



# Cisco TrustSec Quick Start Configuration Guide

## Table of Contents

Introduction .....	5
Using This Guide.....	5
<b>Baseline ISE Configuration for TrustSec.....</b>	<b>7</b>
Active Directory Integration (optional).....	7
Defining the Security Groups (SG) and Security Group Tag (SGT).....	8
Creating the Device SGT.....	8
Defining Security Groups and SGTs .....	9
Auto-generating SGTs .....	9
Reserving a range or manually defining Security Group Tags.....	9
Importing SGs and SGTs from a spreadsheet.....	10
Defining TrustSec Devices within ISE.....	10
Cisco IOS, NX-OS, IOS-XE devices.....	10
Cisco ASA5500 Adaptive Security Appliances.....	12
Network Device Authorization.....	13
Chapter Summary.....	13
<b>TrustSec Policy Acquisition.....</b>	<b>14</b>
Catalyst Devices .....	14
Policy Acquisition.....	14
Verifying Policy Acquisition.....	15
NXOS Devices .....	16
Policy Acquisition.....	16
Verifying Policy Acquisition.....	16
ASA.....	17
Policy Acquisition.....	17
Verifying Policy Acquisition.....	18
Chapter Summary.....	19
<b>Classification.....</b>	<b>21</b>
Dynamic SGT Assignment.....	21
Static SGT Assignment.....	21
Mapping a SGT to a port-profile (Nexus 1000v).....	21
Mapping a SGT to an IP Address .....	22
Using ISE.....	22
Validate IP to SGT Mapping .....	23
Using CLI.....	23

For Catalyst Devices .....	23
IP to SGT Mapping .....	23
Subnet to SGT Mapping .....	23
VLAN to SGT Mapping .....	23
Port to SGT Mapping .....	24
For Nexus Devices.....	24
IP to SGT Mapping .....	24
VLAN to SGT Mapping .....	24
Port to SGT Mapping .....	24
Chapter Summary .....	24
<b>SGT Propagation.....</b>	<b>25</b>
Inline SGT between 3650 and ASA .....	25
3650.....	25
ASA .....	25
Verify inline tagging between 3650 and ASA.....	25
SXP between Nexus 1000v and ASA .....	26
Nexus 1000v.....	26
ASA SXP configuration using ASDM.....	27
Configuring SXP on Switches (other than the Nexus 1000v).....	28
Between Catalyst Platforms .....	28
Example: Catalyst 2K(speaker) to Catalyst 3K(listener) .....	28
Catalyst 3K (listener) to Catalyst 2K(speaker) .....	28
Between Nexus Platforms.....	29
Example: Nexus 1000V(speaker) to Nexus 7000(listener) .....	29
Nexus 7000(listener) to Nexus 1000V(speaker) .....	29
Inline Tagging on Switches (other than the Nexus 1000v).....	29
Nexus 5500/6000 Switches .....	29
Catalyst and Other Nexus Platforms .....	29
Chapter Summary .....	29
<b>Enforcement .....</b>	<b>30</b>
Defining Security Group ACLs (SGACLs).....	30
Defining Egress Policy within ISE .....	31
Enabling Enforcement On Switches.....	32
Catalyst Devices.....	32
Nexus 1000v.....	32
SGACL Download Verification.....	32
Enabling Enforcement on the ASA.....	33

---

Nexus Devices .....	34
Conclusion .....	35
For More Information.....	35

## Introduction

Cisco TrustSec uses tags to represent logical group privilege. This tag, called a Security Group Tag (SGT), is used in access policies. The SGT is understood and is used to enforce traffic by Cisco switches, routers and firewalls. Cisco TrustSec is defined in three phases, classification, propagation and enforcement. When users and devices connect to a network, the network assigns a specific security group. This process is called classification. Classification can be based on the results of the authentication or by associating the SGT with an IP, VLAN, or port-profile (more on this later in this guide). Once user traffic is classified, then the SGT is propagated from where classification took place, to where enforcement action is invoked. This process is called propagation.

Cisco TrustSec has two methods of SGT propagation: inline tagging and SXP. With inline tagging, the SGT is embedded into the ethernet frame. The ability to embed the SGT within an ethernet frame does require specific hardware support. Therefore network devices that don't have the hardware support use a protocol called SXP (SGT Exchange Protocol). SXP is used to share the SGT to IP address mapping. This allows the SGT propagation to continue to the next device in the path.

Finally an enforcement device controls traffic based on the tag information. A TrustSec enforcement point can be a Cisco firewall, router or switch. The enforcement device takes the source SGT and looks it up against the destination SGT to determine if the traffic should be allowed or denied. If the enforcement device is a Cisco firewall it also allows stateful firewall processing and IPS deep packet inspection using the same source SGT in a single firewall rule.

## Using This Guide

The goal of this guide is to illustrate how to enable TrustSec to classify endpoints and servers with a Security Group Tag, propagate Security Group Tag information across the network, and enforce traffic based on the SGT information. This guide provides step by step configuration of a sample test environment comprised of a Cisco Catalyst 3650, a Cisco Adaptive Security Appliance, and a Cisco Nexus 1000v. These platforms were chosen to illustrate that a typical TrustSec network utilizes a combination of different classification, propagation, and enforcement methods. Once the concepts of Cisco TrustSec are familiar, the other use case specific guides may be referenced to expand the Cisco TrustSec environment.

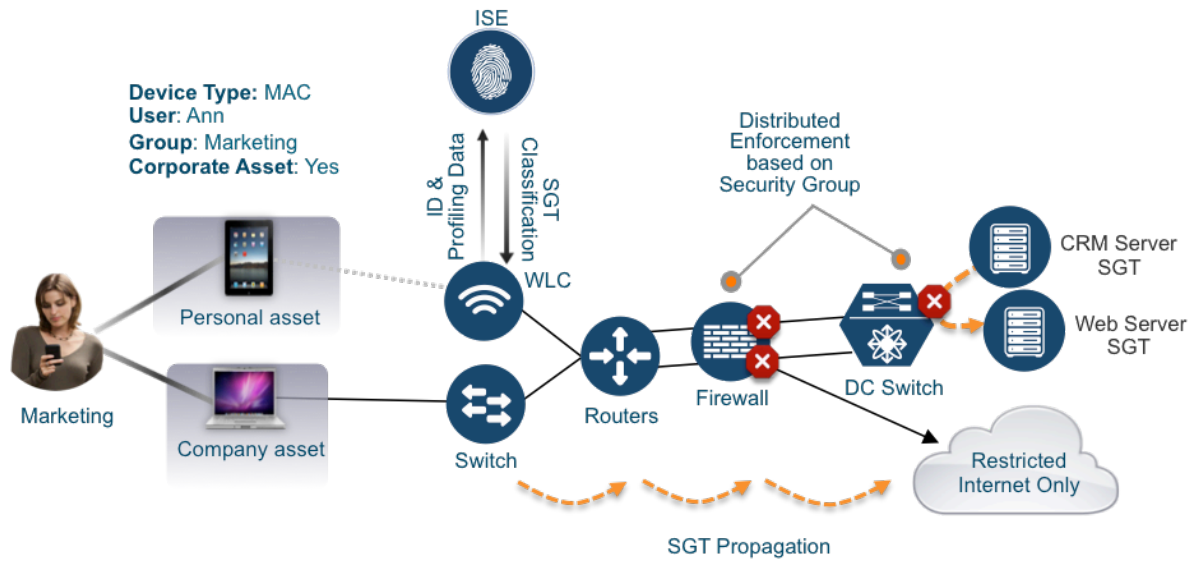
This guide is written using a best practice approach to configuring a Cisco TrustSec solution from start to finish. The approach is outlined below:

1. Baseline Cisco Identity Services Engine Configuration for Cisco TrustSec
2. TrustSec Policy Acquisition
3. Classification
4. Propagation
5. Enforcement

This guide should be used as general guidance to configure the TrustSec solution in a network. Below a sample topology diagram (Figure 2) is used to illustrate a typical enterprise network. This guide will walk through the general configuration steps to illustrate how to enable TrustSec to

classify endpoints and servers with a Security Group Tag, propagate Security Group Tag information across network, and enforce traffic based on the SGT information. Additionally general troubleshooting and best practice tips are provided where relevant.

The sample configuration used in this guide will enable access for employees, connected at campus and branch locations, to access production servers but not the development servers in the data center.



**Note:** Not all platforms that support TrustSec are represented here. However, the platforms shown are representative of the configuration commands for TrustSec. Please refer to the following link for a complete listing of platform support: [http://www.cisco.com/c/en/us/solutions/enterprise-networks/trustsec/trustsec\\_matrix.html](http://www.cisco.com/c/en/us/solutions/enterprise-networks/trustsec/trustsec_matrix.html)

**Note:** This guide does not provide deployment guidance or step-by-step configuration instructions for specific use cases. These topics are covered separately. Please refer to <http://www.cisco.com/c/en/us/solutions/enterprise-networks/trustsec/index.html>

## Baseline ISE Configuration for TrustSec

The Cisco Identity Services Engines (ISE) is commonly used as the central repository for Security Group Tags, Security Groups, and Security Group ACLs. In this section, we are going to configure two of the key policy elements in the TrustSec solution, the Security Group Tags (SGTs) and Security Groups. TrustSec uses the SGT, also known as a “tag” to represent a user or device group. For example, tags such as “Employees\_SGT” and “Development Servers\_SGT” can represent the user group, “Employees” and the server group, “Development Servers”. These tags are then used as sources and/or destinations in an access policy.

**Note:** The scope of this document provides the minimum configuration information needed to support TrustSec functions. It does not cover the advanced ISE functions like complex authentication and authorization of users nor does it cover associated services configuration such as Profiling, Guest management, and On-Boarding for BYOD. Please refer to the following URL for guidance for these configurations: [Design Zone for Security - Cisco](#)

### Active Directory Integration (optional)

This step prepares ISE to associate SGTs with groups in Active Directory. If ISE is already joined to Active Directory for user authentication, this step can be skipped. More details on associating the SGT with an AD group later on in the Classification chapter.

