower Management Center (FMC) 6.2 was configured for pxGrid failover.

Note the IP addresses of the primary and secondary ISE pxGrid nodes. The pxGrid Server CA contains the ISE internal root certificate. The MNT Server CA contains the external CA root certificate. The FMC Server Certificate contains the pxGrid certificate public private key-pair that was generated by the ISE internal CA.



Identity Sources

Service Type: Identity Services Engine

Primary Host Name/IP Address *: 192.168.1.234

Secondary Host Name/IP Address: 192.168.1.233

pxGrid Server CA *: ISE24rootCA

MNT Server CA *: CA_external_root_cert

FMC Server Certificate *: FMC_24

ISE Network Filter: ex. 10.89.31.0/24, 1

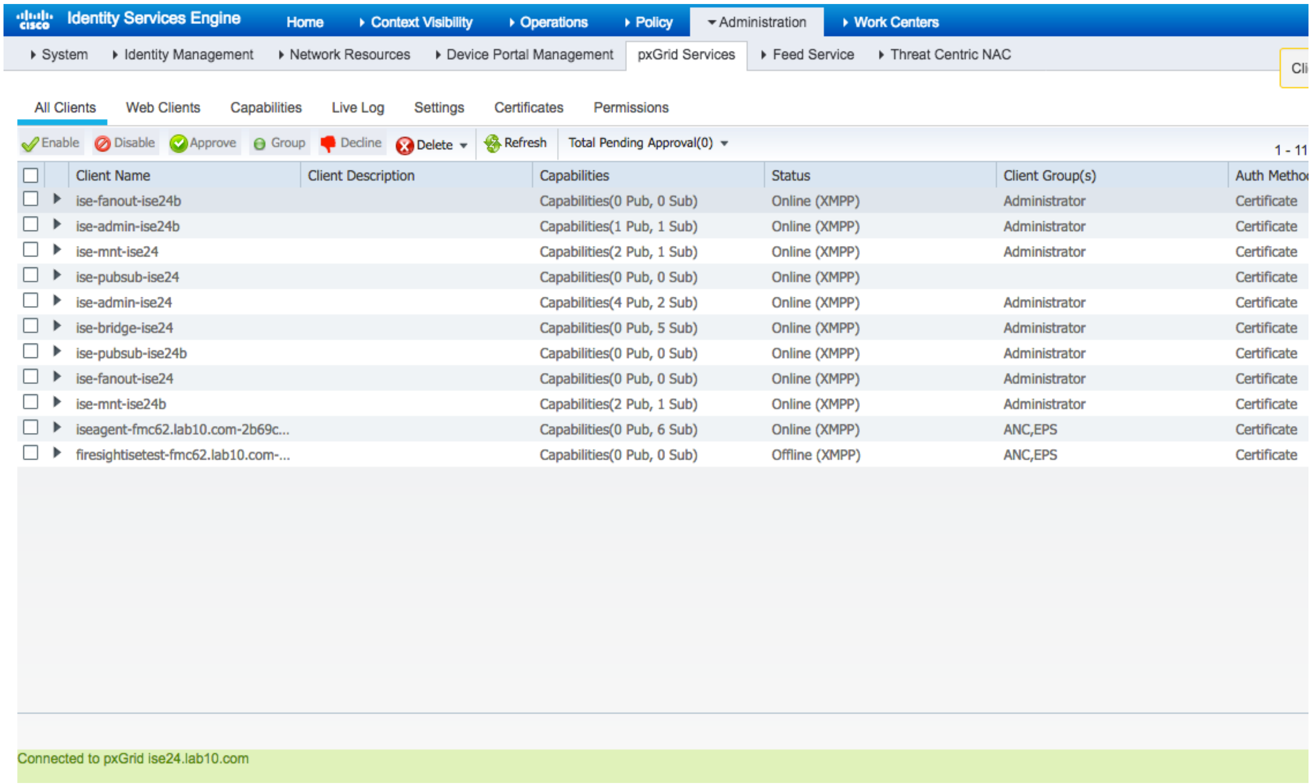
* Required Field

Status

ISE connection status:
Primary host: Success
Secondary host: Failure

Additional Logs

Below you can see the FMC pxGrid client has successfully connected and registered to the ISE primary pxGrid node.

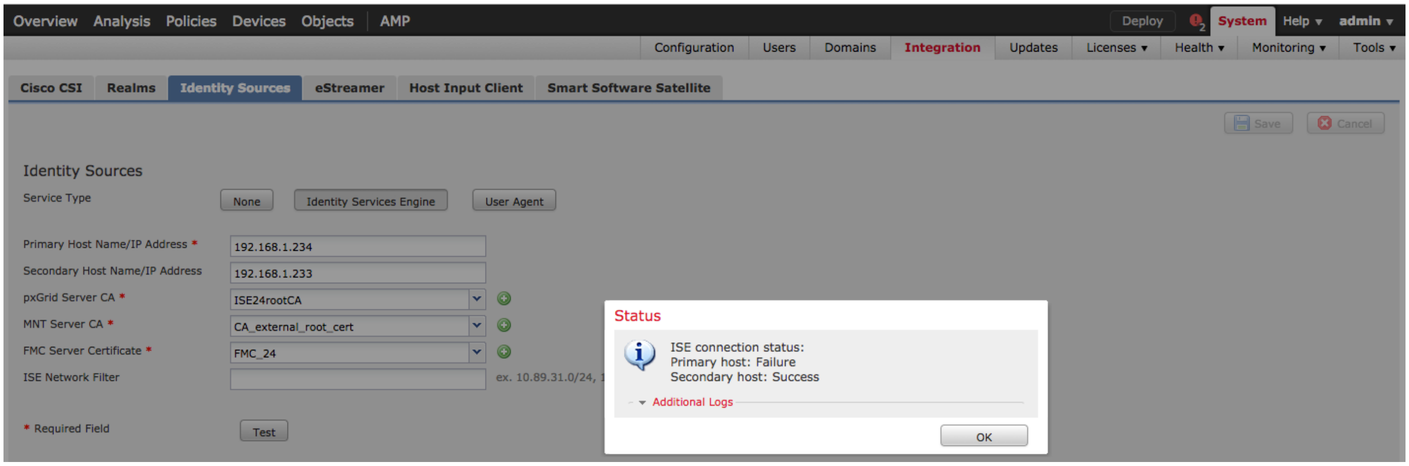


□	Client Name	Client Description	Capabilities	Status	Client Group(s)	Auth Metho
□	ise-fanout-ise24b		Capabilities(0 Pub, 0 Sub)	Online (XMPP)	Administrator	Certificate
□	ise-admin-ise24b		Capabilities(1 Pub, 1 Sub)	Online (XMPP)	Administrator	Certificate
□	ise-mnt-ise24		Capabilities(2 Pub, 1 Sub)	Online (XMPP)	Administrator	Certificate
□	ise-pubsub-ise24		Capabilities(0 Pub, 0 Sub)	Online (XMPP)		Certificate
□	ise-admin-ise24		Capabilities(4 Pub, 2 Sub)	Online (XMPP)	Administrator	Certificate
□	ise-bridge-ise24		Capabilities(0 Pub, 5 Sub)	Online (XMPP)	Administrator	Certificate
□	ise-pubsub-ise24b		Capabilities(0 Pub, 0 Sub)	Online (XMPP)	Administrator	Certificate
□	ise-fanout-ise24		Capabilities(0 Pub, 0 Sub)	Online (XMPP)	Administrator	Certificate
□	ise-mnt-ise24b		Capabilities(2 Pub, 1 Sub)	Online (XMPP)	Administrator	Certificate
□	iseagent-fmc62.lab10.com-2b69c...		Capabilities(0 Pub, 6 Sub)	Online (XMPP)	ANC,EPS	Certificate
□	firesightisetest-fmc62.lab10.com-...		Capabilities(0 Pub, 0 Sub)	Offline (XMPP)	ANC,EPS	Certificate

Connected to pxGrid ise24.lab10.com

The ISE primary pxGrid service was disabled, and the secondary pxGrid node came up.

In the FMC configuration we select **Test** to test the connection to the secondary pxGrid node.


Overview Analysis Policies Devices Objects AMP
Deploy System Help ▾ admin ▾
Configuration Users Domains Integration Updates Licenses ▾ Health ▾ Monitoring ▾ Tools ▾
Cisco CSI Realms Identity Sources eStreamer Host Input Client Smart Software Satellite
Save Cancel

Identity Sources

Service Type	None / Identity Services Engine / User Agent
Primary Host Name/IP Address *	192.168.1.234
Secondary Host Name/IP Address	192.168.1.233
pxGrid Server CA *	ISE24rootCA
MNT Server CA *	CA_external_root_cert
FMC Server Certificate *	FMC_24
ISE Network Filter	ex. 10.89.31.0/24, 1

* Required Field

Test

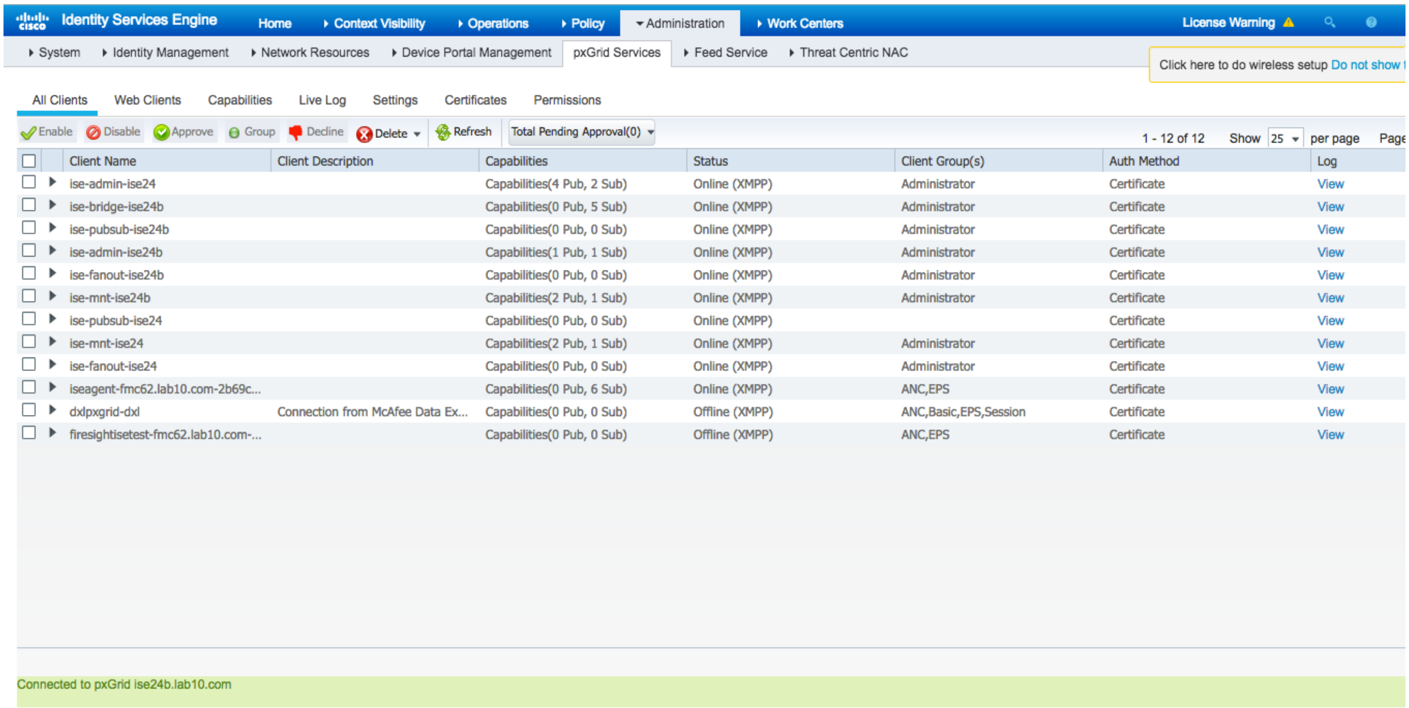
Status

ISE connection status:
Primary host: Failure
Secondary host: Success

Additional Logs

OK

As we see in the in pxGrid services, this looks good.


Identity Services Engine Home ▸ Context Visibility ▸ Operations ▸ Policy ▾ Administration ▸ Work Centers License Warning
▸ System ▸ Identity Management ▸ Network Resources ▸ Device Portal Management pxGrid Services ▸ Feed Service ▸ Threat Centric NAC
Click here to do wireless setup Do not show t
All Clients Web Clients Capabilities Live Log Settings Certificates Permissions
Enable Disable Approve Group Decline Delete ▾ Refresh Total Pending Approval(0) ▾
1 - 12 of 12 Show 25 per page Page

☐	Client Name	Client Description	Capabilities	Status	Client Group(s)	Auth Method	Log
☐	ise-admin-ise24		Capabilities(4 Pub, 2 Sub)	Online (XMPP)	Administrator	Certificate	View
☐	ise-bridge-ise24b		Capabilities(0 Pub, 5 Sub)	Online (XMPP)	Administrator	Certificate	View
☐	ise-pubsub-ise24b		Capabilities(0 Pub, 0 Sub)	Online (XMPP)	Administrator	Certificate	View
☐	ise-admin-ise24b		Capabilities(1 Pub, 1 Sub)	Online (XMPP)	Administrator	Certificate	View
☐	ise-fanout-ise24b		Capabilities(0 Pub, 0 Sub)	Online (XMPP)	Administrator	Certificate	View
☐	ise-mnt-ise24b		Capabilities(2 Pub, 1 Sub)	Online (XMPP)	Administrator	Certificate	View
☐	ise-pubsub-ise24		Capabilities(0 Pub, 0 Sub)	Online (XMPP)		Certificate	View
☐	ise-mnt-ise24		Capabilities(2 Pub, 1 Sub)	Online (XMPP)	Administrator	Certificate	View
☐	ise-fanout-ise24		Capabilities(0 Pub, 0 Sub)	Online (XMPP)	Administrator	Certificate	View
☐	iseagent-fmc62.lab10.com-2b69c...		Capabilities(0 Pub, 6 Sub)	Online (XMPP)	ANC,EPS	Certificate	View
☐	dxlpxgrid-dxl	Connection from McAfee Data Ex...	Capabilities(0 Pub, 0 Sub)	Offline (XMPP)	ANC,Basic,EPS,Session	Certificate	View
☐	firesightisetest-fmc62.lab10.com-...		Capabilities(0 Pub, 0 Sub)	Offline (XMPP)	ANC,EPS	Certificate	View

Connected to pxGrid ise24b.lab10.com

Deploying pxGrid using ISE 2.1 with Internal CA and External CA certificates for ISE nodes

This section describes the details for deploying pxGrid using the ISE Internal CA and using external CA server for the ISE deployment. The pxGrid certificate is not signed by the default ISE internal CA and needs to be provisioned by the Certificate Portal. The ISE nodes will also require provisioned pxGrid certificates.

Note: If you upgraded from a previous version of ISE, the original certificates will be maintained.

Note: If you are not using the ISE internal CA for pxGrid operation, you need to use a customized pxGrid template.

Generating CSR requests for ISE nodes

Step 1 Follow steps 1-14 for generating CSR requests for the ISE nodes for in the section **Generating CSR Requests with ISE 2.2/2.3.** This is for generating the initial ISE node CSR requests and getting them signed by the external CA server.

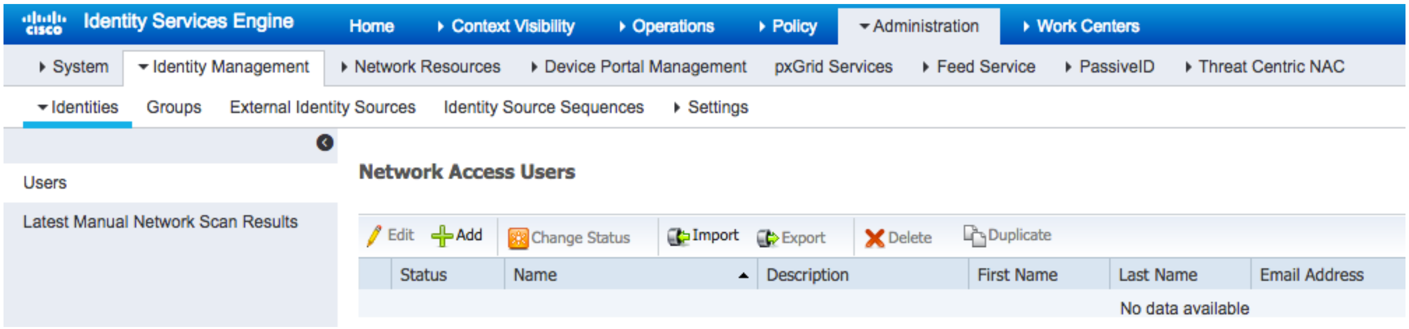
Registering ISE nodes

Step 1 Follow steps 1-30 for registering the ISE nodes in the section **Registering ISE Nodes in ISE 2.2/2.3.** For the pxGrid primary and secondary pxGrid nodes, register them initially as PSN nodes. We will enable them as dedicated pxGrid nodes later on, once they are provisioned from the Certificate Portal.

Certificate Provisioning

This section details the procedure for provisioning the certificate portal if the Internal CA will be used for pxGrid operation.

Step 1 Select **Administration->Identity Management->Identities**

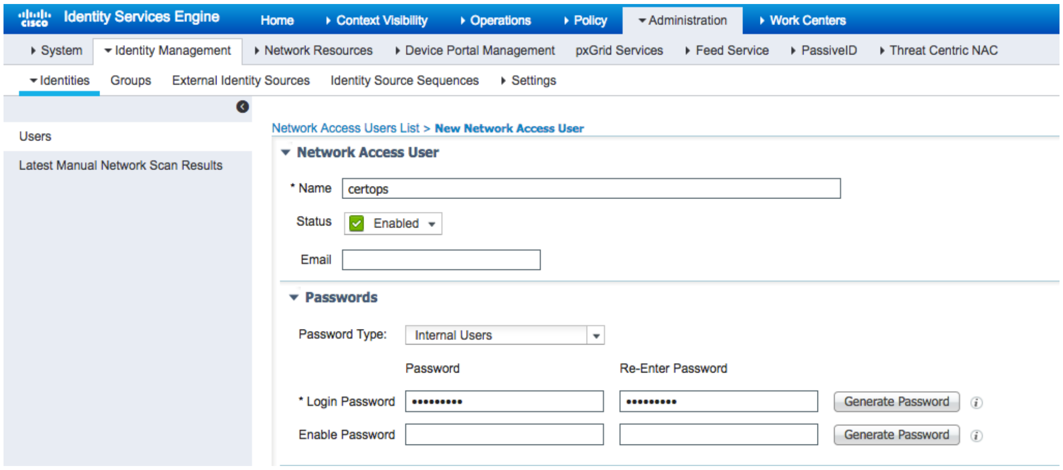


Network Access Users

Status	Name	Description	First Name	Last Name	Email Address
				No data available	

Step 2 Select **Add**

Step 3 Enter **Username** and **password**



Network Access Users List > New Network Access User

Network Access User

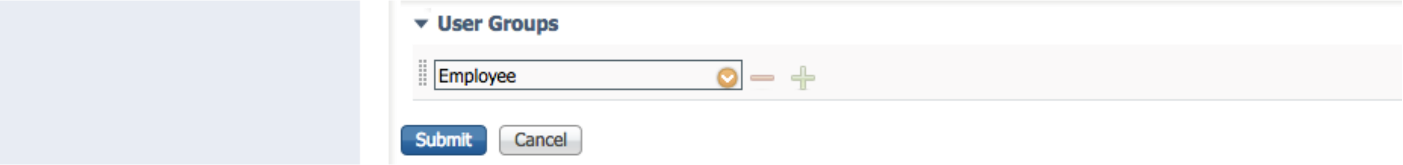
* Name	certops
Status	☑ Enabled
Email	

Passwords

Password Type: Internal Users

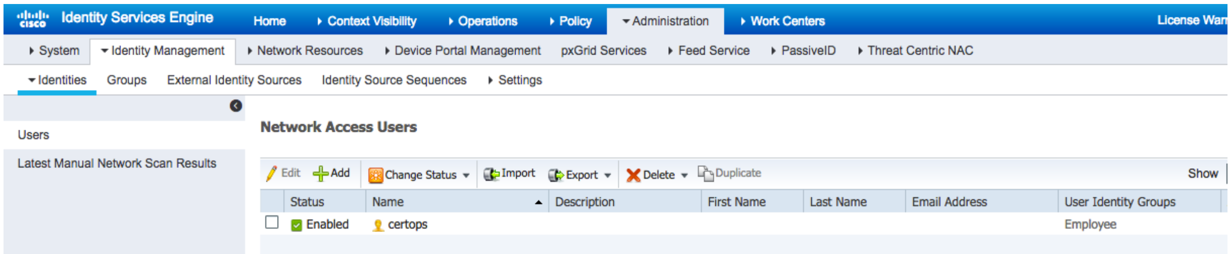
	Password	Re-Enter Password
* Login Password	•••••••••	•••••••••
Enable Password		

Step 4 Select **Employee** Group


User Groups

Employee

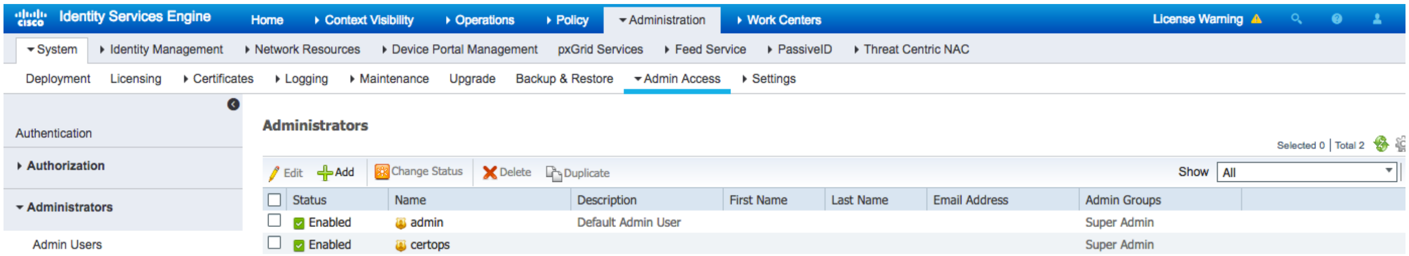
Step 5 Select **Submit**
You should see:



Network Access Users

	Status	Name	Description	First Name	Last Name	Email Address	User Identity Groups
□	☑ Enabled	certops					Employee

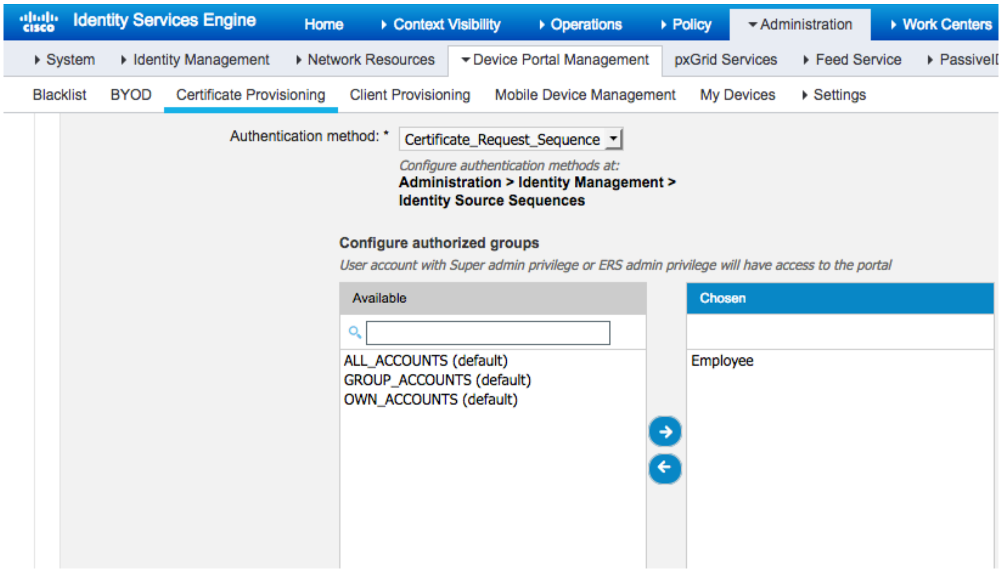
Step 6 Select **Administration->System->Admin Access->Administrators->Admin Users->Add->Select from Network Users->certops->Admin Groups->Super Admin->Save**



Administrators

□	Status	Name	Description	First Name	Last Name	Email Address	Admin Groups
□	☑ Enabled	admin	Default Admin User				Super Admin
□	☑ Enabled	certops					Super Admin

Step 7 Select **Administration->Device Portal Management->Certificate Provisioning->Certificate Provisioning Portal(Default)->Select Portal Settings->Configure Authorized Groups->Employee->move to Chosen**



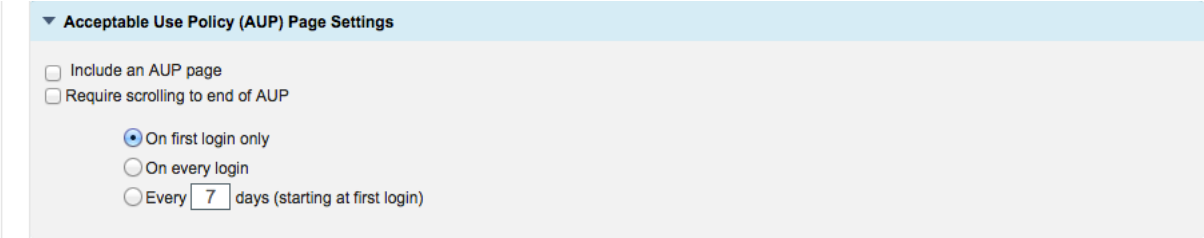
Authentication method: * Certificate_Request_Sequence

Configure authentication methods at:
Administration > Identity Management > Identity Source Sequences

Configure authorized groups
User account with Super admin privilege or ERS admin privilege will have access to the portal

Available	Chosen
ALL_ACCOUNTS (default) GROUP_ACCOUNTS (default) OWN_ACCOUNTS (default)	Employee

Step 8 Select **Acceptable Usage Policy (AUP) Page Settings**, **uncheck** “Include an AUP page”

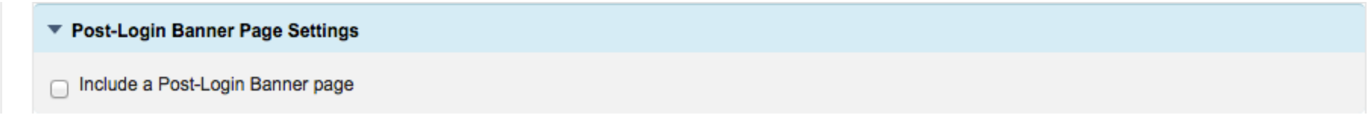


Acceptable Use Policy (AUP) Page Settings

□ Include an AUP page
□ Require scrolling to end of AUP

● On first login only
○ On every login
○ Every 7 days (starting at first login)

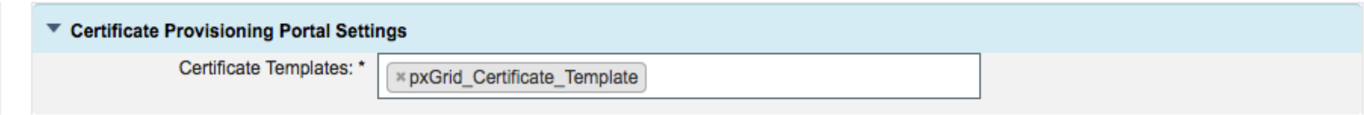
Step 9 Select **Post Login Banner Page Settings**, **uncheck** “Include Post-Login Banner Page Settings”



Post-Login Banner Page Settings

□ Include a Post-Login Banner page

Step 10 Select **Certificate Provisioning Portal Settings**, under Certificate Template, select pxGrid certificate template



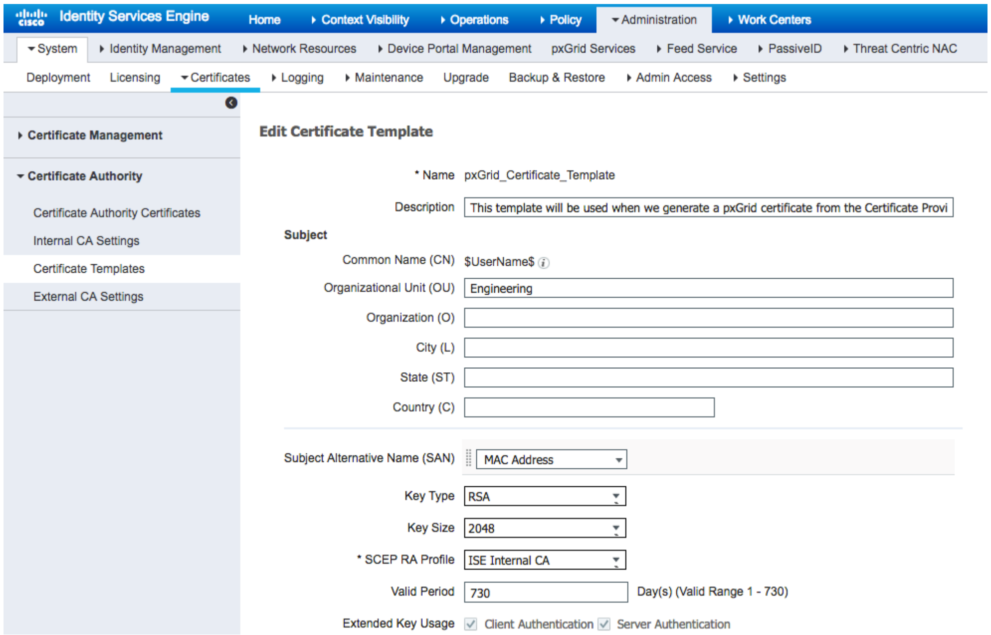
Certificate Provisioning Portal Settings

Certificate Templates: * × pxGrid_Certificate_Template

Step 11 Select **Save**

Generate pxGrid certificate for ISE nodes

Step 1 Configure OU field for Engineering pxGrid template
Select **Administration->System->Certificates->Certificate Authority->Certificate Templates->pxGrid template->edit->add "Engineering" to OU field**



Edit Certificate Template

* Name pxGrid_Certificate_Template

Description This template will be used when we generate a pxGrid certificate from the Certificate Provi

Subject

Common Name (CN) $UserName$

Organizational Unit (OU) Engineering

Organization (O)

City (L)

State (ST)

Country (C)

Subject Alternative Name (SAN) MAC Address

Key Type RSA

Key Size 2048

* SCEP RA Profile ISE Internal CA

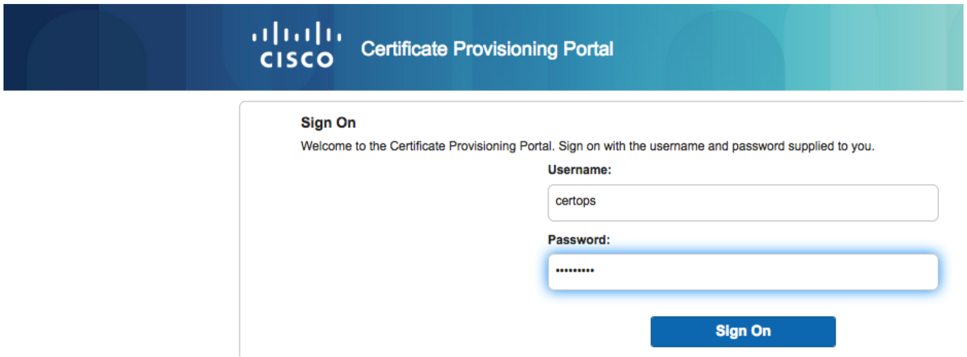
Valid Period 730 Day(s) (Valid Range 1 - 730)

Extended Key Usage ☑ Client Authentication ☑ Server Authentication

Note: It is important to enter Engineering or populate the OU field so it does not contain the same parameters in the OU field of the ISE admin certificates. You do not want to overwrite the admin certificate

Step 2 Select **Save**

Step 3 Select **Administration->Device Portal Management->Certificate Provisioning->Certificate Provisioning Portal (default)-Portal Test URL->login "certops**



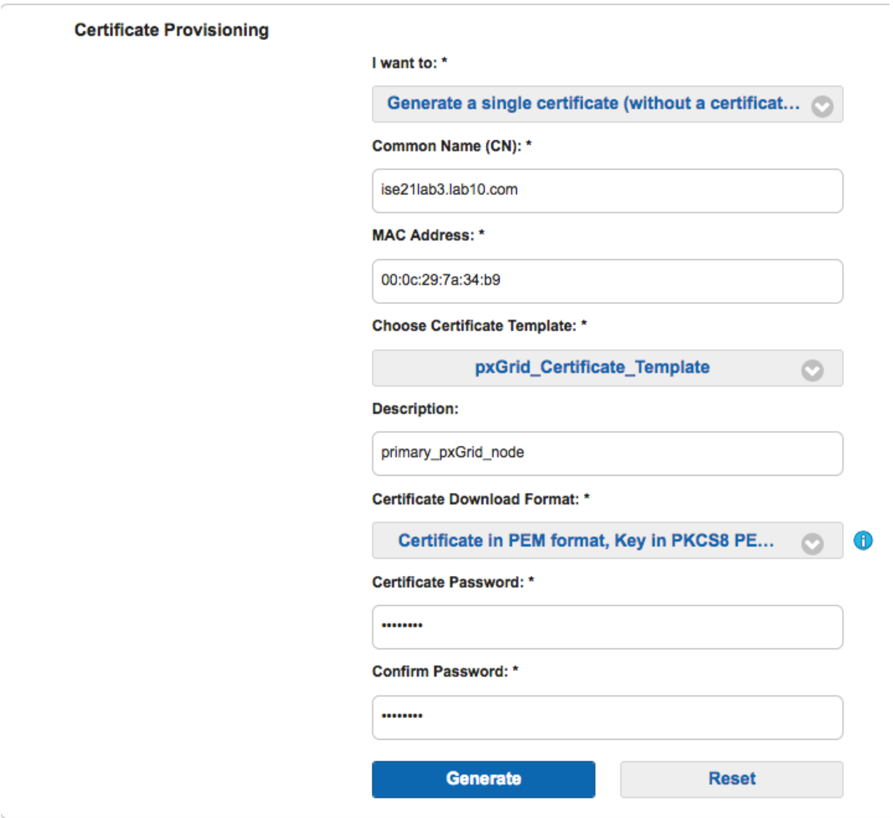
Sign On

Welcome to the Certificate Provisioning Portal. Sign on with the username and password supplied to you.

