



## Configuring Security Group ACL Policies

Using security group access control lists (SGACLs), you can control the operations that users can perform based on the security group assignments of users and destination resources. Policy enforcement within the Cisco TrustSec domain is represented by a permissions matrix, with source security group numbers on one axis and destination security group numbers on the other axis. Each cell in the body of the matrix can contain an ordered list of SGACLs which specifies the permissions that should be applied to packets originating from the source security group and destined for the destination security group.

- [Restrictions for Security Group Access Control Lists \(SGACL\) Policies, on page 1](#)
- [How to Configure SGACL Policies, on page 1](#)
- [Configuration Examples for SGACL Policies, on page 10](#)
- [Feature Information for SGACL Policies, on page 12](#)

## Restrictions for Security Group Access Control Lists (SGACL) Policies

The following restriction apply to the Cisco Catalyst 3650 Series Switches and Cisco Catalyst 3850 Series Switches:

- CTS SGACLs cannot be enforced for punt (CPU bound) traffic due to hardware limitations.

## How to Configure SGACL Policies

The following sections provide information on various SGACL policy configurations.

### SGACL Policy Configuration Process

Follow these steps to configure and enable Cisco TrustSec Security Group ACL (SGACL) policies:

1. Configuration of SGACL policies should be done primarily through the Policy Management function of the Cisco Secure Access Control Server (ACS) or the Cisco Identity Services Engine (ISE).

If you are not using AAA on a Cisco Secure ACS or a Cisco ISE to download the SGACL policy configuration, you can manually configure the SGACL mapping and policies.



**Note** An SGACL policy downloaded dynamically from the Cisco Secure ACS or a Cisco ISE will override any conflicting locally-defined policy.

2. To enable SGACL policy enforcement on egress traffic on routed ports, enable SGACL policy enforcement globally as described in the Enabling SGACL Policy Enforcement Globally section.
3. To enable SGACL policy enforcement on switched traffic within a VLAN, or on traffic that is forwarded to an SVI associated with a VLAN, enable SGACL policy enforcement for specific VLANs as described in the Enabling SGACL Policy Enforcement on VLANs section.

## Enabling SGACL Policy Enforcement Globally

You must enable SGACL policy enforcement globally for Cisco TrustSec-enabled routed interfaces.

To enable SGACL policy enforcement on routed interfaces, perform this task:

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b> <b>Example:</b> Device# <b>enable</b>	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b>	<b>configure terminal</b> <b>Example:</b> Device# <b>configure terminal</b>	Enters global configuration mode.
<b>Step 3</b>	<b>cts role-based enforcement</b> <b>Example:</b> Device(config)# <b>cts role-based enforcement</b>	Enables Cisco TrustSec SGACL policy enforcement on routed interfaces.

## Enabling SGACL Policy Enforcement Per Interface

You must first enable SGACL policy enforcement globally for Cisco TrustSec-enabled routed interfaces. This feature is not supported on Port Channel interfaces.

To enable SGACL policy enforcement on Layer 3 interfaces, perform this task:

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b> <b>Example:</b> Device# <b>enable</b>	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>

	Command or Action	Purpose
<b>Step 2</b>	<b>configure terminal</b> <b>Example:</b> Device# <code>configure terminal</code>	Enters global configuration mode.
<b>Step 3</b>	<b>interface</b> <i>type slot/port</i> <b>Example:</b> Device(config)# <code>interface gigabitethernet 6/2</code>	Configures an interface and enters interface configuration mode.
<b>Step 4</b>	<b>cts role-based enforcement</b> <b>Example:</b> Device(config-if)# <code>cts role-based enforcement</code>	Enables Cisco TrustSec SGACL policy enforcement on routed interfaces.
<b>Step 5</b>	<b>end</b> <b>Example:</b> Device(config-if)# <code>end</code>	Exits to privileged EXEC mode.
<b>Step 6</b>	<b>show cts interface</b> <b>Example:</b> Device# <code>show cts interface</code>	Displays Cisco TrustSec states and statistics per interface.

