Cisco TrustSec Feature Guide

Cisco TrustSec Feature Guide

Contents

Introduction 5
About Cisco TrustSec 5
Audience 5
Cisco TrustSec Overview 6
Cisco TrustSec Device Enrollment 7
PAC Overview 8
PAC Overview 8
Security Access Group Overview 9
Security Group Policy Enforcement 9
Security Group Tag Overview 10
License 11
Configuring 12
Configuring Cisco Devices to Integrate with Cisco TrustSec 12
Registering Cisco Devices with Cisco ISE 13
Configuring Cisco TrustSec Credentials on the Device 14
Configuring RADIUS Attributes on ISE 15
Configuring RADIUS Server on the Device 15
Configuring Environment Data on ISE 16
Creating a Security Group on Cisco ISE 17
Creating an SGACL Mapping on ISE 18
Downloading the SGACL Policy on to the Device 18
Troubleshooting 20
Technical Support Information 24

Introduction

About Cisco TrustSec

Cisco TrustSec is a system that provides security for Cisco TrustSec-enabled network devices at each routing hop. In this system, each network device works to authenticate and authorize its neighbor devices and applies some level of security (group tagging, role-based access control lists (ACLs), encryption, and so on) to traffic between the devices.

- Cisco TrustSec is embedded technology in your existing Cisco switches and routers. Cisco TrustSec can simplify provisioning and management of network access, make security operations more efficient, and help to enforce segmentation policy consistently, anywhere in the network. The centralized policy management platform for TrustSec is the Cisco Identity Services Engine (ISE).
- Cisco TrustSec uses secure RADIUS to prescribe a process of authentication, authorization, session association, encryption, and traffic filtering. Secure RADIUS uses automatic Protected Access Credential (PAC) provisioning as a low overhead method to send PAC metadata and control information to clients. PAC provisioning is used with Extensible Authentication Protocol-Flexible Authentication through Secure Tunneling (EAP-FAST) to establish a Transport Layer Security (TLS) tunnel in which client credentials are verified.
- This document describes Cisco TrustSec and how to configure it on Cisco devices supported in Cisco IOS XE Release Denali 16.2.1.

Audience

This user guide is for networking professionals and experienced network administrators who are responsible for configuring Cisco TrustSec feature on Cisco Devices.

Cisco TrustSec Feature Guide

PLAN

Cisco TrustSec Overview

With enterprises transitioning to borderless networks, the technology that connects people and organizations, and the security requirements for protecting data and networks have evolved significantly. End points are increasingly nomadic and users often employ a variety of end points (for example, laptops, smart phones, tablets and so on), which means that a combination of user attributes plus end-point attributes provide the key characteristics that enforcement devices such as switches and routers with firewalls can reliably use to make access control decisions.

As a result, the availability and propagation of end point attributes or client identity attributes have become important requirements to enable security across the customer networks—at the access, distribution, and core layers of the network, and in the data center.

Cisco TrustSec provides access control that builds upon an existing identity-aware infrastructure to ensure data confidentiality between network devices and integrate security access services on one platform. With Cisco TrustSec, enforcement devices use a combination of user attributes and end-point attributes to make role-based and identity-based access control decisions. The availability and propagation of this information enables security across networks at the access, distribution, and core layers of the network.

The Cisco TrustSec security architecture builds secure networks by establishing a domain of trusted devices. Communication on the links between devices in the Cisco TrustSec cloud is secured with a combination of encryption, message integrity checks, and data-path replay protection mechanism. Cisco TrustSec also uses the device and user identity information acquired during authentication to classify the packets as they enter a network.

This packet classification is maintained by tagging packets on the ingress interface to the Cisco TrustSec network so that they can be correctly identified for the purpose of applying security and other policy criteria along the data path. The Tag, also called Security Group Tag (SGT), allows the network to enforce the access control policy by enabling the endpoint device to act upon the SGT value to filter the traffic.

For more information about Cisco TrustSec, see *http://www.cisco.com/go/trustsec*.

