Cisco TrustSec

Information about Cisco TrustSec

Cisco TrustSec provides security improvements to Cisco network devices based on the capability to strongly identify users, hosts, and network devices within a network. TrustSec provides topology-independent and scalable access controls by uniquely classifying data traffic for a particular role. TrustSec ensures data confidentiality and integrity by establishing trust among authenticated peers and encrypting links with those peers.

The key component of Cisco TrustSec is the Cisco Identity Services Engine (ISE). Cisco ISE can provision switches with TrustSec Identities and Security Group ACLs (SGACLs), though these may be configured manually on the switch.

Note You should manually clear the CTS environment data using the **clear cts environment-data** command before changing CTS server to a new one. This ensures that you get the updated data while running **show cts environment-data** command.

Cisco TrustSec Features

The table below lists the TrustSec features to be eventually implemented on TrustSec-enabled Cisco switches. Successive general availability releases of TrustSec will expand the number of switches supported and the number of TrustSec features supported per switch.

Cisco TrustSec Feature	Description
802.1AE Tagging (MACsec)	Protocol for IEEE 802.1AE-based wire-rate hop-to-hop Layer 2 encryption. Between MACsec-capable devices, packets are encrypted on egress from the transmitting device, decrypted on ingress to the receiving device, and in the clear within the devices. This feature is only available between TrustSec hardware-capable devices.
Endpoint Admission Control (EAC)	EAC is an authentication process for an endpoint user or a device connecting to the TrustSec domain. Usually EAC takes place at the access level switch. Successful authentication and authorization in the EAC process results in Security Group Tag assignment for the user or device. Currently EAC can be 802.1X, MAC Authentication Bypass (MAB), and Web Authentication Proxy (WebAuth).
Network Device Admission Control (NDAC)	NDAC is an authentication process where each network device in the TrustSec domain can verify the credentials and trustworthiness of its peer device. NDAC utilizes an authentication framework based on IEEE 802.1X port-based authentication and uses EAP-FAST as its EAP method. Successful authentication and authorization in NDAC process results in Security Association Protocol negotiation for IEEE 802.1AE encryption.
Security Group Access Control List (SGACL)	A Security Group Access Control List (SGACL) associates a Security Group Tag with a policy. The policy is enforced upon SGT-tagged traffic egressing the TrustSec domain.
Security Association Protocol (SAP)	After NDAC authentication, the Security Association Protocol (SAP) automatically negotiates keys and the cipher suite for subsequent MACSec link encryption between TrustSec peers. SAP is defined in IEEE 802.11i.
Security Group Tag (SGT)	An SGT is a 16-bit single label indicating the security classification of a source in the TrustSec domain. It is appended to an Ethernet frame or an IP packet.

Cisco TrustSec Feature	Description
SGT Exchange Protocol (SXP)	Security Group Tag Exchange Protocol (SXP). With SXP, devices that are not TrustSec-hardware-capable can receive SGT attributes for authenticated users and devices from the Cisco Identity Services Engine (ISE) or the Cisco Secure Access Control System (ACS). The devices can then forward a sourceIP-to-SGT binding to a TrustSec-hardware-capable device will tag the source traffic for SGACL enforcement.

When both ends of a link support 802.1AE MACsec, SAP negotiation occurs. An EAPOL-key exchange occurs between the supplicant and the authenticator to negotiate a cipher suite, exchange security parameters, and manage keys. Successful completion of these tasks results in the establishment of a security association (SA).

Depending on your software version and licensing and link hardware support, SAP negotiation can use one of these modes of operation:

- Galois Counter Mode (GCM)—authentication and encryption
- GCM authentication (GMAC)— GCM authentication, no encryption
- No Encapsulation—no encapsulation (clear text)
- Null—encapsulation, no authentication or encryption

Security Group Access Control List

A security group is a group of users, end-point devices, and resources that share access control policies. Security groups are defined by the administrator in Cisco Identity Services Engine (ISE). As new users and devices are added to the Cisco TrustSec domain, the authentication server assigns these new entities to the appropriate security groups. Cisco TrustSec assigns each of the security group a unique 16-bit number whose scope is global in a Cisco TrustSec domain. The number of security groups in a wireless device is limited to the number of authenticated network entities. You do not have to manually configure the security group numbers.

After a device is authenticated, Cisco TrustSec tags any packet that originates from that device with an SGT that contains the security group number of the device. The packet carries this SGT everywhere in the network, in the Cisco TrustSec header.

