# Secure Group Tag-based Access Control

## User Access Control through SGACL

*Table 1: Feature History*

| Feature Name | Release Information | Description |
|---|---|---|
| User Access Control through Secure Group Tag-based Access Control List (SGACL) | 2024.03.0 | UPF supports Cisco ISE integration for SGACL enforcement on the downlink packets. SGACL is an Access Control List (ACL) that controls and manages the authorization of the security group members.<br>UPF fetches the SGACL matrix from ISE through an API query based on the Destination SGT (D-SGT). The D-SGT is received over the Sx or N4 interface from SMF. Then, UPF applies the SGACLs based on the D-SGT and Source SGT (S-SGT) mapping on the downlink packets. Hence, the policy enforcement from Cisco ISE is enabled.<br>**Default Setting**: Disabled – Configuration Required to Enable |

| Feature Name | Release Information | Description |
|---|---|---|
| Security Group Tag (SGT) for Cisco Identity Service Engine (ISE) Integration on UPF | 2023.03 | UPF supports ISE integration for handling the SGT received from SMF. The SMF receives the SGT from the RADIUS server. Then, the SMF sends the SGT over the Sx or N4 interface to UPF during Session Establishment Request.<br>The creation of SGT is according to the static policy on Cisco ISE or SMF and the UPF requires inserting the SGT into the Cisco Meta Data (CMD) header on uplink packets.<br>**Default Setting**: Not Applicable |

The Security Group Tag (SGT), also referred to as the Scalable Group Tag, specifies the privileges of a traffic source within a trusted network. Security Group Access automatically generates SGT when you add a security group in TrustSec or ISE. Cisco ISE, as a centralized policy engine, provides a unified policy management experience for the other Cisco packet core elements.

The SGT is a 16-bit value that is transmitted in the Cisco Meta Data (CMD) field of a Layer 2 Ethernet Frame. The CMD header is inserted after the ".1Q" tag, if available. If the ".1Q" tag is unavailable, the CMD immediately follows the MAC Source Address.

To support SGT for ISE integration:

- SMF receives the D-SGT from the ISE server.
- SMF updates the D-SGT towards the UPF using the N4 extensions.
- UPF identifies the device packets and applies the corresponding D-SGT to the N6 packets.

Security Group Tag-based Access Control List (SGACL) is an Access Control List (ACL) that controls and manages the authorization of the security group members. SGACLs create SGACL policies, which are represented through a Security Group Tag matrix (SGT matrix).

The SGT matrix, also referred to as the permissions matrix, represents the SGACL policies in the TrustSec domain. This matrix comprises the security group numbers and destination security group numbers, and describes how the two endpoints communicate. The applicable policies are Permit and Deny. The contents of an SGT matrix and the SGACLs are downloaded from the ISE server using the REST API.

UPF inserts the D-SGT value for the outgoing uplink packets sent over the N6 interface. UPF receives the S-SGT value for the downlink packets over the N6 interface. This S-SGT value is used for the matrix lookup and is removed while sending the outgoing downlink packets over the N3 interface.

Based on the mapping between the Destination SGT (D-SGT) and Source SGT (S-SGT), the policies are enforced at UPF and an appropriate SGACL is enforced on the downlink packets.

UPF supports ISE integration for SGACL enforcement for the downlink packets through the following SGT values:

- Destination SGT (D-SGT)—UPF receives this value per subscriber session over the N4 interface from SMF in the Session Establishment Request. SMF receives the D-SGT from ISE in the RADIUS Access Accept message. For this feature, the SMF must send the SGT to UPF in a proprietary IE on the N4 interface.

- Source SGT (S-SGT)—Is received in the CMD header of a downlink packet. A wireless LAN controller (WLC) or an access switch inserts this value.

**Note**

- SMF receives the D-SGT from ISE in the Access Accept message. For this feature, the SMF must send the SGT to UPF in a proprietary IE on the N4 interface.
- When you enable the user access control through SGACL and a subscriber session receives a D-SGT, then the SGACL is applied to the downlink packets. In this case, the APN ACL isn’t applicable to these subscriber sessions.
- When you don’t enable the user access control through SGACL or the UPF doesn't receive the D-SGT during the N4 Session Establishment Request, then the APN ACL is applicable as per the existing configuration.

