Using ISE 2.1 Internal Certificate Authority (CA) to Deploy Certificates to Cisco Platform Exchange Grid (pxGrid) Clients

Author: John Eppich

Table of Contents

About This Document **4**

Technical Details **5**

Creating Certificate Provisioning Portal **7**

Configuring Certificate Provisioning Portal 7

Creating Admin User for provisioning certificates 9

Configuring ISE for pxGrid Operation **11**

Generating and Issuing CSR request for ISE pxGrid node 11

Importing ISE CA certificate into ISE Trusted System Store 12

Importing ISE pxGrid node certificate into ISE system certificate store 14

Verify ISE published pxGrid clients appear 15

Cisco Firesight 5.4 ..... **16**

Generating and Issuing pxGrid Client Certificate from ISE Certificate Provisioning Portal 16

Importing ISE and pxGrid client certificates 18

Cisco Firepower 6.1 ..... **21**

Generating and Issuing pxGrid Client Certificate from ISE Certificate Provisioning Portal 21

Configuring Identity Source 23

Create Firepower 6.1 Realm 25

Configure ISE Identity Policy for Passive Authentication 27

Create Access Rule 28

Create pxGrid IPS Policy 29

Create Quarantine and UnQuarantine Remediation Types 31

Create Quarantine and Unquarantine Correlation Policies 33

Testing Cisco Firepower 6.1 Quarantine and Unquarantine Adaptive Network Control (ANC) Mitigation Actions 36

Splunk for ISE Add-On 2.20 ..... **41**

Generating Splunk pxGrid Client Certificate from ISE Certificate Provisioning Portal 41

Installing ISE and Splunk pxGrid client certificate using Java keystores 42

Testing Connection Between Splunk and the ISE pxGrid node 45

Testing Splunk Quarantine and UnQuarantine Adaptive Network Control (ANC) Mitigation Actions 46

Stealthwatch 50

Generating Stealthwatch pxGrid Client Certificate from ISE Certificate Provisioning Portal 50

Importing ISE and pxGrid client certificates 51

Configuring ISE pxGrid node 55

SMC Client Configuration 62

Testing Stealthwatch Quarantine and Unquarantine Adaptive Network Control (ANC) Mitigation actions 65

Web Security Appliance (WSA) 67

Generating WSA pxGrid client Certificate from ISE Certificate Provisioning Portal 67

Installing ISE and pxGrid client certificates 68

Testing Configuration between the WSA and the ISE pxGrid node 74

USE CASE: Denying Employees with a SGT Tag Access to Gambling Sites 76

Creating an Identification Profile 76

Creating Web Access Security Policy for Employees Denying Access to Gambling Sites 77

End-User Testing 79

References 82

About This Document

This document is for Cisco Engineers and customers deploying who are interested in deploying Cisco Identity Services Engine (ISE) 2.1 Internal Certificate Authority (CA) for Cisco platform Exchange Grid (pxGrid clients). This serves as a replacement for using an external CA server such as Microsoft and a customized pxGrid template for deploying to pxGrid ecosystem partners and Cisco Security Solutions.

This eases pxGrid deployment by using ISE as the CA server. Cisco Security Solutions and pxGrid ecosystem client certificates are generated and issued by the ISE certificate-provisioning portal using a built-in pxGrid template.

The pxGrid client certificate can either be in Privacy Enhanced Mail (PEM) or Public-Key Cryptography Standards (PKCS12) format pending how the solution is implemented with pxGrid. The PEM format is a base64 translation of the X509 ASN.1 keys and contains the certificate public-private key pairs of the pxGrid client, the ISE CA root certificate, the ISE EndpointSubCA, and the ISE Services node certificate. The PKCS 12 file originally defined by RSA in the Public-Key Cryptography Standards contains both the public and private key certificate pairs and is fully encrypted unlike PEM files.

pxGrid "C" client implementations will use the PEM format for their certificates. pxGrid client "Java" client implementations will use the PKCS 12 file format and convert this over to use the Java keystore, which is the "truststore" of the security solution.

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

- Cisco Firesight 5.4
- Cisco Firepower 6.1
- Splunk for ISE Add-on 2.20 (can be used for other security solutions using java keystores)
- Stealthwatch 6.8.2
- Cisco Web Security Appliance 9.0.1 build 162

Technical Details

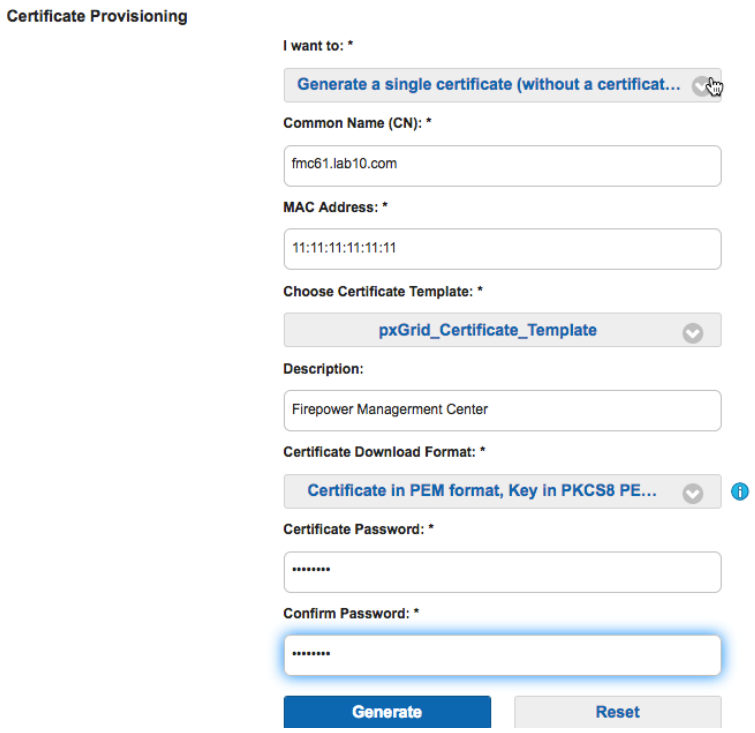
Initially the ISE admin will determine the pxGrid client request. In this document, "Generate a single certificate (without a certificate request) will be generated for the pxGrid clients. "Generating a single certificate with certificate signing request" will be in ISE 2.2.

The Common Name (CN) Fully Qualified Domain Name (FQDN), MAC address and certificate description of the pxGrid client are required. Please make sure all pxGrid clients and ISE are FQDN resolvable or there will be connection issues with the ISE pxGrid node.

The pxGrid template is built-in you no longer need to create a customized pxGrid template containing an EKU for both server and client authentication if you were using an alternate CA server.

The Certificate Download format determines either the PEM or PKCS 12 format. In this document, for the pxGrid clients, Cisco Firesight 5.4, Cisco Firepower 6.1 and Stealthwatch 6.8.2 we will be using the PEM file format. We will use the PKCS 12 file format for Splunk.

The encryption key password is required for generating the certificates



The certificate will be generated as a .ZIP file and contains either PEM or PKCS 12 file formats.

The PEM file will contain the pxGrid client certificate public and private key-pairs, the ISE CA Root certificate, ISE EndpointSubCA certificate, and ISE ServicesNode certificate.

CertificateServicesEndpointSubCA-ise21internalCA_.cer	Yesterday 12:28 AM	2 KB	certificate
CertificateServicesNodeCA-ise21internalCA_.cer	Yesterday 12:28 AM	2 KB	certificate
CertificateServicesRootCA-ise21internalCA_.cer	Yesterday 12:28 AM	2 KB	certificate
sfdc1.lab10.com_00-50-56-86-ab-99.cer	Yesterday 12:28 AM	2 KB	certificate
sfdc1.lab10.com_00-50-56-86-ab-99.key	Yesterday 12:28 AM	2 KB	Keyno...ument

The CertificateServicesRootCA-ise21internalCA_.cer contains the ISE Root CA that will get imported into the trust store of the pxGrid client solution.

The sfdc1.lab10.com_00-50-56-86-ab-99.cer and sfdc1.lab10.com_00-50-56-86-ab-99.key are the public and private key pairs of the pxGrid client certificate that will also get import into the trust store of the pxGrid client solution.

The CertificateServicesEndpointSubCA-ise21internalCA_.cer is the sub CA that gets assigned to the endpoints.

The CertificateServicesNode CA-ise21internalCA_.cer is the certificate used for downloading active bulk session records from the ISE MnT node or in a Stand-Alone ISE environment, the ISE node.

The PKCS 12 file contains the encrypted container for the public and private key pair of the pxGrid client certificate, and the ISE CA root certificate and the certificate chain.

certops-2016-08-19_02-21-03.zip	Aug 18, 2016 10:21 PM	8 KB	ZIP archive
Johns-Macbook-Pro.lab10.com_f0-de-f1-94-65-9c.p12	Aug 19, 2016 2:21 AM	8 KB	perso...ge file

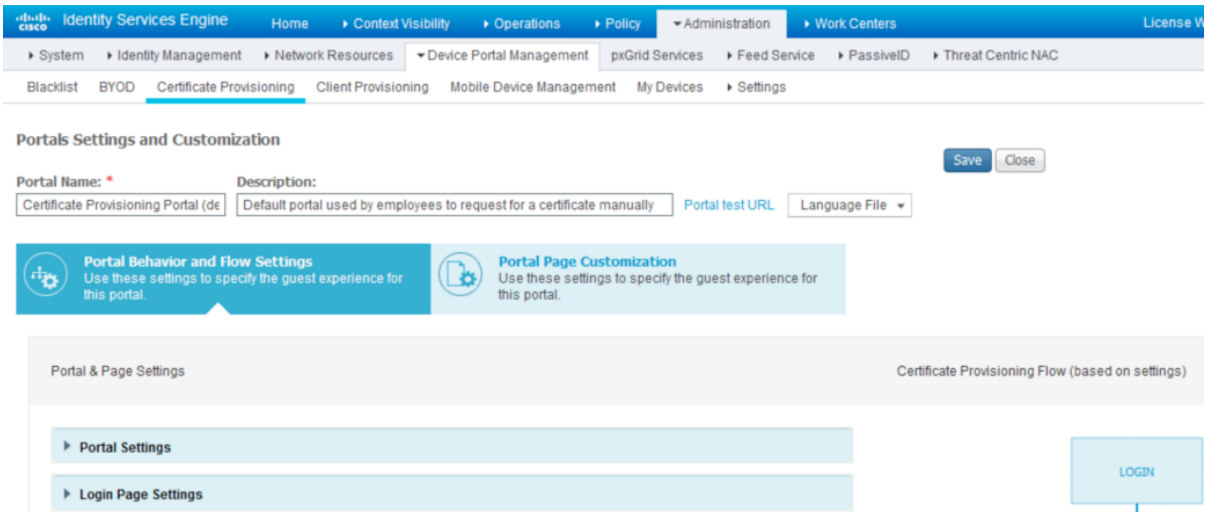
From this .p12 filename the public and private key-pairs from the certificate will be imported into pxGrid client's java keystores using the Java keytool command.

Creating Certificate Provisioning Portal

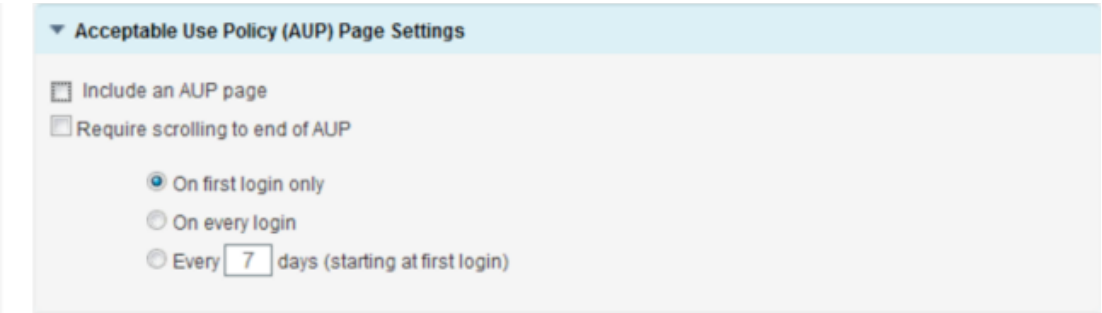
This section describes the procedures for creating and configuring the ISE certificate provisioning portal.

Configuring Certificate Provisioning Portal

Step 1 Select **Administration->Device Portal Management->Certificate Provisioning->Certificate Provisioning Portal (default)**

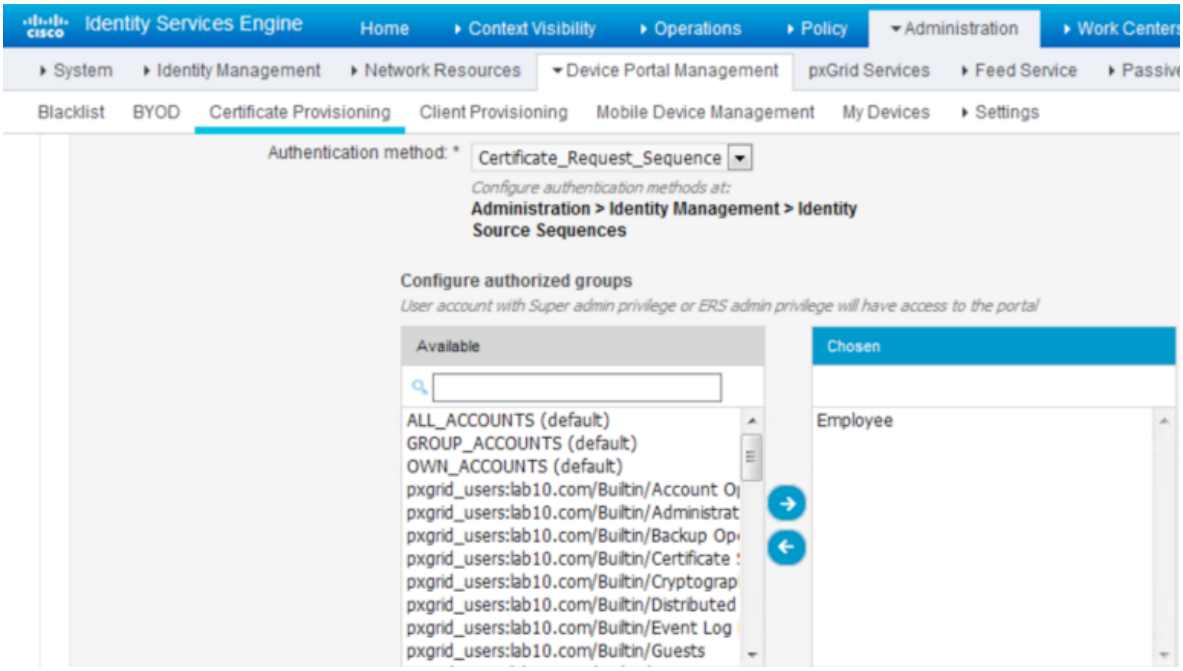


Step 2 Under **Acceptable Usage Policy (AUP) Page settings**, **uncheck or disable** Include and AUP page

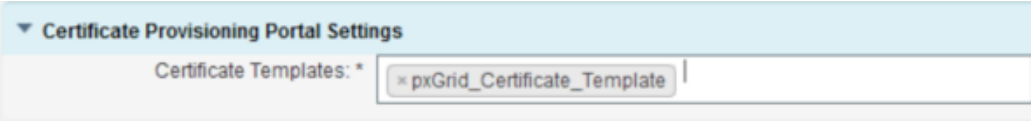


Step 3 Under **Post-Login Banner Page Settings**, **uncheck or disable Include a Post-Login Banner page**

Step 4 Under **Portal and Page Settings** Select **Portal Settings,** select authorized group to access the portal. Under Configure authorized groups, select the authorized group



Step 5 Under **Certificate Portal and Provisioning Settings->Certificate Template,** select **pxGrid Template**

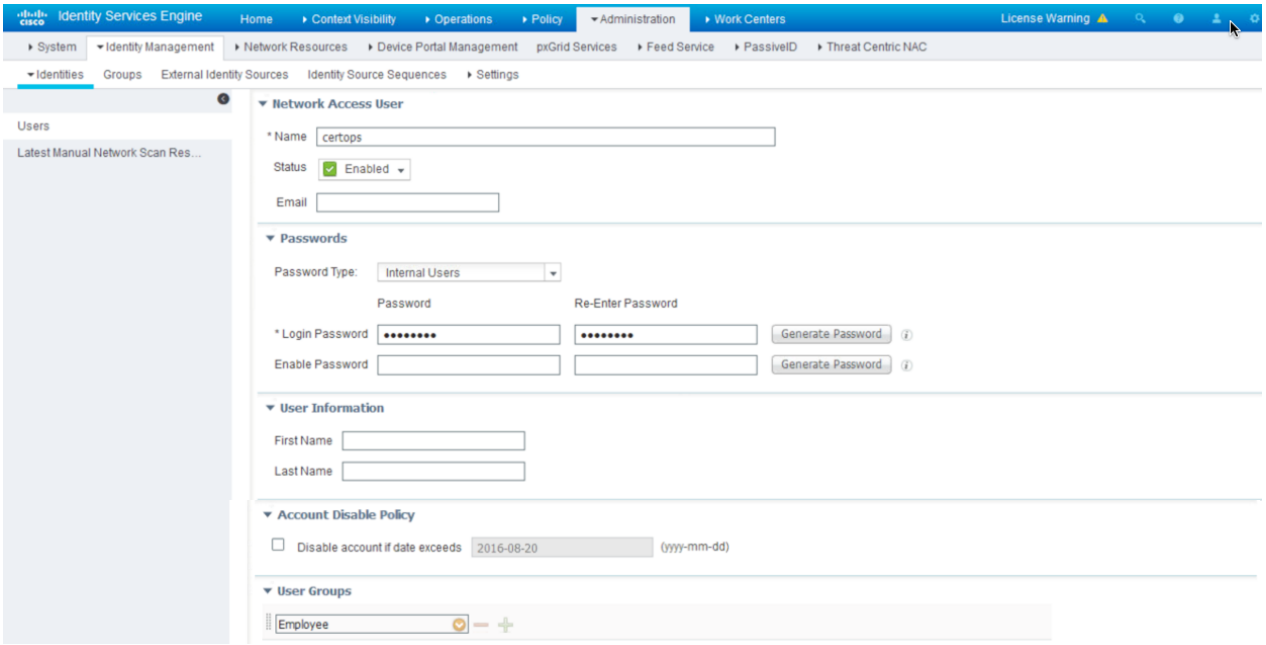


Step 6 Under **Save**

Creating Admin User for provisioning certificates

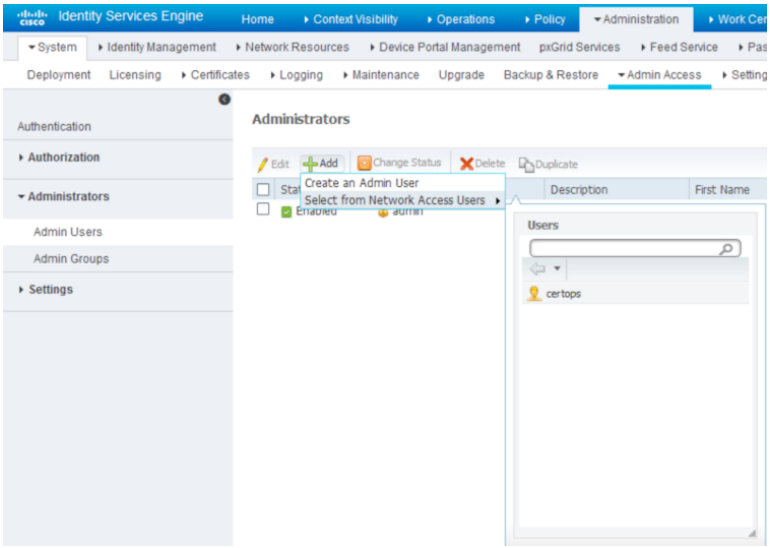
An ISE internal user is created for generating and issuing the pxGrid client requests.

Step 1 Select **Administration->Identity Management->Identities->Users->Add**, enter **Name**, **Login Password** and select the **user group**



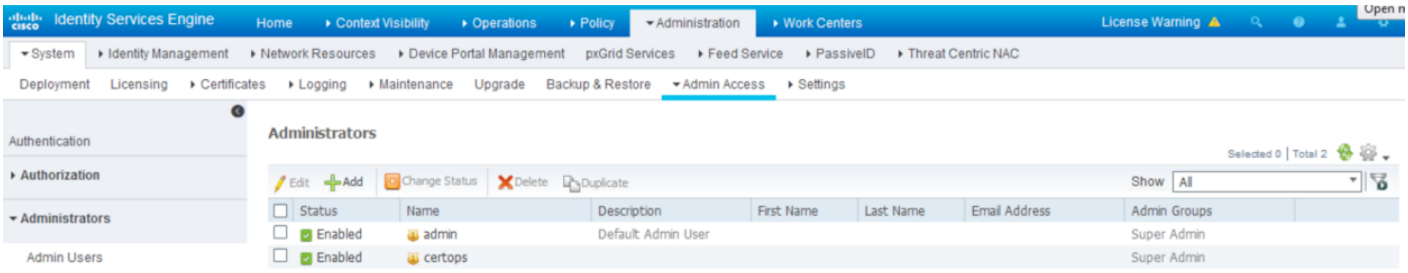
Step 2 Select **Save**

Step 3 Select **Administration->System->Admin Access->Administrators-Add-Select From Network Access Users**



Step 4 From the **Admin Group drop-down**, select **Super Admin,** then **Save**

Step 5 Verify that the certificate ops user account has been created.

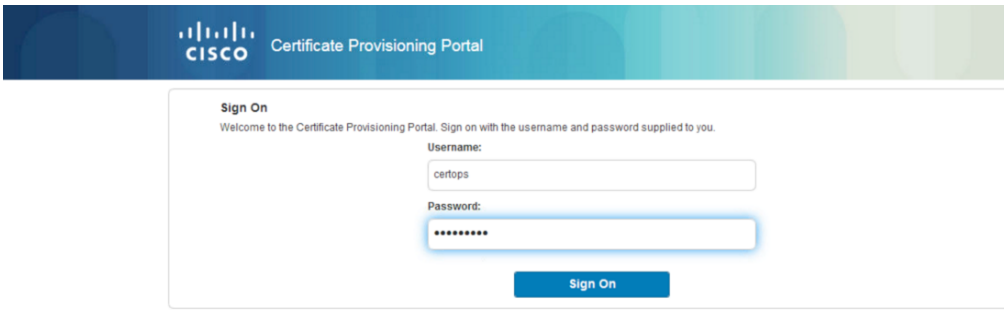

Identity Services Engine
Home
Context Visibility
Operations
Policy
Administration
Work Centers
License Warning
System
Identity Management
Network Resources
Device Portal Management
pxGrid Services
Feed Service
PassiveID
Threat Centric NAC
Deployment
Licensing
Certificates
Logging
Maintenance
Upgrade
Backup & Restore
Admin Access
Settings
Authentication
Authorization
Administrators
Admin Users
Administrators
Selected 0 | Total 2
Edit
Add
Change Status
Delete
Duplicate
Show
All
Status
Name
Description
First Name
Last Name
Email Address
Admin Groups
Enabled
admin
Default Admin User
Super Admin
Enabled
certops
Super Admin

Configuring ISE for pxGrid Operation

This section describes the procedure for creating the ISE pxGrid certificate for the ISE pxGrid node.

Generating and Issuing CSR request for ISE pxGrid node

Step 1 Select **Administration->Device Portal Management->Certificate Provisioning->Certificate Provisioning Details->Certificate Provisioning Portal(Default)-Portal Test** and Sign On with the certificate ops user account



Step 2 Under **Certificate Provisioning**, **I want to**, select Generate a single certificate (without a certificate signing request)

Step 3 Enter the **Common Name (CN)**, FQDN of the ISE pxGrid node

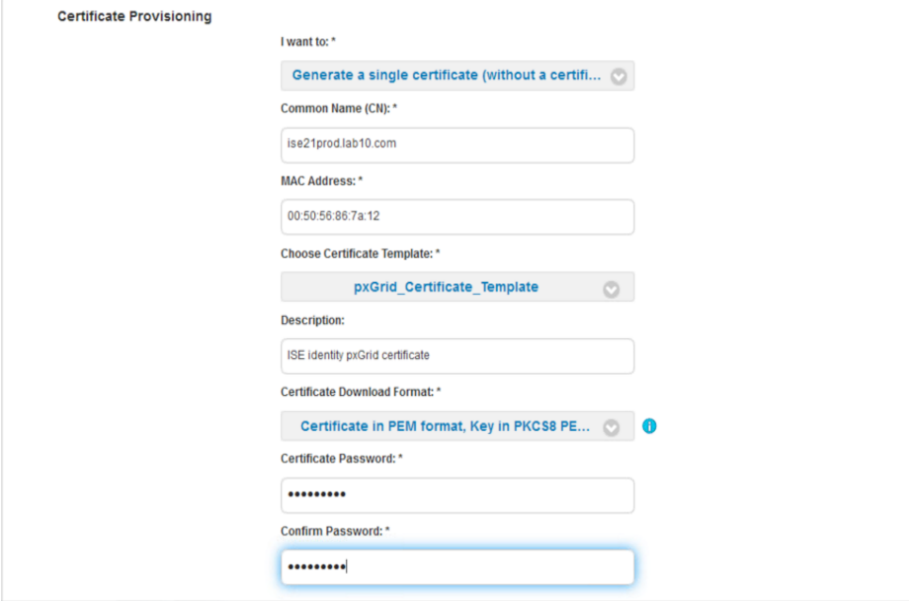
Step 4 Enter the **MAC address** of the ISE pxGrid node

Step 5 Choose the **pxGrid Certificate Template**

Step 6 Enter an optional Description

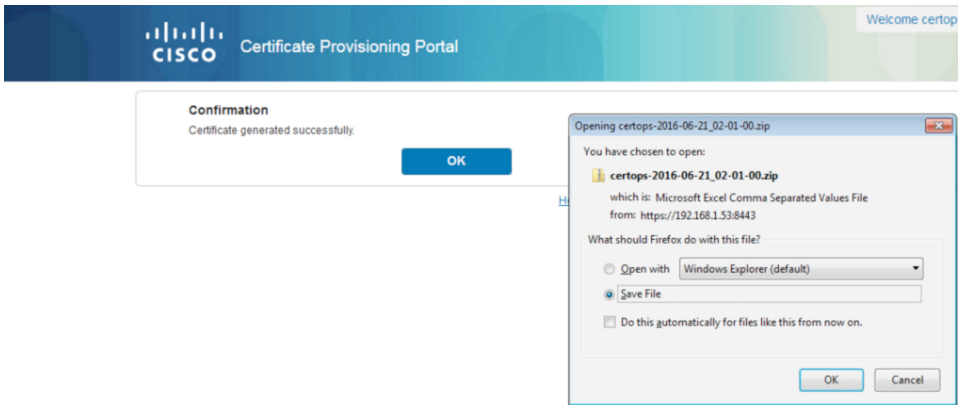
Step 7 From the **Certificate Download Format** Drop-down, select **Certificate in PEM format, including certificate chain**

Step 8 Enter the certificate password, this can be anything. In this example, **ISEisC00L** was used



Step 9 Select **Generate**

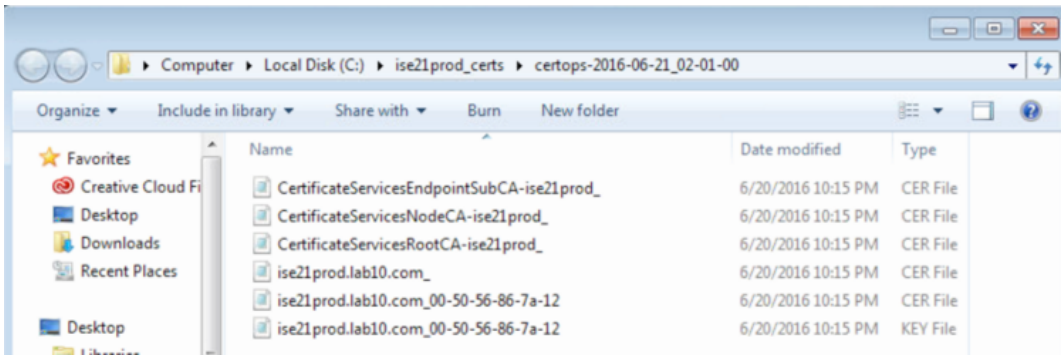
Step 10 The file will be saved as a .zip file



Step 11 Select **OK** to complete the download

Step 12 Select **OK** to complete the certificate generation process.

Step 13 Copy the zipped file over to a folder and extract the files, you should see the following:

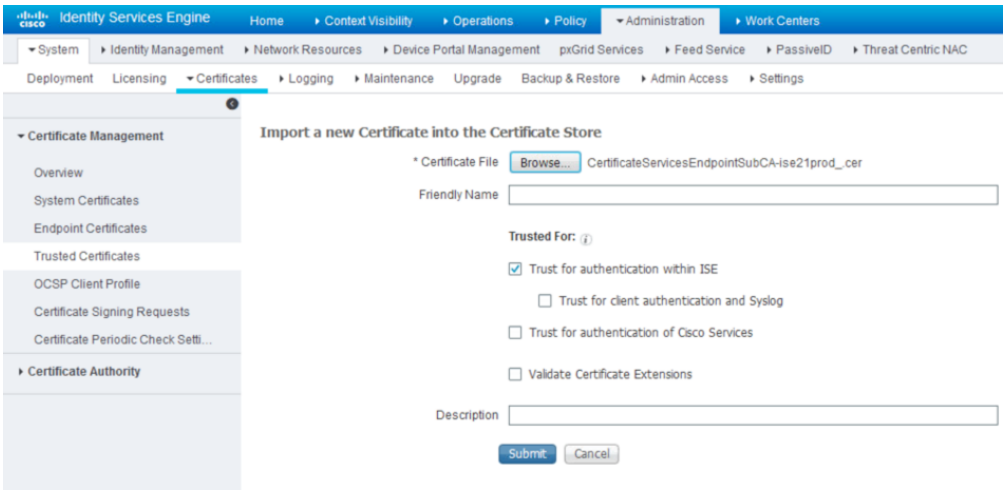


Importing ISE CA certificate into ISE Trusted System Store

Step 1 Import the CertificateServicesEndpointSubCA-ise21prod_CER file into the ISE trusted system store

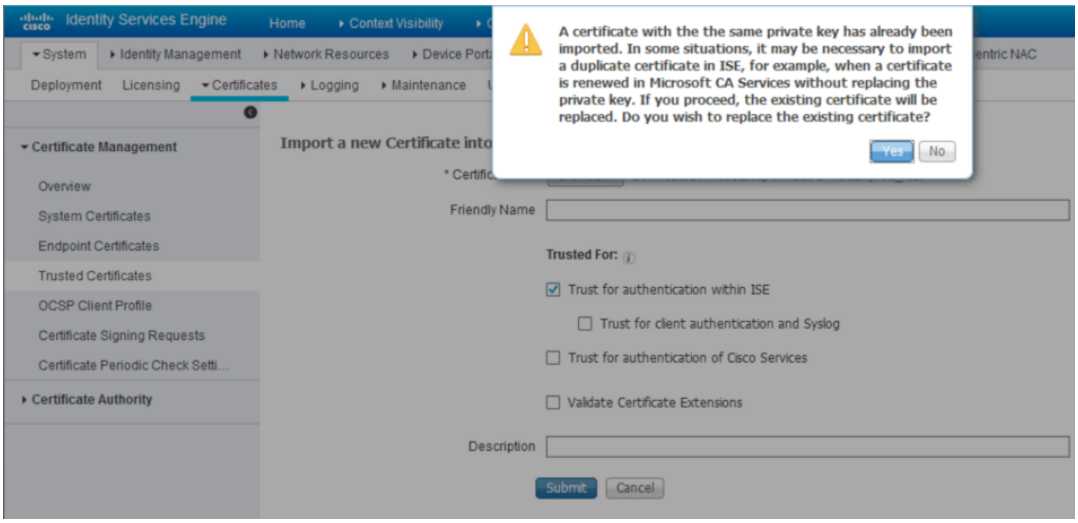
Step 2 Select-> **Administration->System->Certificates->Certificate Management->Trusted Certificates->Import the CertificateServicesEndpointSubCA-ise21prod_CER file**

Step 3 **Under Trusted** for, enable **Trust for authentication within ISE**

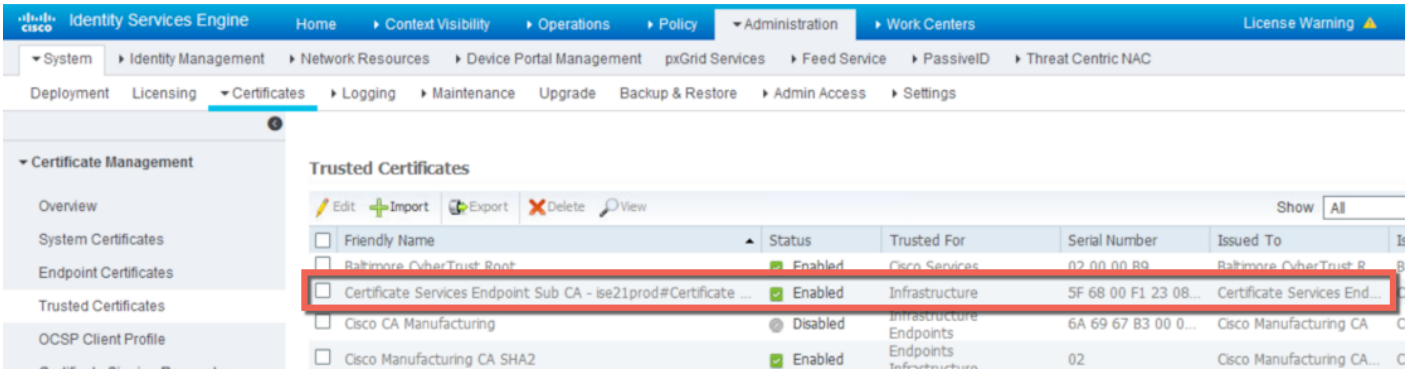


Step 4 Select **Submit**

Step 5 Select **Yes,** when prompted for the following:



Step 6 You should see the following:

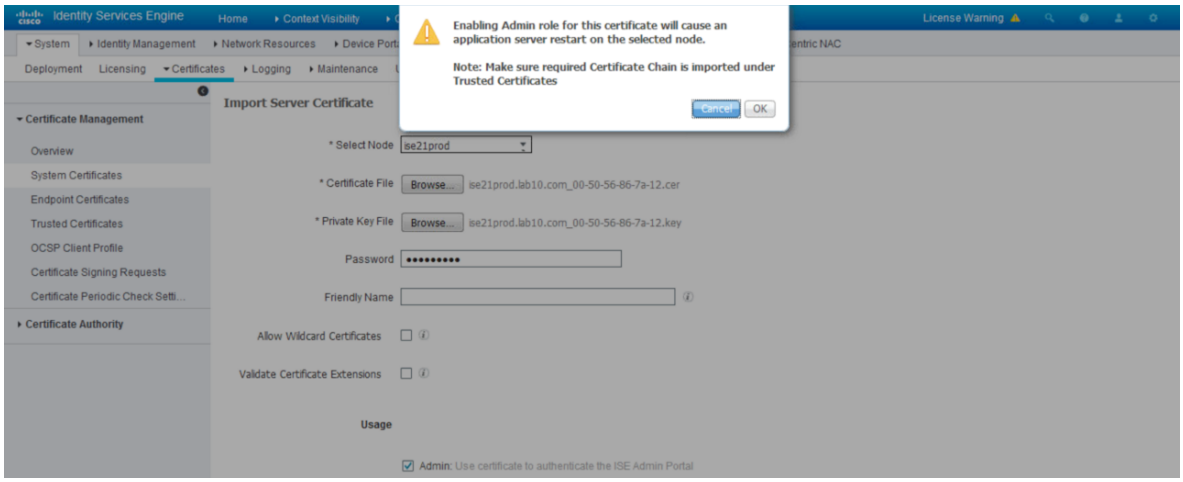


Importing ISE pxGrid node certificate into ISE system certificate store

Step 1 Import the ISEname-MAC.CER and ISEname-MAC.KEY file into the ISE system store.

