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

Author: John Eppich

Table of Contents

About this Document

This document is for Cisco Engineers and customers deploying Cisco Stealthwatch 6.9 with Cisco Identity Service Engine (ISE 2.2 using Cisco platform Exchange Grid (pxGrid). The reader should have some similarity with ISE and Cisco Stealthwatch and pxGrid.

Cisco Stealthwatch 6.9 no longer requires syslog information for obtaining contextual information, instead pxGrid is used. The Cisco Stealthwatch Management Console will register as a pxGrid client and subscribe the ISE pxGrid node Session Directory topic to obtain the contextual information.

ISE 2.2 features an internal Certificate Authority (CA) for deploying pxGrid certificates. These pxGrid client certificates can be generated from ISE in either PEM or PKCS12 formats and imported into the Stealthwatch SSL Client store and ISE internal CA root certificate imported into the Stealthwatch CA store. Additionally, certificates can be generated based on the Certificate Signing Requests (CSR). These scenarios will be covered in this document.

This document starts using the preferred method of using the ISE 2.2 Internal CA for deploying pxGrid and Stealthwatch 6.9 using PKCS12 certificate format and then covers an external CA server deployment.

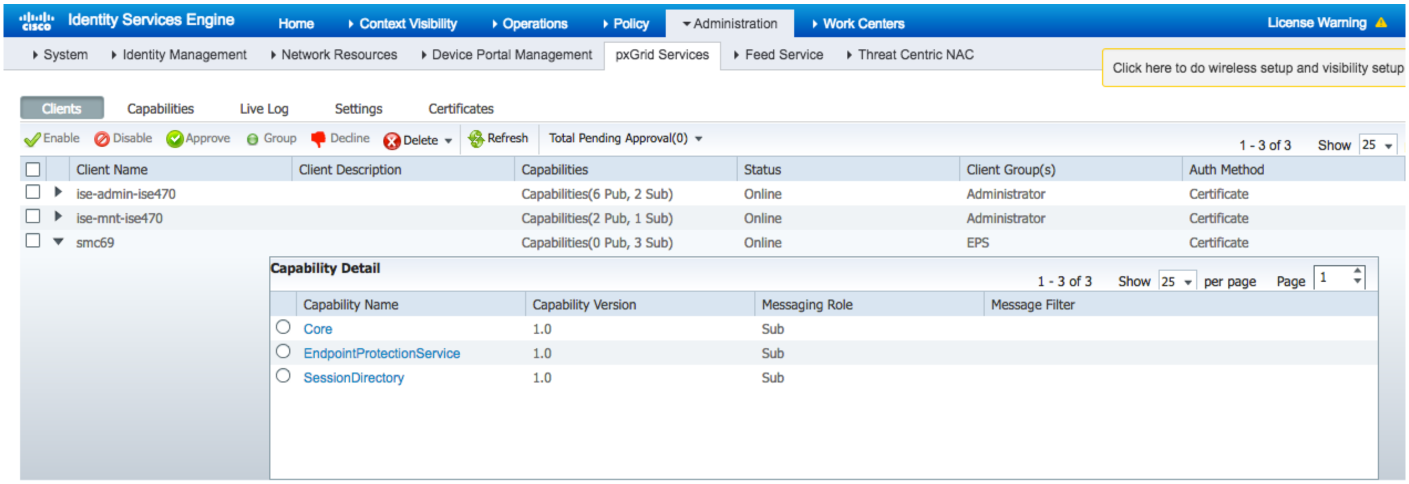
Self-signed certificate deployments and other ISE 2.2 internal CA configurations are covered under the Other Configurations Section.

Technical Details

Cisco Stealthwatch 6.9 uses Cisco platform exchange Grid (pxGrid) for obtaining user session information for populating tables, and for taking Adaptive Network Control (ANC) mitigation actions on the endpoint such as quarantine and quarantining the endpoint.

Stealthwatch Management Console (SMC) will successfully connect and register with the ISE pxGrid node and subscribe to the ISE pxGrid node Session Directory Topic to obtain the: macaddress, ipAddress, lastActiveTime, username, securityGroup, vlan, domainName, interfaceDeviceip, interfaceDevicePortId. These attributes are mapped to the: MacAddress, Endpoint IP Address, Start Active Time, UserName, Security Group ID, vlan, AD Domain Name, NAS IPC Address, NAS Port ID in Stealthwatch.

SMC will also subscribe the ISE pxGrid node EndpointProtectionService Topic to perform legacy EPS functions such as quarantining and unquarantining by the IPAddress.



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

Capability Detail

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

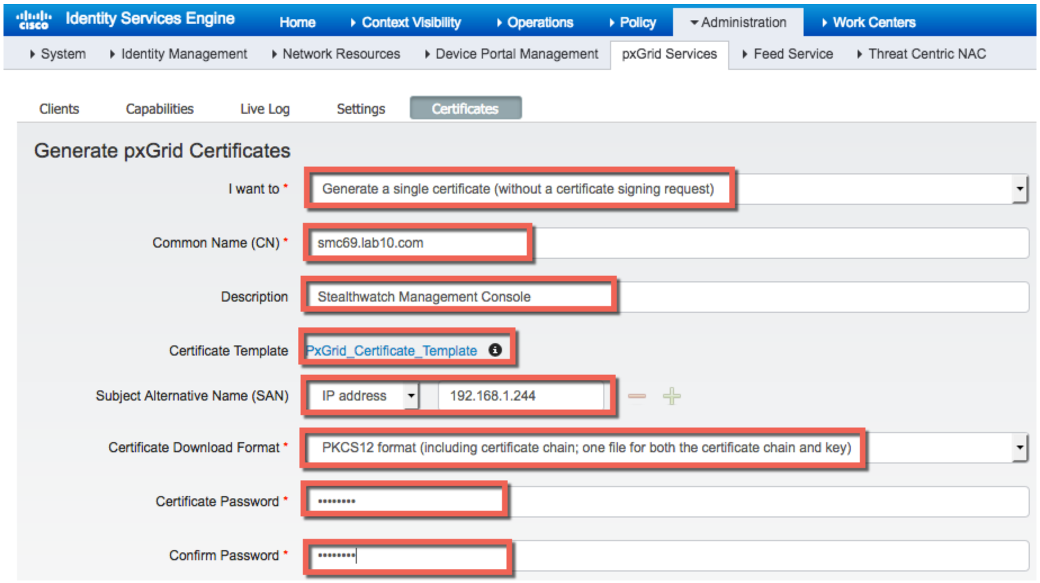
Using ISE 2.2 Internal CA Authority (Preferred Method)

Generating Certificate Signing Request (CSR) using PKCS12 format

Creating Stealthwatch certificate

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

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



Generate pxGrid Certificates

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

Common Name (CN) * smc69.lab10.com

Description Stealthwatch Management Console

Certificate Template PxGrid_Certificate_Template

Subject Alternative Name (SAN) IP address 192.168.1.244

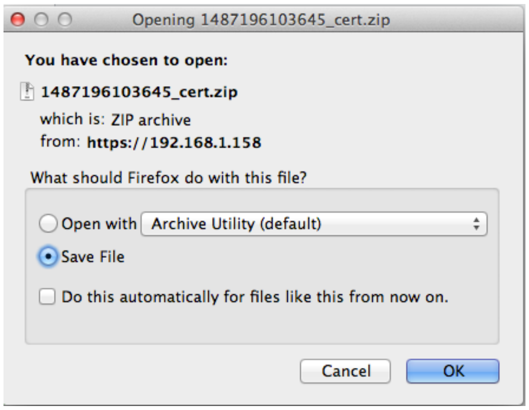
Certificate Download Format * PKCS12 format (including certificate chain; one file for both the certificate chain and key)

Certificate Password * ••••••••

Confirm Password * ••••••••

Step 2 Select **Create**

Step 3 Save the zipped file locally



Opening 1487196103645_cert.zip

You have chosen to open:

1487196103645_cert.zip

which is: ZIP archive

from: https://192.168.1.158

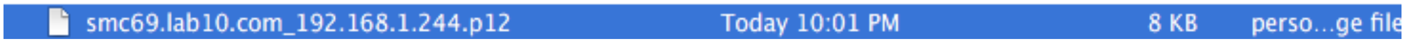
What should Firefox do with this file?

○ Open with Archive Utility (default)

● Save File

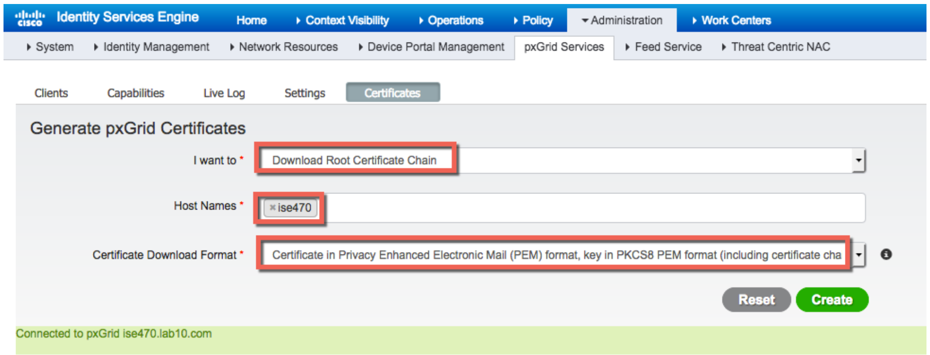
□ Do this automatically for files like this from now on.

Step 4 You should see the following



smc69.lab10.com_192.168.1.244.p12 Today 10:01 PM 8 KB perso...ge file

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



Generate pxGrid Certificates

I want to * Download Root Certificate Chain

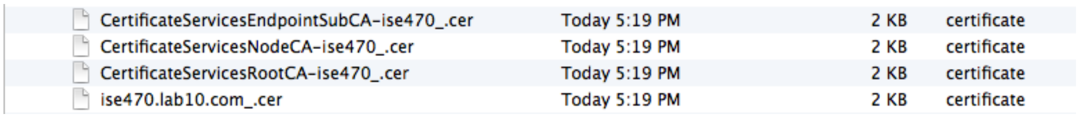
Host Names * ×ise470

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

Connected to pxGrid ise470.lab10.com

Step 6 Select **Create**

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

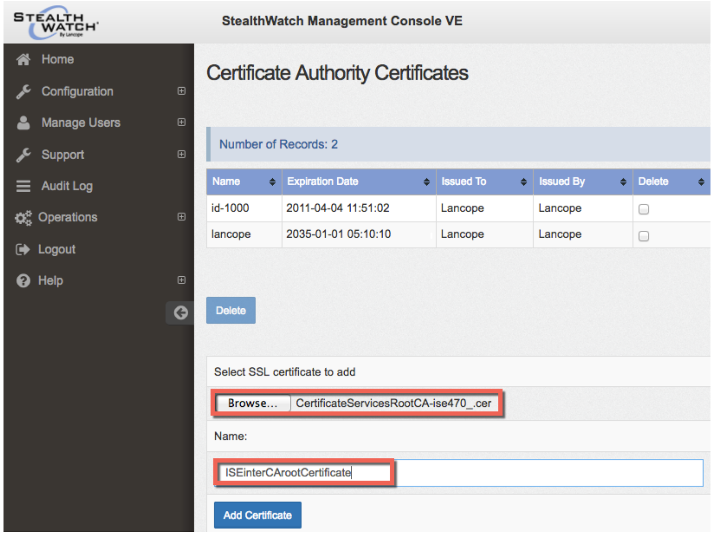


CertificateServicesEndpointSubCA-ise470_.cer	Today 5:19 PM	2 KB	certificate
CertificateServicesNodeCA-ise470_.cer	Today 5:19 PM	2 KB	certificate
CertificateServicesRootCA-ise470_.cer	Today 5:19 PM	2 KB	certificate
ise470.lab10.com_.cer	Today 5:19 PM	2 KB	certificate

Importing ISE CertificateServicesRootCA into Stealthwatch CA store

Step 1 Upload the CertificatesServicesRootCA certificate to the Stealthwatch CA Authority

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



Certificate Authority Certificates

Number of Records: 2

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

Select SSL certificate to add

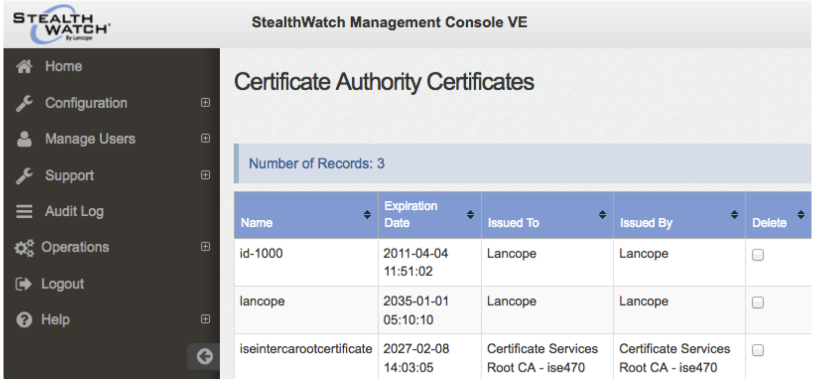
Browse... CertificateServicesRootCA-ise470_.cer

Name:

ISEinterCArootCertificate

Step 2 Select **Add Certificate** and confirm

Step 3 You should see the following:



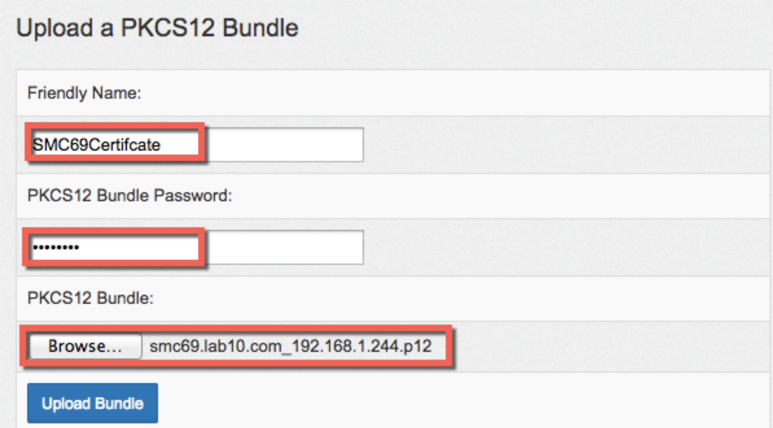
Certificate Authority Certificates

Number of Records: 3

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

Uploading Stealthwatch PKCS12 file

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



Upload a PKCS12 Bundle

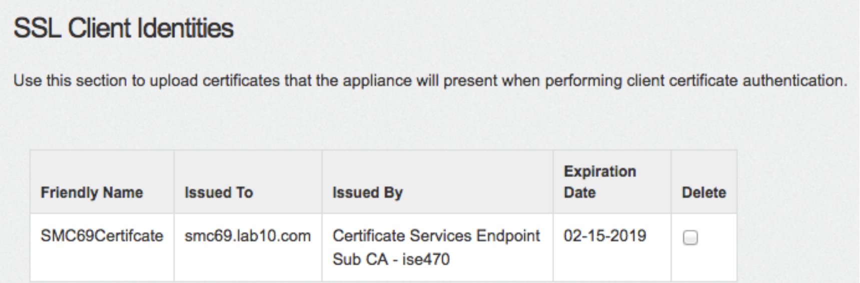
Friendly Name: SMC69Certifcate

PKCS12 Bundle Password: ••••••••

PKCS12 Bundle: Browse... smc69.lab10.com_192.168.1.244.p12

Step 2 Select **Upload Bundle** and confirm

Step 3 You should see the following under SSL Client Identities



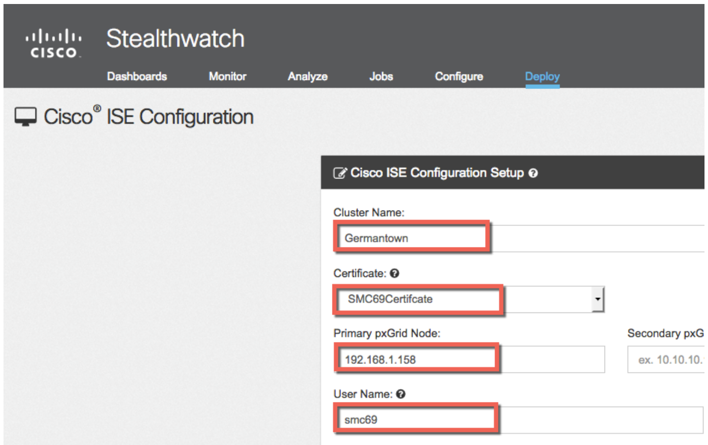
SSL Client Identities

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

Friendly Name	Issued To	Issued By	Expiration Date	Delete
SMC69Certifcate	smc69.lab10.com	Certificate Services Endpoint Sub CA - ise470	02-15-2019	□

Configuring Stealthwatch pxGrid Operation

Step 1 From the Stealthwatch Management Center Dashboard, select **Deploy->Cisco ISE Configuration**



Cluster Name: Germantown

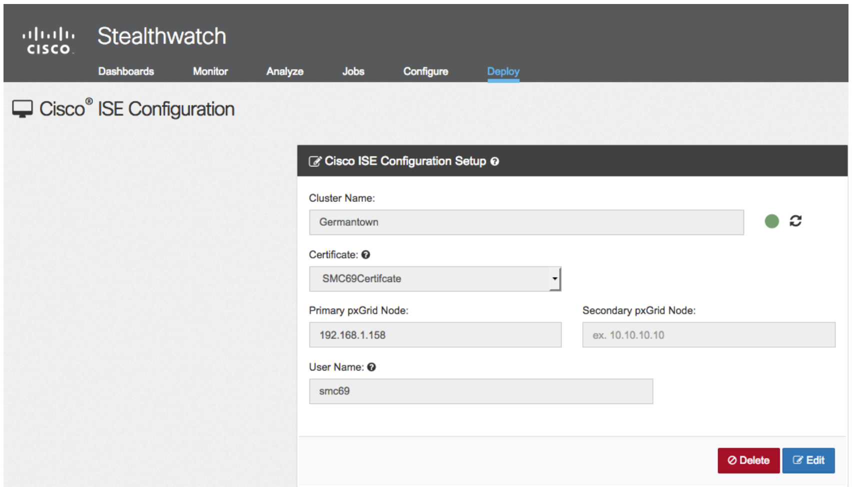
Certificate: SMC69Certifcate

Primary pxGrid Node: 192.168.1.158

Secondary pxG: ex. 10.10.10.

User Name: smc69

Step 2 Select **Save** and **OK,** you should see a successful connection



Cluster Name: Germantown

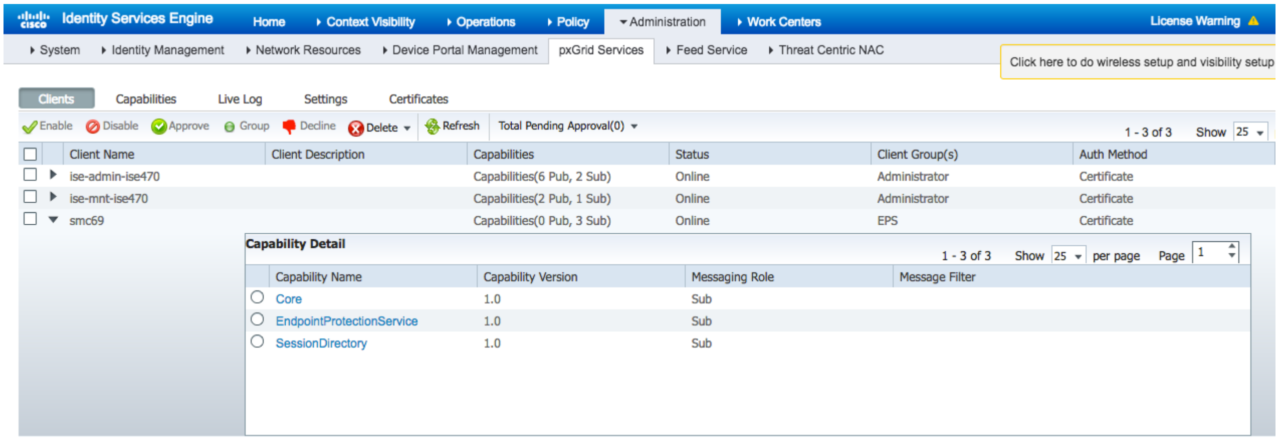
Certificate: SMC69Certifcate

Primary pxGrid Node: 192.168.1.158

Secondary pxGrid Node: ex. 10.10.10.10

User Name: smc69

Step 3 On ISE, select **Administration->pxGrid Services**



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

Capability Detail

1 - 3 of 3 Show 25 per page Page 1

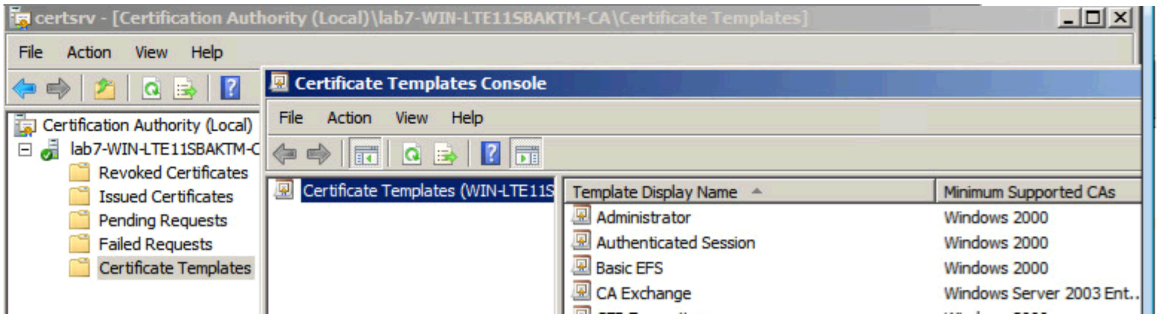
Capability Name	Capability Version	Messaging Role	Message Filter
Core	1.0	Sub	
EndpointProtectionService	1.0	Sub	
SessionDirectory	1.0	Sub	

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 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]

File Action View Help

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

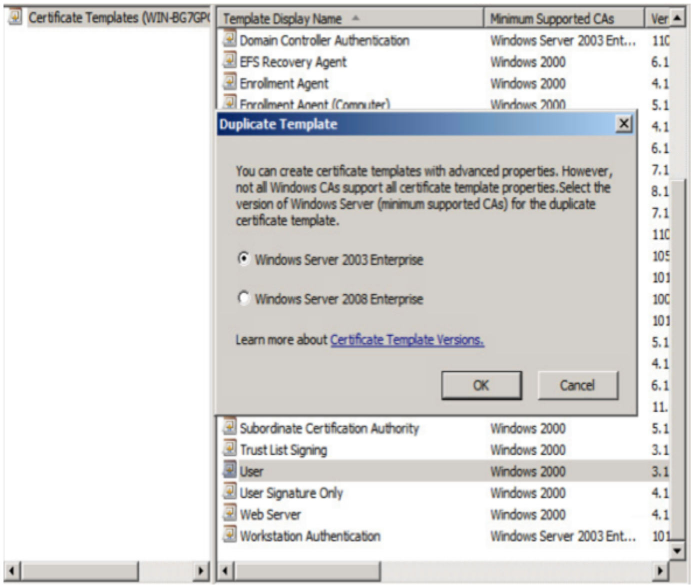
Certificate Templates Console

File Action View Help

Certificate Templates (WIN-LTE11S

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**



Certificate Templates (WIN-BG7GP(

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

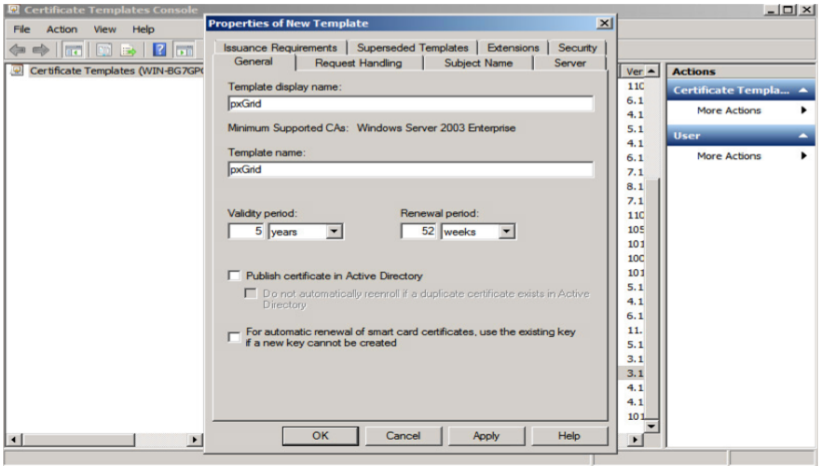
You can create certificate templates with advanced properties. However, not all Windows CAs support all certificate template properties.Select the version of Windows Server (minimum supported CAs) for the duplicate certificate template.

