SGACL and Environment Data Download over REST

This module describes the downloading of SGACL and environment data over REST APIs.

- Prerequisites for SGACL and Environment Data Download over REST, on page 1
- Restrictions for SGACL and Environment Data Download over REST, on page 1
- Information About SGACL and Environment Data Download over REST, on page 2
- How to Configure SGACL and Environment Data Download over REST, on page 7
- Verifying the SGACL and Environment Data Download over REST, on page 11
- Debugging the SGACL and Environment Data over REST Configuration, on page 12
- Configuration Examples for SGACL and Environment Data Download over REST, on page 13
- Feature History for SGACL and Environment Data Download over REST, on page 13

Prerequisites for SGACL and Environment Data Download over REST

- Cisco Identity Services Engine (ISE) Version should be 2.7 and above.
- Cisco TrustSec-enabled devices must use Cisco IOS XE Amsterdam 17.1.1 and later releases.
- The network device configuration on Cisco ISE must be updated to include the configuration to allow REST API calls from a network device IP address (NAS-IP). The device ID and password specified in the Cisco ISE configuration is included as the username and password by the network device that makes REST API calls to Cisco ISE.

Restrictions for SGACL and Environment Data Download over REST

- Cisco TrustSec Change of Authorization (CoA) uses RADIUS as the protocol.
- Only port 9063 is supported as the ERS server port.
- Server statistics is not persistent after a refresh of the environment data.

- Only one Fully Qualified Domain Name (FQDN) per server is supported.
- RADIUS Automated Testing feature is not supported in a VRF environment.
- For RADIUS, policy download over IPv6 server is not supported.

Information About SGACL and Environment Data Download over REST

SGACL and Environment Data Download over REST Overview

Cisco TrustSec uses the REST-based transport protocol for policy provisioning and environment data download from Cisco Identity Services Engine (ISE). The REST-based protocol is more secure, and provides reliable, and faster Security Group access control list (SGACL) policy and environment data provisioning, than older RADIUS protocols.

Both the REST API-based and RADIUS-based download of Cisco TrustSec data is supported. However, only one protocol can be active on a device. REST-based protocol is the default, however, you can change the protocol to RADIUS by configuring the **cts authorization list** command.

Note Cisco TrustSec Change of Authorization (CoA) will still use RADIUS as the protocol.

Cisco TrustSec Security Group Access Control List (SGACL) and environment data are synchronized from the active device to the standby device, after the policy is installed. However, REST API connections or sessions are not synchronized during a switchover.

8 IPv4 and 8 IPv6 addresses are supported per server. Cisco TrustSec device honors the 429 response code from Cisco ISE. This response code is sent by Cisco ISE, when it is overloaded. Once a 429 response code is received for a particular server, the device marks the server as dead, and switches to the next server in the list (private or public). The next retry attempt is done after 60 seconds.

Note Certain device configurations and protocols are identified as insecure and pose a security risk to Cisco devices. While existing deployments continue to function, you must intentionally enable these features for new installations. For more information on remediation, refer to Cisco C9000 Switching IOS XE – Resilient Infrastructure Playbook.

Cisco TrustSec Environment Data

Environment data comprises of operational data that supplement Cisco TrustSec functions. The environment data request from a device to Cisco ISE consists of the following data:

- Device name: Specifies the name of the device.
- Device capability: Specifies additional data.

The environment data response from Cisco ISE to a device consists of the following data:

- Device security group tag (SGT): Derived from Cisco ISE based on the device name.
- Server list: Displays the list of Cisco TrustSec servers specified in Cisco ISE.
- SG-Name Table: Displays the mapping between SGT and the device name. SGT is displayed in numerals and the device name in text format.
- Refresh time: Indicates the time when the environment data will be refreshed.