Cisco TrustSec Device Enrollment

- Any device that participates in the Cisco TrustSec network requires it to be authenticated and trusted. New devices that connect to the network use an enrollment process to obtain Cisco TrustSec authentication credentials and receive general information about the TrustSec environment to facilitate the authentication process. Device enrollment can happen either directly with an Authentication Server (AS) provided the device has Layer 3 connectivity to the AS or through a peer Authenticator (AT) device, such as a switch or router that facilitates enrollment with an AS.
- Access switches or routers are the authentication points in typical branch access scenarios and have direct connectivity to the AS. They authenticate endpoints through EAP-FAST for dynamic PAC provisioning or RADIUS and EAP exchange. When endpoints are successfully authenticated, they receive user-specific AAA attributes that include the SGT, which in turn is relayed to a switch using SGT Exchange Protocol (SXP). The switch initiates EAP-FAST Phase 0 exchange with the available AS and obtains a PAC. This is accomplished by a local PAC-provisioning driver, which acts as a pass-through authenticator to the supplicant EAP-FAST engine running on the switch.

Secure RADIUS

The RADIUS protocol requires a secret to be shared between a client and a server. Shared secrets are used to verify that RADIUS messages are sent by a RADIUS-enabled device that is configured with the same shared secret. Shared secrets also verify that the RADIUS message has not been modified in transit (message integrity). The message integrity is checked by including the Message Authenticator attribute in the RADIUS messages. This attribute is a Hash-based Message Authentication Code-Message Digest 5 (HMAC-MD5) of the entire radius message using the shared secret as the key. The shared secret is also used to encrypt some RADIUS attributes, such as User-Password and Tunnel-Password.

EAP-FAST

EAP-FAST is a publicly accessible IEEE 802.1X extensible authentication protocol type that is used to support customers who cannot enforce a strong password policy. EAP-FAST is used for the following reasons:

- Digital certificates are not required.
- A variety of database types for usernames and passwords are supported.
- Password expiration and change are supported.
- EAP-FAST is flexible, easy to deploy and manage.

Note: Lightweight Directory Access Protocol (LDAP) users cannot be automatically PAC provisioned and must be manually provisioned.

EAP-FAST comprises of three basic phases, but only Phase 0 is supported. Phase 0 initially distributes the PAC to the client device.

Phase 0 or auto-provisioning (also called in-band provisioning) component of EAP-FAST permits the secure distribution of the user PAC to each device. Phase 0 in EAP-FAST permits a PAC to be distributed to the device during an encrypted session after the device credentials are authenticated.

After a successful PAC distribution, the server issues an authentication failure to the access point and the device is disassociated from the network. Then the device reinitiates an EAP-FAST authentication with the network using the newly provisioned PAC and device credentials.

Figure 1 EAP-FAST

PAC Overview

- The PAC is a unique shared credential used to mutually authenticate the client and server. It is associated with a specific client username and a server authority identifier (A-ID). A PAC removes the need for Public Key Infrastructure (PKI) and digital certificates.
- Creating a PAC consists of the following steps:

1. Server A-ID maintains a local key (master key) that is only known by the server.
2. When a client, which is referred to in this context as an initiator identity (I-ID), requests a PAC from the server, the server generates a randomly unique PAC key and PAC-Opaque field for this client.
3. The PAC-Opaque field contains the randomly generated PAC key along with other information such as an I-ID and key lifetime.
4. PAC Key, I-ID, and Lifetime in the PAC-Opaque field are encrypted with the master key.

PAC Overview

- The PAC is a unique shared credential used to mutually authenticate the client and server. It is associated with a specific client username and a server authority identifier (A-ID). A PAC removes the need for Public Key Infrastructure (PKI) and digital certificates.
- Creating a PAC consists of the following steps:

5. Server A-ID maintains a local key (master key) that is only known by the server.
6. When a client, which is referred to in this context as an initiator identity (I-ID), requests a PAC from the server, the server generates a

randomly unique PAC key and PAC-Opaque field for this client.

7. The PAC-Opaque field contains the randomly generated PAC key along with other information such as an I-ID and key lifetime.
8. PAC Key, I-ID, and Lifetime in the PAC-Opaque field are encrypted with the master key.
9. A PAC-Info field that contains the A-ID is created.
10. The PAC is distributed or imported to the client automatically.