## Enabling SGACL Policy Enforcement on VLANs

You must enable SGACL policy enforcement on specific VLANs to apply access control to switched traffic within a VLAN, or to traffic that is forwarded to an SVI associated with a VLAN.

To enable SGACL policy enforcement on a VLAN or a VLAN list, perform this task:

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b> <b>Example:</b> Device# <code>enable</code>	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b>	<b>configure terminal</b> <b>Example:</b> Device# <code>configure terminal</code>	Enters global configuration mode.
<b>Step 3</b>	<b>cts role-based enforcement vlan-list</b> <i>vlan-list</i> <b>Example:</b> Device(config)# <code>cts role-based enforcement vlan-list 31-35,41</code>	Enables Cisco TrustSec SGACL policy enforcement on the VLAN or VLAN list.

## Configuring SGACL Monitor Mode

Before configuring SGACL monitor mode, ensure the following:

- Cisco TrustSec is enabled
- Counters are enabled

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b> <b>Example:</b> Device# <b>enable</b>	Enables privileged EXEC mode. Enter your password if prompted.
<b>Step 2</b>	<b>configure terminal</b> <b>Example:</b> Device# <b>configure terminal</b>	Enters global configuration mode.
<b>Step 3</b>	<b>cts role-based monitor enable</b> <b>Example:</b> Device(config)# <b>cts role-based monitor enable</b>	Enables device level monitor mode. <ul style="list-style-type: none"><li>• By default device level monitor mode is enabled. If device monitor mode is disabled, monitor mode information is still downloaded from ISE but not applied on device until this configuration is turned on.</li></ul>
<b>Step 4</b>	<b>cts role-based monitor permissions from {sgt_num} to {dgt_num} [ipv4   ipv6]</b> <b>Example:</b> Device(config)# <b>cts role-based permissions from 2 to 3 ipv4</b>	Enables monitor mode for IPv4/IPv6 Role Based Access Control List (RBACL) (Security Group Tag (SGT)- Destination Group Tag (DGT) pair).
<b>Step 5</b>	<b>end</b> <b>Example:</b> Device(config)# <b>end</b>	Exits to privileged EXEC mode.
<b>Step 6</b>	<b>show cts role-based monitor permissions from {sgt_num} to {dgt_num} [ipv4   ipv6] [details]</b> <b>Example:</b> Device# <b>show cts role-based permissions from 2 to 3 ipv4 details</b>	Displays the SGACL policies and details about the monitor mode feature for each pair. The command output displays monitored if per cell monitor mode is enabled for the <SGT-DGT> pair
<b>Step 7</b>	<b>show cts role-based counters [ipv4   ipv6]</b> <b>Example:</b> Device# <b>show cts role-based counters ipv4</b>	Displays all SGACL enforcement statistics for IPv4 and IPv6 events.

## Manually Configuring SGACL Policies

A role-based access control list bound to a range of SGTs and DGTs forms an SGACL, a Cisco TrustSec policy enforced on egress traffic. Configuration of SGACL policies are best done through the policy management functions of the Cisco ISE or the Cisco Secure ACS. To manually (that is, locally) configure SGACL policies, do the following:

1. Configure a role-based ACL.
2. Bind the role-based ACL to a range of SGTs.



**Note** An SGACL policy downloaded dynamically from the Cisco ISE or Cisco ACS overrides any conflicting manually configured policy.

## Manually Configuring and Applying IPv4 SGACL Policies



**Note** When configuring SGACLs and Role-Based access control lists (RBACLs), the named access control lists (ACLs) must start with an alphabet.

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b> <b>Example:</b> Device# <b>enable</b>	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b>	<b>configure terminal</b> <b>Example:</b> Device# <b>configure terminal</b>	Enters global configuration mode.
<b>Step 3</b>	<b>ip access-list role-based <i>rbacl-name</i></b> <b>Example:</b> Device(config)# <b>ip access-list role-based allow_webtraff</b>	Creates a Role-based ACL and enters Role-based ACL configuration mode.
<b>Step 4</b>	<b>{ [ <i>sequence-number</i> ]   default   permit   deny   remark }</b> <b>Example:</b> Device(config-rb-acl)# <b>10 permit tcp dst eq 80 dst eq 20</b>	Specifies the access control entries (ACEs) for the RBACL.  You can use most of the commands and options allowed in extended named access list configuration mode, with the source and destination fields omitted.  Press Enter to complete an ACE and begin the next.