Note

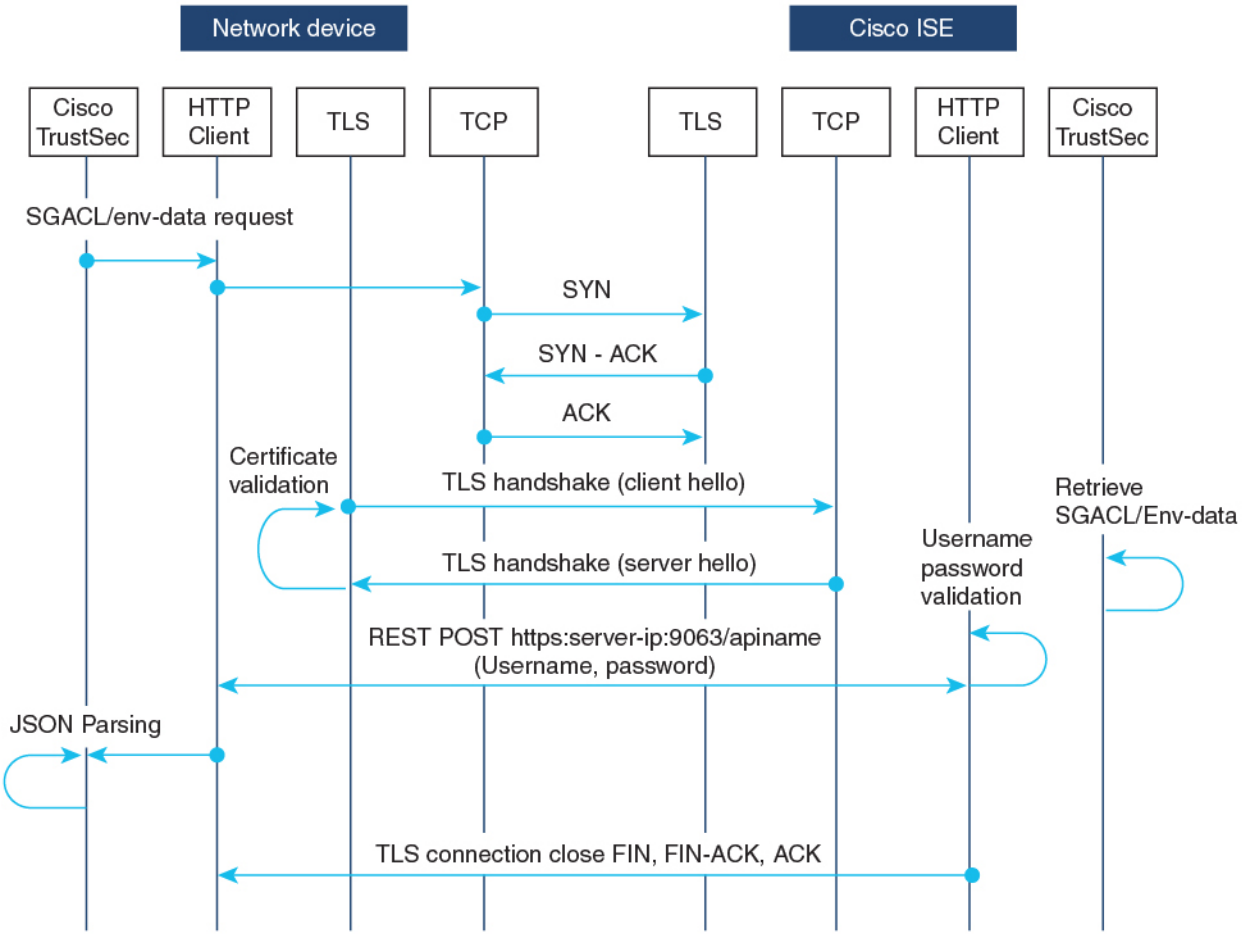
- As part of Cisco TrustSec environment data refresh, the last received servers are deleted and newly received servers are added to the server list. As a result of the refresh, the server list statistics restarts from zero, and the server status is set to *Inactive* and the IP address state is set to *Reachable*. The device then updates the server statistics and status based on the subsequent policy request and response.
- Starting with Cisco IOS XE Bengaluru 17.4.1, you can configure automated tester to be VRF aware. You can use the **vrf** keyword with the **automate-tester** command to enable automate-tester for a non-default VRF.