- Step 1**    Navigate to **Administration->Identity Management->External Identity Sources**
- Step 2**    Pick Active Directory from the left-hand-side panel, and click **ADD**
- Step 3**    Fill in the join point name and domain name and **SUBMIT**



The screenshot shows a configuration window titled "Connection". It has two input fields, both marked with an asterisk (\*). The first field is labeled "Join Point Name" and is empty. The second field is labeled "Active Directory Domain" and is also empty. Below the input fields are two buttons: "Submit" and "Cancel".

- Step 1**    Navigate to **Groups**
- Step 2**    Select **ADD** and choose "Select Groups from Directory"
- Step 3**    Check all of the groups that you want to associate SGTs with.
- Step 4**    Click **OK** and **Save**

**Note:** For additional information on Active Directory with Cisco ISE refer to: [Active Directory Integration with Cisco ISE 1.3 - Cisco](#)

## Defining the Security Groups (SG) and Security Group Tag (SGT)

When following best practice guidelines, there are three types of tags. They are the device tag (device SGT), the SGTs used to represent security groups used to define policies, and the unknown tag.

A *device tag* is used to represent network devices that communicate with ISE for policy information. There is additional significance associated with this tag that will be explained in the Enforcement section.

The *unknown tag*, by default is a SGT=0. This value cannot be modified. Any traffic that is not associated with a SGT is subject to the default catch policy or specific policies defined for SGT=0.

### Creating the Device SGT

**Best Practice:** Create a tag (SGT) to represent network devices that communicate with ISE for *policy* information.

- Step 1** Navigate to **Policy->Policy Elements->Results->TrustSec->Security Groups**
- Step 2** Click the **ADD** button.
- Step 3** Create the security group “**TrustSec\_Device\_SGT**” and **Save**.



Security Groups List > TrustSec\_Devices

### Security Groups

\* Name  Generation Id: 0

Description

Security Group Tag (Dec / Hex): 2/0002

Figure 1: *Creating TrustSec Device SGT*

**Troubleshooting:** If there is an error when creating the SGT, you should look at the error message from ISE and try again. Typically an invalid character was typed. See example below:



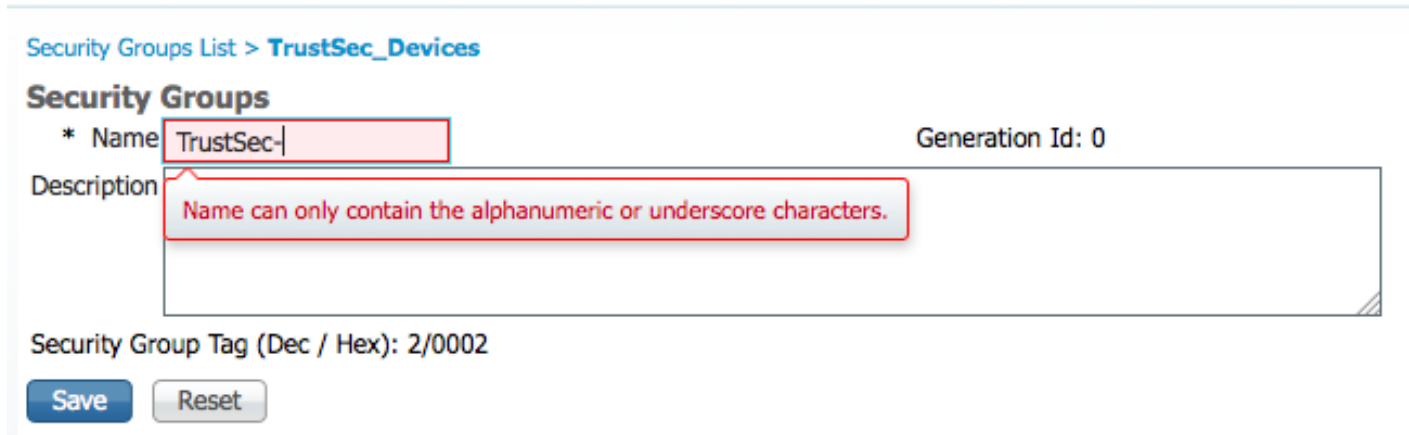


Figure 2: Security Group Syntax Error

## Defining Security Groups and SGTs

To accommodate different environments, there are three ways to define SGs and SGTs. By default, ISE can auto generate the SGTs. This method is commonly used for lab setup or small deployments. Additionally ISE does provide the ability to manually create any SGT value, to auto-generate values from within a specific range, or to import the information from a spreadsheet.

The sample configuration uses automatic SGT creation. The other two methods are shown for reference only.

### Auto-generating SGTs

- Step 1** Navigate to **Policy->Policy Elements->Results->TrustSec->Security Groups**
- Step 2** Click the **ADD** button.
- Step 3** Create the security group “**Employee\_SGT**” and **Save**.
- Step 4** Repeat Step 1 to create the remaining SGTs

Security Groups			
<span>Edit</span> <span>Add</span> <span>Import</span> <span>Export</span> <span>Delete</span> <span>Push</span>			
	Name	SGT (Dec / Hex)	Description
<input type="checkbox"/>	Development_Servers_SGT	5 / 0005	
<input type="checkbox"/>	Employee_SGT	3 / 0003	
<input type="checkbox"/>	Production_Servers_SGT	4 / 0004	
<input type="checkbox"/>	TrustSec_Device_SGT	2 / 0002	
<input type="checkbox"/>	Unknown	0 / 0000	Unknown Security Group

Figure 3: Creating Security Groups

### Reserving a range or manually defining Security Group Tags

- Step 1** Navigate to **Administration->System->Settings->TrustSec**
- Step 2** Check reserve a range
- Step 3** Fill in a range and click the **Save** button

- Step 4** Navigate to **Policy->Policy Elements->Results->TrustSec->Security Groups**  
**Step 5** Create the security group using the desired method.

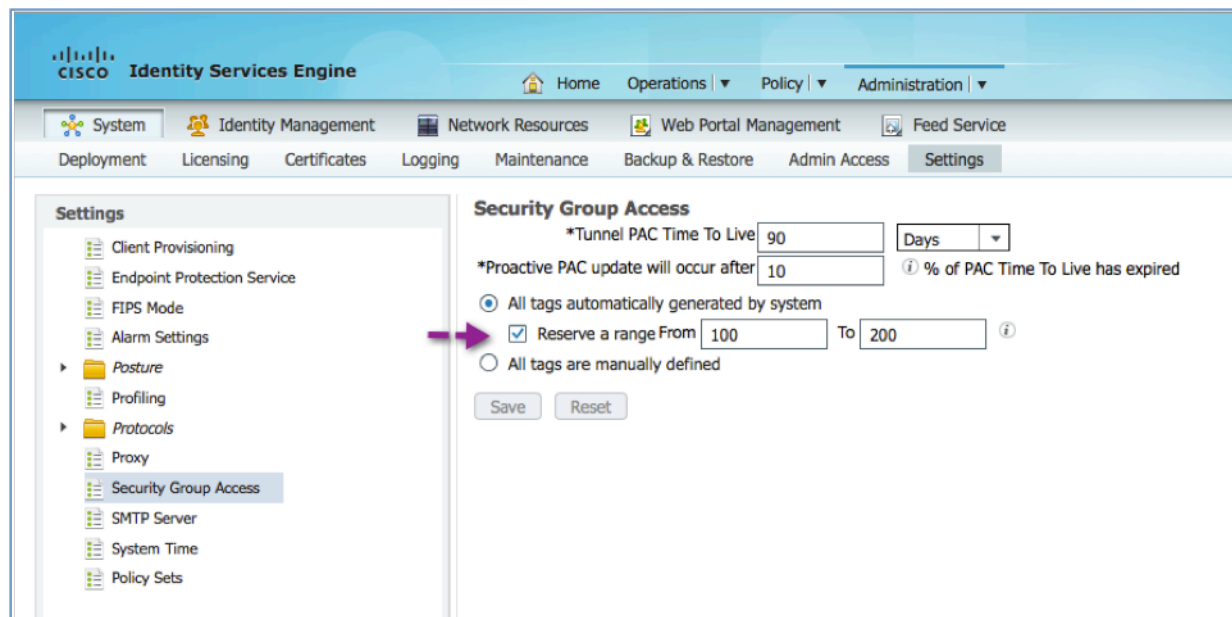


Figure 4: Reserving a range or manually defining Security Group Tags

### Importing SGs and SGTs from a spreadsheet

- Step 1** Navigate to **Policy->Policy Elements->Results->TrustSec->Security Groups->Export**  
**Step 2** Complete the spreadsheet  
**Step 3** Click **Policy->Policy Elements->Results->TrustSec->Security Groups->Import** to import the completed spreadsheet

## Defining TrustSec Devices within ISE

ISE communicates with network devices for many tasks. In the classification phase, network devices query ISE to authenticate and authorize users and devices. For enforcement, the enforcement device queries ISE to retrieve access policy and keeps its policy table up-to-date. Below you will register the Catalyst 3650, Nexus 1000v, and the Adaptive Services Appliance to exchange these pieces of information.

### Cisco IOS, NX-OS, IOS-XE devices

- Step 1** Navigate to **Administration->Network Resources->Network Devices**  
**Step 2** Edit or Add an entry  
**Step 3** Select the **Advanced TrustSec Settings** checkbox. This expands the SGT attributes of the Network Device definition.  
**Step 4** Enter the values as shown in the table below.

**Note:** Items that are bolded are the fields that need modification. The other fields are left at default values

<input checked="" type="checkbox"/> <b>Advanced TrustSec Settings</b>		Description
<b>Device Authentication Settings</b>		
Use Device ID for TrustSec	<input checked="" type="checkbox"/>	
Device Id	3k-access	This is automatically populated from the Device Name if Use Device ID for SGA identification is checked. This ID must match the "cts device-id" command that is later configured on the switch.
Password	<b>ISEisC00L</b>	TrustSec authentication password. This must match the password that is associated with the "cts device-id" command
<b>TrustSec Notifications and Updates</b>		
Download environment data every	1 Days	Specifies the expiry time for environment data. ISE returns this information when the switch queries for environment data. The default is 1 day
Download peer authorization policy every	1 Days	Specifies the expiry time for the peer authorization policy. ISE returns this information to the device in response to a peer policy request. The default is 1 day
Reauthentication every	1 Days	<b>NOT used in this lab.</b> Specifies the dot1x re-authentication period. ISE configures this for the supplicant and returns this information to the authenticator. The default is 1 day
Download SGACL lists every	1 Days	Specifies the expiry time for SGACL lists. ISE returns this information to the device in the response to a request for SGACL lists. The default is 1 day.
Other TrustSec devices to trust the device	<input checked="" type="checkbox"/>	Specifies whether all the device's peer devices trust this device. The default is checked, which means that the peer devices trust this device, and do not change the SGTs on packets arriving from this device. If you uncheck the check box, the peer devices repaint packets from this device with the related peer SGT.
Send configuration changes to device	<input checked="" type="checkbox"/> <b>Using</b> <input checked="" type="radio"/> <b>CoA</b> <input type="radio"/> CLI (SSH)	

**Note:** The step above configures communication between the 3650 and ISE. The step must be repeated to configure the communication between the Nexus1000v and ISE.

