Configure TrustSec SGT SXP Propagation in SD-WAN

Contents

Introduction

Prerequisites

- Requirements
- Components Used

Background Information

- Cisco TrustSec Integration
- SGT Propagation Methods
- SGT Propagation with SXP

Enable SGT SXP Propagation and Download SGACL Policies

- Step 1. Configure the Radius Parameters
- Step 2. Configure the SXP Parameters

Verify

Related Information

Introduction

This document describes Security Group Tag Exchange Protocol (SXP) Propagation method configuration in Software-Defined Wide-Area Networks (SD-WAN).

Prerequisites

Requirements

Cisco recommends that you have knowledge of these topics:

- Cisco Catalyst Software-Defined Wide Area Network (SD-WAN)
- Software-Defined Access (SD-Access) Fabric
- Cisco Identify Service Engine (ISE)

Components Used

The information in this document is based on:

- Cisco IOS® XE Catalyst SD-WAN Edges version 17.9.5a
- Cisco Catalyst SD-WAN Manager version 20.12.4.

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, ensure that you understand the potential impact of any command.

Background Information

Cisco TrustSec Integration

SGT Propagation with Cisco TrustSec Integration is supported by Cisco IOS® XE Catalyst SD-WAN Release 17.3.1a and onwards. This feature enables Cisco IOS® XE Catalyst SD-WAN edge devices to propagate Security Group Tag (SGT) inline tags that are generated by Cisco TrustSec-enabled switches in the branches to other edge devices in the Cisco Catalyst SD-WAN network.

Basic concepts of Cisco TrustSec:

- SGT Bindings: Association between IP and SGT, all bindings have the most common configuration and learn directly from the Cisco ISE.
- SGT Propagation: The propagation methods are used to propagate these SGTs between network hops.
- SGTACLs Policies: Set of rules that specify the privileges of a traffic source within a trusted network.
- SGT Enforcement: Where the policies are enforced, based on the SGT Policy.

SGT Propagation Methods

The SGT propagation methods are:

- SGT Propagation Inline Tagging
- SGT SXP Propagation

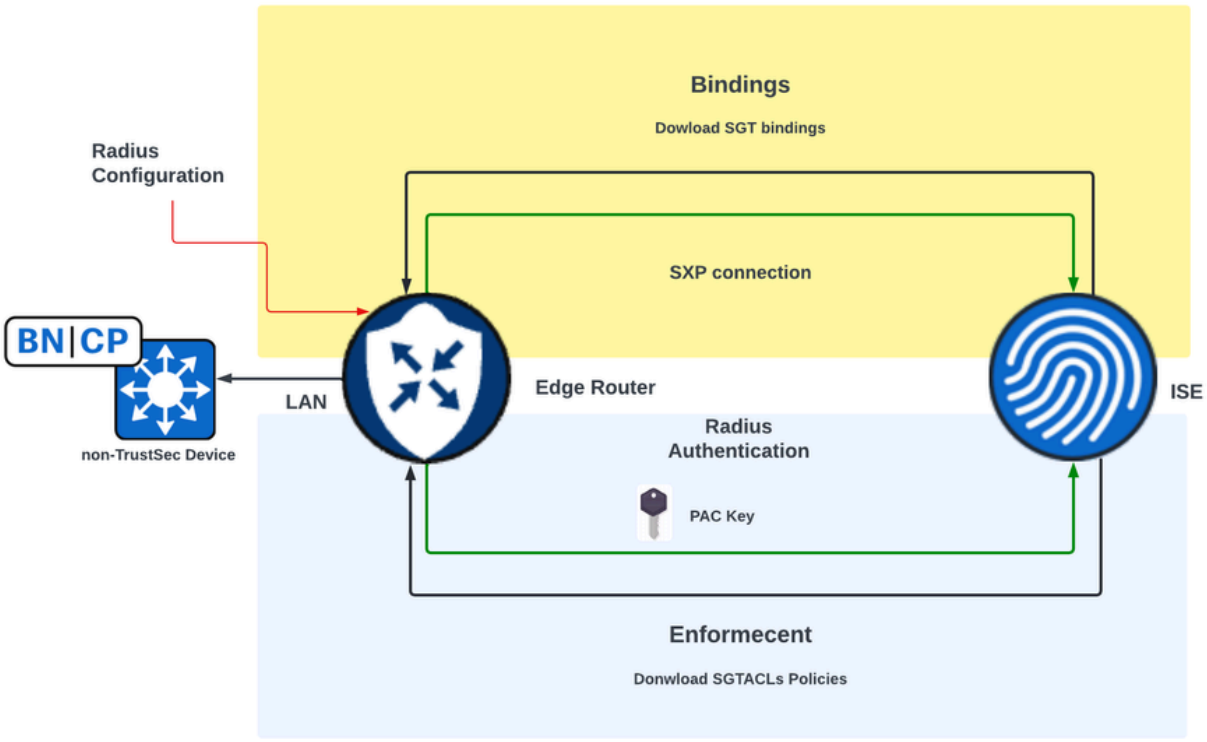
SGT Propagation with SXP

For Inline Tagging Propagation, the branches need to be equipped with Cisco TrustSec-enabled switches that are capable of handling SGT Inline Tagging (Cisco TrustSec Devices). If the hardware does not support Inline Tagging, SGT Propagation uses Security Group Tag Exchange Protocol (SXP) to propagate SGTs across network devices.