● 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.


Certificate Templates Console
File Action View Help
Certificate Templates (WIN-BG7GP
Properties of New Template
Issuance Requirements | Superseded Templates | Extensions | Security
General | Request Handling | Subject Name | Server
Actions
Certificate Templa...
More Actions
User
More Actions
OK Cancel Apply Help

Template display name:
pxGrid

Minimum Supported CAs: Windows Server 2003 Enterprise

Template name:
pxGrid

Validity period: 5 years

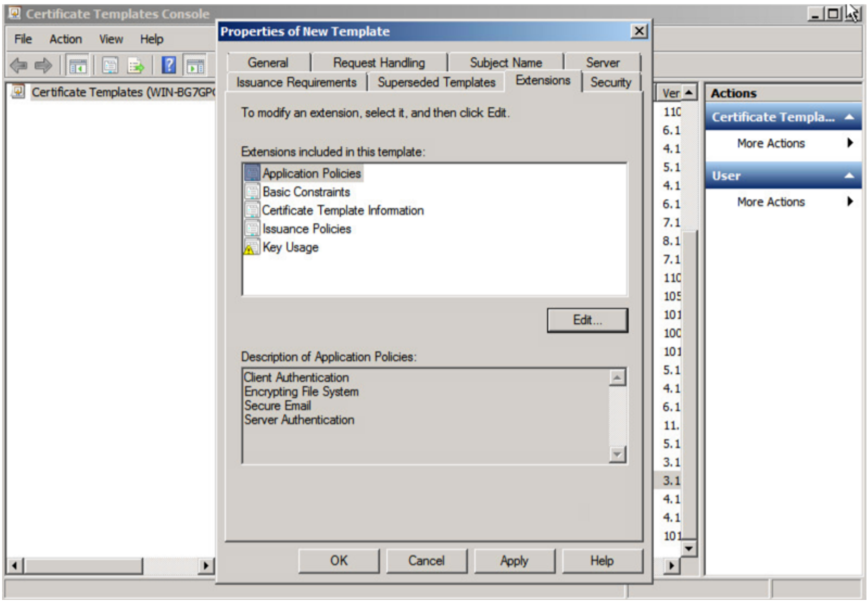
Renewal period: 52 weeks

□ 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**


Certificate Templates Console
File Action View Help
Certificate Templates (WIN-BG7GP
Properties of New Template
General | Request Handling | Subject Name | Server
Issuance Requirements | Superseded Templates | Extensions | Security
Actions
Certificate Templa...
More Actions
User
More Actions
Edit...
OK Cancel Apply Help

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

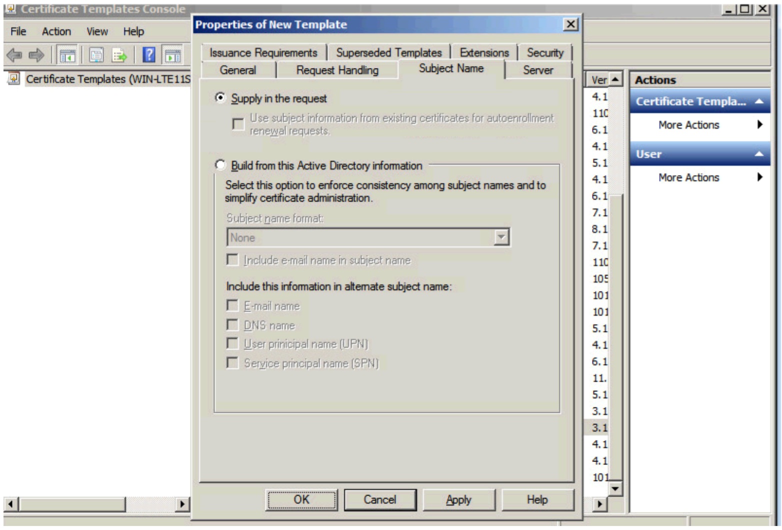
Extensions included in this template:

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


Certificate Templates Console
File Action View Help
Certificate Templates (WIN-LTE11S
Properties of New Template
Issuance Requirements | Superseded Templates | Extensions | Security
General | Request Handling | Subject Name | Server
Ver
Actions
Certificate Templa...
More Actions
User
More Actions
OK Cancel Apply Help

● 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:

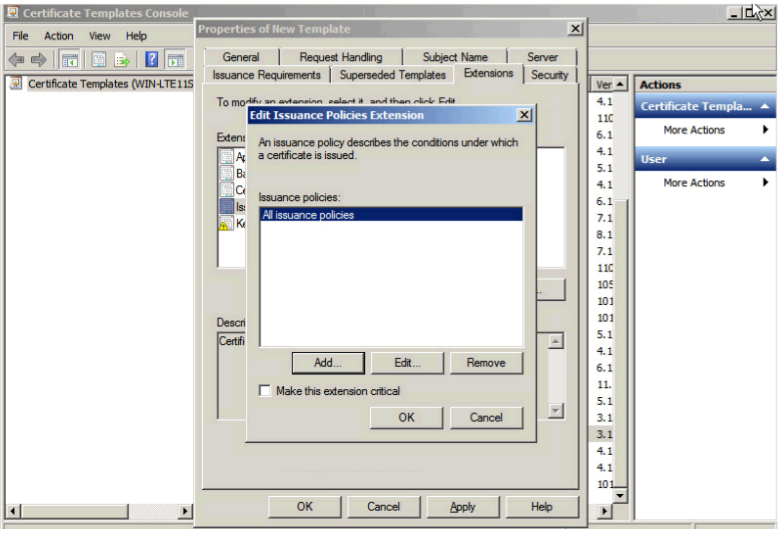
☐ E-mail name

☐ DNS name

☐ User prinicipal name (UPN)

☐ Service principal name (SPN)

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


Certificate Templates Console
File Action View Help
Certificate Templates (WIN-LTE11S
Properties of New Template
General | Request Handling | Subject Name | Server
Issuance Requirements | Superseded Templates | Extensions | Security
To modify an extension, select it, and then click Edit
Extens
Descri
Certifi
Edit Issuance Policies Extension
Add... Edit... Remove
OK Cancel
OK Cancel Apply Help
Ver
Actions
Certificate Templa...
More Actions
User
More Actions

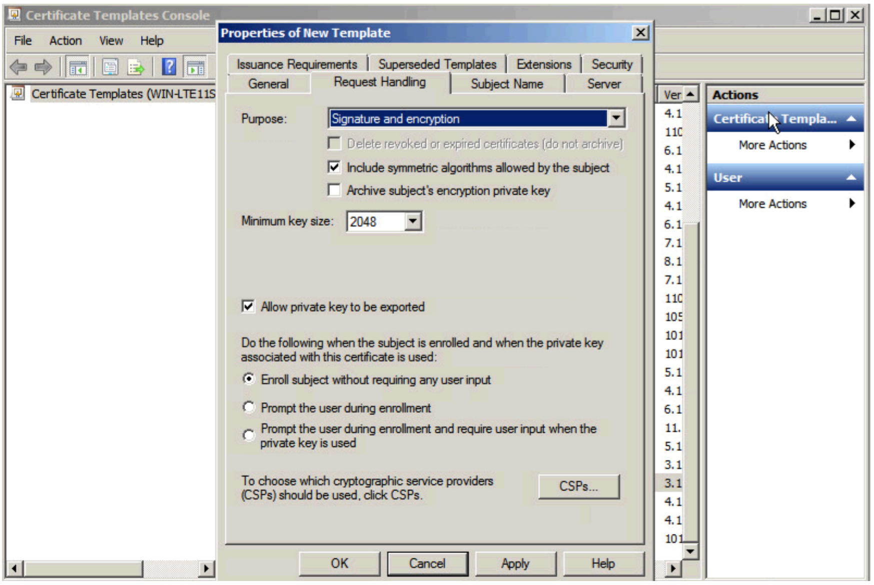
An issuance policy describes the conditions under which a certificate is issued.

Issuance policies:

All issuance policies

☐ Make this extension critical

Step 7 Leave the defaults for request handling



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

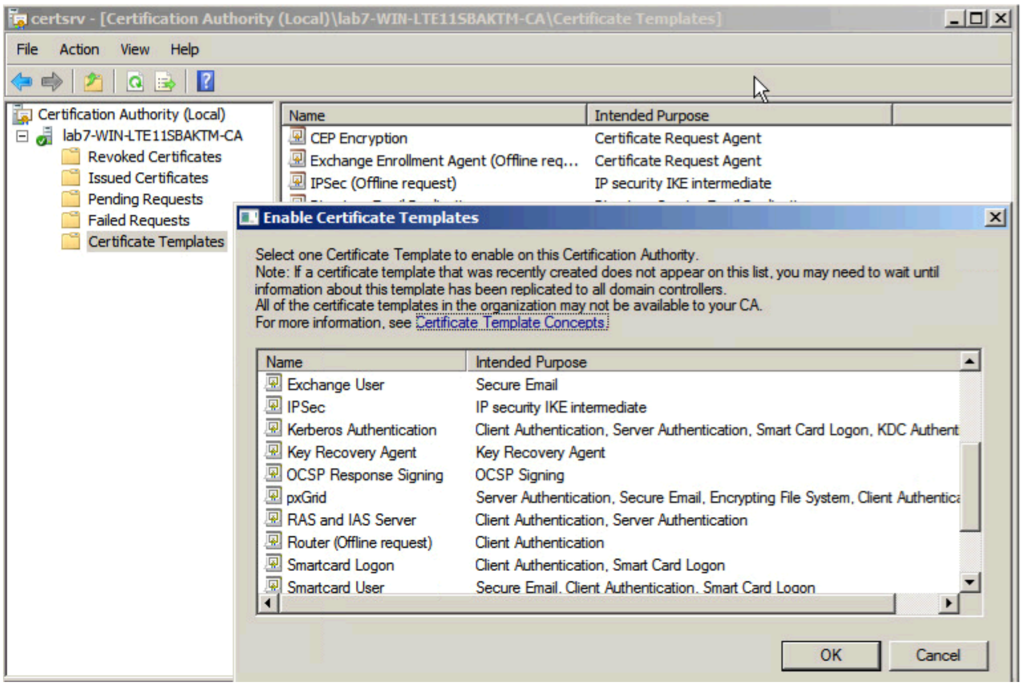
○ Prompt the user during enrollment

○ 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.

Step 8 Right-click on Certificate Templates

Step 9 Select New Template to issue and select pxGrid

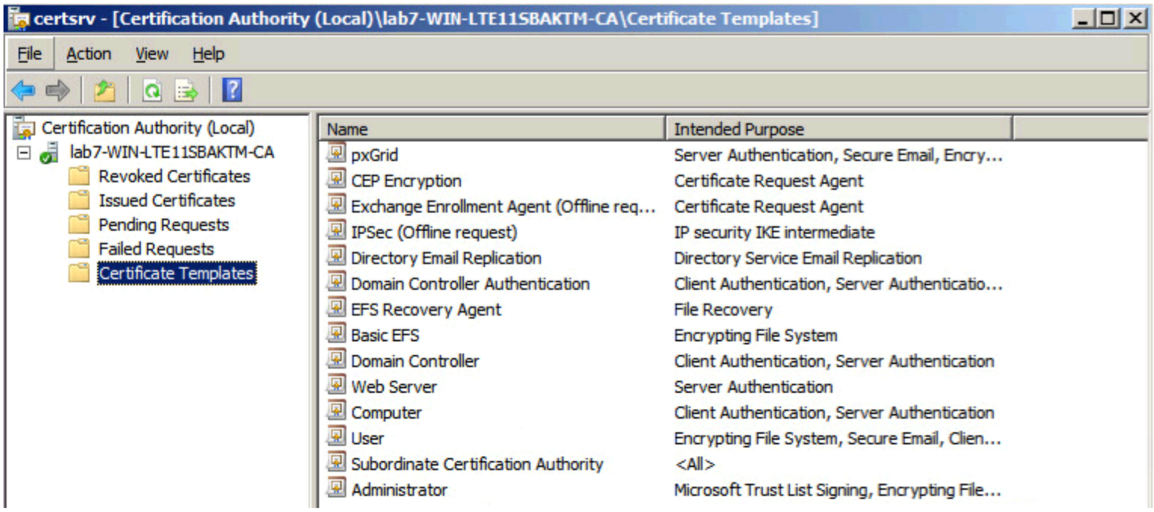

certsrv - [Certification Authority (Local)\lab7-WIN-LTE11SBAKTM-CA\Certificate Templates]
File Action View Help
Certification Authority (Local)
lab7-WIN-LTE11SBAKTM-CA
Revoked Certificates
Issued Certificates
Pending Requests
Failed Requests
Certificate Templates
Enable Certificate Templates
OK
Cancel

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

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

Step 10 You should see the pxGrid template



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

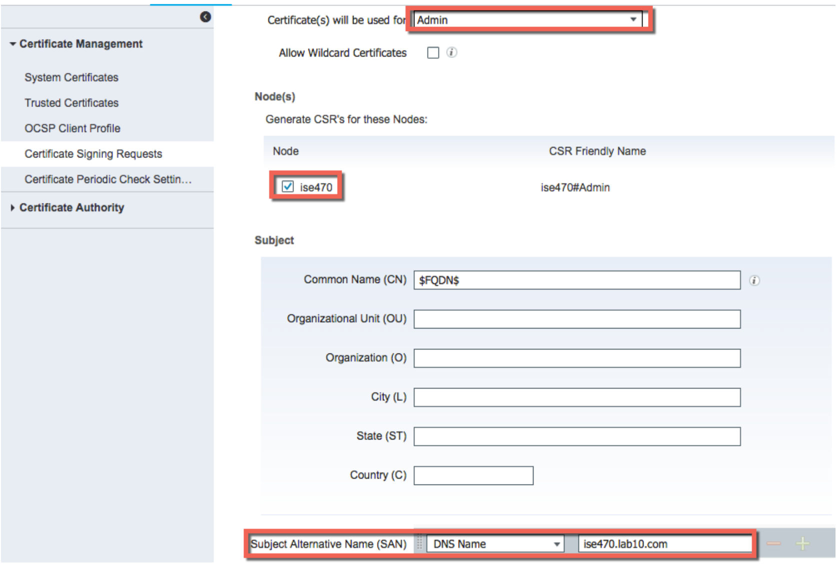
- Certification Authority (Local)
  - lab7-WIN-LTE11SBAKTM-CA
    - Revoked Certificates
    - Issued Certificates
    - Pending Requests
    - Failed Requests
    - Certificate Templates

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...

Configuring ISE 2.2 ISE pxGrid node

Generating Certificate Signing Request (CSR)

Step 1 Select **Administration->System->Certificates->Certificate Management->Certificate Signing Requests->Generate Certificate Signing Request (CSR)**



Certificate(s) will be used for: Admin

Allow Wildcard Certificates □

Node(s)

Generate CSR's for these Nodes:

Node	CSR Friendly Name
☑ ise470	ise470#Admin

Subject

Common Name (CN): $FQDN$

Organizational Unit (OU):

Organization (O):

City (L):

State (ST):

Country (C):

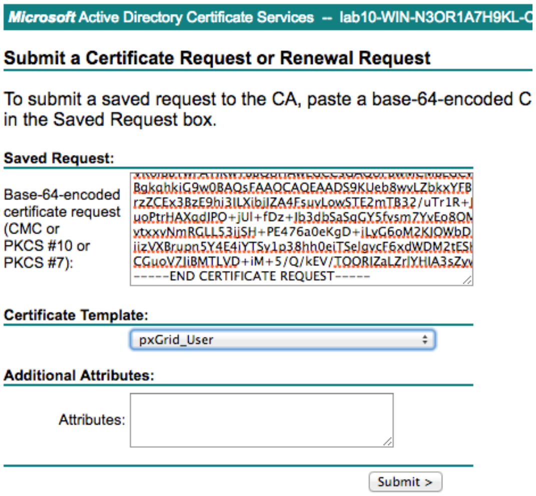
Subject Alternative Name (SAN): DNS Name ise470.lab10.com

Step 2 Select **Generate**

Step 3 Select Export and open the PEM file copy

```
-----BEGIN CERTIFICATE REQUEST-----
MIIC7jCCAdYCAQAwGzEZMBcGA1UEAxMQaXNlNDcwLmxhYjEwLmNvbTCCASIwDQYJ
KoZIhvcNAQEBBQADggEPADCCAQoCggEBAJSM1PM6t1crlvZxEe584Y/dnrrEdE7j
qKiS0RWLXmbEDHXl5F0rIhcn7rAR0e9h8V1oeA4v9+Sj1I0slsfTETUoWbWpqgyo
J5DEj5YxS2vH+cAhKj5Xp4ls7ziqBaUyw9OnaRTjUp40gyOY3O2/8NCWWXvt4r0w
gFYuIbi8emMRuNPn+448f3Rx3mHs2cdARosjtUC/OmAfysl7uPDCahjGqapy/l0E
TuW0MAjdvUaibimDl+WmsWnFvmiSVuoFh5/JYGh3pXdw5MK9tt5hltP0dZMkbANJ
1jwyYmOeVz9Zal51nuWpJJ5bZJjZE88/dA8pQJFOXE/jqTmfZzwhztsCAwEAAaCB
jTCBigYJKoZIhvcNAQkOMX0wezAbBgNVHREEFDASghBpc2U0NzAubGFiMTAuY29t
MAsGA1UdDwQEAwIF4DAdBgNVHQ4EFgQU2jmj7l5rSw0yVb/vlWAYkK/YBwkwHQYD
VR0lBBYwFAYIKwYBBQUHAwEGCCsGAQUFBwMCMBEGCWCGSAGG+EIBAQQEAwIGQDAN
BgkqhkiG9w0BAQsFAAOCAQEAADS9KUeb8wvLZbkxYFB/ecsfGM2kIGhPDtn9/0de
rzZCEx3BzE9hi3ILXibjIZA4FsuvLowSTE2mTB32/uTr1R+JEobS0foc9oLUOTgW
uoPtrHAXqdIPO+jUl+fDz+Ib3dbSaSqGY5fvsm7YvEo8OMvlbM23mTWzHoYgjk3G
vtxxvNmRGLL53ijSH+PE476a0eKgD+iLyG6oM2KJOWbDrBEwHUPDhmiIWal1uP0Y
iizVXBrupn5Y4E4iYTSy1p38hh0eiTSelgvcF6xdWDM2tESKaK6jJRDJNS6QJTR0
CGuoV7JiBMTLVD+iM+5/Q/kEV/TOORIZaLZrlYHIA3sZyw==
-----END CERTIFICATE REQUEST-----
```

Step 4 Paste into CSR request



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

Submit a Certificate Request or Renewal Request

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

Saved Request:

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

```
BgkqhkiG9w0BAQsFAAOCAQEAADS9KUeb8wvLZbkxYFB
rzZCEx3BzE9hi3ILXibjIZA4FsuvLowSTE2mTB32/uTr1R+J
uoPtrHAXqdIPO+jUl+fDz+Ib3dbSaSqGY5fvsm7YvEo8OM
vtxxvNmRGLL53ijSH+PE476a0eKgD+iLyG6oM2KJOWbD
iizVXBrupn5Y4E4iYTSy1p38hh0eiTSelgvcF6xdWDM2tESK
CGuoV7JiBMTLVD+iM+5/Q/kEV/TOORIZaLZrlYHIA3sZyw
-----END CERTIFICATE REQUEST-----
```

Certificate Template:

pxGrid_User

Additional Attributes:

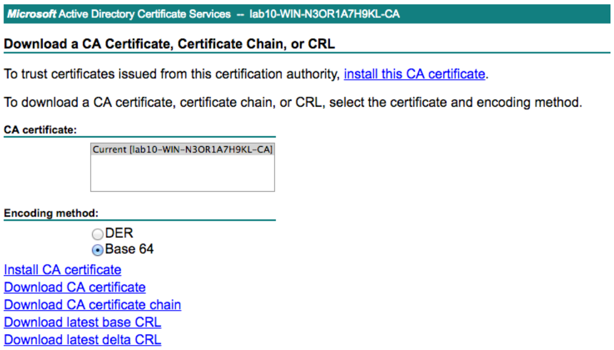
Attributes:

Step 5 Select **Submit**

Step 6 Select **Base64 encoded**

Step 7 Select **Download certificate** and save file locally. This file was renamed to ise470.cer

Step 8 Download the CA root certificate
Select **Download Certificate->Base 64->Download CA 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:

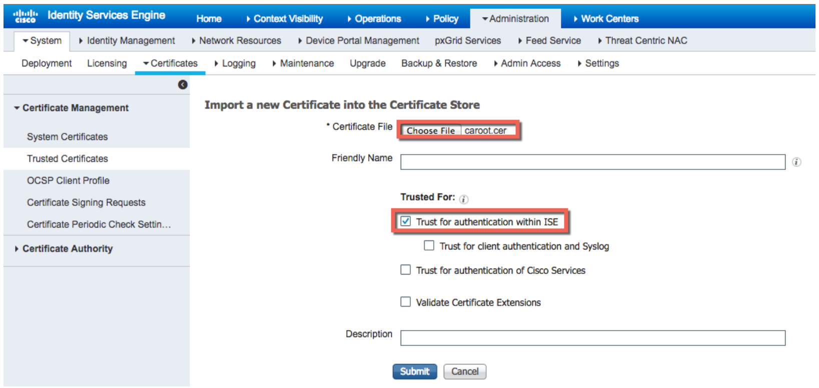
○ DER
● Base 64

Install CA certificate
Download CA certificate
Download CA certificate chain
Download latest base CRL
Download latest delta CRL

Step 9 Rename the certificate to caroot.cer

Importing CA root certificate into ISE Trusted Certificate Store

Step 1 Select **Administration->System->Certificates->Certificate Management->Trusted Certificates->Import->Certificate file and import the root certificate**



Import a new Certificate into the Certificate Store

* Certificate File: Choose File caroot.cer

Friendly Name:

Trusted For:

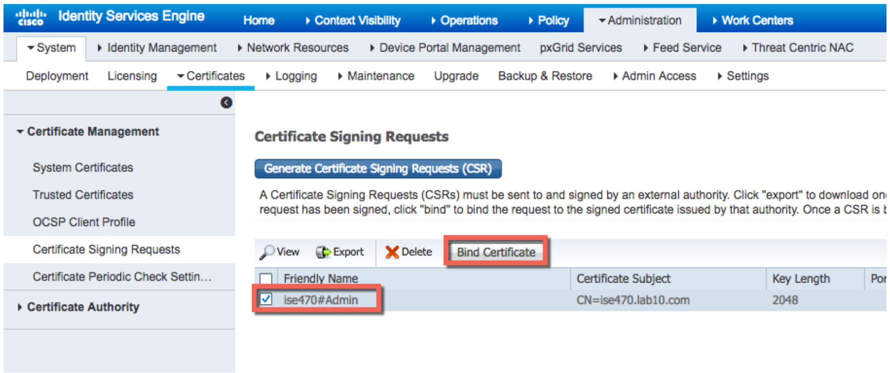
☑ Trust for authentication within ISE
☐ Trust for client authentication and Syslog
☐ Trust for authentication of Cisco Services
☐ Validate Certificate Extensions

Description:

Step 2 Select **Submit**

Bind ISE certificate to Certificate Signing Request (CSR)

Step 1 Select **Administration->System->Certificates->Certificate management->Certificate Signing Requests->select ISE node->Bind Certificate**