Username: certops

Password: ••••••••

Step 4 Select **Certificate Provisioning** and enter the Fully Qualified Domain Names (FQDN) for the Common Name (CN) field details for the ISE node. Also select **Certificate in PEM format, key in PKCS8 PEM format** for certificate download format.



Certificate Provisioning

I want to: * Generate a single certificate (without a certificat...

Common Name (CN): * ise21lab3.lab10.com

MAC Address: * 00:0c:29:7a:34:b9

Choose Certificate Template: * pxGrid_Certificate_Template

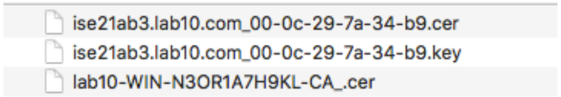
Description: primary_pxGrid_node

Certificate Download Format: * Certificate in PEM format, Key in PKCS8 PE...

Certificate Password: * ••••••••

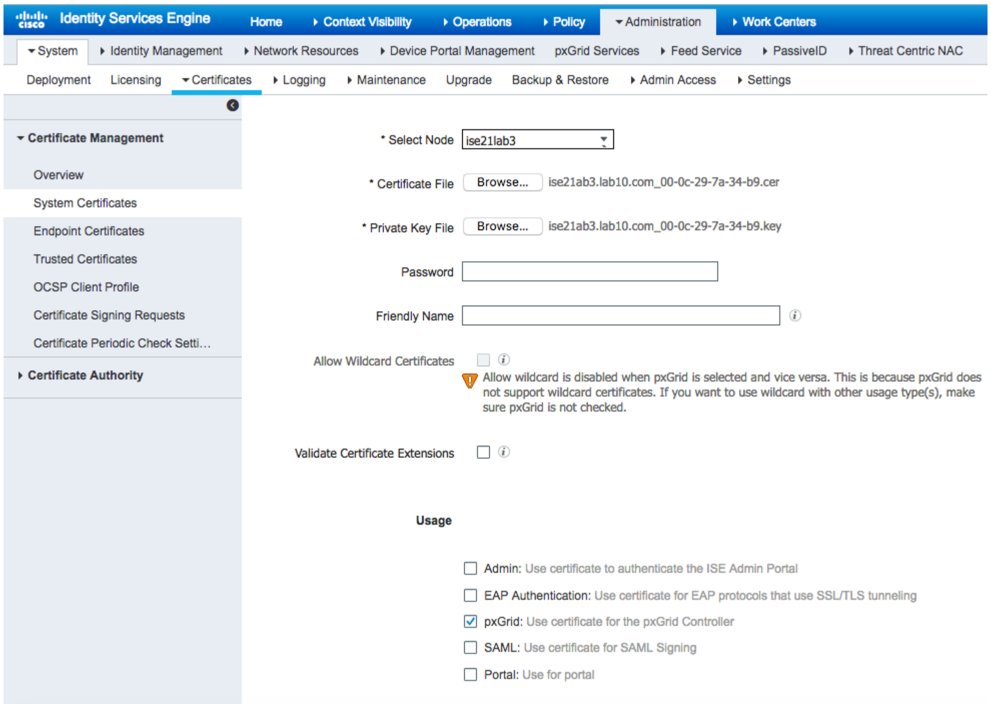
Confirm Password: * ••••••••

Step 5 Select **Generate**, and save the file locally
You should see



ise21ab3.lab10.com_00-0c-29-7a-34-b9.cer
ise21ab3.lab10.com_00-0c-29-7a-34-b9.key
lab10-WIN-N3OR1A7H9KL-CA_.cer

Step 6 Import the pxGrid public private key-pair, for the desired ISE pxGrid node, that will become the primary pxGrid dedicated node
Select **Administration->System->Certificates->Certificate Management->System Certificates->Import->select the desired pxGrid node**



* Select Node: ise21lab3

* Certificate File: Browse... ise21ab3.lab10.com_00-0c-29-7a-34-b9.cer

* Private Key File: Browse... ise21ab3.lab10.com_00-0c-29-7a-34-b9.key

Password:

Friendly Name:

Allow Wildcard Certificates □

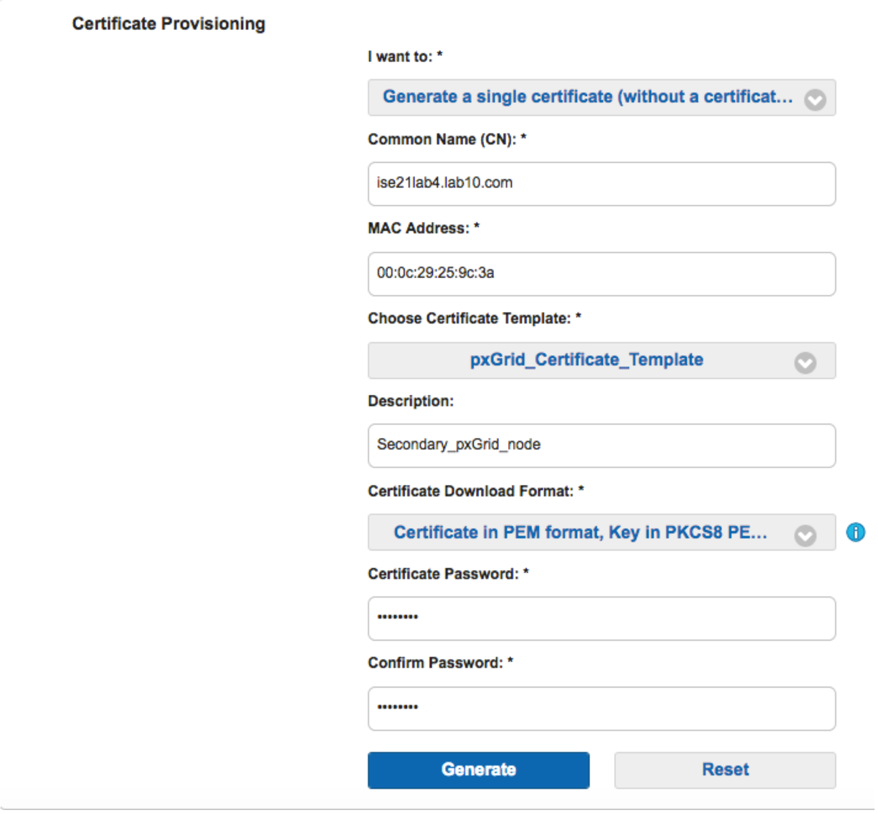
Allow wildcard is disabled when pxGrid is selected and vice versa. This is because pxGrid does not support wildcard certificates. If you want to use wildcard with other usage type(s), make sure pxGrid is not checked.

Validate Certificate Extensions □

Usage

□ Admin: Use certificate to authenticate the ISE Admin Portal
□ EAP Authentication: Use certificate for EAP protocols that use SSL/TLS tunneling
☑ pxGrid: Use certificate for the pxGrid Controller
□ SAML: Use certificate for SAML Signing
□ Portal: Use for portal

Step 7 For the secondary pxGrid node, generate another certificate


Certificate Provisioning

I want to: * Generate a single certificate (without a certificat...

Common Name (CN): * ise21lab4.lab10.com

MAC Address: * 00:0c:29:25:9c:3a

Choose Certificate Template: * pxGrid_Certificate_Template

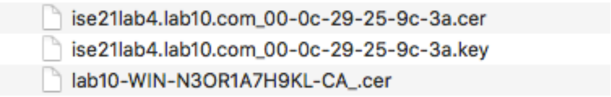
Description: Secondary_pxGrid_node

Certificate Download Format: * Certificate in PEM format, Key in PKCS8 PE...

Certificate Password: * ••••••••

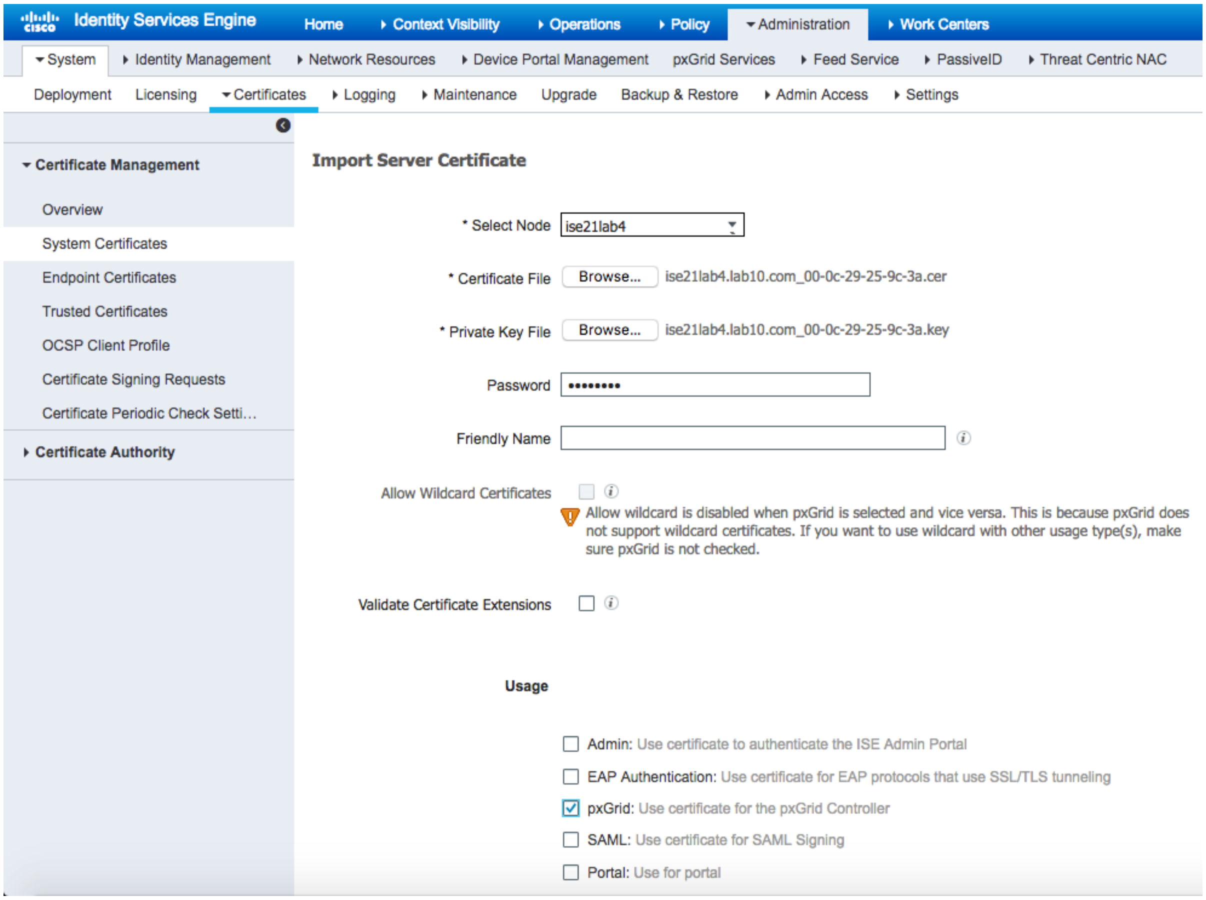
Confirm Password: * ••••••••

Step 8 Download and unzip the file
You should see



ise21lab4.lab10.com_00-0c-29-25-9c-3a.cer
ise21lab4.lab10.com_00-0c-29-25-9c-3a.key
lab10-WIN-N3OR1A7H9KL-CA_.cer

Step 9 Import the pxGrid public private key-pair, for the desired ISE secondary pxGrid node, that will become the pxGrid dedicated node
Select **Administration->System->Certificates->Certificate Management->System Certificates->Import->select the desired pxGrid node**



Import Server Certificate

* Select Node: ise21lab4

* Certificate File: ise21lab4.lab10.com_00-0c-29-25-9c-3a.cer

* Private Key File: ise21lab4.lab10.com_00-0c-29-25-9c-3a.key

Password: ••••••••

Friendly Name:

Allow Wildcard Certificates ☐
Allow wildcard is disabled when pxGrid is selected and vice versa. This is because pxGrid does not support wildcard certificates. If you want to use wildcard with other usage type(s), make sure pxGrid is not checked.

Validate Certificate Extensions ☐

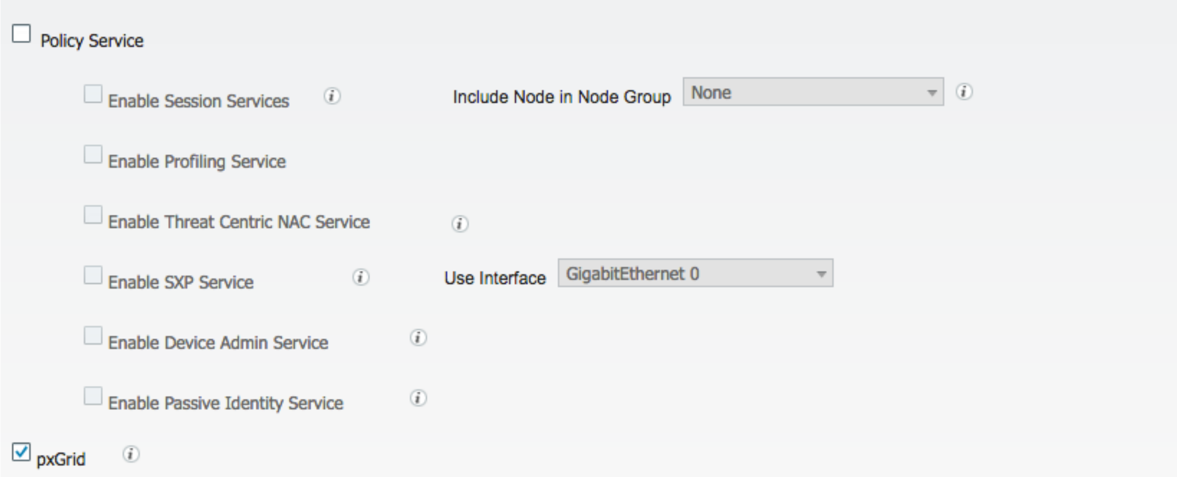
Usage

☐ Admin: Use certificate to authenticate the ISE Admin Portal
☐ EAP Authentication: Use certificate for EAP protocols that use SSL/TLS tunneling
☑ pxGrid: Use certificate for the pxGrid Controller
☐ SAML: Use certificate for SAML Signing
☐ Portal: Use for portal

Step 10 Select **Submit**

Step 11 Follow steps 2-10 to generate the certificates and import the public private-key pair for the ISE primary pxGrid node.

Step 12 Enable pxGrid on the desired PSN node that will be used for the primary pxGrid node, and remove the PSN persona.
Select **Administration->System->Deployment-edit the node, remove PSN and enable pxGrid**



☐ Policy Service

☐ Enable Session Services — Include Node in Node Group: None

☐ Enable Profiling Service

☐ Enable Threat Centric NAC Service

☐ Enable SXP Service — Use Interface: GigabitEthernet 0

☐ Enable Device Admin Service

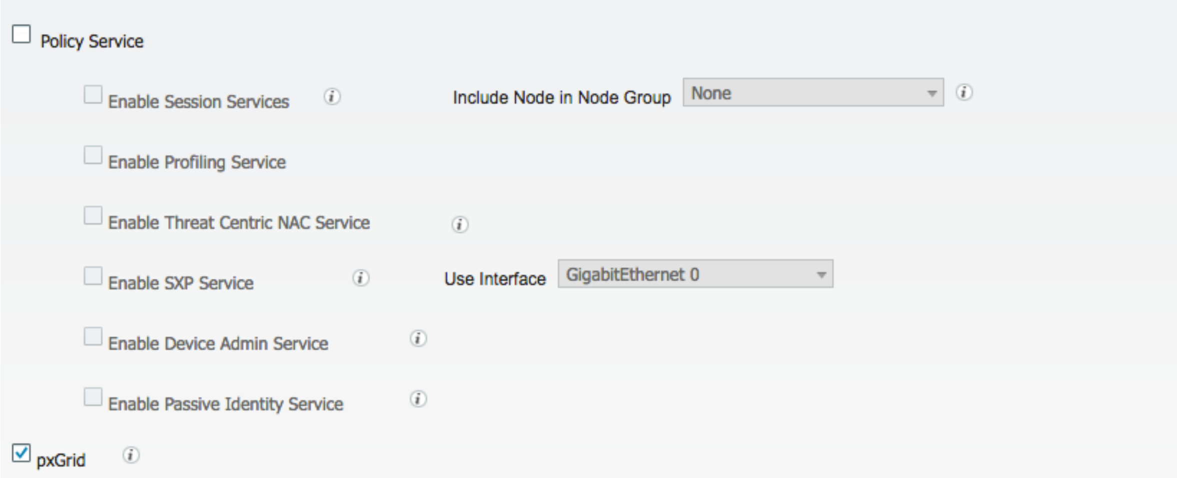
☐ Enable Passive Identity Service

☑ pxGrid

Step 13 Select **Save**

Step 14 Follow steps 2-10 to generate the certificates and import the public private-key pair for the ISE secondary pxGrid node.

Step 15 Enable pxGrid on the desired PSN node that will be used for the secondary pxGrid node, and remove the PSN persona.
Select **Administration->System->Deployment-edit the node, remove PSN and enable pxGrid**



☐ Policy Service

☐ Enable Session Services — Include Node in Node Group: None

☐ Enable Profiling Service

☐ Enable Threat Centric NAC Service

☐ Enable SXP Service — Use Interface: GigabitEthernet 0

☐ Enable Device Admin Service

☐ Enable Passive Identity Service

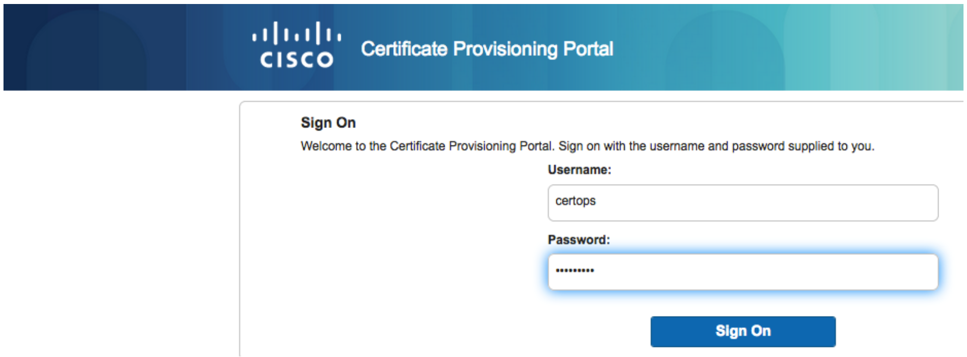
☑ pxGrid

Step 16 Select **Save**

Step 17 Follow steps 2-10 to generate the certificates and import the public private-key pair for the ISE primary admin node, secondary admin, primary MNT and secondary MNT nodes.

Testing pxGrid Integration with FMC 6.2

Step 1 Select **Administration->Device Portal Management->Certificate Provisioning->CertificateProvisioning Portal (default)-Portal Test URL->login "certops"**



Certificate Provisioning Portal

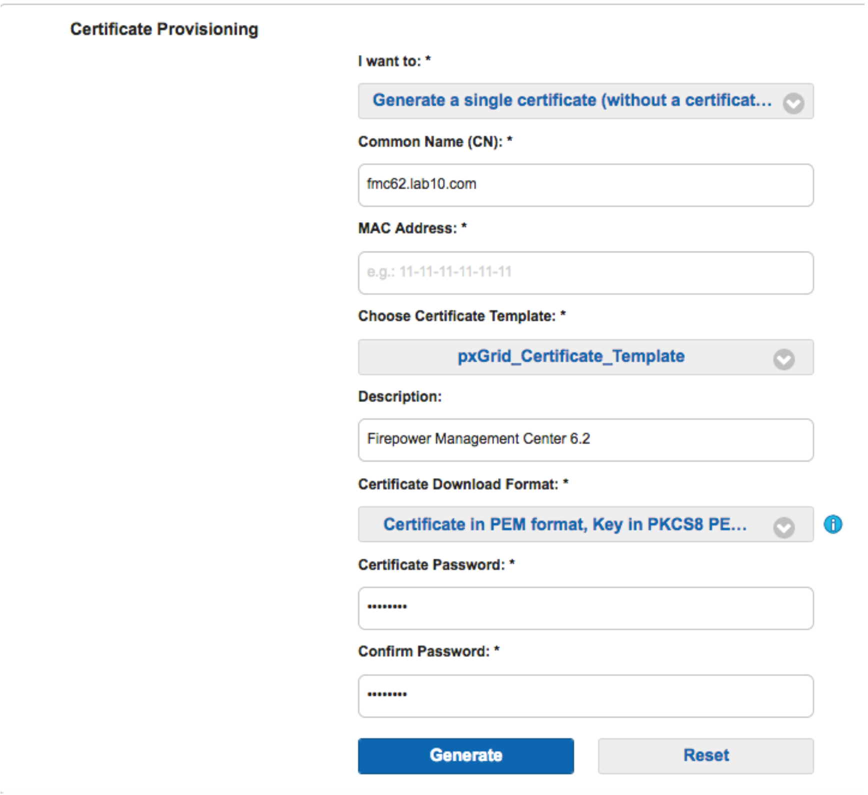
Sign On

Welcome to the Certificate Provisioning Portal. Sign on with the username and password supplied to you.

Username: certops

Password: ••••••••••

Step 2 Select **Certificate Provisioning** and enter the Fully Qualified Domain Names (FQDN) for the Common Name (CN) field details for the FMC



Certificate Provisioning

I want to: * Generate a single certificate (without a certificat...

Common Name (CN): * fmc62.lab10.com

MAC Address: * e.g.: 11-11-11-11-11-11

Choose Certificate Template: * pxGrid_Certificate_Template

Description: Firepower Management Center 6.2

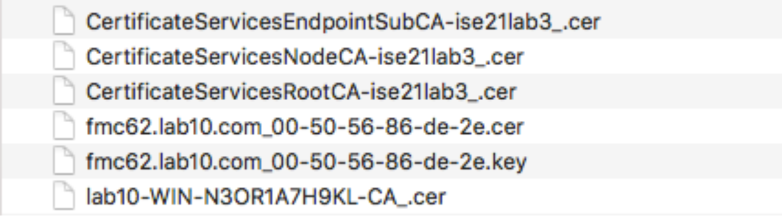
Certificate Download Format: * Certificate in PEM format, Key in PKCS8 PE...

Certificate Password: * ••••••••

Confirm Password: * ••••••••

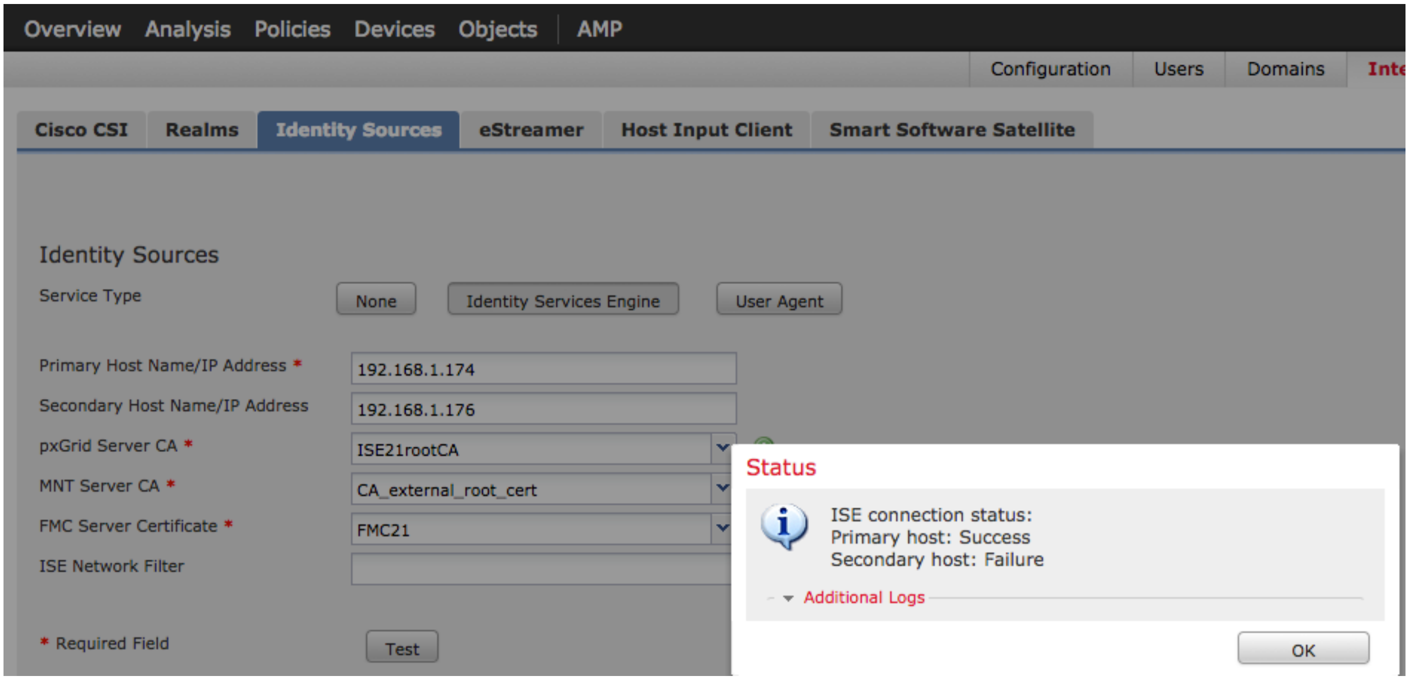
Step 3 Select **Generate**

Step 4 You should see:



CertificateServicesEndpointSubCA-ise21lab3_.cer
CertificateServicesNodeCA-ise21lab3_.cer
CertificateServicesRootCA-ise21lab3_.cer
fmc62.lab10.com_00-50-56-86-de-2e.cer
fmc62.lab10.com_00-50-56-86-de-2e.key
lab10-WIN-N3OR1A7H9KL-CA_.cer

Step 5 Select **System->Integration->Identity Sources**
Enter the primary and secondary pxGrid host IP address
The pxGrid Server CA is the CertificateServicesRootCA-ise21ab3_.cer
The MNT Server CA is the external root certificate



Identity Sources

Service Type

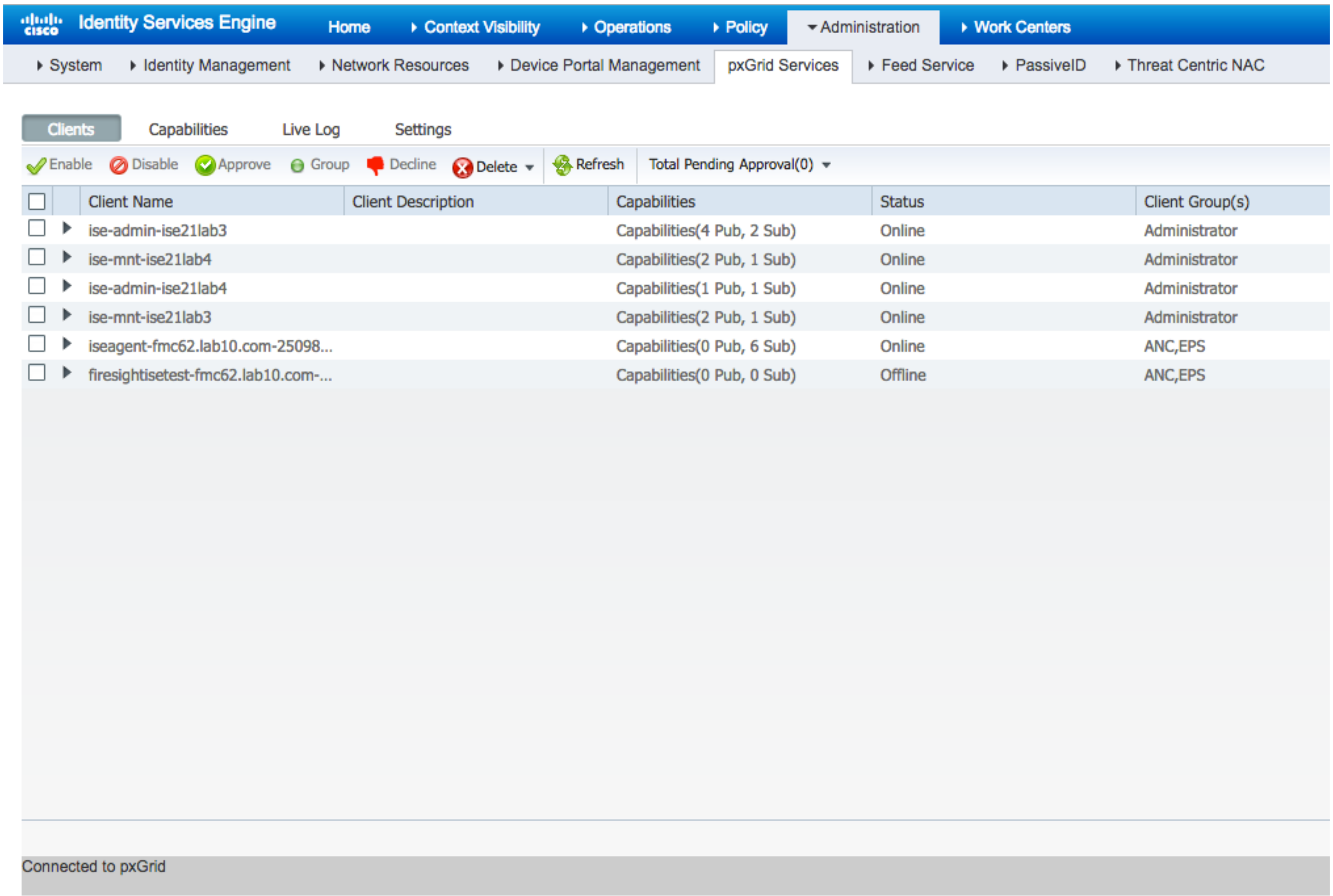
Primary Host Name/IP Address * 192.168.1.174
Secondary Host Name/IP Address 192.168.1.176
pxGrid Server CA * ISE21rootCA
MNT Server CA * CA_external_root_cert
FMC Server Certificate * FMC21
ISE Network Filter