As the SGT contains the security group of the source, the tag can be referred to as the source SGT (S-SGT). The destination device is also assigned to a security group (destination SG) that can be referred to as the destination SGT (D-SGT), even though the Cisco TrustSec packet does not contain the security group number of the destination device.

You can control the operations that users can perform based on the security group assignments of users and destination resources, using the Security Group Access Control Lists (SGACLs). Policy enforcement in a Cisco TrustSec domain is represented by a permission matrix, with the source security group numbers on one axis and the destination security group numbers on the other axis. Each cell in the matrix body contains an ordered list of SGACLs, which specify the permissions that must be applied to packets originating from the source security group and destined for the destination security group. When a wireless client is authenticated, the controller downloads all the SGACLs in the matrix cells.

When a wireless client connects to the network, the client pushes all the ACLs to the controller .

Cisco TrustSec achieves role-based topology-independent access control in a network by assigning users and devices in the network to security groups and applying access control between the security groups. The SGACLs define access control policies based on the device identities. As long as the roles and permissions remain the same, changes to the network topology do not change the security policy. When a user is added to the wireless group, you simply assign the user to an appropriate security group; the user immediately receives permissions to that group.

The size of ACLs are reduced and their maintenance is simplified with the use of role-based permissions. With Cisco TrustSec, the number of Access Control Entities (ACEs) that are configured is determined by the number of permissions specified, resulting in a much smaller number of ACEs.

To know the list of Cisco APs that support SGACL, see the release notes: https://www.cisco.com/c/en/us/support/wireless/catalyst-9800-series-wireless-controllers/products-release-notes-list.html

Note Clients receive zero SGT value and DHCP clients receive an Automatic Private IP Addressing (APIPA) address when TrustSec policy “unknown to unknown” is denied in TrustSec matrix.

Clients receive correct SGT values and DHCP clients receive an IP address when TrustSec policy “unknown to unknown” is permitted in TrustSec matrix.

The scenarios supported for SGACLs on the Cisco Catalyst 9800 Series Wireless Controller are:

- Wireless-to-wireless (within Enterprise network):
  - Flex mode with local switching—SGACL enforcement is done on the egress AP when a packet leaves from a source wireless network to a destination wireless network.
  - Flex mode with central switching—SGACL enforcement is done on the egress AP. To achieve this, controller should export IP address to security group tag (IP-SGT) binding over SGT Exchange Protocol (SXP).
- Wired-to-wireless (DC-to-Enterprise network)—Enforcement takes place when a packet reaches the destination AP.
- Wireless-to-wired (Enterprise network-to-DC)—Enforcement takes place on the uplink switch when a packet reaches the ingress of the wired network.

Guidelines and Restrictions

- SGACL enforcement is carried out on the controller for local mode.
- SGACL enforcement is carried out on an AP for flex-mode APs performing local switching.
- SGACL enforcement for wireless clients is carried out either on the upstream switch or on the border gateway in a Branch-to-DC scenario.
- SGACL enforcement is not supported for non-IP or IP broadcast or multicast traffic.
- Per-WLAN SGT assignment is not supported.
- SGACL enforcement is not carried out for control-plane traffic between an AP and the wireless controller (for upstream or from upstream traffic).

- Non-static SGACL configurations are supported only for dynamic SGACL policies received from ISE.
- Static SGACL configuration on an AP is not supported.
- In case of Allow List model, you need to explicitly allow DHCP protocol for the client devices to get the DHCP IP address and then request the controller for SGACL policies.

Inline Tagging

Inline tagging is a transport mechanism using which a controller or AP understands the source SGT.

Transport mechanism is of two types:

- Central switching—For centrally switched packets, the controller performs inline tagging of all the packets sourced from wireless clients that are associated with the controller, by tagging it with the Cisco Meta Data (CMD) tag. For packets that are inbound from the distribution system, inline tagging also involves the controller stripping off the CMD header from the packet to learn the S-SGT tag. Thereafter, the controller forwards the packet including the S-SGT, for SGACL enforcement.
- Local switching—To transmit locally switched traffic, an AP performs inline tagging for packets that are associated with the AP and sourced from clients. To receive traffic, the AP handles both locally switched packets and centrally switched packets, uses the S-SGT tag for packets, and applies the SGACL policy.

With wireless Cisco TrustSec enabled on the controller , the choice of enabling and configuring SXP to exchange tags with the switches is optional. Both wireless Cisco TrustSec and SXP modes are supported; however, there is no use case to have both wireless Cisco TrustSec (on an AP) and SXP to be in the enabled state concurrently.

