Accessing TrustSec Operational Data Externally

Cisco TrustSec builds secure networks by establishing domains of trusted network devices. Each device in the domain is authenticated by its peers. Communication on the links between devices in the domain is secured with a combination of encryption, message integrity check, and data-path replay protection mechanisms.

Cisco TrustSec also provides security using group-based access control - access policies within the Cisco TrustSec domain are topology-independent, and are based on the roles of source and destination devices rather than on network addresses. Individual packets are tagged with the security group number of the source.

Cisco TrustSec produces two kinds of data - namely configuration data and operational data. Configuration data comes from the config programming model and the operational data comes from the operational data model.

It is possible to access TrustSec operational data from external applications that can handle data that is structured using YANG. Using the Netconf and Restconf protocol, the external device is able to extract operational information from Cisco devices - thereby providing programmability over an external interface.

Prerequisites for Accessing Cisco TrustSec Operational Data Externally

- An understanding of Cisco Trustsec, security tag propagation using SXP across network devices, and policy enforcement.
- Effective Cisco IOS XE Everest 16.5.1, Cisco TrustSec supports crypto k9 image with licenses for IP services or IP base only.
- The NETCONF or RESTCONF protocol should be enabled on the Cisco device. To enable the NETCONF protocol, use the command **netconf-yang** in the configuration mode.

Note The LANbase license supports only SXP; SGACL and IP-SGT operational data are not supported.

Restrictions for Accessing Cisco TrustSec Operational Data Externally

- Operation data limited to SGACL policy and IP-SGT & SXP connection can only be externally accessed.
- The below list of trustsec operational data is not supported in Cisco IOS XE Everest 16.5.1:
  - Cisco Trustsec PAC data, environment data and link-level operation data.
  - IPV6 based SGACL policy, IP-SGT mapping and SXP connection operational data.
  - VFR based IP-SGT mapping and SXP connection operational data.

Information About Cisco TrustSec Operational Data

Applications such as YTOOL provides users the flexibility to access Cisco TrustSec operational data from an external interface, without directly logging into Cisco devices to fetch the information using specific commands.

The following types of operational data can be accessed from an external device:

- The active SXP connections on a particular device.

  The following is a sample output to show SXP connections on a device:

```
Device# show cts sxp connections brief
 SXP              : Enabled
 Highest Version Supported: 4
 Default Password : Not Set
 Default Source IP: Not Set
Connection retry open period: 120 secs
Reconcile period: 120 secs
Retry open timer is running
Peer-Sequence traverse limit for export: Not Set
Peer-Sequence traverse limit for import: Not Set

---------------------------------------------------------------------------------------------------
---------------
Peer_IP          Source_IP        Conn Status
 Duration
---------------------------------------------------------------------------------------------------
---------------
10.10.1.1        11.11.1.1        Off
 0:00:36:24 (dd:hr:mm:sec)
10.10.1.2        11.11.1.2        Off
 0:00:36:24 (dd:hr:mm:sec)
10.10.1.3        11.11.1.3        Off
 0:00:36:23 (dd:hr:mm:sec)
10.10.1.4        11.11.1.4        Off
 0:00:36:22 (dd:hr:mm:sec)
10.10.1.5        11.11.1.5        Off
 0:00:36:22 (dd:hr:mm:sec)
10.10.1.6        11.11.1.6        Off
 0:00:36:21 (dd:hr:mm:sec)
10.10.1.7        11.11.1.7        Off
 0:00:36:21 (dd:hr:mm:sec)
```

```
10.10.1.8        11.11.1.8        Off
 0:00:36:20 (dd:hr:mm:sec)
10.10.1.9        11.11.1.9        Off
 0:00:36:15 (dd:hr:mm:sec)
10.10.1.10       11.11.1.10       Off(Speaker)::Off(Listener)
 0:00:33:40 (dd:hr:mm:sec)::0:00:33:40 (
dd:hr:mm:sec)
```

- The IP-SGT mapping information.

  Every source IP is mapped with the corresponding SGT and an IP-SGT binding is created. This mapping information is stored in the Role-Based Manager (RBM) database.