* Required Field

Status

ISE connection status:
Primary host: Success
Secondary host: Failure

Step 6 Select Administration->pxGrid Services

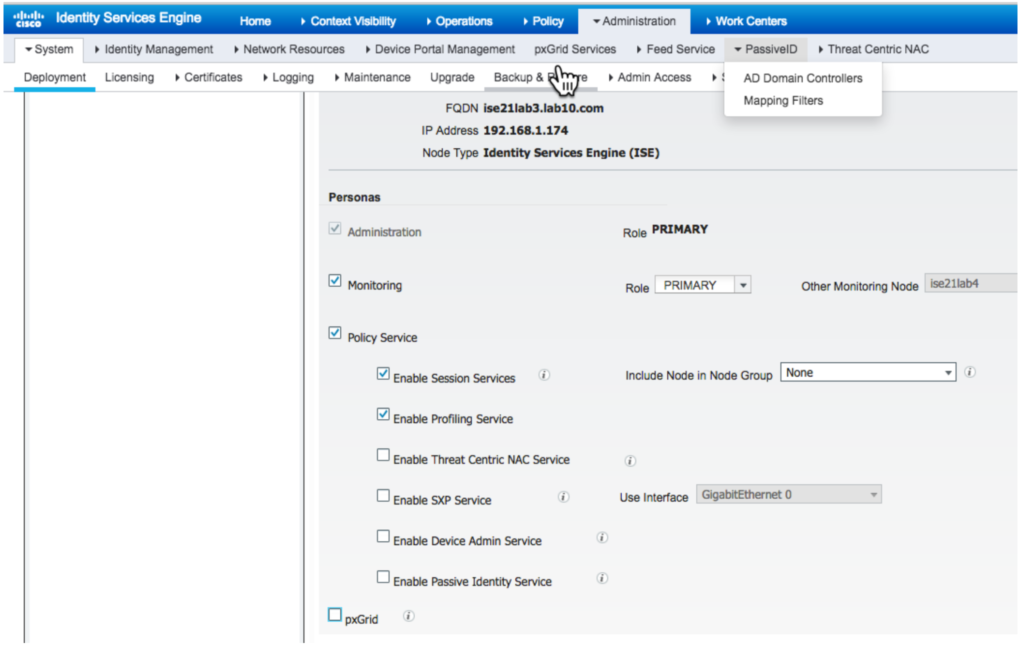


□		Client Name	Client Description	Capabilities	Status	Client Group(s)
□	▸	ise-admin-ise21lab3		Capabilities(4 Pub, 2 Sub)	Online	Administrator
□	▸	ise-mnt-ise21lab4		Capabilities(2 Pub, 1 Sub)	Online	Administrator
□	▸	ise-admin-ise21lab4		Capabilities(1 Pub, 1 Sub)	Online	Administrator
□	▸	ise-mnt-ise21lab3		Capabilities(2 Pub, 1 Sub)	Online	Administrator
□	▸	iseagent-fmc62.lab10.com-25098...		Capabilities(0 Pub, 6 Sub)	Online	ANC,EPS
□	▸	firesightisetest-fmc62.lab10.com-...		Capabilities(0 Pub, 0 Sub)	Offline	ANC,EPS

Connected to pxGrid

Step 7 Disable the primary pxGrid node

Select **Administration->System->Deployments->edit the primary pxGrid node, disable pxGrid**



FQDN **ise21lab3.lab10.com**

IP Address **192.168.1.174**

Node Type **Identity Services Engine (ISE)**

Personas

☑ Administration — Role **PRIMARY**

☑ Monitoring — Role PRIMARY — Other Monitoring Node ise21lab4

☑ Policy Service

☑ Enable Session Services — Include Node in Node Group None

☑ Enable Profiling Service

□ Enable Threat Centric NAC Service

□ Enable SXP Service — Use Interface GigabitEthernet 0

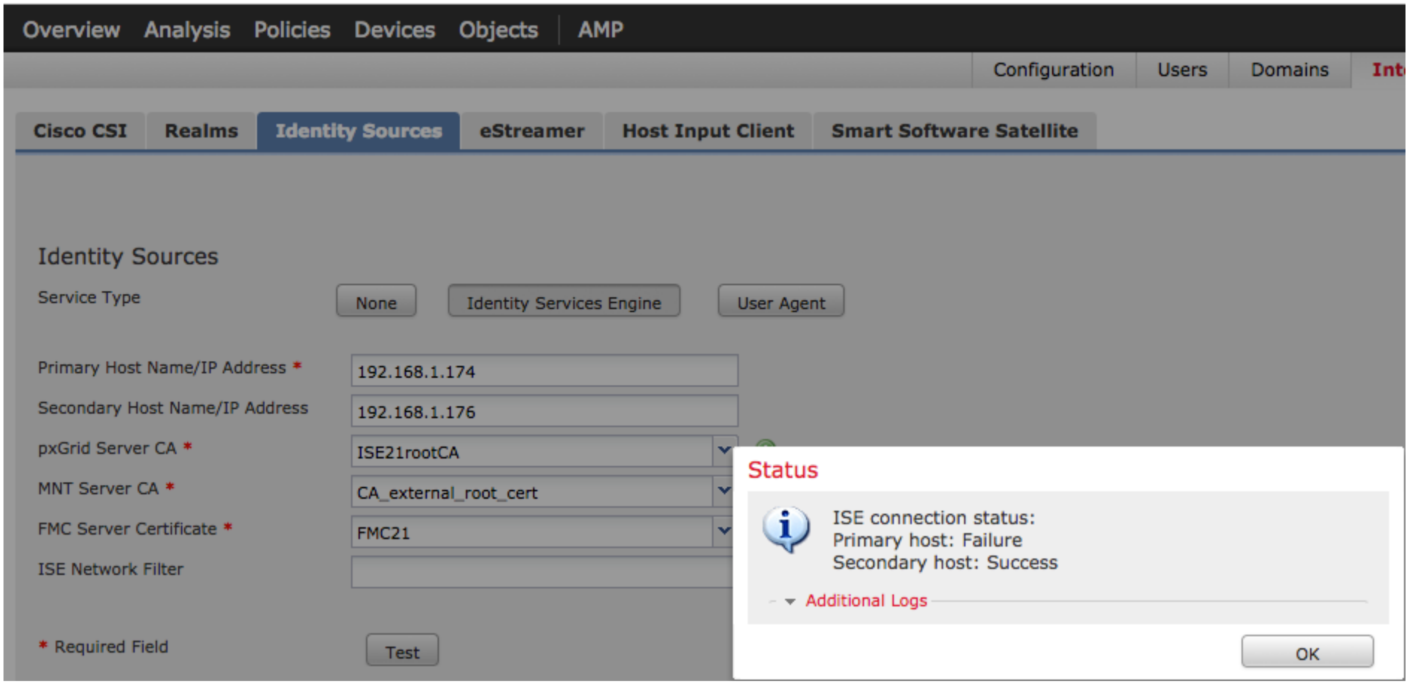
□ Enable Device Admin Service

□ Enable Passive Identity Service

□ pxGrid

Step 8 Select **Save**

Step 9 The secondary pxGrid node will come up. Run “sh application status ise” to see the ISE pxGrid services come up.



Identity Sources

Service Type: Identity Services Engine

Primary Host Name/IP Address *: 192.168.1.174

Secondary Host Name/IP Address: 192.168.1.176

pxGrid Server CA *: ISE21rootCA

MNT Server CA *: CA_external_root_cert

FMC Server Certificate *: FMC21

ISE Network Filter:

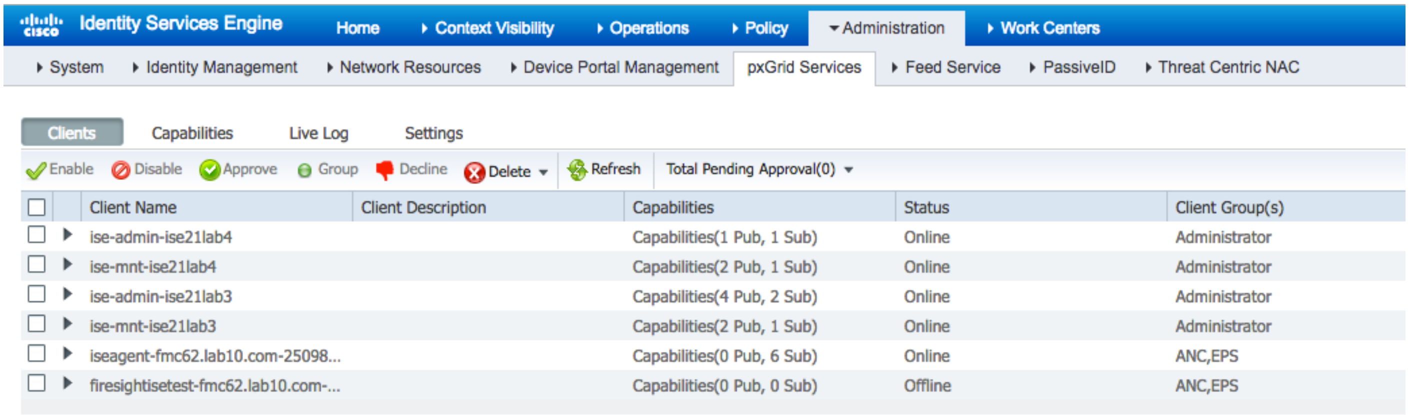
* Required Field

Status

ISE connection status:
Primary host: Failure
Secondary host: Success

Additional Logs

Step 10 You should see the pxGrid published nodes
Select **Administration->pxGrid Services**



□	Client Name	Client Description	Capabilities	Status	Client Group(s)
□	ise-admin-ise21lab4		Capabilities(1 Pub, 1 Sub)	Online	Administrator
□	ise-mnt-ise21lab4		Capabilities(2 Pub, 1 Sub)	Online	Administrator
□	ise-admin-ise21lab3		Capabilities(4 Pub, 2 Sub)	Online	Administrator
□	ise-mnt-ise21lab3		Capabilities(2 Pub, 1 Sub)	Online	Administrator
□	iseagent-fmc62.lab10.com-25098...		Capabilities(0 Pub, 6 Sub)	Online	ANC,EPS
□	firesightisetest-fmc62.lab10.com-...		Capabilities(0 Pub, 0 Sub)	Offline	ANC,EPS

Testing pxGrid Integration with Java-based pxGrid Client

This section details the procedure for configuring java-based pxGrid solution vendors with ISE 2.1 with pxGrid using the Internal CA for pxGrid operation. The solution vendor certificates will be generated by the ISE internal CA.

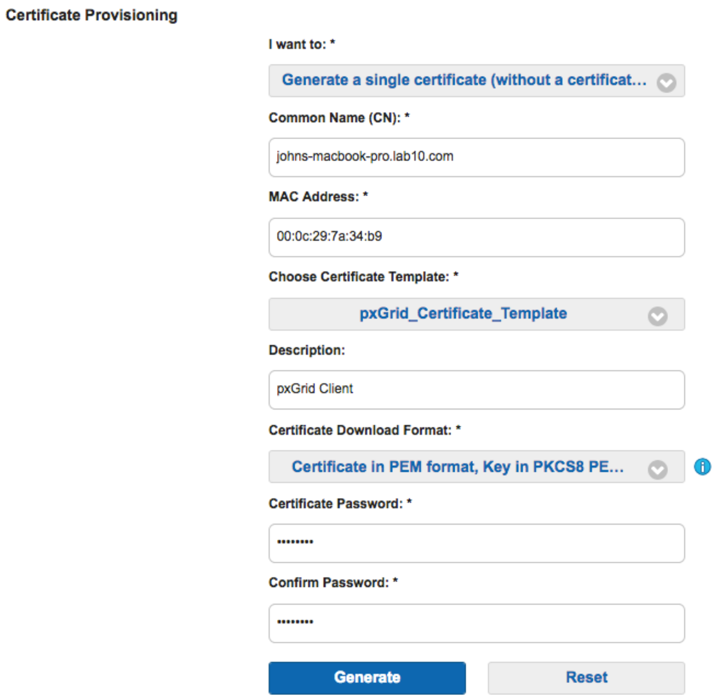
We will create the trust file keystore filename test008.jks and trust root store filename test008_root.jks, password for both Cisco123

If the ecosystem security solution does not support certificate encryption, the private key must be decrypted, below is the procedure and use firepower certificate public private key-pair as example

Note: Firepower supports certificate encryption, we just use it here as a CLI example.

```
cp firepower.lab10.com_00-0c-29-80-27-8a.key firepower.lab10.com_00-0c-29-80-27-8a.key.org
openssl rsa -in firepower.lab10.com_00-0c-29-80-27-8a.key.org -out firepower.lab10.com_00-0c-29-80-27-8a.key
```

Step 1 Generate the pxGrid client certificate, here we use the certificate we created for Firepower.



Certificate Provisioning

I want to: * Generate a single certificate (without a certificat...

Common Name (CN): * johns-macbook-pro.lab10.com

MAC Address: * 00:0c:29:7a:34:b9

Choose Certificate Template: * pxGrid_Certificate_Template

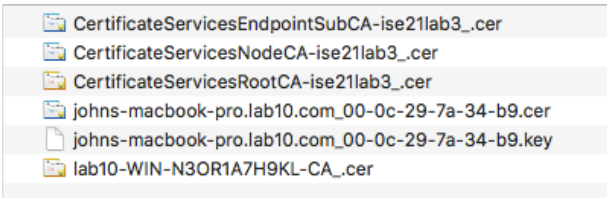
Description: pxGrid Client

Certificate Download Format: * Certificate in PEM format, Key in PKCS8 PE...

Certificate Password: * ••••••••

Confirm Password: * ••••••••

Step 2 Download the certificate you should see:



CertificateServicesEndpointSubCA-ise21lab3_.cer
CertificateServicesNodeCA-ise21lab3_.cer
CertificateServicesRootCA-ise21lab3_.cer
johns-macbook-pro.lab10.com_00-0c-29-7a-34-b9.cer
johns-macbook-pro.lab10.com_00-0c-29-7a-34-b9.key
lab10-WIN-N3OR1A7H9KL-CA_.cer

Step 3 Concatenate files into one certificate

```
cat CertificateServicesEndpointSubCA-ise21lab3_.cer CertificateServicesRootCA-
ise21lab3_.cer CertificateServicesNodeCA-ise21lab3_.cer lab10-WIN-N3OR1A7H9KL-CA_.cer > CA1.cer
```

Step 4 Create PKCS12 file

Note: The passphrase is the password that was typed when generating the certificates from the ISE internal CA

```
openssl pkcs12 -export -out pxGrid.p12 -inkey johns-macbook-pro.lab10.com_00-0c-29-7a-34-b9.key –in johns-
macbook-pro.lab10.com_00-0c-29-7a-34-b9.cer -chain -CAfile CA1.cer

Enter pass phrase for firepower.lab10.com_00-0c-29-80-27-8a.key: Cisco123
Enter Export Password: Cisco123
Verifying - Enter Export Password: Cisco123
```

Step 5 Import PKCS file into keystore

```
keytool -importkeystore -srckeystore pxGrid.p12 -destkeystore test008.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
```

Step 6 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 7 Import the converted CA root certificate in DER format to trusted keystore

```
keytool -import -alias pxGrid1 -keystore test008_root.jks -file CA1.der
Enter keystore password:  Cisco123
Re-enter new password: Cisco123
Owner: CN=Certificate Services Endpoint Sub CA - ise21lab3
Issuer: CN=Certificate Services Node CA - ise21lab3
Serial number: 109b2c4872244d9694707f48079b1446
Valid from: Sun Jul 30 20:10:30 EDT 2017 until: Sun Jul 31 20:10:26 EDT 2022
Certificate fingerprints:
         MD5:  3E:76:5C:6D:8C:26:3B:8F:5B:C4:C0:40:A4:3F:D4:B6
         SHA1: 1B:BC:2A:65:44:1D:D3:D8:97:97:90:9B:25:27:23:16:C2:8D:62:5D
         SHA256:
45:3C:E9:F7:83:25:A9:11:B9:AB:00:A8:BA:0E:B3:DC:0E:3E:40:28:C2:7C:8D:C8:78:54:8A:03:97:B9:01:74
         Signature algorithm name: SHA256withRSA
         Version: 3

Extensions:

#1: ObjectId: 2.5.29.35 Criticality=false
AuthorityKeyIdentifier [
KeyIdentifier [
0000: F4 7F 2E 7B D4 DB 5C 1A   74 09 51 EB 25 24 4E 0F  ......\.t.Q.%$N.
0010: 74 7E 50 54                                        t.PT
]
[CN=Certificate Services Root CA - ise21lab1]
SerialNumber: [    46c64293 c0d94c8c ba9d37f3 6830037d]
]
```

```
#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: 0C 67 46 A2 FA A1 90 35   0E 51 02 A5 9F 46 13 36  .gF....5.Q...F.6
0010: 1E D0 26 7F                                        ..&.
]
]

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

Step 8 Import the pxGrid client certificate into the trusted file keystore

```
keytool -import -alias pxGrid2 -keystore test008.jks -file johns-macbook-pro.lab10.com_00-0c-29-7a-34-b9.cer
Enter keystore password:  Cisco123
Certificate already exists in keystore under alias <1>
Do you still want to add it? [no]:  yes
Certificate was added to keystore
```

Step 9 Import the CA root certificate to trusted root keystore

```
keytool -import -alias pxGrid3 -keystore test008_root.jks -file CA1.cer
Enter keystore password:  Cisco123
Certificate already exists in keystore under alias <macpro1>
Do you still want to add it? [no]:  yes
Certificate was added to keystore
```

Step 10 Import the CertificateServicesRoot certificate into trusted root keystore

```
keytool -import -alias pxGrid4 -keystore test008_root.jks -file CertificateServicesRootCA-ise21lab3_.cer
Enter keystore password: Cisco123
Owner: CN=Certificate Services Root CA - ise21lab3
Issuer: CN=Certificate Services Root CA - ise21lab3
Serial number: 655ffcd9c3cd4fce8462fdc6062c0ea9
Valid from: Sun Jul 30 20:10:13 EDT 2017 until: Sat Jul 31 20:10:13 EDT 2027
Certificate fingerprints:
         MD5:  E6:78:C1:87:BA:47:FE:FB:81:00:A6:40:81:28:57:1F
         SHA1: 07:6B:0D:C7:C3:4F:39:9F:42:E7:2B:9F:33:0A:0D:55:3B:2E:D5:50
         SHA256:
6F:1D:F6:81:D5:AB:CE:EB:72:A4:89:AD:70:BA:11:BD:49:48:57:16:F1:53:A5:1E:E2:34:2E:8D:FD:A5:2D:5B
         Signature algorithm name: SHA256withRSA
         Version: 3

Extensions:

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

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

#3: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: 33 9E 4A 44 BB 04 1B B9   13 C8 F4 00 F8 DC F9 78  3.JD..........x
0010: 6C 17 6F 00                                        l.o.
]
]

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

Step 11 Import the external CA root certificate into trusted root keystore

```
keytool -import -alias pxGrid5 -keystore test008_root.jks -file lab10-WIN-N3OR1A7H9KL-CA_.cer
Enter keystore password:  Cisco123
Owner: CN=lab10-WIN-N3OR1A7H9KL-CA, DC=lab10, DC=com
Issuer: CN=lab10-WIN-N3OR1A7H9KL-CA, DC=lab10, DC=com
Serial number: 6f0fce547462b29a4e866b88536b829d
Valid from: Mon Mar 28 20:33:59 EDT 2016 until: Sun Mar 28 20:43:58 EDT 2021
Certificate fingerprints:
         MD5:  7E:6E:B2:3A:8F:00:17:19:F1:A9:23:C9:F5:C8:B8:25
         SHA1: EA:01:AB:89:F4:A7:77:75:23:0A:29:81:10:D8:AA:F9:02:79:3B:CB
         SHA256:
6A:4C:8E:76:FF:E8:8C:C5:1D:22:5B:ED:4C:E2:7E:8F:A3:55:C4:16:DA:D6:A4:4A:EA:27:47:A4:87:77:25:42
         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: 16 EB 8F 72 43 0F 41 9B   68 16 F9 12 10 7E 86 73  ...rC.A.h......s
0010: 3F 01 1B E1                                        ?...
]
]

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

Step 12 Run Session_download script or the ecosystem partner solution

Note: The session_download sample script is not required for testing. The security vendor should be able to download active session information if supported in their configuration.

The session_download sample script is part of the pxGrid SDK(pxGrid 1.0) which can be downloaded from https://developer.cisco.com/site/pxgrid/. You will need to register which is no cost. For script reference, please see: https://communities.cisco.com/docs/DOC-68291

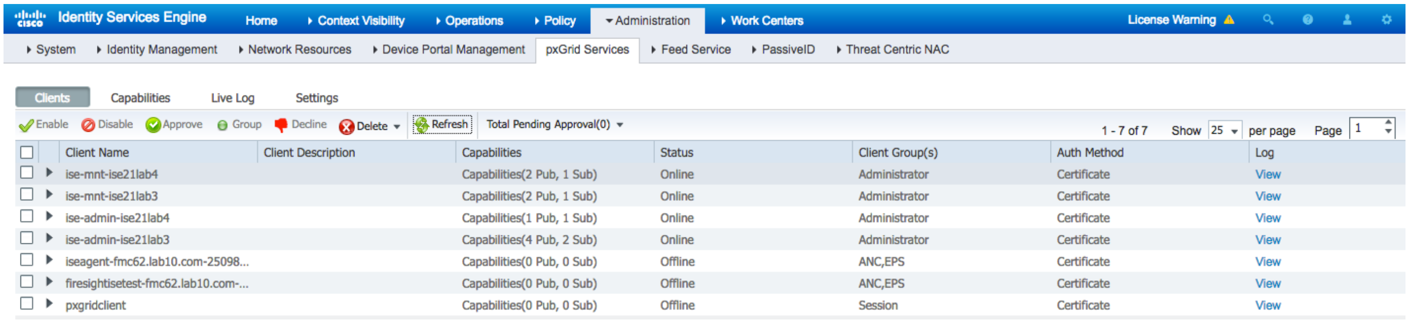
```
./session_download.sh -a 192.168.1.174,192.168.1.176 -u pxGridClient -k test008.jks -p Cisco123 -t
test008_root.jks -q Cisco123
------- properties -------
  version=1.0.4.19
  hostnames=192.168.1.174,192.168.1.176
  username=pxGridClient
  password=
  group=Session
  description=null
  keystoreFilename=test008.jks
  keystorePassword=Richard08
  truststoreFilename=test008_root.jks
  truststorePassword=Richard08
--------------------------
Connecting...
13:21:36.347 [main] INFO  com.cisco.pxgrid.Configuration - Connecting to host 192.168.1.174
13:21:37.443 [main] INFO  com.cisco.pxgrid.Configuration - Connected OK to host 192.168.1.174
13:21:37.444 [main] INFO  com.cisco.pxgrid.Configuration - Client Login to host 192.168.1.174
13:21:37.814 [main] INFO  com.cisco.pxgrid.Configuration - Client Login OK to host 192.168.1.174
Connected
Filters (ex. '1.0.0.0/255.0.0.0,1234::/16...' or <enter> for no filter):
Start time (ex. '2015-01-31 13:00:00' or <enter> for no start time):
End time (ex. '2015-01-31 13:00:00' or <enter> for no end time):
pxGrid controller version=1.0.3.32
Going to url:https://ise21lab3.lab10.com:8910/pxgrid/mnt/sd/getSessionListByTime
Session={ip=[192.168.1.232], Audit Session Id=0A0000010000002E0105D9DB, UserName=00:50:56:86:61:7F,
MacAddresses=[00:50:56:86:61:7F], State=STARTED, EndpointProfile=VMWare-Device, NAS IP=192.168.1.3, NAS
Port=GigabitEthernet1/0/10, RADIUSAVPairs=[ Acct-Session-Id=00000032], Posture Status=null, Posture
Timestamp=, LastUpdateTime=Fri Oct 20 13:22:20 EDT 2017, Session attributeName=Authorization_Profiles,
Session attributeValue=PermitAccess, Providers=[]}
Session={ip=[192.168.1.222], Audit Session Id=0A0000010000001300025A0B, UserName=00:50:56:86:DE:2E,
MacAddresses=[00:50:56:86:DE:2E], State=STARTED, EndpointProfile=VMWare-Device, NAS IP=192.168.1.3, NAS
Port=GigabitEthernet1/0/10, RADIUSAVPairs=[ Acct-Session-Id=00000016], Posture Status=null, Posture
Timestamp=, LastUpdateTime=Fri Oct 20 13:22:18 EDT 2017, Session attributeName=Authorization_Profiles,
Session attributeValue=PermitAccess, Providers=[]}
```

Step 13 Disable pxGrid primary, pxGrid secondary will come up.

```
./session_download.sh -a 192.168.1.174,192.168.1.176 -u pxGridClient -k test008.jks -p Richard08 -t
test008_root.jks -q Richard08

------- properties -------
  version=1.0.4.19
  hostnames=192.168.1.174,192.168.1.176
  username=pxGridClient
  password=
  group=Session
  description=null
  keystoreFilename=test008.jks
  keystorePassword=Richard08
  truststoreFilename=test008_root.jks
  truststorePassword=Richard08
--------------------------
Connecting...
13:39:14.427 [main] INFO  com.cisco.pxgrid.Configuration - Connecting to host 192.168.1.174
```

```
13:39:40.691 [main] ERROR com.cisco.pxgrid.Configuration - Failed to connect to host The following addresses
failed: '192.168.1.174:5222' failed because java.net.ConnectException: Operation timed out192.168.1.174
13:39:40.691 [main] INFO  com.cisco.pxgrid.Configuration - Connecting to host 192.168.1.176
13:39:41.985 [main] INFO  com.cisco.pxgrid.Configuration - Connected OK to host 192.168.1.176
13:39:41.985 [main] INFO  com.cisco.pxgrid.Configuration - Client Login to host 192.168.1.176
13:39:42.264 [main] INFO  com.cisco.pxgrid.Configuration - Client Login OK to host 192.168.1.176
Connected
Filters (ex. '1.0.0.0/255.0.0.0,1234::/16...' or <enter> for no filter):
Start time (ex. '2015-01-31 13:00:00' or <enter> for no start time):
End time (ex. '2015-01-31 13:00:00' or <enter> for no end time):
pxGrid controller version=1.0.3.32
Going to url:https://ise21lab4.lab10.com:8910/pxgrid/mnt/sd/getSessionListByTime
Session={ip=[192.168.1.232], Audit Session Id=0A0000010000002E0105D9DB, UserName=00:50:56:86:61:7F,
MacAddresses=[00:50:56:86:61:7F], State=STARTED, EndpointProfile=VMWare-Device, NAS IP=192.168.1.3, NAS
Port=GigabitEthernet1/0/10, RADIUSAVPairs=[ Acct-Session-Id=00000032], Posture Status=null, Posture
Timestamp=, LastUpdateTime=Fri Oct 20 13:22:20 EDT 2017, Session attributeName=Authorization_Profiles,
Session attributeValue=PermitAccess, Providers=[]}
Session={ip=[192.168.1.222], Audit Session Id=0A00000100000013000025A0B, UserName=00:50:56:86:DE:2E,
MacAddresses=[00:50:56:86:DE:2E], State=STARTED, EndpointProfile=VMWare-Device, NAS IP=192.168.1.3, NAS
Port=GigabitEthernet1/0/10, RADIUSAVPairs=[ Acct-Session-Id=00000016], Posture Status=null, Posture
Timestamp=, LastUpdateTime=Fri Oct 20 13:22:18 EDT 2017, Session attributeName=Authorization_Profiles,
Session attributeValue=PermitAccess, Providers=[]}
```

Step 14 Select **Administration->pxGrid Services** to verify the pxGrid client appears



□		Client Name	Client Description	Capabilities	Status	Client Group(s)	Auth Method	Log
□	▸	ise-mnt-ise21lab4		Capabilities(2 Pub, 1 Sub)	Online	Administrator	Certificate	View
□	▸	ise-mnt-ise21lab3		Capabilities(2 Pub, 1 Sub)	Online	Administrator	Certificate	View
□	▸	ise-admin-ise21lab4		Capabilities(1 Pub, 1 Sub)	Online	Administrator	Certificate	View
□	▸	ise-admin-ise21lab3		Capabilities(4 Pub, 2 Sub)	Online	Administrator	Certificate	View
□	▸	iseagent-fmc62.lab10.com-25098...		Capabilities(0 Pub, 0 Sub)	Offline	ANC,EPS	Certificate	View
□	▸	firesightisetest-fmc62.lab10.com-...		Capabilities(0 Pub, 0 Sub)	Offline	ANC,EPS	Certificate	View
□	▸	pxgridclient		Capabilities(0 Pub, 0 Sub)	Offline	Session	Certificate	View

Deploying pxGrid ISE 2.0/2.1 with External CA Certificates

This section describes the details for deploying pxGrid with ISE 2.0 using an external CA Server. The ISE pxGrid nodes will need to be signed by the extern al CA Server using a customized template with an EKU of both client and server certificates.

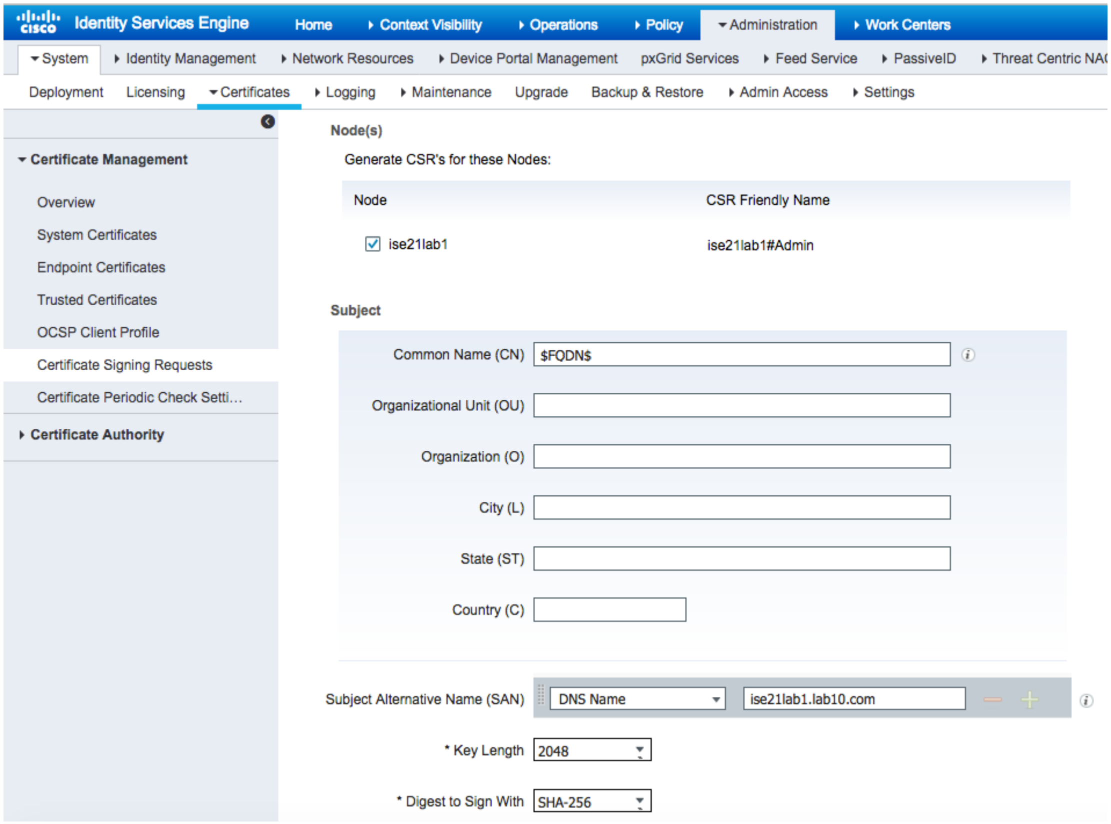
Generating CSR requests for ISE nodes

You can generate CSR request for the ISE nodes using the “admin” purpose and getting them signed by the external CA using the “web server” template. You would also need to create an additional certificate for the Primary Admin, Secondary Admin, Primary MNT and secondary MNT nodes to support pxGrid operation. This also goes for the primary and secondary pxGrid nodes.

As an alternative you can create one certificate using the “admin” purpose and getting them signed by the external CA using the customized pxGrid template. By selecting “admin” purpose this will include pxGrid.

Generating CSR requests using admin node and pxGrid certificate

Step 1 Select **Administration->System->Certificates->Certificate Signing Requests->Generate Certificate Signing Request->Usage “admin”-> select Node**



Node(s)

Generate CSR's for these Nodes:

Node	CSR Friendly Name
☑ ise21lab1	ise21lab1#Admin

Subject

Common Name (CN) $FQDN$

Organizational Unit (OU)

Organization (O)

City (L)

State (ST)

Country (C)

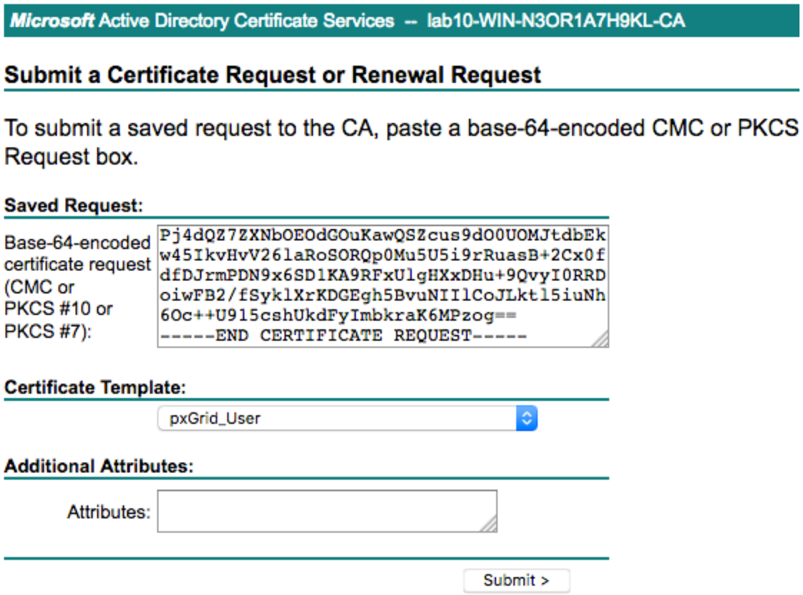
Subject Alternative Name (SAN) DNS Name ise21lab1.lab10.com

* Key Length 2048

* Digest to Sign With SHA-256

Step 1 Select **Generate**

Step 2 Export the PEM File into Advanced User's Request window and specify the customized pxGrid template



Microsoft Active Directory Certificate Services -- lab10-WIN-N3OR1A7H9KL-CA

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS Request box.

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