Cisco ISE allows creating an IP-to-SGT Binding (Dynamic IP-SGT) and then downloads IP-SGT Binding using SXP to a Cisco IOS® XE Catalyst SD-WAN device for propagation of the SGT over the Cisco Catalyst SD-WAN network. Also, the policies for the SGT traffic on SD-WAN egress are enforced by downloading SGACL Policies from ISE.

Example:

- The Cisco Switch (Border node) does not support Inline Tagging (non-TrustSec device).
- Cisco ISE allows downloading IP-SGT Binding through SXP connection to a Cisco IOS® XE Catalyst SD-WAN device (Edge Router).
- Cisco ISE allows downloading SGACL Policies through the Radius integration and PAC key to a Cisco IOS® XE Catalyst SD-WAN device (Edge Router).

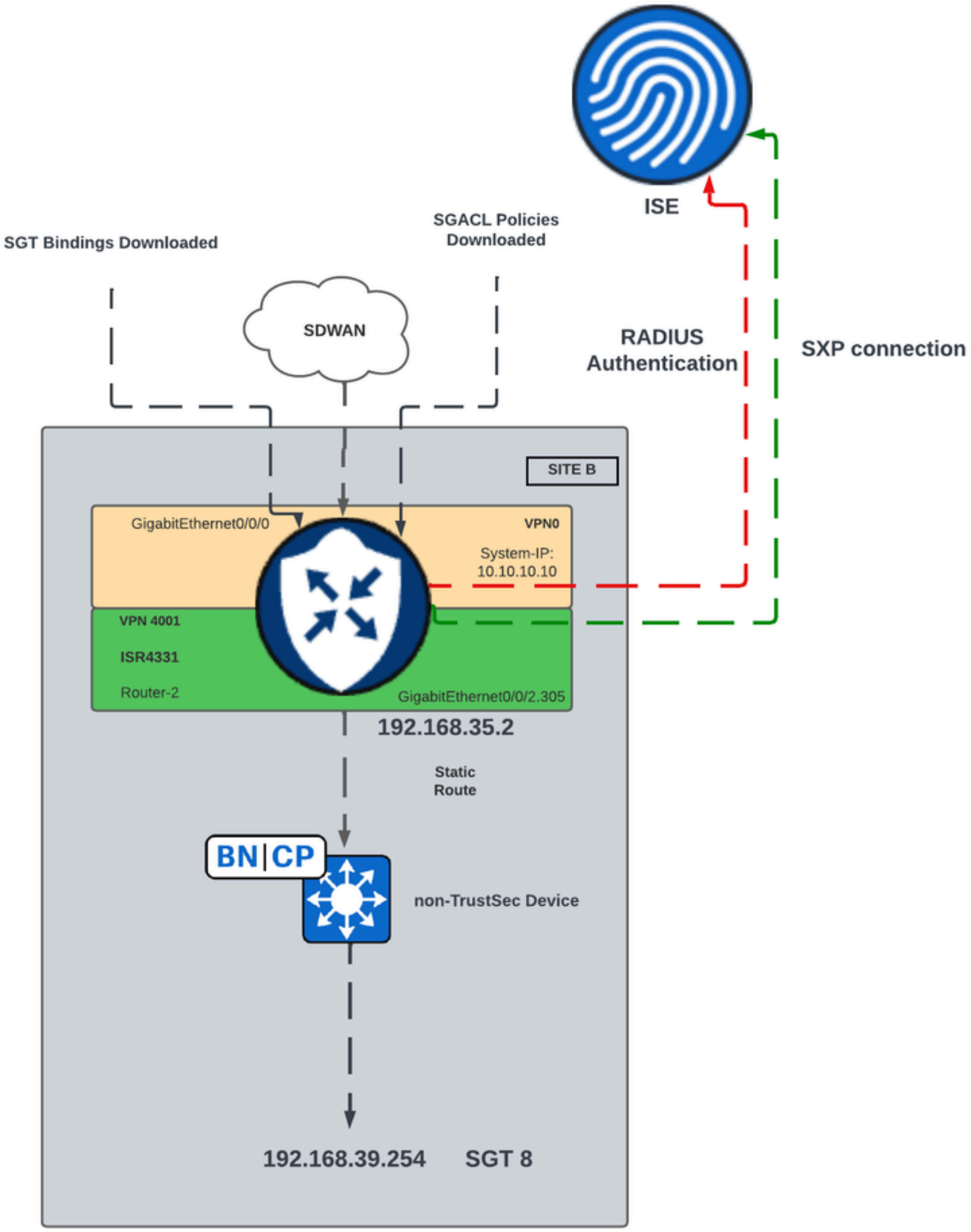


Requirements to Enable the SXP Propagation and Download SGACL Policies on SD-WAN Edge Devices

Note: SGACL Policies are not enforced on the ingress traffic, only on egress traffic in a Cisco Catalyst SD-WAN network.