	Command or Action	Purpose
		The following ACE commands or keywords are not supported: <ul style="list-style-type: none"> <li>• <b>reflect</b></li> <li>• <b>evaluate</b></li> <li>• <b>time-range</b></li> </ul>
<b>Step 5</b>	<b>exit</b> <b>Example:</b> Device(config-rb-acl)# <b>exit</b>	Exits role-based ACL configuration mode and returns to global configuration mode.
<b>Step 6</b>	<b>cts role-based permissions {default   [from {sgt_num   unknown} to {dgt_num   unknown}] {rbacIs   ipv4 rbacIs}</b> <b>Example:</b> Device(config)# <b>cts role-based permissions from 55 to 66 allow_webtraff</b>	Binds SGTs and DGTs to the RBACL. The configuration is analogous to populating the permission matrix configured on the Cisco ISE or the Cisco Secure ACS. <ul style="list-style-type: none"> <li>• <b>Default</b>—Default permissions list</li> <li>• <b>sgt_num</b>—0 to 65,519. Source Group Tag.</li> <li>• <b>dgt_num</b>—0 to 65,519. Destination Group Tag</li> <li>• <b>unknown</b>—SGACL applies to packets where the security group (source or destination) cannot be determined.</li> <li>• <b>ipv4</b>—Indicates the following RBACL is IPv4.</li> <li>• <b>rbacIs</b> —Name of RBACLs</li> </ul>
<b>Step 7</b>	<b>end</b> <b>Example:</b> Device(config)# <b>end</b>	Exits global configuration mode and returns to privileged EXEC mode.
<b>Step 8</b>	<b>show cts role-based permissions</b> <b>Example:</b> Device# <b>show cts role-based permissions</b>	Displays permission to RBACL configurations.
<b>Step 9</b>	<b>show ip access-lists {rbacIs   ipv4 rbacIs}</b> <b>Example:</b> Device# <b>show ip access-lists allow_webtraff</b>	Displays ACEs of all RBACLs or a specified RBACL.

## Configuring IPv6 Policies

To manually configure IPv6 SGACL policies, perform this task:



**Note** IPv6 SGACL is not supported on Cisco IOS XE Everest 16.8.1.

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b> <b>Example:</b> Device# <b>enable</b>	Enables privileged EXEC mode. Enter your password if prompted.
<b>Step 2</b>	<b>configure terminal</b> <b>Example:</b> Device# <b>configure terminal</b>	Enters global configuration mode.
<b>Step 3</b>	<b>ipv6 access-list role-based <i>sgacl-name</i></b> <b>Example:</b> Device(config)# <b>ipv6 access-list role-based <i>sgaclname</i></b>	Creates a named IPv6 SGACL and enters IPv6 role-based ACL configuration mode.
<b>Step 4</b>	<b>{permit   deny } protocol [dest-option   dest-option-type {doh-number   doh-type}] [dscp <i>cp-value</i>] [flow-label <i>fl-value</i>] [mobility   mobility-type {mh-number   mh-type}] [routing   routing-type <i>routing-number</i>] [fragments] [log   log-input] [sequence <i>seqno</i>]</b>	Specifies the access control entries (ACEs) for the RBACL.  You can use most of the commands and options allowed in extended named access list configuration mode, with the source and destination fields omitted.  The following ACE commands or keywords are not supported: <ul style="list-style-type: none"> <li>• <b>reflect</b></li> <li>• <b>evaluate</b></li> <li>• <b>time-range</b></li> </ul>
<b>Step 5</b>	<b>end</b> <b>Example:</b> Device(config-ipv6rb-acl)# <b>end</b>	Exits IPv6 role-based ACL configuration mode and returns to privileged EXEC mode.