Consideration and Restriction for Inline Tagging over Port-Channel

- Configure the **cts manual** command on port-channel and its member interfaces to send or receive a tagged packet.
- If you downgrade to Cisco IOS XE releases that do not support inline tagging over port-channel, the port-channel may be suspended.

Note The inline tagging over port-channel is supported in Cisco IOS XE 17.3.4es17.3.5 release.

Policy Enforcement

Cisco TrustSec access control is implemented using ingress tagging and egress enforcement. At the ingress point to the Cisco TrustSec domain, the traffic from the source is tagged with an SGT containing the security group number of the source entity. The SGT is propagated across the domain with the traffic. At the egress point of the Cisco TrustSec domain, an egress device uses the source SGT (S-SGT) and the security group of the destination entity (D-SGT) to determine the access policy to apply from the SGACL policy matrix.

Policy Enforcement Cisco TrustSec access control is implemented using ingress tagging and egress enforcement. At the ingress point to the Cisco TrustSec domain, the traffic from the source is tagged with an SGT containing the security group number of the source entity. The SGT is propagated across the domain with the traffic. At the egress point of the Cisco TrustSec domain, an egress device uses the source SGT (S-SGT) and the security group of the destination entity (D-SGT) to determine the access policy to apply from the SGACL policy matrix. Policy enforcement can be applied to both central and local switched traffic on an AP. If wired clients communicate with wireless clients, the AP enforces the downstream traffic. If wireless clients communicate with wired clients, the AP enforces the upstream traffic. This way, the AP enforces traffic in both downstream and wireless-to-wireless traffic. You require S-SGT, D-SGT, and ACLs for the enforcement to work. APs get the SGT information for all the wireless clients from the information available on the Cisco ISE server.

Note A Cisco AP must be in either Listener or Both (Listener and Speaker) mode to enforce traffic because the Listener mode maintains the complete set of IP-SGT bindings. After you enable the enforcement on a an AP, the corresponding policies are downloaded and pushed to the AP.

SGACL Support for Wireless Guest Access

When a client joins the wireless network (WLAN), its session is managed by the Cisco Catalyst 9800 Series Wireless LAN Controller (WLC) that the AP is connected to is the foreign controller. Auto-Anchor Mobility allows a specific WLAN (for example, Guest WLAN) to be anchored to a particular controller, regardless of the client's entry point into the network. Auto-Anchor Mobility is the wireless Guest service where all guest traffic tunnels back to the DMZ controller irrespective of where they associate with the network.

In case of Auto-Anchor mobility, the following apply to Cisco TrustSec support:

- Classification: Occurs during authentication and hence on Foreign for Layer 2 security WLANs and on Anchor for Layer 3 security cases.
- Propagation: Always occurs at the Anchor where the client traffic enters the wired network.
- Enforcement: SGACL download and enforcement occurs on Anchor; the Anchor controller must have the connectivity to Cisco Identity Services Engine (ISE) and be registered as Network Access Server (NAS). Enforcement is not supported on foreign controller even when the enforcement CLI is configured on foreign controller.

This feature is supported in local mode and in Flex Central Switching of the controller. Flex mode with local switching and Fabric mode are not supported in guest scenarios as traffic does not go through the controller.

Roaming of a guest client occurs only at Guest Foreign controller and the Guest Anchor remains fixed. The different types of supported roam are Inter-Controller roaming and Intra-Controller roaming. Roaming under WebAuth pending is a special case which is also supported for Central Web Authentication (CWA) and Local Web Authentication (LWA).

Enabling SGACL on the AP (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **Flex**.

Step 2 Click **Add**.

Step 3 In the **General** tab, check **Inline Tagging** and **SGACL Enforcement** check boxes and choose the CTS Profile Name from the **CTS Profile Name** drop-down list.

Step 4 Click **Apply to Device**.

Enabling SGACL on the AP

Note Use the **no** form of the commands given below to disable the configuration. For example, **cts role-based enforcement** disables role-based access control enforcement for APs.

Before you begin

- Security Group Access Control List (SGACL) on an AP can be enabled only when the wireless controller is in FlexConnect mode.
- Configure the **cts manual** command on the uplink port to send or receive a tagged packet.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile flex** *flex-profile* **Example:** `Device(config)# wireless profile flex xyz-flex-profile`	Configures an RF profile and enters RF profile configuration mode.
Step 3	**cts role-based enforcement** **Example:** `Device(config-wireless-flex-profile)# cts role-based enforcement`	Enables role-based access control enforcement for the AP.