### Cisco ASA5500 Adaptive Security Appliances

- Step 1** Navigate to **Administration->Network Resources->Network Devices**
- Step 2** Edit or add a entry for the ASA
- Step 3** Within the “**Advanced TrustSec Settings**”, *set the password to any value*. This password is not used because the ASA supports Out of Band PAC(OOB) PAC provisioning (details in the following step). You must enter valid and non-empty string in order to save this object.

### Advanced TrustSec Settings

<input checked="" type="checkbox"/> <b>Advanced TrustSec Settings</b>		
<b>Device Authentication Settings</b>		
Use Device ID for TrustSec	<input checked="" type="checkbox"/>	
Device Id	T-ASA	
Password	<b>&lt;anything&gt;</b>	This password is not used because ASA supports only OOB PAC provisioning. However it needs to be a valid and non-empty string in order to save the NAD object.

- Step 1** In the section “Out Of Band (OOB) SGA PAC”, click Generate PAC.

Identity	T-ASA
Encryption Key	<b>ISEisC00L</b>
PAC Time to Live	1 Years

- Step 2** In the pop-up dialog box, input a string as the Encryption Key

**Note:** ASA uses this encryption key to import the PAC securely

- Step 1** Click on **Generate PAC**. In the pop-up window, click **OK** to accept the default **Save File** option to save the resulting pac file to the default Downloads folder
- Step 2** Click **Save** to save your changes.
- Step 3** If clicking the submit button doesn’t refresh the screen, your web console session has timed out. Log out of ISE and close ALL browser windows. Then log back into ISE and re-run the ASA steps. This is a known issue, CSCu157034

## Network Device Authorization

In a TrustSec enabled network, all network resources are classified with SGTs. This includes a network device itself. All traffic initiated from network device is going to be tagged with a SGT. Previously you defined this SGT as the “TrustSec Device SGT”. Now you will configure ISE to assign this SGT when a network device authenticates against ISE. Once the switches have this SGT, traffic that is initiated from the switch will be tagged with this SGT.

1. Navigate to **Policy->TrustSec ->Network Device Authorization**. You will find *Default* rule for *Network Device Authorization*.
2. **Edit** link of the rule table and change value of SGT from **Unknown** to **TrustSec\_Device\_SGT**.
3. Click **Done** and Click **Save** button at bottom to save this configuration.



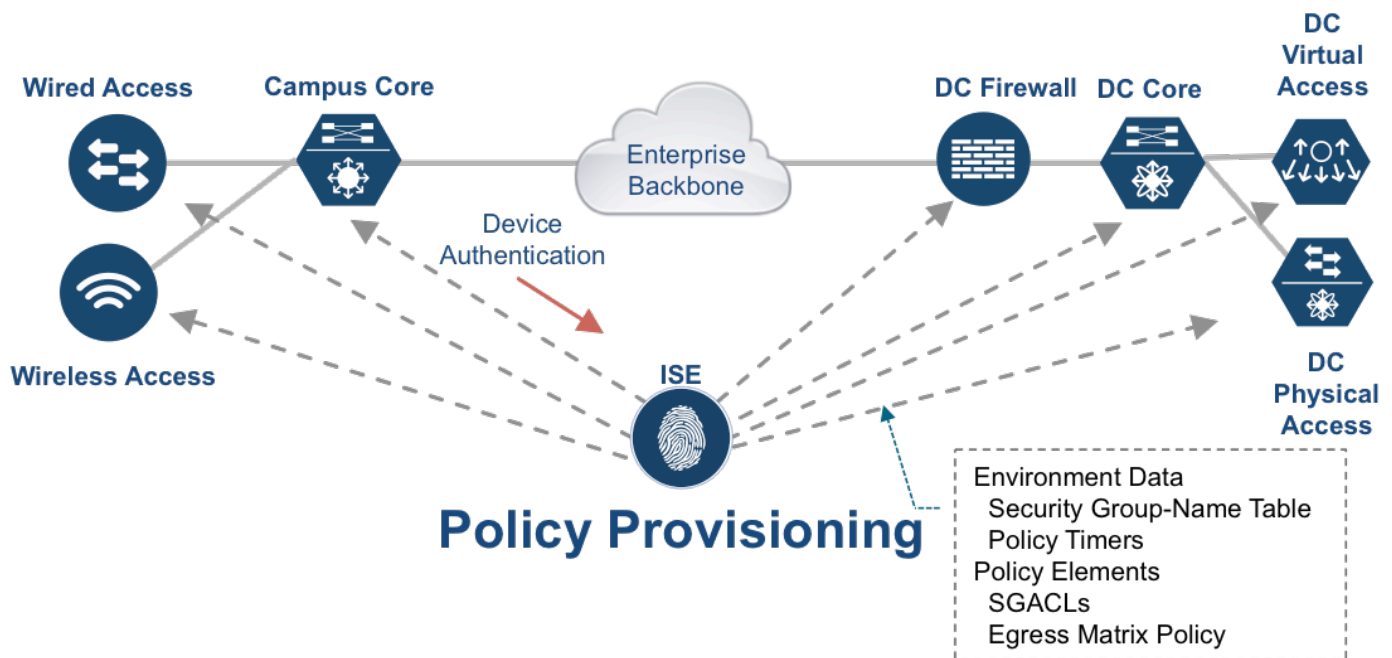
Figure 4: Assigning a SGT to network devices

## Chapter Summary

We have completed the baseline ISE configuration to enable TrustSec. In the following sections, we will come back to ISE user interface to configure specific settings for classification and enforcement. But at this point, your network device is ready to communicate with ISE, download list of SGT values and establish communication pipeline to download policy once a network device is configured.

## TrustSec Policy Acquisition

In the previous section, we've configured ISE as the central repository for the list of Security Groups and the corresponding SGT values. In this section, we will configure the network devices to communicate with ISE to pull this information as well as to download communication specific timers. In order for the network device to query ISE and obtain appropriate policies or policy elements, network devices authenticate to ISE. Once authenticated, the device downloads policies.



### Catalyst Devices

#### Policy Acquisition

**Step 1** Configure the credentials that will be used for Network Device Authorization

```
3650# cts credentials id <device-id> password <password>
```

**Step 2** Configure the switch to obtain policy from ISE. Enter configuration mode and enter the following commands:

```
aaa authorization network cts-list group ise+pac
cts authorization list cts-list
radius server ISE
address ipv4 <ip address of ISE policy services node> auth-port 1812 acct-port 1813
pac key <secret>
exit
aaa group server radius ISE
```

```
server name ISE
```

**Troubleshooting Tip:** Reference CSCty28655. Utilize the suggested workaround if upgrading to the recommend code version is not possible.

## Verifying Policy Acquisition

### Step 3 Verify PAC is provisioned

```
3650# show cts pac
AID: 5CA42F60834DE482B716028EAA4EFA8B
PAC-Info:
PAC-type = Cisco Trustsec
AID: 5CA42F60834DE482B716028EAA4EFA8B
I-ID: 3k-access
A-ID-Info: Identity Services Engine
Credential Lifetime: 15:53:10 UTC Oct 29 2014
PAC-Opaque:
000200B800030001000400105CA42F60834DE482B716028EAA4EFA8B0006009C00030100DCC3AF447CA810C1442E417A2F
B6F8720000001353D1ABB400093A808ACFEF1042BA878EB3585CEE1B108AE45D6F5896B493430DE24C25686AE418C5EEFD
E44606C9D3FB09A0E8AB261C98D00EC9F42567D377636A88CC9125A3FDB458F9A4FBE8AF4530D616584C1B146B92091342
2B30EA50184D6C72923A364B1735F60857591440879815021F9404868FE2DAA13C1807FCB1464C2C57
Refresh timer is set for 12w4d
```

### Step 4 Environment data download verification

```
3650# show cts environment-data
CTS Environment Data
=====
Current state = COMPLETE
Last status = Successful
Local Device SGT:
SGT tag = 2-00:TrustSec_Device_SGT
Server List Info:
Installed list: CTSServerList1-0001, 1 server(s):
*Server: 10.1.100.21, port 1812, A-ID 5CA42F60834DE482B716028EAA4EFA8B
Status = ALIVE
auto-test = TRUE, keywrap-enable = FALSE, idle-time = 60 mins, deadtime = 20 secs
Security Group Name Table:
  0-00:Unknown
  2-00:TrustSec_Device_SGT
  3-00:Employee
  4-00:Production_Servers (reserved)
  5-00:Development_Servers (reserved)
Environment Data Lifetime = 86400 secs
Last update time = 15:54:16 UTC Thu Jul 31 2014
Env-data expires in 0:23:46:47 (dd:hr:mm:sec)
Env-data refreshes in 0:23:46:47 (dd:hr:mm:sec)
Cache data applied = NONE
State Machine is running
```

## NXOS Devices

### Policy Acquisition

#### Step 1 Enable TrustSec

```
svs switch edition advanced
feature cts
feature dot1x
cts device tracking
```

**Note:** "cts device tracking" enables the 1KV to tracking using its IP database (IPDB). The IP database tracks the IP Addresses that are learned.

