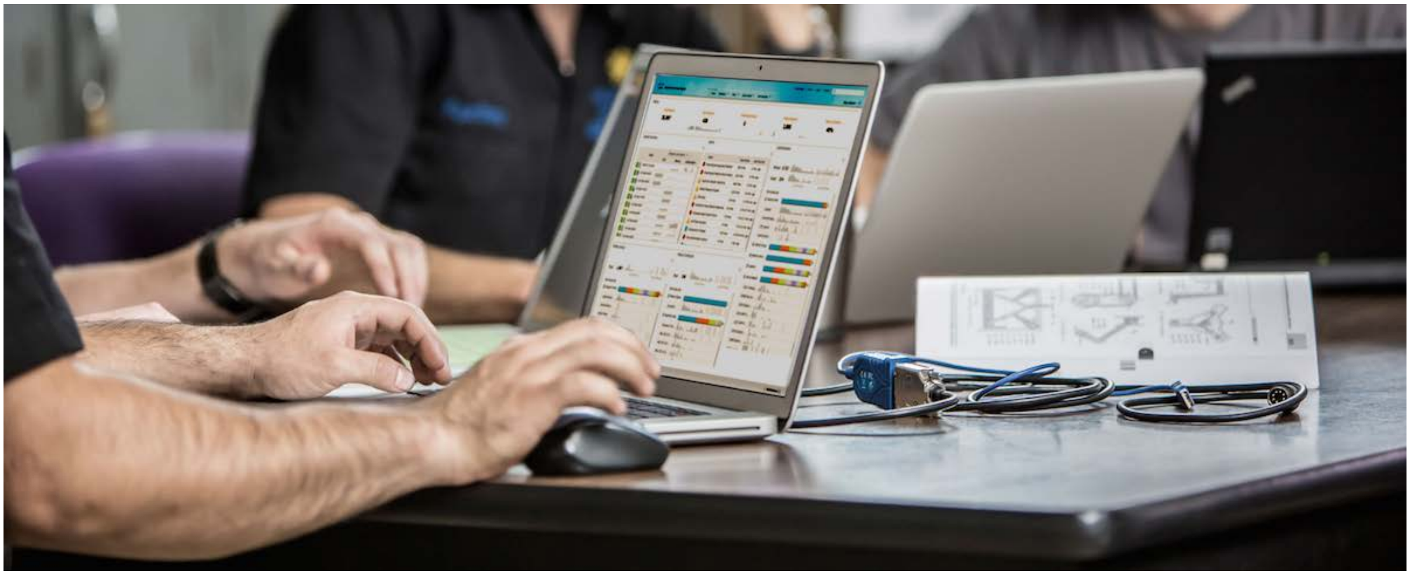


Deploying Cisco StealthWatch 6.7.1 with Cisco pxGrid

Table of Contents

About This Document

This document is intended for Cisco field engineers, technical marketing engineers, partners, and customers deploying Cisco StealthWatch 6.7.1 with Cisco platform exchange Grid (pxGrid) using Cisco Identity Service Engine (ISE) 1.3 or higher.

This document assumes that StealthWatch and ISE are already installed and provides the following:

- Customized pxGrid template creation for both the ISE pxGrid node and the SMC (StealthWatch Management Center)
- Configuring ISE for pxGrid node operation using either Certificate Authority (CA)-signed certificates or self-signed certificates
- Configuring the StealthWatch Management Console (SMC) as a pxGrid client using either Certificate Authority (CA)-signed certificates or self-signed certificates.
- Configuring the StealthWatch Management Center (SMC) for Cisco (Adaptive Network Control) ANC pxGrid mitigation action.

Please note that ISE was deployed in a Stand-alone environment with pxGrid enabled.

If deploying pxGrid in a production environment using CA-signed certificates please see: Configuring pxGrid in an ISE Distributed Environment: http://www.cisco.com/c/en/us/support/security/identity-services-engine/products-implementation-design-guides-list.html

Introduction

Cisco StealthWatch is a network security solution providing real-time visibility into network and user traffic detecting anomalous behavior, APTs, insider threats, DDoS and other malware. Lancope also collects and analyzes holistic network trails and responds to these threats before during and after an incident request performing mitigation actions on these endpoints in real-time.

Cisco Platform Exchange Grid (pxGrid) is a unified framework that enables ecosystem partners to obtain user and device contextual information from Cisco's Identity Service Engine (ISE). ISE publishes topics of information and ecosystem partners subscribes to these published topics, obtaining ISE session information and taking Adaptive Network Control (ANC) mitigation actions on endpoints.

Cisco StealthWatch, registers to the ISE pxGrid node as a client and subscribes to the EndpointProtectionService capability and performs ANC mitigation actions on the endpoint. These mitigation actions in include quarantining/un-quarantining and a IEEE 802.1X endpoint authenticated by ISE.

This document assumes that StealthWatch 6.7.1 or higher and ISE 1.3 or higher have been installed.

StealthWatch as a pxGrid client requires either Certificate Authority (CA)-signed certificate, or a self-signed certificate to be used for pxGrid operation. Both certificate use cases are covered.

- A signed certificate use case includes importing the CA trusted root certificate, and generating a public key pair on the SMC, to be signed by the same CA that signed the ISE pxGrid node certificate. It is assumed that the CA root certificate has been installed in the ISE trusted system certificate store and the pxGrid ISE node certificate has been installed in the ISE system certificate store

- The self-signed certificate use case steps through the complete ISE pxGrid node configuration and self-signed public or private key SMC creation.

- In StealthWatch 6.7.1 the identity certificate must be uploaded to the Client Identity SSL store for pxGrid operation.

Both use cases include SMC mitigation action configuration and examples.

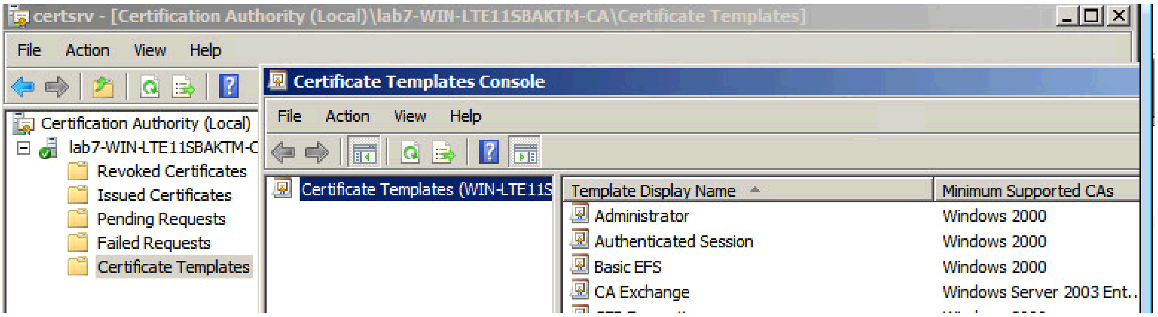
Using CA-Signed Certs for SMC and ISE pxGrid Node

This section takes you through the steps for implementing CA-signed certs on the SMC and for using the java client.

Customized pxGrid Template for CA-Signed Operation

A customized pxGrid template having an Enhanced Key Usage (EKU) of both client authentication and server authentication is required for pxGrid operation between the pxGrid client, the SMC, and the ISE pxGrid node. This is required for a Certificate Authority (CA)-signed environment where both the SMC and the ISE pxGrid node are signed by the same CA.

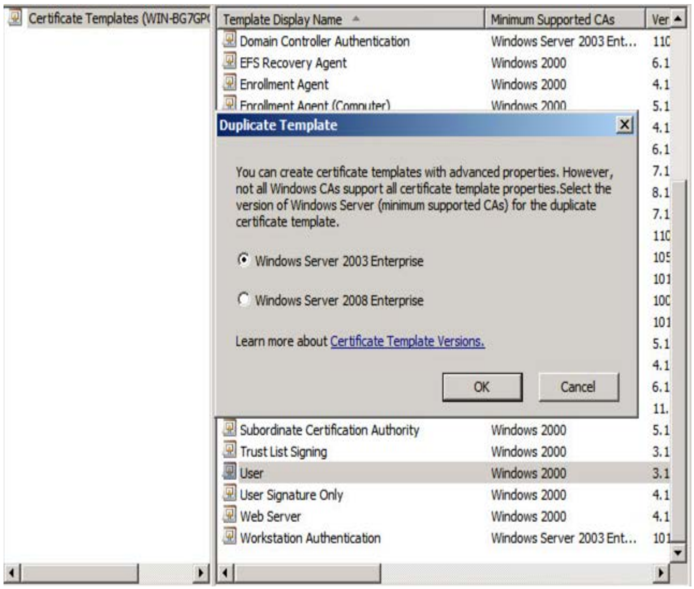
Step 1 Select **Administrative Tools->Certificate Authority-> "+" dropdown next to CA server->Right-Click on Certificate Templates->Manage**



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**



Template Display Name	Minimum Supported CAs	Ver
Domain Controller Authentication	Windows Server 2003 Ent...	11C
EFS Recovery Agent	Windows 2000	6.1
Enrollment Agent	Windows 2000	4.1
Enrollment Agent (Computer)	Windows 2000	5.1
		4.1
		6.1
		7.1
		8.1
		7.1
		11C
		105
		101
		10C
		101
		5.1
		4.1
		6.1
		11.
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

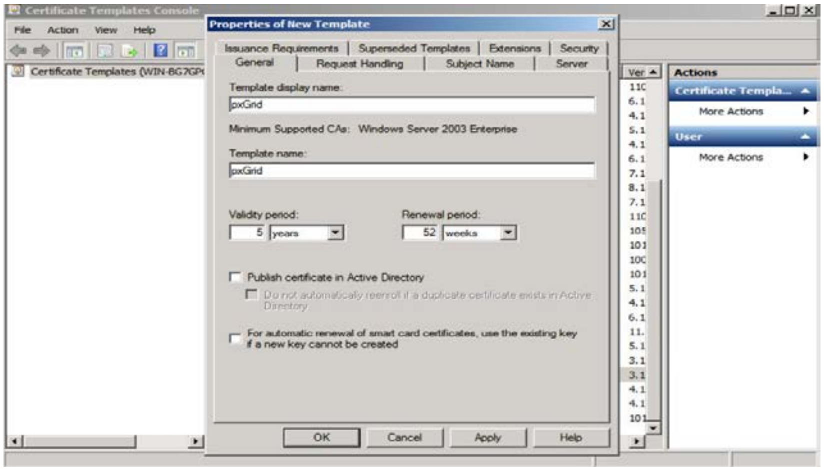
You can create certificate templates with advanced properties. However, not all Windows CAs support all certificate template properties.Select the version of Windows Server (minimum supported CAs) for the duplicate certificate template.

● 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

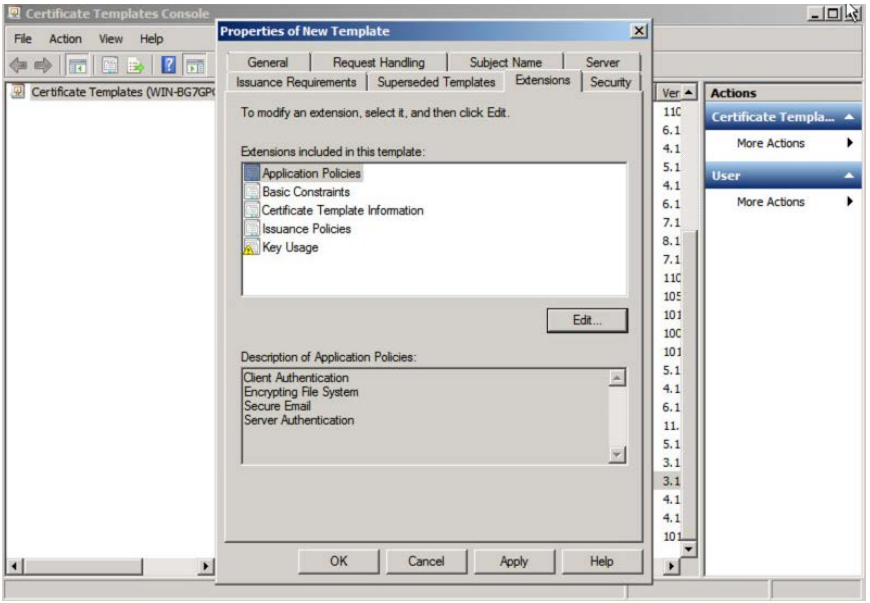
Renewal period: 52 weeks

□ 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.

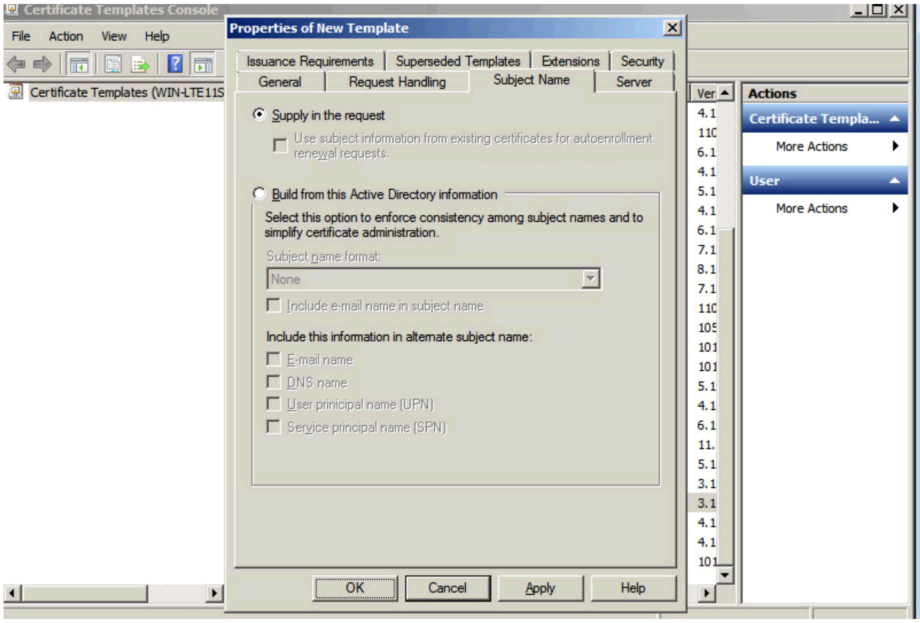
Extensions included in this template:

- 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:

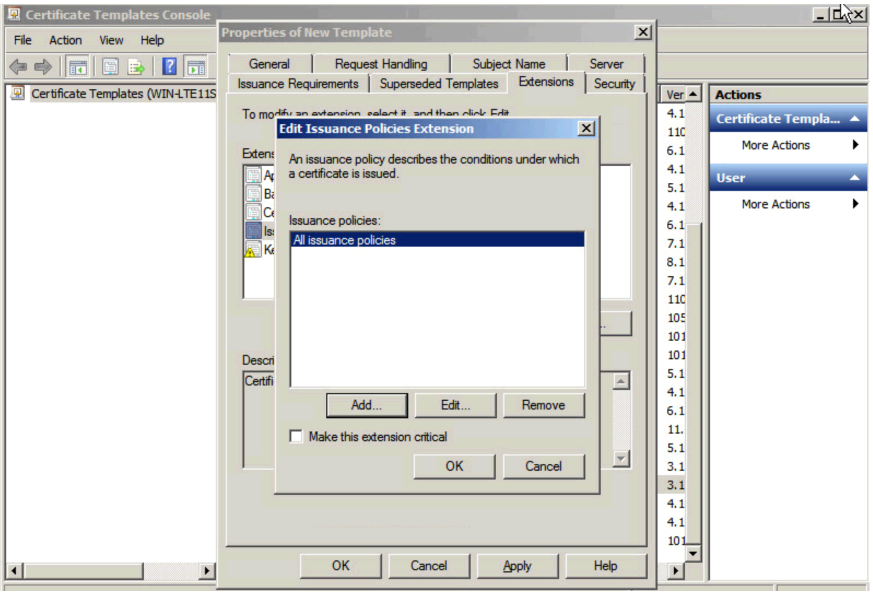
□ E-mail name

□ DNS name

□ User principal name (UPN)

□ Service principal name (SPN)

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

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

Edit Issuance Policies Extension

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

Issuance policies:

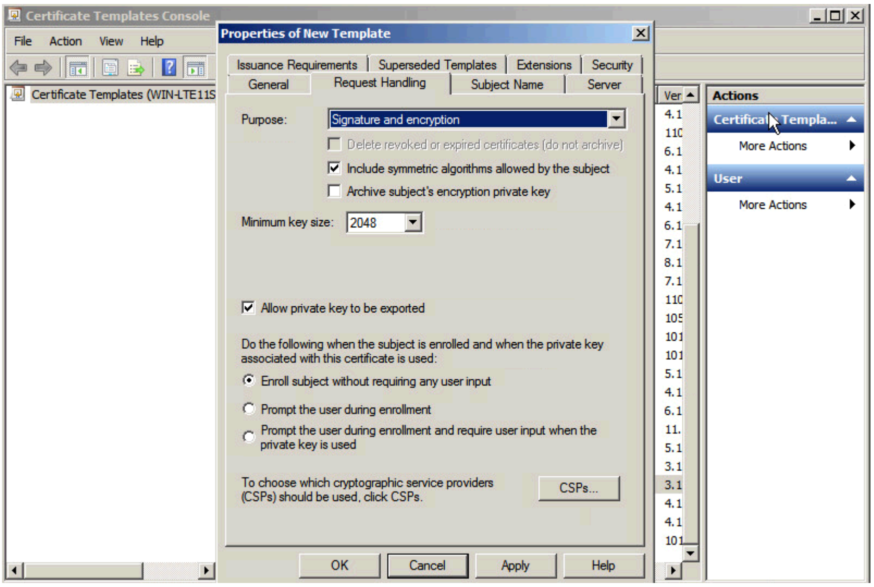
All issuance policies

Add... Edit... Remove

□ Make this extension critical

OK Cancel

Step 7 Leave the defaults for request handling



Properties of New Template

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

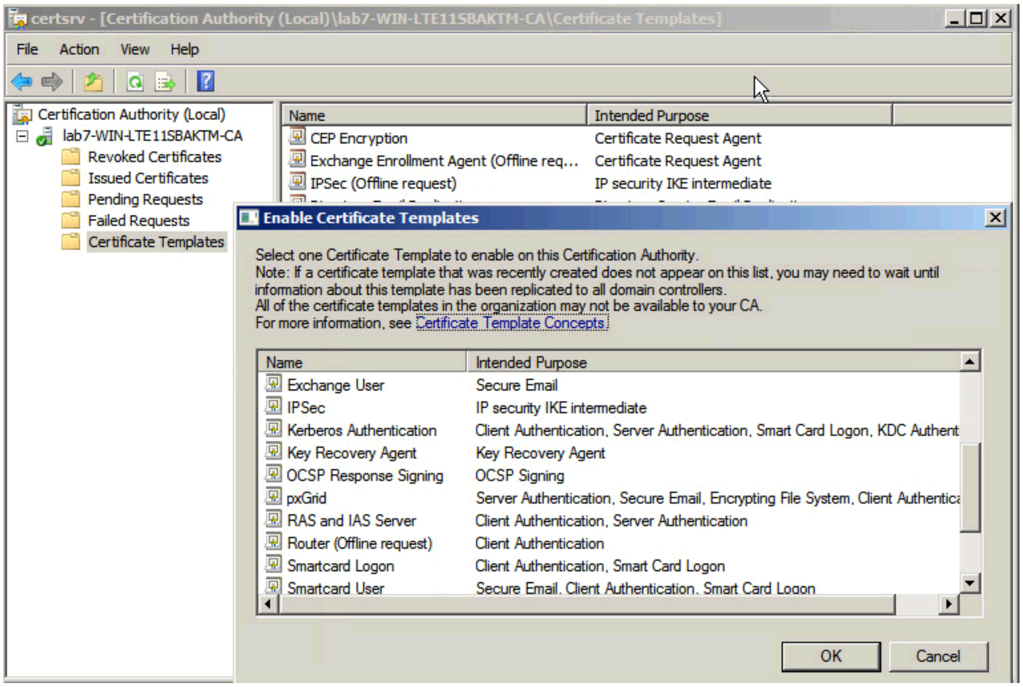
○ Prompt the user during enrollment

○ 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]

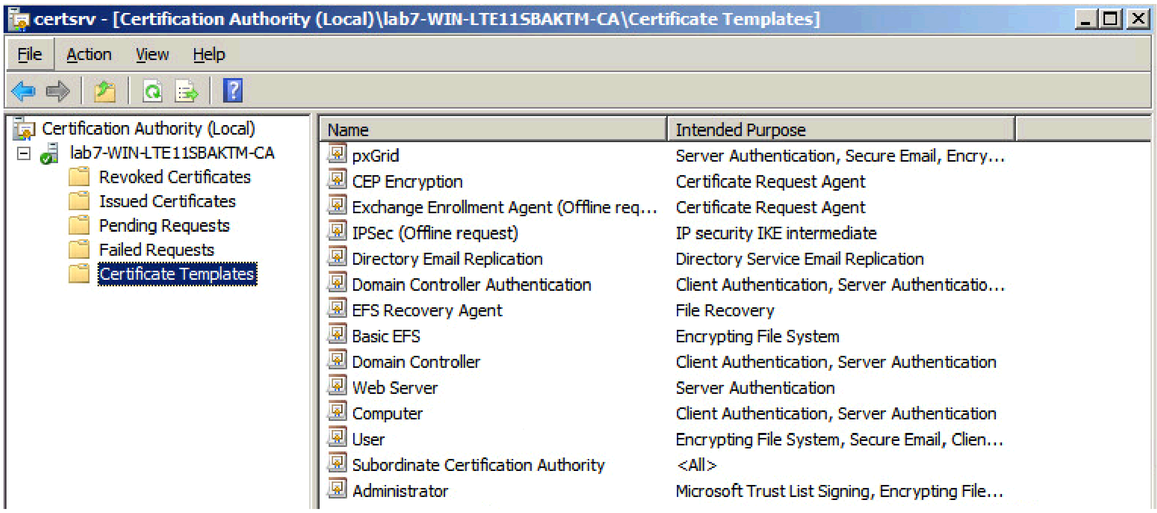
Name	Intended Purpose
CEP Encryption	Certificate Request Agent
Exchange Enrollment Agent (Offline req...	Certificate Request Agent
IPSec (Offline request)	IP security IKE intermediate

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

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...