You can define the ISE server profile through the **ise-server-profile** *profile_name* CLI command and associate the ISE server profile within a UPF service through the **associate ise-server-profile name** *server_profile_name* CLI command.

# How SGACL for ISE Integration Works

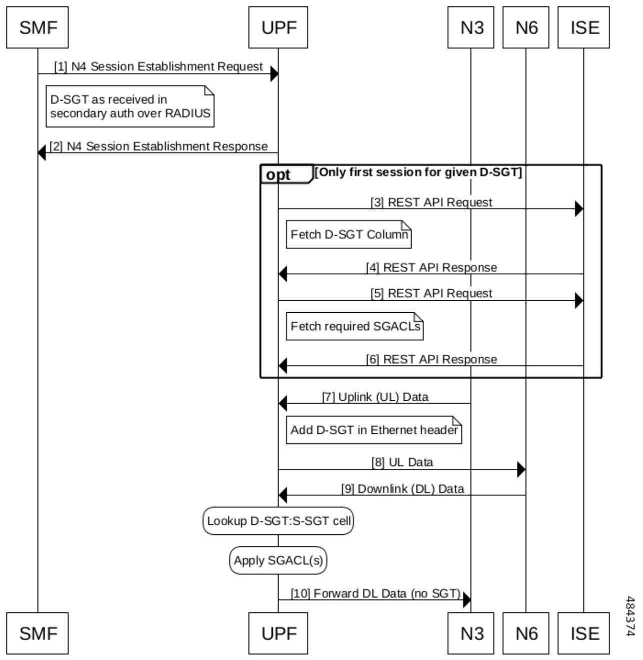
This section describes how SGACL for ISE integration works.

- SMF fetches the corresponding SGT value from ISE over RADIUS and sent on N4 interface to the UPF.
- Each UPF is registered as a Network Access Device (NAD) in ISE server.
- UPF downloads the SGT Matrix and corresponding SGACLs from ISE server using the REST API. UPF applies the SGACL for flow based on the D-SGT to S-SGT mapping.
- A non-real time update is available through periodic or trigger-based pull from UPF.
- The D-SGT value needs to be checkpointed for session recovery and ICSR-based recovery.

## Call Flow

The following figure illustrates the SGT fetch and SGACL enforcement call flow.

*Figure 1: SGT Fetch and SGACL Enforcement Call Flow*



| Step | Description |
|---|---|
| 1 | SMF sends N4 Session Establishment Request to UPF. As part of this request, the UPF receives the D-SGT value from SMF. |
| 2 | UPF sends N4 Session Establishment Response to SMF. |
| 3 | For the first session of a specific D-SGT, UPF sends the REST API Request to the ISE server to fetch the D-SGT column values. |
| 4 | ISE sends the REST API Response to UPF. This response includes the mapped S-SGT values for the D-SGT and the SGACL matrix information containing the SGACL names along with the refresh timer.<br>The SGT matrix cell entries and SGACLs are stored on UPF. Each D-SGT column has a refresh timer that is configured in ISE. |
| 5 | UPF sends the REST API Request to the ISE server to fetch the required SGACLs.<br>ISE sends the REST API Response to UPF with the SGACL definitions. |
| 6 | N3 sends the uplink (UL) data to UPF. |
| 7 | UPF adds D-SGT in Ethernet header and sends the UL data to the N6 interface. |
| 8 | N6 sends the downlink (DL) data to the N3 interface. |
| 9 | The UPF checks the D-SGT and S-SGT mapping and applies the SGACLs. |
| 10 | UPF forwards the DL data, with no SGT, to the N3 interface. |

# Limitations

This feature has the following known limitations:

- The PFCP Session Establishment Request must send the D-SGT value over the N4 interface. The SGT value isn't modified or removed during the life of the session.
- As the ACLs can be stacked for a specific SGT-Pair combination, the SGACLs are applied as per the order of ACLs received for a specific SGT-Pair.
- The maximum number of recommended matrix combinations is 150 D-SGT Columns * 150 S-SGT rows, with 255 distinct SGACLs, including the default SGACL.
- The maximum number of SGACLs in a single cell is limited to 16.
- UPF can store only one default SGACL at a time. Hence, when the Default SGACL changes, only the updated SGACLs information is stored on UPF.