Note: The server does not maintain the PAC or the PAC key, enabling the EAP-FAST server to be stateless.

The figure below describes the PAC's construction. A PAC consists of the PAC-Opaque, PAC Key, and PAC-Info fields. The PAC-Info field contains the A-ID.

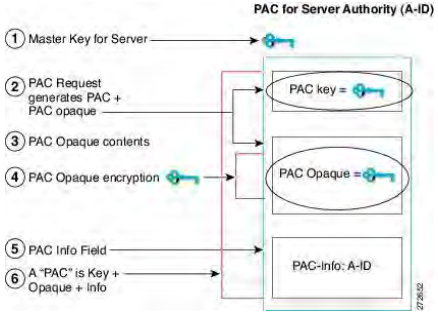

Figure 2 PAC for Server Authority

Security Access Group Overview

Security Group Access (SGA) architecture provides group based access-control using Security Group Tags (SGTs). SGTs are used to tag user traffic with role and identity information, which is carried throughout the network and used by devices in the network for policy control.

SGTs allow enterprises to build simple role-based access policies that are topology-independent and provide operational flexibility compared to downloadable access control lists (ACLs). Additionally, specific resources that are being accessed can be grouped into security groups to simplify operations.

SGTs are unique 16-bit tags assigned to a unique role, which represents privilege of the source user, device or entity. They are tagged at the ingress of a TrustSec domain and filtered at the egress of the TrustSec domain via Security Group access control lists (SGACLs). Policies (Policy ACLs) are distributed from a central policy server (Cisco Integrated Services Engine) or can be configured locally on the TrustSec device.

Security Group Policy Enforcement

Security policy enforcement is based on security group name. An end-point device attempts to access a resource in the data center. Compared to traditional IP-based policies configured on firewalls, identity-based policies are configured based on user and device identities. For example, mktg-contractor is allowed to access mktg-servers; mktg-corp-users are allowed to access mktg-server and corp-servers.

The benefits of this type of deployment include:

- User group and resource are defined and enforced using single object (SGT) simplified policy management.
- User identity and resource identity are retained throughout the Cisco TrustSec-capable switch infrastructure.

This figure shows a deployment for security group name-based policy enforcement.

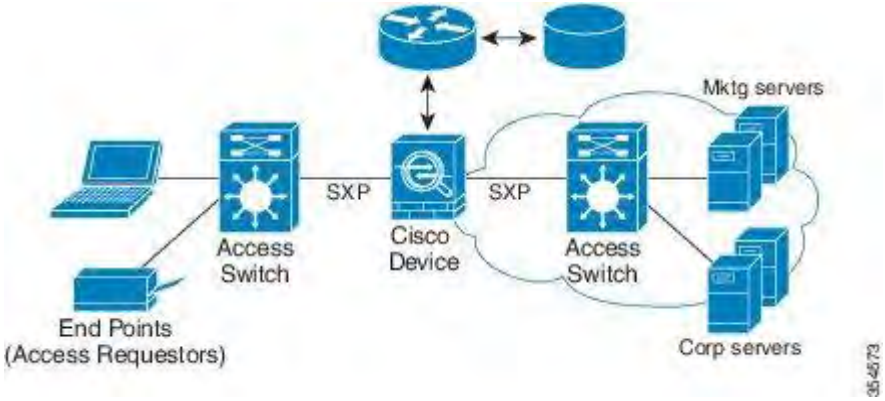

Figure 3 Security Group Name-Based Policy Enforcement

Implementing Cisco TrustSec allows you to configure security policies that support server segmentation and includes the following features:

- A pool of servers can be assigned an SGT for simplified policy management.
- The Cisco device can use the IP-SGT mapping for policy enforcement across the Cisco TrustSec domain.
- Deployment simplification is possible because 802.1x authorization for servers is mandatory.

Security Group Tag Overview

Security group access transforms a topology-aware network into a role-based network, which enables end-to-end policies enforced on the basis of role-based access control list (RBACL). Device and user credentials acquired during authentication are used to classify packets by security groups. Every packet entering the Cisco TrustSec cloud is tagged with a security group tag (SGT). The tagging helps trusted intermediaries identify the source of the packet and enforce security policies along the data path. An SGT can indicate a privilege level across the domain when the SGT is used to define a security group ACL.