Note: Cisco TrustSec feature is not supported for more than 24K SGT Policies in controller mode.

Enable SGT SXP Propagation and Download SGACL Policies

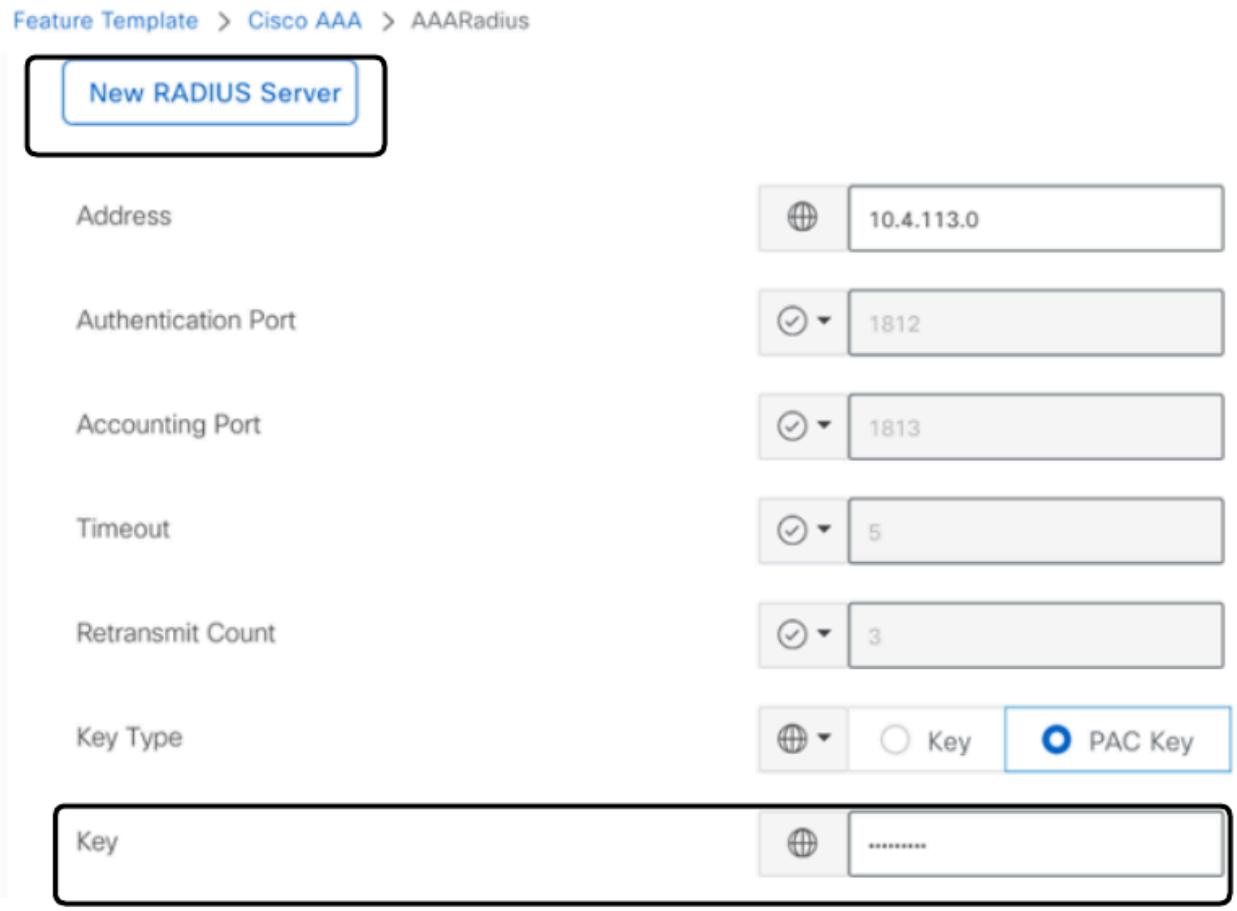


Network Diagram for SGT SXP Propagation in SD-WAN