```
Pj4dQZ7ZXNbOEOdGOuKawQSZcus9dO0UOMJtdbEk
w45IkvHvV26laRoSORQp0Mu5U5i9rRuasB+2Cx0f
dfDJrmPDN9x6SD1KA9RFxUlgHXxDHu+9QvyI0RRD
oiwFB2/fSyklXrKDGEgh5BvuNIIlCoJLktl5iuNh
6Oc++U915cshUkdFyImbkraK6MPzog==
-----END CERTIFICATE REQUEST-----
```

Certificate Template:

pxGrid_User

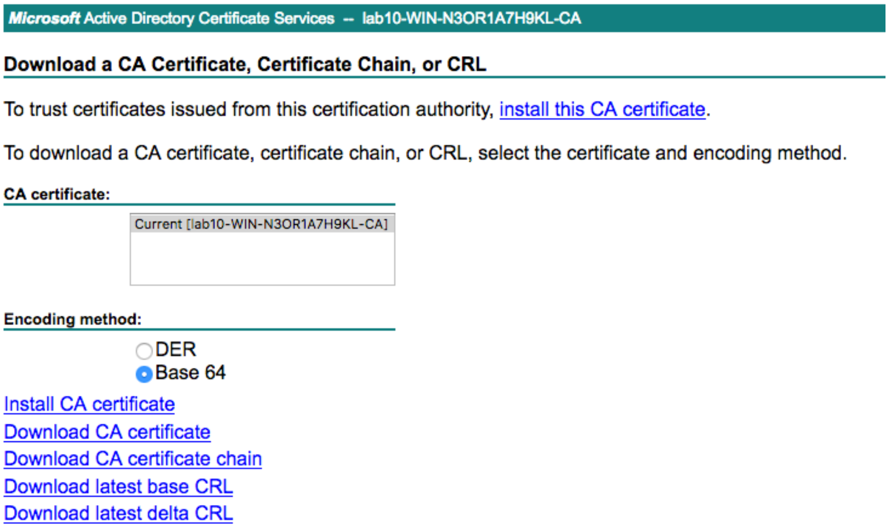
Additional Attributes:

Attributes:

Step 3 Select **Submit**

Step 4 Download in Base 64 encoded format

Step 5 Download the CA root certificate



Microsoft Active Directory Certificate Services -- lab10-WIN-N3OR1A7H9KL-CA

Download a CA Certificate, Certificate Chain, or CRL

To trust certificates issued from this certification authority, install this CA certificate.

To download a CA certificate, certificate chain, or CRL, select the certificate and encoding method.

CA certificate:

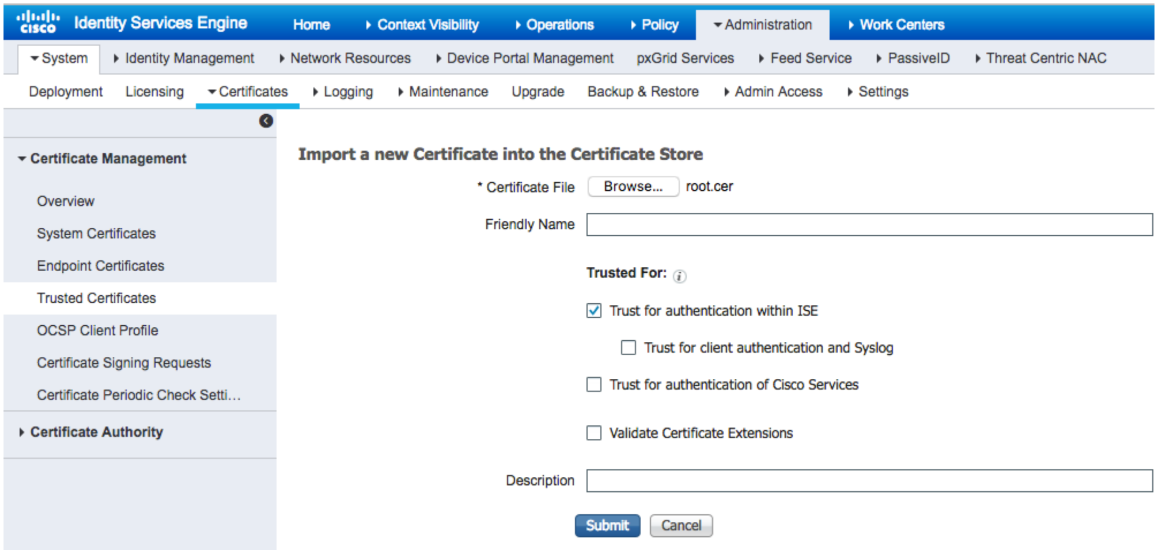
Current [lab10-WIN-N3OR1A7H9KL-CA]

Encoding method:

○ DER
● Base 64

Step 6 Select **Download CA Certificate**

Step 7 Import CA root certificate into ISE trusted certificate store
Select **Administration->System->Certificates->Certificate Management->Trusted Certificates->Import->CAroot certificate->**



Import a new Certificate into the Certificate Store

* Certificate File Browse... root.cer

Friendly Name

Trusted For:

☑ Trust for authentication within ISE

□ Trust for client authentication and Syslog

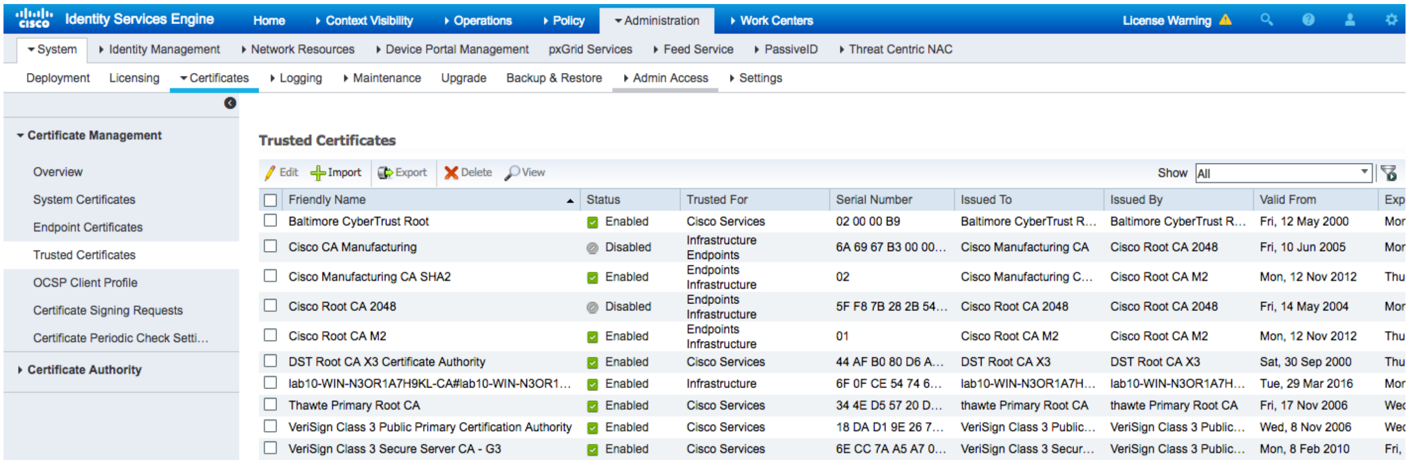
□ Trust for authentication of Cisco Services

□ Validate Certificate Extensions

Description

Step 8 Select **Submit**

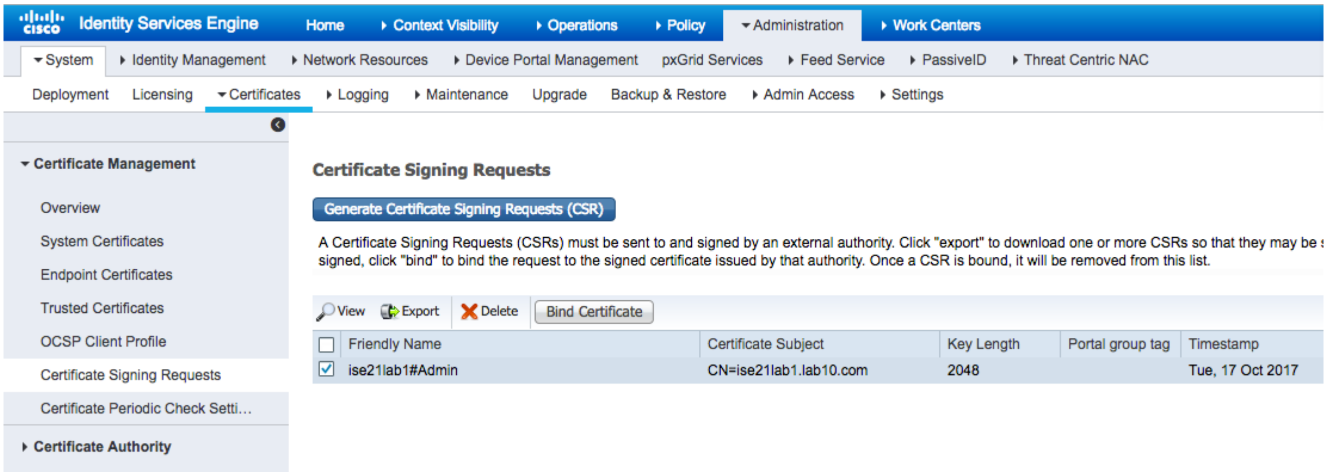
Step 9 You should see:



Trusted Certificates

□	Friendly Name	Status	Trusted For	Serial Number	Issued To	Issued By	Valid From	Exp
□	Baltimore CyberTrust Root	Enabled	Cisco Services	02 00 00 B9	Baltimore CyberTrust R…	Baltimore CyberTrust R…	Fri, 12 May 2000	Mor
□	Cisco CA Manufacturing	Disabled	Infrastructure Endpoints	6A 69 67 B3 00 00…	Cisco Manufacturing CA	Cisco Root CA 2048	Fri, 10 Jun 2005	Mor
□	Cisco Manufacturing CA SHA2	Enabled	Endpoints Infrastructure	02	Cisco Manufacturing C…	Cisco Root CA M2	Mon, 12 Nov 2012	Thu
□	Cisco Root CA 2048	Disabled	Endpoints Infrastructure	5F F8 7B 28 2B 54…	Cisco Root CA 2048	Cisco Root CA 2048	Fri, 14 May 2004	Mor
□	Cisco Root CA M2	Enabled	Endpoints Infrastructure	01	Cisco Root CA M2	Cisco Root CA M2	Mon, 12 Nov 2012	Thu
□	DST Root CA X3 Certificate Authority	Enabled	Cisco Services	44 AF B0 80 D6 A…	DST Root CA X3	DST Root CA X3	Sat, 30 Sep 2000	Thu
□	lab10-WIN-N3OR1A7H9KL-CA#lab10-WIN-N3OR1…	Enabled	Infrastructure	6F 0F CE 54 74 6…	lab10-WIN-N3OR1A7H…	lab10-WIN-N3OR1A7H…	Tue, 29 Mar 2016	Mor
□	Thawte Primary Root CA	Enabled	Cisco Services	34 4E D5 57 20 D…	thawte Primary Root CA	thawte Primary Root CA	Fri, 17 Nov 2006	Wec
□	VeriSign Class 3 Public Primary Certification Authority	Enabled	Cisco Services	18 DA D1 9E 26 7…	VeriSign Class 3 Public…	VeriSign Class 3 Public…	Wed, 8 Nov 2006	Wec
□	VeriSign Class 3 Secure Server CA - G3	Enabled	Cisco Services	6E CC 7A A5 A7 0…	VeriSign Class 3 Secur…	VeriSign Class 3 Public…	Mon, 8 Feb 2010	Fri,

Step 10 Bind the Identity Certificate to the CSR request
Select->**Administration->System->Certificates->Certificate Management->Certificate Signing Request (CSR)->Select the node**

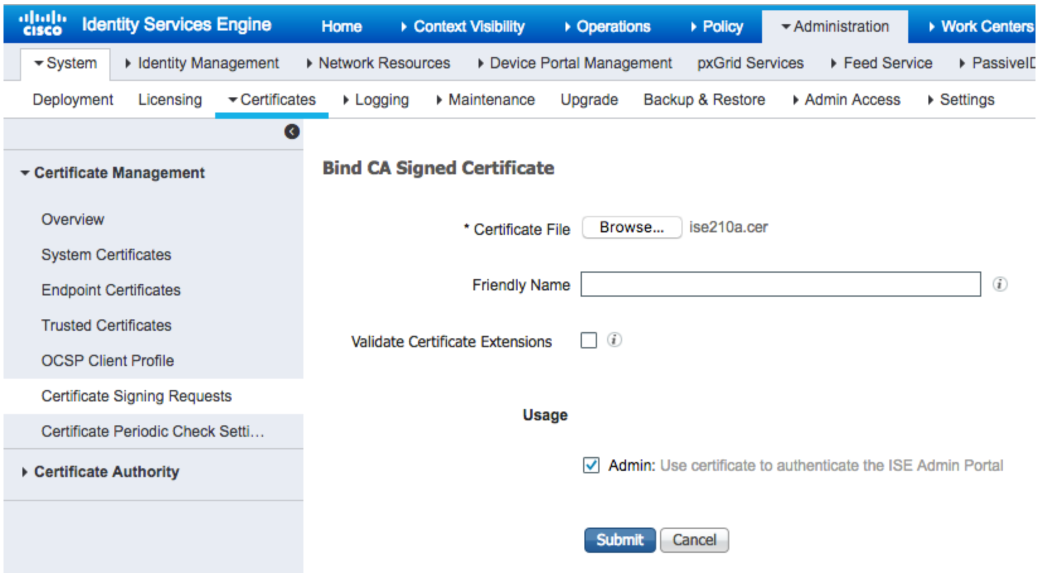


Certificate Signing Requests

A Certificate Signing Requests (CSRs) must be sent to and signed by an external authority. Click "export" to download one or more CSRs so that they may be
signed, click "bind" to bind the request to the signed certificate issued by that authority. Once a CSR is bound, it will be removed from this list.

☐	Friendly Name	Certificate Subject	Key Length	Portal group tag	Timestamp
☑	ise21lab1#Admin	CN=ise21lab1.lab10.com	2048		Tue, 17 Oct 2017

Step 11 Upload the identity certificate



Bind CA Signed Certificate

* Certificate File [Browse...] ise210a.cer

Friendly Name

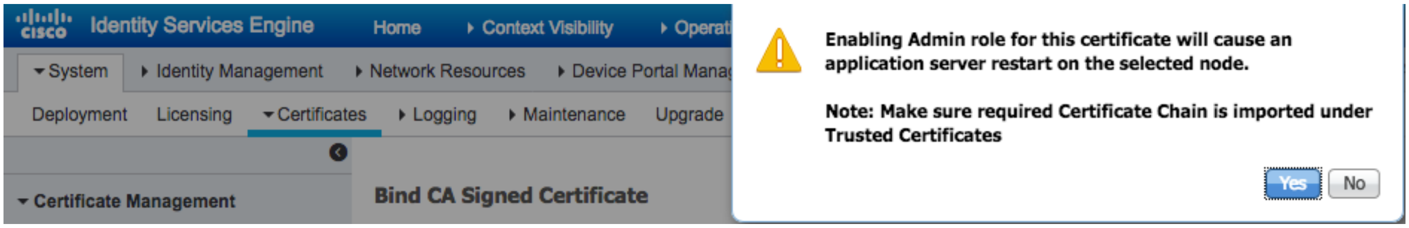
Validate Certificate Extensions ☐

Usage

☑ Admin: Use certificate to authenticate the ISE Admin Portal

Step 12 Select **Submit**

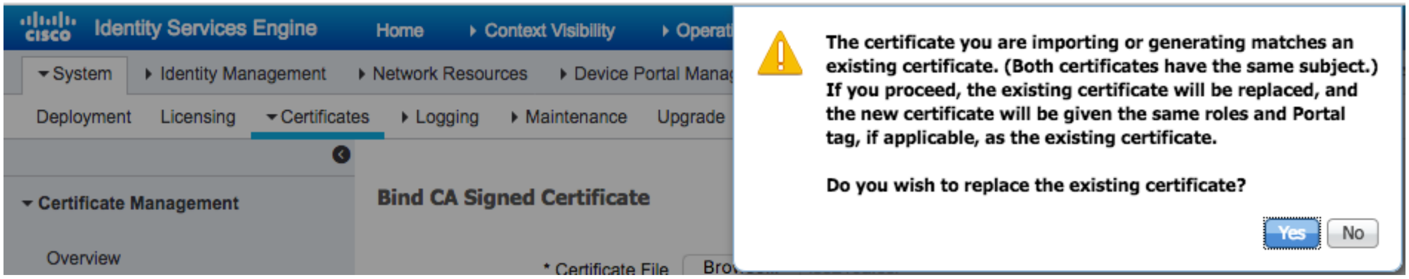
Step 13 When you see the following message, select **Yes**



Enabling Admin role for this certificate will cause an application server restart on the selected node.

Note: Make sure required Certificate Chain is imported under Trusted Certificates

Step 14 You should see following



The certificate you are importing or generating matches an existing certificate. (Both certificates have the same subject.) If you proceed, the existing certificate will be replaced, and the new certificate will be given the same roles and Portal tag, if applicable, as the existing certificate.

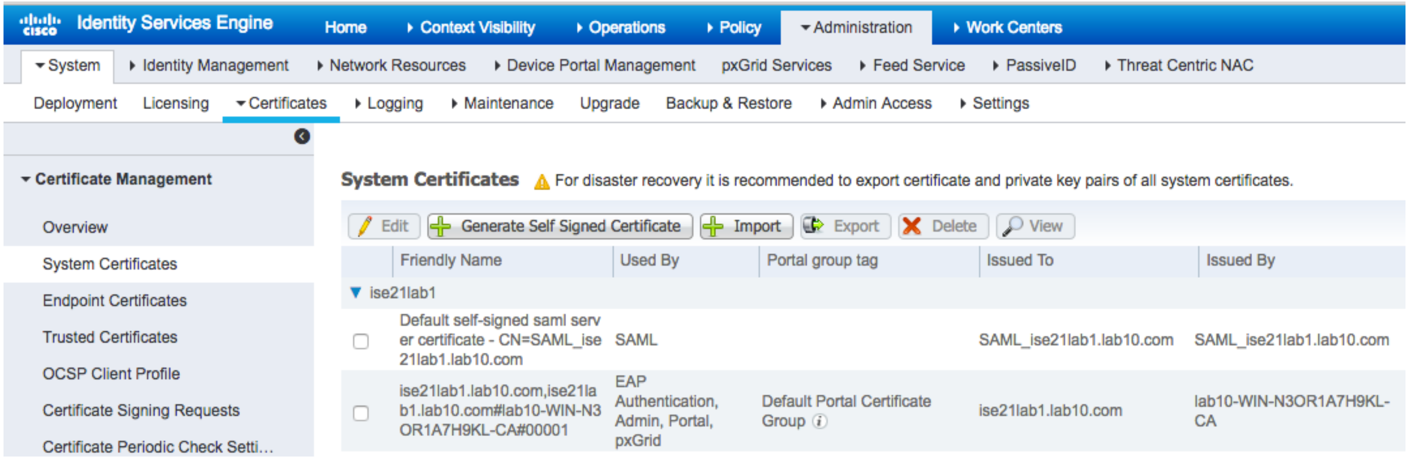
Do you wish to replace the existing certificate?

Step 15 The system will restart

Step 16 When the system comes up, login

Step 17 Select **administration->System->Certificates->Certificate management->System Certificates**

Step 18 You should see:

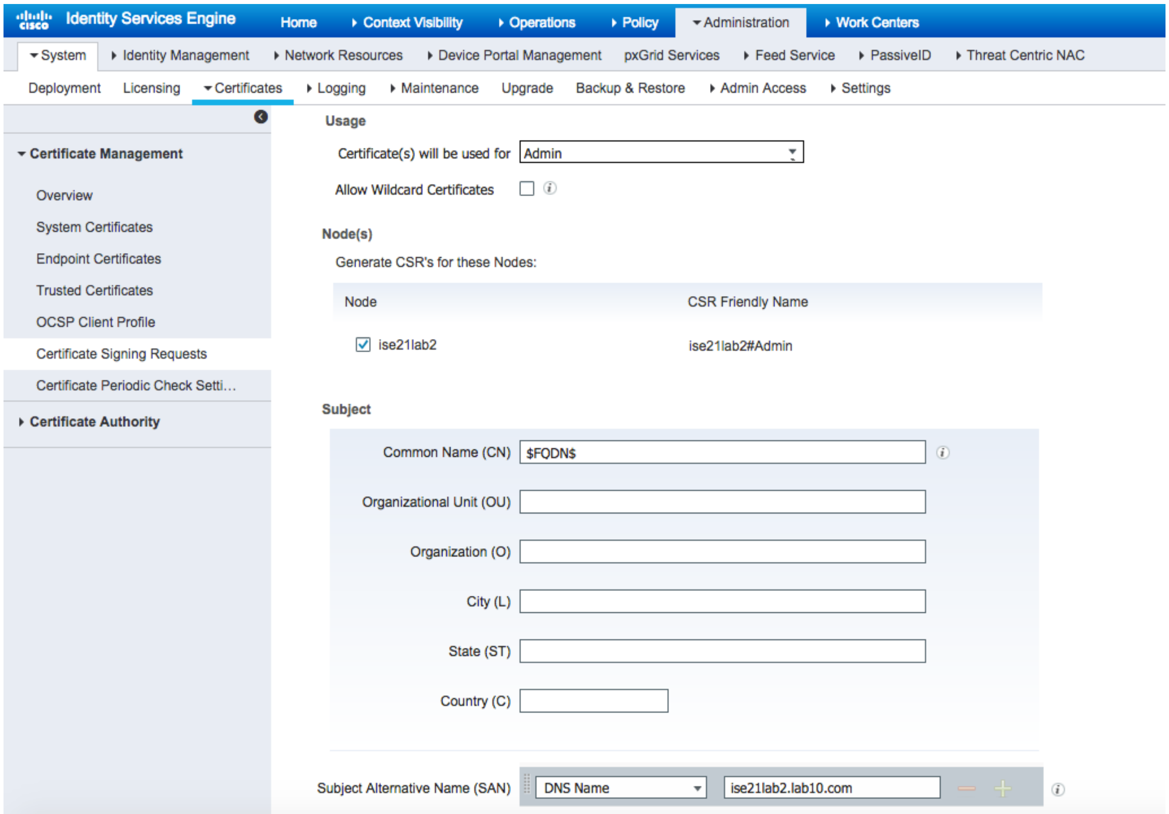


System Certificates ⚠ For disaster recovery it is recommended to export certificate and private key pairs of all system certificates.

	Friendly Name	Used By	Portal group tag	Issued To	Issued By
▼ ise21lab1					
□	Default self-signed saml server certificate - CN=SAML_ise21lab1.lab10.com	SAML		SAML_ise21lab1.lab10.com	SAML_ise21lab1.lab10.com
□	ise21lab1.lab10.com,ise21lab1.lab10.com#lab10-WIN-N3OR1A7H9KL-CA#00001	EAP Authentication, Admin, Portal, pxGrid	Default Portal Certificate Group ⓘ	ise21lab1.lab10.com	lab10-WIN-N3OR1A7H9KL-CA

Generating CSR requests for admin node certificate for pxGrid operation

Step 1 Select **Administration->System->Certificates->Certificate Signing Requests->Generate Certificate Signing Request->Usage “admin”-> select Node**



Usage

Certificate(s) will be used for: Admin

Allow Wildcard Certificates ☐

Node(s)

Generate CSR's for these Nodes:

Node	CSR Friendly Name
☑ ise21lab2	ise21lab2#Admin

Subject

Common Name (CN): $FQDN$

Organizational Unit (OU):

Organization (O):

City (L):

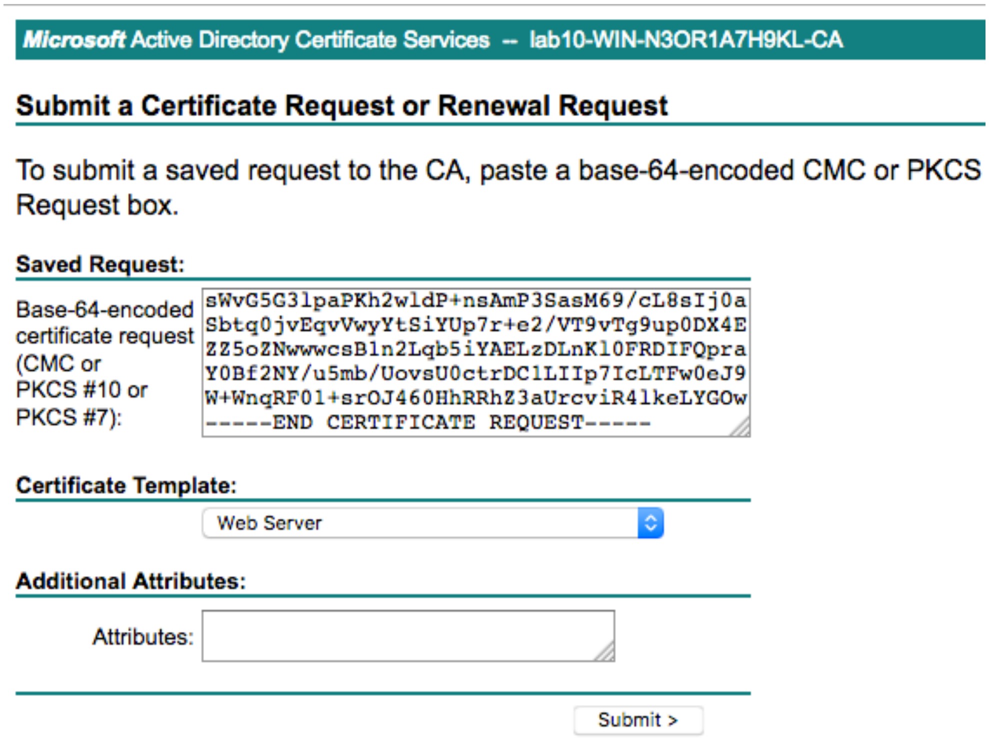
State (ST):

Country (C):

Subject Alternative Name (SAN): DNS Name ise21lab2.lab10.com

Step 2 Select **Generate**

Step 3 Export the PEM File into Advanced User’s Request window and specify the customized pxGrid template



Microsoft Active Directory Certificate Services -- lab10-WIN-N3OR1A7H9KL-CA

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS Request box.

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

