Configuring Group-based Policy on a Fabric Edge

Provisioning a group-based policy secures your network by providing group-based access control and secure communication between the devices in the network. For information, see Cisco TrustSec Switch Configuration Guide.

- Enabling SGACL Policy Enforcement, on page 1
- Configuration Example for Group-based Policy on Fabric Edge, on page 2

Enabling SGACL Policy Enforcement

To enable SGACL policy enforcement, perform this task:

Procedure

	Command or Action	Purpose
Step 1	**enable** **Example:** `Device> enable`	Enables privileged EXEC mode. Enter your password, if prompted.
Step 2	**configure terminal** **Example:** `Device# configure terminal`	Enters global configuration mode.
Step 3	**cts authorization list** *server-list* **Example:** `Device(config)# cts authorization list cts-list`	Configures a AAA server to be used by the seed device.

Step 4	**cts role-based sgt-map vlan-list** *vlan-id* **sgt** *sgt-number*
	
	Example:
	
	`Device(config)# cts role-based sgt-map vlan-list 50 sgt 4`
	`Device(config)# cts role-based sgt-map vlan-list 30 sgt 8`
		Binds an SGT with a specified VLAN or a set of VLANs.

	Command or Action	Purpose
	`Device(config)# `**`cts role-based sgt-map vlan-list 51 sgt 15`**	
Step 5	**cts role-based enforcement** **Example:** `Device(config)# `**`cts role-based enforcement`**	Enables security group access control list (SGACL) policy enforcement on routed interfaces.
Step 6	**cts role-based enforcement vlan-list** *vlan-list* **Example:** `Device(config)# `**`cts role-based enforcement vlan-list 30,40,50-51,91`**	Enables SGACL policy enforcement on the VLAN or VLAN list.
Step 7	**end** **Example:** `Device(config)# `**`end`**	Returns to privileged EXEC mode.

Configuration Example for Group-based Policy on Fabric Edge

This sample configuration shows how to manually map an SGT to VLANs and enforce the SGACL policy on the VLANs.

```
CTS role-based enforcement

cts authorization list cts-list
cts role-based sgt-map vlan-list 50 sgt 4
cts role-based sgt-map vlan-list 30 sgt 8
cts role-based sgt-map vlan-list 51 sgt 15
cts role-based enforcement
cts role-based enforcement vlan-list 30,40,50-51,91
```