Step 1. Configure the Radius Parameters

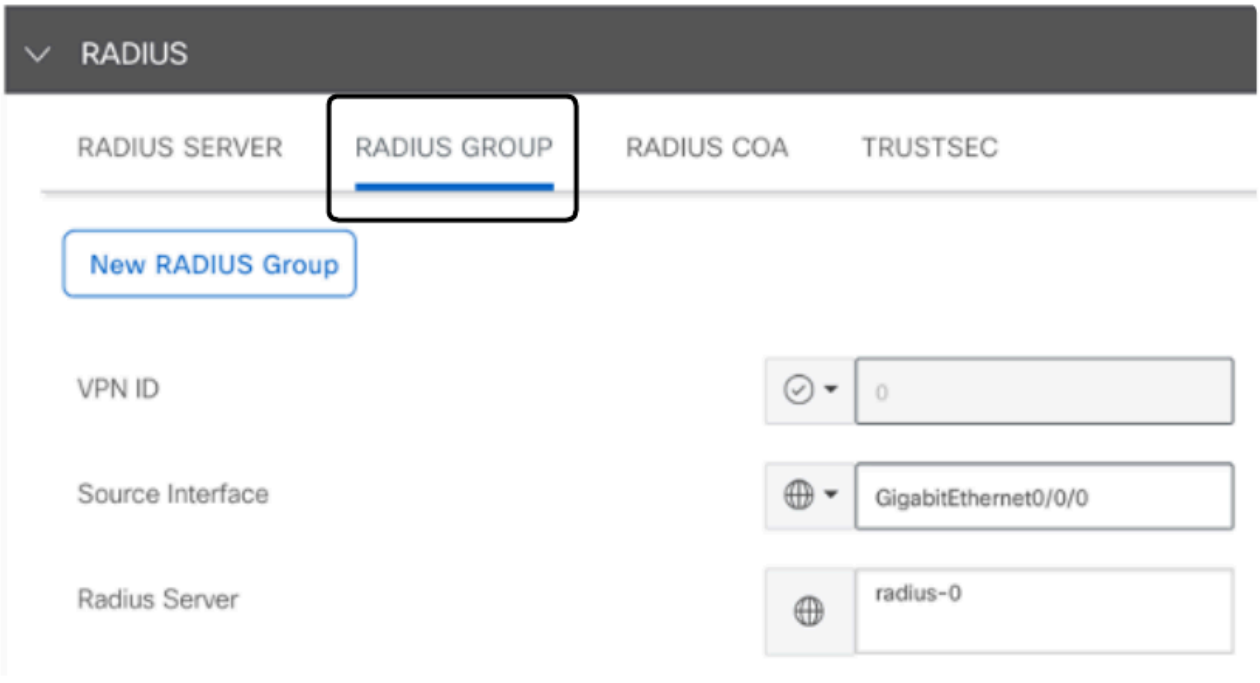
- Log in to Cisco Catalyst SD-WAN Manager GUI.
- Navigate to **Configuration > Templates > Feature Template > Cisco AAA**. Click **RADIUS SERVER**.

- Configure **RADIUS SERVER** parameters and **Key**.