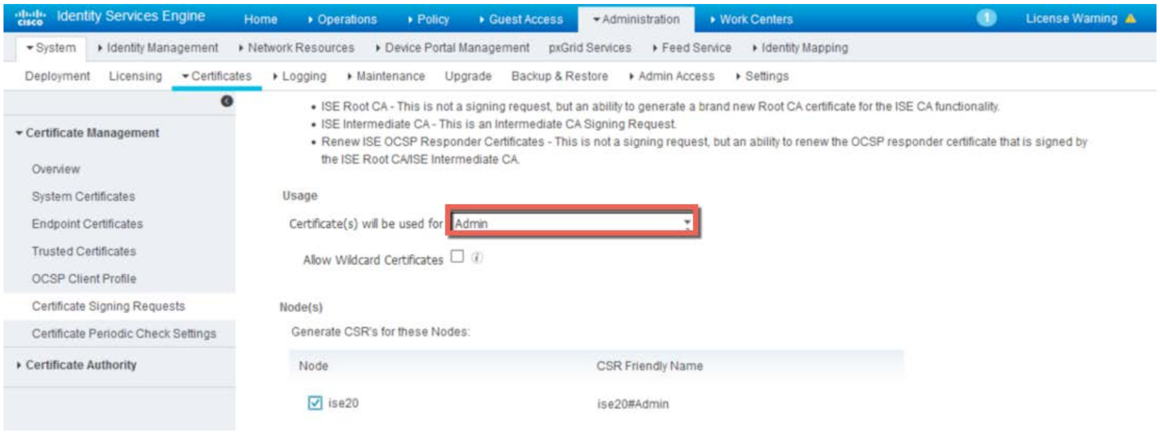
Configuring ISE 2.0

The ISE pxGrid node is configured for a Certificate Authority (CA) signed environment in a stand-alone configuration. Initially, a “pxGrid” CSR request is generated from the ISE node and signed by the CA server using the pxGrid customized template. The certificate will be bound to the initial ISE CSR request.

The CA root certificate will be imported into the ISE certificate trusted store. The ISE identity certificate will be exported in the ISE certificate system store. The ISE node will be enabled for pxGrid operation.

Step 1 Generate a CSR request for the ISE node which will become the ISE pxGrid node **Administration->System->Certificates->Certificate Signing Requests->Generate**

Note: The certificate usage should be admin. This is required for FMC 6.0 for active bulk download sessions



- 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

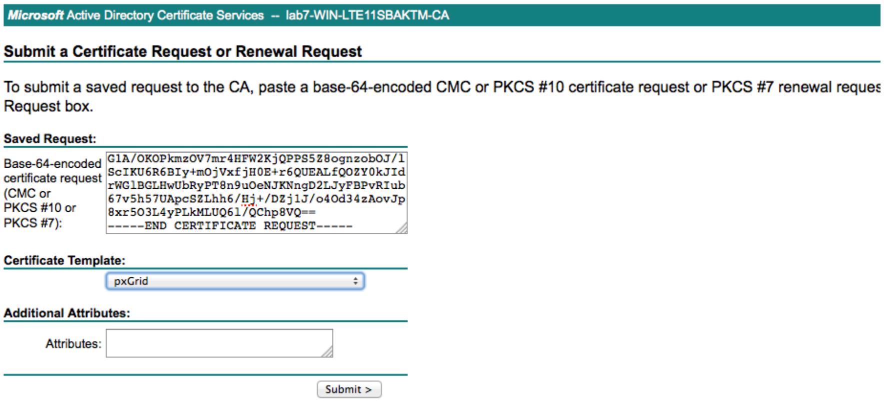
Allow Wildcard Certificates ☐

Node(s)

Generate CSR's for these Nodes:

Node	CSR Friendly Name
☑ ise20	ise20#Admin

Step 2 Copy/paste the CSR information into **Request a certificate**->**Advanced certificate request** selecting the customized pxGrid template, then **Submit**



Microsoft Active Directory Certificate Services -- lab7-WIN-LTE11SBAKTM-CA

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request or PKCS #7 renewal reques
Request box.

Saved Request:

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

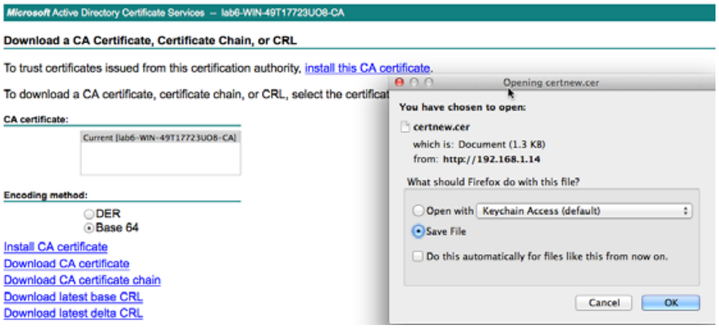
```
G1A/OKOPkmzOV7mr4HFW2KjQPPS5Z8ognzobOJ/l
ScIKU6R6BIy+mOjVxfjH0E+r6QUEALfQOZY0kJId
rWGlBGLHwUbRyPT8n9uOeNJKNngD2LJyFBPvRIub
67v5h57UApcSZLhh6/Hj+/DZj1J/o40d34zAovJp
8xr5O3L4yPLkMLUQ61/QChp8VQ==
-----END CERTIFICATE REQUEST-----
```

Certificate Template: pxGrid

Additional Attributes:

Attributes:

Step 3 Download the CA root in base-64 encoded format



Microsoft Active Directory Certificate Services -- lab6-WIN-49T17723UO8-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 certificat

CA certificate: Current [lab6-WIN-49T17723UO8-CA]

Encoding method:

○ DER
● Base 64

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

Opening certnew.cer

You have chosen to open:

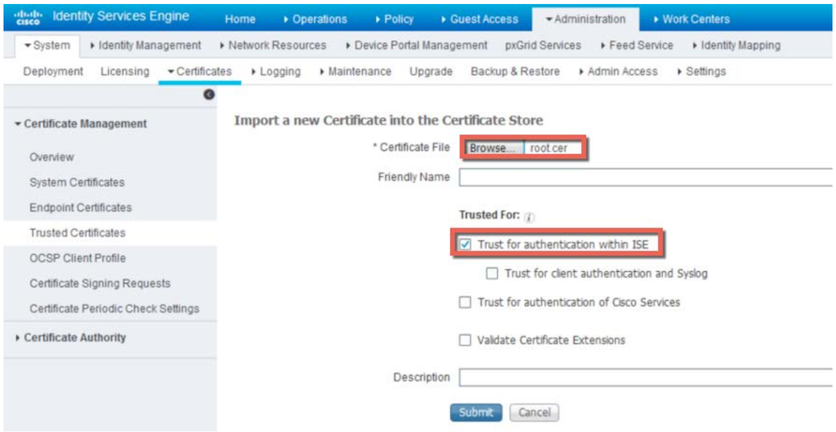
certnew.cer
which is: Document (1.3 KB)
from: http://192.168.1.14

What should Firefox do with this file?

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

Step 4 Upload the CA root into the ISE certificate trusted system store
Select **Administration->System->Certificates->Trusted Certificates->upload the CA root certificate**

Step 5 **Enable "Trust for authentication within ISE",** then **Submit**



Import a new Certificate into the Certificate Store

* Certificate File: Browse... root.cer

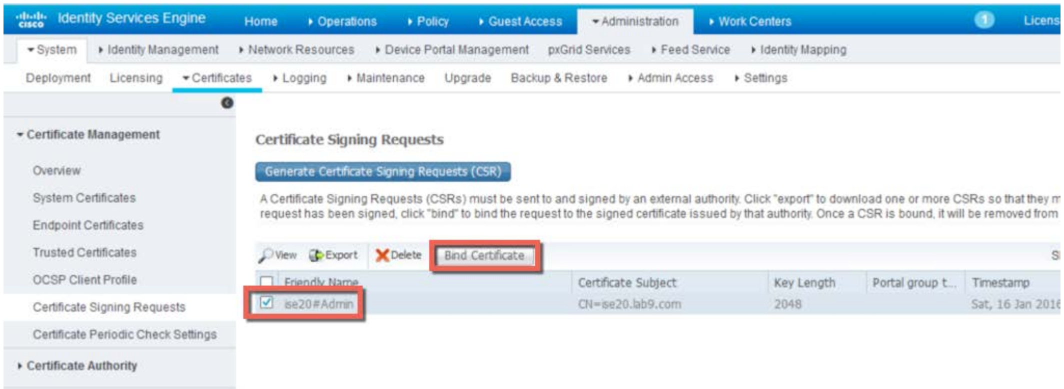
Friendly Name:

Trusted For:

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

Description:

Step 6 Upload the ISE pxGrid node certificate into the ISE certificate system store
Select **Administration->System-Certificate Signing Requests and Bind certificate to the CSR request**



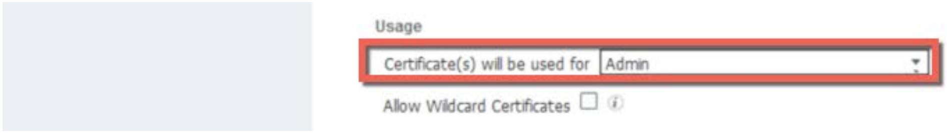
Certificate Signing Requests

Generate Certificate Signing Requests (CSR)

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 m
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

□	Friendly Name	Certificate Subject	Key Length	Portal group t...	Timestamp
☑	ise20#Admin	CN=ise20.lab9.com	2048		Sat, 16 Jan 2016

Step 7 Select **Administration->System->Certificates->Certificate Management->Certificate Signing Request->Generate Certificate Signing Requests (CSR)->Admin for certificate usage**



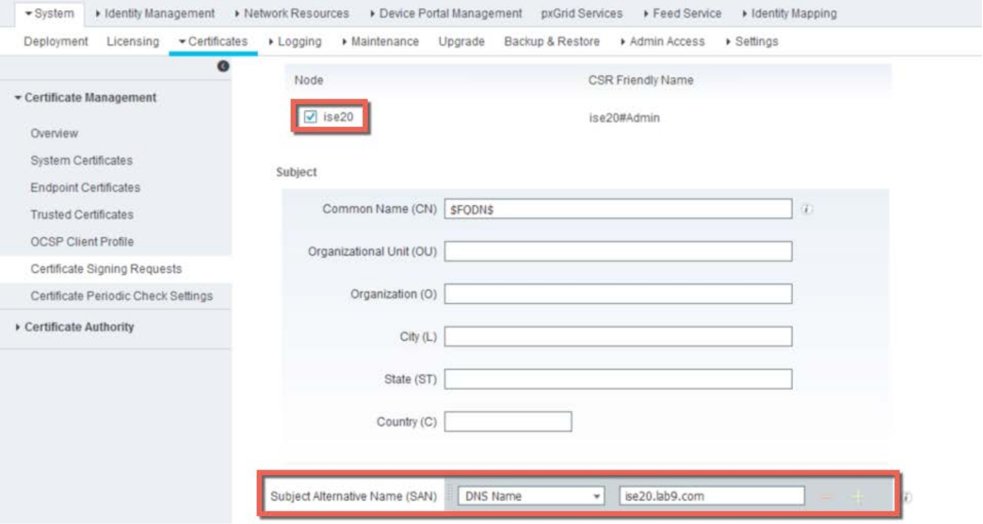
Usage

Certificate(s) will be used for: Admin

Allow Wildcard Certificates □

Step 8 Select **Node**

Step 9 Select DNS name for the Subject Alternative Name (SAN**)** and add the DNS name



Node	CSR Friendly Name
☑ ise20	ise20#Admin

Subject

Common Name (CN): $FQDN$

Organizational Unit (OU):

Organization (O):

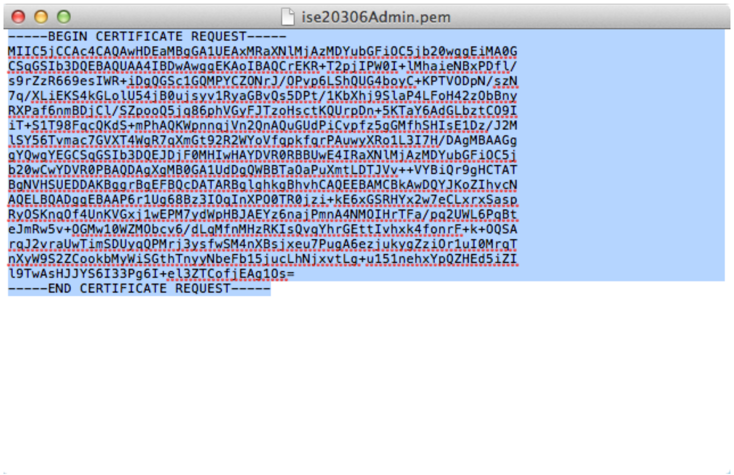
City (L):

State (ST):

Country (C):

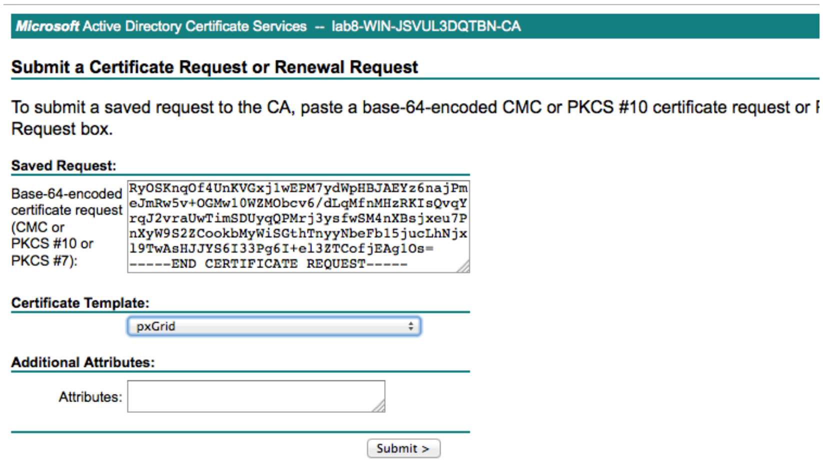
Subject Alternative Name (SAN): DNS Name ise20.lab9.com

Step 10 Select **Generate**
Step 11 Select **Export**
Step 12 Open the pem file and copy or paste the csr request into the customized pxGrid template



```
-----BEGIN CERTIFICATE REQUEST-----
MIIC5jCCAc4CAQAwHDEaMBgGA1UEAxMRaXNlMjAzMDYubGFiOC5jb20wggEiMA0G
CSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCrEKR+T2pjIPW0I+lMhaieNBxPDfl/
s9rZzR669esIWR+iDgQGSc1GQMPYCZONrJ/OPvp6LShQUG4boyC+KPTVODpN/szN
7q/XLiEKS4kGLolU54jB0ujsyv1RyaGBvQs5DPt/1KbXhj9SlaP4LFoH42zObBny
RXPaf6nmBDjCl/SZpooQ5jq86phVGyFJTzoHsctKQUrpDn+5KTaY6AdGLbztCO9I
iT+S1T98FqcQKdS+mPhAQKWpnnqjVn2QnAQuGUdPiCvpfz5gGMfhSHIsE1Dz/J2M
lSY56Tvmac7GVXT4WgR7qXmGt92R2WYoVfqpkfqrPAuwyXRo1L3I7H/DAgMBAAGg
gYQwgYEGCSqGSIb3DQEJDjF0MHIwHAYDVR0RBBUwE4IRaXNlMjAzMDYubGFiOC5j
b20wCwYDVR0PBAQDAgXgMB0GA1UdDgQWBBTaOaPuXmtLDTJVv++VYBiQr9gHCTAT
BgNVHSUEDDAKBggrBgEFBQcDATARBglghkgBhvhCAQEEBAMCBkAwDQYJKoZIhvcN
AQELBQADggEBAAP6r1Ug68Bz3IOqInXPO0TR0jzi+kE6xGSRHYx2w7eCLxrxSasp
RyOSKnqOf4UnKVGxj1wEPM7ydWpHBJAEYz6najPmnA4NMOIHrTFa/pq2UWL6PqBt
eJmRw5v+OGMw10WZMObcv6/dLqMfnMHzRKIsQvqYhrGEttIvhxk4fonrF+k+OQSA
rqJ2vraUwTimSDUyqQPMrj3ysfwSM4nXBsjxeu7PugA6ezjukygZziOr1uI0MrqT
nXyW9S2ZCookbMyWiSGthTnyyNbeFb15jucLhNjxvtLg+u151nehxYpQZHEd5iZI
l9TwAsHJJYS6I33Pg6I+el3ZTCofjEAg1Os=
-----END CERTIFICATE REQUEST-----
```

Step 13 Paste into Request a **Certificate->Advanced Certificate Request**, select **customized pxGrid template->Submit**



Microsoft Active Directory Certificate Services -- lab8-WIN-JSVUL3DQTBN-CA

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request or F Request box.

Saved Request:

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

```
RyOSKnqOf4UnKVGxj1wEPM7ydWpHBJAEYz6najPm
eJmRw5v+OGMw10WZMObcv6/dLqMfnMHzRKIsQvqY
rqJ2vraUwTimSDUyqQPMrj3ysfwSM4nXBsjxeu7P
nXyW9S2ZCookbMyWiSGthTnyyNbeFb15jucLhNjx
l9TwAsHJJYS6I33Pg6I+el3ZTCofjEAg1Os=
-----END CERTIFICATE REQUEST-----
```

Certificate Template:

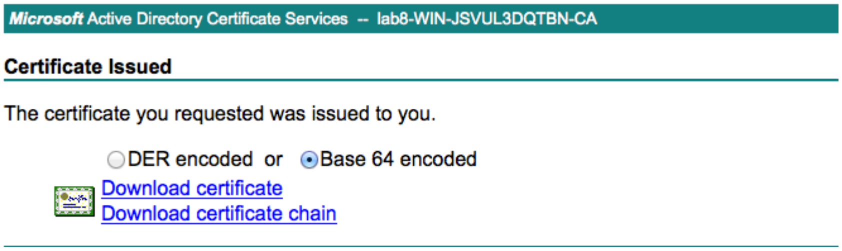
pxGrid

Additional Attributes:

Attributes:

Step 14 Select **Submit**

Step 15 Download certificate in base 64 encoded format



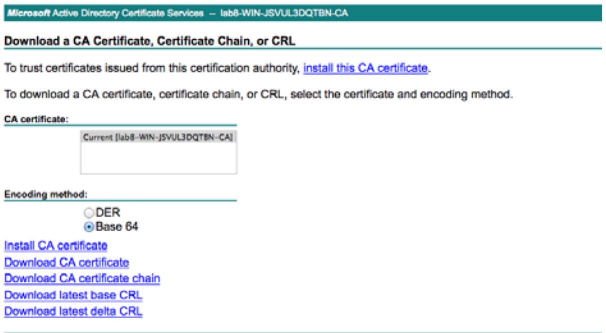
Microsoft Active Directory Certificate Services -- lab8-WIN-JSVUL3DQTBN-CA

Certificate Issued

The certificate you requested was issued to you.