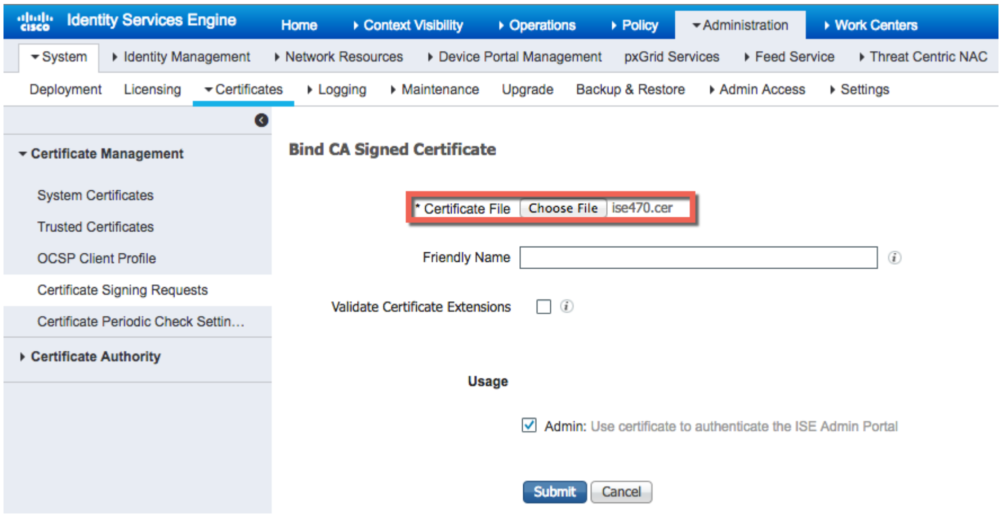


Certificate Signing Requests

A Certificate Signing Requests (CSRs) must be sent to and signed by an external authority. Click "export" to download on
request has been signed, click "bind" to bind the request to the signed certificate issued by that authority. Once a CSR is b

	Friendly Name	Certificate Subject	Key Length	Por
☑	ise470#Admin	CN=ise470.lab10.com	2048	

Step 2 Select ISE certificate file and upload the root certificate



Bind CA Signed Certificate

* Certificate File: ise470.cer

Friendly Name:

Validate Certificate Extensions ☐

Usage

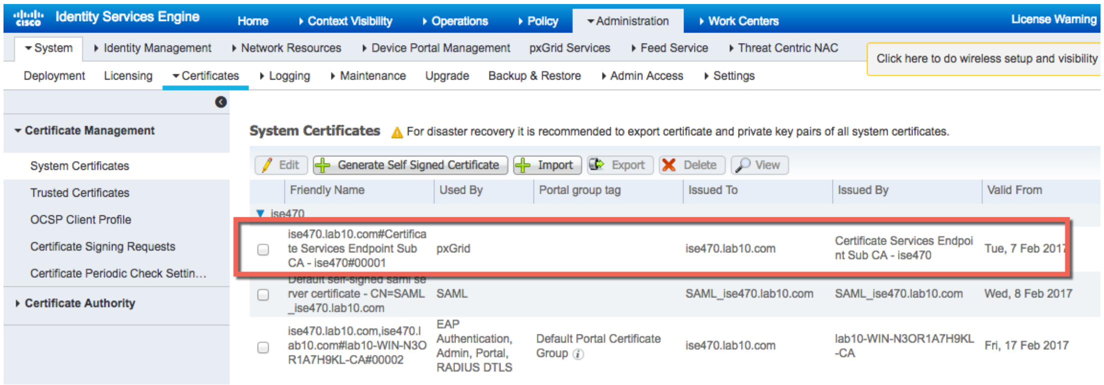
☑ Admin: Use certificate to authenticate the ISE Admin Portal

Step 3 Select **Submit**

Step 4 Select **Yes** for an application restart

Step 5 Select **Yes** to replace the existing certificate. The system will restart

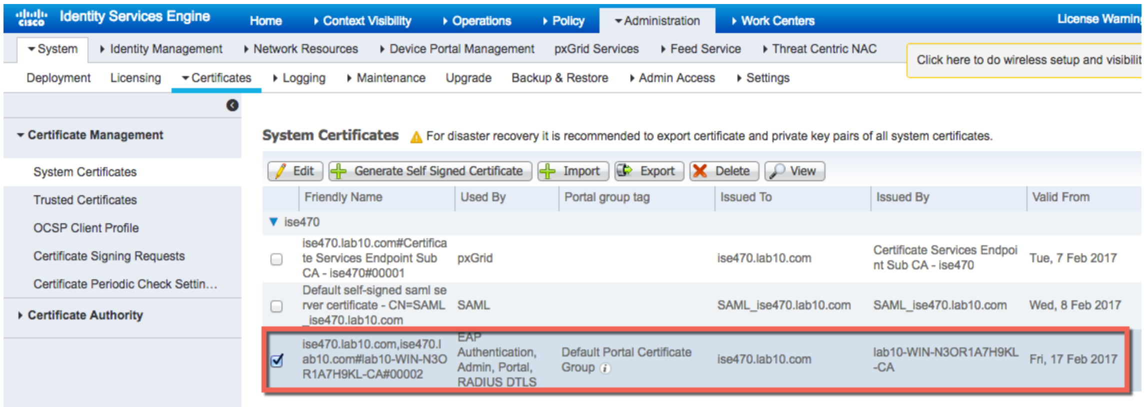
Step 6 Select **Administration->System->Certificates->System Certificates**
You should see the default pxGrid certificate signed by the internal ISE CA



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
▼ ise470						
□	ise470.lab10.com#Certificate Services Endpoint Sub CA - ise470#00001	pxGrid		ise470.lab10.com	Certificate Services Endpoint Sub CA - ise470	Tue, 7 Feb 2017
□	Default self-signed saml server certificate - CN=SAML_ise470.lab10.com	SAML		SAML_ise470.lab10.com	SAML_ise470.lab10.com	Wed, 8 Feb 2017
□	ise470.lab10.com,ise470.lab10.com#lab10-WIN-N3OR1A7H9KL-CA#00002	EAP Authentication, Admin, Portal, RADIUS DTLS	Default Portal Certificate Group ⓘ	ise470.lab10.com	lab10-WIN-N3OR1A7H9KL-CA	Fri, 17 Feb 2017

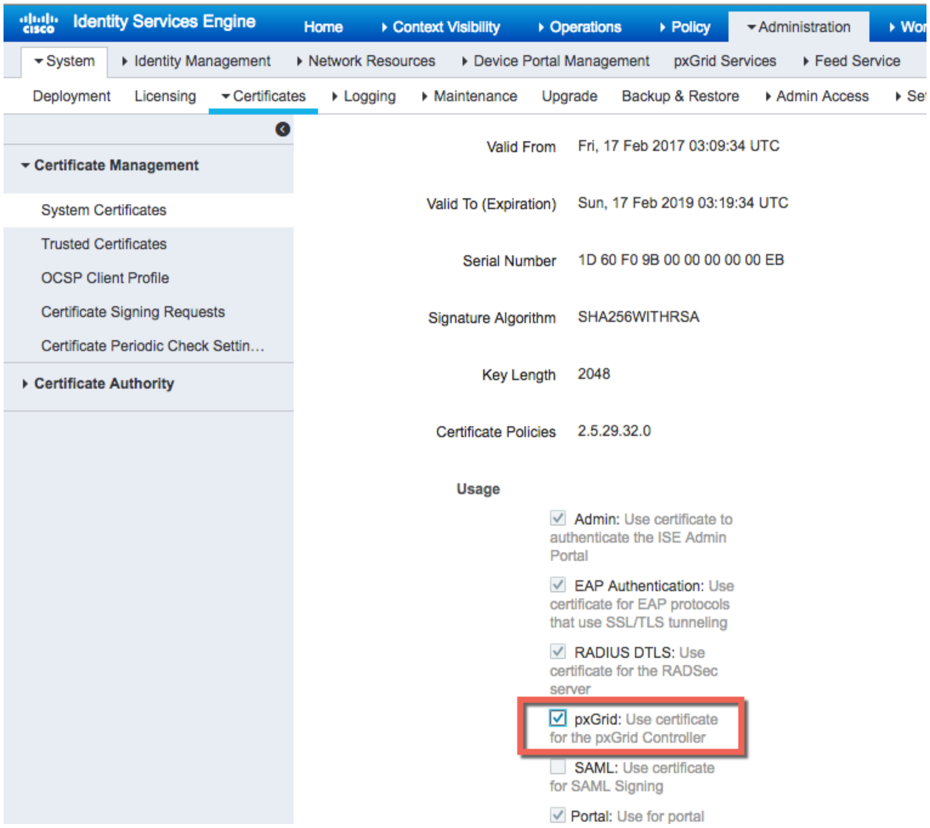
Step 7 Edit the admin certificate



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
▼ ise470						
□	ise470.lab10.com#Certificate Services Endpoint Sub CA - ise470#00001	pxGrid		ise470.lab10.com	Certificate Services Endpoint Sub CA - ise470	Tue, 7 Feb 2017
□	Default self-signed saml server certificate - CN=SAML_ise470.lab10.com	SAML		SAML_ise470.lab10.com	SAML_ise470.lab10.com	Wed, 8 Feb 2017
☑	ise470.lab10.com,ise470.lab10.com#lab10-WIN-N3OR1A7H9KL-CA#00002	EAP Authentication, Admin, Portal, RADIUS DTLS	Default Portal Certificate Group ⓘ	ise470.lab10.com	lab10-WIN-N3OR1A7H9KL-CA	Fri, 17 Feb 2017

Step 8 Select pxGrid



Valid From Fri, 17 Feb 2017 03:09:34 UTC

Valid To (Expiration) Sun, 17 Feb 2019 03:19:34 UTC

Serial Number 1D 60 F0 9B 00 00 00 00 00 EB

Signature Algorithm SHA256WITHRSA

Key Length 2048

Certificate Policies 2.5.29.32.0

Usage

☑ Admin: Use certificate to authenticate the ISE Admin Portal

☑ EAP Authentication: Use certificate for EAP protocols that use SSL/TLS tunneling

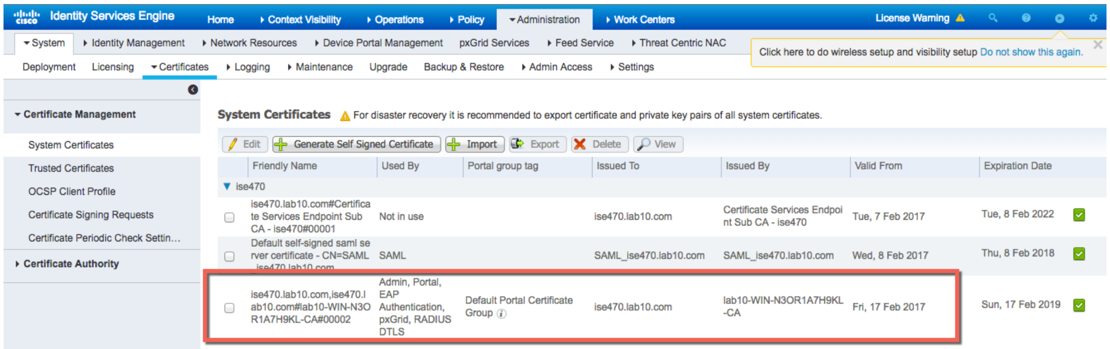
☑ RADIUS DTLS: Use certificate for the RADSec server

☑ pxGrid: Use certificate for the pxGrid Controller

☐ SAML: Use certificate for SAML Signing

☑ Portal: Use for portal

Step 9 Select **Save**
You should see the pxGrid purpose assigned to the admin certificate



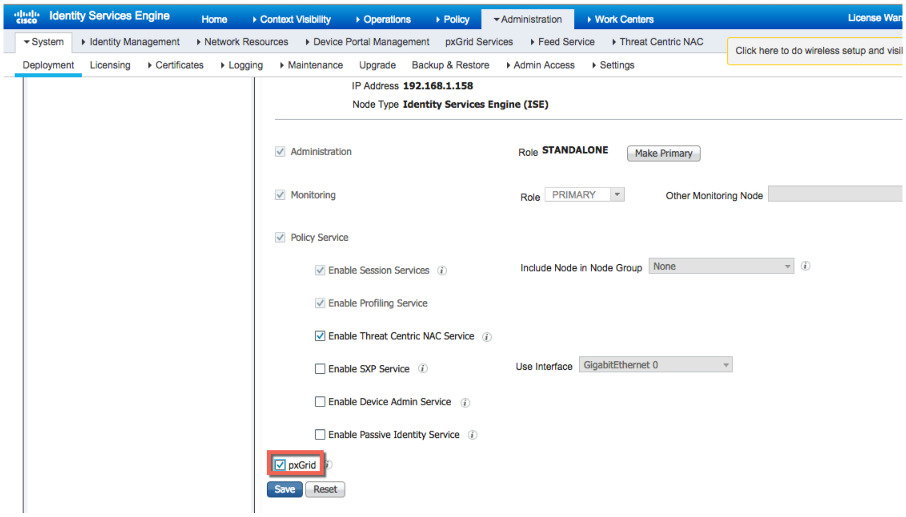
Click here to do wireless setup and visibility setup Do not show this again.

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	
▼ ise470								
☐	ise470.lab10.com#Certificate Services Endpoint Sub CA - ise470#00001	Not in use		ise470.lab10.com	Certificate Services Endpoint Sub CA - ise470	Tue, 7 Feb 2017	Tue, 8 Feb 2022	✓
☐	Default self-signed saml server certificate - CN=SAML_ise470.lab10.com	SAML		SAML_ise470.lab10.com	SAML_ise470.lab10.com	Wed, 8 Feb 2017	Thu, 8 Feb 2018	✓
☐	ise470.lab10.com,ise470.lab10.com#lab10-WIN-N3OR1A7H9KL-CA#00002	Admin, Portal, EAP Authentication, pxGrid, RADIUS DTLS	Default Portal Certificate Group ⓘ	ise470.lab10.com	lab10-WIN-N3OR1A7H9KL-CA	Fri, 17 Feb 2017	Sun, 17 Feb 2019	✓

Enabling pxGrid

Step 1 Select **Administration->System->Deployment->edit ISE node->enable pxGrid**



IP Address **192.168.1.158**
Node Type **Identity Services Engine (ISE)**

☑ Administration — Role **STANDALONE**

☑ Monitoring — Role PRIMARY — 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

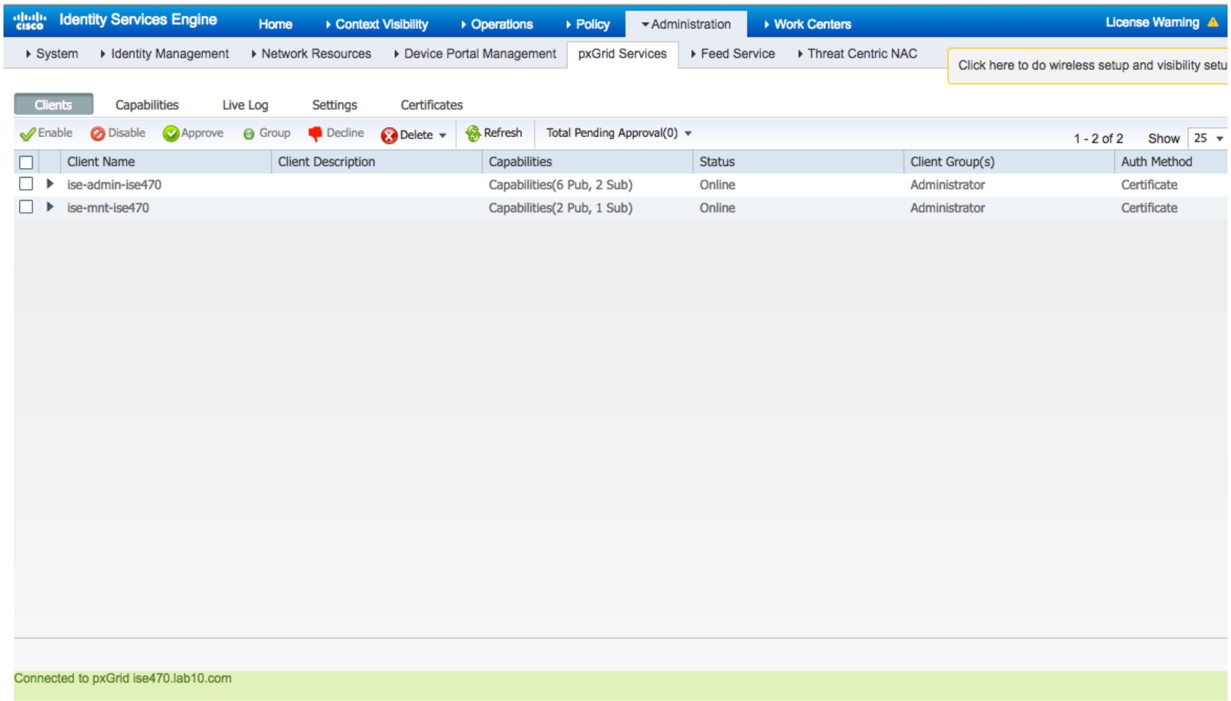
☑ pxGrid

Step 2 Select **Save**

Step 3 Run "sh application status ise" to verify the pxGrid services are running

Step 4 Select **Administration->pxGrid Services**, you should see the published nodes appear and pxGrid node connectivity

Step 5 Select **Administration->pxGrid Services->Settings->pxGrid Settings->Automatically approve new certificate-based accounts**



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

Connected to pxGrid ise470.lab10.com

Generating Stealthwatch certificate

Step 1 Generate private key from the Stealthwatch Management Center

```
openssl genrsa -out smc69.key 2048
Generating RSA private key, 2048 bit long modulus
......+++
........................................+++
e is 65537 (0x10001)
```

Step 2 Generate certificate signing request (CSR) request

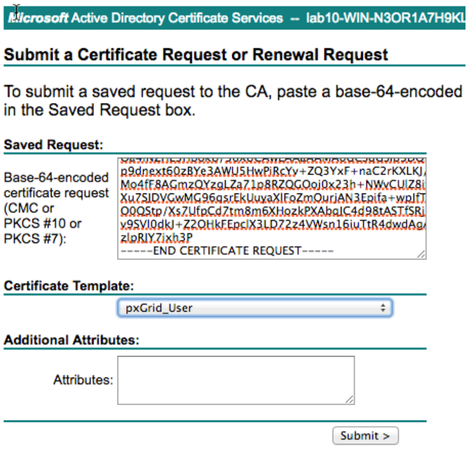
```
openssl req -new -key smc69.key -out smc69.csr
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields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

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

Step 3 Copy the CSR request

```
-----BEGIN CERTIFICATE REQUEST-----
MIIC1TCCAb0CAQAwgY8xCzAJBgNVBAYTAlVTMREwDwYDVQQIDAhNYXJ5bGFuZDET
MBEGA1UEBwwKR2VybWFudG93bjEOMAwGA1UECgwFQ2lzY28xFDASBgNVBAsMC0Vu
Z2luZWVyaW5nMRYwFAYDVQQDDA1zbWMubGFiMTAuY29tMRowGAYJKoZIhvcNAQkB
FgtqQGNpc2NvLmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAK8Q
HHiQnLJVTmKOR1W/h/LqgUJlJIMiQZMh6EeO/ZorSFnG6Ge5bB8KCNdoFgTLoORL
W//WWl+mAZ1oxBzZ+dXItC8GyxJonSkhnxx44yvgDYtwuGMBLUKLV+b/efSAm/ev
2c7MKxse6rw/yGJkoUpVKrjsKLXaJKPecogU1o25aEu2S3JrA3+dUdQUV4V8JmtY
C5qb4C4iSmg3eBcENz66ZnGarPKHghY5W5swC07z/H6pes5AW2w869hbygXKnMMv
LY1uun6AocdtMubzFLKwaCSZXsgBvBfde7qjPJUIVMKtGZKMQSERQSE5UcE87KnU
Oa4iNZHL3HbokU/36XUCAwEAAaAAMA0GCSqGSIb3DQEBCwUAA4IBAQAPrFwocuW1
p9dnext60zBYe3AWU5HwPiRcYv+ZQ3YxF+naC2rKXLKJ/TDW+Woep1/51x0YpC21
Mo4fF8AGmzQYzgLZa71p8RZQGOoj0x23h+NWvCUlZ8iwEqbtgNUGhYF9NEdNbjJR
Xu7SJDVGwMG96qsrEkUuyaXlFoZmOurjAN3Epifa+wpJfThhfs6L8rL3RRV+oXdy
O0QStp/Xs7UfpCd7tm8m6XHozkPXAbqJC4d98tASTfSRjxB5TC3PXiA8fM/EVBW+
v9SVl0dkJ+Z2OHkFEpclX3LD72z4VWsn16iuTtR4dwdAgASU4f0bK3CCX+exjlTA
zlpRJY7ixh3P
-----END CERTIFICATE REQUEST-----
```

Step 4 Paste into request



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

Submit a Certificate Request or Renewal Request

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

Saved Request:

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

```
p9dnext60zBYe3AWU5HwPiRcYy+ZQ3YxF+naC2rKXLKJ
Mo4fF8AGmzQYzgLZa71p8RZQGOoj0x23h+NWvCUlZ8i
Xu7SJDVGwMG96qsrEkUuyaXlFoZmOurjAN3Epifa+wpIfT
O0QStp/Xs7UfpCd7tm8m6XHozkPXAbqIC4d98tAST fSRj
v9SVl0dkJ+Z2OHkFEpclX3LD72z4VWsn16iuTtR4dwdAg
zlpRIY7ixh3P
-----END CERTIFICATE REQUEST-----
```

Certificate Template:

pxGrid_User

Additional Attributes:

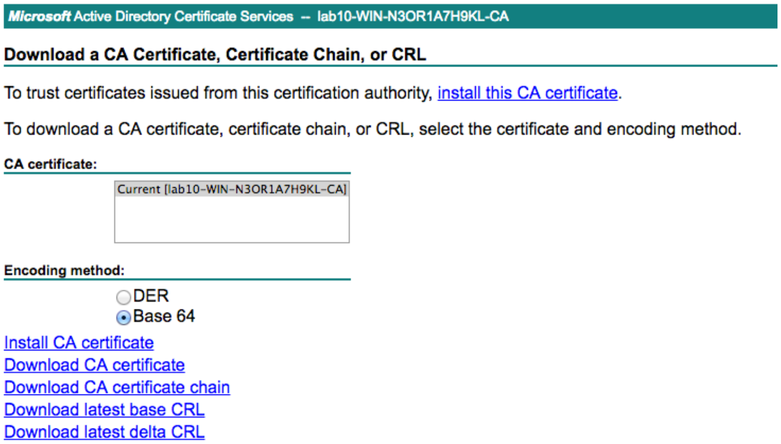
Attributes:

Step 5 Select **Submit**

Step 6 Download certificate in base 64 encoded format and rename to smc69.cer

Step 7 Download the CA root certificate

Select **Download Certificate->Base 64->Download CA 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

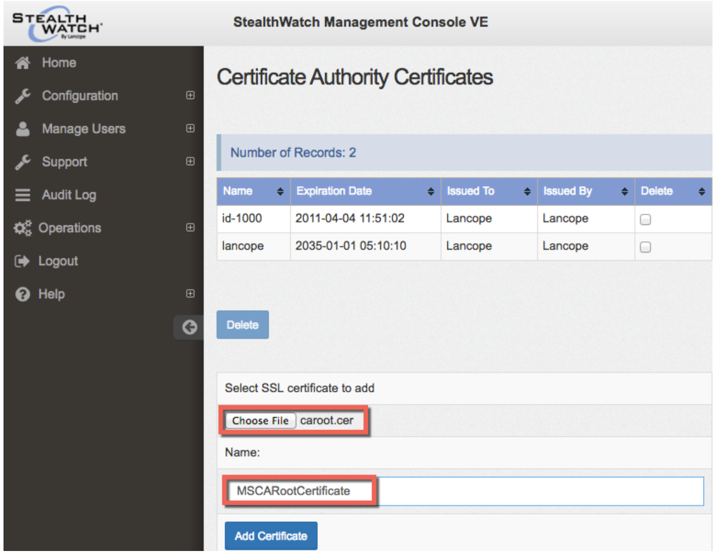
Step 8 Rename the certificate to caroot.cer

Step 9 Upload the root certificate into the Stealthwatch CA Authority Store

Importing CA root certificate into Stealthwatch Certificate Authority Store

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

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



Certificate Authority Certificates

Number of Records: 2

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

Select SSL certificate to add

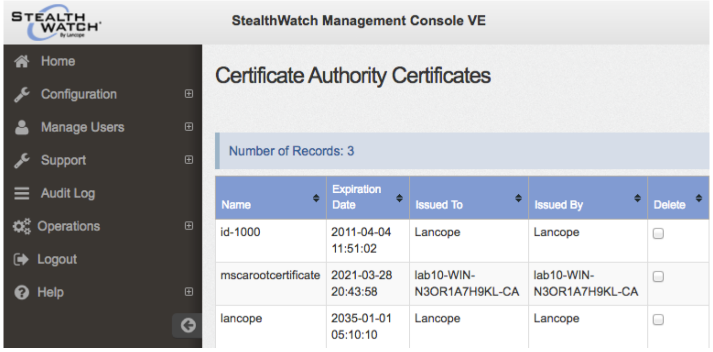
caroot.cer

Name:

MSCARootCertificate

Step 1 Select **Add Certificate** and confirm

Step 2 You should see the following



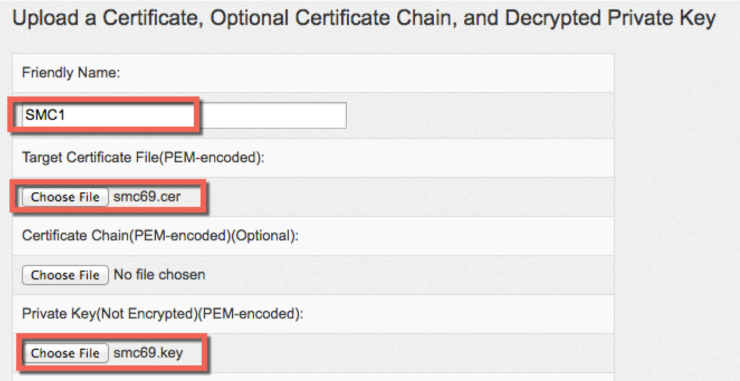
Certificate Authority Certificates

Number of Records: 3

Name	Expiration Date	Issued To	Issued By	Delete
id-1000	2011-04-04 11:51:02	Lancope	Lancope	□
mscarootcertificate	2021-03-28 20:43:58	lab10-WIN-N3OR1A7H9KL-CA	lab10-WIN-N3OR1A7H9KL-CA	□
lancope	2035-01-01 05:10:10	Lancope	Lancope	□

Importing Stealthwatch certificate into Stealthwatch SSL Client Identities Store

Step 1 Select **Configuration->SSL Certificate->SSL Client Identities->Upload Stealthwatch public private-key pair**



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

Friendly Name: SMC1

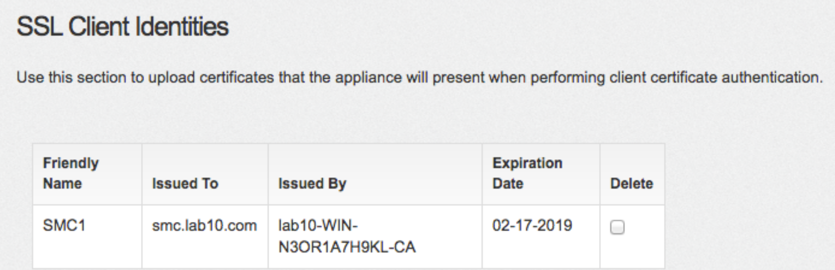
Target Certificate File(PEM-encoded): smc69.cer

Certificate Chain(PEM-encoded)(Optional): No file chosen

Private Key(Not Encrypted)(PEM-encoded): smc69.key

Step 2 Select **Upload Certificate and confirm**

Step 3 You should see the following under Client Identities



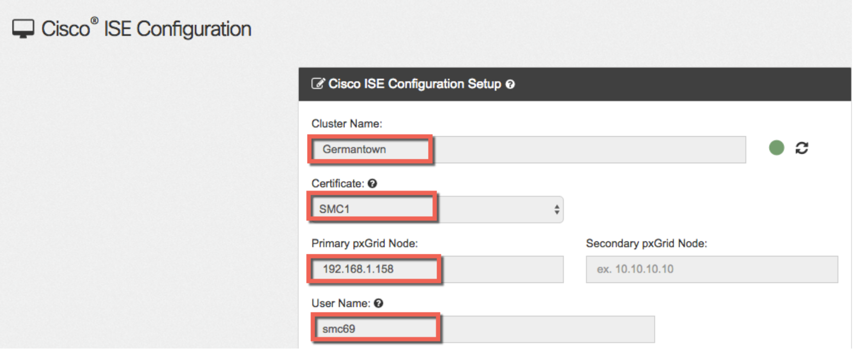
SSL Client Identities

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

Friendly Name	Issued To	Issued By	Expiration Date	Delete
SMC1	smc.lab10.com	lab10-WIN-N3OR1A7H9KL-CA	02-17-2019	□

Configuring Stealthwatch pxGrid Operation

Step 1 From the Stealthwatch Management Center Dashboard, select **Deploy->Cisco ISE Configuration**



Cisco® ISE Configuration

Cisco ISE Configuration Setup

Cluster Name: Germantown

Certificate: SMC1

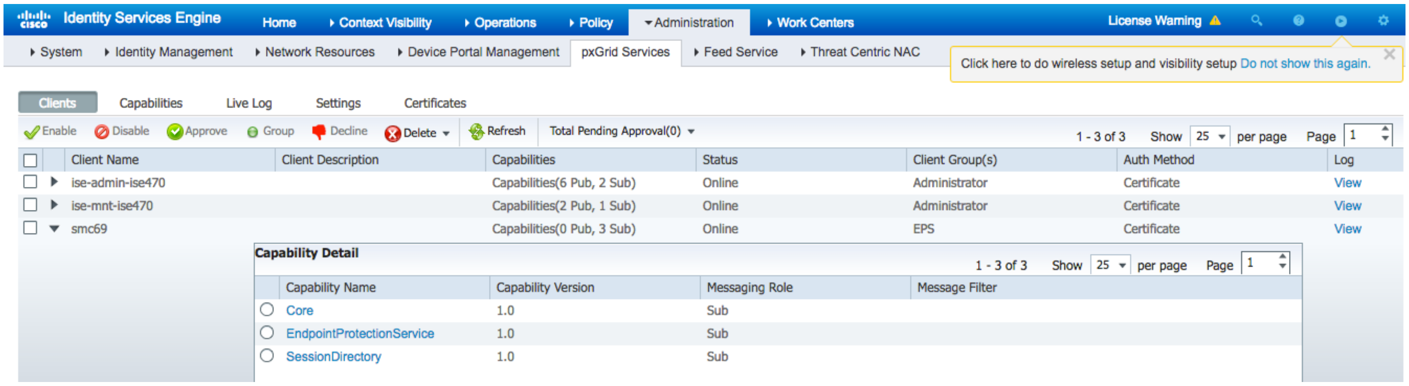
Primary pxGrid Node: 192.168.1.158

Secondary pxGrid Node: ex. 10.10.10.10

User Name: smc69

Step 2 Select **Save**

Step 3 On ISE, select **Administration->pxGrid services**, you should see SMC has successfully registered and subscribed to the pxGrid topics



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

Capability Detail

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

Other Configurations

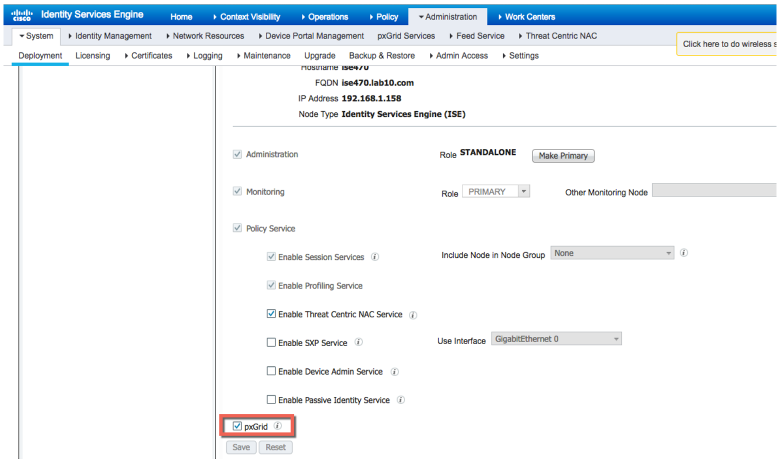
Using Self-Signed Certificates for SMC & ISE pxGrid node

Enabling ISE pxGrid node for Self-Signed Certificates

Enable pxGrid on the designated ISE node.

Note: With ISE 2.0 and above you no longer have to import the ISE identity certificate into the Trusted System Certificate Store, as you had to do with ISE 1.3 and 1.4

Step 1 Select **Administration->System->Deployment->select node->Edit->enable pxGrid**



Hostname ise470
FQDN ise470.lab10.com
IP Address 192.168.1.158
Node Type Identity Services Engine (ISE)

☑ Administration — Role STANDALONE

☑ Monitoring — Role PRIMARY — Other Monitoring Node

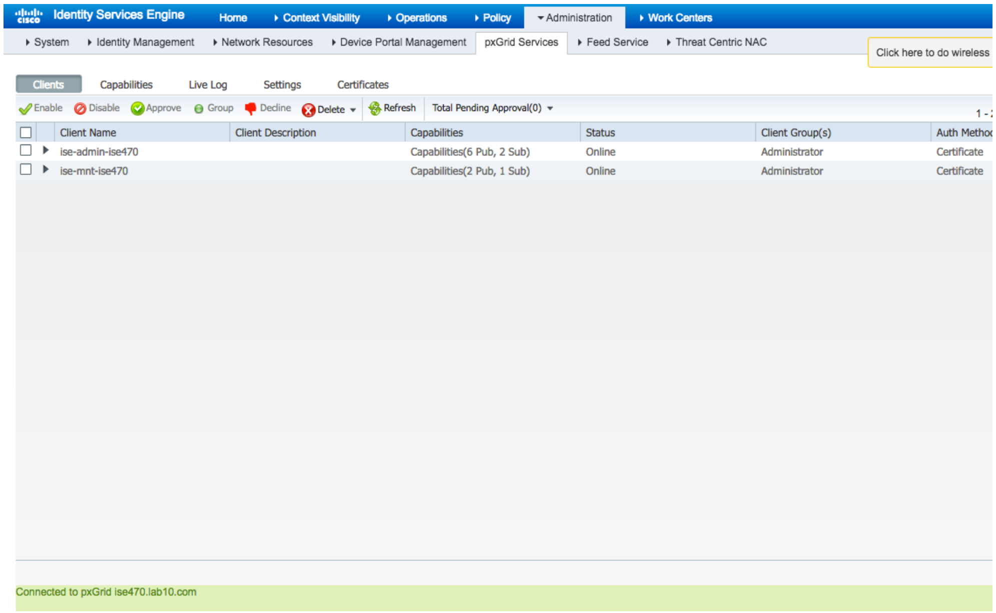
☑ Policy Service

- ☑ 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 2 Select **Save**

Step 3 Verify that the published node appear and that there is connectivity to the ISE pxGrid node Administration **pxGrid Services**

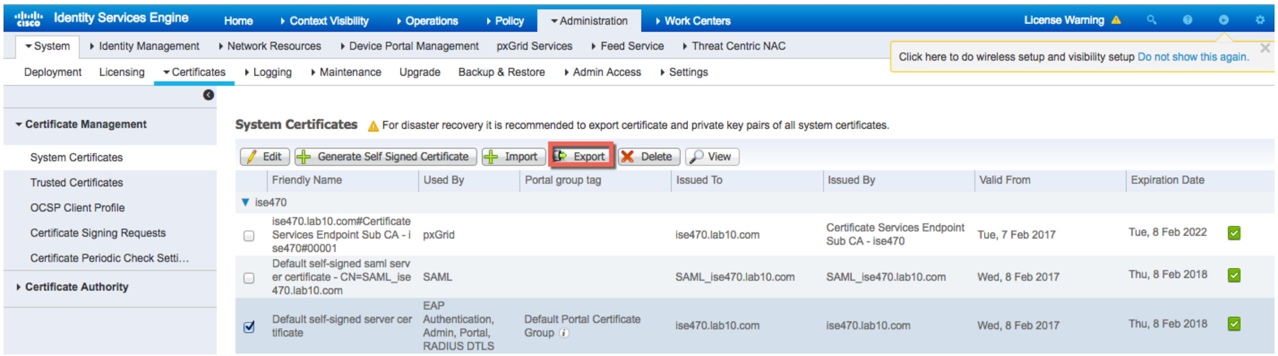


□	Client Name	Client Description	Capabilities	Status	Client Group(s)	Auth Metho
□	ise-admin-ise470		Capabilities(6 Pub, 2 Sub)	Online	Administrator	Certificate
□	ise-mnt-ise470		Capabilities(2 Pub, 1 Sub)	Online	Administrator	Certificate

Connected to pxGrid ise470.lab10.com

Exporting ISE Identity Certificate in Stealthwatch Certificate Authority (CA) Store

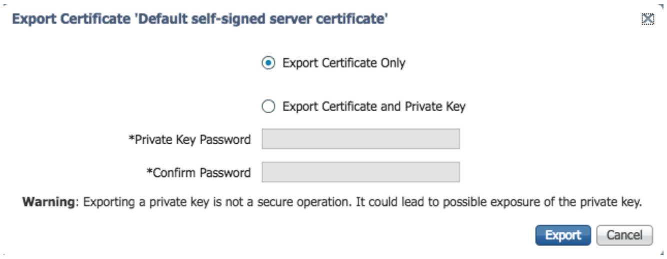
Step 1 Export the ISE self-signed identity certificate into the Stealthwatch Management Center's CA trusted store Select **Administration->System->Certificates->Certificate Management->System Certificates->Default self signed server certificate->Export**



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	
▼ ise470								
□	ise470.lab10.com#Certificate Services Endpoint Sub CA - ise470#00001	pxGrid		ise470.lab10.com	Certificate Services Endpoint Sub CA - ise470	Tue, 7 Feb 2017	Tue, 8 Feb 2022	✓
□	Default self-signed saml server certificate - CN=SAML_ise470.lab10.com	SAML		SAML_ise470.lab10.com	SAML_ise470.lab10.com	Wed, 8 Feb 2017	Thu, 8 Feb 2018	✓
☑	Default self-signed server certificate	EAP Authentication, Admin, Portal, RADIUS DTLS	Default Portal Certificate Group	ise470.lab10.com	ise470.lab10.com	Wed, 8 Feb 2017	Thu, 8 Feb 2018	✓

Step 2 Export the public certificate only



Export Certificate 'Default self-signed server certificate'

● Export Certificate Only

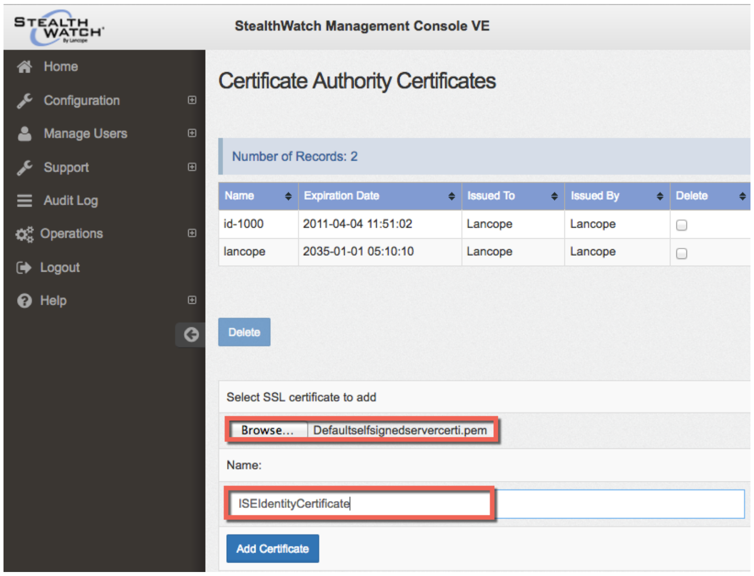
○ Export Certificate and Private Key

*Private Key Password	
*Confirm Password	

Warning: Exporting a private key is not a secure operation. It could lead to possible exposure of the private key.

Step 3 Select **Export**

Step 4 Select Gear ⚙ **->Administer Appliance->Configuration->Certificate Authority Certificates->Browse and upload the ISE certificate and provide a friendly name**



Certificate Authority Certificates

Number of Records: 2

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

Select SSL certificate to add

Browse... Defaultselfsignedservercerti.pem

Name:

ISEIdentityCertificate

Step 5 Select **Add Certificate** and confirm the certificate

Creating and Generating Stealthwatch Certificates

Step 1 Generate private key from the Stealthwatch Management Center

```
openssl genrsa -des3 -out smc69.key 2048
Generating RSA private key, 2048 bit long modulus
......+++
........................................+++
e is 65537 (0x10001)
Enter pass phrase for smc69.key: cisco123
Verifying - Enter pass phrase for smc69.key: Cisco123
```

Step 2 Generate certificate signing request (CSR) request from the Stealthwatch Management Center

```
openssl req -new -key smc69.key -out smc69.csr
Enter pass phrase for smc69.key: cisco123
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:US
State or Province Name (full name) [Some-State]:Maryland
Locality Name (eg, city) []:Germantown
Organization Name (eg, company) [Internet Widgits Pty Ltd]:Cisco
Organizational Unit Name (eg, section) []:Engineering
Common Name (e.g. server FQDN or YOUR name) []:smc69.lab10.com
Email Address []:j@lab10.com

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

Step 3 Generate self-signed certificate from the Stealthwatch Management Console

```
openssl x509 -req -days 365 -in smc69.csr -signkey smc69.key -out smc69.crt
Signature ok
subject=/C=US/ST=Maryland/L=Germantown/O=Cisco/OU=Engineering/CN=smc69.lab10.com/emailAddress=j@lab10.com
Getting Private key
Enter pass phrase for smc69.key: cisco123
```

Step 4 Decrypt passphrase

```
cp smc69.key smc69.key.org
openssl rsa -in smc69.key.org -out smc69.key
Enter pass phrase for smc69.key.org: cisco123
writing RSA key
```

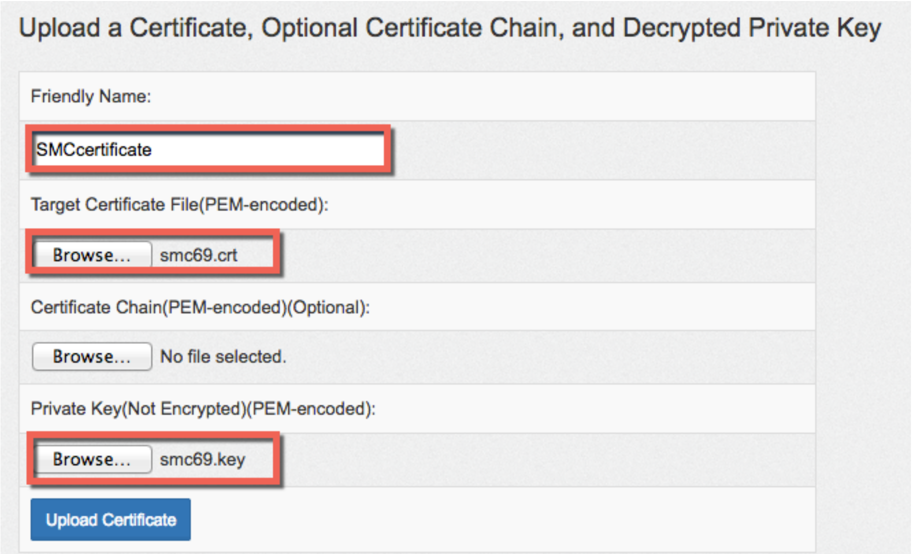
Step 5 Copy the smc public and smc private key from the Stealthwatch Management Console locally

```
scp smc69.crt jeppich@192.168.1.8:/Applications/smc69/
RSA key fingerprint is 10:ce:54:b6:20:8b:3f:86:b1:5f:29:bb:d0:6a:a8:ab.
Are you sure you want to continue connecting (yes/no)? yes
Warning: Permanently added '192.168.1.8' (RSA) to the list of known hosts.
Password: cisco123
smc69.crt                                     100% 1318      1.3KB/s   00:00

scp smc69.key jeppich@192.168.1.8:/Applications/smc69/
Password: cisco123
smc69.key                                     100% 1675      1.6KB/s   00:00
```

Importing Stealthwatch Certificates into SSL Client Store

Step 1 Select **Configuration->SSL Certificates->SSL Certificates->SSL Client Identities->Enter Friendly Name->Upload a Certificate, Optional Certificate Chain and Decrypted Private Key**



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

Friendly Name:

SMCcertificate

Target Certificate File(PEM-encoded):

Browse... smc69.crt

Certificate Chain(PEM-encoded)(Optional):

Browse... No file selected.

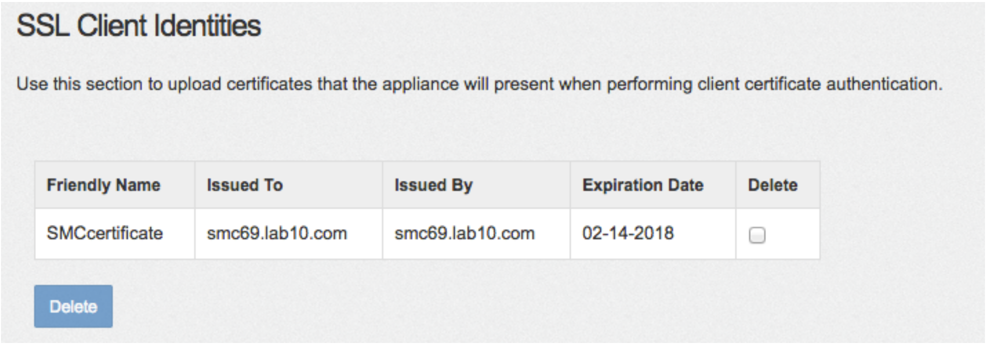
Private Key(Not Encrypted)(PEM-encoded):

Browse... smc69.key

Upload Certificate

Step 2 Select **Upload Certificate**

Step 3 You should see that the client certificate was successfully uploaded



SSL Client Identities

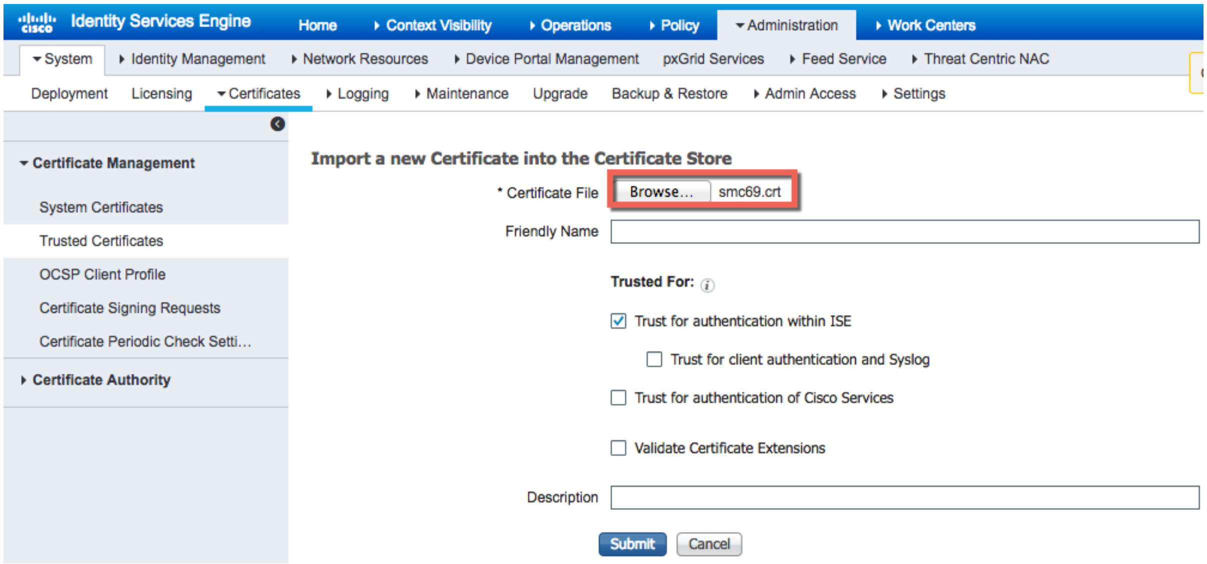
Use this section to upload certificates that the appliance will present when performing client certificate authentication.