  For VRF aware automate-tester to work, you have to configure **global config ipv4/ipv6 source interface** *interface-name* **vrf** *vrf-name* command.

Message Flow Between a Network Device and a Server

The following illustration displays the connection management for REST calls between a network device and server.

Figure 1: Message Flow Between a Network Device and a Server



- Cisco ISE REST API service runs on a secure socket that runs Transport Layer Security (TLS) 1.2 server on port 9063 to service network device requests for SGACL and environment data.
- The device uses a make or break approach to the TLS connection establishment, and there is no persistent TLS connection between the device and Cisco ISE. After the TLS connection is established, the device can use this connection to submit multiple REST API calls to specific resource uniform resource locators (URLs). After all REST requests are processed, the server terminates the connection through a TCP-FIN message. For new REST API calls a new connection must be established with the server.
- The REST API call from the device to Cisco ISE starts with a TCP connection establishment. Cisco ISE must be configured with device IP address to allow ingress connections from the device. TCP connection requests from source IP addresses that are not configured on Cisco ISE are dropped, and an audit log created.
- Username and password: Every RESTAPI call must include the username and password authentication while requesting access to a resource uniform resource identifier (URI). The authentication helps the server to determine if the caller should be given access to the resource or to deny the request.
- A successful TLS connection establishment with Cisco ISE requires its server-certificate signature or PEM to be installed as the trustpoint (by using the **crypto pki trustpoint** command) on the device to

trust the server. Only fingerprint or signature of the server certificate need to be exported and installed on the device under a trustpoint. Import of private-key of the server certificate is not necessary.

- After establishing the TLS connection, the HTTP client on the device initiates a REST call to Cisco ISE on the specified resource.

Policy Server Selection Criteria

Multiple HTTP policy servers are configured on a Cisco TrustSec device. Once a server is selected, the device use this server to interact with Cisco ISE until the server is marked as dead.

There are two types of server selection:

- In-Order Selection: This is the default behavior, where servers are picked in the order in which they are configured (from the public server list) or downloaded (from the private server list). Once a server is selected, the device is used till it is marked as dead, and then the next server in the list is selected.

  When environment data is successfully downloaded, and a server-list is available, these servers are added to the private server list.

- Random Server-Selection: When multiple HTTP policy servers are configured on a device, a single Cisco ISE instance may get overloaded if the device always selects the first configured server. To avoid this situation, each device will randomly select a server. A random number is generated by the device and based on this number a server is selected. For different devices to generate random numbers, the unique board ID and the Cisco TrustSec process ID of the device is used to initialize the random number generator.

  Once a server is selected, all future requests go this server until the server is marked as dead. Once a server is in the dead state, the random server selection logic picks up the next alive server. The dead server is not added to the count of active servers when picking the new server. The server numbering starts with zero.

  Selected Server = (Generated Random Number) % (Total Number of Active Servers).

To change the server selection logic to random, use the **cts policy-server order random** command.

Server and IP Address Selection Process

The order of server-selection is the private server-list (received as part of server-list download), followed by the public server-list (configured servers). Within these server lists, the order can either be random selection or in-order selection based on whether the **cts policy-server order random** command is enabled or not.

In Cisco IOS XE 17.2.1 and later releases, multiple IP (both IPv4 and IPv6) addresses per server are supported. The order of IP selection is IPv4 addresses, followed by IPv6 addresses, and then FQDN.

This section describes how the server and IP address selection works:

1. When a device boots up for the first time, a server from the public (configured) list is selected.
2. If the **cts environment-data enable** command is configured, the device uses the public server to download the private server-list from Cisco ISE.
3. After successfully receiving the private list, all subsequent requests will use the private list.
4. After the server and IP address are selected, the device connects to Cisco ISE using the server/IP address combination. This server will interact with Cisco ISE until it fails to get a response.