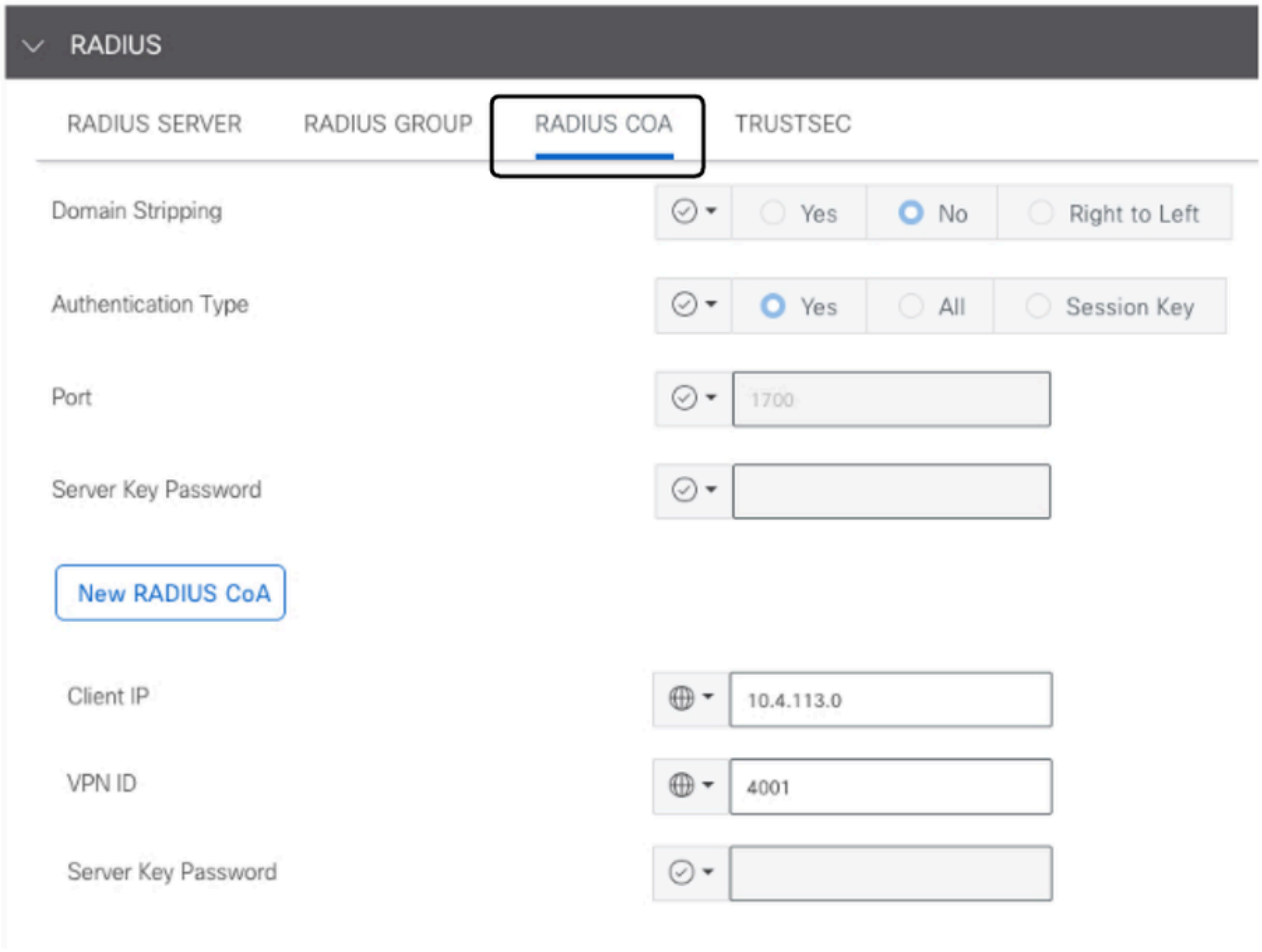
RADIUS Server Configuration

- Enter the **values** to configure **Radius Group** parameters.



RADIUS Group Configuration

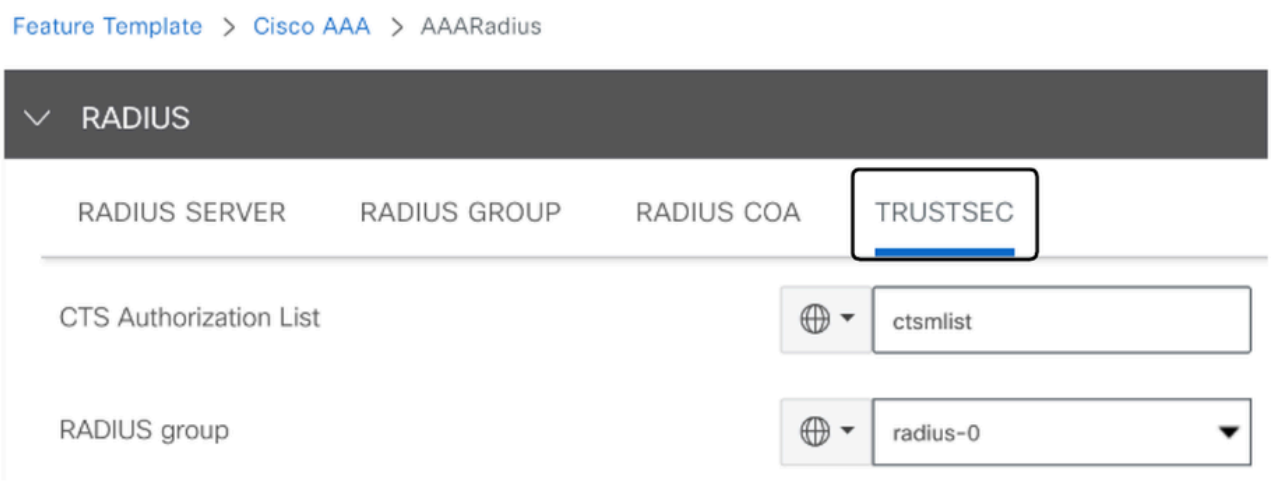
- Enter the **values** to configure **Radius COA** parameters.



RADIUS COA Configuration

Note: If Radius COA is not configured, SD-WAN router is not able to download the SGACL Policies automatically. After create o modify a SGACL Policy from ISE, the command **cts refresh policy** is used to download the policies.

- Navigate to **TRUSTSEC** section and enter the **values**.