**Note:** "svs switch edition advanced" enables the advanced license which is necessary to enable CTS

#### Step 2 Configure the switch to establish a connection with ISE.

```
radius-server host <ip address> key <secret> pac auth-port 1812 acct-port 1813
aaa group server radius cts-radius
server <name or IP of ISE Policy Services Node>
use management vrf
exit
aaa accounting default group cts-radius
aaa authorization cts default group cts-radius
```

#### Step 3 Configure the device credential (this MUST match the "device-id (case sensitive) configured within the Advanced TrustSec settings for the N1Kv on ISE). This command will initiate the communication with ISE.

```
nexus(config)# cts device-id <device-id> password <password>
```

### Verifying Policy Acquisition

#### Step 4 Verify PAC file is provisioned

```
nexus# show cts pac
PAC Info :
=====
PAC Type           : Trustsec
AID                : a6ee87f55c7131943d615cc1d47025bf
I-ID              : N1Kv
AID Info           : Identity services Engine
Credential Lifetime : Thu Jan  2 22:47:50 2014

PAC Opaque        :
000200b00003000100040010a6ee87f55c7131943d615cc1d47025bf00060094000301005a705134937fede63969e66676
ba2cfd00000013524d8aa700093a80ebcf09b38cc61b08e2e24e1e9fb4a9cb3f28907accd3785a356c0f1f3df62df8d673
590614ce4adfb083d05eaa906eef3dac86e2f6de0d7e8c5a86a9845b934e6f814de0fbd0d7213d7c77e3c23b4efbf7b34d
0893f2588b6768d6f545b7a9b11ce11701336bb269650cfa132df6d39240c60b6a
```

#### Step 5 Verify the CTS environment data has been downloaded



```
Nexus# show cts environment-data
CTS Environment Data
=====
Current State       : CTS_ENV_DNLD_ST_ENV_DOWNLOAD_DONE
Last Status        : CTS_ENV_SUCCESS
Local Device SGT    : 0x0002
Transport Type     : CTS_ENV_TRANSPORT_DIRECT
Data loaded from cache : FALSE
Env Data Lifetime  : 86400 seconds after last update
Last Update Time   : Wed Oct 23 14:40:36 2013

Server List        : CTSServerList1
                   AID:a6ee87f55c7131943d615cc1d47025bf IP:10.1.100.21 Port:1812
```

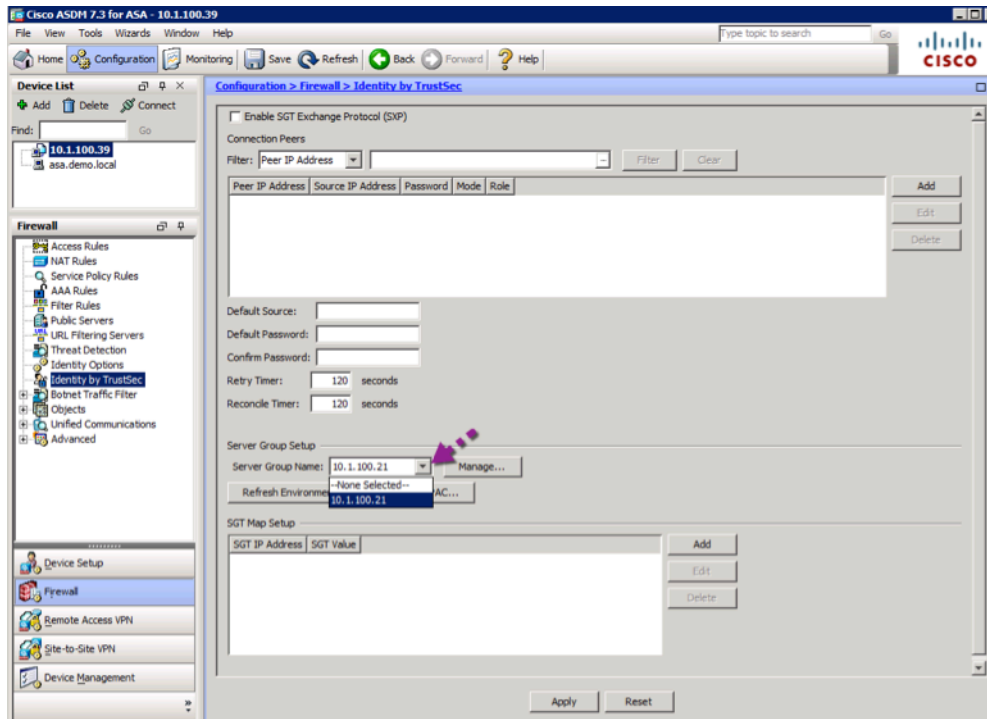
**Troubleshooting Tip:** If these steps fail, the device-id or password is probably mis-typed. Below is a sample Live Log entry of the failure.

Time	Status	Details	Repeat Count	Identity	Event	Authentication Protocol
2014-07-23 11:54:31.529	✖			N1KV	Authentication failed	EAP-FAST (EAP-MSCHAPv2)

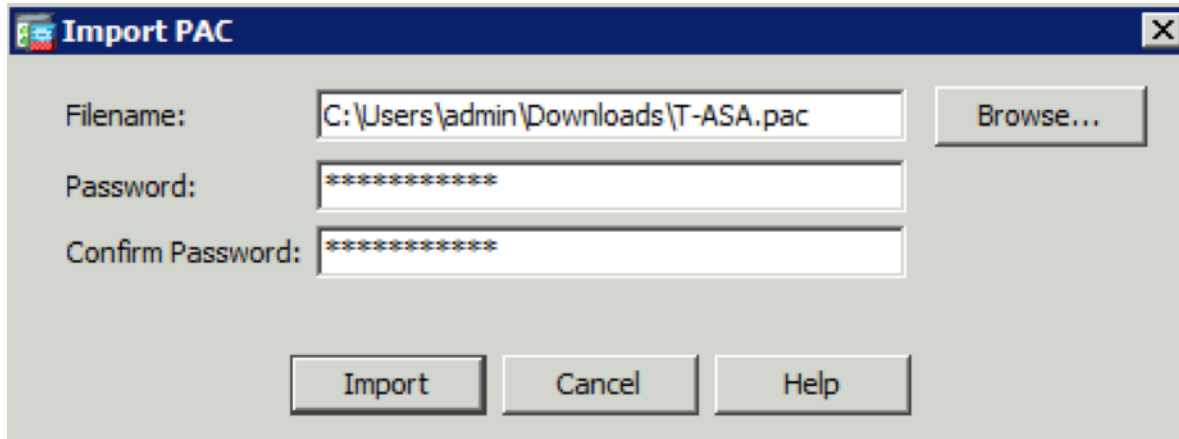
## ASA

### Policy Acquisition

- Step 1** Navigate to **Configuration->Firewall->Identity by TrustSec** (left panel)
- Step 2** At the bottom of the resulting page, choose “10.1.100.21” for the Server group



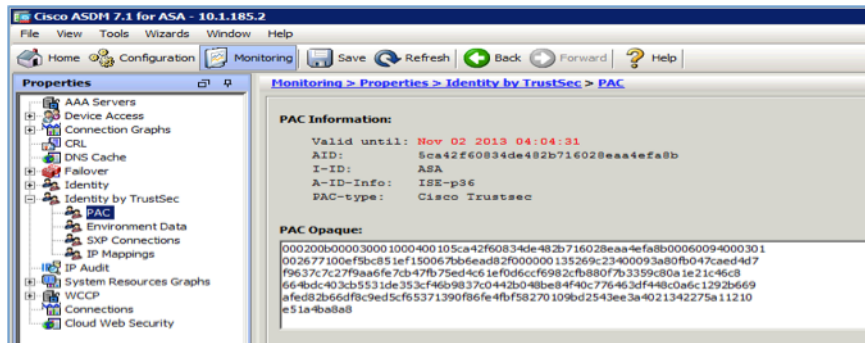
**Step 3** Choose "Import PAC" as shown below, to import the PAC. Enter the password configured within the "Advanced TrustSec Settings" on ISE



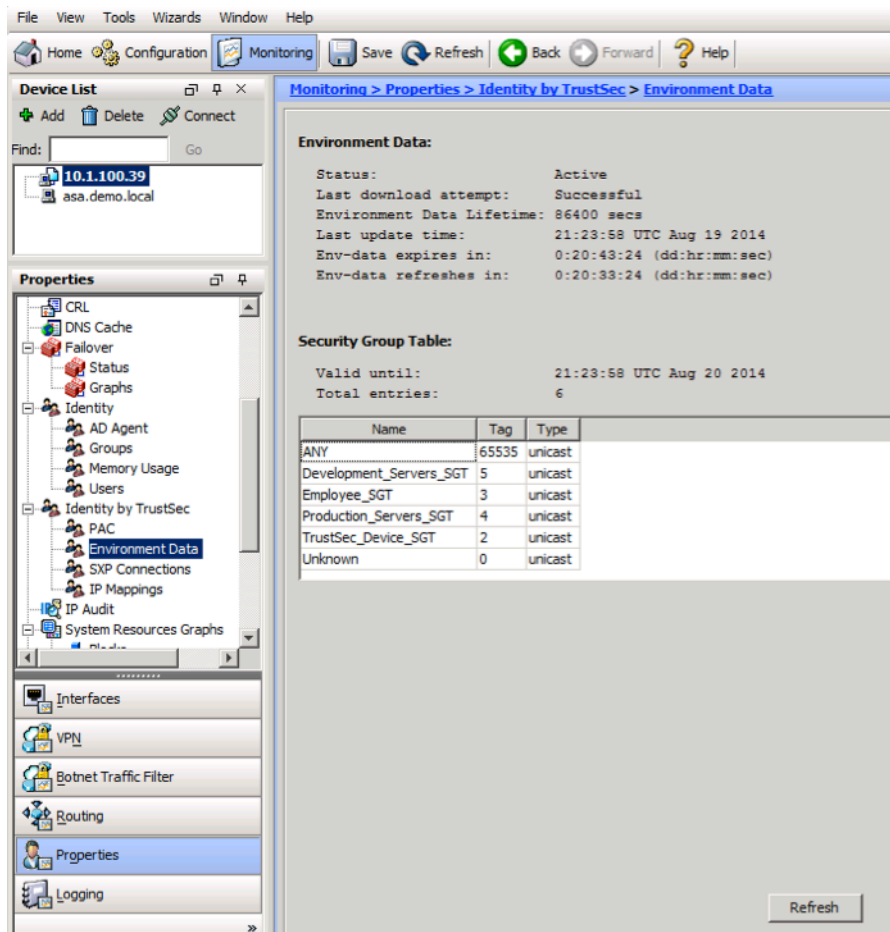
**Step 4** Click Apply

### Verifying Policy Acquisition

**Step 1** Verify PAC file is provisioned. Navigate to **Monitoring->Properties->Identity by TrustSec->PAC**



**Step 2** Verify environment data, device SGT, and the SGTs along with their associated group names were downloaded. Navigate to **Monitoring->Properties->Identity by TrustSec->Environment Data**. Click "Refresh" button if needed.