## Manually Applying SGACL Policies

To manually apply SGACL policies, perform this task:

**Procedure**

	<b>Command or Action</b>	<b>Purpose</b>
<b>Step 1</b>	<b>enable</b> <b>Example:</b> Device# <b>enable</b>	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b>	<b>configure terminal</b> <b>Example:</b> Device# <b>configure terminal</b>	Enters global configuration mode.
<b>Step 3</b>	<b>cts role-based permissions default [ipv4   ipv6] sgacl-name1 [sgacl-name2 [sgacl-name3 ...]]</b> <b>Example:</b> Device(config)# <b>cts role-based permissions default MYDEFAULTSGACL</b>	Specifies the default SGACLs. The default policies are applied when no explicit policy exists between the source and destination security groups.
<b>Step 4</b>	<b>cts role-based permissions from {source-sgt   unknown} to {dest-sgt   unknown} [ipv4   ipv6] sgacl-name1 [sgacl-name2 [sgacl-name3 ...]]</b> <b>Example:</b> Device(config)# <b>cts role-based permissions from 3 to 5 SRB3 SRB5</b>	Specifies the SGACLs to be applied for a source security group (SGT) and destination security group (DGT). Values for source-sgt and dest-sgt range from 1 to 65533. By default, SGACLs are considered to be IPv4. <ul style="list-style-type: none"> <li>• <b>from</b>—Specifies the source SGT.</li> <li>• <b>to</b>—Specifies the destination security group.</li> <li>• <b>unknown</b>—SGACL applies to packets where the security group (source or destination) cannot be determined.</li> </ul> <p><b>Note</b> An SGACL policy downloaded dynamically from the ACS will override any conflicting manual policy.</p>

## Displaying SGACL Policies

After configuring the Cisco TrustSec device credentials and AAA, you can verify the Cisco TrustSec SGACL policies downloaded from the authentication server or configured manually. Cisco TrustSec downloads the SGACL policies when it learns of a new SGT through authentication and authorization on an interface, from SXP, or from manual IP address to SGT mapping.

Using the keywords, you can display all or part of the permissions matrix:

- If the **from** keyword is omitted, a column from the permissions matrix is displayed.
- If the **to** keyword is omitted, a row from the permissions matrix is displayed.



- If the **from** and **to** keywords are omitted, the entire permissions matrix is displayed.
- If the **from** and **to** keywords are specified, a single cell from the permissions matrix is displayed and the **details** keyword is available. When **details** is entered, the ACEs of the SGACL of the single cell are displayed.

To display the contents of the SGACL policies permissions matrix, perform this task:

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b> <b>Example:</b> Device# <b>enable</b>	Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul>
<b>Step 2</b>	<b>show cts role-based permissions default [ipv4   ipv6   details]</b> <b>Example:</b> Device(config)# <b>show cts role-based permissions default MYDEFAULTSGACL</b>	Displays the list of SGACL of the default policy.
<b>Step 3</b>	<b>show cts role-based permissions from {source-sgt   unknown} to {dest-sgt   unknown} [ipv4   ipv6   details]</b> <b>Example:</b> Device(config)# <b>show cts role-based permissions from 3</b>	Specifies the SGACLs to be applied for a source security group (SGT) and destination security group (DGT). Values for source-sgt and dest-sgt range from 1 to 65533. By default, SGACLs are considered to be IPv4. <ul style="list-style-type: none"> <li>• <b>from</b>—Specifies the source SGT.</li> <li>• <b>to</b>—Specifies the destination security group.</li> <li>• <b>unknown</b>—SGACL applies to packets where the security group (source or destination) cannot be determined.</li> </ul> <p><b>Note</b> An SGACL policy downloaded dynamically from the ACS will override any conflicting manual policy.</p>

## Refreshing the Downloaded SGACL Policies

### Procedure

	Command or Action	Purpose
<b>Step 1</b>	<b>enable</b> <b>Example:</b>	Enables privileged EXEC mode. Enter your password if prompted.