	Command or Action	Purpose
Step 4	**cts inline-tagging** **Example:** `Device(config-wireless-flex-profile)# cts inline-tagging`	Enables inline tagging on the AP.
Step 5	**cts profile** *profile-name* **Example:** `Device(config-wireless-flex-profile)# cts profile xyz-profile`	Enables the CTS profile name.
Step 6	**exit** **Example:** `Device(config-wireless-flex-profile)# exit`	Returns to global configuration mode.
Step 7	**wireless tag site** *site-name* **Example:** `Device(config)# wireless tag site xyz-site`	Configures a site tag and enters site tag configuration mode.
Step 8	**flex-profile** *flex-profile-name* **Example:** `Device(config-site-tag)# flex-profile xyz-flex-profile`	Configures a flex profile.
Step 9	**exit** **Example:** `Device(config-site-tag)# exit`	Returns to global configuration mode.
Step 10	**ap** *mac-address* **Example:** `Device(config)# ap F866.F267.7DFB`	Configures an AP and enters AP profile configuration mode.
Step 11	**site-tag** *site-tag-name* **Example:** `Device(config-ap-tag)# site-tag xyz-site`	Maps a site tag to an AP.

What to do next

Use the **show cts ap sgt-info** *ap-name*command to verify the SGACL configuration on the AP.

Enabling SGACL Policy Enforcement Globally (CLI)

You must enable SGACL policy enforcement globally on Cisco Catalyst 9800 Series Wireless Controller. The same configuration commands that are used for enforcement of IPv4 traffic apply for IPv6 traffic as well.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**cts role-based enforcement** **Example:** `Device(config)# cts role-based enforcement`	Enables Cisco TrustSec SGACL policy enforcement on routed interfaces.

Enabling SGACL Policy Enforcement Per Interface (CLI)

After enabling the SGACL policy enforcement globally, you will have to enable Cisco TrustSec-on the uplink interfaces.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**interface gigabitethernet** *interface number* **Example:** `Device(config)# interface gigabitethernet 1`	Specifies interface on which to enable or disable SGACL enforcement.
Step 3	**cts role-based enforcement** **Example:** `Device(config-if)# cts role-based enforcement`	Enables Cisco TrustSec SGACL policy enforcement on routed interfaces.
Step 4	**do show cts interface** **Example:** `Device(config-if)# do show cts interface`	Verifies that SGACL enforcement is enabled.

Manually Configure a Device SGT (CLI)

In normal Cisco TrustSec operation, the authentication server assigns an SGT to the device for packets originating from the device. You can manually configure an SGT to be used if the authentication server is not accessible, but an authentication server-assigned SGT will take precedence over a manually-assigned SGT.

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile policy** *profile-policy* **Example:** `Device(config)# wireless profile policy rr-xyz-policy-1`	Configures a WLAN policy profile and enters wireless policy configuration mode.
Step 3	**cts sgt** *sgt-value* **Example:** `Device(config-wireless-policy)# cts stg 200`	Specifies the Security Group Tag (SGT) number. Valid values are from 0 to 65,535.
Step 4	**exit** **Example:** `Device(config-wireless-policy)# exit`	Returns to global configuration mode.

Configuring SGACL, Inline Tagging, and SGT in Local Mode (GUI)

Procedure

Step 1 Choose **Configuration** > **Tags & Profiles** > **Policy**.

Step 2 Click the Policy Profile Name. The **Edit Policy Profile** is displayed.

Step 3 Choose **General** tab.

Step 4 In the **CTS Policy** settings, check or uncheck the **Inline Tagging** and **SGACL Enforcement** check boxes, and enter the **Default SGT** value.

Step 5 Click **Update & Apply to Device**.

Configuring SGACL, Inline Tagging, and SGT in Local Mode

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 2	**wireless profile policy** *profile-name* **Example:** `Device(config)# wireless profile policy xyz-policy-profile`	Creates a policy profile for the WLAN.
Step 3	**cts inline-tagging** **Example:** `Device(config-wireless-policy)# cts inline-tagging`	Enables CTS inline tagging. **Note** You will also need to configure the **cts manual** in the physical interface. If the **cts manual** is configured in the physical interface and **cts inline-tagging** is skipped, the packets will still remain tagged at egress in the controller.
Step 4	**cts role-based enforcement** **Example:** `Device(config-wireless-policy)# cts role-based enforcement`	Enables CTS SGACL enforcement.
Step 5	**cts sgt** *sgt-value* **Example:** `Device(config-wireless-policy)# cts sgt 100`	(Optional) Sets the default Security Group Tag (SGT). **Note** SGT is required for a user session only when the client uses open authentication, and not the ISE server.