5. If no response is received from the current active server in the private list, the device switches to the next server in the list. If the server is selected for the first time, the IP selection logic searches for the first reachable IP or IPv6 address.
6. After the server and IP address selection, the device is used until it goes down.
7. If none of the servers in the private list are reachable, the device attempts to connect to the servers in the public list. The server switching logic and IP selection are the same for private and public list.
8. The server change happens only when the server list is refreshed.
9. If all servers in both the private and public server list are dead, the device restarts the server/IP address selection logic from the start of the private list.
10. When a specific server/IP address combination fails, the device waits for 60 seconds before it attempts a new combination.

Server Liveliness Check

Whether a server is alive is determined after sending an environment-data or an SGACL request to Cisco ISE. There is no liveliness detection phase after a server is configured or downloaded as part of a server list. The default server status is alive for all types of servers.

When a request is sent to Cisco ISE, and if the server is not reachable or the response is lost, the server is moved to dead state. The server selection logic will pick the same server and the next IP address (if multiple addresses are configured) to send the next set of Cisco ISE requests. The logic will pick the next server in the list, if the device receives the overloaded response (HTTP 429) from Cisco ISE.

A server can be marked as dead because of any of the following reasons:

- The configured IP address is not reachable.
- Incorrect port number.
- The Cisco ISE instance with the IP address is down.
- The interface towards Cisco ISE is down.
- A Transport Layer Security (TLS) handshake failure.
- An HTTP response timeout.
- An incorrectly configured domain name (if a domain name is used).

If a server has both the static IP address and the domain name configured, preference is given to the static IP address. If there is no response to the static IP address, the device tries with the domain name. When no response is received with both the static IP address and the domain-name, the server is marked as dead.

When all servers of the private list are marked as dead, the device uses the public list. If all remaining servers are also marked as dead, then the recovery mechanism starts. The device waits for the next Cisco TrustSec request (for policy refresh, environment data download or refresh, and so on), and marks all the servers as alive to retry the download. If there is no trigger for a new Cisco TrustSec request, the servers remain in the dead state.

How to Configure SGACL and Environment Data Download over REST

Configuring the Username and Password

Configure the username and password in Cisco ISE as the REST API access credentials, before configuring it on the device. See the Cisco TrustSec HTTP Servers section of the "Cisco TrustSec Policies Configuration" chapter for more information.

Note If you try to configure RADIUS-based configuration by using the **cts authorization-list** command, when the HTTP-based configurations are already enabled, the following error message is displayed on the console:

```
Error: 'cts policy-server or cts environment-data' related configs are enabled.
Disable http-based configs, to enable 'cts authorization'
```

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 policy-server name** *server-name* **Example:** `Device(config)# cts policy-server name ISE-server`	Configures a Cisco TrustSec policy server and enters policy-server configuration mode.
Step 4	**exit** **Example:** `Device(config-policy-server)# exit`	Exits policy-server configuration mode and returns to global configuration mode.
Step 5	**cts policy-server username** *username* **password** {**0** | **6** |**7** | *password*} {*password*} **Example:** `Device(config)# cts policy-server username admin password 6 password1`	Configures an username and password. **Note** This username and password must be created on Cisco ISE as the REST API access credentials before configuring it on the device.

	Command or Action	Purpose
Step 6	**end** **Example:** `Device(config)# end`	Exits global configuration mode and returns to privileged EXEC mode.

Configuring Certificate Enrollment

Third-party Certificate Authority (CA) certificate and chain of certificates are supported. Perform the following steps to enrol a certificate:

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	**crypto pki trustpoint** *name* **Example:** `Device(config)# crypto pki trustpoint mytp`	Declares the trustpoint and a given name, and enters ca-trustpoint configuration mode.
Step 4	**exit** **Example:** `Device(ca-trustpoint)# exit`	Exits ca-trustpoint configuration mode and returns to global configuration mode.
Step 5	**crypto pki authenticate** *name* **Example:** `Device(config)# crypto pki authenticate mytp`	Retrieves the Certificate Authority (CA) certificate and authenticates it. Check the certificate fingerprint if prompted. **Note** This command is optional if the CA certificate is already loaded into the configuration.
Step 6	**end** **Example:** `Device(config)# end`	Exits global configuration mode and returns to privileged EXEC mode.