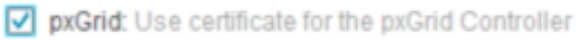
Step 2 Select **Administration->System->Certificates->System Certificates->Import both the public certificate and the private key, enable Admin for Usage**

Note: if the pxGrid client uses bulk session downloads enable "Admin" for Usage. This is required for the Cisco WSA, Cisco Firepower 6.1. Security Solutions.

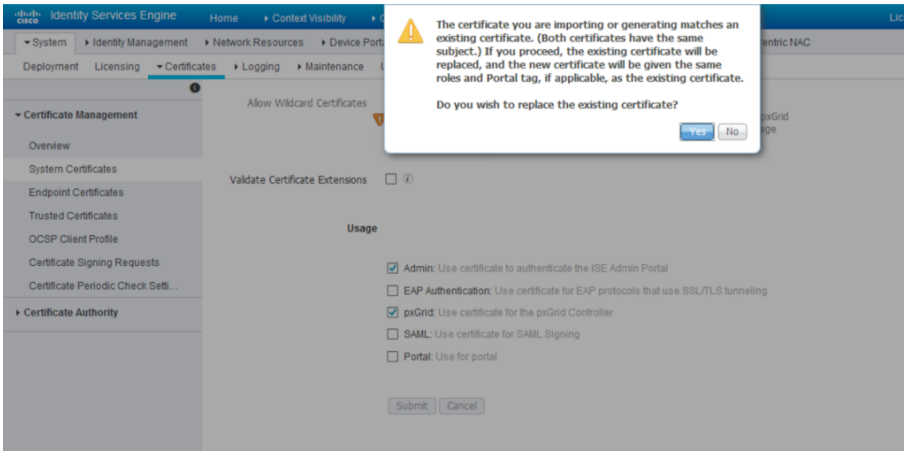


Step 3 When prompted selected **OK**

Step 4 Select pxGrid to enable pxGrid operation

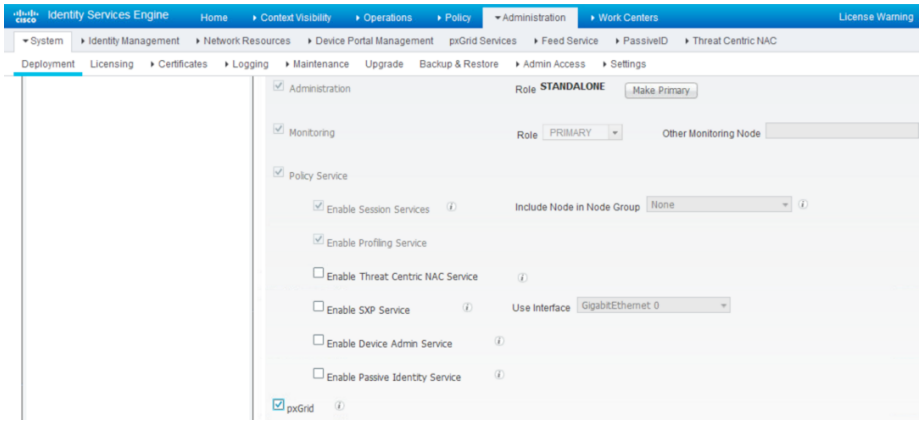


Step 5 Select **Yes** when prompted with the following message



Step 6 The ISE node will be restarted

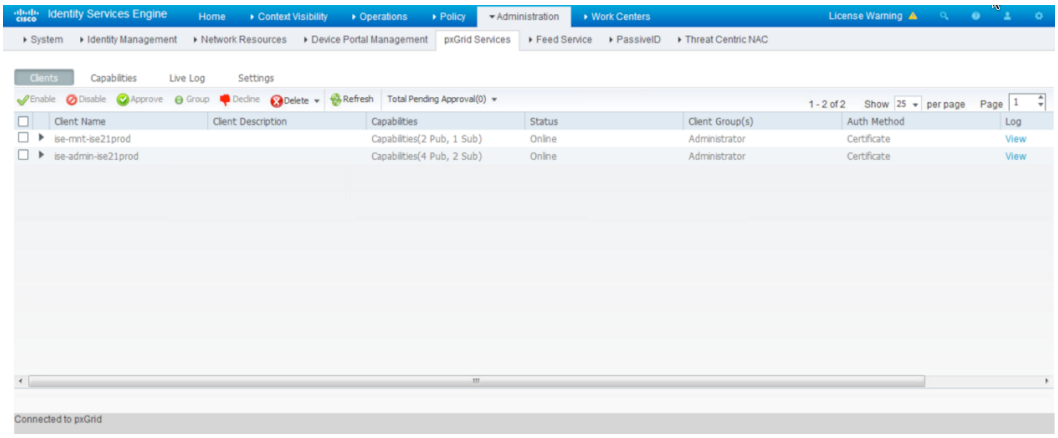
Step 7 Select **Administration->System->Deployment->edit the node->Enable pxGrid**



Step 8 Select **Save**

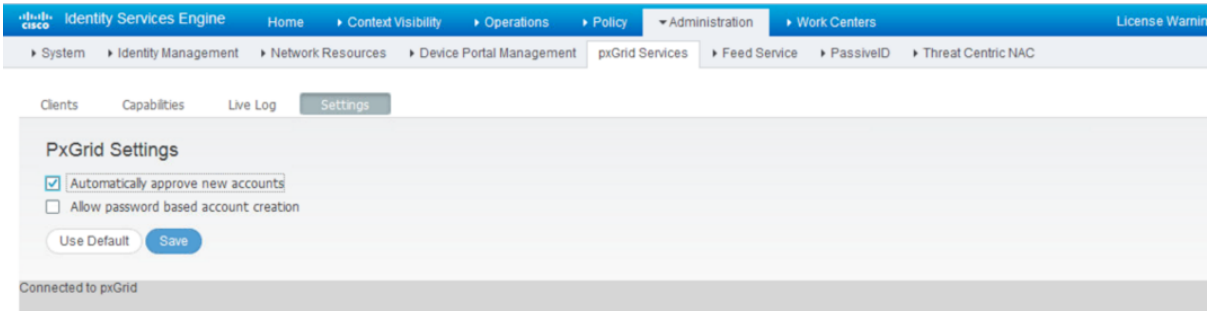
Verify ISE published pxGrid clients appear

Step 1 You should see the pxGrid services and pxGrid connectivity has been established



Step 2 Enable **Auto-Registration**

Step 3 Select **Administration->pxGrid->Settings-> pxGrid settings->enable Automatically approve new accounts**



Step 4 Select **Save**

Cisco Firesight 5.4

The section steps through the procedure for generating and issuing a Cisco Firesight pxGrid client certificate for Cisco Firesight 5.4. This also covers importing the ISE CA root certificate and the ISE EndpointSubCA certificate into the Sourcefire CA Truststore and importing the generated pxGrid client certificate public and private key pair into the Sourcefire Internal Certificate store. The Sourcefire pxGrid connection agent will be configured with the ISE pxGrid node IP address and also with the Sourcefire public certificate, the Sourcefire private key file, and the key password.

Once the certificate installation has been completed, the Cisco Firesight 5.4 will successfully connect and register to the ISE pxGrid node.

It is assumed that the reader is familiar with Cisco Firesight 5.4 and pxGrid integration. Please refer to the How To: Rapid Threat Containment (RTC) with Cisco Firesight and ISE guide: https://communities.cisco.com/docs/DOC-68293, if you are not familiar with this configuration.

It is assumed the ISE Authorization Policy for EPS:SessionStatus:Equals:Quarantine has been created.

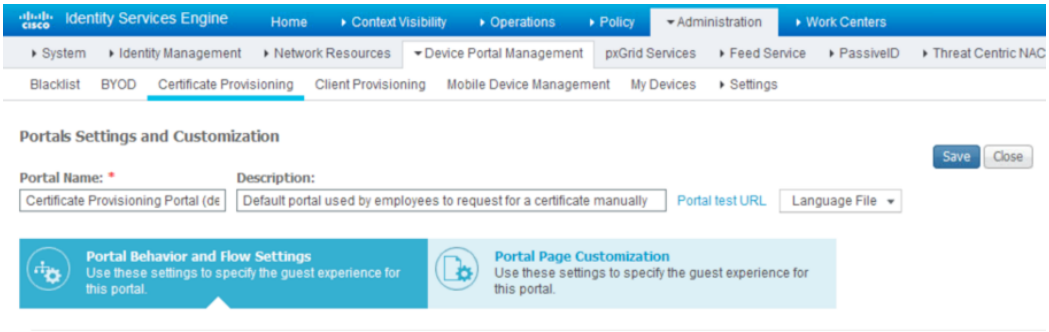
Note: ANC policies in ISE 2.1 will not be used. Cisco Firesight 5.4 subscribes to the EndpointProtectionService Capability when performing quarantine/unquarantine mitigation actions

Generating and Issuing pxGrid Client Certificate from ISE Certificate Provisioning Portal

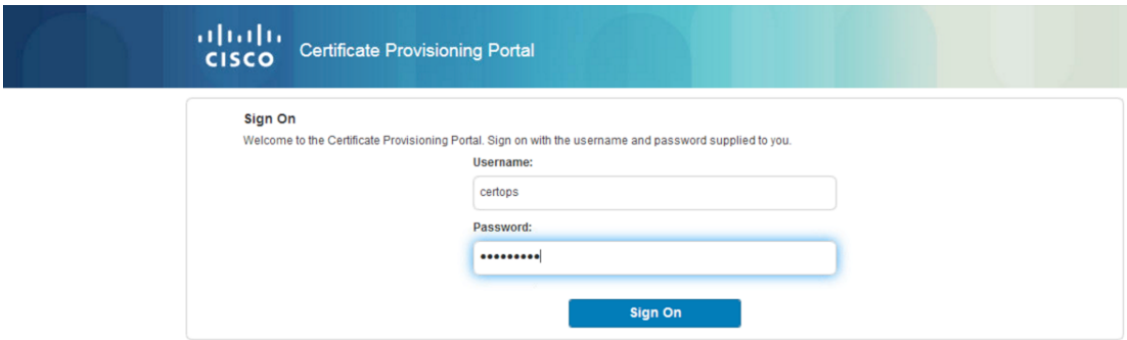
Step 1 Log into Certificate Provisioning Portal

Step 2 Select **Administration->Device Portal Management->Certificate Provisioning->Certificate Provisioning Portal (Default)**

You should see the following:



Step 3 Select **Portal test URL** and login with the ISE credentials you created earlier



Step 4 Select **Sign On**

Step 5 Under Certificate Provisioning, I want to* select **Generate a Single Certificate (without certificate Signing Request)**

Step 6 Select **Sign On**

Step 7 Under Certificate Provisioning, I want to* select **Generate a Single Certificate (without certificate Signing Request)**

Step 8 Provide the CN (Common Name) FQDN (Fully Qualified Domain Name)

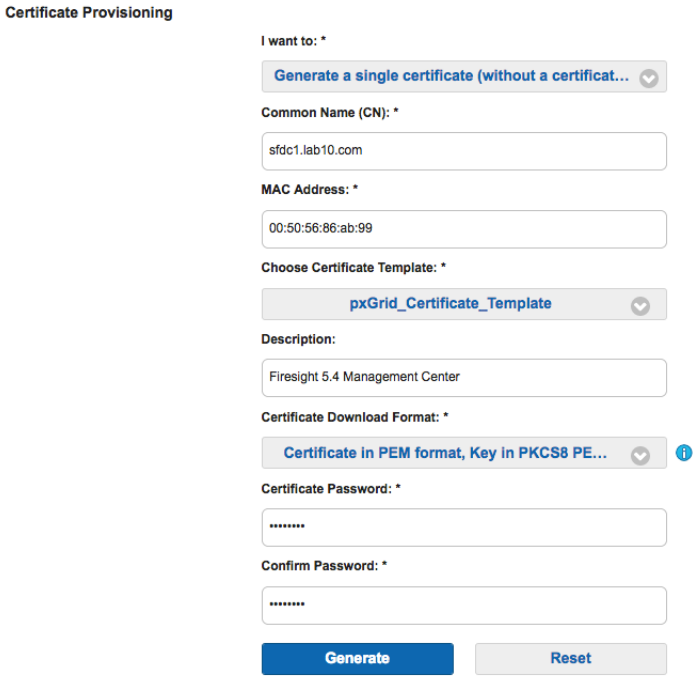
Step 9 Enter the MAC address of the 3rd party device under **MAC address**

Step 10 Under Choose Certificate Template*, select **pxGrid_Certificate_template**

Step 11 Enter an optional description, under **Description**

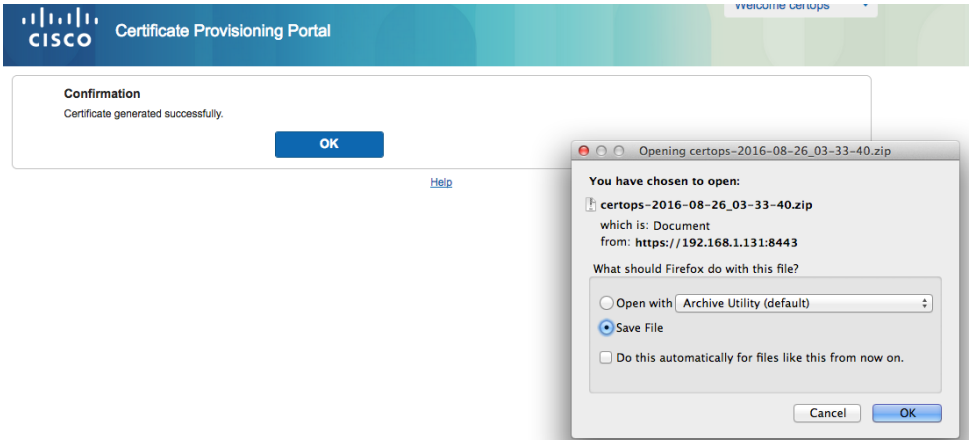
Step 12 Under Certificate Download Format, select **Certificate in PEM format Key in PKCSS PEM format**

Step 13 Enter and Confirm your **Certificate Password**



Step 14 Select **Generate**

Step 15 Download the file locally



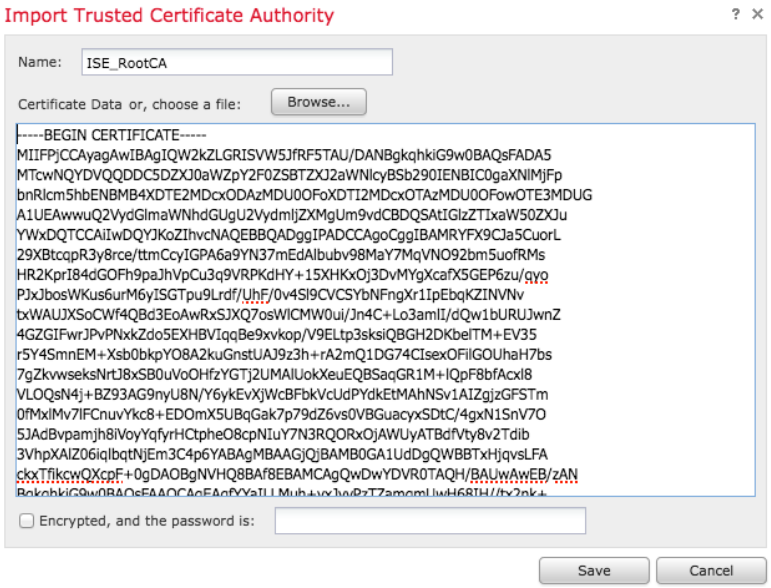
Step 16 You should see the following:

CertificateServicesEndpointSubCA-ise21internalCA_.cer	Tomorrow 3:33 AM	2 KB	certificate
CertificateServicesNodeCA-ise21internalCA_.cer	Tomorrow 3:33 AM	2 KB	certificate
CertificateServicesRootCA-ise21internalCA_.cer	Tomorrow 3:33 AM	2 KB	certificate
sfdc1.lab10.com_00-50-56-86-ab-99.cer	Tomorrow 3:33 AM	2 KB	certificate
sfdc1.lab10.com_00-50-56-86-ab-99.key	Tomorrow 3:33 AM	2 KB	Keyno...ument

Importing ISE and pxGrid client certificates

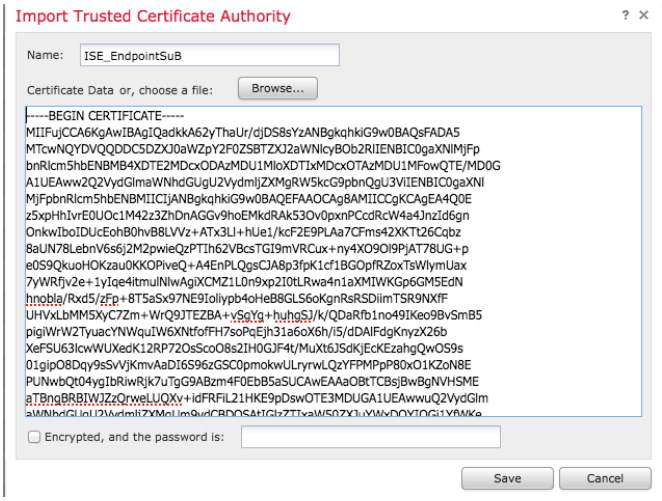
Step 1 Upload the certs to the Firesight 5.4 Management Console

Step 2 Select **Objects->PKI->Trusted CAs->Add Trusted CA add CertificateServicesRootCA-ise21internalCA_.cer** file



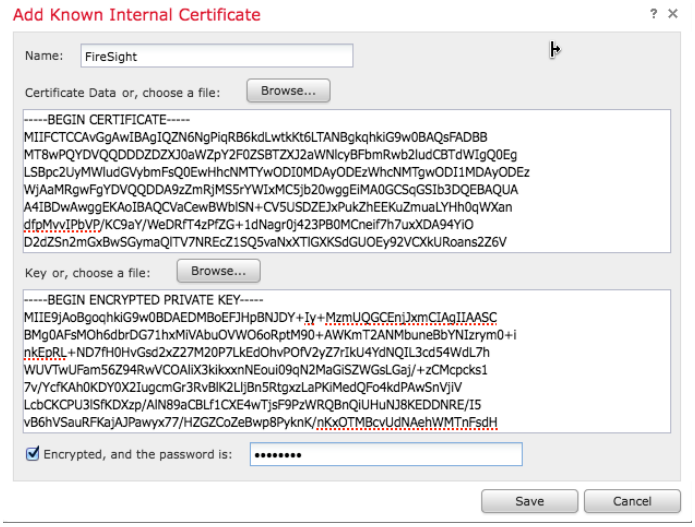
Step 3 Select **Save**

Step 4 Select **Objects->PKI->Trusted CAs->Add Trusted CA add CertificateEndpointSubCA-ise21internalCA_.cer**



Step 5 Select **Save**

Step 6 Select **Objects->PKI->Internal Certs->Add Internal Cert->upload sfdc1.lab10,com_00-50-56-86-ab-99_.cer** and **sfdc1.lab10,com_00-50-56-86-ab-99_.key files**.

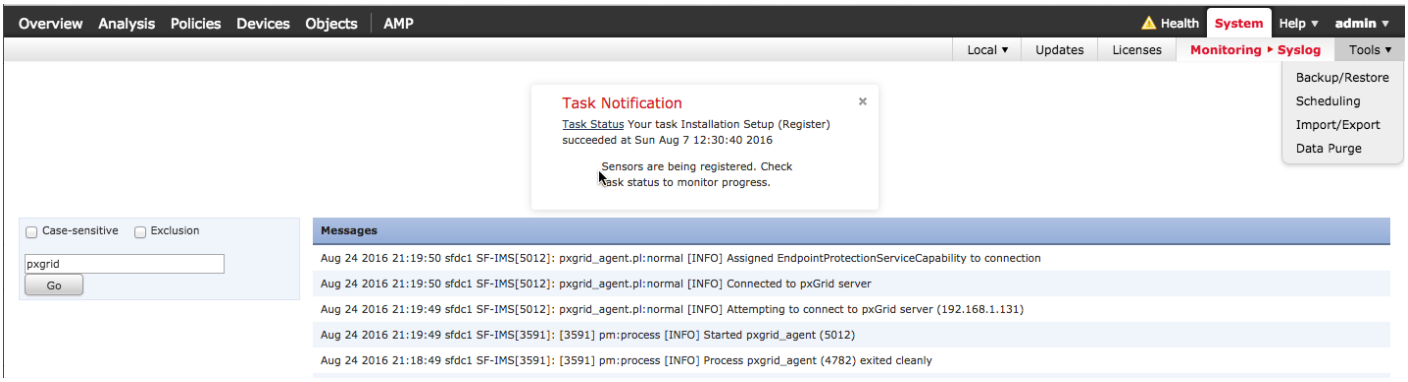


Step 7 Select **Save**

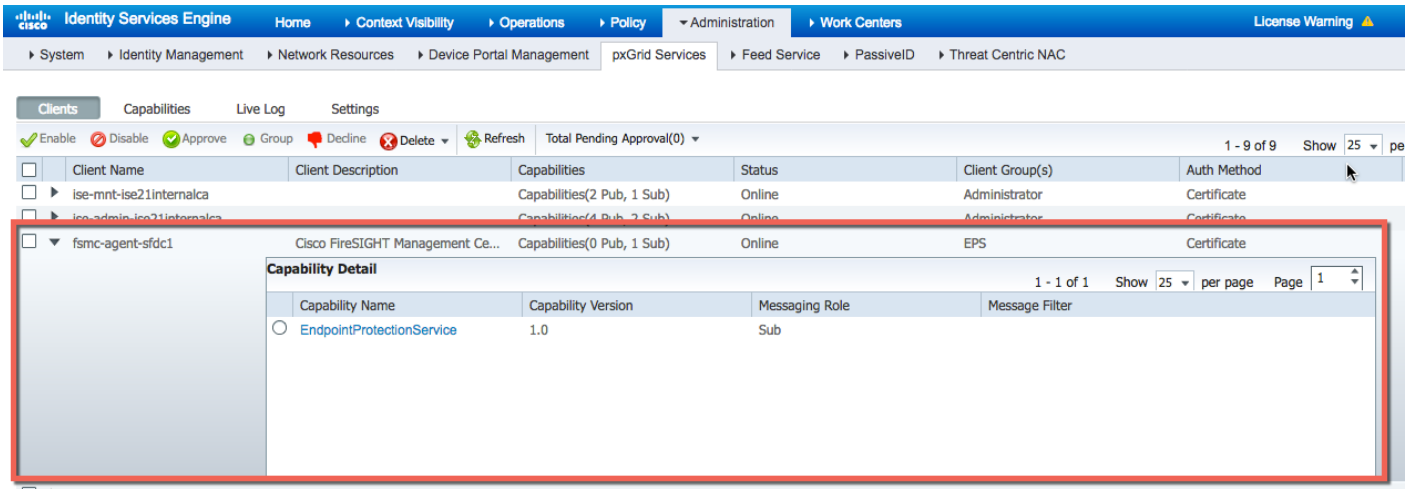
Step 8 Run the Sourcefire pxGrid connection agent and insert the ISE pxGrid node connection parameters

```
sudo bash sfdc-pxgrid_agent_v1.0.35.sh

pxgrid_server = 192.168.1.131
host_cert = /Volume/home/admin/sfdc1.kab10.com_00-50-56-86-ab-99.cer
host_key = /Volume/home/admin/sfdc1.kab10.com_00-50-56-86-ab-99.key
host_key_password = Cisco123
ca_cert = /Volume/home/admin/CertificateServicesRootCA-ise21internalCA_.cer
```

Step 9 Select **System->Monitoring->Syslog to view the successful connection**



Step 10 To view in ISE, select **Administration->pxGrid Services**



Cisco Firepower 6.1

The section steps through the procedure for generating and issuing a Cisco Firepower 6.1 pxGrid client certificate for Cisco Firepower 6.1. This covers importing the ISE CA root certificate and the ISE EndpointSubCA certificate into the Firepower 6.1 CA truststore and importing the generated pxGrid client certificate public and private key-pair into the Firepower 6.1 Internal Certificate store. This occurs under the Firepower Identity Source settings.

You can "Test" the setting configuration settings to verify that Cisco Firepower 6.1 has successfully connected, registered to the ISE pxGrid node and subscribed to the topics or capabilities.

For further testing, remediation types, correlation policies and rules are also included along with testing of Adaptive Network Control (ANC) quarantine/unquarantine mitigation action use cases. At the time of this document Cisco Firepower 6.1 was still in beta.

It is assumed that the ISE Authorization Policy for SessionStatus:Equals:Quarantine has been created.

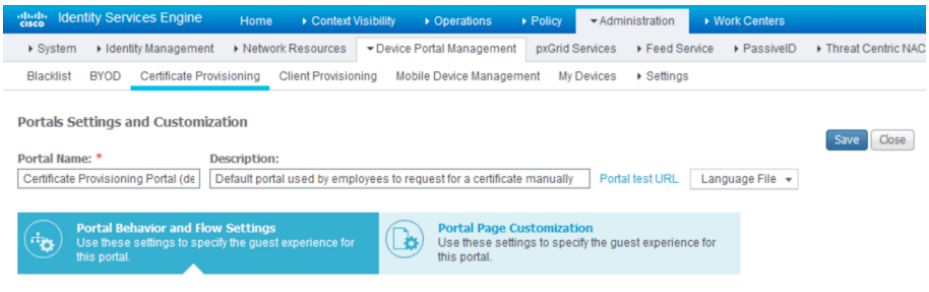
Note: ANC policies in ISE 2.1 will not be used. Cisco Firepower 6.1 subscribes to the EndpointProtectionService Capability when performing quarantine/unquarantine mitigation actions

Generating and Issuing pxGrid Client Certificate from ISE Certificate Provisioning Portal

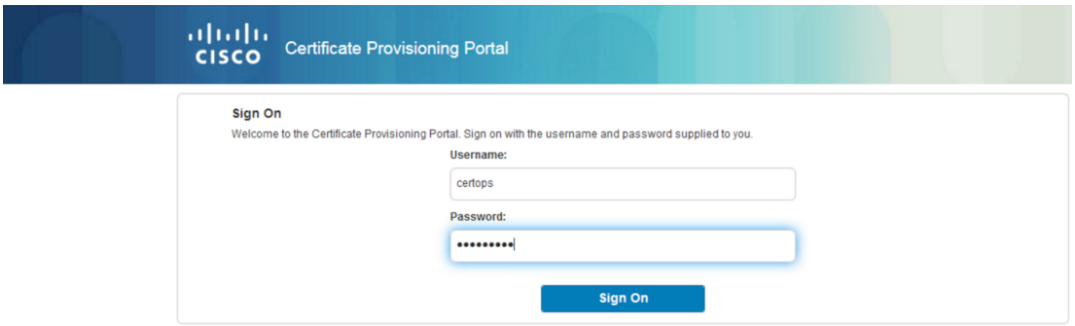
Step 1 Log into Certificate Provisioning Portal

Step 2 Select **Administration->Device Portal Management->Certificate Provisioning->Certificate Provisioning Portal (Default)**

You should see the following:



Step 3 Select **Portal test URL** and login with the ISE credentials you created earlier



Step 4 Select **Sign On**

Step 5 Under Certificate Provisioning, I want to* select **Generate a Single Certificate (without certificate Signing Request)**

Step 6 Provide the CN (Common Name) FQDN (Fully Qualified Domain Name)

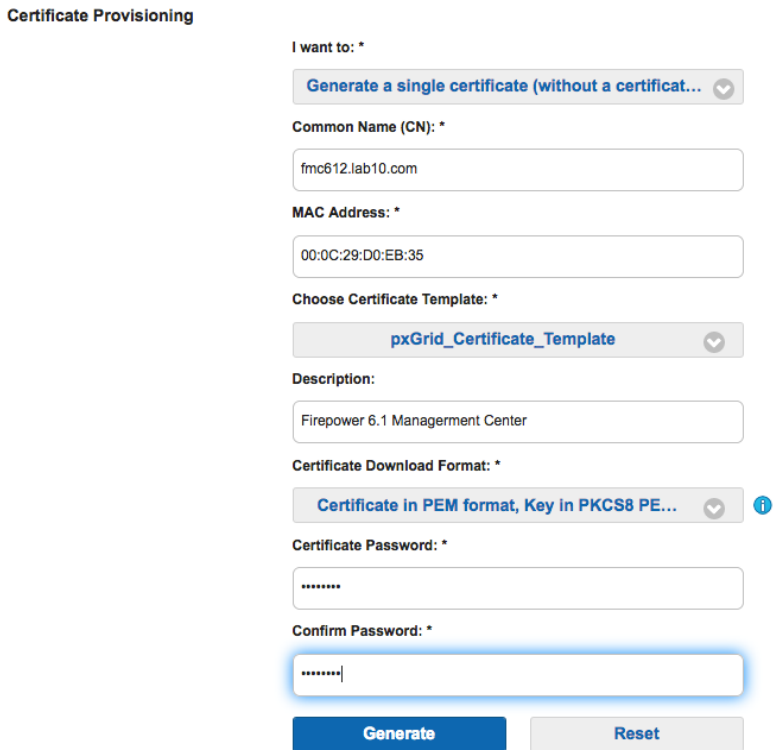
Step 7 Enter the MAC address of the 3rd party device under **MAC address**

Step 8 Under Choose Certificate Template*, select **pxGrid_Certificate_template**

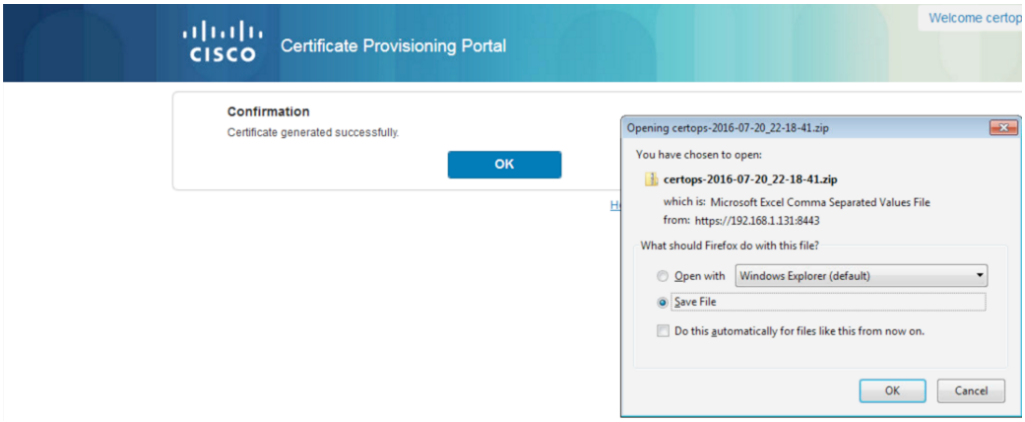
Step 9 Enter an optional description, under **Description**

Step 10 Under Certificate Download Format, select **Certificate in PEM format Key in PKCSS PEM format**

Step 11 Enter and Confirm your **Certificate Password**

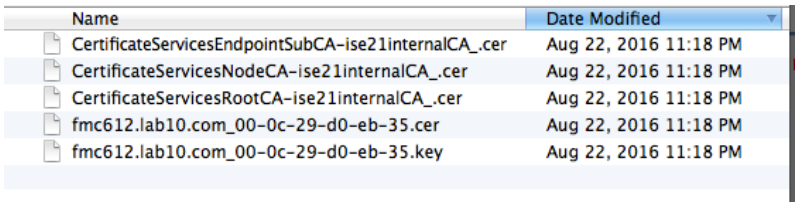


Step 12 Select **Generate**
You should see the following



Step 13 Save the file, select **OK**

Step 14 You should see the following files when you unzip the file

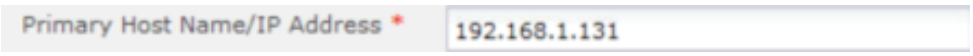


Name	Date Modified
CertificateServicesEndpointSubCA-ise21internalCA_.cer	Aug 22, 2016 11:18 PM
CertificateServicesNodeCA-ise21internalCA_.cer	Aug 22, 2016 11:18 PM
CertificateServicesRootCA-ise21internalCA_.cer	Aug 22, 2016 11:18 PM
fmc612.lab10.com_00-0c-29-d0-eb-35.cer	Aug 22, 2016 11:18 PM
fmc612.lab10.com_00-0c-29-d0-eb-35.key	Aug 22, 2016 11:18 PM

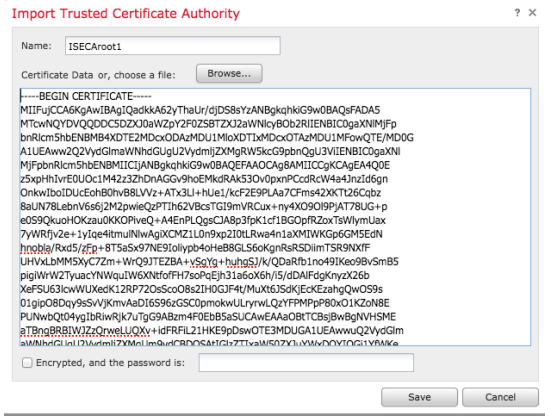
Configuring Identity Source

Step 1 Login to **FMC, select ->System->Integration->Identity Source**

Step 2 Add the ISE pxGrid node IP address



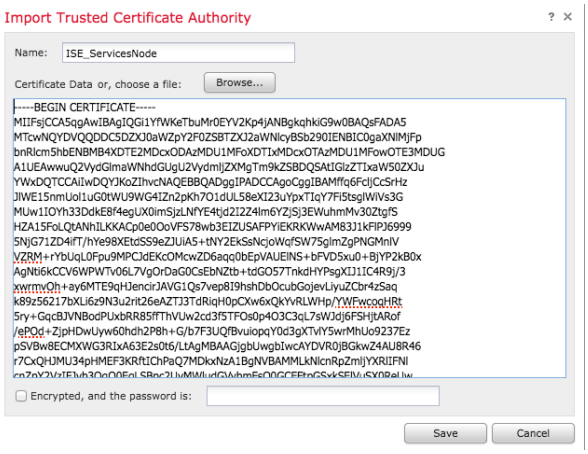
Step 3 Under **pxGrid Server CA**, select "+" , upload the **CertificateServicesRootCA-ise21internalCA_.cer**



Step 4 Provide Name: **ISECAroot1**

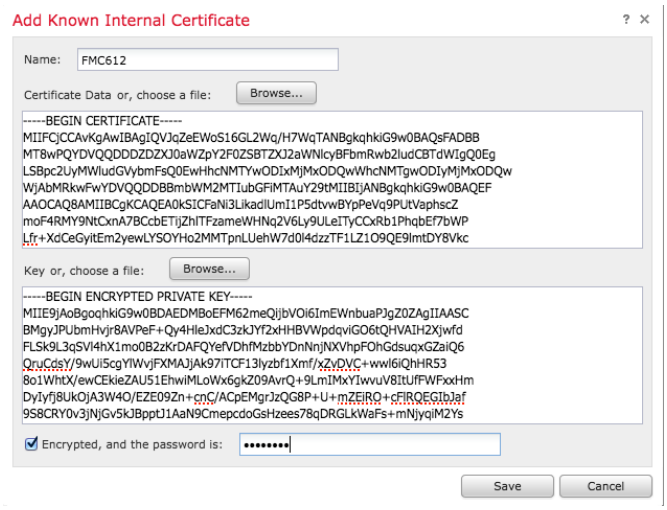
Step 5 Select **Save**

Step 6 Under **MNT Server CA**, select "+" , upload the **CertificateServicesNodeCA-ise21internalCA_.cer**



Step 7 Select **Save**

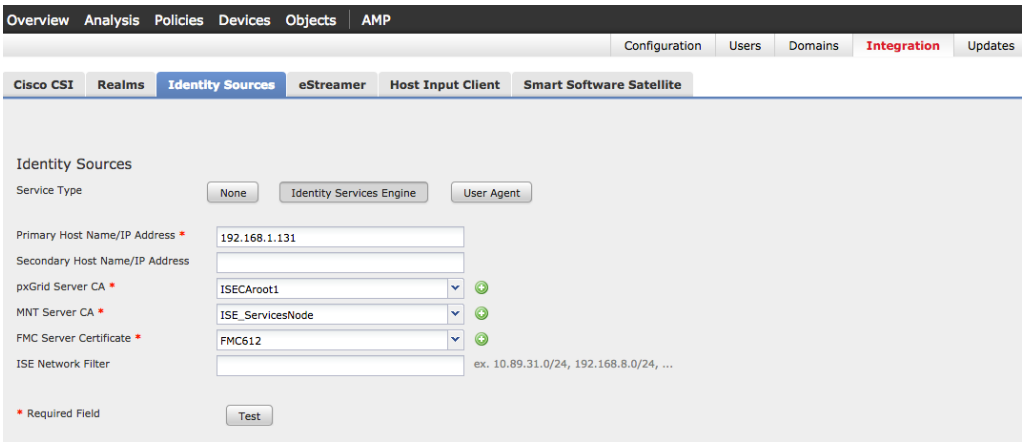
Step 8 Under FMC Server Certificate, upload the **fmc612.lab10.com_00-0c-29-d0-eb-35.cer** for the certificate data file and upload the **fmc612.lab10.com_00-0c-29-d0-eb-35.key** for the private key file.