```
sWvG5G3lpaPKh2wldP+nsAmP3SasM69/cL8sIj0a
Sbtq0jvEqvVwyYtSiYUp7r+e2/VT9vTg9up0DX4E
ZZ5oZNwwwcsBln2Lqb5iYAELzDLnKl0FRDIFQpra
Y0Bf2NY/u5mb/UovsU0ctrDClLIIp7IcLTFw0eJ9
W+WnqRF0l+srOJ460HhRRhZ3aUrcviR4lkeLYGOw
-----END CERTIFICATE REQUEST-----
```

Certificate Template:

Web Server

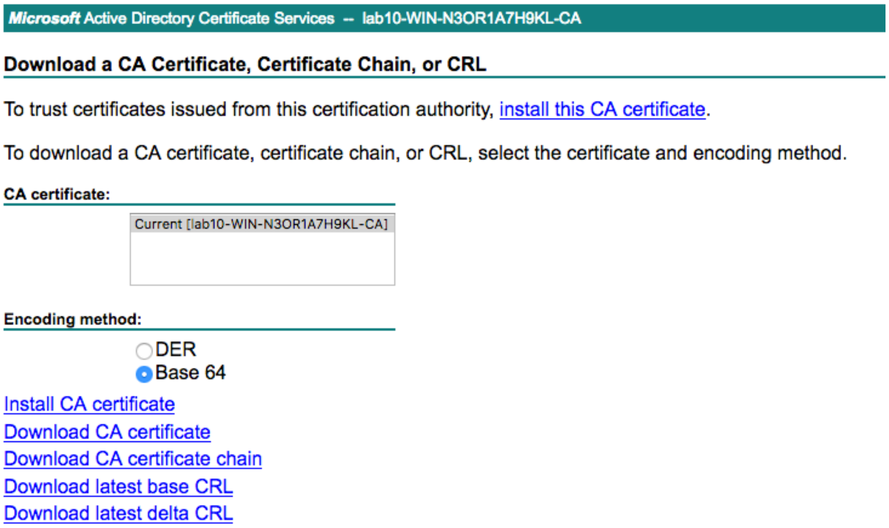
Additional Attributes:

Attributes:

Step 4 Select **Submit**

Step 5 Download in Base 64 encoded format

Step 6 Download the CA root certificate



Microsoft Active Directory Certificate Services -- lab10-WIN-N3OR1A7H9KL-CA

Download a CA Certificate, Certificate Chain, or CRL

To trust certificates issued from this certification authority, install this CA certificate.

To download a CA certificate, certificate chain, or CRL, select the certificate and encoding method.

CA certificate:

Current [lab10-WIN-N3OR1A7H9KL-CA]

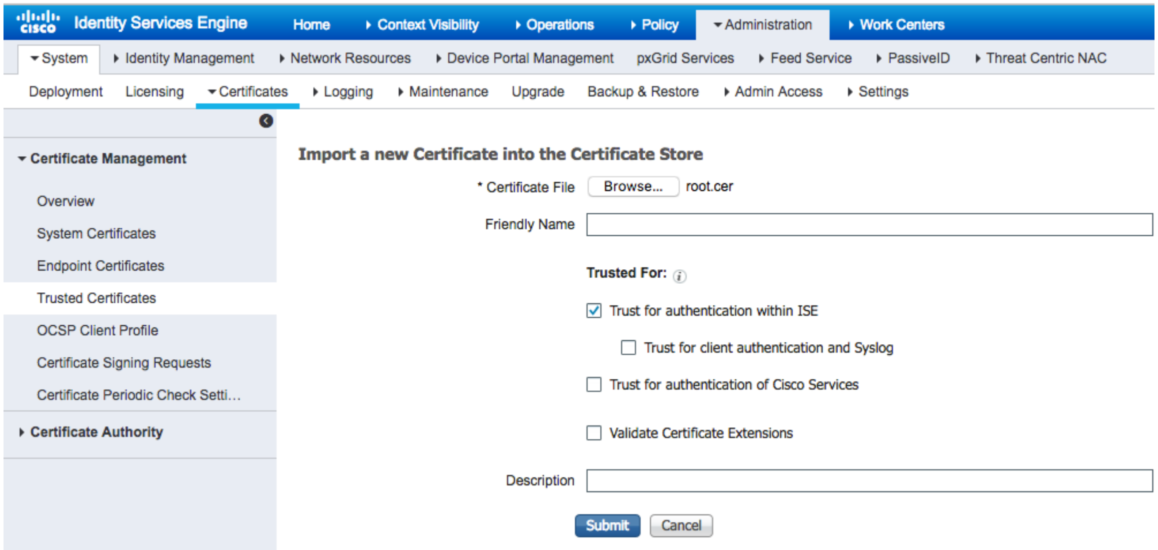
Encoding method:

○ DER
● Base 64

Step 7 Select **Download CA Certificate**

Step 8 Import CA root certificate into ISE trusted certificate store

Select **Administration->System->Certificates->Certificate Management->Trusted Certificates->Import->CAroot certificate->**



Import a new Certificate into the Certificate Store

* Certificate File [Browse...] root.cer

Friendly Name

Trusted For:

☑ Trust for authentication within ISE

☐ Trust for client authentication and Syslog

☐ Trust for authentication of Cisco Services

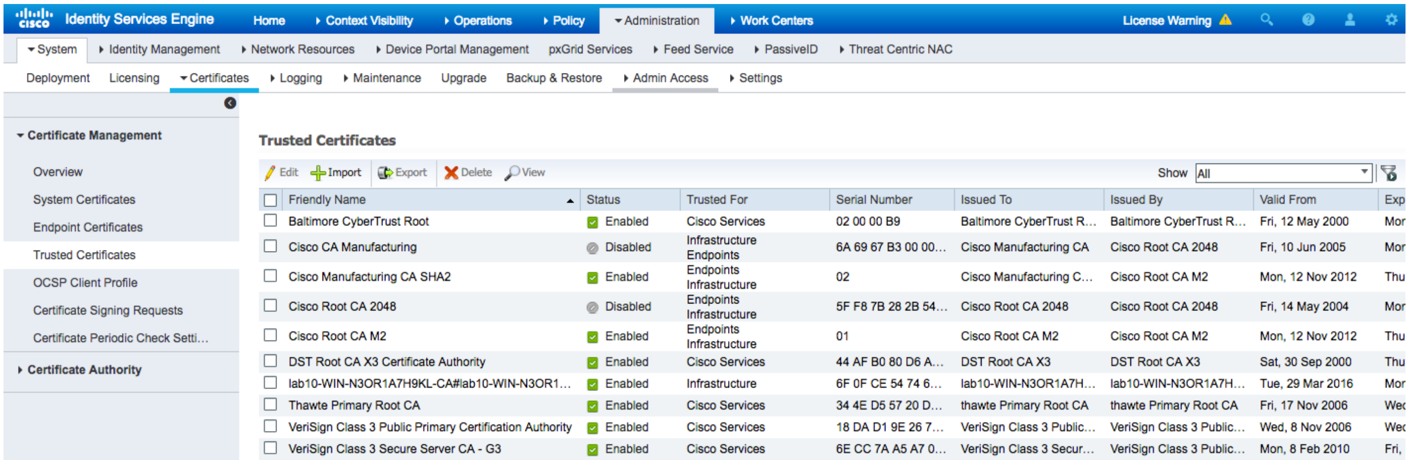
☐ Validate Certificate Extensions

Description

[Submit] [Cancel]

Step 9 Select **Submit**

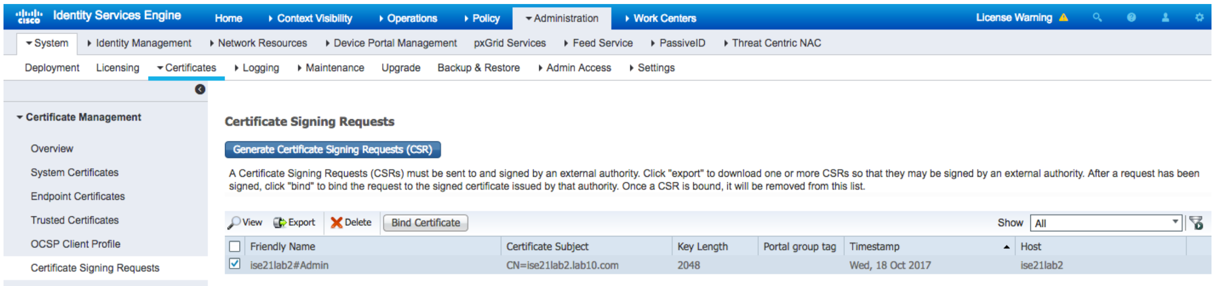
Step 10 You should see:



Trusted Certificates

☐	Friendly Name	Status	Trusted For	Serial Number	Issued To	Issued By	Valid From	Exp
☐	Baltimore CyberTrust Root	Enabled	Cisco Services	02 00 00 B9	Baltimore CyberTrust R…	Baltimore CyberTrust R…	Fri, 12 May 2000	Mor
☐	Cisco CA Manufacturing	Disabled	Infrastructure Endpoints	6A 69 67 B3 00 00…	Cisco Manufacturing CA	Cisco Root CA 2048	Fri, 10 Jun 2005	Mor
☐	Cisco Manufacturing CA SHA2	Enabled	Endpoints Infrastructure	02	Cisco Manufacturing C…	Cisco Root CA M2	Mon, 12 Nov 2012	Thu
☐	Cisco Root CA 2048	Disabled	Endpoints Infrastructure	5F F8 7B 28 2B 54…	Cisco Root CA 2048	Cisco Root CA 2048	Fri, 14 May 2004	Mor
☐	Cisco Root CA M2	Enabled	Endpoints Infrastructure	01	Cisco Root CA M2	Cisco Root CA M2	Mon, 12 Nov 2012	Thu
☐	DST Root CA X3 Certificate Authority	Enabled	Cisco Services	44 AF B0 80 D6 A…	DST Root CA X3	DST Root CA X3	Sat, 30 Sep 2000	Thu
☐	lab10-WIN-N3OR1A7H9KL-CA#lab10-WIN-N3OR1…	Enabled	Infrastructure	6F 0F CE 54 74 6…	lab10-WIN-N3OR1A7H…	lab10-WIN-N3OR1A7H…	Tue, 29 Mar 2016	Mor
☐	Thawte Primary Root CA	Enabled	Cisco Services	34 4E D5 57 20 D…	thawte Primary Root CA	thawte Primary Root CA	Fri, 17 Nov 2006	Wec
☐	VeriSign Class 3 Public Primary Certification Authority	Enabled	Cisco Services	18 DA D1 9E 26 7…	VeriSign Class 3 Public…	VeriSign Class 3 Public…	Wed, 8 Nov 2006	Wec
☐	VeriSign Class 3 Secure Server CA - G3	Enabled	Cisco Services	6E CC 7A A5 A7 0…	VeriSign Class 3 Secur…	VeriSign Class 3 Public…	Mon, 8 Feb 2010	Fri,

Step 11 Bind the Identity Certificate to the CSR request
Select->**Administration->System->Certificates->Certificate Management->Certificate Signing Request (CSR)->Select the node**

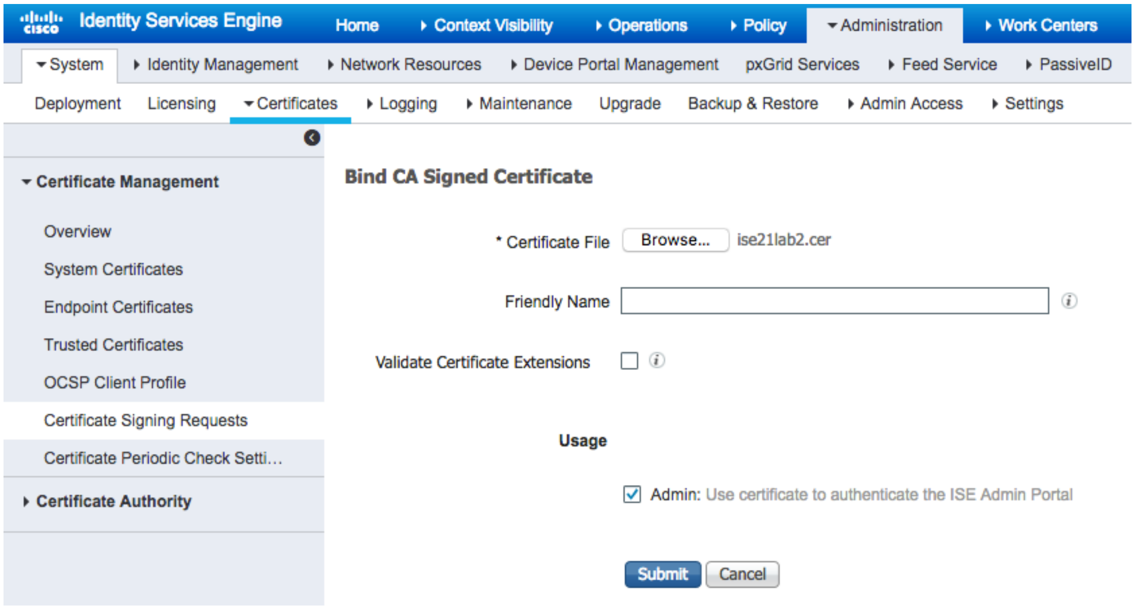


Certificate Signing Requests

A Certificate Signing Requests (CSRs) must be sent to and signed by an external authority. Click "export" to download one or more CSRs so that they may be signed by an external authority. After a request has been signed, click "bind" to bind the request to the signed certificate issued by that authority. Once a CSR is bound, it will be removed from this list.

☐	Friendly Name	Certificate Subject	Key Length	Portal group tag	Timestamp	Host
☑	ise21lab2#Admin	CN=ise21lab2.lab10.com	2048		Wed, 18 Oct 2017	ise21lab2

Step 12 Upload the identity certificate



Bind CA Signed Certificate

* Certificate File Browse... ise21lab2.cer

Friendly Name

Validate Certificate Extensions □

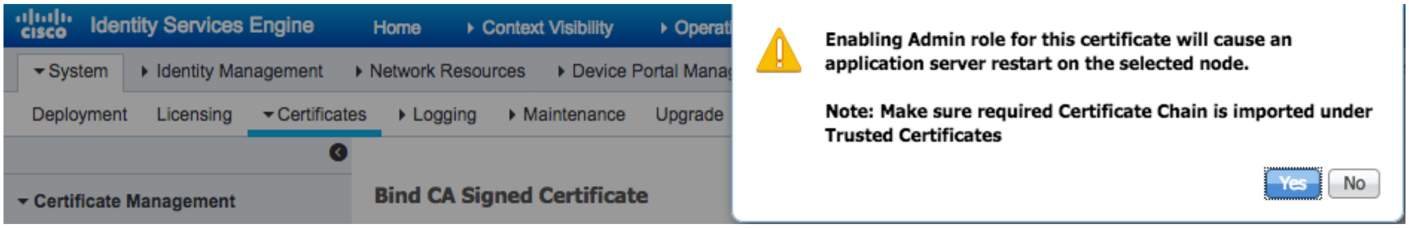
Usage

☑ Admin: Use certificate to authenticate the ISE Admin Portal

Submit Cancel

Step 13 Select **Submit**

Step 14 When you see the following message, select **Yes**

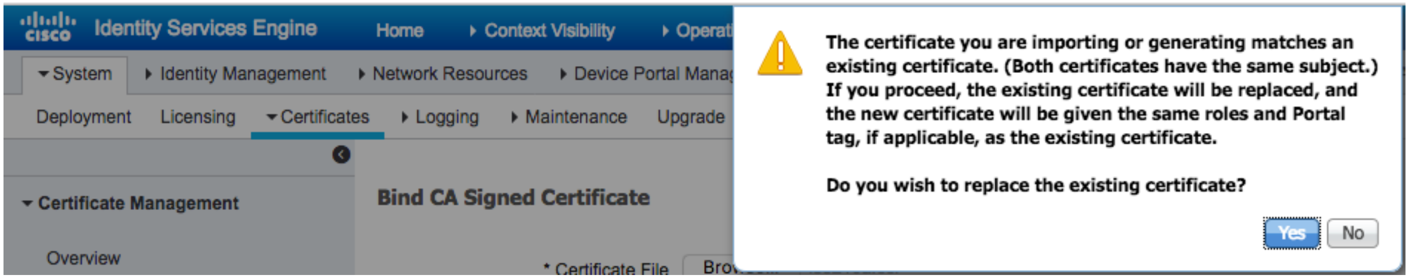


Enabling Admin role for this certificate will cause an application server restart on the selected node.

Note: Make sure required Certificate Chain is imported under Trusted Certificates

Yes No

Step 15 You should see following



The certificate you are importing or generating matches an existing certificate. (Both certificates have the same subject.) If you proceed, the existing certificate will be replaced, and the new certificate will be given the same roles and Portal tag, if applicable, as the existing certificate.

Do you wish to replace the existing certificate?

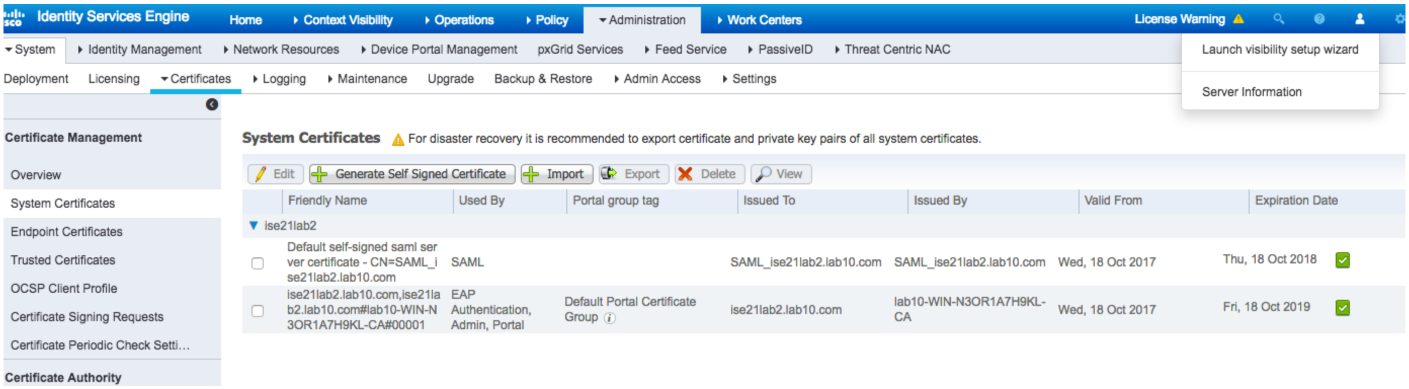
Yes No

Step 16 The system will restart

Step 17 When the system comes up, login

Step 18 Select **administration->System->Certificates->Certificate management->System Certificates**

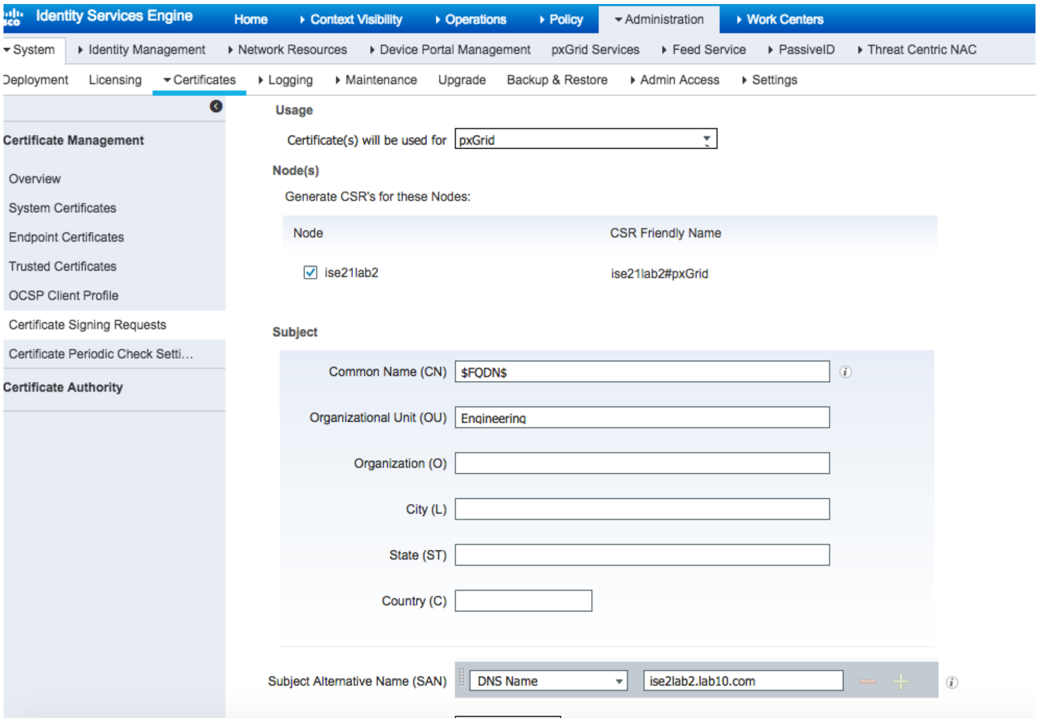
Step 19 You should see



System Certificates ⚠ For disaster recovery it is recommended to export certificate and private key pairs of all system certificates.

	Friendly Name	Used By	Portal group tag	Issued To	Issued By	Valid From	Expiration Date	
▼ ise21lab2								
□	Default self-signed saml server certificate - CN=SAML_ise21lab2.lab10.com	SAML		SAML_ise21lab2.lab10.com	SAML_ise21lab2.lab10.com	Wed, 18 Oct 2017	Thu, 18 Oct 2018	✓
□	ise21lab2.lab10.com,ise21lab2.lab10.com#lab10-WIN-N3OR1A7H9KL-CA#00001	EAP Authentication, Admin, Portal	Default Portal Certificate Group ⓘ	ise21lab2.lab10.com	lab10-WIN-N3OR1A7H9KL-CA	Wed, 18 Oct 2017	Fri, 18 Oct 2019	✓

Step 20 Select **Administration->System->Certificates->Certificate Management->CSR, select pxGrid, and OU field**



Usage

Certificate(s) will be used for: pxGrid

Node(s)

Generate CSR's for these Nodes:

Node	CSR Friendly Name
☑ ise21lab2	ise21lab2#pxGrid

Subject

Common Name (CN): $FQDN$

Organizational Unit (OU): Engineering

Organization (O):

City (L):

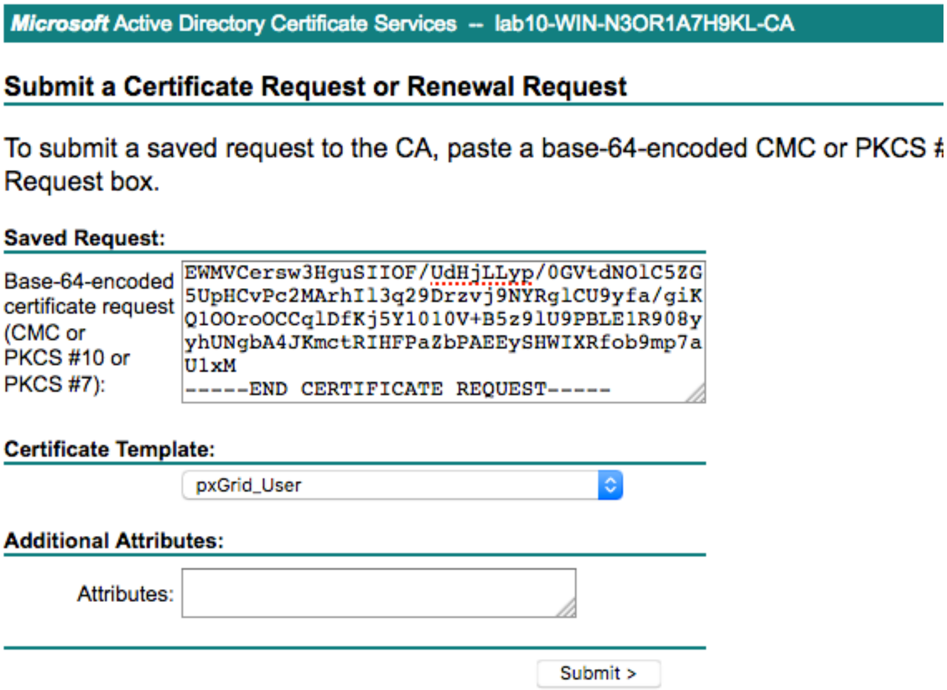
State (ST):

Country (C):

Subject Alternative Name (SAN): DNS Name: ise2lab2.lab10.com

Step 21 Select **Generate**

Step 22 Export the PEM File into Advanced User’s Request window and specify the customized pxGrid template



Microsoft Active Directory Certificate Services -- lab10-WIN-N3OR1A7H9KL-CA

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS # Request box.

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

```
EWMVCersw3HguSIIOF/UdHjLLyp/0GVtdNO1C5ZG
5UpHCvPc2MArhI13q29Drzvj9NYRg1CU9yfa/giK
Q1OOroOCCqlDfKj5Y1010V+B5z91U9PBLE1R908y
yhUNgbA4JKmctRIHFPaZbPAEEySHWIXRfob9mp7a
U1xM
-----END CERTIFICATE REQUEST-----
```

Certificate Template:

pxGrid_User

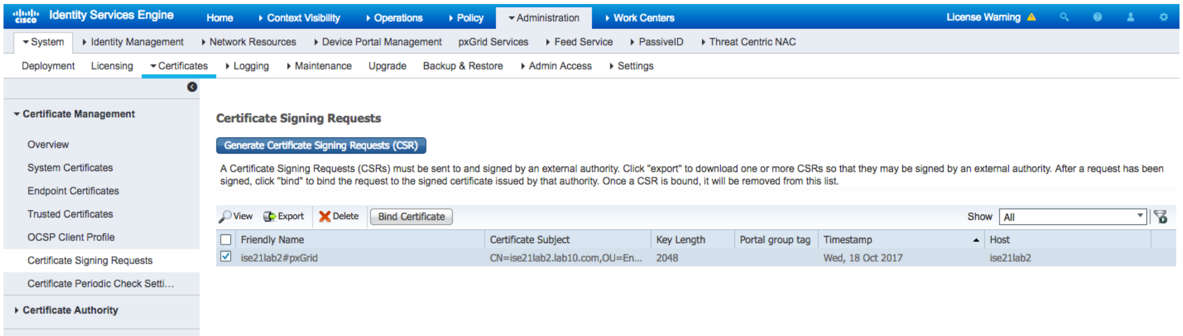
Additional Attributes:

Attributes:

Step 23 Select **Submit**

Step 24 Download in Base 64 encoded format

Step 25 Bind the Identity Certificate to the CSR request
Select->**Administration->System->Certificates->Certificate Management->Certificate Signing Request (CSR)->Select the node**

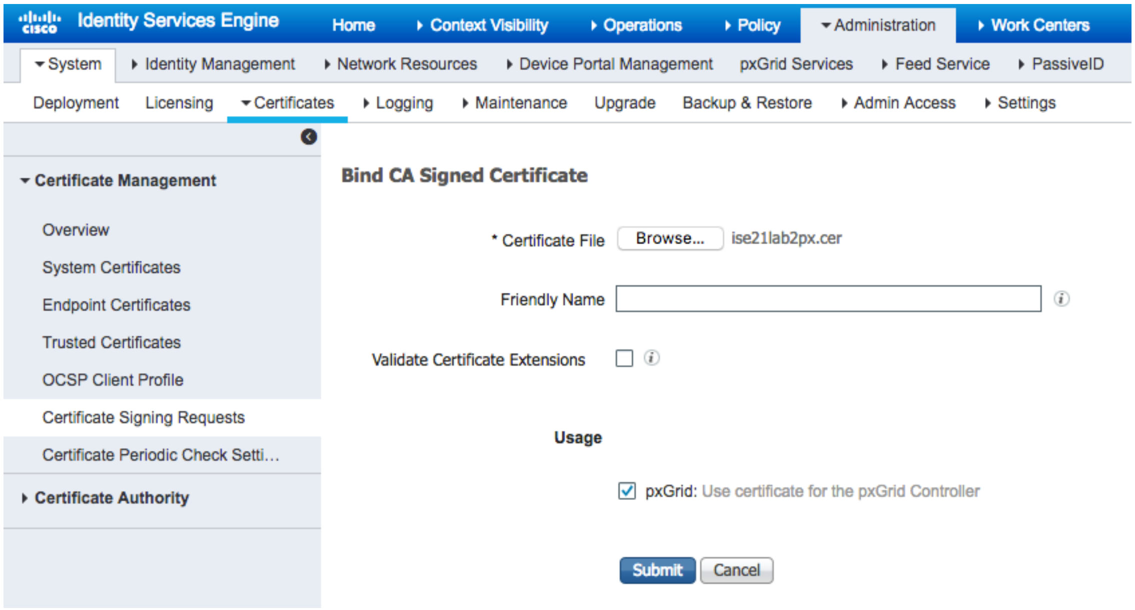


Certificate Signing Requests

A Certificate Signing Requests (CSRs) must be sent to and signed by an external authority. Click "export" to download one or more CSRs so that they may be signed by an external authority. After a request has been signed, click "bind" to bind the request to the signed certificate issued by that authority. Once a CSR is bound, it will be removed from this list.

	Friendly Name	Certificate Subject	Key Length	Portal group tag	Timestamp	Host
☑	ise21lab2#pxGrid	CN=ise21lab2.lab10.com,OU=En...	2048		Wed, 18 Oct 2017	ise21lab2

Step 26 Upload the identity certificate



Bind CA Signed Certificate

* Certificate File [Browse...] ise21lab2px.cer

Friendly Name

Validate Certificate Extensions □

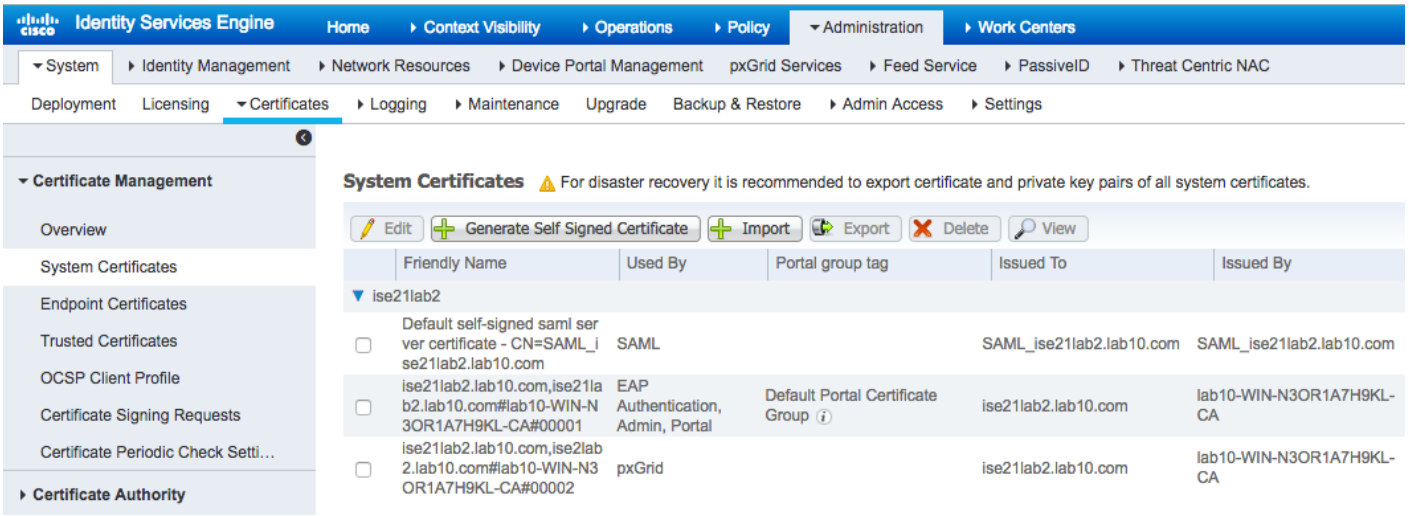
Usage

☑ pxGrid: Use certificate for the pxGrid Controller

[Submit] [Cancel]

Step 27 Select **Submit**

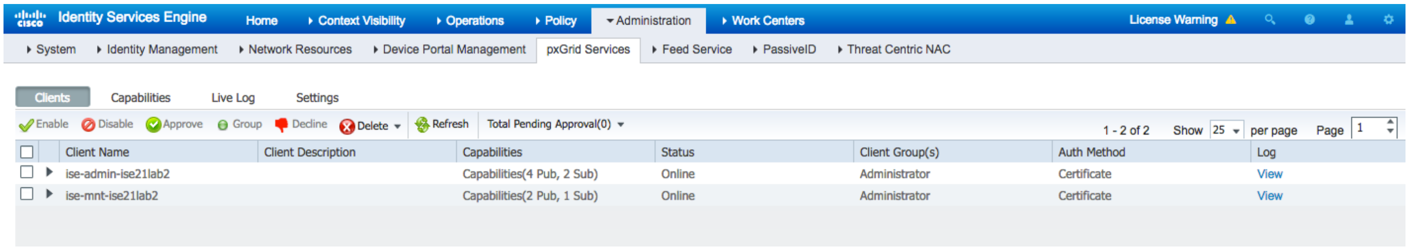
Step 28 You should see the ISE identity certificate signed by the external CA server and the pxGrid certificate signed by the external CA server



System Certificates ⚠ For disaster recovery it is recommended to export certificate and private key pairs of all system certificates.

	Friendly Name	Used By	Portal group tag	Issued To	Issued By
▼ ise21lab2					
□	Default self-signed saml server certificate - CN=SAML_ise21lab2.lab10.com	SAML		SAML_ise21lab2.lab10.com	SAML_ise21lab2.lab10.com
□	ise21lab2.lab10.com,ise21lab2.lab10.com#lab10-WIN-N3OR1A7H9KL-CA#00001	EAP Authentication, Admin, Portal	Default Portal Certificate Group ⓘ	ise21lab2.lab10.com	lab10-WIN-N3OR1A7H9KL-CA
□	ise21lab2.lab10.com,ise2lab2.lab10.com#lab10-WIN-N3OR1A7H9KL-CA#00002	pxGrid		ise21lab2.lab10.com	lab10-WIN-N3OR1A7H9KL-CA

Step 29 Verify that the published nodes appear and there is connectivity to the pxGrid node
Select **Administration->pxGrid Services**



1 - 2 of 2 Show 25 per page Page 1

□		Client Name	Client Description	Capabilities	Status	Client Group(s)	Auth Method	Log
□	▶	ise-admin-ise21lab2		Capabilities(4 Pub, 2 Sub)	Online	Administrator	Certificate	View
□	▶	ise-mnt-ise21lab2		Capabilities(2 Pub, 1 Sub)	Online	Administrator	Certificate	View

Step 30 Based on either method you choose, complete the same steps for all of the ISE nodes

Note: In your deployment scenario, there needs to be an additional certificate for pxGrid for the ISE Primary Admin, Secondary Admin, Primary MNT and secondary MNT nodes to support pxGrid operations in addition to the pxGrid certificates on the ISE pxGrid nodes.

You can create a customized template for supporting pxGrid Certificate Signing Requests (CSR) using “admin” purpose, this way no additional pxGrid certificate is necessary or you can follow step 1 and create an additional pxGrid certificate

Registering ISE pxGrid Nodes.

Step 1 You would need to create customized templates for the ISE admin, ISE MNT nodes and pxGrid nodes CSR request. This customized template must contain an EKU of both client and server authentication. Please **Customized pxGrid Template** under **References**

Note: You also create a certificate specifically for pxGrid. If you go down this route, you would need to change the OU field in the CSR request and ensure that is not the same name if the admin Certificate Signing Requests (CSR).

Generating pxGrid Client Certificates

Step 1 Generate private key using –des3. The –des3 argument provides the encryption password.