Downloading Cisco TrustSec Policies

The **cts role-based enforcement** must already be configured to download Cisco TrustSec Policies.

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 policy-server name** *server-name* **Example:** `Device(config)# cts policy-server name ISE-server`	Configures a Cisco TrustSec policy server and enters policy-server configuration mode.
Step 4	**address domain-name** *name* **Example:** `Device(config-policy-server)# address domain-name domain1`	Configures the domain name address of the policy server.

Step 5	**address** {**ipv4**| **ipv6** *policy-server-address*
	Example:
	`Device(config-policy-server)# address ipv4 10.1.1.1`
	`Device(config-policy-server)# address ipv6 2001.DB8::1`
		Configures the IPv4 or IPv6 address of the policy server.
		• In Cisco IOS XE Amsterdam 17.1.1, only IPv4 addresses are supported.

Step 6	**tls server-trustpoint** *name* **Example:** `Device(config-policy-server)# tls server-trustpoint tls1`	Configures the Transport Layer Security trustpoint.
Step 7	**timeout** *seconds* **Example:** `Device(config-policy-server)# timeout 15`	(Optional) Configures the response timeout in seconds. • The default is 5 seconds.
Step 8	**retransmit** *number-of-retries* **Example:** `Device(config-policy-server)# retransmit 4`	(Optional) Configures the maximum number of retries from the server. • The default is 4.

	Command or Action	Purpose
Step 9	**port** *port-number* **Example:** `Device(config-policy-server)# port 9063`	(Optional) Configures the policy server port number. **Note** The ERS server port number must be 9063. You cannot change this port number.
Step 10	**content-type json** **Example:** `Device(config-policy-server)# content-type json`	(Optional) Configures the content type to source SGACL and environment data from Cisco ISE. **Note** By default, JSON is used as the content type, even if this command is not configured.
Step 11	**end** **Example:** `Device(config-policy-server)# end`	Exits policy-server configuration mode and returns to privileged EXEC mode.

Downloading Environment Data

The source interface to use for HTTP connections must be specified in the **ip http client source-interface** command.

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 policy-server device-id** *device-ID* **Example:** `Device(config)# cts policy-server device-id server1`	Configures the policy server device ID to send environment data requests to Cisco ISE. • This device-ID must be the one used to add the network access device (NAD) on Cisco ISE.
Step 4	**cts environment-data enable** **Example:** `Device(config)# cts environment-data enable`	Enables the downloading of environment data from Cisco ISE. **Note**

	Command or Action	Purpose
		The **cts environment-data enable** command and the **cts authorization list** command are mutually exclusive. These commands cannot be configured together.
Step 5	**end** **Example:** `Device(config)# end`	Exits global configuration mode and returns to privileged EXEC mode.

Verifying the SGACL and Environment Data Download over REST

Use the following commands in any order:

- **show cts policy-server details name**

  Displays information about the specified policy server.

```
Device# show cts policy-server details name ise_server_1

Server Name   : ise_server_1
Server Status : Active
  IPv4 Address     : 10.64.69.84
  IPv6 Address     : 2001:DB::2
  Trustpoint       : ISE84
  Port-num         : 9063
  Retransmit count : 3
  Timeout          : 15
  App Content type : JSON
```

- **show cts policy-server statistics active**

  Displays statistics information about active policy servers.