Step 9 **Enable** Encrypted and enter the password file you entered when you generated the FMC certificate on ISE (i.e. **Cisco123**)

Step 10 Select **Save**

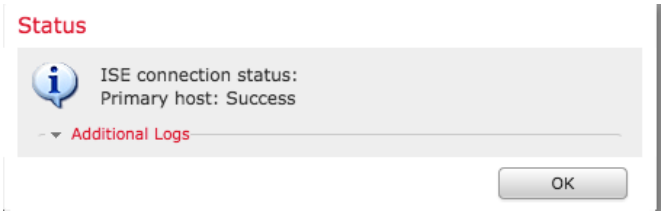
Step 11 You should see the following:



Step 12 Select **System->Integration->Identity Source**

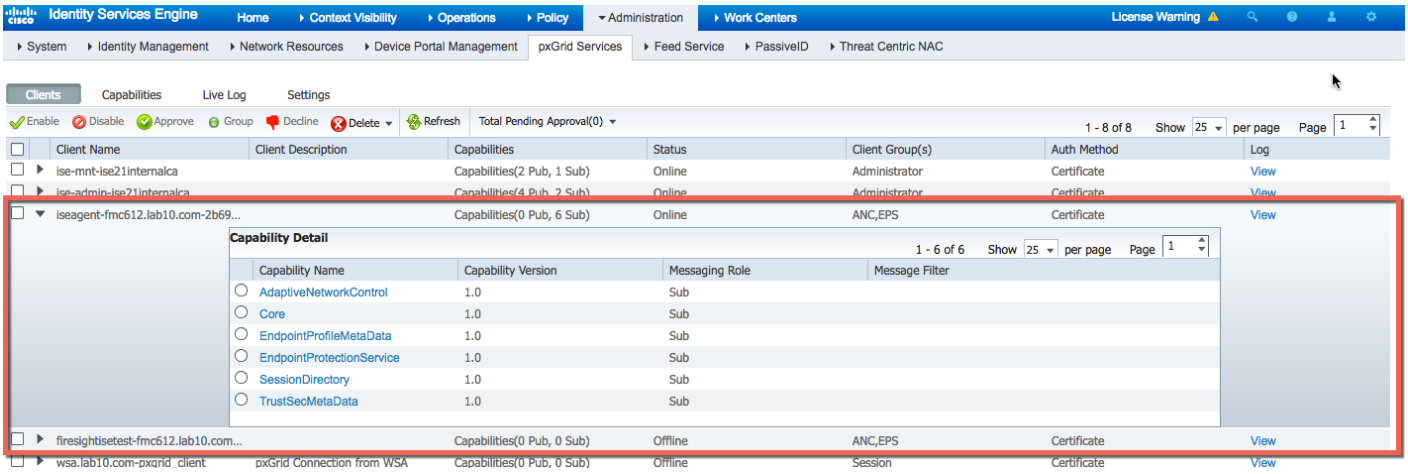
Step 13 Select **Test**

Step 14 You should see the following:



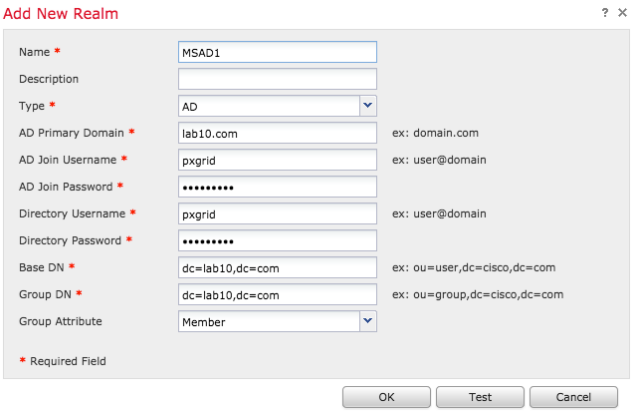
Step 15 Select **OK**

Step 16 Select **Administration->pxGrid Services,** you should see the following:

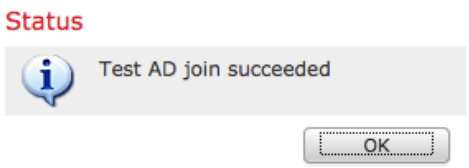


Create Firepower 6.1 Realm

Step 1 Select **System->Integration->Realms->New Realm->enter the Realm Information**



Step 2 Select Test to verify a successful connection

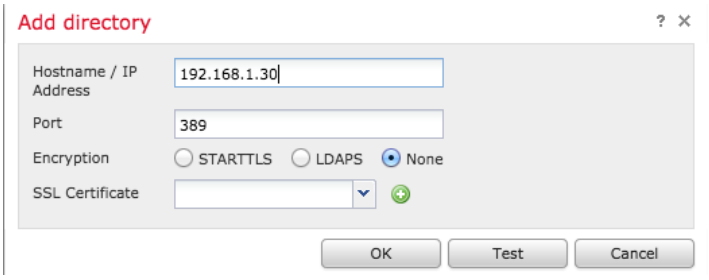


Step 3 Select **OK**

Step 4 Select **OK**

Step 5 Select **Add Directory**

Step 6 Enter the AD IP address information

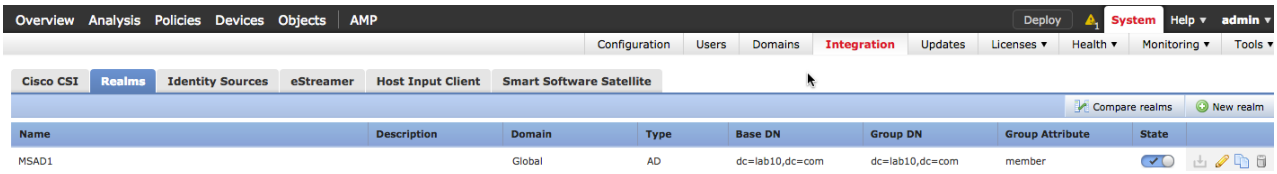


Step 7 Select **Test**
Step 8 Verify that the connection has succeeded
Step 9 Select **OK**
Step 10 Select **OK**
Step 11 You should see the following

Step 12 Select **Save**

Step 13 **Enable** the Realm by clicking on 

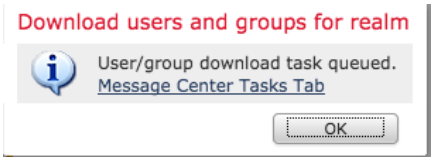
You should now see:



Step 14 Select on the **MSAD1 Realm->User Download->Download Users and Groups->Add all Groups to Include->Download now**

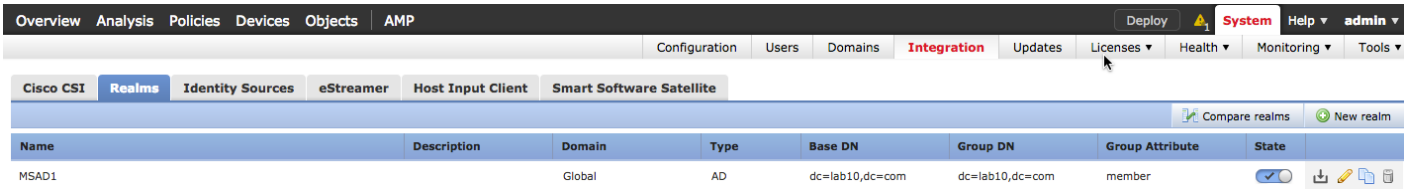
Note: You may have to refresh on "Available Groups"

Step 15 Select **Download Now**
Step 16 Select **OK** for **Download users and groups for realm**



Step 17 Select **Save**

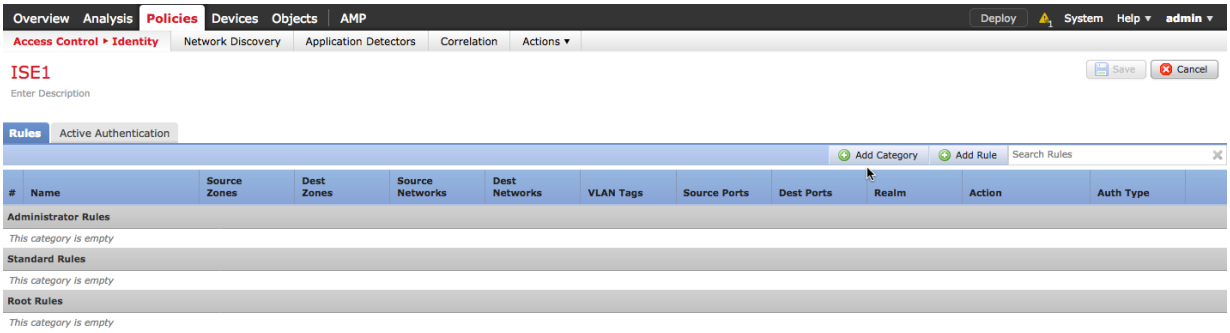
Step 18 You should see the realm:



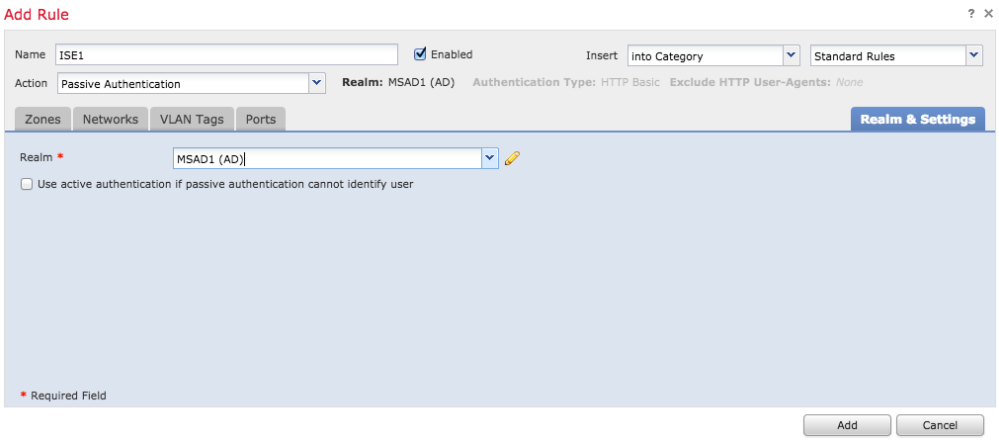
Configure ISE Identity Policy for Passive Authentication

Step 1 Select **Policies->Access Control->Identity->New Policy->New Identity Policy->provide a name**

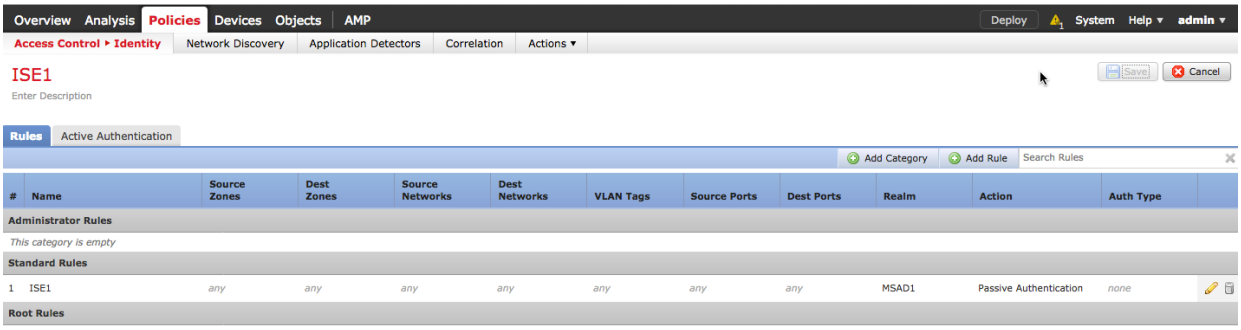
Step 2 Select **Save**
You should see the following:



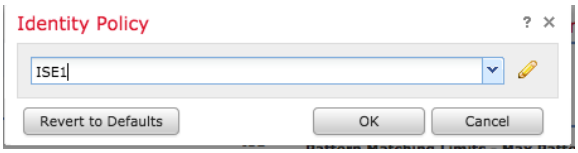
Step 3 Select **Add Rule, provide name: ISE1**
Step 4 Select **MSAD1 Realm**



Step 5 Select **Add**
Step 6 Select **Save**
Step 7 You should see the following:



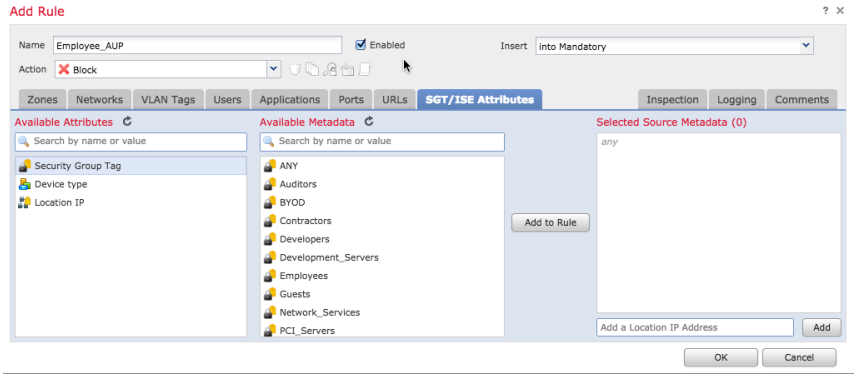
Step 8 Select **Policies->Access Control->Access Control**
Step 9 Select the **Default access policy**
Step 10 Select the **Identity Policy**



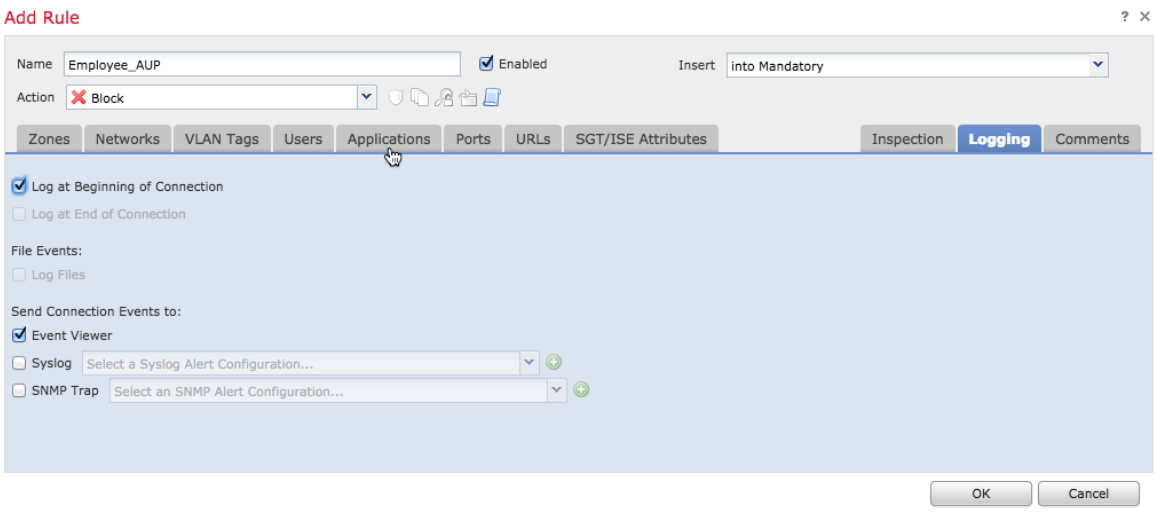
Step 11 Select **OK**
Step 12 Select **Save**

Create Access Rule

Step 1 **Select Rules**
Step 2 Add Rule, provide a name, **Employee_AUP**
Step 3 **Under Action, select Block**
Step 4 Select **URLs->Category, select: Peer to Peer -> Add to Rule**
Step 5 Select **Hacking->Add to Rule**
Step 6 Select **ISE/SGT attributes**
Step 7 Select **SGT Tag**
You should see the tags appear under metadata:



Step 8 Select **Employees** from the available metadata->**Add to Rule**
Step 9 Select **Logging**
Step 10 **Enable** Logging at Beginning of Connection



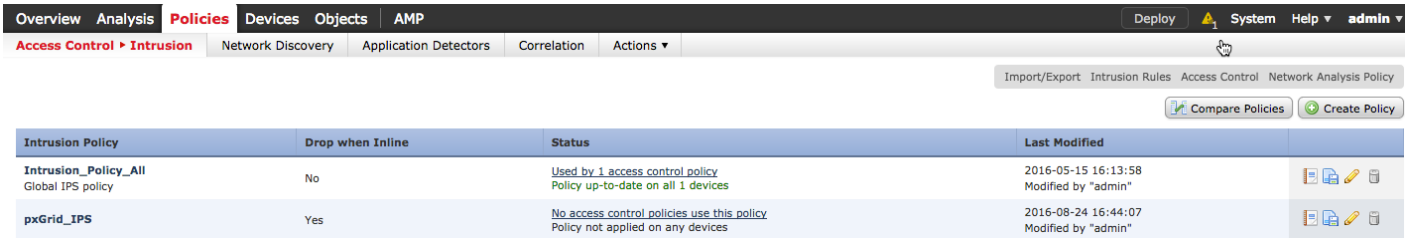
Step 11 Select **OK**
Step 12 Select **Save**

Create pxGrid IPS Policy

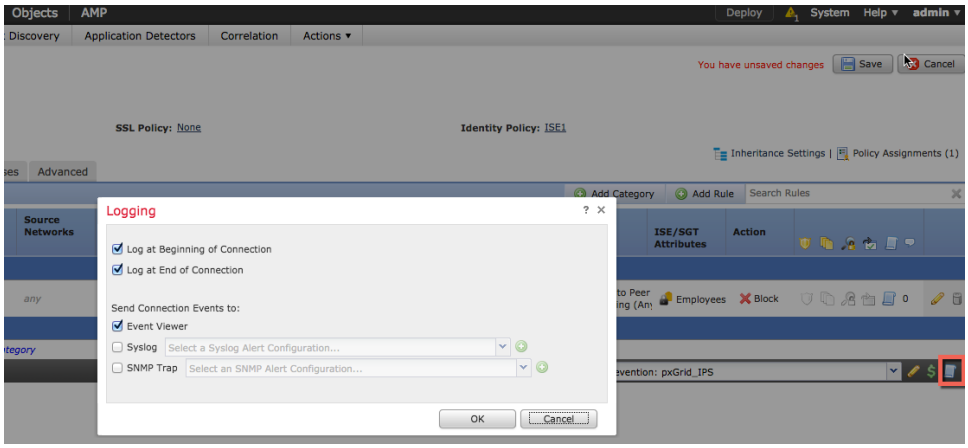
Step 1 Select **Policies->Access Controls-Intrusion->Create Policy**, provide a name: **pxGrid IPS->base Policy, select No Rules Active**

Step 2 Select **Create and Edit Policy**
Step 3 Select **Rules**
Step 4 Enter: **iis cmd exec** for **filter**
Step 5 Select **All**
Step 6 Select **Rule State->Generate Events**
Step 7 **You should see a "successfully set the rule state for 4 rules**
Step 8 **Select OK**
Step 9 Select **Policy Information->Commit Changes-OK**

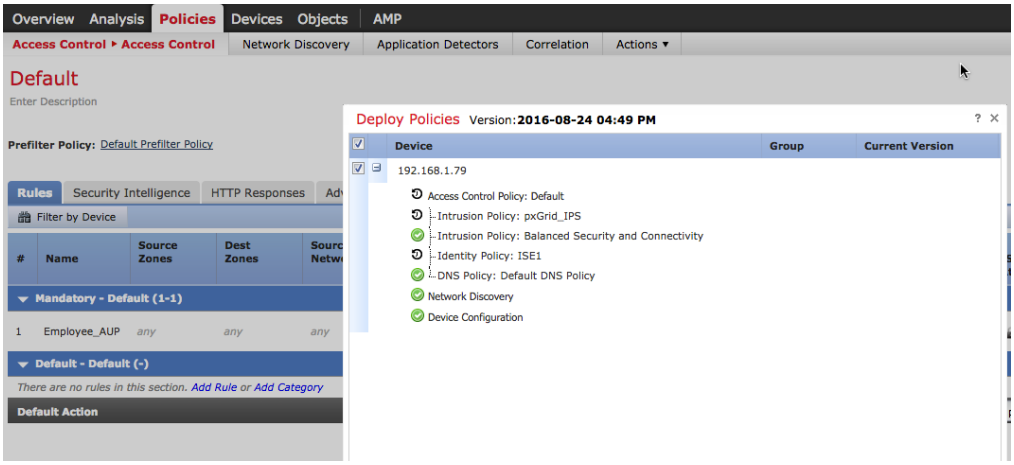
Step 10 You should see the following:



Step 11 Select **Policies->Access Control->Access Control->Edit (click on Pencil)**
Step 12 Under **Default Action->**select **pxGrid IPS Intrusion Policy**
Step 13 **Enable logging**

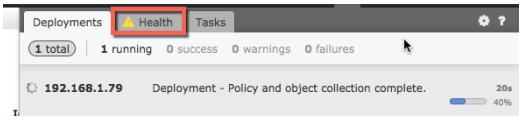


Step 14 Select **OK**
Step 15 Select **Save**
Step 16 Select **Deploy**
Step 17 Select the device IP address



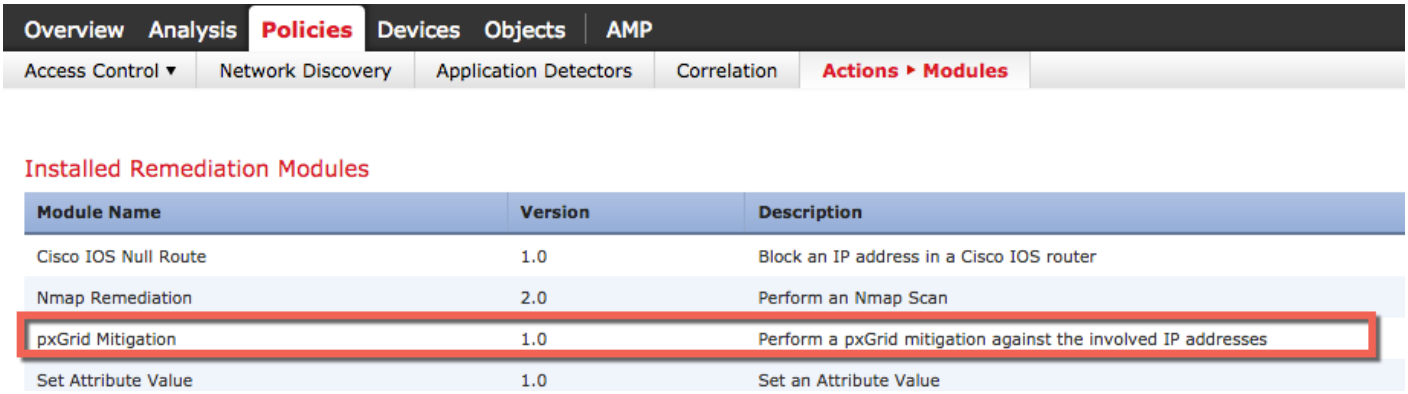
Step 18 Select **Deploy**

Step 19 Select **Health Bar** view deployment status



Create Quarantine and UnQuarantine Remediation Types

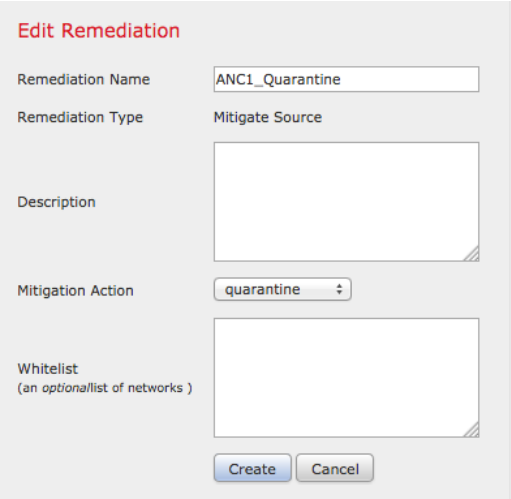
Step 1 Select **Policies->Actions->Remediations->Modules**, verify you see pxGrid mitigation:



Step 2 Select **Remediation->Action->instances->add a new pxGrid mitigation instance->instance name**, type: **pxgrid->create**

Note: Enable logging should be set to on

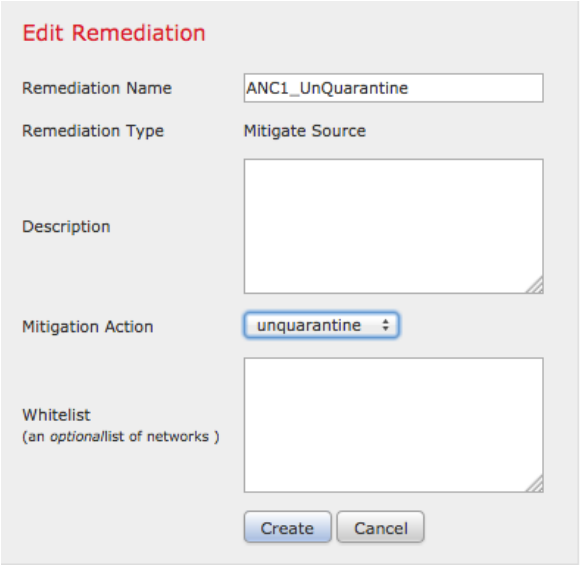
Step 3 Select "**Add a new remediation of type: mitigate source**" **Add**
Step 4 Type: **ANC1_Quarantine for the Remediation Name**, **mitigation action->quarantine**



Step 5 Select **Create**
Step 6 Select **Save**
Step 7 Select **Done**

Step 8 Select **"Add a new remediation of type: mitigate source" Add**

Step 9 Type: **ANC1_UnQuarantine for the Remediation Name, mitigation action->unquarantine**

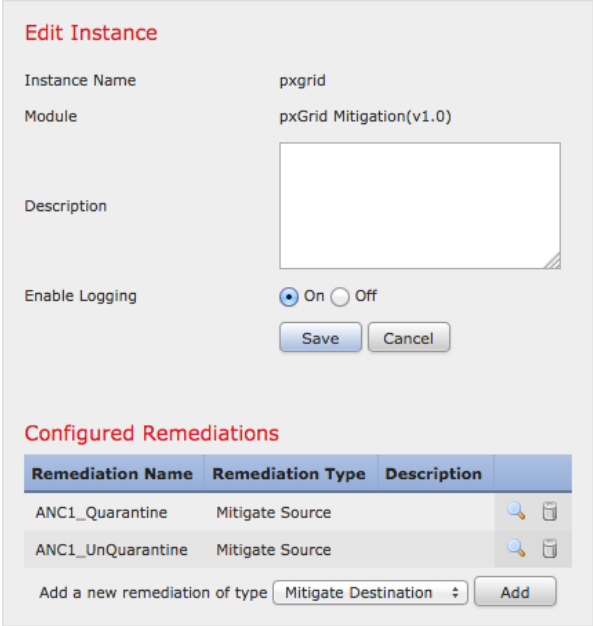


Step 10 Select **Create**

Step 11 Select **Save**

Step 12 Select **Done**

Step 13 You should see the following:



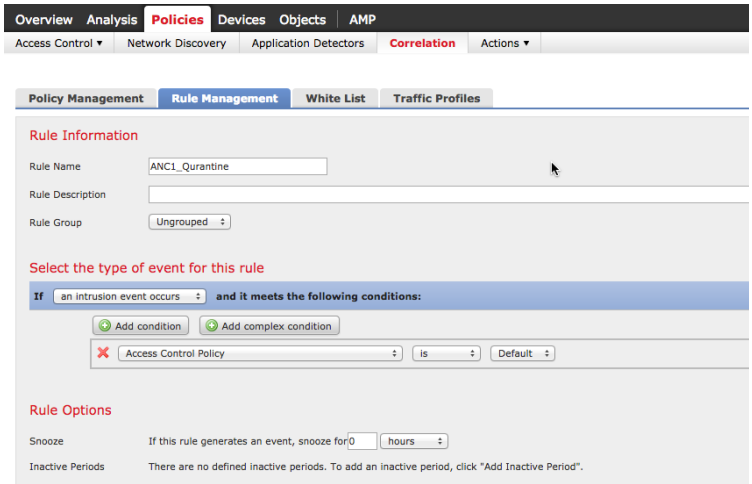
Create Quarantine and Unquarantine Correlation Policies

Step 1 Select **Policies->Correlation->Policy Management->Create Policy->enter:ANC1_quarantine for policy name->Save**

Step 2 Select **Rule Management->Create Rule->**enter: **ANC1_Quarantine** for rule name

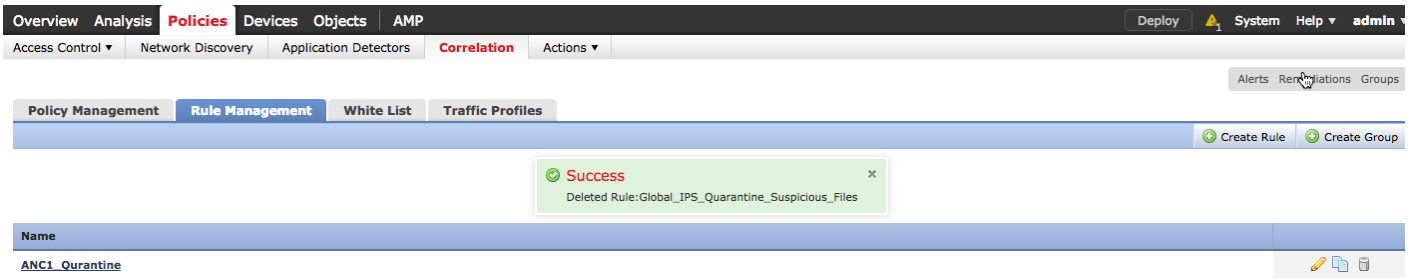
Step 3 Select **an intrusion event occurs** for **select this type of event for this rule**

Step 4 Select **Access Control Policy** is **Default** for the condition rule

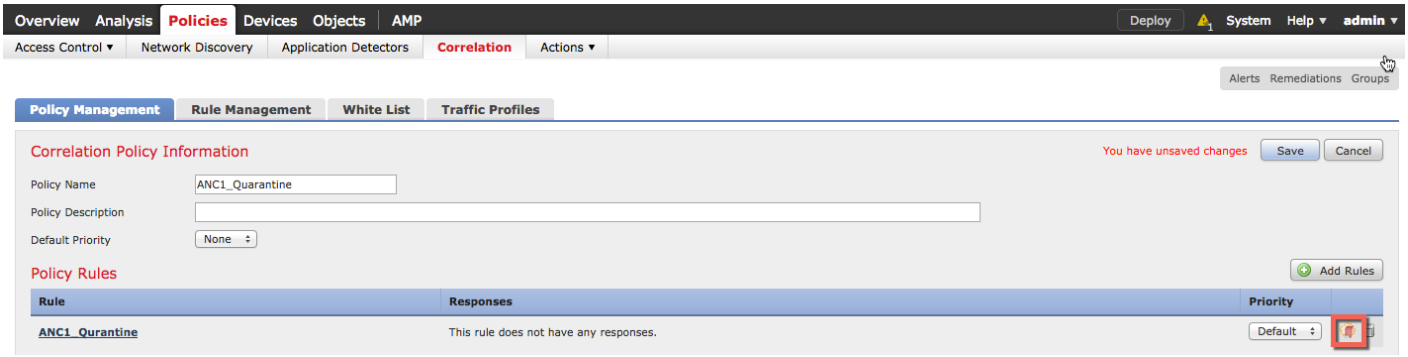


Step 5 Select **Save**

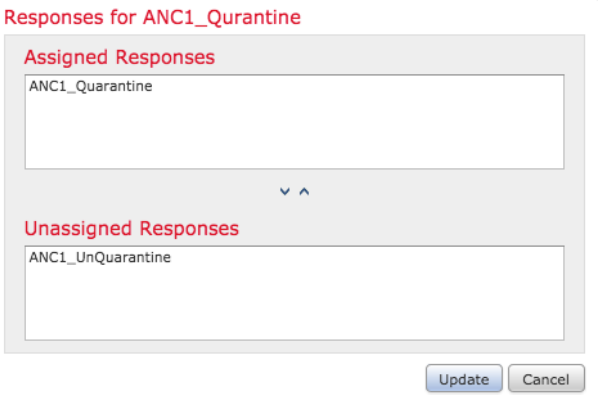
Step 6 You should see the following:



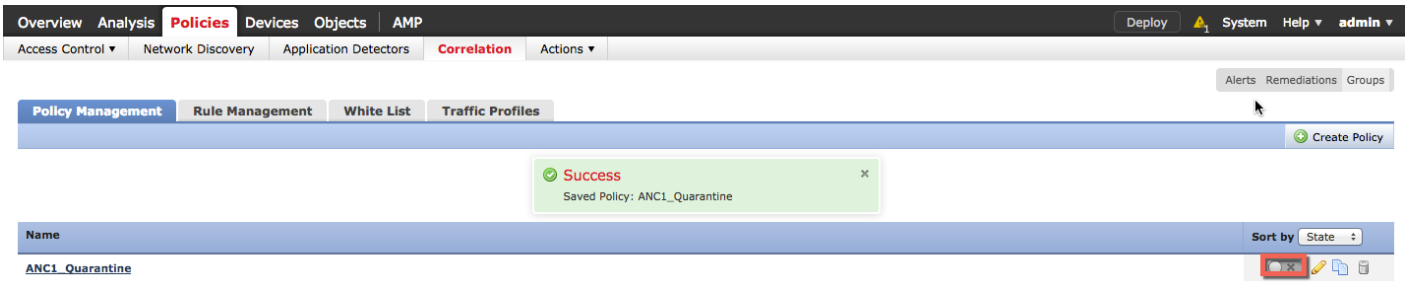
Step 7 Select **Policies->Correlation->Policy Management->ANC1_Quarantine->Add rule->ANC1_Quarantine->Add->Responses**



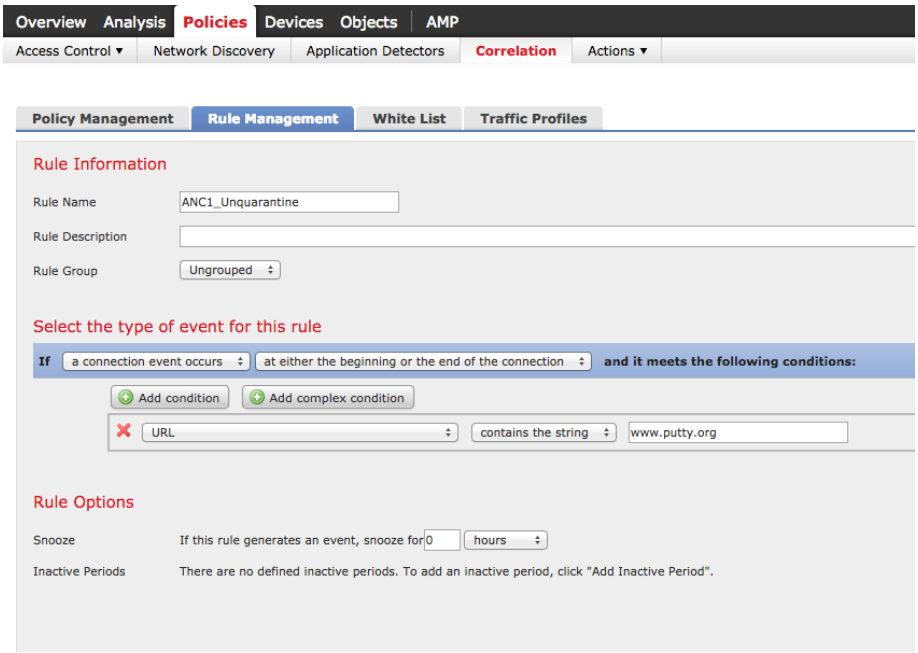
Step 8 Select **ANC1_Quarantine as the assigned Response**