○ DER encoded or ● Base 64 encoded

Step 16 Download CA root certificate in Base 64 format



Microsoft Active Directory Certificate Services -- lab8-WIN-JSVUL3DQTBN-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 [lab8-WIN-JSVUL3DQTBN-CA]

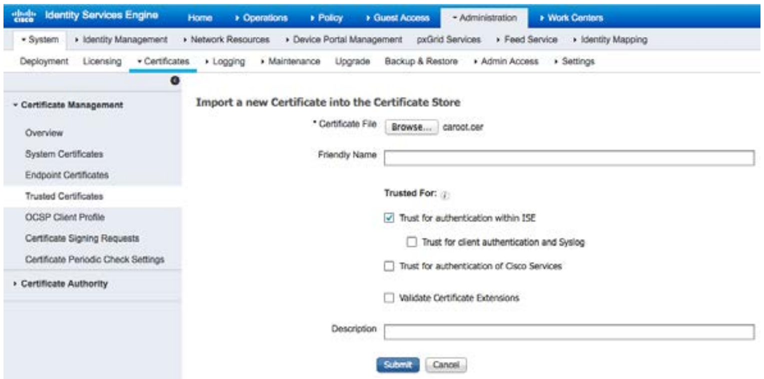
Encoding method:

○ DER
● Base 64

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

Step 17 **Administration System->Certificates->Certificate Management->Trusted Certificates->Import the root certificate**

Step 18 **Enable Trust for authentication within ISE**



Import a new Certificate into the Certificate Store

* Certificate File: Browse... caroot.cer

Friendly Name:

Trusted For:

☑ Trust for authentication within ISE

☐ Trust for client authentication and Syslog

☐ Trust for authentication of Cisco Services

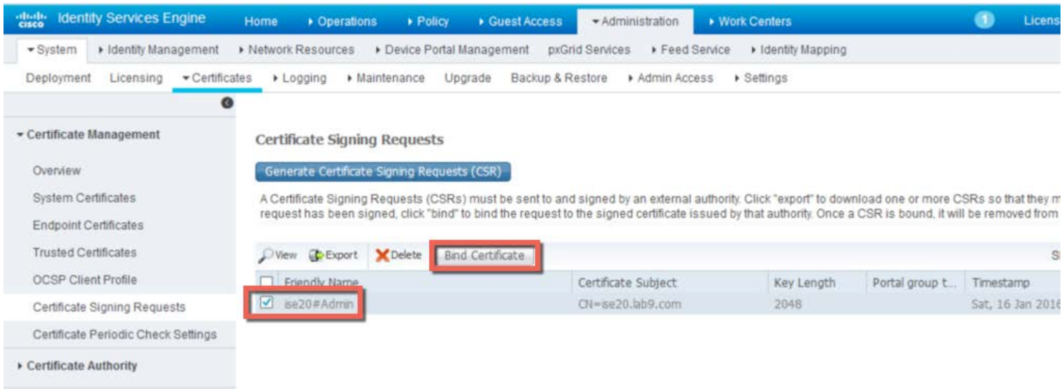
☐ Validate Certificate Extensions

Description:

Submit Cancel

Step 19 Select **Submit**

Step 20 Select **Administration->Certificates->Certificate Management->System Certificates->Certificate Signing Requests->select CSR request->Bind Certificate**



Certificate Signing Requests

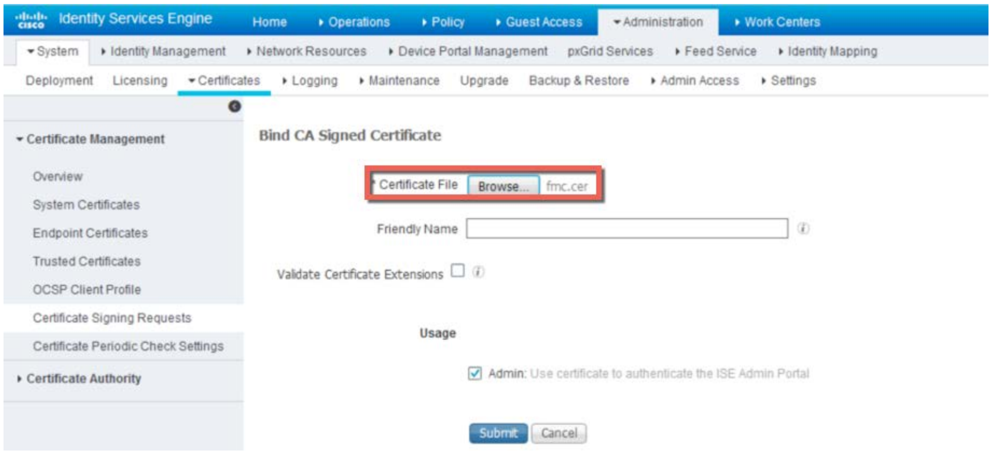
Generate Certificate Signing Requests (CSR)

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 m
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

View Export Delete Bind Certificate S

☐ Friendly Name	Certificate Subject	Key Length	Portal group t...	Timestamp
☑ ise20#Admin	CN=ise20.lab9.com	2048		Sat, 16 Jan 2016

Step 21 Upload the ISE CA-signed identity certificate



Bind CA Signed Certificate

* Certificate File Browse... fmc.cer

Friendly Name

Validate Certificate Extensions □

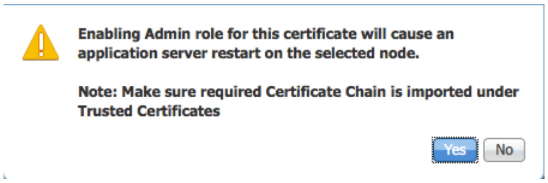
Usage

☑ Admin: Use certificate to authenticate the ISE Admin Portal

Submit Cancel

Step 22 Select **Submit**

Step 23 Select **Yes**, when you see the following message:

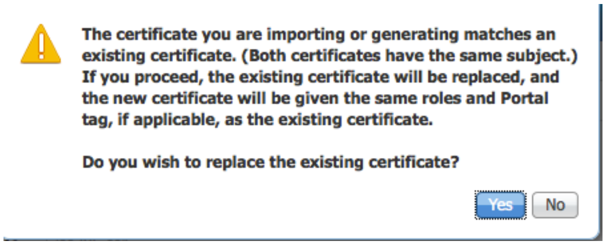


Enabling Admin role for this certificate will cause an application server restart on the selected node.

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

Yes No

Step 24 Select **Yes**, when you see the following message

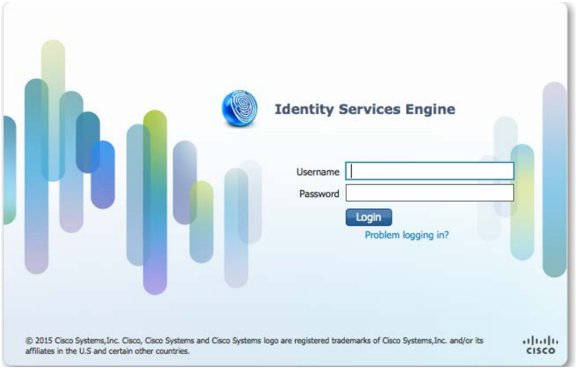


The certificate you are importing or generating matches an existing certificate. (Both certificates have the same subject.) If you proceed, the existing certificate will be replaced, and the new certificate will be given the same roles and Portal tag, if applicable, as the existing certificate.

Do you wish to replace the existing certificate?

Yes No

Step 25 The system will restart, and return to the GUI



Identity Services Engine

Username

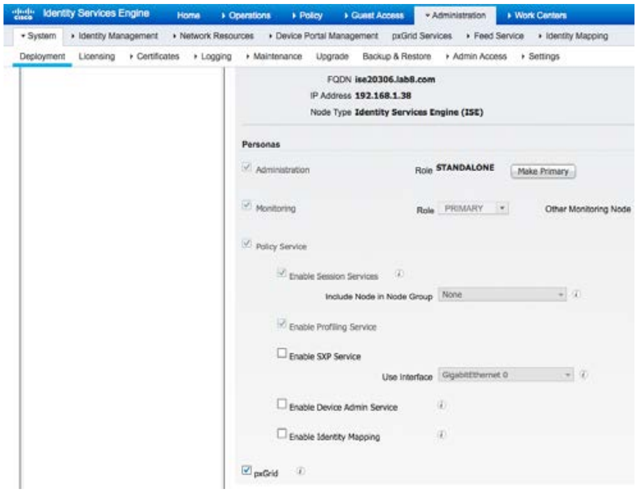
Password

Login

Problem logging in?

© 2015 Cisco Systems,Inc. Cisco, Cisco Systems and Cisco Systems logo are registered trademarks of Cisco Systems,Inc. and/or its affiliates in the U.S and certain other countries.

Step 26 Select **Administration->System->Deployment->edit the Hostname->enable pxGrid**



FQDN **ise20306.lab8.com**
IP Address **192.168.1.38**
Node Type **Identity Services Engine (ISE)**

Personas

☑ Administration Role **STANDALONE** Make Primary

☑ Monitoring Role PRIMARY Other Monitoring Node

☑ Policy Service

☑ Enable Session Services

Include Node in Node Group None

☑ Enable Profiling Service

□ Enable SXP Service

Use Interface GigabitEthernet 0

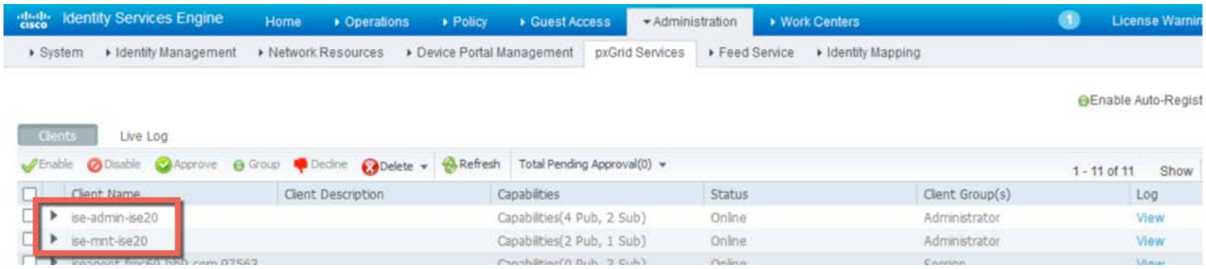
□ Enable Device Admin Service

□ Enable Identity Mapping

☑ pxGrid

Step 27 Select **Save**

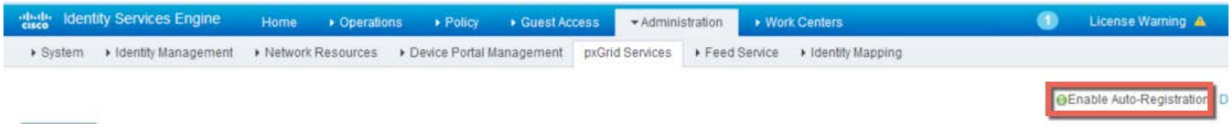
Step 28 Select **Administration->pxGrid Services**, verify that you see the published services



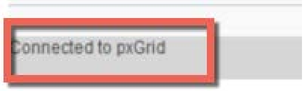
Client Name	Client Description	Capabilities	Status	Client Group(s)	Log
ise-admin-ise20		Capabilities(4 Pub, 2 Sub)	Online	Administrator	View
ise-mnt-ise20		Capabilities(2 Pub, 1 Sub)	Online	Administrator	View
iseagent-fmc60.lab8.com-97563		Capabilities(0 Pub, 3 Sub)	Online	Session	View

Note: This may take a few seconds to appear, verify that the pxGrid services are initializing by running “sh application status ise” on the ISE VM

Step 29 Enable **Enable Auto Registration**



Step 30 Verify that you are connected to pxGrid



Creating SMC Identity Certificate and Downloading CA Root Certificate

Here we generate the SMC private key, certificate-signing request (CSR) to be signed by the CA authority. The CA template for pxGrid must contain an EKU of both client authentication and server authentication to be valid for pxGrid operation.