# SGACL Configuration for ISE Integration

This section describes the procedures to configure SGACL for ISE integration.

## Enable API Manager

API manager is a facility that enables API request and response integration through REST APIs.

**Note** Enabling the API manager is a prerequisite for SGACL integration.

**Step 1** Log in to the configuration mode.

**Step 2** Enter the **require apimgr** command.

**Example:**

```
config
   require apimgr
end
```

This CLI command is part of the boot configuration to spawn the new procedure.

### What to do next

1. Define ISE Server Profile
2. Associate ISE Server Profile

# Define ISE Server Profile

Use this procedure to define the ISE server profile.

**Note** Defining an ISE server profile is a mandatory configuration.

### Before you begin

Enable API Manager.

**Step 1** Enter the context EPC mode.

**Step 2** Enter the **ise-server-profile** *profile_name* command to specify a name for the ISE server profile.

To disable the ISE server profile, use the **no ise-server-profile** *profile_name* CLI command.

**Example:**

```
[local]UPF1(config)# context EPC
[local]UPF1(config-ctx)# ise-server-profile ise_1
```

The following is an example output of the **ise-server-profile** CLI command where the profile name is configured as *ise_1*.

```
[local]UPF1(config)# context EPC
  [local]UPF1(config-ctx)# ise-server-profile ise_1
      bind [ipv4-address <UPF-local-ip>] | [ipv6-address <UPF-local-ip>] port <local-port>
      server [ipv4-address <ISE-server-ip>] | [ipv6-address <ISE-server-ip>]
      username <userid> [encrypted] password <pass>
      policy-unavailable-treatment [pass | drop]
      certificate <client.cert.pem path>
      key <client.key.pem path>
      ca-certificate <ca.cert.pem path>
#exit
```

**Step 3** Enter the **bind [ ipv4-address** *ipv4_address* **| ipv6-address***ipv6_address***]** command to specify the bind IPv4 or IPv6 address.

- **ipv4_address** *ipv4_address* **port** : Designates an IPv4 address. *ipv4_address* must be in the *IPv4 ##.##.##.##* format. Specify the port of the IPv4 address.
- **ipv6_address** *ipv6_address* **port** : Designates an IPv6 address. *ipv6_address* must be in the *IPV6 ####:####:####:####:####:####:####:####* or with the **:: notation** format. Specify the port of the IPv6 address.

**Step 4** Enter the **ca-certificate** *ca_certificate_name_with_path* command to configure the CA certificate with complete path. *ca_certificate_name_with_path* must be a string of size 1–127. For example, */root/certificate/ca.cert.pem*.

**Step 5** Enter the **certificate** *certificate_name_with_path* command to to configure the SSL certificate name with complete path for the certificate. *certificate_name_with_path* must be a string of size 1–127. For example, */root/certificate/client/client.cert.pem* .

**Step 6** Enter the **key** *key_name_with_path* command to configure the key name along with the complete path. *key_name_with_path* must be a string of size 1–127. For example, */root/certificate/client/client.key.pem*.

**Step 7** Enter the **policy-unavailable-treatment [ drop | pass ]** command to specify the traffic treatment when the SGACL matrix is unavailable for a particular D-SGT.

- **drop**: Specify the downlink packets to be dropped.
- **pass**: Specify the downlink packets to be allowed to pass. This option is the default action.

**Step 8** Enter the **server [ ipv4_address** *ipv4_address* **| ipv6-address** *ipv6_address* command to specify the ISE server IPv4 or IPv6 address to which the UPF r.