The screenshot shows the Cisco ISE GUI with the following content:

**Monitoring > Properties > Identity by TrustSec > Environment Data**

**Environment Data:**

- Status: Active
- Last download attempt: Successful
- Environment Data Lifetime: 86400 secs
- Last update time: 21:23:58 UTC Aug 19 2014
- Env-data expires in: 0:20:43:24 (dd:hr:mm:sec)
- Env-data refreshes in: 0:20:33:24 (dd:hr:mm:sec)

**Security Group Table:**

Valid until: 21:23:58 UTC Aug 20 2014  
Total entries: 6

Name	Tag	Type
ANY	65535	unicast
Development_Servers_SGT	5	unicast
Employee_SGT	3	unicast
Production_Servers_SGT	4	unicast
TrustSec_Device_SGT	2	unicast
Unknown	0	unicast

Refresh

**Troubleshooting Tip:** If the environment data download fails, check whether the correct password was entered. It must be the same as the password configured under the TrustSec Advanced Settings configuration for the ASA. Ensure the ASA has been saved in the ISE network device list.

## Chapter Summary

Almost all devices supporting TrustSec requires a PAC file to communicate with ISE to download key policy elements and additional information available in the environment data. Additional information related to this chapter is available in following links:

### Cisco TrustSec Catalyst Switch Configuration Guide:

[http://www.cisco.com/en/US/docs/switches/lan/trustsec/configuration/guide/ident-conn\\_config.html](http://www.cisco.com/en/US/docs/switches/lan/trustsec/configuration/guide/ident-conn_config.html)

### Cisco TrustSec for ISR G2:

[http://www.cisco.com/en/US/docs/ios-xml/ios/sec\\_usr\\_cts/configuration/15-mt/sec-usr-cts-15-mt-book.html](http://www.cisco.com/en/US/docs/ios-xml/ios/sec_usr_cts/configuration/15-mt/sec-usr-cts-15-mt-book.html)

### Nexus 7000:

[http://www.cisco.com/en/US/docs/switches/datacenter/sw/6\\_x/nx-os/security/configuration/guide/b\\_Cisco\\_Nexus\\_7000\\_NX-OS\\_Security\\_Configuration\\_Guide\\_\\_Release\\_6.x\\_chapter\\_01101.html](http://www.cisco.com/en/US/docs/switches/datacenter/sw/6_x/nx-os/security/configuration/guide/b_Cisco_Nexus_7000_NX-OS_Security_Configuration_Guide__Release_6.x_chapter_01101.html)

**Nexus 5000:**

[http://www.cisco.com/en/US/docs/switches/datacenter/nexus5500/sw/security/602\\_N1\\_2/b\\_5500\\_Security\\_Config\\_602N12\\_chapter\\_01000.html](http://www.cisco.com/en/US/docs/switches/datacenter/nexus5500/sw/security/602_N1_2/b_5500_Security_Config_602N12_chapter_01000.html)

**Nexus 1000v:**

[http://www.cisco.com/en/US/docs/switches/datacenter/nexus1000/sw/4\\_2\\_1\\_s\\_v\\_2\\_1\\_1/security/configuration/guide/b\\_Cisco\\_Nexus\\_1000V\\_Security\\_Configuration\\_Guide\\_2\\_1\\_1\\_chapter\\_010001.html](http://www.cisco.com/en/US/docs/switches/datacenter/nexus1000/sw/4_2_1_s_v_2_1_1/security/configuration/guide/b_Cisco_Nexus_1000V_Security_Configuration_Guide_2_1_1_chapter_010001.html)

## Classification

The process of assigning the SGT is called Classification. A SGT can be assigned dynamically as the result of an ISE authorization or it can be assigned via static methods that map the SGT to something, like a VLAN, subnet, IP Address, or port-profile. Dynamic classification is typically used to assign SGT to users because they are mobile. They could be connected from any location via wireless, wired, or vpn. On the other hand, servers tend not to move, so typically static classification methods are used.

The sample configuration in this chapter assigns users the “Employee\_SGT” through dynamic SGT assignment. SGT assignment for the production and development servers is shown using two static classification methods. These methods are mapping the SGT to IP addresses, and mapping the SGT to a port-profile, which is the only method possible for the virtual servers connected to a Nexus 1000v.

Additionally, a listing of the other static classification methods is included for switches other than the Nexus 1000v.

For a list of the classification methods that are supported across Catalyst and Nexus platforms, please refer to the following link:

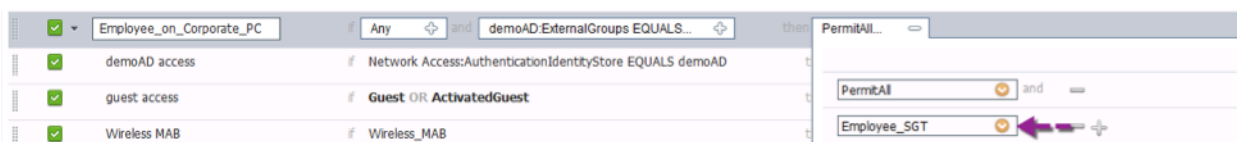
<http://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise-networks/trustsec/cisco-trustsec-platform-capability-matrix.pdf>

## Dynamic SGT Assignment

To assign the endpoint a SGT during authentication, we must modify authorization policy within ISE. This will allow employees authenticating to the network to be assigned SGT 3.

**Step 1** In ISE, Navigate to **Policy->Authorization**

**Step 2** Add the Employee\_SGT to all authorization policies that are associated with employees



**Step 3** Click **Save**

## Static SGT Assignment

### Mapping a SGT to a port-profile (Nexus 1000v)

In this section you are mapping the SGTs for production and development servers to a port profile. The port-profiles are mapped to the virtual interfaces of each of the machines using VMware

vCenter. Once the appropriate port-profile is mapped to the VM, every time the VM is powered up, the Cisco Nexus 1000V applies the appropriate port-profile, and associates the SGT to the VM. This is how classification is done on the Nexus 1000v.

**Step 1** Assign the SGT for production server to the port-profile for production servers

```
port-profile type vethernet production
cts manual
policy static sgt <hex value for SGT>
no propagate-sgt
```

**Best Practice:** “no propagate-sgt” command is necessary because this is a host facing port.

**Step 2** Assign the SGT for development server to the port –profile for development servers

```
port-profile type vethernet development
cts manual
policy static sgt 0x5
no propagate-sgt
```

**Step 3** Verify the SGTs are associate with port-profiles

```
nexus# show port-profile name production

port-profile production
  type: Vethernet
  description:
  status: enabled
  max-ports: 32
  min-ports: 1
  inherit:
  config attributes:
    switchport access vlan 101
    switchport mode access
  cts manual
  policy static sgt 0x64
  no shutdown
  evaluated config attributes:
    switchport access vlan 101
    switchport mode access
  cts manual
  policy static sgt 0x64
  no shutdown
  assigned interfaces:
    Vethernet3
```

## Mapping a SGT to an IP Address

Static classification is configured via the CLI or via a central management server like ISE. In this section, both methods are shown to illustrate how a SGT is mapped without the need for authentication.

### Using ISE

**Step 1** Navigate to **Policy-> Policy Elements-> Results->Trustsec-> Security Group Mappings**

**Step 2** Reference the following links for further detail:

For ISE 1.3+ :

[http://www.cisco.com/c/en/us/td/docs/security/ise/1-3/admin\\_guide/b\\_ise\\_admin\\_guide\\_13/b\\_ise\\_admin\\_guide\\_sample\\_chapter\\_011000.html#concept\\_CC328008C562473995FAD97C636BE360](http://www.cisco.com/c/en/us/td/docs/security/ise/1-3/admin_guide/b_ise_admin_guide_13/b_ise_admin_guide_sample_chapter_011000.html#concept_CC328008C562473995FAD97C636BE360)

For pre- ISE 1.3:

[http://www.cisco.com/c/en/us/td/docs/security/ise/1-2/user\\_guide/ise\\_user\\_guide/ise\\_sga\\_pol.html#pgfld-1059586](http://www.cisco.com/c/en/us/td/docs/security/ise/1-2/user_guide/ise_user_guide/ise_sga_pol.html#pgfld-1059586)

**Step 3** Click **Submit**

**Step 4** Click **Deploy**. This will push the mapping to the switch(es)

### Deploy Mappings

This dialog shows the progress of the deployment of the mappings to the devices. .

```
Starting to deploy. Please wait...
N5K-IP(10.1.160.2): Updated OK
Finished Task.
```

## Validate IP to SGT Mapping

**Step 1** SSH to the switch

**Step 2** Type “show cts role-based sgt-map”

```
Nexus# show cts role-based sgt-map
IP ADDRESS SGT          VRF/VLAN          SGT CONFIGURATION
10.1.160.20 100          vrf:1 CLI Configured
10.1.160.21 101          vrf:1 CLI Configured
```

## Using CLI

### For Catalyst Devices

#### IP to SGT Mapping

```
switch(config)#cts role-based sgt-map <ip address> sgt <tag value>
```

#### Subnet to SGT Mapping

```
switch(config)#cts role-based sgt-map <network>/<length> sgt <tag value>
```

#### VLAN to SGT Mapping

```
switch(config)#cts role-based sgt-map <vlan(s)> sgt <tag value>
```

### Port to SGT Mapping

```
switch(config)# port number (e.g. interface g1/0/1)
switch(config)#cts manual
switch(config)#policy static sgt <tag value> <trusted>
```

The Catalyst 6500 and 6800 series switches have support for additional static mappings to a vrf or layer 3 interface. Please refer to the following link for further details:

[http://www.cisco.com/c/en/us/td/docs/switches/lan/trustsec/configuration/guide/trustsec/command\\_sum.html#wp1548658](http://www.cisco.com/c/en/us/td/docs/switches/lan/trustsec/configuration/guide/trustsec/command_sum.html#wp1548658)

### For Nexus Devices

#### IP to SGT Mapping

```
Switch(config)#cts role-based sgt-map <ip address> <sgt-value>
```

#### VLAN to SGT Mapping

```
Switch(config)#vlan <number>
Switch(config)#cts role-based sgt <sgt-value>
```

#### Port to SGT Mapping

```
switch(config)# port number (e.g. interface e1/2)
switch(config)#cts manual
switch(config)#policy static sgt <tag value> <trusted>
```

## Chapter Summary

You have now completed classifying the users and devices in this TrustSec deployment.