  The following is a sample output to show IP-SGT mapping information:

```
Device# show cts role-based sgt-map all
Active IPv4-SGT Bindings Information

IP Address              SGT     Source
============================================
10.10.10.10             10      CLI
20.20.20.20             20      CLI
30.30.30.30             30      CLI
32.1.1.32               40      CLI
45.1.1.45               100     CLI
69.1.1.1                103     CLI

IP-SGT Active Bindings Summary
============================================
Total number of CLI      bindings = 6
Total number of active   bindings = 6

asr1k-cts-2006#
```

- Names of the policies that are currently applied for every data path.

  SGACL policies are enforced when SGT-tagged packets are transported between two trustsec-aware end points. A policy can either be static or dynamic. Policies that are configured on the device using the CLI command **cts role-based permissions** are static policies. Dynamic policies are configured on CISCO ISE (Identiy Services Engine). Dynamic policies take precedence over static policies. A static policy is enforced only in the absence of a dynamic policy.

  The following is a sample output to show policies for SGT-tagged traffic:

```
Device# show cts role-based permissions
IPv4 Role-based permissions default:
        Permit IP-00
IPv4 Role-based permissions from group 10:SGT_10 to group 10:SGT_10:
        Collab1-10
IPv4 Role-based permissions from group 10:SGT_10 to group 20:SGT_20:
        SGACL_2-30
IPv4 Role-based permissions from group 11:SGT_11 to group 20:SGT_20:
        SGACL_2-30
        SGACL_3-10
        SGACL_4-90
IPv4 Role-based permissions from group 12:SGT_12 to group 20:SGT_20:
        SGACL_3-10
IPv4 Role-based permissions from group 13:SGT_13 to group 20:SGT_20:
        SGACL_4-90
IPv4 Role-based permissions from group 14:SGT_14 to group 20:SGT_20:
        SGACL_5-20
IPv4 Role-based permissions from group 15:SGT_15 to group 20:SGT_20:
        SGACL_6-30
```

```
IPv4 Role-based permissions from group 16:SGT_16 to group 20:SGT_20:
        SGACL_101-90
IPv4 Role-based permissions from group 17:SGT_17 to group 20:SGT_20:
        SGACL_2-30
IPv4 Role-based permissions from group 18:SGT_18 to group 20:SGT_20:
        SGACL_3-10
IPv4 Role-based permissions from group 19:SGT_19 to group 20:SGT_20:
        SGACL_3-10
IPv4 Role-based permissions from group 10:SGT_10 to group 30:SGT_30:
        SGACL_6-30
IPv4 Role-based permissions from group 10:SGT_10 to group 40:SGT_40:
        SGACL_2-30
IPv4 Role-based permissions from group 10:SGT_10 to group 100:SGT_100:
        SGACL_4-90
IPv4 Role-based permissions from group 102:SGT_102 to group 100:SGT_100:
        Permit IP-00
IPv4 Role-based permissions from group 102:SGT_102 to group 103:SGT_103:
        SGACL_2-30
RBACL Monitor All for Dynamic Policies : FALSE
RBACL Monitor All for Configured Policies : FALSE

asr1k-cts-2006#
```

- The contents of each policy - which includes the ACEs (Access Control Entries) in the policy, and the lifetime and refresh time of the policy.

  A policy can have upto a combination of 256 ACEs. Lifetime and refresh time information is only applicable to dynamic policies. The lifetime and refresh time value for a static policy is 0.