Step 1 Create the private key on SMC

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

Step 2 Create the SMC CSR request to be signed by the CA server

```
openssl req -new -key smc.key -out smc.csr

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

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

Step 3 Gain root access to SMC, use SCP to copy the SMC.CSR and SMC.key file over to a secure PC. This PC is used to copy or paste the SMC.CSR into an advanced user request for the pxGrid-customized template.

Note: If using Win Laptop, download freeSSHd or utility that installs SSH service so SCP copy can be used to copy these files from the SMC to a Win Laptop

Step 4 Download the certificate in a base-64 encoded format

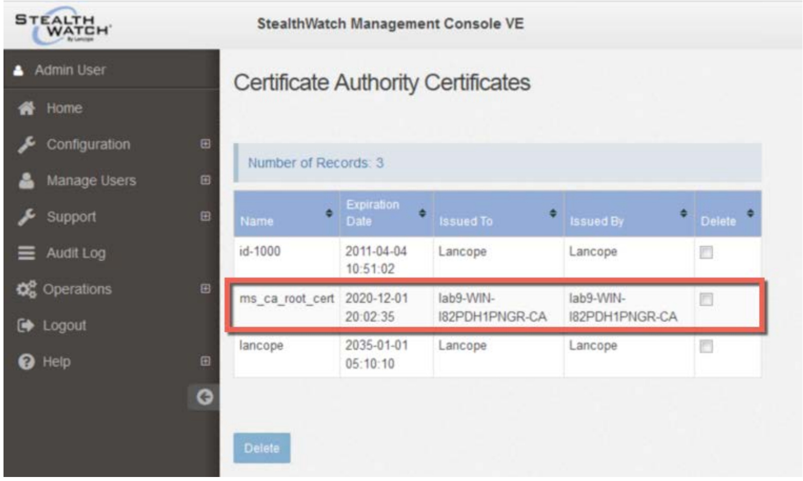
Step 5 Rename the .cer file to a .crt file since this a X509 certificate and was downloaded in base-64 encoded format. This renamed .crt file is used to upload the SSL Client identity certificate. This certificate is used for pxGrid client authentication. This is new in StealthWatch 6.7.1.

Step 6 Download CA root certificate

Upload CA Root Certificate into SMC Trusted Store

Step 1 Select **Admin Users->Administer Appliance->Configuration->Certificate Authority Certificates->Browse Upload the root.cert file**

Step 2 **Provide a description** use underscores, DO NOT USE SPACES->Add Certificate
You should see the following:



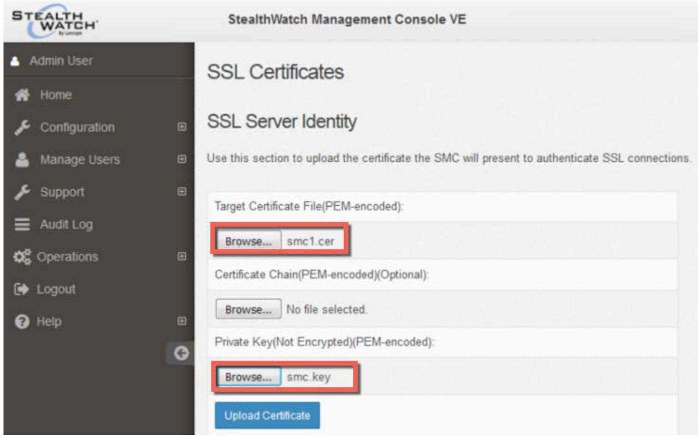
Certificate Authority Certificates

Number of Records: 3

Name	Expiration Date	Issued To	Issued By	Delete
id-1000	2011-04-04 10:51:02	Lancope	Lancope	□
ms_ca_root_cert	2020-12-01 20:02:35	lab9-WIN-I82PDH1PNGR-CA	lab9-WIN-I82PDH1PNGR-CA	□
lancope	2035-01-01 05:10:10	Lancope	Lancope	□

Upload SMC Identity Certificate to SSL Server Identity

Step 3 Select ->Admin Users->Administer Appliance->Configuration->SSL Certificate->SSL Server Identity->Upload the SMC public certificate and private key pair



SSL Certificates

SSL Server Identity

Use this section to upload the certificate the SMC will present to authenticate SSL connections.

Target Certificate File(PEM-encoded): smc1.cer

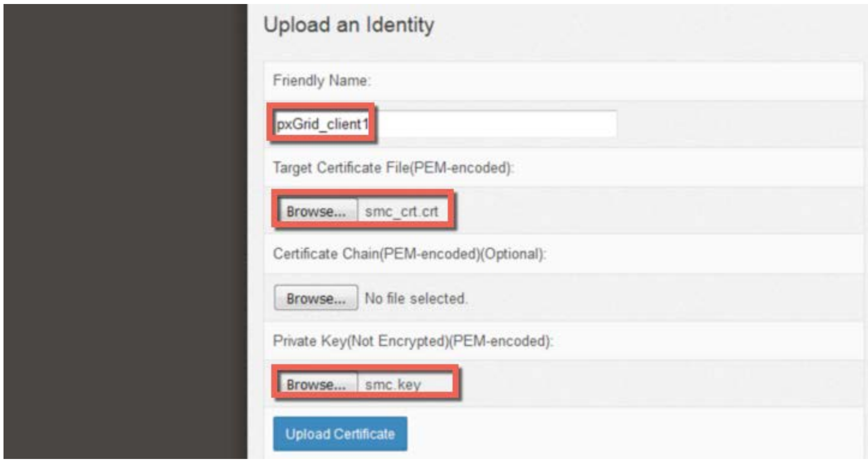
Certificate Chain(PEM-encoded)(Optional): No file selected.

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

Step 4 Click Upload Certificate

Upload SMC Identity Certificate to SSL Client Identities

Step 1 Select **Admin Users->Administer Appliance->Configuration->SSL Certificate->SSL Client Identities->Upload the SMC public certificate.crt file and private key pair**



Upload an Identity

Friendly Name: pxGrid_client1

Target Certificate File(PEM-encoded): smc_crt.crt

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

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

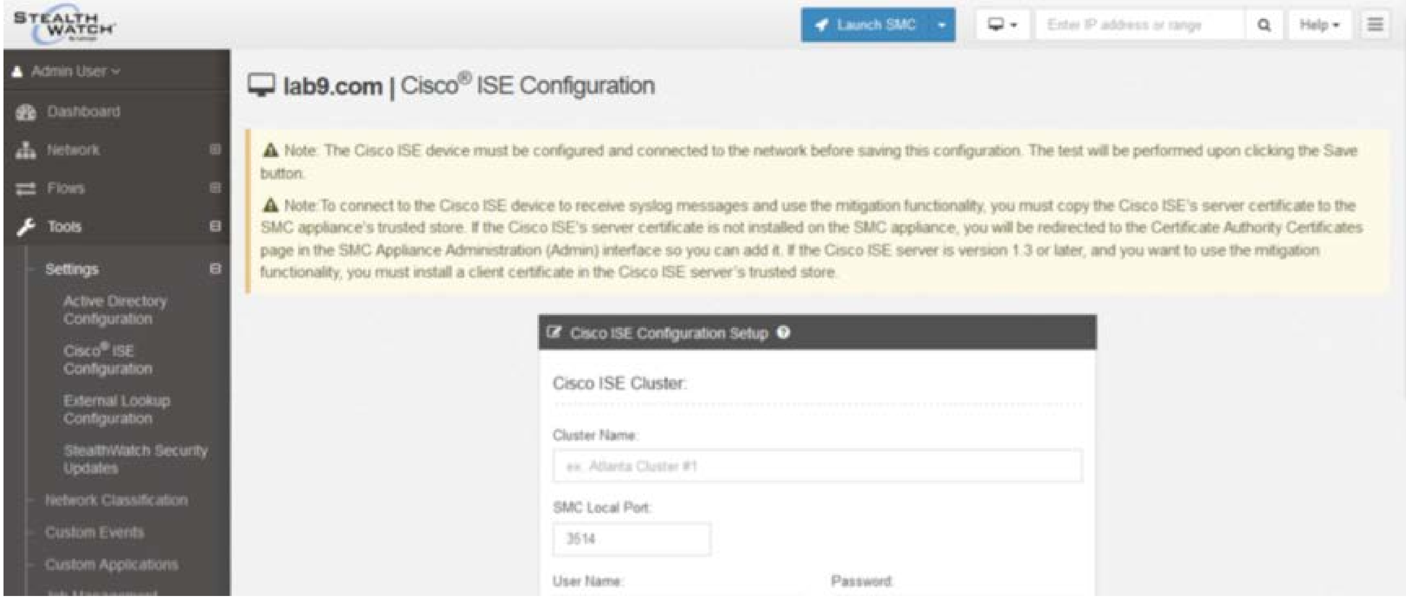
Step 2 Enter **Friendly Name**; use underscores, no spaces are allowed.

Step 3 Click **Upload Certificate**

Receiving Syslog Events from ISE

Step 1 Log in to **SMC->Tools->Settings->Cisco ISE Configuration**, you will see the following configuration If you see the following message, ensure that you have uploaded the CA root certificate to the SMC CA store.

Note: It is assumed that the ISE has already been configured to enable Passed Authentications, RADIUS Accounting, Profiler, Operational, and Administration Audit syslog messages to the SMC over UDP 3514.



lab9.com | Cisco® ISE Configuration

⚠ Note: The Cisco ISE device must be configured and connected to the network before saving this configuration. The test will be performed upon clicking the Save button.

⚠ Note: To connect to the Cisco ISE device to receive syslog messages and use the mitigation functionality, you must copy the Cisco ISE's server certificate to the SMC appliance's trusted store. If the Cisco ISE's server certificate is not installed on the SMC appliance, you will be redirected to the Certificate Authority Certificates page in the SMC Appliance Administration (Admin) interface so you can add it. If the Cisco ISE server is version 1.3 or later, and you want to use the mitigation functionality, you must install a client certificate in the Cisco ISE server's trusted store.

Cisco ISE Configuration Setup

Cisco ISE Cluster:

Cluster Name: ex. Atlanta Cluster #1

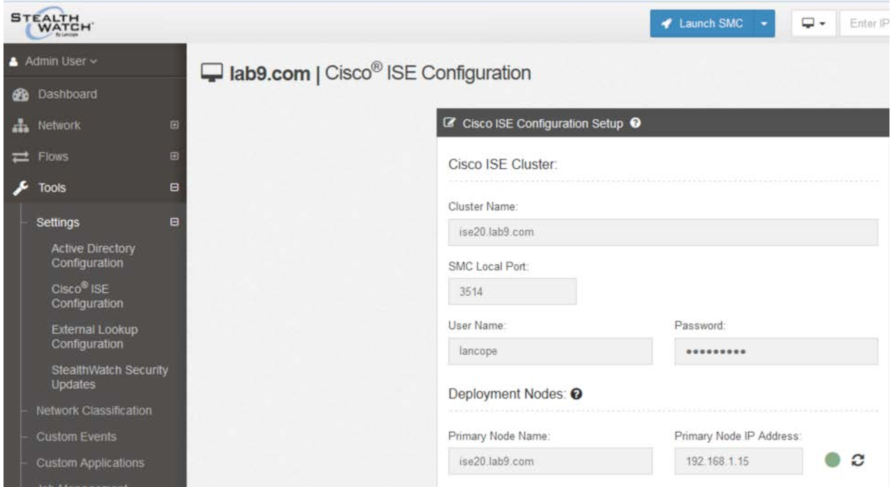
SMC Local Port: 3514

User Name:

Password:

Step 2 Upload the CA root certificate into the SMC

Step 3 Select **Tools->Settings->**fill in the ISE MnT node information, you should see the following



lab9.com | Cisco® ISE Configuration

Cisco ISE Configuration Setup

Cisco ISE Cluster:

Cluster Name: ise20.lab9.com

SMC Local Port: 3514

User Name: lancope

Password: •••••••••

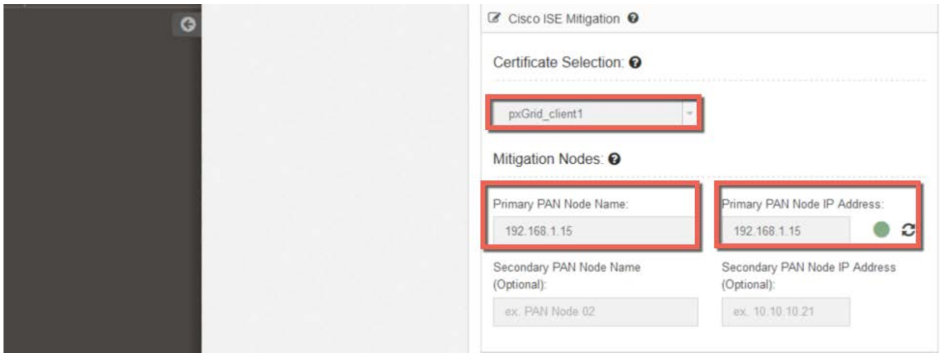
Deployment Nodes:

Primary Node Name: ise20.lab9.com

Primary Node IP Address: 192.168.1.15

Step 4 Add Cisco ISE Mitigation, select the pxGrid_client1 or friendly name you created earlier

Note: The Primary PAN node name is the primary ISE pxGrid node



Cisco ISE Mitigation

Certificate Selection: pxGrid_client1

Mitigation Nodes:

Primary PAN Node Name: 192.168.1.15

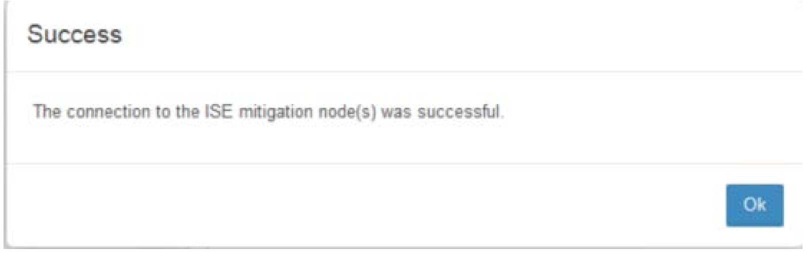
Primary PAN Node IP Address: 192.168.1.15

Secondary PAN Node Name (Optional): ex. PAN Node 02

Secondary PAN Node IP Address (Optional): ex. 10.10.10.21

Step 5 Click **Save**

Step 6 You should see

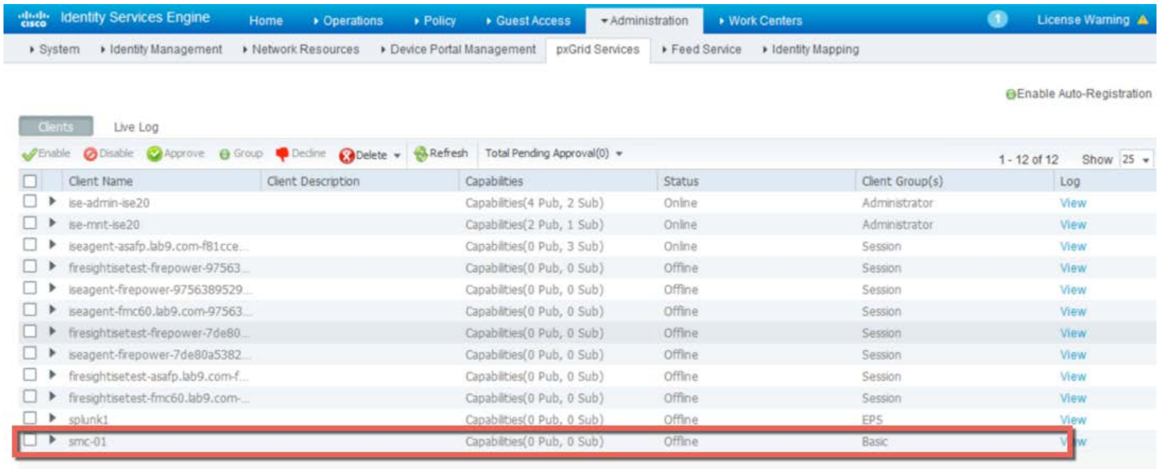


Success

The connection to the ISE mitigation node(s) was successful.

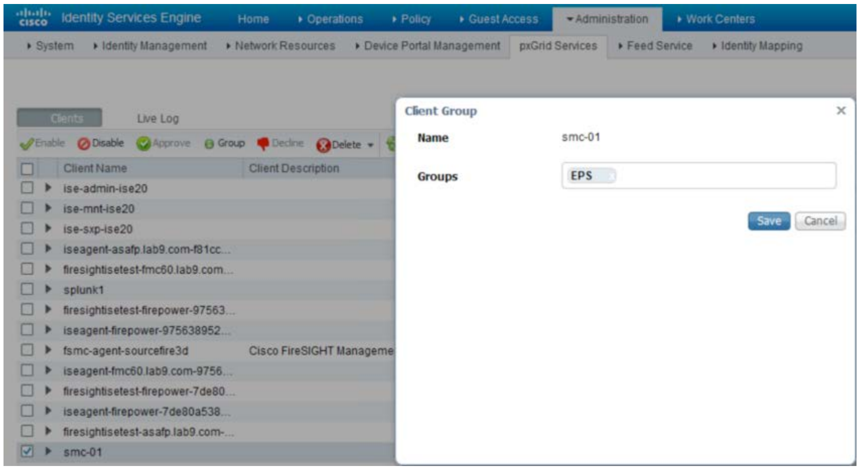
Step 7 Click **OK**

Step 8 You should see the SMC has registered as a pxGrid client



□	Client Name	Client Description	Capabilities	Status	Client Group(s)	Log
□	ise-admin-ise20		Capabilities(4 Pub, 2 Sub)	Online	Administrator	View
□	ise-mnt-ise20		Capabilities(2 Pub, 1 Sub)	Online	Administrator	View
□	iseagent-asafp.lab9.com-f81cce...		Capabilities(0 Pub, 3 Sub)	Online	Session	View
□	firesightisetest-firepower-97563...		Capabilities(0 Pub, 0 Sub)	Offline	Session	View
□	iseagent-firepower-9756389529...		Capabilities(0 Pub, 0 Sub)	Offline	Session	View
□	iseagent-fmc60.lab9.com-97563...		Capabilities(0 Pub, 0 Sub)	Offline	Session	View
□	firesightisetest-firepower-7de80...		Capabilities(0 Pub, 0 Sub)	Offline	Session	View
□	iseagent-firepower-7de80a5382...		Capabilities(0 Pub, 0 Sub)	Offline	Session	View
□	firesightisetest-asafp.lab9.com-f...		Capabilities(0 Pub, 0 Sub)	Offline	Session	View
□	firesightisetest-fmc60.lab9.com-...		Capabilities(0 Pub, 0 Sub)	Offline	Session	View
□	splunk1		Capabilities(0 Pub, 0 Sub)	Offline	EPS	View
□	smc-01		Capabilities(0 Pub, 0 Sub)	Offline	Basic	View

Step 9 Move the registered Lancope smc-01 client to the EPS client group. Select **smc-01->Group->delete Basic, select EPS->Save**



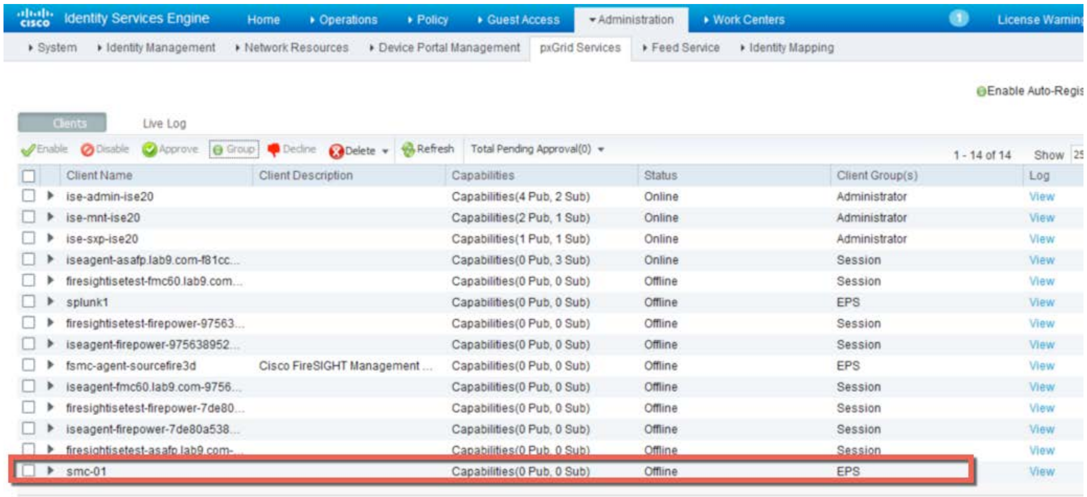
Client Group

Name: smc-01

Groups: EPS

□	Client Name	Client Description
□	ise-admin-ise20	
□	ise-mnt-ise20	
□	ise-sxp-ise20	
□	iseagent-asafp.lab9.com-f81cc...	
□	firesightisetest-fmc60.lab9.com...	
□	splunk1	
□	firesightisetest-firepower-97563...	
□	iseagent-firepower-975638952...	
□	fsmc-agent-sourcefire3d	Cisco FireSIGHT Manageme
□	iseagent-fmc60.lab9.com-9756...	
□	firesightisetest-firepower-7de80...	
□	iseagent-firepower-7de80a538...	
□	firesightisetest-asafp.lab9.com-...	
☑	smc-01	

Step 10 You should see the smc-01 client has moved to the EPS group



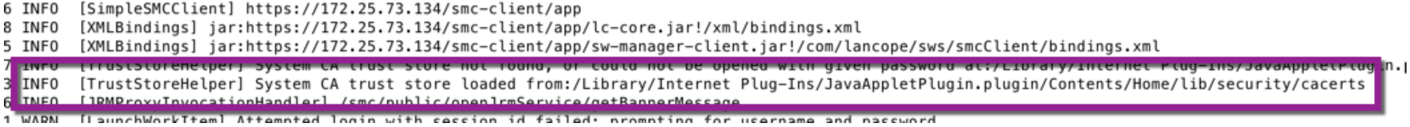
□	Client Name	Client Description	Capabilities	Status	Client Group(s)	Log
□	ise-admin-ise20		Capabilities(4 Pub, 2 Sub)	Online	Administrator	View
□	ise-mnt-ise20		Capabilities(2 Pub, 1 Sub)	Online	Administrator	View
□	ise-sxp-ise20		Capabilities(1 Pub, 1 Sub)	Online	Administrator	View
□	iseagent-asafp.lab9.com-f81cc...		Capabilities(0 Pub, 3 Sub)	Online	Session	View
□	firesightisetest-fmc60.lab9.com...		Capabilities(0 Pub, 0 Sub)	Offline	Session	View
□	splunk1		Capabilities(0 Pub, 0 Sub)	Offline	EPS	View
□	firesightisetest-firepower-97563...		Capabilities(0 Pub, 0 Sub)	Offline	Session	View
□	iseagent-firepower-975638952...		Capabilities(0 Pub, 0 Sub)	Offline	Session	View
□	fsmc-agent-sourcefire3d	Cisco FireSIGHT Management ...	Capabilities(0 Pub, 0 Sub)	Offline	EPS	View
□	iseagent-fmc60.lab9.com-9756...		Capabilities(0 Pub, 0 Sub)	Offline	Session	View
□	firesightisetest-firepower-7de80...		Capabilities(0 Pub, 0 Sub)	Offline	Session	View
□	iseagent-firepower-7de80a538...		Capabilities(0 Pub, 0 Sub)	Offline	Session	View
□	firesightisetest-asafp.lab9.com-...		Capabilities(0 Pub, 0 Sub)	Offline	Session	View
□	smc-01		Capabilities(0 Pub, 0 Sub)	Offline	EPS	View

SMC Client- Getting the Host Java Store to Trust the CA Certificate

Note: If the CA does not have a standard public CA as its root the host java store must be configured to trust the CA root certificate in order to open the java client**.**

Step 1 Open the SMC java client with the Java console enabled.

Step 2 In the Java console, locate the path for the TrustStoreHelper



```
6 INFO  [SimpleSMCClient] https://172.25.73.134/smc-client/app
8 INFO  [XMLBindings] jar:https://172.25.73.134/smc-client/app/lc-core.jar!/xml/bindings.xml
5 INFO  [XMLBindings] jar:https://172.25.73.134/smc-client/app/sw-manager-client.jar!/com/lancope/sws/smcClient/bindings.xml
7 INFO  [TrustStoreHelper] System CA trust store not found, or could not be opened with given password at:/Library/Internet Plug-Ins/JavaAppletPlugin.p
3 INFO  [TrustStoreHelper] System CA trust store loaded from:/Library/Internet Plug-Ins/JavaAppletPlugin.plugin/Contents/Home/lib/security/cacerts
6 INFO  [JRMProxyInvocationHandler] /smc/public/openIrmService/getBannerMessage
1 WARN  [LaunchWorkItem] Attempted login with session id failed; prompting for username and password
```

Step 3 On the host, import the CA root certificate into the cacerts file identified in the previous step. The default password for most cacerts files is “changeit”.

```
keytool -keystore cacerts -importcert -alias myca -file myfile
```

where: myfile represents the CA root certificate (i.e. root.cer)

Step 4 Launch the SMC java client.

SMC Client Example

To launch the SMC java client successfully, import the CA root certificate into the cacerts file, and install the (JDK) Java Development Kit on your PC.

Step 1 Download and install the Oracle Java Development Kit

Step 2 Include the JDK in your path

Step 3 Enable Java Console to appear

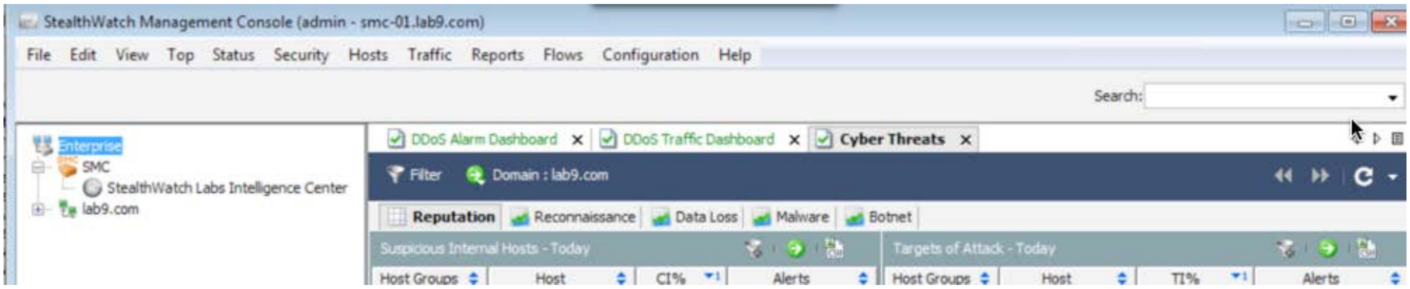
All Programs->Java->Configure Java->Advanced->Java Console->Show Console->Apply->OK

Step 4 Type the following to import (CA root.cert) caroot.cer into the cacerts file:

```
C:\Program Files\Java\jre1.8.0_66\lib\security>path=c:\program files\java\jdk1.8
.0_66\bin

C:\Program Files\Java\jre1.8.0_66\lib\security>keytool.exe -keystore cacerts -im
portcert -alias myca -file caroot.cer
Enter keystore password:changeit
Owner: CN=lab9-WIN-I82PDH1PNGR-CA, DC=lab9, DC=com
Issuer: CN=lab9-WIN-I82PDH1PNGR-CA, DC=lab9, DC=com
Serial number: 913b274e6a35ea34efcdf6dadfe4f0e
Valid from: Tue Dec 01 19:52:35 GMT-05:00 2015 until: Tue Dec 01 20:02:35 GMT-05
:00 2020
Certificate fingerprints:
         MD5:  FD:26:D1:E0:FA:C5:31:79:DC:5A:1E:BA:DD:91:03:D7
         SHA1: 22:2A:22:11:3A:00:50:67:AD:83:85:80:A9:41:25:4A:DE:C0:91:2A
         SHA256: 98:8E:A1:63:AB:C6:22:2B:50:A7:4A:25:77:03:84:E9:9E:95:B7:E8:45:
86:5F:58:77:04:42:D2:A3:82:BB:71
         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: AB D9 CE DB CD 58 19 4A   42 A6 BF 68 7A 96 FF 91  .....X.JB..hz...
0010: 1F 73 BC 67                                        .s.g
]
]

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

C:\Program Files\Java\jre1.8.0_66\lib\security>
```

Step 5 Click->**Launch SMC client**
You should see the following


StealthWatch Management Console (admin - smc-01.lab9.com)
File Edit View Top Status Security Hosts Traffic Reports Flows Configuration Help
Search:
Enterprise
SMC
StealthWatch Labs Intelligence Center
lab9.com
DDoS Alarm Dashboard
DDoS Traffic Dashboard
Cyber Threats
Filter
Domain : lab9.com
Reputation
Reconnaissance
Data Loss
Malware
Botnet
Suspicious Internal Hosts - Today
Host Groups
Host
CI%
Alerts
Targets of Attack - Today
Host Groups
Host
TI%
Alerts

Step 6 You should see the following in the console

```
Java Web Start 11.66.2.17
Using JRE version 1.8.0_66-b17 Java HotSpot(TM) 64-Bit Server VM
User home directory = C:\Users\jsmith
----------------------------------------------------
c:   clear console window
f:   finalize objects on finalization queue
g:   garbage collect
h:   display this help message
m:   print memory usage
o:   trigger logging
p:   reload proxy configuration
q:   hide console
r:   reload policy configuration
s:   dump system and deployment properties
t:   dump thread list
v:   dump thread stack
0-5: set trace level to <n>
----------------------------------------------------
Missing Application-Name manifest attribute for: https://smc-01.lab9.com/smc-client/app/guava.jar
StealthWatch detected JRE version 1.8.0_66
```

