

# Cisco SD-Access | SD-WAN *Independent Domain* Pairwise Integration

## Prescriptive Deployment Guide

June 2021

First Publish: 24 June 2021  
Last Update: 24 June 2021

---

# Contents

Hardware and Software Version Summary	3
About This Guide	4
Define	7
Cisco Software-Defined Wide Area Network Solution Overview	7
Cisco Software-Defined Access Overview	8
Protocol Operational Planes Overview	10
Cisco SD-Access   Cisco SD-WAN Pairwise Introduction	12
<i>Independent Domain</i> Protocol Integrations	14
Design	17
<i>Independent Domain</i> Design Considerations	21
Deploy	29
Process 1: Verifying Prerequisites for <i>Independent Domain</i>	30
Process 2: Configuring Cisco TrustSec Inline Tagging	42
Process 3: Defining Group-Based Access Control Policies	55
Operate	63
Process 1: Monitoring and Assuring the Cisco SD-Access Infrastructure	63
Process 2: Monitoring SD-WAN Edge TrustSec Configuration	67
Process 3: Validating Policy Enforcement	68
Appendix A: Hardware and Software Versions	71
Appendix B: References Used in This Guide	74
Appendix C: Acronym Glossary	75
Appendix D: Recommended for You	81
Appendix E: TrustSec Inline Tagging Syntax History and Explanation	82
Feedback	84



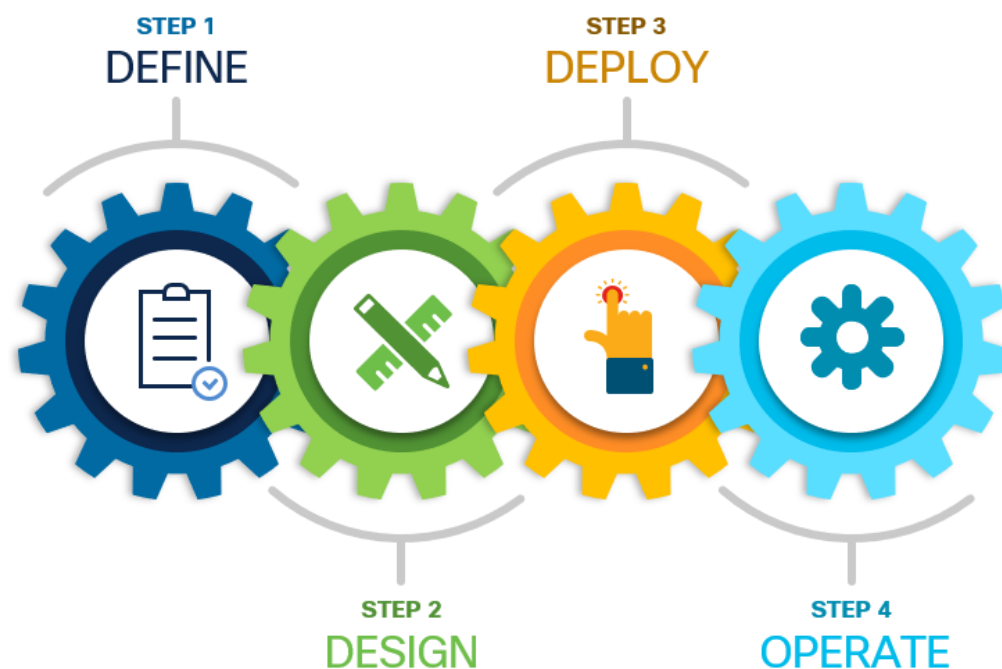
# Hardware and Software Version Summary

**Table 1.** Hardware and Software Version Summary

Product	Software version
Cisco DNA Center Appliance	2.1.2.6 (System 1.5.279)
Cisco Identity Services Engine	2.7 Patch 3
Cisco SD-WAN Controllers	20.3.3
Cisco IOS XE WAN Edge Devices	IOS XE 17.3.3
Cisco SD-Access Devices	IOS XE 17.3.3

---

## About This Guide



This document contains four major sections:

The **DEFINE** section provides a high-level overview of the Cisco SD-WAN, SD-Access architecture and components.

The **DESIGN** section provides a detailed discussion on the design considerations, deployment topology options and prerequisites needed to integrate the solutions.

The **DEPLOY** section discusses step-by-step procedures, workflows to connect multiple SD-Access fabric sites with SD-WAN network.

The **OPERATE** section briefly discusses how to monitor and troubleshoot the common issues.

Refer to [Appendix A](#) for details on the platform and software versions used to build this document.

## Introduction

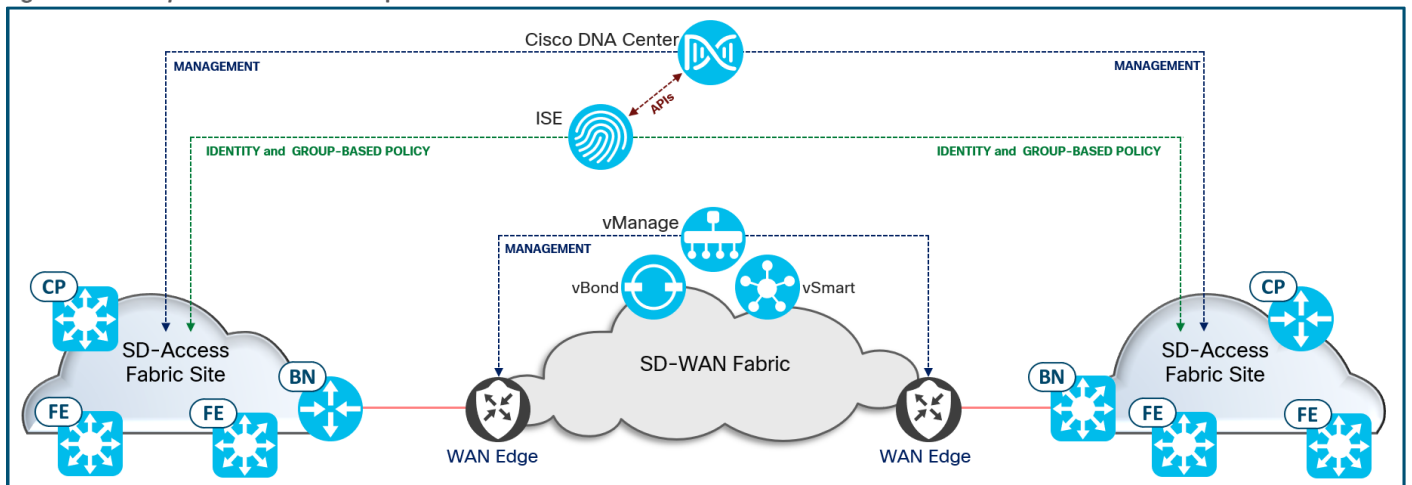
This guide provides design and deployment steps to use the Cisco SD-Access and Cisco SD-WAN solutions to achieve end-to-end segmentation and consistent policy for the enterprise and branch. The guide focuses on the design considerations, best practices, and the step-by-step procedures needed to integrate the two solutions together.

The Cisco SD-Access | Cisco SD-WAN *Independent* Domain and *Integrated* Domain deployment models provide network administrators the ability to:

- Securely onboard network devices and interconnect campus and branch locations
- Preserve Scalable Group Tags (SGTs) across the SD-WAN transport
- Maintain end-to-end segmentation across the enterprise campus and branch locations
- Define and enforce group-based policy throughout the network

These capabilities coupled with the unique capabilities provided through each solution enables organizations to build the next-generation Intent-Based Networking solution.

**Figure 1. Independent Domain Components**



The guide focuses on the *Independent* Domain deployment model where the SD-WAN controllers and Cisco DNA Center are independently managed and not integrated. In this approach, the WAN Edge devices perform only the SD-WAN functionality and are managed and provisioned by the SD-WAN controllers. The SD-Access Fabric devices are managed and provisioned by the Cisco DNA Center.

---

## Companion Resources

For more information on the SD-WAN Design and Deployment best practices, please see:

- [Cisco SD-WAN Design Guide](#)
- [Cisco WAN Edge Onboarding Prescriptive Deployment Guide](#)
- [Cisco SD-WAN End-to-End Deployment Guide](#)

For more information on the SD-Access best practices design and deployment, please see:

- [SD-Access Solution Design Guide](#),
- [SD-Access & Cisco DNA Center Management Infrastructure](#)
- [SD-Access Fabric Provisioning Prescriptive Deployment Guide](#)
- [SD-Access for Distributed Campus Deployment Guide](#)

For all full list of related deployment guides, design guides, and white papers, please visit the following pages:

- <https://cs.co/en-cvds>
- <https://www.cisco.com/go/designzone>

If you didn't download this guide from Cisco Community or Design Zone, you can [check for the latest version](#) of this guide.

## Audience

The intended audience for this document includes network design engineers and network operations personnel who are looking to deploy multiple Cisco SD-Access sites, interconnect with Cisco SD-WAN solution, while still maintaining the two domains independently, and require maintaining end-to-end segmentation and consistent group-based policy.

## Define

This chapter is organized into the following sections:

Chapter	Section
Define	<a href="#">Cisco SD-WAN Solution Overview</a>
	<a href="#">Cisco SD-Access Solution Overview</a>
	<a href="#">Protocol Operational Planes Overview</a>
	<a href="#">Cisco SD-Access   SD-WAN Pairwise Overview</a>
	<a href="#">Independent Domain Protocol Integrations</a>

## Cisco Software-Defined Wide Area Network Solution Overview

The Cisco® Software-Defined Wide Area Network (SD-WAN) solution is an enterprise-grade SD-WAN overlay architecture that enables digital and cloud transformation. The solution fully integrates routing, security, centralized policy, management, and orchestration into large-scale networks and addresses the problems and challenges of common WAN deployments.

### Cisco SD-WAN Solution Components

There are four key components that make up the Cisco SD-WAN solution, each performing distinct activities in different network planes of operation: orchestration plane, management plane, control plane, and data plane.

**Orchestration Plane Controller**—Securely onboards the SD-WAN Edge routers into the SD-WAN overlay.

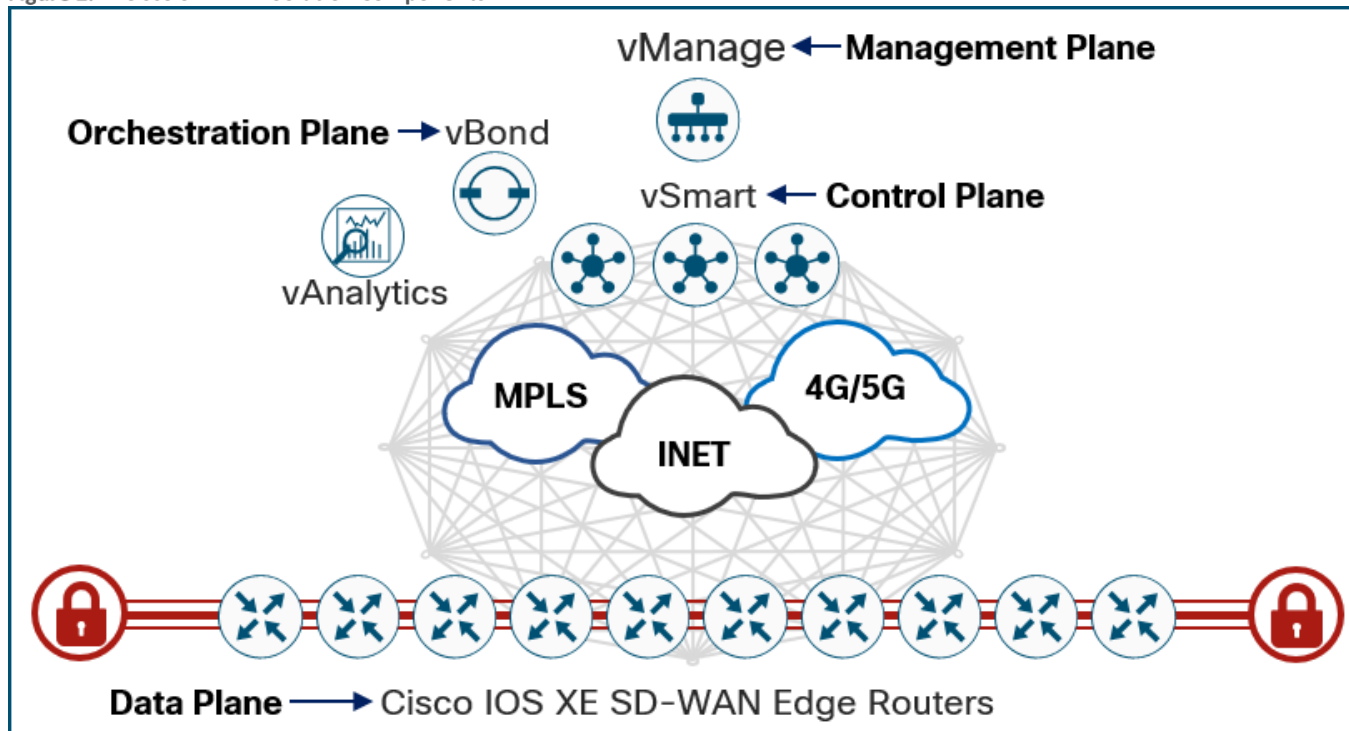
**Management Plane Controller**—Provides assurance, visibility, and management.

**Control Plane Controller**—Responsible for central configuration and monitoring.

**Data Plane Devices**—Forwards packets based on decisions from the control plane.

In Cisco SD-WAN, Cisco vBond is responsible for the orchestration plane, the management plane is enabled and powered through Cisco vManage, Cisco vSmart drive the control plane, and Cisco IOS XE SD-WAN Edge routers are responsible for the data plane.

Figure 2. Cisco SD-WAN Solution Components



**vBond**—The vBond controller, or vBond *orchestrator*, authenticates and authorizes the SD-WAN routers and controllers into the network. The vBond orchestrator uses a distribute list to propagate vSmart and vManage controller information to the WAN Edge routers.

**vManage**—The vManage controller is the centralized network management system that provides the GUI interface. This single pane of glass allows easy deployment, configuration, monitoring, and troubleshooting of the Cisco SD-WAN network.

**vSmart**—vSmart builds and maintains the network topology and make decisions on the traffic flows. The vSmart controller disseminates control plane information between WAN Edge devices, enforces centralized control plane policies, and distributes data plane policies to the WAN Edge devices to do enforcement.

**vAnalytics**—Cisco vAnalytics is a cloud-based service that provides visibility and insights into the network infrastructure, application usage, and performance across the SD-WAN network.

**SD-WAN Edge Routers**—WAN Edge devices provide secure data plane connectivity across locations connected to the WAN network. These routers are responsible for traffic forwarding and provide security, encryption, and Quality of Service (QoS) enforcement.

## Cisco Software-Defined Access Overview

Cisco® Software-Defined Access (SD-Access) is the evolution from traditional campus designs to networks that directly implement the intent of an organization. SD-Access is a software application running on Cisco DNA Center hardware that is used to automate wired and wireless campus networks.