## SGT Propagation

Now that classification is done, the next step is to propagate the SGTs through the environment to the point of enforcement. There are two methods of propagation, SGT inline tagging and a peering protocol called SGT eXchange Protocol (SXP). The three platforms in the sample topology all support inline tagging. While inline tagging is the preferred propagation method, for illustrative purposes, the connection between the 3650 and the ASA will use inline tagging and the connection between the ASA and the Nexus 1000Kv uses SXP. Most deployments use a combination of inline tagging and SXP.

### Inline SGT between 3650 and ASA

#### 3650

On the interface connected to the ASA's outside interface

```
3K(config-if)#cts manual
3K(config-if)#policy static sgt <decimal value of SGT> trusted
3K(config-if)#no sap
```

**Note:** The ASA does not support SAP currently. SAP is enabled by default on all switches. Therefore the "no sap" is required for inline tagging to work between a switch and the ASA (code version 9.3.x)

#### ASA

- Step 1** Navigate to **Configuration->Device Setup->Interfaces**
- Step 2** Edit the entry for the **outside** interface
- Step 3** On the resulting window, navigate to the Advanced tab
- Step 4** Enable inline tagging
- Step 5** Click **OK** and the **Apply**

### Verify inline tagging between 3650 and ASA

The ASA has a unique packet capture tool. Below are the steps to enable the tool to show the SGT

```
ciscoasa# capture <capture-name> type inline-tag interface <interface-name> real-time
```

- Step 1** From the 3650, initiate a ping to the ASA outside interface

```
3650#ping 10.1.128.1
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 10.1.128.1, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 1/10/30 ms
```

**Step 2** Look at the capture output on the ASA. You will see the icmp packets are tagged with the value of 2 .

```
1: 14:10:42.278504      INLINE-TAG 2 10.1.128.2 > 10.1.128.1: icmp: echo request
2: 14:10:42.279007      INLINE-TAG 0 10.1.128.1 > 10.1.128.2: icmp: echo reply
3: 14:10:42.282318      INLINE-TAG 2 10.1.128.2 > 10.1.128.1: icmp: echo request
4: 14:10:42.282562      INLINE-TAG 0 10.1.128.1 > 10.1.128.2: icmp: echo reply
```

## SXP between Nexus 1000v and ASA

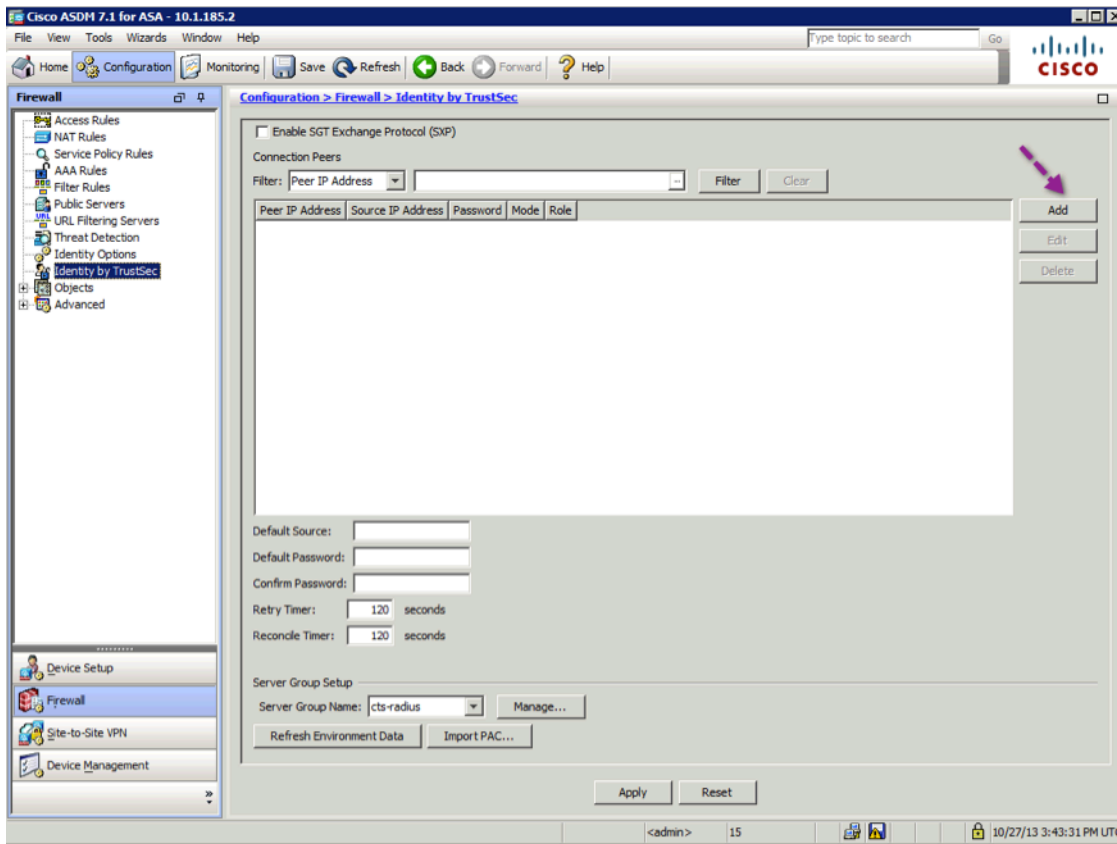
In the steps below, you will configure the N1Kv to communicate the Data Center server SGTs to the ASA via SXP. Remember the goal is to have the ASA act as the enforcement point for user to data center server access, thus it is necessary to communicate the SGTs from the data center to the ASA. Since the N1Kv is communicating the SGTs, the N1Kv is considered the "speaker". The ASA is receiving the SGT information so it is the "listener".

### Nexus 1000v

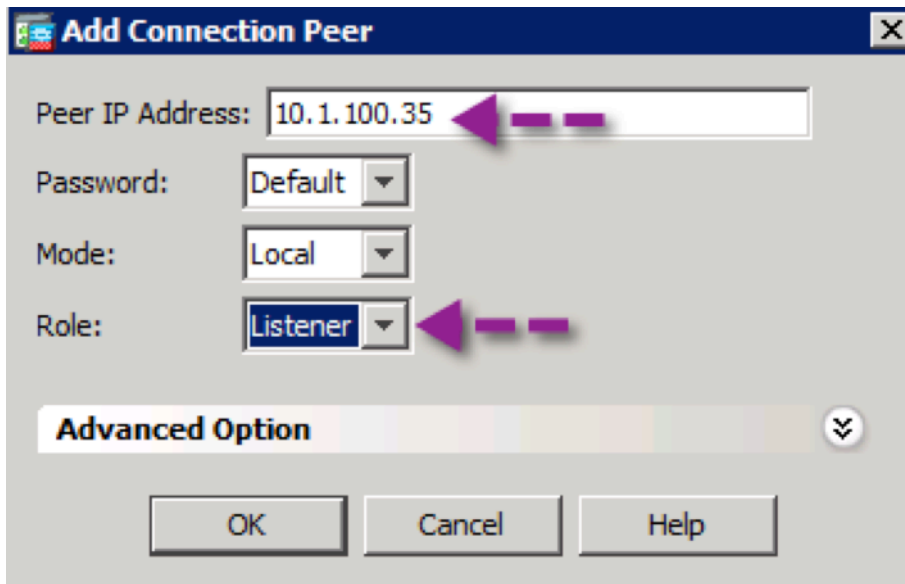
```
cts sxp enable
cts sxp default password <password for SXP>
cts sxp connection peer <ip address of ASA> source <ip address of Nexus 1000v> password default
mode listener vrf management
```

# ASA SXP configuration using ASDM

**Step 1** Navigate to **Configuration->Firewall->Identity by TrustSec** and Click the ADD button.



**Step 2** Enter the peer's IP address and specify the ASA's role



**Step 3** Click **OK**

**Step 4** On the resulting window, enable SXP and set the password for the SXP connection. This password must match what is configured on the peer device

Configuration > Firewall > Identity by TrustSec

Enable SGT Exchange Protocol (SXP) ←

Connection Peers

Filter: Peer IP Address [ ] [Filter] [Clear]

Peer IP Address	Source IP Address	Password	Mode	Role
10.1.100.35	Default	Default	Local	Listener

Default Source: 10.1.100.39

Default Password:  trustsec123

Confirm Password:

Retry Timer: 120 seconds

Reconcile Timer: 120 seconds

### Step 5 Click Apply

**Note:** You can verify the SXP connection by navigating to **Monitoring**→**Properties**→**Identity by TrustSec**→**SXP Connections**. When the SXP connection between the ASA and the N1Kv is working, the status will show as “ON”.

## Configuring SXP on Switches (other than the Nexus 1000v)

### Between Catalyst Platforms

#### Example: Catalyst 2K(speaker) to Catalyst 3K(listener)

```
2K(config)#cts sxp enable
2K(config)#cts sxp default password <sxp-password>
2K(config)#cts sxp connection peer <3K IP> source <2K IP> password default mode peer listener
```

#### Catalyst 3K (listener) to Catalyst 2K(speaker)

```
3K(config)#cts sxp enable
3K(config)#cts sxp default password <sxp-password>
3K(config)#cts sxp connection peer <2K IP> source <3K IP >password default mode peer speaker vrf <vrf>
```

---

**Note:** The SXP connection from either switch can be verified with the “**show cts sxp connection all**” command

---

## Between Nexus Platforms

### Example: Nexus 1000V(speaker) to Nexus 7000(listener)

```
cts sxp enable
cts sxp default password <sxp-password>
cts sxp connection peer <N7K IP> source <N1Kv IP> password default mode listener
```

---

**Note:** On the Nexus 1000v, SXP function is supported on the management VRF only

**Note:** On Nexus platforms, the mode refers to the peer's mode. In the example above, the “mode listener” command indicates that the peer device is the SXP listener.