```
2016-01-31 00:34:39,306 INFO  [LogManager] resource=jar:https://smc-01.lab9.com/smc-client/app/sw-manager-
client.jar!/com/lancope/sws/smcClient/log4j.xml
2016-01-31 00:34:39,306 INFO  [LogManager] level=default
2016-01-31 00:34:39,306 INFO  [SimpleSMCClient] https://smc-01.lab9.com/smc-client/app
2016-01-31 00:34:39,311 INFO  [XMLBindings] jar:https://smc-01.lab9.com/smc-client/app/lc-
core.jar!/xml/bindings.xml
2016-01-31 00:34:39,725 INFO  [XMLBindings] jar:https://smc-01.lab9.com/smc-client/app/sw-manager-
client.jar!/com/lancope/sws/smcClient/bindings.xml
2016-01-31 00:34:40,230 INFO  [TrustStoreHelper] System CA trust store not found, or could not be opened with
given password at:C:\Program Files\Java\jre1.8.0_66\lib\security\jssecacerts
2016-01-31 00:34:40,240 INFO  [TrustStoreHelper] System CA trust store loaded from:C:\Program
Files\Java\jre1.8.0_66\lib\security\cacerts
Jan 31, 2016 12:34:40 AM java.util.prefs.WindowsPreferences <init>
WARNING: Could not open/create prefs root node Software\JavaSoft\Prefs at root 0x80000002. Windows
RegCreateKeyEx(...) returned error code 5.
2016-01-31 00:34:40,343 INFO  [JRMProxyInvocationHandler] /smc/public/openJrmService/getBannerMessage
2016-01-31 00:34:41,195 INFO  [JRMProxyInvocationHandler] /smc/jrmService/userService/getUserProfile
2016-01-31 00:34:41,352 INFO  [JRMProxyInvocationHandler] /smc/jrmService/objectService/get
2016-01-31 00:34:41,459 INFO  [SMCClientObjectModel] added LObjectKey:{Domain:{143}}
2016-01-31 00:34:41,460 INFO  [SMCClientObjectModel] added LObjectKey:{SMC:{0}}
2016-01-31 00:34:41,460 INFO  [SMCClientObjectModel] added LObjectKey:{Domain:{143},CiscoISE:{162}}
.
.
.
```

Using Self-Signed Certificates for SMC and ISE pxGrid node

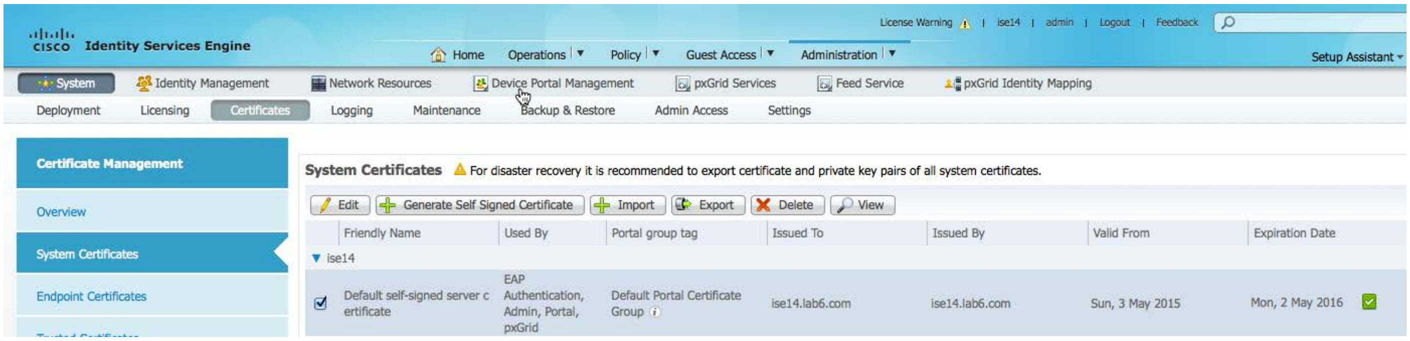
This section discusses using self-signed certificates for the StealthWatch SMC and the ISE pxGrid node. Self-signed certificates are primarily used for testing PoC (Proof of Concept). The ISE pxGrid node is deployed in a stand-alone environment. Please note that in ISE productional deployments, pxGrid will be a dedicated node.

Configuring ISE 1.3/1.4 for Self-Signed certificates

The ISE Identity certificate needs to be trusted, the public certificate needs to be exported into the ISE trusted system certificate store. This is not required for ISE 2.0.

Note: You may not have to perform this step in ISE 1.4; the ISE identity certificate may already be trusted.

Step 1 **Administration->System->Certificates->System Certificates->select the ISE Identity certificate and export**

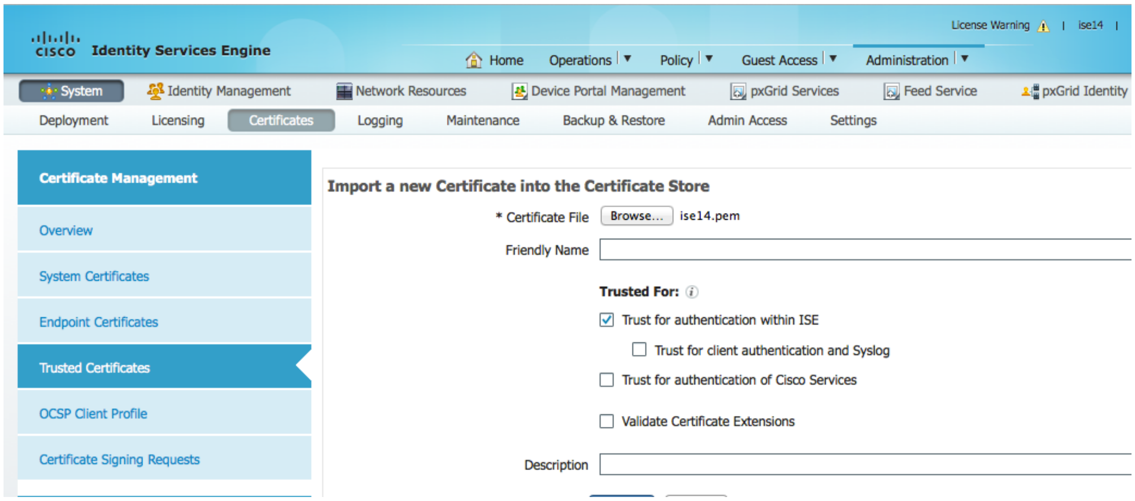


System Certificates ⚠ For disaster recovery it is recommended to export certificate and private key pairs of all system certificates.

	Friendly Name	Used By	Portal group tag	Issued To	Issued By	Valid From	Expiration Date	
▼ ise14								
☑	Default self-signed server certificate	EAP Authentication, Admin, Portal, pxGrid	Default Portal Certificate Group	ise14.lab6.com	ise14.lab6.com	Sun, 3 May 2015	Mon, 2 May 2016	✓

Note: Export out the public certificate only, you can change the default certificate name. In these examples, the certificate name was changed to ise14.pem

Step 2 **Administration->System->Certificates->Trusted Certificates->Import->certificate file->enable Trust for authentication within ISE->Submit**



Import a new Certificate into the Certificate Store

* Certificate File ise14.pem

Friendly Name

Trusted For:

☑ Trust for authentication within ISE

☐ Trust for client authentication and Syslog

☐ Trust for authentication of Cisco Services

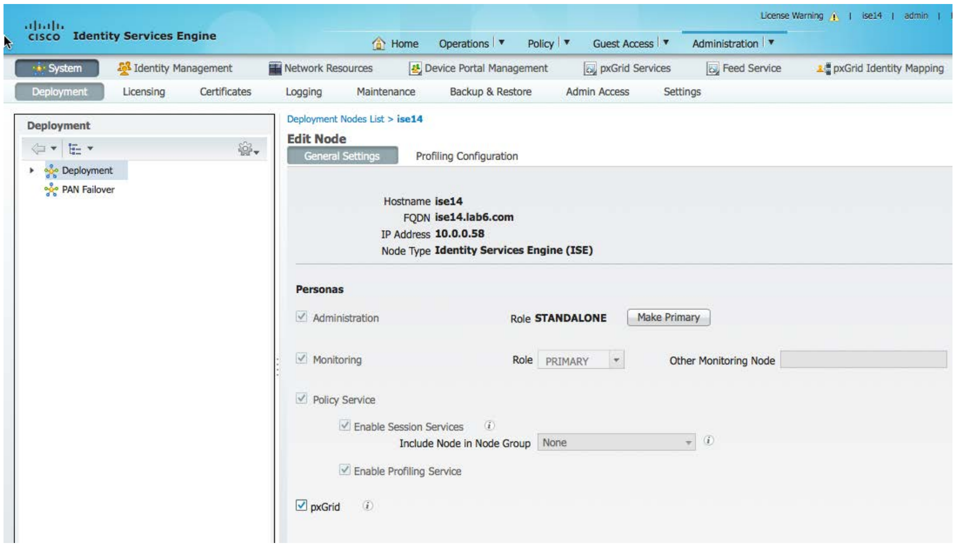
☐ Validate Certificate Extensions

Description

Enabling pxGrid

Enable pxGrid and persona, pxGrid services should start in ISE.

Step 1 **Enable** pxGrid persona under **Administration->System->Deployment->Save**



Hostname **ise14**
FQDN **ise14.lab6.com**
IP Address **10.0.0.58**
Node Type **Identity Services Engine (ISE)**

Personas

☑ Administration Role **STANDALONE** Make Primary

☑ Monitoring Role PRIMARY Other Monitoring Node

☑ Policy Service

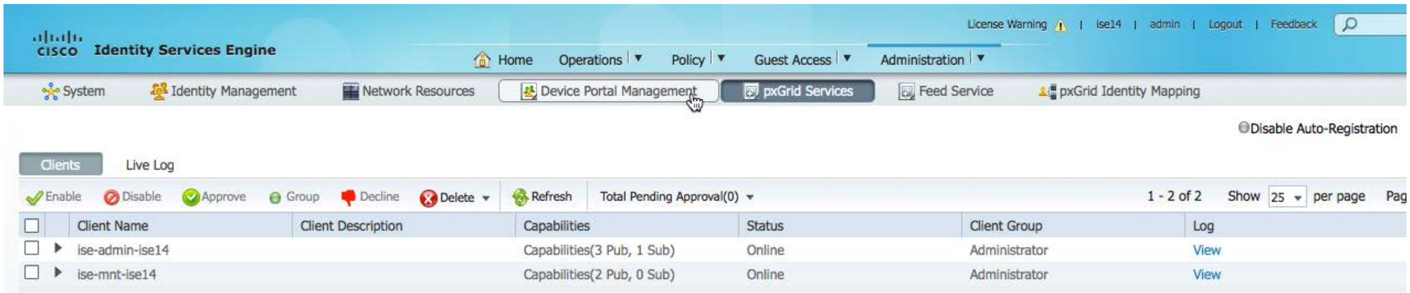
☑ Enable Session Services
Include Node in Node Group None

☑ Enable Profiling Service

☑ pxGrid

Step 2 Verify that the pxGrid services are enabled. **Administration->pxGrid Services**

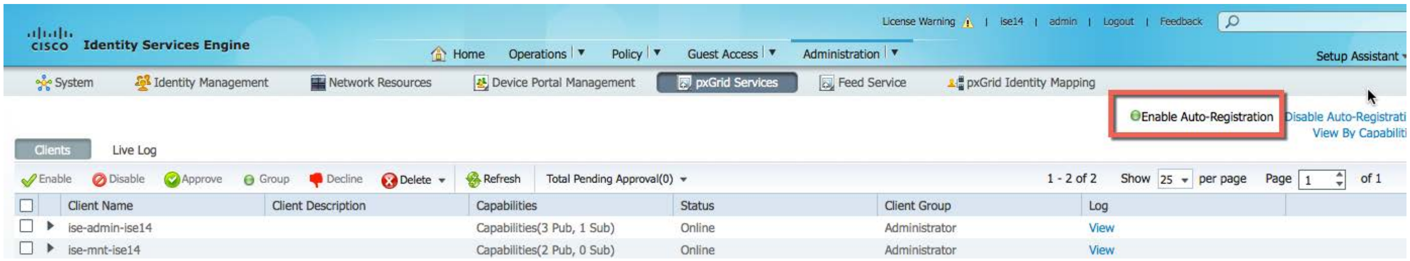
Note: this may take a minute, please verify that the pxGrid services are initializing, run “application status ise” on the ISE pxGrid node.
If the services still do not come up, please export the ISE Identity certificate into the ISE Trusted System Certificate store.



□	Client Name	Client Description	Capabilities	Status	Client Group	Log
□	ise-admin-ise14		Capabilities(3 Pub, 1 Sub)	Online	Administrator	View
□	ise-mnt-ise14		Capabilities(2 Pub, 0 Sub)	Online	Administrator	View

Step 3 Enable **“Enable Auto Registration”**

Note: If “Auto Registration” is not enabled, you will see the pxGrid client requests in the pending state.

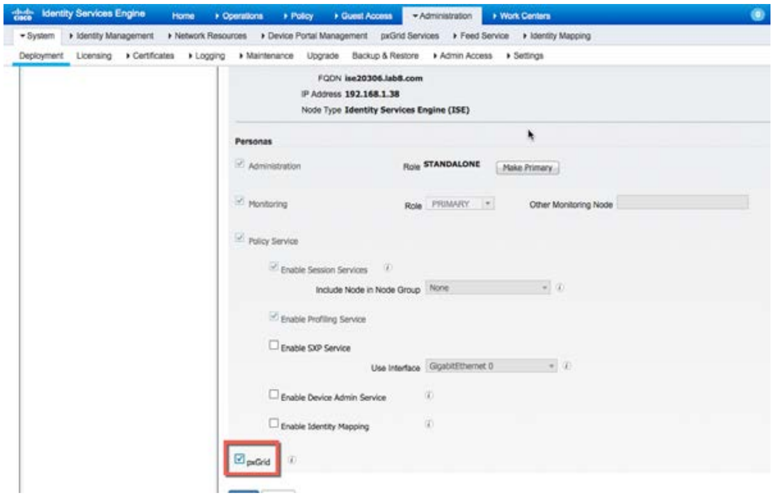


□	Client Name	Client Description	Capabilities	Status	Client Group	Log
□	ise-admin-ise14		Capabilities(3 Pub, 1 Sub)	Online	Administrator	View
□	ise-mnt-ise14		Capabilities(2 Pub, 0 Sub)	Online	Administrator	View

Configuring ISE 2.0 for Self-Signed certificates

Note: The ISE self-signed identity certificate is no longer required to be exported into the ISE certificate trusted store as in ISE 1.3 and ISE 1.4.

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



FQDN **ise20306.lab8.com**
IP Address **192.168.1.38**
Node Type **Identity Services Engine (ISE)**

Personas

☑ Administration — Role **STANDALONE**

☑ Monitoring — Role PRIMARY — Other Monitoring Node

☑ Policy Service

☑ Enable Session Services
Include Node in Node Group: None

☑ Enable Profiling Service

□ Enable SXP Service
Use Interface: GigabitEthernet 0

□ Enable Device Admin Service

□ Enable Identity Mapping

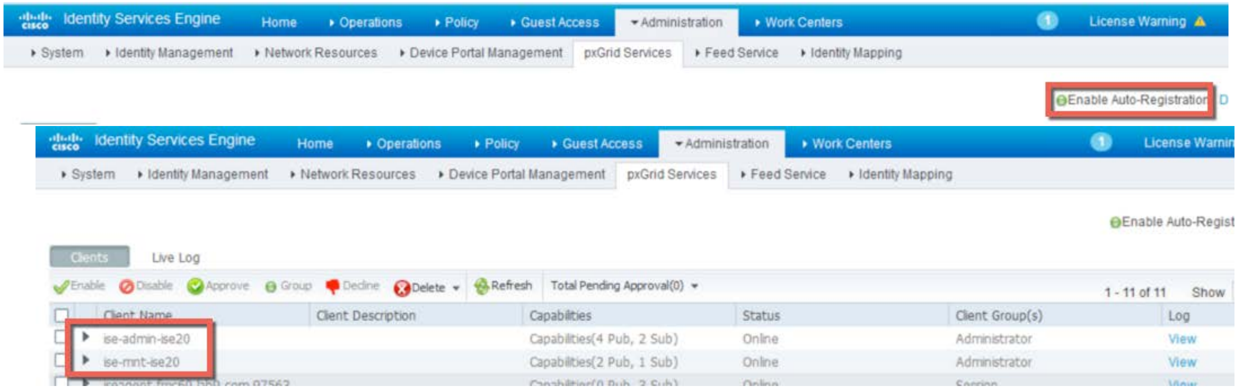
☑ pxGrid

Step 2 Select **Save**

Step 3 Verify that the published nodes appear under pxGrid Services and there is connectivity. **Administration->pxGrid Services**

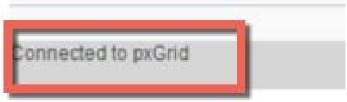
Note: The published nodes may take a while to appear. Verify that pxGrid services have started by running: **sh application status ise** on the ISE VM node.

Step 4 Enable **Enable Auto-Registration**



	Client Name	Client Description	Capabilities	Status	Client Group(s)	Log
□	ise-admin-ise20		Capabilities(4 Pub, 2 Sub)	Online	Administrator	View
□	ise-mnt-ise20		Capabilities(2 Pub, 1 Sub)	Online	Administrator	View

Step 5 Verify that you are **connected to pxGrid**

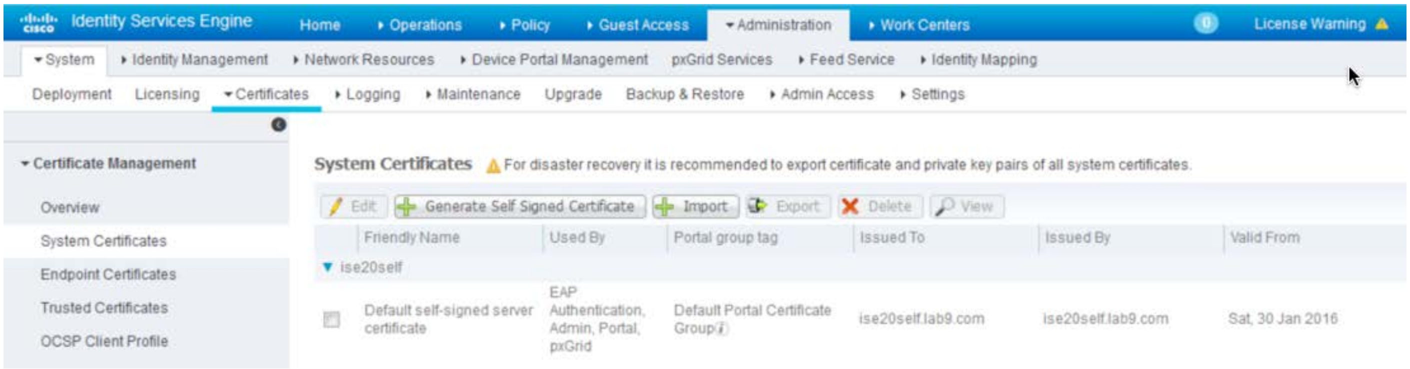


Connected to pxGrid

Exporting ISE Identity Certificate into SMC

Step 1 Import ISE identity cert into SMC Certificate Authority Store.

Step 2 Select **Administration->System->Certificates->System Certificates**
You should see the following:

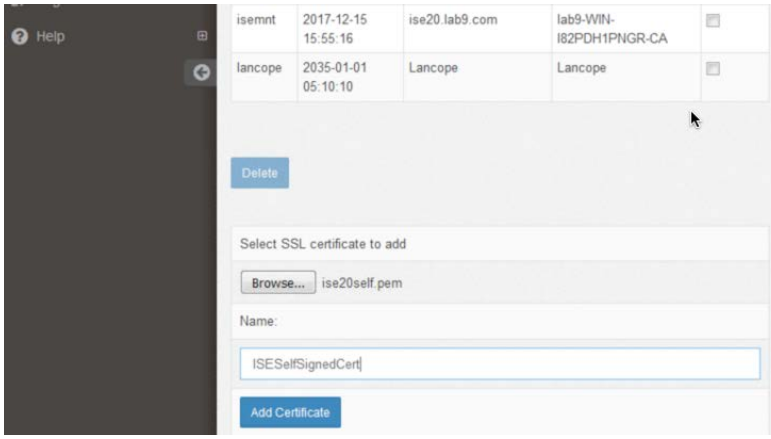


System Certificates ⚠ For disaster recovery it is recommended to export certificate and private key pairs of all system certificates.

	Friendly Name	Used By	Portal group tag	Issued To	Issued By	Valid From
▼ ise20self						
□	Default self-signed server certificate	EAP Authentication, Admin, Portal, pxGrid	Default Portal Certificate Group	ise20self.lab9.com	ise20self.lab9.com	Sat, 30 Jan 2016

Step 3 Select the Default self-signed server certificate->**Export the public certificate only**. You can also rename the PEM filename to make it easier to work with.

Step 4 Open the SMC, select **Admin User->Administer Appliance->Configuration->Certificate Authority Certificates->browse and upload the ISE identity certificate from Step 3**



isemnt	2017-12-15 15:55:16	ise20.lab9.com	lab9-WIN-I82PDH1PNGR-CA	□
lancope	2035-01-01 05:10:10	Lancope	Lancope	□

Select SSL certificate to add

Browse... ise20self.pem

Name:

ISESelfSignedCert

Step 5 Name the certificate, in the example, ISESelfSignedCert. Please note you must add a value, you can use underscores but no empty spaces.

Step 6 Select->**Add Certificate**, you will receive a confirmation that the certificate has been added successfully.

Creating Self Signed Certificates for SMC

Here we create the self-signed certificates for the SMC, the pxGrid client. You need to gain root access on the SMC.

Note: These steps are documented on SMC->Help-Self-Signed Certificates

Step 1 Generate a private key for SMC, you will also be prompted for a passphrase to be used in later steps

```
openssl genrsa –des3 –out selfsmc.key 2048
```

You should see the following:

```
Generating RSA private key, 2048 bit long modulus
.............................................................................................................
...............................................+++
.+++
e is 65537 (0x10001)
Enter pass phrase for smc1.key:
Verifying - Enter pass phrase for smc1.key:
smc:~#
```

Step 2 Generate the self-signed certificate request (CSR)

```
openssl req -new -key selfsmc.key -out selfsmc.csr
```

Note: All the field are required except for the challenge password [] and company name []

You should see the following:

```
Enter pass phrase for selfsmc.key:
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]:Lancope
Organizational Unit Name (eg, section) []:Engineering
Common Name (e.g. server FQDN or YOUR name) []:smc.lab6.com
Email Address []:jdoe@lancope.com

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

Step 3 Generate the self-signed certificate

```
openssl x509 -req -days 365 -in selfsmc.csr -signkey selfsmc.key -out selfsmc.crt
```

You should see the following:

```
Signature ok
subject=/C=US/ST=Maryland/L=Germantown/O=Lancope/OU=Engineering/CN=smc.lab6.com/emailAddress=jdoe@lancope.com
Getting Private key
Enter pass phrase for selfsmc.key:
smc:~#
```

Step 4 To decrypt the passphrase you typed earlier

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

You should see the following:

```
Enter pass phrase for selfsmc.key.org:
writing RSA key
smc:~#
```

Step 5 You should have the following in the /root/smc directory

```
smc:~# ls
selfsmc.crt  selfsmc.csr  selfsmc.key  selfsmc.key.org
smc:~#
```

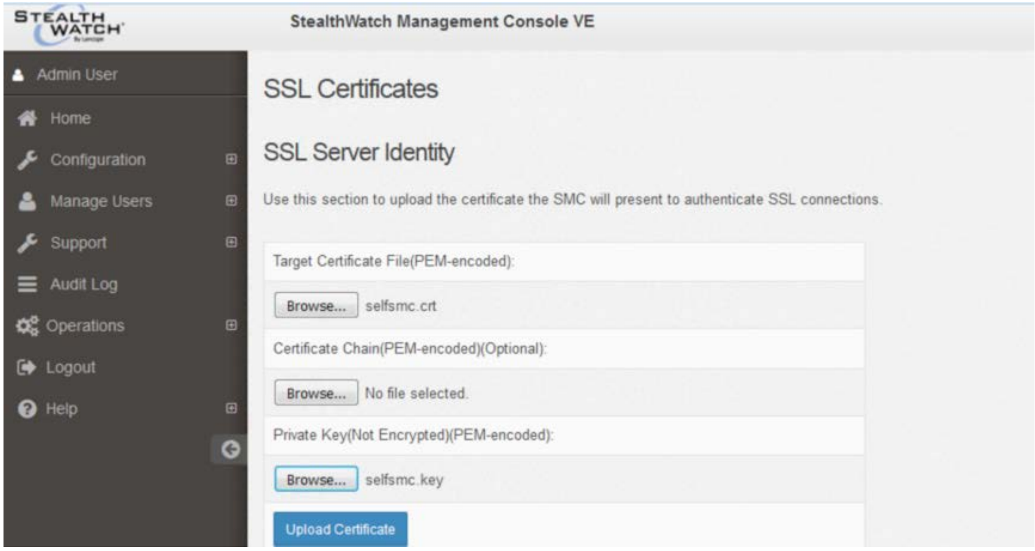
The selfsmc.cert and selfsmc.key will be uploaded into the SMC under SSL certificates as Admin User

Step 6 Copy the selfsmc.crt and selfsmc.key files over locally using SCP, please “Enabling SSH on a MAC” in Appendices for reference, if you receive connection refused when copying to your local PC.