  The following is a sample output to show policies for SGT-tagged traffic (only a part of the output is displayed):

```
Device# show cts policy sgt
CTS SGT Policy
==============
RBACL Monitor All : FALSE
RBACL IP Version Supported: IPv4
SGT: 0-02:Unknown
SGT Policy Flag: 0x41408001
RBACL Source List: Empty
RBACL Destination List: Not exist
RBACL Multicast List: Not exist
RBACL Policy Lifetime = 1800 secs
RBACL Policy Last update time = 15:56:42 IST Mon Feb 20 2017
Policy expires in 0:00:03:04 (dd:hr:mm:sec)
Policy refreshes in 0:00:03:04 (dd:hr:mm:sec)
Cache data applied = NONE

SGT: 65535-52:ANY
SGT Policy Flag: 0x41400001
RBACL Source List:
  Source SGT: 65535-52:ANY-0, Destination SGT: 65535-52:ANY-0
  rbacl_type = 80
  rbacl_index = 1
  name   = Permit IP-00
  IP protocol version = IPV4
  refcnt = 4
  flag   = 0x41000000
  stale  = FALSE
  RBACL ACEs:
    permit ip
```

```
RBACL Destination List: Not exist
RBACL Multicast List: Not exist
RBACL Policy Lifetime = 1800 secs
RBACL Policy Last update time = 15:56:43 IST Mon Feb 20 2017
Policy expires in 0:00:03:05 (dd:hr:mm:sec)
Policy refreshes in 0:00:03:05 (dd:hr:mm:sec)
Cache data applied = NONE

SGT: 10-2770:SGT_10
SGT Policy Flag: 0x41400001
RBACL Source List:
  Source SGT: 10-2770:SGT_10-0, Destination SGT: 10-2770:SGT_10-0
  rbacl_type = 80
  rbacl_index = 1
  name   = Collab1-10
  IP protocol version = IPV4
  refcnt = 2
  flag   = 0x41000000
  stale  = FALSE
  RBACL ACEs:
    permit ip

RBACL Destination List: Not exist
RBACL Multicast List: Not exist
RBACL Policy Lifetime = 1800 secs
RBACL Policy Last update time = 15:56:43 IST Mon Feb 20 2017
Policy expires in 0:00:03:04 (dd:hr:mm:sec)
Policy refreshes in 0:00:03:04 (dd:hr:mm:sec)
Cache data applied = NONE

SGT: 20-44:SGT_20
SGT Policy Flag: 0x41400001
RBACL Source List:
  Source SGT: 10-2770:SGT_10-0, Destination SGT: 20-44:SGT_20-0
  rbacl_type = 80
  rbacl_index = 1
  name   = SGACL_2-30
  IP protocol version = IPV4
  refcnt = 8
  flag   = 0x41000000
  stale  = FALSE
  RBACL ACEs:
    permit ip

  Source SGT: 12-17:SGT_12-0, Destination SGT: 20-44:SGT_20-0
  rbacl_type = 80
  rbacl_index = 2
  name   = SGACL_3-10
  IP protocol version = IPV4
  refcnt = 5
  flag   = 0x41000000
  stale  = FALSE
  RBACL ACEs:
    permit ip

  Source SGT: 13-14:SGT_13-0, Destination SGT: 20-44:SGT_20-0
  rbacl_type = 80
  rbacl_index = 3
  name   = SGACL_4-90
  IP protocol version = IPV4
  refcnt = 5
  flag   = 0x41000000
  stale  = FALSE
  RBACL ACEs:
```

```
  deny tcp

Source SGT: 14-14:SGT_14-0, Destination SGT: 20-44:SGT_20-0
rbacl_type = 80
rbacl_index = 4
name   = SGACL_5-20
IP protocol version = IPV4
refcnt = 2
flag   = 0x41000000
stale  = FALSE
RBACL ACEs:
  permit ip

Source SGT: 15-1410:SGT_15-0, Destination SGT: 20-44:SGT_20-0
rbacl_type = 80
rbacl_index = 5
name   = SGACL_6-30
IP protocol version = IPV4
refcnt = 4
flag   = 0x41000000
stale  = FALSE
RBACL ACEs:
  permit icmp log
  permit udp log
  permit tcp log

Source SGT: 16-14:SGT_16-0, Destination SGT: 20-44:SGT_20-0
rbacl_type = 80
rbacl_index = 6
name   = SGACL_101-90
IP protocol version = IPV4
refcnt = 2
flag   = 0x41000000
stale  = FALSE
RBACL ACEs:
  permit ip
```

How to Configure the External Device YTOOL

Before you configure the YTOOL, ensure that the NETCONF or RESTCONF protocol is enabled on the Cisco device. One of these protocols is required for the YTOOL to communicate with the Cisco device.

Note To enable the NETCONF protocol, use the command **netconf-yang** in the configuration mode. After enabling NETCONF, execute the CLI **show onep session all** to check if the three processes that are needed to use Netconf are running. Netconf is usable only after these three processes are running.

Also, identify the IP address that you are going to use for communicating with the device.

Note YTOOL is also known as yang-explorer. You can download this application from the following location:

Yang Explorer at

To connect the YTOOL to a Cisco device, add the Cisco device in the YTOOL. Steps to add a Cisco device in the YTOOL:

1. Open YTOOL
2. Select **Admin**
3. On the **Ytool Utilities** page, select **Manage Profiles** (under **Manage Device Profiles**)
4. Choose **New Device** from the **Device Profile Name** dropdown
5. On the **Manage Device Profile** page, provide all the details of the device such as **Test Device IP Address, Test Device SSH Port Number, Netconf Username, NetConf Password** etc.