Friendly Name	Issued To	Issued By	Expiration Date	Delete
SMCcertificate	smc69.lab10.com	smc69.lab10.com	02-14-2018	☐

Delete

Exporting Stealthwatch Certificates into ISE Trusted Certificate Store

Step 1 Import SMC certificate into ISE trusted system certificate store
Select **Administration->System->Certificates->Certificate Management->Trusted Certificates->Import the smc public certificate**



Import a new Certificate into the Certificate Store

* Certificate File: smc69.crt

Friendly Name:

Trusted For:

☑ Trust for authentication within ISE

□ Trust for client authentication and Syslog

□ Trust for authentication of Cisco Services

□ Validate Certificate Extensions

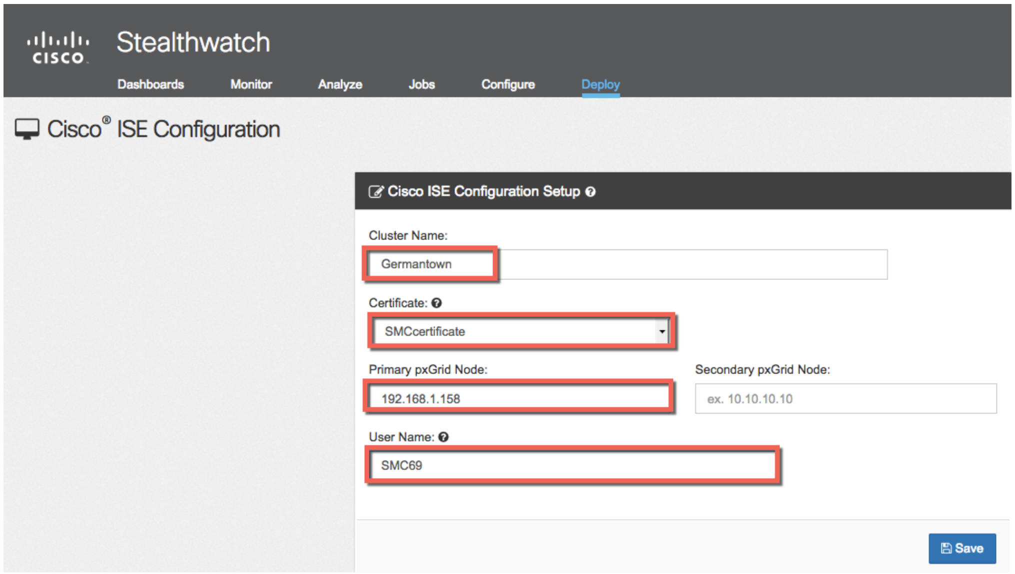
Description:

Step 2 Enable **Trust for Authentication within ISE**

Step 3 Select **Submit**

Configuring Stealthwatch pxGrid operation

Step 1 On SMC, select **Deploy->Cisco ISE Configuration->**



Cisco ISE Configuration Setup

Cluster Name: Germantown

Certificate: SMCcertificate

Primary pxGrid Node: 192.168.1.158

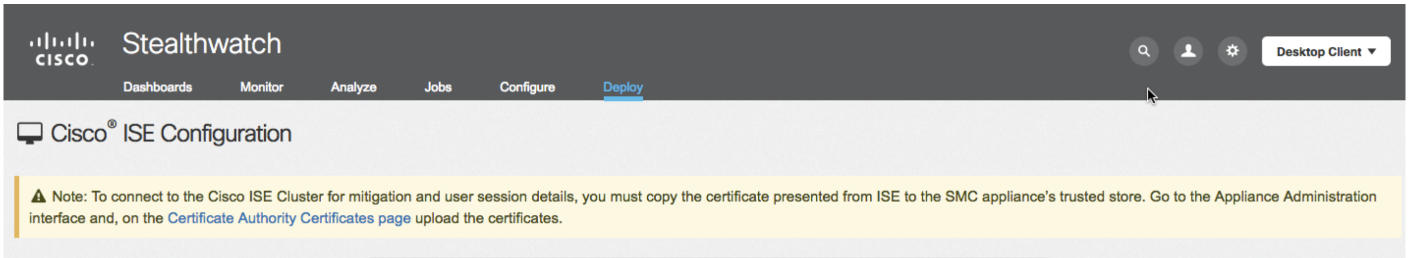
Secondary pxGrid Node: ex. 10.10.10.10

User Name: SMC69

Step 2 Select **Save**

Step 3 You should see a Success message select OK

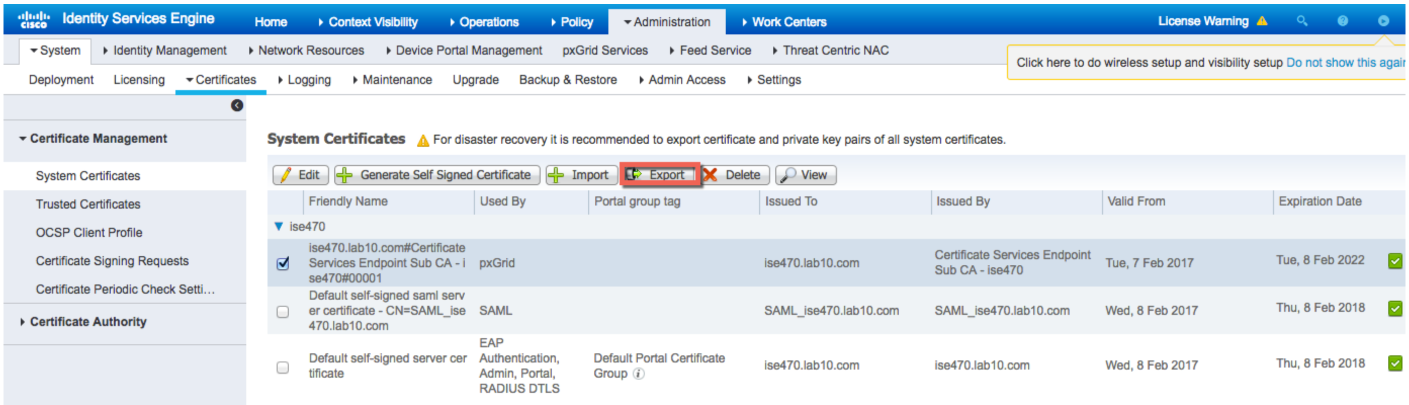
Step 4 If you see the following message, this means that perhaps the certificate chain was not imported.



Cisco® ISE Configuration

⚠ Note: To connect to the Cisco ISE Cluster for mitigation and user session details, you must copy the certificate presented from ISE to the SMC appliance's trusted store. Go to the Appliance Administration interface and, on the Certificate Authority Certificates page upload the certificates.

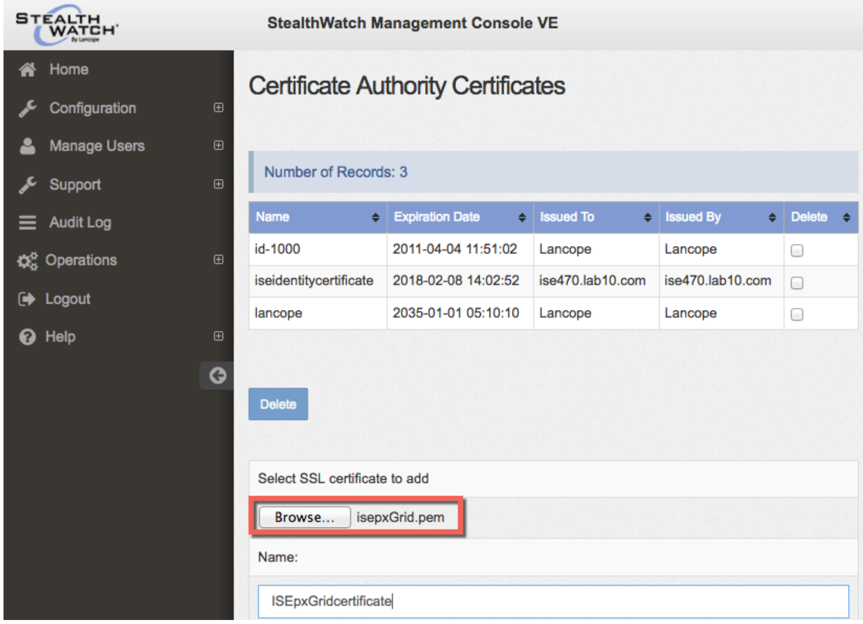
Step 5 If using ISE 2.2, export the pxGrid certificate as well.



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	
▼ ise470								
☑	ise470.lab10.com#Certificate Services Endpoint Sub CA - ise470#00001	pxGrid		ise470.lab10.com	Certificate Services Endpoint Sub CA - ise470	Tue, 7 Feb 2017	Tue, 8 Feb 2022	✓
□	Default self-signed saml server certificate - CN=SAML_ise470.lab10.com	SAML		SAML_ise470.lab10.com	SAML_ise470.lab10.com	Wed, 8 Feb 2017	Thu, 8 Feb 2018	✓
□	Default self-signed server certificate	EAP Authentication, Admin, Portal, RADIUS DTLS	Default Portal Certificate Group ⓘ	ise470.lab10.com	ise470.lab10.com	Wed, 8 Feb 2017	Thu, 8 Feb 2018	✓

Step 6 Select **Certificate Authority Certificate** page and import the ISE pxGrid certificate add a friendly name



Certificate Authority Certificates

Number of Records: 3

Name	Expiration Date	Issued To	Issued By	Delete
id-1000	2011-04-04 11:51:02	Lancope	Lancope	□
iseidentitycertificate	2018-02-08 14:02:52	ise470.lab10.com	ise470.lab10.com	□
lancope	2035-01-01 05:10:10	Lancope	Lancope	□

Select SSL certificate to add

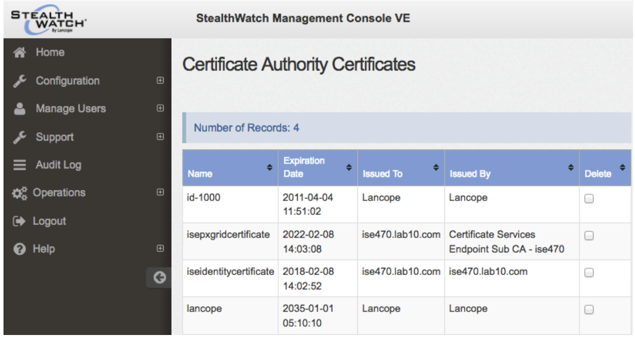
Browse... isepxGrid.pem

Name:

ISEpxGridcertificate

Step 7 Select **Add Certificate** and confirm

Step 8 You should see the updated certificates

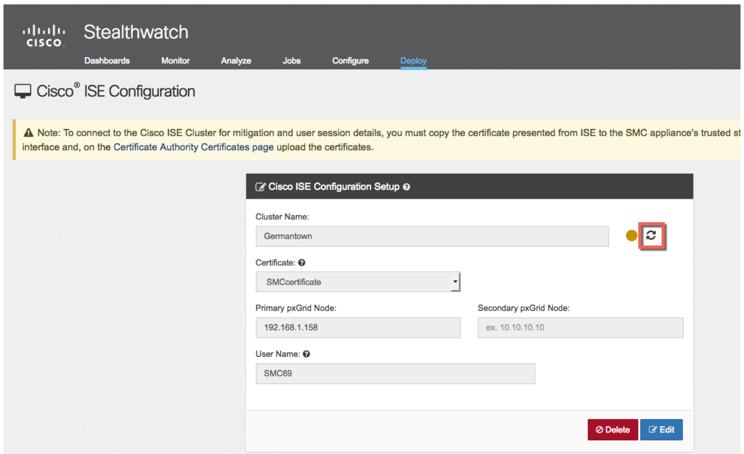


Certificate Authority Certificates

Number of Records: 4

Name	Expiration Date	Issued To	Issued By	Delete
id-1000	2011-04-04 11:51:02	Lancope	Lancope	□
isepxgridcertificate	2022-02-08 14:03:08	ise470.lab10.com	Certificate Services Endpoint Sub CA - ise470	□
iseidentitycertificate	2018-02-08 14:02:52	ise470.lab10.com	ise470.lab10.com	□
lancope	2035-01-01 05:10:10	Lancope	Lancope	□

Step 9 Go back and refresh



Cisco® ISE Configuration

Note: To connect to the Cisco ISE Cluster for mitigation and user session details, you must copy the certificate presented from ISE to the SMC appliance's trusted st interface and, on the Certificate Authority Certificates page upload the certificates.

Cisco ISE Configuration Setup

Cluster Name: Germantown

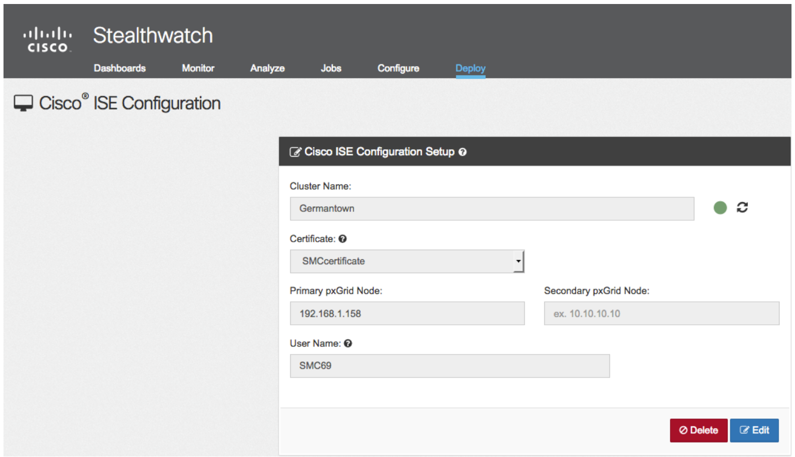
Certificate: SMCcertificate

Primary pxGrid Node: 192.168.1.158

Secondary pxGrid Node: ex. 10.10.10.10

User Name: SMC69

Step 10 You should see this now green



Cisco® ISE Configuration

Cisco ISE Configuration Setup

Cluster Name: Germantown

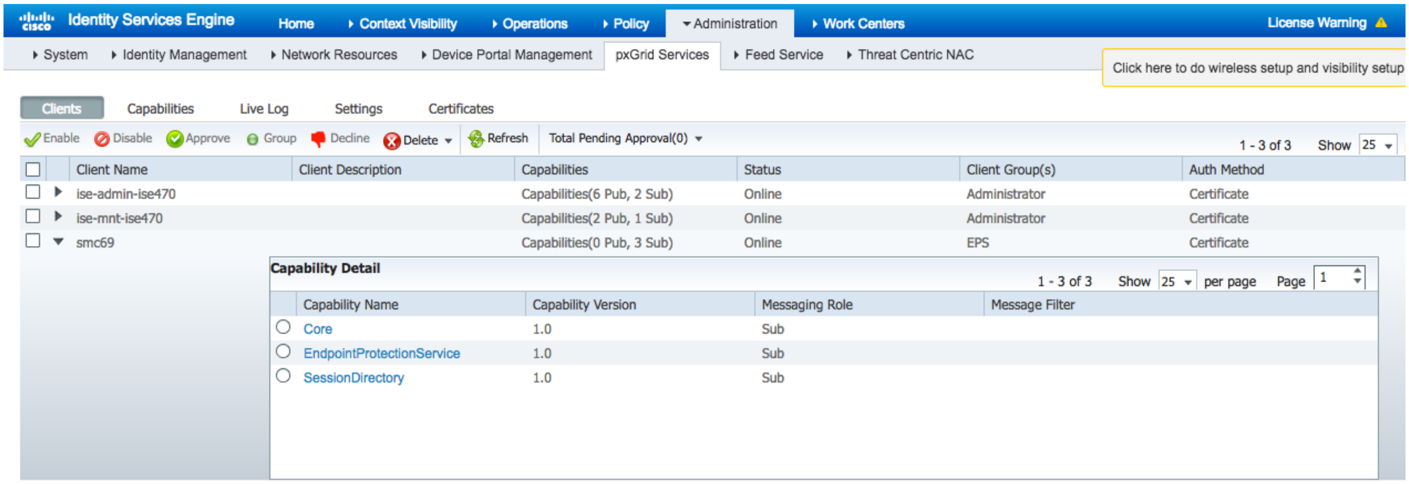
Certificate: SMCcertificate

Primary pxGrid Node: 192.168.1.158

Secondary pxGrid Node: ex. 10.10.10.10

User Name: SMC69

Step 11 On ISE, select **Administration->pxGrid Services**, you should see Stealthwatch Management Center has successfully registered and subscribed to the session topics.



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

Capability Detail

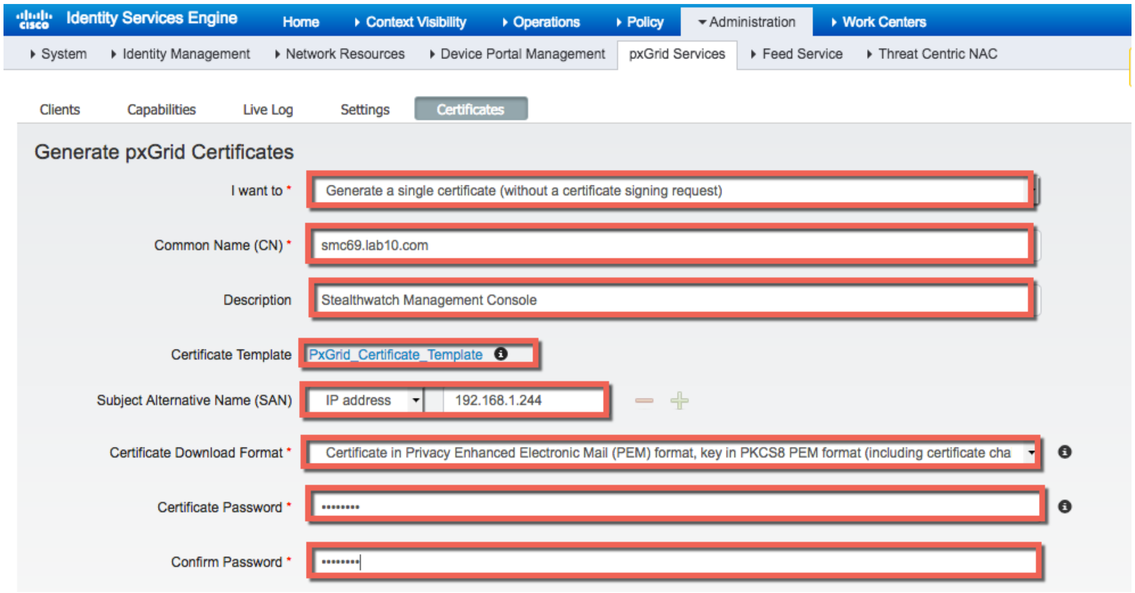
	Capability Name	Capability Version	Messaging Role	Message Filter
○	Core	1.0	Sub	
○	EndpointProtectionService	1.0	Sub	
○	SessionDirectory	1.0	Sub	

Generating Single Certificate (without CSR) in PEM format

Create and Generate Stealthwatch certificate

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

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

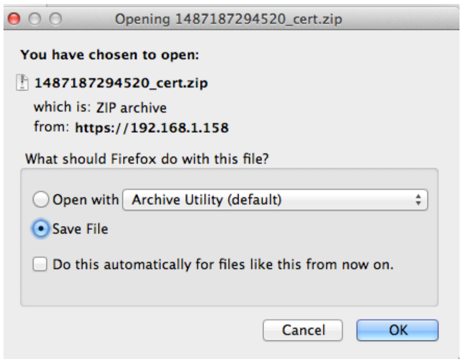


Generate pxGrid Certificates

I want to *	Generate a single certificate (without a certificate signing request)
Common Name (CN) *	smc69.lab10.com
Description	Stealthwatch Management Console
Certificate Template	PxGrid_Certificate_Template
Subject Alternative Name (SAN)	IP address 192.168.1.244
Certificate Download Format *	Certificate in Privacy Enhanced Electronic Mail (PEM) format, key in PKCS8 PEM format (including certificate cha
Certificate Password *	••••••••
Confirm Password *	••••••••

Step 2 Select **Create**

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



Opening 1487187294520_cert.zip

You have chosen to open:

1487187294520_cert.zip

which is: ZIP archive

from: **https://192.168.1.158**

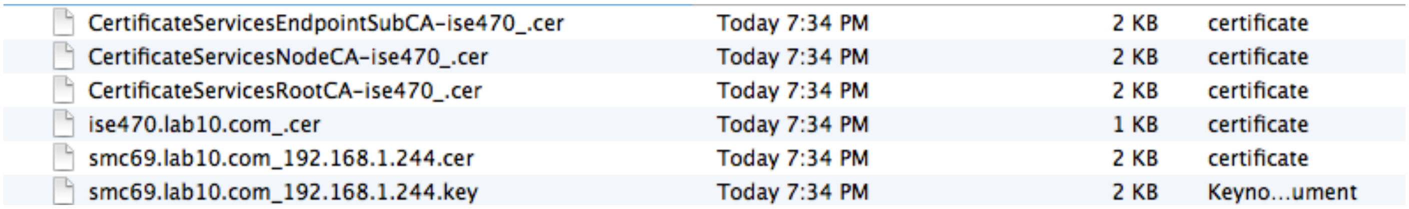
What should Firefox do with this file?

○ Open with Archive Utility (default)

● Save File

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

Step 4 You should see the following files

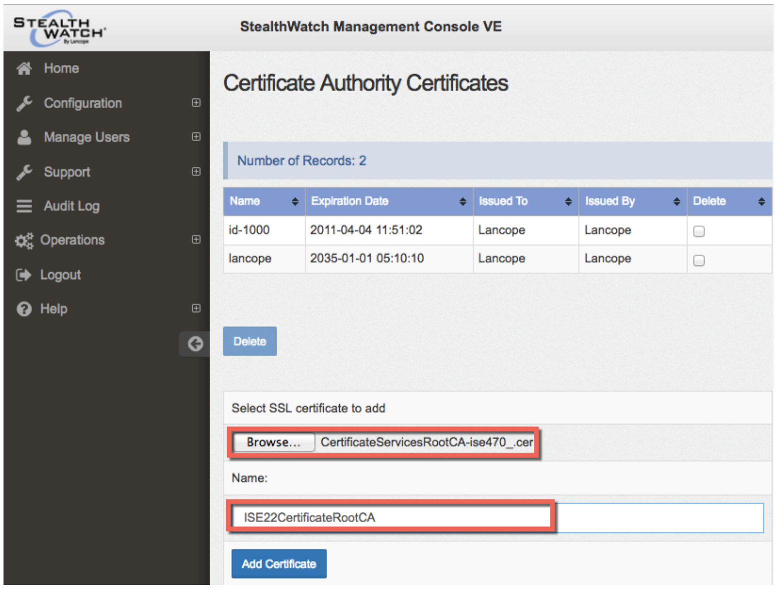


CertificateServicesEndpointSubCA-ise470_.cer	Today 7:34 PM	2 KB	certificate
CertificateServicesNodeCA-ise470_.cer	Today 7:34 PM	2 KB	certificate
CertificateServicesRootCA-ise470_.cer	Today 7:34 PM	2 KB	certificate
ise470.lab10.com_.cer	Today 7:34 PM	1 KB	certificate
smc69.lab10.com_192.168.1.244.cer	Today 7:34 PM	2 KB	certificate
smc69.lab10.com_192.168.1.244.key	Today 7:34 PM	2 KB	Keyno...ument

Exporting ISE CertificateServicesRootCA into SMC Certificate Authority (CA) Store

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

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



Certificate Authority Certificates

Number of Records: 2

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

Select SSL certificate to add

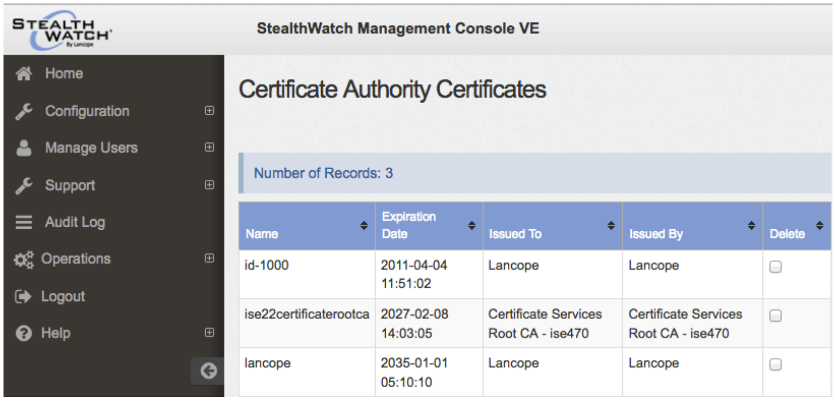
Browse... CertificateServicesRootCA-ise470_.cer

Name:

ISE22CertificateRootCA

Step 3 Select **Add Certificate** and confirm

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



Certificate Authority Certificates

Number of Records: 3

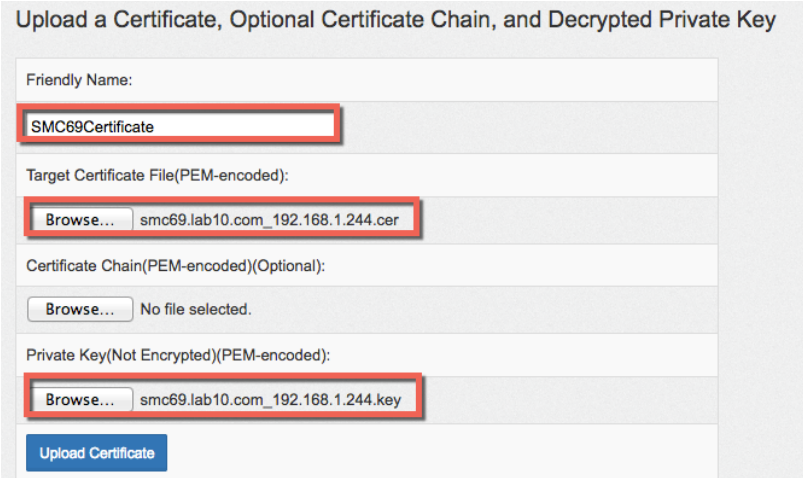
Name	Expiration Date	Issued To	Issued By	Delete
id-1000	2011-04-04 11:51:02	Lancope	Lancope	□
ise22certificaterootca	2027-02-08 14:03:05	Certificate Services Root CA - ise470	Certificate Services Root CA - ise470	□
lancope	2035-01-01 05:10:10	Lancope	Lancope	□

Adding Stealthwatch certificate to SSL Client Identities Store

Step 1 Decrypt passphrase

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

Step 2 Under **Configuration->SSL Certificate->SSL Client Identities, Upload a certificate, Optional certificate chain, and decrypted private key**



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

Friendly Name: SMC69Certificate

Target Certificate File(PEM-encoded): Browse... smc69.lab10.com_192.168.1.244.cer

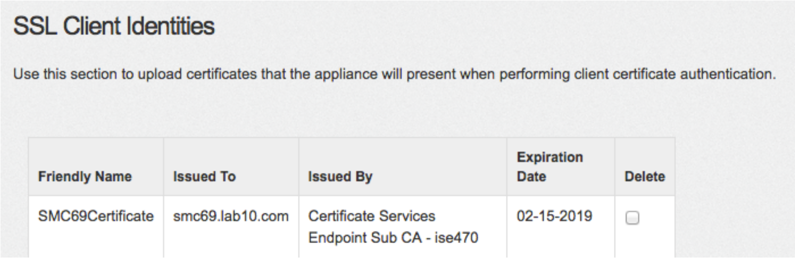
Certificate Chain(PEM-encoded)(Optional): Browse... No file selected.