Upload self-signed certificates to SMC

Here we upload the public certificate and private key pair of the self-signed certificate to SMC.

Step 1 Select **Admin User->Configuration->SSL Certificates->SSL Server Identity and upload selfsmc.crt and selfsmc.key->Upload Certificate**



SSL Certificates

SSL Server Identity

Use this section to upload the certificate the SMC will present to authenticate SSL connections.

Target Certificate File(PEM-encoded):

Browse... selfsmc.crt

Certificate Chain(PEM-encoded)(Optional):

Browse... No file selected.

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

Browse... selfsmc.key

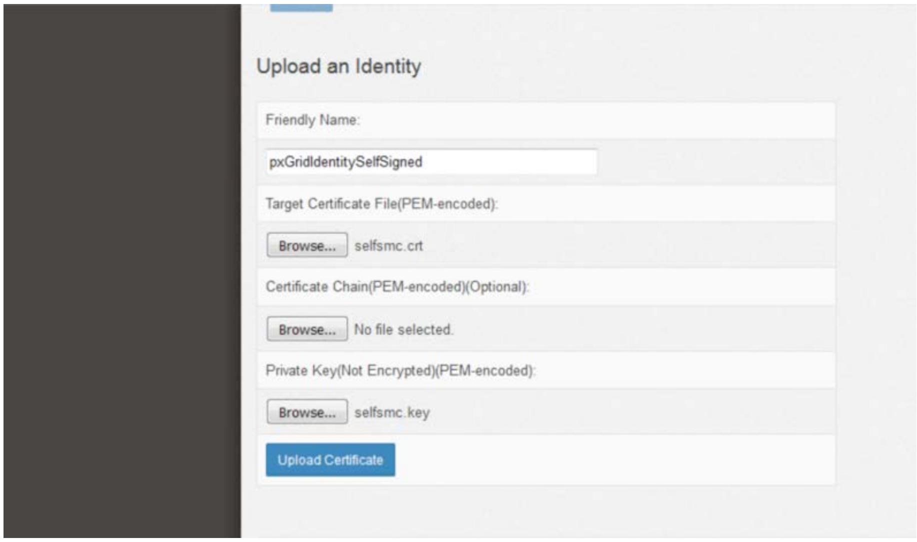
Upload Certificate

Step 2 Select **Upload Certificate**

Step 3 You should see the certificate was uploaded successfully, and a restart is required.

Step 4 Once the SMC services have started, log back in and add the client identity certificate

Step 5 Select **Admin User->Configuration->SSL Certificates->SSL Client Identities and upload selfsmc.crt and selfsmc.key->Upload Certificate**



Upload an Identity

Friendly Name:

pxGridIdentitySelfSigned

Target Certificate File(PEM-encoded):

Browse... selfsmc.crt

Certificate Chain(PEM-encoded)(Optional):

Browse... No file selected.

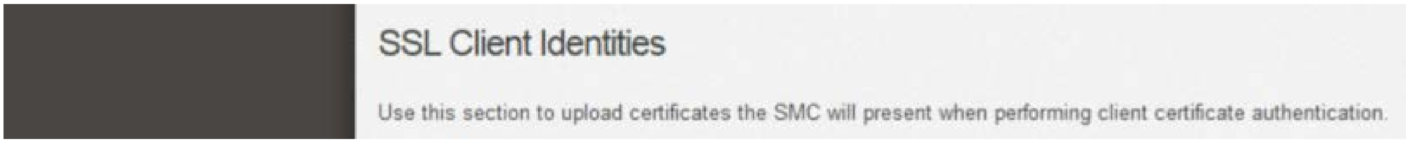
Private Key(Not Encrypted)(PEM-encoded):

Browse... selfsmc.key

Upload Certificate

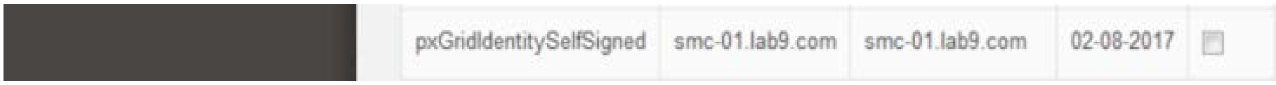
Step 6 Add the friendly name ->**Upload Certificate**

Step 7 You should see the uploaded certificate under SSL client identities



SSL Client Identities

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

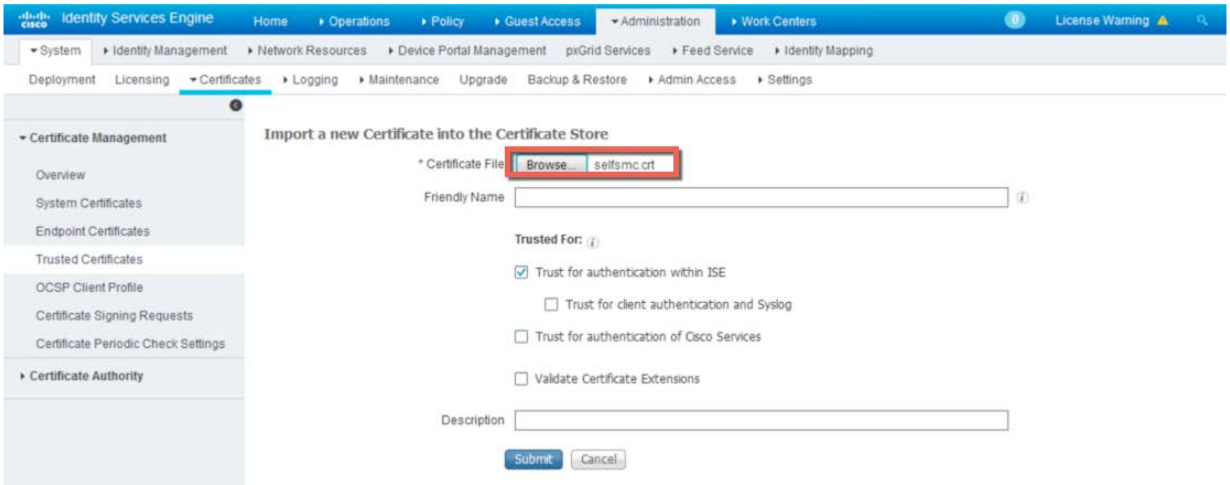


pxGridIdentitySelfSigned	smc-01.lab9.com	smc-01.lab9.com	02-08-2017	□

Upload SMC Self-Signed certificate to ISE Trusted System Certificate Store

Here we upload the SMC self-signed certificate into the ISE trusted system certificate store

Step 1 **Administration->System->Certificates->Trusted Certificates->Import the SMC self-signed certificate. Enable "trust for authentication within ISE and Submit**



Import a new Certificate into the Certificate Store

* Certificate File Browse... selfsmc.crt

Friendly Name

Trusted For:

☑ Trust for authentication within ISE

□ Trust for client authentication and Syslog

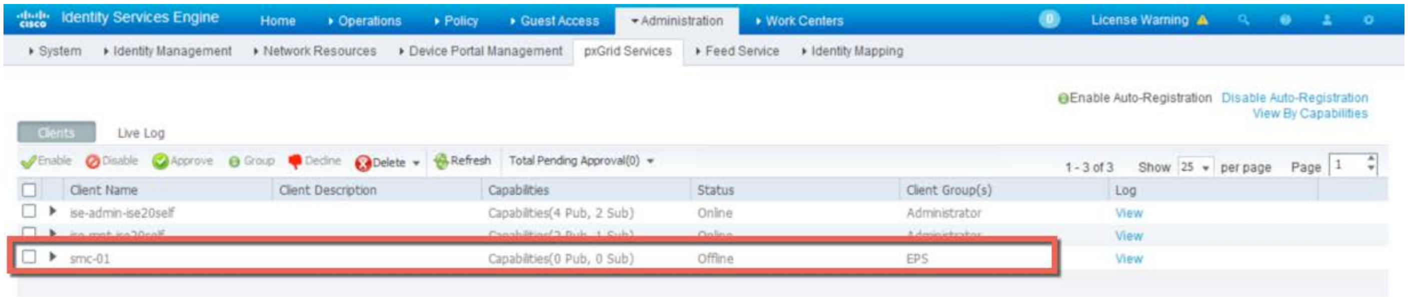
□ Trust for authentication of Cisco Services

□ Validate Certificate Extensions

Description

Submit Cancel

Step 2 You should see that SMC has registered to the ISE pxGrid node

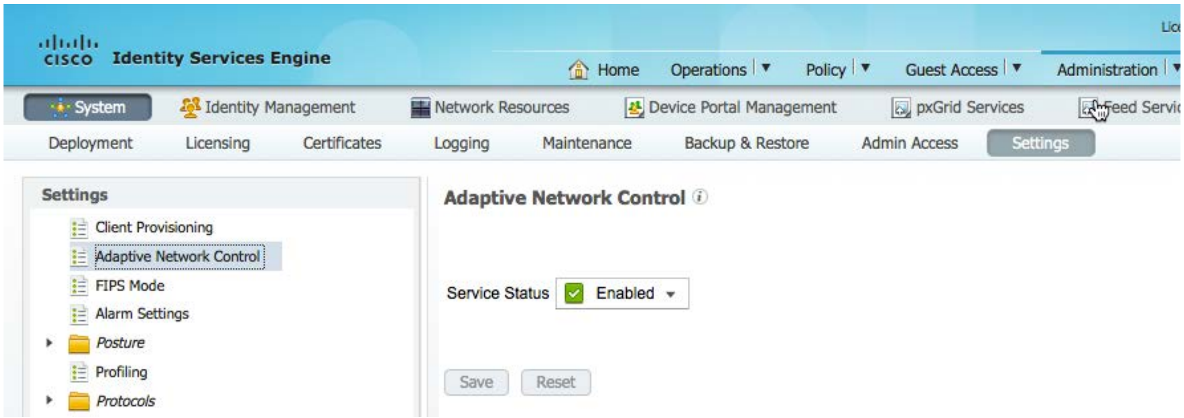


□	Client Name	Client Description	Capabilities	Status	Client Group(s)	Log
□	ise-admin-ise20self		Capabilities(4 Pub, 2 Sub)	Online	Administrator	View
□	ise-mnt-ise20self		Capabilities(2 Pub, 1 Sub)	Online	Administrator	View
□	smc-01		Capabilities(0 Pub, 0 Sub)	Offline	EPS	View

Enabling Adaptive Network Control (ANC)

This section discusses enabling Adaptive Network Control (ANC) on ISE 1.4 and configuring the Authorization policy. ANC is formerly known as Endpoint Protection Service (EPS) in ISE 1.3. This is not required in ISE 2.0 and above, and is automatically enabled. However, the ISE quarantine authorization policy must be configured.

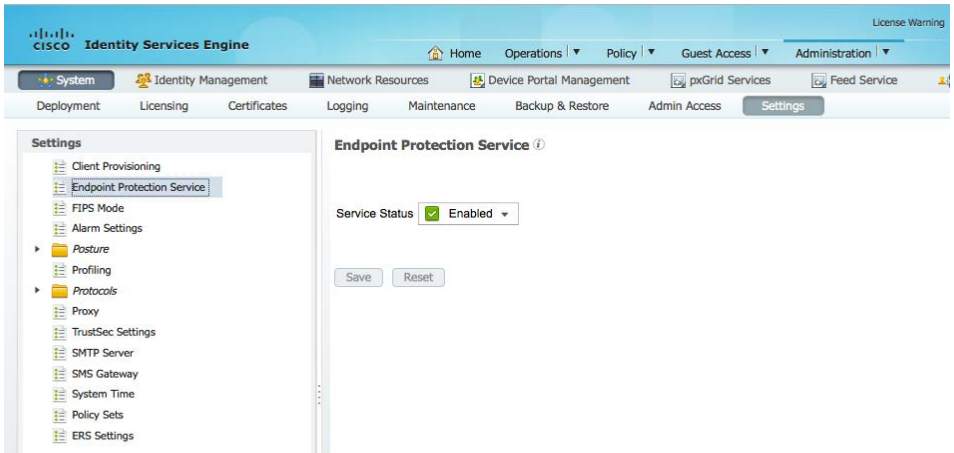
Step 1 To enable ANC in ISE 1.4, **Administration->System->Settings->Adaptive Network Control->Enable->Save**



Adaptive Network Control

Service Status: Enabled

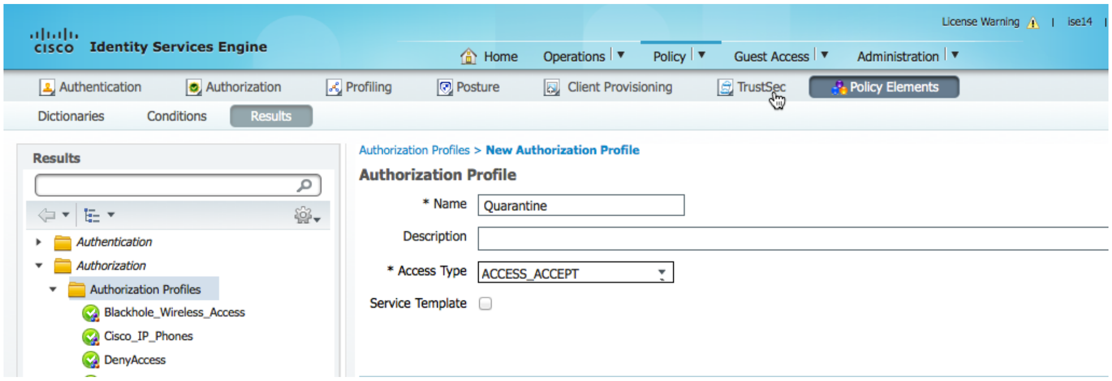
Step 2 To enable EPS in ISE 1.3, **Administration->System->Settings->enable Service Status then Save**



Endpoint Protection Service

Service Status: Enabled

Step 3 **Policy->Policy Elements->Results->Authorization->Authorization Profiles->Add->Quarantine, enter Quarantine for Name->Submit**

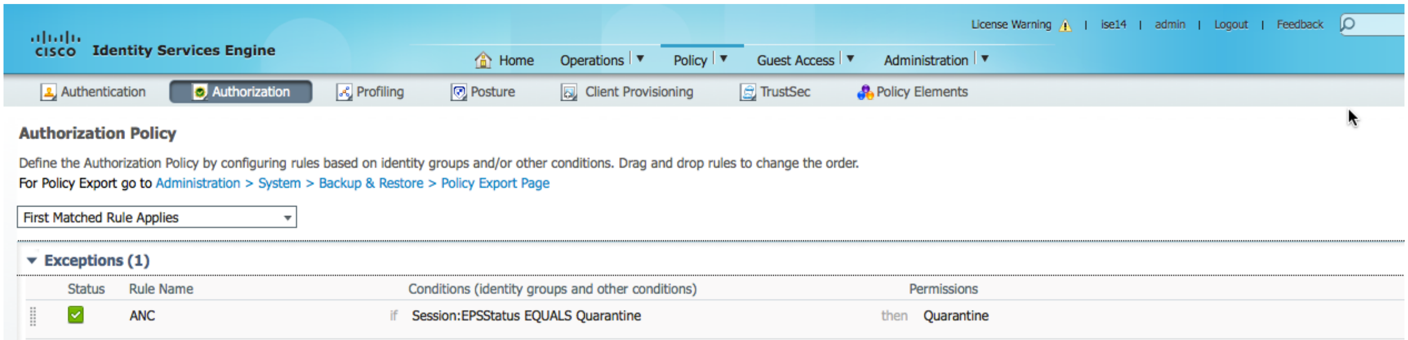


Authorization Profiles > New Authorization Profile

Authorization Profile

* Name	Quarantine
Description	
* Access Type	ACCESS_ACCEPT
Service Template	☐

Step 4 **Policy->Authorization->Exceptions** and add the following:



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

First Matched Rule Applies

Exceptions (1)

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

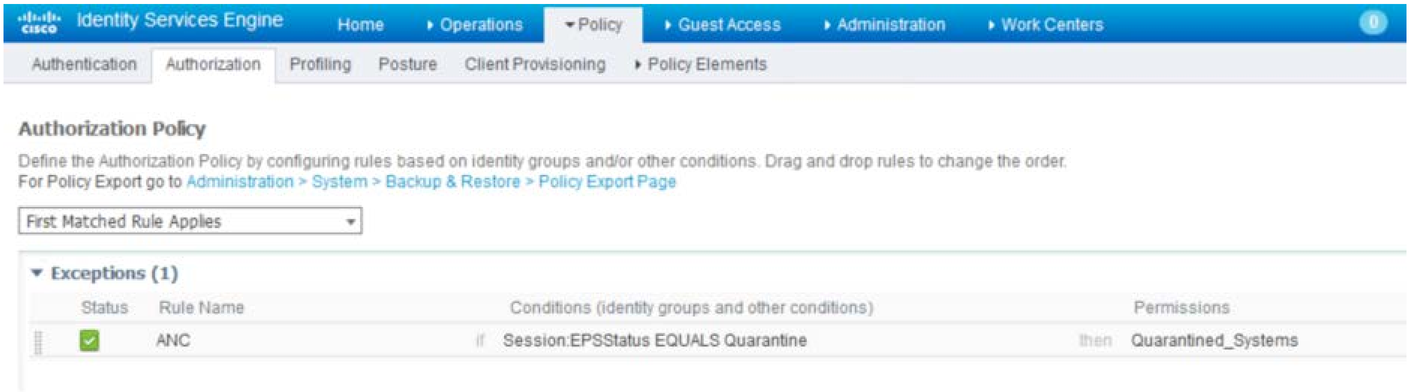
Step 5 Rule Name: **ANC**

Step 6 New Condition Rule Add a new attribute value: **Session:EPStatus:Equals:Quarantine**

Step 7 **Permissions**:**Profiles:Standard**:**Quarantine**

Step 8 Click->**Done->Save**

In ISE 2.0, you can create the following policy with a default Quarantined Systems SGT as defined below:



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

First Matched Rule Applies

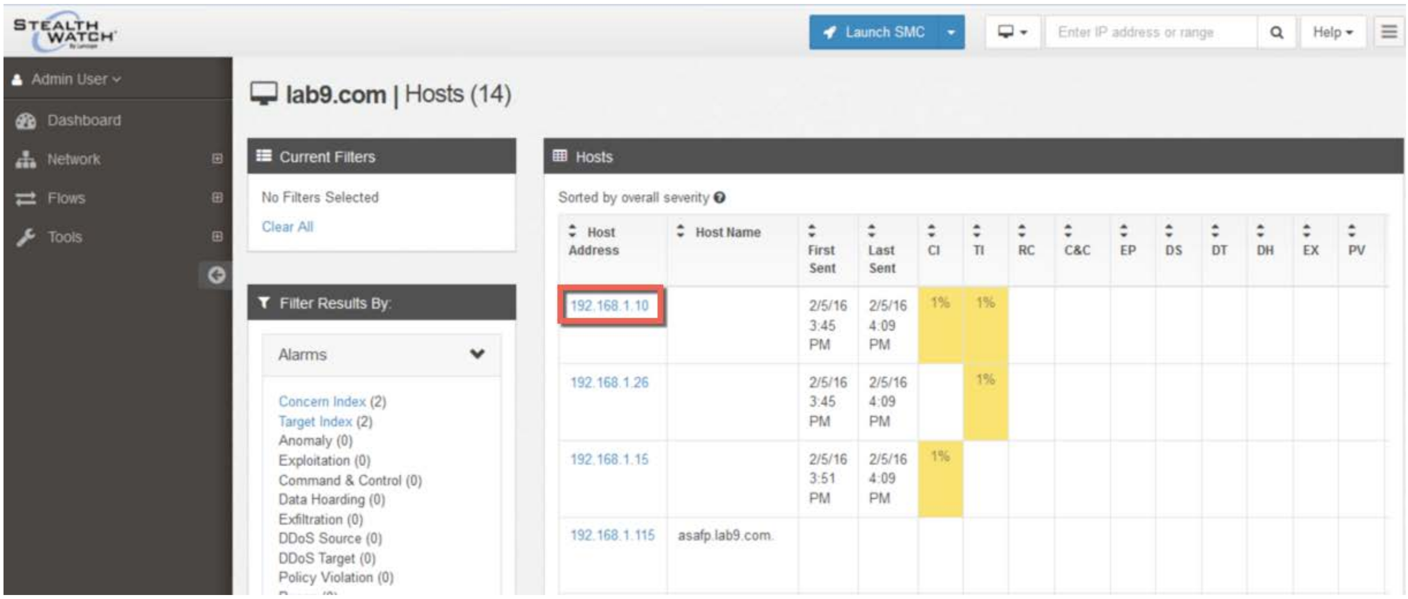
Exceptions (1)

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

Testing using CA-signed certs

In the following use case, an endpoint is quarantined/unquarantined.