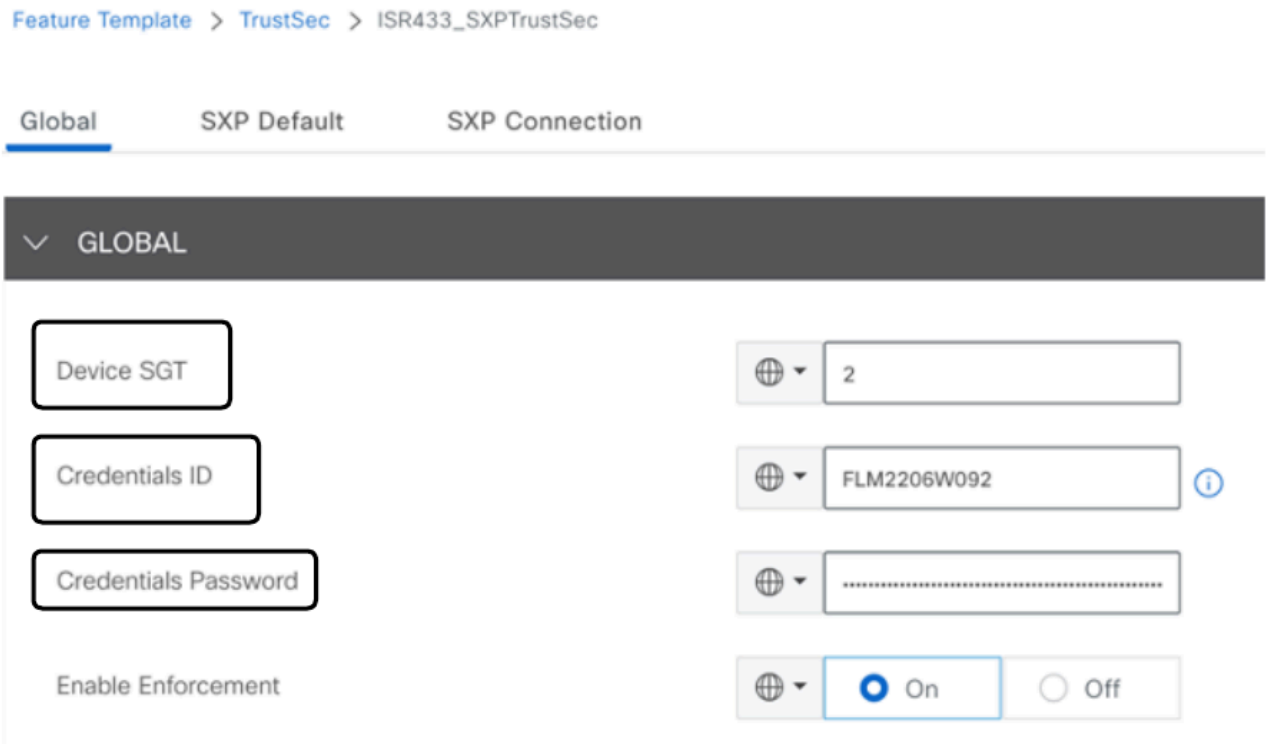


TRUSTSEC Configuration

- Attach the **Cisco AAA** feature template to Device template.

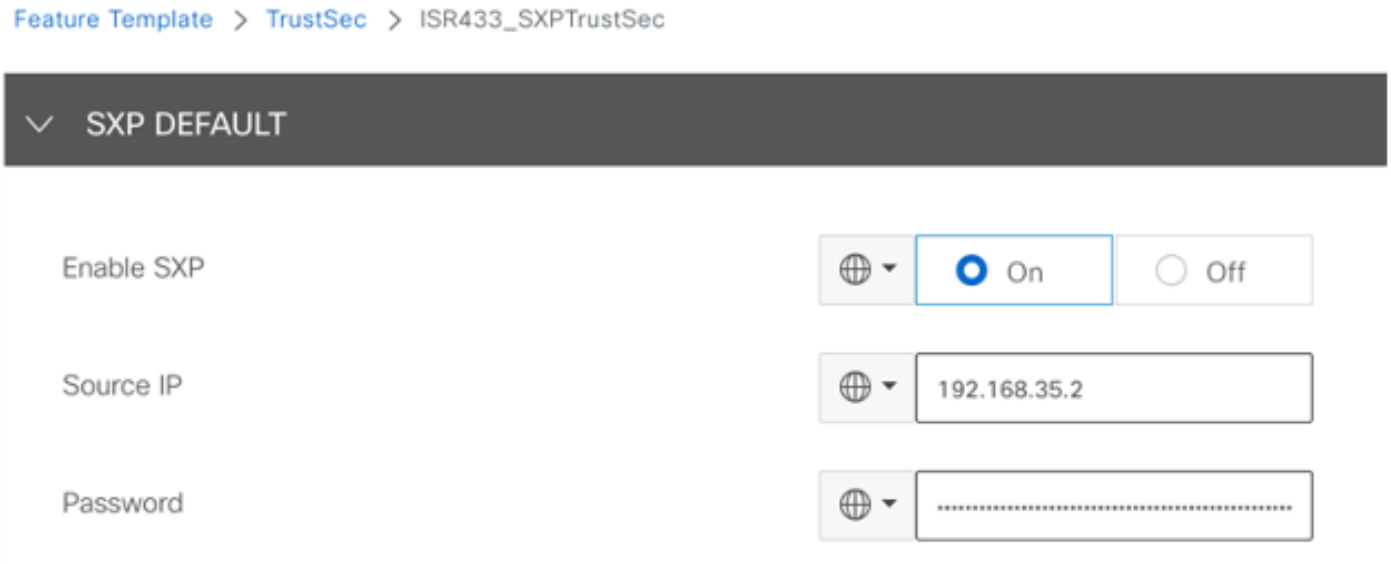
Step 2. Configure the SXP Parameters

- Navigate to **Configuration > Templates > Feature Template > TrustSec**.
- Configure the **CTS credentials** and assign a **SGT Binding** to device Interfaces.



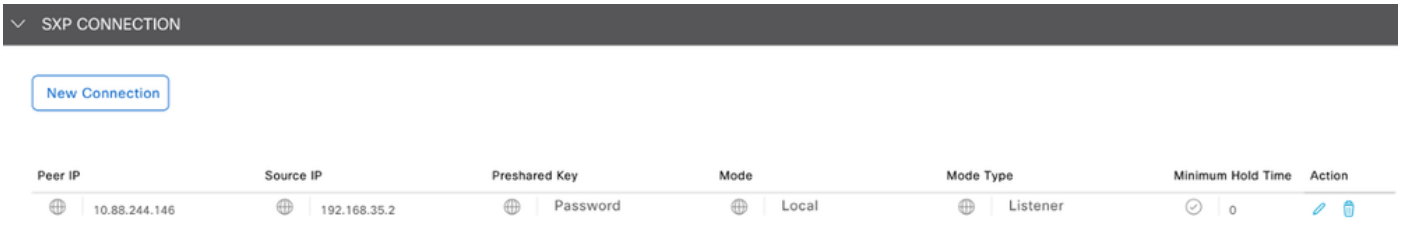
TrustSec Feature Template

- Navigate to **SXP Default** section and enter the **values** to configure the **SXP Default** parameters.



SXP Default Configuration

- Navigate to **SXP Conection** and configure the **SXP Connection** parameters, then click **Save**.

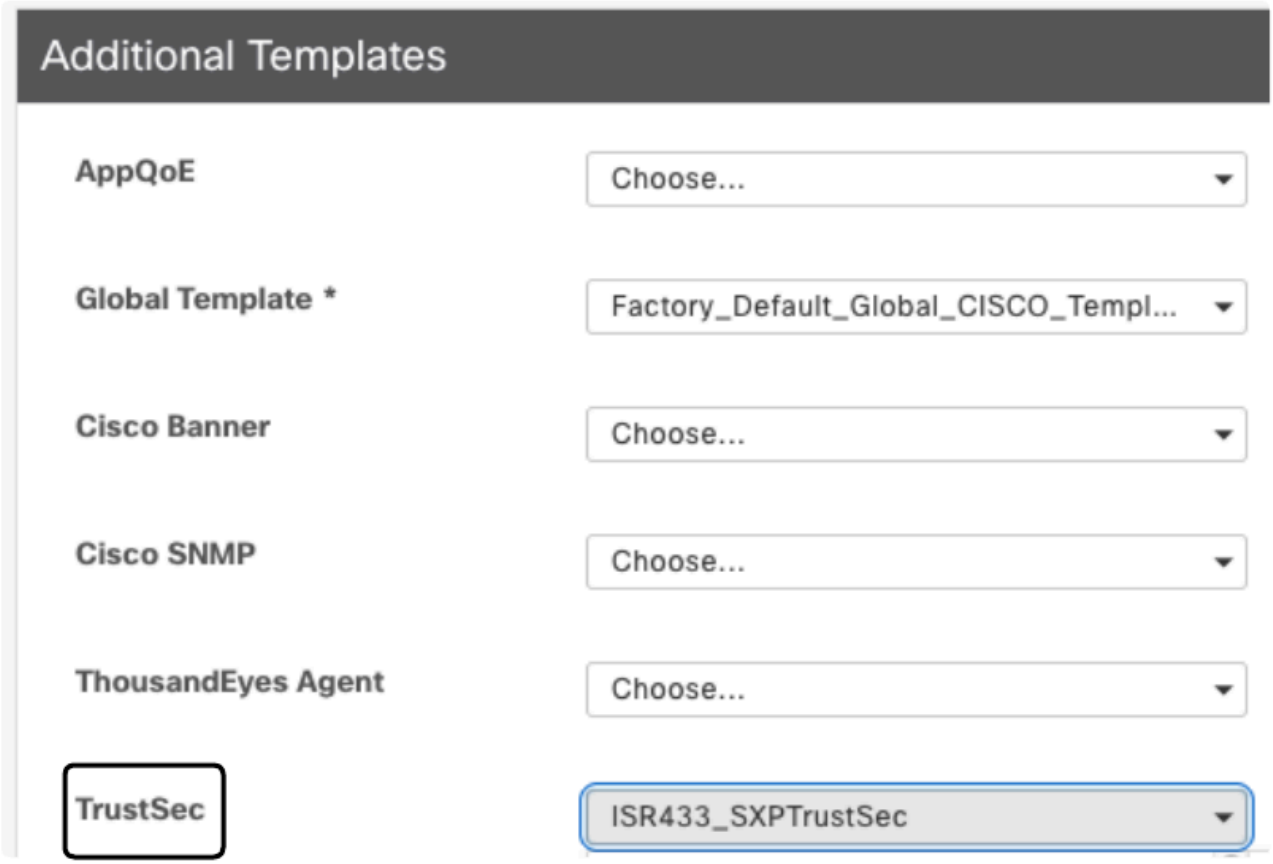


SXP Connection Configuration

Note: Cisco ISE has a limit on the number of SXP sessions it can handle. Therefore, as an alternative, a SXP Reflector for scale network horizontal could be used.