An SGT is assigned to a device through IEEE 802.1X authentication, web authentication, or MAC authentication bypass (MAB), which occurs with a RADIUS vendor-specific attribute. An SGT can be assigned statically to a particular IP address or to a switch interface. An SGT is dynamically routed to a switch or access point after successful authentication.

The Source-Group Tag (SGT) eXchange Protocol (SXP) is a protocol developed for Cisco TrustSec to propagate the IP-to-SGT mapping database across network devices that do not have SGT-capable hardware to support SGTs and security group ACLs. SXP passes IP-SGT mapping from authentication points (such as legacy access layer switches) to upstream devices in the network.

The SXP connections are point-to-point and use TCP as the underlying transport protocol. SXP uses the well-known TCP port number 64999 to initiate a connection. Additionally, an SXP connection is uniquely identified by the source and destination IP addresses. Each SXP connection has one peer designated as SXP speaker and the other peer as SXP listener.

License

Cisco TrustSec SGT/SGACL requires a minimum of IP Base license. Evaluation license can be obtained from *http://www.cisco.com/go/license*. After obtaining the license, set the license level appropriately in the switch as showed below:

```
Device(config)# license boot level {ipbase | ipservices | lanbase}
```

Configuring

Configuring Cisco Devices to Integrate with Cisco TrustSec

- Register Cisco devices with Cisco ISE.
- Create a security group on the ISE.
- Configure the RADIUS server on the device.
- Configuring dynamic ACL on the ISE.
- Enable and set the default values for SXP.
- Add SXP connection peers for the Cisco TrustSec architecture.
- Configure a security policy.

Registering Cisco Devices with Cisco ISE

As part of the policy acquisition phase, all the TrustSec-capable devices receive an SGT called a Device SGT. This represents the security group to which the device itself belongs and is exchanged with neighboring trusted devices.

Note: It is recommended to use a single SGT value for all the Cisco TrustSec-capable devices. A single SGT value makes it convenient to write policies and to troubleshoot.

Login to the Cisco Integrated Services Engine (ISE) GUI and follow these steps:

Figure 4 ISE Login Page

1. Navigate to Administration >> Network Resources >> Network Devices
2. In the Network Devices page, Click Add.
3. Provide a name for the Cisco device. If required add a description about the device.