---

### Nexus 7000(listener) to Nexus 1000V(speaker)

```
cts sxp enable
cts sxp default password <sxp-password>
cts sxp connection peer <N1Kv IP> password default mode speaker
```

---

**Note:** The SXP connection from either switch can be verified with the “**show cts sxp connection**” command

---

## Inline Tagging on Switches (other than the Nexus 1000v)

---

**Best Practice:** Bounce (shut and no shut) the interface once configuration is completed

---

### Nexus 5500/6000 Switches

```
cts manual
policy static sgt <hex value of SGT> [trusted]
```

### Catalyst and Other Nexus Platforms

```
cts manual
sap pmk <key> modelist [gcm-encrypt | gmac | no-encap | null]
policy static sgt <decimal value of SGT> [trusted]
```

## Chapter Summary

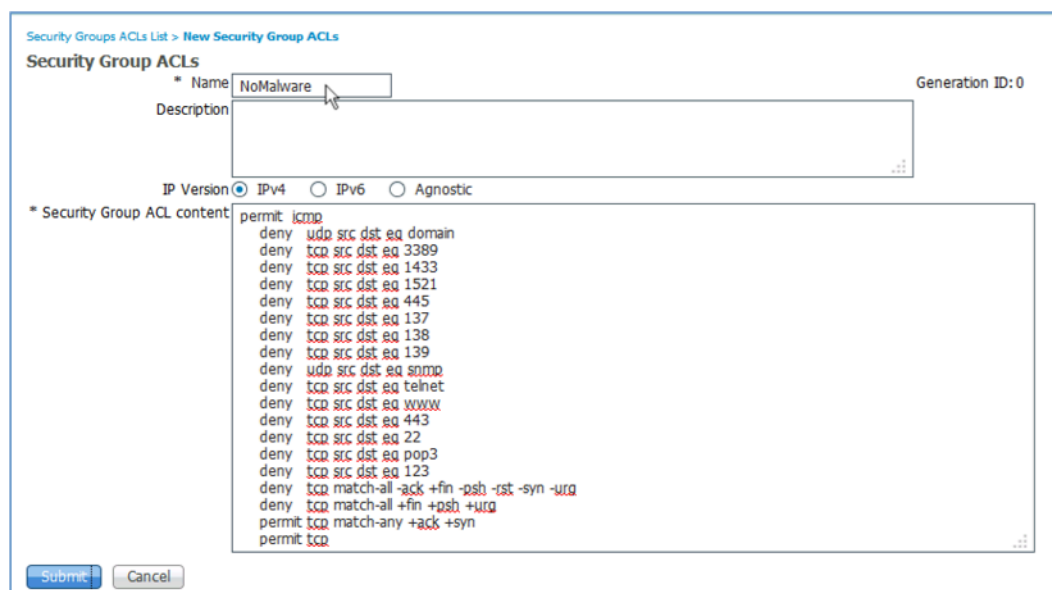
We have now completed propagating SGTs in this TrustSec deployment.

## Enforcement

Now that the SGTs are defined and communicated to all of the network devices, enforcement via SGACLs or SGFW is possible. SGACLs are centrally defined on ISE and pushed/downloaded to both Catalyst and Nexus switches. SGFW rules are defined locally on the ASA via ASDM.

### Defining Security Group ACLs (SGACLs)

- Step 1** On ISE, Navigate to **Policy->Results->TrustSec**
- Step 2** Click the down arrow and select **Security Group ACLs**
- Step 3** Click Add to create a new SGACL. The example below is a SGACL that can be used to prevent malware propagation. The SGACL also shows the syntax difference from a typical ACL.
- Step 4** Click **Save**



Security Groups ACLs List > New Security Group ACLs

**Security Group ACLs**

\* Name: NoMalware Generation ID: 0

Description:

IP Version:  IPv4  IPv6  Agnostic

\* Security Group ACL content:

```

permit icmp
deny udp src dst eq domain
deny tcp src dst eq 3389
deny tcp src dst eq 1433
deny tcp src dst eq 1521
deny tcp src dst eq 445
deny tcp src dst eq 137
deny tcp src dst eq 138
deny tcp src dst eq 139
deny udp src dst eq snmp
deny tcp src dst eq telnet
deny tcp src dst eq www
deny tcp src dst eq 443
deny tcp src dst eq 22
deny tcp src dst eq pop3
deny tcp src dst eq 123
deny tcp match-all -ack +fin -psh -rst -syn -urg
deny tcp match-all +fin +psh +urg
permit tcp match-any +ack +syn
permit tcp
  
```

Submit Cancel

**Note:** The list of rules below is provided to cut and paste to create a malware prevention SGACL

```

permit icmp
deny udp src dst eq domain
deny tcp src dst eq 3389
deny tcp src dst eq 1433
deny tcp src dst eq 1521
deny tcp src dst eq 445
deny tcp src dst eq 137
deny tcp src dst eq 138
deny tcp src dst eq 139
deny udp src dst eq snmp
deny tcp src dst eq telnet
deny tcp src dst eq www
deny tcp src dst eq 443
deny tcp src dst eq 22
deny tcp src dst eq pop3
deny tcp src dst eq 123
  
```

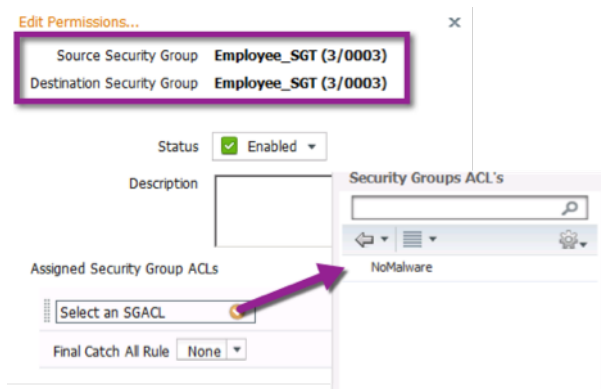
```
deny tcp match-all -ack +fin -psh -rst -syn -urg
deny tcp match-all +fin +psh +urg
permit tcp match-any +ack +syn
permit tcp
```

## Defining Egress Policy within ISE

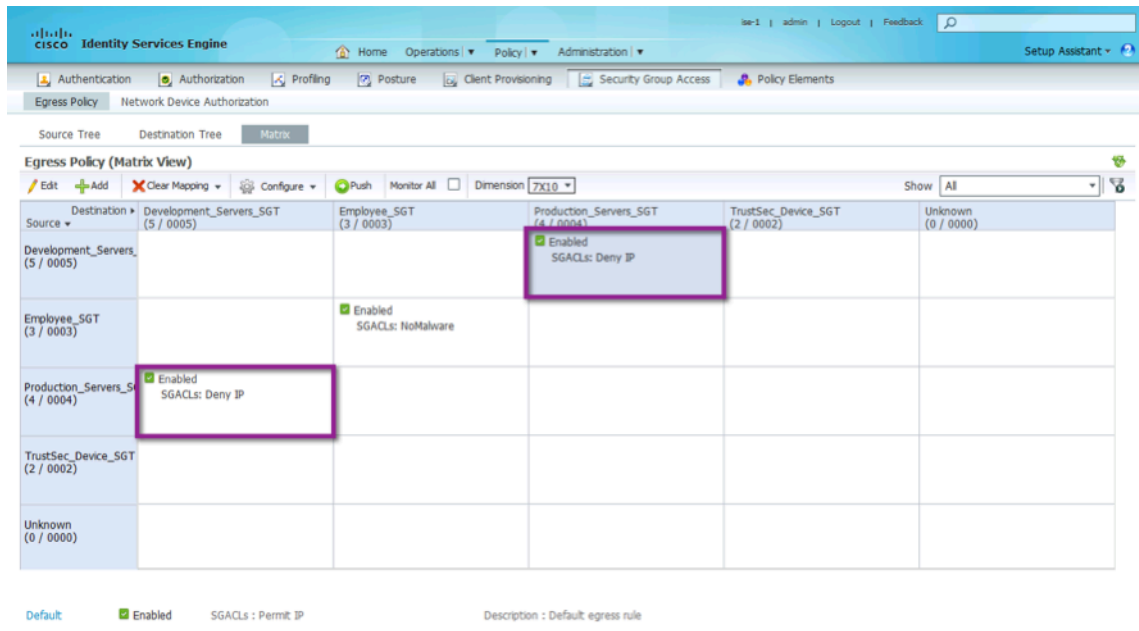
- Step 1** Navigate to Policy->TrustSec->Egress Policy
- Step 2** Click Matrix

**Note:** The matrix view highlights the cell and the corresponding row (Source SGT) and column (Destination SGT) when a cell is selected. The coordinates (Source SGT and Destination SGT) of the selected cell are displayed below the matrix content area.

- Step 3** Select a cell, click ADD to apply a policy
- Step 4** Click the orange down arrow and select “NoMalware” for **Assigned Security Group ACLs**.



- Step 5** Click Save



**Note:** Notice the Default, “catch all”, rule is Permit IP. Traffic that does not match the policies defined in the matrix as subject to the Default Egress rule.

## Enabling Enforcement On Switches

In order for a switch to enforce policy, enforcement must be specifically enabled. Once enforcement is enabled, switches will pull the policy(ies) relevant to the SGTs that they are protecting.