Configuring ISE for TrustSec

Procedure

	Command or Action	Purpose
Step 1	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.

	Command or Action	Purpose
Step 2	**radius server** *server-name* **Example:** `Device(config)# radius server Test-SERVER1`	Specifies the RADIUS server name.
Step 3	**address ipv4** *ip address* **Example:** `Device(config-radius-server)# address ipv4 124.3.50.62`	Specifies the primary RADIUS server parameters.
Step 4	**pac key** *key* **Example:** `Device(config-radius-server)# pac key cisco`	Specify the authentication and encryption key used between the Device and the key string RADIUS daemon running on the RADIUS server.
Step 5	**exit** **Example:** `Device(config-radius-server)# exit`	Returns to the configuration mode.
Step 6	**aaa group server radius** *server-group* **Example:** `Device(config)# aaa group server radius authc-server-group`	Creates a radius server-group identification. **Note** *server-group* refers to the server group name. The valid range is from 1 to 32 alphanumeric characters.
Step 7	**cts authorization list** *mlist-name* **Example:** `Device(config)# cts authorization list authc-list`	Creates a CTS authorization list.
Step 8	**aaa authorization network** *mlist-name* **group** *name* **Example:** `Device(config)# aaa authorization network default group group1`	Creates an authorization method list for web-based authorization. **Note** Ensure that the ISE IP address configured on your controller is the same as the IP address configured on ISE (**Work Center** > **TrustSec** > **Components** > **Trustsec AAA Servers**) **Note** If the ISE version is 002.005(000.239), 002.004(000.357), 002.003(000.298), 002.002(000.470), 002.001(000.474), 002.000(001.130), or 002.000(000.306), use the **access-session tls-version 1.0** command to download PAC from ISE. For other ISE versions, the above command is not required.

Verifying Cisco TrustSec Configuration

To display the wireless CTS SGACL configuration summary, use the following command:

```
Device# show wireless cts summary

Local Mode CTS Configuration

Policy Profile Name               SGACL Enforcement     Inline-Tagging   Default-Sgt
-------------------------------------------------------------------------------------
xyz-policy                        DISABLED              ENABLED          0
wireless-policy1                  DISABLED              DISABLED         0
w-policy-profile1                 DISABLED              DISABLED         0
default-policy-profile            DISABLED              DISABLED         0


Flex Mode CTS Configuration

Flex Profile Name                 SGACL Enforcement     Inline-Tagging
------------------------------------------------------------------------
xyz-flex                          DISABLED              ENABLED
demo-flex                         DISABLED              DISABLED
flex-demo                         DISABLED              DISABLED
xyz-flex-profile                  DISABLED              DISABLED
default-flex-profile              DISABLED              DISABLED
```

To display CTS-specific configuration status for various wireless profiles, use the following command:

```
Device# show cts wireless profile policy xyz-policy

Policy Profile Name           : xyz-policy
CTS
  Role-based enforcement         : ENABLED
  Inline-tagging                 : ENABLED
   Default SGT   : 100

Policy Profile Name            : foo2
CTS
  Role-based enforcement         : DISABLED
  Inline-tagging                 : ENABLED
  Default SGT           : NOT-DEFINED

Policy Profile Name                    : foo3
CTS
  Role-based enforcement         : DISABLED
  Inline-tagging                 : DISABLED
  Default SGT    : 65001
```

To display CTS configuration for a given wireless profile, use the following command:

```
Device# show wireless profile policy detailed xyz-policy

Policy Profile Name           : xyz-policy
Description                   :
Status                        : DISABLED
VLAN                          : 1
Client count                  : 0
Passive Client                : DISABLED
ET-Analytics                  : DISABLED
StaticIP Mobility             : DISABLED
!
```

```
.
.
.WGB Policy Params
  Broadcast Tagging           : DISABLED
  Client VLAN                 : DISABLED
Mobility Anchor List
  IP Address                                Priority
CTS
  Role-based enforcement         : ENABLED
  Inline-tagging                 : ENABLED
  Default SGT                   : NOT-DEFINED
```