Step 9 Select **Update**
Step 10 Select **Save**
Step 11 Activate the policy by clicking on tab below:

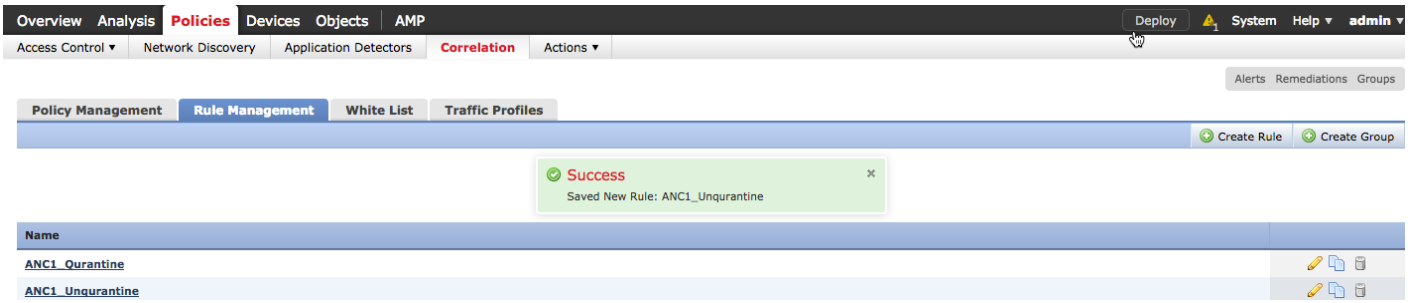


Step 12 Select **Policies->Correlation->Policy Management->Create Policy->enter:ANC1_Unquarantine for policy name->Save**
Step 13 Select **Rule Management->Create Rule->enter: ANC1_Unquarantine for rule name**
Step 14 Select **a connection event occurs** for **select this type of event for this rule**
Step 15 Select **URL contains the string www.putty.org** for the condition rule

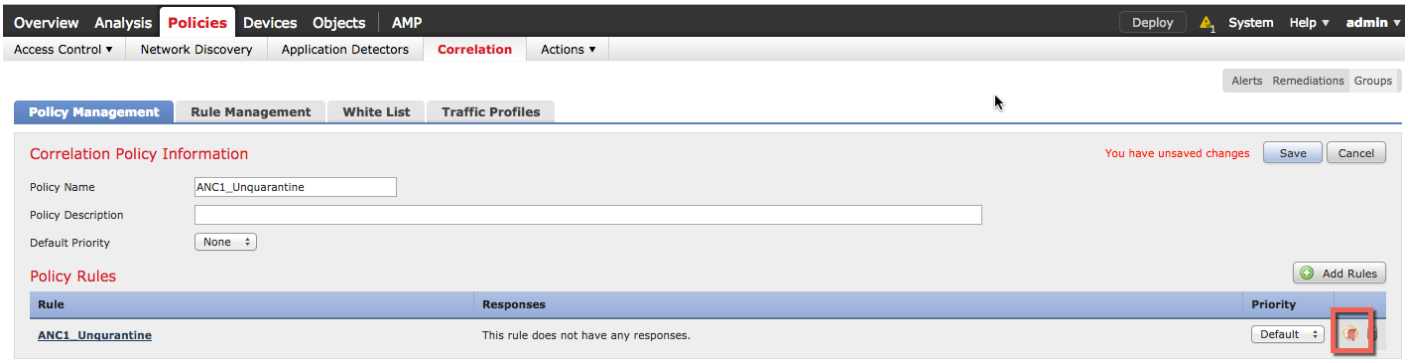


Step 16 Select **Save**

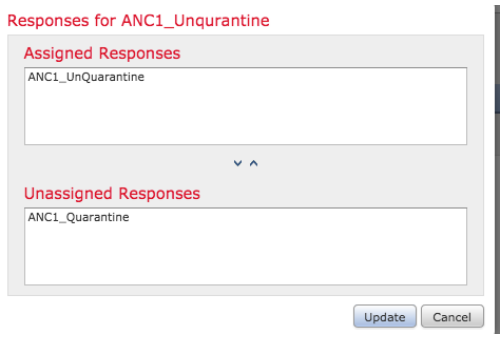
Step 17 You should see the following:



Step 18 Select **Policies->Correlation->Policy Management->ANC1_Unquarantine->Add rule->ANC1_Unquarantine->Add->Responses**



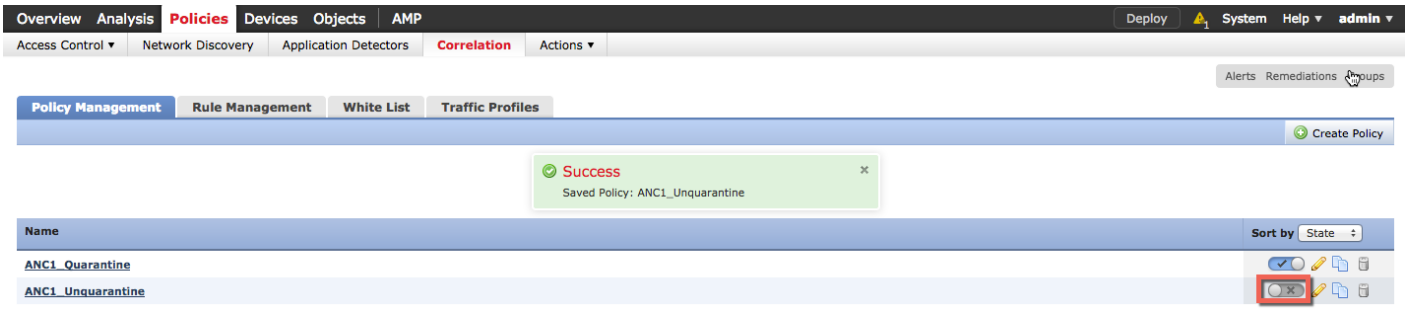
Step 19 Select **ANC1_Unquarantine**



Step 20 Select **Update**

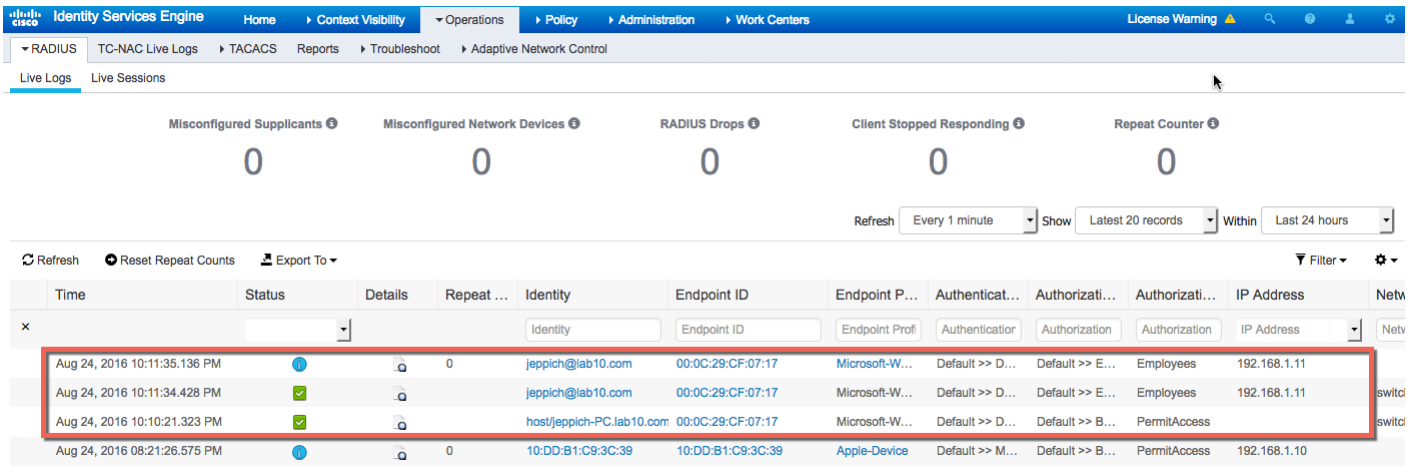
Step 21 Select **Save**

Step 22 Activate the rule by clicking on the tab

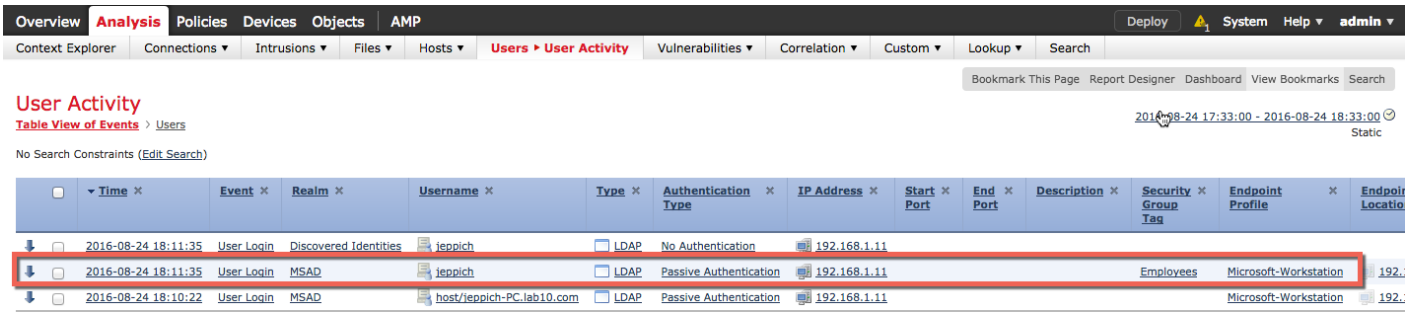


Testing Cisco Firepower 6.1 Quarantine and Unquarantine Adaptive Network Control (ANC) Mitigation Actions

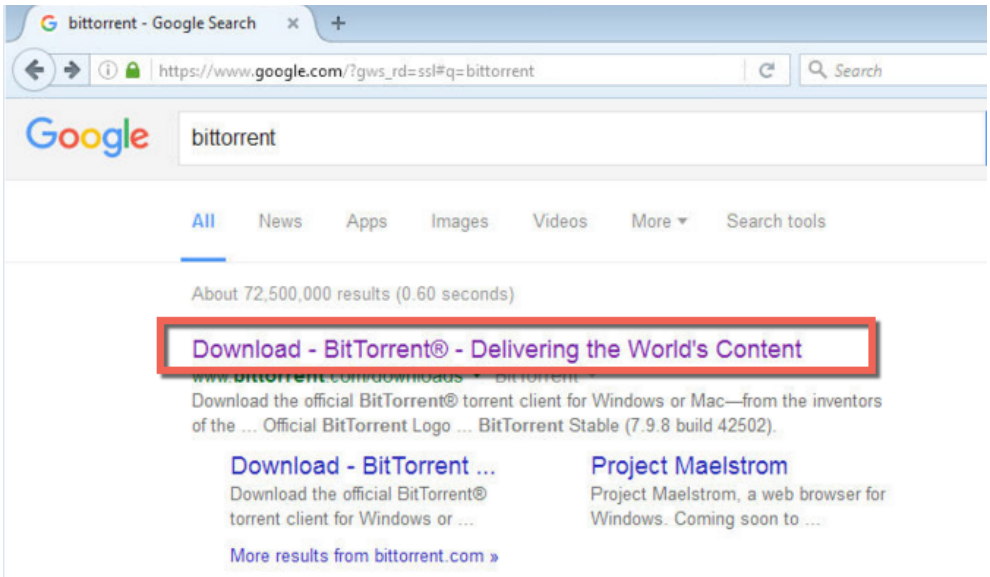
Step 1 The end-user successfully logs into the network



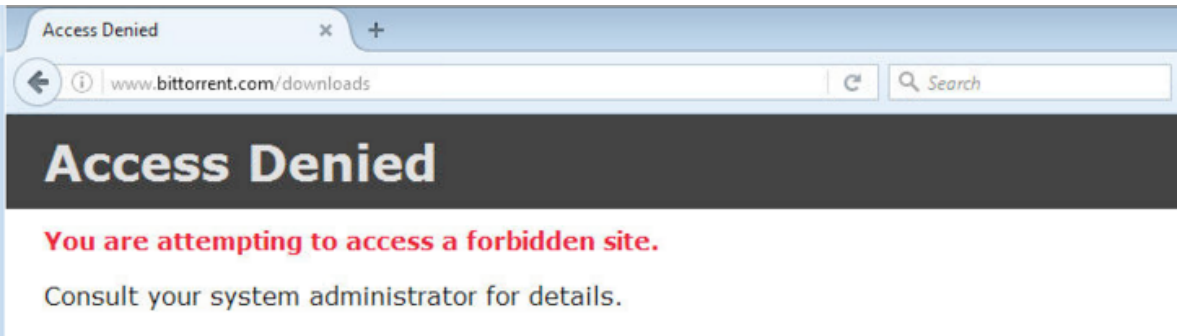
Step 2 Under the FMC user activity screen, we see the authenticated ISE session.



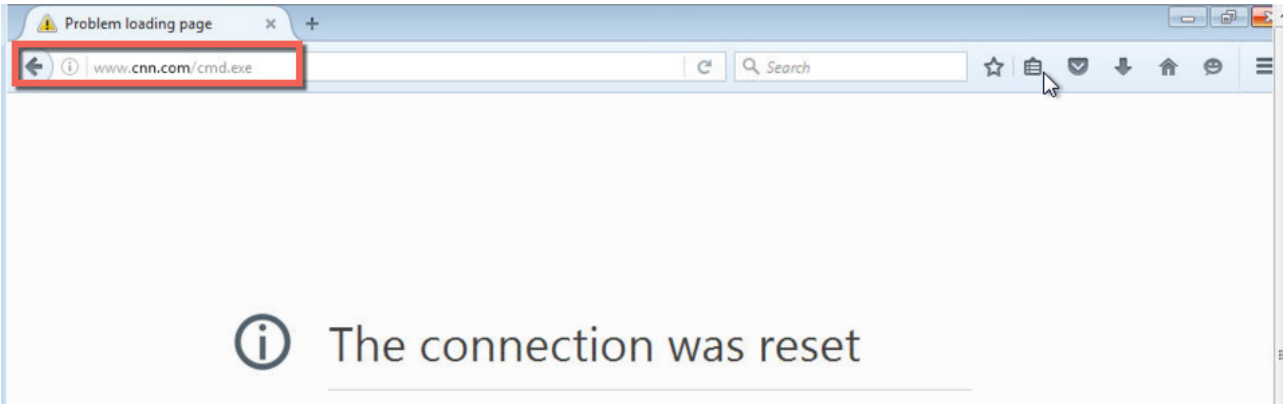
Step 3 Open browser and Google "bittorrent"



Step 4 You should see access to the bittorrent site is denied due the FMC access policy denying user who are tagged with an Employee SGT.



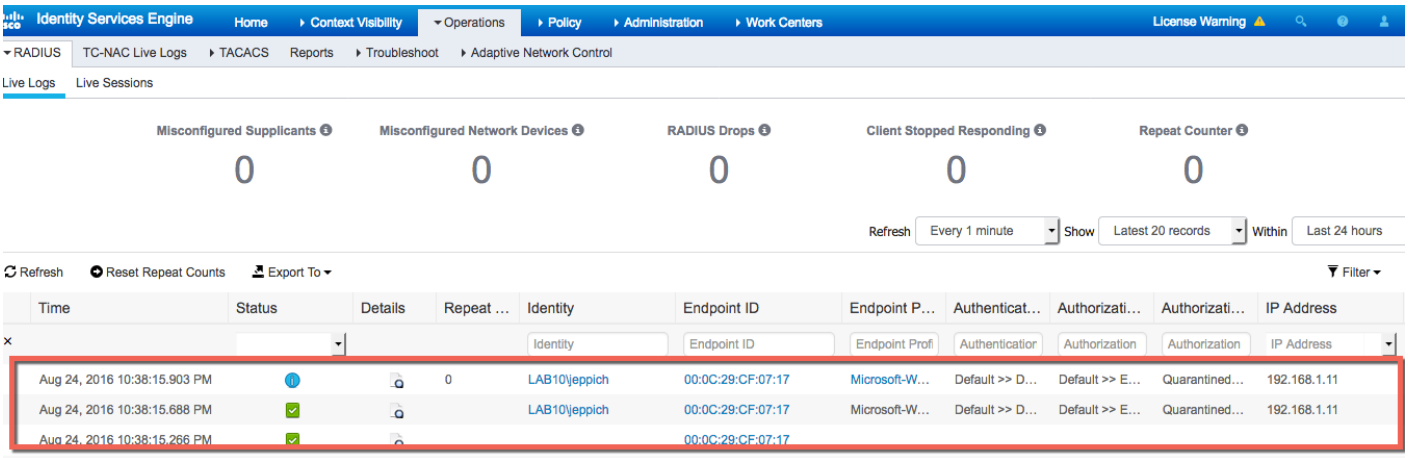
Step 5 Open browser, www.cnn.com/cmd.exe, the connection was reset



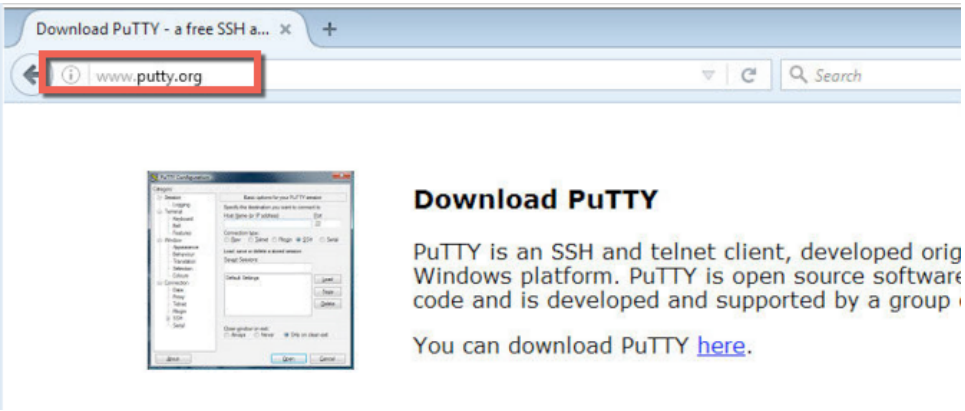
Step 6 This triggers an intrusion event

Step 7 The intrusion event triggers the Quarantine Correlation policy and associated rule, which triggers the ANC, quarantine mitigation action.

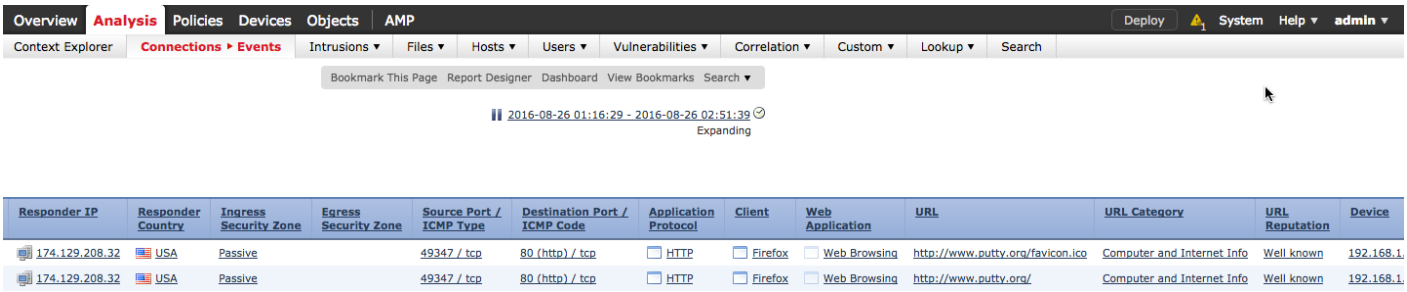
Step 8 The endpoint is quarantined



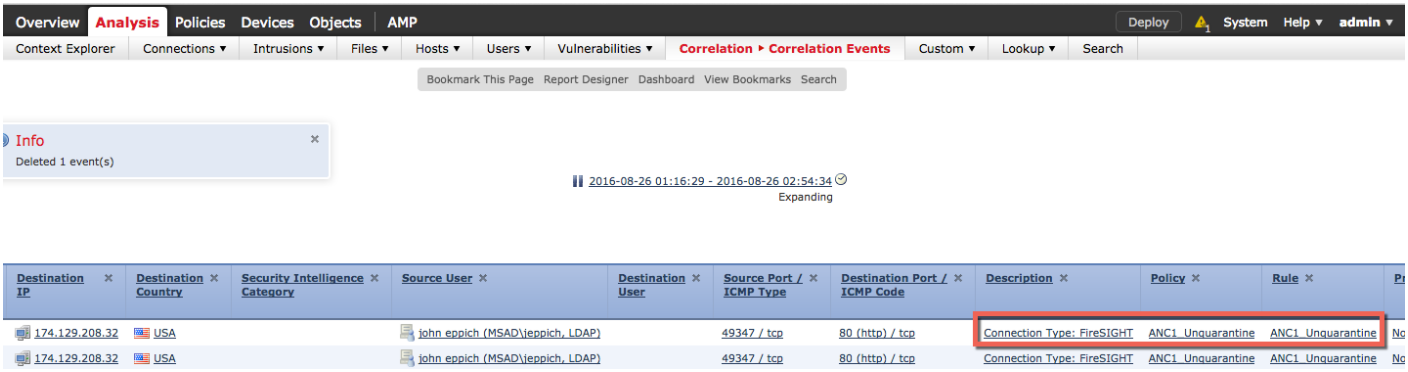
Step 9 Open browser, if Firefox, open up a new private windows, and type: www.putty.org



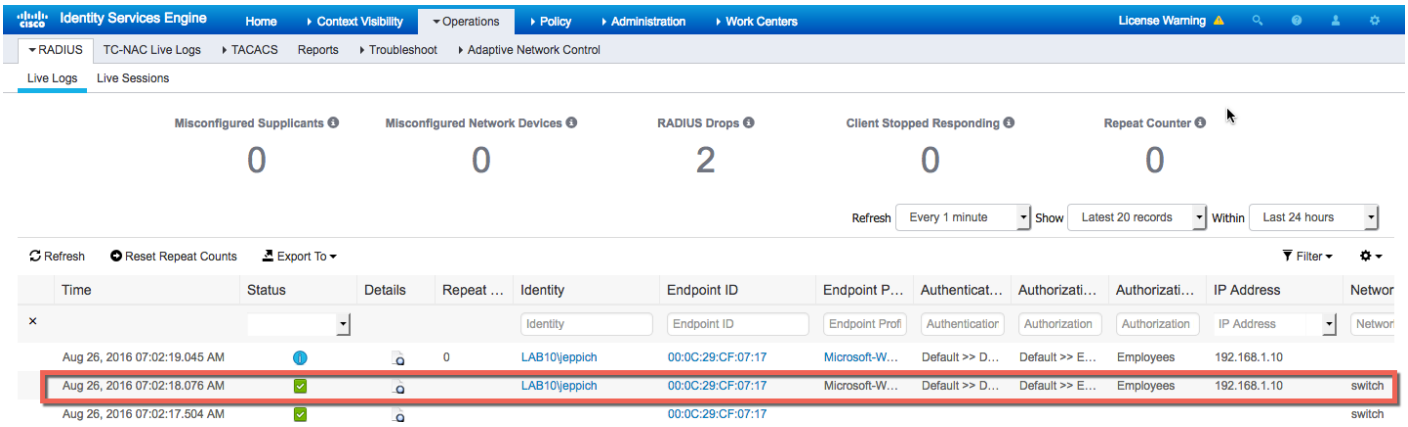
Step 10 Here's the connection event for www.putty.org



Step 11 This triggers the unquarantine correlation policy and correlation rule.



Step 12 The endpoint is unquarantined



Splunk for ISE Add-On 2.20

The section steps through the procedure for generating and issuing the Splunk pxGrid client from the ISE certificate provisioning portal. This also can be used for other security solutions that use java keystores.

This also covers creating the java keystores, the Splunk pxGrid client certificate public and private key-pairs from the PKCS 12 file. Additionally, a step is added to quarantine/unquarantine an endpoint to ensure that everything is working correctly. It is assumed that the reader is familiar with Splunk and ISE pxGrid integration, if not please refer to the: How to: Splunk and ISE pxGrid Adaptive Network Control (ANC) Mitigation Workflow Actions https://communities.cisco.com/docs/DOC-68289

It is assumed that ISE is configured to send Passed/Failed syslog events to Splunk. You will also want to make a change to the pxGrid quarantine and pxGrid unquarantine Splunk workflow action to allow the Framed_IP_Address field

Below is the workflow action for the ANC Quarantine by Framed_IP_Address

```
Label: ANC Quarantine by Framed_IP_Address $Framed_IP_Address$
Apply only to the following fields: Framed_IP_Address
Show action in: Event menu
Action type: search
Search string: | pxgremediate xgridAction=quarantine xgridType=ip xgridTarget="$Framed_IP_Address$"
Run in spp: search
Run search in New window
Use the same time range as the search that created the field listing: enabled
```

Below is the workflow action for the ANC Quarantine by Framed_IP_Address

```
Label: ANC UnQuarantine by Framed_IP_Address $Framed_IP_Address$
Apply only to the following fields: Framed_IP_Address
Show action in: Event menu
Action type: search
Search string: | pxgremediate xgridAction=unquarantine xgridType=ip xgridTarget="$Framed_IP_Address$"
Run in spp: search
Run search in New window
Use the same time range as the search that created the field listing: enabled
```

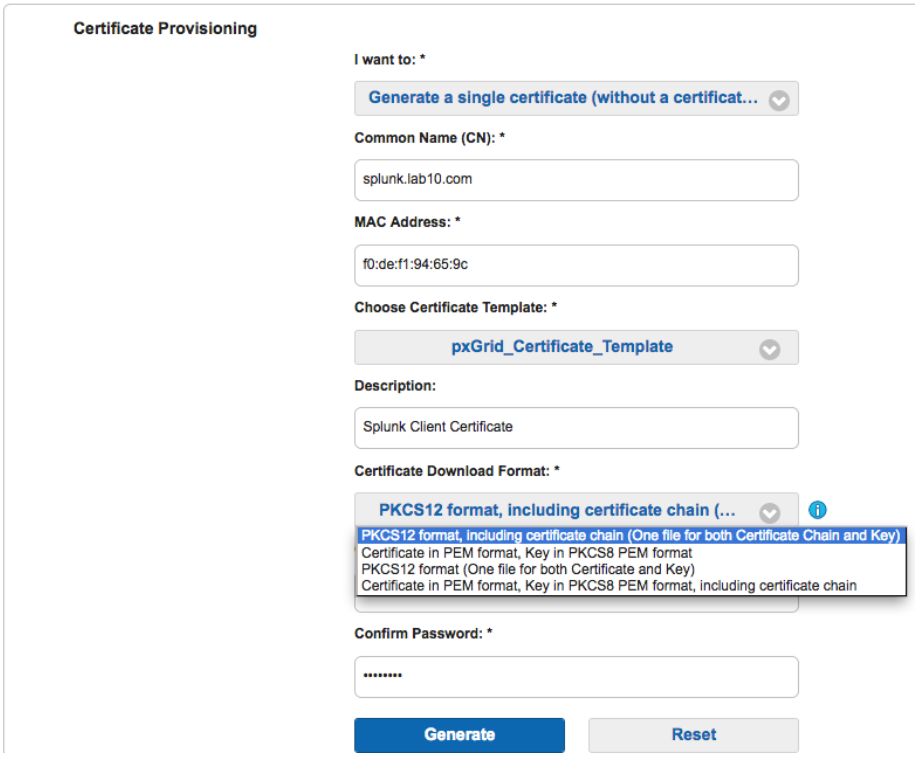
To make the changes in the Splunk for ISE Add-on app, select **Settings->Fields->Workflow actions** and cloning both the pxGrid_QuarantineByIP and pxGrid_UnQuarantineByIP and renaming them to ANC Quarantine by Framed_IP_Address $Framed_IP_Address$ and ANC UnQuarantine by Framed_IP_Address $Framed_IP_Address$ respectively.

It is also assumed the ISE Authorization Policy for EPS:SessionStatus:Equals:Quarantine has been created.

Note: ANC policies in ISE 2.1 will not be used. Splunk subscribes to the EndpointProtectionService Capability when performing quarantine/unquarantine mitigation actions

Generating Splunk pxGrid Client Certificate from ISE Certificate Provisioning Portal

Step 1 Create the certificate for the Splunk client, select **Generate a single certificate (without a certificate signing request)**



Step 2 **Generate** the certificate and save the **certops-2016-08-19_02-21-03.zip** file locally.

Installing ISE and Splunk pxGrid client certificate using Java keystores

On the Linux client where Splunk is installed, use openssl and keytool run the following commands to extract the public certificate and private ley from the PKCS12 file and convert to JKS key stores.

Step 1 Unzip the certops file, you should see the following:

```
splunk.lab10.com_f0-de-f1-94-65-9c.p12
```

Step 2 You can rename or copy the certificate to a more manageable PKCS12 file

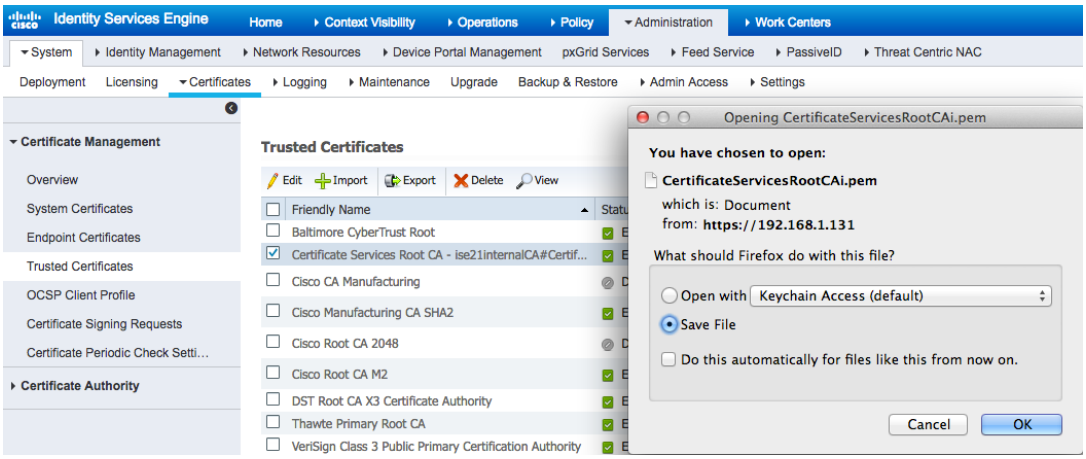
```
cp Johns-Macbook-Pro.lab10.com_f0-de-f1-94-65-9c.p12 splunk.p12
```

Step 3 Create keystore from PKCS12 file

```
keytool -importkeystore -srckeystore splunk.p12 -destkeystore splunk.jks -srcstoretype PKCS12
Enter destination keystore password:  Cisco123
Re-enter new password: Cisco123
Enter source keystore password:  Cisco123
Entry for alias johns-macbook-pro.lab10.com_f0-de-f1-94-65-9c successfully imported.
Import command completed:  1 entries successfully imported, 0 entries failed or cancelled
```

Step 4 Export the public ISEinternalRootCA certificate only

Select **Administration->System->Certificates->Trusted Certificates->Certificate Services Root CA->Export**



Step 5 Convert the ISEinternalRootCA.PEM file over from ISE and convert to DER format

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

Step 6 Add the ISE root certificate to the truststore file keystore (i.e. rootiseCA.jks)

```
keytool -import -alias splunk -keystore rootiseCA.jks -file CertificateServicesRootCAi.der
Enter keystore password: Cisco123
Re-enter new password: Cisco123
Owner: CN=Certificate Services Root CA - ise21internalCA
Issuer: CN=Certificate Services Root CA - ise21internalCA
Serial number: 5b69192c64484955b925f445e53014fc
Valid from: Sun Jul 17 23:05:48 EDT 2016 until: Sat Jul 18 23:05:48 EDT 2026
Certificate fingerprints:
         MD5:  7B:AA:73:88:21:7F:45:70:50:F9:6C:F0:24:40:EA:AA
         SHA1: 0C:4B:7F:A7:42:FC:5C:30:22:9E:C8:BF:FB:E0:AB:C1:33:48:44:18
         SHA256:
3C:27:24:70:8F:EC:22:8B:86:5C:8F:78:CF:D6:83:90:98:4E:11:0F:AF:5C:19:67:9F:F4:90:A8:33:A9:37:54
         Signature algorithm name: SHA256withRSA
         Version: 3

Extensions:

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

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

#3: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: F1 1E 3A AF B0 B1 40 72   4C 53 7E 29 1C C1 05 DC  ..:...@rLS.)....
0010: A4 5F B4 80                                        ._..
]
]
```

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

Step 7 Generate splunk public certificate from splunk PKCS 12 file

```
openssl pkcs12 -nokeys -clcerts -in splunk.p12 -out splunk.cer
Enter Import Password: Cisco123
MAC verified OK
```

Step 8 Generate splunk private key from splunk PKCS 12 file

```
openssl pkcs12 -nocerts -in splunk.p12 -out splunk.key
Enter Import Password: Cisco123
MAC verified OK
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
```