	Command or Action	Purpose
	Device# <code>enable</code>	
<b>Step 2</b>	<b>configure terminal</b> <b>Example:</b> Device# <code>configure terminal</code>	Enters global configuration mode.
<b>Step 3</b>	<b>cts refresh policy {peer [peer-id]   sgt [sgt_number   default   unknown]}</b> <b>Example:</b> Device(config)# <code>cts refresh policy peer my_cisco_ise</code>	Performs an immediate refresh of the SGACL policies from the authentication server. <ul style="list-style-type: none"> <li>• If a <i>peer-id</i> is specified, only the policies related to the specified peer connection are refreshed. To refresh all peer policies, press Enter without specifying an ID.</li> <li>• If an SGT number is specified, only the policies related to that SGT are refreshed. To refresh all security group tag policies, press Enter without specifying an SGT number. Select default to refresh the default policy. Select unknown to refresh unknown policy.</li> </ul>

## Configuration Examples for SGACL Policies

The following sections provide information on various SGACL policy configuration examples.

### Example: Enabling SGACL Policy Enforcement Globally

```
Device# configure terminal
Device(config)# cts role-based enforcement
```

### Example: Enabling SGACL Policy Enforcement Per Interface

```
Device# configure terminal
Device(config)# interface gigabitethernet 1/0/2
Device(config-if)# cts role-based enforcement
Device(config-if)# end
```

### Example: Enabling SGACL Policy Enforcement on VLANs

```
Device# configure terminal
Device(config)# cts role-based enforcement vlan-list 31-35,41
Device(config)# exit
```

## Example: Configuring SGACL Monitor Mode

```

Device# configure terminal
Device(config)# cts role-based monitor enable
Device(config)# cts role-based permissions from 2 to 3 ipv4
Device# show cts role-based permissions from 2 to 3 ipv4

IPv4 Role-based permissions from group 2:sgt2 to group 3:sgt3 (monitored):
denytcpudpicmp-10
Deny IP-00

Device# show cts role-based permissions from 2 to 3 ipv4 details

IPv4 Role-based permissions from group 2:sgt2 to group 3:sgt3 (monitored):
denytcpudpicmp-10
Deny IP-00

Details:
Role-based IP access list denytcpudpicmp-10 (downloaded)
 10 deny tcp
 20 deny udp
 30 deny icmp
Role-based IP access list Permit IP-00 (downloaded)
 10 permit ip

Device# show cts role-based counters ipv4

Role-based IPv4 counters
From      To      SW-Denied  HW-Denied  SW-Permitt  HW_Permitt  SW-Monitor  HW-Monitor
*         *       0          0          8           18962       0           0
2         3       0          0          0           0           0           341057

```

## Example: Manually Configuring SGACL Policies

```

Device# configure terminal
Device(config)# ip access role allow_webtraff
Device(config-rb-acl)# 10 permit tcp dst eq 80
Device(config-rb-acl)# 20 permit tcp dst eq 443
Device(config-rb-acl)# 30 permit icmp
Device(config-rb-acl)# 40 deny ip
Device(config-rb-acl)# exit
Device(config)# cts role-based permissions from 55 to 66 allow_webtraff
Device# show ip access allow_webtraff

Role-based IP access list allow_webtraff
 10 permit tcp dst eq www
 20 permit tcp dst eq 443
 30 permit icmp
 40 deny ip
Device# show show cts role-based permissions from 50 to 70

```

## Example: Manually Applying SGACLs

```

Device# configure terminal
Device(config)# cts role-based permissions default MYDEFAULTSGACL

```

```
Device(config)# cts role-based permissions from 3 to 5 SRB3 SRB5
Device(config)# exit
```

## Example: Displaying SGACL Policies

This example shows how to display the content of the SGACL policies permissions matrix for traffic sourced from security group 3:

```
Device# show cts role-based permissions from 3

Role-based permissions from group 3 to group 5:
  SRB3
  SRB5
Role-based permissions from group 3 to group 7:
  SRB4
```

## Feature Information for SGACL Policies

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use the Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to [www.cisco.com/go/cfn](http://www.cisco.com/go/cfn). An account on Cisco.com is not required.

**Table 1: Feature Information for SGACL Policies**

Feature Name	Release	Feature Information
SGACL Policies	Cisco IOS XE Denali 16.1.1	This feature was introduced.