Step 1 From the SMC, select **Network->Hosts** and select the desired endpoint that you will want to quarantine



lab9.com | Hosts (14)

Current Filters

No Filters Selected

Clear All

Filter Results By:

Alarms

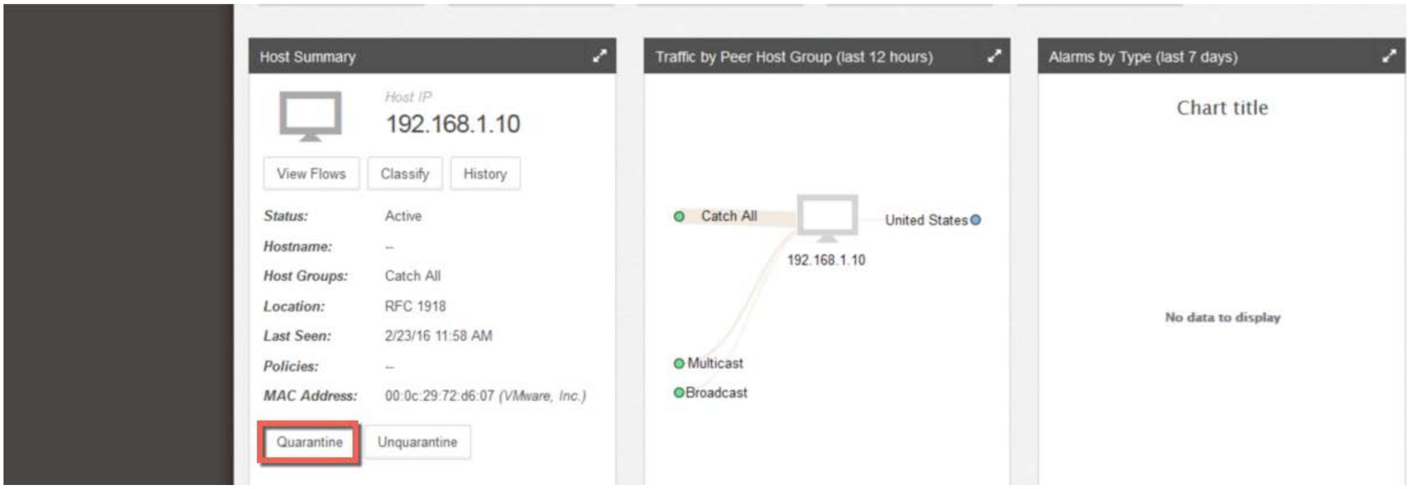
Concern Index (2)
Target Index (2)
Anomaly (0)
Exploitation (0)
Command & Control (0)
Data Hoarding (0)
Exfiltration (0)
DDoS Source (0)
DDoS Target (0)
Policy Violation (0)

Hosts

Sorted by overall severity

Host Address	Host Name	First Sent	Last Sent	CI	TI	RC	C&C	EP	DS	DT	DH	EX	PV
192.168.1.10		2/5/16 3:45 PM	2/5/16 4:09 PM	1%	1%								
192.168.1.26		2/5/16 3:45 PM	2/5/16 4:09 PM		1%								
192.168.1.15		2/5/16 3:51 PM	2/5/16 4:09 PM	1%									
192.168.1.115	asafp.lab9.com												

Step 2 Select the endpoint and then **"Quarantine"**



Host IP

192.168.1.10

Status: Active

Hostname: --

Host Groups: Catch All

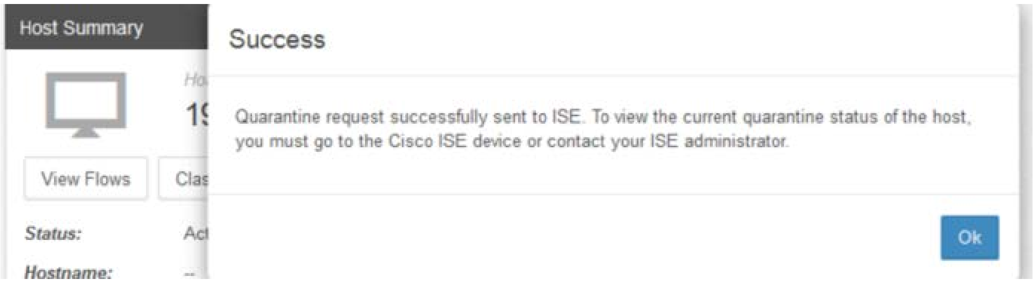
Location: RFC 1918

Last Seen: 2/23/16 11:58 AM

Policies: --

MAC Address: 00:0c:29:72:d6:07 (VMware, Inc.)

Step 3 You should see that the quarantine request message was successfully sent.

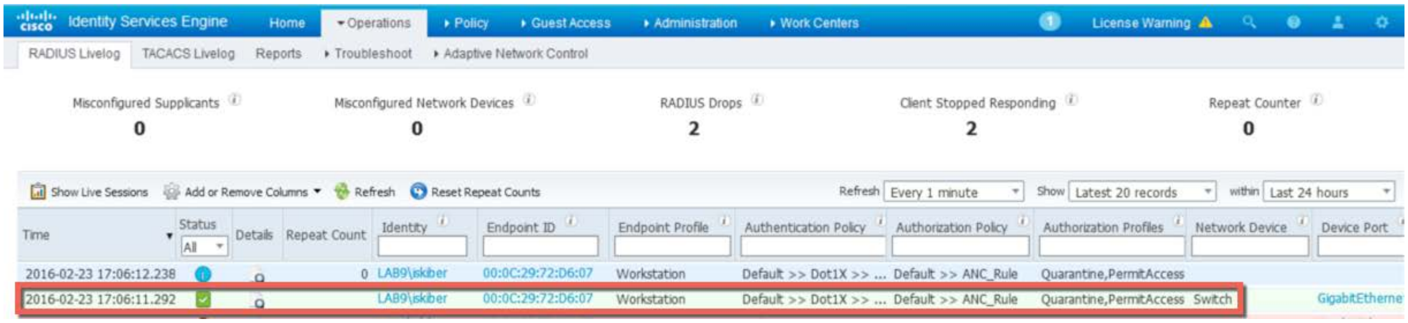


Success

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

Step 4 Select **OK**

Step 5 From the ISE Operations select **RADIUS Livelog** view you should see that the endpoint has been quarantined



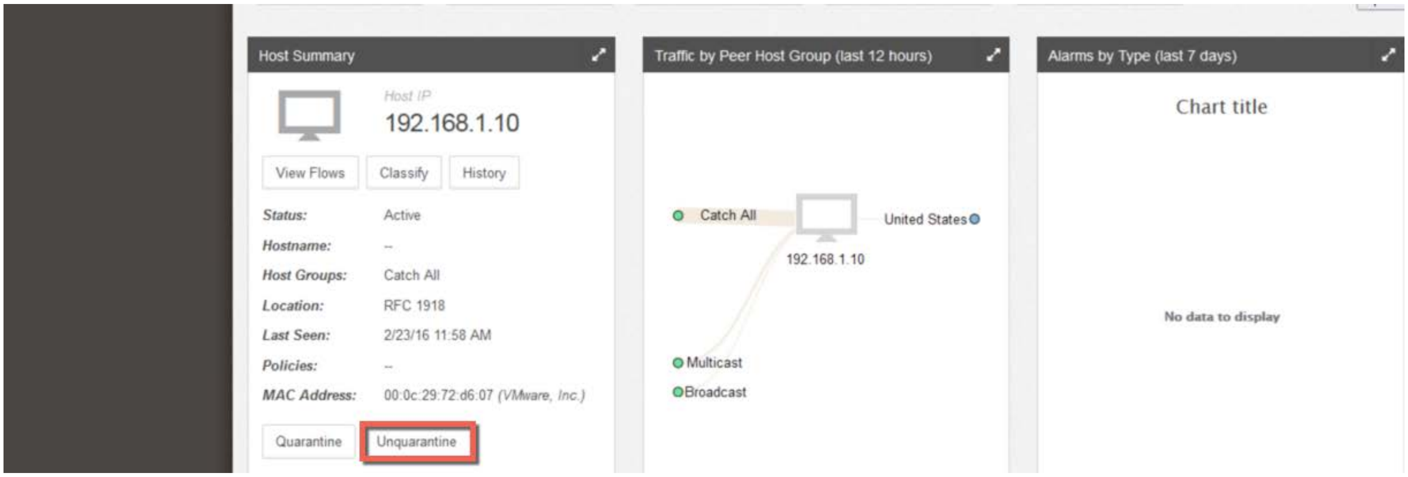
Misconfigured Supplicants	Misconfigured Network Devices	RADIUS Drops	Client Stopped Responding	Repeat Counter
0	0	2	2	0

Refresh: Every 1 minute; Show: Latest 20 records; within: Last 24 hours

Time	Status	Details	Repeat Count	Identity	Endpoint ID	Endpoint Profile	Authentication Policy	Authorization Policy	Authorization Profiles	Network Device	Device Port
	All										
2016-02-23 17:06:12.238	●		0	LAB9\iskiber	00:0C:29:72:D6:07	Workstation	Default >> Dot1X >> ...	Default >> ANC_Rule	Quarantine,PermitAccess		
2016-02-23 17:06:11.292	✓			LAB9\iskiber	00:0C:29:72:D6:07	Workstation	Default >> Dot1X >> ...	Default >> ANC_Rule	Quarantine,PermitAccess	Switch	GigabitEtherne

Step 6 Next, let's unquarantine the endpoint. Select the endpoint, and then **"Unquarantine"**.

Note: In ISE 2.0, there is no manual way to unquarantine the endpoint, this must be done through the SMC, or you can use the EPS unquarantine RESTFUL API. There should be a future patch that will address this issue.

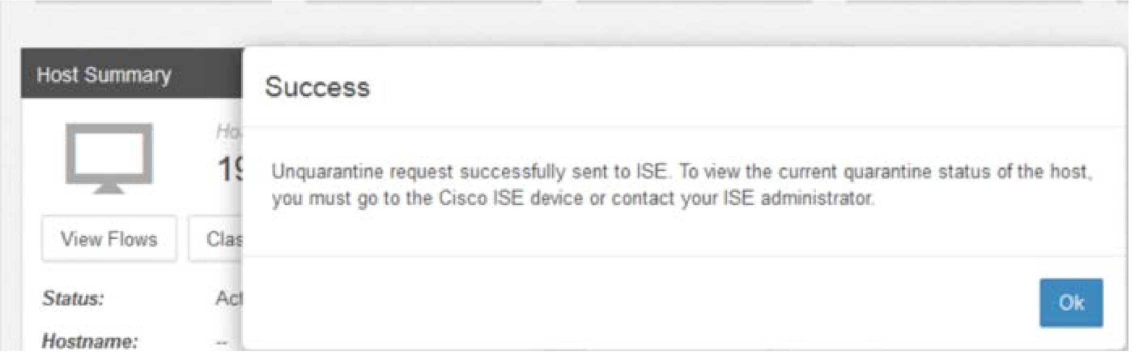


Host Summary

Host IP: 192.168.1.10

Status:	Active
Hostname:	--
Host Groups:	Catch All
Location:	RFC 1918
Last Seen:	2/23/16 11:58 AM
Policies:	--
MAC Address:	00:0c:29:72:d6:07 (VMware, Inc.)

Step 7 You should see that the unquarantine message was successfully sent.

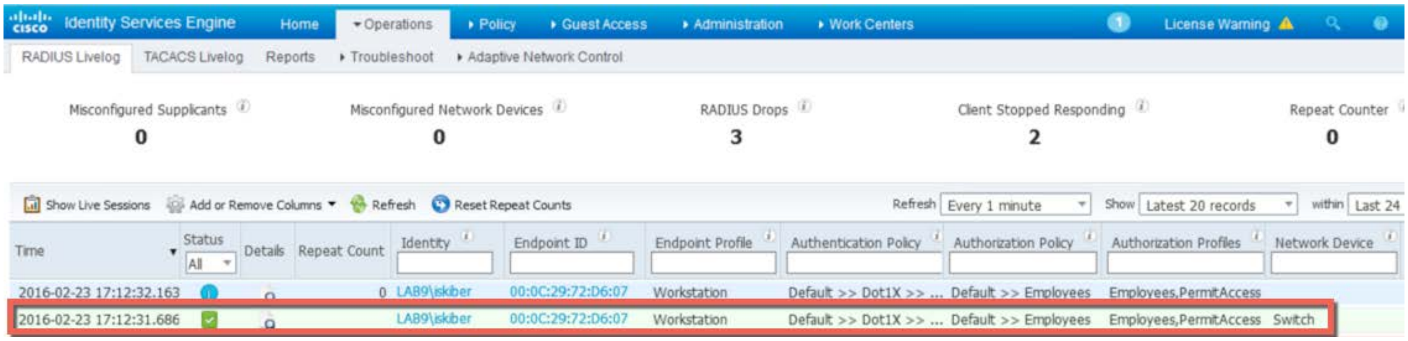


Success

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

Step 8 Select **OK**

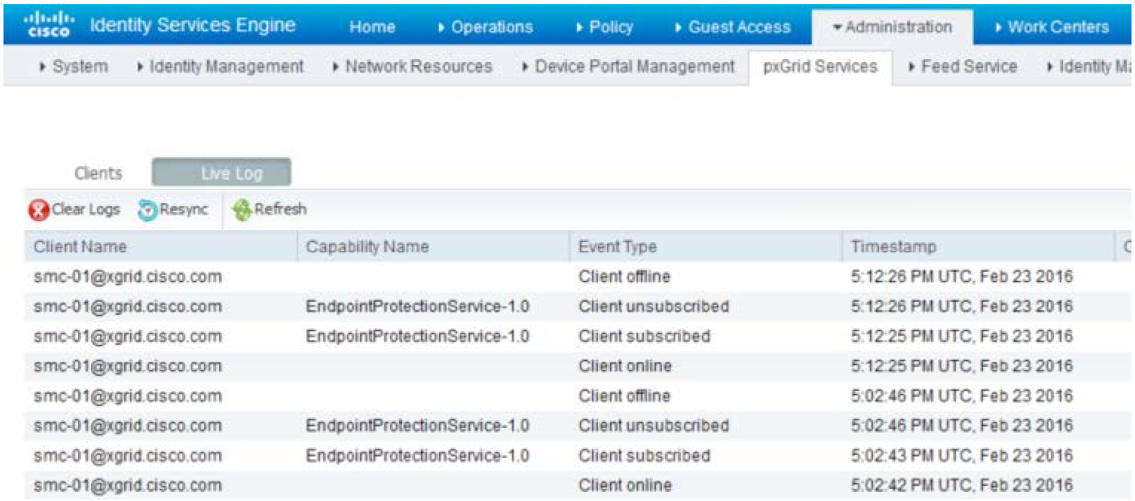
Step 9 From the **ISE Operations** select **RADIUS Livelog** view, note the endpoint has been unquarantined



Misconfigured Supplicants	Misconfigured Network Devices	RADIUS Drops	Client Stopped Responding	Repeat Counter
0	0	3	2	0

Time	Status	Details	Repeat Count	Identity	Endpoint ID	Endpoint Profile	Authentication Policy	Authorization Policy	Authorization Profiles	Network Device
2016-02-23 17:12:32.163	●		0	LAB9\iskiber	00:0C:29:72:D6:07	Workstation	Default >> Dot1X >> ...	Default >> Employees	Employees,PermitAccess	
2016-02-23 17:12:31.686	✓			LAB9\iskiber	00:0C:29:72:D6:07	Workstation	Default >> Dot1X >> ...	Default >> Employees	Employees,PermitAccess	Switch

Step 10 Note the pxGrid client live logs for the SMC, which indicates the time when the smc has subscribed to the EndpointProtection Service Capability to intiate the quarantine/unquarantine (ANC) Adaptive Network Control mitigation actions.

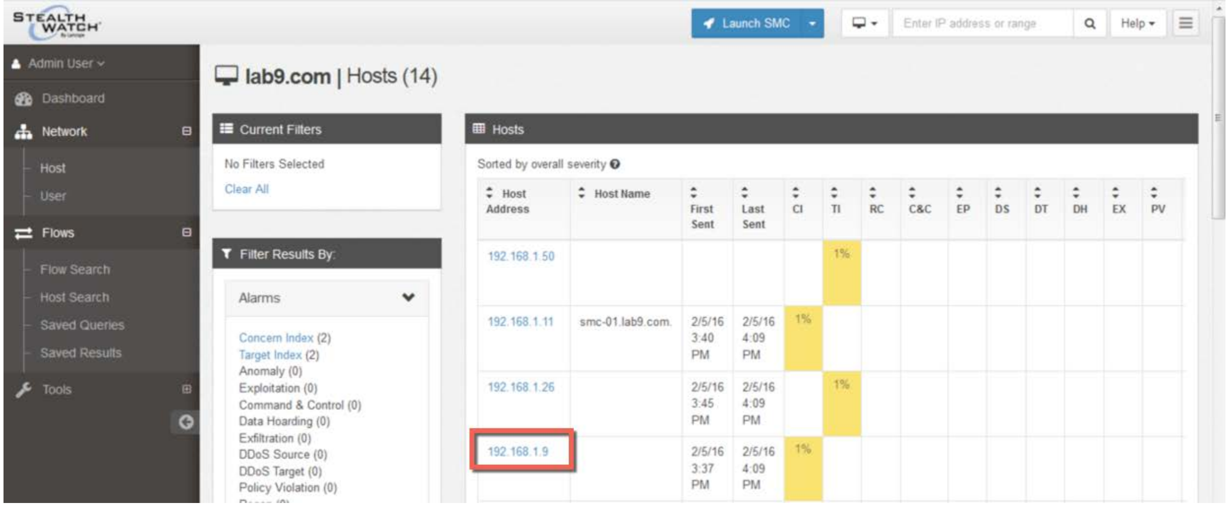


Client Name	Capability Name	Event Type	Timestamp
smc-01@xgrid.cisco.com		Client offline	5:12:26 PM UTC, Feb 23 2016
smc-01@xgrid.cisco.com	EndpointProtectionService-1.0	Client unsubscribed	5:12:26 PM UTC, Feb 23 2016
smc-01@xgrid.cisco.com	EndpointProtectionService-1.0	Client subscribed	5:12:25 PM UTC, Feb 23 2016
smc-01@xgrid.cisco.com		Client online	5:12:25 PM UTC, Feb 23 2016
smc-01@xgrid.cisco.com		Client offline	5:02:46 PM UTC, Feb 23 2016
smc-01@xgrid.cisco.com	EndpointProtectionService-1.0	Client unsubscribed	5:02:46 PM UTC, Feb 23 2016
smc-01@xgrid.cisco.com	EndpointProtectionService-1.0	Client subscribed	5:02:43 PM UTC, Feb 23 2016
smc-01@xgrid.cisco.com		Client online	5:02:42 PM UTC, Feb 23 2016

Testing Using Self-Signed Certs

In the following use case, an endpoint is quarantined/unquarantined.