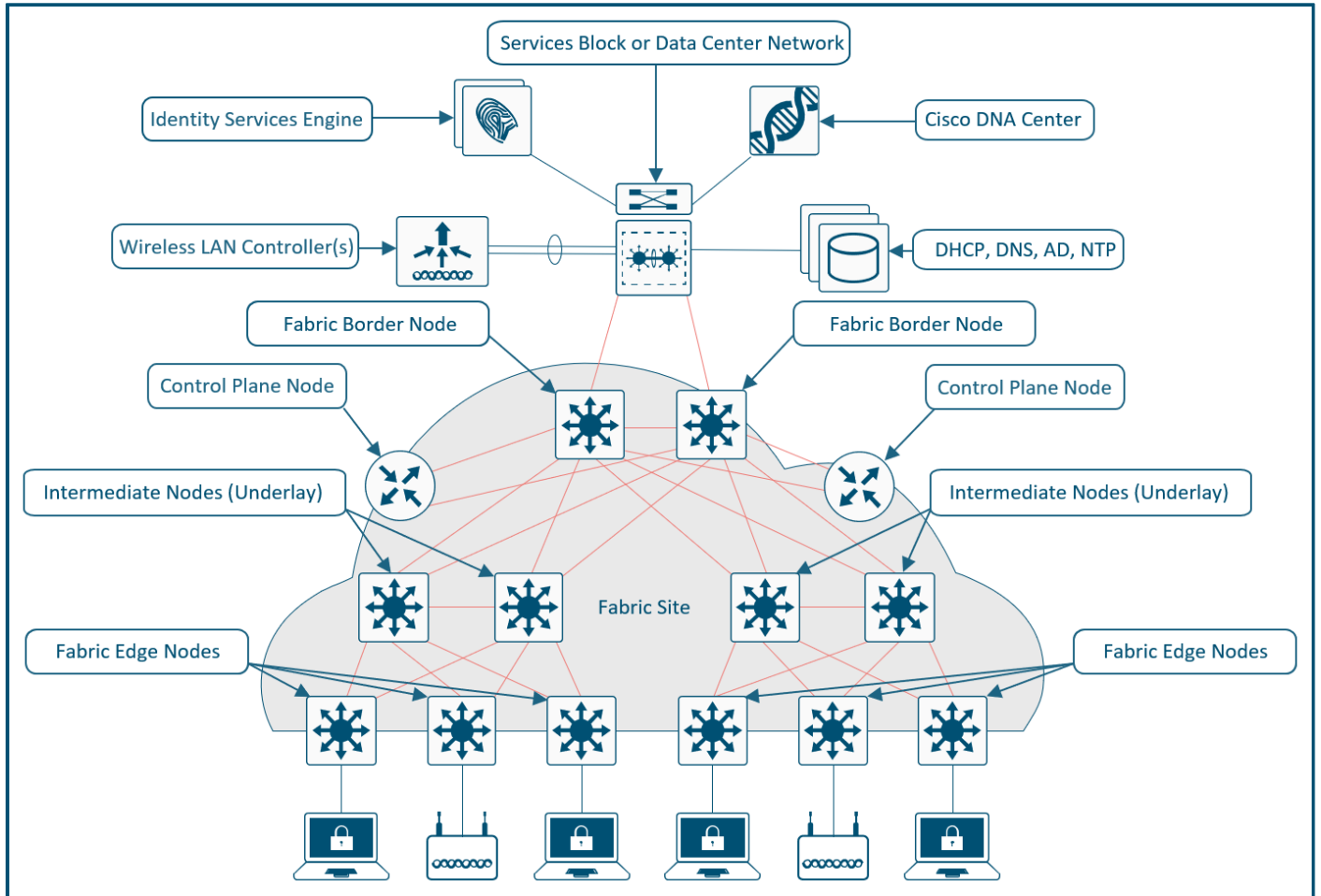
*Fabric technology*, an integral part of SD-Access, provides wired and wireless campus networks with programmable overlays and easy-to-deploy network virtualization, permitting a physical network to host one or more logical networks to meet the design intent. In addition to network virtualization, fabric technology in the campus network enhances control of communications, providing software-defined segmentation and policy enforcement based on user identity and group membership. Software-



defined segmentation is seamlessly integrated using Cisco TrustSec® (CTS) technology, providing micro-segmentation for groups within a virtual network using scalable group tags (SGTs). Using Cisco DNA Center to automate the creation of virtual networks with integrated security and segmentation reduces operational expenses and reduces risk. Network performance, network insights, and telemetry are provided through the Assurance and Analytics capabilities.

## Cisco SD-Access Solution Components

Figure 3. Cisco SD-Access Solution Components



The Cisco SD-Access solution is comprised of the following components:

**Fabric Site**—An independent fabric that includes a control plane node, border node, edge node and usually includes an ISE Policy Service Node (PSN) and fabric-mode Wireless LAN Controller (WLC).

**Fabric Edge Nodes**—Equivalent to an access layer switch in a traditional campus LAN design. Endpoints, IP phones, and wireless access points are directly connected to edge nodes.

**Fabric Border Node**—Serves as the gateway between the SD-Access fabric site and networks external to the fabric. The border node is the device physically connected to a transit (either SD-WAN transit, IP-Transit or SD-Access transit) or to a next-hop device connected to the outside world.

**Fabric Control Plane Node**—The SD-Access fabric control plane node is based on the LISP Map-Server (MS) and Map-Resolver (MR) functionality combined on the same node. The control plane database tracks all endpoints in the fabric site and associates

the endpoints to fabric edge nodes, decoupling the endpoint IP address or MAC address from the location (closest router) in the network.

**Fabric Wireless LAN Controller**— The Wireless LAN Controller (WLC) provides centralized AP image and configuration management and client session management. The WLC integrates and communicates with the Fabric Control Plane Node to provide mobility services for endpoints attached to Fabric Access Points.

**Fabric Access Points**— Access Points (APs) operating with Fabric SSIDs build a VXLAN data tunnel to Fabric Edge Nodes. Control traffic is still tunneled to the WLC. By terminating client traffic at the first-hop Edge Node, policy for wired and wireless traffic can be enforced at the same location in the network.

**Identity Service Engine**—Cisco ISE is a secure network access platform enabling increased management awareness, control, and consistency for users and devices accessing an organization's network. ISE is an integral part of SD-Access for policy implementation, enabling dynamic mapping of users and devices to scalable groups and simplifying end-to-end security policy enforcement.

**Cisco DNA Center**—Cisco DNA Center software, including the SD-Access application package, is designed to run on the Cisco DNA Center Appliance. The UCS appliance is available in form factors sized to support not only the SD-Access application but also network assurance.

The same enterprise Cisco DNA Center cluster can be used to discover, provision and manage all the network devices across the enterprise - campus and remote branch locations.

**Virtual Networks (Macro-segmentation)**—Use virtual networks (VNs) when requirements dictate isolation at both the data plane and control plane. In general, if devices need to communicate with each other, they should be placed in the same virtual network. If communication is required between different virtual networks, use an external firewall or other device to enable inter-VN communication. A Virtual Network provides the same behavior and isolation as VRFs.

**SGTs (Micro-segmentation)**—SGTs allow for simple-to-manage group-based policies and enable granular data plane isolation between groups of endpoints within a virtualized network. Using SGTs also enables scalable deployment of policy without having to do cumbersome updates for these policies based on IP addresses.

## Protocol Operational Planes Overview

This chapter is organized into the following sections:

Chapter	Section
Protocol Operational Planes	<a href="#">Control Plane Protocols</a> <a href="#">Data Plane Protocols</a> <a href="#">Policy Plane Protocols</a>

In SD-Access the control plane is based on LISP (Locator/ID Separation Protocol), the data plane is based on VXLAN (Virtual Extensible LAN), the policy plane is based on Cisco TrustSec and the management plane is enabled and powered by Cisco DNA Center.

In SD-WAN the control plane is based on OMP (Overlay Management Protocol), the data plane is based on IPSec/GRE, the policy plane is based on Layer 3/Layer 4 IP information managed by vSmart, and the management plane is enabled and powered by vManage.

An overview of each of these protocols is provided in this section. The interaction of these protocols and how they are used to carry segmentation, policy, and traffic end-to-end is discussed in the [next section](#).

<b>Tech tip</b>
For additional details on the SD-Access protocols, please see: <a href="#">SD-Access Operational Planes</a> in the Cisco SD-Access Solution Design Guide.

## Control Plane Protocols

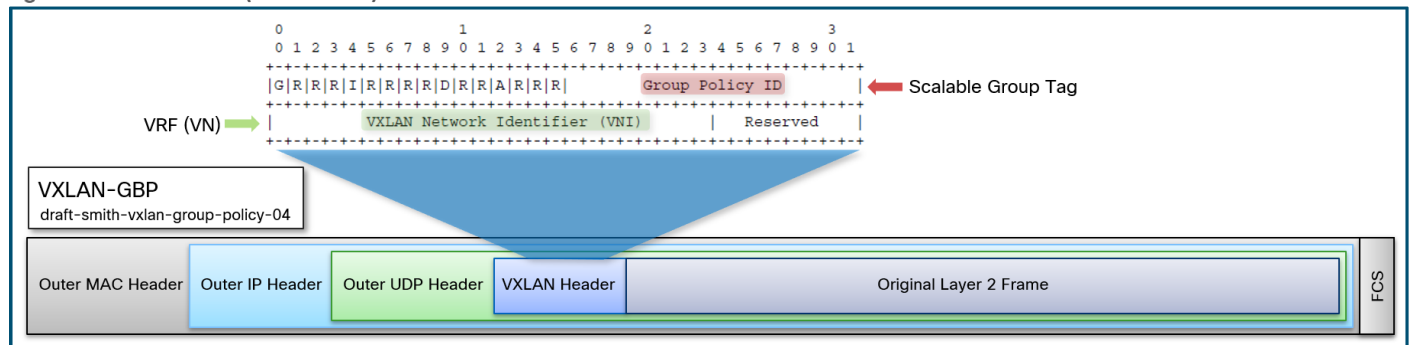
Cisco SD-Access leverages LISP control plane to communicate and exchange the endpoint’s identity (EID) in relationship to its routing locator (RLOCs). The fabric devices query the control plane nodes to determine the RLOC information associated with the destination address (EID-to-RLOC mapping) and use the RLOC information as the traffic destination.

Cisco SD-WAN leverages OMP to communicate and exchange the route prefixes, next-hop routes, crypto and policy information between WAN Edge routers and vSmart controllers. The LAN Segment routes are redistributed into OMP and advertised to the vSmart controller. The vSmart controller then redistributes these learned routes to other WAN Edge routers in the SD-WAN network.

## Data Plane Protocols

Cisco SD-Access uses VXLAN as the encapsulation method for data packets. When encapsulation is added to the data packets, a tunnel network is created between the fabric devices. The fabric devices place additional information in the fabric VXLAN header including attributes that can be used to make forwarding decisions by identifying each overlay virtual network using VXLAN network identifier (VNI) and policy decision with the Scalable Group Tag. At minimum, these extra headers add additional 50 bytes of overhead to the original packet.

Figure 4. VXLAN-GBP (VXLAN-GPO) Packet Header

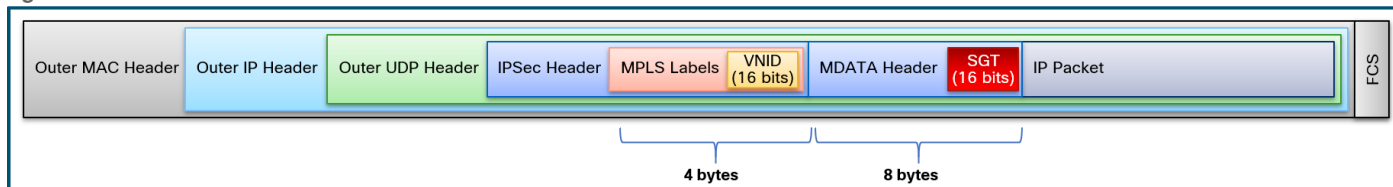


Cisco SD-WAN secures the data traffic with IPsec authentication and encryption. The secure data plane connection is established at the time of the WAN Edge onboarding process to ensure data plane integrity.

Cisco WAN Edge devices support MPLS extensions to data packets that are transported within IPsec connections. These extensions provide the ability to carry the network segmentation (Virtual Network ID) information across the WAN environment.

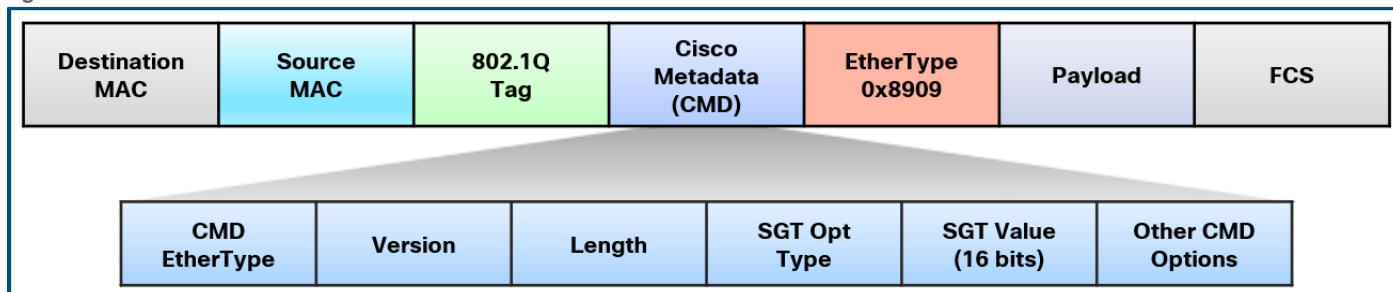
Cisco IOS XE 17.3.1a introduced Cisco TrustSec capabilities which adds an additional 8 bytes header. This header, Cisco Meta Data (CMD) or MDATA, is used to carry the SGT in the WAN environment.

Figure 5. SD-WAN IPSec Packet Header



Cisco WAN Edge routers support carrying SGT information in the Ethernet Frame towards the LAN environment on routed interfaces through inline tagging.

Figure 6. Ethernet Frame with CMD Header



## Policy Plane Protocols

Cisco SD-Access solution leverages Cisco TrustSec solution as the policy plane. The solution is defined in three phases: classification, propagation and enforcement. Cisco TrustSec implementation uses ingress classification and egress enforcement.

**Classification**—An SD-Access Edge Node sends user and device authentication requests to the ISE Policy Services Node (PSN) persona via RADIUS packets. The ISE Policy Service Node persona provides the scalable group tag (SGT) as part of the authorization profile. This provides an association between the SGT and the endpoint.

**Propagation**—Any data traffic from the endpoint traversing the Edge Node is tagged with the SGT value. This SGT information is carried to the fabric node in a VXLAN-encapsulated packet.

**Enforcement**—Security policies relevant to the SGT are downloaded from ISE PSN persona and installed on the fabric edge for policy enforcement. The fabric edge only downloads policies relevant to directly connected end-points. The destination fabric node leverages the SGT information in the VXLAN data packet and SGT value of the directly connected endpoint for policy enforcement at the destination egress direction.

### Tech tip

[Cisco SD-WAN IOS-XE 17.3.1a](#) and [Cisco vManage 20.3.1](#) introduced support for Cisco TrustSec Security Group Tag (SGT) propagation feature (Inline Tagging). This allows the WAN Edge devices to learn and propagate the SGT to other WAN Edge devices across the Cisco SD-WAN environment.

## Cisco SD-Access | Cisco SD-WAN Pairwise Introduction

The focus of the SD-Access | SD-WAN Pairwise Integration is to connect multiple, independent SD-Access fabric sites using a Cisco SD-WAN transport. This transport preserves the macro- and micro-segmentation constructs of virtual network (VN) and security group tags (SGTs), respectively. This enables secure endpoint onboarding, consistent user experience, and consistent end-to-end security policies across the enterprise for any user, any device, or any application that are anywhere on the network.

The SD-Access | SD-WAN Pairwise Integration can be deployed in the three following ways:

- [Independent Domain](#)
- [Integrated Domain](#)
- [Both Independent and Integrated Domains](#)

### Independent Domain Deployment

In this deployment approach, the SD-WAN controllers and Cisco DNA Center are **not** integrated. The SD-Access fabric roles are deployed on one set of network devices, while the SD-WAN Edge functionality is deployed on a separate set of network devices. In this deployment, the SD-Access components are managed independently by Cisco DNA Center, and Cisco SD-WAN components are managed independently by vManage controller.

Cisco SD-Access | SD-WAN *Independent Domain* integration provide the capability of carrying end-to-end segmentation and policy with the flexibility of managing the domains independently. Using Inline tagging and 802.1Q tags, the segmentation constructs are carried across the *Independent* domains.

### Integrated Domain Deployment

In this deployment approach, the SD-WAN controllers and Cisco DNA Center are integrated together. This allows for the sharing of network device information and configuration between the controllers for an end-to-end automation and seamless integration. In this model, the SD-WAN Edge functionality is colocated with the SD-Access Border Node and Control Plane Node functionality on the same device.

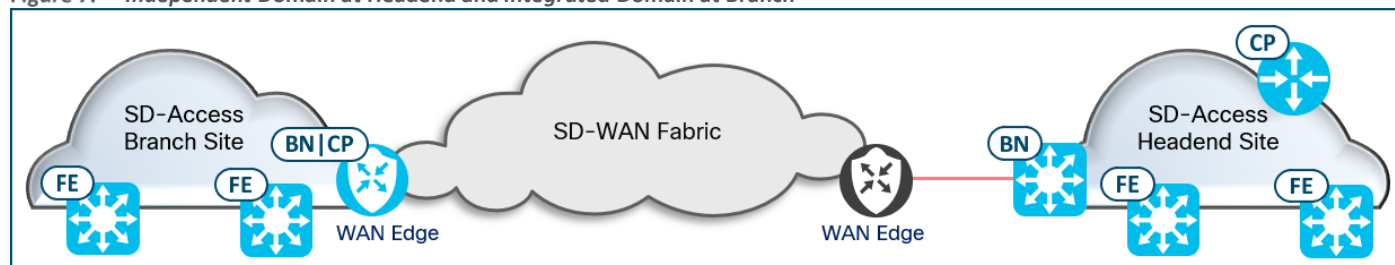
Cisco SD-Access | SD-WAN *Integrated Domain* integration provide the capability of carrying end-to-end segmentation and policy with the simplicity of managing the domains together. This is best suited for a branch or remote location across the WAN.

