Deploying Cisco Stealthwatch 7.0 with Cisco ISE 2.4 using pxGrid

Author: John Eppich

Table of Contents

About this Document

This document is for Cisco Engineers, partners and customers deploying Cisco Stealthwatch 7.0 with Cisco Identity Services Engine (ISE) 2.4 using Cisco Platform Exchange Grid (pxGrid 1.0). Cisco Stealthwatch uses pxGrid 1.0 which is XMPP-based for integration with pxGrid.

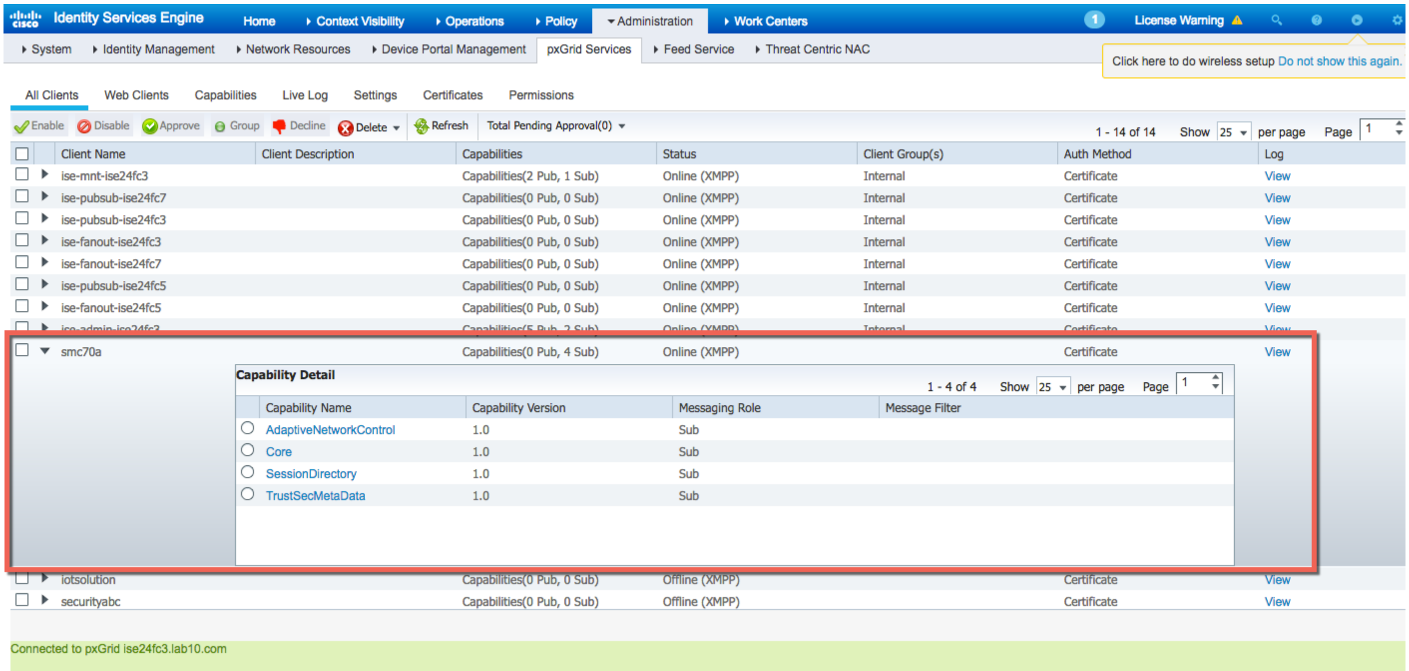
The minimal supported version of ISE is 2.0. Please note that ISE 2.0 does not contain the ISE internal CA for signing pxGrid certificates. If deploying ISE pxGrid 2.0, please refer to: https://community.cisco.com/t5/security-documents/ise-security-ecosystem-integration-guides/ta-p/3621164#toc-hId--292074806 , for Deploying pxGrid Using Self-Signed Certificates Updates to Cisco ISE 2.0/2.1/2.2, Deploying pxGrid Using an External CA with Updates to ISE 2.0/2.1/22, and How to Configure ISE in Productional Environments.

This document covers the following:

- Using an External CA Server and ISE internal CA for Stealthwatch and ISE pxGrid Integration
- Creating ISE Adaptive Network Control (ANC) 2.0 mitigation action policies and illustrate how Stealtwatch uses these policies for quarantining the endpoint. These ANC policies do not rely on EPS:Session:Qurantine for ISE Authorization policies, instead they use the Session:ANCPolicy:desired ANC policy.
- Illustrating Cisco Segmentation using Security Group Tags (SGT) to demonstrate the Subject TrustSec Name, Subject TrustSec ID, Peer TrustSec Name and Peer TrustSec ID in viewing the network flows. This includes also includes configuring ISE, Cisco Catalyst Switch 3750-X, and ASA 5506-X for Cisco TrustSec operation.
- Creating Stealthwatch custom event violation policy to view the flow from the Subject TrustSec ID to the Peer TrustSec ID.

Technical Details

Cisco Stealthwatch 7.0 uses Cisco Platform Exchange Grid (pxGrid 1.0) for integration with Cisco Identity Services (ISE) Engine. pxGrid 1.0 is XMPP-based, and Cisco Stealthwatch registers as a pxGrid client and subscribes to the Session Directory, AdaptiveNetworkControl, and TrustSecMetadata Topics.



□	Client Name	Client Description	Capabilities	Status	Client Group(s)	Auth Method	Log
□	ise-mnt-ise24fc3		Capabilities(2 Pub, 1 Sub)	Online (XMPP)	Internal	Certificate	View
□	ise-pubsub-ise24fc7		Capabilities(0 Pub, 0 Sub)	Online (XMPP)	Internal	Certificate	View
□	ise-pubsub-ise24fc3		Capabilities(0 Pub, 0 Sub)	Online (XMPP)	Internal	Certificate	View
□	ise-fanout-ise24fc3		Capabilities(0 Pub, 0 Sub)	Online (XMPP)	Internal	Certificate	View
□	ise-fanout-ise24fc7		Capabilities(0 Pub, 0 Sub)	Online (XMPP)	Internal	Certificate	View
□	ise-pubsub-ise24fc5		Capabilities(0 Pub, 0 Sub)	Online (XMPP)	Internal	Certificate	View
□	ise-fanout-ise24fc5		Capabilities(0 Pub, 0 Sub)	Online (XMPP)	Internal	Certificate	View
□	ise-admin-ise24fc3		Capabilities(5 Pub, 2 Sub)	Online (XMPP)	Internal	Certificate	View
□	smc70a		Capabilities(0 Pub, 4 Sub)	Online (XMPP)		Certificate	View
□	iotsolution		Capabilities(0 Pub, 0 Sub)	Offline (XMPP)		Certificate	View
□	securityabc		Capabilities(0 Pub, 0 Sub)	Offline (XMPP)		Certificate	View

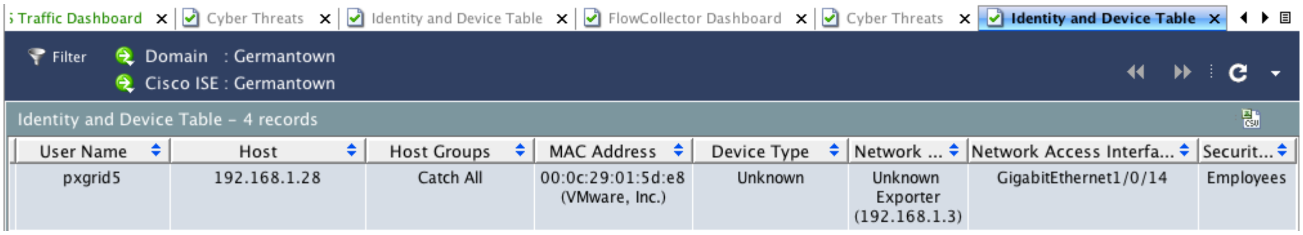
Capability Detail

1 - 4 of 4 Show 25 per page Page 1

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

Connected to pxGrid ise24fc3.lab10.com

The SessionDirectory Topic provides detailed information about the authenticated session, Stealthwatch obtains the User Name, MAC address, Device Type, and Security Group Tag attributes.

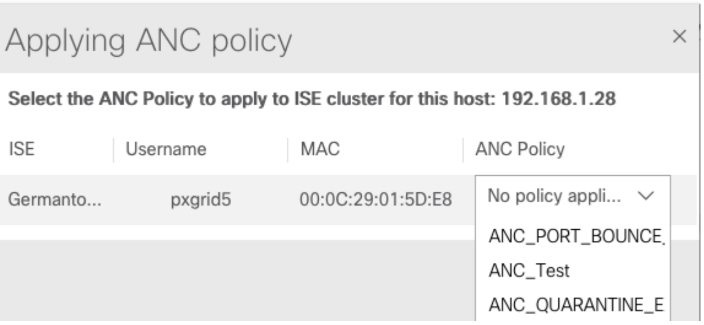


Domain : Germantown
Cisco ISE : Germantown

Identity and Device Table – 4 records

User Name	Host	Host Groups	MAC Address	Device Type	Network ...	Network Access Interfa...	Securit...
pxgrid5	192.168.1.28	Catch All	00:0c:29:01:5d:e8 (VMware, Inc.)	Unknown	Unknown Exporter (192.168.1.3)	GigabitEthernet1/0/14	Employees

When Cisco Stealthwatch subscribes to the AdaptiveNetworkControl, it is able to retrieve the ISE Adaptive Network Control (ANC) 2.0 policies from ISE and perform mitigation actions on the endpoint automatically from the GUI.



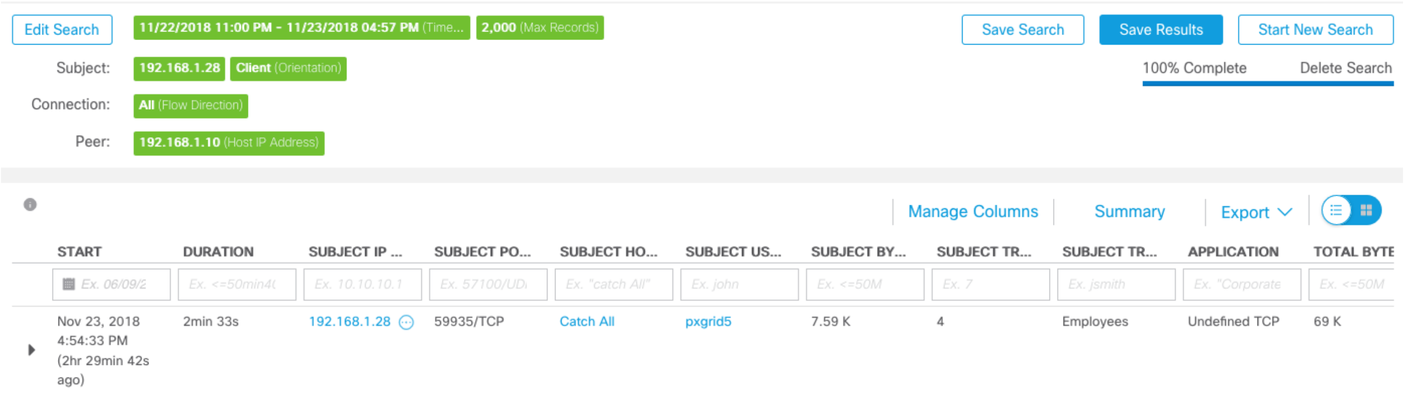
Applying ANC policy

Select the ANC Policy to apply to ISE cluster for this host: 192.168.1.28

ISE	Username	MAC	ANC Policy
Germanto...	pxgrid5	00:0C:29:01:5D:E8	No policy appli...

The TrustSecMetada topic provides Security Group Tag (SGT) id, name, description and tag details. Additionally, source and peer sequences are obtained as the SXP connection information is published.

The below example is a Stealthwatch network flow between the Subject TrustSec name and the Subject Peer name Production Servers.



11/22/2018 11:00 PM - 11/23/2018 04:57 PM (Time... 2,000 (Max Records)

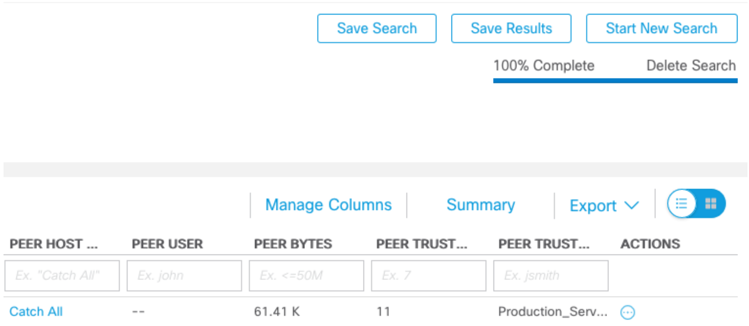
Subject: 192.168.1.28 Client (Orientation)

Connection: All (Flow Direction)

Peer: 192.168.1.10 (Host IP Address)

100% Complete

START	DURATION	SUBJECT IP ...	SUBJECT PO...	SUBJECT HO...	SUBJECT US...	SUBJECT BY...	SUBJECT TR...	SUBJECT TR...	APPLICATION	TOTAL BYTE
Ex. 06/09/2	Ex. <=50min4(	Ex. 10.10.10.1	Ex. 57100/UD	Ex. "catch All"	Ex. john	Ex. <=50M	Ex. 7	Ex. jsmith	Ex. "Corporate	Ex. <=50M
Nov 23, 2018 4:54:33 PM (2hr 29min 42s ago)	2min 33s	192.168.1.28	59935/TCP	Catch All	pxgrid5	7.59 K	4	Employees	Undefined TCP	69 K



100% Complete

PEER HOST ...	PEER USER	PEER BYTES	PEER TRUST...	PEER TRUST...	ACTIONS
Ex. "Catch All"	Ex. john	Ex. <=50M	Ex. 7	Ex. jsmith	
Catch All	--	61.41 K	11	Production_Serv...	

Generating Certificates

In this document, we will create certificates for Stealthwatch using an external CA server such as Microsoft and also using the ISE Internal CA. Please note that starting in ISE 2.2 and above the pxGrid certificate is signed by the ISE internal CA.

When using an external CA sever, to create certificates, it is assumed that the ISE pxGrid node is already configured for the external CA operation. If this is not the case, please see: https://community.cisco.com/t5/security-documents/deploying-certificates-with-cisco-pxgrid-using-an-external/ta-p/3639677

The operation is as follows:

- Disabling the ISE for pxGrid operation, then generating a certificate signing request, and getting this signed by the external CA server using a customized certificate template having an EKU of both client and server authentication.

- The external CA root certificate will be imported into the ISE trusted certificate store, and the ISE identity certificate will be bound to the ISE Certificate Signing Request (CSR). You can then enable the ISE pxGrid node for ISE operation.

If this is an ISE productional ISE deployment, please see: https://community.cisco.com/t5/security-documents/how-to-configure-pxgrid-in-ise-production-environments/ta-p/3646330

When using the ISE internal CA to create certificates, using the ISE internal CA to generate certificates for the Stealthwatch, use the RSA key length value of 2048 bits for generating the Stealthwatch CSR request. Also use the PKCS12 format, when generating the certificate within ISE.

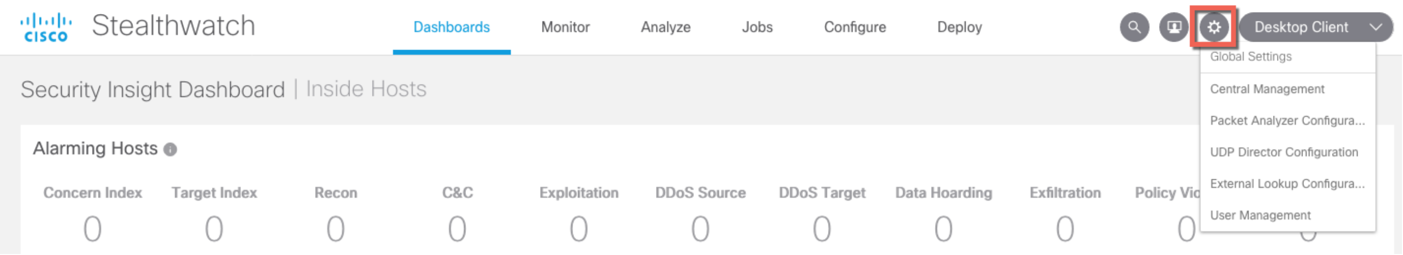
Using an External CA Server

In this example, a Microsoft Enterprise 2008 R2 Enterprise server was used as the external CA Server.

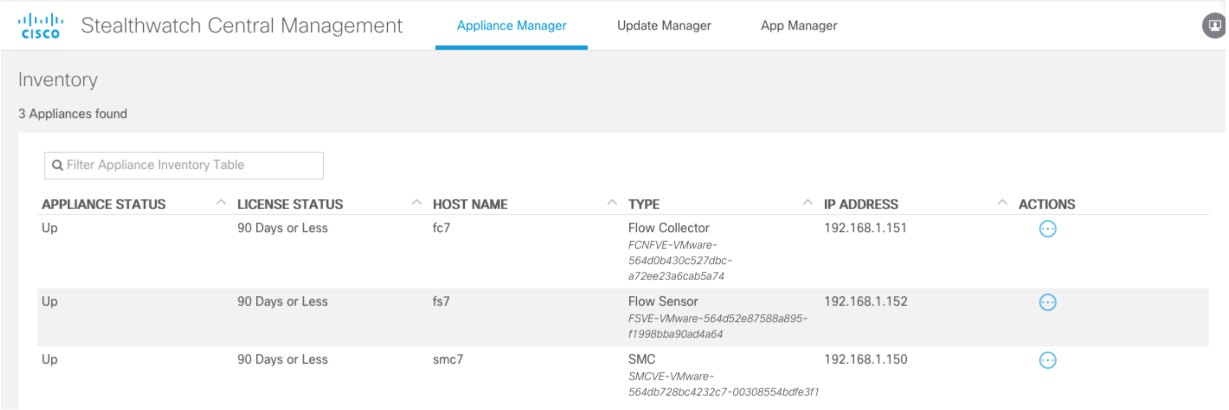
Importing the CA Root Certificate

First, we will import the root certificate into the Stealthwatch truststore.

Step 1 Login to SMC, Click on the Gear below



Step 2 Select **Central Management**, you should see:



Stealthwatch Central Management
Appliance Manager
Update Manager
App Manager

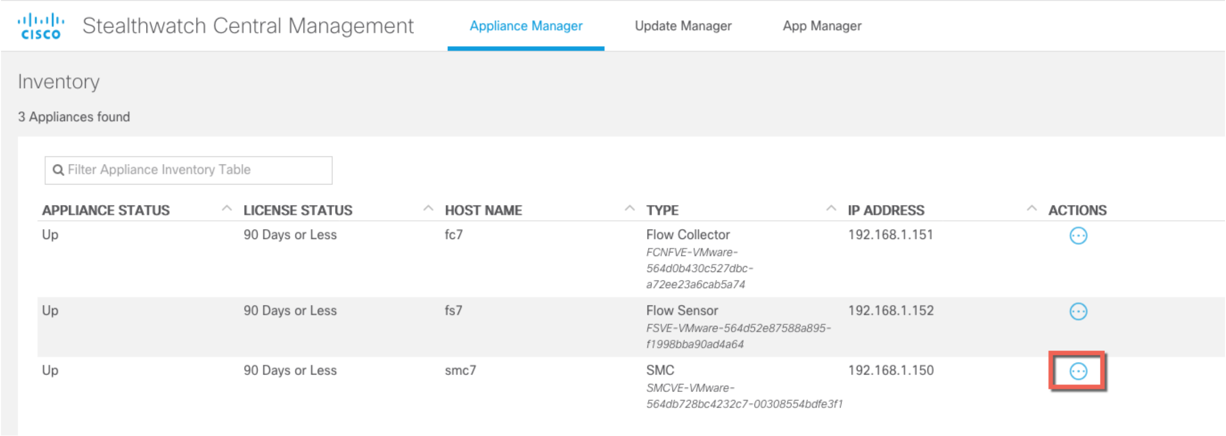
Inventory

3 Appliances found

Filter Appliance Inventory Table

APPLIANCE STATUS	LICENSE STATUS	HOST NAME	TYPE	IP ADDRESS	ACTIONS
Up	90 Days or Less	fc7	Flow Collector *FCNFVE-VMware-564d0b430c527dbc-a72ee23a6cab5a74*	192.168.1.151	⋯
Up	90 Days or Less	fs7	Flow Sensor *FSVE-VMware-564d52e87588a895-f1998bba90ad4a64*	192.168.1.152	⋯
Up	90 Days or Less	smc7	SMC *SMCVE-VMware-564db728bc4232c7-00308554bdfe3f1*	192.168.1.150	⋯

Step 3 Under **SMC**, click on the button under **Actions** as seen below:



Stealthwatch Central Management
Appliance Manager
Update Manager
App Manager

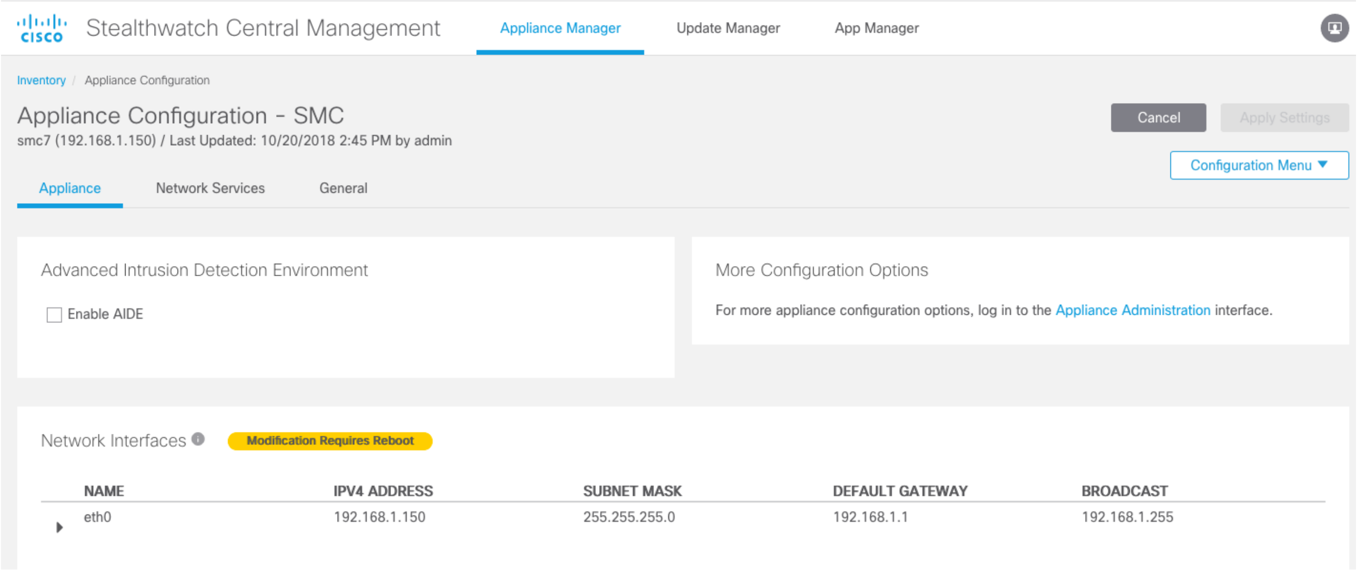
Inventory

3 Appliances found

Filter Appliance Inventory Table

APPLIANCE STATUS	LICENSE STATUS	HOST NAME	TYPE	IP ADDRESS	ACTIONS
Up	90 Days or Less	fc7	Flow Collector *FCNFVE-VMware-564d0b430c527dbc-a72ee23a6cab5a74*	192.168.1.151	⋯
Up	90 Days or Less	fs7	Flow Sensor *FSVE-VMware-564d52e87588a895-f1998bba90ad4a64*	192.168.1.152	⋯
Up	90 Days or Less	smc7	SMC *SMCVE-VMware-564db728bc4232c7-00308554bdfe3f1*	192.168.1.150	⋯

Step 4 Select **Edit Appliance Configurations,** you should see:



Stealthwatch Central Management
Appliance Manager
Update Manager
App Manager
Inventory / Appliance Configuration

Appliance Configuration - SMC

smc7 (192.168.1.150) / Last Updated: 10/20/2018 2:45 PM by admin

Advanced Intrusion Detection Environment

□ Enable AIDE

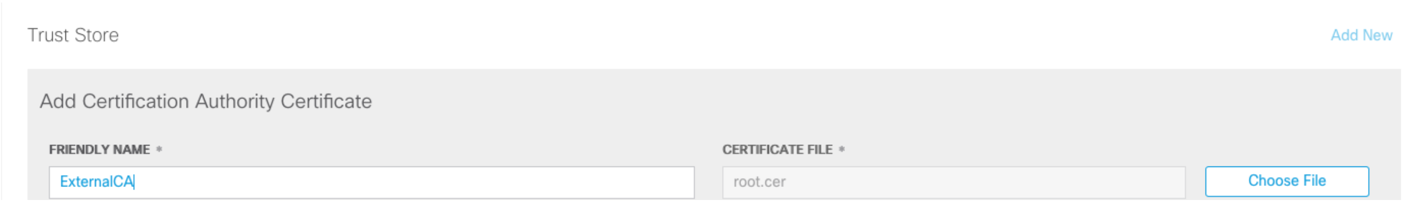
More Configuration Options

For more appliance configuration options, log in to the Appliance Administration interface.

Network Interfaces

NAME	IPV4 ADDRESS	SUBNET MASK	DEFAULT GATEWAY	BROADCAST
eth0	192.168.1.150	255.255.255.0	192.168.1.1	192.168.1.255

Step 5 Click on **General->Truststore->Add New->**choose and upload the external root certificate

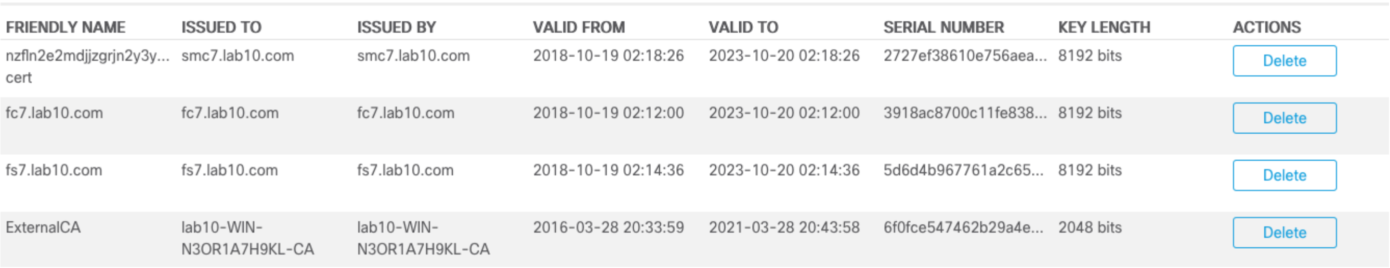


Add Certification Authority Certificate

FRIENDLY NAME *: ExternalCA

CERTIFICATE FILE *: root.cer

Step 6 Select **Add Certificate,** you should see the certificate:

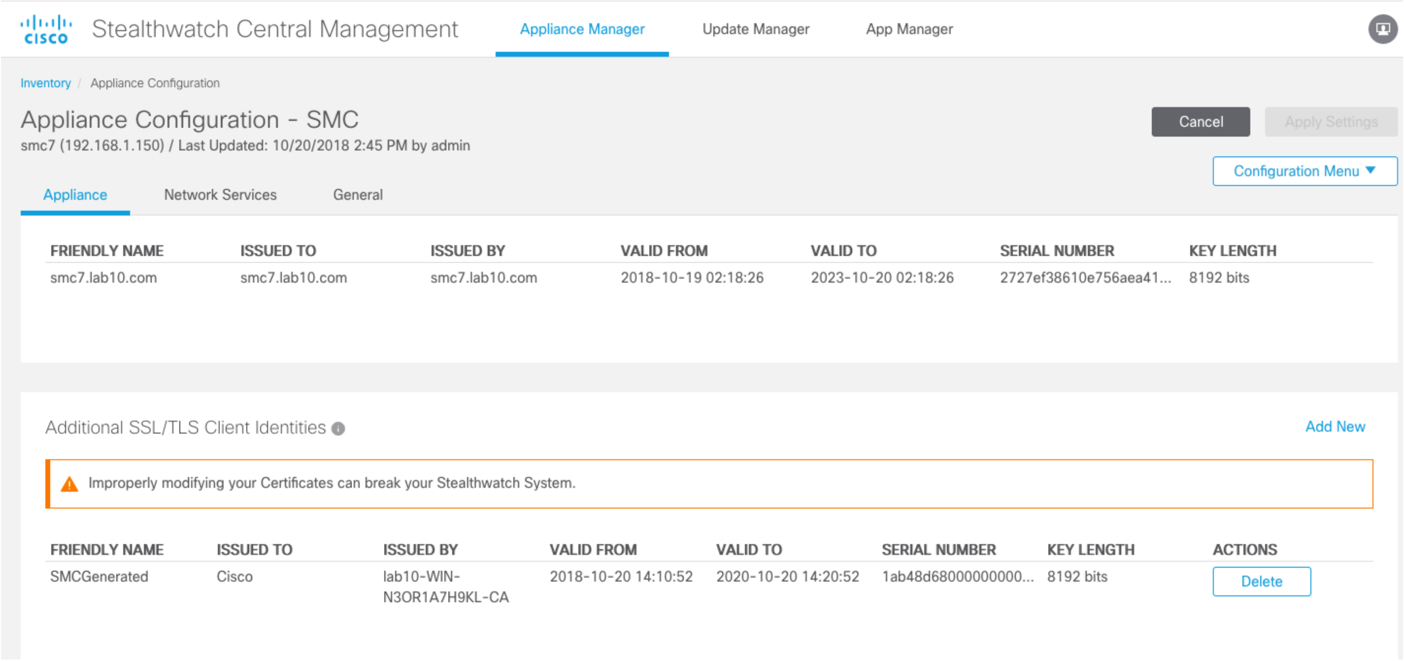


FRIENDLY NAME	ISSUED TO	ISSUED BY	VALID FROM	VALID TO	SERIAL NUMBER	KEY LENGTH	ACTIONS
nzfln2e2mdjjzgrjn2y3y... cert	smc7.lab10.com	smc7.lab10.com	2018-10-19 02:18:26	2023-10-20 02:18:26	2727ef38610e756aea...	8192 bits	Delete
fc7.lab10.com	fc7.lab10.com	fc7.lab10.com	2018-10-19 02:12:00	2023-10-20 02:12:00	3918ac8700c11fe838...	8192 bits	Delete
fs7.lab10.com	fs7.lab10.com	fs7.lab10.com	2018-10-19 02:14:36	2023-10-20 02:14:36	5d6d4b967761a2c65...	8192 bits	Delete
ExternalCA	lab10-WIN-N3OR1A7H9KL-CA	lab10-WIN-N3OR1A7H9KL-CA	2016-03-28 20:33:59	2021-03-28 20:43:58	6f0fce547462b29a4e...	2048 bits	Delete

Step 7 Select **Apply Settings**

Generating Stealthwatch CSR request

Step 1 Select **Configuration Menu->Appliance->Additional SSL/TLS Client Identities**
You should see



Appliance Configuration - SMC
smc7 (192.168.1.150) / Last Updated: 10/20/2018 2:45 PM by admin

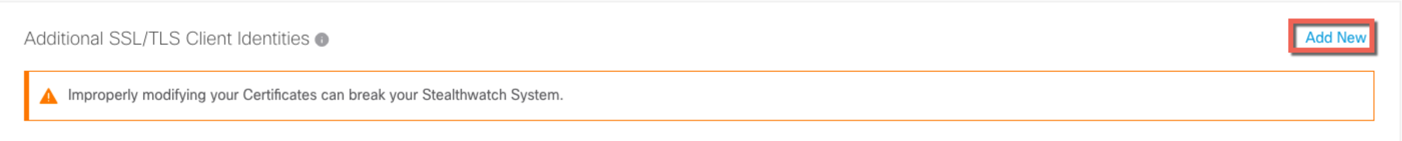
FRIENDLY NAME	ISSUED TO	ISSUED BY	VALID FROM	VALID TO	SERIAL NUMBER	KEY LENGTH
smc7.lab10.com	smc7.lab10.com	smc7.lab10.com	2018-10-19 02:18:26	2023-10-20 02:18:26	2727ef38610e756aea41...	8192 bits

Additional SSL/TLS Client Identities

Improperly modifying your Certificates can break your Stealthwatch System.

FRIENDLY NAME	ISSUED TO	ISSUED BY	VALID FROM	VALID TO	SERIAL NUMBER	KEY LENGTH	ACTIONS
SMCGenerated	Cisco	lab10-WIN-N3OR1A7H9KL-CA	2018-10-20 14:10:52	2020-10-20 14:20:52	1ab48d68000000000...	8192 bits	Delete

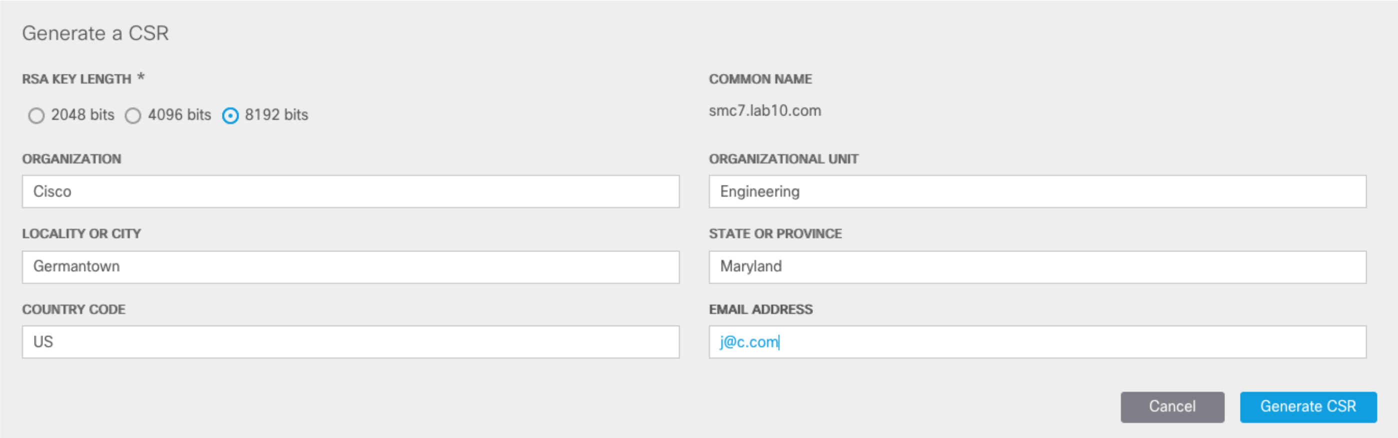
Step 2 Select **Add New**



Additional SSL/TLS Client Identities

Improperly modifying your Certificates can break your Stealthwatch System.

Step 3 Fill out the CSR Request



Generate a CSR

RSA KEY LENGTH *

○ 2048 bits ○ 4096 bits ● 8192 bits

COMMON NAME: smc7.lab10.com

ORGANIZATION: Cisco

ORGANIZATIONAL UNIT: Engineering

LOCALITY OR CITY: Germantown

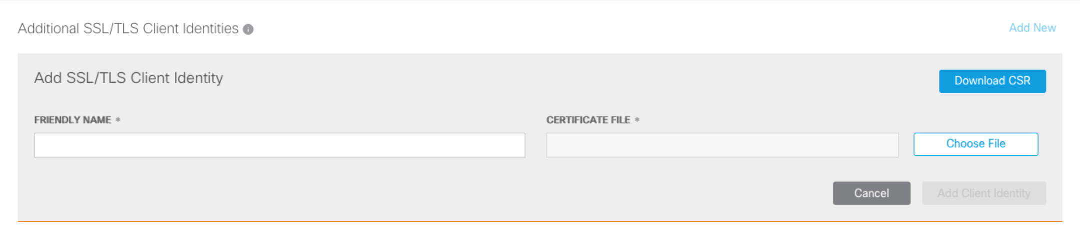
STATE OR PROVINCE: Maryland

COUNTRY CODE: US

EMAIL ADDRESS: j@c.com

Step 4 Select **Generate CSR**

Step 5 You will see the following



Additional SSL/TLS Client Identities

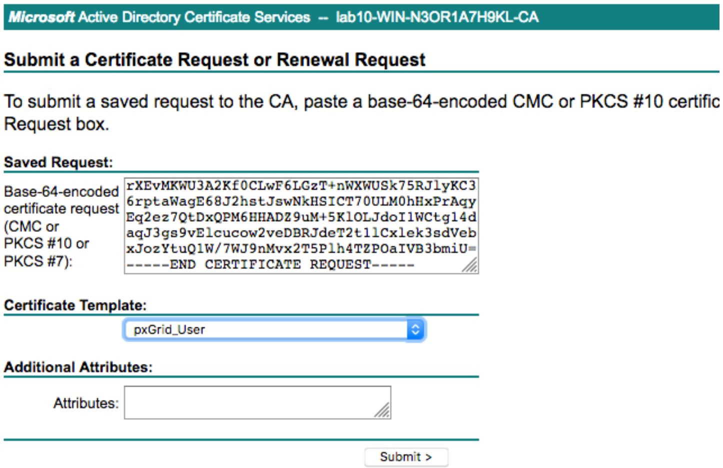
Add SSL/TLS Client Identity

FRIENDLY NAME *

CERTIFICATE FILE *

Step 6 Select **Download CSR**

Step 7 Paste the request in the customized pxGrid template



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

Submit a Certificate Request or Renewal Request

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

Saved Request:

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

```
rXEvMKWU3A2Kf0CLwF6LGzT+nWXWUSk75RJlyKC3
6rptaWagE68J2hstJswNkHSICT70ULM0hHxPrAqy
Eq2ez7QtDxQPM6HHADZ9uM+5Kl0LJdoIlWCtgl4d
aqJ3gs9vElcucow2veDBRJdeT2tllCxlek3sdVeb
xJozYtuQlW/7WJ9nMvx2T5Plh4TZPOaIVB3bmiU=
-----END CERTIFICATE REQUEST-----
```

Certificate Template: pxGrid_User

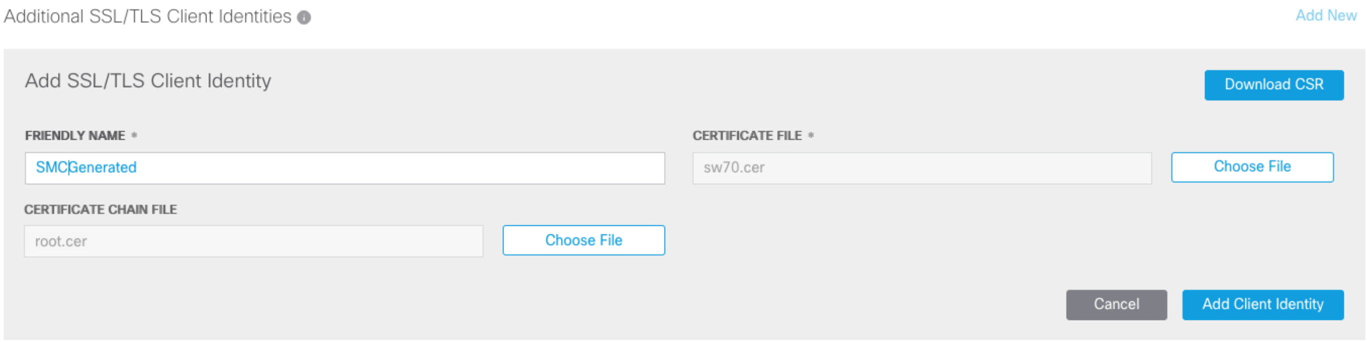
Additional Attributes:

Attributes:

Step 8 Select **Submit**

Step 9 **Download** certificate in **Base 64 encoded** format

Step 10 Upload **Stealthwatch certificate** and **chain certificate** and add the friendly name



Additional SSL/TLS Client Identities

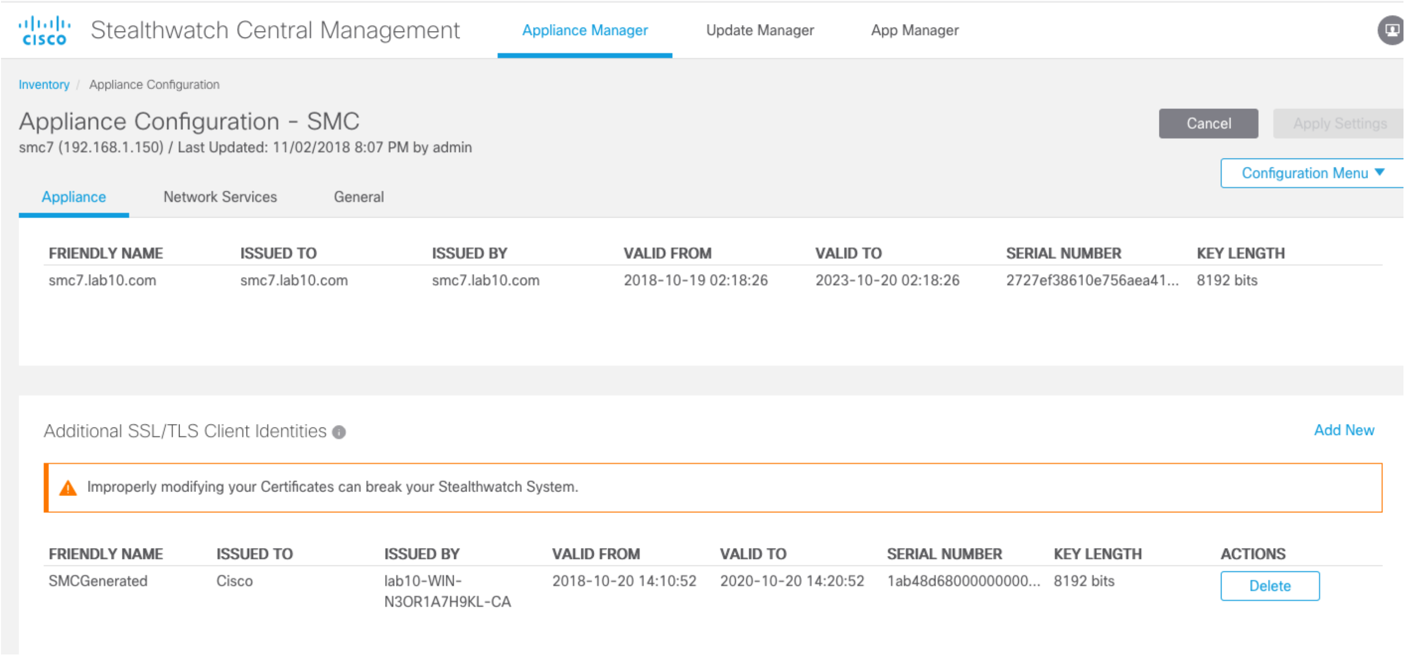
Add SSL/TLS Client Identity

FRIENDLY NAME *: SMCGenerated

CERTIFICATE FILE *: sw70.cer

CERTIFICATE CHAIN FILE: root.cer

Step 11 Select **Add Client Identity**
You should see:



Appliance Configuration - SMC

smc7 (192.168.1.150) / Last Updated: 11/02/2018 8:07 PM by admin

FRIENDLY NAME	ISSUED TO	ISSUED BY	VALID FROM	VALID TO	SERIAL NUMBER	KEY LENGTH
smc7.lab10.com	smc7.lab10.com	smc7.lab10.com	2018-10-19 02:18:26	2023-10-20 02:18:26	2727ef38610e756aea41...	8192 bits

Additional SSL/TLS Client Identities

⚠ Improperly modifying your Certificates can break your Stealthwatch System.

FRIENDLY NAME	ISSUED TO	ISSUED BY	VALID FROM	VALID TO	SERIAL NUMBER	KEY LENGTH	ACTIONS
SMCGenerated	Cisco	lab10-WIN-N3OR1A7H9KL-CA	2018-10-20 14:10:52	2020-10-20 14:20:52	1ab48d68000000000...	8192 bits	Delete

Step 12 Select **Apply Settings**

Using ISE Internal CA

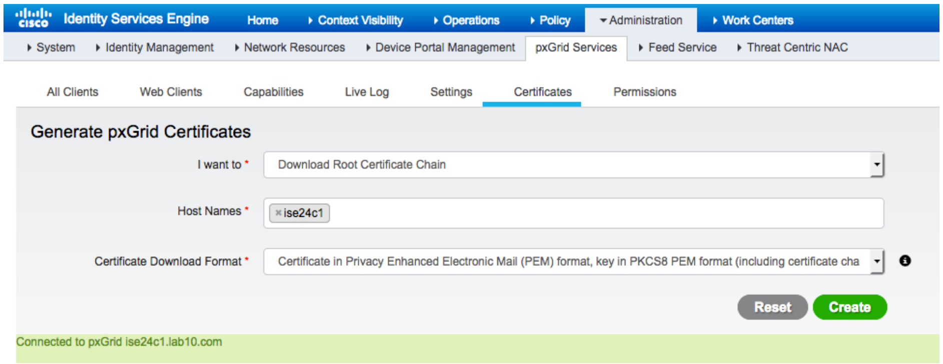
Importing the ISE Internal Root Certificate

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

Step 2 Under **I want to**, select Download **Root Certificate Chain**

Step 3 Select the **Host name** of ise24c1

Step 4 Select **Create**



Generate pxGrid Certificates

I want to * Download Root Certificate Chain

Host Names * ise24c1

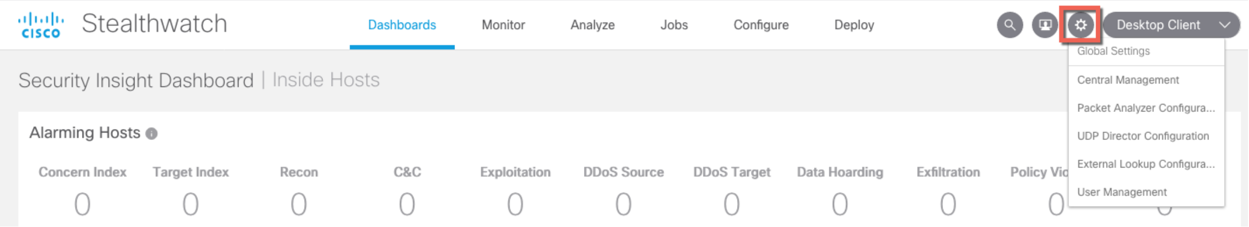
Certificate Download Format * Certificate in Privacy Enhanced Electronic Mail (PEM) format, key in PKCS8 PEM format (including certificate cha

Connected to pxGrid ise24c1.lab10.com

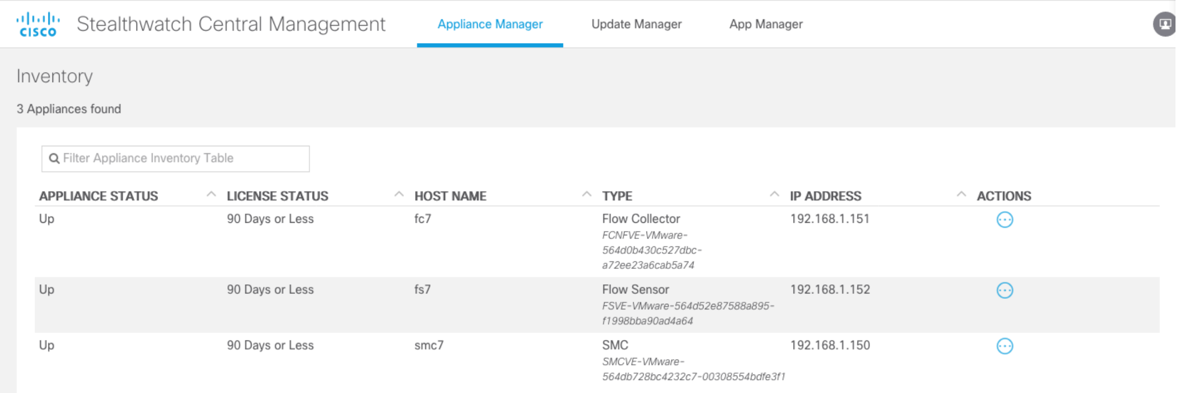
Step 5 Download the zipped file

Note: We will upload the root certificate CertificateServicesRootCA-ise24c1_.cer in the Stealthwatch truststore

Step 6 Login to SMC, Click on the Gear below



Step 7 Select **Central Management**, you should see:

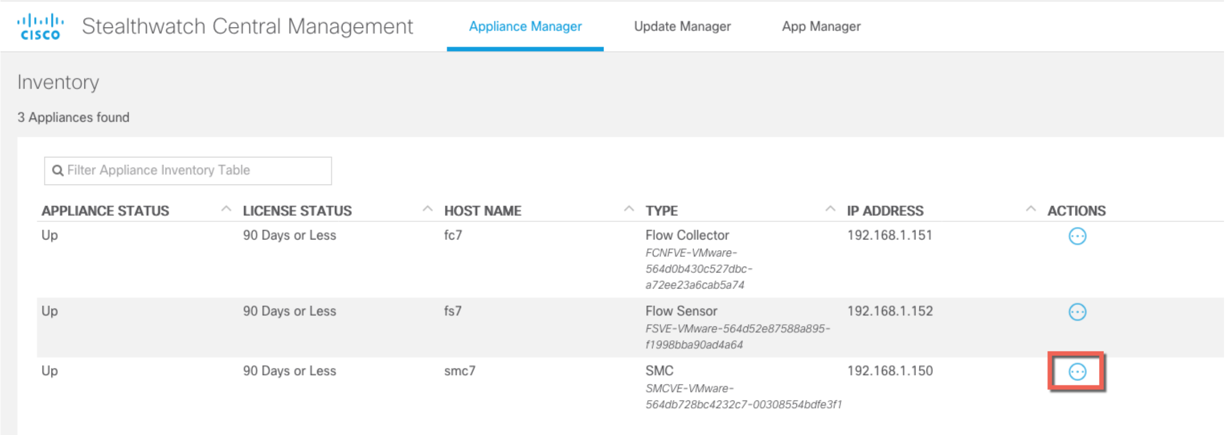

Stealthwatch Central Management
Appliance Manager
Update Manager
App Manager
Filter Appliance Inventory Table

Inventory

3 Appliances found

APPLIANCE STATUS	LICENSE STATUS	HOST NAME	TYPE	IP ADDRESS	ACTIONS
Up	90 Days or Less	fc7	Flow Collector *FCNFVE-VMware-564d0b430c527dbc-a72ee23a6cab5a74*	192.168.1.151	⋯
Up	90 Days or Less	fs7	Flow Sensor *FSVE-VMware-564d52e87588a895-f1998bba90ad4a64*	192.168.1.152	⋯
Up	90 Days or Less	smc7	SMC *SMCVE-VMware-564db728bc4232c7-00308554bdfe3f1*	192.168.1.150	⋯

Step 8 Under **SMC**, click on the button under **Actions** as seen below:



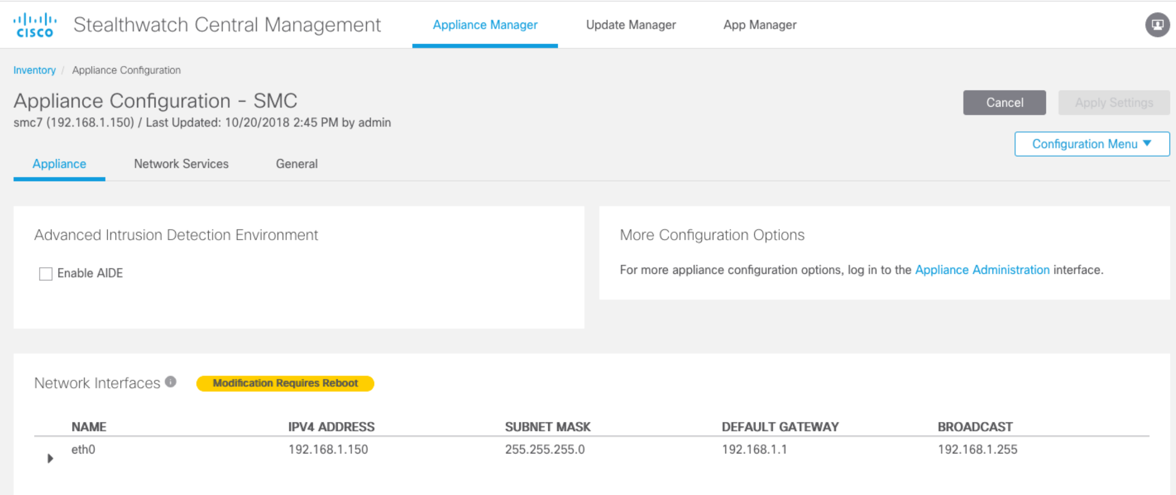
Inventory

3 Appliances found

Filter Appliance Inventory Table

APPLIANCE STATUS	LICENSE STATUS	HOST NAME	TYPE	IP ADDRESS	ACTIONS
Up	90 Days or Less	fc7	Flow Collector *FCNFVE-VMware-564d0b430c527dbc-a72ee23a6cab5a74*	192.168.1.151	⊙
Up	90 Days or Less	fs7	Flow Sensor *FSVE-VMware-564d52e87588a895-f1998bba90ad4a64*	192.168.1.152	⊙
Up	90 Days or Less	smc7	SMC *SMCVE-VMware-564db728bc4232c7-00308554bdfe3f1*	192.168.1.150	⊙

Step 9 Select **Edit Appliance Configurations,** you should see:



Appliance Configuration - SMC

smc7 (192.168.1.150) / Last Updated: 10/20/2018 2:45 PM by admin

Advanced Intrusion Detection Environment

□ Enable AIDE

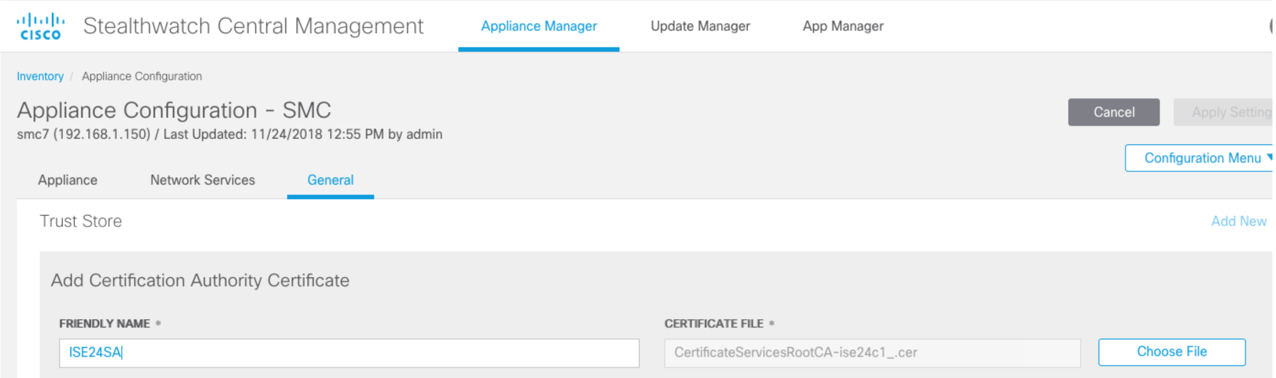
More Configuration Options

For more appliance configuration options, log in to the Appliance Administration interface.

Network Interfaces Modification Requires Reboot

NAME	IPV4 ADDRESS	SUBNET MASK	DEFAULT GATEWAY	BROADCAST
eth0	192.168.1.150	255.255.255.0	192.168.1.1	192.168.1.255

Step 10 Click on **General->Truststore->Add New->**choose and upload the external root certificate



Appliance Configuration - SMC

smc7 (192.168.1.150) / Last Updated: 11/24/2018 12:55 PM by admin

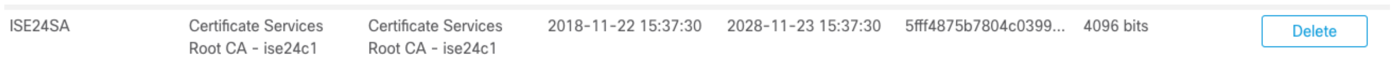
Trust Store

Add Certification Authority Certificate

FRIENDLY NAME * ISE24SA|

CERTIFICATE FILE * CertificateServicesRootCA-ise24c1_.cer

Step 11 Select **Add Certificate,** you should see the certificate:

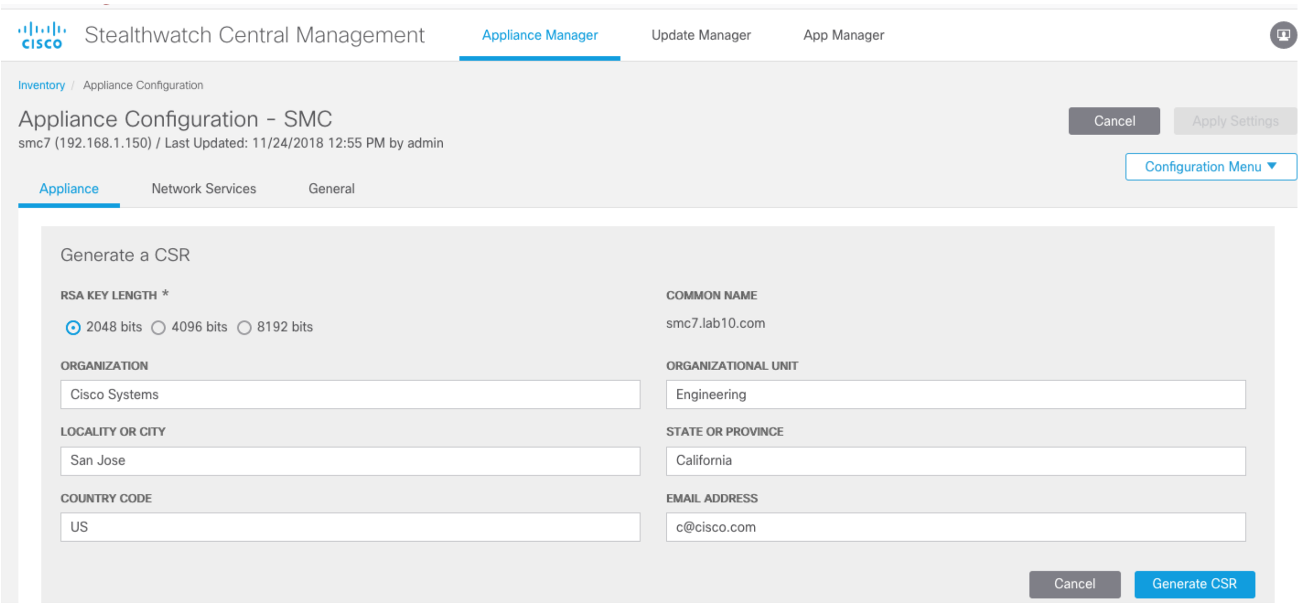


ISE24SA	Certificate Services Root CA - ise24c1	Certificate Services Root CA - ise24c1	2018-11-22 15:37:30	2028-11-23 15:37:30	5fff4875b7804c0399...	4096 bits	Delete

Step 12 Select **Apply Settings**

Generating Stealthwatch CSR request

Step 1 Under **Generate a CSR->RSA Key Length->**change the RSA key length to **2048 bits**



Appliance Configuration - SMC

smc7 (192.168.1.150) / Last Updated: 11/24/2018 12:55 PM by admin

Generate a CSR

RSA KEY LENGTH * ● 2048 bits ○ 4096 bits ○ 8192 bits

COMMON NAME: smc7.lab10.com

ORGANIZATION: Cisco Systems

ORGANIZATIONAL UNIT: Engineering

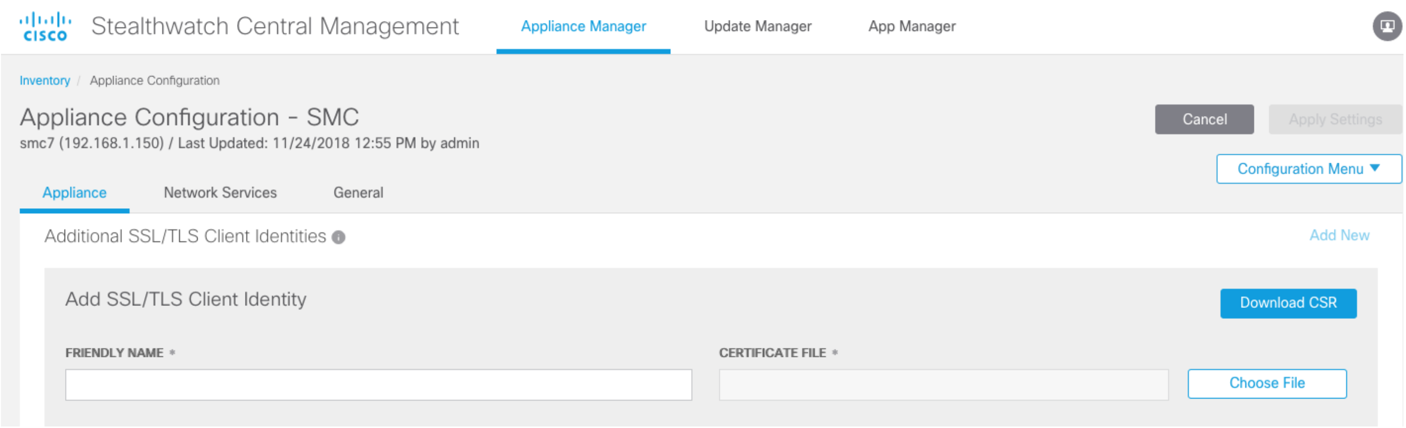
LOCALITY OR CITY: San Jose

STATE OR PROVINCE: California

COUNTRY CODE: US

EMAIL ADDRESS: c@cisco.com

Step 2 Select **Generate CSR**



Appliance Configuration - SMC

smc7 (192.168.1.150) / Last Updated: 11/24/2018 12:55 PM by admin

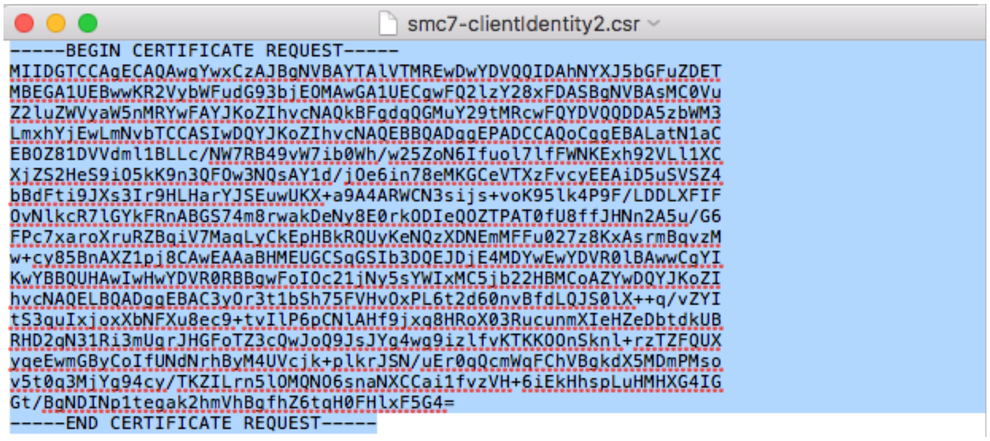
Additional SSL/TLS Client Identities

Add SSL/TLS Client Identity

FRIENDLY NAME *

CERTIFICATE FILE *

Step 3 Download the CSR file and open using “TextEdit” or other editor.

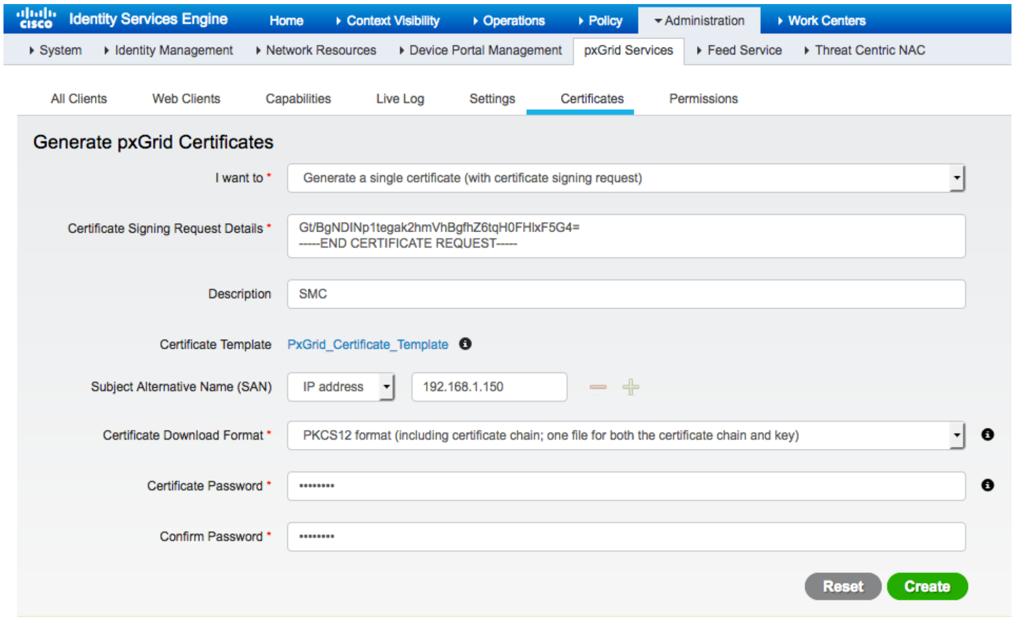


```
-----BEGIN CERTIFICATE REQUEST-----
MIIDGTCCAgECAQAwgYwxCzAJBgNVBAYTAlVTMREwDwYDVQQIDAhNYXJ5bGFuZDET
MBEGA1UEBwwKR2VybWFudG93bjEOMAwGA1UECgwFQ2lzY28xFDASBgNVBAsMC0Vu
Z2luZWVyaW5nMRYwFAYJKoZIhvcNAQkBFgdqQGMuY29tMRcwFQYDVQQDDA5zbWM3
LmxhYjEwLmNvbTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBALatN1aC
EBOZ81DVVdml1BLLc/NW7RB49vW7ib0Wh/w25ZoN6Ifuol7lfFWNKExh92VLl1XC
XjZS2HeS9iO5kK9n3QFOw3NQsAY1d/jOe6in78eMKGCeVTXzFvcyEEAiD5uSVSZ4
bBdFti9JXs3Ir9HLHarYJSEuwUKX+a9A4ARWCN3sijs+voK95lk4P9F/LDDLXFIF
OvNlkcR7lGYkFRnABGS74m8rwakDeNy8E0rkODIeQOZTPAT0fU8ffJHNn2A5u/G6
FPc7xaroXruRZBqiV7MaqLyCkEpHBkRQUyKeNQzXDNEmMFFu027z8KxAsrmBqvzM
w+cy85BnAXZ1pj8CAwEAAaBHMEUGCSqGSIb3DQEJDjE4MDYwEwYDVR0lBAwwCgYI
KwYBBQUHAwIwHwYDVR0RBBgwFoIOc21jNy5sYWIxMC5jb22HBMCoAZYwDQYJKoZI
hvcNAQELBQADggEBAC3yOr3t1bSh75FVHvOxPL6t2d60nvBfdLQJS0lX++q/vZYI
tS3quIxjoxXbNFXu8ec9+tvIlP6pCNlAHf9jxq8HRoX03RucunmXIeHZeDbtdkUB
RHD2qN31Ri3mUgrJHGFoTZ3cQwJoQ9JsJYg4wg9izlfvKTKKOOnSknl+rzTZFQUX
yqeEwmGByCoIfUNdNrhByM4UVcjk+plkrJSN/uEr0qQcmWqFChVBgkdX5MDmPMso
v5t0q3MjYg94cy/TKZILrn5lOMQNO6snaNXCCai1fvzVH+6iEkHhspLuHMHXG4IG
Gt/BgNDINp1tegak2hmVhBgfhZ6tqH0FHlxF5G4=
-----END CERTIFICATE REQUEST-----
```

Step 4 Goto to ISE, Select **Administration->pxGrid Services->Certificates->Generate pxGrid Certificates**

Step 5 Under **I want to**, select **Generate a single certificate with (certificate signing request)**

Step 6 Paste the CSR request into Certificate Signing Request Details



Generate pxGrid Certificates

I want to *	Generate a single certificate (with certificate signing request)
Certificate Signing Request Details *	Gt/BgNDINp1tegak2hmVhBgfhZ6tqH0FHlxF5G4= -----END CERTIFICATE REQUEST-----
Description	SMC
Certificate Template	PxGrid_Certificate_Template
Subject Alternative Name (SAN)	IP address 192.168.1.150
Certificate Download Format *	PKCS12 format (including certificate chain; one file for both the certificate chain and key)
Certificate Password *	••••••••
Confirm Password *	••••••••

Step 7 Enter a **description name**

Step 8 Leave defaults for **pxGrid_Certificate_template** (RSA key size 2048 bits)

Step 9 Enter the IP address of the SMC console under the **Subject Alternative Name** (SAN) name

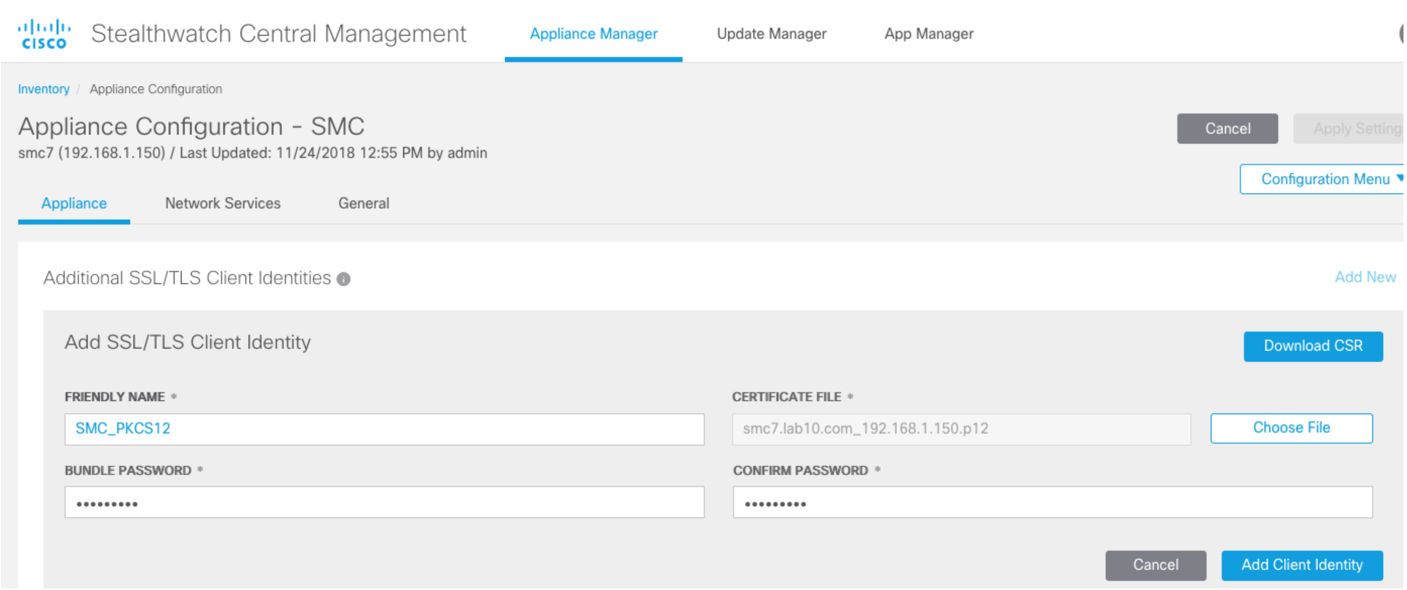
Step 10 Under **Certificate Download Format**, select **PKCS12 format (including certificate chain, one file fore both the certificate and key)**

Step 11 Enter the password and confirm the password

Step 12 Select **Create**

Step 13 Unzip the file

Step 14 Upload the .p12 filename into Stealtwatch



Appliance Configuration - SMC

smc7 (192.168.1.150) / Last Updated: 11/24/2018 12:55 PM by admin

Additional SSL/TLS Client Identities

Add SSL/TLS Client Identity

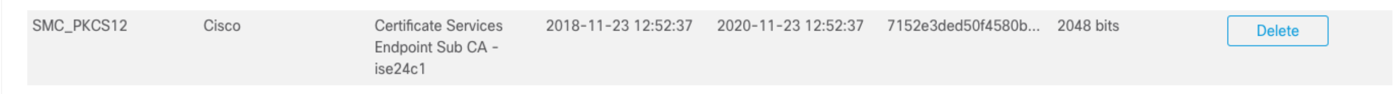
FRIENDLY NAME * SMC_PKCS12

CERTIFICATE FILE * smc7.lab10.com_192.168.1.150.p12

BUNDLE PASSWORD * •••••••••

CONFIRM PASSWORD * •••••••••

Step 15 Select **Add Client Identity**, you should see



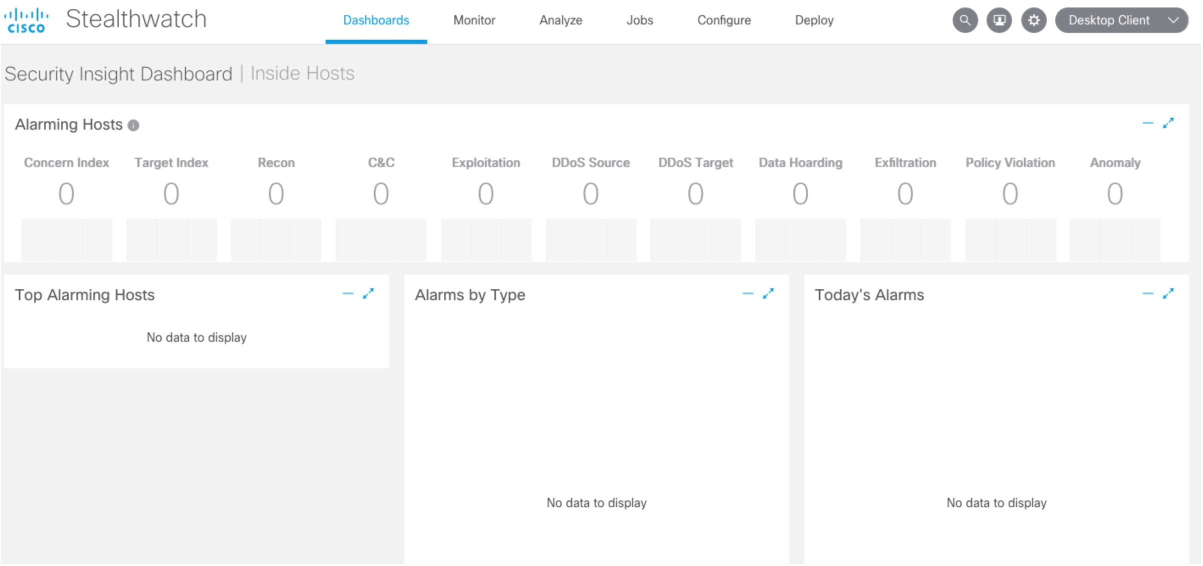
SMC_PKCS12	Cisco	Certificate Services Endpoint Sub CA - ise24c1	2018-11-23 12:52:37	2020-11-23 12:52:37	7152e3ded50f4580b...	2048 bits

Step 16 Select **Apply Settings**

Configuring ISE pxGrid Integration

In this section, Stealthwatch 7.0 is configured to successfully connect, register and subscribe to the ISE pxGrid node.

Step 1 Go to the Dashboard Screen, select **Dashboards**



Security Insight Dashboard | Inside Hosts

Alarming Hosts

Concern Index	Target Index	Recon	C&C	Exploitation	DDoS Source	DDoS Target	Data Hoarding	Exfiltration	Policy Violation	Anomaly
0	0	0	0	0	0	0	0	0	0	0

Top Alarming Hosts

No data to display

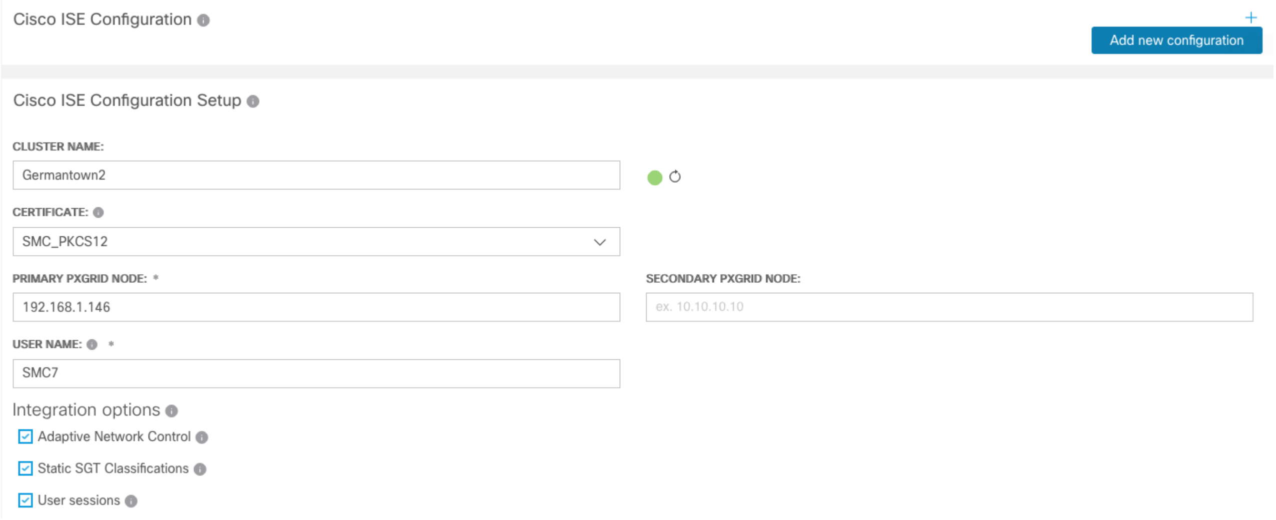
Alarms by Type

No data to display

Today's Alarms

No data to display

Step 2 Select **Deploy**
Step 3 Select **Deploy Cisco ISE Configuration->Add New Configuration**
Step 4 Enter the ISE Cluster Name: i.e. **Germantown2**
Step 5 Select Stealthwatch certificate from the certificate drop down, i.e. **SMC_PKCS12**
Step 6 Enter the IP address of ISE pxGrid node, i.e. **192.168.1.251**
Step 7 Enter the username which will be the pxGrid client name, i.e. **SMC7**
Step 8 Ensure all the topic settings are enabled under **Integration Options**



Cisco ISE Configuration

Cisco ISE Configuration Setup

CLUSTER NAME: Germantown2

CERTIFICATE: SMC_PKCS12

PRIMARY PXGRID NODE: * 192.168.1.146

SECONDARY PXGRID NODE: ex. 10.10.10.10

USER NAME: * SMC7

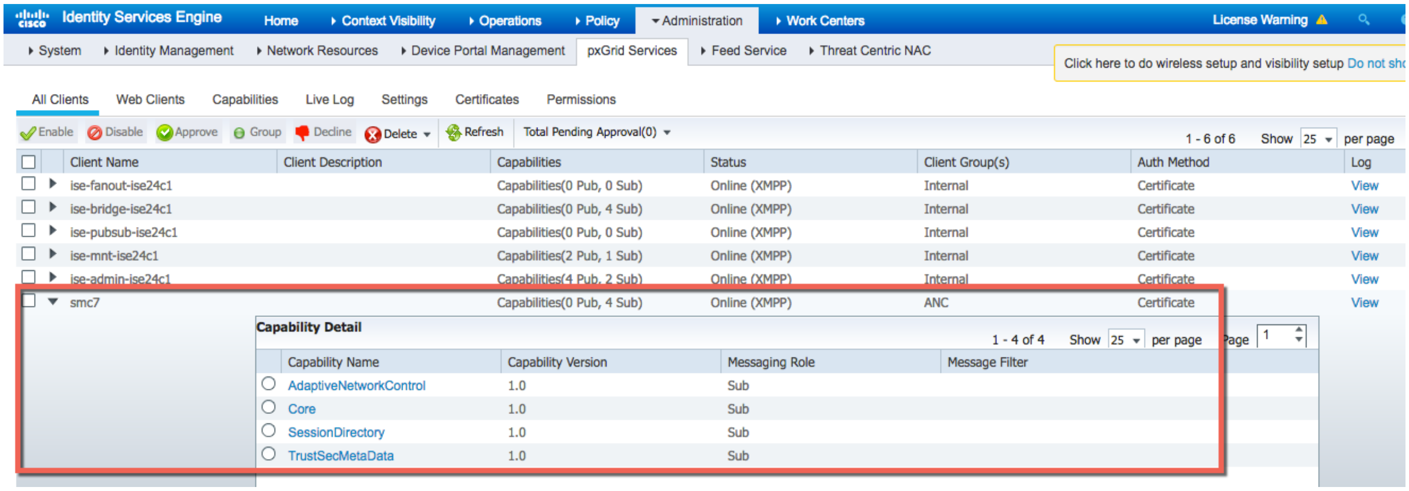
Integration options

☑ Adaptive Network Control
☑ Static SGT Classifications
☑ User sessions

Step 9 Select **Save**

Step 10 You Status icon will turn Green

Step 11 In ISE, select **Administration->pxGrid Services**, you should see:



□		Client Name	Client Description	Capabilities	Status	Client Group(s)	Auth Method	Log
□	▶	ise-fanout-ise24c1		Capabilities(0 Pub, 0 Sub)	Online (XMPP)	Internal	Certificate	View
□	▶	ise-bridge-ise24c1		Capabilities(0 Pub, 4 Sub)	Online (XMPP)	Internal	Certificate	View
□	▶	ise-pubsub-ise24c1		Capabilities(0 Pub, 0 Sub)	Online (XMPP)	Internal	Certificate	View
□	▶	ise-mnt-ise24c1		Capabilities(2 Pub, 1 Sub)	Online (XMPP)	Internal	Certificate	View
□	▶	ise-admin-ise24c1		Capabilities(4 Pub, 2 Sub)	Online (XMPP)	Internal	Certificate	View
□	▼	smc7		Capabilities(0 Pub, 4 Sub)	Online (XMPP)	ANC	Certificate	View

Capability Detail

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

ISE Adaptive Network Control (ANC) Policies

ISE ANC policies align with organizations security policies. For example, when malware or breaches are detected, the organization may investigate further by providing segmented network access, or if the threat is more severe, and capable of propagating through the network, the IT admin may want to shut down the port.

Possible ANC actions are: quarantine (Change or Authorization), port-shut and port bounce.

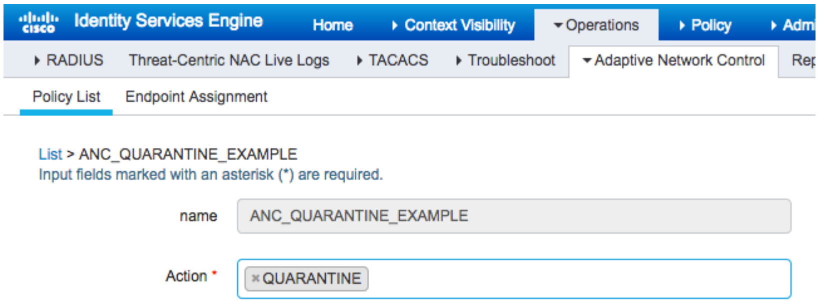
These ANC policies will then be used as condition rules in ISE authorization policies to enforce the organizations security policy.

In this section, the ISE ANC policies are created along with their associated actions. Three policies are created: ANC_QUARANTINE_EXAMPLE, ANC_PORT_SHUT_EXAMPLE, and ANC_PORT_BOUNCE. These ANC policies are added to Global Exceptions List in the ISE Authorization Policies.

Creating ANC Policies

The ANC policies are created along with the associated actions

Step 1 Select **Operations->Adaptive Network Control->Policy List->Add** and enter ANC_QUARANTINE_EXAMPLE for the Policy Name and Quarantine for the Action:



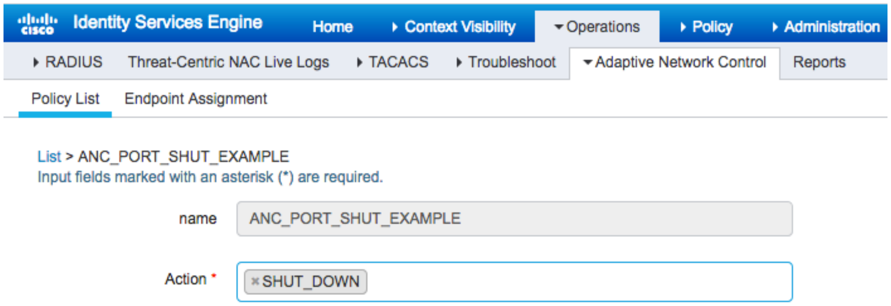
List > ANC_QUARANTINE_EXAMPLE
Input fields marked with an asterisk (*) are required.

name ANC_QUARANTINE_EXAMPLE

Action * QUARANTINE

Step 2 Select **Submit**

Step 3 Select **Policy List->Add** and enter **ANC_PORT_SHUT_EXAMPLE** for the **Name** and **SHUT_DOWN** for the **Action**



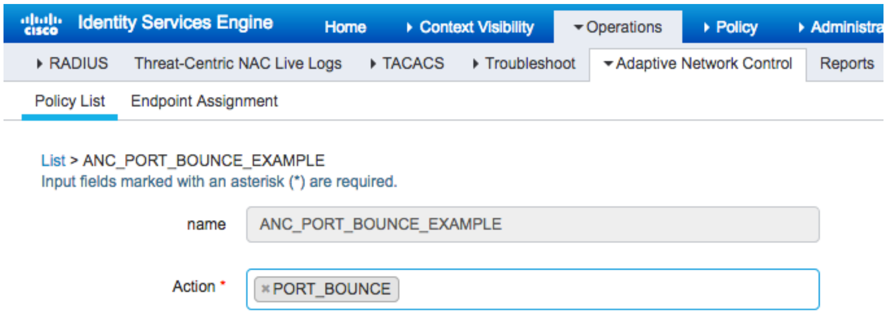
List > ANC_PORT_SHUT_EXAMPLE
Input fields marked with an asterisk (*) are required.

name ANC_PORT_SHUT_EXAMPLE

Action * SHUT_DOWN

Step 4 Select **Submit**

Step 5 Select **Policy List->Add** and enter **ANC_PORT_BOUNCE_EXAMPLE** for the **Name** and **PORT_BOUNCE** for the Action



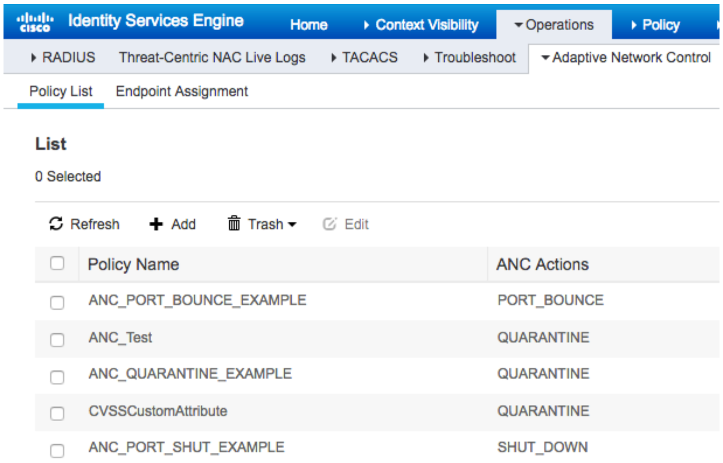
List > ANC_PORT_BOUNCE_EXAMPLE
Input fields marked with an asterisk (*) are required.

name: ANC_PORT_BOUNCE_EXAMPLE

Action *: PORT_BOUNCE

Step 6 Select **Submit**

Step 7 When completed you should see a list of the ANC Policies



List

0 Selected

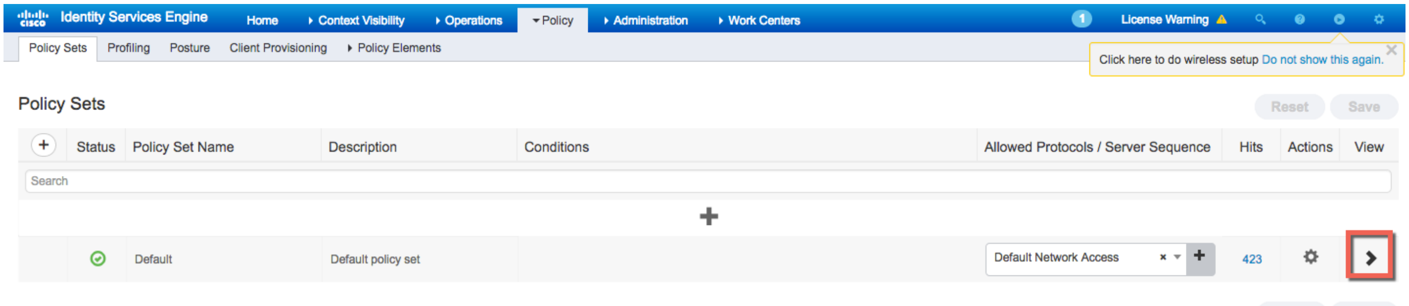
□	Policy Name	ANC Actions
□	ANC_PORT_BOUNCE_EXAMPLE	PORT_BOUNCE
□	ANC_Test	QUARANTINE
□	ANC_QUARANTINE_EXAMPLE	QUARANTINE
□	CVSSCustomAttribute	QUARANTINE
□	ANC_PORT_SHUT_EXAMPLE	SHUT_DOWN

Adding ISE ANC policies to ISE Authorization Policies

The ANC policies are added as conditions rules to an authorization policy.

Step 1 Select **Policy->Policy Sets**

Step 2 Click on "**>**" as seen below:



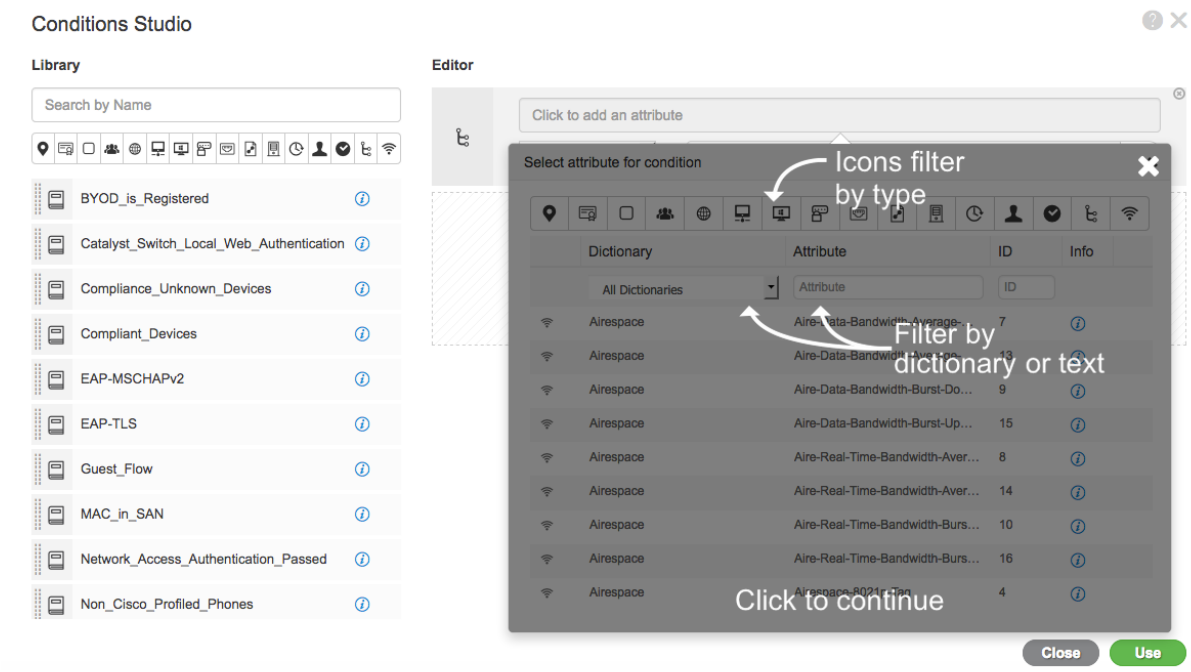
Policy Sets

+	Status	Policy Set Name	Description	Conditions	Allowed Protocols / Server Sequence	Hits	Actions	View
	✓	Default	Default policy set		Default Network Access	423	⚙	>

Step 3 Click on **Authorization Policy->Global Exceptions->"+"**

Step 4 Enter Rule Name: **ANC_Quarantine**

Step 5 Click on "+" under **Conditions,** this brings up the Editor Menu



Conditions Studio

Library

Search by Name

- BYOD_is_Registered
- Catalyst_Switch_Local_Web_Authentication
- Compliance_Unknown_Devices
- Compliant_Devices
- EAP-MSCHAPv2
- EAP-TLS
- Guest_Flow
- MAC_in_SAN
- Network_Access_Authentication_Passed
- Non_Cisco_Profiled_Phones

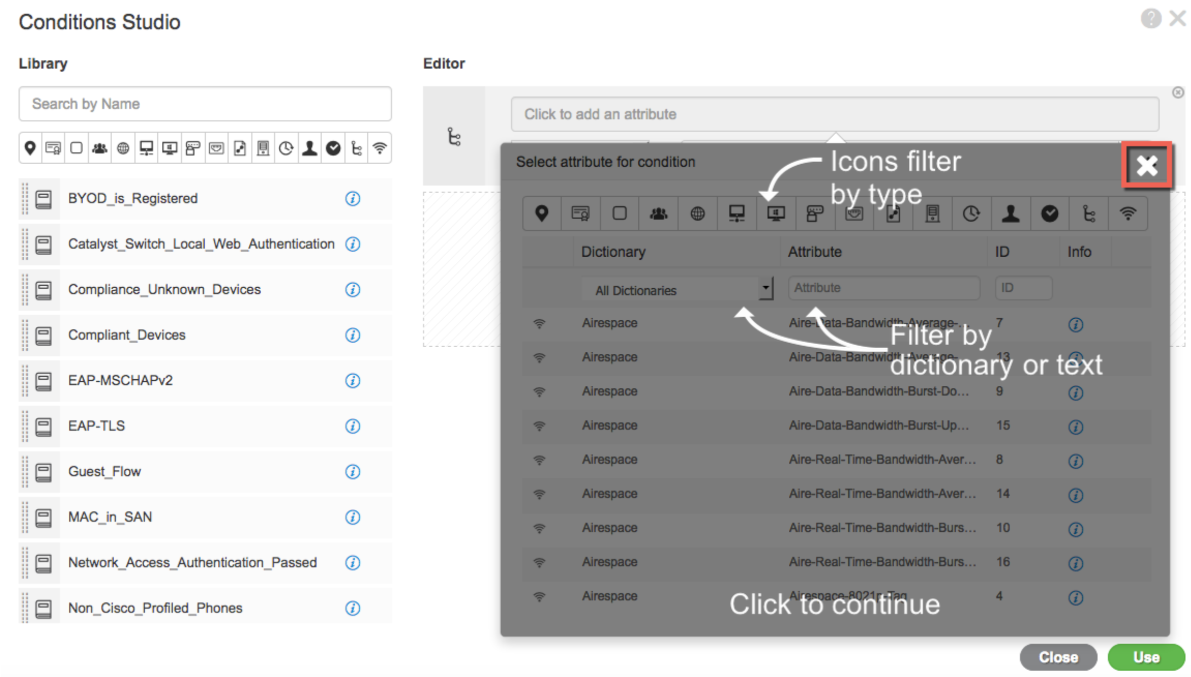
Editor

Click to add an attribute

Select attribute for condition

Dictionary	Attribute	ID	Info
All Dictionaries	Attribute	ID	
Airespace	Aire-Data-Bandwidth-Average-	7	ⓘ
Airespace	Aire-Data-Bandwidth-Average...	13	ⓘ
Airespace	Aire-Data-Bandwidth-Burst-Do...	9	ⓘ
Airespace	Aire-Data-Bandwidth-Burst-Up...	15	ⓘ
Airespace	Aire-Real-Time-Bandwidth-Aver...	8	ⓘ
Airespace	Aire-Real-Time-Bandwidth-Aver...	14	ⓘ
Airespace	Aire-Real-Time-Bandwidth-Burs...	10	ⓘ
Airespace	Aire-Real-Time-Bandwidth-Burs...	16	ⓘ
Airespace	Airespace-8021p-Tag	4	ⓘ

Step 6 Click on "x" to close the tutorial screen



Conditions Studio

Library

Search by Name

- BYOD_is_Registered
- Catalyst_Switch_Local_Web_Authentication
- Compliance_Unknown_Devices
- Compliant_Devices
- EAP-MSCHAPv2
- EAP-TLS
- Guest_Flow
- MAC_in_SAN
- Network_Access_Authentication_Passed
- Non_Cisco_Profiled_Phones

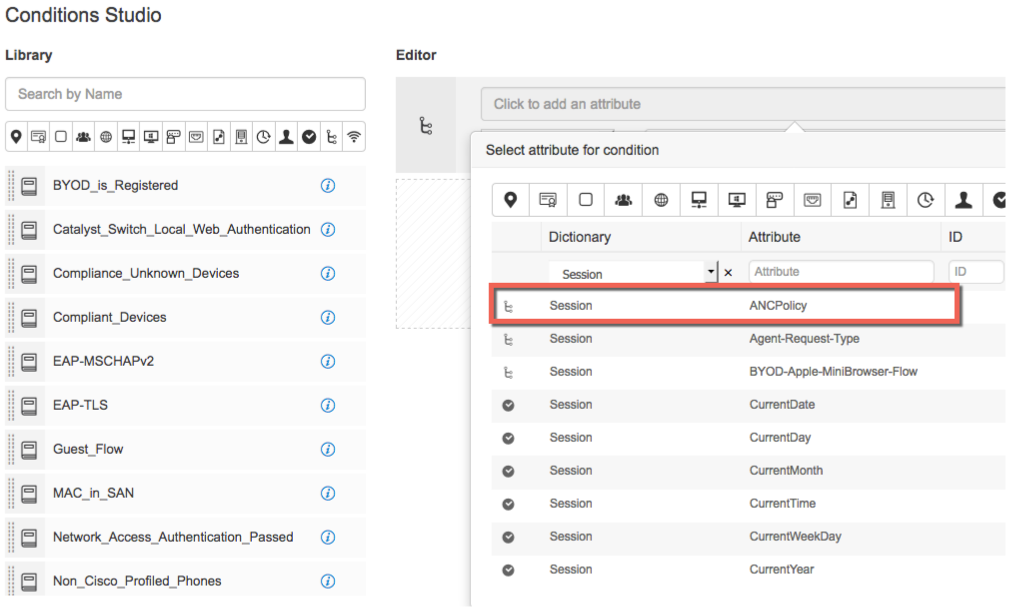
Editor

Click to add an attribute

Select attribute for condition

Dictionary	Attribute	ID	Info
All Dictionaries	Attribute	ID	
Airespace	Aire-Data-Bandwidth-Average-	7	ⓘ
Airespace	Aire-Data-Bandwidth-Average...	13	ⓘ
Airespace	Aire-Data-Bandwidth-Burst-Do...	9	ⓘ
Airespace	Aire-Data-Bandwidth-Burst-Up...	15	ⓘ
Airespace	Aire-Real-Time-Bandwidth-Aver...	8	ⓘ
Airespace	Aire-Real-Time-Bandwidth-Aver...	14	ⓘ
Airespace	Aire-Real-Time-Bandwidth-Burs...	10	ⓘ
Airespace	Aire-Real-Time-Bandwidth-Burs...	16	ⓘ
Airespace	Airespace-8021p-Tag	4	ⓘ

Step 7 Under Dictionary, select **Session** that matches the attribute **ANCPolicy**



Conditions Studio

Library

Search by Name

- BYOD_is_Registered
- Catalyst_Switch_Local_Web_Authentication
- Compliance_Unknown_Devices
- Compliant_Devices
- EAP-MSCHAPv2
- EAP-TLS
- Guest_Flow
- MAC_in_SAN
- Network_Access_Authentication_Passed
- Non_Cisco_Profiled_Phones

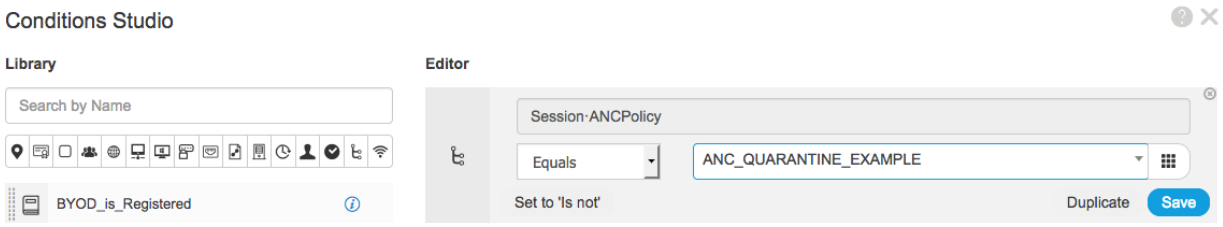
Editor

Click to add an attribute

Select attribute for condition

Dictionary	Attribute	ID
Session	Attribute	ID
Session	ANCPolicy	
Session	Agent-Request-Type	
Session	BYOD-Apple-MiniBrowser-Flow	
Session	CurrentDate	
Session	CurrentDay	
Session	CurrentMonth	
Session	CurrentTime	
Session	CurrentWeekDay	
Session	CurrentYear	

Step 8 From the dropdown, select the **ANC_QUARANTINE_EXAMPLE** policy



Conditions Studio

Library

Search by Name

- BYOD_is_Registered

Editor

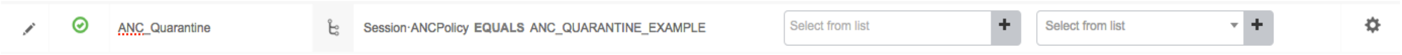
Session·ANCPolicy

Equals | ANC_QUARANTINE_EXAMPLE

Set to 'Is not'

Step 9 Select **Use**

Step 10 You should see

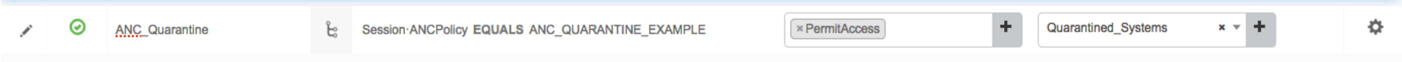


ANC_Quarantine | Session·ANCPolicy EQUALS ANC_QUARANTINE_EXAMPLE | Select from list | Select from list

Step 11 From the **Profiles** drop down menu select **Permit Access**

Step 12 From the **Security Groups** drop down menu select **Quarantined Systems**

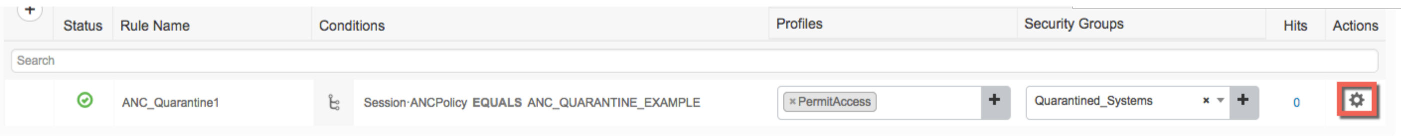
You should see



ANC_Quarantine | Session·ANCPolicy EQUALS ANC_QUARANTINE_EXAMPLE | × PermitAccess | Quarantined_Systems

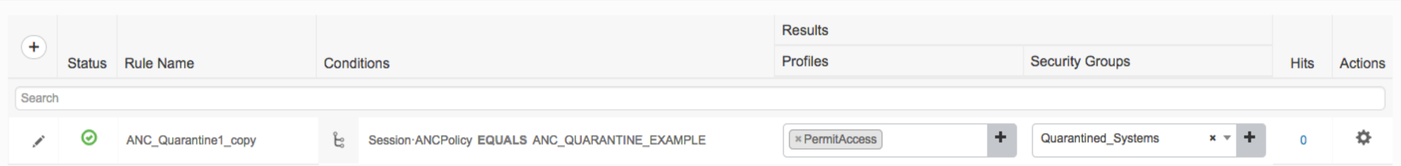
Step 13 Select **Save**

Step 14 To add the ANC policies to the ISE Authorization polices, Under Actions click on “gear”



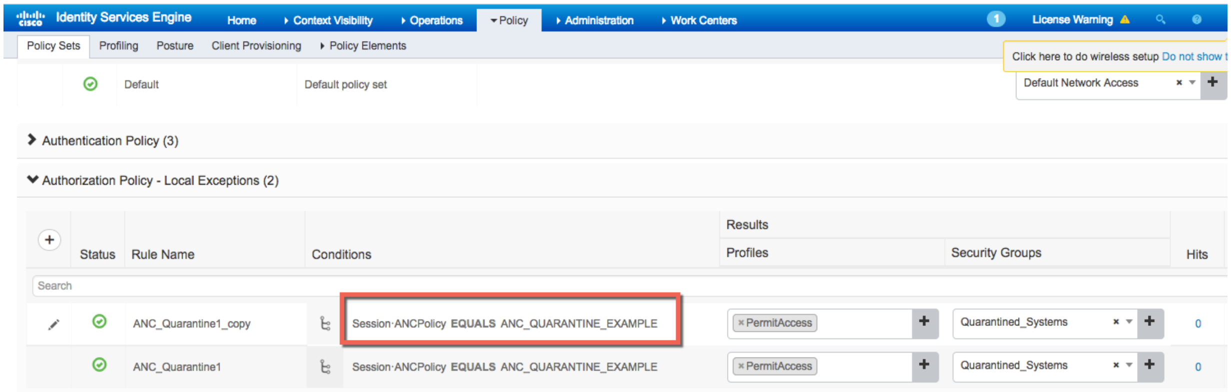
Status	Rule Name	Conditions	Profiles	Security Groups	Hits	Actions
✓	ANC_Quarantine1	Session·ANCPolicy EQUALS ANC_QUARANTINE_EXAMPLE	× PermitAccess	Quarantined_Systems	0	⚙

Step 15 Select **Duplicate Above**
You will see the following:



Status	Rule Name	Conditions	Results Profiles	 Security Groups	Hits	Actions
✓	ANC_Quarantine1_copy	Session·ANCPolicy EQUALS ANC_QUARANTINE_EXAMPLE	× PermitAccess	Quarantined_Systems	0	⚙

Step 16 Click on the condition rule



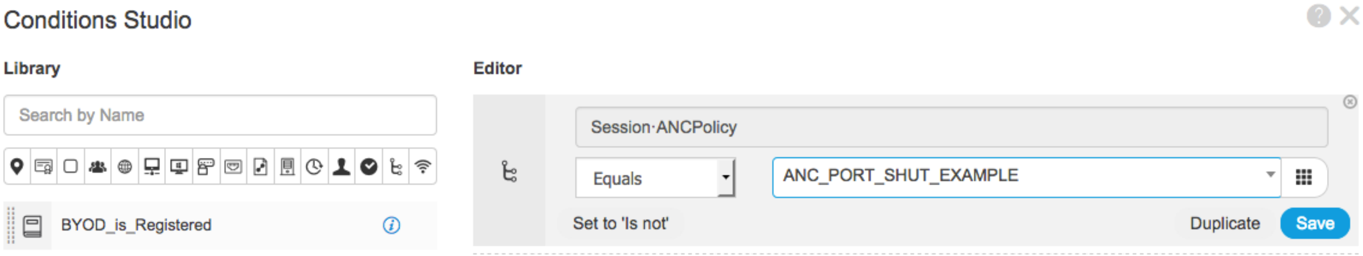
Default — Default policy set — Default Network Access

Authentication Policy (3)

Authorization Policy - Local Exceptions (2)

Status	Rule Name	Conditions	Results Profiles	 Security Groups	Hits
✓	ANC_Quarantine1_copy	Session·ANCPolicy EQUALS ANC_QUARANTINE_EXAMPLE	× PermitAccess	Quarantined_Systems	0
✓	ANC_Quarantine1	Session·ANCPolicy EQUALS ANC_QUARANTINE_EXAMPLE	× PermitAccess	Quarantined_Systems	0

Step 17 Select **ANC_PORT_SHUT_EXAMPLE**



Conditions Studio

Library

Search by Name

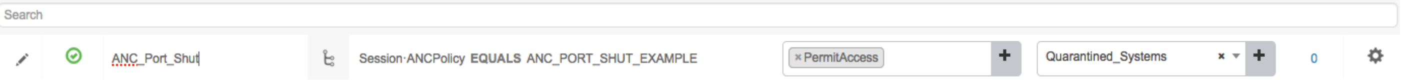
BYOD_is_Registered

Editor

Session·ANCPolicy

Equals — ANC_PORT_SHUT_EXAMPLE

Step 18 Select **Use**
Step 19 Rename rule name to **ANC_Port_Shut**



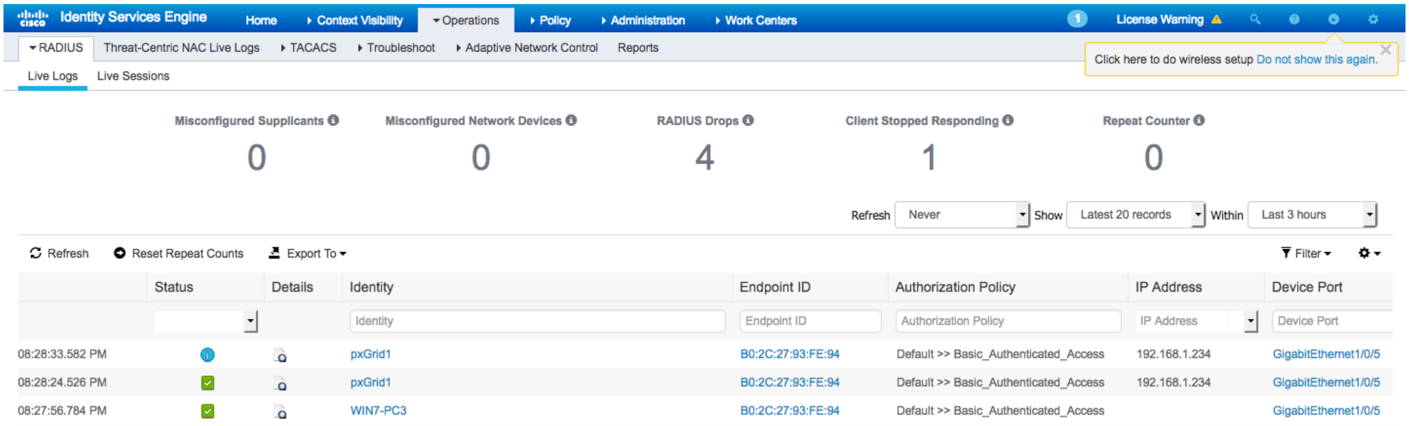
Rule Name	Conditions	Profiles	Security Groups	Hits
ANC_Port_Shut	Session·ANCPolicy EQUALS ANC_PORT_SHUT_EXAMPLE	× PermitAccess	Quarantined_Systems	0

Step 20 Select **Save**
Step 21 Follow Steps 21-28 to create the ANC_Port_Bounce Global Exception Authorization Policy Rule

Stealthwatch Quarantine Example

In this example, the endpoint is automatically quarantined by assigning the endpoint to the ANC_QUARANTINE_EXAMPLE policy

Step 1 User Authenticates to ISE

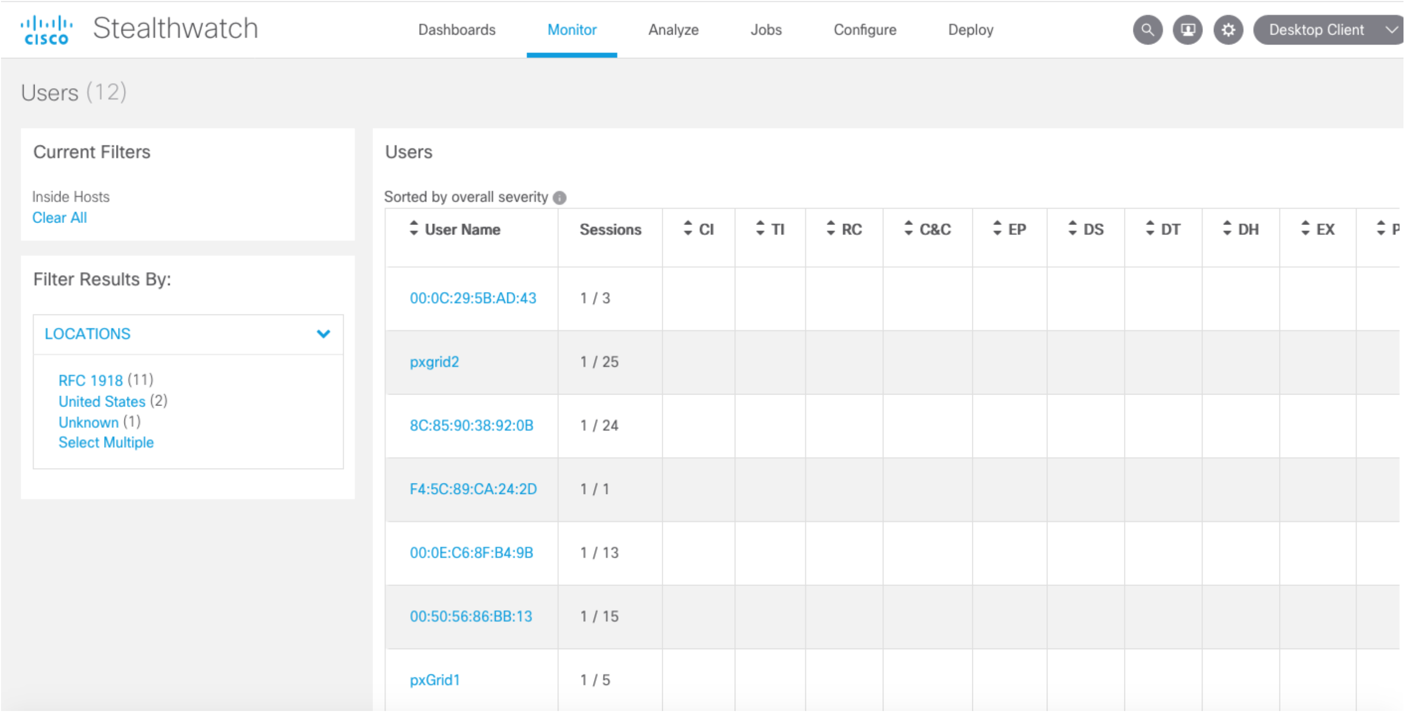


Misconfigured Supplicants	Misconfigured Network Devices	RADIUS Drops	Client Stopped Responding	Repeat Counter
0	0	4	1	0

Refresh Never Show Latest 20 records Within Last 3 hours

	Status	Details	Identity	Endpoint ID	Authorization Policy	IP Address	Device Port
08:28:33.582 PM	ⓘ		pxGrid1	B0:2C:27:93:FE:94	Default >> Basic_Authenticated_Access	192.168.1.234	GigabitEthernet1/0/5
08:28:24.526 PM	✓		pxGrid1	B0:2C:27:93:FE:94	Default >> Basic_Authenticated_Access	192.168.1.234	GigabitEthernet1/0/5
08:27:56.784 PM	✓		WIN7-PC3	B0:2C:27:93:FE:94	Default >> Basic_Authenticated_Access		GigabitEthernet1/0/5

Step 2 Select **Monitor->Users**, you will see the following:



Users (12)

Current Filters

Inside Hosts
Clear All

Filter Results By:

LOCATIONS

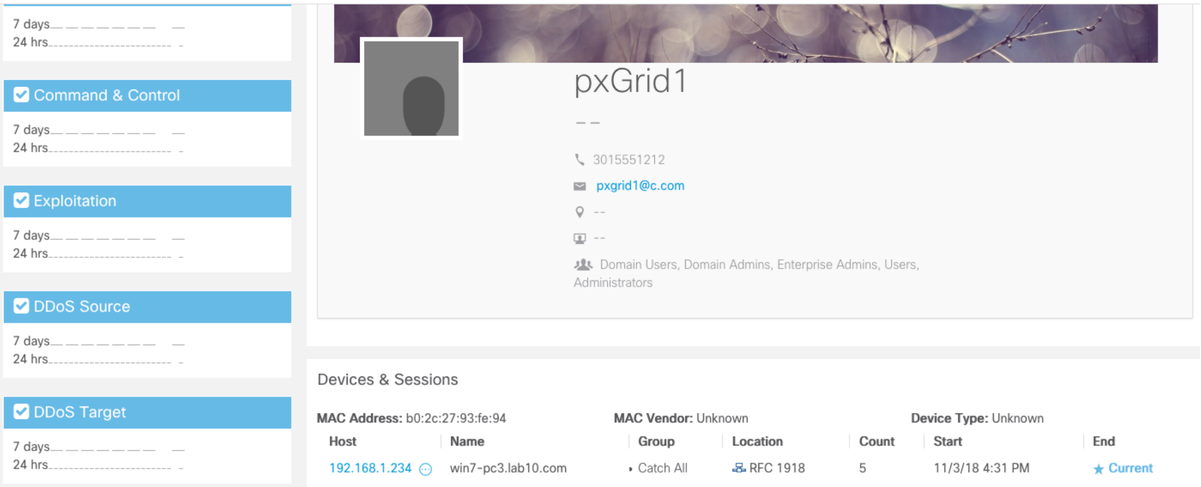
RFC 1918 (11)
United States (2)
Unknown (1)
Select Multiple

Users

Sorted by overall severity

User Name	Sessions	CI	TI	RC	C&C	EP	DS	DT	DH	EX	P
00:0C:29:5B:AD:43	1 / 3										
pxgrid2	1 / 25										
8C:85:90:38:92:0B	1 / 24										
F4:5C:89:CA:24:2D	1 / 1										
00:0E:C6:8F:B4:9B	1 / 13										
00:50:56:86:BB:13	1 / 15										
pxGrid1	1 / 5										

Step 3 We select **pxGrid1**



pxGrid1

--

☎ 3015551212

pxgrid1@c.com

--

--

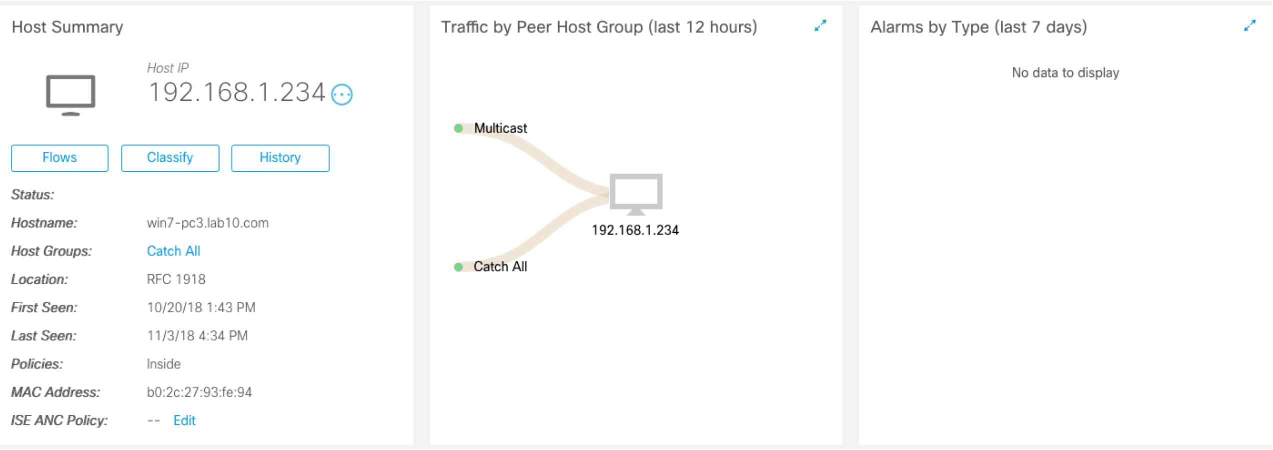
Domain Users, Domain Admins, Enterprise Admins, Users, Administrators

Devices & Sessions

MAC Address: b0:2c:27:93:fe:94 **MAC Vendor:** Unknown **Device Type:** Unknown

Host	Name	Group	Location	Count	Start	End
192.168.1.234	win7-pc3.lab10.com	Catch All	RFC 1918	5	11/3/18 4:31 PM	★ Current

Step 4 Select the host **192.168.1.234**



Host Summary

Host IP
192.168.1.234

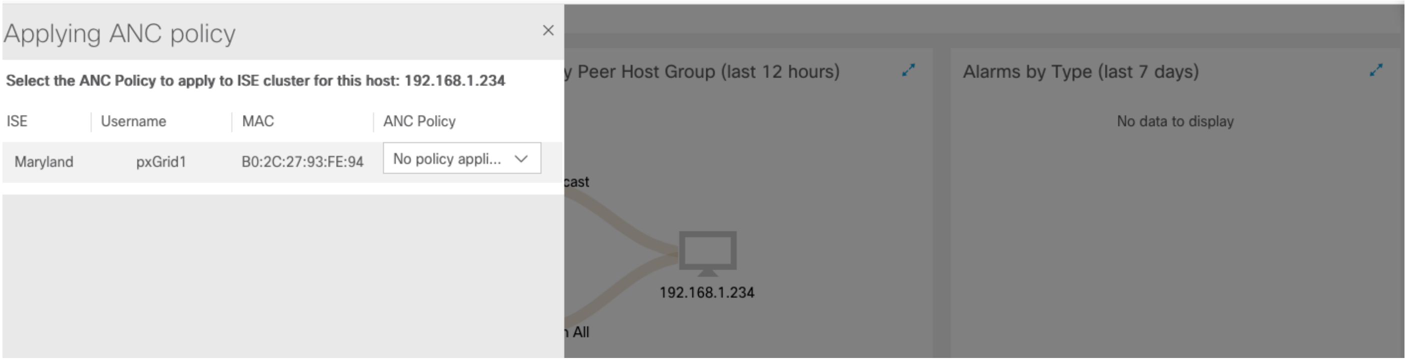
Status:	
Hostname:	win7-pc3.lab10.com
Host Groups:	Catch All
Location:	RFC 1918
First Seen:	10/20/18 1:43 PM
Last Seen:	11/3/18 4:34 PM
Policies:	Inside
MAC Address:	b0:2c:27:93:fe:94
ISE ANC Policy:	-- Edit

Traffic by Peer Host Group (last 12 hours)

Alarms by Type (last 7 days)

No data to display

Step 5 Select **Edit** for the **ISE ANC Policy,** you should see:



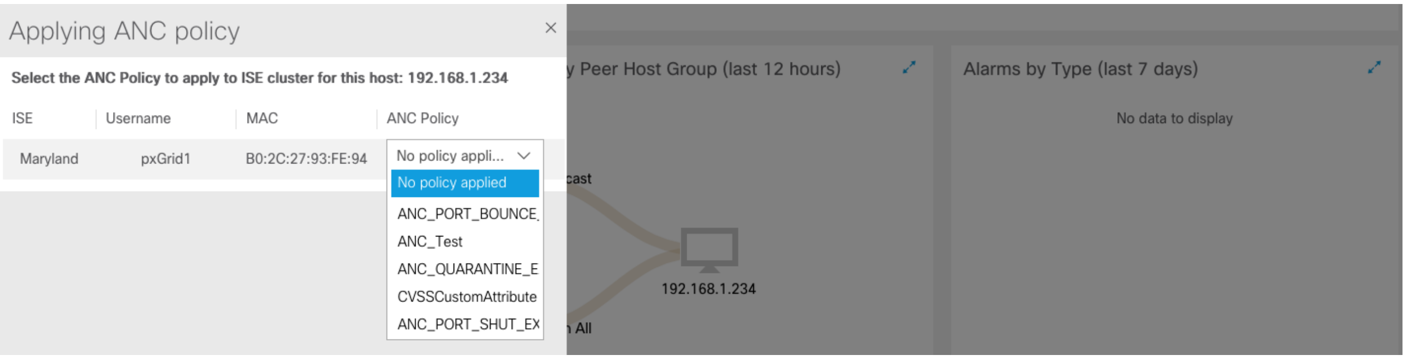
Applying ANC policy ×

Select the ANC Policy to apply to ISE cluster for this host: 192.168.1.234

ISE	Username	MAC	ANC Policy
Maryland	pxGrid1	B0:2C:27:93:FE:94	No policy appli... ⌄

y Peer Host Group (last 12 hours)
Alarms by Type (last 7 days)
No data to display
cast
192.168.1.234
All

Step 6 From the **ANC Policy** drop down menu, you should see all the ISE ANC policies

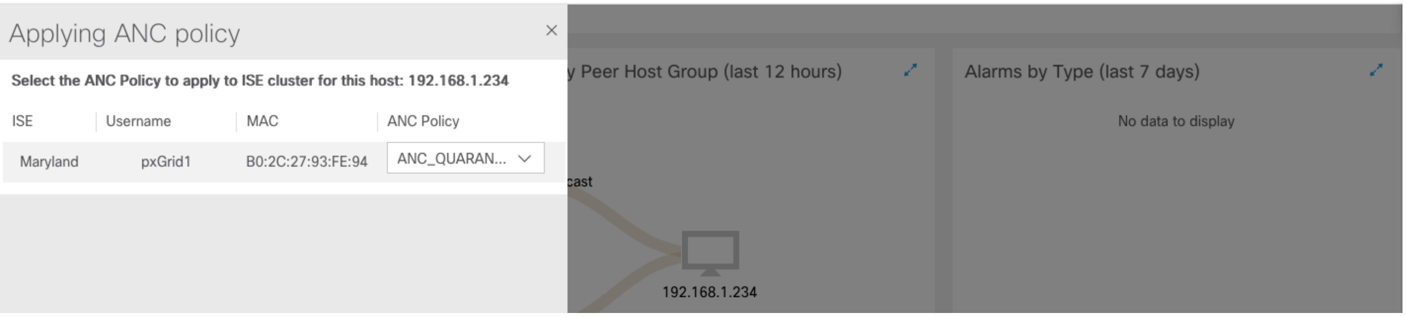


Applying ANC policy

Select the ANC Policy to apply to ISE cluster for this host: 192.168.1.234

ISE	Username	MAC	ANC Policy
Maryland	pxGrid1	B0:2C:27:93:FE:94	No policy appli...

Step 7 Select **ANC_QUARANTINE_EXAMPLE** policy



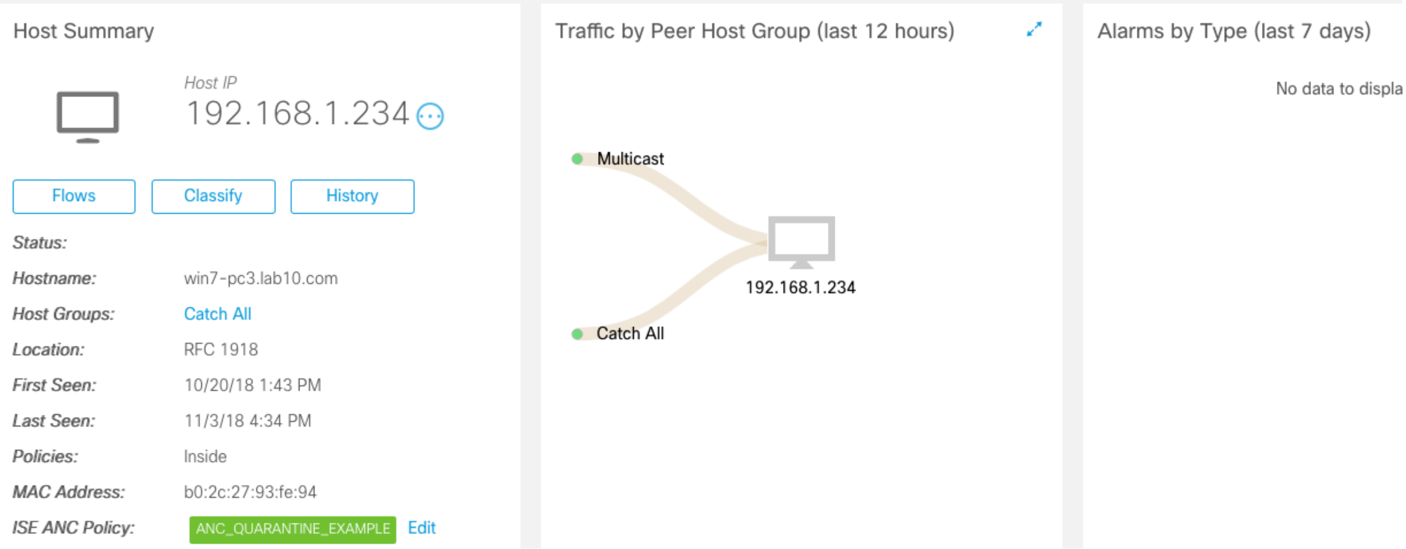
Applying ANC policy

Select the ANC Policy to apply to ISE cluster for this host: 192.168.1.234

ISE	Username	MAC	ANC Policy
Maryland	pxGrid1	B0:2C:27:93:FE:94	ANC_QUARAN...

×
y Peer Host Group (last 12 hours)
Alarms by Type (last 7 days)
No data to display
cast
192.168.1.234

Step 8 Select **Save**
You should see:



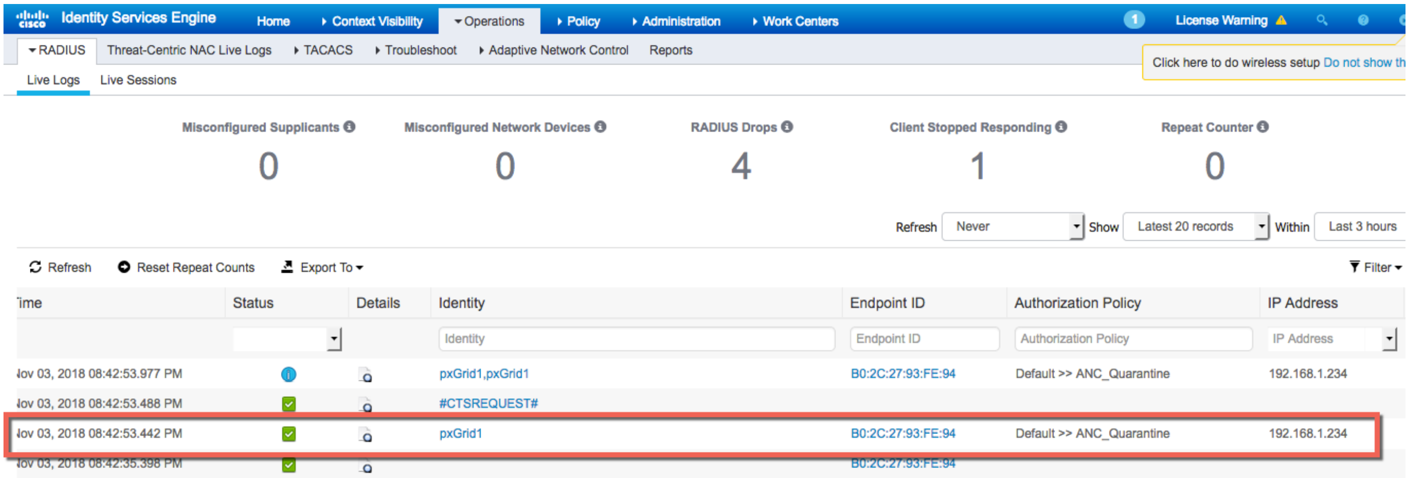
Host Summary

Host IP
192.168.1.234

Flows
Classify
History
Traffic by Peer Host Group (last 12 hours)
Multicast
192.168.1.234
Catch All
Alarms by Type (last 7 days)
No data to displa

Status:
Hostname: win7-pc3.lab10.com
Host Groups: Catch All
Location: RFC 1918
First Seen: 10/20/18 1:43 PM
Last Seen: 11/3/18 4:34 PM
Policies: Inside
MAC Address: b0:2c:27:93:fe:94
ISE ANC Policy: ANC_QUARANTINE_EXAMPLE Edit

Step 9 Go to ISE, select **Operations->RADIUS->Live Logs**

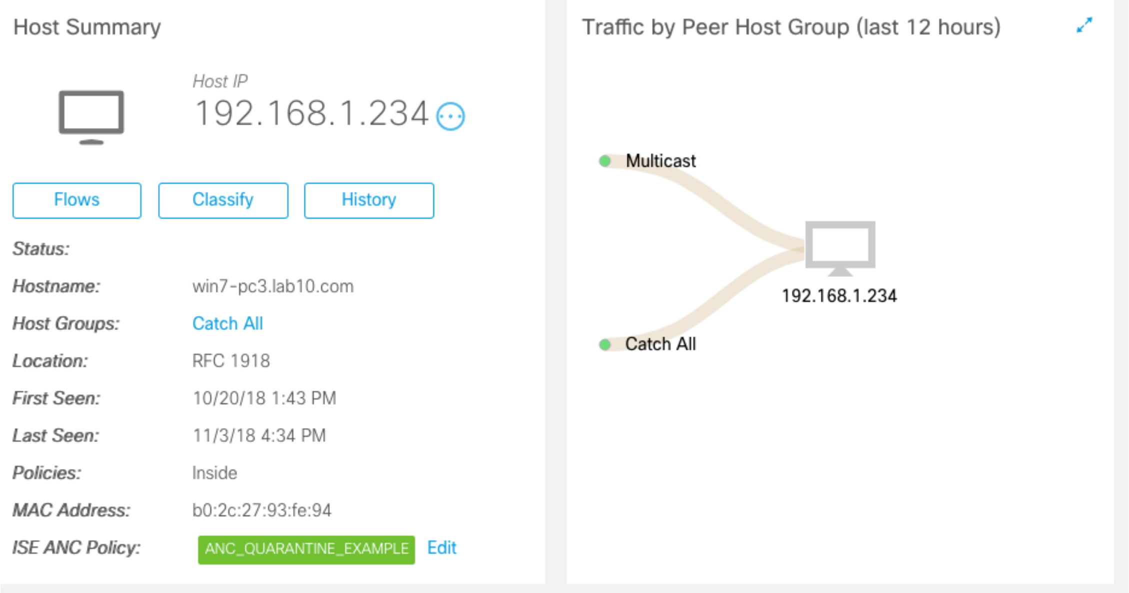


Misconfigured Supplicants	Misconfigured Network Devices	RADIUS Drops	Client Stopped Responding	Repeat Counter
0	0	4	1	0

Refresh Never Show Latest 20 records Within Last 3 hours

ime	Status	Details	Identity	Endpoint ID	Authorization Policy	IP Address
lov 03, 2018 08:42:53.977 PM	●		pxGrid1,pxGrid1	B0:2C:27:93:FE:94	Default >> ANC_Quarantine	192.168.1.234
lov 03, 2018 08:42:53.488 PM	✓		#CTSREQUEST#			
lov 03, 2018 08:42:53.442 PM	✓		pxGrid1	B0:2C:27:93:FE:94	Default >> ANC_Quarantine	192.168.1.234
lov 03, 2018 08:42:35.398 PM	✓			B0:2C:27:93:FE:94		

Step 10 To unquarantine the endpoint



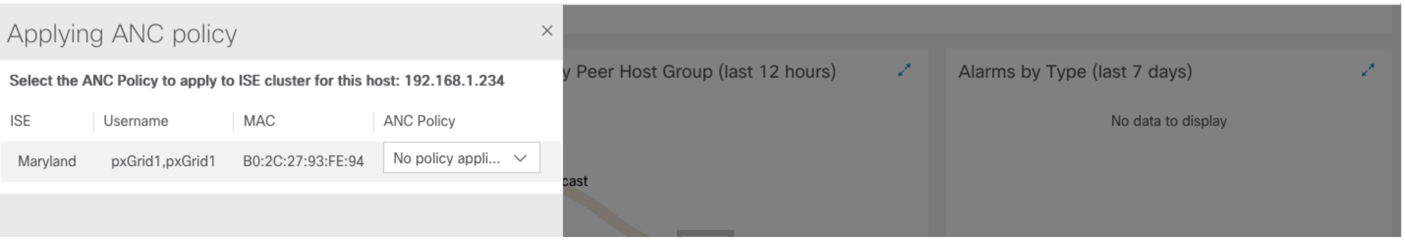
Host Summary

Host IP
192.168.1.234

Status:
Hostname: win7-pc3.lab10.com
Host Groups: Catch All
Location: RFC 1918
First Seen: 10/20/18 1:43 PM
Last Seen: 11/3/18 4:34 PM
Policies: Inside
MAC Address: b0:2c:27:93:fe:94
ISE ANC Policy: ANC_QUARANTINE_EXAMPLE Edit

Step 11 Select **Edit**

Step 12 From the drop-down select "**No policy applied**"

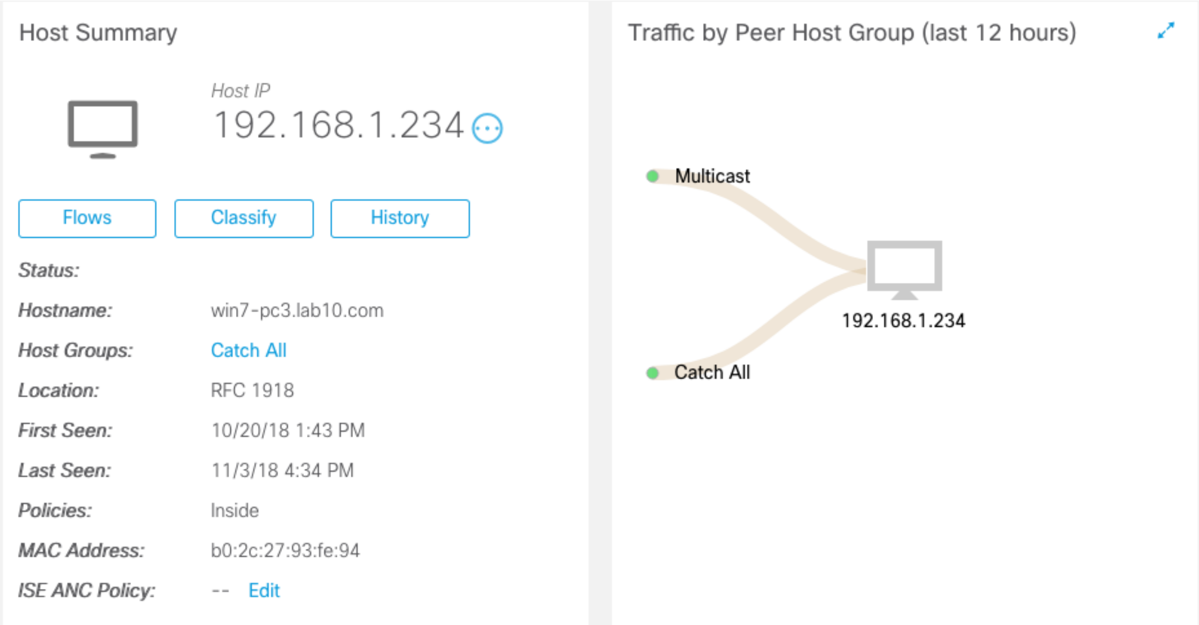

y Peer Host Group (last 12 hours)
Alarms by Type (last 7 days)
No data to display
cast

Applying ANC policy

Select the ANC Policy to apply to ISE cluster for this host: 192.168.1.234

ISE	Username	MAC	ANC Policy
Maryland	pxGrid1,pxGrid1	B0:2C:27:93:FE:94	No policy appli...

Step 13 Select **Save**, you should see:



Host Summary

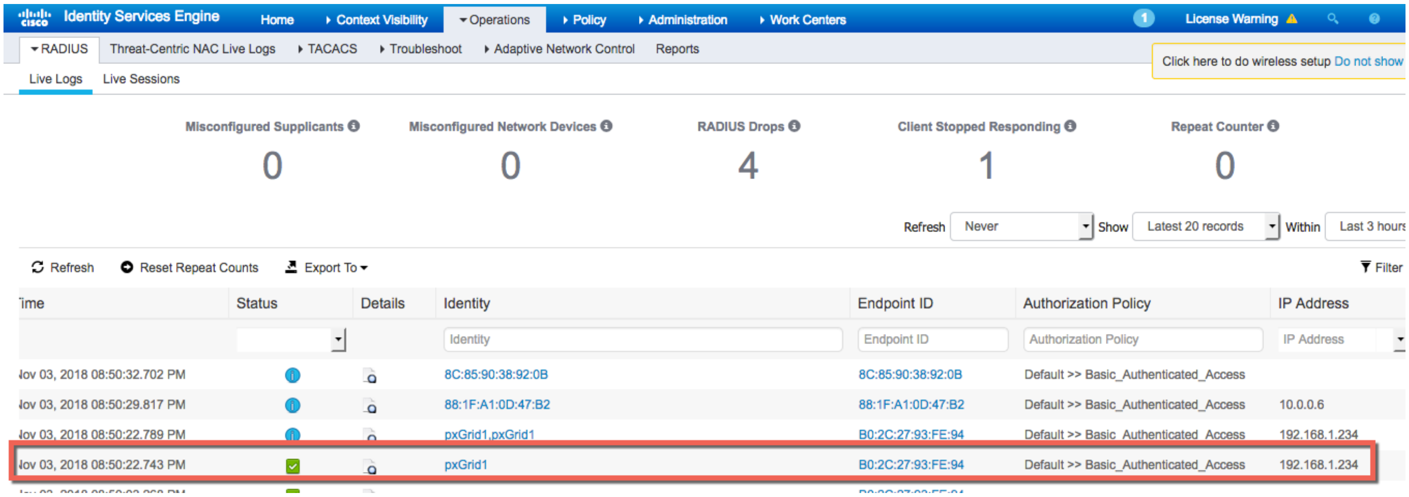
Host IP
192.168.1.234

Flows | Classify | History

Status:
Hostname: win7-pc3.lab10.com
Host Groups: Catch All
Location: RFC 1918
First Seen: 10/20/18 1:43 PM
Last Seen: 11/3/18 4:34 PM
Policies: Inside
MAC Address: b0:2c:27:93:fe:94
ISE ANC Policy: -- Edit

Traffic by Peer Host Group (last 12 hours)

Step 14 Goto ISE, select **Operations->RADIUS->Live Logs**, the endpoint should be unquarantined



Misconfigured Supplicants	Misconfigured Network Devices	RADIUS Drops	Client Stopped Responding	Repeat Counter
0	0	4	1	0

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

ime	Status	Details	Identity	Endpoint ID	Authorization Policy	IP Address
lov 03, 2018 08:50:32.702 PM	ⓘ	🔍	8C:85:90:38:92:0B	8C:85:90:38:92:0B	Default >> Basic_Authenticated_Access	
lov 03, 2018 08:50:29.817 PM	ⓘ	🔍	88:1F:A1:0D:47:B2	88:1F:A1:0D:47:B2	Default >> Basic_Authenticated_Access	10.0.0.6
lov 03, 2018 08:50:22.789 PM	ⓘ	🔍	pxGrid1,pxGrid1	B0:2C:27:93:FE:94	Default >> Basic_Authenticated_Access	192.168.1.234
lov 03, 2018 08:50:22.743 PM	✓	🔍	pxGrid1	B0:2C:27:93:FE:94	Default >> Basic_Authenticated_Access	192.168.1.234

Cisco TrustSec Software-Defined Segmentation

Stealthwatch 7.0 makes use of TrustSec segmentation through Security Group Tags (SGT) and SGT Exchange Protocol (SXP). SGT are labels that are assigned to users, endpoint devices based on the ISE authorization policies. They may be statically assigned to endpoints such as servers and other entities as well and are used by TrustSec capable devices to make forwarding decisions. In this document, we will be using Cisco Catalyst 3750-X Switch and ASA 5506-X.

Security Group Tag is a unique 16 bit tag that is assigned a unique role. It represents the privilege of the source user, device, or entity that is logged at the ingress of the Cisco TrustSec domain. Cisco TrutSec uses the device and user credentials acquired during authentication for classifying packets by security groups (SGs) as they enter the network. This packet classification is maintained by tagging packets on the ingress to the Cisco TrustSec network so that they may be identified for the purpose of applying security and other policy criteria in the data path. The SGT allows the network to enforce the access control policy by enabling the endpoint device to act upon the SGT to filter traffic.

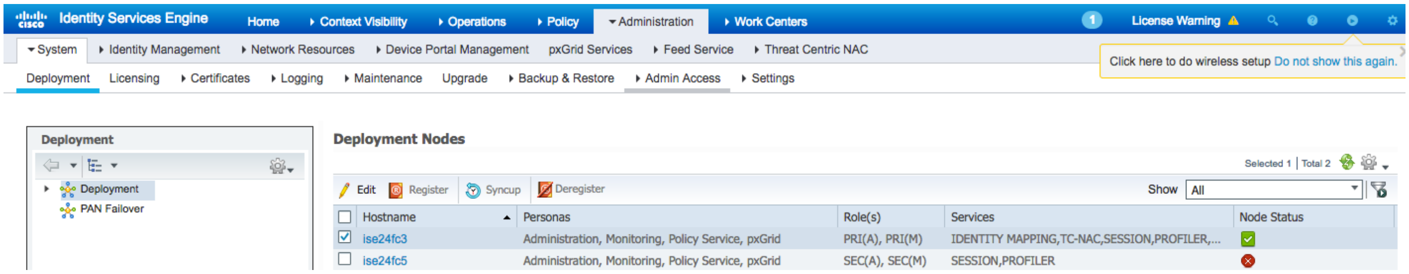
Cisco TrustSec Secure Group ACLs (SG-ACL) are used to allow or restrict network access based on source and destination SGTs based on business decisions.

The SGT Exchange Protocol (SXP) is a control protocol for propagating IP-to-SGT binding information across network devices that do not have hardware support for Cisco TrustSec. Cisco TrustSec filters packets at the egress interface. During the endpoint authentication, a host accessing the Cisco TrustSec domain (the endpoint IP address) is associated with an SGT at the access device through Dynamic Host Control Protocol (DHCP) snooping and IP device tracking. The access device transmits that association or binding through SXP to Cisco TrustSec hardware-capable egress devices. These devices maintain a table of source IP-to-SGT bindings. Packets are filtered on the egress interface by Cisco hardware-capable devices by applying security group access control lists (SG-ACLS). SXP passes IP-to-SGT bindings from authentication points to upstream devices in the network. This process allows security services on switches, routers, or firewalls to learn identity information.

ISE is enabled as an SXP listener and pxGrid is used to publish the SXP connection information such as the IP address, SGT-Tag, Source and Peer Sequences.

Enabling ISE as an SXP Listener

Step 1 Select **Administration->System->Deployment->edit the node**

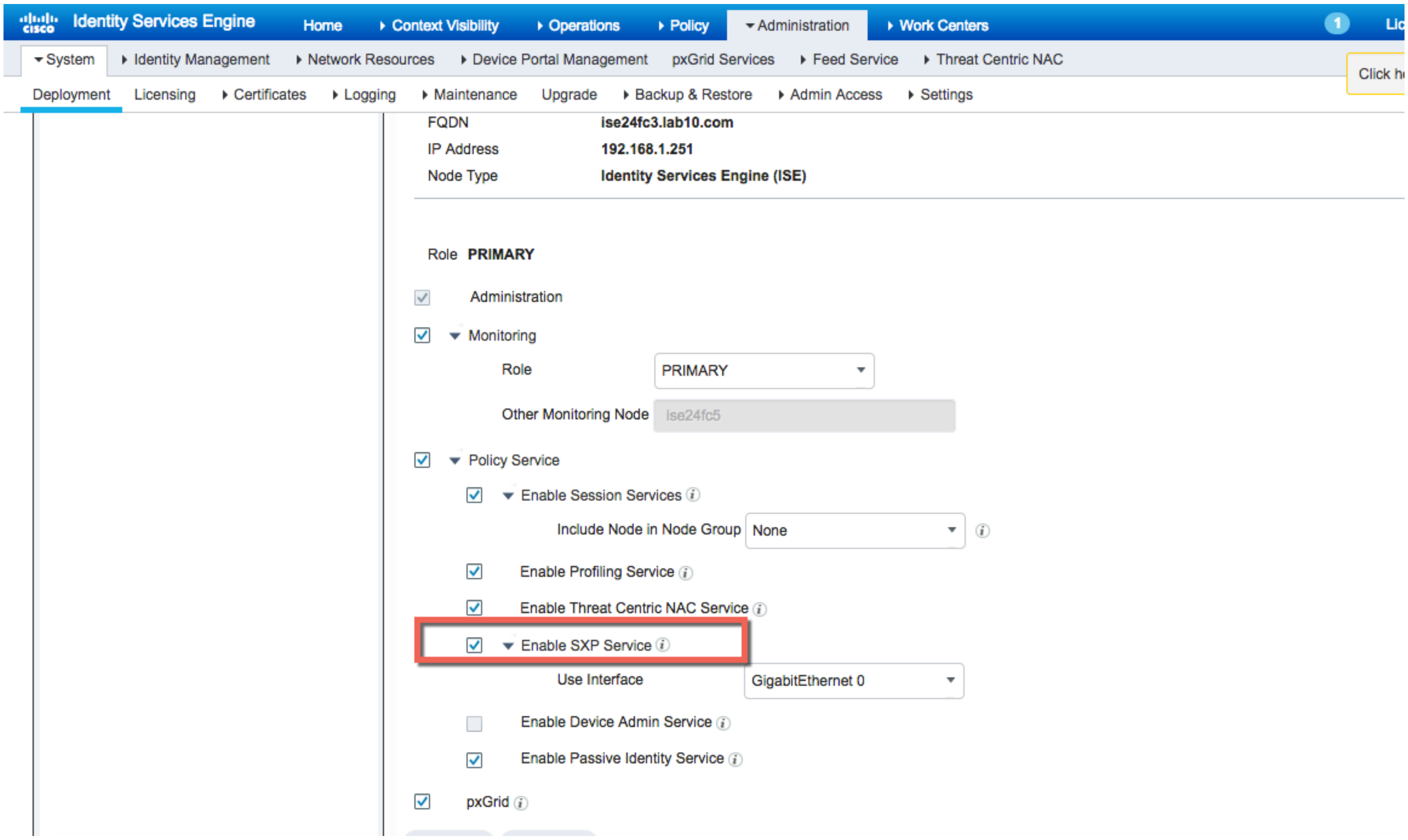


Deployment Nodes

Selected 1 | Total 2

☐	Hostname	Personas	Role(s)	Services	Node Status
☑	ise24fc3	Administration, Monitoring, Policy Service, pxGrid	PRI(A), PRI(M)	IDENTITY MAPPING,TC-NAC,SESSION,PROFILER,...	✓
☐	ise24fc5	Administration, Monitoring, Policy Service, pxGrid	SEC(A), SEC(M)	SESSION,PROFILER	✗

Step 2 **Enable** Enable SXP Service



FQDN ise24fc3.lab10.com

IP Address 192.168.1.251

Node Type Identity Services Engine (ISE)

Role PRIMARY

☑ Administration

☑ Monitoring

Role PRIMARY

Other Monitoring Node ise24fc5

☑ Policy Service

☑ Enable Session Services

Include Node in Node Group None

☑ Enable Profiling Service

☑ Enable Threat Centric NAC Service

☑ Enable SXP Service

Use Interface GigabitEthernet 0

☐ Enable Device Admin Service

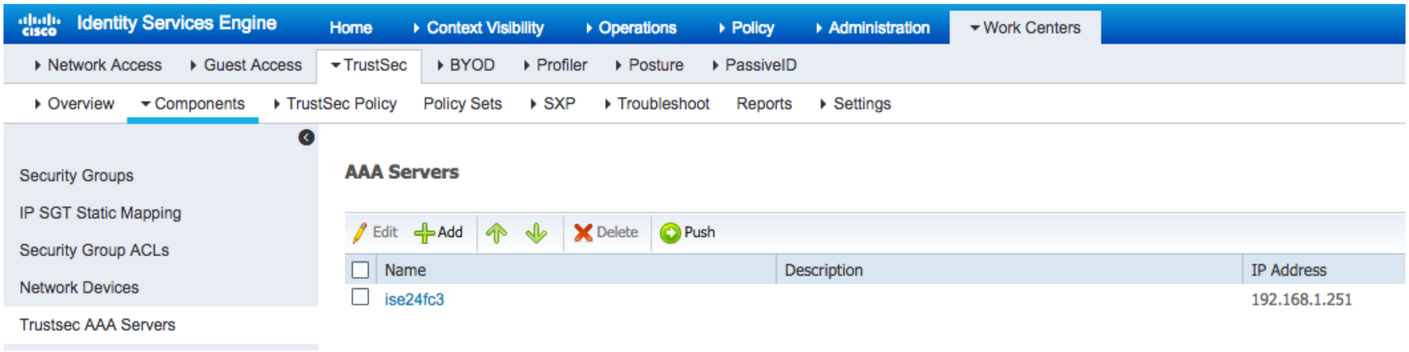
☑ Enable Passive Identity Service

☑ pxGrid

Step 3 Select **Save**

TrustSec AAA Devices

Step 1 Select **Work Centers->TrustSec->Components->Trustsec AAA Servers**
ISE will be configured as the AAA server



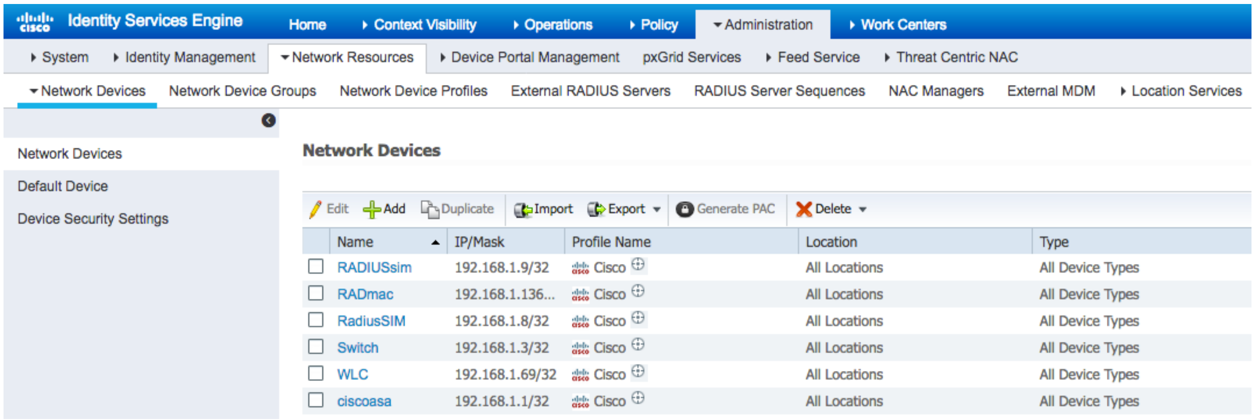
AAA Servers

☐ Name	Description	IP Address
☐ ise24fc3		192.168.1.251

Configure Network Devices for TrustSec

In this document I have configured the Cisco Catalyst 375x switch and the ASA 5506-X for TrustSec operation.

Step 1 Select **Work Centers->TrustSec->Components->Network Devices**



Network Devices

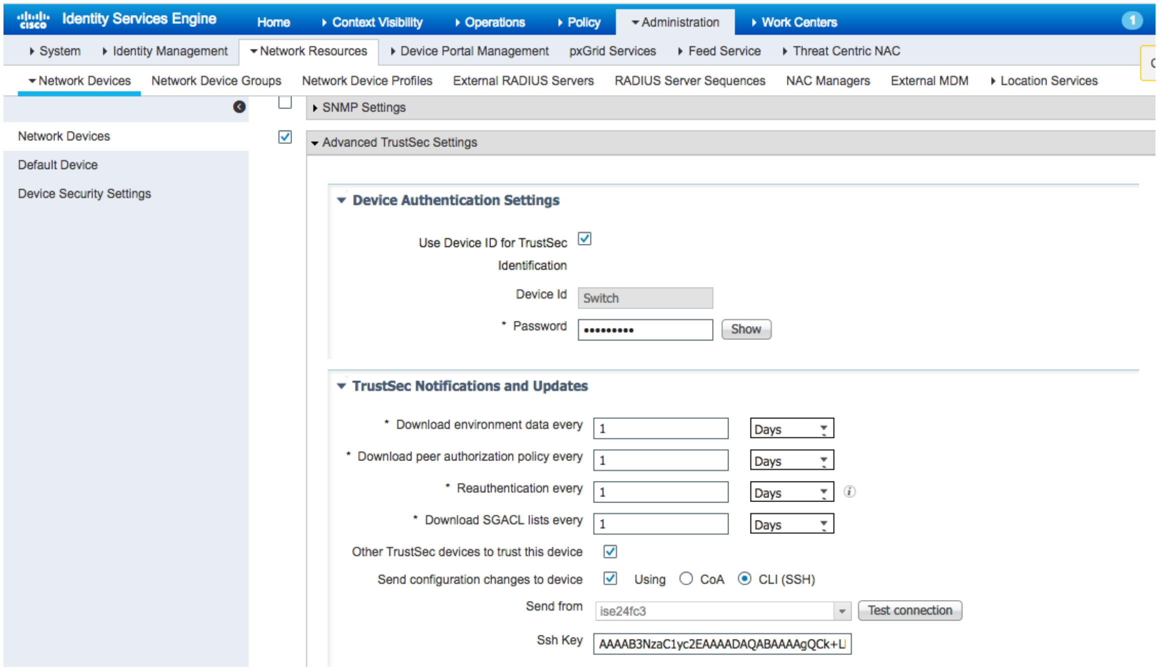
	Name	IP/Mask	Profile Name	Location	Type
□	RADIUSsim	192.168.1.9/32	Cisco	All Locations	All Device Types
□	RADmac	192.168.1.136...	Cisco	All Locations	All Device Types
□	RadiusSIM	192.168.1.8/32	Cisco	All Locations	All Device Types
□	Switch	192.168.1.3/32	Cisco	All Locations	All Device Types
□	WLC	192.168.1.69/32	Cisco	All Locations	All Device Types
□	ciscoasa	192.168.1.1/32	Cisco	All Locations	All Device Types

Step 2 Select **Work Centers->TrustSec->Components->Network Devices->select Switch->Edit->Enable->Advanced TrustSec Settings**

Step 3 Select **Use Device ID for Trustsec Identification**

Step 4 Select Send configuration changes to devices using CLI (SSH)

Note: You will need to know the SSH key. If you do not know the SSH key, you can delete the IP address of the device under the known-hosts file. When you ssh into the IP address of the device you will see the SSH key displayed. You can also use CoA if possible.



□ SNMP Settings

☑ Advanced TrustSec Settings

Device Authentication Settings

Use Device ID for TrustSec Identification ☑

Device Id: Switch

* Password: •••••••••

TrustSec Notifications and Updates

* Download environment data every: 1 Days

* Download peer authorization policy every: 1 Days

* Reauthentication every: 1 Days

* Download SGACL lists every: 1 Days

Other TrustSec devices to trust this device ☑

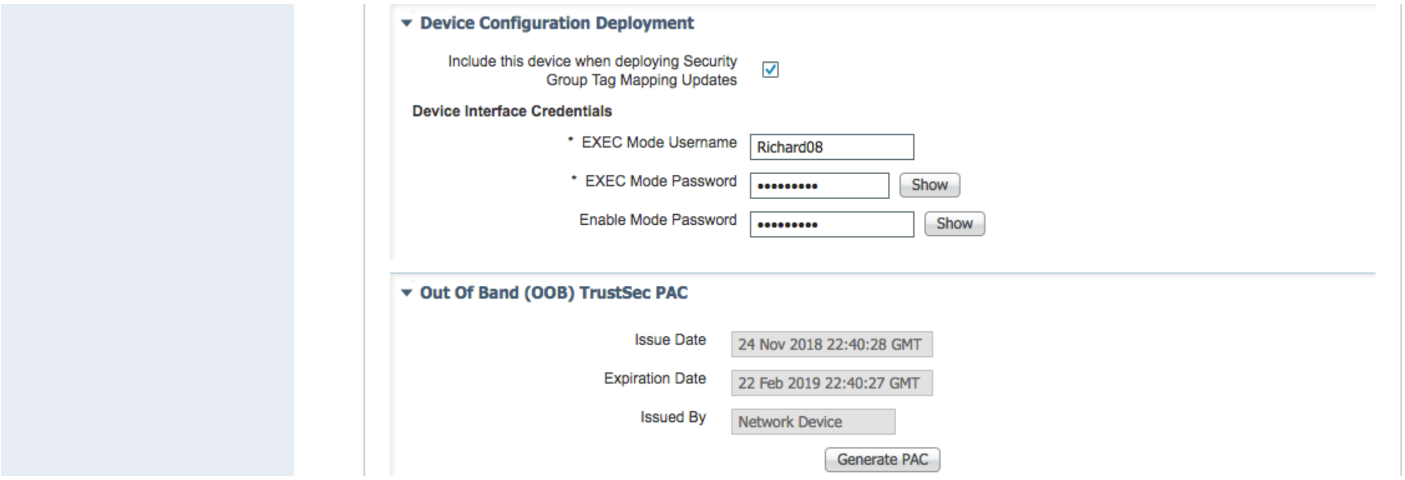
Send configuration changes to device ☑ Using ○ CoA ● CLI (SSH)

Send from: ise24fc3

Ssh Key: AAAAB3NzaC1yc2EAAAADAQABAAAAgQCk+L

Step 5 Under **Device Configuration Deployment->Enable->Include this device when deploying Security Group Tag Updates**

Step 6 Enter **Device Interface Credentials information**



▾ Device Configuration Deployment

Include this device when deploying Security Group Tag Mapping Updates ☑

Device Interface Credentials

* EXEC Mode Username: Richard08

* EXEC Mode Password: •••••••••

Enable Mode Password: •••••••••

▾ Out Of Band (OOB) TrustSec PAC

Issue Date: 24 Nov 2018 22:40:28 GMT

Expiration Date: 22 Feb 2019 22:40:27 GMT

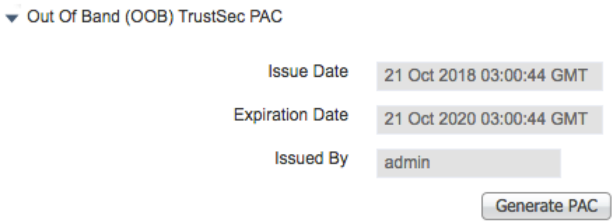
Issued By: Network Device

Step 7 The Cisco Catalyst 3750-X supports automatic PAC provisioning and uses the shared password. In order to have PAC use these credentials, enter the following:

```
Switch#cts credentials id Switch password Richard08
Switch#sh cts pacs
  AID: 19F065F78776F28731AEEC40C10F86F2
  PAC-Info:
    PAC-type = Cisco Trustsec
    AID: 19F065F78776F28731AEEC40C10F86F2
    I-ID: Switch
    A-ID-Info: Identity Services Engine
    Credential Lifetime: 17:40:28 UTC Feb 22 2019
  PAC-Opaque:
000200B0000300010004001019F065F78776F28731AEEC40C10F86F20006009400030100 0F654879EA539F3AD73D259783C36CB600000
0135BF8BDD100093A802FDEBE94618E6A40A7FCA02BE1F8910564996ED0A6212CA1C563C5D3E6F549E701FB65E83211B397E4D7FCB120
5C6CB279FB8BAFEAE79BEA68305D0324A180C7B7E84C752C033205344A075FBFD4D893698926920D6747863C79CD2F84788A46B2C3A5F
E53CA52CB5F4DBE9B694ADAFEFA10F80B
  Refresh timer is set for 25y51w
```

Step 8 The ASA supports only manual PAC provisioning. This means that you must generate it manually on ISE (Network Devices/ASA)

Note: Skip this step for the Cisco Catalyst 3750-X



▾ Out Of Band (OOB) TrustSec PAC

Issue Date: 21 Oct 2018 03:00:44 GMT

Expiration Date: 21 Oct 2020 03:00:44 GMT

Issued By: admin

Step 9 The PAC file must be installed on the ASA where password ‘Richard08’ is the CTS password

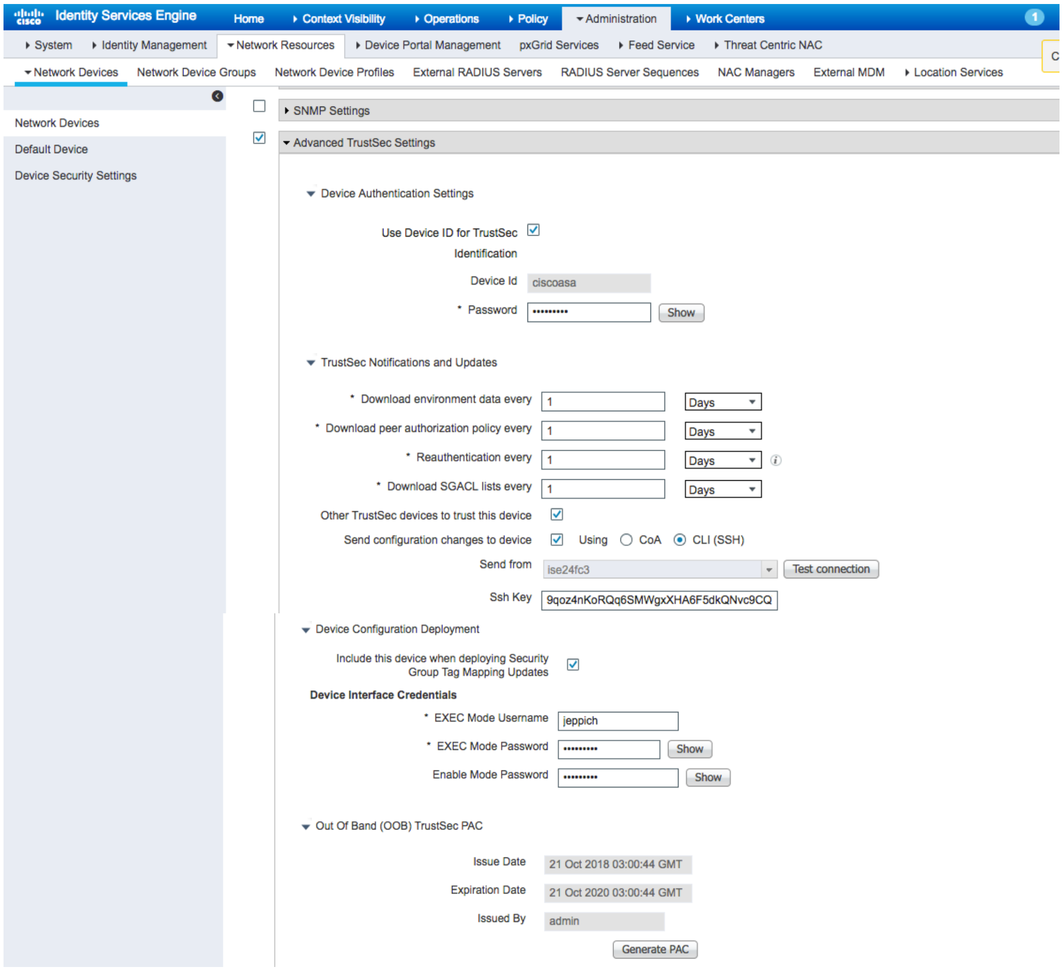
Note: Skip this step for Cisco Catalyst 3750-X

```
ciscoasa(config)# cts import ftp://john1:Richard08@192.168.1.233/ciscoasa.pac password Richard08

ciscoasa# sh cts pac

  PAC-Info:
    Valid until: Oct 21 2020 03:00:44
    AID:         19f065f78776f28731aeec40c10f86f2
    I-ID:        ciscoasa
    A-ID-Info:   Identity Services Engine
    PAC-type:    Cisco Trustsec
  PAC-Opaque:
    000200b00003000100040010 19f065f78776f28731aeec40c10f86f200060094000301
    00e827fa68b4c245ead849d4855028a5f5000000135bca995100093a80a4aa1dfb5eea
    f7d1ce82e422e758362b465c50d63a7b2e0cc7e039f872f9eebf26694e5d87b891bff5
    45a4dbf765bc3b2dc2487d7dd434aa05d77ad5f7a65088951b417aa6146bb159b62f98
    17e07b0c03fc91810e9fe93f7786b7aef7063cd2036b6f56dd1e638d2679e8d02d4de1
    470f4089da
```

Step 10 Follow steps 1-6 and 8,9 for configuring the ASA



□ SNMP Settings

☑ Advanced TrustSec Settings

Device Authentication Settings

Use Device ID for TrustSec Identification ☑

Device Id: ciscoasa

* Password: ••••••••••

TrustSec Notifications and Updates

* Download environment data every: 1 Days

* Download peer authorization policy every: 1 Days

* Reauthentication every: 1 Days

* Download SGACL lists every: 1 Days

Other TrustSec devices to trust this device ☑

Send configuration changes to device ☑ Using ○ CoA ● CLI (SSH)

Send from: ise24fc3

Ssh Key: 9qoz4nKoRQq6SMWgxXHA6F5dkQNvc9CQ

Device Configuration Deployment

Include this device when deploying Security Group Tag Mapping Updates ☑

Device Interface Credentials

* EXEC Mode Username: jeppich

* EXEC Mode Password: ••••••••••

Enable Mode Password: ••••••••••

Out Of Band (OOB) TrustSec PAC

Issue Date: 21 Oct 2018 03:00:44 GMT

Expiration Date: 21 Oct 2020 03:00:44 GMT

Issued By: admin

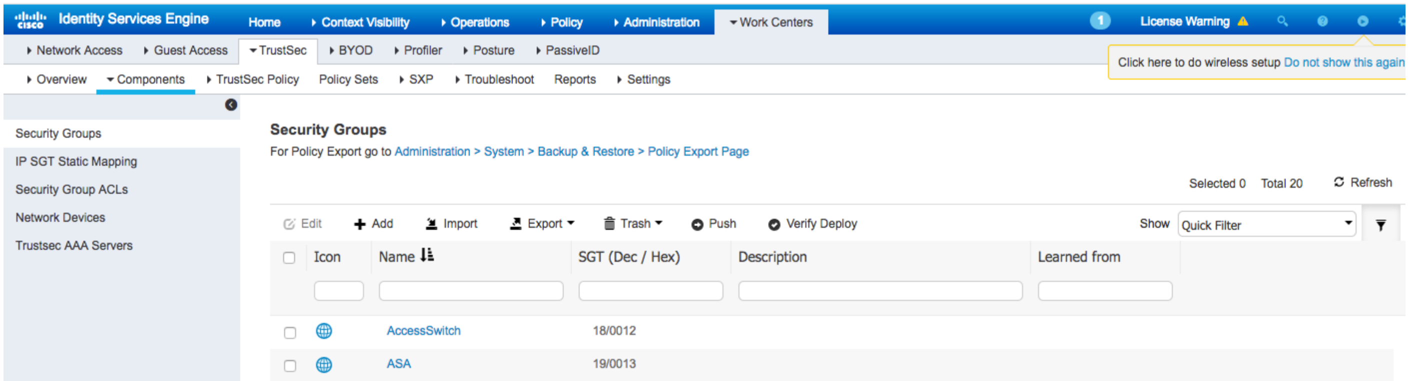
Configure Security Groups

Security Group Tags (SGT) were created for the Cisco Catalyst 3750-X, ASA 5506-X. Default SGT were used for Employees and Production_Servers

Step 1 Select **Work Centers->Components->Security Groups->Add AccessSwitch and ASA selecting Submit after each one.**

Step 2 AccessSwitch will represent the Cisco Catalyst 3750-X switch

Step 3 ASA will represent the ASA 5506-X.



Security Groups

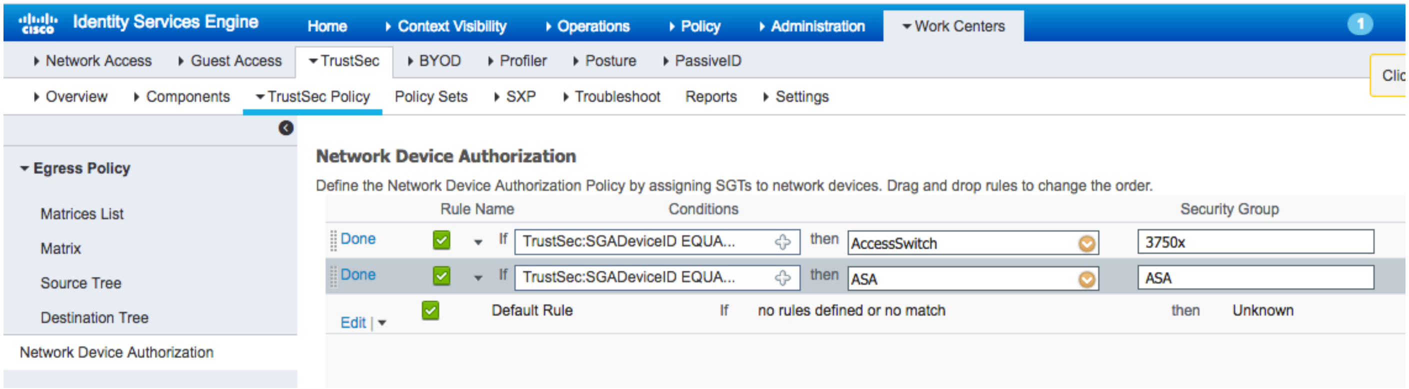
For Policy Export go to Administration > System > Backup & Restore > Policy Export Page

Icon	Name	SGT (Dec / Hex)	Description	Learned from
🌐	AccessSwitch	18/0012		
🌐	ASA	19/0013		

Configure Network Devices Authorization Policy

Two rules were created for the ASA 5506-X and Cisco Catalyst 3750-X security groups

Step 1 Select **Work Center->TrustSec->TrustSec Policy->Network Device Authorization->Add network device rules**



Network Device Authorization

Define the Network Device Authorization Policy by assigning SGTs to network devices. Drag and drop rules to change the order.

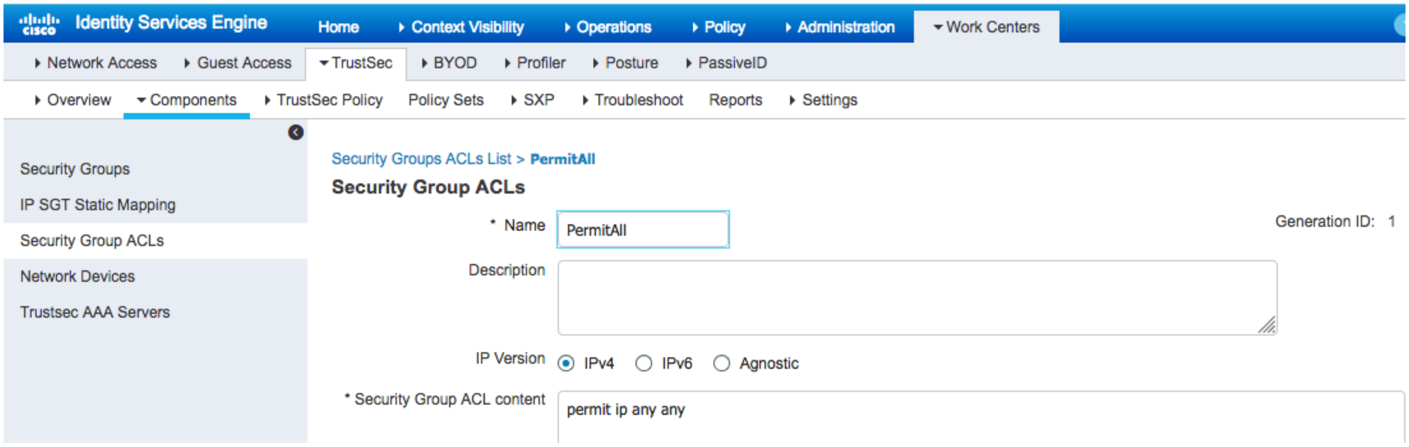
		Rule Name		Conditions		Security Group
Done	☑		If	TrustSec:SGADeviceID EQUA...	then AccessSwitch	3750x
Done	☑		If	TrustSec:SGADeviceID EQUA...	then ASA	ASA
Edit	☑	Default Rule	If	no rules defined or no match	then	Unknown

Step 2 Select **Save**

Define SG-ACLs

Step 1 Select **Work Centers->TrustSec->Components->Security Group ACLs->add->Name: permit all**

Step 2 Enter: **permit ip any any** for the Security Group ACL content



* Name: PermitAll

Generation ID: 1

Description:

IP Version: ● IPv4 ○ IPv6 ○ Agnostic

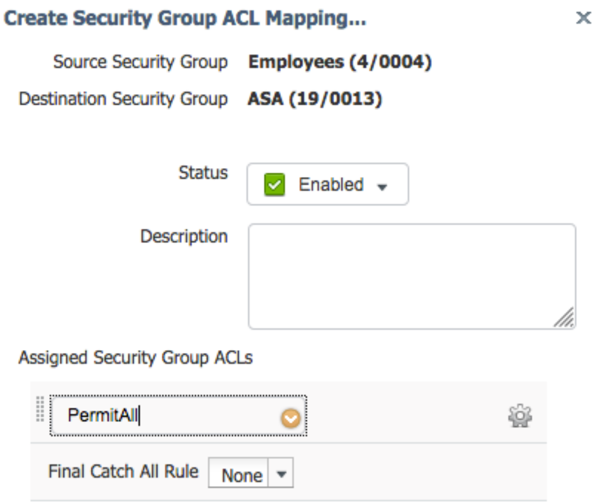
* Security Group ACL content: permit ip any any

Step 3 Select **Save**

Assign SG-ACLs to Egress Policy

SG-ACLs are assigned to the Egress policy matrix to allow the source to reach the destination SGT-based on the SG-ACL policy enforced on the TrustSec supported device. We define a SG-ACL rule to permit all traffic from the source Employee SGT group to the destination AccessSwitch, ASA and Production_Server SGT groups.

Step 1 Select **Work Centers->TrustSec->TrustSec Policy->Egress Policy->Source Tree->**Add the following



Source Security Group: Employees (4/0004)

Destination Security Group: ASA (19/0013)

Status: ☑ Enabled

Description:

Assigned Security Group ACLs: PermitAll

Final Catch All Rule: None

Step 2 Select **Save**

Step 3 Select **Add**

Step 4 Repeat for **Source Security Group:Employee** with **Destination Security Group: Production_Servers**, and **Permit All** for the SG-ACL

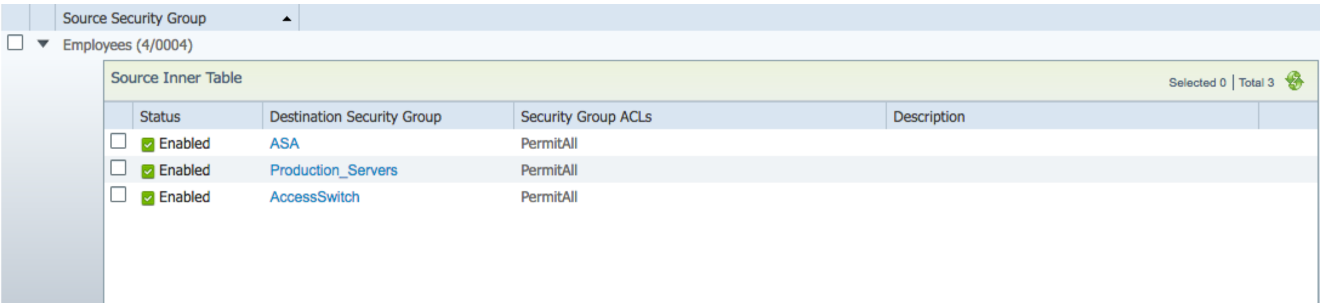
Step 5 Select **Save**

Step 6 Select **Add**

Step 7 Repeat for **Source Security Group:Employee** with **Destination Security Group: AccessSwitch**, and **Permit All** for the SG-ACL

Step 8 Select **Save**

You should see:



Source Security Group ▲

□ ▼ Employees (4/0004)

Source Inner Table — Selected 0 | Total 3

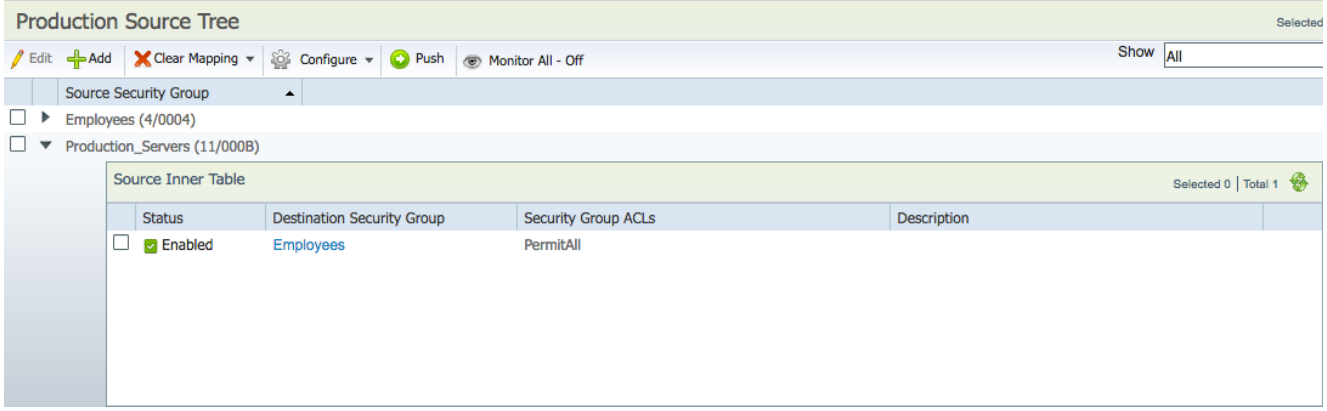
	Status	Destination Security Group	Security Group ACLs	Description
□	✓ Enabled	ASA	PermitAll	
□	✓ Enabled	Production_Servers	PermitAll	
□	✓ Enabled	AccessSwitch	PermitAll	

Step 9 Select **Add**

Step 10 For **Source Security Group: Production_Servers** with **Destination Security Group: Employees** and **Permit All** for the SG-ACL

Step 11 Select **Save**

You should see:



Production Source Tree — Selected

Show: All

Source Security Group ▲

□ ▶ Employees (4/0004)

□ ▼ Production_Servers (11/000B)

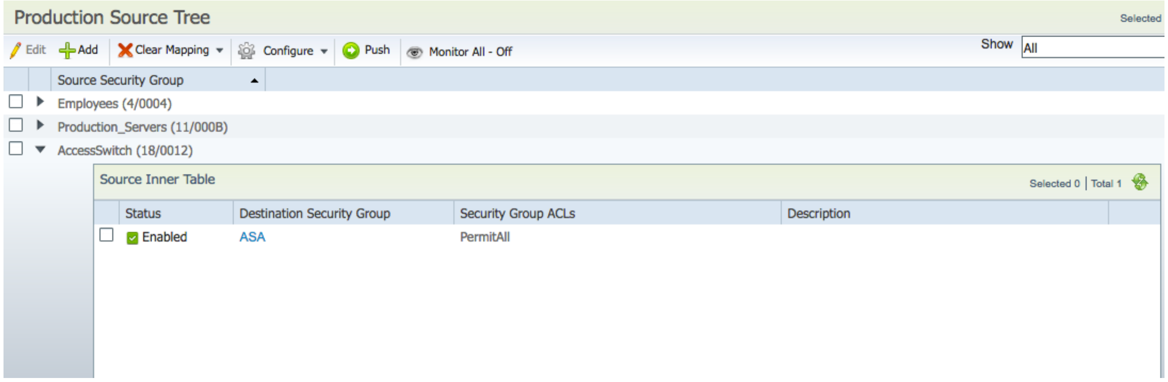
Source Inner Table — Selected 0 | Total 1

	Status	Destination Security Group	Security Group ACLs	Description
□	✓ Enabled	Employees	PermitAll	

Step 12 Select **Add**

Step 13 For **Source Security Group: AccessSwitch** with **Destination Security Group: ASA** and **Permit All** for the SG-ACL

Step 14 Select **Save**
You should see:



	Source Security Group
□	▸ Employees (4/0004)
□	▸ Production_Servers (11/000B)
□	▾ AccessSwitch (18/0012)

Source Inner Table

Selected 0 | Total 1

	Status	Destination Security Group	Security Group ACLs	Description
□	☑ Enabled	ASA	PermitAll	

Step 15 You can also select **Matrix**, and enter the cells directly

Configure SXP to allow distribution of IP to SGT mappings to non-TrustSec devices

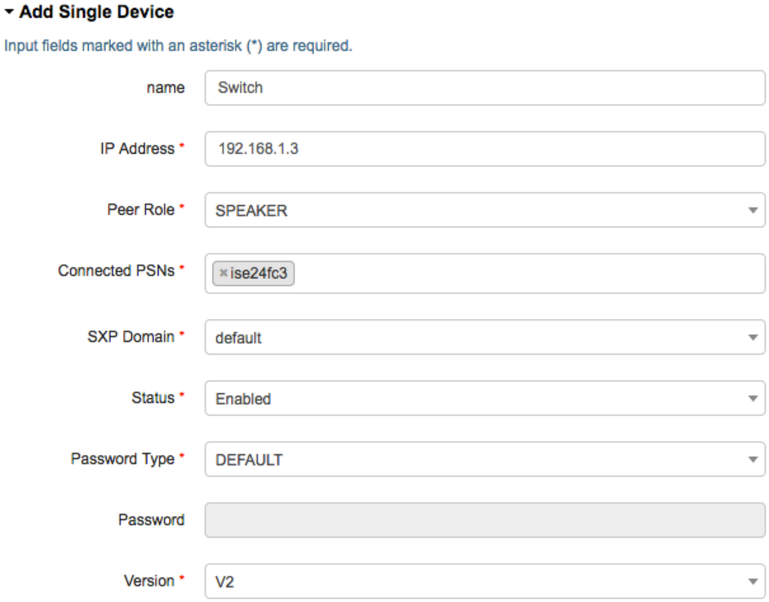
The SGT Exchange Protocol (SXP) is used to propagate the SGTs across network devices that do not have hardware support for TrustSec. SXP is used to transport an endpoint's SGT along with the IP address of the SGT from one SGT-aware network device to another, this is called the IP-SGT mapping. The SGT to which an endpoint belongs can be assigned statically or dynamically, and the SGT can be used as a classifier in network policies.

SXP uses TCP as its transport protocol to set up SXP connection between the two separate network devices. Each SXP connection has one peer designated as SXP speaker and the other as SXP listener. The peers can also be configured in a bi-directional mode where each of them acts as both speaker and listener. Connections can be initiated by either peers, but mapping information is always propagated from speaker to listener. Note session bindings are always propagated on the default SXP domain.

So the SXP speaker is the peer that sends the IP-SGT mappings over the SXP connection. The SXP listener is the peer that receives the IP-SGT mappings over the SXP connection and the IP-SGT mapping is the IP address to SGT mapping that is exchanged over the SXP connection.

The Cisco Catalyst 3750-X will be configured as the speaker for the peer role. The Cisco ASA will be configured as the listener for the peer role.

Step 1 Select **Work Centers->TrustSec->TrustSec Policy->SXP Devices->Add the following:**



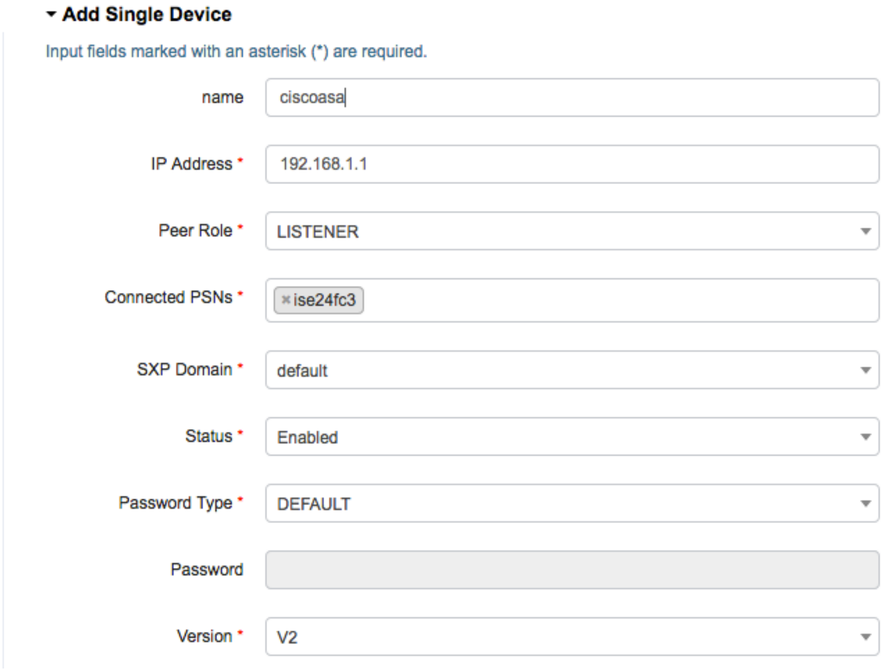
Add Single Device

Input fields marked with an asterisk (*) are required.

name	Switch
IP Address *	192.168.1.3
Peer Role *	SPEAKER
Connected PSNs *	× ise24fc3
SXP Domain *	default
Status *	Enabled
Password Type *	DEFAULT
Password	
Version *	V2

Step 2 Select **Save**

Step 3 Select **Add**

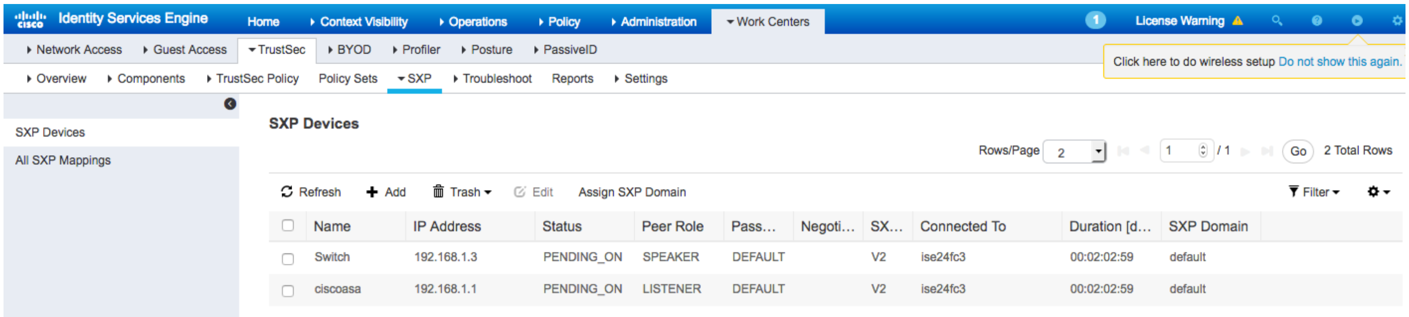


Add Single Device

Input fields marked with an asterisk (*) are required.

name	ciscoasa
IP Address *	192.168.1.1
Peer Role *	LISTENER
Connected PSNs *	× ise24fc3
SXP Domain *	default
Status *	Enabled
Password Type *	DEFAULT
Password	
Version *	V2

Step 4 Select **Save**
You should see:



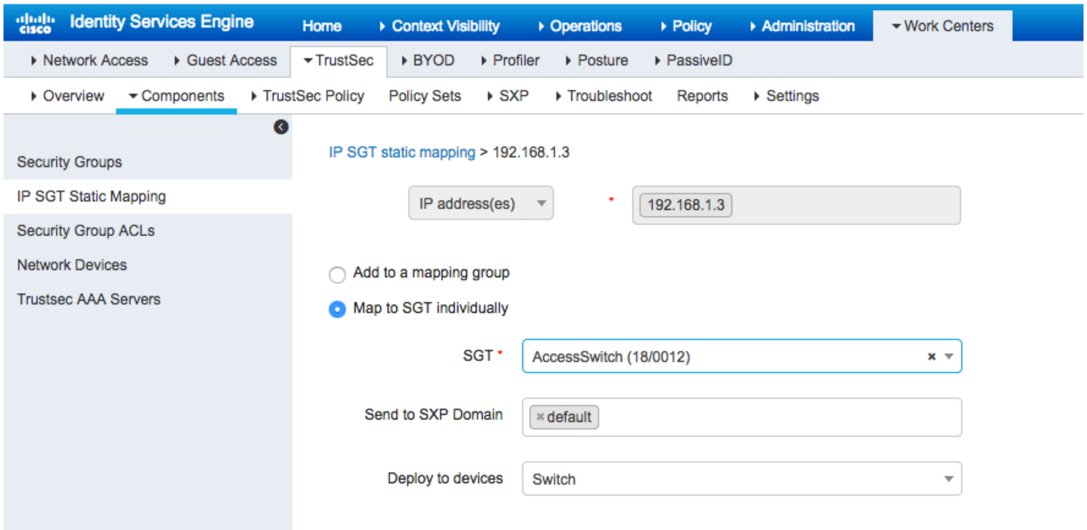
SXP Devices

□	Name	IP Address	Status	Peer Role	Pass…	Negoti…	SX…	Connected To	Duration [d…	SXP Domain
□	Switch	192.168.1.3	PENDING_ON	SPEAKER	DEFAULT		V2	ise24fc3	00:02:02:59	default
□	ciscoasa	192.168.1.1	PENDING_ON	LISTENER	DEFAULT		V2	ise24fc3	00:02:02:59	default

Assign Static Mappings

We assign the IP-SGT mappings manually to the Cisco Catalyst Switch, which is assigned the AccessSwitch SGT and the to the server, which is assigned the Production_Server SGT, using the default SXP domain.

Step 1 Select **Work Centers->TrustSec->Components->IP SGT Mapping** and assign **AccessSwitch SGT** to the IP address of the switch



IP SGT static mapping > 192.168.1.3

IP address(es) * 192.168.1.3

○ Add to a mapping group

● Map to SGT individually

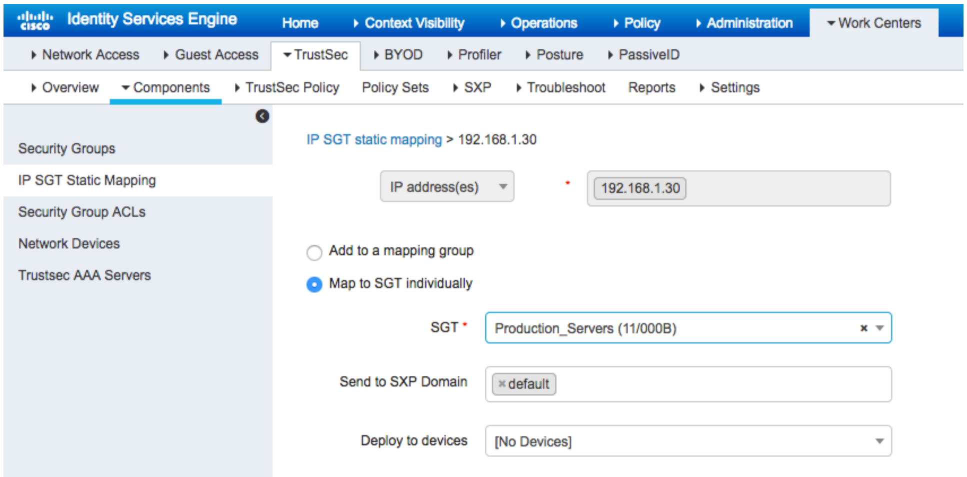
SGT * AccessSwitch (18/0012)

Send to SXP Domain: default

Deploy to devices: Switch

Step 2 Select **Save**

Step 3 Select **Work Centers->TrustSec->Components->IP SGT Mapping** and assign **Production_Server SGT** to the IP address of the server



IP SGT static mapping > 192.168.1.30

IP address(es) * 192.168.1.30

○ Add to a mapping group

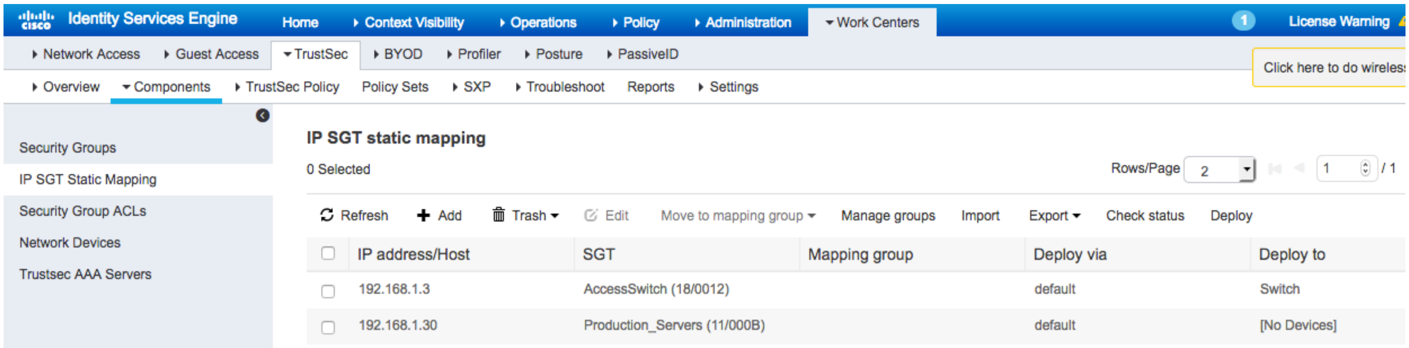
● Map to SGT individually

SGT * Production_Servers (11/000B)

Send to SXP Domain: default

Deploy to devices: [No Devices]

Step 4 Select **Save**
You should see:



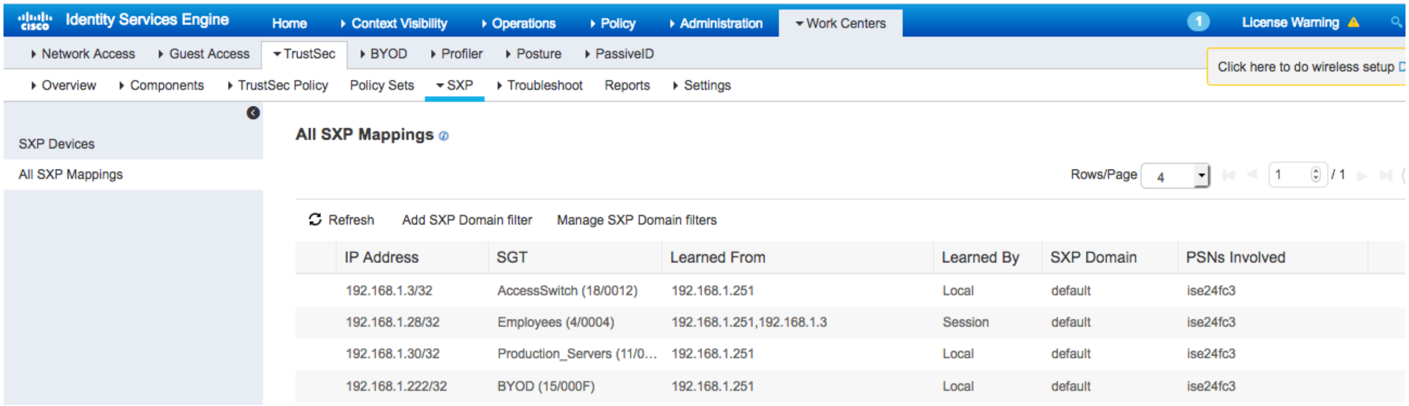
IP SGT static mapping

0 Selected

Rows/Page 2 | 1 / 1

	IP address/Host	SGT	Mapping group	Deploy via	Deploy to
□	192.168.1.3	AccessSwitch (18/0012)		default	Switch
□	192.168.1.30	Production_Servers (11/000B)		default	[No Devices]

Step 5 Select **Work Centers->TrustSec->SXP-> define the static mappings of the network device**



All SXP Mappings

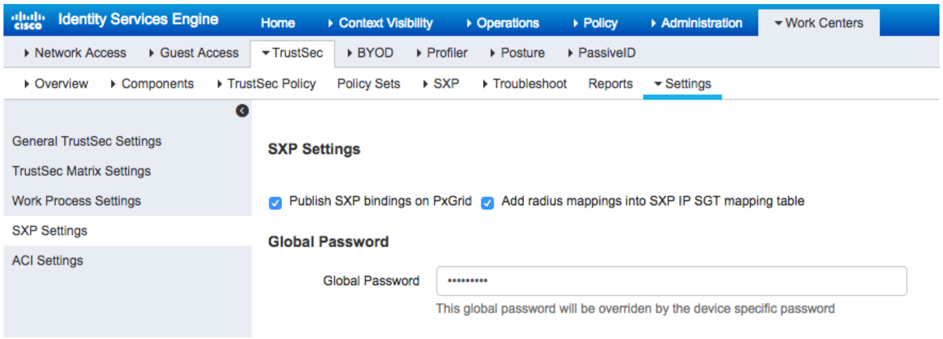
Rows/Page 4 | 1 / 1

IP Address	SGT	Learned From	Learned By	SXP Domain	PSNs Involved
192.168.1.3/32	AccessSwitch (18/0012)	192.168.1.251	Local	default	ise24fc3
192.168.1.28/32	Employees (4/0004)	192.168.1.251,192.168.1.3	Session	default	ise24fc3
192.168.1.30/32	Production_Servers (11/0...	192.168.1.251	Local	default	ise24fc3
192.168.1.222/32	BYOD (15/000F)	192.168.1.251	Local	default	ise24fc3

Publish SXP Bindings on pxGrid

The SXP bindings are published on pxGrid and the radius mappings into SXP IP SGT mapping table are added.

Step 1 Select **Work Centers->TrustSec->Settings->Enable Publish SXP bindings on pxGrid**
Step 2 **Enable->Add radius mappings into SXP IP SGT mapping table**
Step 3 **Enter Global Password**



SXP Settings

☑ Publish SXP bindings on PxGrid ☑ Add radius mappings into SXP IP SGT mapping table

Global Password

Global Password ••••••••••

This global password will be overriden by the device specific password

Step 4 Select **Save**

Analyzing Flow Records

Stealthwatch 7.0 includes Cisco TrustSec Security Group Tag (SGT) names and ID numbers as Subject TrustSec Name, Subject TrustSec ID as the source and the Peer TrustSec Name, and Peer TrustSec ID as the destination or peer.

In the example below, pxGrid1 has an Employee Security Group Tag assigned to it based on the ISE authorization policy and an authorization condition rule of pxGrid1 belonging to the /domain/users group.

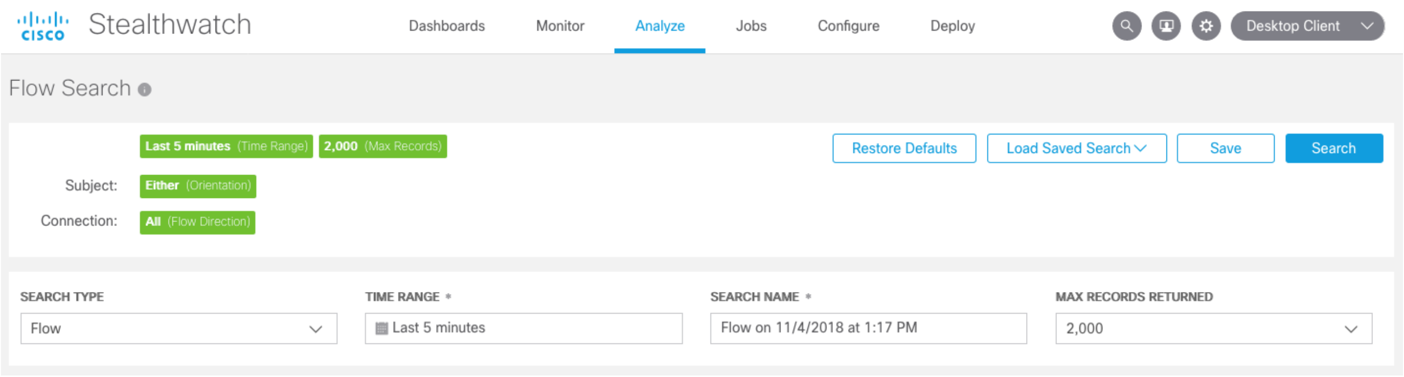
A server has been statically assigned a Production Server Security Group Tag based on its IP address.

Before we begin, we need to enable the Subject TrustSec Name, Subject TrustSec ID, Peer Trustsec Names, and Peer TrustSec ID columns in the flow records.

Enabling TrustSec Columns for Flow Records

Enable the Subject TrutSec Name, Subject TrustSec ID, Peer TrustSeec Name, and Peer TrustSec ID columns to appear in flow records.

Step 1 Select **Analyze->Flow Search**, you should see



Flow Search

Last 5 minutes (Time Range) 2,000 (Max Records)

Subject: Either (Orientation)

Connection: All (Flow Direction)

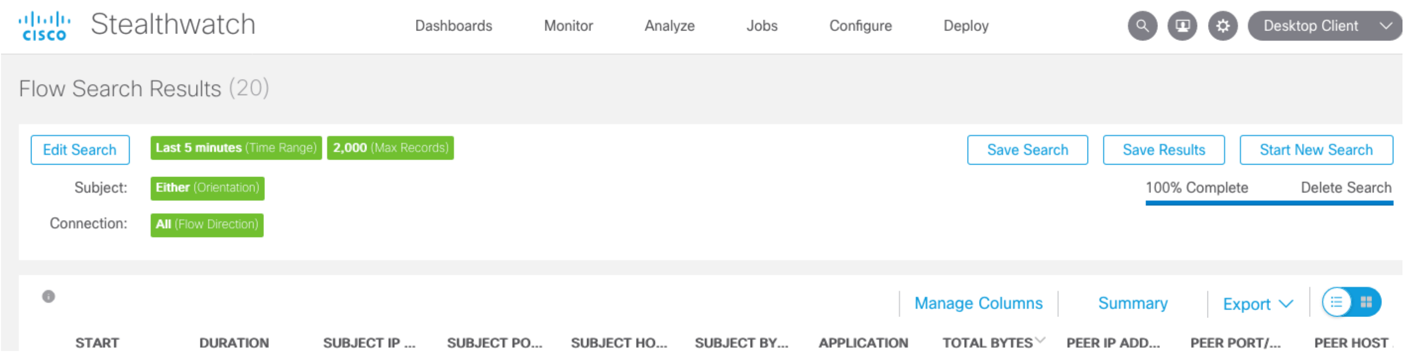
SEARCH TYPE: Flow

TIME RANGE *: Last 5 minutes

SEARCH NAME *: Flow on 11/4/2018 at 1:17 PM

MAX RECORDS RETURNED: 2,000

Step 2 Select **Search,** you should see:



Flow Search Results (20)

Last 5 minutes (Time Range) 2,000 (Max Records)

Subject: Either (Orientation)

Connection: All (Flow Direction)

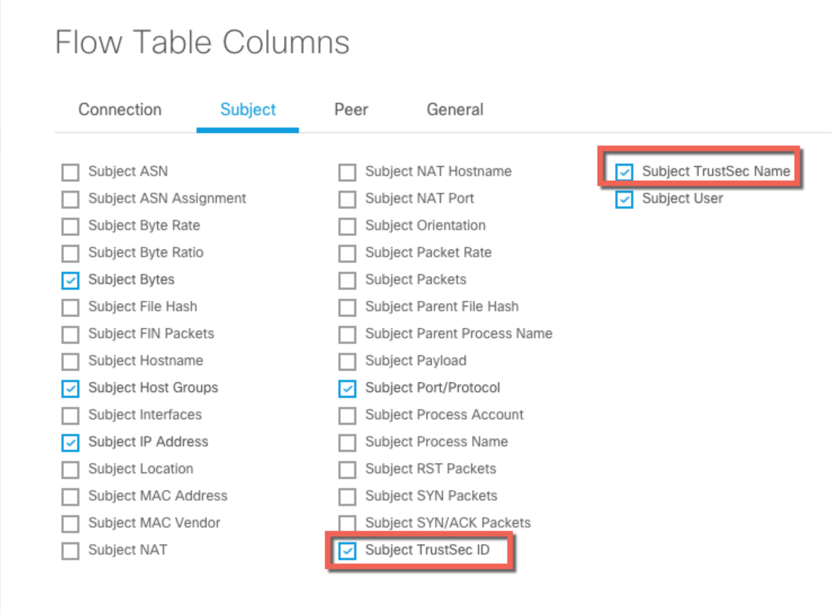
100% Complete

START | DURATION | SUBJECT IP ... | SUBJECT PO... | SUBJECT HO... | SUBJECT BY... | APPLICATION | TOTAL BYTES | PEER IP ADD... | PEER PORT/... | PEER HOST

Step 3 Select **Manage Columns**

Step 4 Select **Subject**

Step 5 Enable the following: **Subject TrustSec ID**, **Subject TrustSec Name**



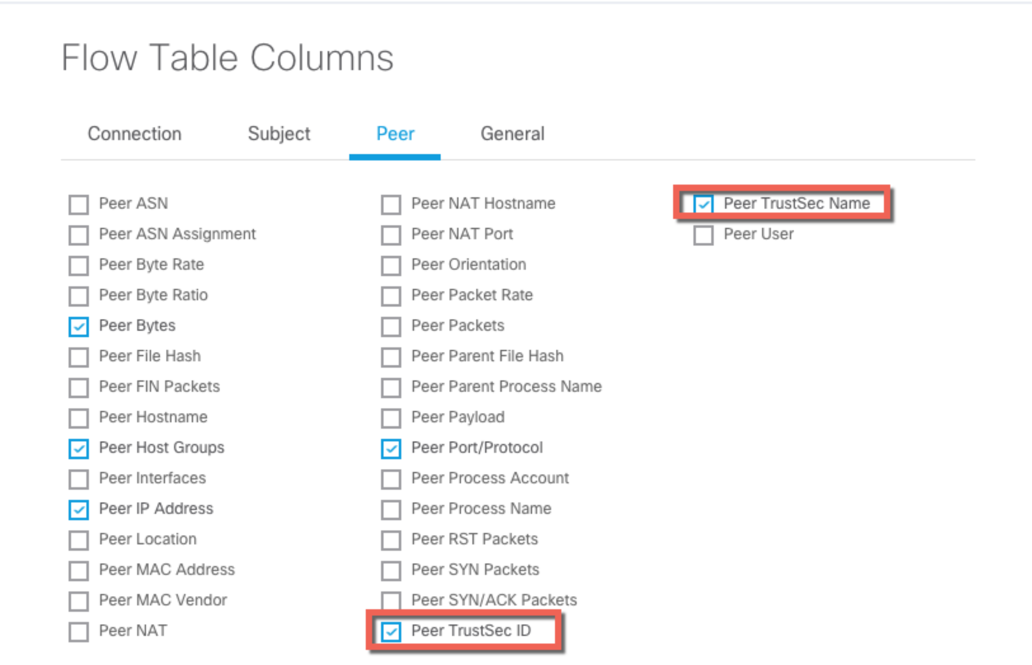
Flow Table Columns

Connection | Subject | Peer | General

- □ Subject ASN
- □ Subject ASN Assignment
- □ Subject Byte Rate
- □ Subject Byte Ratio
- ☑ Subject Bytes
- □ Subject File Hash
- □ Subject FIN Packets
- □ Subject Hostname
- ☑ Subject Host Groups
- □ Subject Interfaces
- ☑ Subject IP Address
- □ Subject Location
- □ Subject MAC Address
- □ Subject MAC Vendor
- □ Subject NAT
- □ Subject NAT Hostname
- □ Subject NAT Port
- □ Subject Orientation
- □ Subject Packet Rate
- □ Subject Packets
- □ Subject Parent File Hash
- □ Subject Parent Process Name
- □ Subject Payload
- ☑ Subject Port/Protocol
- □ Subject Process Account
- □ Subject Process Name
- □ Subject RST Packets
- □ Subject SYN Packets
- □ Subject SYN/ACK Packets
- ☑ Subject TrustSec ID
- ☑ Subject TrustSec Name
- ☑ Subject User

Step 6 Select **Peer**

Enable the following: **Peer TrustSec Name**, **Peer TrustSec ID**



Flow Table Columns

Connection | Subject | Peer | General

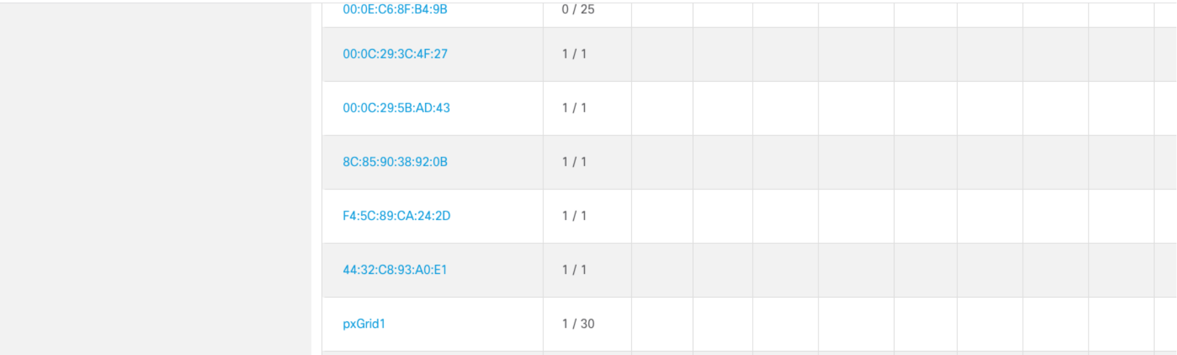
- □ Peer ASN
- □ Peer ASN Assignment
- □ Peer Byte Rate
- □ Peer Byte Ratio
- ☑ Peer Bytes
- □ Peer File Hash
- □ Peer FIN Packets
- □ Peer Hostname
- ☑ Peer Host Groups
- □ Peer Interfaces
- ☑ Peer IP Address
- □ Peer Location
- □ Peer MAC Address
- □ Peer MAC Vendor
- □ Peer NAT
- □ Peer NAT Hostname
- □ Peer NAT Port
- □ Peer Orientation
- □ Peer Packet Rate
- □ Peer Packets
- □ Peer Parent File Hash
- □ Peer Parent Process Name
- □ Peer Payload
- ☑ Peer Port/Protocol
- □ Peer Process Account
- □ Peer Process Name
- □ Peer RST Packets
- □ Peer SYN Packets
- □ Peer SYN/ACK Packets
- ☑ Peer TrustSec ID
- ☑ Peer TrustSec Name
- □ Peer User

Step 7 Select **Set**

Viewing TrustSec SGTs in Flow Records

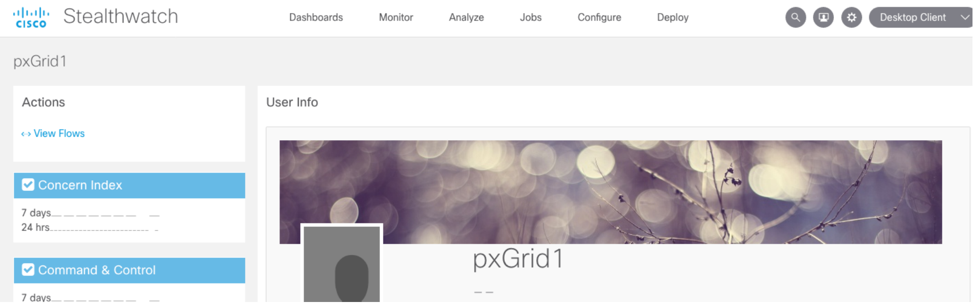
In this example, we will view the network flow between the user pxGrid1, which has a Subject TrustSec Name of Employee and a Subject Trustsec ID of 4 sharing a network connection with a server with a Peer TrustSec Name of Production_Server and a Peer TrustSec ID of 11.

Step 1 Select **Monitor->User,** you should see:



00:0E:C6:8F:B4:9B	0 / 25
00:0C:29:3C:4F:27	1 / 1
00:0C:29:5B:AD:43	1 / 1
8C:85:90:38:92:0B	1 / 1
F4:5C:89:CA:24:2D	1 / 1
44:32:C8:93:A0:E1	1 / 1
pxGrid1	1 / 30

Step 2 Select **pxGrid1**



pxGrid1

Actions

‹› View Flows

☑ Concern Index

7 days

24 hrs

☑ Command & Control

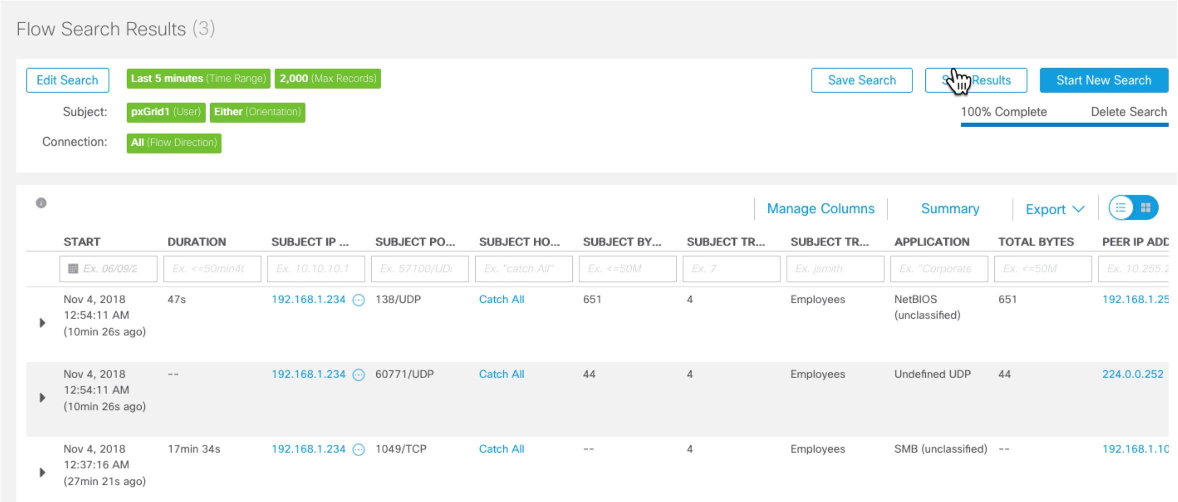
7 days

User Info

pxGrid1

--

Step 3 Select **View Flows**, note the Subject TrustSec ID of 4 and the Subject TrustSec Name of Employees



Flow Search Results (3)

Last 5 minutes (Time Range) **2,000** (Max Records)

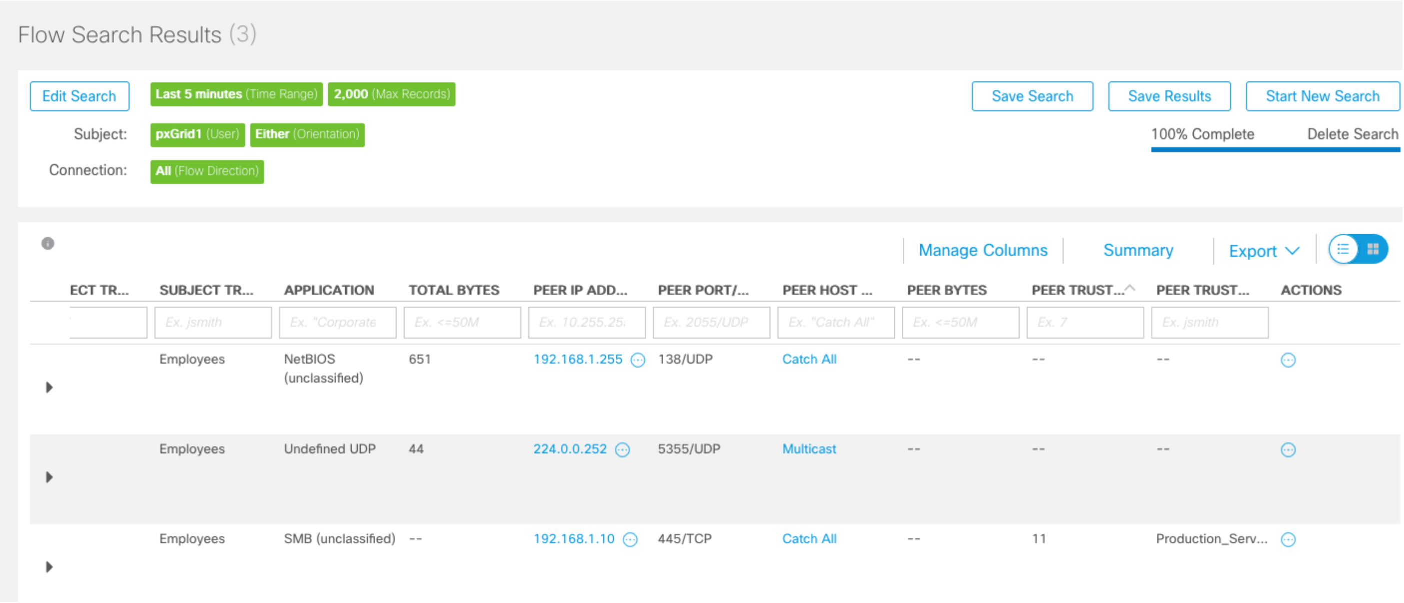
Subject: **pxGrid1** (User) **Either** (Orientation)

Connection: **All** (Flow Direction)

100% Complete Delete Search

START	DURATION	SUBJECT IP ...	SUBJECT PO...	SUBJECT HO...	SUBJECT BY...	SUBJECT TR...	SUBJECT TR...	APPLICATION	TOTAL BYTES	PEER IP ADD
Ex. 06/09/2	Ex. <=50min4(	Ex. 10.10.10.1	Ex. 57100/UD	Ex. "catch All"	Ex. <=50M	Ex. 7	Ex. jsmith	Ex. "Corporate	Ex. <=50M	Ex. 10.255.2
Nov 4, 2018 12:54:11 AM (10min 26s ago)	47s	192.168.1.234	138/UDP	Catch All	651	4	Employees	NetBIOS (unclassified)	651	192.168.1.25
Nov 4, 2018 12:54:11 AM (10min 26s ago)	--	192.168.1.234	60771/UDP	Catch All	44	4	Employees	Undefined UDP	44	224.0.0.252
Nov 4, 2018 12:37:16 AM (27min 21s ago)	17min 34s	192.168.1.234	1049/TCP	Catch All	--	4	Employees	SMB (unclassified)	--	192.168.1.10

Also, note the Peer TrustSec ID of 11, and the Peer TrustSec name of Production Servers



Last 5 minutes (Time Range) **2,000** (Max Records)

Subject: **pxGrid1** (User) **Either** (Orientation)

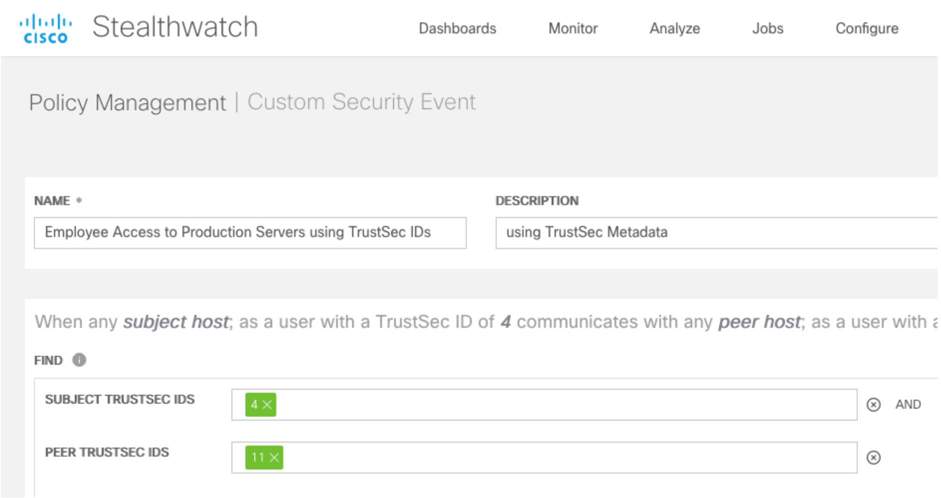
Connection: **All** (Flow Direction)

ECT TR...	SUBJECT TR...	APPLICATION	TOTAL BYTES	PEER IP ADD...	PEER PORT/...	PEER HOST ...	PEER BYTES	PEER TRUST...	PEER TRUST...	ACTIONS
	Ex. jsmith	Ex. "Corporate	Ex. <=50M	Ex. 10.255.25.	Ex. 2055/UDP	Ex. "Catch All"	Ex. <=50M	Ex. 7	Ex. jsmith	
	Employees	NetBIOS (unclassified)	651	192.168.1.255	138/UDP	Catch All	--	--	--	
	Employees	Undefined UDP	44	224.0.0.252	5355/UDP	Multicast	--	--	--	
	Employees	SMB (unclassified)	--	192.168.1.10	445/TCP	Catch All	--	11	Production_Serv...	

Policy Violations

Stealthwatch 7.0 provides creating policy violation alarms from custom security events. In this example, a sample policy violation alarm is created for Employees. Subject TrustSec ID 4, communicating with Production Services, Peer Trustsec ID, Peer 11.

Step 1 Select **Configure->Policy Management**
Step 2 Select **Create New Policy->Custom Security Event**
Step 3 Enter Name: **Employee Access to Production Servers using Trustsec IDs**
Step 4 Enter Description: **using TrustSec Metadata**
Step 5 Under **Alarm When->Find,** click on "**+**" Add a rule
Step 6 Select **Subject TrustSec IDs**, select **4** from the drop-down menu
Step 7 Click on "+"
Step 8 Select **Peer TrustSec IDs**, select **11** from the drop-down menu



Policy Management | Custom Security Event

NAME *
Employee Access to Production Servers using TrustSec IDs

DESCRIPTION
using TrustSec Metadata

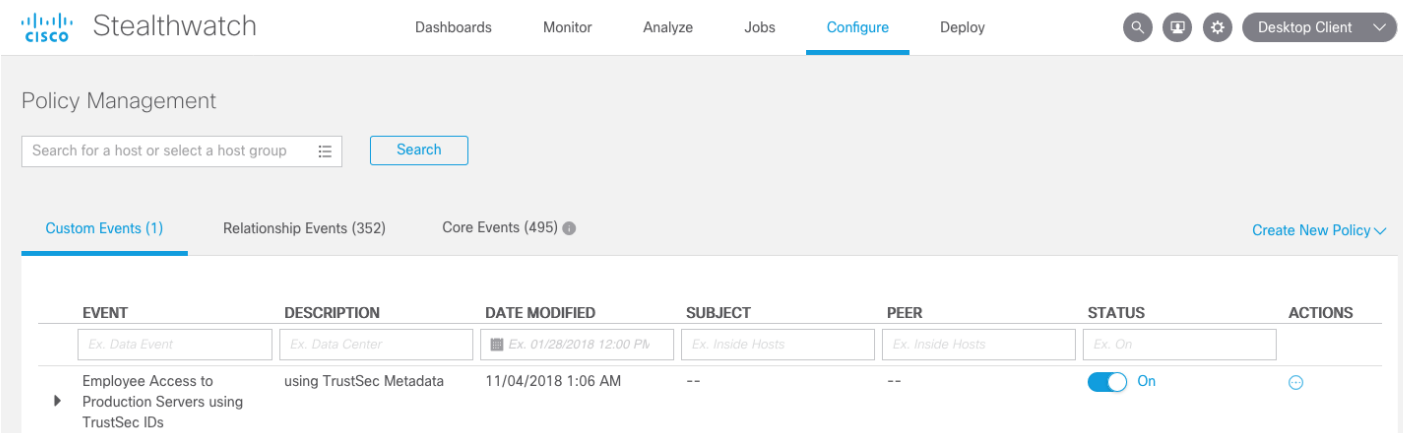
When any *subject host*; as a user with a TrustSec ID of *4* communicates with any *peer host*; as a user with a

FIND

SUBJECT TRUSTSEC IDS: 4 × AND

PEER TRUSTSEC IDS: 11 ×

Step 9 Select **Save**
Step 10 Click on **STATUS** to enable or turn on



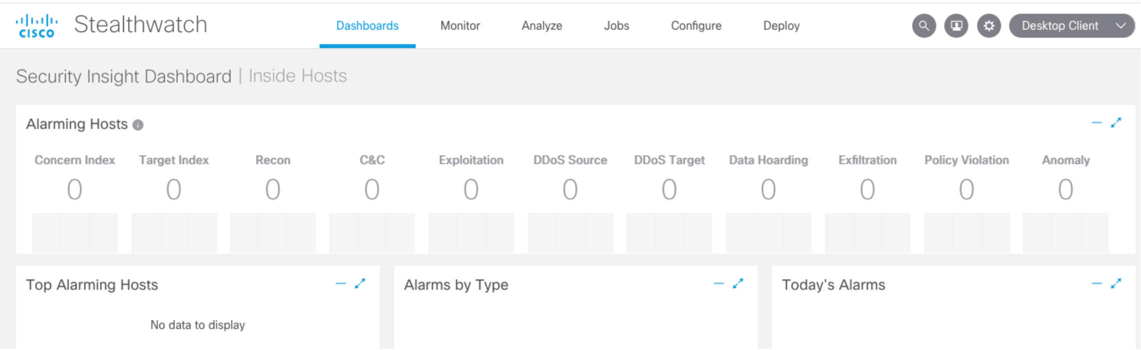
Policy Management

Search for a host or select a host group | Search

Custom Events (1) | Relationship Events (352) | Core Events (495) | Create New Policy

	EVENT	DESCRIPTION	DATE MODIFIED	SUBJECT	PEER	STATUS	ACTIONS
	Ex. Data Event	Ex. Data Center	Ex. 01/28/2018 12:00 PM	Ex. Inside Hosts	Ex. Inside Hosts	Ex. On	
▸	Employee Access to Production Servers using TrustSec IDs	using TrustSec Metadata	11/04/2018 1:06 AM	--	--	On	⋯

Step 11 Select **Dashboards->Network Security**



Security Insight Dashboard | Inside Hosts

Alarming Hosts

Concern Index	Target Index	Recon	C&C	Exploitation	DDoS Source	DDoS Target	Data Hoarding	Exfiltration	Policy Violation	Anomaly
0	0	0	0	0	0	0	0	0	0	0

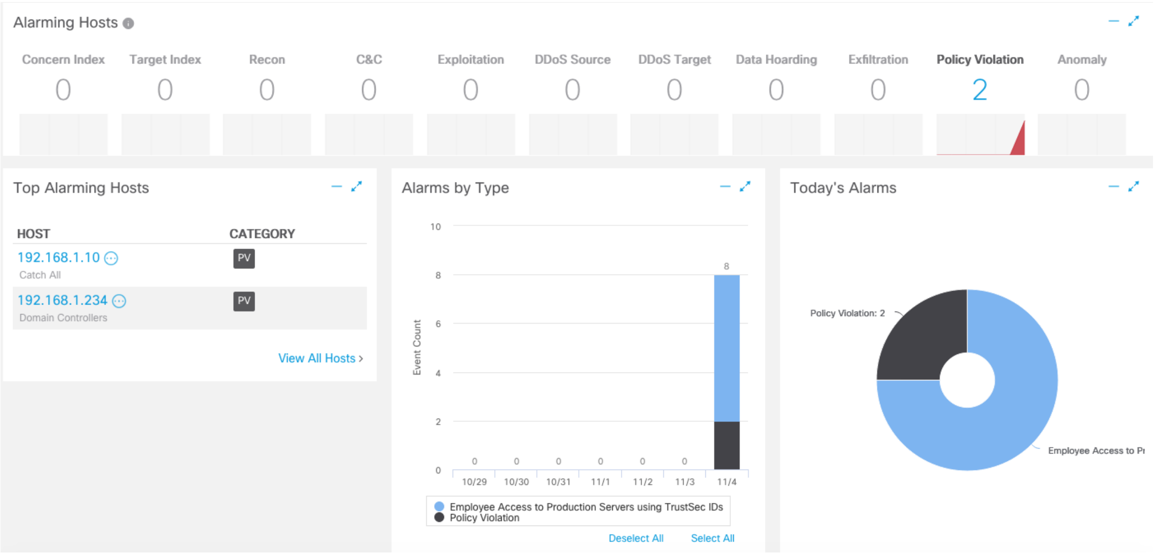
Top Alarming Hosts

No data to display

Alarms by Type

Today's Alarms

Step 12 You should see the **Policy Violations** under Alarming Hosts



Alarming Hosts

Concern Index	Target Index	Recon	C&C	Exploitation	DDoS Source	DDoS Target	Data Hoarding	Exfiltration	Policy Violation	Anomaly
0	0	0	0	0	0	0	0	0	2	0

Top Alarming Hosts

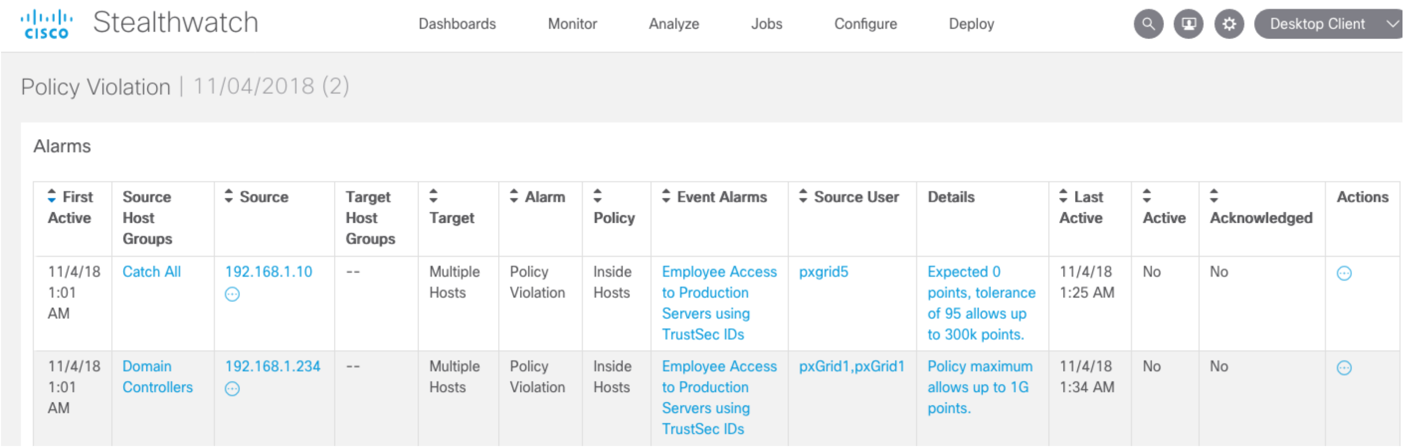
HOST	CATEGORY
192.168.1.10 Catch All	PV
192.168.1.234 Domain Controllers	PV

View All Hosts ›

Alarms by Type

Today's Alarms

Step 13 Drill down on the policy violations to see the flow details



Policy Violation | 11/04/2018 (2)

Alarms

First Active	Source Host Groups	Source	Target Host Groups	Target	Alarm	Policy	Event Alarms	Source User	Details	Last Active	Active	Acknowledged	Actions
11/4/18 1:01 AM	Catch All	192.168.1.10	--	Multiple Hosts	Policy Violation	Inside Hosts	Employee Access to Production Servers using TrustSec IDs	pxgrid5	Expected 0 points, tolerance of 95 allows up to 300k points.	11/4/18 1:25 AM	No	No	⋯
11/4/18 1:01 AM	Domain Controllers	192.168.1.234	--	Multiple Hosts	Policy Violation	Inside Hosts	Employee Access to Production Servers using TrustSec IDs	pxGrid1,pxGrid1	Policy maximum allows up to 1G points.	11/4/18 1:34 AM	No	No	⋯

References

Below are the configurations for the ASA 5506-X and the Cisco Catalyst 3750-X Switch

TrustSec Device Configuration

Device Configuration for ASA 5506-X

Step 1 Configure RADIUS on ASA

```
conf t
aaa-server ise1 protocol radius
aaa-server ise1 host 192.168.1.251 Richard08
```

Step 2 Create Server-Group

```
conf t
aaa-server protocol ciscoasa protocol radius
aaa-server ciscoasa(inside) host 192.168.1.251
key Richard08
exit
cts server-group ciscoasa
```

Step 3 Import OOB PAC file from network configuration

```
conf t
cts import ftp://jeppich:Richard08@192.168.1.13/ciscoasa.pac password Richard08
```

Step 4 Configuring the ASA as a SPX Listener

```
conf t
cts sxp enable
cts sxp default password Richard08 (password should match other SXP devices)
cts sxp default source-ip 192.168.1.1 (ASA internal IP address)
cts sxp connection peer 192.168.1.3 (switch IP address) password default mode local listener
```

Step 5 Verify if the ASA is receiving SGT mappings

```
conf t
sh cts sxp sgt-map ipv4 detail
```

Device Configuration for Cisco Catalyst Switch 3750-X

Step 6 Configuring for RADIUS

```
conf t
aaa authorization network ise1 group radius
cts authorization list ise1
ip device tracking
radius-server host 192.168.1.251 key Richard08
```

Step 7 Configuring for CTS

```
cts sxp enable
cts sxp default source-ip 192.168.1.3 (ip address of switch)
cts sxp default password Richard08 (shared secret)
cts sxp connection peer 192.168.1.1 (ip address of ASA) password default mode local
```

Reference Documents

Cisco ASA and Catalyst 3750-X Series TrustSec Configuration Example and Troubleshooting Guide:

https://www.cisco.com/c/en/us/support/docs/security/adaptive-security-appliance-asa-software/116497-configure-trustsec-00.html

TrutSec Documentation:

https://community.cisco.com/t5/security-documents/segmentation-amp-group-based-policy-resources/ta-p/3656481

Cisco pxGrid Documentation:

https://community.cisco.com/t5/security-documents/ise-security-ecosystem-integration-guides/ta-p/3621164#toc-hId--292074806