

SGACL High Availability

- Feature History for SGACL High Availability, on page 1
- Cisco TrustSec SGACL High Availability, on page 1
- Data Synchronization and Switchover Process, on page 2
- Verify Cisco TrustSec SGACL High Availability, on page 2

Feature History for SGACL High Availability

This table provides release and platform support information for the features explained in this module.

These features are available in all the releases subsequent to the one they were introduced in, unless noted otherwise.

Release	Feature Name and Description	Supported Platform
Cisco IOS XE 26.2.1ea	SGACL High Availability: Cisco TrustSec Security Group Access Control Lists (SGACLs) feature support has been introduced.	Cisco C9550 Series Smart Switches
Cisco IOS XE 17.18.1	SGACL High Availability: Cisco TrustSec SGACLs support high availability on switches equipped with Cisco StackWise technology.	Cisco C9350 Series Smart Switches Cisco C9610 Series Smart Switches

Cisco TrustSec SGACL High Availability

Cisco TrustSec Security Group Access Control Lists (SGACLs) support high availability on switches equipped with Cisco StackWise technology. StackWise provides stateful redundancy, allowing a switch stack to enforce and process access control entries (ACEs) even during failover events.

High Availability Operation in Switch Stacks

Within a switch stack, the stack manager designates the switch with the highest priority as the active switch, and the next highest as the standby. During a stateful switchover, whether automatic or CLI-initiated, the standby switch becomes active, while the next in line assumes the standby role.

Operational data is synchronized from the active to the standby switch during system bootup, when operational data changes (such as Change of Authorization [CoA]), or during an operational data refresh.

Deploying Devices in High Availability Setup

Perform the following steps when deploying devices in an high availability setup:

1. Remove any existing credentials from all devices that will be part of the high availability setup.
2. Power up the stack and assign device roles (active, standby, and member switches).
3. On the active device, set up the credentials using the **cts credentials id** *id* **password** *password* command.

Data Synchronization and Switchover Process

When a stateful switchover occurs, the new active switch requests and downloads the necessary operational data. Environment data (ENV-data) and Role-Based Access Control Lists (RBACLs) are updated only after the refresh period completes.

The following are the different types of operational data that are downloaded to the active switch.

Operational Data	Description
Environment Data (ENV-data)	Contains a preferred server list for retrieving RBACL information during refresh or initialization.
Protected Access Credential (PAC)	A unique shared secret between the switch and the authenticator, used to secure Extensible Authentication Protocol Flexible Authentication via Secure Tunneling (EAP-FAST).
Role-Based Policy (RBACL or SGACL)	A variable-length list defining policies for all Security Group Tag (SGT) mappings on the switch.

Note Cisco TrustSec credential that consists of the device ID and password details is run as a command on the active switch.

Verify Cisco TrustSec SGACL High Availability

To verify the Cisco TrustSec SGACL high availability configuration, run the **show cts role-based permissions** command on both the active and standby switches. The output from the command must be the same on both switches.

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

```
Device# show cts role-based permissions

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
```

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

```
Device-stby# show cts role-based permissions

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
```

After a stateful switchover, run the following commands on the active switch to verify the feature:

The following is a sample output from the **show cts pacs** command:

```
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:
000200B80003000100040010A3B6D4D8353F102346786CF220FF151C0006009C00030100E044B2650D8351FD06
F23623C470511E0000001356DEA96C00093A80538898D40F633C368B053200D4C9D2422A7FEB4837EA9DBB89D1
E51DA4E7B184E66D3D5F2839C11E5FB386936BB85250C61CA0116FDD9A184C6E96593EEAF5C39BE08140AFBB19
4EE701A0056600CFF5B12C02DD7ECEAA3CCC8170263669C483BD208052A46C31E39199830F794676842ADEECBB
A30FC4A5A0DEDA93
Refresh timer is set for 01:00:05
```

The following is a sample output from the **show cts environment-data** command:

```
Device# show cts environment-data

CTS Environment Data
====================
Current state = COMPLETE
Last status = Successful
Local Device SGT:
  SGT tag = 0: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 = FALSE, keywrap-enable = FALSE, idle-time = 60 mins, deadtime = 20 secs
```

```
Multicast Group SGT Table:
Security Group Name Table:
0001-45 :
  0-00:Unknown
  2-ba: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
!
!
!
Environment Data Lifetime = 3600 secs
Last update time = 14:32:53 IST Mon Mar 14 2016
Env-data expires in 0:00:10:04 (dd:hr:mm:sec)
Env-data refreshes in 0:00:10:04 (dd:hr:mm:sec)
Cache data applied = NONE
State Machine is running
```

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

```
Device# show cts role-based permissions

IPv4 Role-based permissions default:
        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
```