Cisco TrustSec Quick Start Configuration Guide
# Table of Contents

Introduction .........................................................................................................................5
Using This Guide..................................................................................................................5

**Baseline ISE Configuration for TrustSec** .......................................................................7
  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

**TrustSec Policy Acquisition** .......................................................................................14
  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

**Classification** ...............................................................................................................21
  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
Enabling Enforcement on the ASA

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
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

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

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
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.

![Creating TrustSec Device SGT](image)

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:
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

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.

![Image of a network device configuration screen]

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.
**Advanced TrustSec Settings**

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Device Authentication Settings</strong></td>
<td></td>
</tr>
<tr>
<td>Use Device ID for TrustSec</td>
<td>✅</td>
</tr>
<tr>
<td>Device Id</td>
<td>3k-access</td>
</tr>
<tr>
<td>Password</td>
<td>ISEisC00L</td>
</tr>
<tr>
<td></td>
<td>This is automatically populated from the Device Name if Use Device ID for SGA identification is checked. This ID must match the &quot;cts device-id&quot; command that is later configured on the switch.</td>
</tr>
<tr>
<td></td>
<td>TrustSec authentication password. This must match the password that is associated with the &quot;cts device-id&quot; command.</td>
</tr>
<tr>
<td><strong>TrustSec Notifications and Updates</strong></td>
<td></td>
</tr>
<tr>
<td>Download environment data every</td>
<td>1 Days</td>
</tr>
<tr>
<td>Download peer authorization policy every</td>
<td>Specifies the expiry time for peer authorization policy. ISE returns this information to the device in response to a peer policy request. The default is 1 day</td>
</tr>
<tr>
<td>Reauthentication every</td>
<td>1 Days</td>
</tr>
<tr>
<td>Download SGACL lists every</td>
<td>1 Days</td>
</tr>
<tr>
<td>Other TrustSec devices to trust the device</td>
<td>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.</td>
</tr>
<tr>
<td>Send configuration changes to device</td>
<td>✅ Using CoA CLI (SSH)</td>
</tr>
</tbody>
</table>

*Note: Items that are bolded are the fields that need modification. The other fields are left at default values.*
Cisco ASA5500 Adaptive Security Appliances

**Step 1** Navigate to Administration-Netraork 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 a valid and non-empty string in order to save this object.

### Advanced TrustSec Settings

<table>
<thead>
<tr>
<th>Device Authentication Settings</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Use Device ID for TrustSec</td>
<td>✓</td>
</tr>
<tr>
<td>Device Id</td>
<td>T-ASA</td>
</tr>
<tr>
<td>Password</td>
<td>&lt;anything&gt;</td>
</tr>
</tbody>
</table>

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.

<table>
<thead>
<tr>
<th>Identity</th>
<th>T-ASA</th>
</tr>
</thead>
<tbody>
<tr>
<td>Encryption Key</td>
<td>ISEisC00L</td>
</tr>
<tr>
<td>PAC Time to Live</td>
<td>1 Years</td>
</tr>
</tbody>
</table>

**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 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, CSCul57034.
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.

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
cuts authorization list cts-list
radius server ISE
address ipv4 <ip address of ISE policy servies node> auth-port 1812 acct-port 1813
pac key <secret>
exit
aaa group server radius 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: 5CA2F60834DE482B716028EA4EFA8B
  PAC-Info:
  PAC-type = Cisco Trustsec
    AID: 5CA2F60834DE482B716028EA4EFA8B
    I-ID: 3k-access
  A-ID-Info: Identity Services Engine
  Credential Lifetime: 15:53:10 UTC Oct 29 2014
  PAC-Opaque:
  000200B800030001000400105CA42F60834DE482B716028EA4EFA8B0006009C00030100DCC3AF447CA810C142E417A2F
  B6F720000001355D1ABB400093A808ACFFEF1042BA878EB3585CEE1B108AE45D6F5896B493430DE24C25686AE418C5EEFD
  E4460EC9D3FB09A0E8AB261C98D00E8C9F25567D377636A88CC9125A3FDB458F9A4FBEAF430D61584C1B146B92091342
  2B30EA50184D6C72923A364B1735F60857591440879815021F9404868FE2DA13C1807FCB1464C2C57
    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 5CA2F60834DE482B716028EA4EFA8B
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

```bash
svs switch edition advanced
feature cts
feature dot1x
crs 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.