```
openssl genrsa -des3 -out client.key 4096
Generating RSA private key, 4096 bit long modulus
.........
........................
e is 65537 (0x10001)
Enter pass phrase for client.key: Cisco123
Verifying - Enter pass phrase for client.key: Cisco123
```

Step 2 Generate CSR request

```
openssl req -new -key client.key -out client.csr
Enter pass phrase for client.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 Code []:US
State or Province Name []:Maryland
Locality Name []:Germantown
Organization Name []:Cisco
Organizational Unit Name []:Engineering
Common Name []:fmc62.lab10.com
Email Address []:j@c.com
```

Testing using Cisco Firepower Management Center 6.1

Step 1 Copy CSR request into pxGrid template

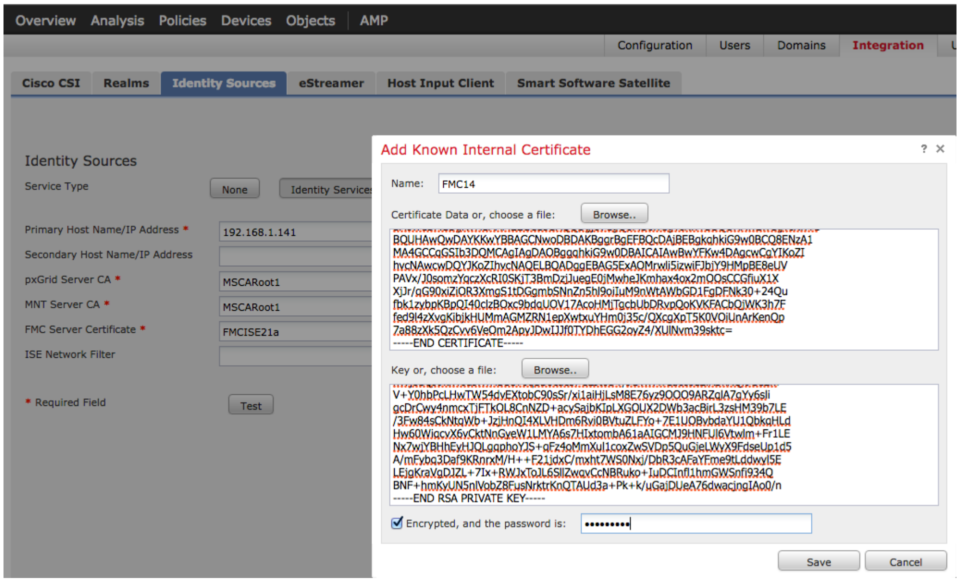
```
cat client.csr
-----BEGIN CERTIFICATE REQUEST-----
MIIE0zCCArsCAQAwgY0xCzAJBgNVBAYTAlVTMREwDwYDVQQIEwhNYXJ5bGFuZDET
MBEGA1UEBxMKR2VybWFudG93bjEOMAwGA1UEChMFQ2lzY28xFDASBgNVBAsTC0Vu
Z2luZWVyaW5nMRgwFgYDVQQDEw9mbWM2Mi5sYWIxMC5jb20xFjAUBgkqhkiG9w0B
CQEWB2pAYy5jb20wggIiMA0GCSqGSIb3DQEBAQUAA4ICDwAwggIKAoICAQC6gXkN
wGLdzv3P5IApJIRePWAKd+2uab6ikZX+HfIsAdg8sMxw/VVqCiJ7eu1zoeApZn2L
7JJ4tq4iHjyI9N0kTMrBlqHsoKPrvQZUMAKWs8LLK5jgElhShNpidClmWW9kZtE+
6179ig21j7V0BFo+pmx0cLNoOA/rTXhAJKbuKsLpyEnALDjgDXYpIHuRKJOSps6C
6geiK7jJ4lzoG4lxvRuudDiauUxLDKh2L/ga44STTAeahXWBkF0u43zkmrPFR0Ck
7vo3yQf0ha/5Kl/41Q0oULe1rkmE5/ApNsQ90r8wpm961biog3GnRg0uEww2ODIp
dPI5bJSgup8y+gsS0CilFCUDXgywRdt/DRTxJjiPX/YQiPvwS+rcxeDg/PqlmtwA
uVhcGdCEMRqYY08yPhIomDuGpVL0vu1iNo3CDjYH/r5W2tAEPOLWx8nArJjsCkfC
Z8ld/BBdfHoh4X9xcfteLr48zxSoh0RgD9wCjkbF7N0m+313weARnOBkKWAIpOFu
G60ceERm8rf6xDQdgBtLWRhfBPKNuS5Ljsb0m5QeD/340KwGCKxMem7hUPCxLNxC
XUhmszqhppBhKymw0iw/f7th0XkBPuw4amXlgsi3tMgaK5DG17D105XDb4ssChZf
4iym5WZ0Inxo1g+27tQGnMgYePqG58YCMaHegQIDAQABoAAwDQYJKoZIhvcNAQEL
BQADggIBAEEJKjsEak/ud/mFJrjz5GaedsnIxF1tXZDjQyqZH1HS7+TUuaHrQGOn
tYpVoiT60Js8o516T0eAbXTnTh3mP9yHpHbRKBWpNNB1H/+FcSI9uSzrzJymyb8a
URLAJKcw0in6weVC/52F7DYeVTrEZfwHJFKaxS0033KEi+4fphPde+cHZsmB0aQG
Aa2jdn7zuaY6ZxE8YfZsvwRMkEwVu/ZGKRuBAsX6RFokH5OUAH1A6wG7jaRFrcUf
3UAGaD3DFN5c5NsFItTX/5YaUjqFHD4KA8KOuXhw7i8sui0EBJAKVZIGTipJ2qFR
Um/VfNDztwb7TsBkhbSSMuEBJwtst9czHCvz+YeJ3nACn8e4otNborqYCLmKTnIr
WMW8Exe/QhW1mn6CFbUsve+C75TLLoEGfuSRalavE+Bermd0ouqwcszsrZHXXdlN
IJXfwd6E9Ll4og3JQGu6/E8dJpUSuynOW3vyzqRbiNjw6yl/cwLRU56QDpPVn53s
y3+Z11YS73mxlbLxAeGqYiGVJPsIUF78oVe6DDBlg0hTa7omhrhOup4QkdxOk+7R
rW9qT74x53lE+0oSMlFfqmVHaONbe/VSSWZsVd+SXppF0u91XQ2gRLxnR2VD1u2m
hopyrupUaY8z7kjvgw+4o5Eiwxuny5SUWbbNPsLLe35NfO0Jdyyd
-----END CERTIFICATE REQUEST-----
```

Step 2 Get FMC CSR request, client.csr, signed by CA server using the pxGrid customized template.

Step 3 Enter the IP address of the pxGrid node

Step 4 Upload the external root CA certificate for both the pxGrid Server CA and the MNT Server CA, in this case, MSCARoot1

Step 5 Upload the FMC public certificate and private key, and enter the encryption password, **Save**



Service Type

Primary Host Name/IP Address * 192.168.1.141

Secondary Host Name/IP Address

pxGrid Server CA * MSCARoot1

MNT Server CA * MSCARoot1

FMC Server Certificate * FMCISE21a

ISE Network Filter

* Required Field

Add Known Internal Certificate

Name: FMC14

Certificate Data or, choose a file:

```
BQUHAwQwDAYKKwYBBAGCNwoDBDAKBggrBgEFBQcDAjBEBgkqhkiG9w0BCQ8ENzA1
MA4GCCqGSIb3DQMCAgIAgDAOBggqhkiG9w0DBAICAIAwBwYFKw4DAgcwCgYIKoZI
hvcNAwcwDQYJKoZIhvcNAQELBQADggEBAG5ExAOMrwli5izwiFJbjY9HMpBE8eUV
PAVx/J0somzYqczXcRI0SKjT3BmDzjJuegE0jMwheJKmhax4ox2mOOsCCGfiuX1X
XjJr/qG90xiZiOR3XmgS1tDGgmbSNnZn5hl9oiIuM9nWtAWbGD1FgDFNk30+24Qu
fbk1zybpKBpQI40clzBOxc9bdqUOV17AcoHMjTgcbUbDRvpQoKVKFACbQjWK3h7F
fed9l4zXvgKibjkHUMmAGMZRN1epXwtxuYHm0j35c/QXcgXpT5K0VOiUnArKenQp
7a88zXk5QzCvv6VeOm2ApyJDwIJJf0TYDhEGG2oyZ4/XUlNvm39sktc=
-----END CERTIFICATE-----
```

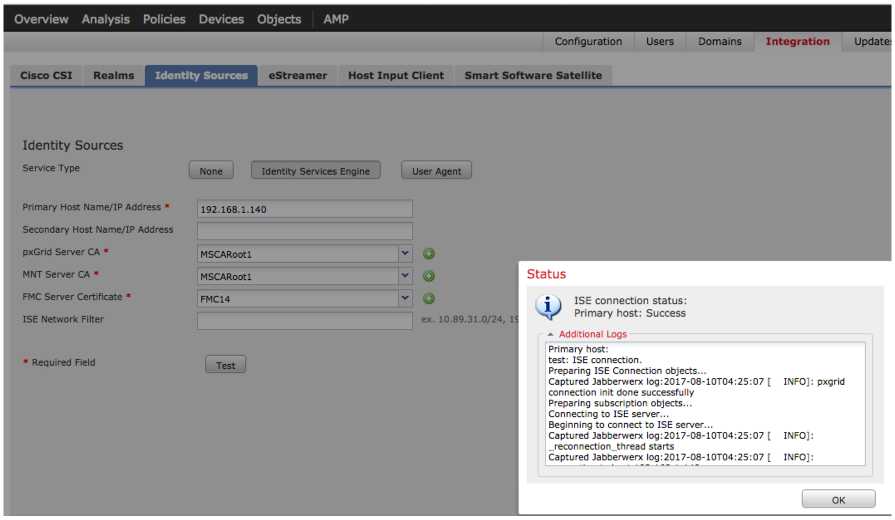
Key or, choose a file:

```
V+Y0hbPcLHwTW54dvEXtobC90sSr/xi1aiHjLsM8E76yz9OOO9ARZqlA7gYy6sli
gcDrCwy4nmcxTjFTkOL8CnNZD+acySajbKIpLXGOUX2DWb3acBirL3zsHM39b7LE
/3Fw84sCkNtqWb+JzjHnQI4XLVHDm6Rvi0BVtuZLFYo+7E1UOBvbdaYU1QbkqHLd
Hw60WiqcvX6vCktNnGyeW1LMYA6s7HIxtombA61aAIGCMJ9HNFUl6Vtwlm+Fr1LE
Nx7wjYBHhEyHJQLggphoYJS+qFz4oMmXul1coxZwSVDp5QuGjeLWyX9FdseUp1d5
A/mFybq3Daf9KRnrxM/H++F21jdxC/mxht7WS0Nxj/DbR3cAFaYFme9tLddwyl5E
LEjgKraVgDJZL+7Ix+RWJxToJL6SllZwqvCcNBRuko+IuDCInfl1hmGWSnfi934Q
BNF+hmKyUN5nlVobZ8FusNrktrKnQTAUd3a+Pk+k/uGajDUeA76dwacjngIAo0/n
-----END RSA PRIVATE KEY-----
```

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

Note: You can also use "cat client.key" to copy/paste into the FMC private key window.

Step 6 You should see:



Identity Sources

Service Type: Identity Services Engine

Primary Host Name/IP Address *: 192.168.1.140

Secondary Host Name/IP Address:

pxGrid Server CA *: MSCARoot1

MNT Server CA *: MSCARoot1

FMC Server Certificate *: FMC14

ISE Network Filter: ex. 10.89.31.0/24, 19

* Required Field

Status

ISE connection status:
Primary host: Success

Additional Logs

```
Primary host:
test: ISE connection.
Preparing ISE Connection objects...
Captured Jabberwerx log:2017-08-10T04:25:07 [    INFO]: pxgrid
connection init done successfully
Preparing subscription objects...
Connecting to ISE server...
Beginning to connect to ISE server...
Captured Jabberwerx log:2017-08-10T04:25:07 [    INFO]:
_reconnection_thread starts
Captured Jabberwerx log:2017-08-10T04:25:07 [    INFO]:
```

Testing pxGrid Integration with Java-based pxGrid Client

Most ecosystem security solution vendors will use the java keystore method instead of working with certificates directly. In this example, pxGridclient.jks is the trusted file keystore and root3.jks is the trusted root keystore. For more references please see: https://communities.cisco.com/docs/DOC-68285

We will create the trust file keystore filename pxGridClient.jks and trust root store filename root3.jks, password for both Cisco123

If the ecosystem security solution does not support certificate encryption, the private key must be decrypted, below is the procedure:

```
cp pxGridClient.key pxGridClient.key.org
openssl rsa -in pxGridClient.key.org -out pxGridClient.key
```

Step 1 Generate a private key

```
openssl genrsa –out pxGridClient.key 4096
```

Step 2 Generate a Certificate Signing Request (CSR)

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

Step 3 Import CA root certificate into PKCS12 file

```
openssl pkcs12 –export –out pxGridClient.p12 –inkey pxGridClient.key –in pxGridClient.cer –chain –CAfile
ca_root.cer
```

Step 4 Create the trusted file keystore

```
keytool –import –srckeystore pxGridClient.p12 –destkeystore pxGridClient.jks –srcstoretype PKCS12
```

Step 5 Convert the .cer file to .der format

```
openssl x509 –outform der –in ca_oot.cer –out ca_root.der
```

Step 6 Import the CA root certificate into the trusted root keystore

```
keytool –import –alias isemnt –keystore root3.jks –file ca_root.der
```

Step 7 Import the client certificate into trusted root keystore

```
keytool –import –alias pxGridMAC –keystore pxGridCient.jks –file pxGridClient.cer
```

Step 8 Import root certificate into trusted root keystore

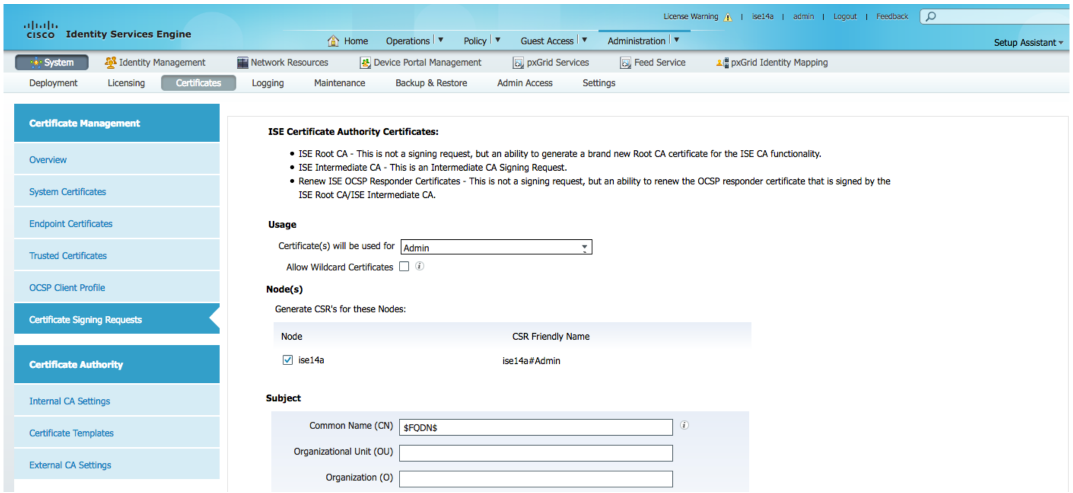
```
keytool –import –alias ca_root1 –keystore root3.jks –file ca_root.cer
```

Deploying Cisco ISE 1.3/1.4 with External CA Certificates

This section discusses pxGrid deployment for ISE I.3/1.4 in productional environments using and external Certificate Authority (CA) for certificate deployment. A pxGrid certificate is required for the ISE Primary Admin, ISE Secondary Admin, ISE Primary MNT, ISE Secondary, Primary and Secondary pxGrid nodes. The external CA server requires a customized "pxGrid" template to services this request. This customized template must contain an EKU of both client authentication and server authentication. If you are not familiar with creating this template, please see **Customized pxGrid Template** under **References** section.

Generating CSR Requests for ISE nodes

Step 1 Generate the Certificate Signing Requests (CSR) for all the ISE nodes. Below is a sample for the ISE admin node.
Select **Administration->System->Certificates->Certificate Management->Certificate Signing Requests**



ISE Certificate Authority Certificates:

- ISE Root CA - This is not a signing request, but an ability to generate a brand new Root CA certificate for the ISE CA functionality.
- ISE Intermediate CA - This is an Intermediate CA Signing Request.
- Renew ISE OCSP Responder Certificates - This is not a signing request, but an ability to renew the OCSP responder certificate that is signed by the ISE Root CA/ISE Intermediate CA.

Usage

Certificate(s) will be used for: Admin

Allow Wildcard Certificates □

Node(s)

Generate CSR's for these Nodes:

Node	CSR Friendly Name
☑ ise14a	ise14a#Admin

Subject

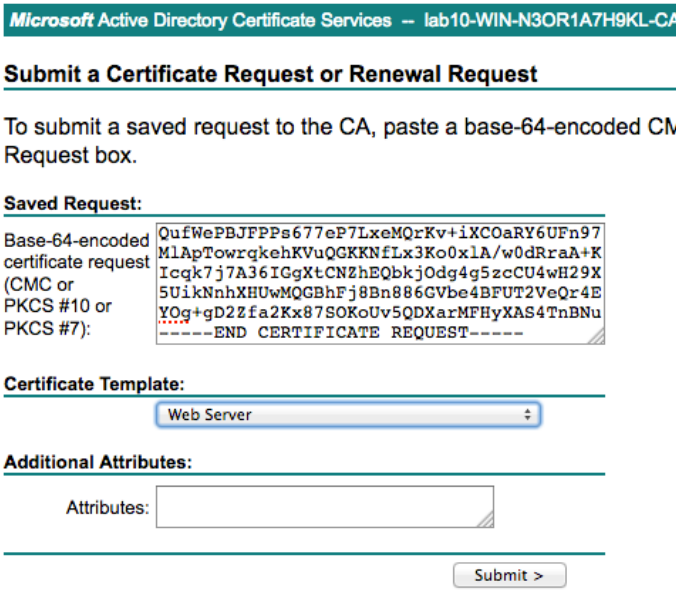
Common Name (CN): $FQDN$

Organizational Unit (OU):

Organization (O):

Step 2 Select **Generate** and **Export**, copy/paste the CSR request into CA authority Advanced Server request and get the certificate signed by the CA using the "web server" template

Note: For admin and MNT nodes, you can use the "customized" pxGrid template, by default the 'usage" for pxGrid will be enabled. If you have the "web server" template" for the certificate, you will need to generate an additional certificate for pxGrid as demonstrated in the following steps



Microsoft Active Directory Certificate Services -- lab10-WIN-N3OR1A7H9KL-CA

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CM
Request box.

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

```
QufWePBJFPPs677eP7LxeMQrKv+iXCOaRY6UFn97
MlApTowrqkehKVuQGKKNfLx3Ko0xlA/w0dRraA+K
Icqk7j7A36IGgXtCNZhEQbkjOdg4g5zcCU4wH29X
5UikNnhXHUwMQGBhFj8Bn886GVbe4BFUT2VeQr4E
YOg+gD2Zfa2Kx87SOKoUv5QDXarMFHyXAS4TnBNu
-----END CERTIFICATE REQUEST-----
```

Certificate Template:

Web Server

Additional Attributes:

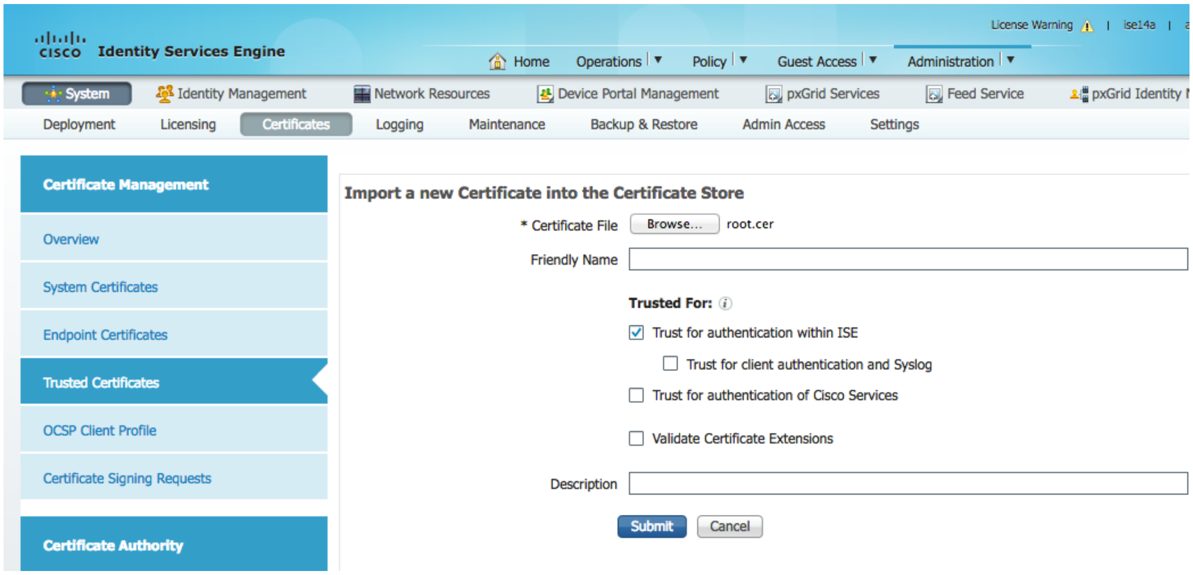
Attributes:

Step 3 Select **Submit**

Step 4 Download the certificate in base 64 encoded format.

Step 5 Also download the CA root certificate in based 64 encoded format.

Step 6 Import the CA root certificate into the ISE trusted certificate store.
Select **Administration->System->Certificates->Certificate Management->Trusted Certificates and** upload the root certificate



Import a new Certificate into the Certificate Store

* Certificate File Browse... root.cer

Friendly Name

Trusted For:

☑ Trust for authentication within ISE

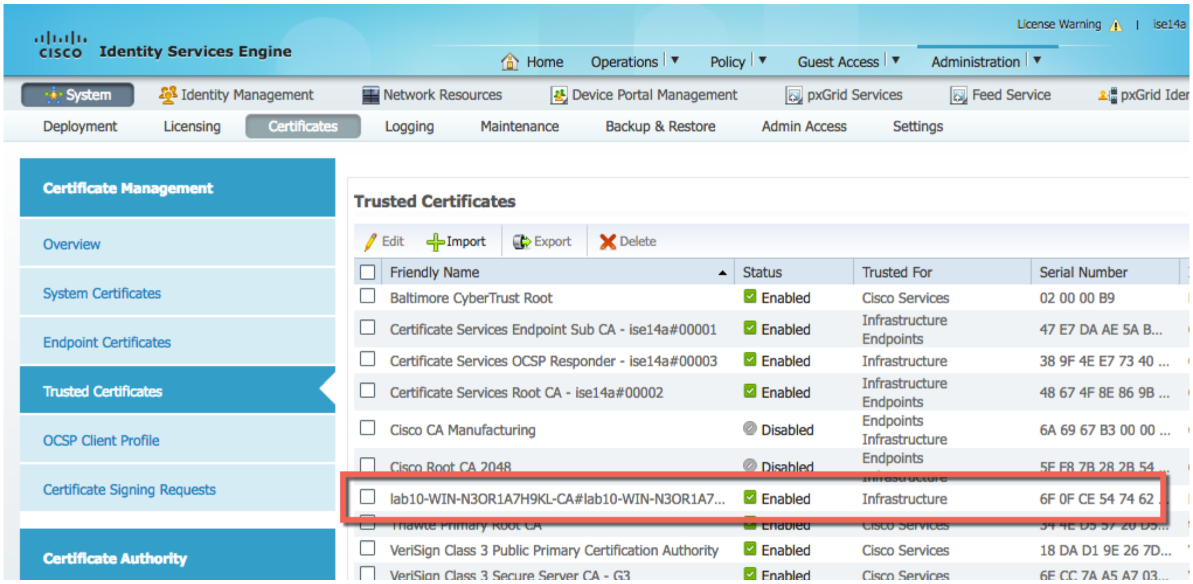
☐ Trust for client authentication and Syslog

☐ Trust for authentication of Cisco Services

☐ Validate Certificate Extensions

Description

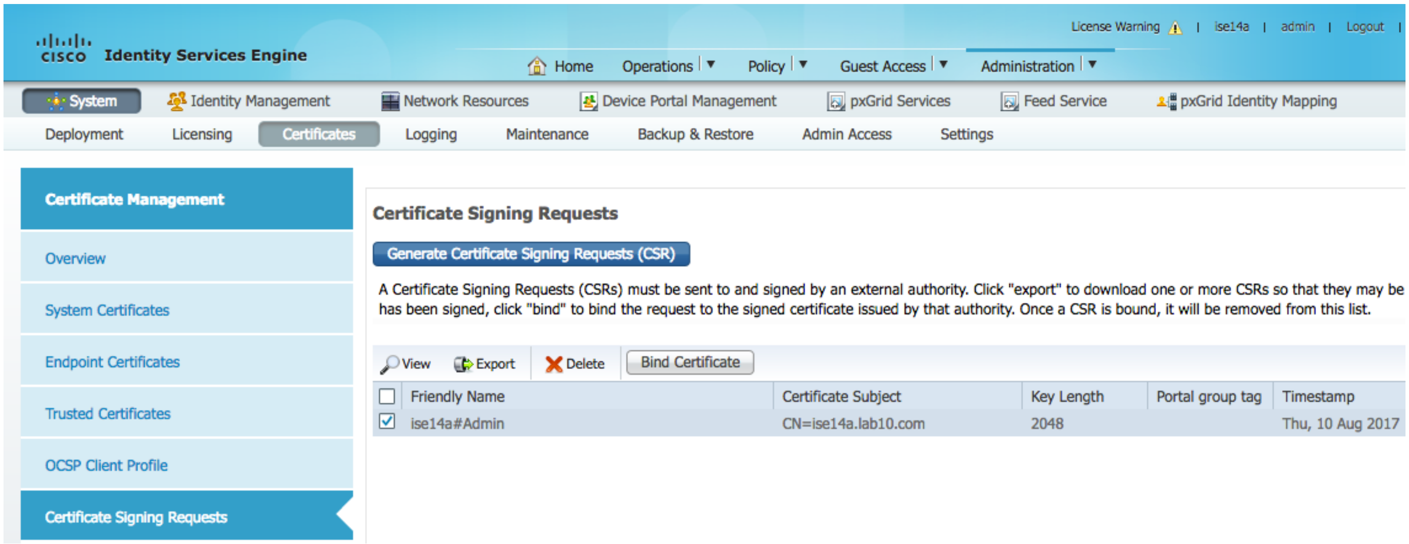
Step 7 Select **Submit**, you should see:


Identity Services Engine
License Warning | ise14a
Home Operations Policy Guest Access Administration
System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service pxGrid Ider
Deployment Licensing Certificates Logging Maintenance Backup & Restore Admin Access Settings
Certificate Management
Overview
System Certificates
Endpoint Certificates
Trusted Certificates
OCSP Client Profile
Certificate Signing Requests
Certificate Authority
Edit Import Export Delete

Trusted Certificates

□	Friendly Name	Status	Trusted For	Serial Number
□	Baltimore CyberTrust Root	Enabled	Cisco Services	02 00 00 B9
□	Certificate Services Endpoint Sub CA - ise14a#00001	Enabled	Infrastructure Endpoints	47 E7 DA AE 5A B...
□	Certificate Services OCSP Responder - ise14a#00003	Enabled	Infrastructure	38 9F 4E E7 73 40 ...
□	Certificate Services Root CA - ise14a#00002	Enabled	Infrastructure Endpoints	48 67 4F 8E 86 9B ...
□	Cisco CA Manufacturing	Disabled	Endpoints Infrastructure	6A 69 67 B3 00 00 ...
□	Cisco Root CA 2048	Disabled	Endpoints Infrastructure	5F F8 7B 28 2B 54 ...
□	lab10-WIN-N3OR1A7H9KL-CA#lab10-WIN-N3OR1A7...	Enabled	Infrastructure	6F 0F CE 54 74 62 ...
□	Thawte Primary Root CA	Enabled	Cisco Services	34 4E D5 57 20 D5...
□	VeriSign Class 3 Public Primary Certification Authority	Enabled	Cisco Services	18 DA D1 9E 26 7D...
□	VeriSign Class 3 Secure Server CA - G3	Enabled	Cisco Services	6E CC 7A A5 A7 03...

Step 8 Bind the certificates to their associated Binding request. Select **Administration->System->Certificates->Certificate Management->Certificate Signing Requests->edit the node->Bind Certificate**

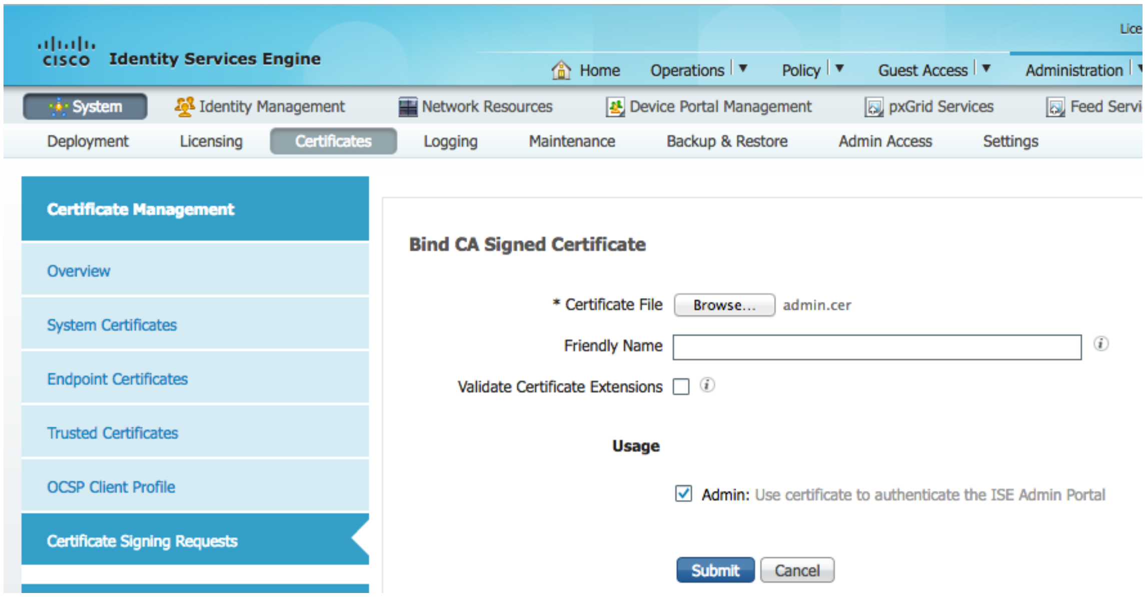

Identity Services Engine
License Warning | ise14a | admin | Logout
Home Operations Policy Guest Access Administration
System Identity Management Network Resources Device Portal Management pxGrid Services Feed Service pxGrid Identity Mapping
Deployment Licensing Certificates Logging Maintenance Backup & Restore Admin Access Settings
Certificate Management
Overview
System Certificates
Endpoint Certificates
Trusted Certificates
OCSP Client Profile
Certificate Signing Requests
Generate Certificate Signing Requests (CSR)
View Export Delete Bind Certificate

Certificate Signing Requests

A Certificate Signing Requests (CSRs) must be sent to and signed by an external authority. Click "export" to download one or more CSRs so that they may be has been signed, click "bind" to bind the request to the signed certificate issued by that authority. Once a CSR is bound, it will be removed from this list.

□	Friendly Name	Certificate Subject	Key Length	Portal group tag	Timestamp
☑	ise14a#Admin	CN=ise14a.lab10.com	2048		Thu, 10 Aug 2017

Step 9 Upload the ISE admin node certificate select **Submit**



Bind CA Signed Certificate

* Certificate File: Browse... admin.cer

Friendly Name:

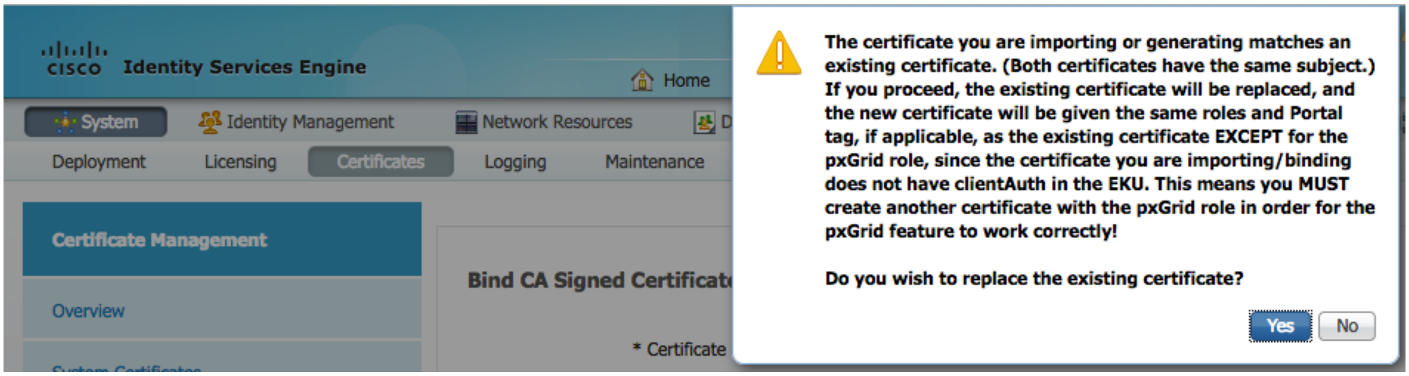
Validate Certificate Extensions □

Usage

☑ Admin: Use certificate to authenticate the ISE Admin Portal

Step 10 Select **Submit**

Step 11 You will see the following message



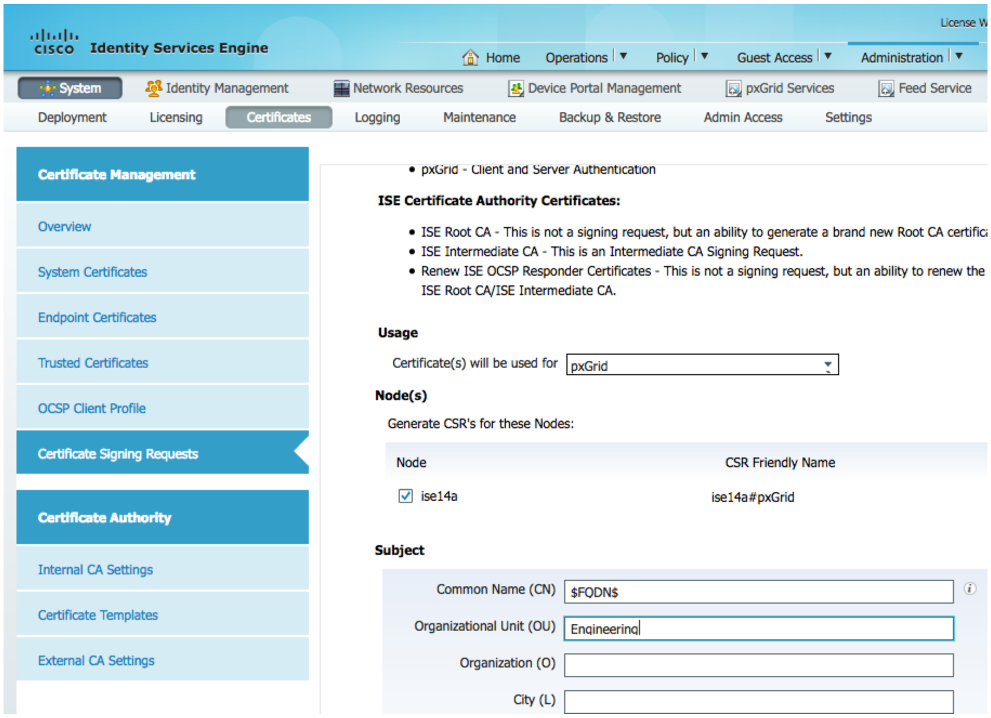
The certificate you are importing or generating matches an existing certificate. (Both certificates have the same subject.) If you proceed, the existing certificate will be replaced, and the new certificate will be given the same roles and Portal tag, if applicable, as the existing certificate EXCEPT for the pxGrid role, since the certificate you are importing/binding does not have clientAuth in the EKU. This means you MUST create another certificate with the pxGrid role in order for the pxGrid feature to work correctly!

Do you wish to replace the existing certificate?

Step 12 Select **Yes**

Step 13 System will restart

Step 14 Generate another certificate for pxGrid communication
Select **Administration->System->Certificates>Certificate Management->Certificate Signing Requests->Select "pxGrid" usage**
Enter "**Engineering**" in the OU field or some other description. This must not match the OU field in the admin certificate.



- pxGrid - Client and Server Authentication

ISE Certificate Authority Certificates:

- ISE Root CA - This is not a signing request, but an ability to generate a brand new Root CA certific
- ISE Intermediate CA - This is an Intermediate CA Signing Request.
- Renew ISE OCSP Responder Certificates - This is not a signing request, but an ability to renew the ISE Root CA/ISE Intermediate CA.

Usage

Certificate(s) will be used for: pxGrid

Node(s)

Generate CSR's for these Nodes:

Node	CSR Friendly Name
☑ ise14a	ise14a#pxGrid

Subject

Common Name (CN): $FQDN$

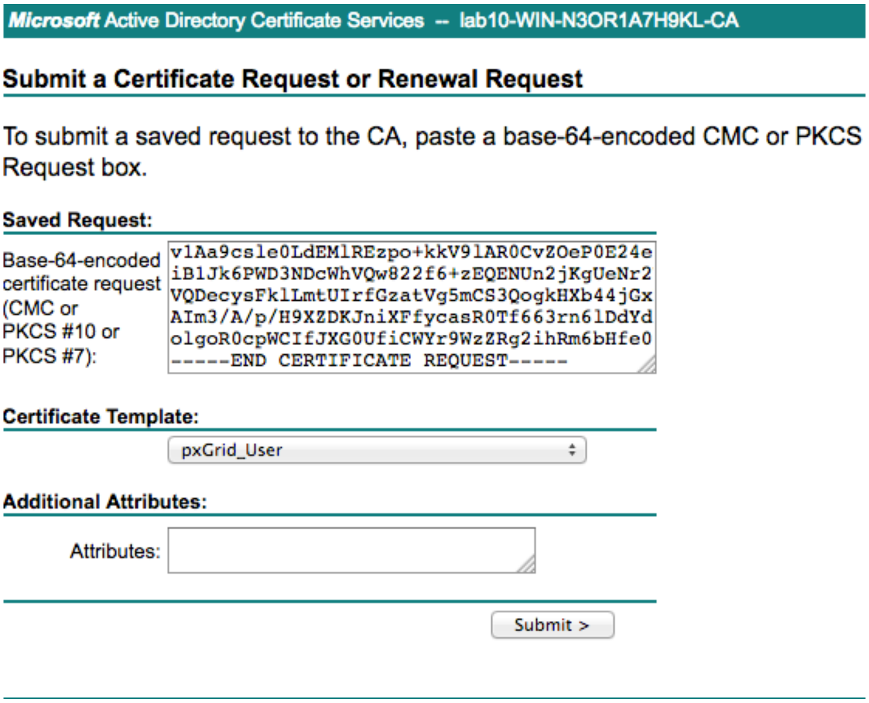
Organizational Unit (OU): Engineering

Organization (O):

City (L):

Step 15 Select **Generate** and **Export**

Step 16 Copy/Paste the CSR request into the Advanced user request and select the customized pxGrid template



Microsoft Active Directory Certificate Services -- lab10-WIN-N3OR1A7H9KL-CA

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS Request box.

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