### Catalyst Devices

**Step 1** From the CLI, enable enforcement globally

```
cts role-based enforcement
```

**Step 2** Now enable enforcement on the desired vlan

```
cts role-based enforcement vlan <vlan # or all vlans>
```

### Nexus 1000v

Enforcement on the N1Kv is done at the port-profile level

**Step 1** Enable enforcement.

```
port-profile type vethernet development
cts manual
role-based enforcement

port-profile type vethernet production
cts manual
role-based enforcement
```

**Step 2** From the CLI, refresh the policy on the N1Kv

```
n1kv# cts refresh role-based-policy
```

### SGACL Download Verification

**Step 1** Verify the policy downloaded

```
n1kv# show cts role-based policy
sgt:4
dgt:5 rbacl:Deny IP
deny ip

sgt:5
dgt:4 rbacl:Deny IP
deny ip
```

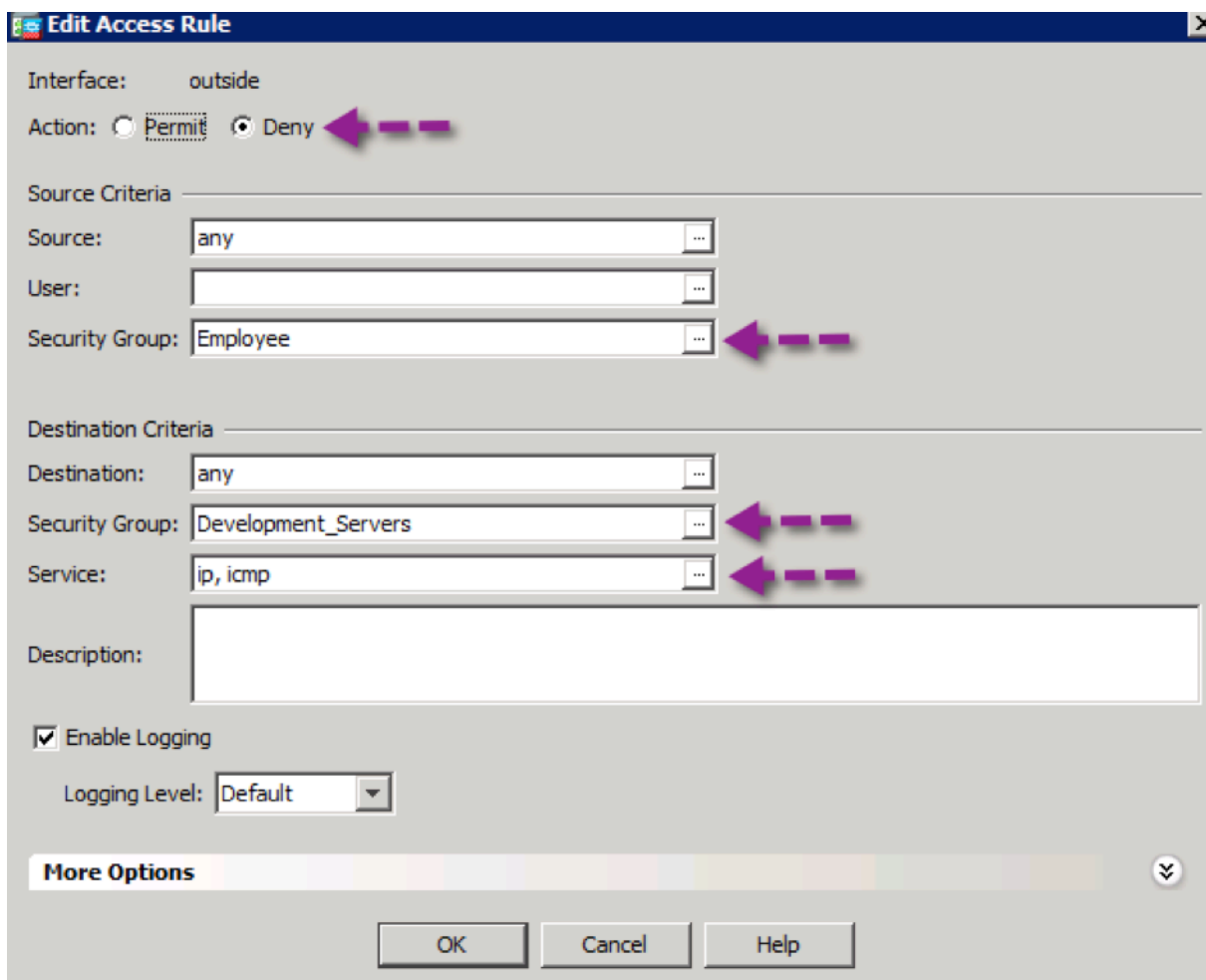


```
sgt:any
dgt:any rbacl:Permit IP
permit ip
```

## Enabling Enforcement on the ASA

In this section, we will use ASDM to configure enforcement on the ASA. Create two rules that use the CTS environment data obtained from ISE to deny ICMP traffic but permit HTTP to each server for the correct identity.

- Step 1** From ASDM, navigate to **Configuration->Firewall->Access Rules**
- Step 2** Configure a rule to deny traffic from employees to development servers on the outside interface. This rule will apply to traffic from employees that are connected via wired or wireless.



**Edit Access Rule**

Interface: outside

Action:  Permit  Deny

Source Criteria

Source: any

User:

Security Group: Employee

Destination Criteria

Destination: any

Security Group: Development\_Servers

Service: ip, icmp

Description:

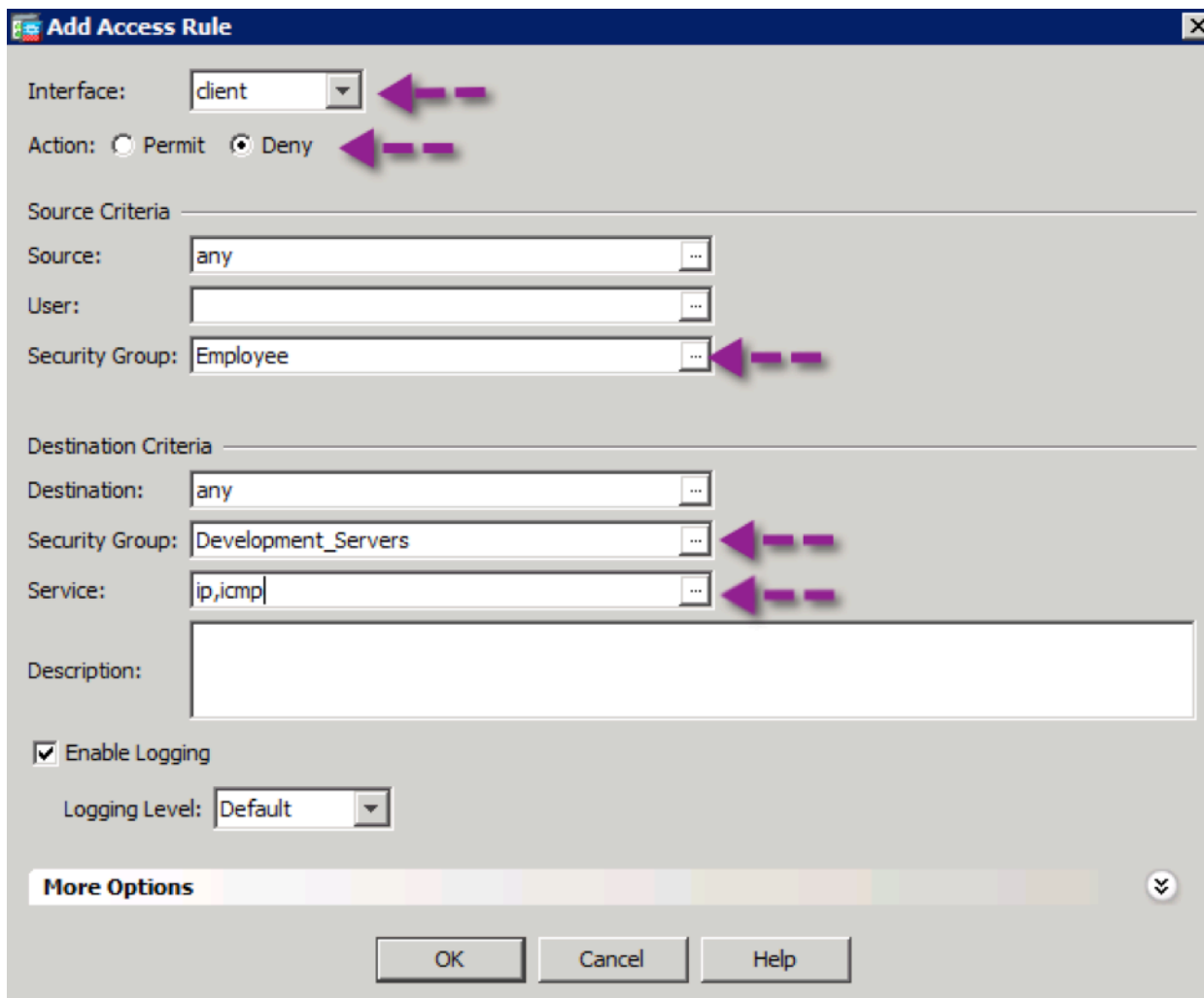
Enable Logging

Logging Level: Default

More Options

OK Cancel Help

- Step 3** Click **OK**
- Step 4** Since policies are applied from top down, move the rule just created above the existing “any, any” policy



**Step 5** Click **OK**

**Step 6** Add a rule to allow the employees to access the production server. Click **OK**

**Step 7** Click **Apply**

## Nexus Devices

**Step 1** Configure role-based enforcement globally and enable role-based counters so we can verify policy enforcement

```
n1kv(config)# cts enable
n1kv(config)# cts role-based counters enable
```

**Step 2** Verify the policy is accurate on the Nexus 1000v

```
n1kv(config)# show cts role-based policy

sgt:4
dgt:5   rbacl:Deny IP
deny ip
```

```
sgt:5
dgt:4  rbacl:Deny IP
deny ip

sgt:any
dgt:any rbacl:Permit IP
permit ip
```

## Conclusion

In this guide we have seen a tested best practice approach to enabling Cisco TrustSec. We have reviewed the three foundational pillars of Cisco TrustSec technology: classification, propagation, and enforcement. Classification is the ability to accept the tag for a particular network authentication session. Propagation, or transport, is the ability to send that assigned tag to upstream neighbors through either native tagging or SXP. Enforcement may be on switches using SGACLs or on an SGFW.

Additionally, we have covered the basic configurations of all of these features across the many supported platforms.

## For More Information

Reference <http://www.cisco.com/go/trustsec>