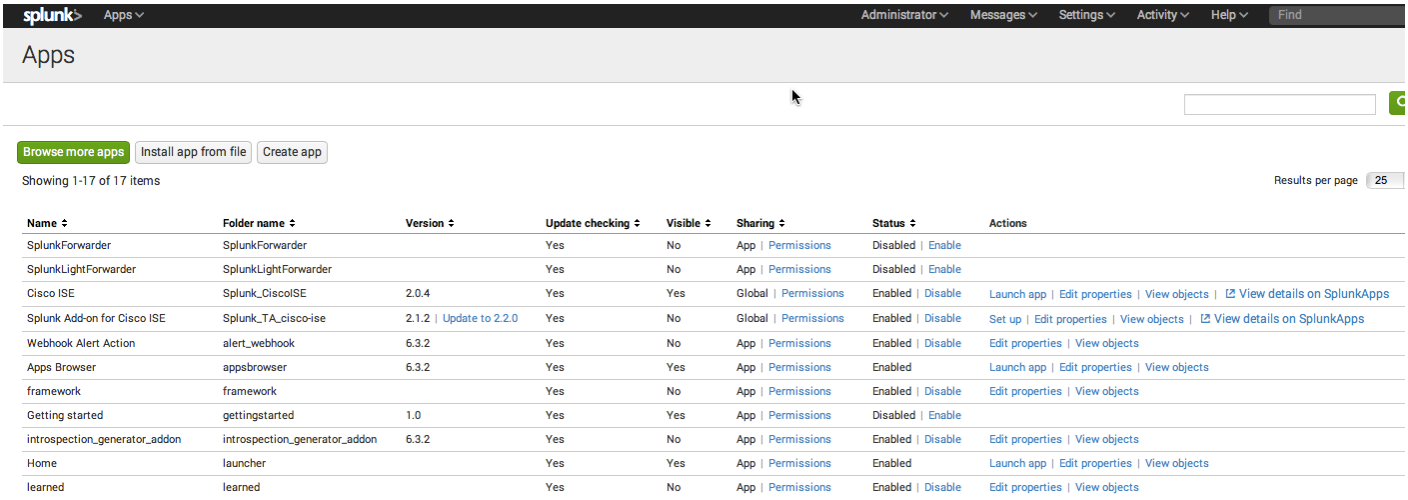
Step 9 Add the splunk public certificate to client keystore

```
keytool -import -alias splunk1 -keystore splunk.jks -file splunk.cer
Enter keystore password: Cisco123
Re-enter new password: Cisco123
Owner: CN=Johns-Macbook-Pro.lab10.com
Issuer: CN=Certificate Services Endpoint Sub CA - ise21internalCA
Serial number: 5b762edb18854a4787f4b71bf7d44dd6
Valid from: Wed Aug 17 22:21:03 EDT 2016 until: Sat Aug 18 22:21:03 EDT 2018
Certificate fingerprints:
         MD5:  21:43:AF:9F:06:13:4A:D1:C3:0B:6C:46:EE:52:35:90
         SHA1: 42:B1:E0:D6:7B:4B:CF:34:C7:F2:A5:29:D4:CB:CE:37:8C:11:3A:A7
         SHA256:
64:AA:7A:2B:AA:13:20:FB:E4:EE:FA:CC:08:30:C4:1F:9E:7B:15:3E:7D:B4:BB:15:31:10:F1:69:D9:42:E2:0E
         Signature algorithm name: SHA256withRSA
         Version: 3

Extensions:

#1: ObjectId: 1.3.6.1.4.1.9.21.2.5 Criticality=false
0000: 04 1B 70 78 47 72 69 64   5F 43 65 72 74 69 66 69  ..pxGrid_Certifi
0010: 63 61 74 65 5F 54 65 6D   70 6C 61 74 65           cate_Template


#2: ObjectId: 2.5.29.35 Criticality=false
AuthorityKeyIdentifier [
KeyIdentifier [
0000: BB 37 EA 0C E7 36 91 72   E3 9F 2A FA 4D 51 95 5A  .7...6.r..*.MQ.Z
0010: 7F EA 29 D1                                        ..).
]
[CN=Certificate Services Node CA - ise21internalCA]
SerialNumber: [    69d92403 adb24e16 94aff763 0d2f2c63]
]

#3: ObjectId: 2.5.29.19 Criticality=true
BasicConstraints:[
  CA:false
  PathLen: undefined
]

#4: ObjectId: 2.5.29.37 Criticality=true
ExtendedKeyUsages [
  serverAuth
  clientAuth
```

```
]

#5: ObjectId: 2.5.29.15 Criticality=true
KeyUsage [
  DigitalSignature
  Non_repudiation
  Key_Encipherment
]

#6: ObjectId: 2.5.29.17 Criticality=true
SubjectAlternativeName [
  RFC822Name: f0-de-f1-94-65-9c
]

#7: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: 22 8A BD A2 64 59 DB A2   1F 4B 22 62 16 84 1B 1D  "...dY...K"b....
0010: A9 B7 FD 0F                                        ....
]
]

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

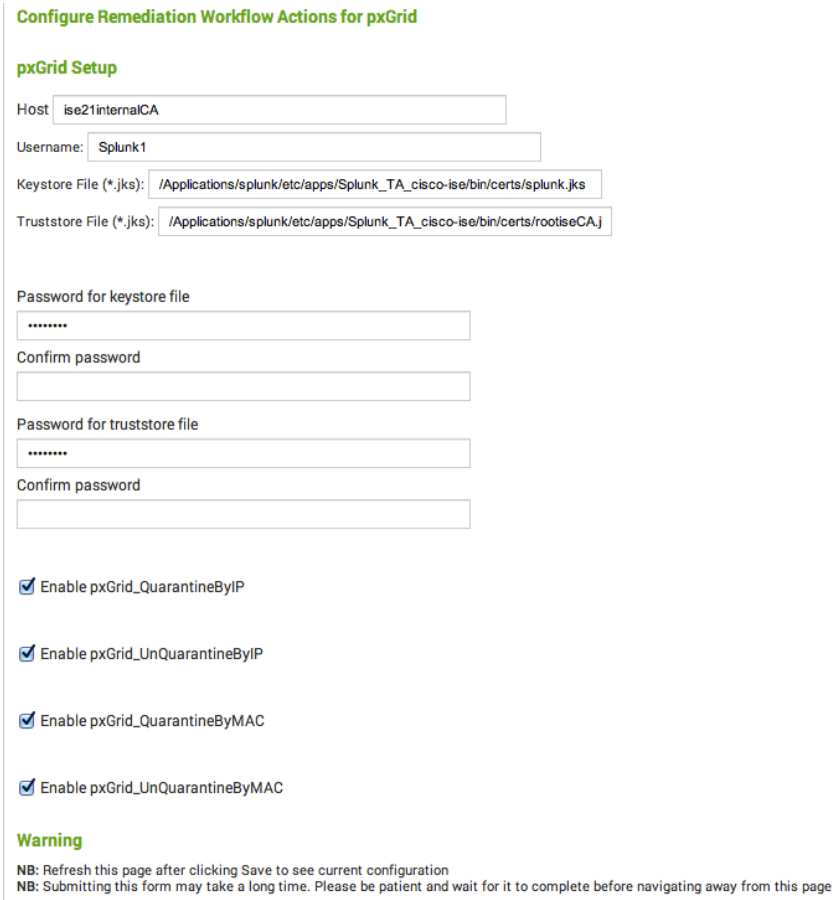
Testing Connection Between Splunk and the ISE pxGrid node

Step 1 Select **Splunk->Apps,** you should see the Splunk Add-on for Cisco ISE



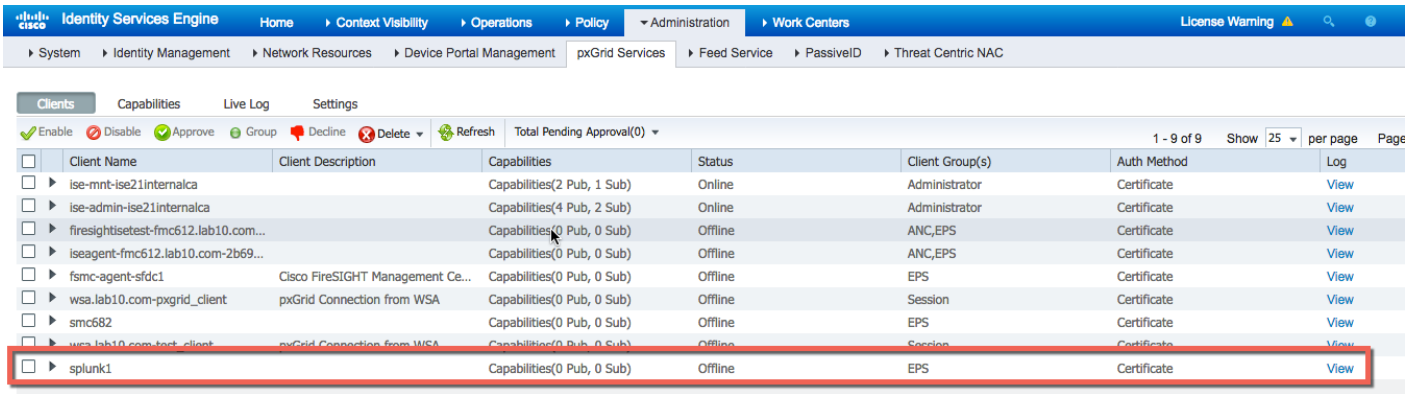
Step 2 Select **Set Up**
You should see the following:

Host: refers to the ISE pxGrid node FQDN or IP Address
Username: pxGrid client
Keystore File: Path and filename of keystore JKS file (i.e.splunk.jks)
Truststore File: Path and filename of Truststore JKS file (i.e. rootiseCA.jks)
Password for Keystore File
Password for Truststore File



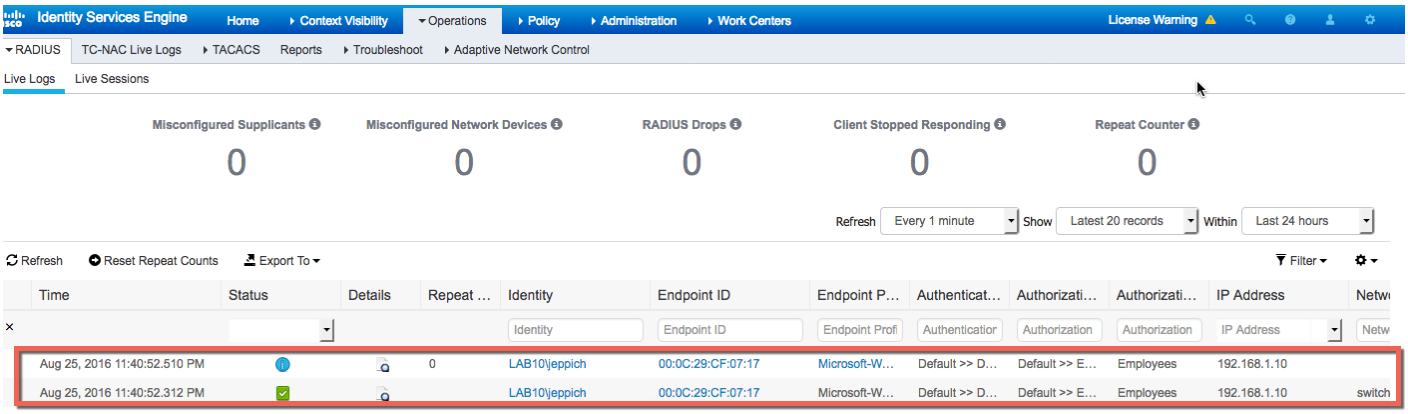
Step 3 Select **Save**

Step 4 You should see the following:

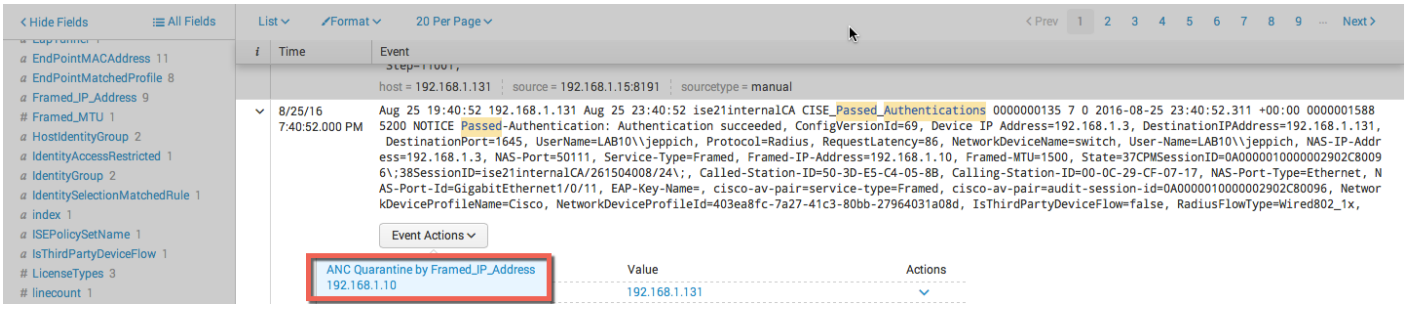


Testing Splunk Quarantine and UnQuarantine Adaptive Network Control (ANC) Mitigation Actions

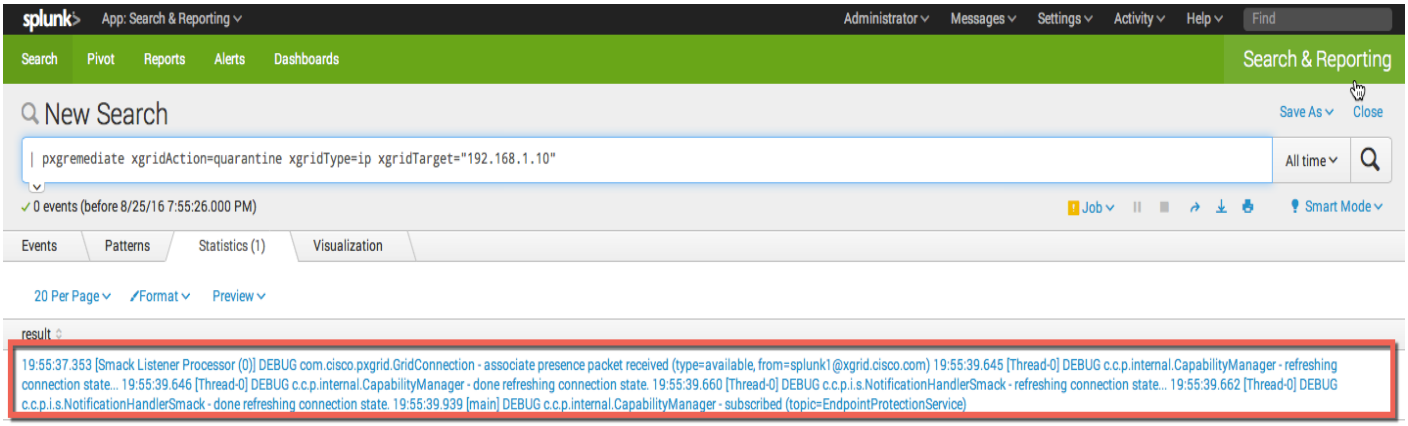
Step 1 The end-use successfully authenticates to the network



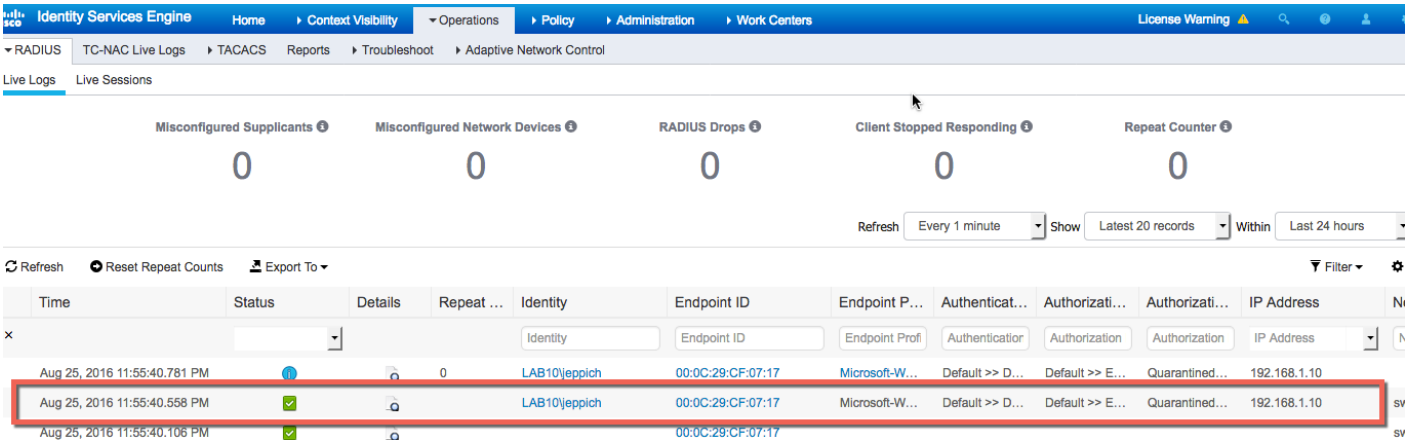
Step 2 Based on the received Passed Authentications syslog event the pxGrid Quarantine and pxGrid Unquarantine workflow actions will appear under the Event Actions. Select ANC Quarantine by Framed_IP Address workflow event to trigger the quarantine mitigation action.



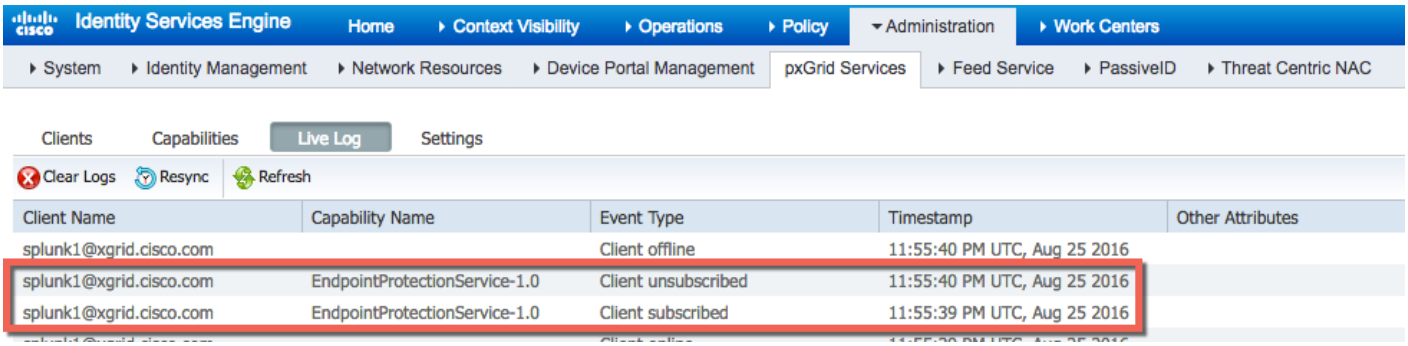
Step 3 You should see the results of the ANC mitigation action in Splunk.



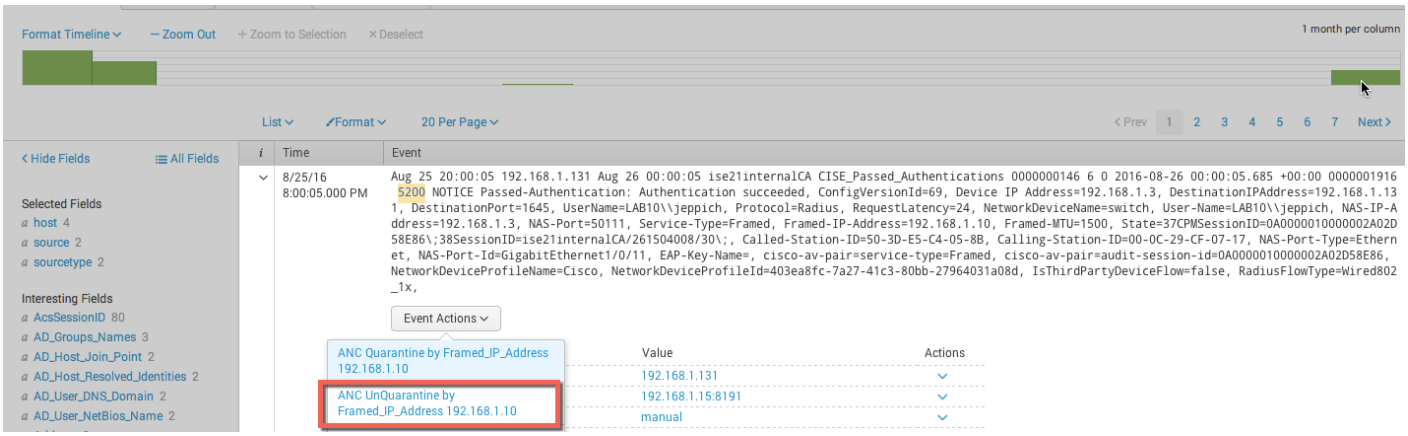
Step 4 The endpoint is quarantined in ISE



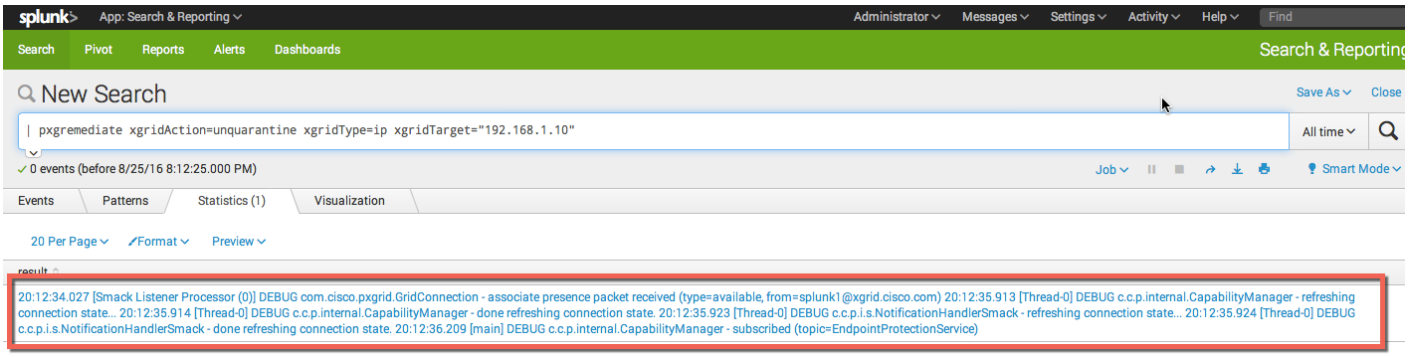
Step 5 Below are the results of the subscription to the EndpointPointProtectionService Capability when performing the EPS quarantine mitigation action.



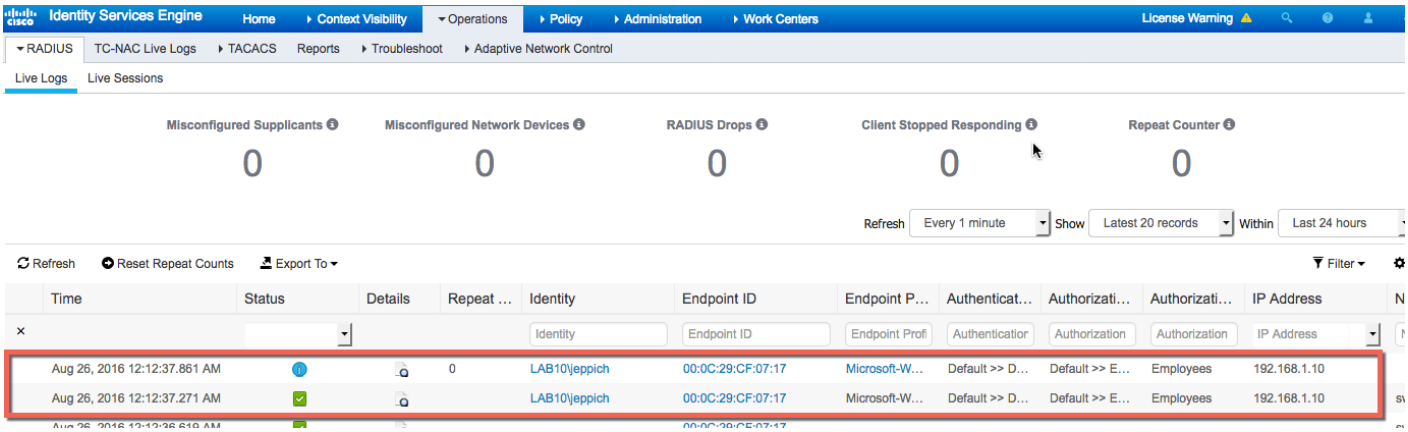
Step 6 In the below example, the pxGrid Unquarantine workflow action is selected.



Step 7 The results of the pxGrid unquarantine mitigation are displayed.



Step 8 The endpoint is dynamically unquarantined.



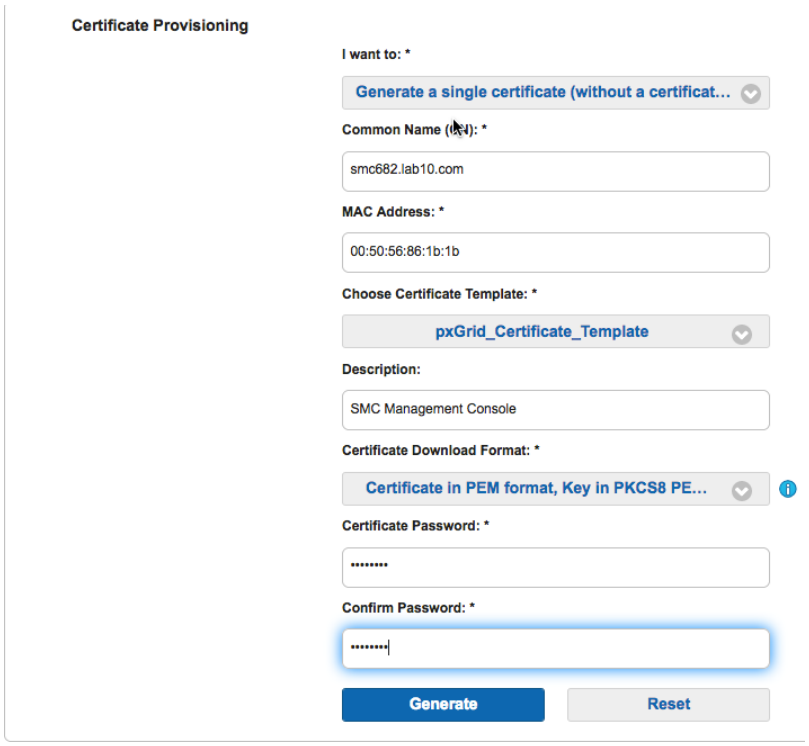
Stealthwatch

The section steps through the procedure for generating and issuing the Stealthwatch pxGrid client from the ISE certificate provisioning portal. This also covers importing the ISECArootservices , ISEEndPointSUBCA, and Stealthwatch pxGrid client certificate public and private key-pair into the Stealthwatch truststore. Additionally, a step is added to quaranatine/unquarantine an endpoint to ensure that everything is working correctly. It is assumed that the reader is familiar with Stealthwatch and ISE integration, please see: How To: Deploy Lancope Stealthwatch with pxGrid https://communities.cisco.com/docs/DOC-68288 It is also assumed that ISE is configured to send the Passed/Failed Authentication, Administrative and Operational Audit, RADIUS Accounting, Profiler syslog events to Stealthwatch and the ISE Authorization Quarantine policy has been pre-configured for EPS:SesssionStatus:Equals:Quarantine.

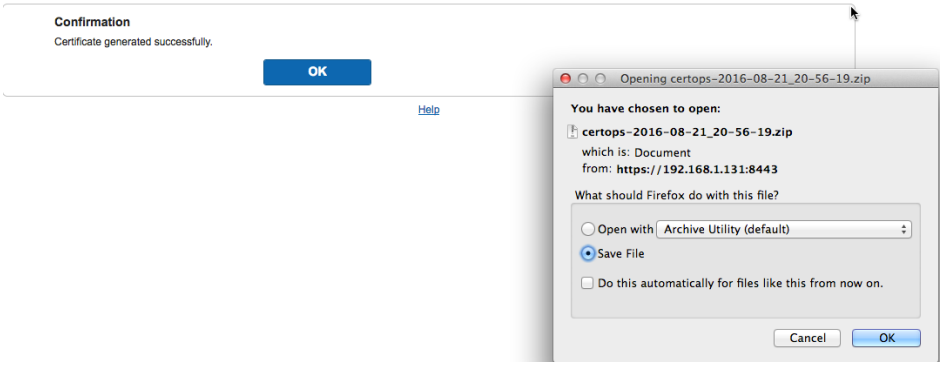
Note: ANC policies in ISE 2.1 will not be used. Stealthwatch subscribes to the EndpointProtectionService Capability when performing quarantine/unquarantine mitigation actions

Generating Stealthwatch pxGrid Client Certificate from ISE Certificate Provisioning Portal

Step 1 Create the certificate for the Splunk client, select **Generate a single certificate (without a certificate signing request)**



Step 2 **Generate** the certificate and save the **certops-2016-08-19_02-21-03.zip** file locally.



Step 3 You should see the following files:

CertificateServicesEndpointSubCA-ise21internalCA_.cer	Aug 21, 2016 8:56 PM	2 KB	certificate
CertificateServicesNodeCA-ise21internalCA_.cer	Aug 21, 2016 8:56 PM	2 KB	certificate
CertificateServicesRootCA-ise21internalCA_.cer	Aug 21, 2016 8:56 PM	2 KB	certificate
smc682.lab10.com_00-50-56-86-1b-1b.cer	Aug 21, 2016 8:56 PM	2 KB	certificate
smc682.lab10.com_00-50-56-86-1b-1b.key	Aug 21, 2016 5:27 PM	2 KB	Keyno...ument

Step 4 Select **Admin User->Administer Appliance->Configuration->Certificate Authority Certificates->Browse**

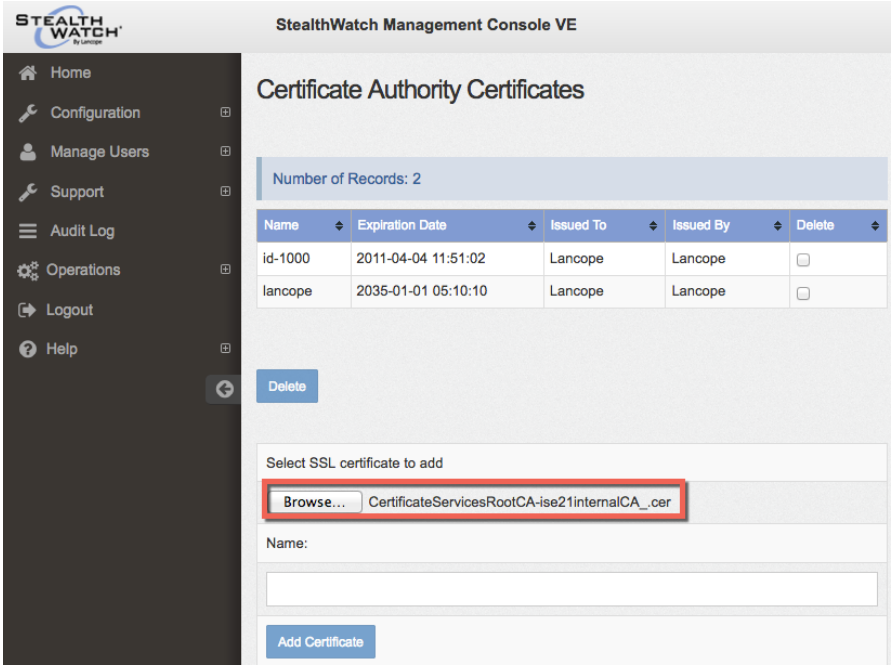
Note: **You will be prompted again by Stealthwatch to verify your credentials**

Importing ISE and pxGrid client certificates

Step 1 Select **Admin User->Administer Appliance->Configuration->Certificate Authority Certificates->Browse**

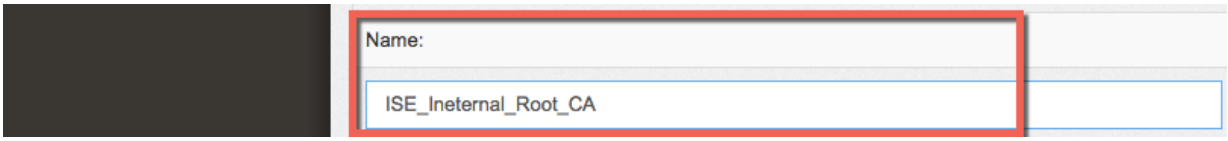
Note: **You will be prompted again be Stealthwatch to verify your credentials**

Step 2 Select Ce**rtfiicateServicesRootCA-iseinternalCA_.cer certificate**

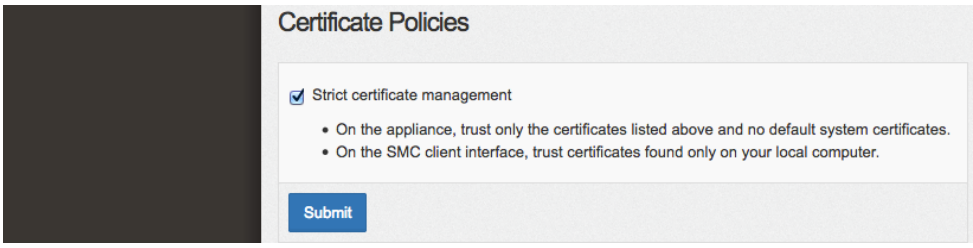


Step 3 Provide a description for the certificate

```
Note: Use Underscores, DO NOT use spaces
```

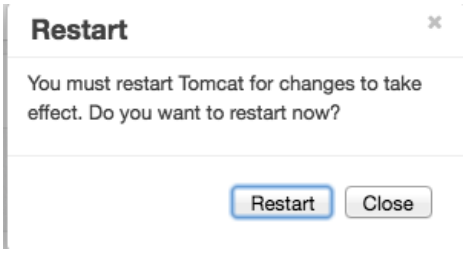


Step 4 Select **Enable Strict Management**

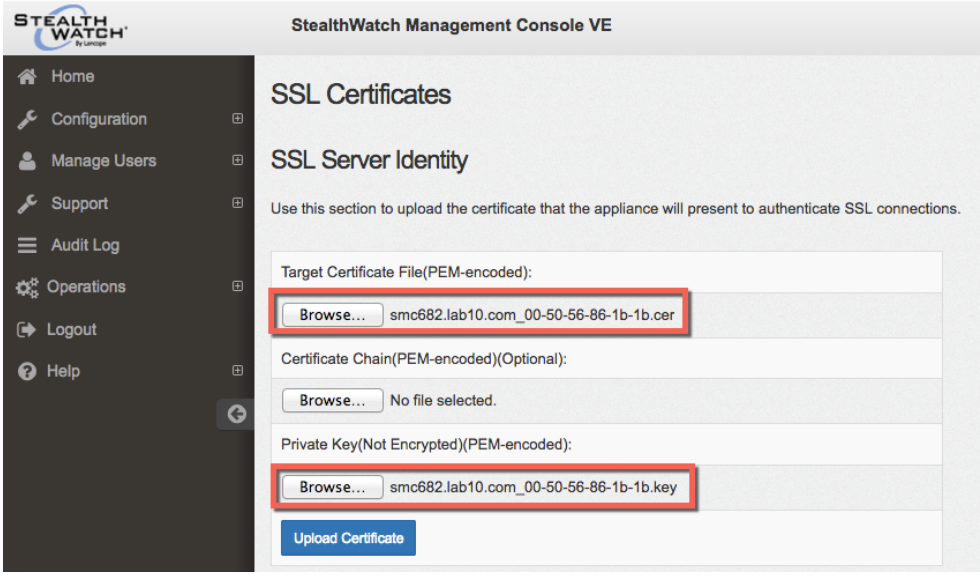


Step 5 Select **Submit**

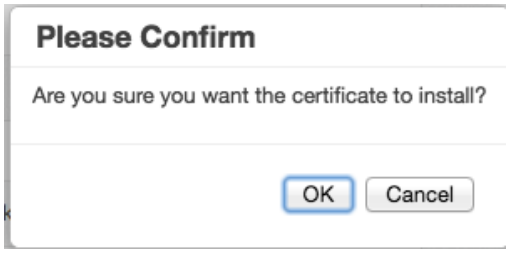
Step 6 Select **Restart**



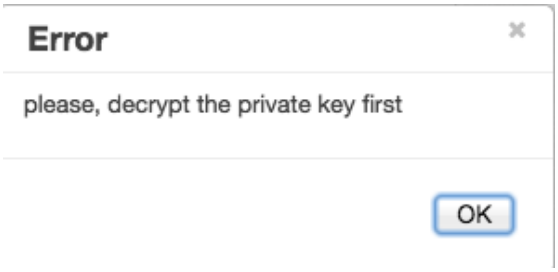
Step 7 Select **Admin User->Administer Appliance->Configuration-SSL Certificate->SSL Server Identity**



Step 8 Select **OK**



Step 9 You will see a message to decrypt the private keys

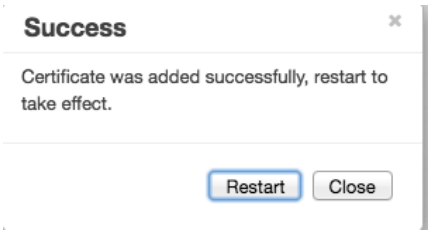


Step 10 Type the following to decrypt the private keys

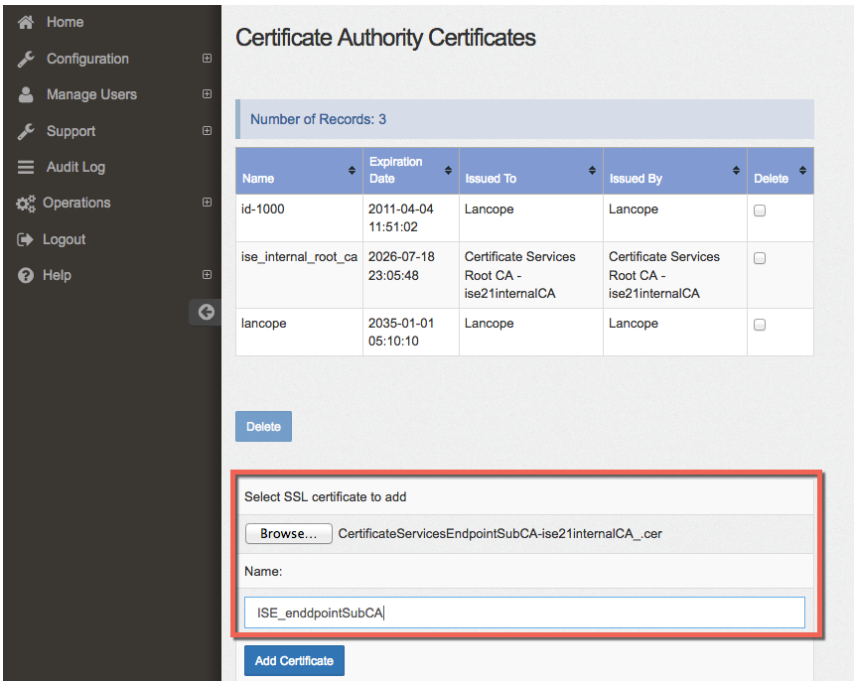
Note: This is the password you typed in for generating the Stealthwatch certificate on ISE

```
cp smc682.lab10.com_00-50-56-86-1b-1b.key smc682.lab10.com_00-50-56-86-1b-1b.key.org

openssl rsa -in smc682.lab10.com_00-50-56-86-1b-1b.key.org -out smc682.lab10.com_00-50-56-86-1b-1b.key
Enter pass phrase for smc682.lab10.com_00-50-56-86-1b-1b.key.org: Cisco123
writing RSA key
```

Step 11 You should see certificate was added successfully restart

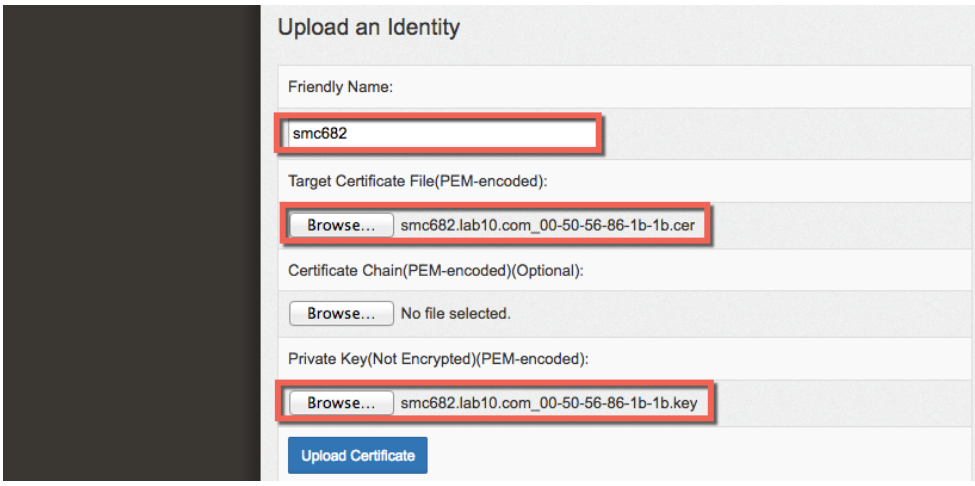


Step 12 Upload the ISE subordinate certificate, **CertificateServicesEndpointSubCA-is21internalCA_.cer**



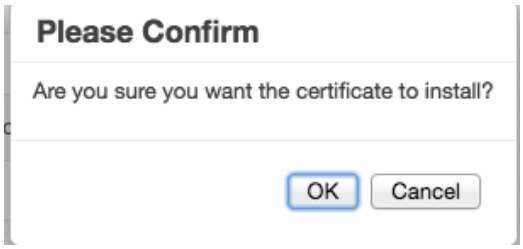
Step 13 Provide a description name (i.e. **ISE_endpointSubCA**)

Step 14 Under **SSL Certificates->Upload an identity->** Select the **Stealthwatch public and private keys**

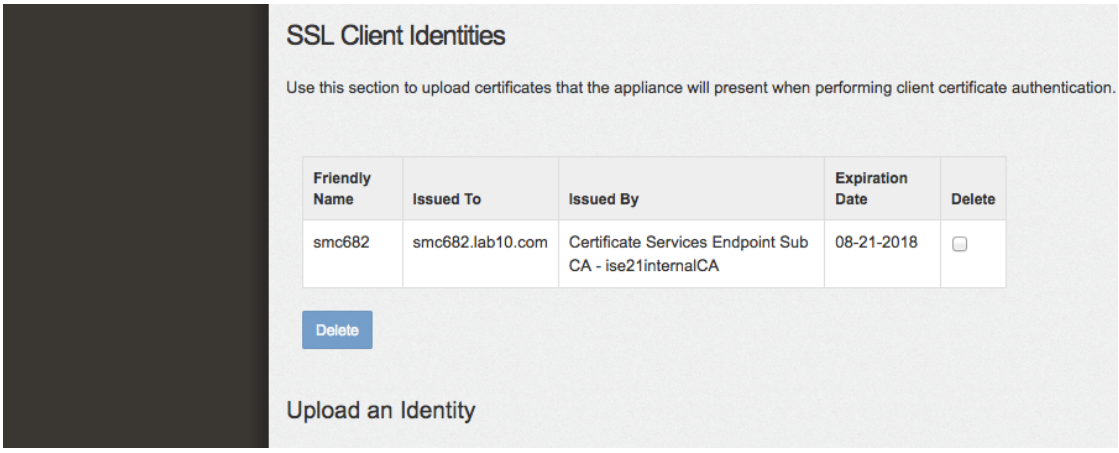


Step 15 Provide friendly name description for the Stealthwatch client certificate (i.e. smc682)

Step 16 Select OK to confirm the install

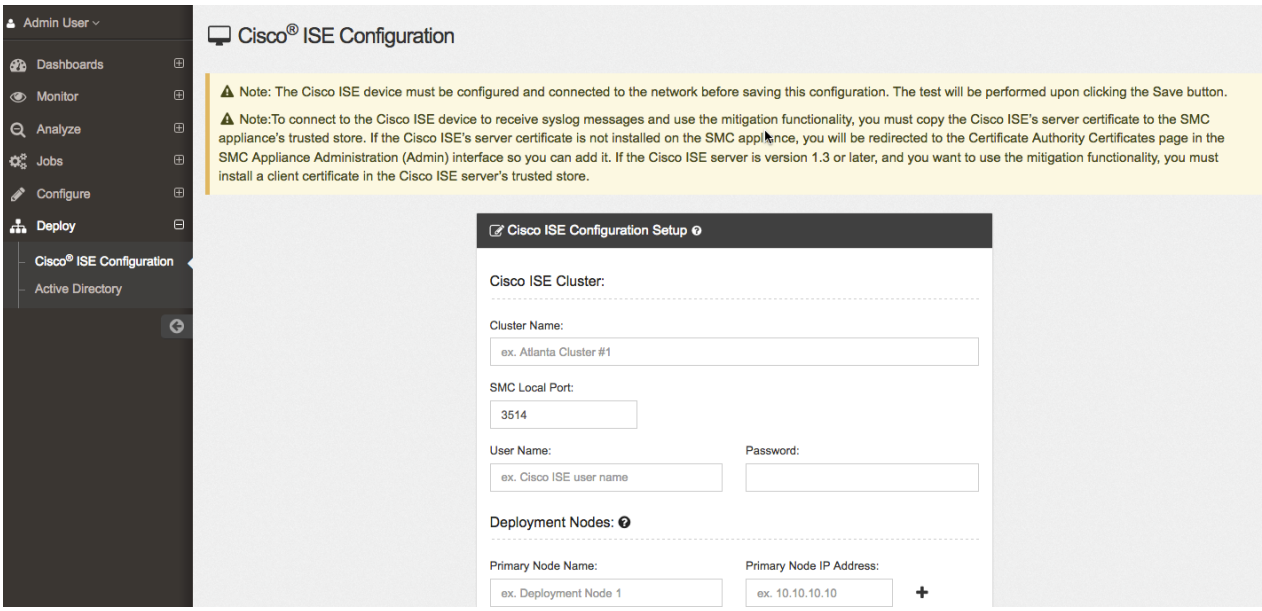


Step 17 You should see the following:

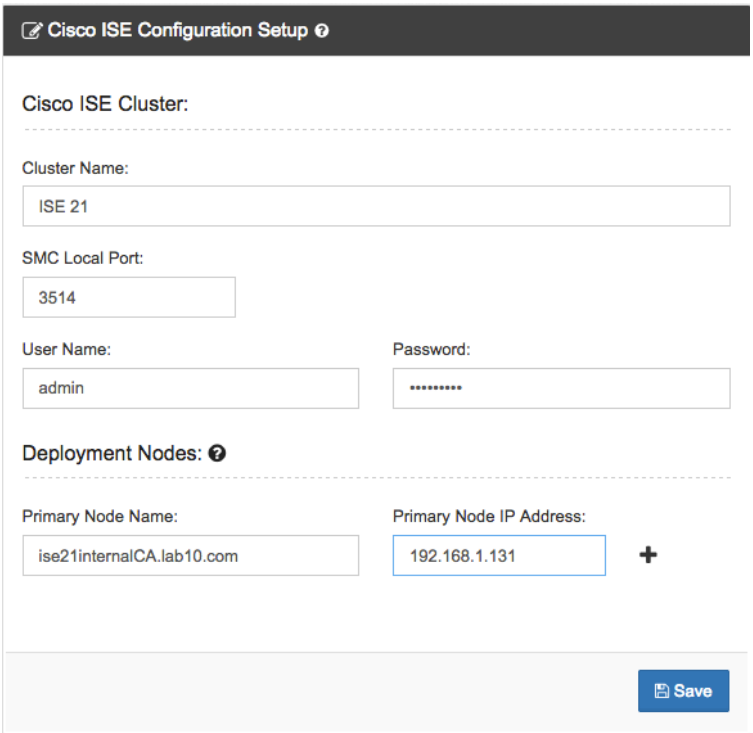


Configuring ISE pxGrid node

Step 1 Select **Deploy->Cisco ISE Configuration,** you should see the following:

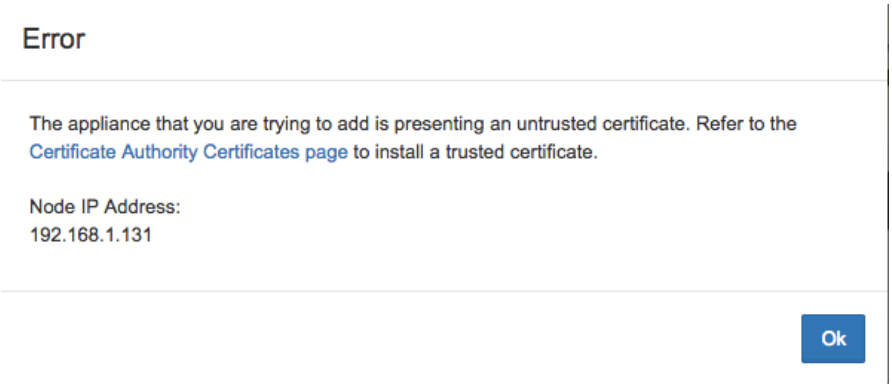


Step 2 Enter the following

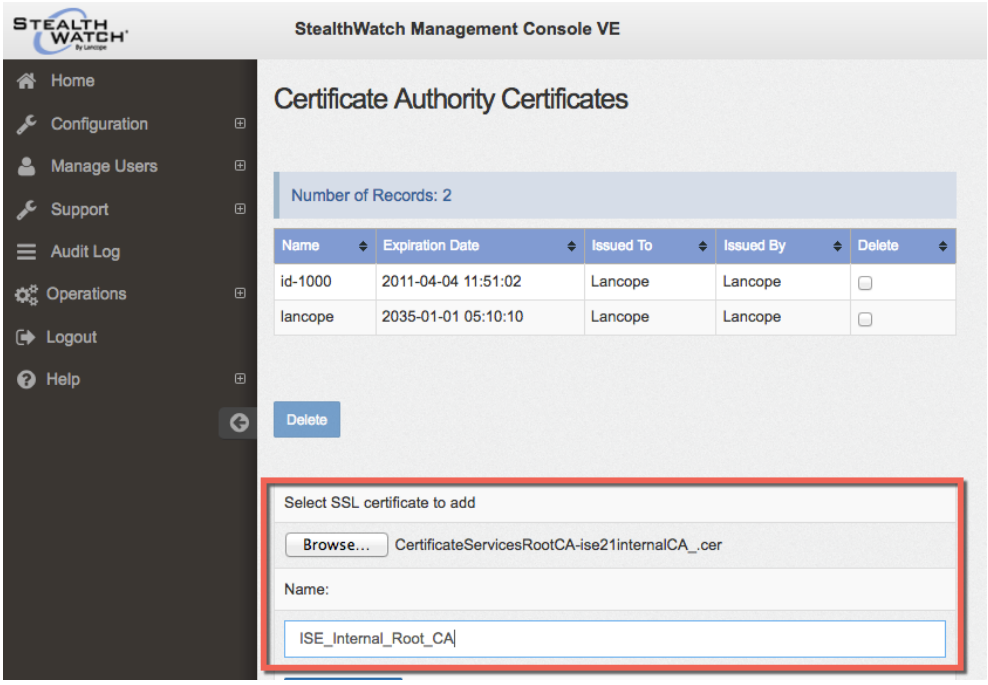


Step 3 Select **Save**

Step 4 You may see the following message, select **OK**

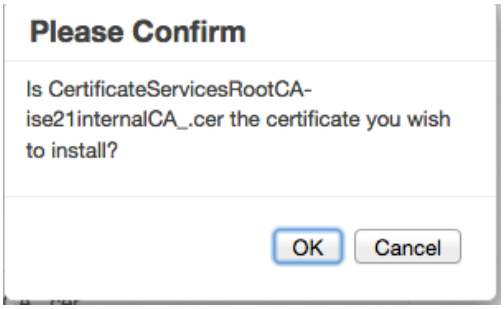


Step 5 Ensure the CA certificate is there, if not, You will need to upload the ISE CA root certificate again



Step 6 Select **Add->Certificate**

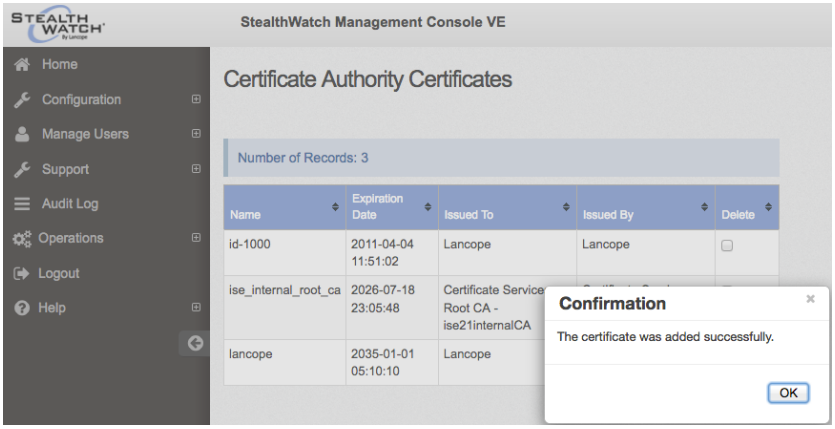
Step 7 You will see the following



`

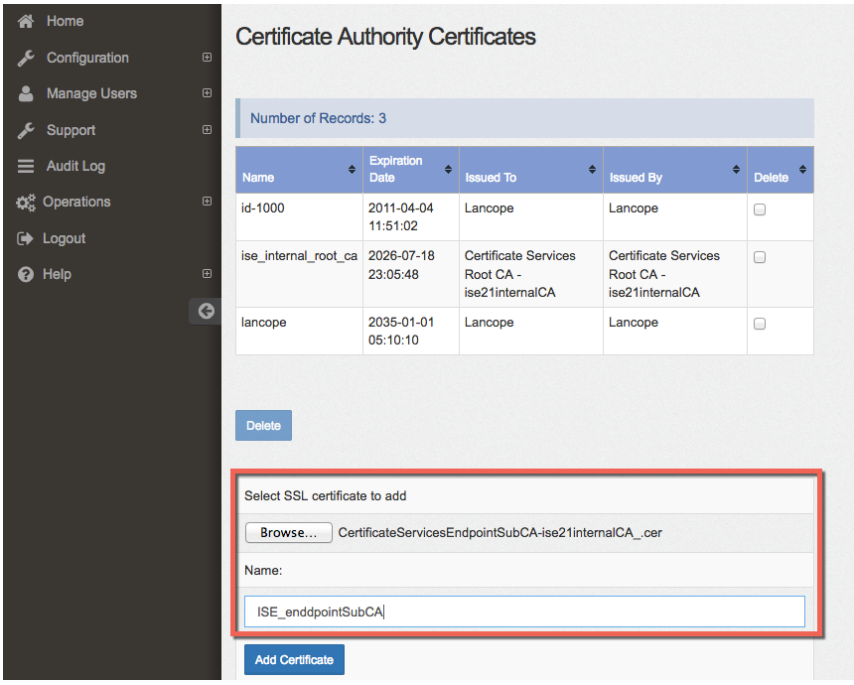
Step 8 Select **OK**

Step 9 You should see the certificate was added successfully

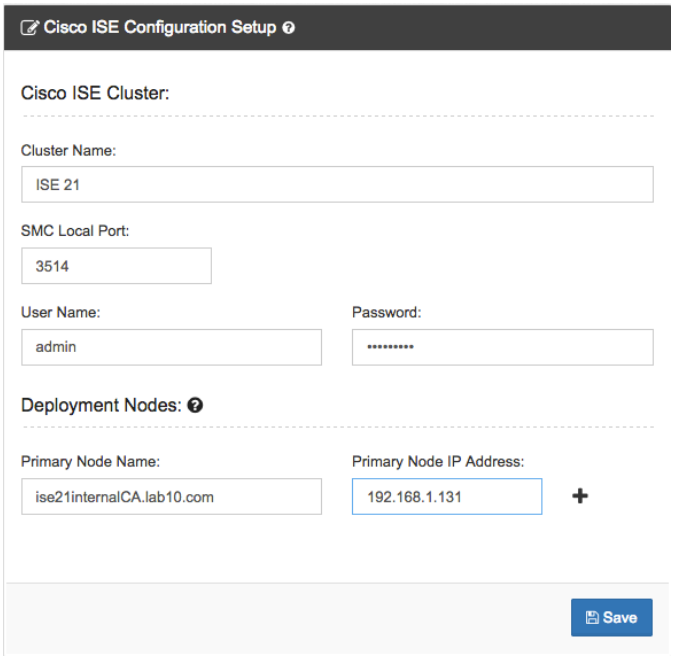


Step 10 Select **OK**

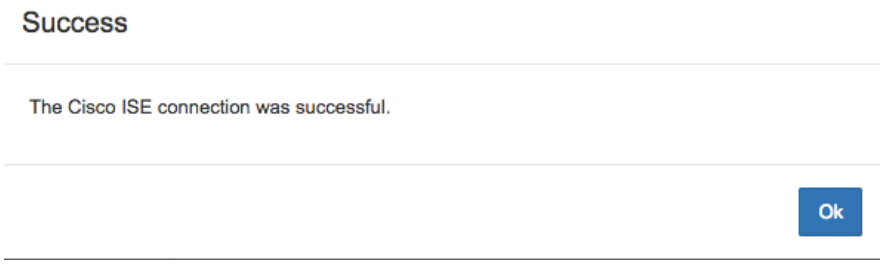
Step 11 Verify the ISE subordinate endpoint certificate is there as well.



Step 12 Go back and re-try the ISE configuration

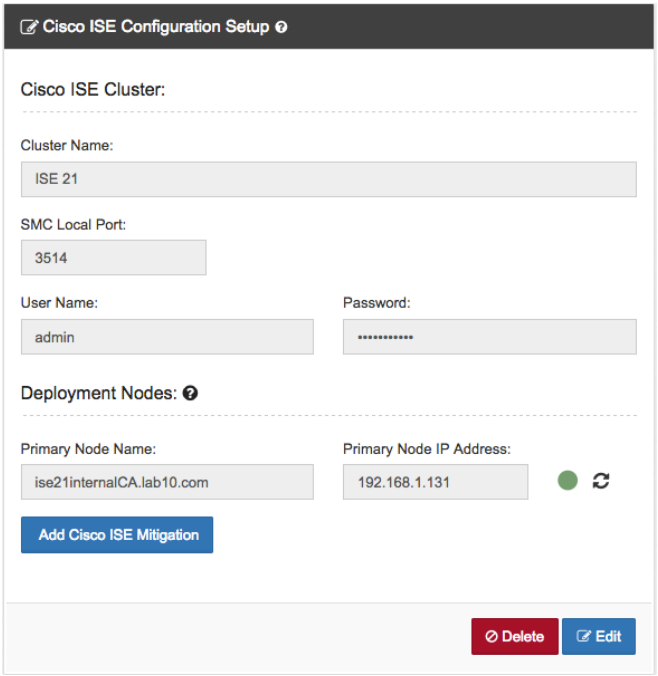


Step 13 You should see a successfully connection

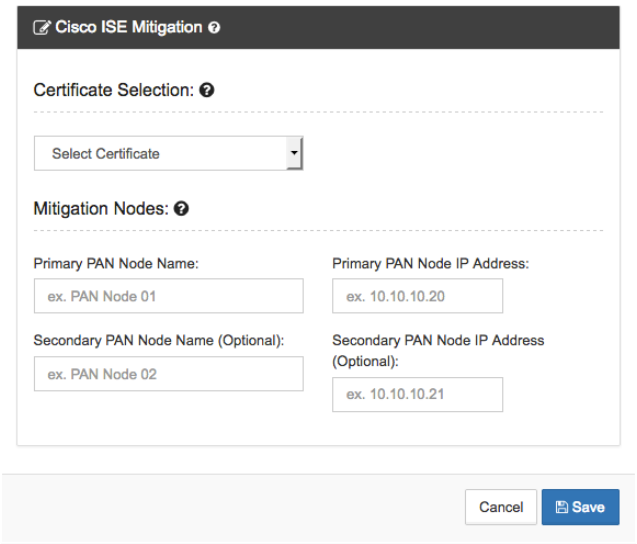


Step 14 Select **OK**

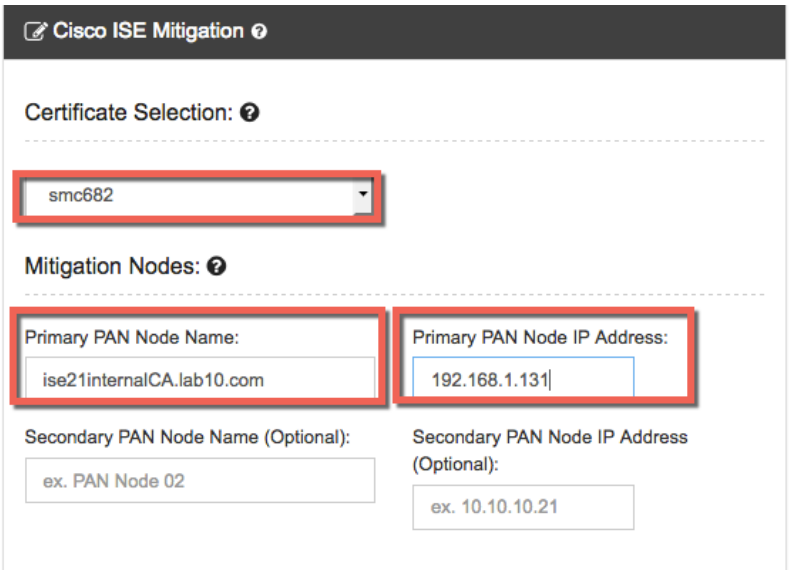
Step 15 You should see the following:



Step 16 Select **Add Cisco ISE Mitigation**
You should see the following:

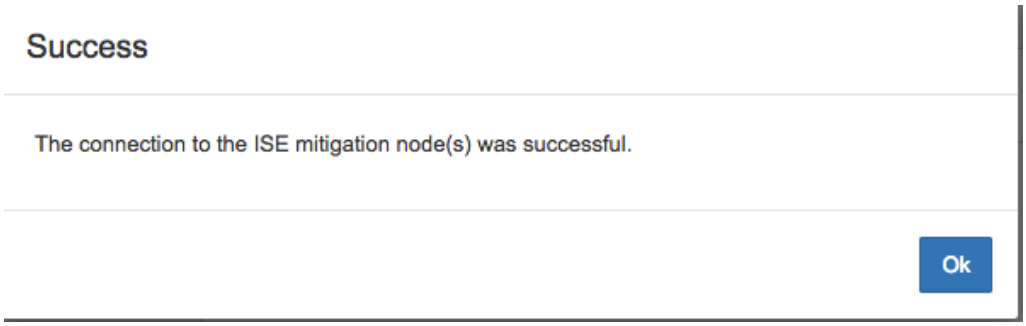


Step 17 Select the smc682 client certificate, and enter the ISE pxGrid node FQDN and IP address



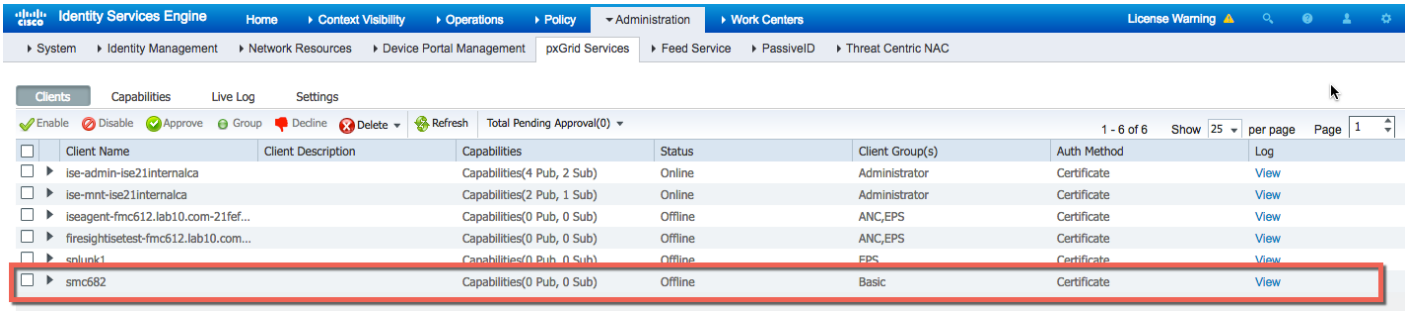
Step 18 Select **Save**

Step 19 You should see successful

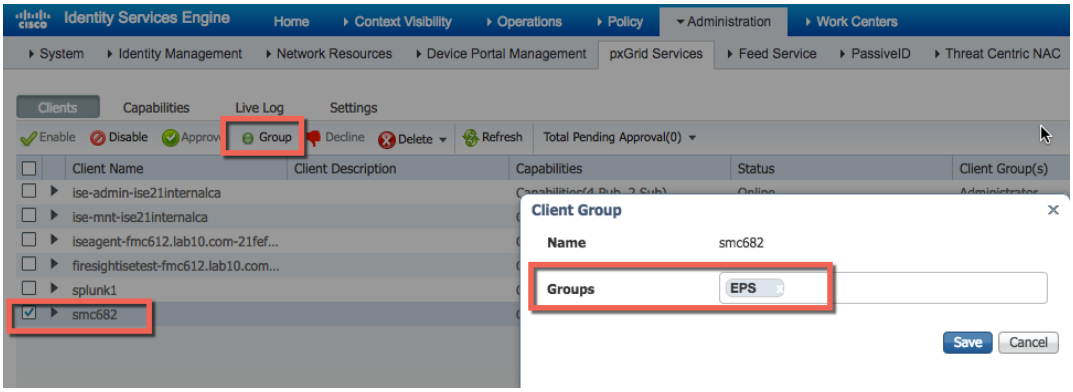


Step 20 Select **OK**

Step 21 Ensure the Stealthwatch pxGrid client is successfully registered to the ISE pxGrid node
Select **Administration->pxGrid Services,** you should see the Stealthwatch registered client registered to the Basic Client Group

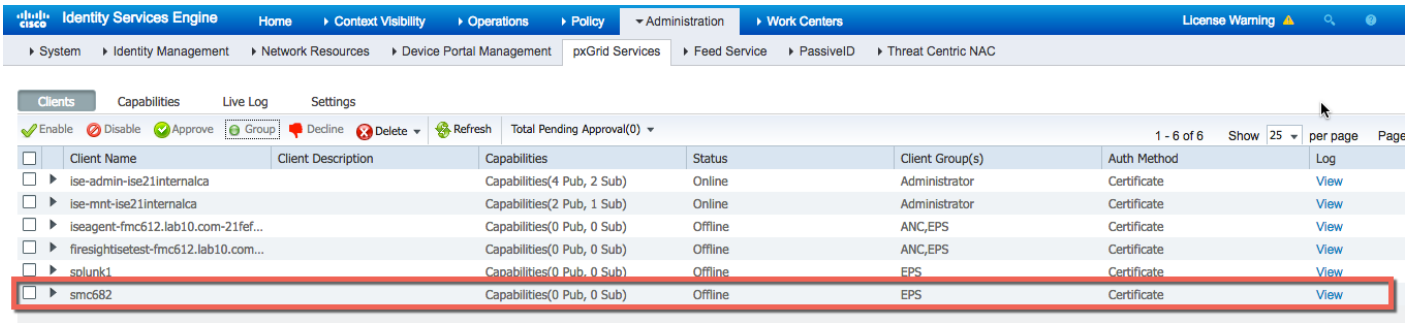


Step 22 Select the **Stealthwatch client->Group-> add to EPS group**, remove Basic group



Step 23 Select **Save**

Step 24 The Stealthwatch client should now be assigned to the EPS client group



SMC Client Configuration

Step 1 Download and install the Oracle Java Development kit, and include JDK in your path

Step 2 Enable Java Console to appear
Select **All programs->Java->Configure Java->Advanced->Java Console->Show Console->Apply->OK**

Step 3 Launch the SMC client, you will see **unable to launch Stealthwatch SMC client**, locate the path for theTrustStoreHelper

```
…[TrustoreHelper] System CA trust store loaded from :/Library/Internet Plug-
Ins/JavaAppletPlugin.plugin/Contents/Home/lib/security/cacerts
```

Step 4 On the host, import the ISE CA root certificate into the cacerts file identified in the previous step, the default password for the cacerts file is: **changeit**

```
keytool -keystore cacerts -importcert -alias myca -file /Applications/sw682/CertificateServicesRootCA-
ise21internalCA_.cer
Enter keystore password:  changeit
Owner: CN=Certificate Services Root CA - ise21internalCA
Issuer: CN=Certificate Services Root CA - ise21internalCA
Serial number: 5b69192c64484955b925f445e53014fc
Valid from: Sun Jul 17 23:05:48 EDT 2016 until: Sat Jul 18 23:05:48 EDT 2026
Certificate fingerprints:
         MD5:  7B:AA:73:88:21:7F:45:70:50:F9:6C:F0:24:40:EA:AA
         SHA1: 0C:4B:7F:A7:42:FC:5C:30:22:9E:C8:BF:FB:E0:AB:C1:33:48:44:18
         SHA256:
3C:27:24:70:8F:EC:22:8B:86:5C:8F:78:CF:D6:83:90:98:4E:11:0F:AF:5C:19:67:9F:F4:90:A8:33:A9:37:54
         Signature algorithm name: SHA256withRSA
         Version: 3

Extensions:

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

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

#3: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: F1 1E 3A AF B0 B1 40 72   4C 53 7E 29 1C C1 05 DC  ..:...@rLS.)....
0010: A4 5F B4 80                                        ._..
]
]

Trust this certificate? [no]:  yes
Certificate was added to keystore
keytool error: java.io.FileNotFoundException: cacerts (Permission denied)
Johns-MacBook-Pro:security jeppich$ sudo keytool -keystore cacerts -importcert -alias myca -file
/Applications/sw682/CertificateServicesRootCA-ise21internalCA_.cer
Password:
Sorry, try again.
Password:
Sorry, try again.
Password:
Sorry, try again.
sudo: 3 incorrect password attempts
Johns-MacBook-Pro:security jeppich$ sudo keytool -keystore cacerts -importcert -alias myca -file
/Applications/sw682/CertificateServicesRootCA-ise21internalCA_.cer
Password:
Enter keystore password:
Owner: CN=Certificate Services Root CA - ise21internalCA
Issuer: CN=Certificate Services Root CA - ise21internalCA
Serial number: 5b69192c64484955b925f445e53014fc
Valid from: Sun Jul 17 23:05:48 EDT 2016 until: Sat Jul 18 23:05:48 EDT 2026
Certificate fingerprints:
         MD5:  7B:AA:73:88:21:7F:45:70:50:F9:6C:F0:24:40:EA:AA
         SHA1: 0C:4B:7F:A7:42:FC:5C:30:22:9E:C8:BF:FB:E0:AB:C1:33:48:44:18
         SHA256:
3C:27:24:70:8F:EC:22:8B:86:5C:8F:78:CF:D6:83:90:98:4E:11:0F:AF:5C:19:67:9F:F4:90:A8:33:A9:37:54
         Signature algorithm name: SHA256withRSA
         Version: 3

Extensions:

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

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

#3: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: F1 1E 3A AF B0 B1 40 72   4C 53 7E 29 1C C1 05 DC  ..:...@rLS.)....
0010: A4 5F B4 80                                        ._..
]
]

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

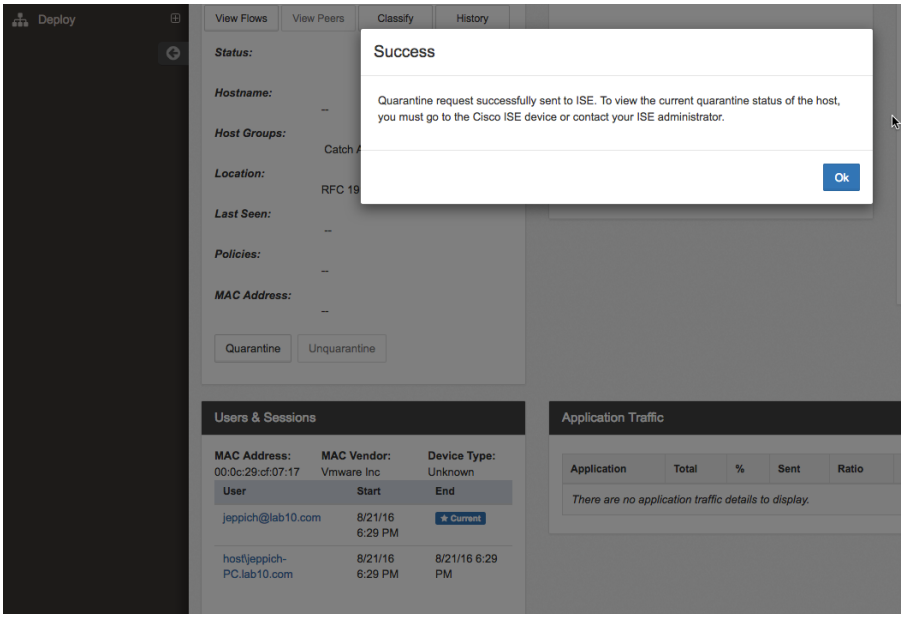
Step 5 On the host, import the ISE CA subordinate certificate into the cacerts

```
sudo keytool -keystore cacerts -importcert -alias myca1 -file
/Applications/sw682/CertificateServicesEndpointSubCA-ise21internalCA_.cer
Enter keystore password:  changeit
Owner: CN=Certificate Services Endpoint Sub CA - ise21internalCA
Issuer: CN=Certificate Services Node CA - ise21internalCA
Serial number: 69d92403adb24e1694aff7630d2f2c63
Valid from: Sun Jul 17 23:05:52 EDT 2016 until: Sun Jul 18 23:05:50 EDT 2021
Certificate fingerprints:
         MD5:  80:FF:5E:15:EF:34:52:84:20:C3:7C:1A:EF:66:FA:CD
         SHA1: B1:A6:43:69:0A:7A:39:20:DA:14:03:01:E7:C6:2C:B4:3A:1F:B1:E8
         SHA256:
D1:1C:3D:AA:1F:ED:DD:4D:11:33:77:BD:CA:E6:CA:E6:8A:CE:6E:CF:2E:B8:A4:12:7E:99:D9:E9:8E:FE:17:9F
         Signature algorithm name: SHA256withRSA
         Version: 3

Extensions:

#1: ObjectId: 2.5.29.35 Criticality=false
AuthorityKeyIdentifier [
KeyIdentifier [
0000: 41 21 62 59 CD 0A F0 78   B5 10 5E FF A2 74 54 45  A!bY...x..^..tTE
0010: 88 BD B5 1C                                        ....
]
[CN=Certificate Services Root CA - ise21internalCA]
SerialNumber: [    1a2d587d 629e4dbb 8caf4118 5762a9e2]
]

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

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

#4: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: BB 37 EA 0C E7 36 91 72   E3 9F 2A FA 4D 51 95 5A  .7...6.r..*.MQ.Z
0010: 7F EA 29 D1                                        ..).
]
]
```

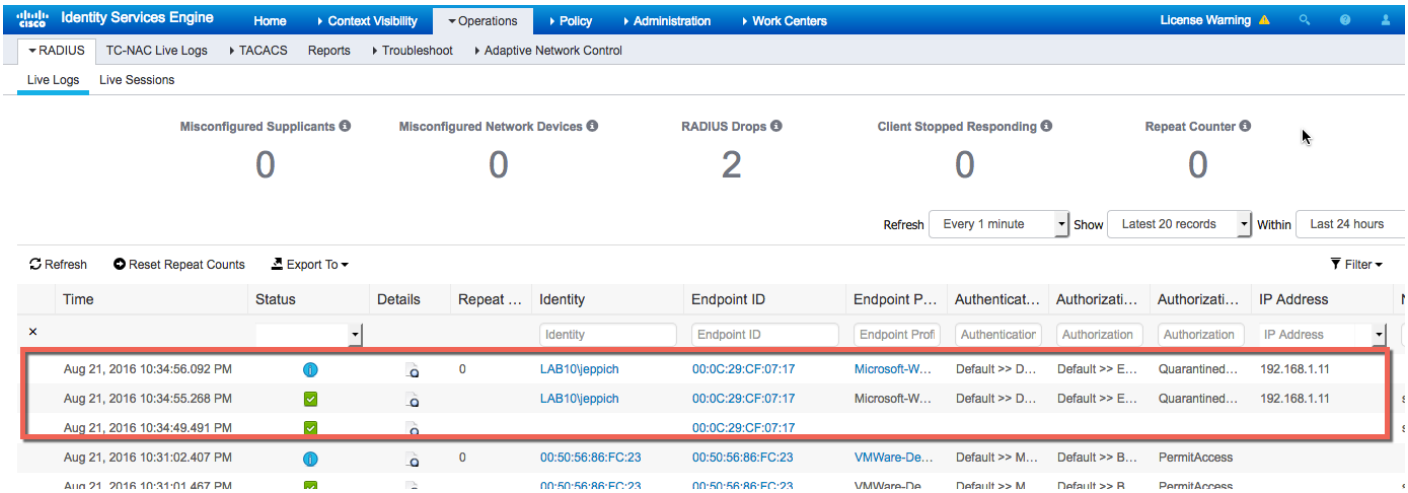
```
Trust this certificate? [no]:  yes
Certificate was added to keystore
```

Testing Stealthwatch Quarantine and Unquarantine Adaptive Network Control (ANC) Mitigation actions

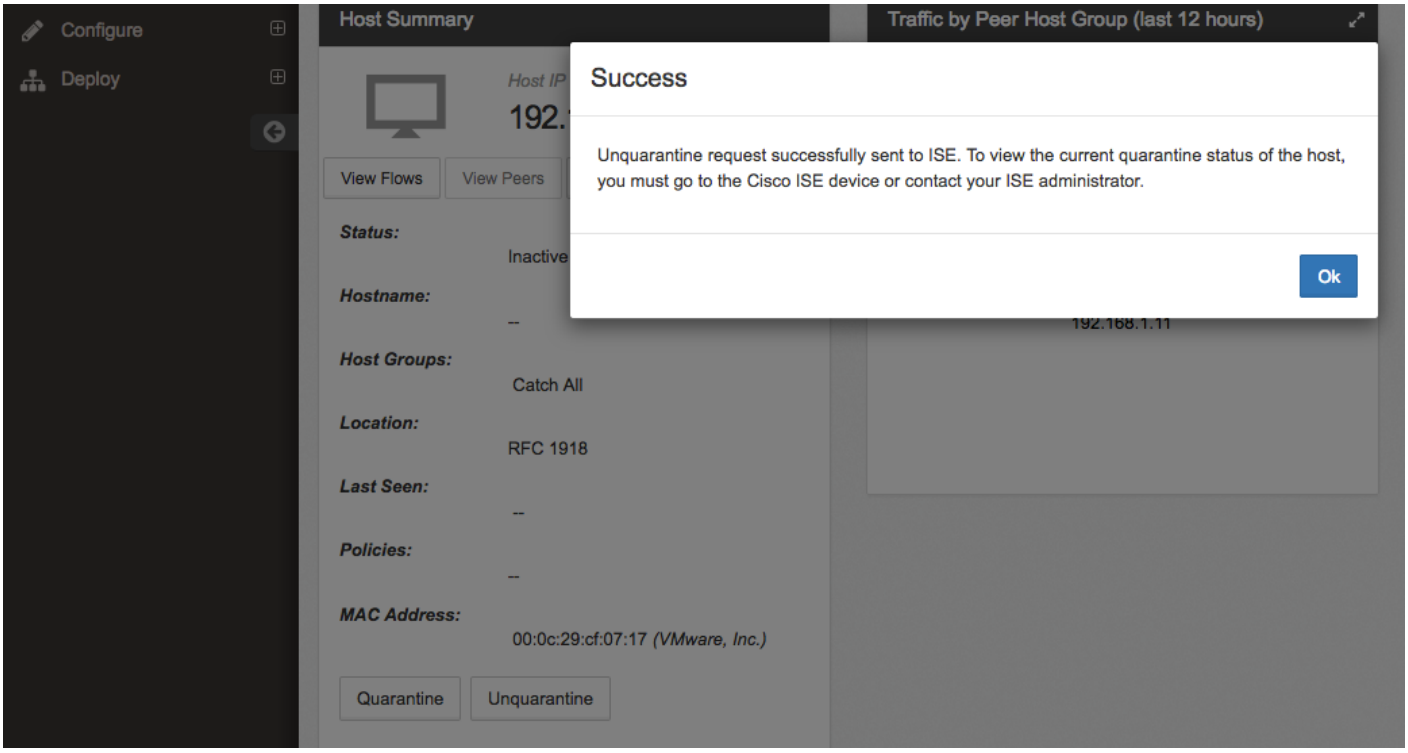
Step 1 Quarantine the endpoint
Select **Monitor->Users->jeppich@lab10.com->Quarantine the IP address of the endpoint**



Step 2 Select **OK**
Step 3 To see the quarantine results in ISE, select **Operations->RADIUS->Live Logs**

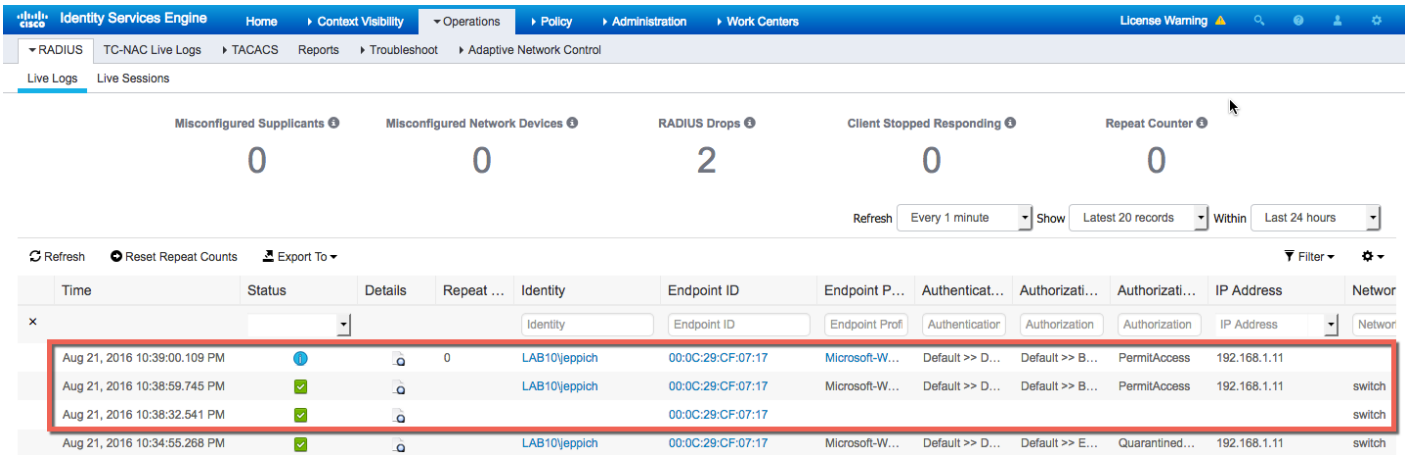


Step 4 Unquarantine the endpoint
Select **Monitor->Users->jeppich@lab10.com->UnQuarantine the IP address of the endpoint**



Step 5 Select **OK**

Step 6 To view in ISE, select **Operations->RADIUS-Live Logs**



Web Security Appliance (WSA)

The section steps through the procedure for generating and issuing the WSA pxGrid client from the ISE certificate provisioning portal. This also covers importing the ISE CA root certificate, ISEEndPointSUBCA, and WSA pxGrid client certificate public and private key-pair into the WSA truststore. A Web access policy denying users access to gambling sites is also provided to ensure everything is working correctly. It is assumed the reader is familiar with the WSA and ISE pxGrid integration, if not please refer to How To: Integrate Cisco WSA using ISE and TrustSec via pxGrid: https://communities.cisco.com/docs/DOC-68290

Generating WSA pxGrid client Certificate from ISE Certificate Provisioning Portal

Step 1 Create the certificate for the WSA client, select **Generate a single certificate (without a certificate signing request**

Step 2 Provide a Fully Qualified Domain Name (FQDN) for the Common Name (CN) (i.e. **wsa.lab10.com**)

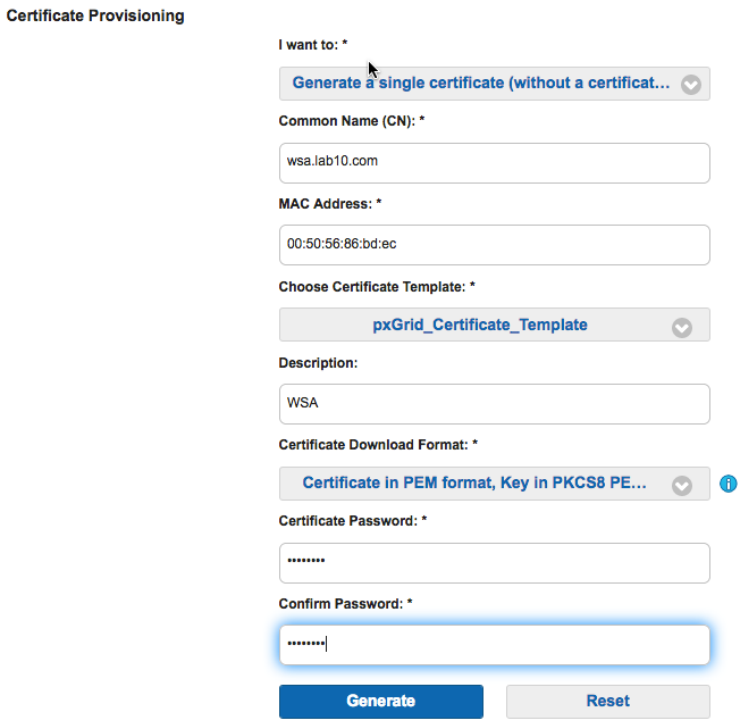
Step 3 Provide the MAC address of the WSA (i.e. **00:50:56:86:bd:ec**)

Step 4 Select the **pxGrid template** for the Certificate Template

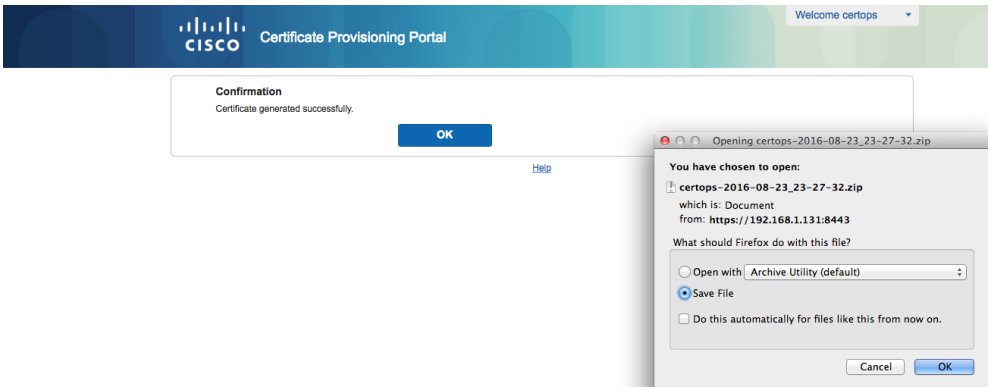
Step 5 Provide a **Description** (i.e. **WSA**)

Step 6 Select **Certificate in PEM format, Key in PKCS8 PEM format**

Step 7 Provide the Encrypted Password (i.e. **Cisco123**)



Step 8 Select **Generate**



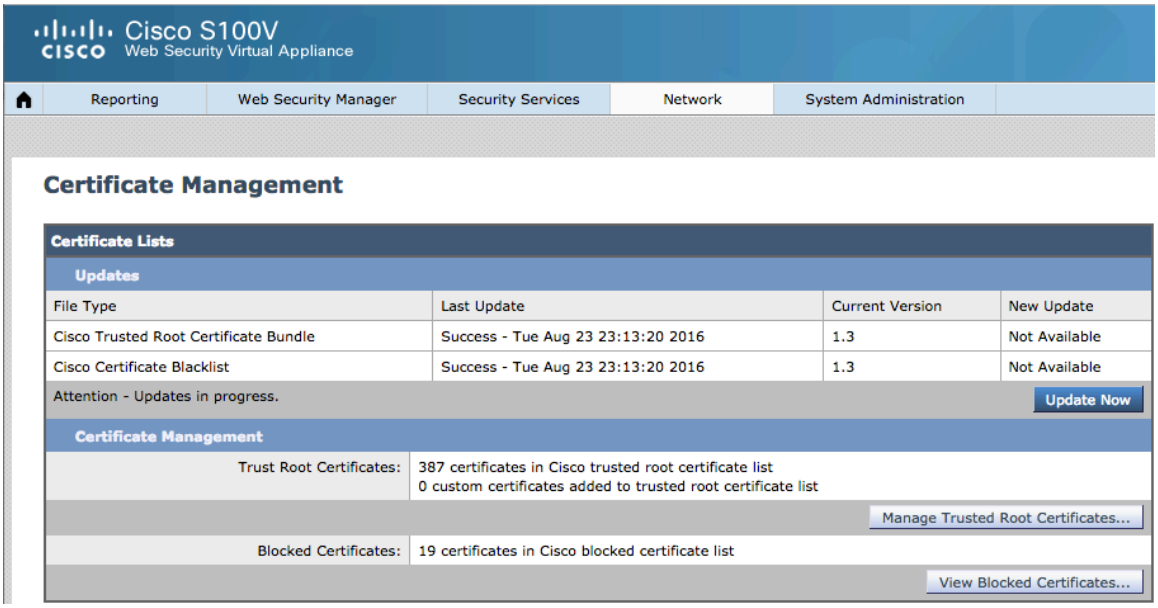
Step 9 Save the file locally.

Step 10 You should see the following files:

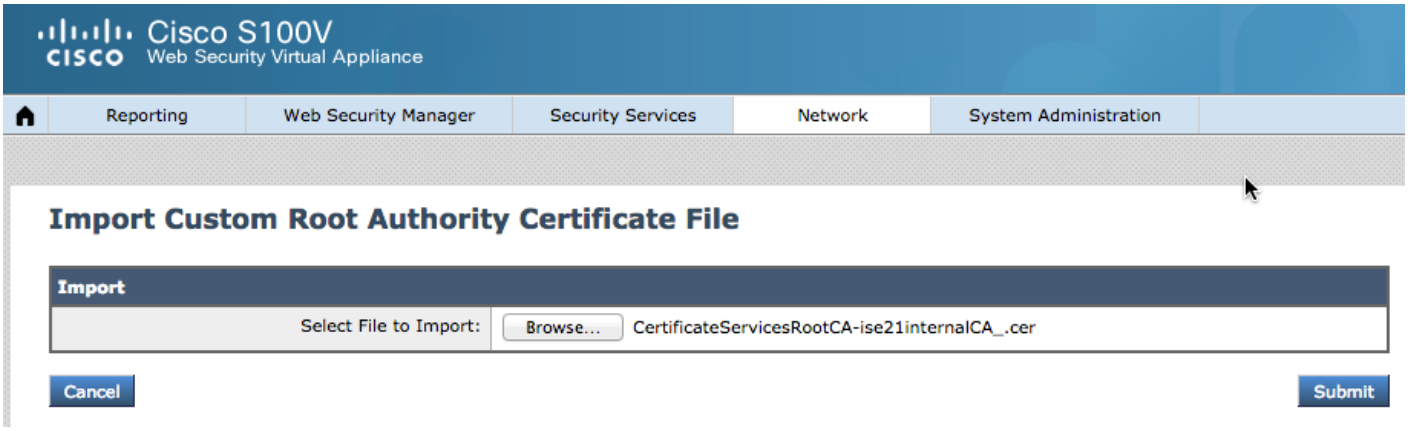
CertificateServicesEndpointSubCA-ise21internalCA_.cer	Aug 23, 2016 11:27 PM	2 KB	certificate
CertificateServicesNodeCA-ise21internalCA_.cer	Aug 23, 2016 11:27 PM	2 KB	certificate
CertificateServicesRootCA-ise21internalCA_.cer	Aug 23, 2016 11:27 PM	2 KB	certificate
wsa.lab10.com_00-50-56-86-bd-ec.cer	Aug 23, 2016 11:27 PM	2 KB	certificate
wsa.lab10.com_00-50-56-86-bd-ec.key	Aug 23, 2016 11:27 PM	2 KB	Keyno...ument

Installing ISE and pxGrid client certificates

Step 1 Select **Network->Certificate Management**
You should see the following:

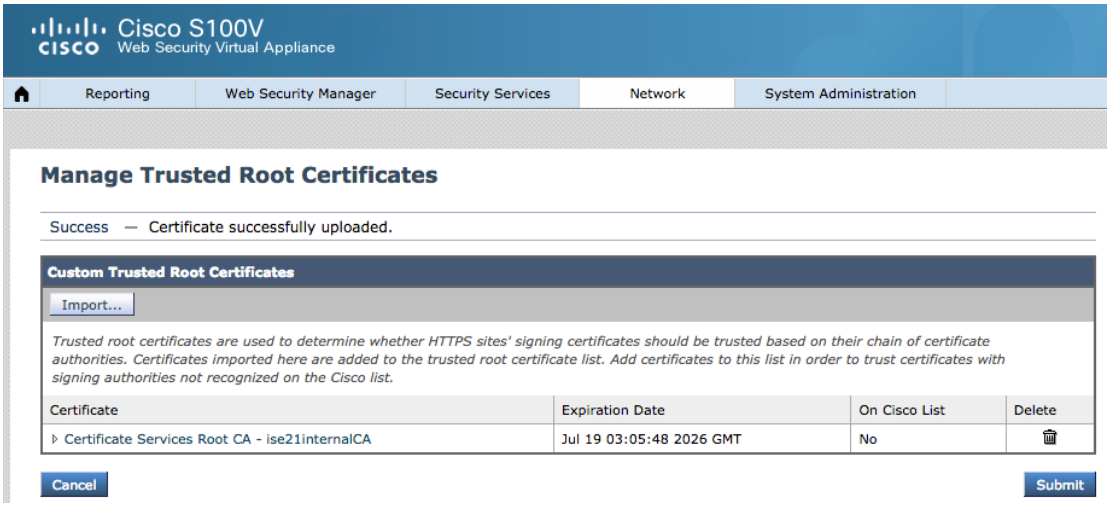


Step 2 Select **Manage Trusted Root Certificates->Import->CertificateServicesRootCA-ise21initernalCA_.cer**

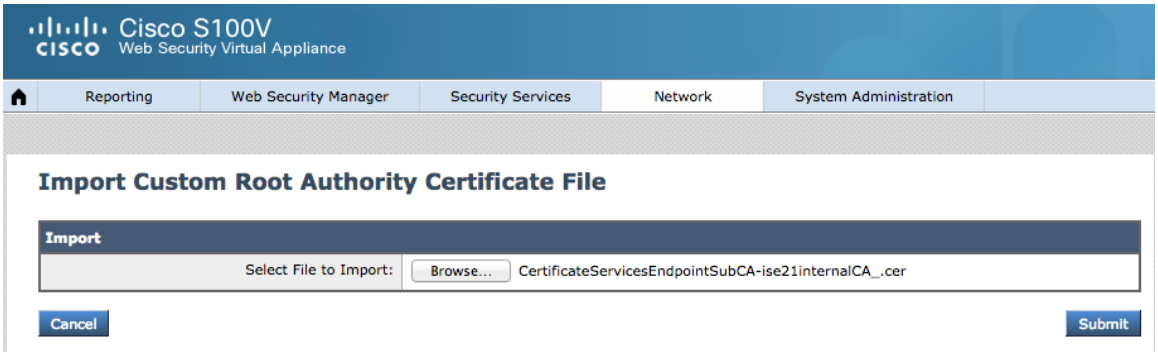


Step 3 Select **Submit**

Step 4 You should see the following:

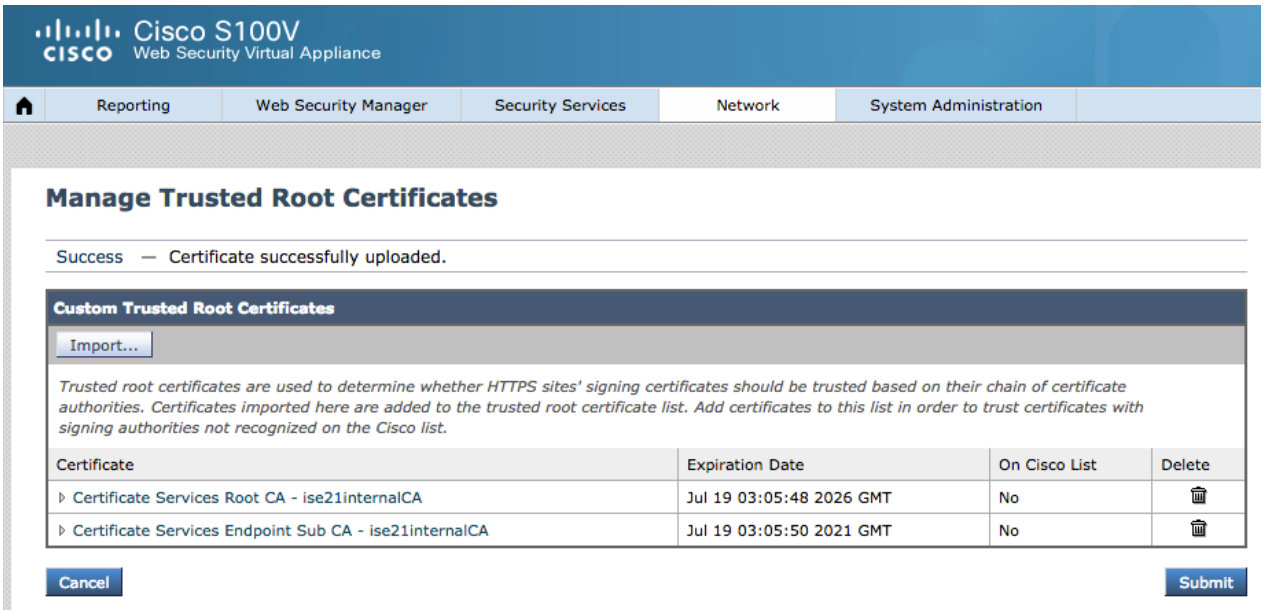


Step 5 Select->**Import->CertificateServicesEndpointSubCA-ise21internalCA_.cer**



Step 6 Select **Submit**

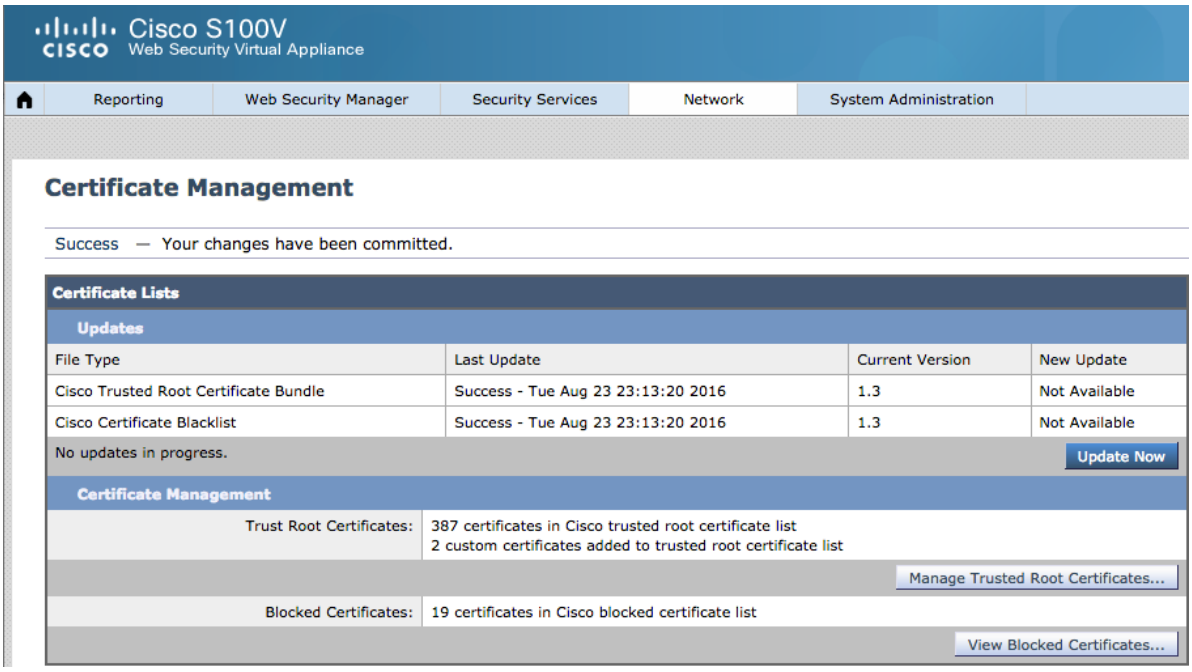
Step 7 You should see the following:



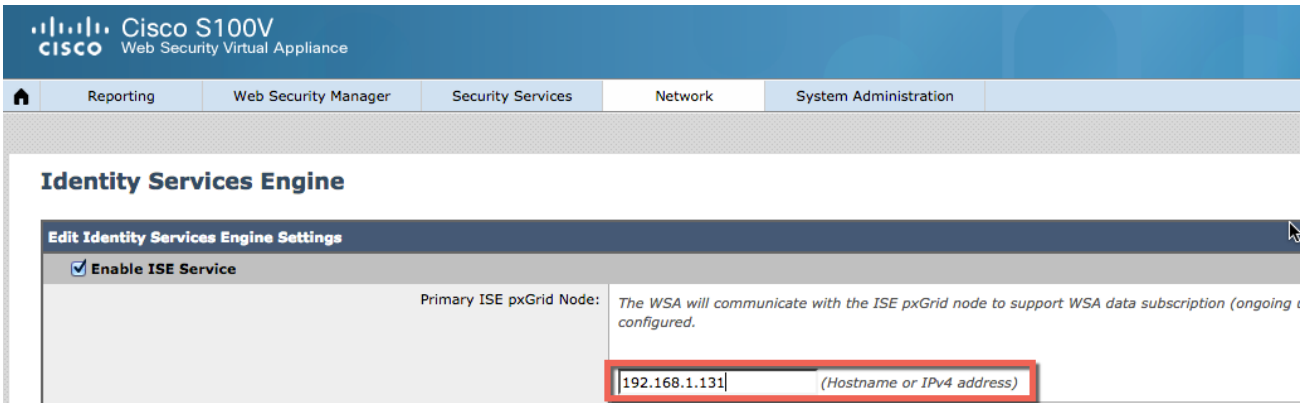
Step 8 Select **Submit**

Step 9 Select **Commit Changes->Commit Changes**

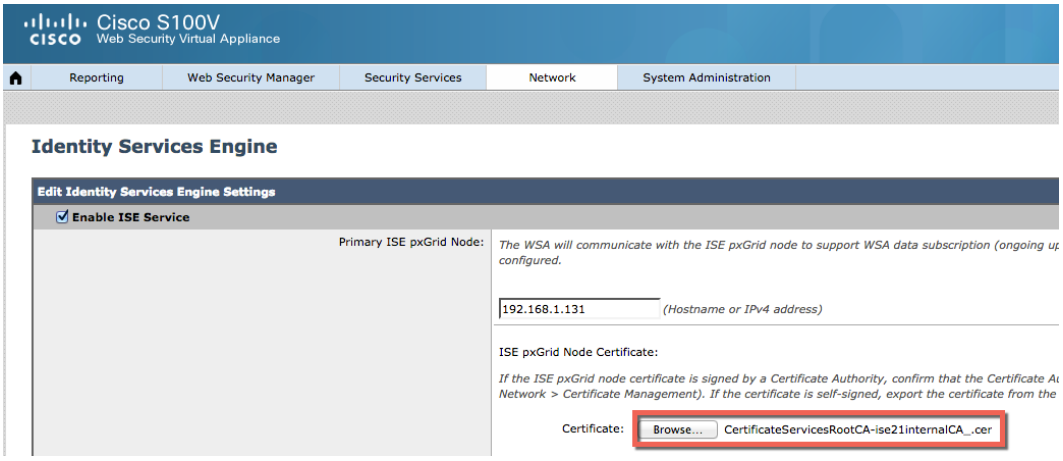
Step 10 You should see the following:



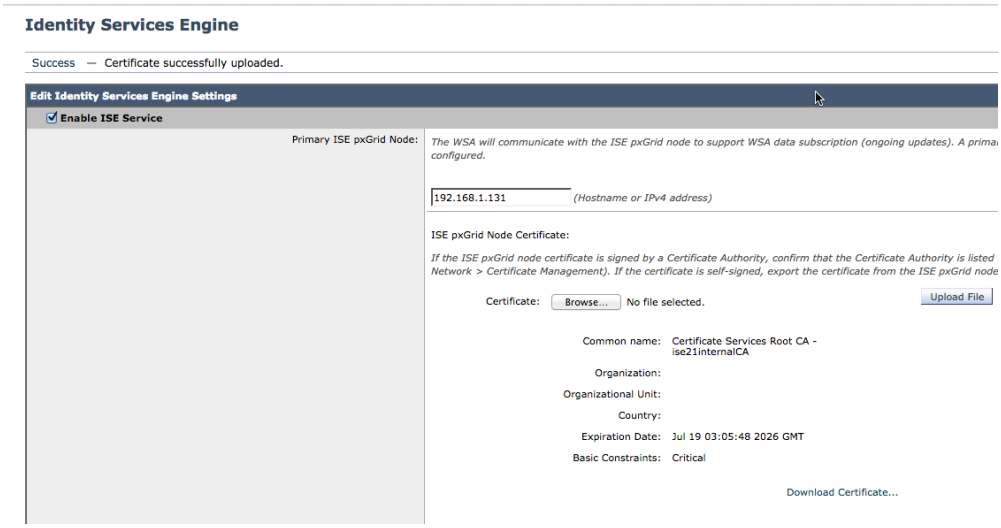
Step 11 Select **Network->Identification Services->Identity Services Engine->Enable ->Edit Settings enter the IP address of the primary pxGrid node**



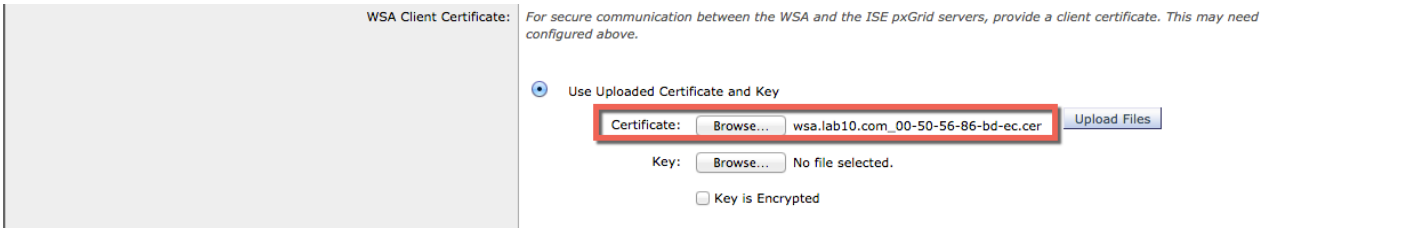
Step 12 Select **CertificateServicesRootCA-ise21internalCA_cer** for the ISE pxGrid node certificate



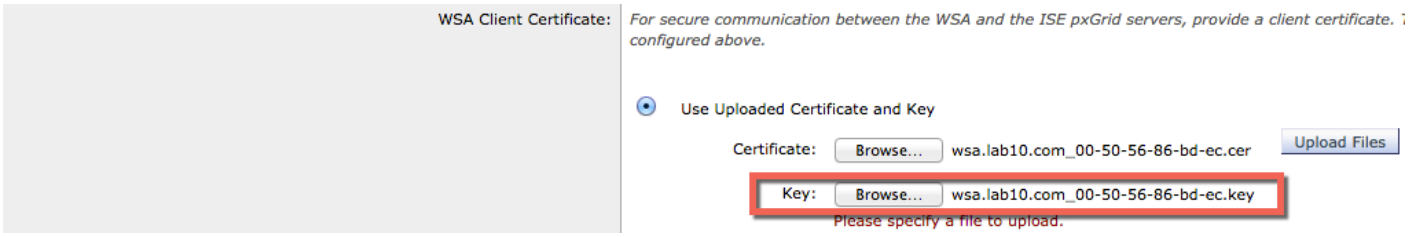
Step 13 Select **Upload File**
You should see the following:



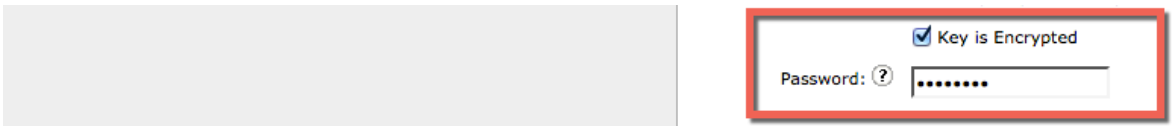
Step 14 Under **WSA Client Certificate->Use Uploaded Certificate and Key** ->**Certificate->browse WSA certificate**



Step 15 Select **Key->browse WSA private key**

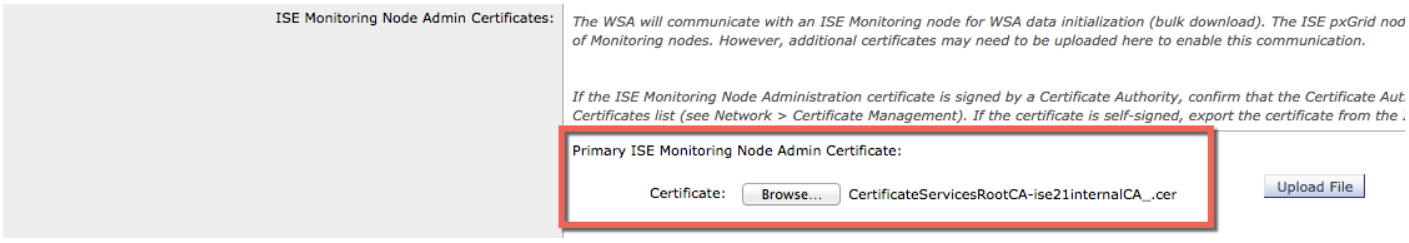


Step 16 Enable **Key is encrypted** and **enter the Password (i.e. Cisco123)**



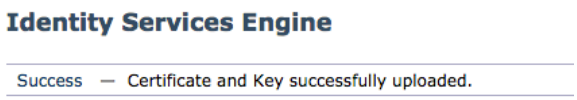
Step 17 Select **Upload Files**

Step 18 Under **ISE Monitoring Node Admin Certificates->Primary ISE Monitoring Node Admin Certificate->Certificate->browse CertificateServicesRootCA-ise21internalCA_.cer**

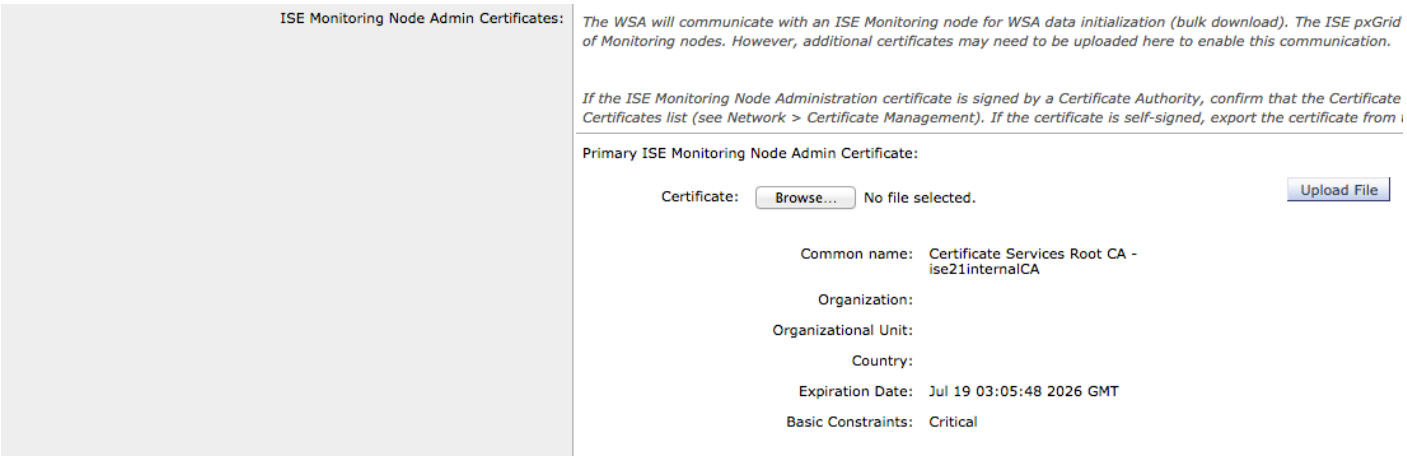


Step 19 Select **Upload Files**

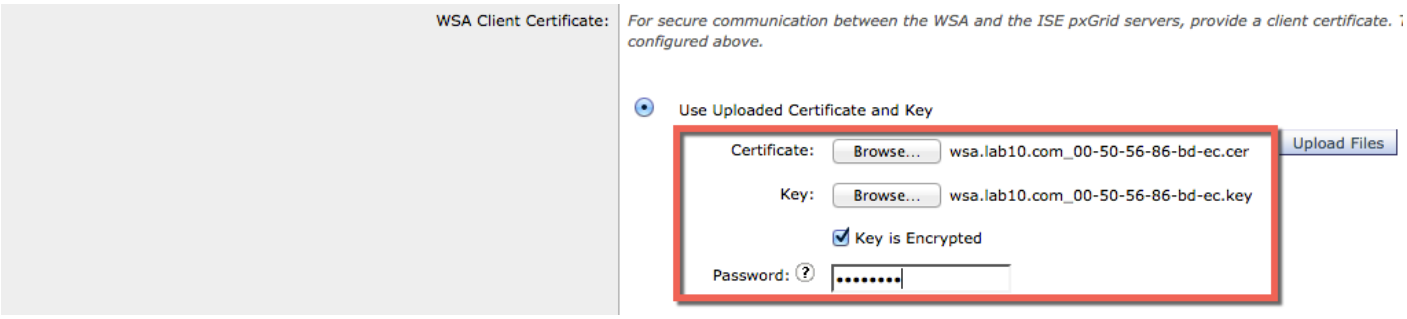
Step 20 You should see:



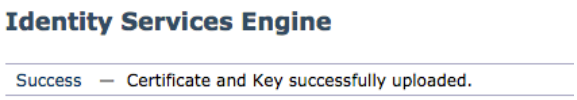
Step 21 Verify that the Certificate Services Root-CA- ise21internalCA has been successfully uploaded.