- **ipv4_address** *ipv4_address* : Designate an IPv4 address. *ipv4_address* must be in the *IPv4 ##.##.##.##* format.
- **ipv6_address** *ipv6_address* : Designate an IPv6 address. *ipv4_address* must be in the *IPV6 ####:####:####:####:####:####:####:####* or with the **:: notation** format.

**Step 9** Enter the **username** *user_name* **[ encrypted | password** *password* **]** command to specify the ISE user name. *password* must be a string of size 1–128.

- **encrypted**: Designate the use of password encryption.
- **password** *password*: Configure the ISE server password. *password* must be a string of size 1–127.

**Step 10** Enter the **exit** command to exit the current configuration mode and return to the previous mode.

### What to do next

Associate ISE Server Profile

## Associate ISE Server Profile

Once defined, associate the ISE server profile with an existing UPF service configuration.

### Before you begin

Define ISE Server Profile

**Step 1** Enter the User Plane Service configuration mode.

**Step 2** Associate the defined ISE server profile with an existing UPF service configuration.

**Example:**

```
user-plane-service UPlane1
      associate ise-server-profile name ise_1
  #exit
```

## Refresh D-SGT Column

Each D-SGT column has a refresh timer that is configured in ISE. Based on the refresh timer configuration or through the UPF CLI trigger, the D-SGT column value is fetched from the ISE server again through the REST API query. Based on the API response from ISE, if the version of SGT matrix or SGACL is changed, UPF updates the respective matrix cell or SGACL information locally. The corresponding SGACLs are downloaded after the refresh, as required.

### Before you begin

1. Define ISE Server Profile
2. Associate ISE Server Profile

**Step 1** Enter the Exec Mode.

**Step 2** Enter the **refresh-sgt-column** *d_sgt* command to trigger the refresh of a D-SGT column by fetching the column values from the ISE server.

**Example:**

```
refresh-sgt-column <d-sgt>
```

**Note** Although the CLI returns immediately, the policy download in the background takes some time and hence the refresh completion may also take some time.

The following is an example output of the **refresh-sgt-column** *d_sgt* CLI command where the *d_sgt* value is configured as *65535*.

```
refresh-sgt-column 65535
```

# Monitoring and Troubleshooting

## Verify SGACL with SGT Integration

This section provides information about show commands and their outputs for the SGACL with SGT Integration feature.

### show subscribers user-plane-only full callid *callid_value*

The output of this CLI command is enhanced with the **SGT Value** field for displaying information related to D-SGT for ISE integration on UPF and **SGACL match stats** field for displaying information related to User Access Control through SGACL.

```
show subscribers user-plane-only full callid 00004e3a
   Local SEID      : [0x0004000000000003] 1125899906842627
  Remote SEID     : [0x00000436b7616206] 4633051357702
  State           : Connected

....

  input pkts: 20                                  output pkts: 16
  input bytes: 9246                               output bytes: 11248
  input bytes dropped: 0                          output bytes dropped: 5624
  input pkts dropped: 0                           output pkts dropped: 8

....

  SGT Value: 0x001a

....

QoS-Group Statistics:
QGR Name             Pkts-Down  Bytes-Down Pkts-Up    Bytes-Up   Hits       Match-Bypassed
  FP-Down(Pkts/Bytes)  FP-Up(Pkts/Bytes)
-------------------- ---------- ---------- ---------- ---------- ---------- --------------
  -------------------  -----------------
```

```
SGACL Match stats:
ACL Name             Pkts-Down  Bytes-Down Pkts-Up    Bytes-Up   Pkts dropped
-------------------- ---------- ---------- ---------- ---------- -------------
ACL2611                       4       1432          0          0             2
ACL2612                       4       4112          0          0             2
ACL2621                       8       5704          0          0             4
....

Total subscribers matching specified criteria: 1
```

## show subscribers user-plane-only callid *callid_value* flows full

The output of this CLI command is enhanced with the **Uplink SGT**, **Downlink SGT**, and **Matched SGACL** fields for displaying information related to User Access Control through SGACL.

```
show subscribers user-plane-only callid 00004e21 flows full
  Callid: 00004e21
  Interface Type: Sxab
  IP address: n/a

  Flow ID: 1:1
  Uplink pkts: 1                    Downlink pkts: 1
  Uplink bytes: 1040                Downlink bytes: 40
…
  Downlink Sfp Id: NA
  Uplink SGT: 0xA1
  Downlink SGT: 0xB5
  Matched SGACL: ACL_123
```

## show user-plane-service sgt-column summary

The output of this CLI command shows the summary of all the available D-SGT values on UPF along with their refresh timers as received from the ISE server.

The following example output shows the D-SGT values of **D-SGT Columns fetched** and **D-SGT Version** fields.

```
show user-plane-service sgt-column summary
 D-SGT Columns fetched:
 D-SGT Version
 ---------------------------------------
 65535 0
 7 0
 Total D-SGT column(s) found: 2
```

## show user-plane-service sgt-column dsgt

The output of this CLI command shows the summary of the SGACL matrix per D-SGT with the respective SGACL mapping per D-SGT and S-SGT, which are received from ISE during the D-SGT query.

The following example output shows the **D-SGT**, **Refresh TimeS-SGT**, **SGACL Name**, **Version**, and **Total SGT column(s) found** fields.

```
show user-plane-service sgt-column dsgt 26

    D-SGT: 26            Refresh Time: 86400
    S-SGT: 1
    SGACL Name           Version
    ---------------------------------------
    ACL2611                               0
    ACL2612                               0
```

```
  S-SGT: 2
  SGACL Name                      Version
  ---------------------------------------
  ACL2621                               0

Total SGT column(s) found: 1
```

## show user-plane-service sgacl name

The output of this CLI command shows the specific SGACLs definition rule lines as received from ISE during the SGACL query.

```
show user-plane-service sgacl name AACL2
 SGACL Name: AACL2
 permit ip
 Total SGACL(s) found: 1
```

## show user-plane-service statistics sgacl all

The output of this CLI command shows the packet match statistics as per SGACL.

```
show user-plane-service statistics sgacl all

ACL Name             Pkts-Down  Bytes-Down Pkts-Up    Bytes-Up   Pkts dropped
-------------------- ---------- ---------- ---------- ---------- -------------
SGACL1-REFRESH2         6           1156       0         0          2
SGACL1-REFRESH1        13           9344       0         0          6
Allow All               0              0       0         0          0

Total SGACL(s) : 3
```

## show user-plane-service statistics drop-counter

The output of this CLI command is enhanced to shows the dropped packets due to the SGACL application.

```
show user-plane-service statistics drop-counter
Packet Drop Data Statistics:
        -----------------------------------------------
...
        FastPath Misc Drops:
            Overload Protection:                    0
            Invalid Client:                         0
            Stream ID 0:                            0
            Invalid Stream ID:                      0
        OHR Mismatch Packet Drops:                  0
       SGACL Packet Drops:                       8
        SGACL No Policy Packet Drops:               2
        No Default SGT cell Packet Drops:           0
```

**Note**

- **No Default SGT cell Packet Drops** is an obsolete counter. The existing design allows packets to be passed only if no default ACL is available.
- The statistics for ISE server REST API request and response are supported.

## show apimgr statistics ise-server

The output of this CLI command shows UPFs API interaction with ISE server

```
show apimgr statistics ise-server

Ise-Server Connection Statistics:

Request sent:      4
Response Success:  4
Response Fail:     2
```

# OAM Support

### Bulk Statistics

Following new bulk statistics are supported for the user access control through SGACL feature.

| SCHEMA: UPF | |
|---|---|
| **Statistics** | **Description** |
| downlink-total-pkts-sgacl-matched | Total downlink packets matched against SGACL |
| downlink-total-bytes-sgacl-matched | Total downlink bytes matched against SGACL |
| downlink-total-pkts-sgacl-dropped | Total downlink packets dropped due to SGACL match |
| downlink-total-bytes-sgacl-dropped | Total downlink bytes dropped due to SGACL match |