### Both Independent and Integrated Domain Deployments

This model allows Enterprises with multiple fabric sites to deploy a combination of *Independent Domain* and *Integrated Domain* deployment models across their network.

This deployment model is commonly seen in branch deployments with centralized headend locations. At the branch locations, the SD-Access functionality and SD-WAN functionality are colocated on the same device(s). At the headend location, the SD-Access and SD-WAN functionality are deployed on separate devices.

**Figure 7. Independent Domain at Headend and Integrated Domain at Branch**



#### Tech tip

An SD-Access Fabric Site can be deployed with the *Independent Domain* model or the *Integrated Domain* model. Both models cannot be deployed together at the same Fabric Site.

## Independent Domain Protocol Integrations

This chapter is organized into the following sections:

Chapter	Section
Independent Domain Protocol Integrations	<a href="#">Control Plane Integration</a>
	<a href="#">Data Plane Integration</a>
	<a href="#">Policy Plane Integration</a>
	<a href="#">Putting It All Together</a>

### Control Plane Integrations – Independent Domain

In the *Independent Domain* Pairwise Integration, the fabric border node is configured with handoff interface(s) that connect to the SD-WAN device(s) to create a BGP peering. The prefixes associated with the endpoints in the SD-Access fabric are advertised via BGP. The WAN Edge device learns these prefixes from the BGP peering and redistributes them into OMP using a 1:1 mapping of a dedicated service VPN for each fabric VN. This maintains the end-to-end control plane separation across the network.

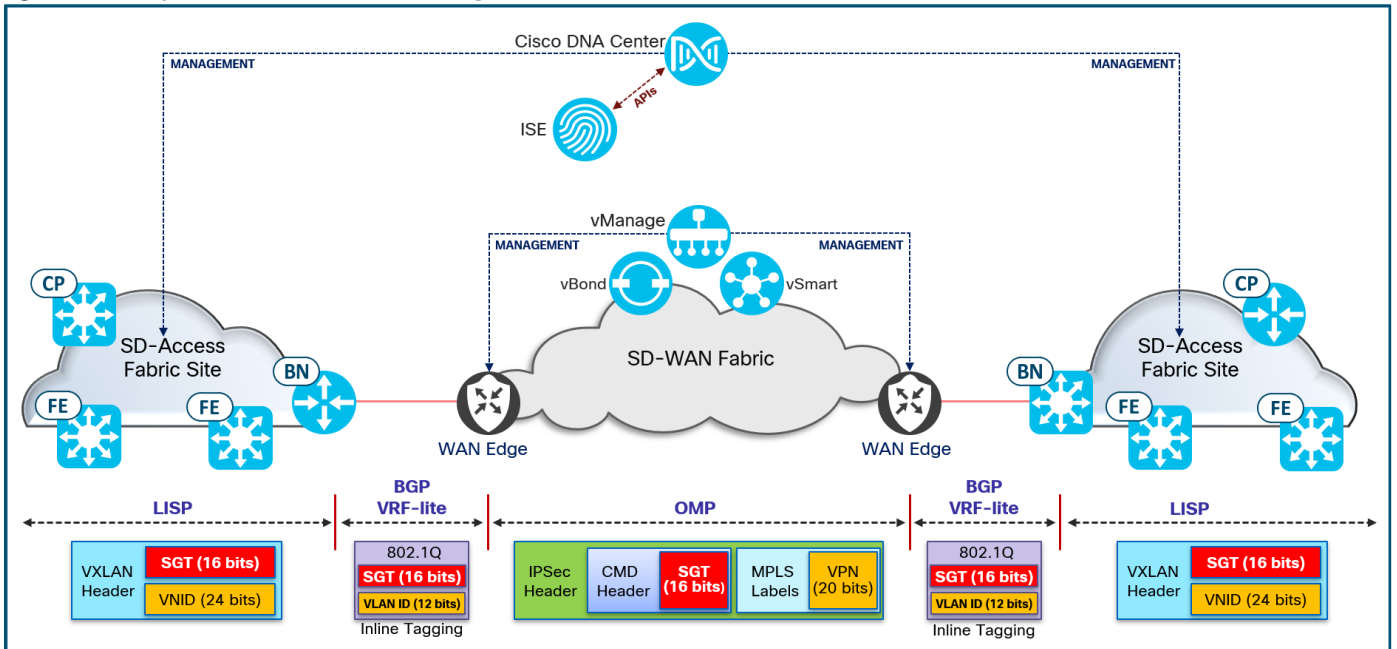
### Data Plane Integrations – Independent Domain

The handoff on the SD-Access border node and the WAN Edge router uses VRF-lite. VRF-lite associates each SVI or sub-interface with a different fabric VN (VRF). An 802.1Q VLAN is associated with each SVI or sub-interface to maintain the end-to-end macro-segmentation in the data plane.

### Policy Plane Integrations – Independent Domain

In the *Independent Domain* Pairwise Integration, the SGT is extracted from the fabric VXLAN header (VXLAN-GPO) by the Border Node and placed in the CMD header of the Ethernet frame. The SGT is carried inline between the Border Node and the WAN Edge router. Once the frame is received by the WAN Edge router, the SGT is transferred from the Ethernet CMD header into the IPsec CMD header. This allows the SGT to be carried across WAN transports to other SD-Access fabric sites. Once received by the WAN edge router on the other side of the IPsec tunnel, the process of transferring the SGT occurs in reverse. The SGT is copied back to the Ethernet CMD header, sent across the wire, and then transferred into the VXLAN header by the Border Node. This preserves the end-to-end segmentation in the policy plane.

Figure 8. Independent Domain Protocols Integrations



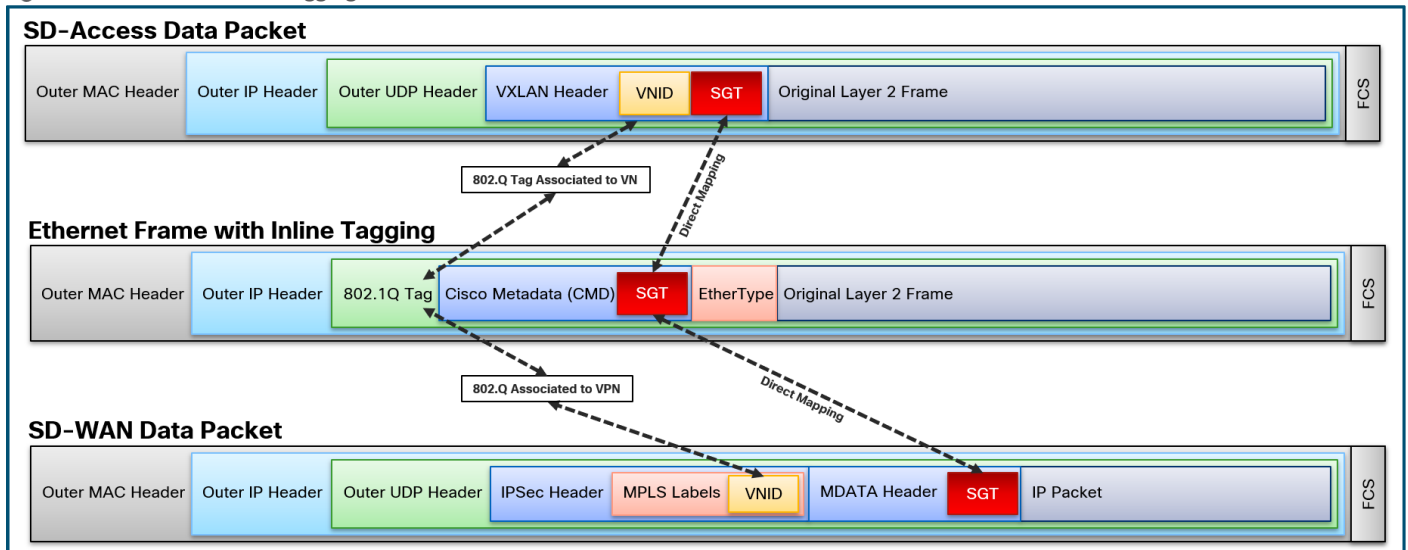
## Putting it All Together

Cisco DNA Center provides network operators the ability to automate the LAN segment with SD-Access workflows. Cisco vManage SD-WAN Controller provides WAN segment automation with feature templates. In the *Independent Domain* deployment model, there is no integration between the domain controllers. This provides enterprise deployments the flexibility to completely isolate the two domains and provision and manage respective network devices independently while still gaining the benefits of Cisco SD-Access: maintaining end-to-end segmentation and consistent policy across sites.

With the *Independent Domain* deployment:

- The Virtual Network segmentation in the Cisco SD-Access environment is mapped to corresponding service VPN on the WAN Edge device to extend the macro-segmentation.
- The Scalable Group Tag is carried from the Cisco SD-Access environment to the WAN Edge router on the Layer 3 handoff interface with additional Cisco TrustSec Inline configuration.
- The WAN Edge device transfers the SGT data from the CTS-inline tagged ethernet header frame and carries it across the WAN environment in the IPSec data packet header preserving the micro-segmentation.

Figure 9. VXLAN to Inline Tagging to IPSec





## Design

This chapter is organized into the following sections:

Chapter	Section
Design	<a href="#">SD-WAN Flexible Topologies Overview</a>
	<a href="#">SD-WAN High Availability Topologies</a>
	<a href="#">SD-Access Flexible Topologies Overview</a>
	<a href="#">Flexible Topologies Integration</a>
	<a href="#">Independent Domain Design Considerations</a>

This section discusses design consideration, provides an overview of the topology used in this guide, and deployment steps to build distributed SD-Access fabric sites interconnect with the SD-WAN transport using the *Independent Domain* deployment approach.

### SD-WAN Flexible Topologies Overview

Cisco SD-WAN solution provides flexibility in creating various WAN overlay topologies. By default, Cisco WAN Edge devices establish full-mesh IPsec data plane connections with other WAN Edge devices in the SD-WAN overlay infrastructure. Depending on the size of the network, it might not be desirable to build full-mesh WAN topology either due to routing platform limitations or number of tunnels the router can support.

Based on the deployment requirements, SD-WAN overlay network can be modified to establish hub-and-spoke, partial-mesh, or a combination of both with simple control policies defined in vManage. Additionally, any SD-WAN specific use-cases such as Direct Internet Access (DIA), Application-Aware Routing, and App QoE can be provisioned and monitored from vManage .

Please refer to [Cisco SD-WAN Design Guide](#) for design recommendation and best practices to build SD-WAN infrastructure.

Figure 10. SD-WAN Hub-and-Spoke Deployment

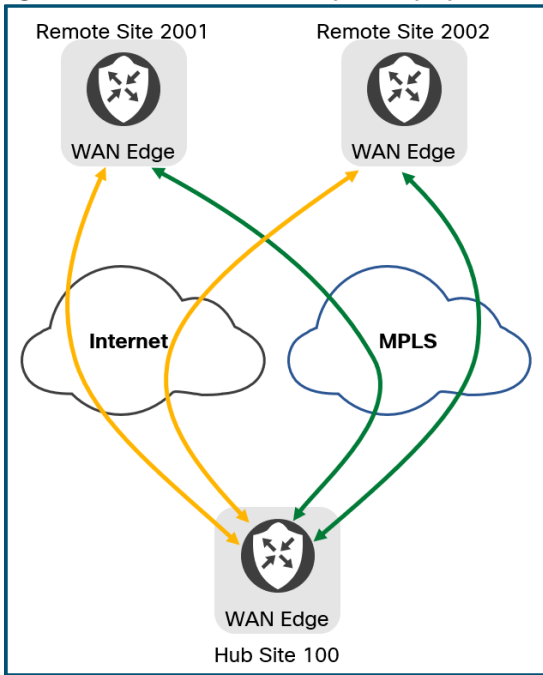


Figure 11. SD-WAN Partial-Mesh Deployment

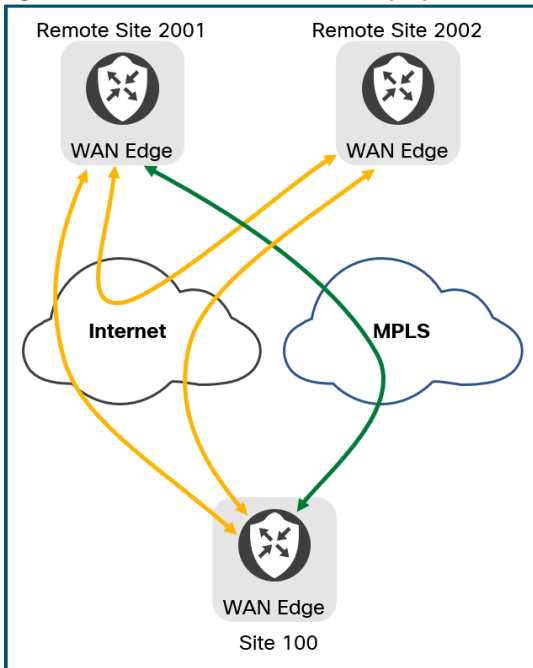
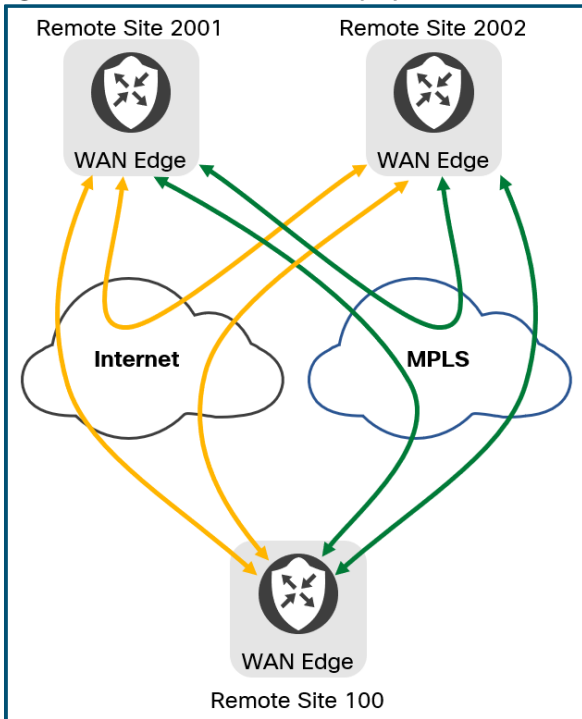


Figure 12. SD-WAN Full-Mesh Deployment



### SD-WAN High Availability Topologies

High Availability in the SD-WAN network can be achieved through several different topologies. For high availability in the physical network, a WAN Edge device can connect to multiple WAN transports. For high availability in the physical network and physical devices, two WAN Edge devices can be deployed in a dual multihomed topology where both WAN Edge devices connect to both WAN transports. For environments that cannot dual multihome, an alternative is single multihoming. Each WAN Edge device is connected to a single WAN transport, and the TLOC Extension is used between the routers to connect to the other WAN Transport.

Figure 13. Single WAN Edge Dual Homed

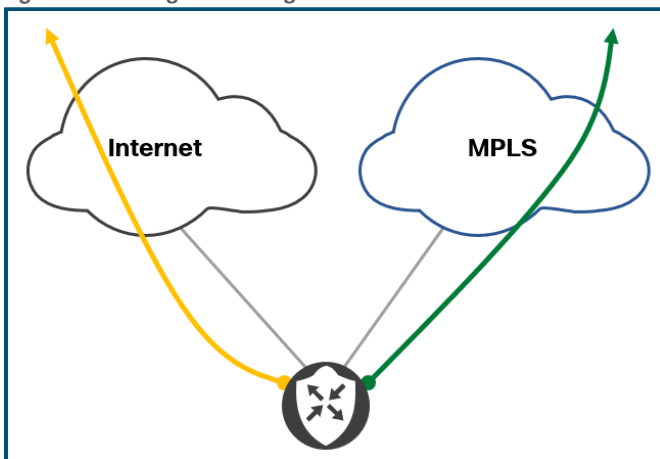


Figure 14. Two WAN Edge Devices Dual Multihomed

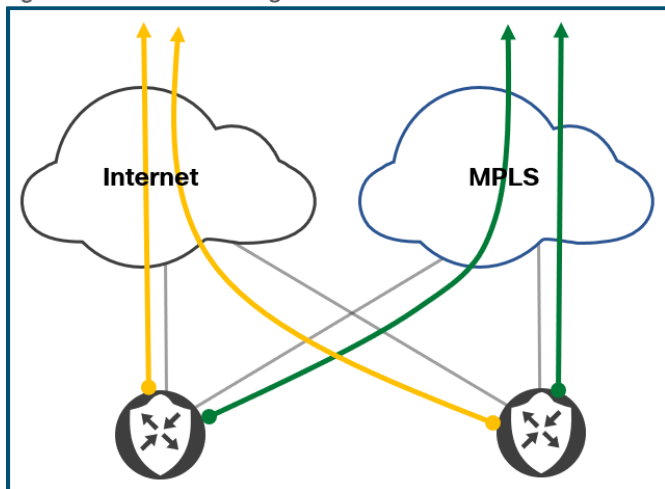
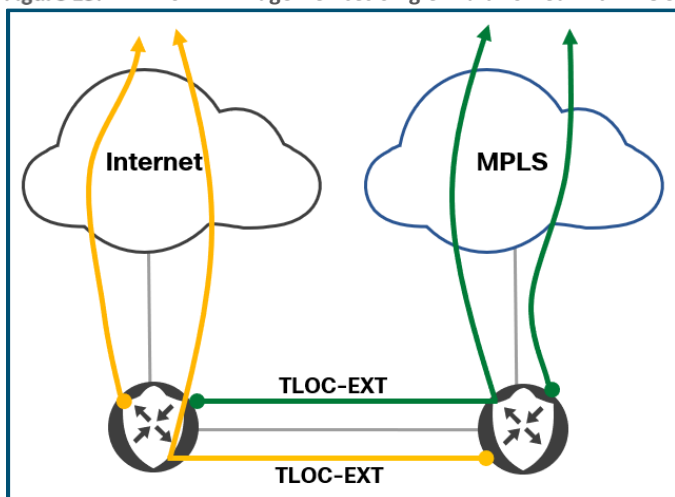


Figure 15. Two WAN Edge Devices Single Multihomed with TLOC Extension



### SD-Access Flexible Topology Overview

Having a well-designed network foundation on which to build the overlay ensures the highest stability, performance, and most efficient utilization of the SD-Access network. This underlay network foundation can be built manually, which provides the largest degree of configuration granularity or automated through Cisco DNA Center LAN Automation. LAN Automation is the Plug-n-Play (PnP) zero-touch automation of the underlay network in the SD-Access solution. The simplified procedure builds a solid, error-free underlay network using the principles of a Layer 3 routed access design.

Whether using Layer 2 switched access or Layer 3 routed access, the network should utilize full-mesh, equal-cost routing paths leveraging Layer 3 forwarding in the core and distribution layers of the network to provide the most reliable and fastest converging design for those layers. For optimum convergence at the core and distribution layer, build triangles, not squares, to take advantage of equal-cost redundant paths.

Please refer to [Cisco SD-Access Solution Design Guide - Underlay Network Design Chapter](#) for design recommendation and best-practices to build SD-Access infrastructure.

When deploying the SD-Access fabric nodes, the reference network architecture provisions the fabric roles in the same way the underlying network architecture is built: *distribution of function*. Separating roles onto different devices provides the highest

degree of availability, resilience, deterministic convergence, and scale. Based on the deployment requirements, [colocation of function](#) is supported, including colocating the SD-Access Border and Control Plane Nodes. For small branch and remote locations, [Fabric in a Box](#) (with or without Embedded Wireless) can be utilized. This deployment option provides flexibility at very small locations by colocating the Border Node, Control Plane Node, and Edge Node function with the option of also deploying the SD-Access Wireless Controller. These solution deployment options provide flexibility to design a zero-trust, highly-resilient, and always-available wired and wireless infrastructure as shown in [Figure 16](#) below.

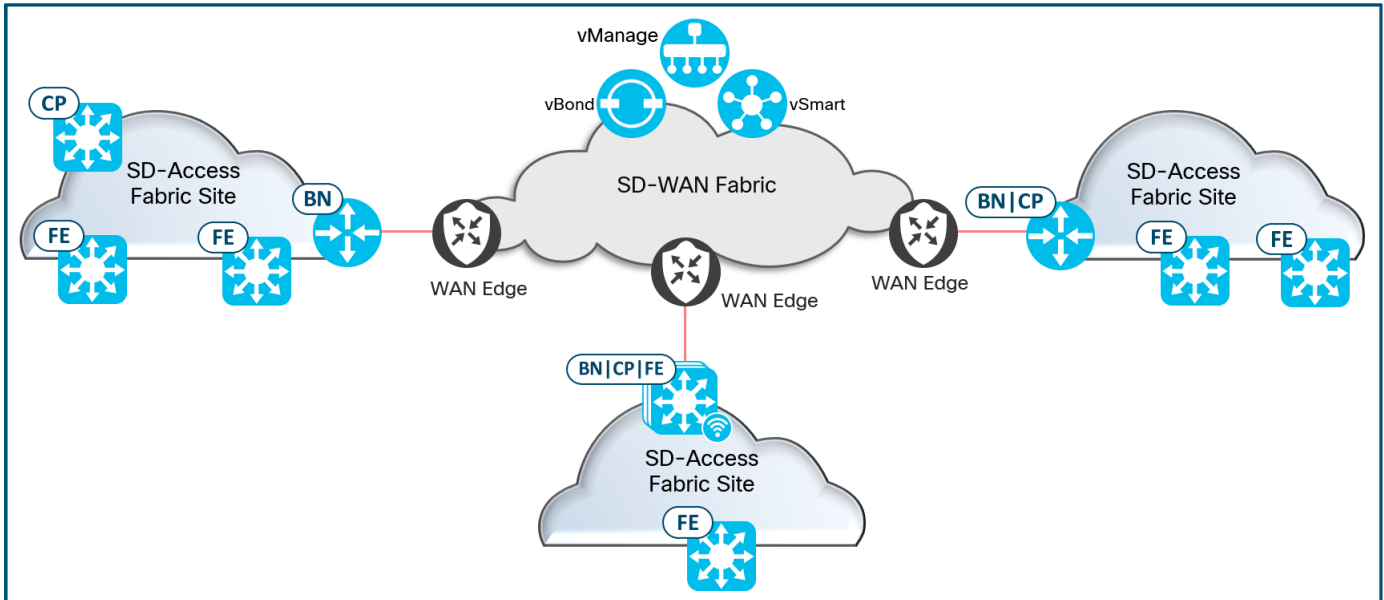
Please refer to [Cisco SD-Access Solution Design Guide](#) for further design recommendation and best practices to build SD-Access infrastructure.

### Flexible Topology Integration

With *Integrated Domain* SD-Access | SD-WAN Pairwise Integration, the SD-Access fabric sites must be new deployments. With *Independent Domain*, there is increased flexibility. The SD-Access fabric sites can be new or existing sites. The SD-WAN Edge routers at these locations can be new or existing as well. *Independent Domain* provides significant flexibility by separating the two domains, with still preserving:

- End-to-end macro- and micro-segmentation across the enterprise.
- Consistent policy for wired and wireless across the fabric sites.
- Consistent network access experience for any users, any device, any application at any location in the network.

**Figure 16. Flexible Topologies Example**



### Independent Domain Design Considerations

This chapter is organized into the following sections:

Chapter	Section
Design Considerations	<a href="#">Service VPN and VN Considerations</a> <a href="#">Underlay Infrastructure Considerations</a> <a href="#">MTU Considerations</a> <a href="#">Latency Considerations</a> <a href="#">Scale Considerations</a> <a href="#">Platform Requirements for Inline Tagging</a> <a href="#">Macro-Segmentation Considerations</a> <a href="#">Micro-Segmentation Considerations</a> <a href="#">SD-WAN Edge SGT Forwarding Interoperability</a>

### Service VPN and VN Considerations

Cisco SD-WAN components have two predefined Service VPNs: VPN 0 and VPN 512. WAN Edge devices leverage routes in VPN 0, which is associated with the WAN Global Routing Table (GRT), to securely connect to the SD-WAN controllers and establish secure control and data plane connections with other SD-WAN routers. VPN 512 is the Management VPN which provides out-of-band (OOB) management access for the SD-WAN devices.

Network administrators can configure additional Service VPNs to segment the LAN traffic across the WAN environment. The supported VPN numbers are VPN 1 through VPN 511 (1-511) and VPN 513 through VPN 65500 (513-65500). Other VPNs IDs are reserved for internal use by the WAN Edge device and should be avoided as the routes in these reserved VPN IDs are not shared across the WAN environment.

Each Layer 3 Virtual Network in the SD-Access environment is mapped to a corresponding Service VPN in the SD-WAN environment. The SD Access fabric site underlay, which is part of the global routing table (GRT), is mapped to a dedicated Service VPN on the WAN Edge devices. This same service VPN must be used at all fabric sites to provide end-to-end IP reachability for the devices within the fabric site.

#### Tech tip

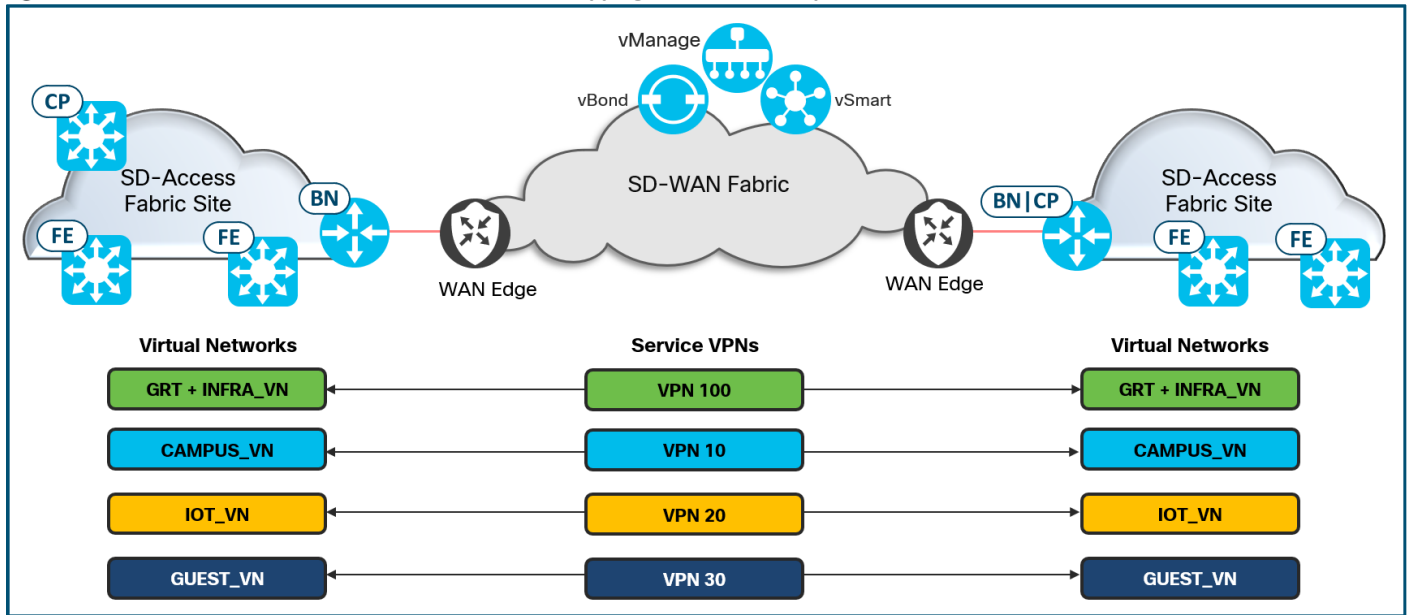
The SD-WAN Global Routing Table uses VPN 0 to build the WAN Fabric. The SD-Access Global Routing Table maps to a user-defined SD-WAN Service VPN. The SD-WAN GRT and SD-Access GRT do not need to communicate with each other and are not mapped together.

### Underlay Infrastructure Considerations

Cisco SD-Access fabric site's *underlay* is defined by the physical switches and routers that are used to deploy the SD-Access overlay network. Establish a stable, resilient, and fast converged underlay either manually or using LAN Automation. Please refer to the [Cisco SD-Access Design Guide](#) on design requirements and recommendations to build resilient and highly-available networks for an SD-Access Deployment.

Cisco SD-WAN Edge devices connect to the SD-Access infrastructure using a Layer 3 routed interface. Deployments can have a WAN Edge with a dedicated link for underlay and another interface for Layer 3 handoff (or) a single interface carrying both underlay and overlay towards the SD-Access fabric border network device.

Figure 17. SD-Access VN and SD-WAN Service VPN – Mapping Across the Enterprise



### MTU Considerations

Cisco SD-Access VXLAN header adds additional 50 bytes, optionally 54 bytes, of encapsulation overhead. On switching platforms in SD-Access, the MTU is increased at system level with `'system MTU <mtu value>'` command which tunes the MTU on all the interfaces. On routing platforms, the MTU is set per interface using the command `'mtu <mtu value>'` on the physical interface. This MTU value is inherited by all sub-interfaces associated with the physical interface.

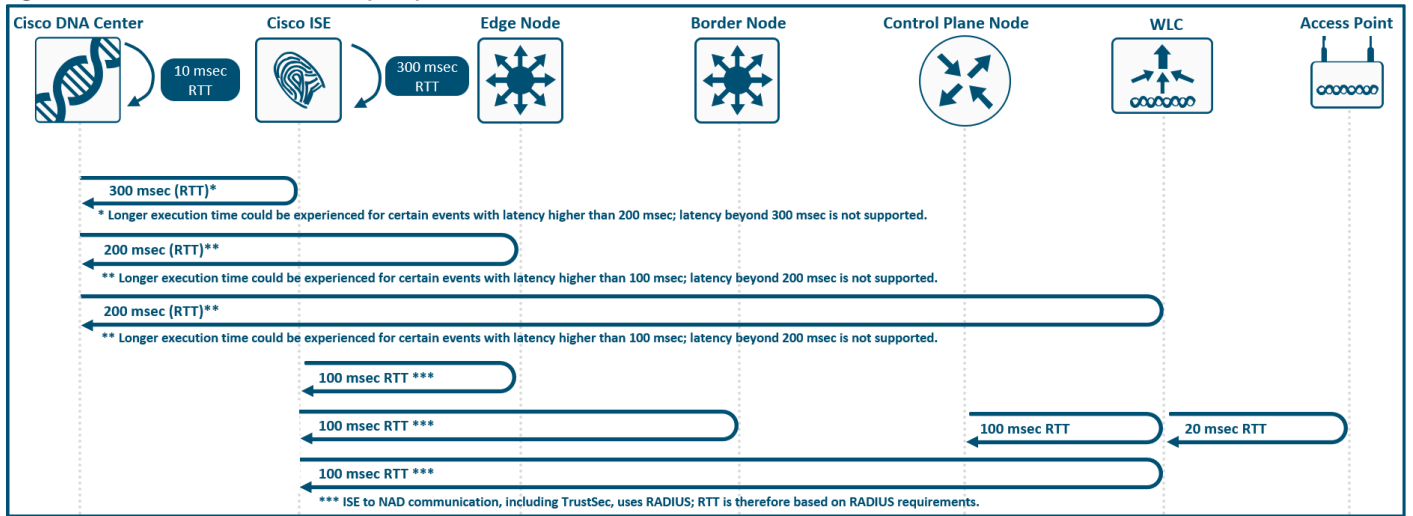
Cisco SD-WAN Edge devices use the default MTU of 1500 bytes on the physical interfaces. Sub-interfaces are used to keep the end-to-end data plane segmentation which results in an additional 4 bytes that are needed to carry the 802.1Q tag. As shown later in the guide, the IP MTU on the WAN Edge sub-interfaces is configured as 1500 bytes. The border node's physical and logical interfaces connecting to the WAN Edge router should be configured to match the IP MTU on the WAN Edge sub-interface to ensure IP packets are transported between the devices without fragmentation or drops.

MTU within the SD-WAN environment is addressed using Bidirectional Forwarding Detection (BFD) packets. These packets are used to periodically probe each WAN transports for path liveliness and quality, which includes tunnel status, loss/latency/jitter, and IPSec tunnel MTU. WAN Edge devices use this probing information to natively fragment and reassemble the packet before forwarding them on the WAN transport

### Latency Considerations

Latency in the network is an important consideration for performance, and the RTT between Cisco DNA Center and any network device it manages must be taken into strict account. The RTT should be equal to or less than 100 milliseconds to achieve optimal performance for all solutions provided by Cisco DNA Center including SD-Access. The maximum supported latency is 200ms RTT. Latency between 100ms and 200ms is supported, although longer execution times could be experienced for certain functions including Inventory Collection, Fabric Provisioning, SWIM, and other processes that involve interactions with the managed devices.

Figure 18. Cisco SD-Access Latency Requirements



### SD-Access Scale Considerations

SD-Access has a number of scaling components that must be taken into consideration. Platform-specific scale includes items such as the number of endpoints, the number of virtual networks, the number of routes, and the number of SGTs. Cisco DNA Center has scale components such as the number of fabric sites, the number of fabric devices within a site, and the total number of concurrent endpoints. For details, please consult the SD-Access Platform Scale, Appliance Scale, and Fabric VN Scale Tables on the Cisco DNA Center [data sheet](#).

### Platform Requirements for Inline Tagging

Cisco SD-Access | SD-WAN *Independent Domain* Integration requires the Interface that connects the WAN Edge and the SD-Access Fabric Border to support Cisco TrustSec SGT Inline tagging. Refer to the [SD-WAN Security Configuration Guide](#) for the supported platform and NIM modules on the WAN Edge devices and the [Cisco Group Based Policy System Bulletin](#) for supported platforms on the SD-Access devices.

The following tables list the supported hardware and network interface module (NIM) that are supported for SD-WAN Edge devices and support SGT Inline Tagging.



**Table 2.** Independent Domain SD-WAN Edge Supported Platforms

Supported Hardware	Additional Details
ISR 1000 Series Routers	The ISR 1000 Series Routers support up to two WAN ports only.
ISR 4200 Series Routers	–
ISR 4300 Series Routers	–
ISR 4400 Series Routers	–
ASR 1001-X Series Routers	–
ASR 1002-X Series Routers	–
ASR 1001-HX Series Routers	–
ASR 1002-HX Series Routers	–
Cisco 5000 Series ENCS	WAN Ports Only
CSR 1000V	–
Catalyst 8000 Series Edge Platforms	Cisco DNA Center ≥2.1.2.6 IOS XE ≥17.3.3

**Table 3.** Independent Domain SD-WAN Edge Supported Network Modules

Supported Network Modules	Additional Details
NIM-1GE-CU-SFP	ISR 4000 Series WAN Module <a href="#">Data Sheet</a>
NIM-2GE-CU-SFP	ISR 4000 Series WAN Module <a href="#">Data Sheet</a>
SM-X-6X1G	ISR 4000 Series WAN Module <a href="#">Data Sheet</a>
SM-X-4X1G-1X10	ISR 4000 Series WAN Module <a href="#">Data Sheet</a>
C-NIM-1X	Cisco Catalyst 8300 Series Edge Platforms Cisco DNA Center ≥2.1.2.6 IOS XE ≥17.3.3

### Macro-Segmentation Considerations

Cisco DNA Center can automate the handoff configuration on the border nodes through an *IP-based Layer 3 handoff*. By *IP-based*, this means native IP forwarding, rather than VXLAN encapsulation, is used; the fabric packet is de-encapsulated before being forwarded. The configuration is *Layer 3* which means it uses sub-interfaces when the border node is a routing platform or Switched Virtual Interfaces (SVIs) when the border node is a switching platform, to connect to the upstream peers.

This Layer 3 handoff automation provisions VRF-lite by associating each SVI or sub-interface with a different fabric VN (VRF). External BGP is used as the routing protocol to advertise the endpoint space (EID-space) prefixes from the fabric site to the

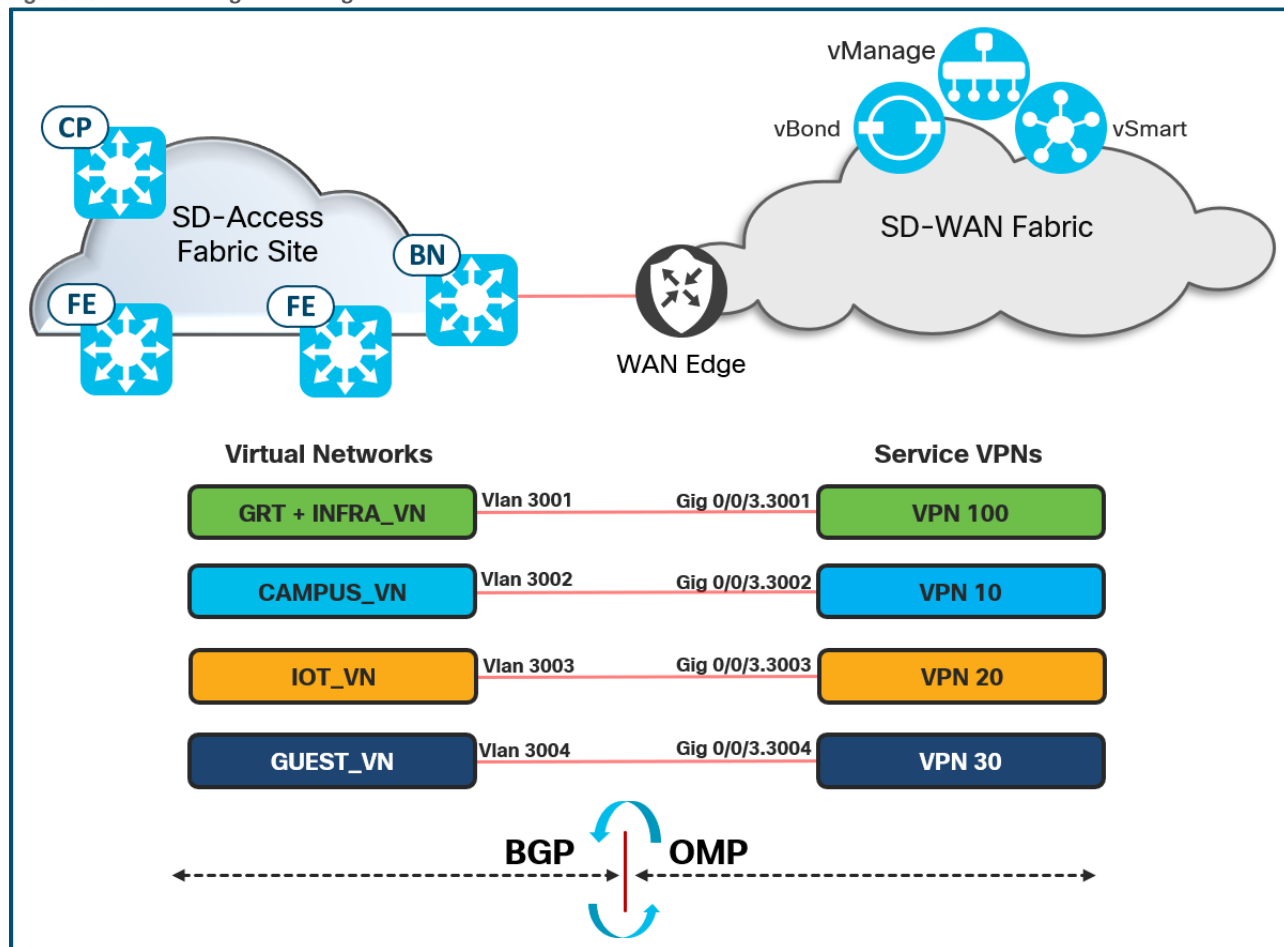
external routing domain and to attract traffic back to the EID-space. This BGP peering can also be used to advertise routes into the overlay such as for access to shared services.

This handoff is used to establish a BGP neighborhood with the WAN Edge router for each Virtual Network. This allows the border node to extend the SD-Access Virtual Network prefixes to a corresponding WAN Edge Service VPN while ensuring data plane isolation. BGP prefixes learned on the WAN Edge device, via eBGP neighborhood from the fabric border, are mutually redistributed into OMP to advertise the EID-space across the WAN environment to remote sites. The global routing table in the SD-Access fabric site (SD-Access underlay) must be mapped to a dedicated service VPN on the WAN Edge devices to provide reachability between fabric devices across sites.

**Tech tip**

Optionally, deployments with the requirement to do route leaking between shared services and the SD-Access network at the local site can leverage the vManage policies to perform Service VPN route leaking between prefixes in the Service VPN associated with shared services and the Service VPN(s) associated with the fabric VNs.

**Figure 19. Extending Macro-Segmentation – SD-Access VN to SD-WAN Service VPN**



### Micro-Segmentation Considerations

Cisco TrustSec Inline Tagging on the WAN Edge device is enabled using the *Cisco VPN Interface Ethernet* Feature Template in vManage. On the WAN Edge device, inline tagging configuration is applied on the physical interface and on each associated sub-interface that connects to the border node.

Inline tagging on the border node can either be performed manually using the CLI or through using Cisco DNA Center Day-N templates. On routing platforms, the inline tagging configuration is applied to the physical interface and on each associated sub-interface that connects to the WAN Edge router. On switching platforms, inline tagging is applied on the physical trunk interface that connects to the WAN Edge router. If the interface is deployed as an EtherChannel, inline tagging configuration is applied to each member interface and not to the port-channel itself.

Tech tip
When CTS inline tagging is enabled on an interface, the interface flaps which results in loss of connectivity for a brief period. In Cisco IOS XE SD-WAN software version used in this prescriptive guide, SD-WAN devices will drop untagged frames while the border nodes do not. Therefore, it is recommended to enable inline tagging on the WAN Edge router first, wait for the link to flap and return to the <i>Up/Up</i> state, and then enable inline tagging on the border node interface.

## SD-WAN Edge SGT Forwarding Interoperability

Cisco SD-WAN solution can contain WAN Edge devices running either IOS-XE SD-WAN or Viptela software. For the Cisco SD-Access | SD-WAN Pairwise Integration, it is required to deploy supported IOS-XE SD-WAN Edge devices running  $\geq 17.3.2a$ .

The following table shows the interoperability behavior for various WAN Edge platforms and their corresponding software version with respect to carrying SGTs in the data plane.

**Table 4.** SD-WAN Forwarding Interoperability

Traffic To	$\geq$ IOS XE 17.3.x SD-WAN (CTS Enabled)	$\geq$ IOS XE 17.3.x SD-WAN (CTS NOT Enabled)	<IOS XE 17.2.x SD-WAN	Colocated SD-Access IOS XE WAN Edge	vEdge Router
Traffic From					
$\geq$ IOS XE 17.3.x SD-WAN (CTS Enabled)	SGT carried in MDATA Header.	IP and SGT are carried; SGT is discarded.	Traffic is sent without SGT.	SGT carried in MDATA Header.	Traffic is sent without SGT.
$\geq$ IOS XE 17.3.x SD-WAN (CTS NOT Enabled)	Traffic is sent without SGT.	Traffic is sent without SGT.	Traffic is sent without SGT.	Traffic is sent without SGT.	Traffic is sent without SGT.
<IOS XE 17.2.x SD-WAN	Traffic is sent without SGT.	Traffic is sent without SGT.	Traffic is sent without SGT.	Traffic is sent without SGT.	Traffic is sent without SGT.
Colocated SD-Access IOS XE WAN Edge	SGT carried in MDATA Header.	IP and SGT are carried; SGT is discarded.	Traffic is sent without SGT.	SGT carried in MDATA Header.	Traffic is sent without SGT.
vEdge Router	Traffic is sent without SGT.	Traffic is sent without SGT.	Traffic is sent without SGT.	Traffic is sent without SGT.	Traffic is sent without SGT.

## TrustSec Inline Tagging Configuration Conventions

A standard template and configuration convention is used to ensure consistent behavior across platforms that support CTS inline tagging. This standard convention uses the SGT value of 2 as, by default in ISE, this SGT value is assigned to the *TrustSec\_Devices* Security Group (SG).

The SGT value that is assigned can technically be any value that is registered and defined in ISE, that has a human-readable, relevant name and description to the administrator, and that is not used for another purpose or assigned to another SG in the TrustSec domain.

---

The recommended practice in inline tagging is to assign a single SGT to all CTS network devices, to ensure that SGT value is assigned in ISE for **TrustSec\_Devices** SG devices, and to use the SGT value of 2. The value can be changed for policy reasons though that practice calls for careful consideration. If changed, the corresponding SGT in ISE must be changed for full system continuity and integrity.

**Tech tip**

For further details on this configuration convention along with its background and history, please see [Appendix E](#).

# Deploy

This chapter is organized into the following sections:

Chapter	Section
Deploy	<a href="#">Deployment Topology Overview</a>
	<a href="#">Deployment Prerequisites</a>
	<a href="#">Deployment Steps</a>

This section provides an overview of the topology used throughout this guide and covers the prerequisites and steps needed for this *Independent Domain* deployment.

## Deployment Topology Overview

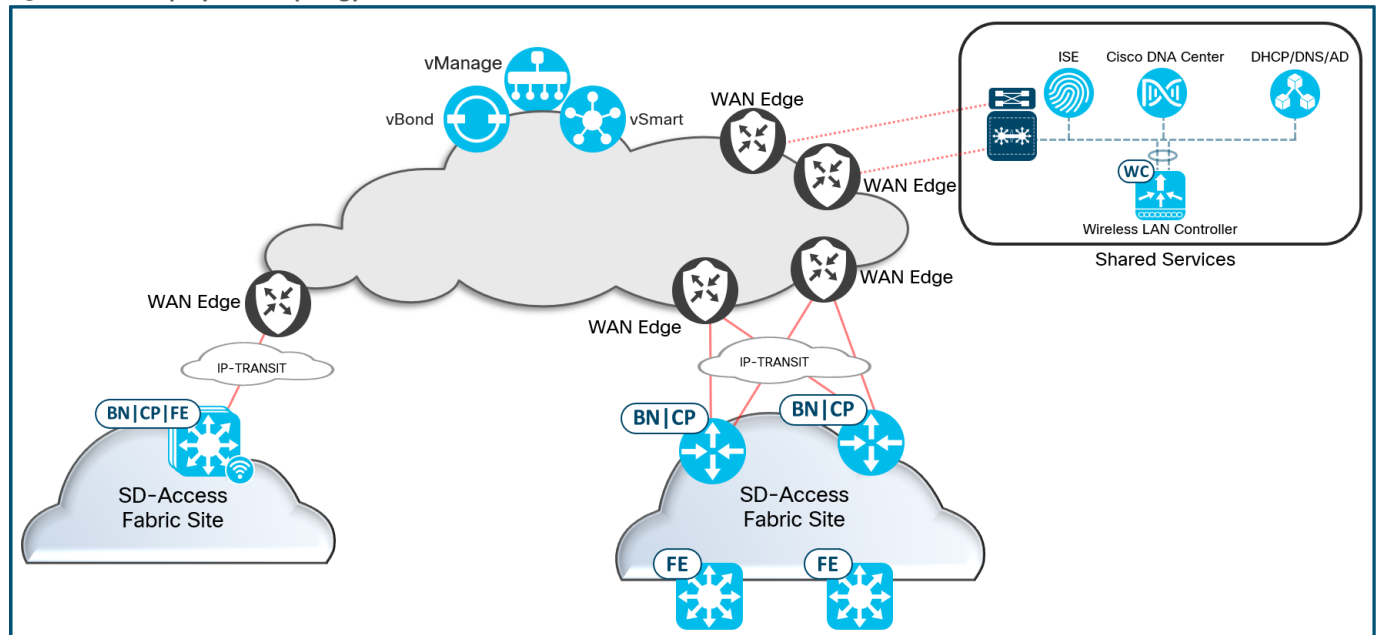
The validation topology has two SD-Access fabric sites connected via a Cisco SD-WAN Fabric representing a branch site and headend location. At the branch, a Fabric in a Box is deployed with an Embedded Wireless Controller. It is directly connected to a WAN Edge router.

At the headend site, two colocated Border and Control Plane Nodes are deployed. Each is directly connected to the two WAN Edge routers present at this location.

Cisco DNA Center, the Identity Service Engine, and shared services such as the DHCP, DNS, and Windows Active Directory (AD) servers are deployed at an on-premises data center that is accessible through the SD-WAN fabric.

The Cisco SD-WAN controllers are deployed in the enterprise private cloud. The WAN Edge routers are connected to both an Internet WAN transport and MPLS transport.

Figure 20. Deployment Topology



## Deployment Prerequisites

Before beginning with this guide, the following items must be completed in advance.

- Cisco SD-WAN Controllers (vManage, vBond, and vSmart) are deployed with valid certificates.
- *Independent Domain* supported Cisco WAN Edge devices are onboarded and have established secure control connections with the Cisco SD-WAN controllers and secure data plane connections to the other WAN Edge devices in the SD-WAN environment using all available WAN transports.
- Cisco DNA Center is installed and integrated with the Identity Services Engine as an Authentication and Policy Server.
- The Design Application in Cisco DNA Center is appropriately configured for the deployment. This includes the Network Hierarchy and Network Settings such as Device Credentials, IP Address Pools, and Wireless settings for each fabric site.
- The SD-Access fabric is deployed at both locations. The border nodes are connected to the WAN Edge routers and have IP reachability to Cisco DNA Center.

## Deployment Steps

The validated deployment is divided into the following processes and procedures:

Process	Procedure
<a href="#">Verifying Prerequisites for Independent Domain</a>	<a href="#">Verify the SD-WAN Infrastructure</a> <a href="#">Verify the WAN Edge Secure Data Plane Connections</a> <a href="#">Verify Cisco DNA Center is Installed with SD-Access Application</a> <a href="#">Verify Cisco DNA Center is Integrated with ISE</a> <a href="#">Verify Cisco DNA Center Design Application Configuration</a> <a href="#">Verify SD-Access Fabric Site is Deployed</a> <a href="#">Verify the SD-Access Border Node Layer 3 Handoff Configuration</a> <a href="#">Verify the WAN Edge End-to-End Reachability</a>
<a href="#">Configuring Cisco TrustSec Inline Tagging</a>	<a href="#">Identify vManage Feature Templates Association</a> <a href="#">Configure CTS Inline Tagging on the SD-WAN Edge Physical Interface</a> <a href="#">Configure CTS Inline Tagging on the SD-WAN Edge Sub-interface</a> <a href="#">Configure Cisco TrustSec Inline Tagging on the Border Node</a>
<a href="#">Defining Group-Based Access Control Policies</a>	<a href="#">Configure Group-Based Access Control Policies</a> <a href="#">(Optional) Provision Static Host Onboarding on the Edge Node</a>

### Process 1: Verifying Prerequisites for *Independent Domain*

Before beginning the Independent Domain deployment, the SD-WAN and SD-Access controllers must be deployed, and their respective devices onboarded and provisioned.

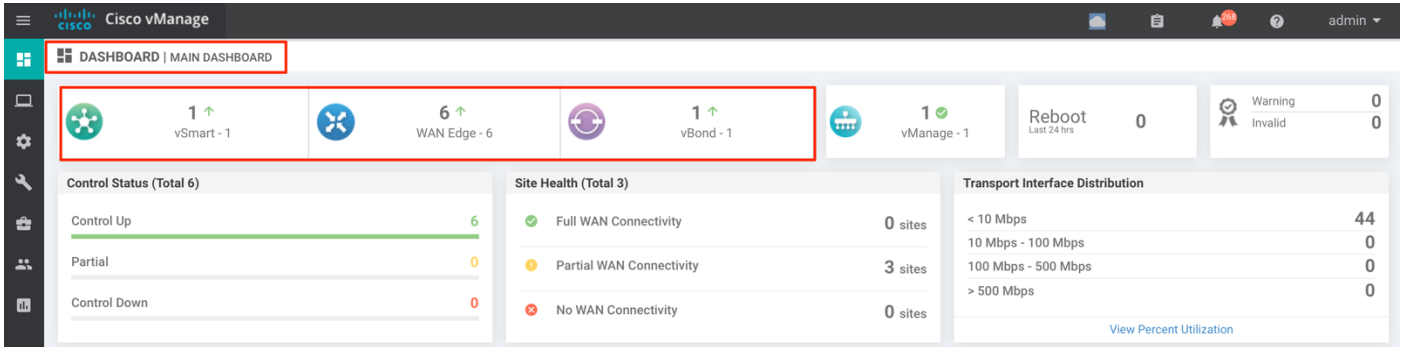
#### Procedure 1. Verify the SD-WAN Infrastructure

Use this procedure to verify that vManage, vBond, vSmart, and the WAN Edge devices are successfully onboarded, in healthy state, and to verify their applicable software versions.

**Step 1.** Login to vManage and navigate to **Dashboard > Main Dashboard**.

**Step 2.** Verify the state of vManage, vBond, vSmart, and the WAN Edge devices.

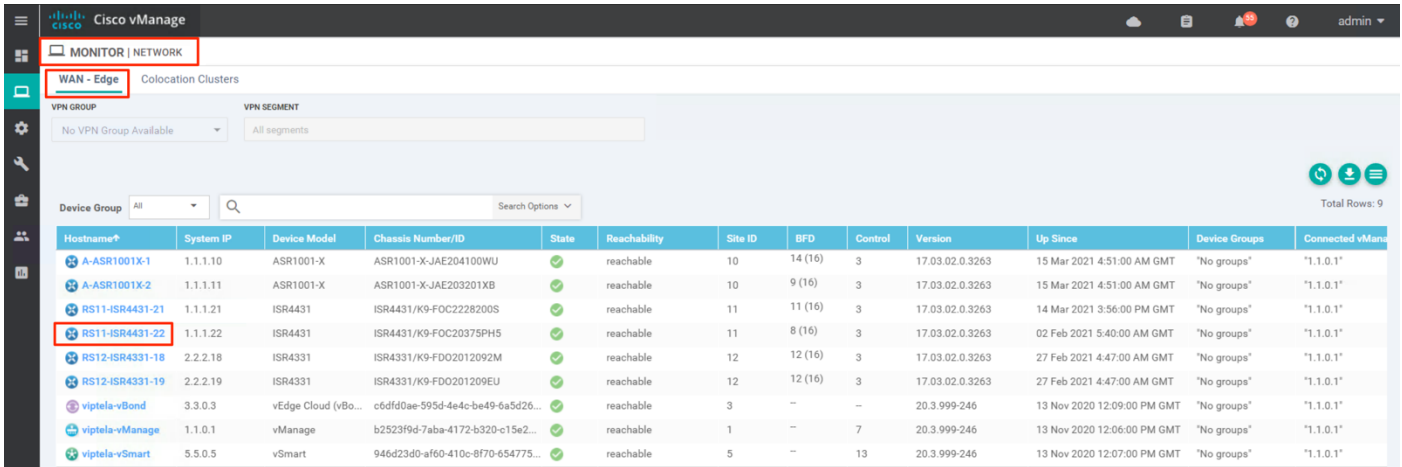
The  green up arrow indicates a healthy, onboarded state.



The screenshot shows the Cisco vManage Main Dashboard. A red box highlights the top row of summary cards: vSmart - 1 (with a green up arrow), WAN Edge - 6 (with a green up arrow), and vBond - 1 (with a green up arrow). Other cards show vManage - 1 (with a green checkmark), Reboot (0), and Warning Invalid (0). Below these are three sections: Control Status (Total 6) with Control Up at 6, Partial at 0, and Control Down at 0; Site Health (Total 3) with Full WAN Connectivity at 0 sites, Partial WAN Connectivity at 3 sites, and No WAN Connectivity at 0 sites; and Transport Interface Distribution with < 10 Mbps at 44, 10 Mbps - 100 Mbps at 0, 100 Mbps - 500 Mbps at 0, and > 500 Mbps at 0.

**Step 3.** In vManage, navigate to **Monitor > Network**.

**Step 4.** Select the device from the **WAN - Edge** list.

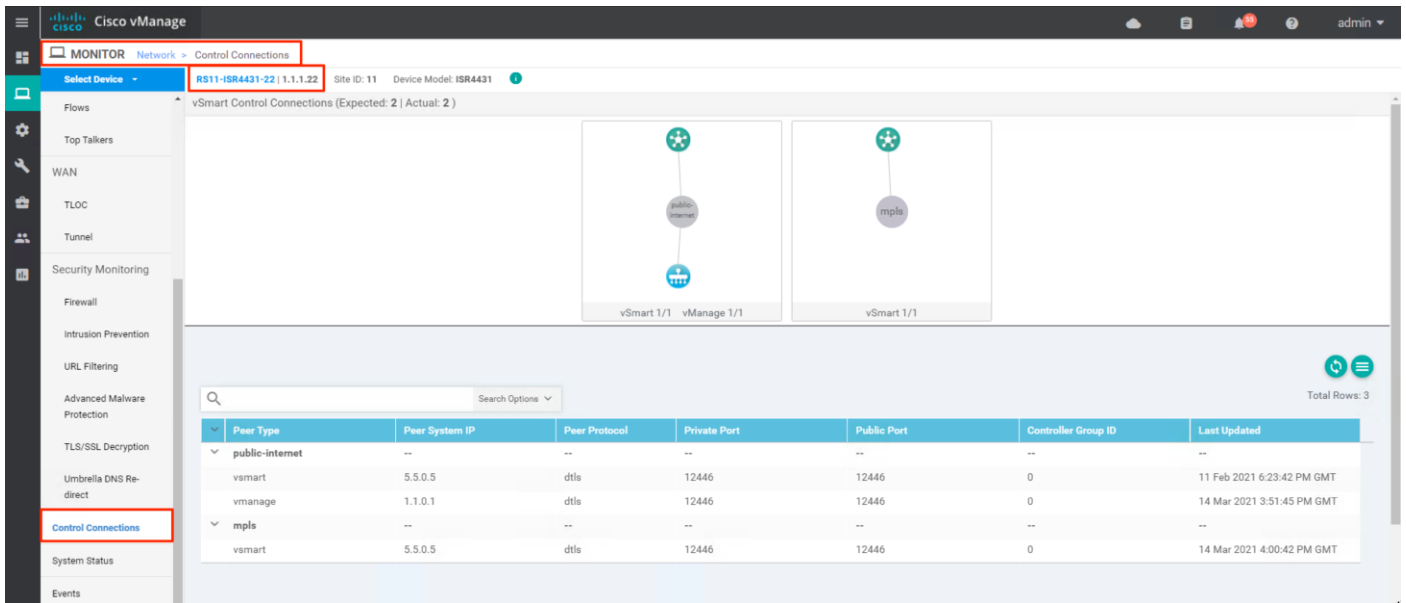


The screenshot shows the Cisco vManage Monitor Network WAN - Edge list. A red box highlights the 'WAN - Edge' tab. Below it is a table of devices. The row for 'RS11-ISR4431-22' is highlighted with a red box. The table has columns for Hostname, System IP, Device Model, Chassis Number/ID, State, Reachability, Site ID, BFD, Control, Version, Up Since, Device Groups, and Connected vManage.

Hostname	System IP	Device Model	Chassis Number/ID	State	Reachability	Site ID	BFD	Control	Version	Up Since	Device Groups	Connected vManage
A-ASR1001X-1	1.1.1.10	ASR1001-X	ASR1001-X-JAE204100WU	✓	reachable	10	14 (16)	3	17.03.02.0.3263	15 Mar 2021 4:51:00 AM GMT	"No groups"	"1.1.0.1"
A-ASR1001X-2	1.1.1.11	ASR1001-X	ASR1001-X-JAE203201XB	✓	reachable	10	9 (16)	3	17.03.02.0.3263	15 Mar 2021 4:51:00 AM GMT	"No groups"	"1.1.0.1"
RS11-ISR4431-21	1.1.1.21	ISR4431	ISR4431/K9-FOC228200S	✓	reachable	11	11 (16)	3	17.03.02.0.3263	14 Mar 2021 3:56:00 PM GMT	"No groups"	"1.1.0.1"
RS11-ISR4431-22	1.1.1.22	ISR4431	ISR4431/K9-FOC20375PH5	✓	reachable	11	8 (16)	3	17.03.02.0.3263	02 Feb 2021 5:40:00 AM GMT	"No groups"	"1.1.0.1"
RS12-ISR4331-18	2.2.2.18	ISR4331	ISR4331/K9-FDO2012092M	✓	reachable	12	12 (16)	3	17.03.02.0.3263	27 Feb 2021 4:47:00 AM GMT	"No groups"	"1.1.0.1"
RS12-ISR4331-19	2.2.2.19	ISR4331	ISR4331/K9-FDO201209EU	✓	reachable	12	12 (16)	3	17.03.02.0.3263	27 Feb 2021 4:47:00 AM GMT	"No groups"	"1.1.0.1"
viptela-vBond	3.3.0.3	vEdge Cloud (vBo...	c6dfd0ae-595d-4e4c-be49-6a5d26...	✓	reachable	3	-	-	20.3.999-246	13 Nov 2020 12:09:00 PM GMT	"No groups"	"1.1.0.1"
viptela-vManage	1.1.0.1	vManage	b2523f9d-7aba-4172-b320-c15e2...	✓	reachable	1	-	7	20.3.999-246	13 Nov 2020 12:06:00 PM GMT	"No groups"	"1.1.0.1"
viptela-vSmart	5.5.0.5	vSmart	946d23d0-af60-410c-8f70-654775...	✓	reachable	5	-	13	20.3.999-246	13 Nov 2020 12:07:00 PM GMT	"No groups"	"1.1.0.1"

**Step 5.** Select **Control Connections** from the left panel to view the device control connections status.

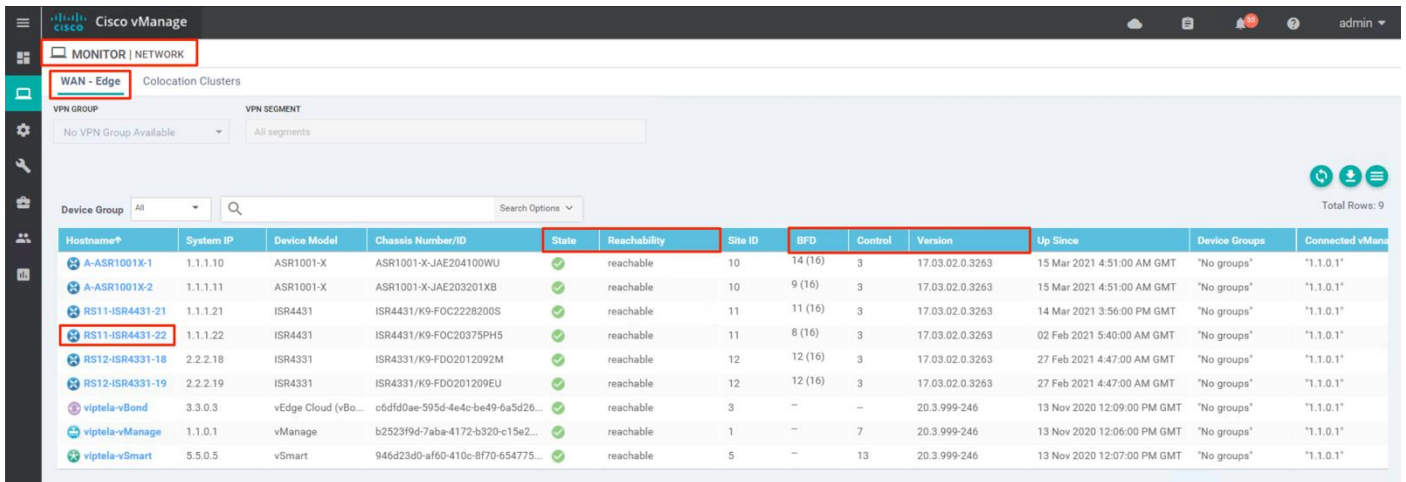
Verify the DTLS session are established with the SD-WAN controllers across the available WAN Transport connections.



**Step 6.** In vManage, navigate to **Monitor > Network**.

**Step 7.** Verify the **State**, **Reachability**, **BFD**, **Control**, and **Version** sections for the devices.

- The desired **State** is **✓**.
- The desired **Reachability** is **reachable**.
- BFD and Control will vary based on the deployment though should have non-zero numbers.
- The **Version** must be **≥17.03.01a**.



**Procedure 2.** Verify the WAN Edge Secure Data Plane Connections

**Step 1.** In vManage, navigate to **Monitor > Network**.

**Step 2.** Select the device from the **WAN - Edge** list.

**Step 3.** Select **WAN > Tunnel** option from the left panel.

**Step 4.** Verify the WAN Edge device has successfully established data plane connections to other WAN Edge devices across the WAN environment.



- The desired **State** is **↑**.
- The desired **Protocol** is **IPSEC**.

The screenshot shows the Cisco vManage interface for monitoring a WAN Tunnel. The top navigation bar indicates the current view is 'MONITOR Network > WAN - Tunnel'. The selected device is 'RS11-ISR4431-22' at 'Site ID: 11' with 'Device Model: ISR4431'. The left sidebar shows various monitoring categories, with 'WAN' and 'Tunnel' highlighted. The main area features a chart for 'Loss Percentage' and 'FEC Loss Recovery Rate' over time, showing a 100% loss rate and 0% recovery rate. Below the chart is a table of tunnel endpoints.

Tunnel Endpoints	Interface Endpoints	Local Interface Description	Remote Interface Description	Protocol	State	Jitter (ms)	Loss (%)	FEC
public-internet	**	**	**	**	**	**	**	**
RS11-ISR4431-22:public-internet-A-ASR1001X-1:mpls	GigabitEthernet0/0/0-Giga...	VPN0 INET interface	VPN0 MPLS interface	IPSEC	↑	0.00	0.00	N/A
RS11-ISR4431-22:public-internet-RS12-ISR4331-18:public...	GigabitEthernet0/0/0-Giga...	VPN0 INET interface	VPN0 INET interface	IPSEC	↑	0.00	0.00	N/A

### Procedure 3. Verify Cisco DNA Center is Installed with SD-Access Application

- Step 1.** Login to Cisco DNA Center, and navigate to **System > Software Updates**,
- Step 2.** Select **Installed Apps** from the left panel.
- Step 3.** Under the **Automation** section, verify **SD Access** is installed.

The screenshot shows the Cisco DNA Center interface. The left sidebar has 'System' selected, and 'Software Updates' is highlighted in the sub-menu. The main content area shows a 'Get Started' button and a 'Critical Issues' section with 'Last 24 Hours' showing 0 issues. There are also metrics for 'Wired Clients' and 'P1'.

Cisco DNA Center System - Software Updates

Updates

Installed Apps

### Installed Applications

**Cisco DNA Center Core**

Automation - Base	2.1.210.62240	Uninstall
Cisco DNA Center Global Search	1.1.0.4	Uninstall
Cisco DNA Center UI	1.5.0.520	Uninstall
Cloud Connectivity - Data Hub	1.6.0.103	Uninstall
Cloud Connectivity - Tethering	1.3.1.44	Uninstall
NCP - Base	2.1.210.62240	Uninstall
NCP - Services	2.1.210.62240	Uninstall
Network Controller Platform	2.1.210.62240	Uninstall
Network Data Platform - Base Analytics	1.5.1.122	Uninstall
Network Data Platform - Core	1.5.1.329	Uninstall
Network Data Platform - Manager	1.5.1.90	Uninstall
RBAC Extensions	2.1.210.1900054	Uninstall
System Commons	2.1.210.62240	Uninstall

**Automation**

Application Policy	2.1.210.170157	Uninstall
Application Registry	2.1.210.170157	Uninstall
Command Runner	2.1.210.62240	Uninstall
Device Onboarding	2.1.210.62240	Uninstall
Image Management	2.1.210.62240	Uninstall
SD Access	2.1.210.62240	Uninstall
Stealthwatch Security Analytics	2.1.210.1090128	Uninstall

**Procedure 4. Verify Cisco DNA Center is Integrated with the Identity Services Engine**

- Step 1.** In Cisco DNA Center, navigate to **System > Settings**.
- Step 2.** Under **External Services**, select **Authentication and Policy Servers** from the left panel.
- Step 3.** Verify the ISE server is integrated and in **ACTIVE** state.

Cisco DNA Center System - Settings

Settings / External Services

### Authentication and Policy Servers

Use this form to specify the servers that authenticate Cisco DNA Center users. Cisco Identity Services Engine (ISE) servers can also supply policy and user information.

Last updated: 10:01 AM Refresh Export Add

IP Address	Protocol	Type	Status
<input type="radio"/> 10.4.250.200	RADIUS_TACACS	ISE	ACTIVE

**Procedure 5. Verify Cisco DNA Center Design Application Configuration**

- Step 1.** In Cisco DNA Center, navigate to **Design > Network Settings > Network**.
- Step 2.** Under the appropriate site hierarchy make sure the **AAA Server**, **DHCP Server**, **DNS Server**, and **NTP Server** are configured.

Cisco DNA Center Design - Network Settings

Network Device Credentials IP Address Pools SP Profiles Wireless Telemetry

EQ Find Hierarchy

- Global
- North America
  - Region - NY**
  - Building-01
    - Floor-01
    - Region - RTP
    - Region - SJ

Configure AAA, NTP, and Image Distribution (SFTP) servers using the "Add Servers" link. Once devices are discovered, DNA Center will deploy using these settings. + Add Servers

**AAA Server**

Network  Client/Endpoint

**NETWORK**

Servers  ISE  AAA Protocol  RADIUS  TACACS

Network  x  x  x

(Only device administration nodes)

[Change Shared Secret](#)

**CLIENT/ENDPOINT**

Servers  ISE  AAA Protocol  RADIUS  TACACS

Client/Endpoint  x  x  x

[Change Shared Secret](#)

**DHCP Server**

DHCP  +

**Step 3.** Under **IP Address Pools** tab, make sure IP address are reserved appropriately for the site hierarchy.

Cisco DNA Center Design - Network Settings

Network Device Credentials **IP Address Pools** SP Profiles Wireless Telemetry

EQ Find Hierarchy

- Global
- North America
  - Region - NY**
  - Building-01
    - Floor-01
    - Region - RTP
    - Region - SJ

**IP Address Pools (9)** Last updated: 2:38 PM Refresh

Filter  Reserve  Actions  SUBNET TYPE  All  IPv4 only  Dual-Stack

Name	Type	IPv4 Subnet	IPv6 Subnet	Inherited from	Actions
NY_AP_Pool	Generic	10.4.221.0/24 0% IPs available	-		Edit   Clone   Release
NY_Border_Handoff_Pool	Generic	10.4.229.0/24 88% IPs available	-		Edit   Clone   Release
NY_Campus_Critical_Data	Generic	10.4.224.0/25 100% IPs available	-		Edit   Clone   Release
NY_Campus_Critical_Voice	Generic	10.4.224.128/25 100% IPs available	-		Edit   Clone   Release
NY_Underlay_Pool	LAN	10.4.228.0/24 100% IPs available	-		Edit   Clone   Release
NY_VN_Campus_Data_Pool	Generic	10.4.222.0/24 0% IPs available	-		Edit   Clone   Release
NY_VN_Campus_Voice_Pool	Generic	10.4.223.0/24 0% IPs available	-		Edit   Clone   Release
NY_VN_Guest_Pool	Generic	10.4.225.0/24 0% IPs available	-		Edit   Clone   Release
NY_VN_IoT_Pool	Generic	10.4.227.0/24 0% IPs available	-		Edit   Clone   Release

Showing 9 of 9

**Step 4.** (Optional) Under the **Wireless** tab, select **Global** in the hierarchy.  
Confirm the wireless **Network SSID** are configured and associated with **Wireless Profile**.

Cisco DNA Center Design - Network Settings

Network Device Credentials IP Address Pools SP Profiles **Wireless** Telemetry

Find Hierarchy

- Global
- North America
  - Region - NY
  - Region - RTP
  - Region - SJC

Enterprise Wireless + Add

Filter Edit Delete

Network Name (SSID)	Security	Wireless Profiles
<input type="checkbox"/> SSID_Open	open	North_America_Wireless_Fabric_Profile
<input type="checkbox"/> SSID_PSK	wpa2_personal	North_America_Wireless_Fabric_Profile
<input type="checkbox"/> SSID_Secure	wpa2_enterprise	North_America_Wireless_Fabric_Profile

## Procedure 6. Verify SD-Access Fabric Site is Deployed

**Step 1.** In Cisco DNA Center, navigate to **Provision > Fabric**.

Cisco DNA Center Design - Network Settings

Design Policy **Provision** Assurance Workflows Tools Platform Activity Reports System

NETWORK DEVICES

- Inventory
- Plug and Play

SERVICES

- Service Catalog
- Cisco User Defined Network
- Application Visibility
- Stealthwatch Security Analytics
- App Hosting for Switches
- IoT Services
- Umbrella
- Site to Site VPN
- Cloud

Protocol

RADIUS  TACACS

IP Address (Primary)

10.4.250.223

(Only device administration nodes)

Reset Save

**Step 2.** Select the applicable Fabric Site from the **Fabrics** section.

Cisco DNA Center Provision - Fabric

### SD-Access Fabrics and Transit/Peer Networks

Choose a Fabric or Transit/Peer Network below to manage, or add a new item by clicking "Add Fabric or Transit/Peer Network".

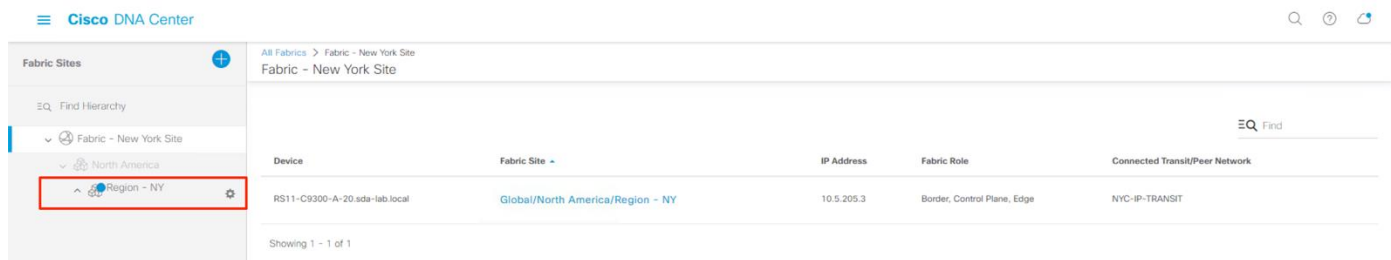
**Fabrics**

- Default LAN Fabric
  - 0 Site, 0 Fabric Device, 0 Control Plane, 0 Border
- Fabric - New York Site**
  - 1 Site, 1 Fabric Device, 1 Control Plane, 1 Border
- Fabric - San Jose Site
  - 1 Site, 5 Fabric Devices, 2 Control Planes, 2 Borders

Transit/Peer Networks

- NYC-IP-TRANSIT
  - Transit: IP
- SDWAN 10.4.246.11
  - Transit: SDWAN
- SJC-IP-TRANSIT
  - Transit: IP

**Step 3.** Select the site from the hierarchy list in the left panel.

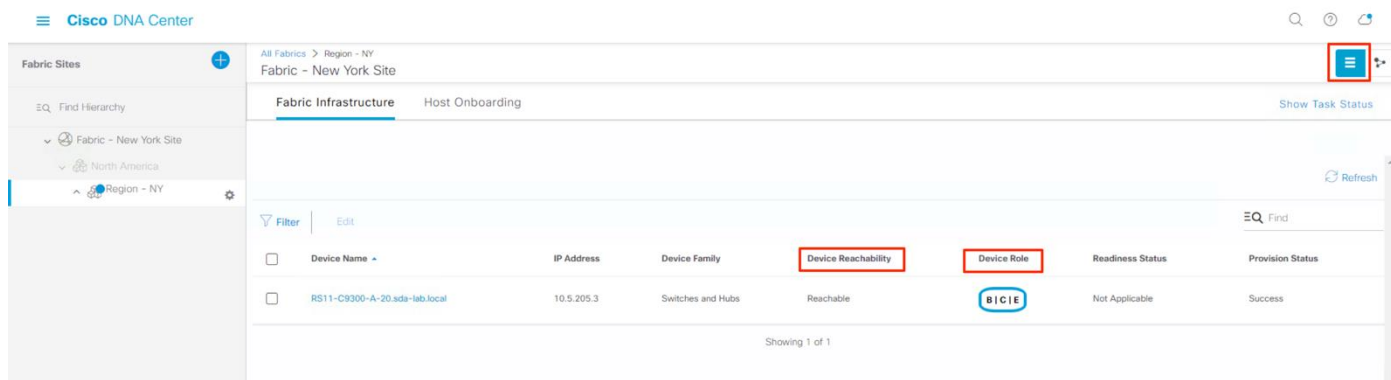


**Step 4.** Select **Fabric Infrastructure** to see the network topology view.



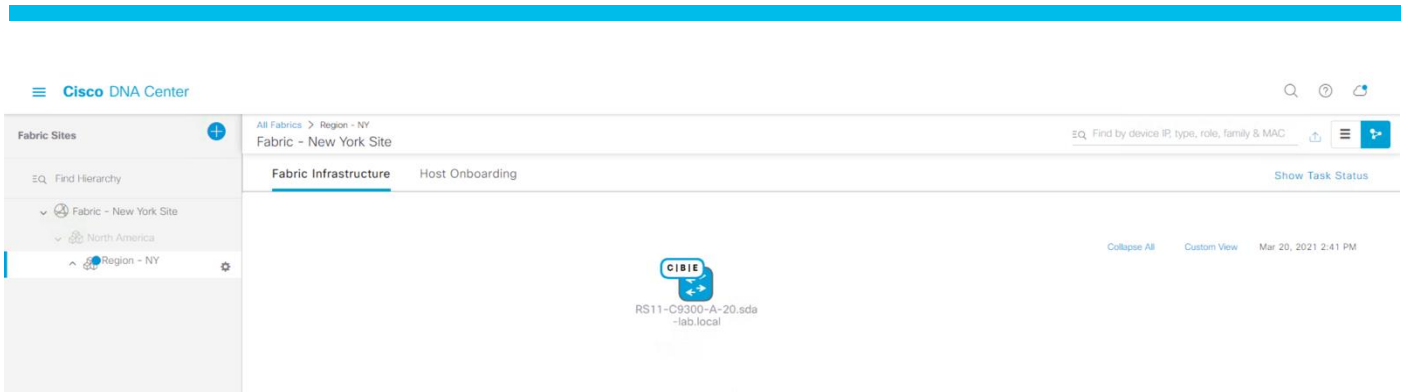
**Step 5.** Click the button to change to List View.

Verify the network devices at the fabric site has been provisioned with fabric **Device Role** assigned and are in reachable state.



**Procedure 7.** Verify the SD-Access Border Node Layer 3 Handoff Configuration

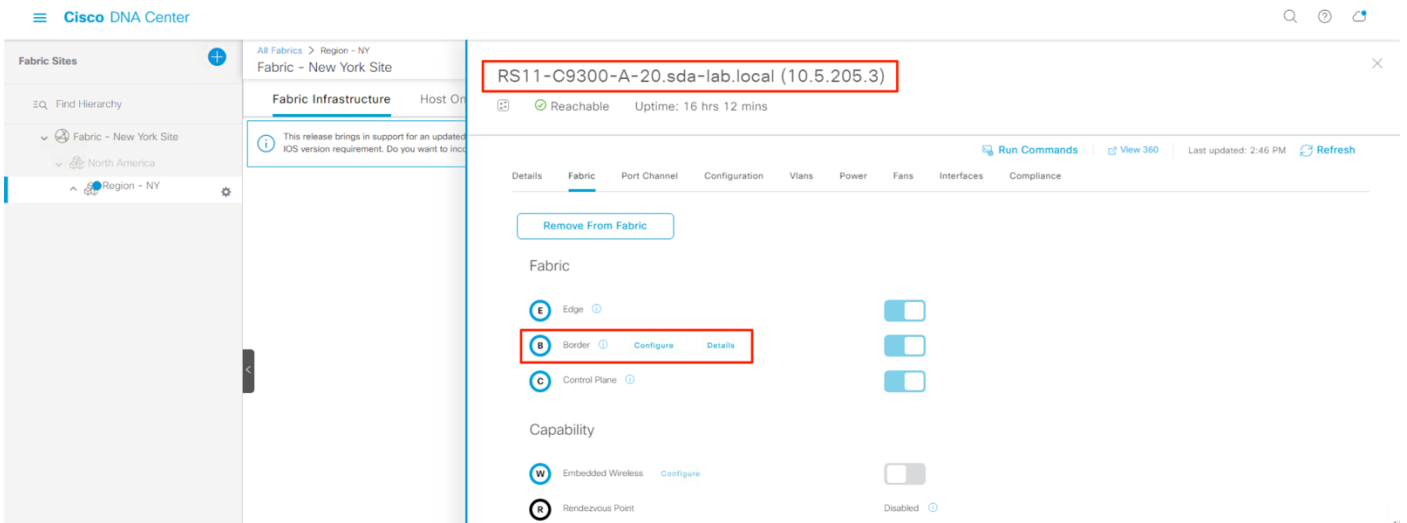
- Step 1.** In Cisco DNA Center, navigate to **Provision > Fabric**.
- Step 2.** Select the Fabric site in the **Fabrics** section.
- Step 3.** Select the site from the hierarchy list in the left panel.