  When you use the command without the **active** the statistics of all servers are listed.

```
Device# show cts policy-server statistics active

Server Name  : ise_server_1
Server State : ALIVE
  Number of Request sent        : 7
  Number of Request sent fail   : 0
  Number of Response received   : 4
  Number of Response recv fail  : 3
    HTTP 200 OK                 : 4
    HTTP 400 BadReq             : 0
    HTTP 401 UnAuthorized Req   : 0
    HTTP 403 Req Forbidden      : 0
    HTTP 404 NotFound           : 0
    HTTP 408 ReqTimeout         : 0
    HTTP 415 UnSupported Media  : 0
    HTTP 500 ServerErr          : 0
    HTTP 501 Req NoSupport      : 0
    HTTP 503 Service Unavailable: 0
    TCP or TLS handshake error  : 3
```

```
    HTTP Other Error            : 0
```

- **show cts server-list**

  Displays the list of servers that are downloaded as part of the environment data. These servers will be part of private server-list.

Note The following output displays the HTTP-based download information:

```
Device# show cts server-list

HTTP Server-list:
  Server Name      : cts_private_server_0
  Server State     : ALIVE
  IPv4 Address     : 10.64.69.151
  IPv6 Address     : 2001:DB8:8086:6502::
  IPv6 Address     : 2001:db8::2
  IPv6 Address     : 2001:db8::402:99
  IPv6 Address     : 2001:DB8:4::802:16
  Domain-name      : ise-267.cisco.com
  Trustpoint       : cts_trustpoint_0

  Server Name      : cts_private_server_1
  Server State     : ALIVE
  IPv4 Address     : 10.10.10.3
  IPv4 Address     : 10.10.10.2
  IPv6 Address     : 2001:DB8::20
  IPv6 Address     : 2001:DB8::21
  Domain-name      : www.ise.cisco.com
  Trustpoint       : cts_trustpoint_1
```

Debugging the SGACL and Environment Data over REST Configuration

Use the following **debug** commands for debugging the configuration.

- **debug cts policy-server http**

  Enables HTTP client debugging.

- **debug cts policy-server json**

  Enables JSON client debugging.

Configuration Examples for SGACL and Environment Data Download over REST

Example: Configuring the Username and Password

```
Device> enable
Device# configure terminal
Device(config)# cts policy-server name ISE-server
Device(config-policy-server)# exit
Device(config)# cts policy-server username admin 6 password1
Device(config)# end
```

Example: Downloading Cisco TrustSec Policies

```
Device> enable
Device# configure terminal
Device(config)# cts role-based enforcement
Device(config)# cts policy-server name ISE-server
Device(config-policy-server)# address domain-name domain1
Device(config-policy-server)# address ipv4 10.1.1.1
Device(config-policy-server)# address ipv6 2001:DB8::1
Device(config-policy-server)# tls server-trustpoint tls1
Device(config-policy-server)# timeout 15
Device(config-policy-server)# retransmit 4
Device(config-policy-server)# port 2010
Device(config-policy-server)# end
```

Example: Downloading Environment Data

```
Device> enable
Device# configure terminal
Device(config)# cts policy-server name ISE-server
Device(config-policy-server)# exit
Device(config)# cts policy-server device-id server1
Device(config)# cts env-data enable
Device(config)# end
```

Feature History for SGACL and Environment Data Download over REST

This table provides release and related 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	Feature Information
Cisco IOS XE Amsterdam 17.1.1	SGACL and Environment Data Download over REST	Cisco TrustSec uses the REST-based transport protocol for SGACL policy provisioning and data download from Cisco ISE.
Cisco IOS XE Amsterdam 17.2.1	HTTP SGACL Enforcement with IPv6 Policy Server	IPv6 addresses for policy servers are supported.
Cisco IOS XE Cupertino 17.7.1	SGACL and Environment Data Download over REST	This feature was implemented on Cisco Catalyst 9600 Series Supervisor 2 Module (C9600X-SUP-2)..
Cisco IOS XE Cupertino 17.7.1	SGACL and Environment Data Download over REST HTTP SGACL Enforcement with IPv6 Policy Server	This feature was implemented on supervisor modules C9400X-SUP-2 and C9400X-SUP-2XL.
Cisco IOS XE 26.1.1	CTS policy server list enablement over RADIUS for IPv6	Introduced the support for CTS policy server list enablement over RADIUS for IPv6.

Use the Cisco Feature Navigator to find information about platform and software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn.