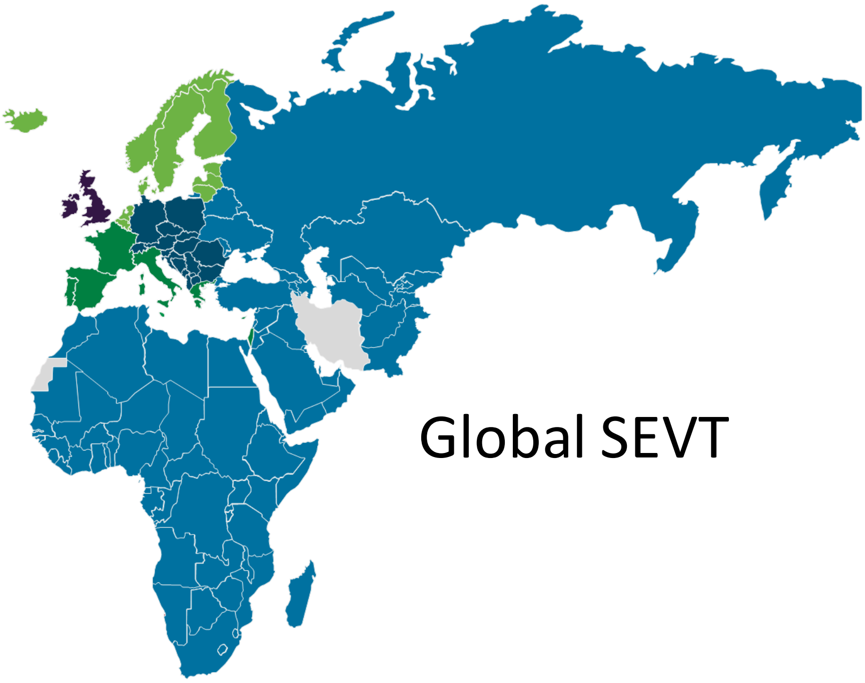


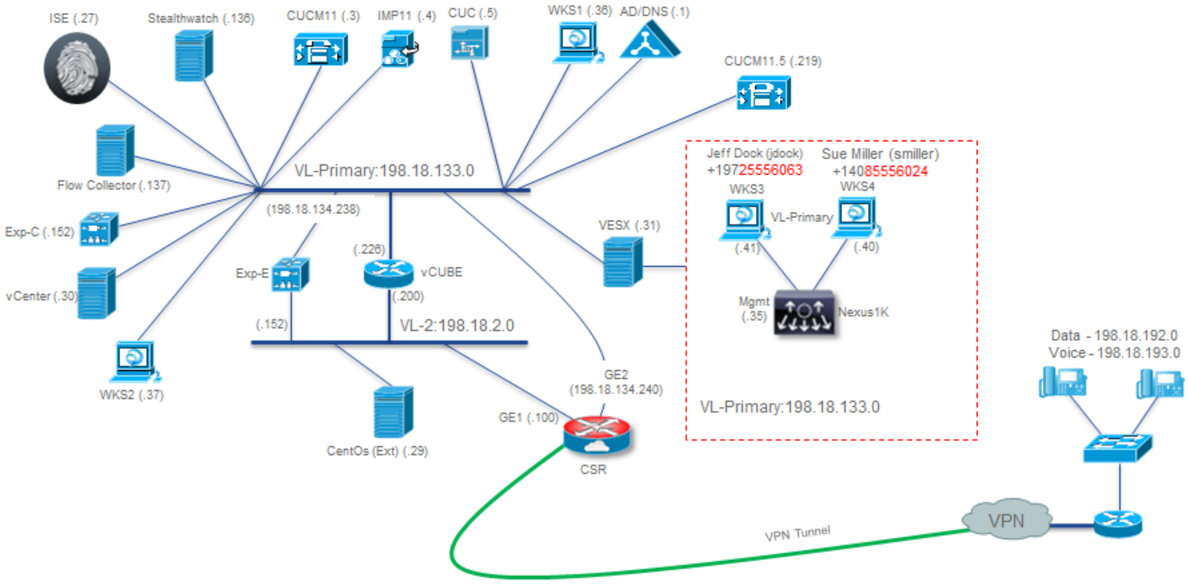
E2E Security Lab

TrustSec Module

Lab Quick Start Introduction

Note: The following information is included to help you get started with the Module you choose to run through. All of the lab pods are numbered. Use the anyconnect VPN details on the excel spreadsheet provided to access your lab pod. Use a browser, RDP, Telnet and SSH to access the various components of the lab. More detailed access information is provided in each of the lab Module configuration guides.

Endpoint	User	Directory Number	Self-Provisioning ID	AD / UC Password	PIN
Phone 1	Kelli Melby (kmelby)	+19725556050	6050	C1sco12345	12345
Phone 2	Frederick Baker (fbaker)	+19195556087	6087	C1sco12345	12345
Jabber WKST1 (csfcholland)	Charles Holland (cholland)	+14085556018	6018	C1sco12345	12345
Jabber WKST2 (csfaperez)	Anita Perez (aperez)	+12125556017	6017	C1sco12345	12345
Jabber WRKST3 (csfjdock)	Jeff Dock (jdock)	+19725556063	6063	C1sco12345	12345
Jabber WRKST4 (smiller)	Sue Miller (smiller)	+14085556024	6024	C1sco12345	12345



Device	**IP Address**	**Username**	**Password**
AD	198.18.133.1	administrator	C1sco12345
CUCM11	198.18.133.3	administrator	dCloud123!
IMP11	198.18.133.4	administrator	dCloud123!
CUC11	198.18.133.3	administrator	dCloud123!
ISE	198.18.133.27	admin	C1sco12345
vCenter	198.18.133.30	root	C1sco12345
Nexus 1000V	198.18.133.35	admin	C1sco12345
WKST1	198.18.133.36	cholland	C1sco12345
WKST2	198.18.133.37	aperez	C1sco12345
WKS3	198.18.133.41	jdock	C1sco12345
WKS4	198.18.133.40	Smiller	C1sco12345
StealthWatch Mgmt Console	198.18.133.137	admin	lan411cope
StealthWatch Flow Collector	198.18.133.136	admin	lan411cope
Exp-C	198.18.133.152	admin	dCloud123!
CUCM11.5	198.18.133.219	administrator	dCloud123!
vCUBE (Inside)	198.18.133.226	admin	C1sco12345
Exp-E	198.18.134.238	admin	dCloud123!
CentOS	198.18.2.29	root	dCloud123!
vCUBE (Outside)	198.18.2.200	admin	C1sco12345

TrustSec Module Aim

Cisco has a whole suite of IT Security related products and technologies. One thing that is missing in most of our current documentation is; how does Collaboration interact with Cisco's existing Security portfolio?

This lab tries to answer this question, at least for Identity Services Engine (ISE), TrustSec and Lancope StealthWatch devices.

During the course of this module you'll learn the basics of configuring IEEE802.1x for CUCM registered devices. You'll then create a centralised TrustSec Segmentation policy and use Security Group Access Control Lists (SGACLs) to enforce it policy within the lab's datacentre infrastructure.

You'll then use NetFlow to monitor the lab's Collaboration traffic and export it to a StealthWatch Flow Collector. After which you'll use a StealthWatch Management Console to create a custom event to report on any suspicious traffic between the lab's Jabber clients and the US Servers.

Note: Although this guide provides configurations and reasoning behind the creation of system elements such as SGTs (Security Group Tags), this document is not a Cisco validated design document.

Introduction

Cisco has historically advocated separate data and audio/video VLANs. This is a great best practice as it enables Access Control Lists (ACLs) to be easily added at the Layer 3 boundary to control both signalling and media traffic. This has worked well for many years, but unfortunately the proliferation of mobile soft clients, such as Jabber, has somewhat broken the traditional design guidance. Whether it's due to Jabber deployed on laptops using the wired infrastructure, or on smart phones over wireless, the topological demarcation between the data and collaboration environments has disappeared. This can make it very complex to use traditional VLANs to secure access to core collaboration services; as Jabber enabled devices can roam the Enterprise and often share the same VLAN with non-Jabber enabled data devices.

From a security perspective this creates a problem, which the traditional VLAN approach doesn't really provide a good answer for. What is really needed for modern security conscious collaboration deployments is a dynamic policy based enforcement solution. Hence, it's a good thing that Cisco Security Technology Group invented TrustSec!

For the uninitiated TrustSec is Cisco's software defined segmentation technology embedded into its network infrastructure equipment. TrustSec uses contextual data about whom and what is accessing the network, and enables role based access using Security Group Tags (SGT) to segment the infrastructure. The ultimate goal of Cisco TrustSec technology is to assign a SGT to the user's or device's traffic at ingress (inbound into the network), and then enforce the access policy based on the tag elsewhere in the infrastructure (in the data centre, for example). This SGT is used by switches, routers, and firewalls to make forwarding decisions

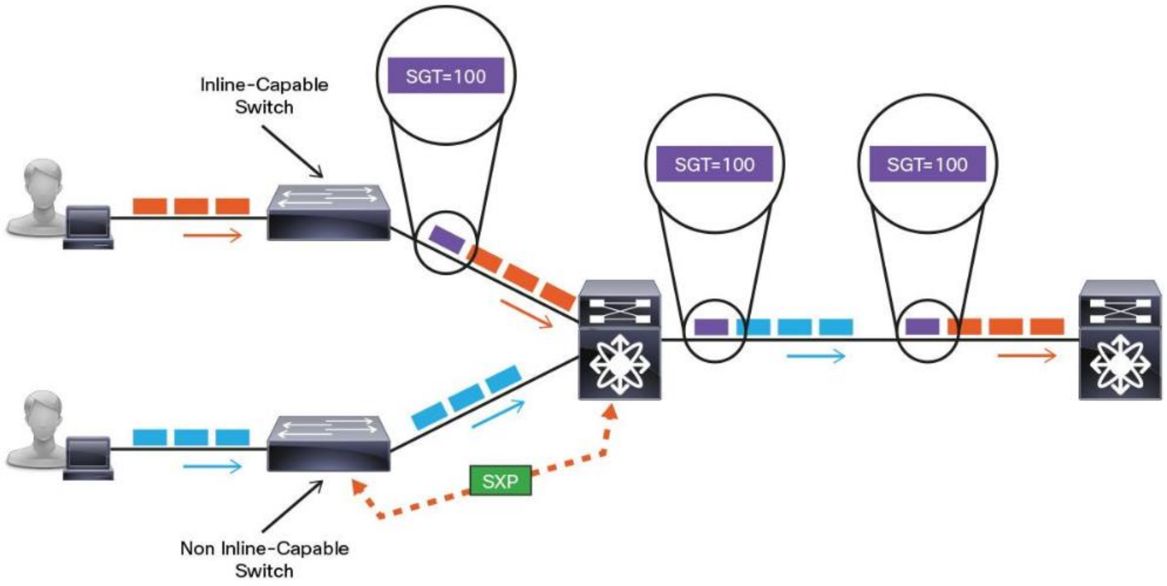
Cisco TrustSec is defined in three phases: classification, propagation, and enforcement:

Classification

In order to use SGTs within your infrastructure, your devices must support SGTs. All Cisco switches and wireless controllers embedded with Cisco TrustSec technology support the assignment of SGTs. A SGT can be assigned dynamically or statically. Dynamic classification occurs via an authentication sequence, via 802.1x, MAB, or web authentication. When authentication isn't available, static classification methods are necessary. In static classification the tag maps to something (an IP, subnet, VLAN, or interface) rather than relying on an authorization from the Cisco ISE. This process of assigning the SGT is defined as "classification." These classifications are then transported deeper into the network for policy enforcement.

Propagation

Now that the SGT is assigned to the user's session, the next step is to communicate the tag upstream to TrustSec devices that enforce policy based on SGTs. This communication process is defined as "propagation". Cisco TrustSec has two methods to propagate a SGT, inline and Source Exchange Protocol (SXP). The figure below shows an example of one access switch that has native tagging. The packets get tagged on the uplink port and through the infrastructure. It also shows a non-inline capable switch, which uses a peering protocol to update the upstream switch. In both cases, the upstream switch continues to tag the traffic throughout the infrastructure



Enforcement

Once we have SGTs assigned (classification), and they are being transmitted across the network (propagation), the final component of TrustSec that will be implemented is enforcement. There are multiple ways to enforce traffic based on the tag, but in our lab we are going to look at enforcement on a switch using a Security Group ACL (SGACL).

One way a SGACL can be visualized is as a spreadsheet entry as they are always based on a source tag to a destination tag and in ISE SGACLs are just entries in the Policy Matrix.

There are two main ways to deploy SGACLs: North-South and East-West. “North-South” refers to the case of a user or device being classified at the access layer, but enforcement with the SGACL occurring at the data centre. For example, a guest entering the access layer is assigned a Guest SGT. Traffic with a Guest SGT will be dropped if it tries to reach a server with financial data. “East-West” refers to the case of an SGACL protecting resources that exist on the same switch. For example, if a development server and a production server are on the same Cisco Nexus 5000 Series Switch in the data centre, an SGACL may be deployed to prevent the development server from communicating with the production server. Another East-West example is a guest and an employee using the same access layer switch. Traffic may be filtered between these two devices so the guest cannot communicate to the employee who is in the same VLAN on the same switch.

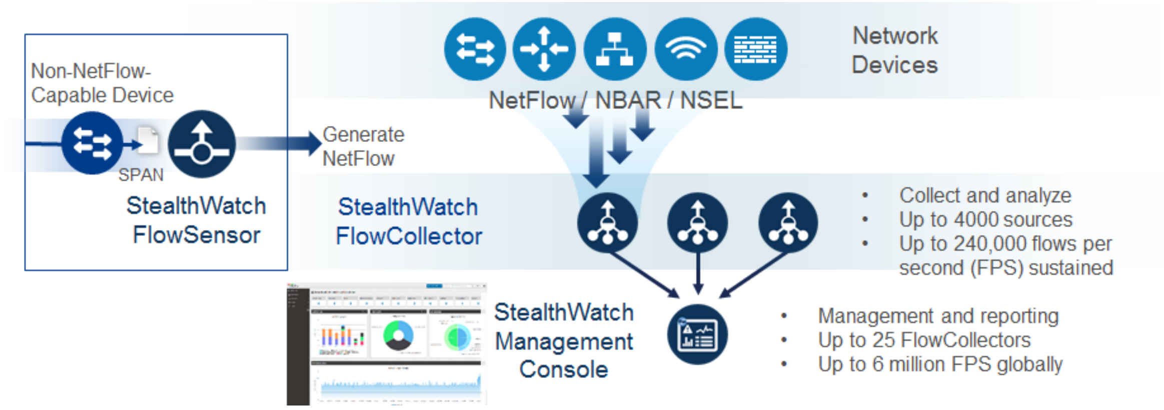
Our TrustSec lab set up will only allow collaboration media traffic to pass (East-West) between the Jabber endpoints, and between Jabber and our lab phones. We will only allow North-South signalling from our Jabber endpoints to the Unified CM and IMP servers.

To learn more about TrustSec please check out this URL:

http://www.cisco.com/c/en/us/solutions/enterprise-networks/trustsec/index.html

Monitoring our Security Deployment

Having TrustSec enforce security policies is great but one of the other key requirements of a modern day security solution for Collaboration or any other type of mission critical application is robust and accurate security monitoring. Two key components of Cisco's security monitoring suite are the StealthWatch Management Console and the StealthWatch FlowCollector.

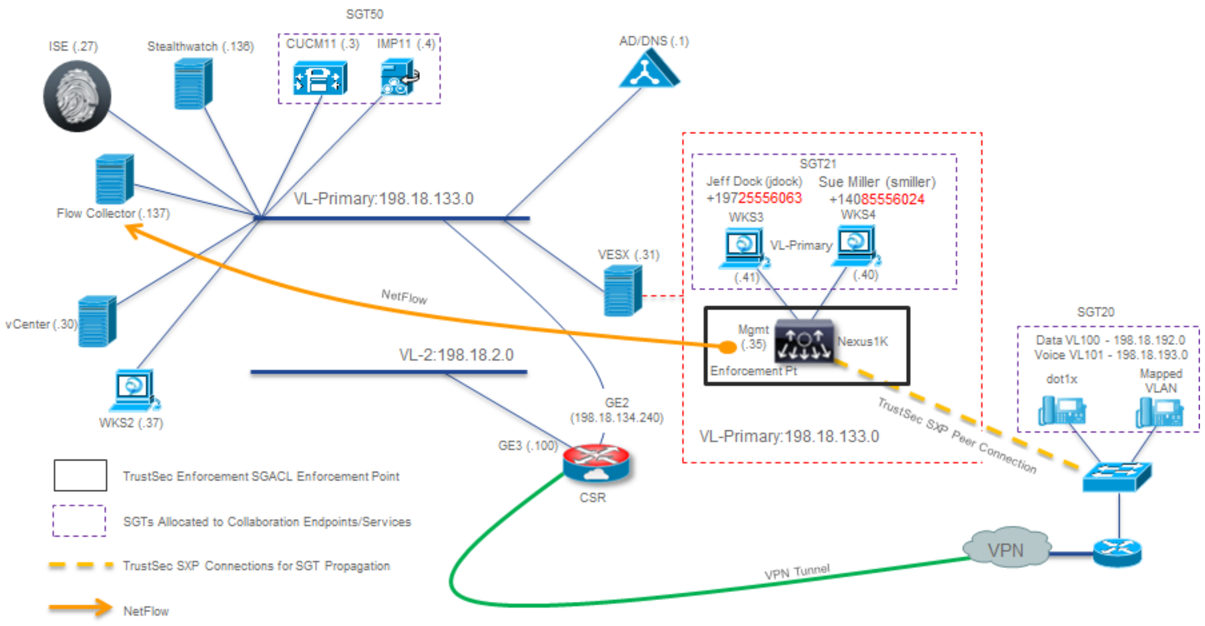


Using Cisco's StealthWatch Management Console (SMC), administrators can easily view, understand and act upon a plethora of network and security data all through a single interface. Snapshot views and sophisticated drill-down capabilities provide the exact level of information you need exactly when you need it. Dynamic querying, customized reports and intuitive visualizations of network data enhance the advanced threat detection capabilities of the StealthWatch System, helping to decrease the time between problem onset and resolution.

The StealthWatch FlowCollector collects and analyses vast amounts of valuable data from the network infrastructure to provide a complete picture of everything happening in an enterprise environment. Sophisticated behavioural analytics and advanced security context enable early detection and enhanced protection for a wide range of threats including APTs (Advanced Persistent Threats), insider threats, DDoS and zero-day malware. The FlowCollector uses flow-based anomaly detection to zoom in on any unusual behaviour and immediately sends an alarm with actionable intelligence that allows you to take quick, decisive steps to mitigate any issues. Operators can use the StealthWatch Console's unique drill-down features to identify and isolate the root cause within seconds, enhancing operational efficiency, decreasing costs and dramatically reducing the time from problem onset to resolution.

Lab Configurations

The lab topology we will use for our Collaboration TrustSec Module is shown below:



Classification

In keeping with traditional best practice the lab phones are allocated their own Voice VLANs, and IEEE802.1x authentication will be used to allocate the appropriate SGT to a test phone that is connected to the lab's access switch. This is undoubtedly the most secure approach but it is also possible to statically map Voice VLANS to a SGT, if for any reason, an organisation was unable to implement Network Access Control (NAC). To demonstrate this, our access switch also statically maps a SGT to the Voice VLAN, this subsequently allows us to apply TrustSec policies to the second lab phone.

In the virtual part of the lab we have two Jabber clients (WKS3 and WKS4) installed on two VMs connected to a L2 Nexus 1000V, this device is acting as our Classification point for the lab's Datacentre devices. In a production TrustSec environment it is unlikely that a Jabber client would be connected to a Datacentre Nexus 1000V, but for the purpose of keeping the lab as virtual as possible (while still being able to deploy TrustSec) this was necessary. The down side of this approach is that the Nexus 1000V does not support IEEE802.1x and hence the Jabber client's SGT will be statically mapped. As you are most likely aware the device (PC/Mobile) owner, not the Jabber client, would be authenticated using IEEE802.1x.

The core collaboration servers (CUCM/IMP/CUC) will be configured with a static IP to SGT mapping on the Nexus 1000V.

Propagation

We will create a SXP peer connection between the lab's Access Switch and the Nexus 1000V to propagate the phone traffic's SGT information across the lab's VPN tunnel and CSR 1000V router.

Enforcement

In our lab the only enforcement point will be the Nexus 1000V switch. The SGACLs will be defined centrally on ISE and then downloaded onto the Nexus 1000V. If you look at the lab topology, what traffic from the phones do you think we can enforce? The answer is media traffic to/from the Jabber clients. The phone signalling traffic does not pass through the Nexus 1000V.

As stated previously:

Our TrustSec lab set up will only allow collaboration media traffic to pass (East-West) between the Jabber endpoints, and between Jabber and our lab phones. We will only allow North-South signalling from our Jabber endpoints to the Unified CM and IMP servers.

Monitoring

In the final part of the lab we will enable NetFlow on our Nexus 1000, and use the StealthWatch Flow Collector as the destination for the export. We'll then use the StealthWatch Management Console (SMC) to analyse traffic to/from our Jabber-WKS and compare this to what we'd expect to see during a Jabber call or IM session.

We're also going to create a couple of Custom Events in the SMC to monitor our TrustSec SGACLs, which we are using to enforce our TrustSec Policy on the Nexus 1000V. The idea behind these Custom Events is to create a Policy Violation alert on the SMC when any Jabber-WKS tries to connect to the core UC Servers or lab IP Phones over ports that are not authorized in our ISE TrustSec Policy.

At the end of the lab we'll have an automated monitoring system that will alert us to suspicious activity in our TrustSec enabled Collaboration deployment!

Connectivity Baseline

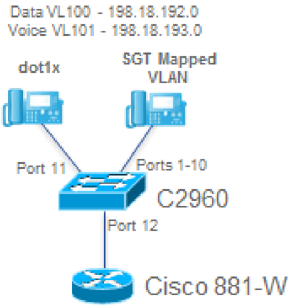
Log onto WKS3 and WKS4 and perform the following to verify:

- Ping between WKS3 and WKS4
- You can ping the phones from WKS3 and WKS4
- You can ping the CUCM and IMP Servers
- Also use http://198.18.133.3 to access CUCM. Important – use http and not https in the URL.
- Use http://Phone_IP_Address to access 8845\8865 web page
-

Note: If you are familiar with IEEE802.1x, then you can actually skip the section below and move directly onto the TrustSec section. All you will miss is the dynamic allocation of the Phone's SGT. However, as we are performing a VLAN based static mapping on the switch, you'll still be able to enforce phone media on the NEXUS 1000V. Avoiding this section will give you a better chance of reaching and completing the Lancope part of the Module. If you complete the monitoring portion of the lab you can always cycle back to configure IEEE802.1x

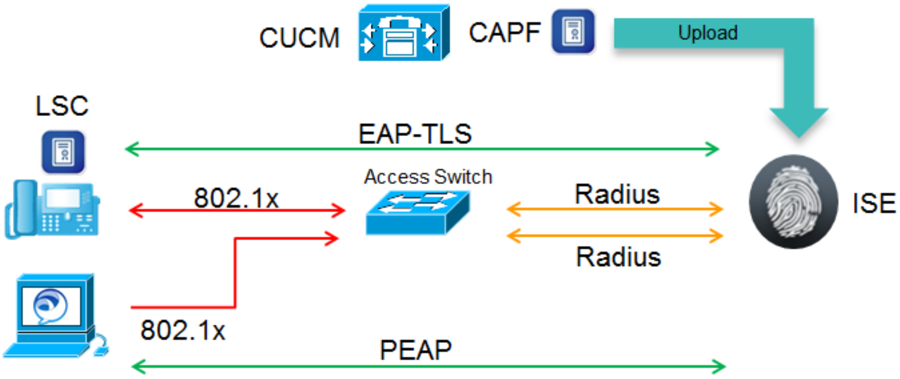
Kicking Off with IEEE802.1x

Note: Port 11 on the lab switch is enabled for IEEE802.1x. This is the port you will connect 8845/8865 to when you test.



The initial starting point for our TrustSec Lab is to implement dynamic NAC (Network Access Control) for our 8845/8865 phone.

Note: In a production deployment we would also use IEEE 802.1X for the Windows PCs running the Jabber clients. However, in the lab we can't do this as the virtual Nexus 1000V does not offer IEEE 802.1x support.



The main configuration requirement is the generation of the LSCs (Locally Significant Certificates) on the phones. This requires enrolment to the CAPF (Certificate Authority Proxy Function), which is responsible for signing each phone's LSC. In our lab we're not going to turn on Mixed Mode as cryptography is not a requirement for 802.1x authentication. More details on LSC and CAPF enrolment can be found here:

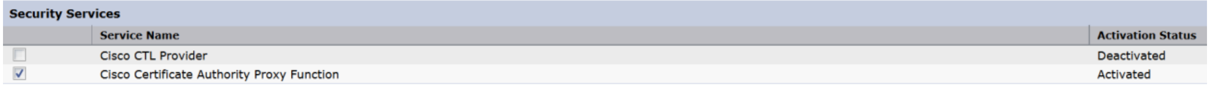
http://www.cisco.com/c/en/us/td/docs/voice_ip_comm/cucm/security/11_0_1/secugd/CUCM_BK_C1A78C1D_00_cucm-security-guide-1101/CUCM_BK_C1A78C1D_00_cucm-security-guide-1101_chapter_01010.html

Once the phone has a valid LSC it's just a matter of ticking a checkbox to enable IEEE802.1x, or leaving it under user control.

Enabling Authentication:

CUCM - https://198.18.133.3 (administrator/dCloud123!)

1) Activate CAPF



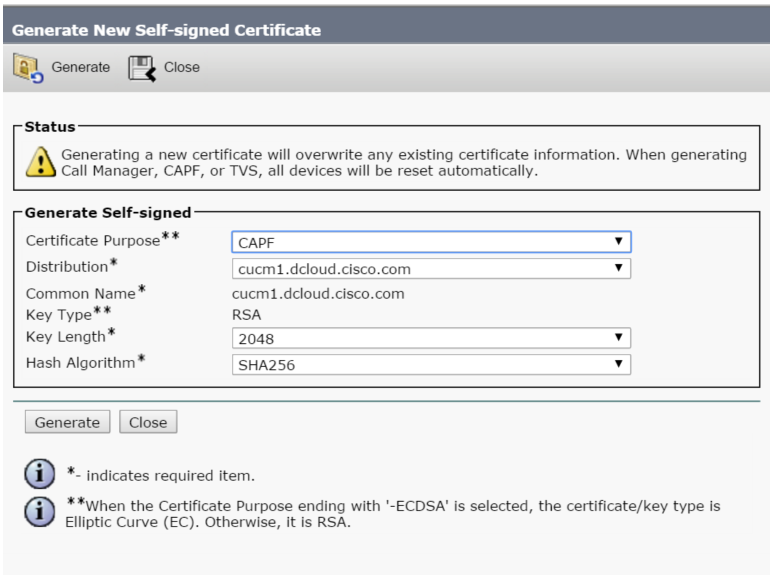
Security Services

	Service Name	Activation Status
☐	Cisco CTL Provider	Deactivated
☑	Cisco Certificate Authority Proxy Function	Activated

You do this from the Service Activation Screen found under the CCM Serviceability pages.

2) Regenerate the CUCM CAPF Cert just to make sure it has a 2048 bit key and uses SHA2.

Navigate to the OS Administration pages and go to Security>Certificate Management. Then click of Generate Self-signed button.



Status

Generating a new certificate will overwrite any existing certificate information. When generating Call Manager, CAPF, or TVS, all devices will be reset automatically.

Generate Self-signed

Certificate Purpose** CAPF

Distribution* cucm1.dcloud.cisco.com

Common Name* cucm1.dcloud.cisco.com

Key Type** RSA

Key Length* 2048

Hash Algorithm* SHA256

*- indicates required item.

**When the Certificate Purpose ending with '-ECDSA' is selected, the certificate/key type is Elliptic Curve (EC). Otherwise, it is RSA.

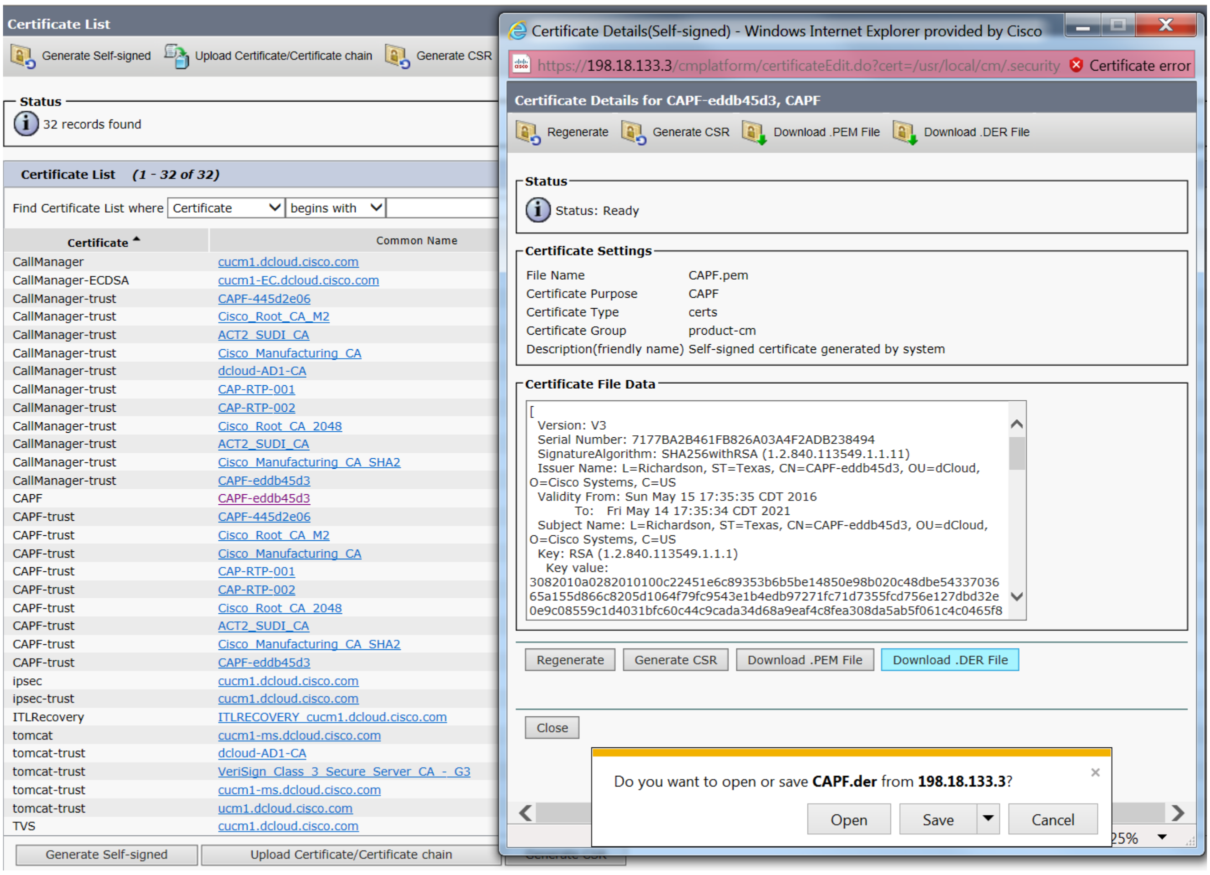
Create a self-signed 2048bit SHA256 CAPF certificate. You should see – “Success: certificate generated” in the GUI when the operation has completed.

Why are we doing this?

IMPORTANT: Please don’t forget to restart the TFTP Server and then the CAPF service after you update the certificate. Do this NOW ☺

Next we download the new CAPF certificate. Navigate back to the Certificate Management window on the CUCM OS GUI. Press “Find” and click the CAPF certificate.

Download the .der version of the certificate onto your local PC.



Certificate List

Status

32 records found

Certificate List *(1 - 32 of 32)*

Find Certificate List where Certificate begins with

Certificate	Common Name
CallManager	cucm1.dcloud.cisco.com
CallManager-ECDSA	cucm1-EC.dcloud.cisco.com
CallManager-trust	CAPF-445d2e06
CallManager-trust	Cisco_Root_CA_M2
CallManager-trust	ACT2_SUDI_CA
CallManager-trust	Cisco_Manufacturing_CA
CallManager-trust	dcloud-AD1-CA
CallManager-trust	CAP-RTP-001
CallManager-trust	CAP-RTP-002
CallManager-trust	Cisco_Root_CA_2048
CallManager-trust	ACT2_SUDI_CA
CallManager-trust	Cisco_Manufacturing_CA_SHA2
CallManager-trust	CAPF-eddb45d3
CAPF	CAPF-eddb45d3
CAPF-trust	CAPF-445d2e06
CAPF-trust	Cisco_Root_CA_M2
CAPF-trust	Cisco_Manufacturing_CA
CAPF-trust	CAP-RTP-001
CAPF-trust	CAP-RTP-002
CAPF-trust	Cisco_Root_CA_2048
CAPF-trust	ACT2_SUDI_CA
CAPF-trust	Cisco_Manufacturing_CA_SHA2
CAPF-trust	CAPF-eddb45d3
ipsec	cucm1.dcloud.cisco.com
ipsec-trust	cucm1.dcloud.cisco.com
ITLRecovery	ITLRECOVERY_cucm1.dcloud.cisco.com
tomcat	cucm1-ms.dcloud.cisco.com
tomcat-trust	dcloud-AD1-CA
tomcat-trust	VeriSign_Class_3_Secure_Server_CA_-_G3
tomcat-trust	cucm1-ms.dcloud.cisco.com
tomcat-trust	ucm1.dcloud.cisco.com
TVS	cucm1.dcloud.cisco.com

Certificate Details(Self-signed) - Windows Internet Explorer provided by Cisco

https://198.18.133.3/cmplatform/certificateEdit.do?cert=/usr/local/cm/.security Certificate error

Certificate Details for CAPF-eddb45d3, CAPF

Status

Status: Ready

Certificate Settings

File Name	CAPF.pem
Certificate Purpose	CAPF
Certificate Type	certs
Certificate Group	product-cm
Description(friendly name)	Self-signed certificate generated by system

Certificate File Data

```
[
  Version: V3
  Serial Number: 7177BA2B461FB826A03A4F2ADB238494
  SignatureAlgorithm: SHA256withRSA (1.2.840.113549.1.1.11)
  Issuer Name: L=Richardson, ST=Texas, CN=CAPF-eddb45d3, OU=dCloud,
O=Cisco Systems, C=US
  Validity From: Sun May 15 17:35:35 CDT 2016
           To:   Fri May 14 17:35:34 CDT 2021
  Subject Name: L=Richardson, ST=Texas, CN=CAPF-eddb45d3, OU=dCloud,
O=Cisco Systems, C=US
  Key: RSA (1.2.840.113549.1.1.1)
    Key value:
3082010a0282010100c22451e6c89353b6b5be14850e98b020c48dbe54337036
65a155d866c8205d1064f79fc9543e1b4edb97271fc71d7355fcd756e127dbd32e
0e9c08559c1d4031bfc60c44c9cada34d68a9eaf4c8fea308da5ab5f061c4c0465f8
```

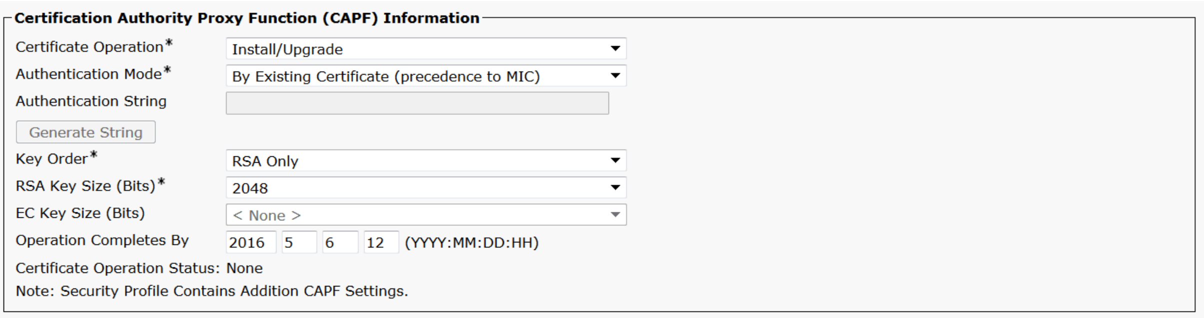
Do you want to open or save **CAPF.der** from **198.18.133.3**?

Note: If the CAPF certificate has a key size of 1024 and uses SHA1, then ISE should present a security warning if you try to upload a 1024 bit CAPF certificate for the IEEE802.1x authentication.

Generate a LSC on the 8845/8865 Phone and have it signed by CAPF

Verify that there is no LSC on the phone that you intend to authenticate using IEEE802.1x. You can do this by navigating to the Security setup from the phone “Admin settings” GUI. If there is a LSC present, perform a factory reset to clear any previous configuration and re-register the phone. If you need help with the factory reset, please ask a Proctor to save you some research time.

On the 8845/8865 phone’s CUCM configuration page configure CAPF parameters as shown below. Use the largest RSA key size and use the MIC (Manufacturing Installed Certificate) to authenticate the phone’s connection to the CAPF service.



Certification Authority Proxy Function (CAPF) Information

Certificate Operation*	Install/Upgrade
Authentication Mode*	By Existing Certificate (precedence to MIC)
Authentication String	
Key Order*	RSA Only
RSA Key Size (Bits)*	2048
EC Key Size (Bits)	< None >
Operation Completes By	2016 5 6 12 (YYYY:MM:DD:HH)

Certificate Operation Status: None

Note: Security Profile Contains Addition CAPF Settings.

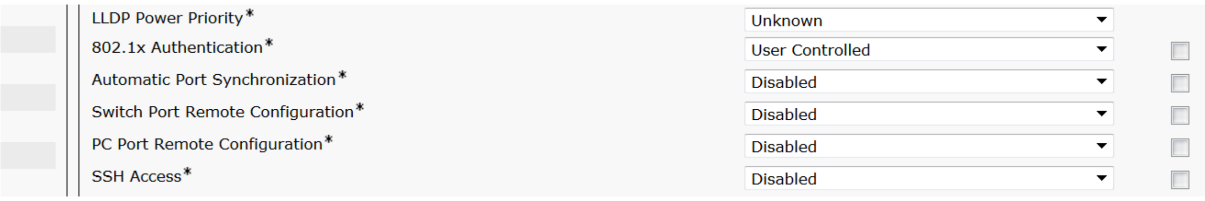
Save and “Apply” the configuration change.

On the phone, from the Security Setup screen, you should see the LSC field move into a Pending State, and shortly afterwards the display will change to Installed. The phone should then reboot.

3) Verify 802.1x setting on the IP Phone

Navigate to the phone’s IEEE 802.1x setting on CUCM to make sure it is configured correctly.

Suggestion: leave the configuration as “User Controlled” as this will allow you to switch IEEE 802.1x on and off from the phone, which might help with any troubleshooting during the course of the lab.



LLDP Power Priority*	Unknown	
802.1x Authentication*	User Controlled	☐
Automatic Port Synchronization*	Disabled	☐
Switch Port Remote Configuration*	Disabled	☐
PC Port Remote Configuration*	Disabled	☐
SSH Access*	Disabled	☐

4) Upload the CAPF certificate into ISE.

The next step is to configure the ISE (Identity Services Engine) to authenticate and authorize our CUCM devices.

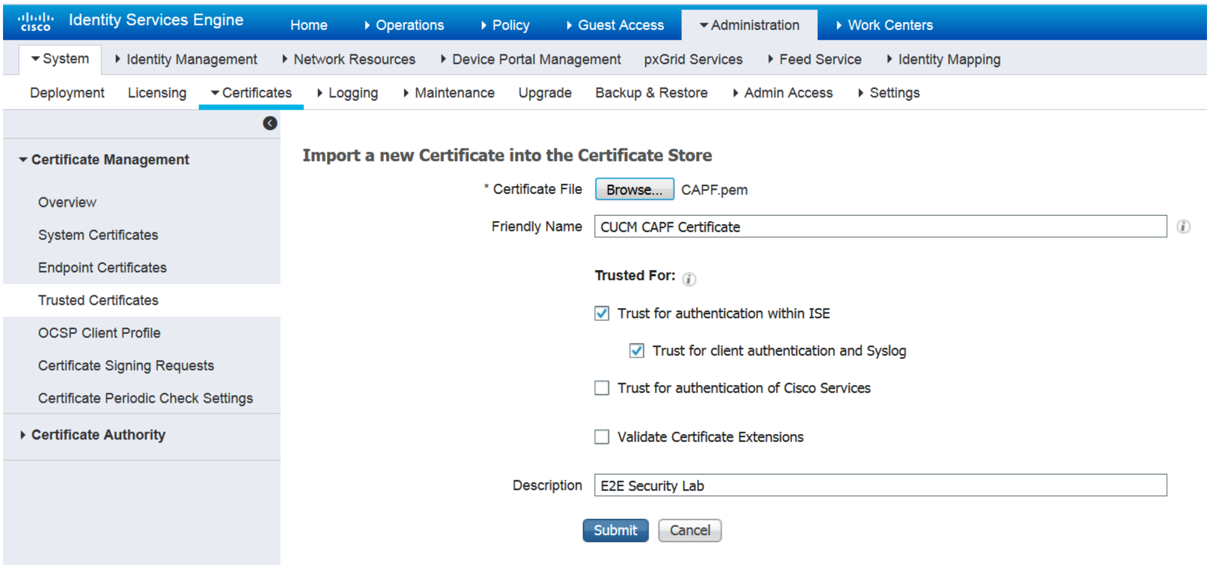
Upload the CUCM CAPF Certificate

The CAPF service signs a phone or video device’s LSC. To support certificate based EAP-TLS authentication you need to add the CAPF certificate to the ISE’s Trusted Certificate store.

Log onto ISE using: https://198.18.133.27/admin (admin/C1sco12345)

Say No to the Assistant Wizard.

Navigate to the Trusted Certificates GUI, Administration>System>Certificates, and import the CAPF cert that you previously downloaded from CUCM onto your local PC.



Import a new Certificate into the Certificate Store

* Certificate File: CAPF.pem

Friendly Name: CUCM CAPF Certificate

Trusted For:

☑ Trust for authentication within ISE

☑ Trust for client authentication and Syslog

☐ Trust for authentication of Cisco Services

☐ Validate Certificate Extensions

Description: E2E Security Lab

After you have uploaded CAPF you should see it displayed in the Trusted Certificate store.

5) Configure the lab's edge switch on ISE

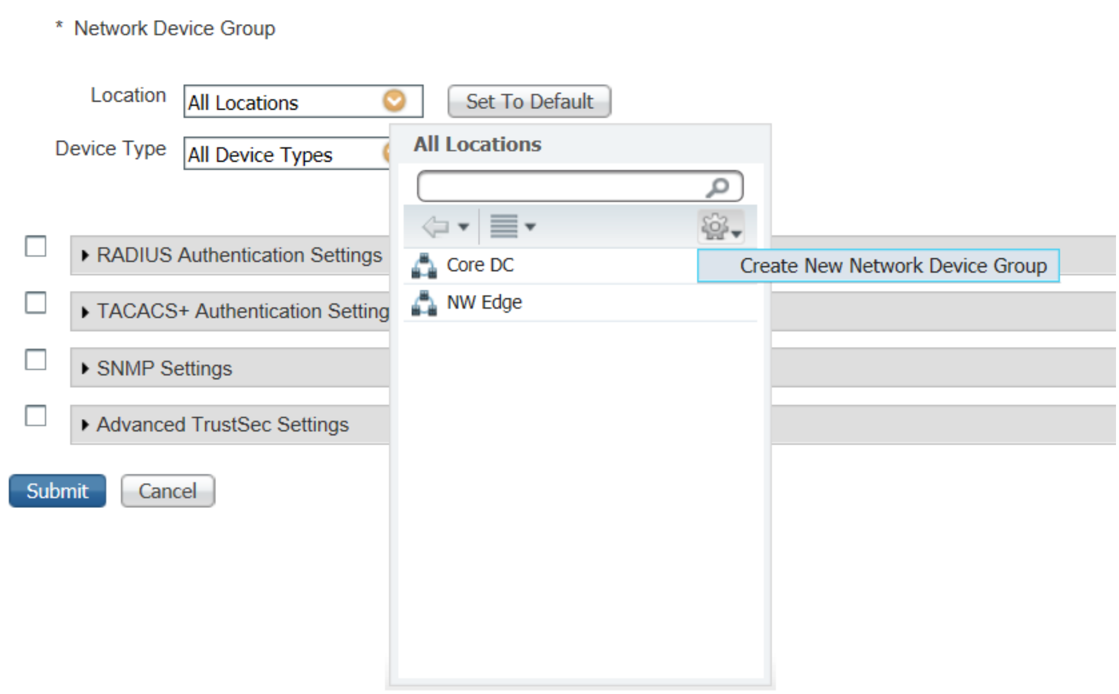
In our lab we only have a single edge switch, so we are going to define it and initially only configure it for RADIUS. Navigate to Administration>Network Resources>Network Devices

Configuration Help:

- Ensure the Name matches the Switch Hostname: CPE-E2E-Seclab-Sw
- Use 198.18.192.2 for the switch's IP Address
- Model Name and SW Type are free text, use C3560 and 12.255rEX11 respectively
- Create Location and Device Groups

The first time you do this it's a bit tricky. Refer to the diagram below. To create and configure a Location: Press the orange arrow button and then click the COG icon. Then use the "Create New Network Device Group" to add and allocate a Location to your edge switch.

If you get stuck, don't burn too many cycles. Just ask a Proctor for some help.



* Network Device Group

Location: All Locations

Device Type: All Device Types

☐ RADIUS Authentication Settings

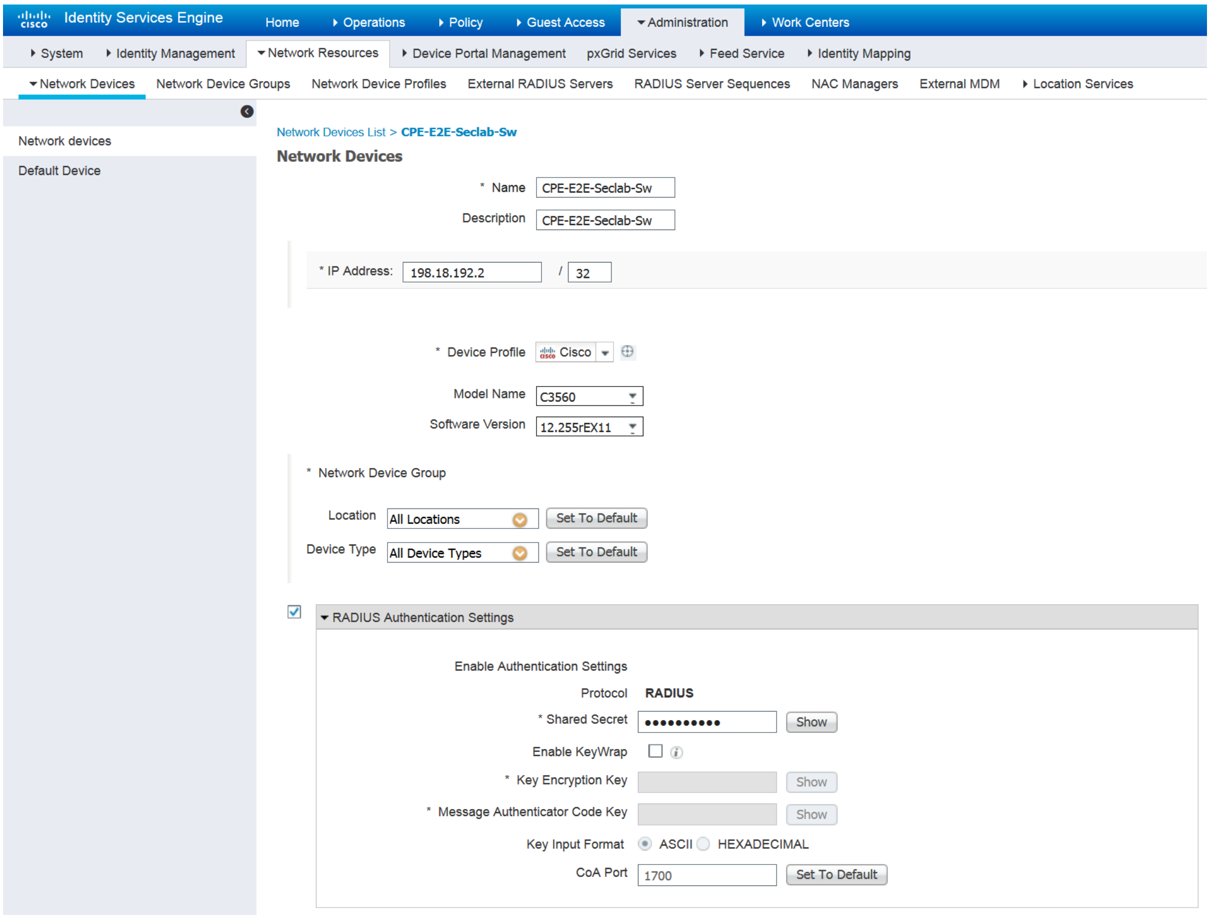
☐ TACACS+ Authentication Setting

☐ SNMP Settings

☐ Advanced TrustSec Settings

Then repeat this for the Device Type.

Enable Radius and use C1sco12345 as the RADIUS Shared Secret, this will always need to match what is defined on the access switch



Network Devices

* Name: CPE-E2E-Seclab-Sw

Description: CPE-E2E-Seclab-Sw

* IP Address: 198.18.192.2 / 32

* Device Profile: Cisco

Model Name: C3560

Software Version: 12.255rEX11

* Network Device Group

Location: All Locations

Device Type: All Device Types

☑ RADIUS Authentication Settings

Enable Authentication Settings

Protocol: **RADIUS**

* Shared Secret: ••••••••••

Enable KeyWrap: ☐

* Key Encryption Key:

* Message Authenticator Code Key:

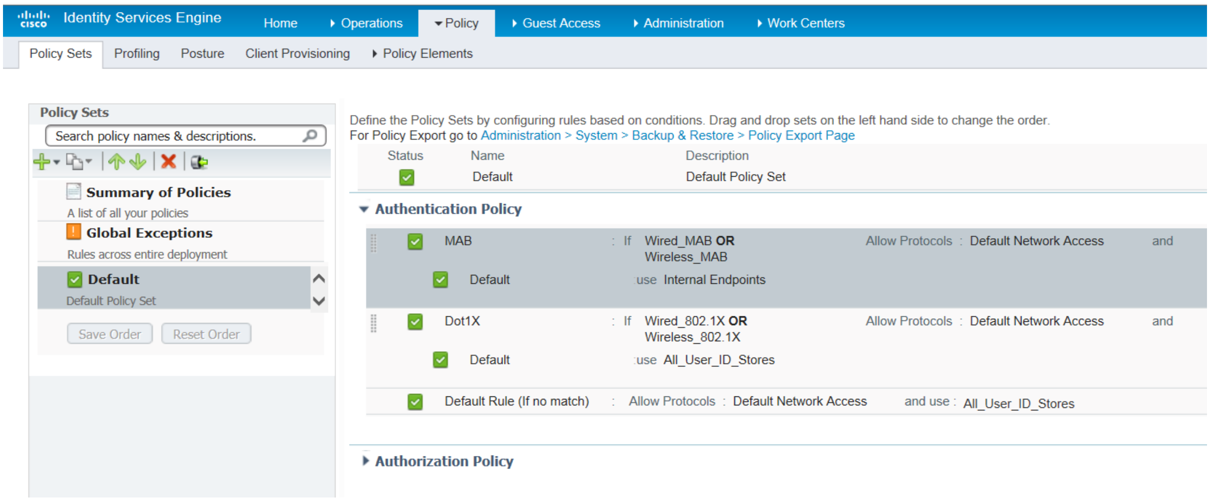
Key Input Format: ● ASCII ○ HEXADECIMAL

CoA Port: 1700

Note: Any Radius request from a device that is not defined in ISE will be immediately dropped.

6) Enabling the Authentication Policy

To save time we are going to use and modify (a little) the Default Authentication and Authorization policy. ISE can actually support more than one Policy Set but for the purposes of this lab using the Default is adequate.



Define the Policy Sets by configuring rules based on conditions. Drag and drop sets on the left hand side to change the order.
For Policy Export go to Administration > System > Backup & Restore > Policy Export Page

Status	Name	Description
✓	Default	Default Policy Set

Authentication Policy

✓ MAB : If Wired_MAB **OR** Wireless_MAB Allow Protocols : Default Network Access and
✓ Default use Internal Endpoints

✓ Dot1X : If Wired_802.1X **OR** Wireless_802.1X Allow Protocols : Default Network Access and
✓ Default use All_User_ID_Stores

✓ Default Rule (If no match) : Allow Protocols : Default Network Access and use : All_User_ID_Stores

Allow Protocols: Default Network Access and use All_User_ID_Stores:

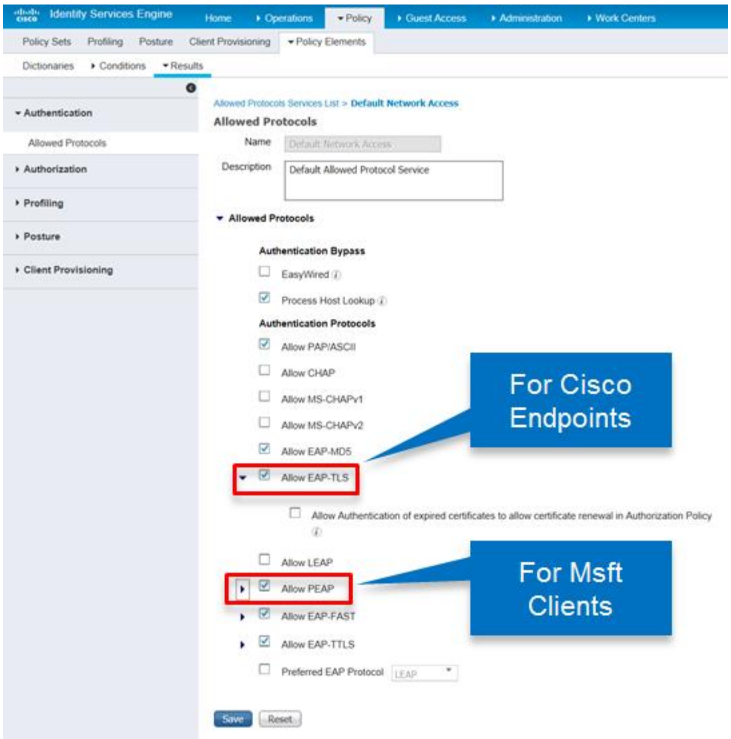
During the IEEE802.1x authentication process the Default Network Access table is used to enable/disable which protocols can be used for incoming authentications. EAP-TLS will allow the ISE server to verify a Phone’s offered LSC against the uploaded CAPF certificate. Then the All User ID Stores with dictate the how the Identify of the phone is defined in ISE. In our deployment we are using a phone’s Subject Common Name as the identity. The next few sections will walk through each of the relevant configuration screens.

Note: In the lab our default authentication policy also supports both MAB (MAC Authentication Bypass) and IEEE802.1x. We can control what authentication is used by the Phone endpoints from the access switch configuration and also the order of authentication mechanisms the switch will try. In our lab we will only use “dot1x”. We could also delete the MAB policy completely from ISE if it’s not required for the security deployment.

7) Default Network Access

As mentioned previously the authentication protocols allowed on the system are determined by the Default Network Access template. ISE is configured to verify the identity of the Collaboration devices through the Default Network Access configuration.

Navigate to the Default Network Access configuration screen to check if EAP-TLS is enabled. Policy>Policy Elements>Results>Authentication>Allowed Protocols



Allowed Protocols

Name: Default Network Access

Description: Default Allowed Protocol Service

Allowed Protocols

Authentication Bypass

☐ EasyWired

☑ Process Host Lookup

Authentication Protocols

☑ Allow PAP/ASCII

☐ Allow CHAP

☐ Allow MS-CHAPv1

☐ Allow MS-CHAPv2

☑ Allow EAP-MD5

☑ Allow EAP-TLS

☐ Allow Authentication of expired certificates to allow certificate renewal in Authorization Policy

☐ Allow LEAP

☑ Allow PEAP

☑ Allow EAP-FAST

☑ Allow EAP-TTLS

☐ Preferred EAP Protocol: LEAP

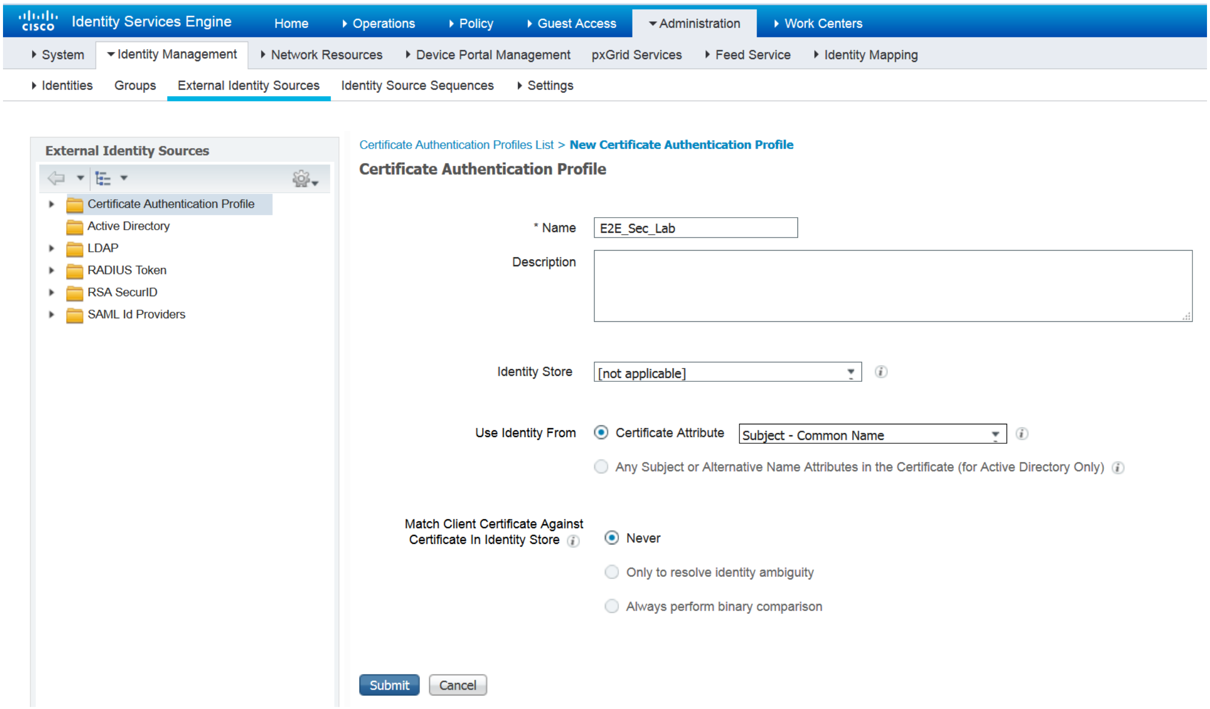
Note: In our lab we don't have IEEE 802.1x switched on the Jabber clients as they sit on VMs that connect into a Nexus1000v, which does not support IEEE802.1x. In a production deployment, the windows client supplicant could use PEAP and any unused protocols would be disabled.

8) Defining the Certificate Authentication Profile

Now go to the Certificate Authentication Profile section of the ISE configuration.
Administration>Identity Management>External Identity Services>Certificate Authentication Profile

Create a new Certificate Authentication Profile and ensure the "Use Identity From Certificate Attribute" is set to use the Subject – Common Name.

We're doing this so that the phone's LSC's Subject - Common Name will be the Identity that we'll use for the authorization part of the IEEE802.1x operation described later.



Certificate Authentication Profiles List > **New Certificate Authentication Profile**

Certificate Authentication Profile

* Name: E2E_Sec_Lab

Description:

Identity Store: [not applicable]

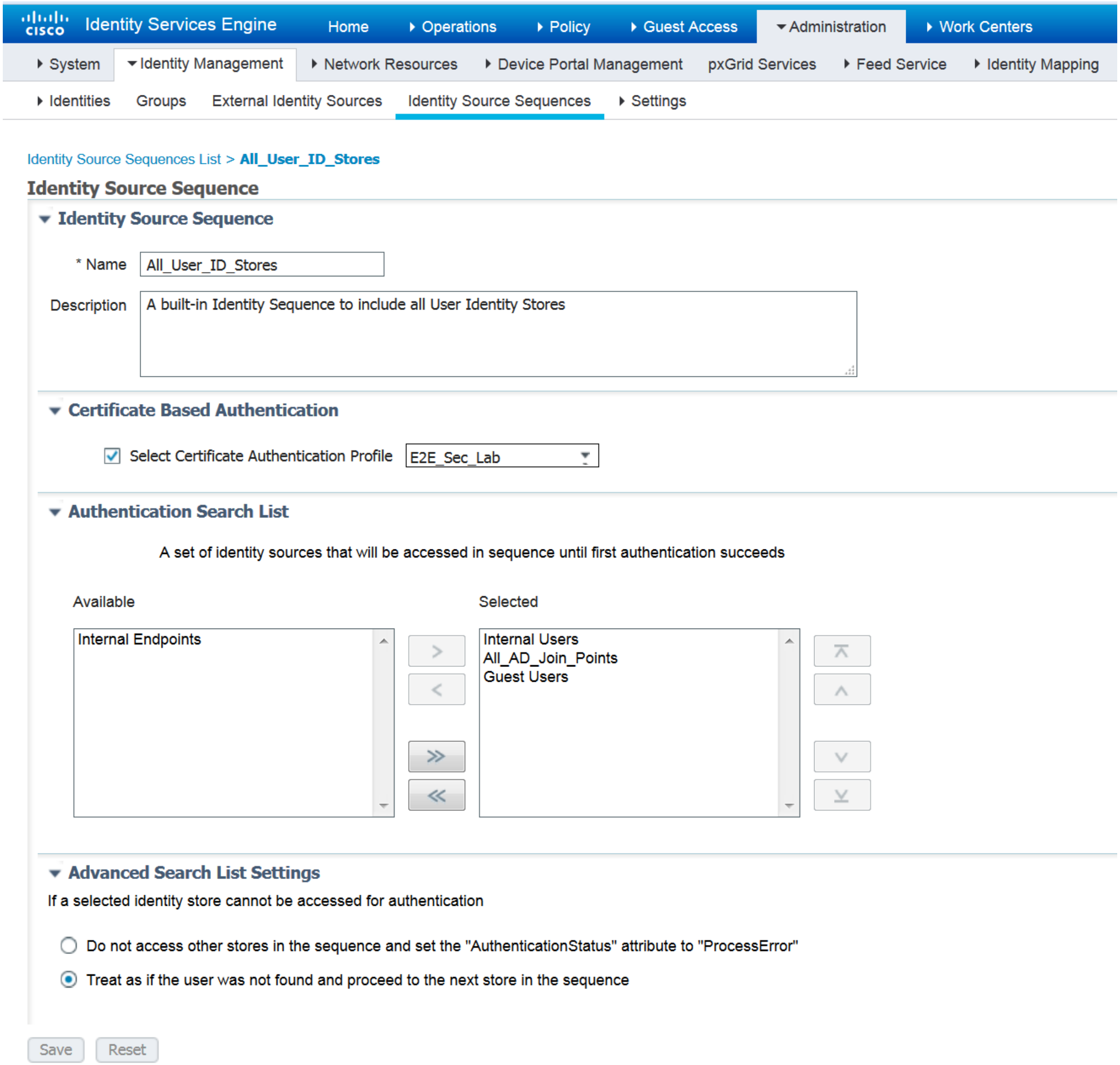
Use Identity From:
● Certificate Attribute: Subject - Common Name
○ Any Subject or Alternative Name Attributes in the Certificate (for Active Directory Only)

Match Client Certificate Against Certificate In Identity Store:
● Never
○ Only to resolve identity ambiguity
○ Always perform binary comparison

9) Checking the Authentication Identity Store

We now add our new Certificate Authentication Profile to the default All User Identity Store we discussed previously.

Go to Administration>Identity Management>Identity Source Sequence and select the All_User_ID_Stores



Identity Source Sequence

Identity Source Sequence

* Name: All_User_ID_Stores

Description: A built-in Identity Sequence to include all User Identity Stores

Certificate Based Authentication

☑ Select Certificate Authentication Profile: E2E_Sec_Lab

Authentication Search List

A set of identity sources that will be accessed in sequence until first authentication succeeds

Available:
Internal Endpoints

Selected:
Internal Users
All_AD_Join_Points
Guest Users

Advanced Search List Settings

If a selected identity store cannot be accessed for authentication

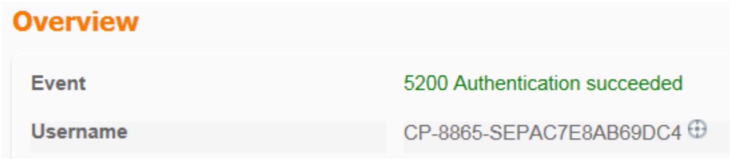
○ Do not access other stores in the sequence and set the "AuthenticationStatus" attribute to "ProcessError"

● Treat as if the user was not found and proceed to the next store in the sequence

Enabling Authorization:

10) Using SEP as a Flag in our Authorization Policy

An example of the Subject-CN of a phone is shown below. The common syntax across all Cisco phones is “SEP”, which is a legacy acronym from the early days of CallManager. Ask if you don’t know what it stands for and want to find out.

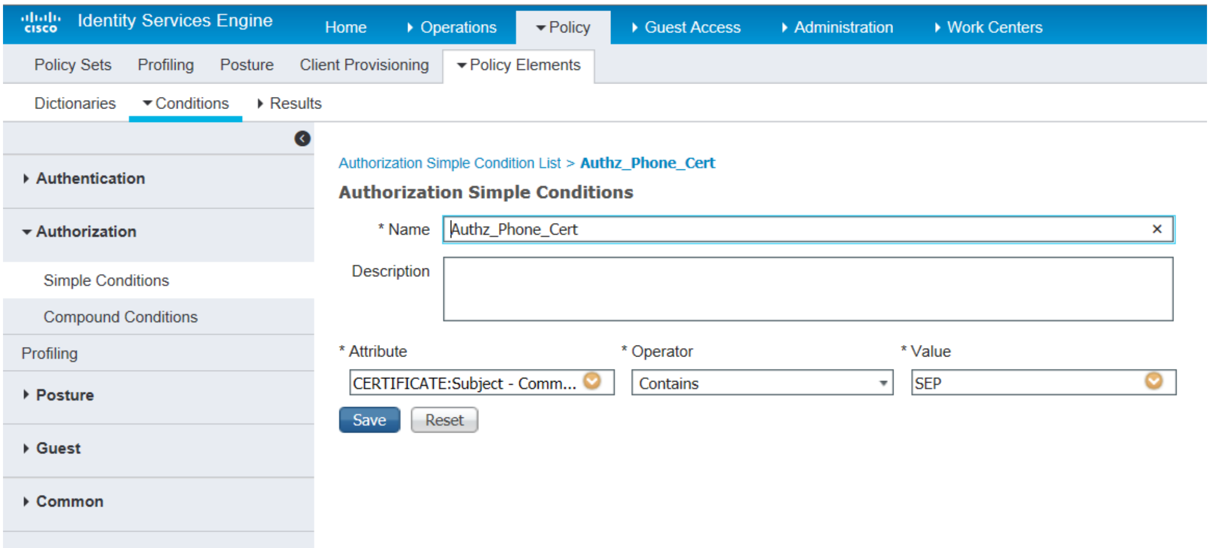


Overview

Event	5200 Authentication succeeded
Username	CP-8865-SEPAC7E8AB69DC4

In our lab we are just going to use it as a flag to specifically identity a Cisco phone, which then allows us to apply a basic Authorization policy for the phone.

The first thing we do is to navigate to the Authorization Simple Conditions GUI, as shown in the screenshot below. Policy>Conditions>Authorization>Simple Conditions



Authorization Simple Condition List > **Authz_Phone_Cert**

Authorization Simple Conditions

* Name: Authz_Phone_Cert

Description:

* Attribute: CERTIFICATE:Subject - Comm...

* Operator: Contains

* Value: SEP

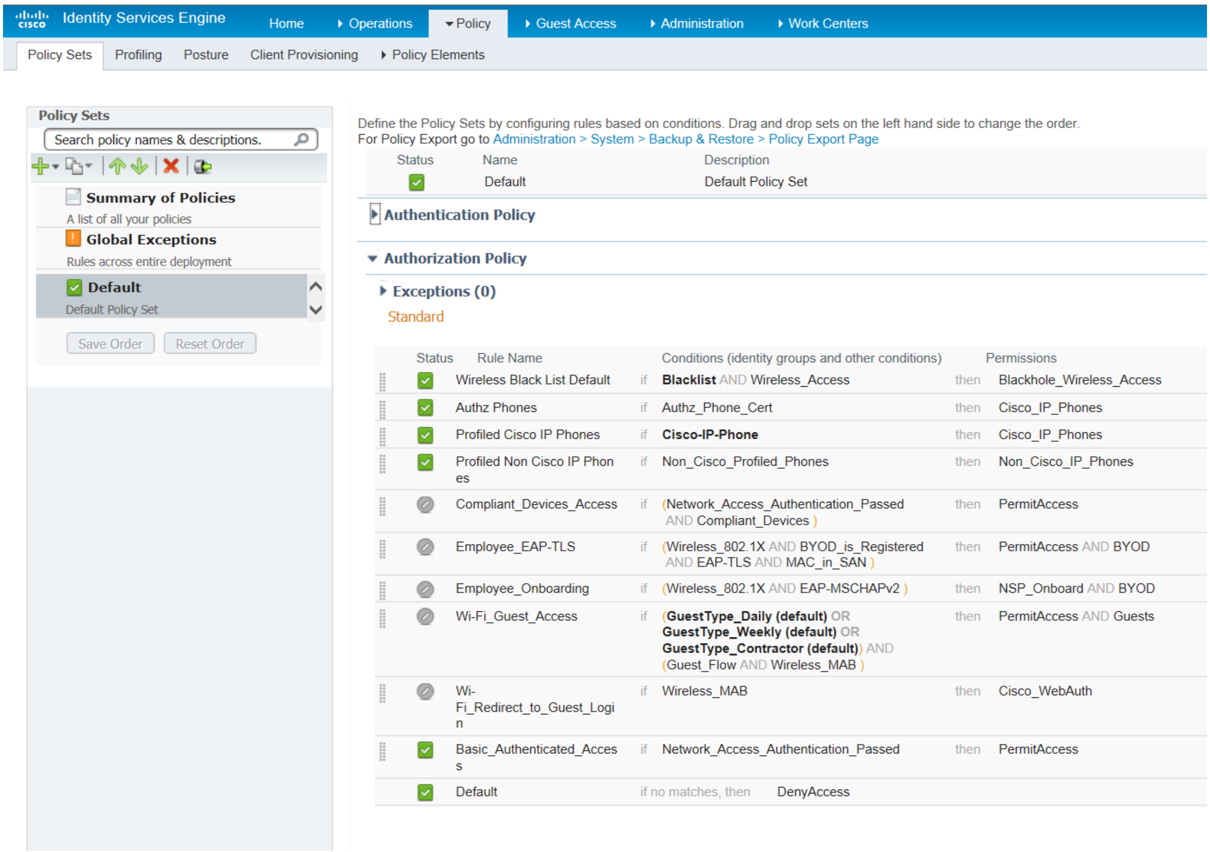
Create the above condition. From the Attribute setting use the orange arrow button to select the correct Certificate Attribute. In the Value box manually type in the “SEP”.

Note: Just in case you didn’t know SEP = Selsius Ethernet Phone

11) Authorization Policy

We are now going to create a new Authorization Rule “Authz Phones”, and then if the phone presents a certificate that is authenticated and the certificate also has “SEP” in the Subject-CN, we’ll add the phone to the Cisco_IP_Phone profile, which (as we will see in a moment) contains a set of basic Network Access permissions.

Policy>Policy Sets>Default



Define the Policy Sets by configuring rules based on conditions. Drag and drop sets on the left hand side to change the order.
For Policy Export go to Administration > System > Backup & Restore > Policy Export Page

Status	Name	Description
✓	Default	Default Policy Set

Authentication Policy

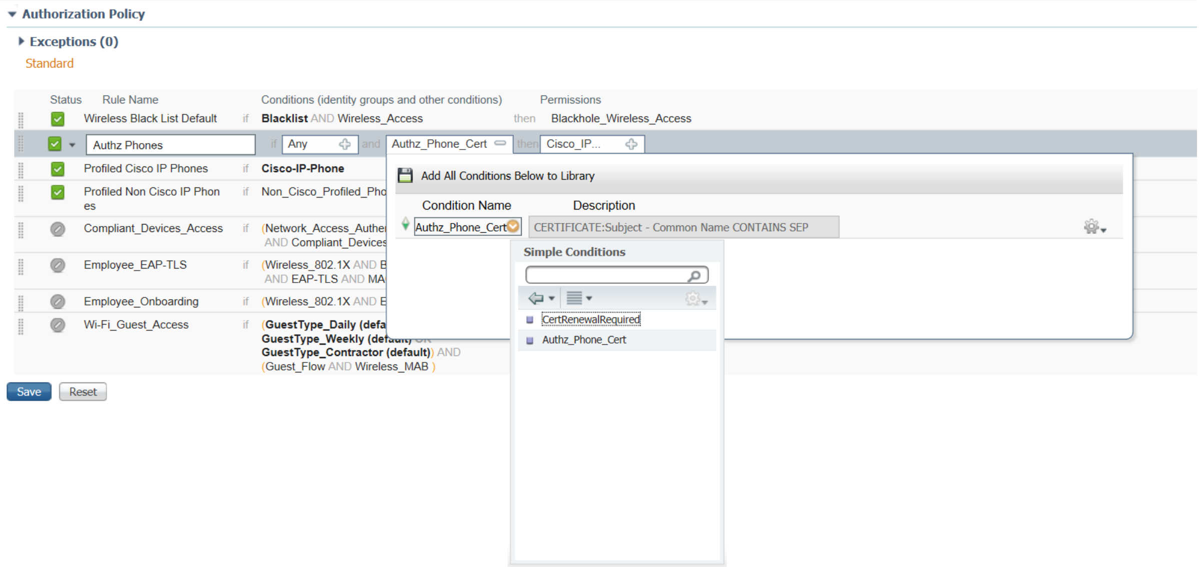
Authorization Policy

Exceptions (0)

Standard

Status	Rule Name		Conditions (identity groups and other conditions)		Permissions
✓	Wireless Black List Default	if	**Blacklist** AND Wireless_Access	then	Blackhole_Wireless_Access
✓	Authz Phones	if	Authz_Phone_Cert	then	Cisco_IP_Phones
✓	Profiled Cisco IP Phones	if	**Cisco-IP-Phone**	then	Cisco_IP_Phones
✓	Profiled Non Cisco IP Phones	if	Non_Cisco_Profiled_Phones	then	Non_Cisco_IP_Phones
⊘	Compliant_Devices_Access	if	(Network_Access_Authentication_Passed AND Compliant_Devices)	then	PermitAccess
⊘	Employee_EAP-TLS	if	(Wireless_802.1X AND BYOD_is_Registered AND EAP-TLS AND MAC_in_SAN)	then	PermitAccess AND BYOD
⊘	Employee_Onboarding	if	(Wireless_802.1X AND EAP-MSCHAPv2)	then	NSP_Onboard AND BYOD
⊘	Wi-Fi_Guest_Access	if	(**GuestType_Daily (default)** OR **GuestType_Weekly (default)** OR **GuestType_Contractor (default)**) AND (Guest_Flow AND Wireless_MAB)	then	PermitAccess AND Guests
⊘	Wi-Fi_Redirect_to_Guest_Login	if	Wireless_MAB	then	Cisco_WebAuth
✓	Basic_Authenticated_Access	if	Network_Access_Authentication_Passed	then	PermitAccess
✓	Default		if no matches, then		DenyAccess

Use the "Edit" button on the right hand side of the GUI (not shown in the above screenshot) to add a rule below the Wireless Black List Default. All the other rules shown are default ones that come with ISE, and can be deleted in a production environment if not used.



Authorization Policy

Exceptions (0)

Standard

Status	Rule Name		Conditions (identity groups and other conditions)		Permissions
✓	Wireless Black List Default	if	**Blacklist** AND Wireless_Access	then	Blackhole_Wireless_Access
✓	Authz Phones	if	Any and Authz_Phone_Cert	then	Cisco_IP...
✓	Profiled Cisco IP Phones	if	**Cisco-IP-Phone**		
✓	Profiled Non Cisco IP Phones	if	Non_Cisco_Profiled_Pho		
⊘	Compliant_Devices_Access	if	(Network_Access_Authe AND Compliant_Devices		
⊘	Employee_EAP-TLS	if	(Wireless_802.1X AND B AND EAP-TLS AND MA		
⊘	Employee_Onboarding	if	(Wireless_802.1X AND E		
⊘	Wi-Fi_Guest_Access	if	(**GuestType_Daily (defa** **GuestType_Weekly (def** **GuestType_Contractor (default)**) AND (Guest_Flow AND Wireless_MAB)		

Condition Name	Description
Authz_Phone_Cert	CERTIFICATE:Subject - Common Name CONTAINS SEP

If you are not familiar with ISE the configuration of the new rule is not particularly intuitive. You type in the Rule Name, then you leave the "if" statement as "Any", then for the "and" statement press the “+” sign and find the Authz_Phone_Cert condition you created earlier. In the “then” statement box you need to press the “+” sign and select the Cisco_IP_Phones from the Standard Group.

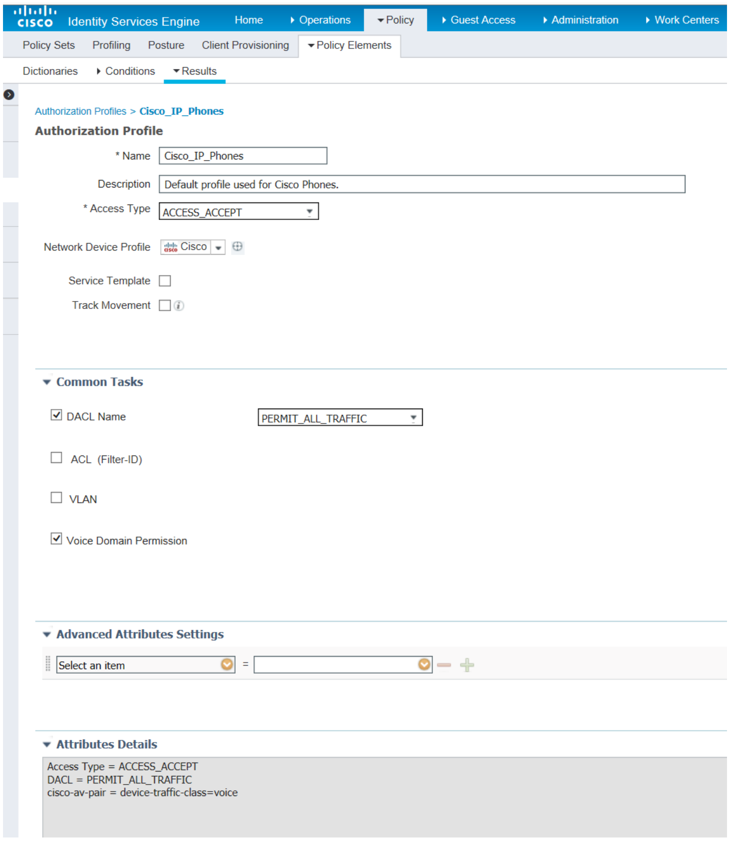
If you get stuck or lost, ask a Proctor for help.

Note: By default ISE creates two default rules for telephony devices. These are Profiled Cisco IP Phones and Profiled Non Cisco IP Phones. These are not needed for our lab and could be removed.

12) Review the Cisco_IP_Phone Authorization Profile

Policy>Policy Elements>Results>Authorization>Authorization Profiles

Our Authorization profile “Cisco_IP_Phones” downloads the PERMIT_ALL_TRAFFIC dynamic access control list and also allows the switch to add the phone to the switch’s locally configured Voice VLAN.



Authorization Profile

* Name: Cisco_IP_Phones

Description: Default profile used for Cisco Phones.

* Access Type: ACCESS_ACCEPT

Network Device Profile: Cisco

Service Template ☐

Track Movement ☐

Common Tasks

☑ DACL Name: PERMIT_ALL_TRAFFIC

☐ ACL (Filter-ID)

☐ VLAN

☑ Voice Domain Permission

Advanced Attributes Settings

Select an item =

Attributes Details

Access Type = ACCESS_ACCEPT
DACL = PERMIT_ALL_TRAFFIC
cisco-av-pair = device-traffic-class=voice

Once we have completed the configuration on ISE, we’d normally need to enable our access switches for 802.1x.

13) Configuring IEEE802.1x on the Access Switch

To save time and make life easier the IEEE802.1x configuration has already been added to the switch. For reference the relevant AAA and dot1x commands used for our simple 802.1x configuration are provided below. The full switch configuration is provided in the appendix.

The global 802.1x commands used in the lab are standard and more details about specific commands can be found on the Cisco web site or using a web search. Just note that the pac (protected access credentials) key in an access switch maps onto the shared secret in ISE. This is C1sco12345 in our lab.

Be sure to make sure that 802.1x authentication is enabled on the Phone. You can check this from the Admin Settings on the phone itself.

As per the earlier diagram, the example below uses FastEthernet 0/11 as the dot1x port.

```
aaa new-model
!
aaa authentication dot1x default group radius
aaa authorization network default group radius
aaa authorization network auth-list-name group radius
aaa accounting dot1x default start-stop group radius
!
aaa server radius dynamic-author
 client 198.18.133.27 server-key C1sco12345
!
aaa session-id common
dot1x system-auth-control
!
interface FastEthernet 0/11
 description dot1x port for TrustSec Lab
 switchport access vlan 100
 switchport mode access
 switchport voice vlan 101
 authentication host-mode multi-domain
 authentication order dot1x
 authentication priority dot1x
 authentication port-control auto
 dot1x pae authenticator
 spanning-tree portfast
!
radius server ise
```

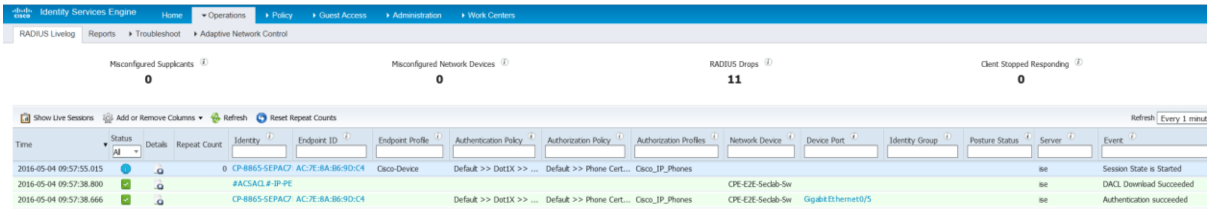
```
address ipv4 198.18.133.27 auth-port 1812 acct-port 1813
pac key C1sco12345
```

14) Testing for Correct Operation

If you haven't already plug the phone into Port 11 of the switch and ensure IEEE802.1x is enabled.

Operations>RADIUS Livelog

Apart from the phone registering, the simplest way to check if the Access Switch is passing the RADIUS authentication request to ISE and to ensure the Phone is indeed authenticated is to review ISE's RADIUS Livelog. An example of which is show below:



Misconfigured Supplicants 0

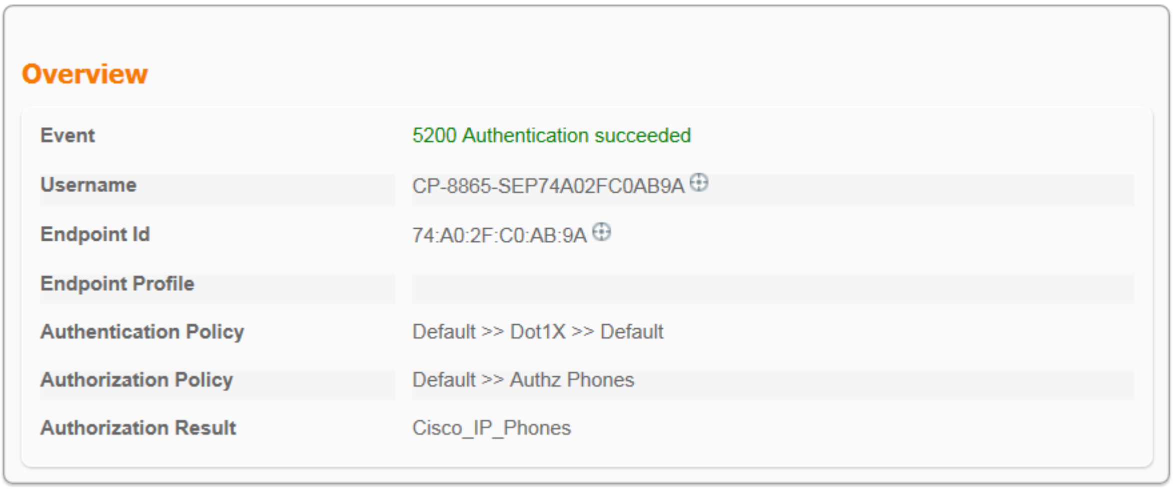
Misconfigured Network Devices 0

RADIUS Drops 11

Client Stopped Responding 0

Time	Status	Details	Repeat Count	Identity	Endpoint ID	Endpoint Profile	Authentication Policy	Authorization Policy	Authorization Profiles	Network Device	Device Port	Identity Group	Posture Status	Server	Event
2016-05-04 09:57:55.015	●		0	CP-8865-SEPAC7	AC:7E:8A:B6:9D:C4	Cisco-Device	Default >> Dot1X >> ...	Default >> Phone Cert...	Cisco_IP_Phones					ise	Session State is Started
2016-05-04 09:57:38.800	✓			#ACSACL#-IP-PE						CPE-E2E-Seclab-Sw				ise	DACL Download Succeeded
2016-05-04 09:57:38.666	✓			CP-8865-SEPAC7	AC:7E:8A:B6:9D:C4		Default >> Dot1X >> ...	Default >> Phone Cert...	Cisco_IP_Phones	CPE-E2E-Seclab-Sw	GigabitEthernet0/5			ise	Authentication succeeded

One thing you should do is to click on the endpoint session information (blue circle) and verify that you are hitting the Authorization you previously created.



Overview

Event	5200 Authentication succeeded
Username	CP-8865-SEP74A02FC0AB9A
Endpoint Id	74:A0:2F:C0:AB:9A
Endpoint Profile	
Authentication Policy	Default >> Dot1X >> Default
Authorization Policy	Default >> Authz Phones
Authorization Result	Cisco_IP_Phones

If your phone does not register and you cannot spot a configuration error, ask a Proctor to help you troubleshoot.

TrustSec Configuration

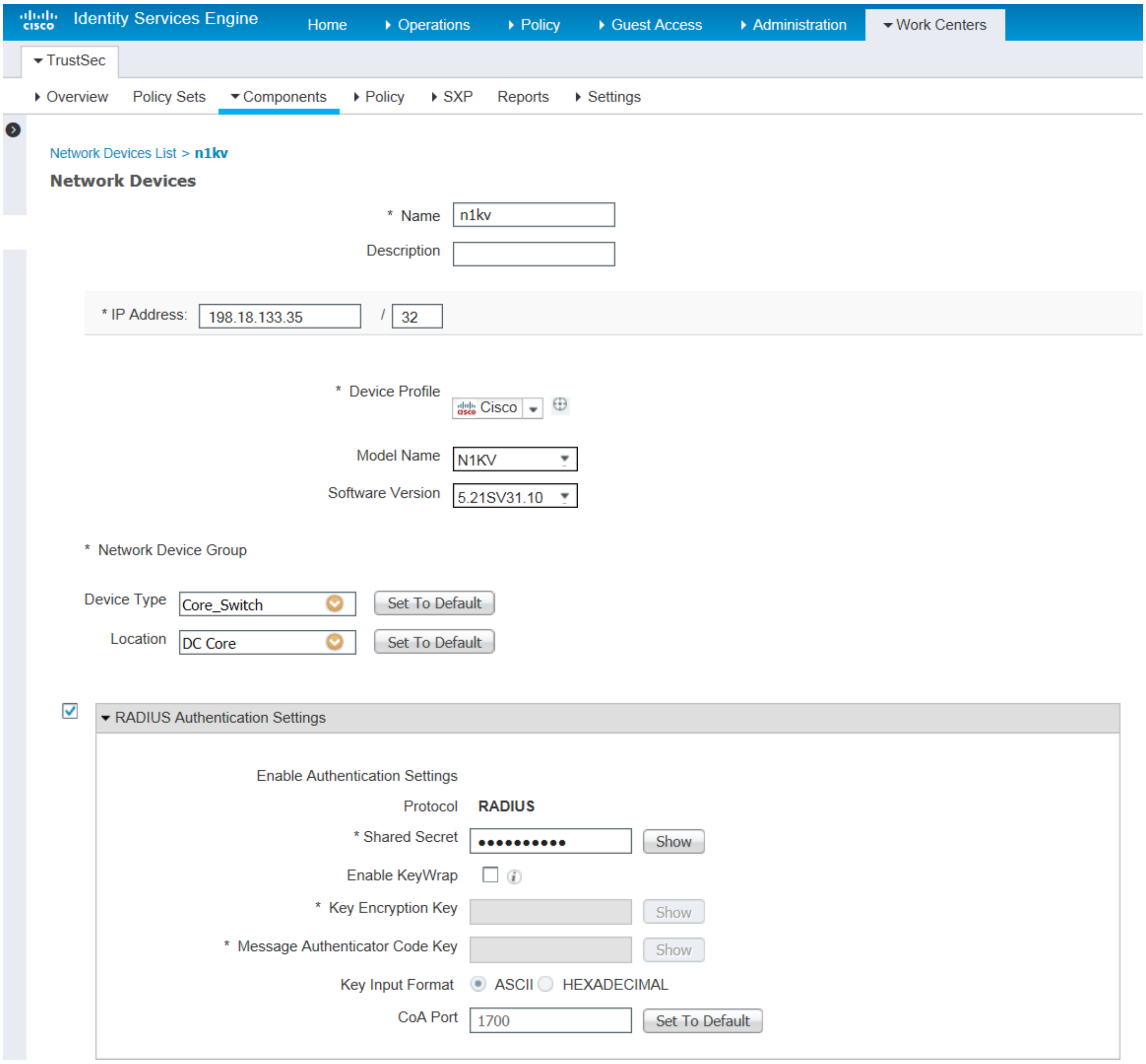
Before reading the rest of the TrustSec section of this document ensure you're familiar with its generic classification, propagation and enforcement capabilities. If you skipped the earlier sections of this document that covered these, please take a few minutes to read them now. It will hopefully make what you do next more meaningful.

The steps we will take to configure the lab's TrustSec deployment are provided below:

1) Define Nexus 1000VTrustSec Device in ISE

Configure the Default and Radius Parameters as shown. Create a suitable Device Type and Location. Just repeat the procedure you used for the Edge Switch. Make sure that the "Name" (n1kv) and "Shared Secret" (C1sco12345) entries match what are configured on the Nexus 1000V. Use n1kv and 5.2.1SV31.10 for the model name and Software Version. The IP Address of the Nexus 1000V is: 198.18.133.35

Work Centers>Components>Network Devices



Network Devices List > **n1kv**

Network Devices

* Name: n1kv

Description:

* IP Address: 198.18.133.35 / 32

* Device Profile: Cisco

Model Name: N1KV

Software Version: 5.21SV31.10

* Network Device Group

Device Type: Core_Switch

Location: DC Core

☑ RADIUS Authentication Settings

Enable Authentication Settings

Protocol: **RADIUS**

* Shared Secret: ●●●●●●●●●●●

Enable KeyWrap: ☐

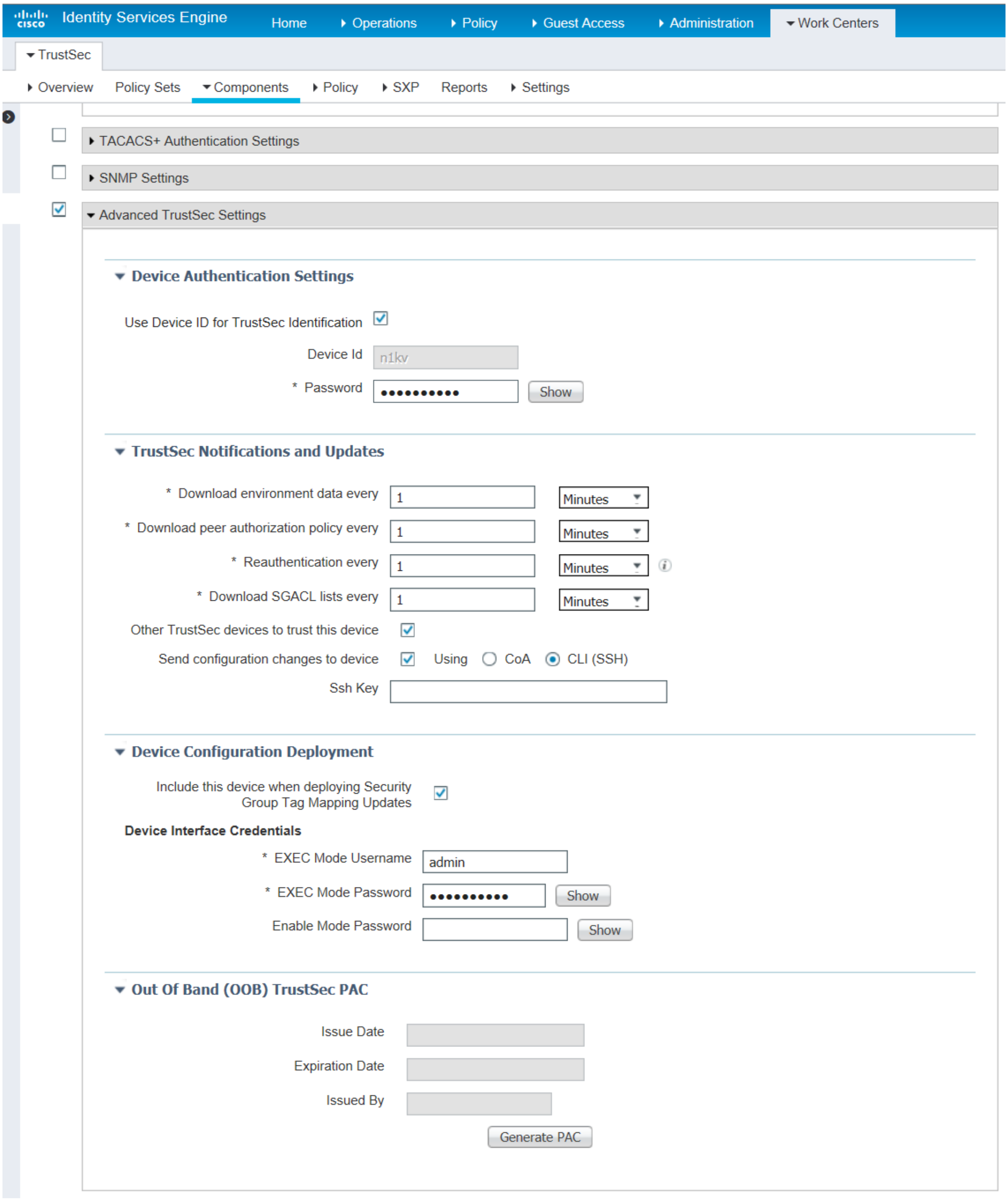
* Key Encryption Key:

* Message Authenticator Code Key:

Key Input Format: ● ASCII ○ HEXADECIMAL

CoA Port: 1700

Now enter the TrustSec configuration as shown below. All passwords should reflect those used on the Nexus 1000V. In all cases it should be: C1sco12345



☐ TACACS+ Authentication Settings

☐ SNMP Settings

☑ Advanced TrustSec Settings

Device Authentication Settings

Use Device ID for TrustSec Identification ☑

Device Id: n1kv

* Password: ●●●●●●●●●●

TrustSec Notifications and Updates

* Download environment data every: 1 Minutes

* Download peer authorization policy every: 1 Minutes

* Reauthentication every: 1 Minutes

* Download SGACL lists every: 1 Minutes

Other TrustSec devices to trust this device ☑

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

Ssh Key:

Device Configuration Deployment

Include this device when deploying Security Group Tag Mapping Updates ☑

Device Interface Credentials

* EXEC Mode Username: admin

* EXEC Mode Password: ●●●●●●●●●●

Enable Mode Password:

Out Of Band (OOB) TrustSec PAC

Issue Date:

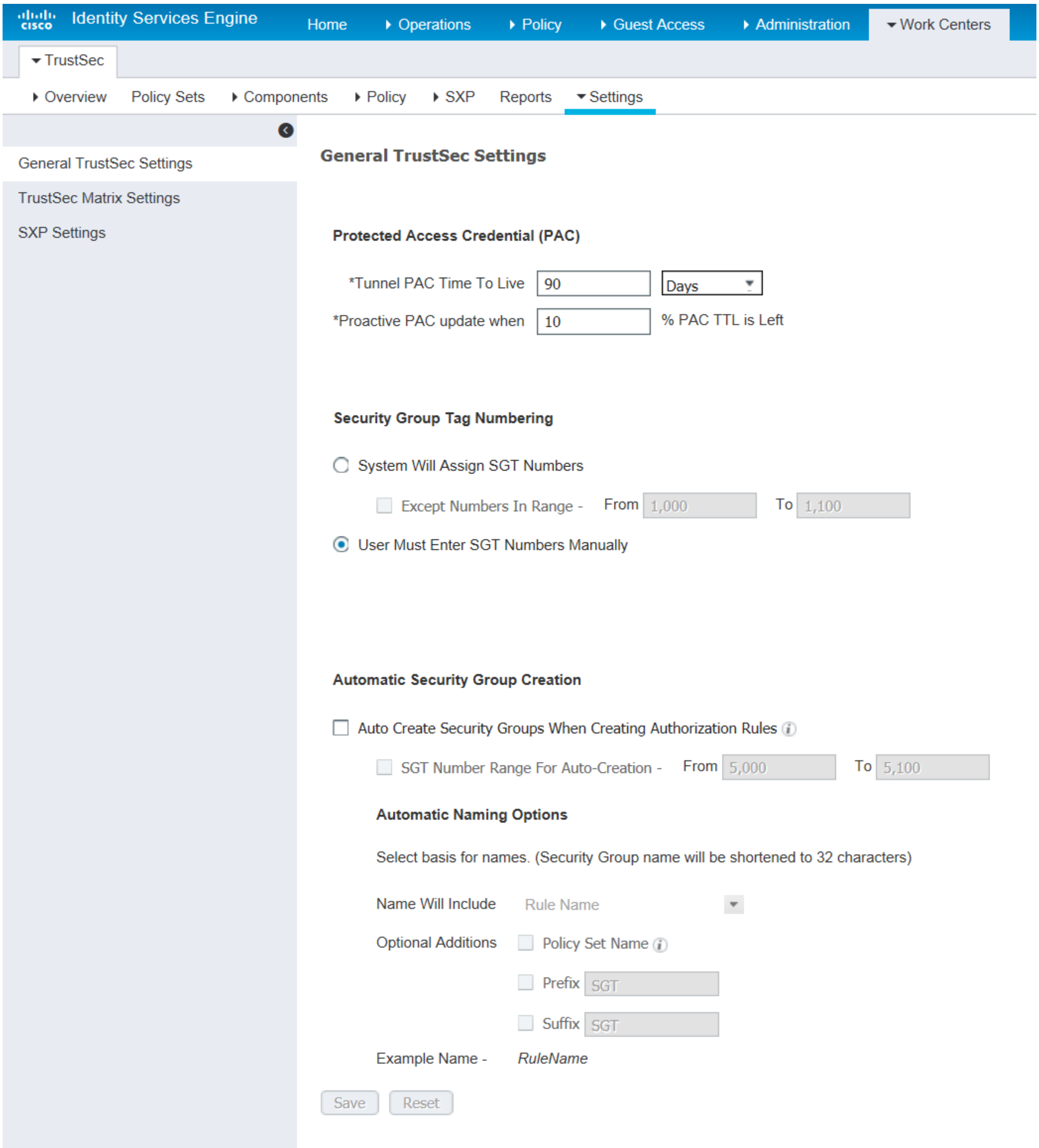
Expiration Date:

Issued By:

ISE will use CLI commands to download TrustSec data and SGACLs to the Nexus. We don't need to add a SSH Key as this will be uploaded automatically. In our lab there is no enable password on the switch so leave this blank. Note: The Nexus 1000V does not support Change of Authorization RADIUS updates, so CoA will not be enabled. However, we don't lose anything by using the CLI, it's just that some devices in the portfolio support this and some customers prefer to use RADIUS to download TrustSec updates.

2) General TrustSec Settings

Navigate to the TrustSec Settings GUI and enable “User Must Enter SGT Numbers Manually”.



General TrustSec Settings

Protected Access Credential (PAC)

*Tunnel PAC Time To Live 90 Days

*Proactive PAC update when 10 % PAC TTL is Left

Security Group Tag Numbering

○ System Will Assign SGT Numbers

☐ Except Numbers In Range - From 1,000 To 1,100

● User Must Enter SGT Numbers Manually

Automatic Security Group Creation

☐ Auto Create Security Groups When Creating Authorization Rules

☐ SGT Number Range For Auto-Creation - From 5,000 To 5,100

Automatic Naming Options

Select basis for names. (Security Group name will be shortened to 32 characters)

Name Will Include Rule Name

Optional Additions ☐ Policy Set Name

☐ Prefix SGT

☐ Suffix SGT

Example Name - *RuleName*

The above setting change, simply allows us to control the SGT number allocation for our collaboration endpoints and services.

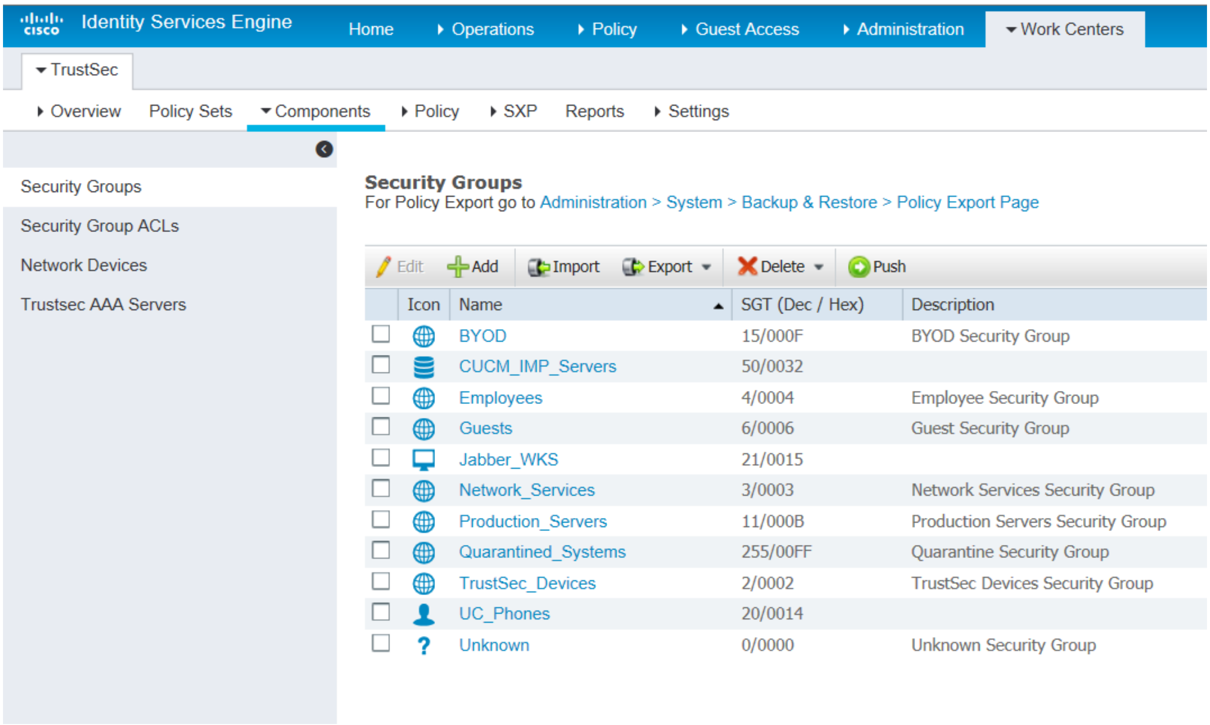
3) System Security Groups

The Security Group table below shows the SGT mapping we are going to use for the collaboration assets. In our lab we are going to group the CUCM and IMP servers (CUCM_IMP_Servers) together under a single SGT (SGT50). In a production you could potentially split these into two separate SGTs. In a real life deployment you would also very likely want to create SGTs for your CUBE/Router Gateways and also allocate SGTs to your peripheral Collaboration devices/services such as MCUs and Unity Connection.

Any phone device (UC_Phones) will receive a SGT mapping of 20 and Jabber devices (Jabber_Wks) on WKS3 and WKS4 will be allocated SGT21.

Navigate to Work Centers>TrustSec>Components>Security Groups and add the following SGTs:

• CUCM_IMP_Servers	50
• UC_Phones	20
• Jabber_WKS	21



Security Groups

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

	Icon	Name	SGT (Dec / Hex)	Description
☐		BYOD	15/000F	BYOD Security Group
☐		CUCM_IMP_Servers	50/0032	
☐		Employees	4/0004	Employee Security Group
☐		Guests	6/0006	Guest Security Group
☐		Jabber_WKS	21/0015	
☐		Network_Services	3/0003	Network Services Security Group
☐		Production_Servers	11/000B	Production Servers Security Group
☐		Quarantined_Systems	255/00FF	Quarantine Security Group
☐		TrustSec_Devices	2/0002	TrustSec Devices Security Group
☐		UC_Phones	20/0014	
☐	?	Unknown	0/0000	Unknown Security Group

Note: ISE ships with a number of pre-defined SGTs, which are not used for our lab. In a production environment the Collaboration SGTs we have defined will need to either co-exist with, or in the case of the Jabber-WKS be incorporated with, the SGTs that cover all the other critical applications/services on the network.

4) Updating the Authorization Policy to map SGT20 to an Authenticated Phone

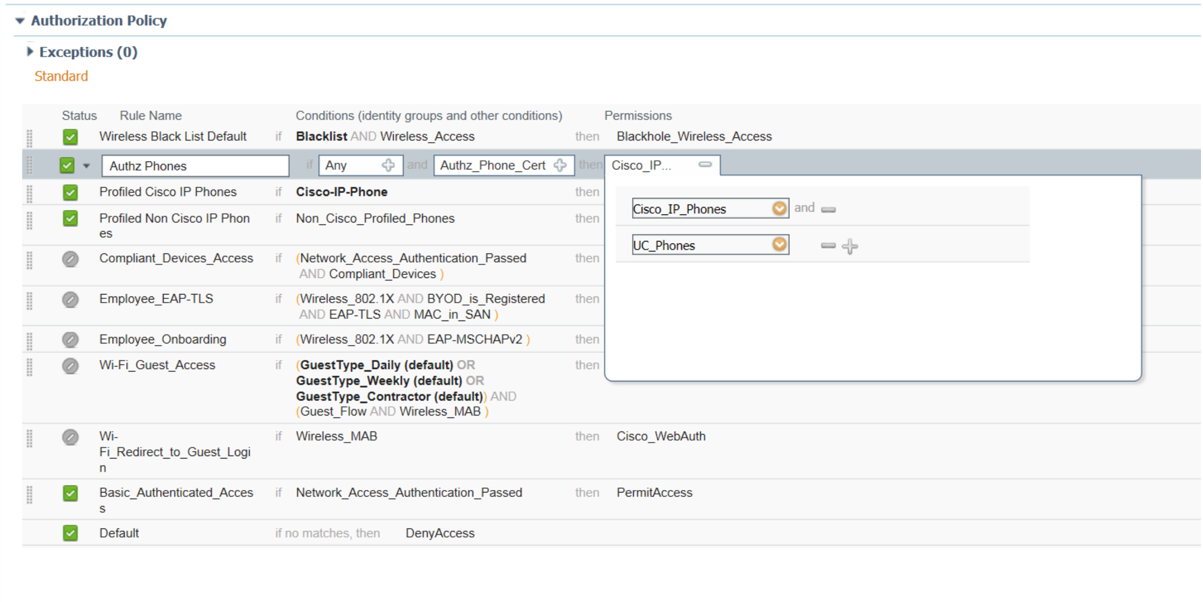
Note: You can skip this step if you did not configure IEEE802.1x. Go to step 5)

Our current IEEE802.1x Authorization policy does not automatically allocate SGT20 to our Authenticated IP Phone traffic. We now need to modify our Authz_Phones rule so that it does.

This is pretty straight forward.

Navigate to the Policy>Policy Sets>Default and edit the Authz_Phones rule so that the “then” statement includes the UC_Phones Security Group. Remember that UC_Phones is the name we have given to SGT20.

Refer to the screenshot below for guidance:



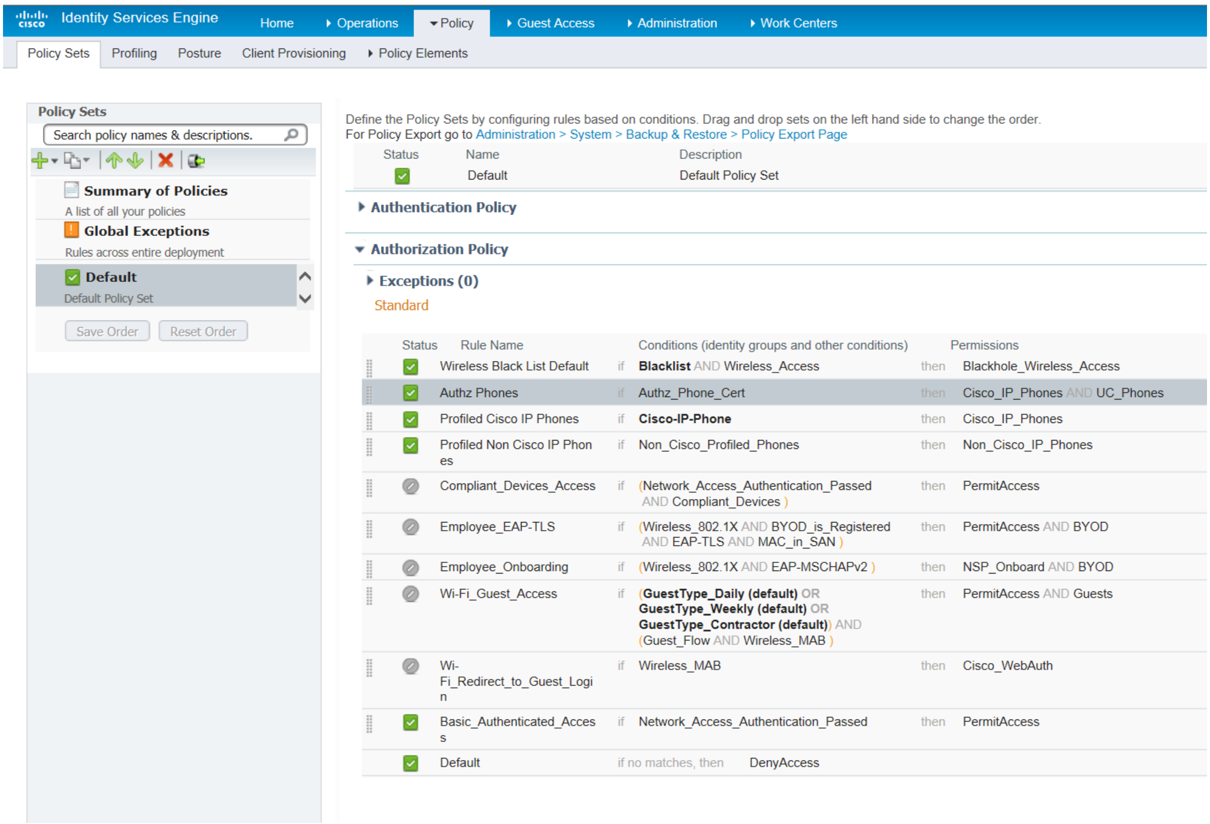
Authorization Policy

Exceptions (0)

Standard

Status	Rule Name		Conditions (identity groups and other conditions)		Permissions
✓	Wireless Black List Default	if	**Blacklist** AND Wireless_Access	then	Blackhole_Wireless_Access
✓	Authz Phones	if	Any and Authz_Phone_Cert	then	Cisco_IP... Cisco_IP_Phones and UC_Phones
✓	Profiled Cisco IP Phones	if	**Cisco-IP-Phone**	then	
✓	Profiled Non Cisco IP Phones	if	Non_Cisco_Profiled_Phones	then	
⊘	Compliant_Devices_Access	if	(Network_Access_Authentication_Passed AND Compliant_Devices)	then	
⊘	Employee_EAP-TLS	if	(Wireless_802.1X AND BYOD_is_Registered AND EAP-TLS AND MAC_in_SAN)	then	
⊘	Employee_Onboarding	if	(Wireless_802.1X AND EAP-MSCHAPv2)	then	
⊘	Wi-Fi_Guest_Access	if	(**GuestType_Daily (default)** OR **GuestType_Weekly (default)** OR **GuestType_Contractor (default)**) AND (Guest_Flow AND Wireless_MAB)	then	
⊘	Wi-Fi_Redirect_to_Guest_Login	if	Wireless_MAB	then	Cisco_WebAuth
✓	Basic_Authenticated_Access	if	Network_Access_Authentication_Passed	then	PermitAccess
✓	Default		if no matches, then		DenyAccess

After we have saved the change our modified Authorization Rule will look as follows:



Define the Policy Sets by configuring rules based on conditions. Drag and drop sets on the left hand side to change the order.
For Policy Export go to Administration > System > Backup & Restore > Policy Export Page

Status	Name	Description
☑	Default	Default Policy Set

Status	Rule Name		Conditions (identity groups and other conditions)		Permissions
☑	Wireless Black List Default	if	**Blacklist** AND Wireless_Access	then	Blackhole_Wireless_Access
☑	Authz Phones	if	Authz_Phone_Cert	then	Cisco_IP_Phones AND UC_Phones
☑	Profiled Cisco IP Phones	if	**Cisco-IP-Phone**	then	Cisco_IP_Phones
☑	Profiled Non Cisco IP Phones	if	Non_Cisco_Profiled_Phones	then	Non_Cisco_IP_Phones
⊘	Compliant_Devices_Access	if	(Network_Access_Authentication_Passed AND Compliant_Devices)	then	PermitAccess
⊘	Employee_EAP-TLS	if	(Wireless_802.1X AND BYOD_is_Registered AND EAP-TLS AND MAC_in_SAN)	then	PermitAccess AND BYOD
⊘	Employee_Onboarding	if	(Wireless_802.1X AND EAP-MSCHAPv2)	then	NSP_Onboard AND BYOD
⊘	Wi-Fi_Guest_Access	if	(**GuestType_Daily (default)** OR **GuestType_Weekly (default)** OR **GuestType_Contractor (default)**) AND (Guest_Flow AND Wireless_MAB)	then	PermitAccess AND Guests
⊘	Wi-Fi_Redirect_to_Guest_Login	if	Wireless_MAB	then	Cisco_WebAuth
☑	Basic_Authenticated_Access	if	Network_Access_Authentication_Passed	then	PermitAccess
☑	Default	if no matches, then	DenyAccess		

Now when a phone passes its IEEE802.1x authentication its traffic will be tagged as SGT20 by the Edge Switch. Later in the lab we'll verify that SGT tagging is correctly received in the Nexus 1000V from the Edge Switch over a SXP connection.

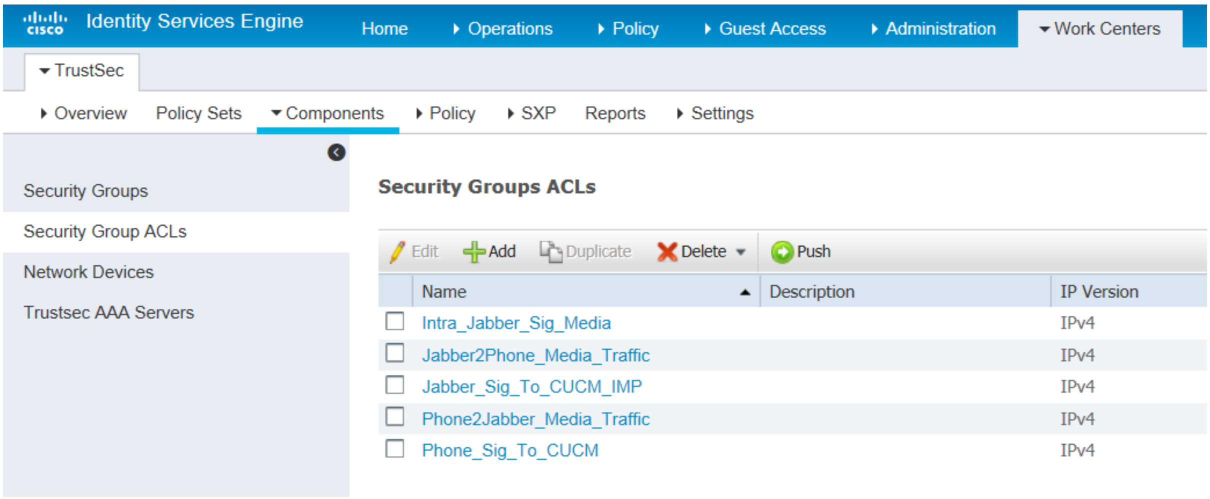
5) Security Group ACLs

As described at the beginning of this document we use Source Group ACLs (SGACLs) to enforce source to destination traffic in a TrustSec implementation.

We're now going to create SGACLs for our Collaboration Lab. To make it easy we're just going to concentrate on our collaboration signalling and media traffic. In real life we'd need to include additional application relevant ACL entries for the Jabber clients as they reside on general purpose data devices.

We are also going to try and be as descriptive as possible with our SGACL naming, to make enforcement testing more meaningful.

On ISE, navigate to the Work Centers>TrustSec>Components>Security Group ACLs and configure the SGACLs shown below:



Security Groups ACLs

	Name	Description	IP Version
☐	Intra_Jabber_Sig_Media		IPv4
☐	Jabber2Phone_Media_Traffic		IPv4
☐	Jabber_Sig_To_CUCM_IMP		IPv4
☐	Phone2Jabber_Media_Traffic		IPv4
☐	Phone_Sig_To_CUCM		IPv4

Why is there no SGACL for Phone2Phone Media?

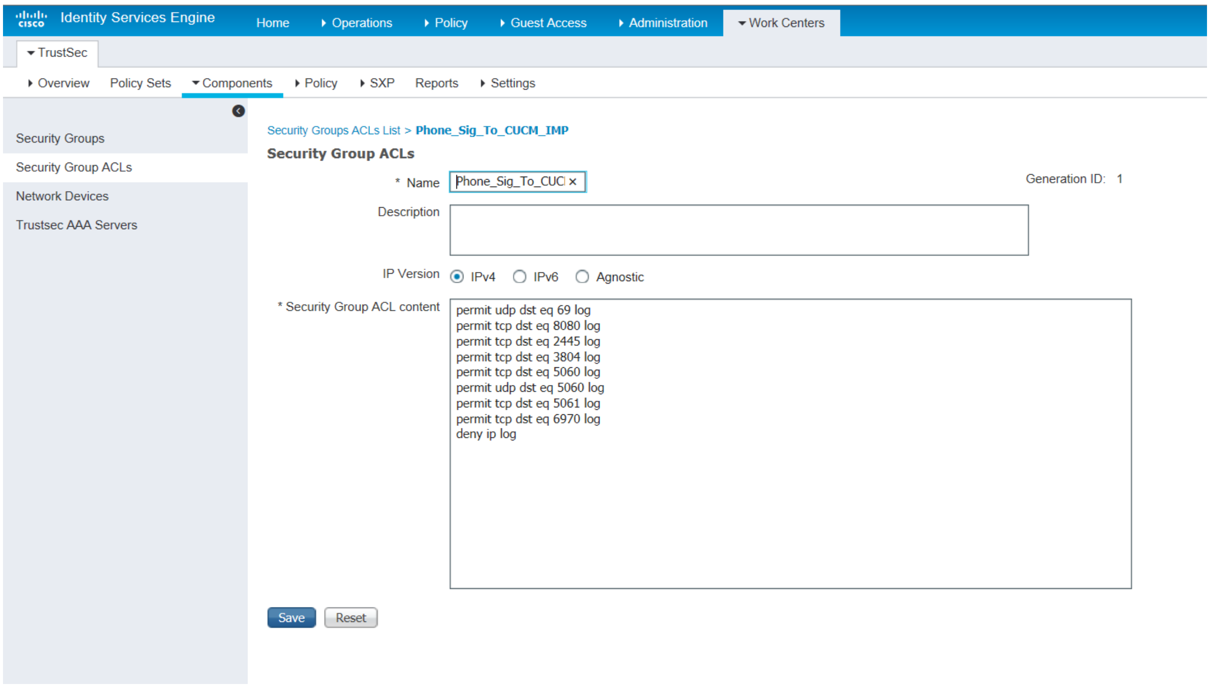
Note: The ACL syntax used needs to be supported by all of the enforcement devices. This should to be taken into careful consideration when the ACLs are being built in a production environment so that when downloaded they are accepted by every enforcement point and function correctly.

Each of the following SGACLS has been created from the relevant Cisco “port usage” documentation. The main assumption these ACLs make is that SIP will be the only Signalling protocol used in the lab. Hence, our SGACLs will not pass SCCP traffic.

Note: If we wanted to enforce phone to phone traffic we’d need to add enforcement at the access layer and this does become a question of hardware support. Our lab 2960Cs support TrustSec classification but not enforcement. The TrustSec hardware support information can be found here: http://www.cisco.com/c/en/us/solutions/enterprise-networks/trustsec/trustsec_matrix.html

Phone_Sig_To_CUCM

The ports used for the SGACL were obtained from the Unified Communications Manager port usage guide.



Security Groups ACLs List > **Phone_Sig_To_CUCM_IMP**

Security Group ACLs

* Name: Phone_Sig_To_CUC

Generation ID: 1

Description:

IP Version: ● IPv4 ○ IPv6 ○ Agnostic

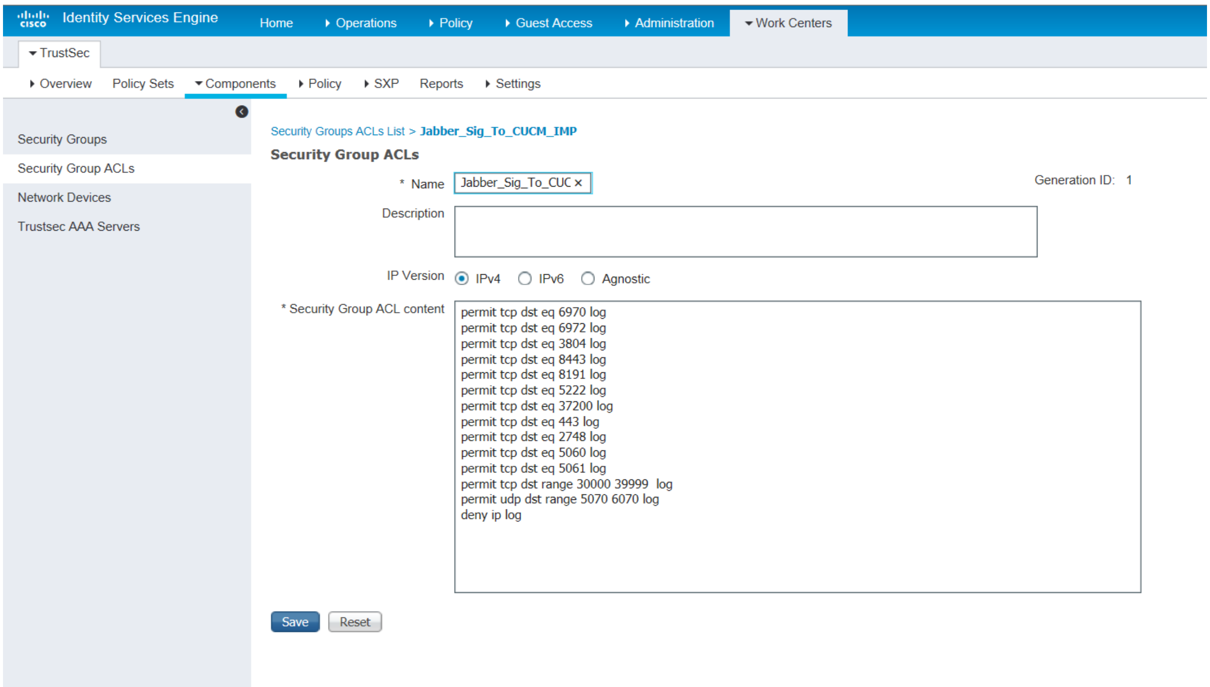
* Security Group ACL content:

```
permit udp dst eq 69 log
permit tcp dst eq 8080 log
permit tcp dst eq 2445 log
permit tcp dst eq 3804 log
permit tcp dst eq 5060 log
permit udp dst eq 5060 log
permit tcp dst eq 5061 log
permit tcp dst eq 6970 log
deny ip log
```

The ACL is provided below in case you want to cut and paste:

```
permit udp dst eq 69 log
permit tcp dst eq 8080 log
permit tcp dst eq 2445 log
permit tcp dst eq 3804 log
permit tcp dst eq 5060 log
permit udp dst eq 5060 log
permit tcp dst eq 5061 log
permit tcp dst eq 6970 log
deny ip log
```

Jabber_Sig_To_CUCM_IMP



Security Groups ACLs List > **Jabber_Sig_To_CUCM_IMP**

Security Group ACLs

* Name: Jabber_Sig_To_CUC

Generation ID: 1

Description:

IP Version: ● IPv4 ○ IPv6 ○ Agnostic

* Security Group ACL content:

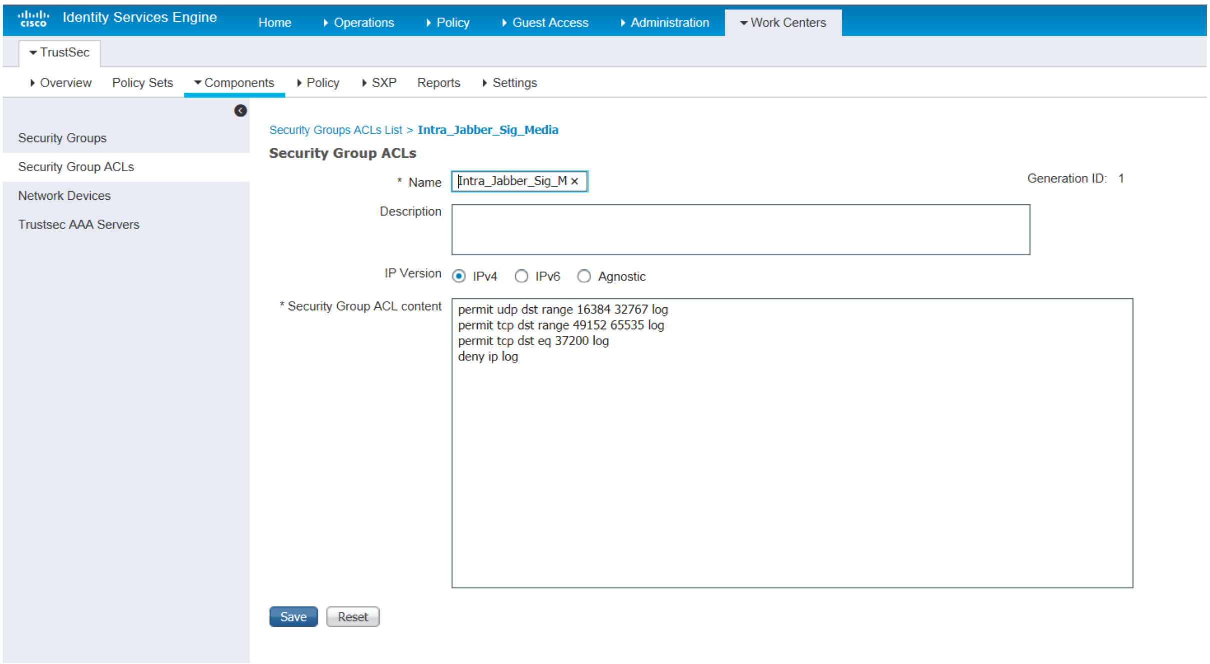
```
permit tcp dst eq 6970 log
permit tcp dst eq 6972 log
permit tcp dst eq 3804 log
permit tcp dst eq 8443 log
permit tcp dst eq 8191 log
permit tcp dst eq 5222 log
permit tcp dst eq 37200 log
permit tcp dst eq 443 log
permit tcp dst eq 2748 log
permit tcp dst eq 5060 log
permit tcp dst eq 5061 log
permit tcp dst range 30000 39999  log
permit udp dst range 5070 6070 log
deny ip log
```

The ACL is provided below in case you want to cut and paste:

```
permit tcp dst eq 6970 log
permit tcp dst eq 6972 log
permit tcp dst eq 3804 log
permit tcp dst eq 8443 log
permit tcp dst eq 8191 log
permit tcp dst eq 5222 log
permit tcp dst eq 37200 log
permit tcp dst eq 443 log
permit tcp dst eq 2748 log
permit tcp dst eq 5060 log
permit tcp dst eq 5061 log
permit tcp dst range 30000 39999 log
permit udp dst range 5070 6070 log
deny ip log
```

The Jabber_Sig port ranges were obtained from the Jabber port usage guide.

Intra_Jabber_Media



Security Groups ACLs List > **Intra_Jabber_Sig_Media**

Security Group ACLs

* Name: Intra_Jabber_Sig_M

Generation ID: 1

Description:

IP Version: ● IPv4 ○ IPv6 ○ Agnostic

* Security Group ACL content:

```
permit udp dst range 16384 32767 log
permit tcp dst range 49152 65535 log
permit tcp dst eq 37200 log
deny ip log
```

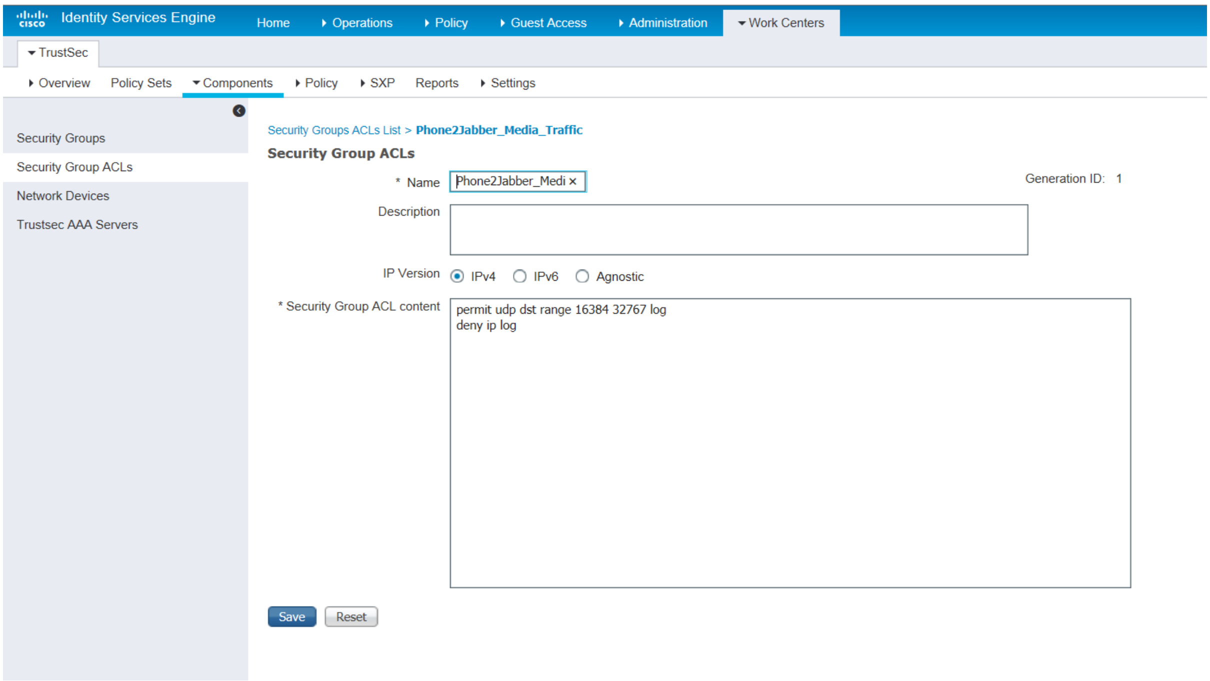
The ACL is provided below in case you want to cut and paste:

permit udp dst range 16384 32767 log
permit tcp dst range 49152 65535 log
permit tcp dst eq 37200 log
deny ip log

The Intra_Jabber_Media SGACL allows RTP traffic between Jabber clients as well as screen share and file sharing.

The ports used for the SGACL were obtained from the Unified Communications Manager port usage guide

Phone2Jabber_Media_Traffic



Security Groups ACLs List > Phone2Jabber_Media_Traffic

Security Group ACLs

* Name: Phone2Jabber_Medi

Generation ID: 1

Description:

IP Version: ● IPv4 ○ IPv6 ○ Agnostic

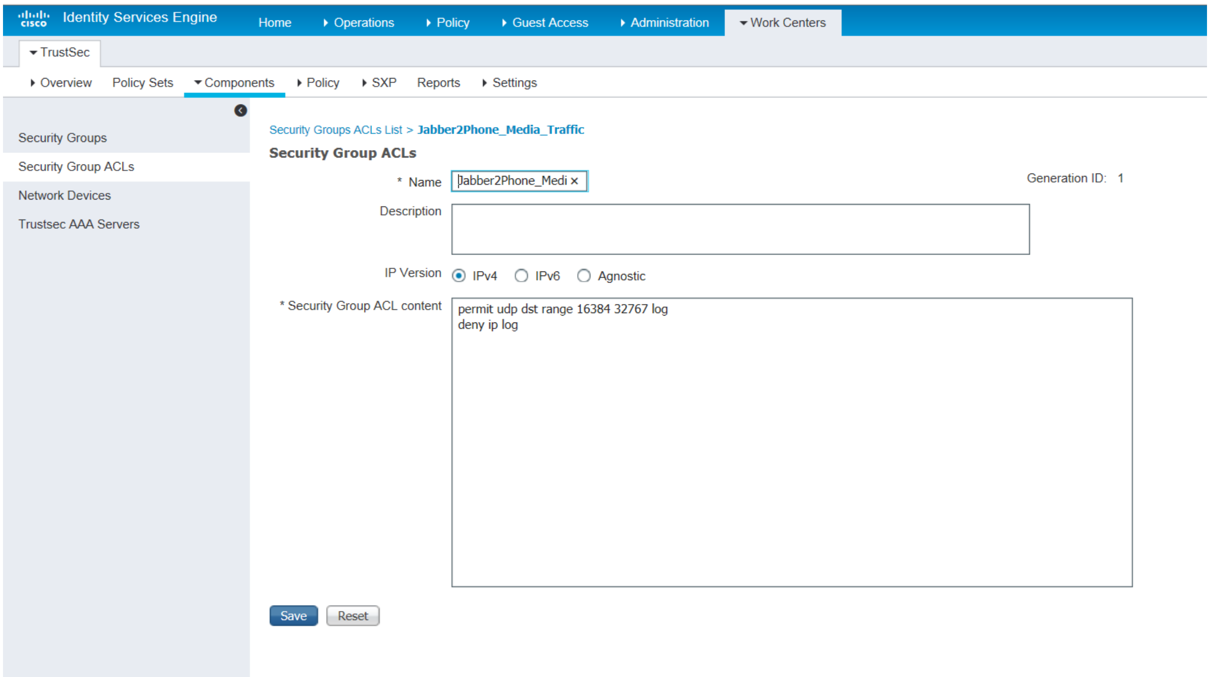
* Security Group ACL content:

```
permit udp dst range 16384 32767 log
deny ip log
```

The ACL is provided below in case you want to cut and paste:

permit udp dst range 16384 32767 log
deny ip log

Jabber2Phone_Media_Traffic



Security Groups ACLs List > Jabber2Phone_Media_Traffic

Security Group ACLs

* Name: Jabber2Phone_Medi

Generation ID: 1

Description:

IP Version: ● IPv4 ○ IPv6 ○ Agnostic

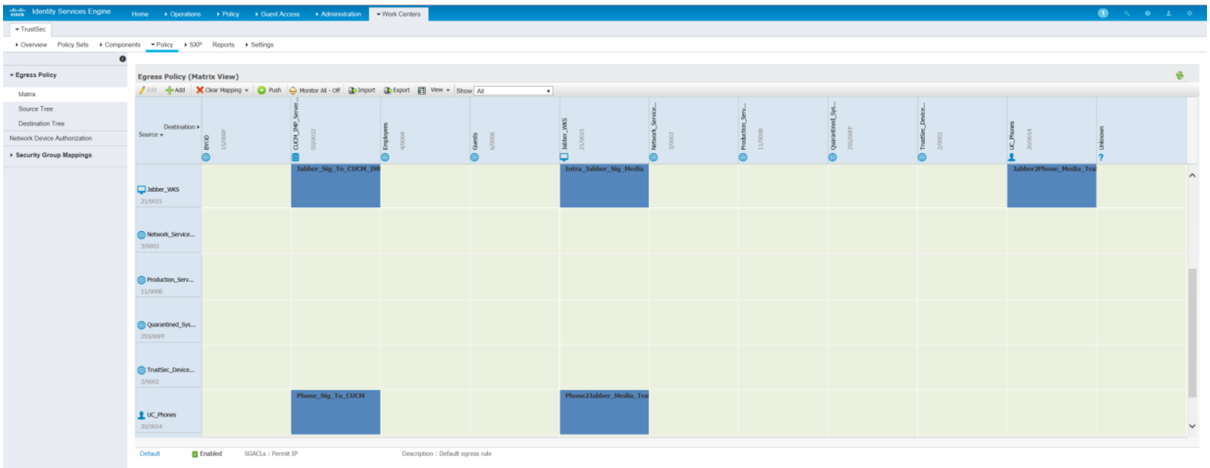
* Security Group ACL content:

```
permit udp dst range 16384 32767 log
deny ip log
```

The ACL is provided below in case you want to cut and paste:

```
permit udp dst range 16384 32767 log
deny ip log
```

6) TrustSec Policy Matrix



Egress Policy (Matrix View)

Destination ▸ Source ▾	BYOD 15/000F	CUCM_IMP_Server... 50/0032	Employees 4/0004	Guests 6/0006	Jabber_WKS 21/0015	Network_Service... 3/0003	Production_Serv... 11/000B	Quarantined_Sys... 255/00FF	TrustSec_Device... 2/0002	UC_Phones 20/0014	Unknown
Jabber_WKS 21/0015		Jabber_Sig_To_CUCM_IM			Intra_Jabber_Sig_Media					Jabber2Phone_Media_Tra	
Network_Service... 3/0003											
Production_Serv... 11/000B											
Quarantined_Sys... 255/00FF											
TrustSec_Device... 2/0002											
UC_Phones 20/0014		Phone_Sig_To_CUCM			Phone2Jabber_Media_Tra						

Default　Enabled　SGACLs : Permit IP　Description : Default egress rule

The Egress Policy Matrix is used to map source SGTs to destination SGTs. We are going to add SGACLs to the cells where the SGTs intersect to centrally create the traffic policies for all of our different types of collaboration traffic. In a production environment the policies for collaboration applications would need to be combined with those for the data based services.

In ISE, bring up the empty Policy matrix.

Work Centers>Policy>Egress Policy>Matrix

You add the SGACL by double clicking the appropriate cell and then selecting the relevant SGACL. It should be intuitive but feel free to ask a proctor to help or provide further explanation if required, as this is one of the major cornerstones of a Cisco TrustSec solution.

7) Access Switch TrustSec configuration

To save time all TrustSec commands for our Edge Device are already in place.

The access switch configuration provided below shows the TrustSec configuration we are using. This includes the Source Exchange Protocol connection used to propagate SGTs to the Nexus 1000V.

As mentioned previously in some circumstances it might not be possible to use IEEE802.1x authentication for collaboration devices. The workaround we're going to use in this lab is a VLAN (VLAN 101) to SGT (SGT20) static mapping (`cts role-based sgt-map vlan-list`) on the access switch. This allows the lab 8841 to have its traffic marked even though it has not been authenticated using ISE.

```
cts role-based sgt-map vlan-list 101 sgt 20
cts sxp enable
cts sxp default source-ip 198.18.192.2
cts sxp default password C1sco12345
cts sxp connection peer 198.18.133.35 password default mode local speaker hold-time 0
```

The “cts sxp” commands are used to establish the sxp connection with the core Nexus 1000V so that SGT20 can be used for the enforcement of any phone traffic that flows through the switch.

8) Nexus 1000V TrustSec Configuration

To be quite honest the Nexus 1000V is quite a specialised datacentre device, so don’t be overly perturbed if you are not familiar with it. If you have some familiarity with IOS you will definitely be able to configure the switch for what we need to do and should have a good idea of what’s going on.

To load the IOS commands below you can use Putty installed on WKS2 (RDP to 198.18.133.37) or use the terminal client on your own PC to SSH into the Nexus. The IP address to use is: 198.18.133.35 (admin / C1sco12345)

We then use “conf t” which allows us to paste in the configuration. To save our new configuration use “copy run start”.

Note: the Nexus 1000v does not support “wr mem”

Warning: If you copy and paste this text you should copy the commands below into notepad (or similar) as some hidden control characters might be included if you paste directly. This issue has previously been seen by Apple MAC users but it is probably good practice for everyone to do this.

```
feature cts

cts device-id n1kv password C1sco12345

cts role-based counters enable

cts sxp default password C1sco12345

!

port-profile type ethernet uplink-vem2

  cts manual

    role-based enforcement

port-profile type ethernet uplink-vem

  cts manual

    role-based enforcement
```

```
port-profile type vethernet hq-uplink
  cts manual
    role-based enforcement
    policy static sgt 0x15
!
cts device tracking
cts interface delete-hold 60
cts role-based sgt-map 198.18.133.3 50
cts role-based sgt-map 198.18.133.4 50
cts sxp enable
cts sxp default source-ip 198.18.133.35
cts sxp connection peer 198.18.192.2 password default mode speaker vrf management
```

Note: the “cts” commands above enable TrustSec and authenticate the Nexus from a TrustSec perspective to ISE. (The Nexus 1000V Radius commands for ISE are already configured). The “cts sxp” commands are needed to complete our SXP tunnel establishment with the lab’s Edge Switch so it can send across (for enforcement purposes) the Phone’s SGT20 tag. The “cts role-based sgt-map” commands statically map the CUCM and IMP Server’s SGT50 to each box’s IP address.

Note: ISE also supports SXP so we could provision this centrally on ISE and use SXP to push this type of static mapping down to infrastructure enforcement points that support it.

While we’re entering commands into the Nexus let’s also add the NetFlow configuration we’ll need to the Lancope section of the lab. It takes 4-5 minutes for flows to begin propagating up into the StealthWatch Management Console, so this should save us some time.

Warning: If you copy and paste this text you should copy the commands below into notepad (or similar) as it appears some hidden control characters might be included if you paste directly. This issue has previously been seen by Apple MAC users but it’s probably good practice for everyone to do this.

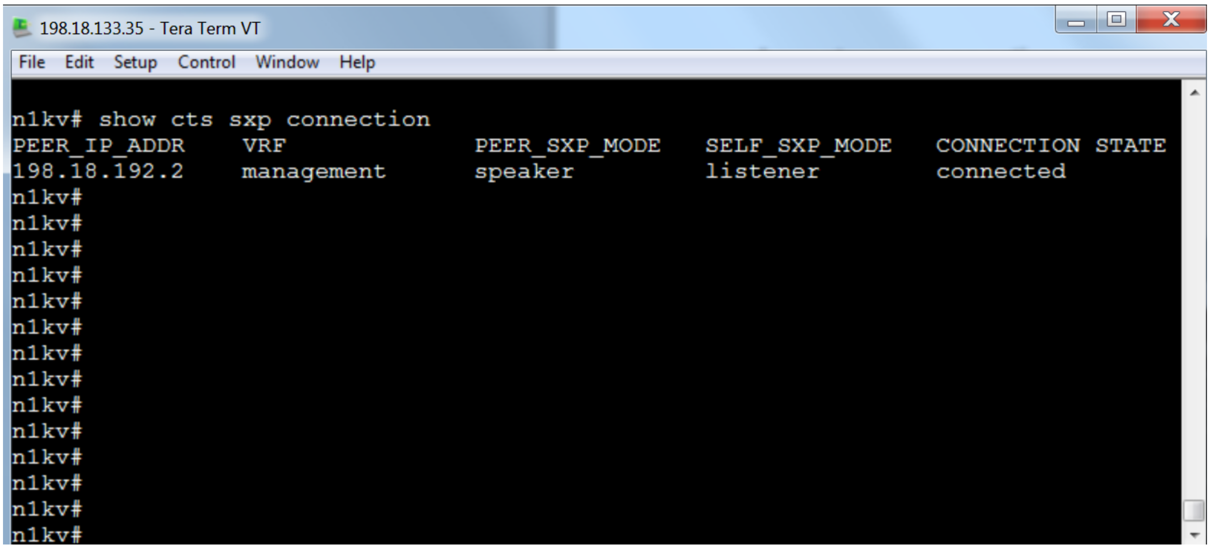
```
feature netflow
!
flow timeout active 60
flow exporter netflow_to_stealthwatch
  description Export NetFlow to StealthWatch
  destination 198.18.133.137 use-vrf management
  transport udp 2055
  source lc-exp 198.18.133.35/18
  version 9
!
flow monitor standard_v9netflow
  record netflow-original
  exporter netflow_to_stealthwatch
!
port-profile type ethernet uplink-vem2
  ip flow monitor standard_v9netflow input
  !
port-profile type ethernet uplink-vem
  ip flow monitor standard_v9netflow input
!
  port-profile type vethernet hq-uplink
  ip flow monitor standard_v9netflow input
```

9) Verifying Correct TrustSec Enforcement

We're going to do this from the Nexus 1000V and the two Jabber enabled clients (WKS3 and WKS4).

show cts sxp connection

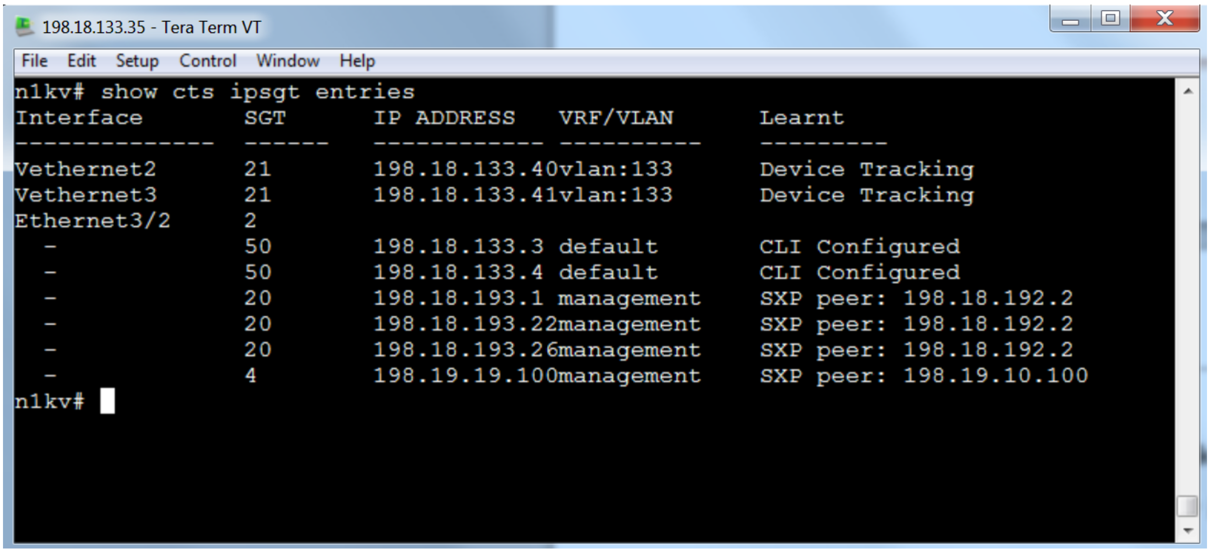
This command show us that the SXP tunnel between the Nexus and the Edge switch is up and running.


198.18.133.35 - Tera Term VT
File Edit Setup Control Window Help

```
n1kv# show cts sxp connection
PEER_IP_ADDR     VRF             PEER_SXP_MODE   SELF_SXP_MODE   CONNECTION STATE
198.18.192.2     management      speaker         listener        connected
n1kv#
n1kv#
n1kv#
n1kv#
n1kv#
n1kv#
n1kv#
n1kv#
n1kv#
n1kv#
n1kv#
n1kv#
n1kv#
n1kv#
```

show cts ipsgt entries

Looking at the ipsgt entries we should be able to see the SGT tags for the Edge devices and the statically mapped UC Servers. The Nexus 1000V has also learnt about the Jabber WKS and allocated SGT21 to them.



198.18.133.35 - Tera Term VT
File Edit Setup Control Window Help

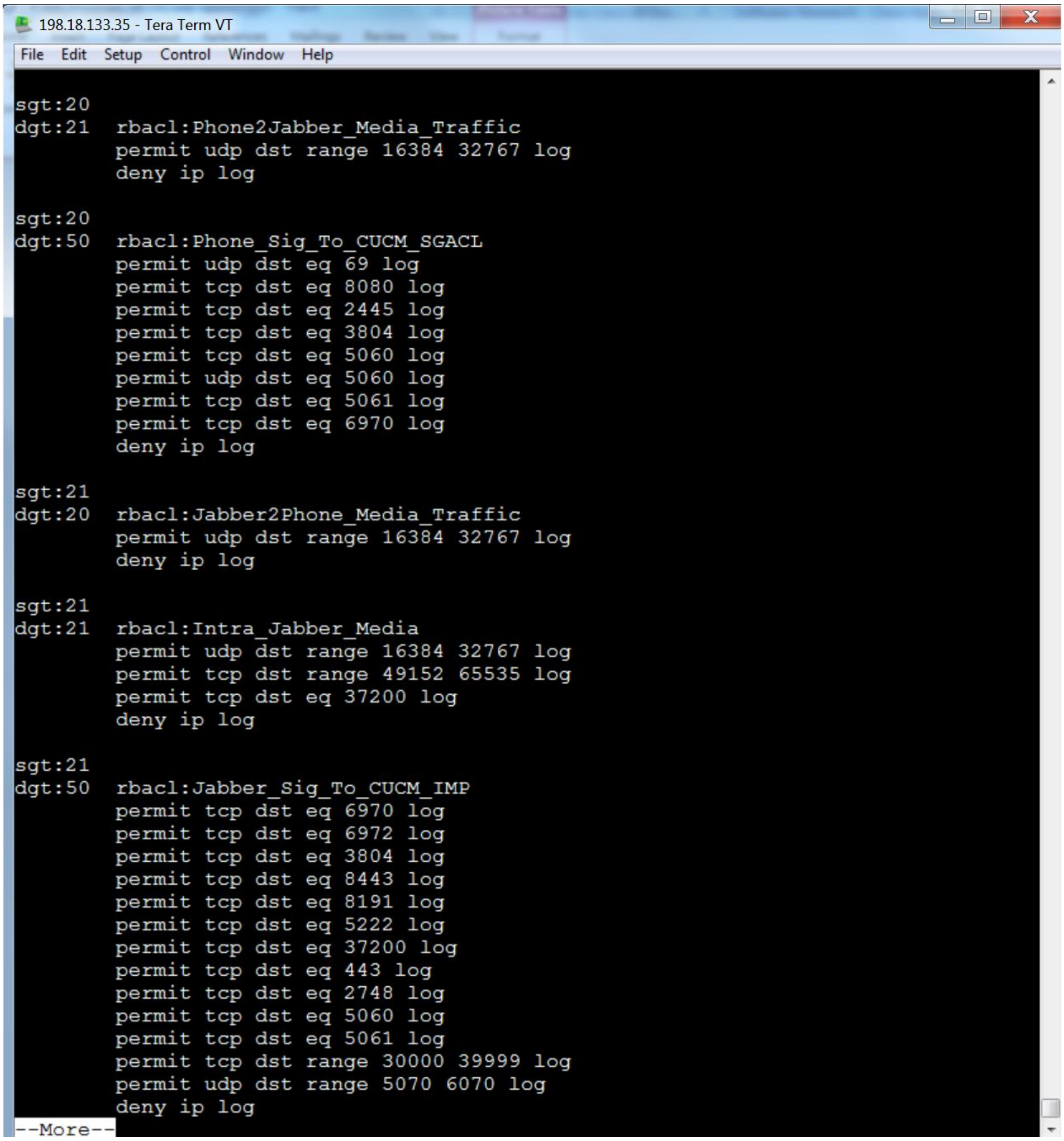
```
n1kv# show cts ipsgt entries
Interface       SGT      IP ADDRESS   VRF/VLAN      Learnt
--------------  ------   ------------ ----------    ---------
Vethernet2      21       198.18.133.40vlan:133      Device Tracking
Vethernet3      21       198.18.133.41vlan:133      Device Tracking
Ethernet3/2     2
  -             50       198.18.133.3 default       CLI Configured
  -             50       198.18.133.4 default       CLI Configured
  -             20       198.18.193.1 management    SXP peer: 198.18.192.2
  -             20       198.18.193.22management    SXP peer: 198.18.192.2
  -             20       198.18.193.26management    SXP peer: 198.18.192.2
  -             4        198.19.19.100management    SXP peer: 198.19.10.100
n1kv# █
```

Note: Even if you did not configure IEEE802.1x you should still be seeing SXP entries (SGT20) for the phones. This is because in the access switch configuration there is a pre-configured static phone vlan to SGT mapping. Refer back to the access switch configuration provided in 13) of the IEEE802.1x section. The preference would be to use IEEE802.1x to dynamically allocate the SGT, but if for any reason that's not possible, TrustSec provides the flexibility to statically map our collaboration devices.

show cts role-based policy and cts refresh role-based-policy

ISE should dynamically download the role based polices we defined in the Policy Matrix but if it doesn't and we want to manually pull down the policy (due to time constraints) we can use the “cts refresh” command.

Note: the Nexus 1000V has some old TrustSec source to destination policies that are not part of our collaboration lab. Please ignore these.


198.18.133.35 - Tera Term VT
File Edit Setup Control Window Help

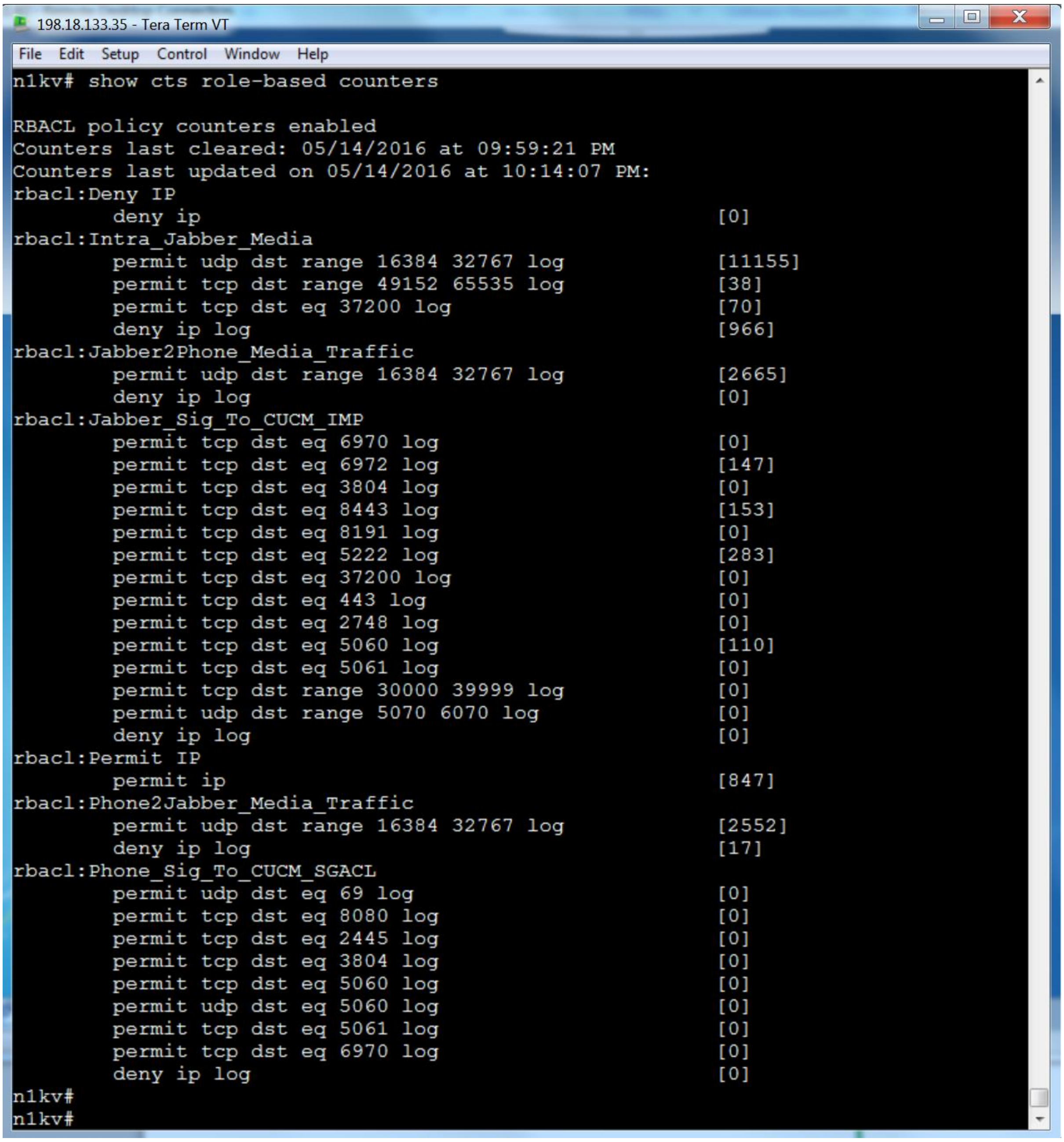
```
sgt:20
dgt:21   rbacl:Phone2Jabber_Media_Traffic
         permit udp dst range 16384 32767 log
         deny ip log

sgt:20
dgt:50   rbacl:Phone_Sig_To_CUCM_SGACL
         permit udp dst eq 69 log
         permit tcp dst eq 8080 log
         permit tcp dst eq 2445 log
         permit tcp dst eq 3804 log
         permit tcp dst eq 5060 log
         permit udp dst eq 5060 log
         permit tcp dst eq 5061 log
         permit tcp dst eq 6970 log
         deny ip log

sgt:21
dgt:20   rbacl:Jabber2Phone_Media_Traffic
         permit udp dst range 16384 32767 log
         deny ip log

sgt:21
dgt:21   rbacl:Intra_Jabber_Media
         permit udp dst range 16384 32767 log
         permit tcp dst range 49152 65535 log
         permit tcp dst eq 37200 log
         deny ip log

sgt:21
dgt:50   rbacl:Jabber_Sig_To_CUCM_IMP
         permit tcp dst eq 6970 log
         permit tcp dst eq 6972 log
         permit tcp dst eq 3804 log
         permit tcp dst eq 8443 log
         permit tcp dst eq 8191 log
         permit tcp dst eq 5222 log
         permit tcp dst eq 37200 log
         permit tcp dst eq 443 log
         permit tcp dst eq 2748 log
         permit tcp dst eq 5060 log
         permit tcp dst eq 5061 log
         permit tcp dst range 30000 39999 log
         permit udp dst range 5070 6070 log
         deny ip log
--More--
```

show cts role-based counters and clear cts role-based counters

Issue “clear cts role-based counters”

Let’s create some traffic to and from WKS3 and WKS4. Make some calls to/from the IP Phones. Make a call between the two Jabber clients. Create some IM traffic and also perform a screen capture and file transfer between WKS3 and WKS4.

When you run “show cts role-based counters” you should see something like the screenshot below:



```
n1kv# show cts role-based counters

RBACL policy counters enabled
Counters last cleared: 05/14/2016 at 09:59:21 PM
Counters last updated on 05/14/2016 at 10:14:07 PM:
rbacl:Deny IP
        deny ip                                         [0]
rbacl:Intra_Jabber_Media
        permit udp dst range 16384 32767 log            [11155]
        permit tcp dst range 49152 65535 log            [38]
        permit tcp dst eq 37200 log                     [70]
        deny ip log                                     [966]
rbacl:Jabber2Phone_Media_Traffic
        permit udp dst range 16384 32767 log            [2665]
        deny ip log                                     [0]
rbacl:Jabber_Sig_To_CUCM_IMP
        permit tcp dst eq 6970 log                      [0]
        permit tcp dst eq 6972 log                      [147]
        permit tcp dst eq 3804 log                      [0]
        permit tcp dst eq 8443 log                      [153]
        permit tcp dst eq 8191 log                      [0]
        permit tcp dst eq 5222 log                      [283]
        permit tcp dst eq 37200 log                     [0]
        permit tcp dst eq 443 log                       [0]
        permit tcp dst eq 2748 log                      [0]
        permit tcp dst eq 5060 log                      [110]
        permit tcp dst eq 5061 log                      [0]
        permit tcp dst range 30000 39999 log            [0]
        permit udp dst range 5070 6070 log              [0]
        deny ip log                                     [0]
rbacl:Permit IP
        permit ip                                       [847]
rbacl:Phone2Jabber_Media_Traffic
        permit udp dst range 16384 32767 log            [2552]
        deny ip log                                     [17]
rbacl:Phone_Sig_To_CUCM_SGACL
        permit udp dst eq 69 log                        [0]
        permit tcp dst eq 8080 log                      [0]
        permit tcp dst eq 2445 log                      [0]
        permit tcp dst eq 3804 log                      [0]
        permit tcp dst eq 5060 log                      [0]
        permit udp dst eq 5060 log                      [0]
        permit tcp dst eq 5061 log                      [0]
        permit tcp dst eq 6970 log                      [0]
        deny ip log                                     [0]
n1kv#
n1kv#
```

Note: The Phone_Sig_to_CUCM SGACL does not increment its counters. This is expected as the phone signalling traffic never passes through the Nexus. To enforce phone signalling we'd need to create an enforcement point in the signalling flow.

Verify the Baseline Connectivity

Log onto WKS3 and WKS4 and perform the following to verify:

- Ping between WKS3 and WKS4
- You can ping the phones from WKS3 and WKS4
- You can ping the CUCM and IMP Servers
- Also use http://198.18.133.3 to access CUCM. Important – use http and not https in the URL.
- Use http://Phone_IP_Address to access 8845\8865 web page

How do the results compare with the original testing you did?

Note: To summarize, we have now created a TrustSec Policy that locks down the permitted signalling and media traffic that flows through the Nexus 1000V. The strength of this solution is that it's a set of flexible, centrally administered policies, which scales much better than traditional ACL deployments.

Monitoring our Collaboration Deployment

Let's now turn our attention to the final part of the lab in which we're going to monitor and analyse the traffic that is being created in our small collaboration deployment. We will also create a customer event to highlight any suspicious activity between the Jabber WKS and our UC Servers.

1) Log onto the Lancope Servers.

Flow Collector – https:\\198.18.133.136 (admin/lan411cope)

How many flows are currently logged?

Stealth Watch Manager – https:\\198.18.133.137 (admin/lan411cope)

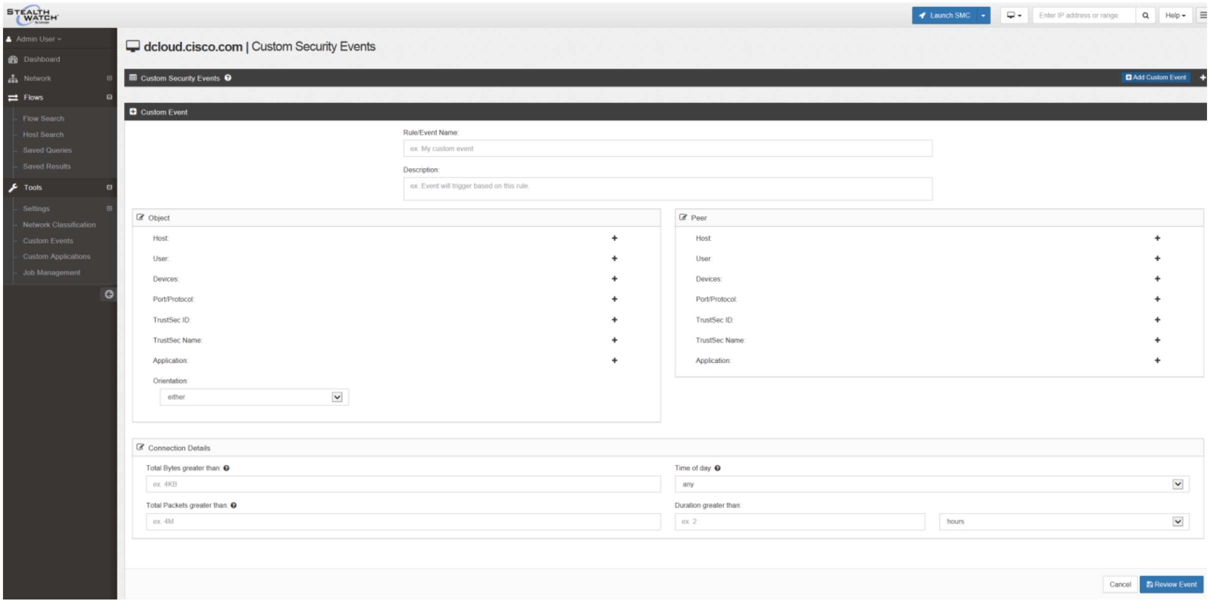
2) On the Flow Collector verify you are seeing flows arrive.

3) Now navigate to the StealthWatch Management Console

Before we start looking at the received Nexus 1000V flows, let's add a Custom Event that will be used to monitor one of our TrustSec Policies.

Under Tools, select Customer Events

At the top right hand side of the GUI, select Add Custom Event – you should then see the following:


dcloud.cisco.com | Custom Security Events

Custom Security Events

Custom Event

Orientation: either

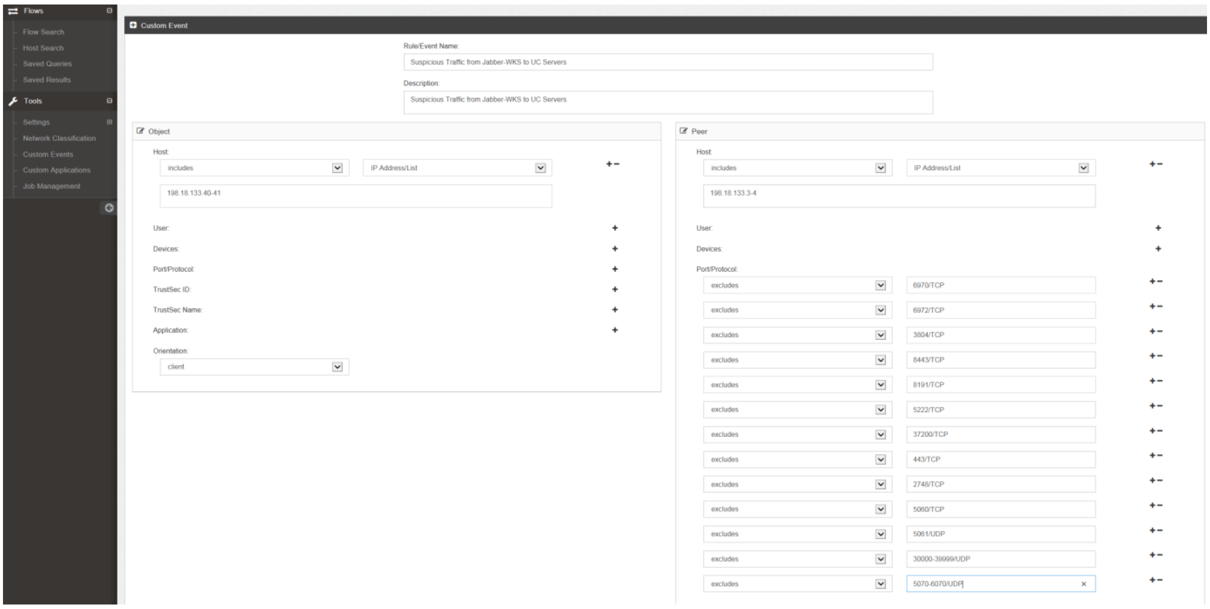
Time of day: any

Duration greater than: hours

.

The custom event we are going to create will look for suspicious traffic that emanates from Jabber WKS3 and WKS4 towards the UC Servers. In our event any port that is not in the specified signalling port range will be classed as a policy violation and cause an alarm on the console.

Use the screenshot below to create the custom event:


Custom Event

Rule/Event Name: Suspicious Traffic from Jabber-WKS to UC Servers

Description: Suspicious Traffic from Jabber-WKS to UC Servers

Object

Host: includes IP Address/List
198.18.133.40-41

Orientation: client

Peer

Host: includes IP Address/List
198.18.133.3-4

Port/Protocol:
excludes 6970/TCP
excludes 6972/TCP
excludes 3804/TCP
excludes 8443/TCP
excludes 8191/TCP
excludes 5222/TCP
excludes 37200/TCP
excludes 443/TCP
excludes 2748/TCP
excludes 5060/TCP
excludes 5061/UDP
excludes 30000-39999/UDP
excludes 5070-6070/UDP

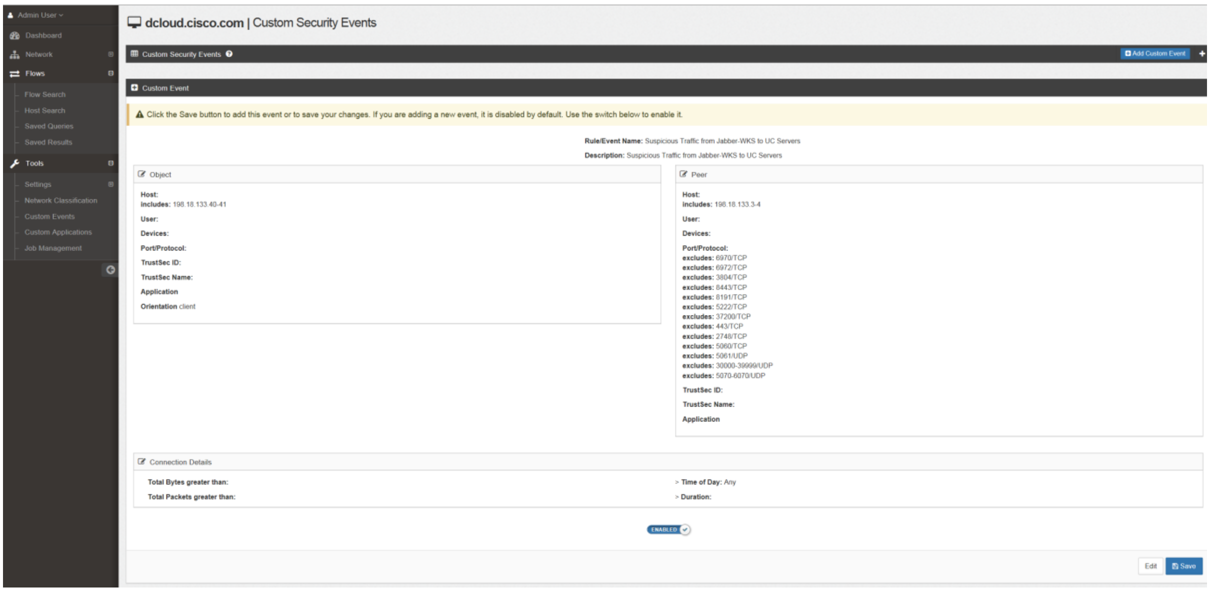
The port range we’re going to use is provided below:

6970/TCP
6972/TCP
3804/TCP
8443/TCP

8191/TCP
5222/TCP
37200/TCP
443/TCP
2748/TCP
5060/TCP
5061/UDP
30000-39999/UDP
5070-6070/UDP

As you have probably noticed, it’s the same port range we used for a TrustSec policy. So in actual fact we’re using the Cisco Lancope solution to monitor any TrustSec violations between our Jabber Clients and UC Servers.