```bash
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.

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

Verifying Policy Acquisition

Step 4  Verify PAC file is provisioned

```bash
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 : 000200b000030010004001a6ee87f55c7131943d615cc1d47025bf00060094000301005a705134937fede63969e66676ba2cfd000013524d84a370093a800e8cf09b38cc61b08e2e4e1e9fb4a9cbb3f28907accd3785a356c0f1f3d62df8d673590614ce4adfb083d5eaaa906eeef3dac86e2f6de0d7e8c58a6a98e5b934e6f814e0fbd0d7213d7c7e3c23b4efbf7b34d0893f2588b6768d6f545b7a9b11ce11701336bb269650cfa132df639240c60b6a
```

Step 5  Verify the CTS environment data has been downloaded
**TRUSTSEC HOW-TO GUIDES**

```
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
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 mistyped. Below is a sample Live Log entry of the failure.

<table>
<thead>
<tr>
<th>Time</th>
<th>Status</th>
<th>Details</th>
<th>Identity</th>
<th>Event</th>
<th>Authentication Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>2014-07-23 11:54:31.529</td>
<td>✗</td>
<td>N1KV</td>
<td></td>
<td>Authentication failed</td>
<td>EAP-FAST (EAP-MSCHAPv2)</td>
</tr>
</tbody>
</table>

**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.
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:

Cisco TrustSec for ISRG2:

Nexus 7000:

Nexus 5000:


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
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:


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.
TRUSTSEC HOW-TO GUIDES

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
cps 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
cps 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+:  

For pre-ISE 1.3:  

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...  
NSK-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”

<table>
<thead>
<tr>
<th>IP ADDRESS</th>
<th>SGT</th>
<th>VRF/VLAN</th>
<th>SGT CONFIGURATION</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.1.160.20</td>
<td>100</td>
<td>vrf:1</td>
<td>CLI Configured</td>
</tr>
<tr>
<td>10.1.160.21</td>
<td>101</td>
<td>vrf:1</td>
<td>CLI Configured</td>
</tr>
</tbody>
</table>

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
Port to SGT Mapping

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

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

For Nexus Devices

IP 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>
```

VLAN to SGT Mapping

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

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.

<table>
<thead>
<tr>
<th></th>
<th>Time</th>
<th></th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>14:10:42.278504</td>
<td>INLINE-TAG 2</td>
<td>10.1.128.2 &gt; 10.1.128.1: icmp: echo request</td>
</tr>
<tr>
<td>2</td>
<td>14:10:42.279007</td>
<td>INLINE-TAG 0</td>
<td>10.1.128.1 &gt; 10.1.128.2: icmp: echo reply</td>
</tr>
<tr>
<td>3</td>
<td>14:10:42.282318</td>
<td>INLINE-TAG 2</td>
<td>10.1.128.2 &gt; 10.1.128.1: icmp: echo request</td>
</tr>
<tr>
<td>4</td>
<td>14:10:42.282562</td>
<td>INLINE-TAG 0</td>
<td>10.1.128.1 &gt; 10.1.128.2: icmp: echo reply</td>
</tr>
</tbody>
</table>

**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**

```plaintext
cts sxp enable
cts sxp default password <password for SXP>
ccts 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.
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)

```bash
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)

```bash
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

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

Catalyst and Other Nexus Platforms

```bash
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

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
```
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 acl.

step 5  click save
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
tcs manual
tct role-based enforcement

port-profile type vethernet production
tcs manual
tct 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
```
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.

**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
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