Private Key(Not Encrypted)(PEM-encoded): Browse... smc69.lab10.com_192.168.1.244.key

Step 3 Select **Upload Certificate** and confirm

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

Step 4 You should see the following under SSL Client Identities



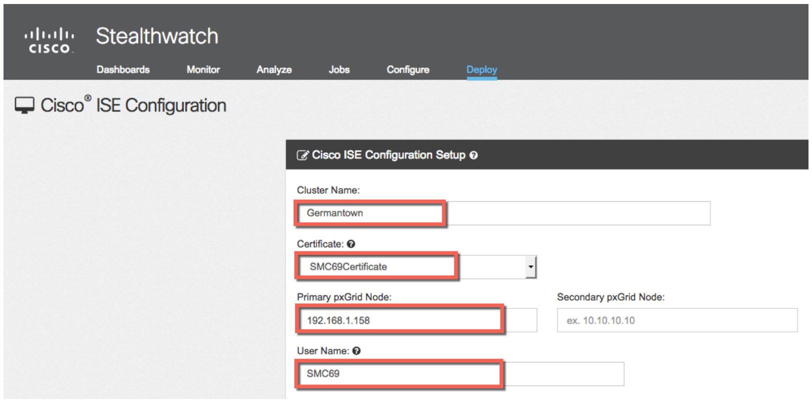
SSL Client Identities

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

Friendly Name	Issued To	Issued By	Expiration Date	Delete
SMC69Certificate	smc69.lab10.com	Certificate Services Endpoint Sub CA - ise470	02-15-2019	□

Configuring Stealthwatch for pxGrid operation

Step 1 On the SMC Dashboard, select **Deploy->Cisco ISE Configuration**, and enter the following:



Cisco® ISE Configuration

Cisco ISE Configuration Setup

Cluster Name: Germantown

Certificate: SMC69Certificate

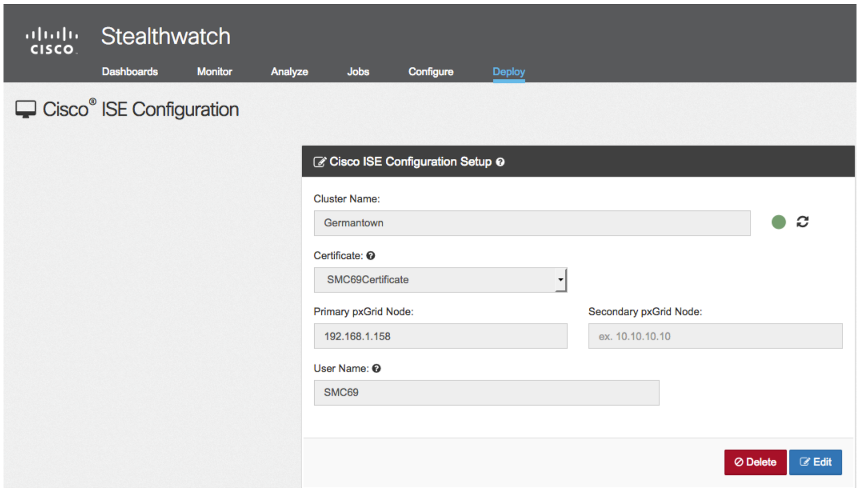
Primary pxGrid Node: 192.168.1.158

Secondary pxGrid Node: ex. 10.10.10.10

User Name: SMC69

Step 2 Select **Save**

Step 3 You should see the configuration saved successfully and the status updated successfully by the green dot



Cisco® ISE Configuration

Cisco ISE Configuration Setup

Cluster Name: Germantown ●

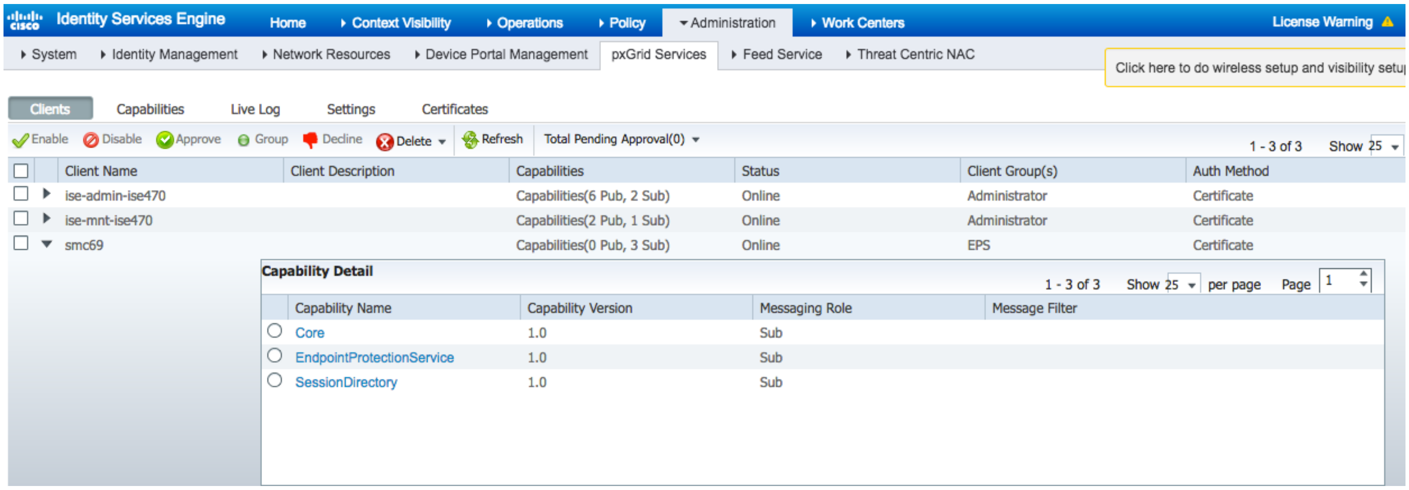
Certificate: SMC69Certificate

Primary pxGrid Node: 192.168.1.158

Secondary pxGrid Node: ex. 10.10.10.10

User Name: SMC69

Step 4 In ISE, select **Administration->pxGrid Services**



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

Capability Detail

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

Generating Certificate Signing Request CSR (with certificate signing request) using ISE 2.2 Internal CA

Creating Stealthwatch Certificate

Step 1 Generate the private key from the Stealthwatch Management Console

Note: The –des3 argument provides the pass phrase password. Here Cisco123 is entered as the passphrase.

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

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

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

Please enter the following 'extra' attributes
```

```
to be sent with your certificate request
A challenge password []:
An optional company name []:
```

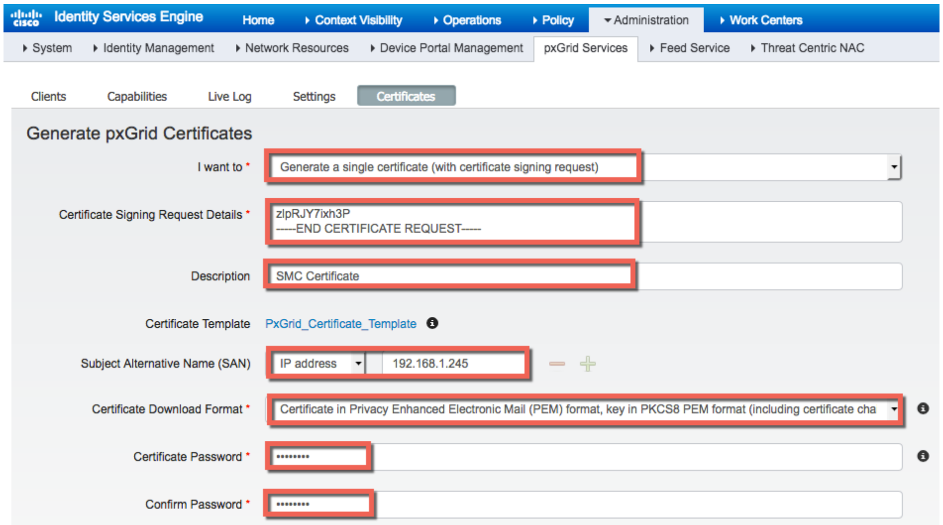
Step 3 Copy files locally

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

ISE Generating Certificate based on CSR request in PEM format

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

Note: You can only generate a key size of 2096; there is a bug in the pxGrid template. Enter the same pass phrase as you entered using the –des3 argument. In this example, Cisco123 was used.



Generate pxGrid Certificates

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

Certificate Signing Request Details * zlpRJY7ixh3P
-----END CERTIFICATE REQUEST-----

Description SMC Certificate

Certificate Template PxGrid_Certificate_Template

Subject Alternative Name (SAN) IP address 192.168.1.245

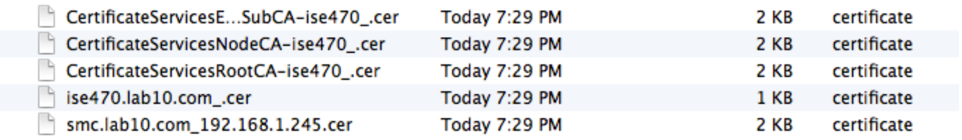
Certificate Download Format * Certificate in Privacy Enhanced Electronic Mail (PEM) format, key in PKCS8 PEM format (including certificate cha

Certificate Password * ••••••••

Confirm Password * ••••••••

Step 2 Select **Create**

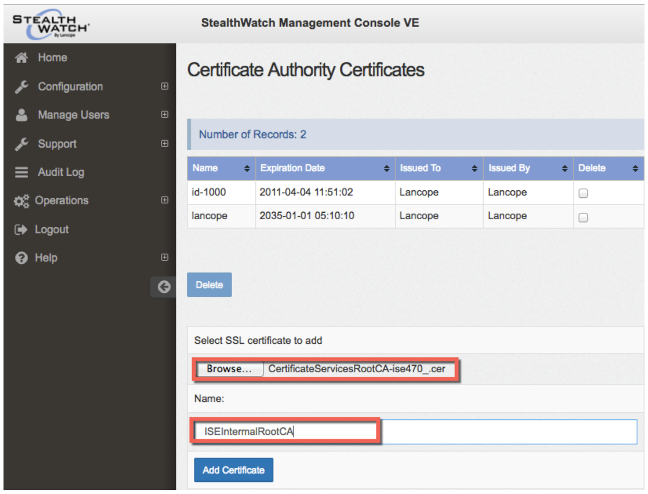
Step 3 Download the zipped file locally, you should see the following files



CertificateServicesE...SubCA-ise470_.cer	Today 7:29 PM	2 KB	certificate
CertificateServicesNodeCA-ise470_.cer	Today 7:29 PM	2 KB	certificate
CertificateServicesRootCA-ise470_.cer	Today 7:29 PM	2 KB	certificate
ise470.lab10.com_.cer	Today 7:29 PM	1 KB	certificate
smc.lab10.com_192.168.1.245.cer	Today 7:29 PM	2 KB	certificate

Import ISE CAServicesRoot certificate into Stealthwatch CA store

Step 1 On SMC, add root to CA authority



Certificate Authority Certificates

Number of Records: 2

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

Select SSL certificate to add

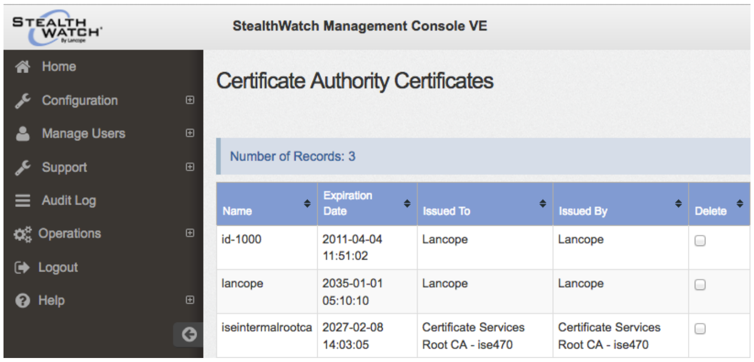
Browse... CertificateServicesRootCA-ise470_.cer

Name:

ISEIntermalRootCA

Step 2 Select **Add Certificate and confirm**

Step 3 You should see the following:



Certificate Authority Certificates

Number of Records: 3

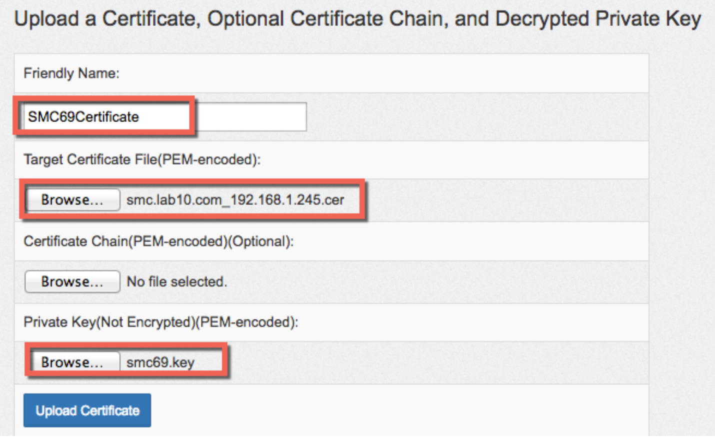
Name	Expiration Date	Issued To	Issued By	Delete
id-1000	2011-04-04 11:51:02	Lancope	Lancope	□
lancope	2035-01-01 05:10:10	Lancope	Lancope	□
iseintermalrootca	2027-02-08 14:03:05	Certificate Services Root CA - ise470	Certificate Services Root CA - ise470	□

Import Stealthwatch certificates into SSL Client Store

Step 1 Decrypt password

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

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



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

Friendly Name: SMC69Certificate

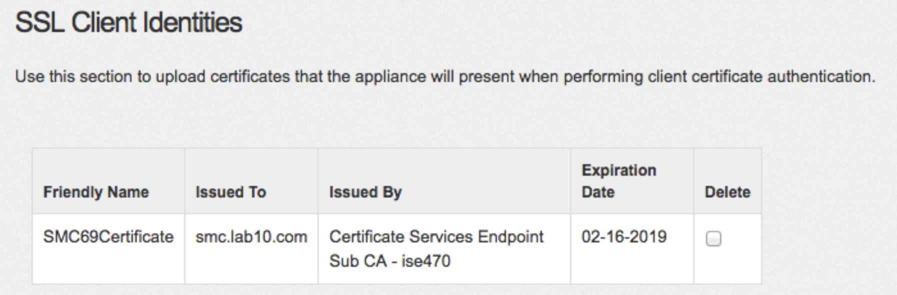
Target Certificate File(PEM-encoded): smc.lab10.com_192.168.1.245.cer

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

Private Key(Not Encrypted)(PEM-encoded): smc69.key

Step 3 Select **Upload Certificate and confirm**

Step 4 You should see the following under SSL Client Identities



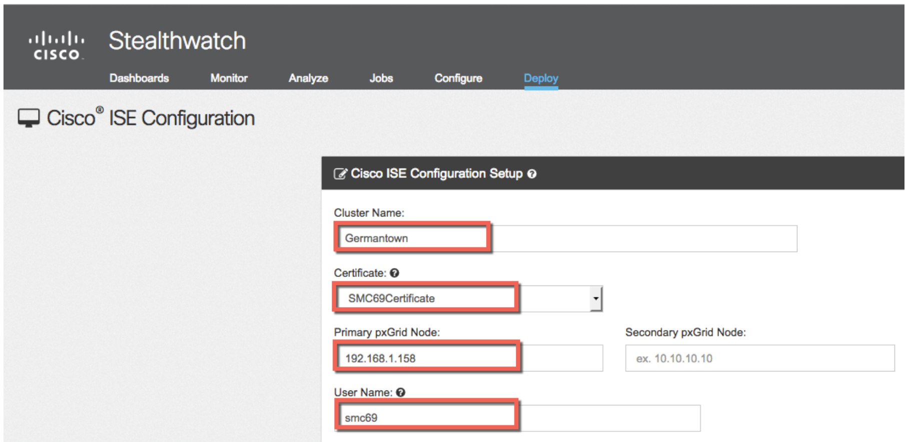
SSL Client Identities

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

Friendly Name	Issued To	Issued By	Expiration Date	Delete
SMC69Certificate	smc.lab10.com	Certificate Services Endpoint Sub CA - ise470	02-16-2019	□

Configuring Stealthwatch for pxGrid Operation

Step 1 On the SMC Dashboard, select **Deploy->Cisco ISE Configuration** and configure pxGrid



Cisco® ISE Configuration

Cisco ISE Configuration Setup

Cluster Name: Germantown

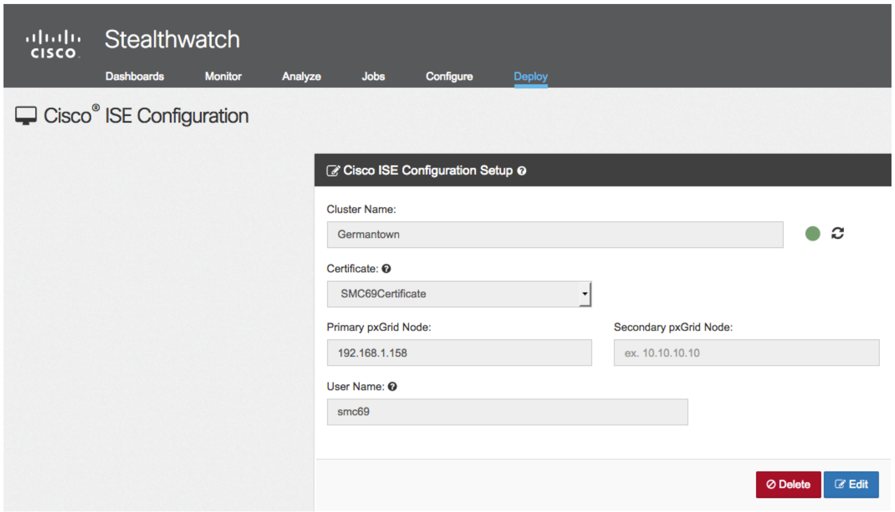
Certificate: SMC69Certificate

Primary pxGrid Node: 192.168.1.158

Secondary pxGrid Node: ex. 10.10.10.10

User Name: smc69

Step 2 Select Save and OK, you should see a successful connection



Cisco® ISE Configuration

Cisco ISE Configuration Setup

Cluster Name: Germantown

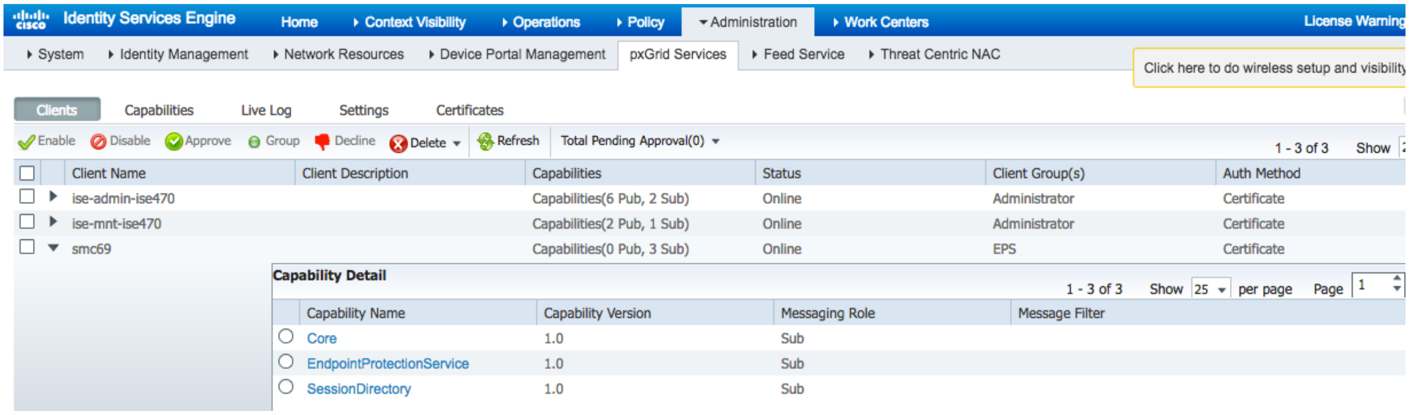
Certificate: SMC69Certificate

Primary pxGrid Node: 192.168.1.158

Secondary pxGrid Node: ex. 10.10.10.10

User Name: smc69

Step 3 In ISE, select **Administration->pxGrid services**, you should see the SMC successfully registered and subscribed to the ISE pxGrid node



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

Capability Detail

1 - 3 of 3 Show 25 per page Page 1

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

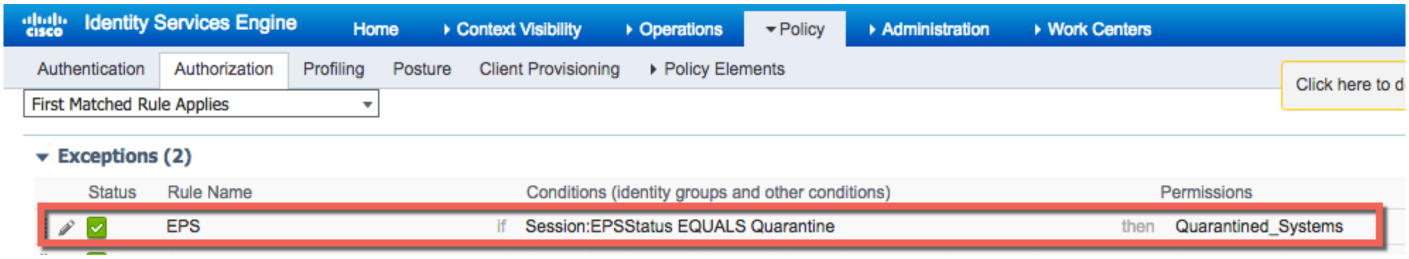
Configuring ISE Authorization Policy

In this section, we configure ISE authorization policies to quarantine endpoints once the Stealthwatch Management Console, issues an ANC request to quarantine/unquarantine endpoints and also to assign an Employee Security Group Tag (SGT) to end-users who successfully authenticate and belong to the Microsoft /users/domain group.

Stealthwatch subscribes to the ISE pxGrid node EndpointProtection Service to perform these mitigation actions and thus uses legacy EPS functionality, where the Sessison:EPSTATUS:quarantine policy is used instead of the newer Adaptive Network Control (ANC) Policies which were introduced in ISE 2.0.

Configuring ISE Quarantine Rule

Step 1 Select Policy->Authorization->Exceptions->Create New->for the **rule name**, type: **EPS**
Step 2 Select "**+**" next to **Conditions**, and **Create New Condition->Session:EPSTATUS:Quarantine**
Step 3 Select "+" next to **Authz Policy**, select **Security Group->Quarantined Systems->Done**
Step 4 You should see the following:



Status	Rule Name		Conditions (identity groups and other conditions)		Permissions
✓	EPS	if	Session:EPSStatus EQUALS Quarantine	then	Quarantined_Systems

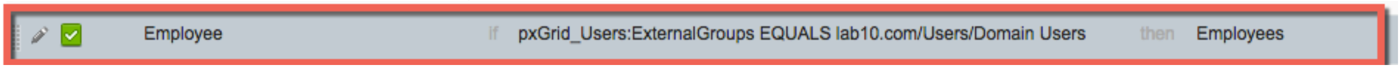
Step 5 Select **Save**

Configuring Employee Access Rule

Step 1 Select **Insert New Rule Above->**for the **Rule Name** type **Employee**
Step 2 Select "**+**" next to **Conditions**, and **Create New Condition->pxGrid_Users:External Groups:lab10.com/domain users**

Note: Please note that you have your own External identity source configured in ISE, and pxGrid_Users, will reflect the Joint Point Name

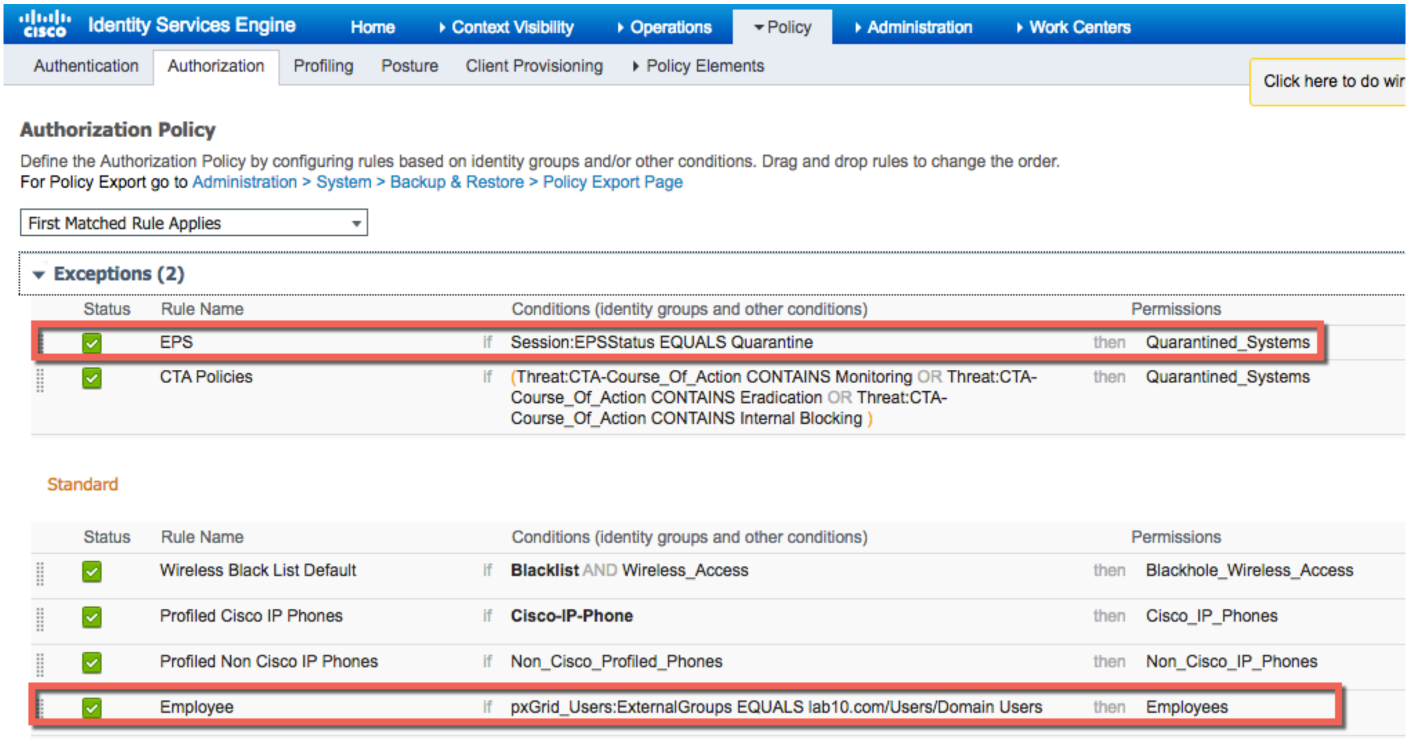
Step 3 Select "+" next to **Authz Policy**, select **Security Group->Employees->Done**
Step 4 You should see the following:



Status	Rule Name		Conditions		Permissions
✓	Employee	if	pxGrid_Users:ExternalGroups EQUALS lab10.com/Users/Domain Users	then	Employees

Step 5 Select **Save**

Step 6 You should see:



Authorization Policy

Define the Authorization Policy by configuring rules based on identity groups and/or other conditions. Drag and drop rules to change the order.
For Policy Export go to Administration > System > Backup & Restore > Policy Export Page

Exceptions (2)

Status	Rule Name		Conditions (identity groups and other conditions)		Permissions
✓	EPS	if	Session:EPSStatus EQUALS Quarantine	then	Quarantined_Systems
✓	CTA Policies	if	(Threat:CTA-Course_Of_Action CONTAINS Monitoring OR Threat:CTA-Course_Of_Action CONTAINS Eradication OR Threat:CTA-Course_Of_Action CONTAINS Internal Blocking)	then	Quarantined_Systems

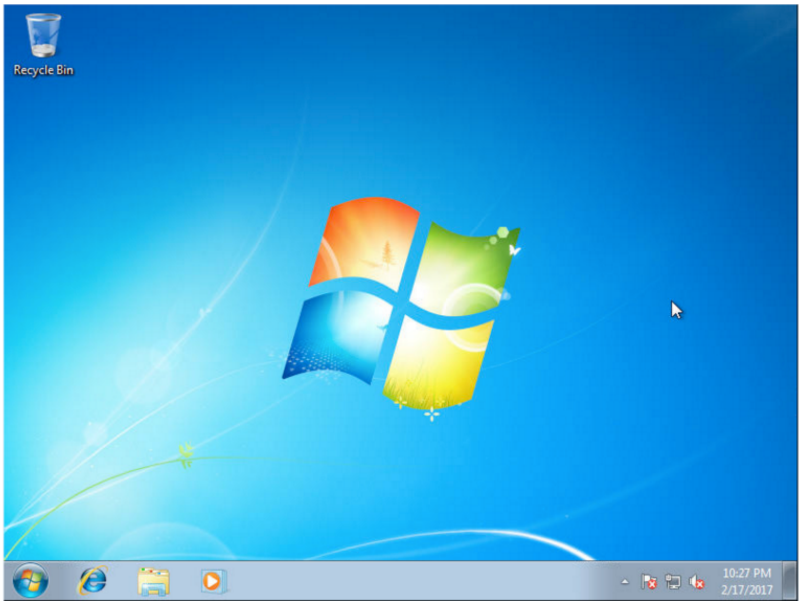
Standard

Status	Rule Name		Conditions (identity groups and other conditions)		Permissions
✓	Wireless Black List Default	if	**Blacklist** AND Wireless_Access	then	Blackhole_Wireless_Access
✓	Profiled Cisco IP Phones	if	**Cisco-IP-Phone**	then	Cisco_IP_Phones
✓	Profiled Non Cisco IP Phones	if	Non_Cisco_Profiled_Phones	then	Non_Cisco_IP_Phones
✓	Employee	if	pxGrid_Users:ExternalGroups EQUALS lab10.com/Users/Domain Users	then	Employees

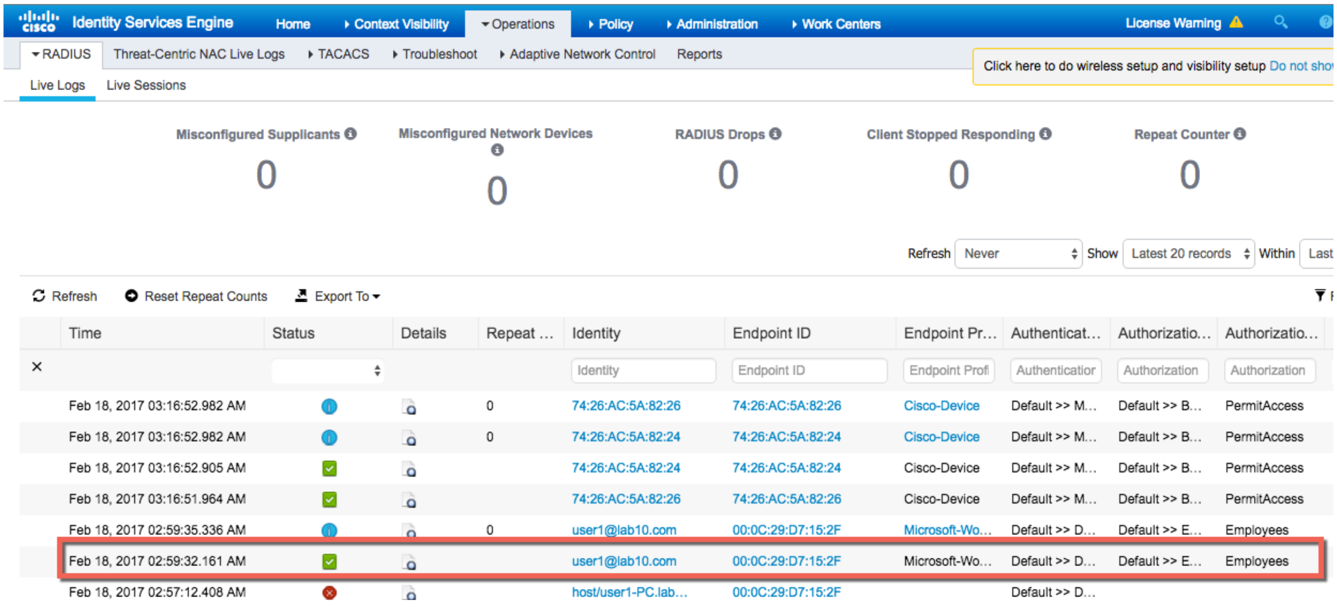
Testing

In this section, we authenticate an end-user via 802.1X. Using the Stealthwatch Management Console, the endpoint is quarantined and unquarantined. The results are seen in ISE under the RADIUS Live logs. In addition, the endpoint can also be unquarantined via the ISE GUI.

Step 1 User successfully authenticates via 802.1X



Step 2 On ISE, select **Operations->RADIUS->Live Logs**

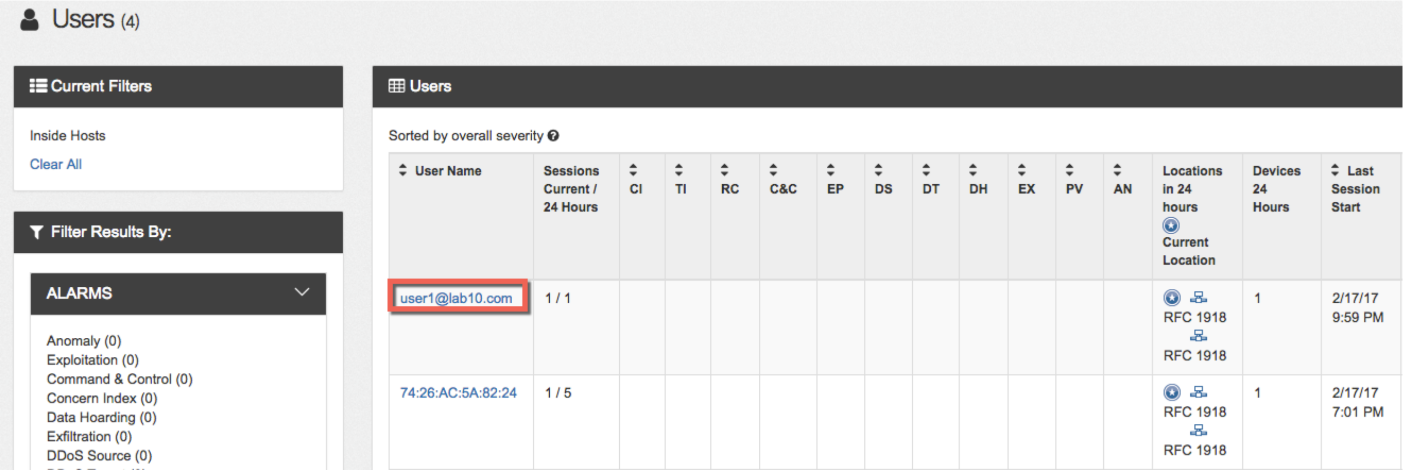


Misconfigured Supplicants	Misconfigured Network Devices	RADIUS Drops	Client Stopped Responding	Repeat Counter
0	0	0	0	0

Refresh: Never Show: Latest 20 records Within: Last

Time	Status	Details	Repeat ...	Identity	Endpoint ID	Endpoint Pr...	Authenticat...	Authorizatio...	Authorizatio...
Feb 18, 2017 03:16:52.982 AM	●		0	74:26:AC:5A:82:26	74:26:AC:5A:82:26	Cisco-Device	Default >> M...	Default >> B...	PermitAccess
Feb 18, 2017 03:16:52.982 AM	●		0	74:26:AC:5A:82:24	74:26:AC:5A:82:24	Cisco-Device	Default >> M...	Default >> B...	PermitAccess
Feb 18, 2017 03:16:52.905 AM	✓			74:26:AC:5A:82:24	74:26:AC:5A:82:24	Cisco-Device	Default >> M...	Default >> B...	PermitAccess
Feb 18, 2017 03:16:51.964 AM	✓			74:26:AC:5A:82:26	74:26:AC:5A:82:26	Cisco-Device	Default >> M...	Default >> B...	PermitAccess
Feb 18, 2017 02:59:35.336 AM	●		0	user1@lab10.com	00:0C:29:D7:15:2F	Microsoft-Wo...	Default >> D...	Default >> E...	Employees
Feb 18, 2017 02:59:32.161 AM	✓			user1@lab10.com	00:0C:29:D7:15:2F	Microsoft-Wo...	Default >> D...	Default >> E...	Employees
Feb 18, 2017 02:57:12.408 AM	✗			host/user1-PC.lab...	00:0C:29:D7:15:2F		Default >> D...		

Step 3 On the Stealthwatch Management Console, select **Monitor->Users**



Users (4)

Current Filters

Inside Hosts

Clear All

Filter Results By:

ALARMS

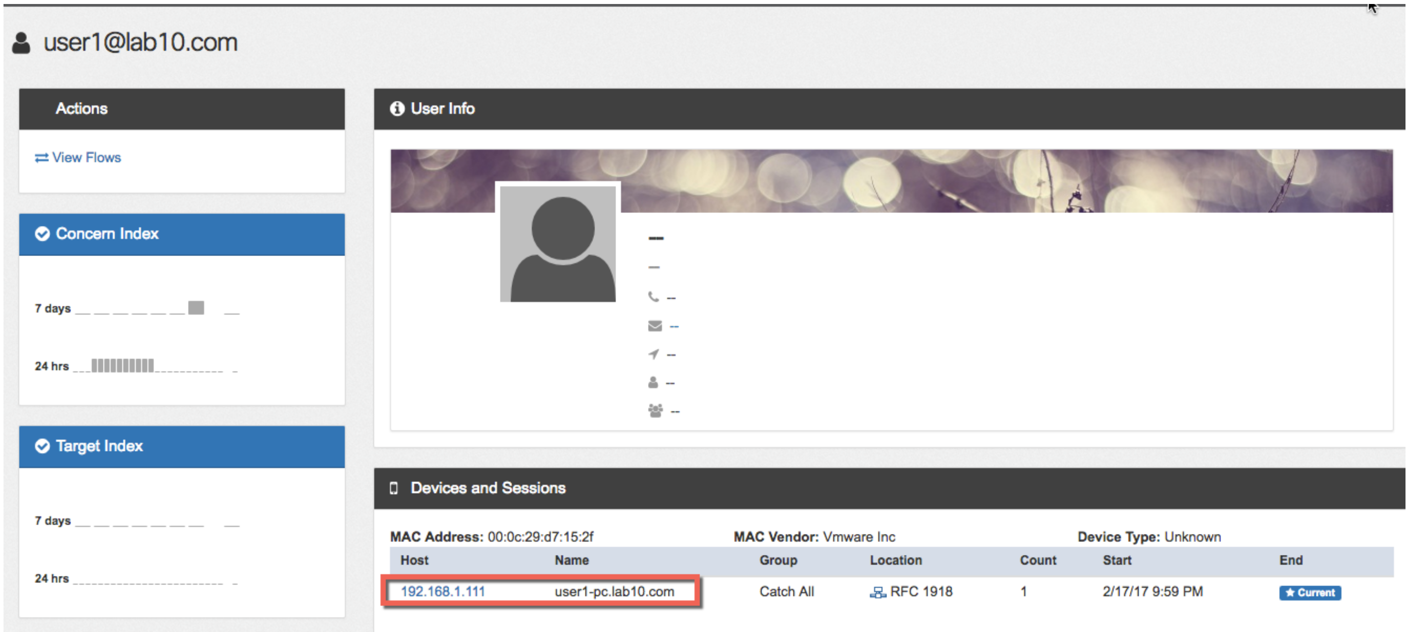
Anomaly (0)
Exploitation (0)
Command & Control (0)
Concern Index (0)
Data Hoarding (0)
Exfiltration (0)
DDoS Source (0)

Users

Sorted by overall severity

User Name	Sessions Current / 24 Hours	CI	TI	RC	C&C	EP	DS	DT	DH	EX	PV	AN	Locations in 24 hours Current Location	Devices 24 Hours	Last Session Start
user1@lab10.com	1 / 1												RFC 1918 RFC 1918	1	2/17/17 9:59 PM
74:26:AC:5A:82:24	1 / 5												RFC 1918 RFC 1918	1	2/17/17 7:01 PM

Step 4 Select user1@lab10.com , you should see:



user1@lab10.com

Actions

View Flows

Concern Index

7 days

24 hrs

Target Index

7 days

24 hrs

User Info

--

--

☎ --

✉ --

--

--

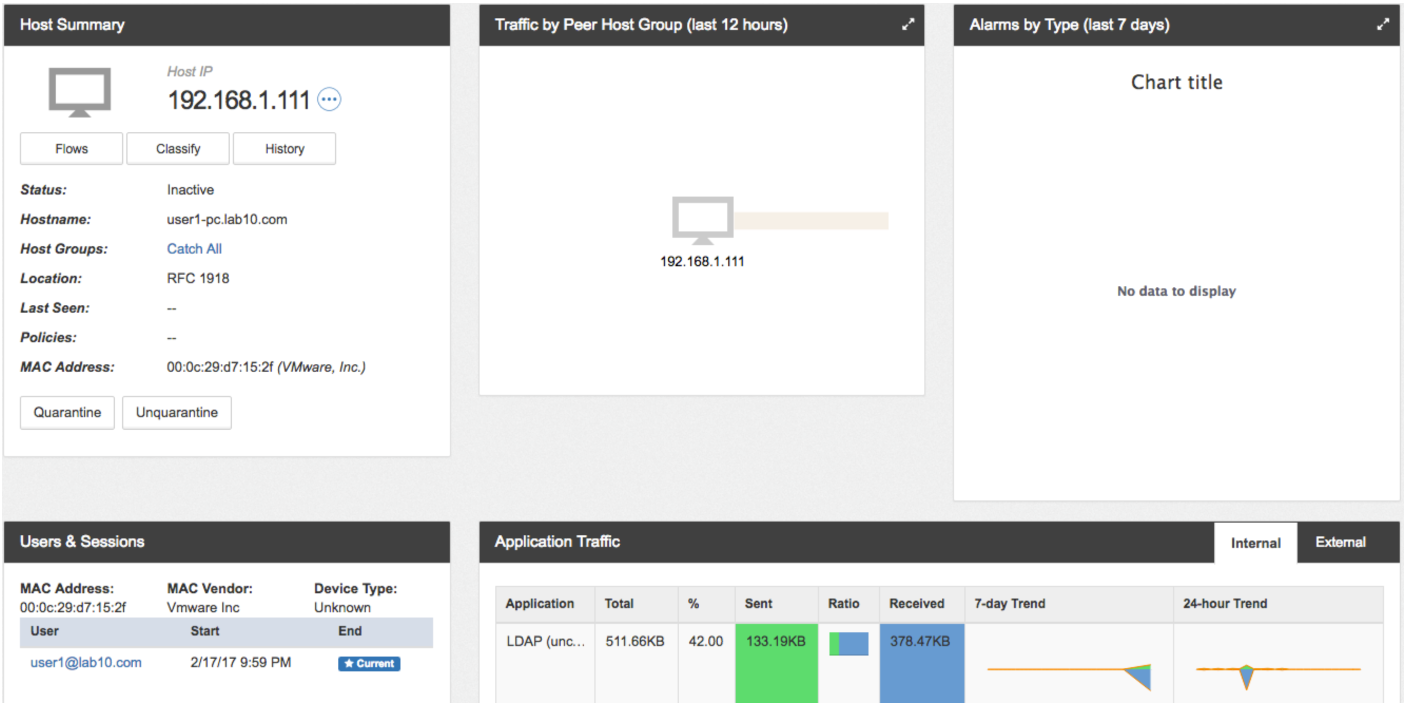
--

Devices and Sessions

MAC Address: 00:0c:29:d7:15:2f **MAC Vendor:** Vmware Inc **Device Type:** Unknown

Host	Name	Group	Location	Count	Start	End
192.168.1.111	user1-pc.lab10.com	Catch All	RFC 1918	1	2/17/17 9:59 PM	★ Current

Step 5 Select IP Address, you should see host information



Host Summary

Host IP
192.168.1.111

Status:	Inactive
Hostname:	user1-pc.lab10.com
Host Groups:	Catch All
Location:	RFC 1918
Last Seen:	--
Policies:	--
MAC Address:	00:0c:29:d7:15:2f *(VMware, Inc.)*

Quarantine
Unquarantine
Traffic by Peer Host Group (last 12 hours)
192.168.1.111
Alarms by Type (last 7 days)
Chart title
No data to display

Users & Sessions

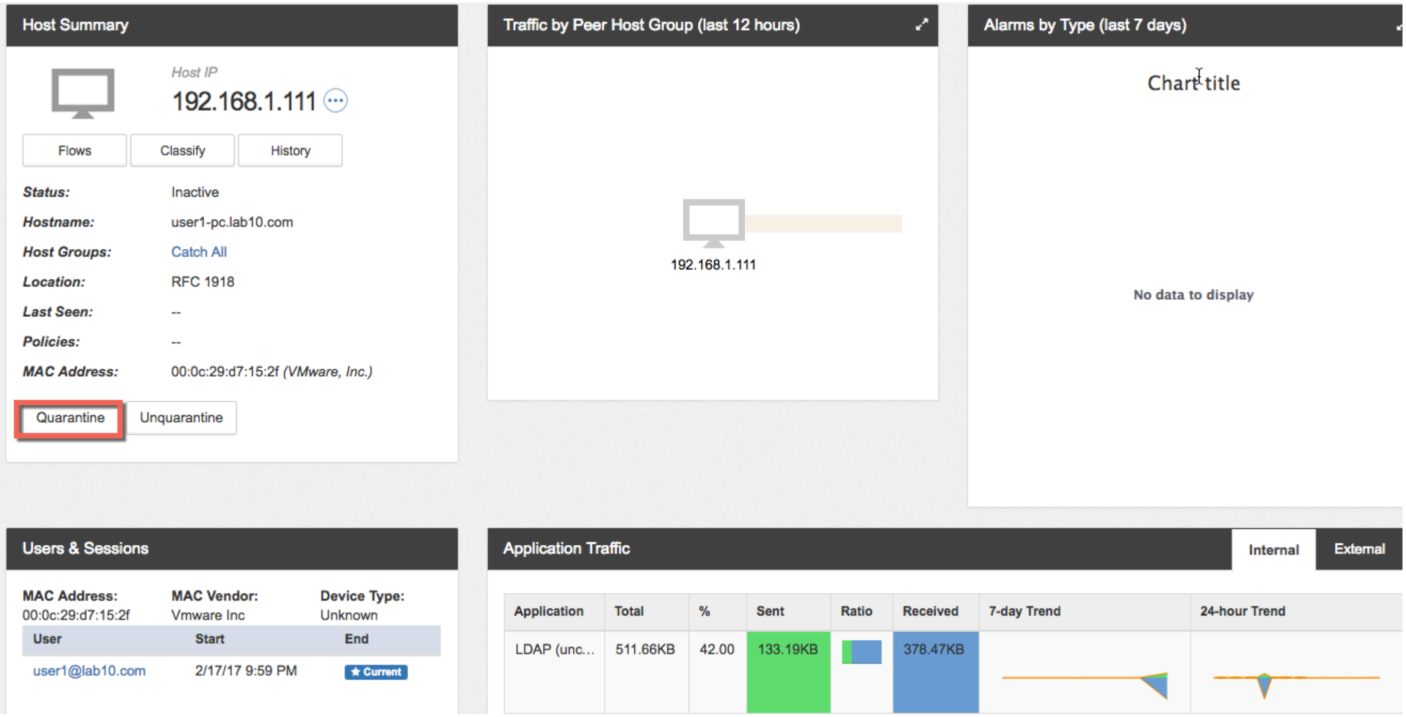
MAC Address: 00:0c:29:d7:15:2f
MAC Vendor: Vmware Inc
Device Type: Unknown

User	Start	End
user1@lab10.com	2/17/17 9:59 PM	★ Current

Application Traffic

Application	Total	%	Sent	Ratio	Received	7-day Trend	24-hour Trend
LDAP (unc...	511.66KB	42.00	133.19KB		378.47KB		

Step 6 Select Quarantine



Host Summary

Host IP
192.168.1.111

Status:	Inactive
Hostname:	user1-pc.lab10.com
Host Groups:	Catch All
Location:	RFC 1918
Last Seen:	--
Policies:	--
MAC Address:	00:0c:29:d7:15:2f *(VMware, Inc.)*

Quarantine
Unquarantine
Traffic by Peer Host Group (last 12 hours)
192.168.1.111
Alarms by Type (last 7 days)
Chart title
No data to display

Users & Sessions

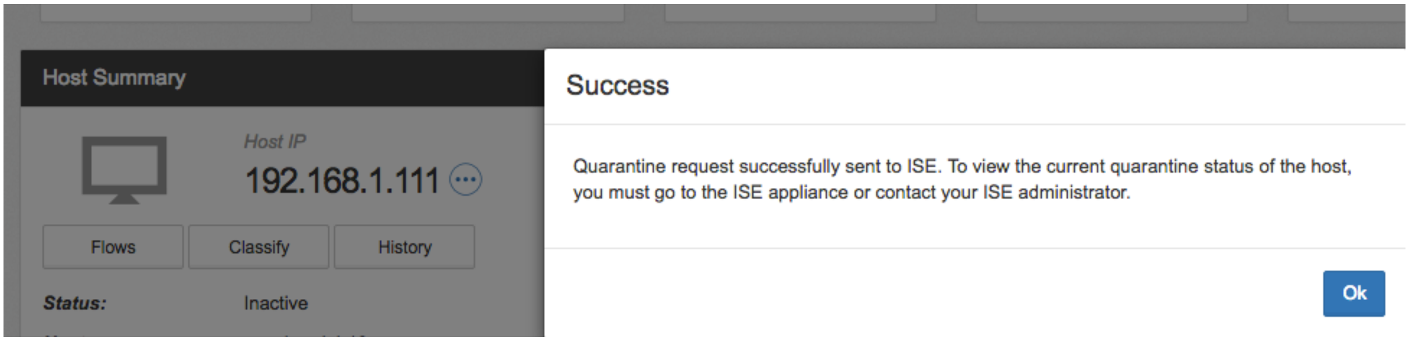
MAC Address: 00:0c:29:d7:15:2f
MAC Vendor: Vmware Inc
Device Type: Unknown

User	Start	End
user1@lab10.com	2/17/17 9:59 PM	★ Current

Application Traffic

Application	Total	%	Sent	Ratio	Received	7-day Trend	24-hour Trend
LDAP (unc...	511.66KB	42.00	133.19KB		378.47KB		

Step 7 You should see that the endpoint has been successful quarantined.



Host Summary

Host IP

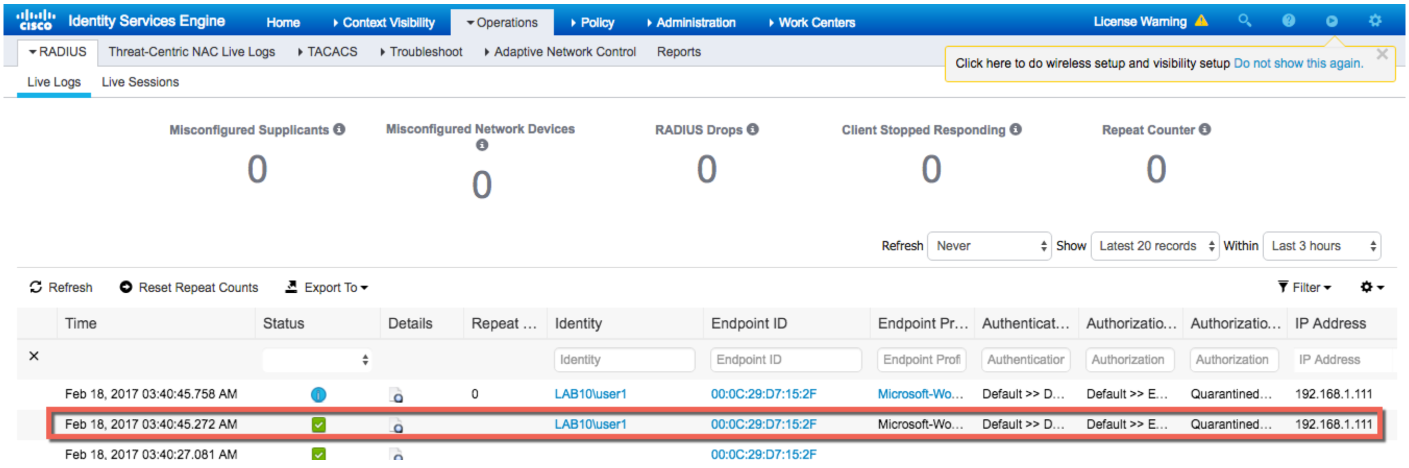
192.168.1.111

Status: Inactive

Success

Quarantine request successfully sent to ISE. To view the current quarantine status of the host, you must go to the ISE appliance or contact your ISE administrator.

Step 8 On ISE, select **Operations->RADIUS->Live Logs**



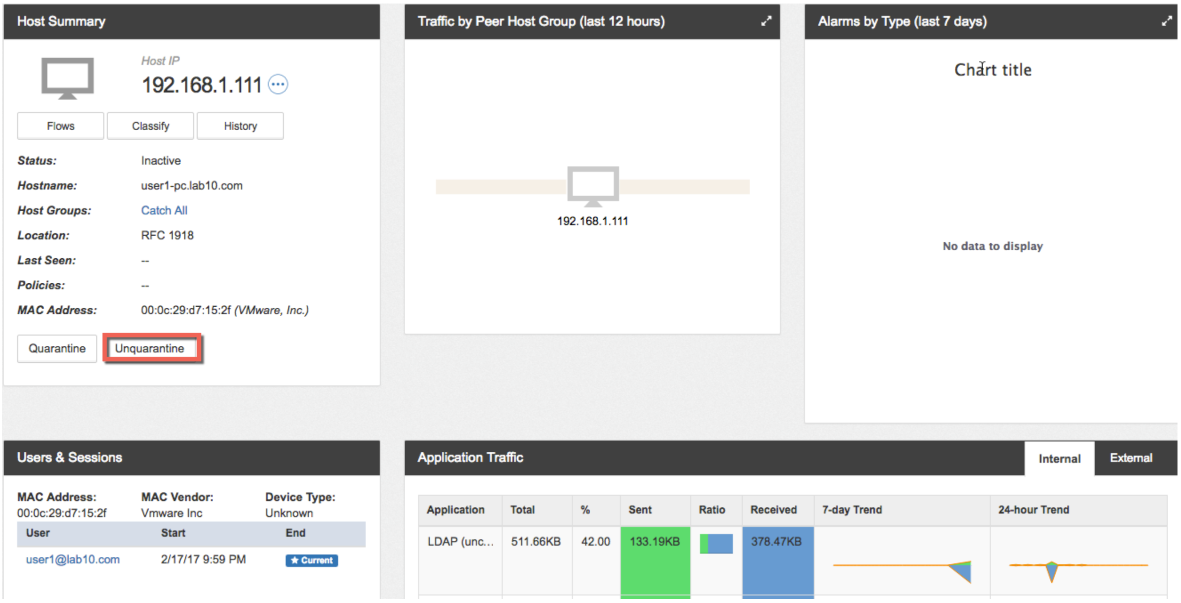
Click here to do wireless setup and visibility setup Do not show this again.

Misconfigured Supplicants	Misconfigured Network Devices	RADIUS Drops	Client Stopped Responding	Repeat Counter
0	0	0	0	0

Refresh: Never | Show: Latest 20 records | Within: Last 3 hours

Time	Status	Details	Repeat ...	Identity	Endpoint ID	Endpoint Pr...	Authenticat...	Authorizatio...	Authorizatio...	IP Address
×				Identity	Endpoint ID	Endpoint Profi	Authenticatior	Authorization	Authorization	IP Address
Feb 18, 2017 03:40:45.758 AM	●		0	LAB10\user1	00:0C:29:D7:15:2F	Microsoft-Wo...	Default >> D...	Default >> E...	Quarantined...	192.168.1.111
Feb 18, 2017 03:40:45.272 AM	✓			LAB10\user1	00:0C:29:D7:15:2F	Microsoft-Wo...	Default >> D...	Default >> E...	Quarantined...	192.168.1.111
Feb 18, 2017 03:40:27.081 AM	✓				00:0C:29:D7:15:2F					

Step 9 To unquarantine the endpoint, select **Unquarantine**



Host Summary

Host IP

192.168.1.111

Status: Inactive
Hostname: user1-pc.lab10.com
Host Groups: Catch All
Location: RFC 1918
Last Seen: --
Policies: --
MAC Address: 00:0c:29:d7:15:2f *(VMware, Inc.)*

Traffic by Peer Host Group (last 12 hours)

Alarms by Type (last 7 days)

Users & Sessions

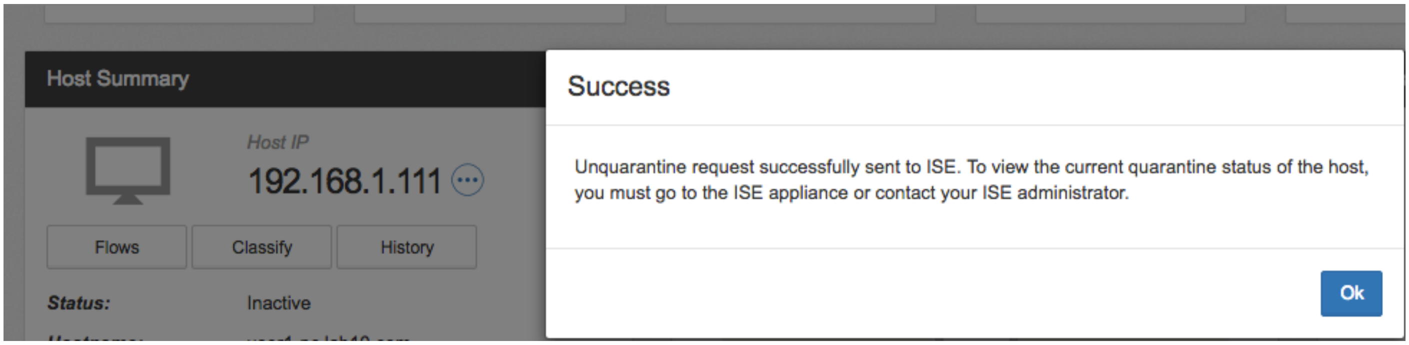
MAC Address: 00:0c:29:d7:15:2f
MAC Vendor: Vmware Inc
Device Type: Unknown

User	Start	End
user1@lab10.com	2/17/17 9:59 PM	★ Current

Application Traffic

Application	Total	%	Sent	Ratio	Received	7-day Trend	24-hour Trend
LDAP (unc...	511.66KB	42.00	133.19KB		378.47KB		

Step 10 You should see that the endpoint has been successfully unquarantined

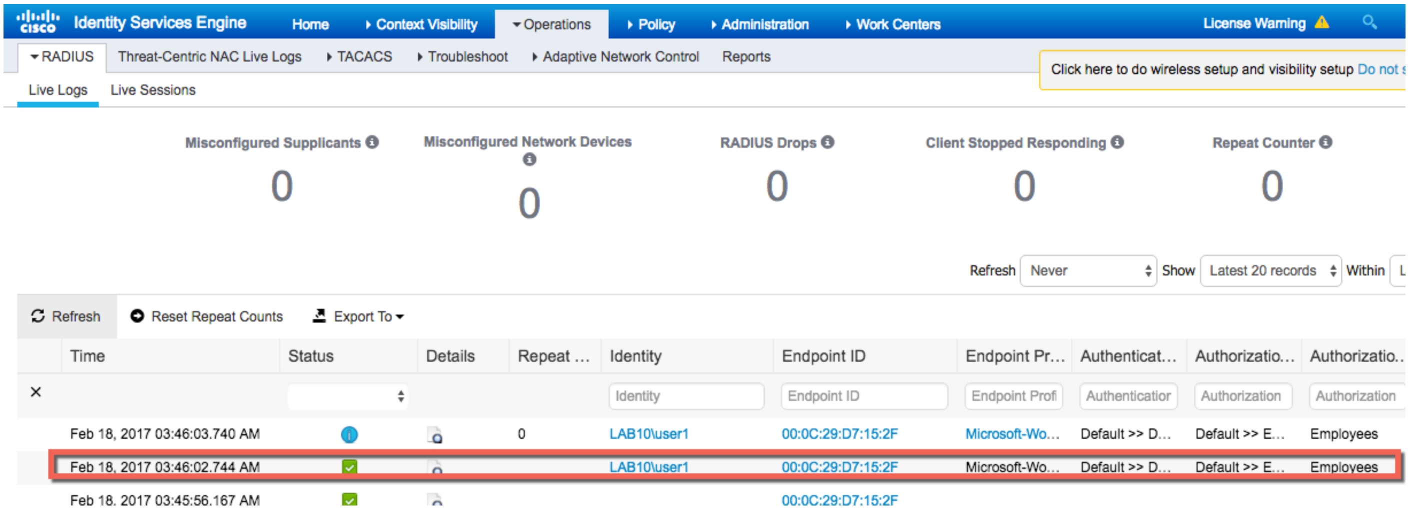


Status: Inactive

Success

Unquarantine request successfully sent to ISE. To view the current quarantine status of the host, you must go to the ISE appliance or contact your ISE administrator.

Step 11 On ISE, select **Operations->RADIUS->Live Logs**



Click here to do wireless setup and visibility setup Do not s

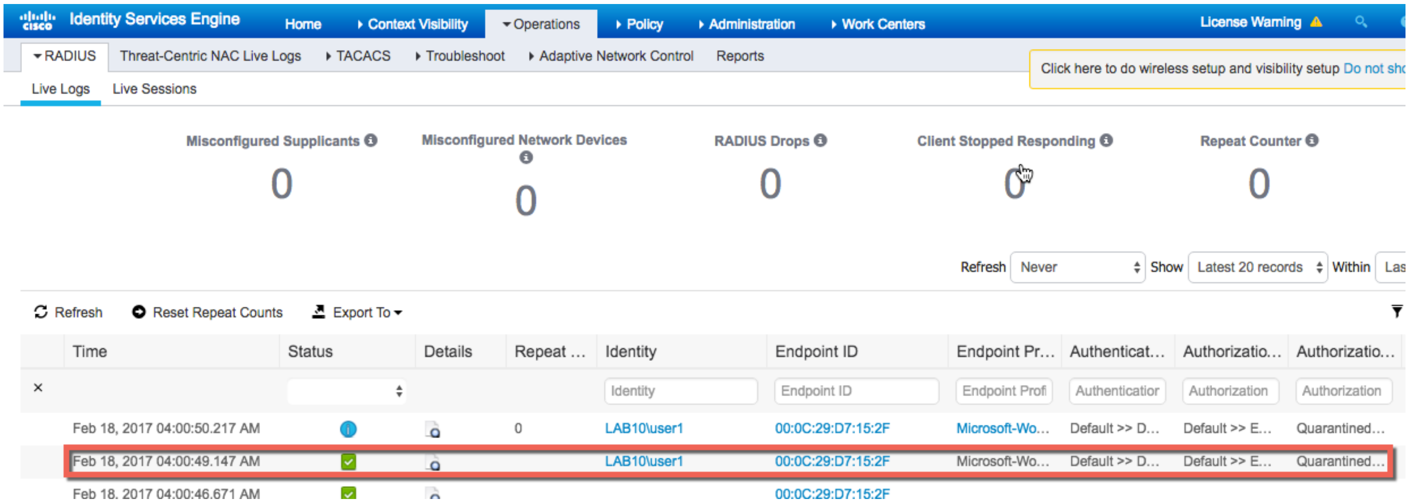
Misconfigured Supplicants	Misconfigured Network Devices	RADIUS Drops	Client Stopped Responding	Repeat Counter
0	0	0	0	0

Refresh Never Show Latest 20 records Within L

Time	Status	Details	Repeat ...	Identity	Endpoint ID	Endpoint Pr...	Authenticat...	Authorizatio...	Authorizatio..
Feb 18, 2017 03:46:03.740 AM	●		0	LAB10\user1	00:0C:29:D7:15:2F	Microsoft-Wo...	Default >> D...	Default >> E...	Employees
Feb 18, 2017 03:46:02.744 AM	✓			LAB10\user1	00:0C:29:D7:15:2F	Microsoft-Wo...	Default >> D...	Default >> E...	Employees
Feb 18, 2017 03:45:56.167 AM	✓				00:0C:29:D7:15:2F				

Unquarantine using ISE GUI

Step 1 Select **Operations->RADIUS->Live Logs**, you see the endpoint as quarantined



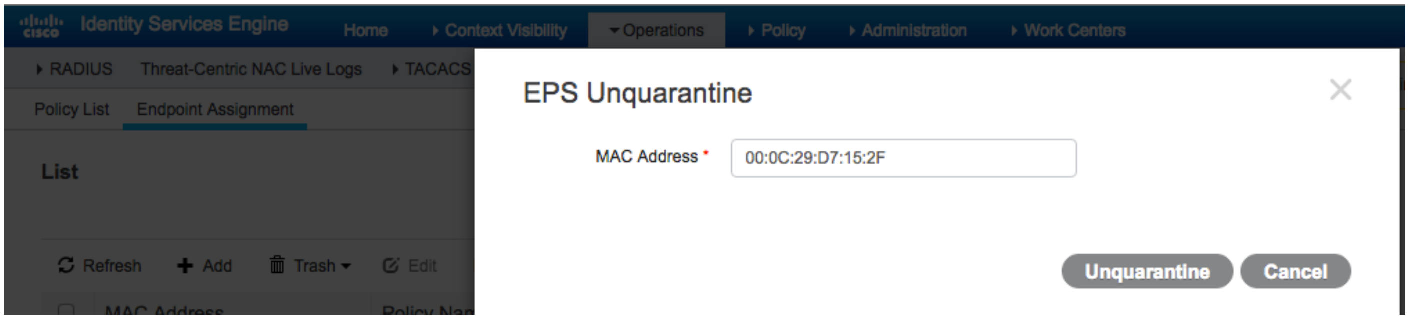
Click here to do wireless setup and visibility setup Do not sho

Misconfigured Supplicants	Misconfigured Network Devices	RADIUS Drops	Client Stopped Responding	Repeat Counter
0	0	0	0	0

Refresh Never Show Latest 20 records Within Las

Time	Status	Details	Repeat ...	Identity	Endpoint ID	Endpoint Pr...	Authenticat...	Authorizatio...	Authorizatio...
Feb 18, 2017 04:00:50.217 AM	●		0	LAB10\user1	00:0C:29:D7:15:2F	Microsoft-Wo...	Default >> D...	Default >> E...	Quarantined...
Feb 18, 2017 04:00:49.147 AM	✓			LAB10\user1	00:0C:29:D7:15:2F	Microsoft-Wo...	Default >> D...	Default >> E...	Quarantined...
Feb 18, 2017 04:00:46.671 AM	✓				00:0C:29:D7:15:2F				

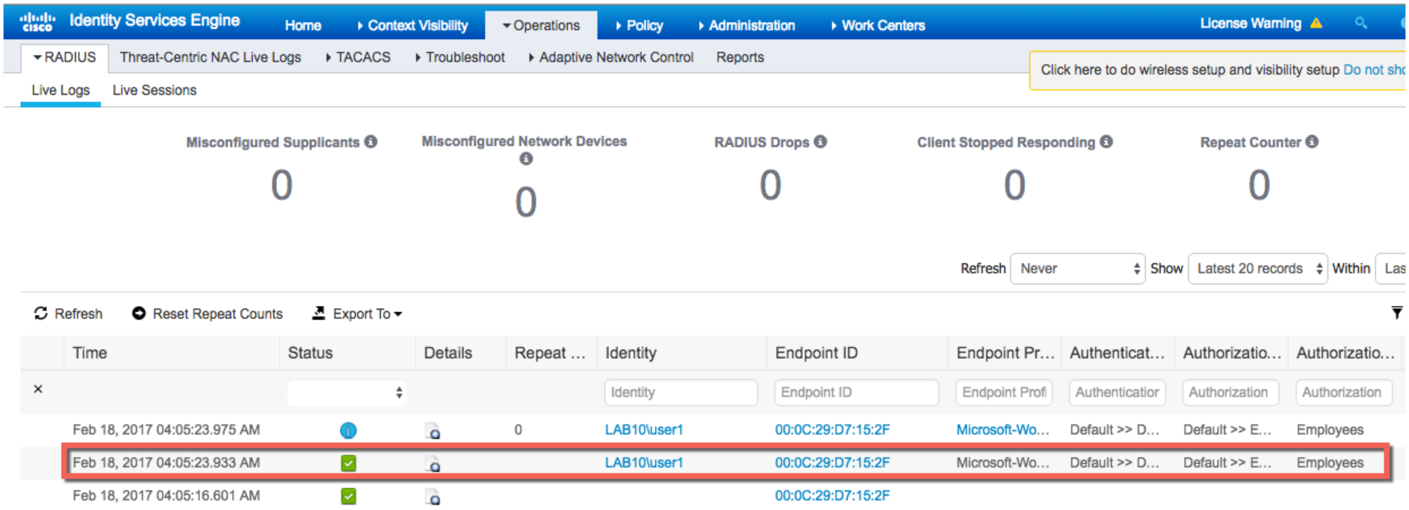
Step 2 Select **Operations->Adaptive Network Control->Endpoint Assignment->EPS Unquarantine** and enter the MAC address of the endpoint to unquarantine



EPS Unquarantine

MAC Address * 00:0C:29:D7:15:2F

Step 3 Select **Unquarantine,** the endpoint should be unquarantined



Click here to do wireless setup and visibility setup Do not sho

Misconfigured Supplicants	Misconfigured Network Devices	RADIUS Drops	Client Stopped Responding	Repeat Counter
0	0	0	0	0

Refresh Never Show Latest 20 records Within Las

Time	Status	Details	Repeat ...	Identity	Endpoint ID	Endpoint Pr...	Authenticat...	Authorizatio...	Authorizatio...
Feb 18, 2017 04:05:23.975 AM	●		0	LAB10\user1	00:0C:29:D7:15:2F	Microsoft-Wo...	Default >> D...	Default >> E...	Employees
Feb 18, 2017 04:05:23.933 AM	✓			LAB10\user1	00:0C:29:D7:15:2F	Microsoft-Wo...	Default >> D...	Default >> E...	Employees
Feb 18, 2017 04:05:16.601 AM	✓				00:0C:29:D7:15:2F				

Troubleshooting

Stealthwatch pxGrid configuration errors

Ensure that you have the ISE internal 2.2 certificate root services in the Stealthwatch Certificate Authority (CA) store, the external CA root certificate and intermediate certificates (if applicable), or ISE self-signed identity certificate + pxGrid certificate, pending your ISE configuration.