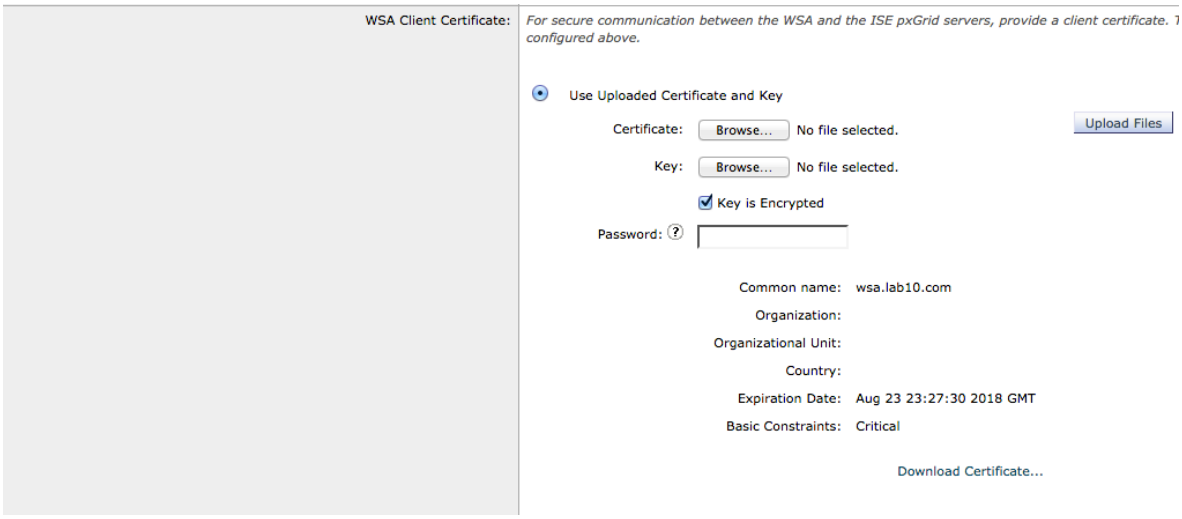
Step 22 Under **WSA Client certificate->Use Uploaded Certificate and Key->Certificate->browse->wsa..cer**
Step 23 Under **WSA Client certificate->Use Uploaded Certificate and Key->Certificate->browse->wsa..key**
Step 24 **Enable Key is Encrypted**, and type in the password that was generated from creating the WSA certificate in ISE.



Step 25 Select **Upload File**
Step 26 You should see:



Step 27 Verify that the WSA client certificate has been uploaded



Testing Configuration between the WSA and the ISE pxGrid node

Step 1 Select **Start test,** you should see:

```
Checking DNS resolution of ISE pxGrid Node hostname(s) ...
Success: Resolved '192.168.1.131' address: 192.168.1.131

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

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

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

Checking connection to ISE pxGrid Node(s) ...
Success: Connection to ISE pxGrid Node was successful.
Retrieved 17 SGTs from: 192.168.1.131

Checking connection to ISE Monitorting Node (REST server(s)) ...
Success: Connection to ISE Monitorting Node was successful.
REST Host contacted: ise21internalCA.lab10.com

Test completed successfully.
```

Step 2 Select **Submit**

Step 3 You should see the following:

Identity Services Engine Settings

Primary ISE pxGrid Node:	192.168.1.131 ISE pxGrid Node Certificate: Common name: Certificate Services Root CA - ise21internalCA Organization: Organizational Unit: Country: Expiration Date: Jul 19 03:05:48 2026 GMT Basic Constraints: Critical
Secondary ISE pxGrid Node (optional):	Node is not configured
ISE Monitoring Node Admin Certificates:	Primary ISE Monitoring Node Admin Certificate: Common name: Certificate Services Node CA - ise21internalCA Organization: Organizational Unit: Country: Expiration Date: Jul 19 03:05:50 2021 GMT Basic Constraints: Critical Secondary ISE Monitoring Node Admin Certificate is not configured
WSA Client Certificate:	Using Uploaded Certificate: Common name: wsa.lab10.com Organization: Organizational Unit: Country: Expiration Date: Aug 23 23:27:30 2018 GMT Basic Constraints: Critical

Edit Settings...

Step 4 Select **Commit Changes->Commit Changes**

Step 5 You should see:

Cisco S100V
Web Security Virtual Appliance

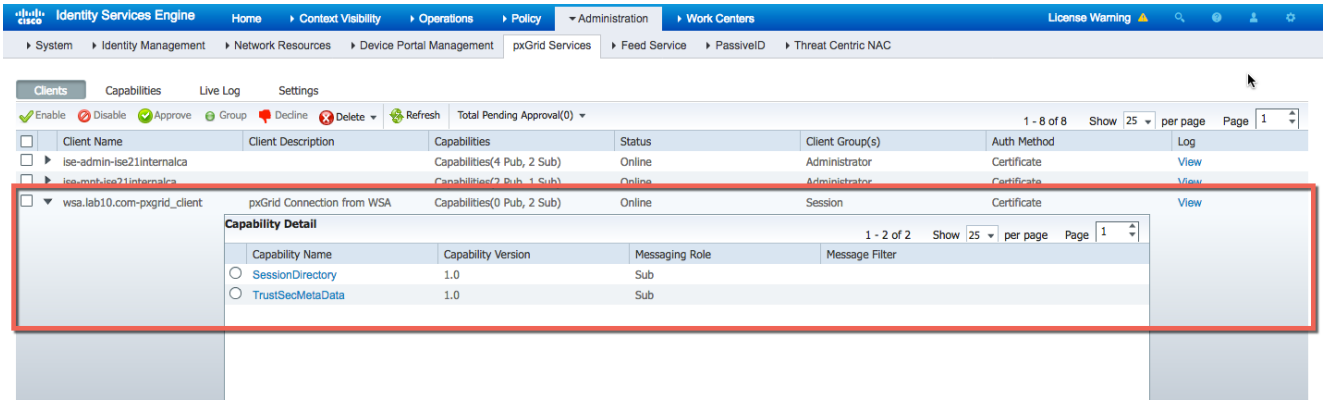
Reporting | Web Security Manager | Security Services | Network | System Administration

Identity Services Engine

Success — Your changes have been committed.

Step 6 Ensure that the WSA has registered as a pxGrid client and subscribed to the SessionDirectory and TrustSecMetaData topics

Select **Administration->pxGrid services**

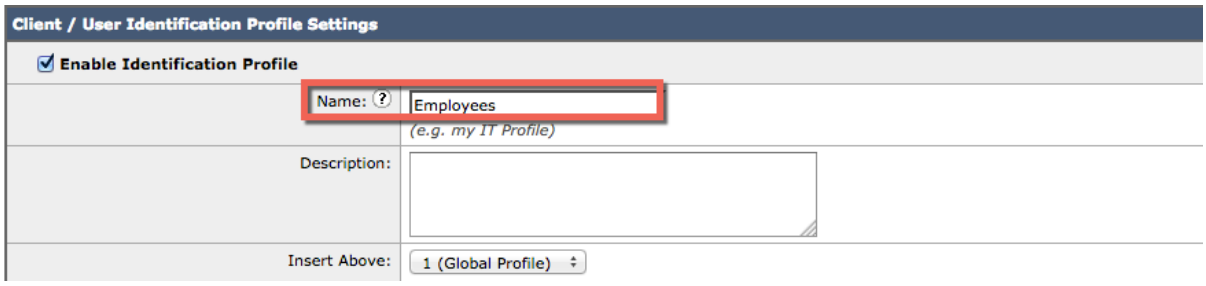


USE CASE: Denying Employees with a SGT Tag Access to Gambling Sites

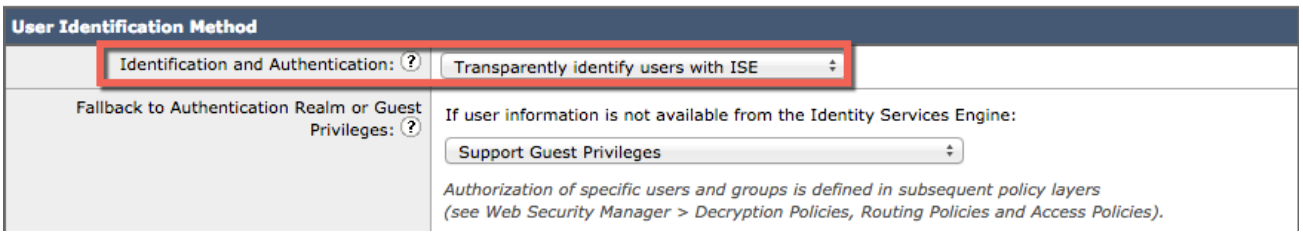
Creating an Identification Profile

An Identification profile for Employees is created

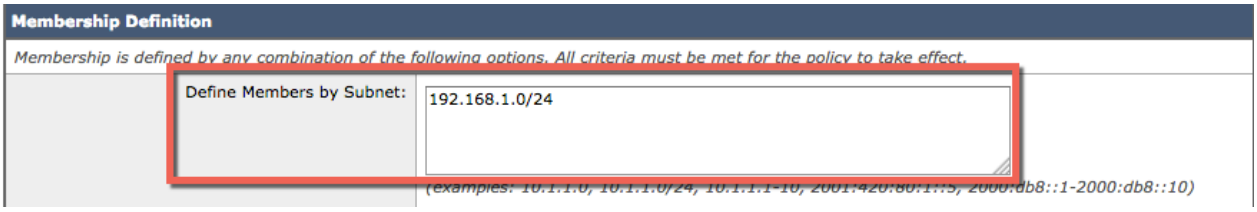
Step 1 Select **Web Security Manager->Authentication->Identification Profiles->Add Identification Profile->Name Employees**



Step 2 Under **User Identification Method->Identification and Authentication->Transparently identify users with ISE**



Step 3 Under **Membership Definition->Define Members by Subnet->enter range** (i.e. 192.168.1.0/24)

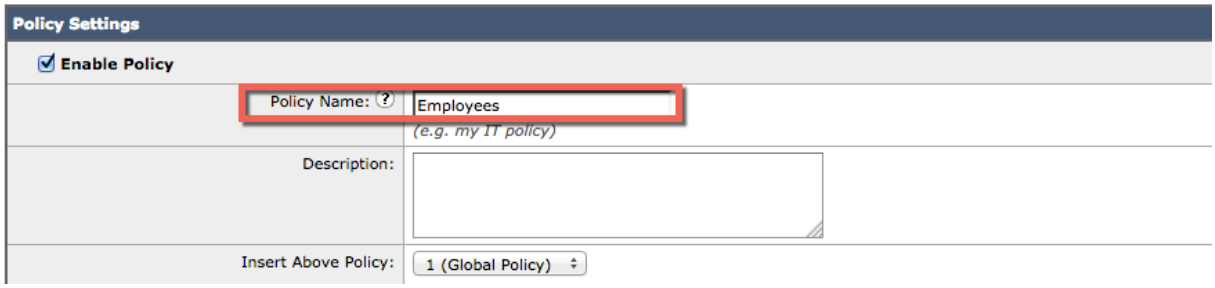


Step 4 Select **Submit**

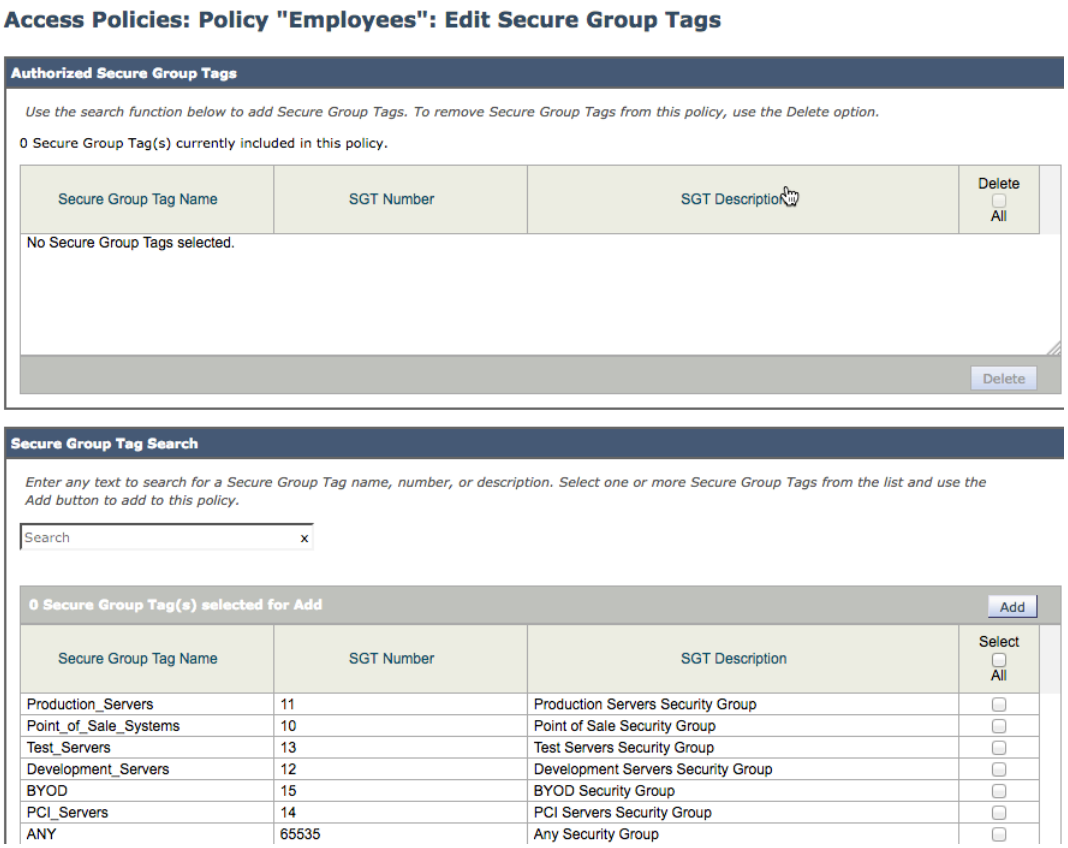
Creating Web Access Security Policy for Employees Denying Access to Gambling Sites

A web access security policy for Employee SGT tagged users is created and denied access to Gambling Sites

Step 1 Select **Web Security Manager->Web Policies->Access Policies->Policy Name->Employees**



Step 2 Under **Policy Member Definition->Identification Profiles and Users->Select one or more Identification Profiles->Identification Profile->Employees->Authorized Users and Groups->Selected Groups and Users->No Tags Entered**

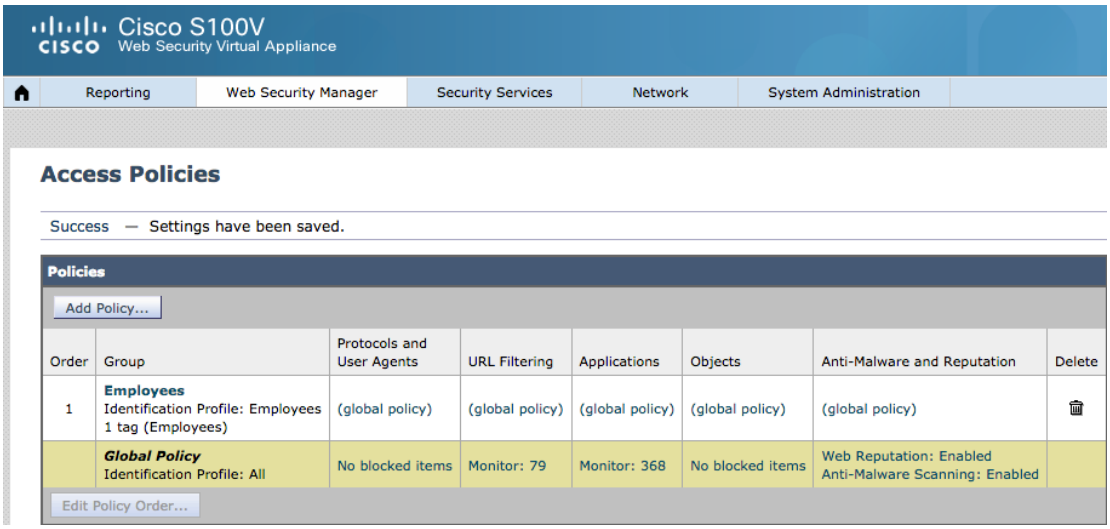


Step 3 Select **Employees** under Secure Group Tag Search and **Add**

Step 4 You should see **Employees** SGT appear under **Authorized Secure Group Tags**

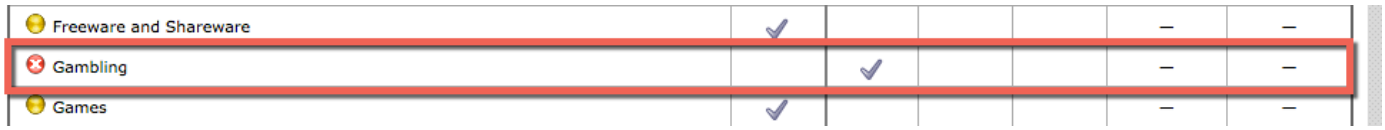
Step 5 Select **Done->Submit**

Step 6 You should see the following:



Step 7 Select **Commit Changes->Commit Changes**

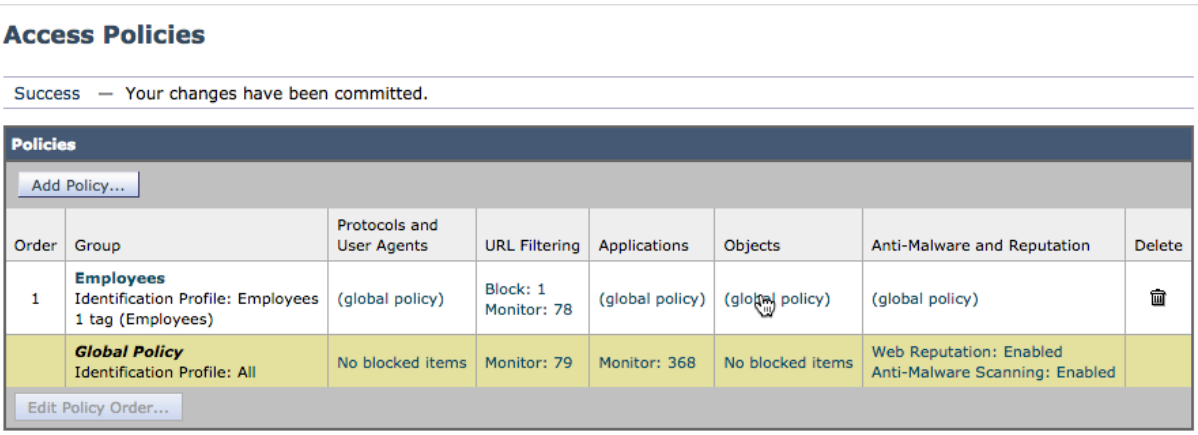
Step 8 Select **Web Security Manager->Web Policies->Access Policies->Employees->URL Filtering->Block Gambling**



Step 9 Select **Submit**

Step 10 Select **Commit Changes->Commit Changes**

Step 11 You should see the following:

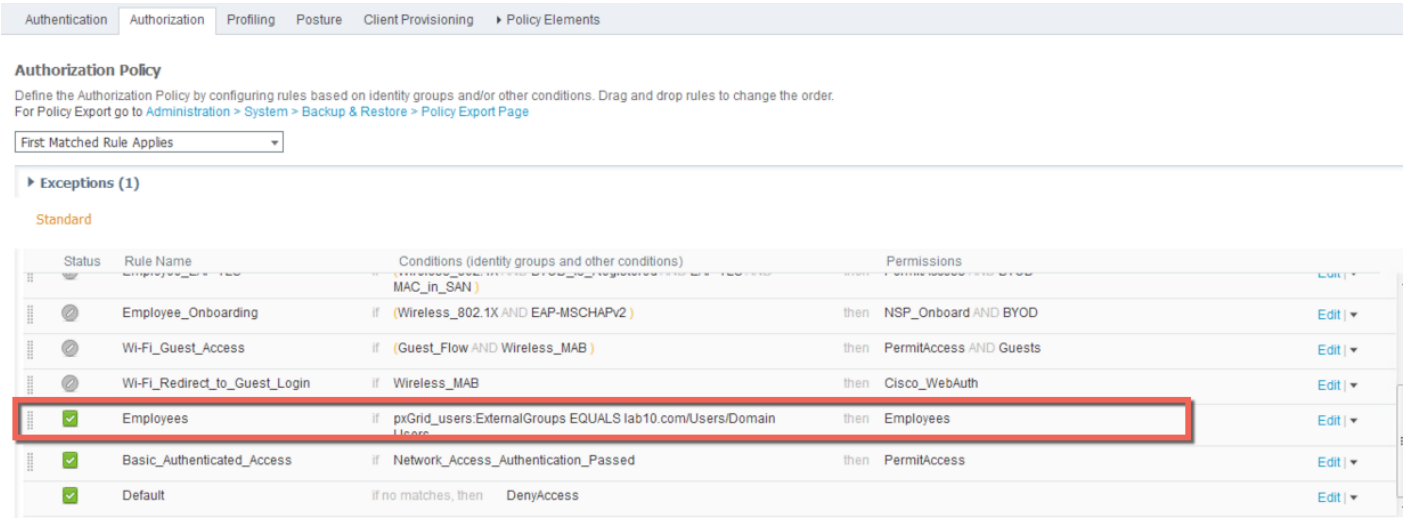


End-User Testing

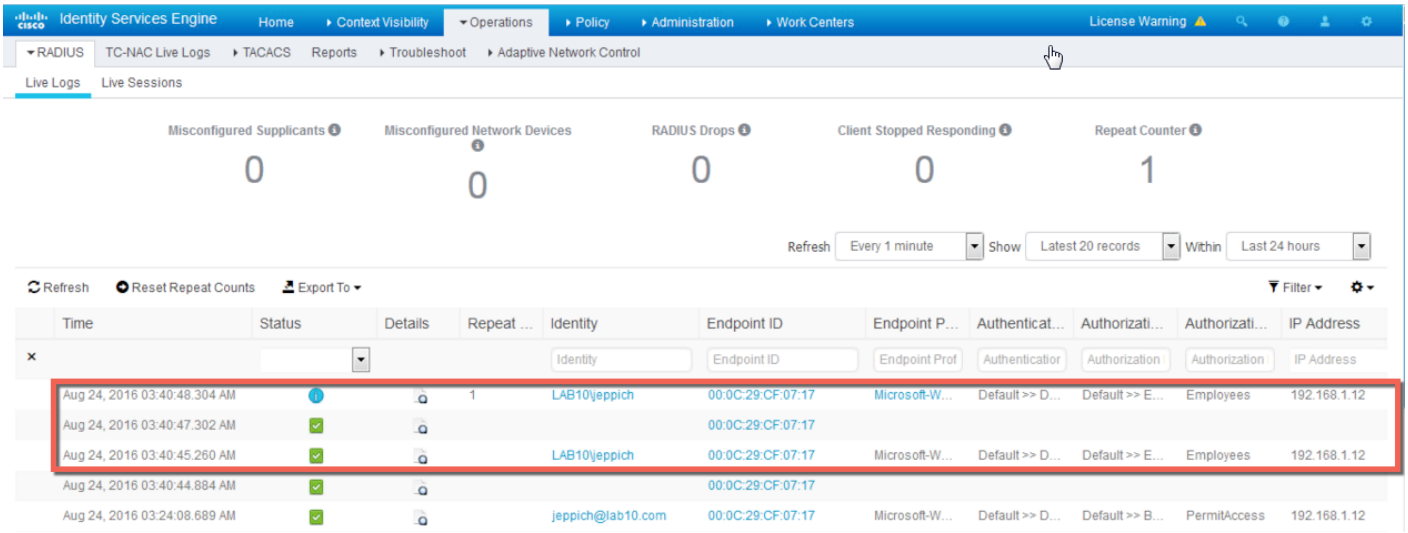
An end-user logs in and gets assigned an SGT of employee and is denied access to Gambling sites. It is assumed that the ISE authorization policies have been created.

Step 1 End-User successfully logs in

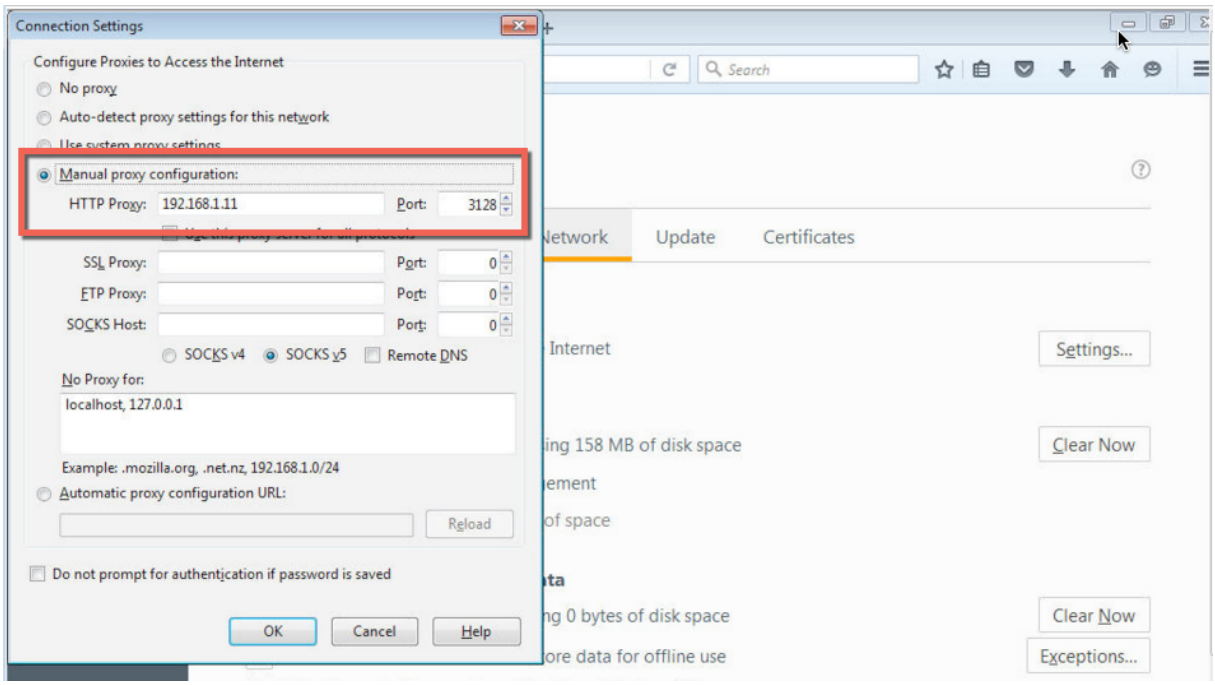
Step 2 Select **Policy->Authorization**



Step 3 Select **Operations->RADIUS->Live Logs**

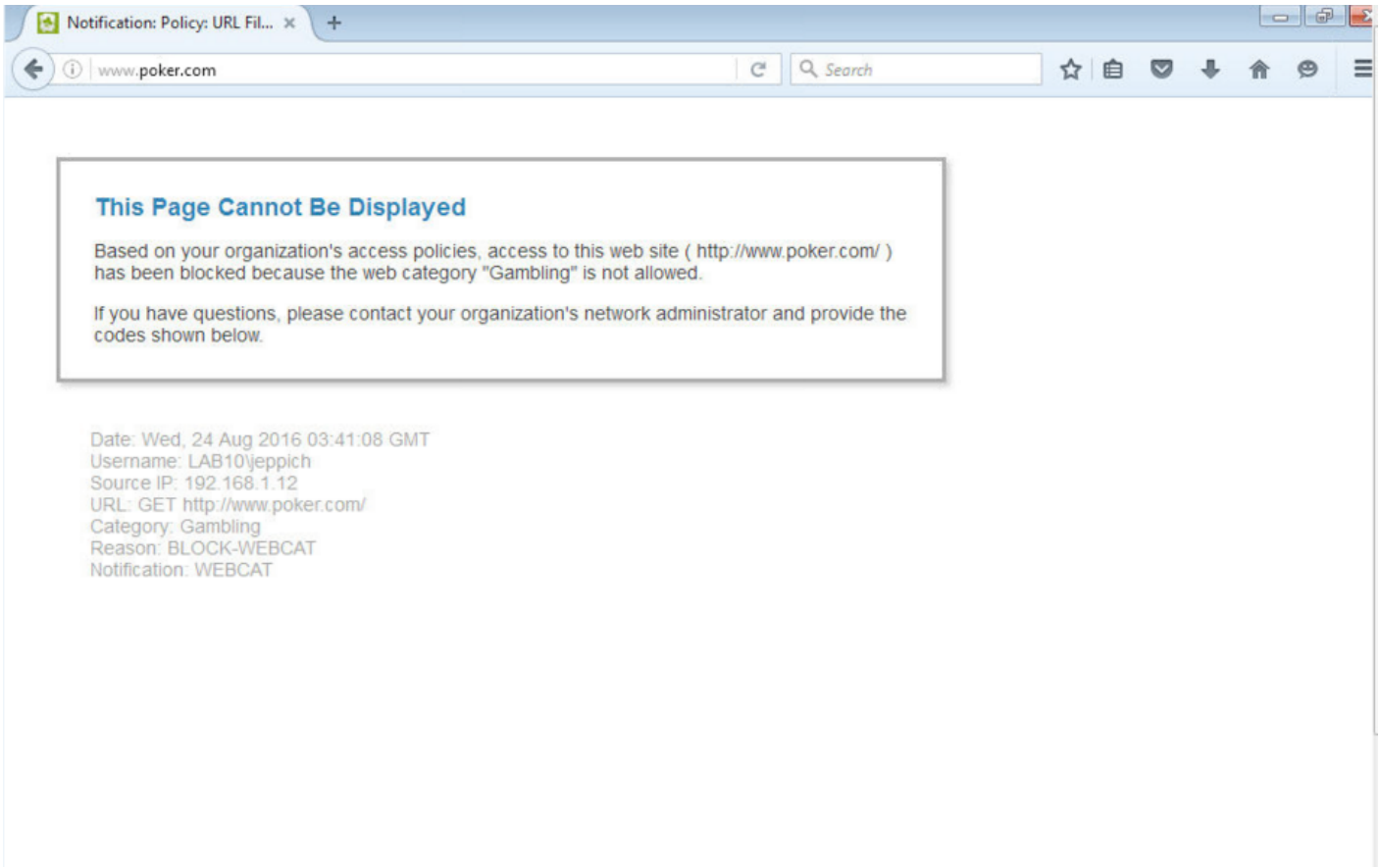


Step 4 Set the proxy settings
Open **Browser ->Firefox->options->Advanced->Network->Connection->Settings**



Step 5 Select **OK**

Step 6 End-User is denied access to wwww.poker.com


Notification: Policy: URL Fil...
www.poker.com
Search
This Page Cannot Be Displayed
Based on your organization's access policies, access to this web site (http://www.poker.com/) has been blocked because the web category "Gambling" is not allowed.
If you have questions, please contact your organization's network administrator and provide the codes shown below.
Date: Wed, 24 Aug 2016 03:41:08 GMT
Username: LAB10\jeppich
Source IP: 192.168.1.12
URL: GET http://www.poker.com/
Category: Gambling
Reason: BLOCK-WEBCAT
Notification: WEBCAT

References

How To: Rapid Threat Containment (RTC) with Cisco Firesight and ISE guide: https://communities.cisco.com/docs/DOC-68293

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

How To: Deploy Lancope Stealthwatch with pxGrid https://communities.cisco.com/docs/DOC-68288

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

How To: Integrate Firepower Management Center 6.0 with ISE and TrustSec through pxGrid: https://communities.cisco.com/docs/DOC-68292