Step 1 From the SMC, select the 192.168.1.9 host under Network->Host menu



lab9.com | Hosts (14)

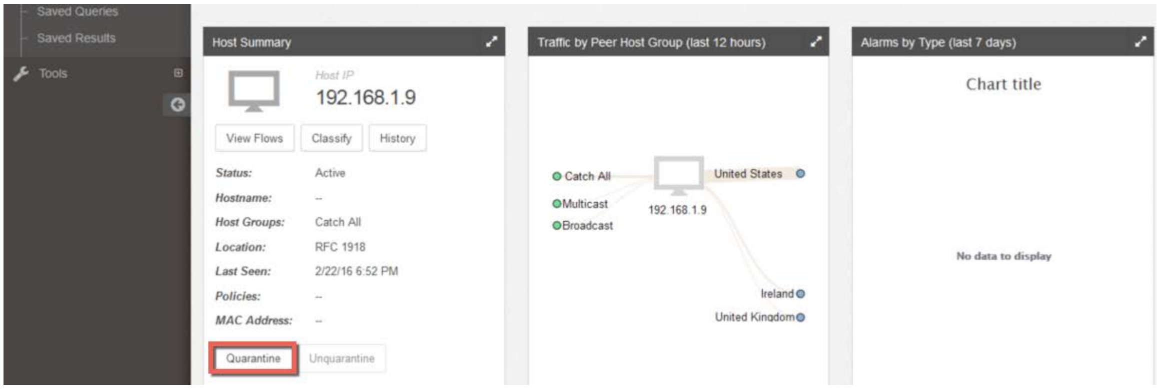
No Filters Selected
Clear All

Concern Index (2)
Target Index (2)
Anomaly (0)
Exploitation (0)
Command & Control (0)
Data Hoarding (0)
Exfiltration (0)
DDoS Source (0)
DDoS Target (0)
Policy Violation (0)

Sorted by overall severity

Host Address	Host Name	First Sent	Last Sent	CI	TI	RC	C&C	EP	DS	DT	DH	EX	PV
192.168.1.50					1%								
192.168.1.11	smc-01.lab9.com.	2/5/16 3:40 PM	2/5/16 4:09 PM	1%									
192.168.1.26		2/5/16 3:45 PM	2/5/16 4:09 PM		1%								
192.168.1.9		2/5/16 3:37 PM	2/5/16 4:09 PM	1%									

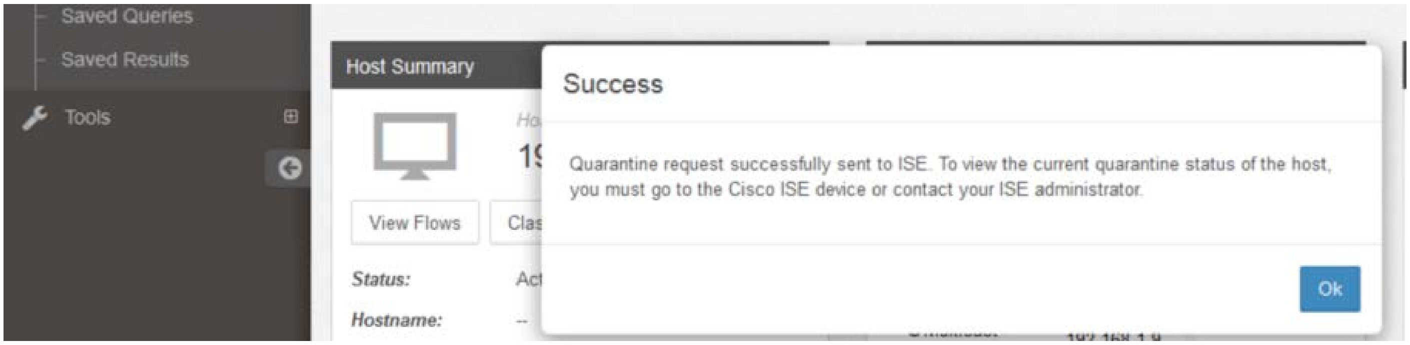
Step 2 You should see the following:



Host IP
192.168.1.9

Status: Active
Hostname: --
Host Groups: Catch All
Location: RFC 1918
Last Seen: 2/22/16 6:52 PM
Policies: --
MAC Address: --

Step 3 Select Quarantine, you should see the endpoint has been quarantined successfully



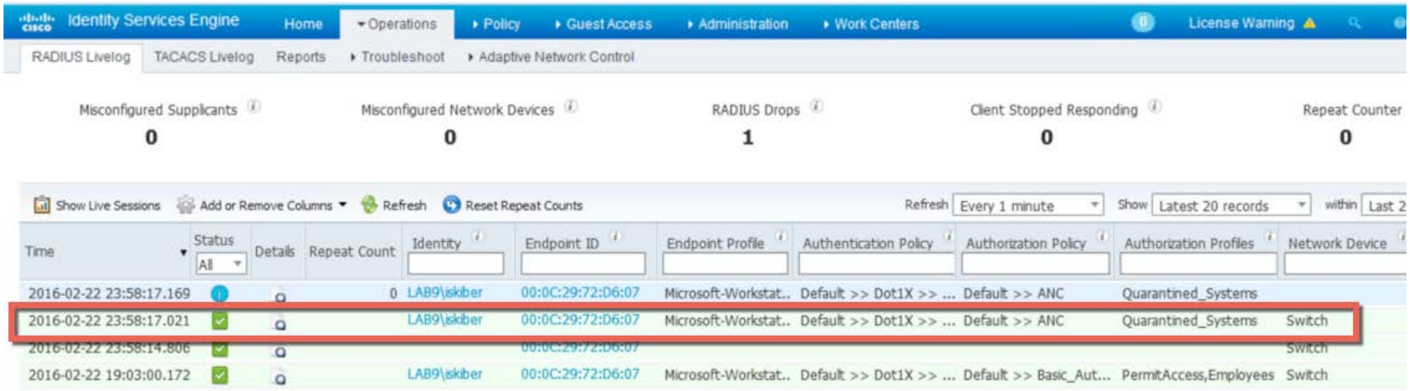
Success

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

Ok

Step 4 Select **OK**

Step 5 View the quarantined endpoint

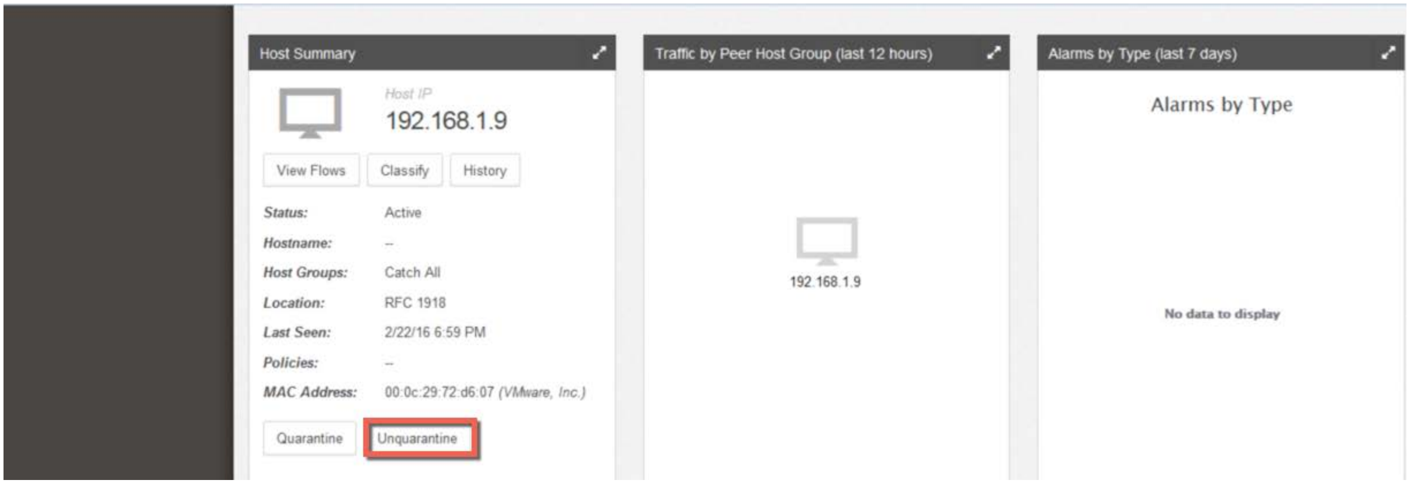


Misconfigured Supplicants	Misconfigured Network Devices	RADIUS Drops	Client Stopped Responding	Repeat Counter
0	0	1	0	0

Refresh: Every 1 minute — Show: Latest 20 records — within: Last 2

Time	Status	Details	Repeat Count	Identity	Endpoint ID	Endpoint Profile	Authentication Policy	Authorization Policy	Authorization Profiles	Network Device
	All									
2016-02-22 23:58:17.169	●		0	LAB9\iskiber	00:0C:29:72:D6:07	Microsoft-Workstat..	Default >> Dot1X >> ...	Default >> ANC	Quarantined_Systems	
2016-02-22 23:58:17.021	☑			LAB9\iskiber	00:0C:29:72:D6:07	Microsoft-Workstat..	Default >> Dot1X >> ...	Default >> ANC	Quarantined_Systems	Switch
2016-02-22 23:58:14.806	☑				00:0C:29:72:D6:07					Switch
2016-02-22 19:03:00.172	☑			LAB9\iskiber	00:0C:29:72:D6:07	Microsoft-Workstat..	Default >> Dot1X >> ...	Default >> Basic_Aut...	PermitAccess,Employees	Switch

Step 6 To unquarantine the endpoint, select unquarantine from the SMC operations menu


Traffic by Peer Host Group (last 12 hours)
192.168.1.9
Alarms by Type (last 7 days)
Alarms by Type
No data to display

Host Summary

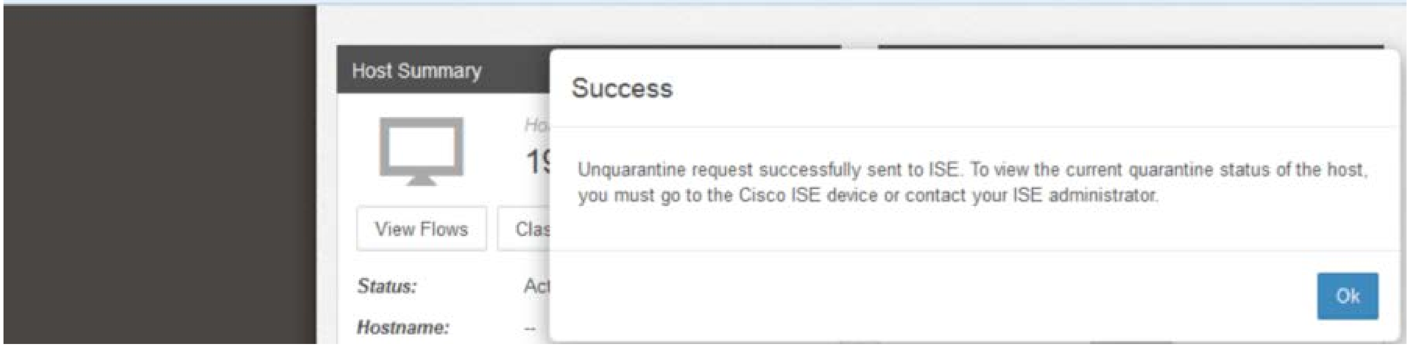
Host IP
192.168.1.9

View Flows Classify History

Status: Active
Hostname: --
Host Groups: Catch All
Location: RFC 1918
Last Seen: 2/22/16 6:59 PM
Policies: --
MAC Address: 00:0c:29:72:d6:07 (VMware, Inc.)

Quarantine Unquarantine

Step 7 You should see the unquarantine results successfully sent, select OK

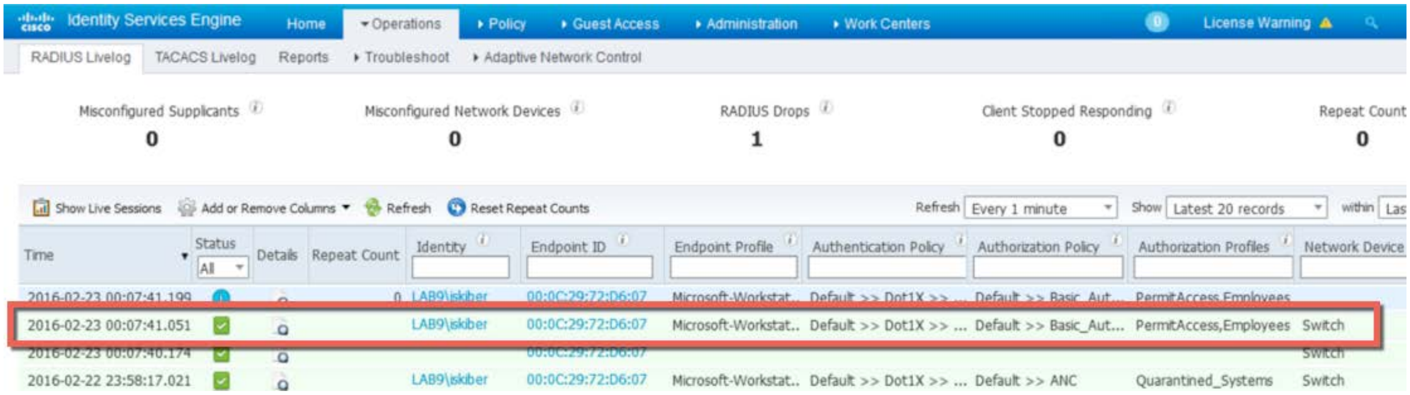


Success

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

Ok

Step 8 From the ISE menu, select Operations->**RADIUS Livelog**, you should see that the endpoint has been unquarantined

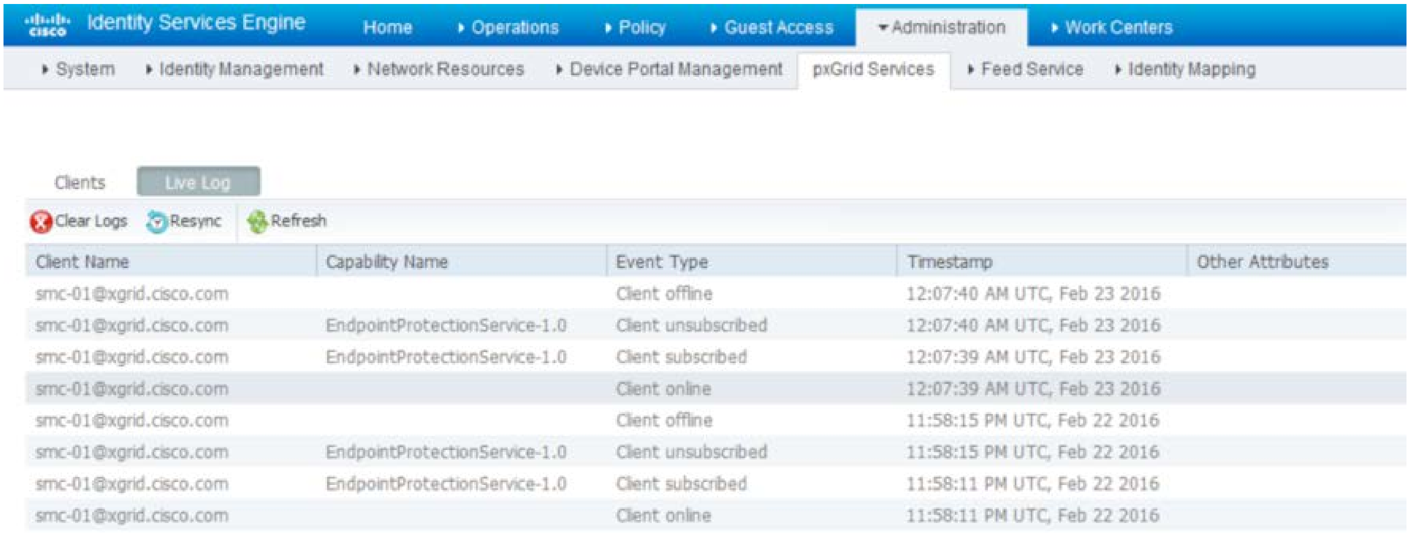


Misconfigured Supplicants	Misconfigured Network Devices	RADIUS Drops	Client Stopped Responding	Repeat Count
0	0	1	0	0

Refresh Every 1 minute Show Latest 20 records within Las

Time	Status All	Details	Repeat Count	Identity	Endpoint ID	Endpoint Profile	Authentication Policy	Authorization Policy	Authorization Profiles	Network Device
2016-02-23 00:07:41.199	●		0	LAB9\iskiber	00:0C:29:72:D6:07	Microsoft-Workstat..	Default >> Dot1X >> ...	Default >> Basic_Aut...	PermitAccess,Employees	
2016-02-23 00:07:41.051	✓			LAB9\iskiber	00:0C:29:72:D6:07	Microsoft-Workstat..	Default >> Dot1X >> ...	Default >> Basic_Aut...	PermitAccess,Employees	Switch
2016-02-23 00:07:40.174	✓				00:0C:29:72:D6:07					Switch
2016-02-22 23:58:17.021	✓			LAB9\iskiber	00:0C:29:72:D6:07	Microsoft-Workstat..	Default >> Dot1X >> ...	Default >> ANC	Quarantined_Systems	Switch

Step 9 Note the smc pxGrid client Live Logs which indicate the times that the smc has subscribed to the EndpointProtectionService capability and performed the ANC quarantine/unquarantine mitigation actions.



Client Name	Capability Name	Event Type	Timestamp	Other Attributes
smc-01@xgrid.cisco.com		Client offline	12:07:40 AM UTC, Feb 23 2016	
smc-01@xgrid.cisco.com	EndpointProtectionService-1.0	Client unsubscribed	12:07:40 AM UTC, Feb 23 2016	
smc-01@xgrid.cisco.com	EndpointProtectionService-1.0	Client subscribed	12:07:39 AM UTC, Feb 23 2016	
smc-01@xgrid.cisco.com		Client online	12:07:39 AM UTC, Feb 23 2016	
smc-01@xgrid.cisco.com		Client offline	11:58:15 PM UTC, Feb 22 2016	
smc-01@xgrid.cisco.com	EndpointProtectionService-1.0	Client unsubscribed	11:58:15 PM UTC, Feb 22 2016	
smc-01@xgrid.cisco.com	EndpointProtectionService-1.0	Client subscribed	11:58:11 PM UTC, Feb 22 2016	
smc-01@xgrid.cisco.com		Client online	11:58:11 PM UTC, Feb 22 2016	

References

Other pxGrid documents can be found at: http://www.cisco.com/c/en/us/support/security/identity-services-engine/products-implementation-design-guides-list.html

- Deploying Certificates with pxGrid: using Self-Signed pxGrid client and self-signed ISE pxGrid node certificate
- Deploying Certificates with pxGrid: Certificate Authority (CA) signed pxGrid client and self-signed ISE pxGrid node certificate
- Deploying Certificates with pxGrid: Certificate Authority (CA) signed pxGrid client and CA-signed ISE pxGrid node certificate
- Configure and Test Integration with Cisco pxGrid

Appendices

Enabling SSH on MAC

Step 1 Enable ssh on MC

```
Johns-Macbook-Pro:Utilities jeppich$ sudo launchctl load -w /System/Library/LaunchDaemons/ssh.plist
Johns-Macbook-Pro:Utilities jeppich$
```

Step 2 Copying files over from SMC to local PC

```
Dddd smc:~# scp smc1.crt jeppich@10.0.0.5:/Applications/ise14_certs/
Password:
smc1.crt                                      100% 1330     1.3KB/s   00:00
smc:~# ls
jeppich@10.0.0.5  smc1.crt  smc1.csr  smc1.key  smc1.key.org
smc:~# scp smc1.key jeppich@10.0.0.5:/Applications/ise14_certs/
Password:
smc1.key                                      100% 1675     1.6KB/s   00:00
smc:~#
```

Troubleshooting

Using pxGrid-Active Standby configuration

There can only be two pxGrid nodes per ISE deployment. Only one ISE pxGrid node can be active, check “application status ise” to see that you have the correct ISE pxGrid node active.

SMC ANC Mitigation Error Message: Quarantine request failed to be sent to ISE

Under Administration->pxGrid services assign the SMC registered client into EPS group

No connectivity to pxGrid in ISE pxGrid node

For Certificate Authority (CA)-signed certificates, ensure you have the root CA certificate in the ISE trusted system certificate store, and the ISE pxGrid node certificate in the ISE system certificate store. The pxGrid client certificate must have an EKU of both client authentication and server authentication.

For ISE self-signed certificates, the self-signed Identity certificate must be exported from the system certificate store and imported into the ISE trusted system certificate store. This is not required in ISE 2.0