4. Enter the IP address of the device. The IP subnet mask must be 32-bit.

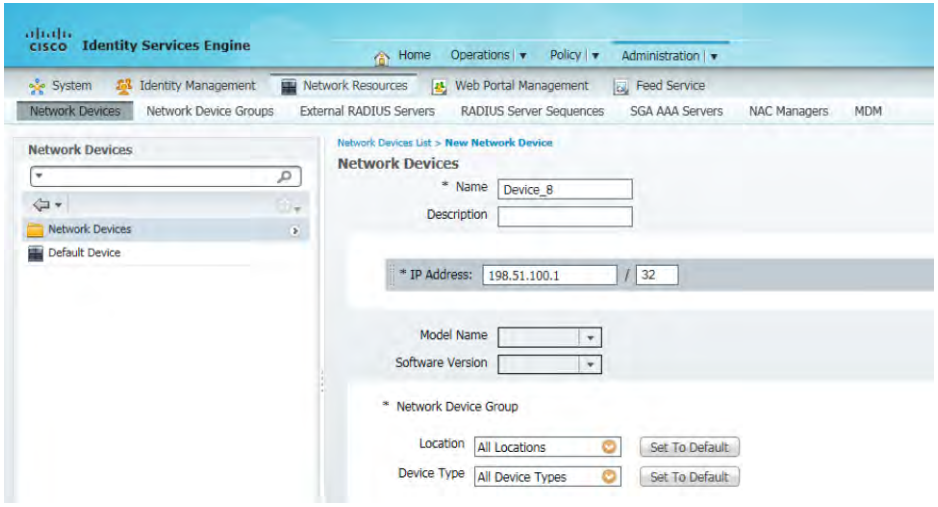

Figure 5 ISE Network Devices Configuration Page

Configuring Cisco TrustSec Credentials on the Device

	Command	Purpose
Step 1	`Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	`Switch# cts credentials id cts-id password cts-password`	Specifies the TrustSec ID and password of the network device. • The *cts-id* argument specifies the Cisco TrustSec device ID configured in ISE. The device uses this ID when authenticating with other Cisco TrustSec devices using EAP-FAST. It has a maximum length of 32 characters and is case sensitive. • The **cts-password** argument specifies the password configured for the device in ISE. The device uses this password when authenticating with other Cisco TrustSec devices using EAP-FAST.
Step 3	`Switch# show cts credentials`	Displays the device information used for Cisco TrustSec authentication.

The following example shows the Cisco TrustSec credentials configuration:

```
Device# cts credentials id Device_8 password password1

Device# show cts credentials

CTS password is defined in keystore, device-id = device_8
```

This task ensures that the connectivity between device and ISE is established.

Configuring RADIUS Attributes on ISE

1. Select the Authentication Settings check box.
2. In the Authentication Settings page, enter a shared secret.

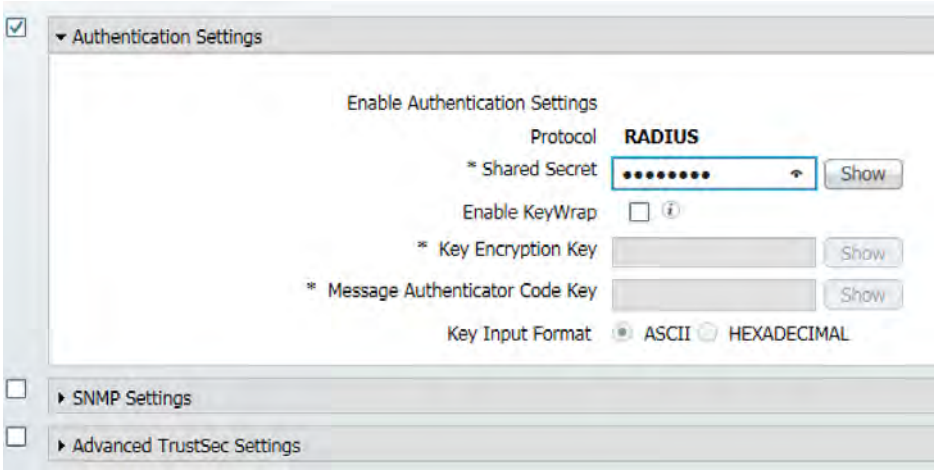

Figure 6 ISE Authentication Settings Page

Configuring RADIUS Server on the Device

	Command	Purpose
Step 1	`Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	`Switch# configure terminal`	Enters global configuration mode.
Step 3	`Switch(cfg-call-home)# radius server server-name`	Specifies the name for the RADIUS server configuration for Protected Access Credential (PAC) provisioning and enters RADIUS server configuration mode. • The *server-name* argument refers to the ISE server name.

Step 4	`Switch(config-radius-server)#` **address** {**ipv4** | **ipv6**} *ip-address* **auth-port** *port-number* **acct-port** *port-number*	Configures an IPv4 or IPv6 address for the RADIUS server accounting and authentication parameters. • *ip-address*—Specifies the IP address of the ISE server. • **auth-port**—Specifies the UDP port for the RADIUS authentication server. • **acct-port**—Specifies the UDP port for the RADIUS accounting server. • ISE and the device communicate with each other using the authentication and accounting ports.
Step 6	`Switch(config-radius-server)#` **pac key** {**0** | **7** | *shared-key*}	Specifies the Protected Access Credential (PAC) encryption key. • The PAC key or the shared-key argument is the RADIUS shared secret configured on ISE.
Step 7	`Switch(config-radius-server)#` **end**	Exits RADIUS server configuration mode and returns to privileged EXEC mode.

The following is example shows the RADIUS server configuration on the device:

```
Device(config)# radius-server ISE-5

Device(config-radius-server)# address ipv4 10.51.100.1 auth-port
1813 acct-port 1812

Device(config-radius-server)# pac key password 1

Device(config-radius-server)# end
```

The PAC information is downloaded to the device after this configuration task is complete. Use the **show cts pacs** command to view the downloaded PAC information.