   Figure 1: Manage Device Profile

6. To check the connectivity to the device, navigate to **Build** > **Device Settings**. Select your device from **Profile** and click **Hello**. If you see a response under **Console**, it implies that the YTOOL is able to communicate with the device.

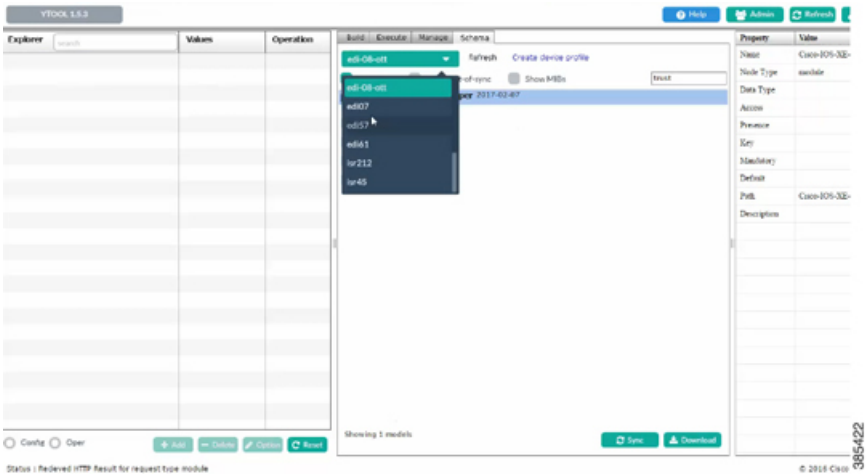
Note To communicate with Cisco devices, you can choose other external applications that can handle data that is structured using YANG. This section is relevant only if you have selected YTOOL to access Cisco devices.

Accessing Operational Data

Before you begin, ensure that the Cisco device from which you are going to extract operational data is configured on the YTOOL. See the "How to Configure the External Device YTOOL" section for details.

1. Download the Cisco TrustSec operational information schema from the Cisco device:
   a. Select **Schema**.
   b. Select the device. The list of schemas in the device will be displayed.

Figure 2: Select a Device

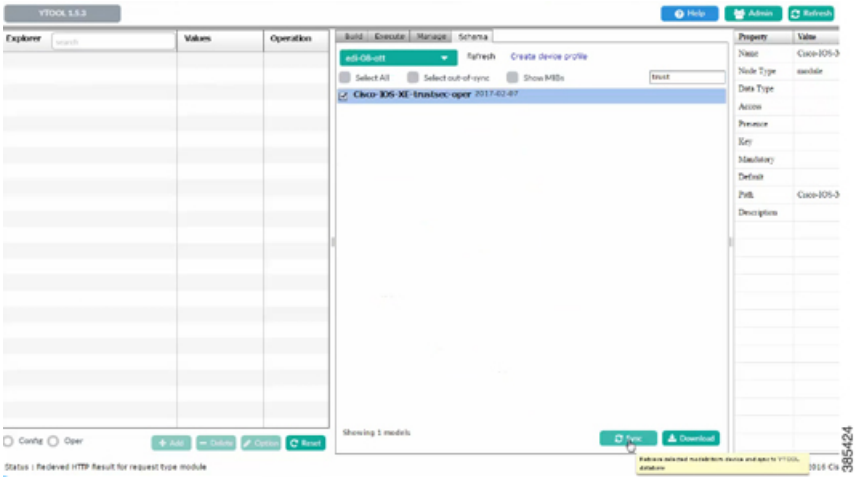


c. Select the Cisco TrustSec operational information schema. Use the search box to search for this schema.

Note The name of an operational information schema ends with **oper**.

d. Click **Sync**. The schema is downloaded into the YTOOL.