Note: It is recommended to use an SXP reflector to establish an SXP peer with Cisco IOS® XE Catalyst SD-WAN devices.

- Navigate to **Configuration > Templates > Device Template > Additional Templates > TrustSec**.
- Select the **TrustSec** feature template previously created, click **Save**.



Additional Templates Section

Verify

Run the command show cts sxp connections vrf (service vrf)to display the Cisco TrustSec SXP connections information.

<#root>

#show

cts

sxp

connections

vrf

4001

SXP : Enabled

Highest Version Supported: 5
Default Password : Set
Default Key-Chain: Not Set

```
Default Key-Chain Name: Not Applicable
Default Source IP: 192.168.35.2
Connection retry open period: 120 secs
Reconcile period: 120 secs
Retry open timer is not running
Peer-Sequence traverse limit for export: Not Set
Peer-Sequence traverse limit for import: Not Set
---------------------------------------------
```

Peer IP : 10.88.244.146

Source IP : 192.168.35.2

Conn status : On

```
Conn version     : 4
Conn capability  : IPv4-IPv6-Subnet
Conn hold time   : 120 seconds
Local mode       : SXP Listener
Connection inst# : 1
TCP conn fd      : 1
TCP conn password: default SXP password
Hold timer is running
```

Total num of SXP Connections = 1

Run the command **show cts role-based sgt-map** to display the global Cisco TrustSec SGT map between IP-Address and SGT Bindings.

<#root>

#

show

cts

role-based

sgt

-map

vrf

4001 all

```
Active IPv4-SGT Bindings Information
IP Address              SGT     Source
============================================
192.168.1.2             2       INTERNAL
192.168.35.2            2       INTERNAL
```

192.168.39.254 8 SXP <<< Bindings learned trough SXP for the host connected in the

```
IP-SGT Active Bindings Summary
```

```
==========================================
Total number of CLI      bindings = 0
Total number of SXP      bindings = 1

Total number of INTERNAL bindings = 2
Total number of active   bindings = 3
```

Run the command **show cts environment-data** to display the global Cisco TrustSec Environment Data.

<#root>

#show

cts

environment-data

```
CTS Environment Data
====================
```

Current state = COMPLETE

```
Last status = Successful
Service Info Table:
Local Device SGT:
  SGT tag = 2-01:TrustSec_Devices
Server List Info:
Installed list: CTSServerList1-0002, 1 server(s):
 Server: 10.88.244.146, port 1812, A-ID B546BF54CA5778A0734C8925EECE2215
          Status = ALIVE
          auto-test = FALSE, keywrap-enable = FALSE, idle-time = 60 mins, deadtime = 20 secs
```

Security Group Name Table:

0-00:Unknown

2-01:TrustSec_Devices

3-00:Network_Services

4-00:Employees

5-00:Contractors

6-00:Guests

```
    7-00:Production_Users

    8-02:Developers
          <<<<< Security Group assigned to the host connected in the LAN side (SGT 8)
    9-00:Auditors

    10-00:Point_of_Sale_Systems

    11-00:Production_Servers

    12-00:Development_Servers

    13-00:Test_Servers

    14-00:PCI_Servers

    15-01:BYOD

Environment Data Lifetime = 86400 secs
```

Run the command show cts pacs to display the Cisco TrustSec PAC provisioned.

```
<#root>
#show cts pacs

AID: B546BF54CA5778A0734C8925EECE2215
PAC-Info:
  PAC-type = Cisco Trustsec
  AID: B546BF54CA5778A0734C8925EECE2215

  I-ID: FLM2206W092


A-ID-Info: Identity Services Engine
  Credential Lifetime: 22:24:54 UTC Tue Dec 17 2024
```

PAC-Opaque: 000200B800030001000400010B546BF54CA5778A0734C8925EECE22150006009C00030100BE30CE655A7649A5CED8

Run the command show cts role-based permissions to display the SGACL Policies.

<#root>

#show

cts

role-based permissions

```
IPv4 Role-based permissions default:
        Permit IP-00
IPv4 Role-based permissions from group 5:Contractors to group 2:TrustSec_Devices:
        Deny IP-00
```

IPv4 Role-based permissions from group 5:Contractors to group 8:Developers:

DNATELNET-00

```
IPv4 Role-based permissions from group 5:Contractors to group 15:BYOD:
        Deny IP-00
```

Run the command show cts rbacl (SGACLName) to display the access control list (SGACL) configuration.

<#root>

#show

cts

rbacl

DNATELNET

```
CTS RBACL Policy
================
RBACL IP Version Supported: IPv4 & IPv6
  name   =
```

DNATELNET-00

```
  IP protocol version = IPV4, IPV6
  refcnt = 2
  flag   = 0xC1000000
  stale  = FALSE
```

RBACL ACEs:

```
    deny
tcp


dst
 eq 23 log
       <<<<< SGACL action
    permit
ip
```

Related Information

- Cisco Catalyst SD-WAN Security Configuration Guide
- Cisco TrustSec Configuration Guide