Review the configuration and be sure to “enable” the event, then press save.



dcloud.cisco.com | Custom Security Events

Click the Save button to add this event or to save your changes. If you are adding a new event, it is disabled by default. Use the switch below to enable it.

Rule/Event Name: Suspicious Traffic from Jabber-WKS to UC Servers
Description: Suspicious Traffic from Jabber-WKS to UC Servers

Object

Host:
includes: 198.18.133.40-41
User:
Devices:
Port/Protocol:
TrustSec ID:
TrustSec Name:
Application
Orientation client

Peer

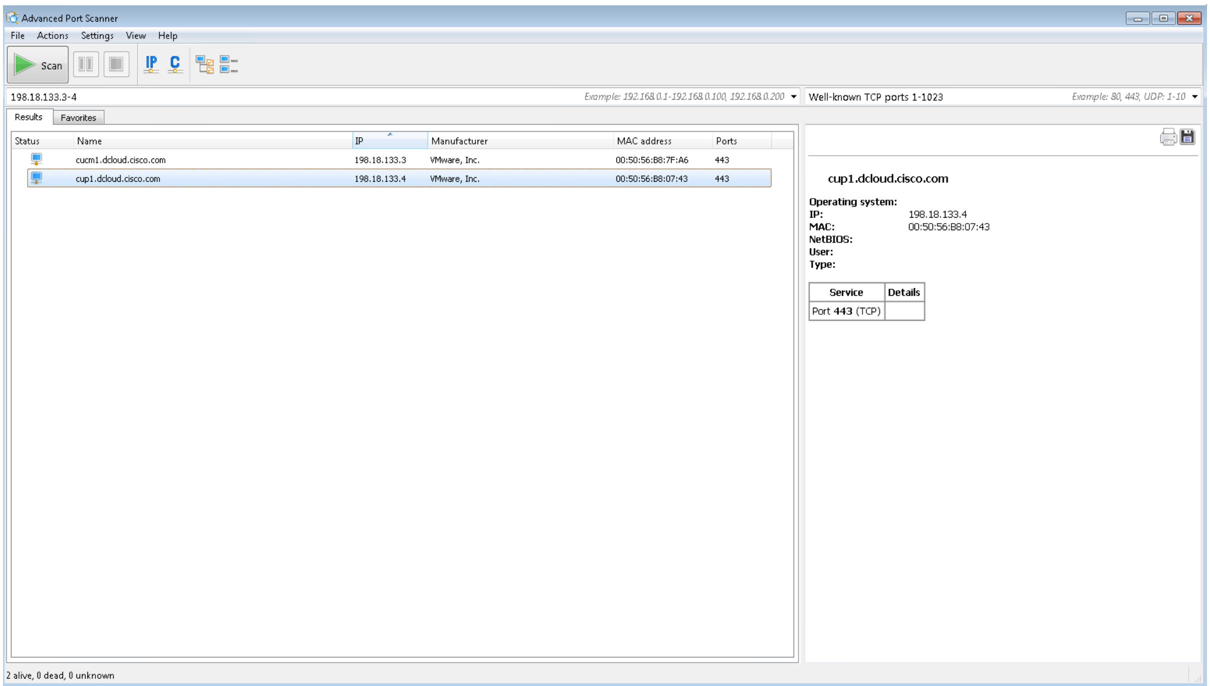
Host:
includes: 198.18.133.3-4
User:
Devices:
Port/Protocol:
excludes: 6970/TCP
excludes: 6972/TCP
excludes: 3804/TCP
excludes: 8443/TCP
excludes: 8191/TCP
excludes: 5222/TCP
excludes: 37200/TCP
excludes: 443/TCP
excludes: 2748/TCP
excludes: 5060/TCP
excludes: 5061/UDP
excludes: 30000-39999/UDP
excludes: 5070-6070/UDP
TrustSec ID:
TrustSec Name:
Application

Connection Details

Total Bytes greater than:
Total Packets greater than:
> **Time of Day:** Any
> **Duration:**

4) Testing our Custom Event

Log onto either WKS3 or WKS4 and run the Port Scanner tool which is installed on the desktop.


Advanced Port Scanner
File Actions Settings View Help
Scan
IP C
Example: 192.168.0.1-192.168.0.100, 192.168.0.200
Example: 80, 443, UDP: 1-10
Results Favorites

198.18.133.3-4

Well-known TCP ports 1-1023

Status	Name	IP	Manufacturer	MAC address	Ports
	cucm1.dcloud.cisco.com	198.18.133.3	VMware, Inc.	00:50:56:B8:7F:A6	443
	cup1.dcloud.cisco.com	198.18.133.4	VMware, Inc.	00:50:56:B8:07:43	443

cup1.dcloud.cisco.com

Operating system:
IP: 198.18.133.4
MAC: 00:50:56:B8:07:43
NetBIOS:
User:
Type:

Service	Details
Port **443** (TCP)	

2 alive, 0 dead, 0 unknown

Scan 198.18.133.3-4 and just use the default “Well-known TCP ports 1-1023”. The scan only takes a few seconds.

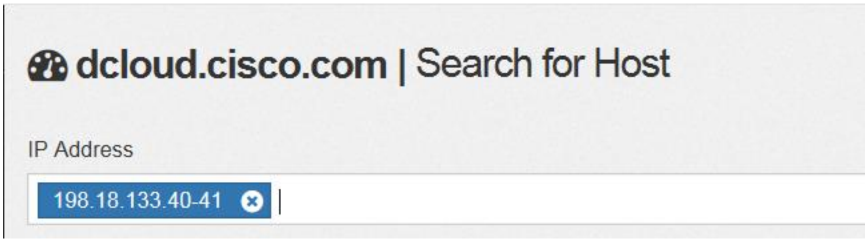
Any invoked policy violation should appear in the StealthWatch Management Console after approximately 5 minutes.

5) Now let’s look at the received flows for our two Jabber-WKS.

While we are waiting to receive our custom event, let’s take a look at the actual traffic being generated on our Jabber clients and compare it to the ports we saw traffic on from the Nexus 1000V “show cts role-based counters” command.

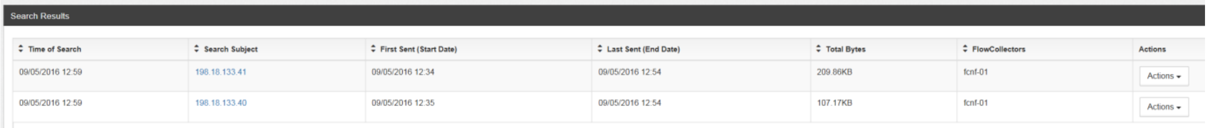
Navigate to Flows and select Host Search.

Type in the IP addresses of our two Jabber-WSKs as shown below and perform a search:



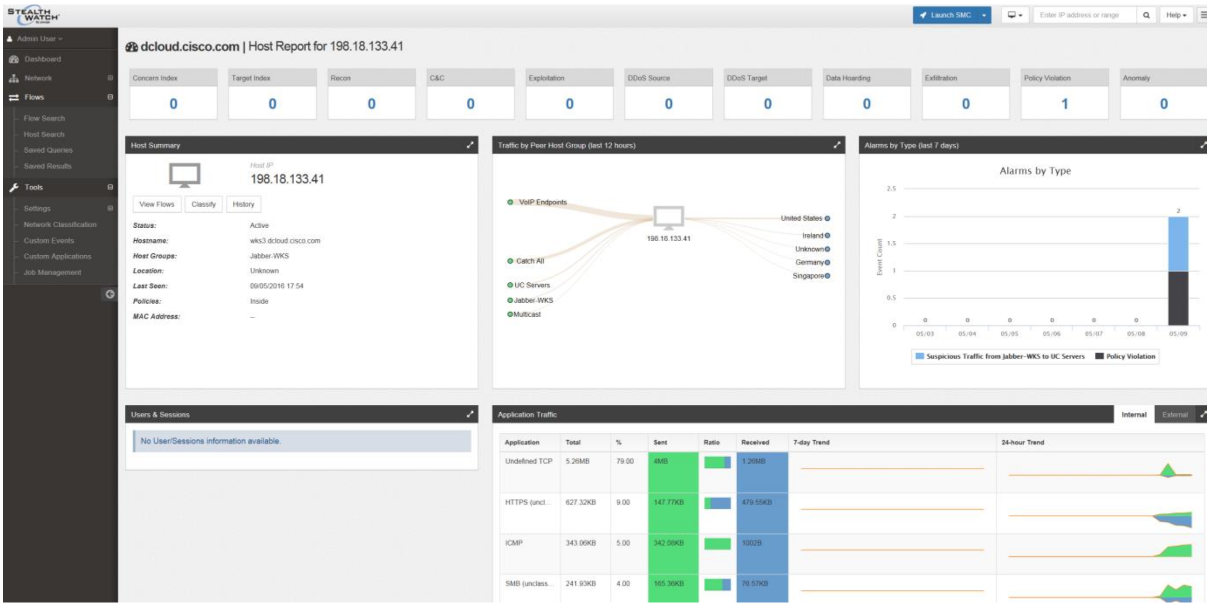
IP Address

198.18.133.40-41


Search Results

Time of Search	Search Subject	First Sent (Start Date)	Last Sent (End Date)	Total Bytes	FlowCollectors	Actions
09/05/2016 12:59	198.18.133.41	09/05/2016 12:34	09/05/2016 12:54	209.86KB	fcnf-01	Actions
09/05/2016 12:59	198.18.133.40	09/05/2016 12:35	09/05/2016 12:54	107.17KB	fcnf-01	Actions

Now let’s investigate the NetFlow traffic results for each host. Choose one of the IP addresses and click it.



dcloud.cisco.com | Host Report for 198.18.133.41

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	1	0

Host IP 198.18.133.41

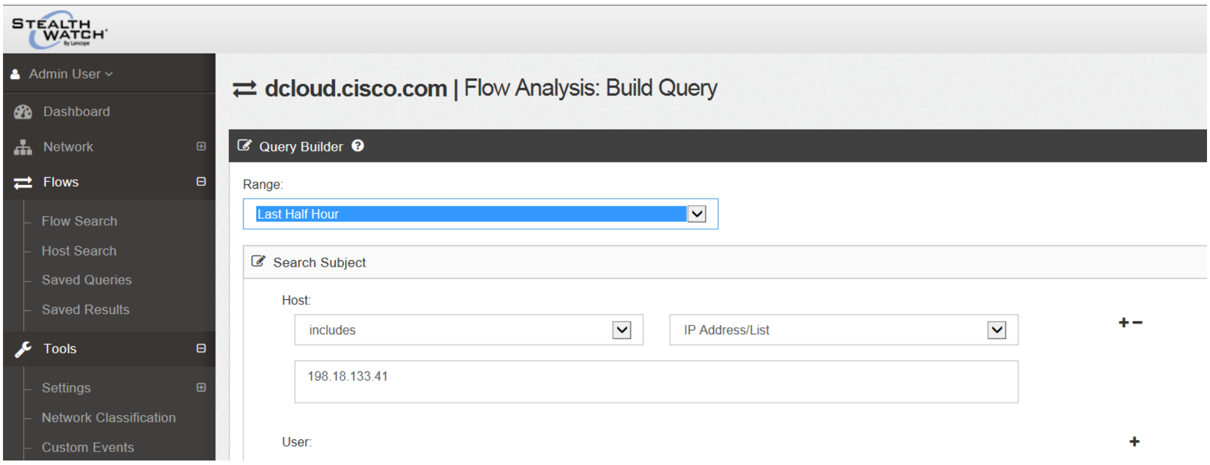
Status:	Active
Hostname:	wks3.dcloud.cisco.com
Host Groups:	Jabber-WKS
Location:	Unknown
Last Seen:	09/05/2016 17:54
Policies:	Inside
MAC Address:	–

No User/Sessions information available.

Application	Total	%	Sent	Ratio	Received	7-day Trend	24-hour Trend
Undefined TCP	5.26MB	79.00	4MB		1.26MB		
HTTPS (uncl...	627.32KB	9.00	147.77KB		479.55KB		
ICMP	343.06KB	5.00	342.08KB		1002B		
SMB (unclass...	241.93KB	4.00	165.36KB		76.57KB		

You should see something like the above screenshot. To see more details on the flows, click the “View Flows” button.

Select the Last Half Hour, Review Query and then press Run. You can leave all of the filter fields blank.



dcloud.cisco.com | Flow Analysis: Build Query

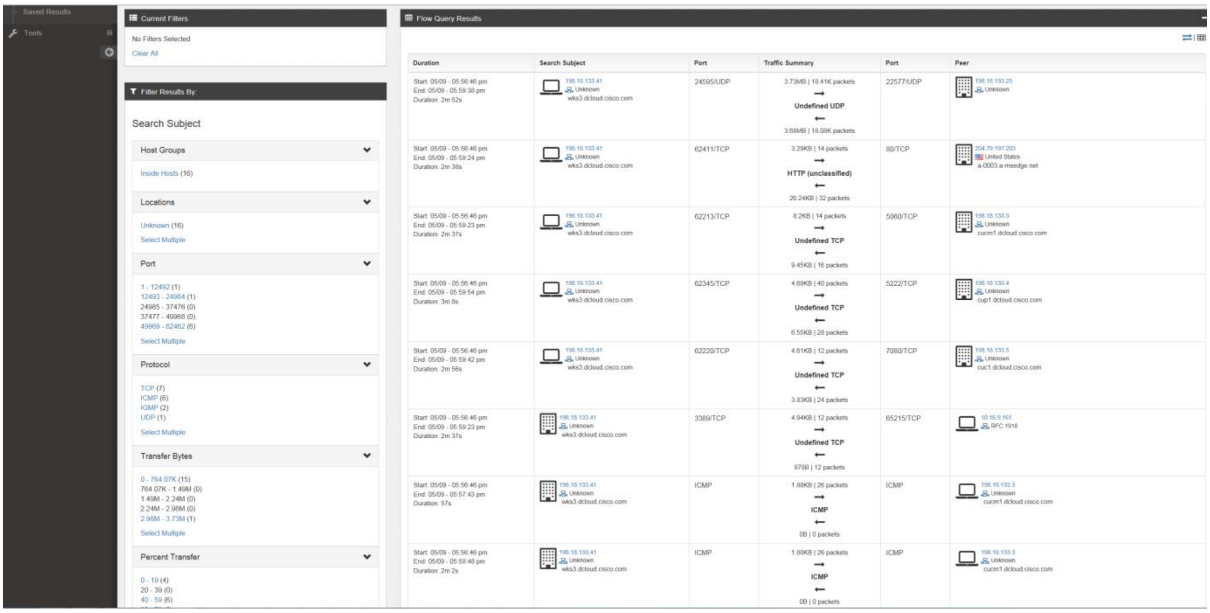
Range: Last Half Hour

Host: includes | IP Address/List

198.18.133.41

User:

Apart from the UC Servers and Phones, what else has the Jabber WKS been communicating with?



Current Filters

No Filters Selected

Clear All

Filter Results By:

Search Subject

Host Groups

Inside Hosts (16)

Locations

Unknown (16)
Select Multiple

Port

1 - 12492 (1)
12493 - 24984 (1)
24985 - 37476 (0)
37477 - 49968 (0)
49969 - 62462 (6)
Select Multiple

Protocol

TCP (7)
ICMP (6)
IGMP (2)
UDP (1)
Select Multiple

Transfer Bytes

0 - 764.07K (15)
764.07K - 1.49M (0)
1.49M - 2.24M (0)
2.24M - 2.98M (0)
2.98M - 3.73M (1)
Select Multiple

Percent Transfer

0 - 19 (4)
20 - 39 (0)
40 - 59 (6)

Flow Query Results

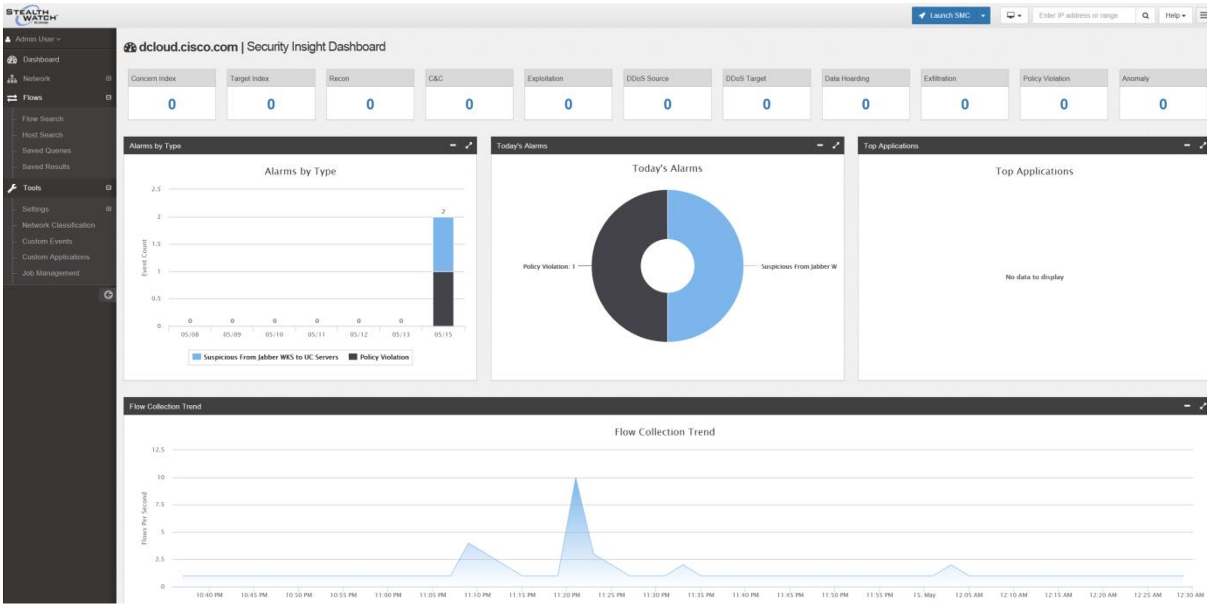
Duration	Search Subject	Port	Traffic Summary	Port	Peer
Start: 05/09 - 05:56:46 pm End: 05/09 - 05:59:38 pm Duration: 2m 52s	198.18.133.41 Unknown wks3.dcloud.cisco.com	24595/UDP	3.73MB | 18.41K packets → **Undefined UDP** ← 3.68MB | 18.08K packets	22577/UDP	198.18.193.25 Unknown
Start: 05/09 - 05:56:46 pm End: 05/09 - 05:59:24 pm Duration: 2m 38s	198.18.133.41 Unknown wks3.dcloud.cisco.com	62411/TCP	3.29KB | 14 packets → **HTTP (unclassified)** ← 28.24KB | 32 packets	80/TCP	204.79.197.203 United States a-0003.a-msedge.net
Start: 05/09 - 05:56:46 pm End: 05/09 - 05:59:23 pm Duration: 2m 37s	198.18.133.41 Unknown wks3.dcloud.cisco.com	62213/TCP	8.2KB | 14 packets → **Undefined TCP** ← 9.45KB | 16 packets	5060/TCP	198.18.133.3 Unknown cucm1.dcloud.cisco.com
Start: 05/09 - 05:56:46 pm End: 05/09 - 05:59:54 pm Duration: 3m 8s	198.18.133.41 Unknown wks3.dcloud.cisco.com	62345/TCP	4.69KB | 40 packets → **Undefined TCP** ← 6.55KB | 28 packets	5222/TCP	198.18.133.4 Unknown cup1.dcloud.cisco.com
Start: 05/09 - 05:56:46 pm End: 05/09 - 05:59:42 pm Duration: 2m 56s	198.18.133.41 Unknown wks3.dcloud.cisco.com	62220/TCP	4.61KB | 12 packets → **Undefined TCP** ← 3.83KB | 24 packets	7080/TCP	198.18.133.5 Unknown cuc1.dcloud.cisco.com
Start: 05/09 - 05:56:46 pm End: 05/09 - 05:59:23 pm Duration: 2m 37s	198.18.133.41 Unknown wks3.dcloud.cisco.com	3389/TCP	4.94KB | 12 packets → **Undefined TCP** ← 878B | 12 packets	65215/TCP	10.16.9.161 RFC 1918
Start: 05/09 - 05:56:46 pm End: 05/09 - 05:57:43 pm Duration: 57s	198.18.133.41 Unknown wks3.dcloud.cisco.com	ICMP	1.88KB | 26 packets → **ICMP** ← 0B | 0 packets	ICMP	198.18.133.3 Unknown cucm1.dcloud.cisco.com
Start: 05/09 - 05:56:46 pm End: 05/09 - 05:58:48 pm Duration: 2m 2s	198.18.133.41 Unknown wks3.dcloud.cisco.com	ICMP	1.88KB | 26 packets → **ICMP** ← 0B | 0 packets	ICMP	198.18.133.3 Unknown cucm1.dcloud.cisco.com

Note: This goes back to what was said earlier about Jabber sitting on a general purpose data client. In a real TrustSec deployment, you would include additional ACLs to control access to other important application services on the network.

6) Reviewing the Policy Violation

If your customer event configuration was successful you should, after approximately 5 minutes, see an Alert.

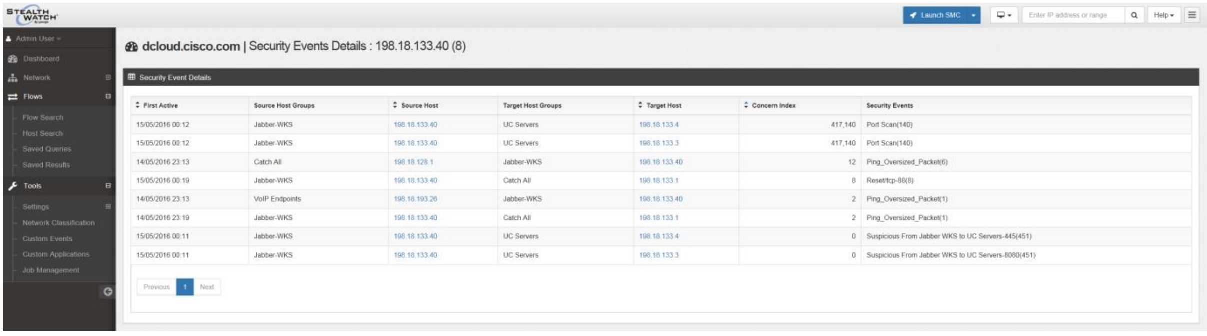
Click the Alarm in the Today's Alarms panel.



dcloud.cisco.com | Security Insight Dashboard

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

You are taken the Alarms Table where you can view the details of the Alarm.



dcloud.cisco.com | Security Events Details : 198.18.133.40 (8)

Security Event Details

First Active	Source Host Groups	Source Host	Target Host Groups	Target Host	Concern Index	Security Events
15/05/2016 00:12	Jabber-WKS	198.18.133.40	UC Servers	198.18.133.4	417,140	Port Scan(140)
15/05/2016 00:12	Jabber-WKS	198.18.133.40	UC Servers	198.18.133.3	417,140	Port Scan(140)
14/05/2016 23:13	Catch All	198.18.128.1	Jabber-WKS	198.18.133.40	12	Ping_Oversized_Packet(6)
15/05/2016 00:19	Jabber-WKS	198.18.133.40	Catch All	198.18.133.1	8	Reset/tcp-88(8)
14/05/2016 23:13	VoIP Endpoints	198.18.193.26	Jabber-WKS	198.18.133.40	2	Ping_Oversized_Packet(1)
14/05/2016 23:19	Jabber-WKS	198.18.133.40	Catch All	198.18.133.1	2	Ping_Oversized_Packet(1)
15/05/2016 00:11	Jabber-WKS	198.18.133.40	UC Servers	198.18.133.4	0	Suspicious From Jabber WKS to UC Servers-445(451)
15/05/2016 00:11	Jabber-WKS	198.18.133.40	UC Servers	198.18.133.3	0	Suspicious From Jabber WKS to UC Servers-8080(451)

Hopefully, you should see something like the screenshot above, which shows the Port Scan as a Security Event!

Phew!

In this lab we created policy based segmentation rules for our collaboration traffic and used TrustSec to enforce them. We have also used the Lancope solution to look out for suspicious activity in our lab and can quickly determine if a Jabber user is behaving unusually and running port scans against our mission critical UC servers. The good news is that the port scan never reached CUCM and IMP, and we can now go and investigate why the Jabber-WKS (.40) has a port scanner installed.

Note: In a more sophisticated Lancope deployment we could have integrated the StealthWatch Management Console with ISE and actually quarantined the suspicious Jabber WKS. We simply change the client's SGT, which corresponds to a different ACL policy. We could even pop a message to the user via their browser informing of the Security Action taken against them.

You've reached the end of the lab. Thanks for your time……