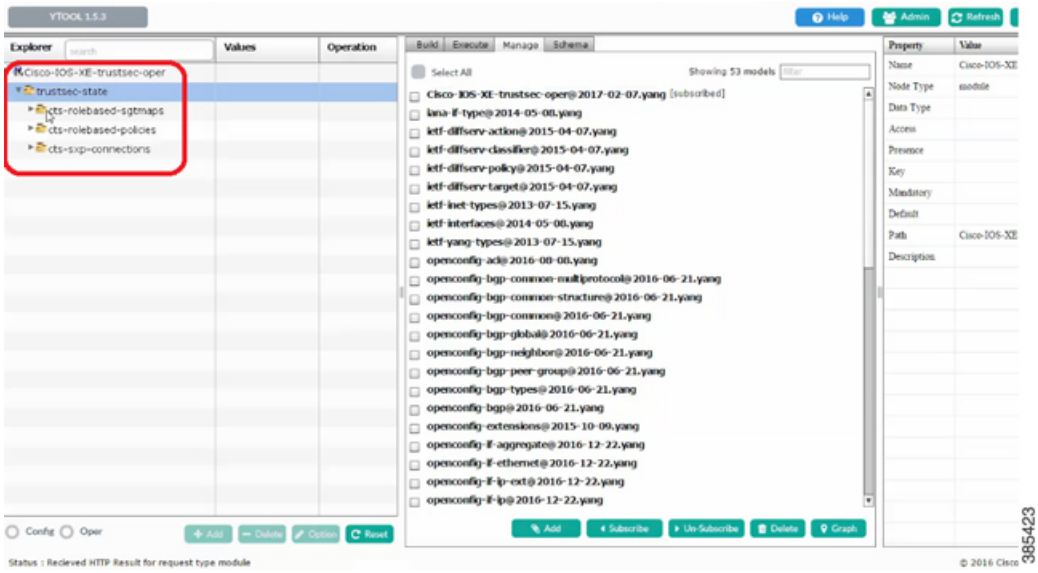
Figure 3: Download Schema



2. Subscribe to the downloaded operational information schema on YTOOL.
   a. Select **Manage**.
   b. From the list of schemas, select the operational information schema.
   c. Click **Subscribe**.

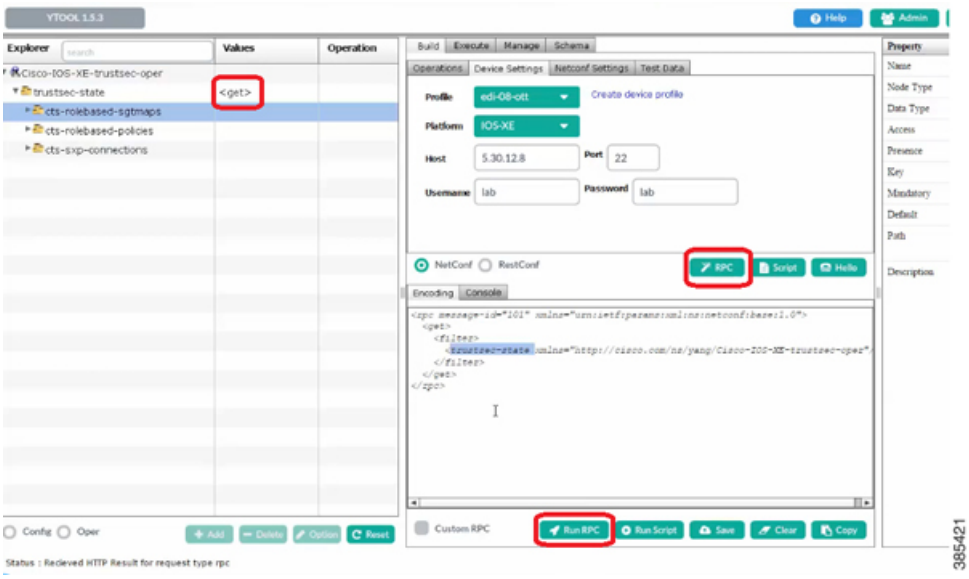
Note Once you have subscribed, the schema will be displayed under explorer.

Figure 4: Subscribe Schema



3. Retrieve selected operational data using the schema:
   a. Against the relevant information level of the operation information schema, select **get** under **values** .
   b. Click **RPC**. An XML generated RPC message will be generated.
   c. Click **Run RPC**. The operation data is retrieved from the Cisco device in the RPC-generated XML format.

Figure 5: Retrieve Operational Data



Note For information on the commands that are used to access operational data, see the section Information About Cisco TrustSec Operational Data, on page 2.

Note To communicate with Cisco devices, you can choose other external applications that can handle data that is structured using YANG. This section is relevant only if you have selected YTOOL to access Cisco devices.