```
vlAa9csle0LdEMlREzpo+kkV9lAR0CvZOeP0E24e
iBlJk6PWD3NDcWhVQw822f6+zEQENUn2jKgUeNr2
VQDecysFklLmtUIrfGzatVg5mCS3QogkHXb44jGx
AIm3/A/p/H9XZDKJniXFfycasR0Tf663rn6lDdYd
olgoR0cpWCIfJXG0UfiCWYr9WzZRg2ihRm6bHfe0
-----END CERTIFICATE REQUEST-----
```

Certificate Template:

pxGrid_User

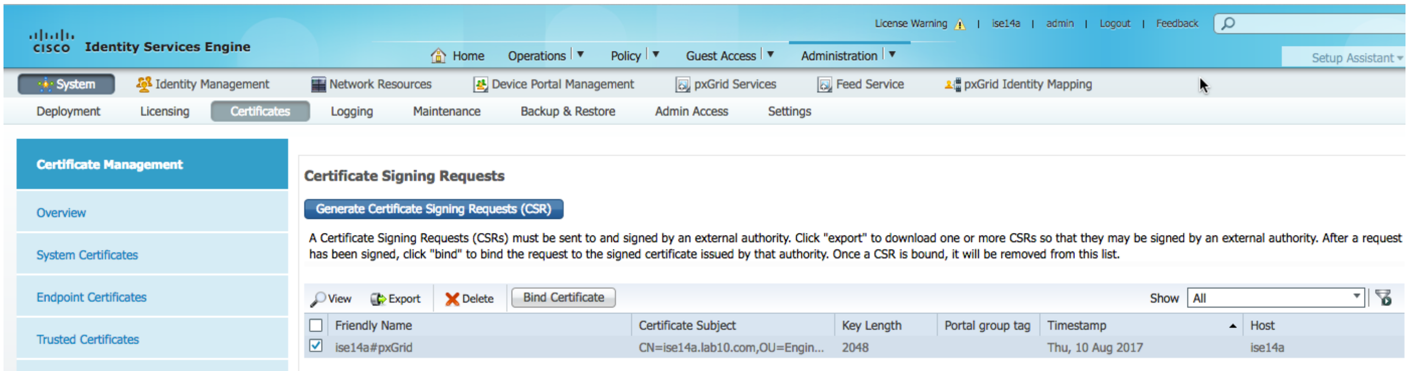
Additional Attributes:

Attributes:

Step 17 Select **Submit** and download the certificate in base 64 encoded format

Step 18 Bind certificate to the CSR request

Select **Administration->System->Certificates->Certificate Management->Certificate Signing Requests (CSR)-edit node->Bind Certificate**

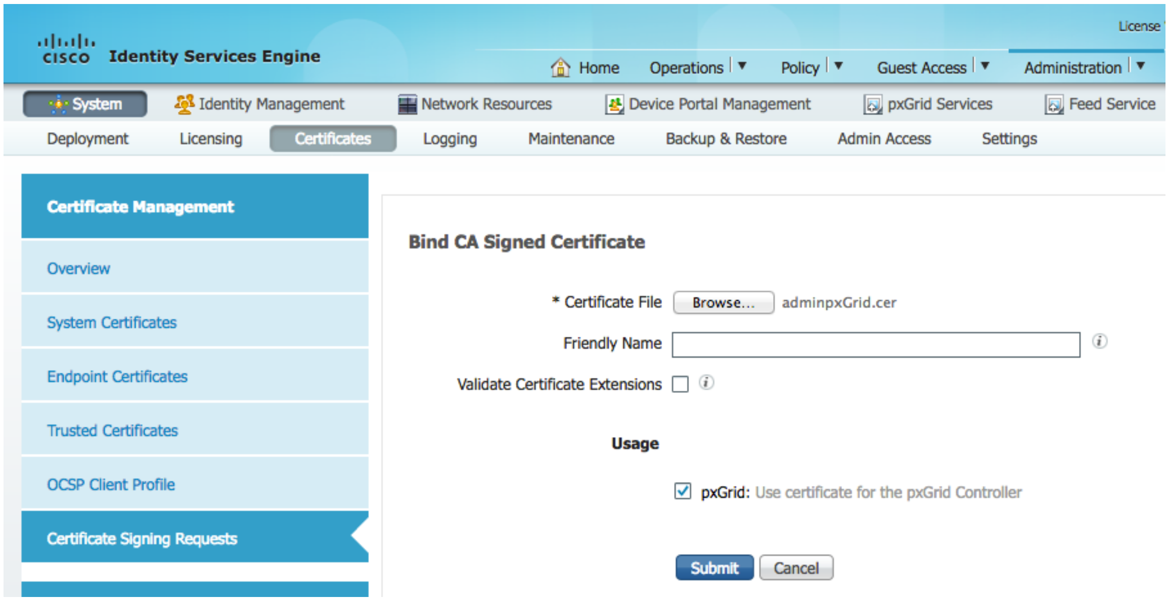


Certificate Signing Requests

A Certificate Signing Requests (CSRs) must be sent to and signed by an external authority. Click "export" to download one or more CSRs so that they may be signed by an external authority. After a request has been signed, click "bind" to bind the request to the signed certificate issued by that authority. Once a CSR is bound, it will be removed from this list.

	Friendly Name	Certificate Subject	Key Length	Portal group tag	Timestamp	Host
☑	ise14a#pxGrid	CN=ise14a.lab10.com,OU=Engin...	2048		Thu, 10 Aug 2017	ise14a

Step 19 Upload the pxGrid certificate for the admin node



Bind CA Signed Certificate

* Certificate File adminpxGrid.cer

Friendly Name

Validate Certificate Extensions □

Usage

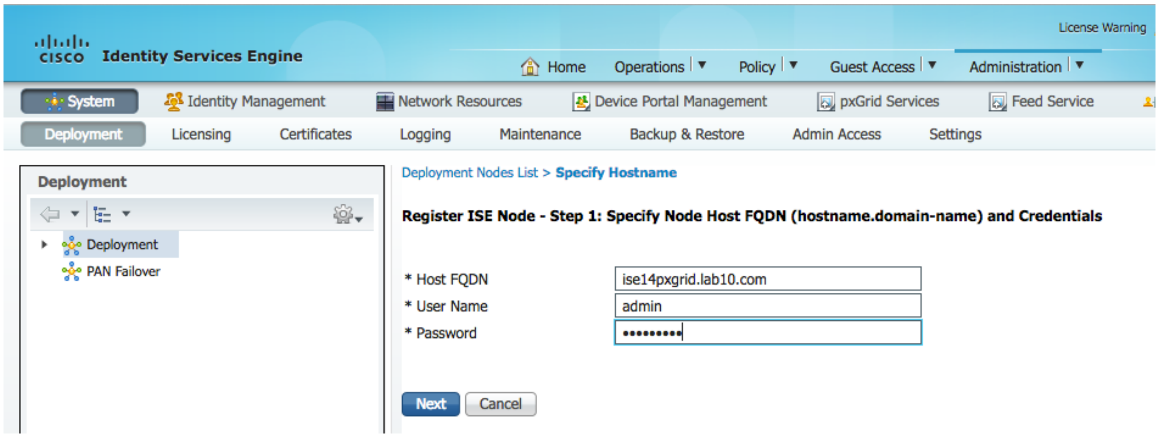
☑ pxGrid: Use certificate for the pxGrid Controller

Step 20 Select **submit**

Step 21 Perform the steps 1-21 for all the ISE nodes.

Registering ISE Nodes

Step 1 Register the desired ISE pxGrid node via the Primary Admin node and enable for pxGrid operation ONLY. Select **Administration->System->Deployment->Deployment Nodes->Register and enter the HOST FQDN name of the ISE pxGrid node**



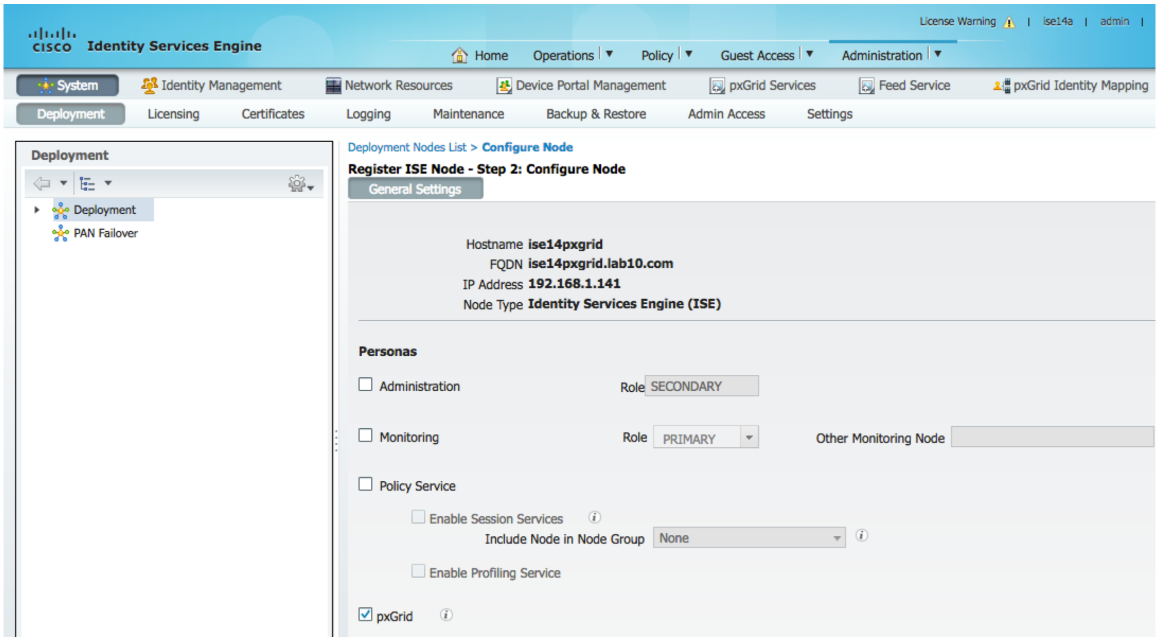
Deployment Nodes List > **Specify Hostname**

Register ISE Node - Step 1: Specify Node Host FQDN (hostname.domain-name) and Credentials

* Host FQDN ise14pxgrid.lab10.com
* User Name admin
* Password •••••••••

Step 2 Select **Next**

Step 3 Enable **pxGrid**



Deployment Nodes List > **Configure Node**

Register ISE Node - Step 2: Configure Node

Hostname **ise14pxgrid**
FQDN **ise14pxgrid.lab10.com**
IP Address **192.168.1.141**
Node Type **Identity Services Engine (ISE)**

Personas

□ Administration Role SECONDARY

□ Monitoring Role PRIMARY Other Monitoring Node

□ Policy Service

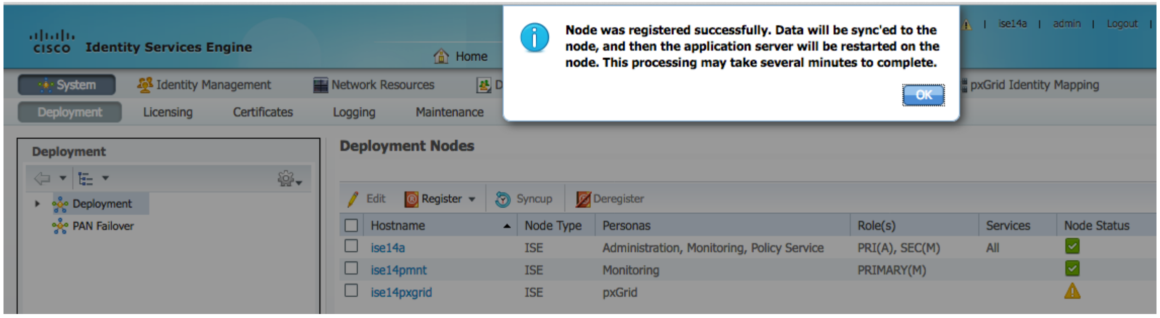
□ Enable Session Services
Include Node in Node Group None

□ Enable Profiling Service

☑ pxGrid

Step 4 Select Save

Step 5 You should see that the dedicated pxGrid node sync process has begun

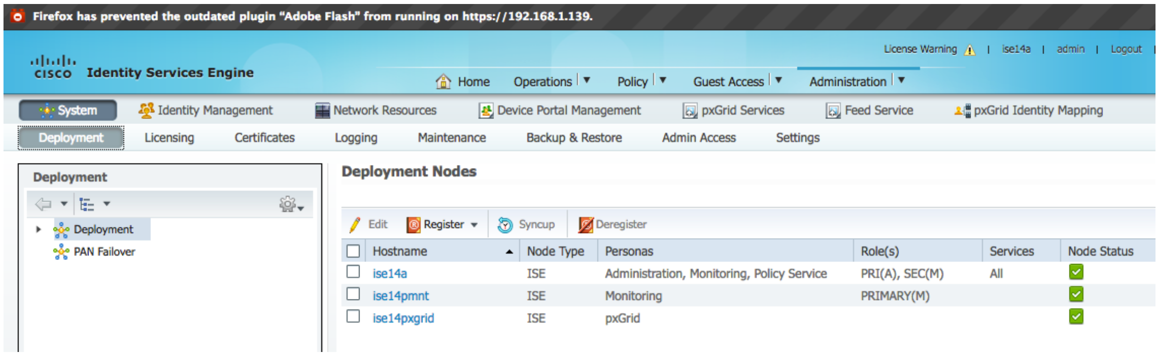


Node was registered successfully. Data will be sync'ed to the node, and then the application server will be restarted on the node. This processing may take several minutes to complete.

Deployment Nodes

□	Hostname	Node Type	Personas	Role(s)	Services	Node Status
□	ise14a	ISE	Administration, Monitoring, Policy Service	PRI(A), SEC(M)	All	✓
□	ise14pmnt	ISE	Monitoring	PRIMARY(M)		✓
□	ise14pxgrid	ISE	pxGrid			⚠

Step 6 After a couple of minutes you should see that the ISE pxGrid node has successfully synced



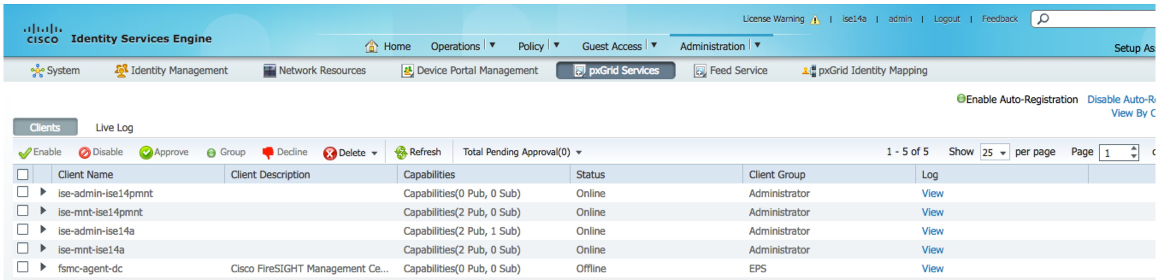
Firefox has prevented the outdated plugin "Adobe Flash" from running on https://192.168.1.139.

Deployment Nodes

□	Hostname	Node Type	Personas	Role(s)	Services	Node Status
□	ise14a	ISE	Administration, Monitoring, Policy Service	PRI(A), SEC(M)	All	✓
□	ise14pmnt	ISE	Monitoring	PRIMARY(M)		✓
□	ise14pxgrid	ISE	pxGrid			✓

Step 7 Register all the ISE nodes through the ISE Primary admin node

Step 8 Verify the published ISE nodes appear and there is connectivity
Select **Administration->pxGrid Services**



□		Client Name	Client Description	Capabilities	Status	Client Group	Log
□	▸	ise-admin-ise14pmnt		Capabilities(0 Pub, 0 Sub)	Online	Administrator	View
□	▸	ise-mnt-ise14pmnt		Capabilities(2 Pub, 0 Sub)	Online	Administrator	View
□	▸	ise-admin-ise14a		Capabilities(2 Pub, 1 Sub)	Online	Administrator	View
□	▸	ise-mnt-ise14a		Capabilities(2 Pub, 0 Sub)	Online	Administrator	View
□	▸	fsmc-agent-dc	Cisco FireSIGHT Management Ce...	Capabilities(0 Pub, 0 Sub)	Offline	EPS	View

Generating pxGrid Client Certificates

Step 1 Generate private key using –des3. The –des3 argument provides the encryption password.

```
openssl genrsa -des3 -out client.key 4096
Generating RSA private key, 4096 bit long modulus
.........
........................
e is 65537 (0x10001)
Enter pass phrase for client.key: Cisco123
Verifying - Enter pass phrase for client.key: Cisco123
```

Step 2 Generate CSR request

```
openssl req -new -key client.key -out client.csr
Enter pass phrase for client.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 Code []:US
State or Province Name []:Maryland
Locality Name []:Germantown
Organization Name []:Cisco
Organizational Unit Name []:Engineering
Common Name []:fmc62.lab10.com
Email Address []:j@c.com
```

Testing using Cisco Firepower Management Center 6.1

In this example, Firepower Management Center 6.1 was used for testing. For other Cisco Security Solutions and Ecosystem partner integrations, please see: https://communities.cisco.com/docs/DOC-64012#/jive_content_id_Cisco_Platform_Exchange_Grid_pxGrid

Step 1 Copy CSR request into pxGrid template

```
cat client.csr
-----BEGIN CERTIFICATE REQUEST-----
MIIE0zCCArsCAQAwgY0xCzAJBgNVBAYTAlVTMREwDwYDVQQIEwhNYXJ5bGFuZDET
MBEGA1UEBxMKR2VybWFudG93bjEOMAwGA1UEChMFQ2lzY28xFDASBgNVBAsTC0Vu
Z2luZWVyaW5nMRgwFgYDVQQDEw9mbWM2Mi5sYWIxMC5jb20xFjAUBgkqhkiG9w0B
CQEWB2pAYy5jb20wggIiMA0GCSqGSIb3DQEBAQUAA4ICDwAwggIKAoICAQC6gXkN
wGLdzv3P5IApJIRePWAKd+2uab6ikZX+HfIsAdg8sMxw/VVqCiJ7eu1zoeApZn2L
7JJ4tq4iHjyI9N0kTMrBlqHsoKPrvQZUMAKWs8LLK5jgElhShNpidClmWW9kZtE+
6179ig21j7V0BFo+pmx0cLNoOA/rTXhAJKbuKsLpyEnALDjgDXYpIHuRKJOSps6C
6geiK7jJ4lzoG4lxvRuudDiauUxLDKh2L/ga44STTAeahXWBkF0u43zkmrPFR0Ck
7vo3yQf0ha/5Kl/41Q0oULe1rkmE5/ApNsQ90r8wpm961biog3GnRg0uEww2ODIp
dPI5bJSgup8y+gsS0CilFCUDXgywRdt/DRTxJjiPX/YQiPvwS+rcxeDg/PqlmtwA
uVhcGdCEMRqYY08yPhIomDuGpVL0vu1iNo3CDjYH/r5W2tAEPOLWx8nArJjsCkfC
Z8ld/BBdfHoh4X9xcfteLr48zxSoh0RgD9wCjkbF7N0m+313weARnOBkKWAIpOFu
G60ceERm8rf6xDQdgBtLWRhfBPKNuS5Ljsb0m5QeD/340KwGCKxMem7hUPCxLNxC
```

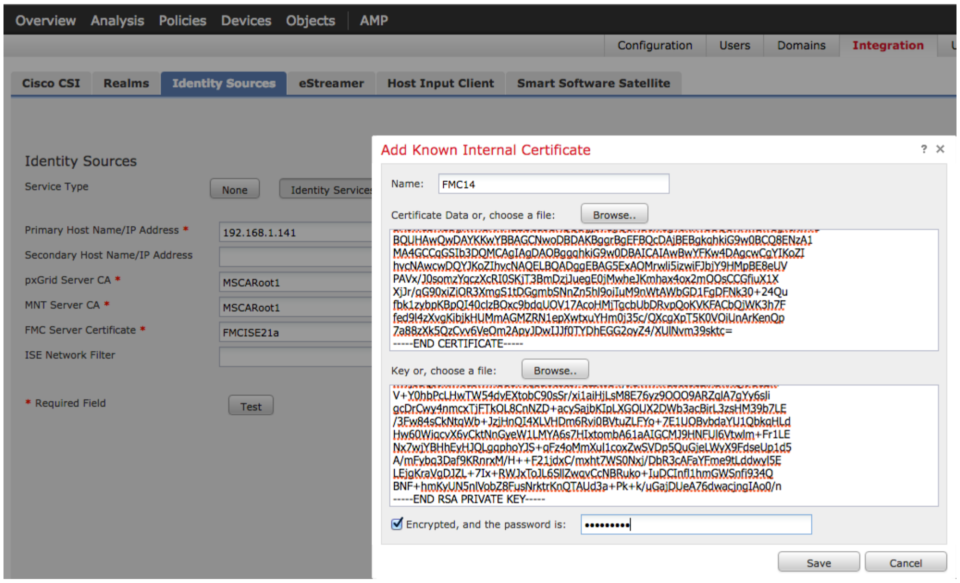
```
XUhmszqhppBhKymw0iw/f7th0XkBPuw4amXlgsi3tMgaK5DG17D105XDb4ssChZf
4iym5WZ0Inxo1g+27tQGnMgYePqG58YCMaHegQIDAQABoAAwDQYJKoZIhvcNAQEL
BQADggIBAEEJKjsEak/ud/mFJrjz5GaedsnIxF1tXZDjQyqZH1HS7+TUuaHrQGOn
tYpVoiT60Js8o516T0eAbXTnTh3mP9yHpHbRKBWpNNB1H/+FcSI9uSzrzJymyb8a
URLAJKcw0in6weVC/52F7DYeVTrEZfwHJFKaxS0033KEi+4fphPde+cHZsmB0aQG
Aa2jdn7zuaY6ZxE8YfZsvwRMkEwVu/ZGKRuBAsX6RFokH5OUAH1A6wG7jaRFrcUf
3UAGaD3DFN5c5NsFItTX/5YaUjqFHD4KA8KOuXhw7i8sui0EBJAKVZIGTipJ2qFR
Um/VfNDztwb7TsBkhbSSMuEBJwtst9czHCvz+YeJ3nACn8e4otNborqYCLmKTnIr
WMW8Exe/QhW1mn6CFbUsve+C75TLLoEGfuSRalavE+Bermd0ouqwcszsrZHXXdlN
IJXfwd6E9Ll4og3JQGu6/E8dJpUSuynOW3vyzqRbiNjw6yl/cwLRU56QDpPVn53s
y3+Z11YS73mxlbLxAeGqYiGVJPsIUF78oVe6DDBlg0hTa7omhrhOup4QkdxOk+7R
rW9qT74x53lE+0oSMlFfqmVHaONbe/VSSWZsVd+SXppF0u91XQ2gRLxnR2VD1u2m
hopyrupUaY8z7kjvgw+4o5Eiwxuny5SUWbbNPsLLe35Nf O0Jdyyd
-----END CERTIFICATE REQUEST-----
```

Step 2 Get FMC CSR request, client.csr, signed by CA server using the pxGrid customized template.

Step 3 Enter the IP address of the pxGrid node

Step 4 Upload the external root CA certificate for both the pxGrid Server CA and the MNT Server CA, in this case, MSCARoot1

Step 5 Upload the FMC public certificate and private key, and enter the encryption password, **Save**



Identity Sources

Service Type

Primary Host Name/IP Address * 192.168.1.141

Secondary Host Name/IP Address

pxGrid Server CA * MSCARoot1

MNT Server CA * MSCARoot1

FMC Server Certificate * FMCISE21a

ISE Network Filter

Add Known Internal Certificate

Name: FMC14

Certificate Data or, choose a file:

```
BQUHAwQwDAYKKwYBBAGCNwoDBDAKBggrBgEFBQcDAjBEBgkqhkiG9w0BCQ8ENzA1
MA4GCCqGSIb3DQMCAgIAgDAOBggqhkiG9w0DBAICAIAwBwYFKw4DAgcwCgYIKoZI
hvcNAwcwDQYJKoZIhvcNAQELBQADggEBAG5ExAOMrwli5izwiFJbjY9HMpBE8eUV
PAVx/J0somzYqczXcRI0SKjT3BmDzjJuegE0jMwheJKmhax4ox2mOOsCCGfiuX1X
XjJr/qG90xiZiOR3XmgS1tDGgmbSNnZn5hl9oiIuM9nWtAWbGD1FgDFNk30+24Qu
fbk1zybpKBpQI40clzBOxc9bdqUOV17AcoHMjTgcbUbDRvpQoKVKFACbQjWK3h7F
fed9l4zXvgKibjkHUMmAGMZRN1epXwtxuYHm0j35c/QXcgXpT5K0VOiUnArKenQp
7a88zXk5QzCvv6VeOm2ApyJDwIJJf0TYDhEGG2oyZ4/XUlNvm39sktc=
-----END CERTIFICATE-----
```

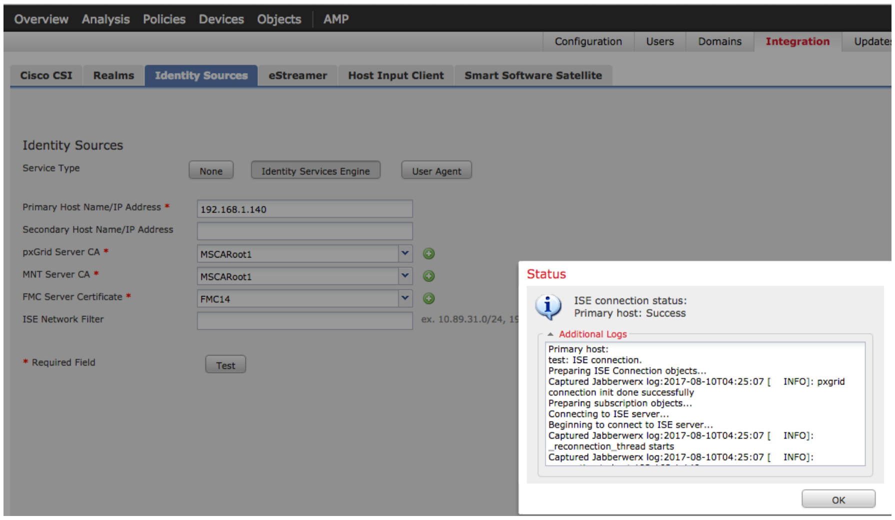
Key or, choose a file:

```
V+Y0hbPcLHwTW54dvEXtobC90sSr/xi1aiHjLsM8E76yz9OOO9ARZqlA7gYy6sli
gcDrCwy4nmcxTjFTkOL8CnNZD+acySajbKIpLXGOUX2DWb3acBirL3zsHM39b7LE
/3Fw84sCkNtqWb+JzjHnQI4XLVHDm6Rvi0BVtuZLFYo+7E1UOBvbdaYU1QbkqHLd
Hw60WiqcvX6vCktNnGyeW1LMYA6s7HIxtombA61aAIGCMJ9HNFUl6Vtwlm+Fr1LE
Nx7wjYBHhEyHJQLgqphoYJS+qFz4oMmXul1coxZwSVDp5QuGjeLWyX9FdseUp1d5
A/mFybq3Daf9KRnrxM/H++F21jdxC/mxht7WS0Nxj/DbR3cAFaYFme9tLddwyl5E
LEjgKraVgDJZL+7Ix+RWJxToJL6SllZwqvCcNBRuko+IuDCInfl1hmGWSnfi934Q
BNF+hmKyUN5nlVobZ8FusNrktrKnQTAUd3a+Pk+k/uGajDUeA76dwacjngIAo0/n
-----END RSA PRIVATE KEY-----
```

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

Note: You can also use “cat client.key” to copy/paste into the FMC private key window.

Step 6 You should see:



Identity Sources

Service Type: Identity Services Engine

Primary Host Name/IP Address *: 192.168.1.140

Secondary Host Name/IP Address:

pxGrid Server CA *: MSCARoot1

MNT Server CA *: MSCARoot1

FMC Server Certificate *: FMC14

ISE Network Filter: ex. 10.89.31.0/24, 19

* Required Field

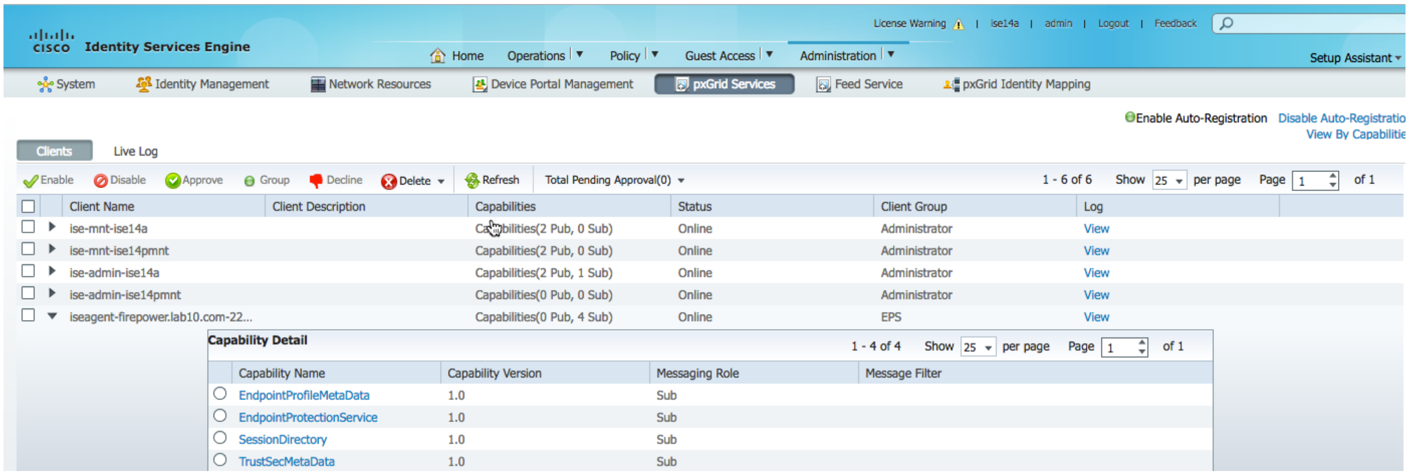
Status

ISE connection status:
Primary host: Success

Additional Logs

```
Primary host:
test: ISE connection.
Preparing ISE Connection objects...
Captured Jabberwerx log:2017-08-10T04:25:07 [    INFO]: pxgrid
connection init done successfully
Preparing subscription objects...
Connecting to ISE server...
Beginning to connect to ISE server...
Captured Jabberwerx log:2017-08-10T04:25:07 [    INFO]:
_reconnection_thread starts
Captured Jabberwerx log:2017-08-10T04:25:07 [    INFO]:
```

Step 7 Select **Administration->pxGrid Services**



1 - 6 of 6 Show 25 per page Page 1 of 1

	Client Name	Client Description	Capabilities	Status	Client Group	Log
□	ise-mnt-ise14a		Capabilities(2 Pub, 0 Sub)	Online	Administrator	View
□	ise-mnt-ise14pmnt		Capabilities(2 Pub, 0 Sub)	Online	Administrator	View
□	ise-admin-ise14a		Capabilities(2 Pub, 1 Sub)	Online	Administrator	View
□	ise-admin-ise14pmnt		Capabilities(0 Pub, 0 Sub)	Online	Administrator	View
□	iseagent-firepower.lab10.com-22...		Capabilities(0 Pub, 4 Sub)	Online	EPS	View

Capability Detail

1 - 4 of 4 Show 25 per page Page 1 of 1

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

Testing pxGrid Integration with Java-based pxGrid Client

Most ecosystem security solution vendors will use the java keystore method instead of working with certificates directly. In this example, pxGridclient.jks is the trusted file keystore and root3.jks is the trusted root keystore and the password for both is Cisco123. For more references please see: https://communities.cisco.com/docs/DOC-68285

If the ecosystem security solution does not support certificate encryption, the private key must be decrypted, below is the procedure:

```
cp firepower.lab10.com_00-0c-29-80-27-8a.key firepower.lab10.com_00-0c-29-80-27-8a.key.org
openssl rsa -in firepower.lab10.com_00-0c-29-80-27-8a.key.org -out firepower.lab10.com_00-0c-29-80-27-8a.key
```

Step 1 Generate a private key

```
openssl genrsa –out pxGridClient.key 4096
```

Step 2 Generate a Certificate Signing Request (CSR)

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

Step 3 Import CA root certificate into PKCS12 file

```
openssl pkcs12 –export –out pxGridClient.p12 –inkey pxGridClient.key –in pxGridClient.cer –chain –CAfile
ca_root.cer
```

Step 4 Create the trusted file keystore

```
keytool –import –srckeystore pxGridClient.p12 –destkeystore pxGridClient.jks –srcstoretype PKCS12
```

Step 5 Convert the .cer file to .der format

```
openssl x509 –outform der –in ca_oot.cer –out ca_root.der
```

Step 6 Import the CA root certificate into the trusted root keystore

```
keytool –import –alias isemnt –keystore root3.jks –file ca_root.der
```

Step 7 Import the client certificate into trusted root keystore

```
keytool –import –alias pxGridMAC –keystore pxGridCient.jks –file pxGridClient.cer
```

Step 8 Import root certificate into trusted root keystore

```
keytool –import –alias ca_root1 –keystore root3.jks –file ca_root.cer
```

Troubleshooting

ISE 1.3/14

Self-Signed Certificates

- For Proof of Concept (POV) environments, you can use self-signed certificates. For self-signed certificates you would need to import the ISE Identity certificate into the ISE trusted system store.

Bulk-Download Active Hosts not working

- Promote the ISE-stand-alone to primary node. There was an issue with the Fully Qualified Domain Name (FQDN). This was resolved in ISE 2.0+
- Ensure the CA root certificate is used for MNT certificate selection if this is applicable to the pxGrid client
- Ensure the CA root certificate is in the trusted root keystore if the JAVA keystores are used.

ISE 1.3/1.4/2.0/2.1/2.2+

pxGrid clients not connecting

- Can be stuck waiting for admin approval- Ensure Auto Registration is enabled and Client settings set for Auto Approval.
- Ensure that the external root certificate is in the in the application's trusted root keystore if java or in the trusted Certificate Authority (CA) store if using certificates directly.
- Ensure that times are synced between the ecosystem or Cisco Security Solution and ISE pxGrid nodes or ISE in general
- The pxGrid client and ISE should be Fully Qualified Domain Name (FQDN) name resolvable
- Certificate downloads should be in based 64 encoded format
- If using an external CA server directly, please make you are using the customized pxGrid template for ISE 1.3-1SE 2.1 (if not using ISE internal CA)
- For pxGrid client certificate configuration settings in the pxGrid clients, if this is ISE 2.1 (internal ISE CA), or ISE 2.2+, this should be set to the ISE root CA certificate, otherwise should be the external root CA.
- For bulk download settings or MNT configuration settings in the pxGrid clients, if this is ISE 2.1 (internal CA), or ISE 2.2+, this should be set to the external CA root certificate.

Bulk Download or REST failures

- For bulk download settings or MNT configuration settings in the pxGrid clients, if this is ISE 2.1 (internal CA), or ISE 2.2+, this should be set to the external CA root certificate.

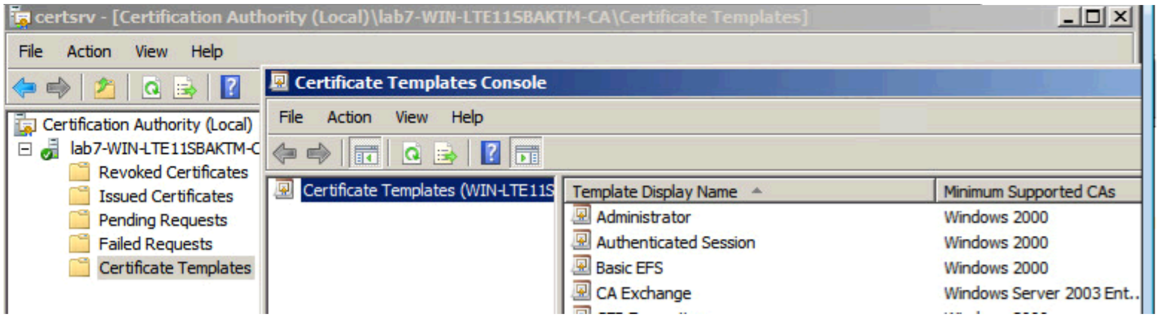
References

Using an External Certificate Authority (CA) Server

Using an external CA server to generate pxGrid certificate, a customized template with an EKU of both client and server authentication must be configured. In this example, Microsoft 2008 Enterprise CA R2 Server was used.

Customized pxGrid Template

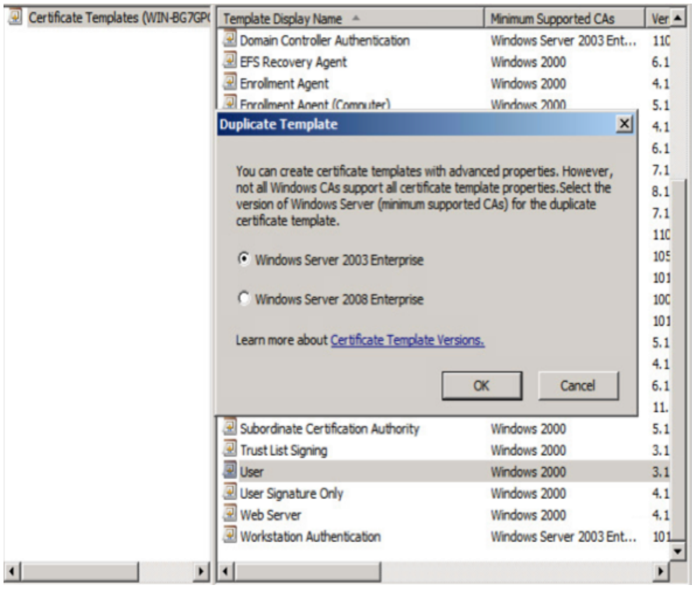
Step 1 Select **Administrative Tools->Certificate Authority-> "+" dropdown next to CA server->Right-Click on Certificate Templates->Manage**



certsrv - [Certification Authority (Local)\lab7-WIN-LTE11SBAKTM-CA\Certificate Templates]

Template Display Name	Minimum Supported CAs
Administrator	Windows 2000
Authenticated Session	Windows 2000
Basic EFS	Windows 2000
CA Exchange	Windows Server 2003 Ent..

Step 2 **Right-Click** and **Duplicate User template->Select Windows 2003 Enterprise->OK**



Template Display Name	Minimum Supported CAs	Ver
Domain Controller Authentication	Windows Server 2003 Ent...	110
EFS Recovery Agent	Windows 2000	6.1
Enrollment Agent	Windows 2000	4.1
Enrollment Agent (Computer)	Windows 2000	5.1
Subordinate Certification Authority	Windows 2000	5.1
Trust List Signing	Windows 2000	3.1
User	Windows 2000	3.1
User Signature Only	Windows 2000	4.1
Web Server	Windows 2000	4.1
Workstation Authentication	Windows Server 2003 Ent...	101

Duplicate Template

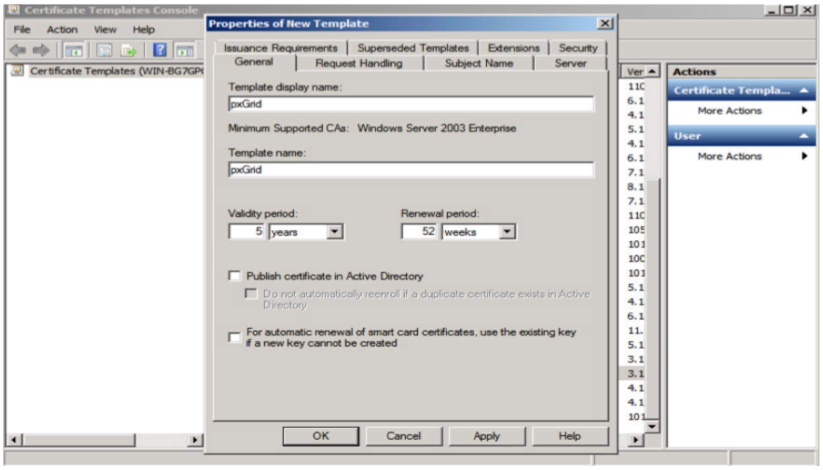
You can create certificate templates with advanced properties. However, not all Windows CAs support all certificate template properties.Select the version of Windows Server (minimum supported CAs) for the duplicate certificate template.

● Windows Server 2003 Enterprise

○ Windows Server 2008 Enterprise

Learn more about Certificate Template Versions.

Step 3 Enter name of certificate template, uncheck "Publish certificate in Active Directory", and provide validity period and renewal period.



Properties of New Template

Template display name: pxGrid

Minimum Supported CAs: Windows Server 2003 Enterprise

Template name: pxGrid

Validity period: 5 years

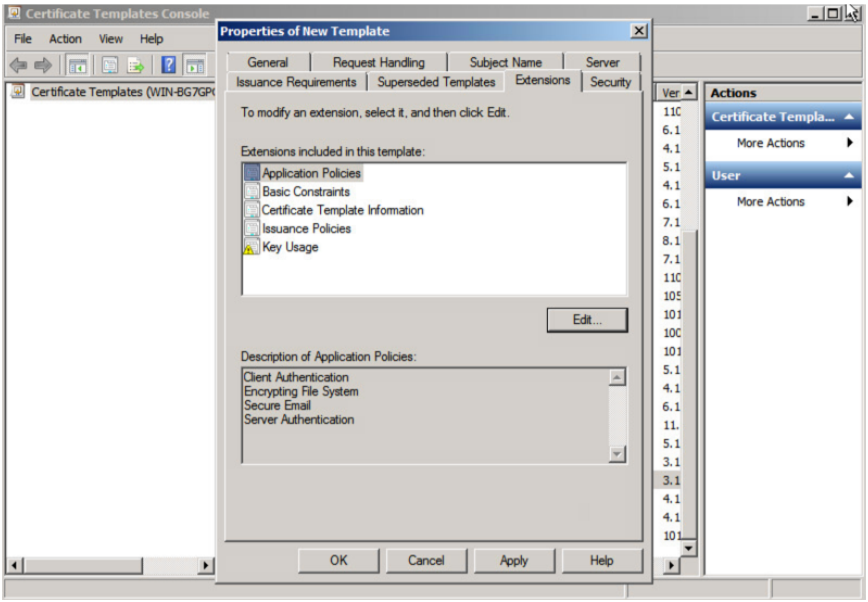
Renewal period: 52 weeks

□ Publish certificate in Active Directory

□ Do not automatically reenroll if a duplicate certificate exists in Active Directory

□ For automatic renewal of smart card certificates, use the existing key if a new key cannot be created

Step 4 Click **Extensions->Add->Server Authentication->Ok->Apply**



Properties of New Template

To modify an extension, select it, and then click Edit.

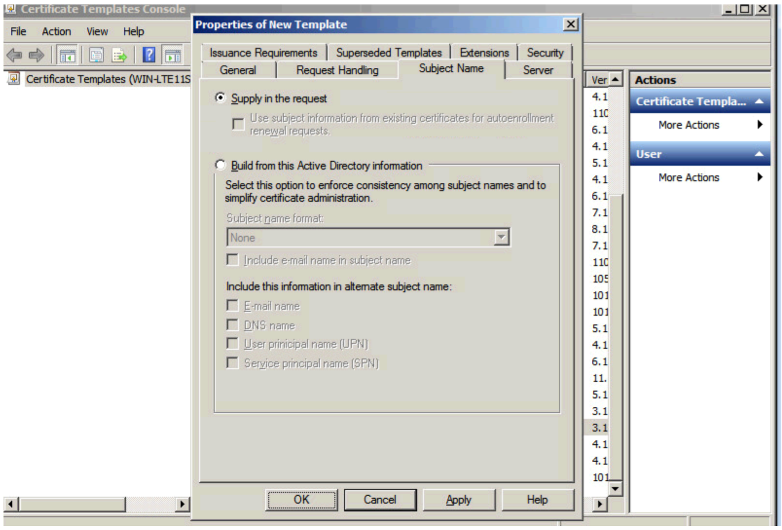
Extensions included in this template:

- Application Policies
- Basic Constraints
- Certificate Template Information
- Issuance Policies
- Key Usage

Description of Application Policies:

Client Authentication
Encrypting File System
Secure Email
Server Authentication

Step 5 Click Subject Name, Enable Supply in the request



Properties of New Template

Issuance Requirements | Superseded Templates | Extensions | Security
General | Request Handling | Subject Name | Server

● Supply in the request

□ Use subject information from existing certificates for autoenrollment renewal requests.

○ Build from this Active Directory information

Select this option to enforce consistency among subject names and to simplify certificate administration.

Subject name format:

None

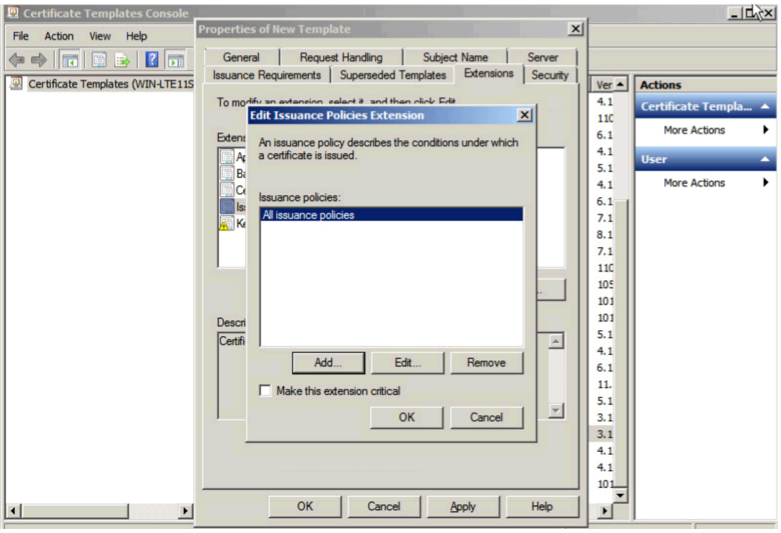
□ Include e-mail name in subject name

Include this information in alternate subject name:

□ E-mail name
□ DNS name
□ User prinicipal name (UPN)
□ Service principal name (SPN)

OK | Cancel | Apply | Help

Step 6 Click **Extensions->Issuance Policies->Edit->All Issuance Policies**



Properties of New Template

General | Request Handling | Subject Name | Server
Issuance Requirements | Superseded Templates | Extensions | Security

Edit Issuance Policies Extension

An issuance policy describes the conditions under which a certificate is issued.

Issuance policies:

All issuance policies

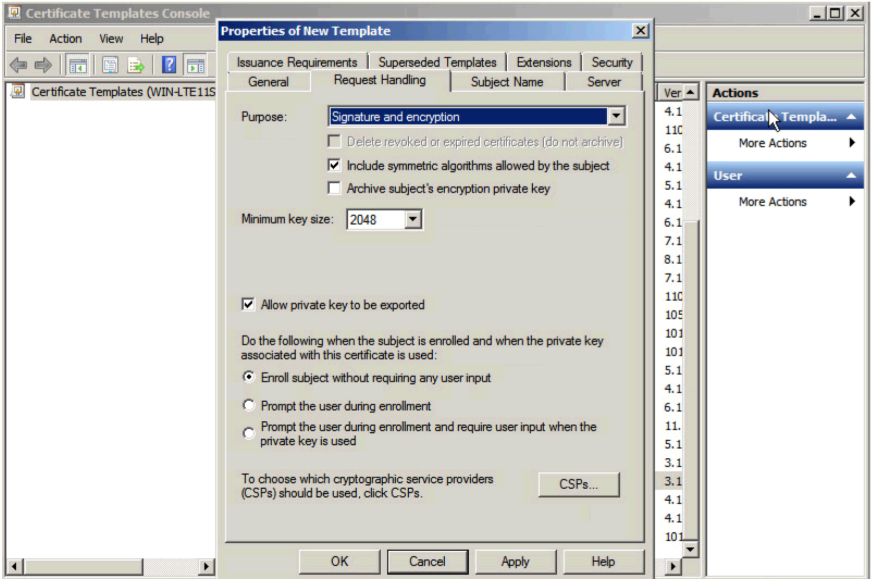
Add... | Edit... | Remove

□ Make this extension critical

OK | Cancel

OK | Cancel | Apply | Help

Step 7 Leave the defaults for request handling



Properties of New Template

Tabs: Issuance Requirements | Superseded Templates | Extensions | Security | General | Request Handling | Subject Name | Server

Purpose: Signature and encryption

☐ Delete revoked or expired certificates (do not archive)

☑ Include symmetric algorithms allowed by the subject

☐ Archive subject's encryption private key

Minimum key size: 2048

☑ Allow private key to be exported

Do the following when the subject is enrolled and when the private key associated with this certificate is used:

● Enroll subject without requiring any user input

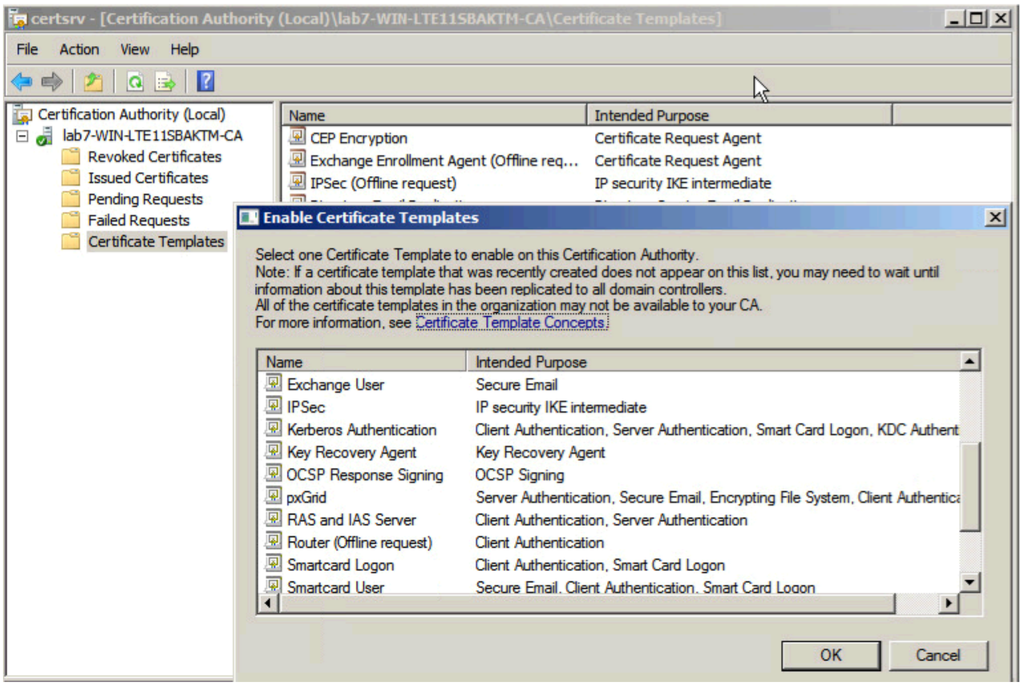
○ Prompt the user during enrollment

○ Prompt the user during enrollment and require user input when the private key is used

To choose which cryptographic service providers (CSPs) should be used, click CSPs. [CSPs...]

[OK] [Cancel] [Apply] [Help]

Step 9 Select New Template to issue and select pxGrid



certsrv - [Certification Authority (Local)\lab7-WIN-LTE11SBAKTM-CA\Certificate Templates]

Name	Intended Purpose
CEP Encryption	Certificate Request Agent
Exchange Enrollment Agent (Offline req...	Certificate Request Agent
IPSec (Offline request)	IP security IKE intermediate

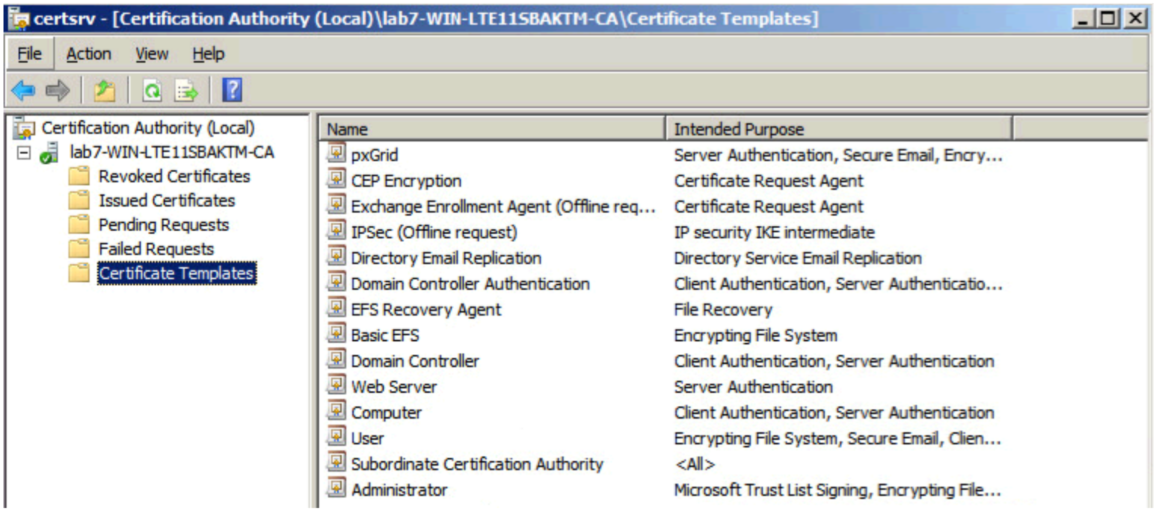
Enable Certificate Templates

Select one Certificate Template to enable on this Certification Authority.
Note: If a certificate template that was recently created does not appear on this list, you may need to wait until information about this template has been replicated to all domain controllers.
All of the certificate templates in the organization may not be available to your CA.
For more information, see Certificate Template Concepts.

Name	Intended Purpose
Exchange User	Secure Email
IPSec	IP security IKE intermediate
Kerberos Authentication	Client Authentication, Server Authentication, Smart Card Logon, KDC Authent
Key Recovery Agent	Key Recovery Agent
OCSP Response Signing	OCSP Signing
pxGrid	Server Authentication, Secure Email, Encrypting File System, Client Authentica
RAS and IAS Server	Client Authentication, Server Authentication
Router (Offline request)	Client Authentication
Smartcard Logon	Client Authentication, Smart Card Logon
Smartcard User	Secure Email, Client Authentication, Smart Card Logon

[OK] [Cancel]

Step 10 You should see the pxGrid template



certsrv - [Certification Authority (Local)\lab7-WIN-LTE11SBAKTM-CA\Certificate Templates]

Certification Authority (Local)
- lab7-WIN-LTE11SBAKTM-CA
  - Revoked Certificates
  - Issued Certificates
  - Pending Requests
  - Failed Requests
  - Certificate Templates

Name	Intended Purpose
pxGrid	Server Authentication, Secure Email, Encry...
CEP Encryption	Certificate Request Agent
Exchange Enrollment Agent (Offline req...	Certificate Request Agent
IPSec (Offline request)	IP security IKE intermediate
Directory Email Replication	Directory Service Email Replication
Domain Controller Authentication	Client Authentication, Server Authenticatio...
EFS Recovery Agent	File Recovery
Basic EFS	Encrypting File System
Domain Controller	Client Authentication, Server Authentication
Web Server	Server Authentication
Computer	Client Authentication, Server Authentication
User	Encrypting File System, Secure Email, Clien...
Subordinate Certification Authority	<All>
Administrator	Microsoft Trust List Signing, Encrypting File...

References

https://communities.cisco.com/docs/DOC-71927 Using ISE 2.1 Internal Certificate Authority (CA) to Deploy Certificates to Cisco pxGrid clients *(not using external CA Server)*

https://communities.cisco.com/docs/DOC-71928 Using ISE 2.2 Internal Certificate Authority (CA) to Deploy Certificates to Cisco pxGrid clients *(not using external CA Server)*

https://communities.cisco.com/docs/DOC-71926 Deploying Certificates with Cisco pxGrid- Using an external Certificate Authority (CA) with updates to Cisco ISE 2.0/2.1/2.2

https://communities.cisco.com/docs/DOC-71925 Deploying Certificates with pxGrid- Using Self-Signed Certificates Updates to Cisco ISE 2.0/2.1/2.2

https://communities.cisco.com/docs/DOC-68285 Using an External CA Server for ISE 1.3/1.4 Deployments

https://communities.cisco.com/docs/DOC-68286 Using Self Signed certificates for ISE 1.3/1.4 Deployments