Configuring Environment Data on ISE

1. Select the Advanced TrustSec Settings checkbox.
2. In the Device Authentication Settings section, select the Use Device ID for SGA Identification box.
3. Enter the shared secret in the Password dialog box.
4. In the SGA Notifications and Updates section, add the download timer settings.
5. Select the Other SGA devices to trust this device checkbox.
6. Click Submit.

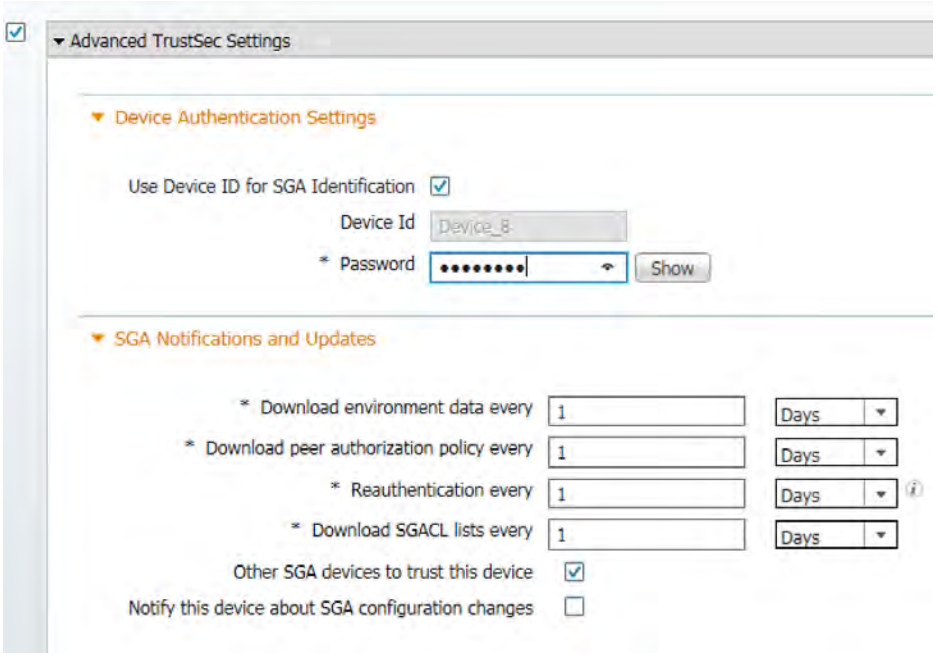

Figure 7 Advanced Cisco TrustSec Settings Page

Creating a Security Group on Cisco ISE

1. Navigate to Policy >> Policy Elements >> Results >> Security Group Access >> Security Group ACLs
2. Click Add to create a new security group ACL.
3. Use the **permit**, and **deny** commands to create SGACLs. Create as many ACLs as per your requirements and click Save.

Note: Only IPv4 is supported.

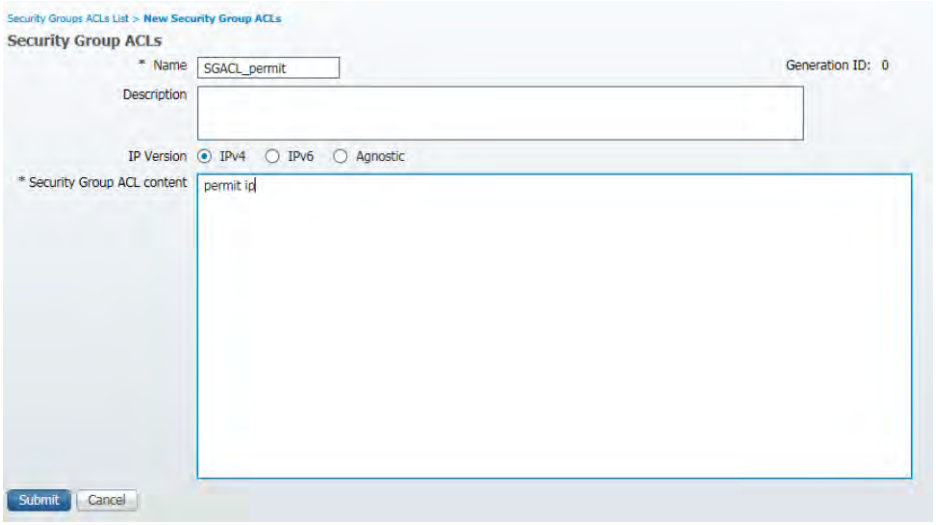

Figure 8 Security Group ACLs Page

Creating an SGACL Mapping on ISE

1. Navigate to Policy >> Security Group Access >> Egress Policy and select Matrix. The Egress Policy Matrix view opens up.
2. Click Add.
3. Select a source security group from the drop-down menu.
4. Select a destination security group.
5. In the Assigned Security Group ACLs drop-down menu, select the configured SGACL. Here it will be SGACL_permit.
6. In the Egress Policy page, select Destination Tree. The Destination Tree view opens up. Select the expand button next to the destination security group you selected in Step 4. All SGACLs configured with this destination group is displayed.

Downloading the SGACL Policy on to the Device

	Command	Purpose
Step 1	`Switch> enable`	Enables privileged EXEC mode. • Enter your password if prompted.
Step 2	`Switch# configure terminal`	Enters global configuration mode.
Step 3	`Switch(config)# cts role-based sgt-map` *ip-address* `sgt` *sgt-number*	Assigns Security Group Tag (SGT) to an IP host or network address. • The *sgt-number* argument uses the destination security group number created in the ISE.
Step 4	`Switch(config)# exit`	Exits global configuration mode and returns to privileged EXEC mode.
Step 5	`Switch# show cts role-based permissions`	Lists the role-based permissions of the configured SGT maps.

The following is sample output from the **show cts role-based permissions** command:

```
IPv4 Role-based permissions default (monitored):

default_sgacl-01

Deny IP-00

IPv4 Role-based permissions from group 10:SGT_10 to group
15:SGT_15:

SGACL_3-01

IPv4 Role-based permissions from group 14:SGT_14 to group
15:SGT_15:

multple_ace-14

RBACL Monitor All for Dynamic Policies : FALSE

RBACL Monitor All for Configured Policies : FALSE
```

Troubleshooting

Verify the device has connectivity to AAA server and PAC is downloaded successfully:

```
Device# show cts pacs

AID: A3B6D4D8353F102346786CF220FF151C

PAC-Info:

PAC-type = Cisco Trustsec

AID: A3B6D4D8353F102346786CF220FF151C

I-ID: CTS_ED_21

A-ID-Info: Identity Services Engine

Credential Lifetime: 17:22:32 IST Mon Mar 14 2016

PAC-Opaque:
000200B800030001000400010A3B6D4D8353F102346786CF220FF151C0006009C
00030100E044B2650D8351FD06F23623C470511E0000001356DEA96C00093A80
538898D40F633C368B053200D4C9D2422A7FEB4837EA9DBB89D1E51DA4E7B184
E66D3D5F2839C11E5FB386936BB85250C61CA0116FDD9A184C6E96593EEAF5C3
9BE08140AFBB194EE701A0056600CFF5B12C02DD7ECEAA3CCC8170263669C483
BD208052A46C31E39199830F794676842ADEECBBA30FC4A5A0DEDA93

Refresh timer is set for 01:00:05
```

Use the **show cts interface** summary command to verify whether the device has authenticated successfully and the Cisco TrustSec interface state is in OPEN state.

```
Device# show cts interface summary


Global Dot1x feature is Disabled

CTS Layer2 Interfaces

---------------------

Interface  Mode    IFC-state dot1x-role peer-id    IFC-cache
Critical-Authentication

-------------------------------------------------------------------
------------

Gi1/0/1    MANUAL  OPEN      unknown    unknown    invalid
Invalid


CTS Layer3 Interfaces

---------------------

Interface   IPv4 encap       IPv6 encap       IPv4 policy
IPv6 policy

-------------------------------------------------------------------
----------

Summary Not implemented yet.
```

Use the **show cts environment-data** command to verify the device SGT value and whether the Cisco TrustSec environment variables are updated properly.

```
Device# show cts environment-data


CTS Environment Data

====================

Current state = COMPLETE

Last status = Successful

Local Device SGT:

  SGT tag = 0-02:Unknown
```

```
Server List Info:
Installed list: CTSServerList1-000D, 1 server(s):
  *Server: 10.78.105.47, port 1812, A-ID
A3B6D4D8353F102346786CF220FF151C
  Status = ALIVE
  auto-test = TRUE, keywrap-enable = FALSE, idle-time = 60 mins,
deadtime = 20 secs
Multicast Group SGT Table:
Security Group Name Table:
0001-45 :
  0-00:Unknown
  2-5d:SGT_2
  3-00:SGT_3
  4-00:SGT_4
  5-00:SGT_5
  6-00:SGT_6
  7-00:SGT_7
  8-00:SGT_8
  9-00:SGT_9
  10-16:SGT_10
  11-00:SGT_11
  12-00:SGT_12
  13-00:SGT_13
  14-00:SGT_14
  15-00:SGT_15
  16-00:SGT_16
  17-00:SGT_17
  18-00:SGT_18
  19-00:SGT_19
  20-00:SGT_20
  21-00:SGT_21
  22-00:SGT_22
  23-00:SGT_23
  24-00:SGT_24
  25-00:SGT_25
  26-00:SGT_26
  27-00:SGT_27
  28-00:SGT_28
  29-00:SGT_29
  30-00:SGT_30
Environment Data Lifetime = 3600 secs
Last update time = 14:02:31 IST Tue Mar 22 2016
Env-data expires in 0:00:52:39 (dd:hr:mm:sec)
Env-data refreshes in 0:00:52:39 (dd:hr:mm:sec)
Cache data applied = NONE
State Machine is running
```

Use the **show cts role-based permissions** command to verify the assigned role-based permissions.

```
Device# show cts role-based permissions

IPv4 Role-based permissions default:
       default_sgacl-01
       Permit IP-00
IPv4 Role-based permissions from group 10:SGT_10 to group
15:SGT_15:
       SGACL_3-01
IPv4 Role-based permissions from group 14:SGT_14 to group
15:SGT_15:
       multple_ace-14
RBACL Monitor All for Dynamic Policies : FALSE
RBACL Monitor All for Configured Policies : FALSE
```

Use the **show cts rbacl** command to verify the defined RBACLs.

```
CTS_ED_21# show cts rbacl

CTS RBACL Policy
================
RBACL IP Version Supported: IPv4 & IPv6
  name    =multple_ace-14
  IP protocol version = IPV4
  refcnt = 1
  flag = 0x40000000
  stale = FALSE
  RBACL ACEs:
      deny icmp
      permit tcp

name    =default_sgacl-01
IP protocol version = IPV4
refcnt = 1
flag = 0x40000000
stale = FALSE
RBACL ACEs:
    permit ip

name    =Permit IP-00
IP protocol version = IPV4
refcnt = 1
flag = 0x40000000
stale = FALSE
RBACL ACEs:
    permit ip

name    =SGACL_3-01
IP protocol version = IPV4
refcnt = 1
flag = 0x40000000
```

```
  stale = FALSE
  RBACL ACEs:
      permit ip
```

Use the **show cts role-based sgt-map all** command to display all the configured SGT maps.

```
Device# show cts role-based sgt-map all

Active IPv4-SGT Bindings Information

IP Address              SGT     Source
========================================
12.1.1.15               15      CLI

IP-SGT Active Bindings Summary
========================================
Total number of CLI      bindings = 1
Total number of active   bindings = 1
```

Technical Support Information

For technical support, please contact Cisco Smart Services Bureau (SSB) via:

Email: ask-smart-services@cisco.com<mailto:ask-smart-services@cisco.com>

Telephone:

US and Canada: +1-877-330-9746

Europe: Austria 0800 006 206

Belgium 0800 49913

France 0805 119 745

Germany 0800 589 1725

Italy 800 085 681

Netherlands 0800 0201 276

Spain 800 600472

Switzerland 0800 840011

UK 0800 2795112

From the rest of the world, choose the appropriate phone number from http://www.cisco.com/en/US/support/tsd_cisco_worldwide_contacts.html

TOMORROW starts here.