**Step 4.** Select **Fabric Infrastructure** to see the network topology view.

Click on the border node device to open the slide out panel.

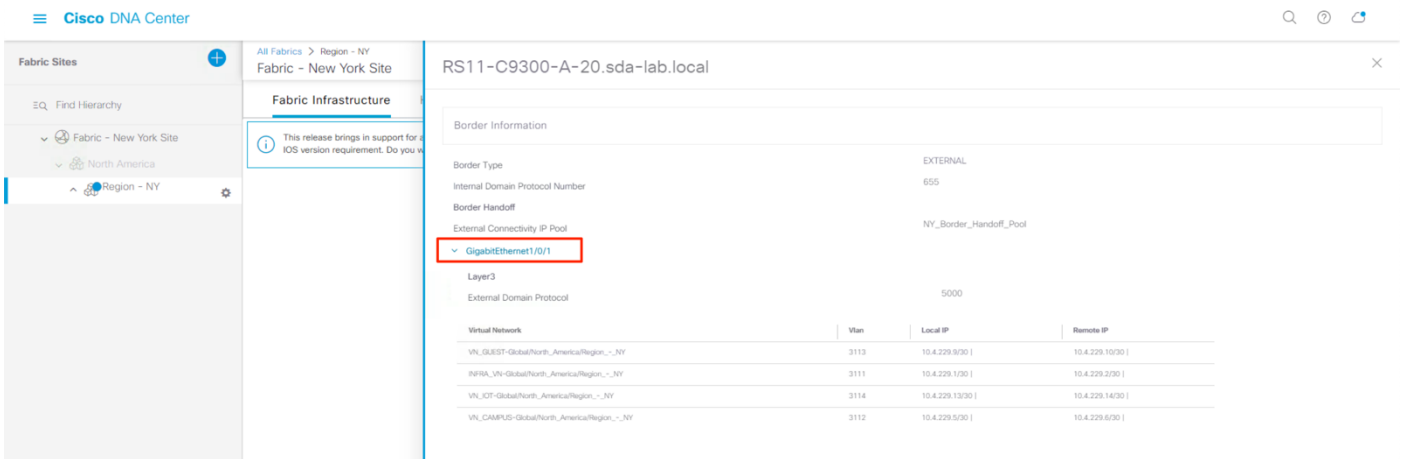
**Step 5.** Select the **Fabric** tab and click **Details** next to **Border** to view the Layer 3 Handoff information.



**Step 6.** Select the handoff interface from the list.

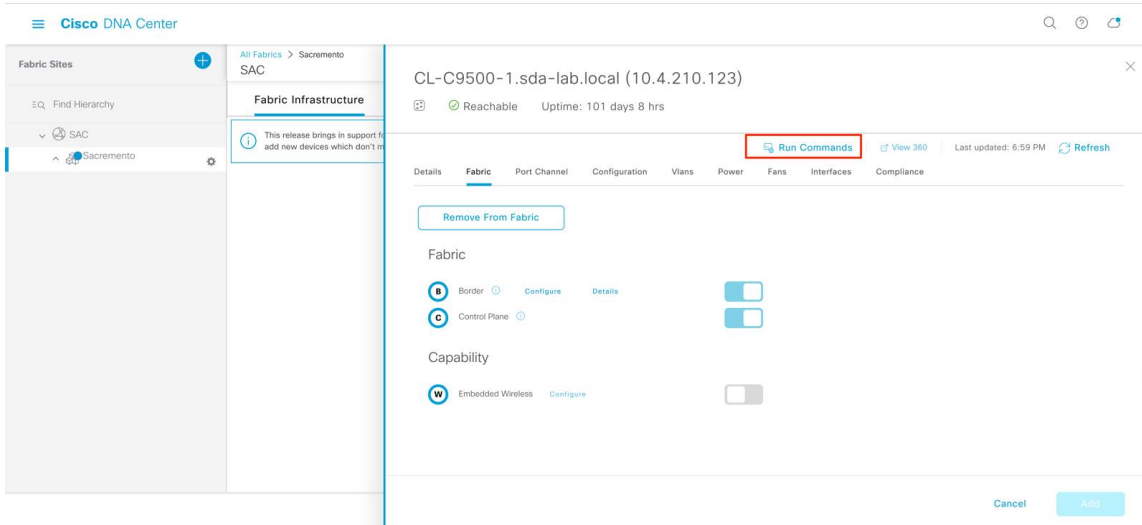
Verify all the virtual networks at the fabric site have been handed off to the peer device.

These steps should be completed for each Layer 3 Handoff interface that connects to each WAN Edge device on each border node.



**Step 7.** Click **Cancel** at the bottom of the page to navigate back to the device view.

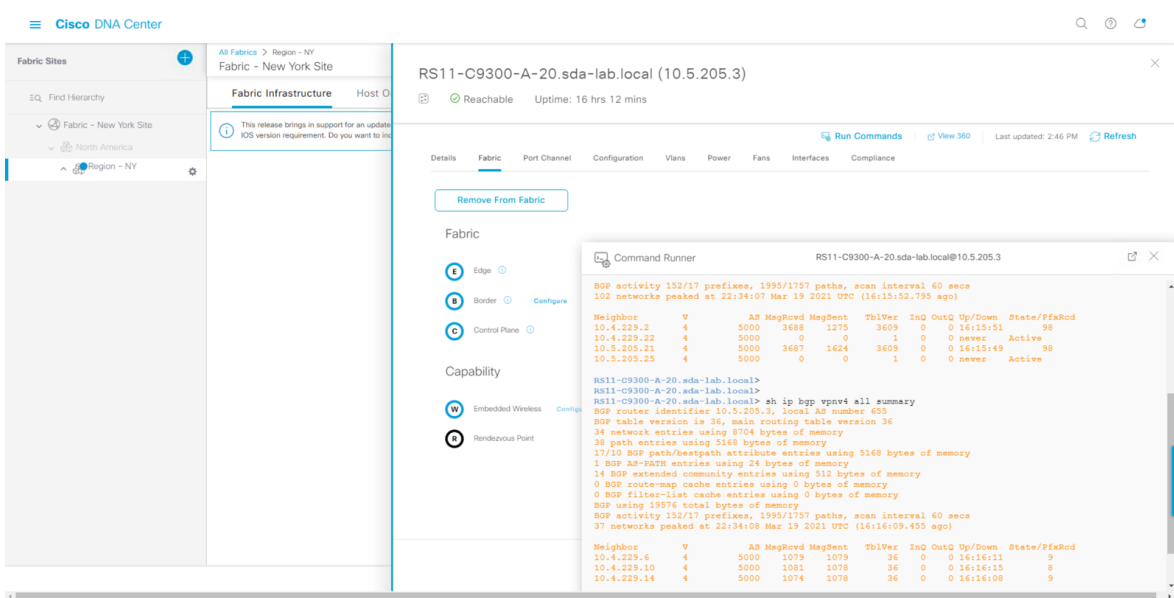
**Step 8.** Click **Run Commands**.



**Step 9.** Issue the following commands to verify the border node has successfully established a BGP peering with the WAN Edge peer device(s) for each virtual network:

**Table 5.** BGP Verification – SD-Access Border Node

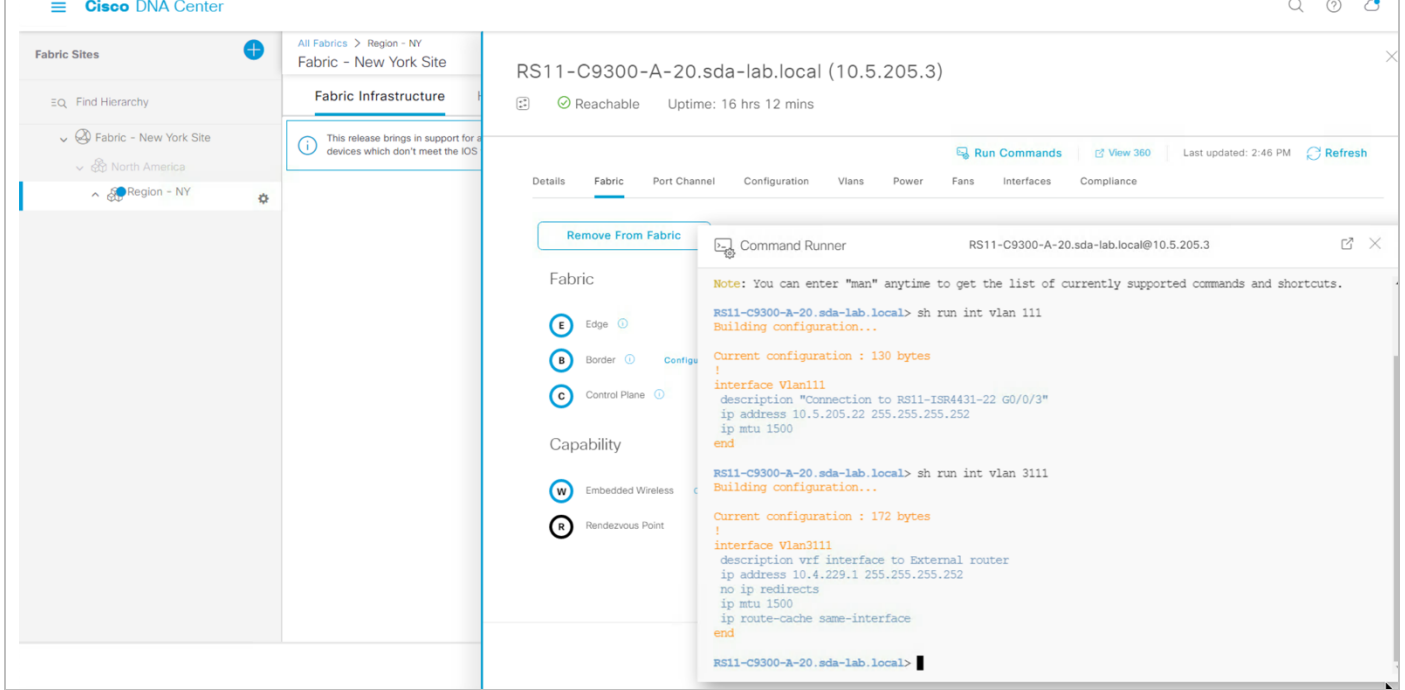
Command	Command Details
show ip bgp summary	Verifies BGP adjacencies for the Global Routing Table
show ip bgp vpnv4 all summary	Verifies BGP adjacencies for VRFs in the IPv4 address-family
show ip bgp vpnv6 unicast all summary	Verifies adjacencies for VRFs in the IPv6 address-family



**Step 10.** Repeat these verification commands at each border node configured with a Layer 3 handoff connected to WAN Edge peer device(s).

**Tech tip**

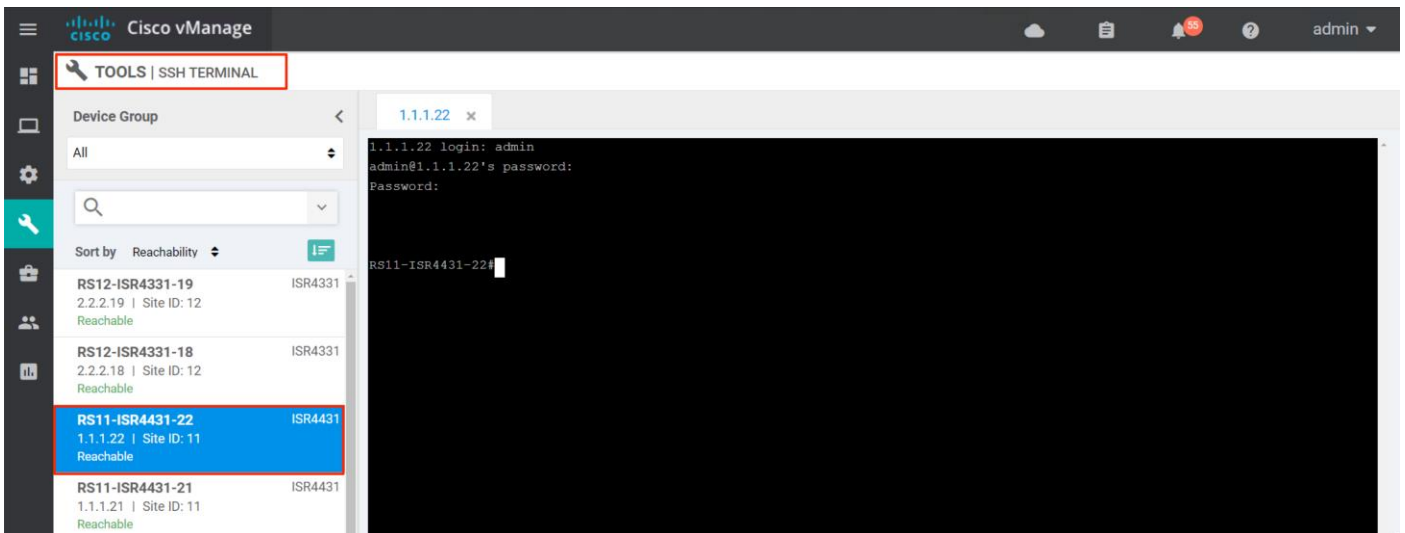
Cisco SD-Access border node is configured with jumbo-frame with 'system-MTU', the command configures all the physical interface on the network device with the higher MTU value. To match the MTU value on the upstream device, configure the SVI or the sub-interface that connects to the WAN Edge with MTU of 1500 bytes.



**Procedure 8. Verify the WAN Edge End-to-End Reachability**

**Step 1.** In vManage, navigate to **TOOLS > SSH Terminal**.

Select the IOS-XE WAN Edge device from the **Device Group** list.

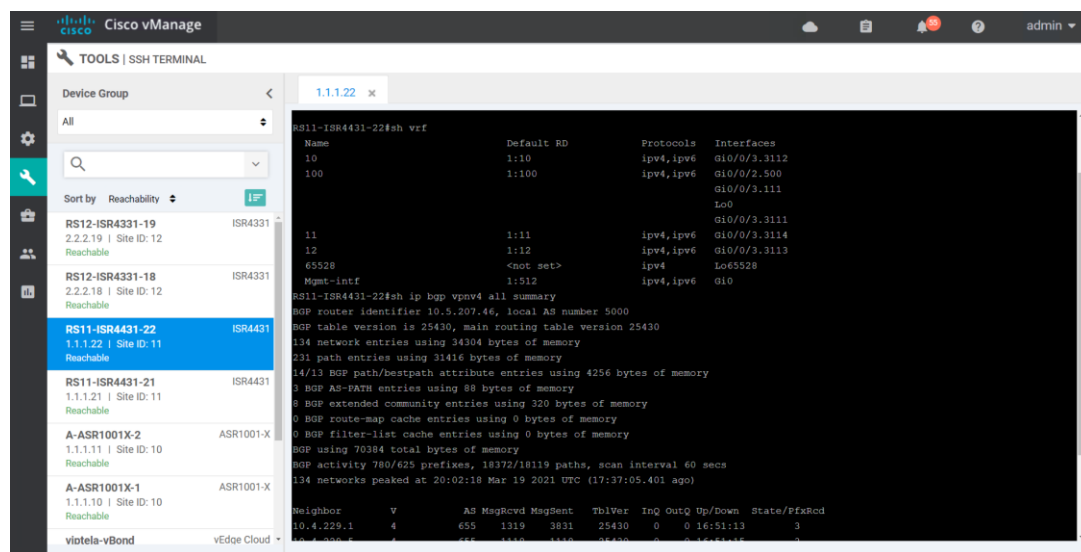




**Step 2.** Issue the following commands to verify the WAN Edge has successfully established a BGP peering to the border node on each Service VPN.

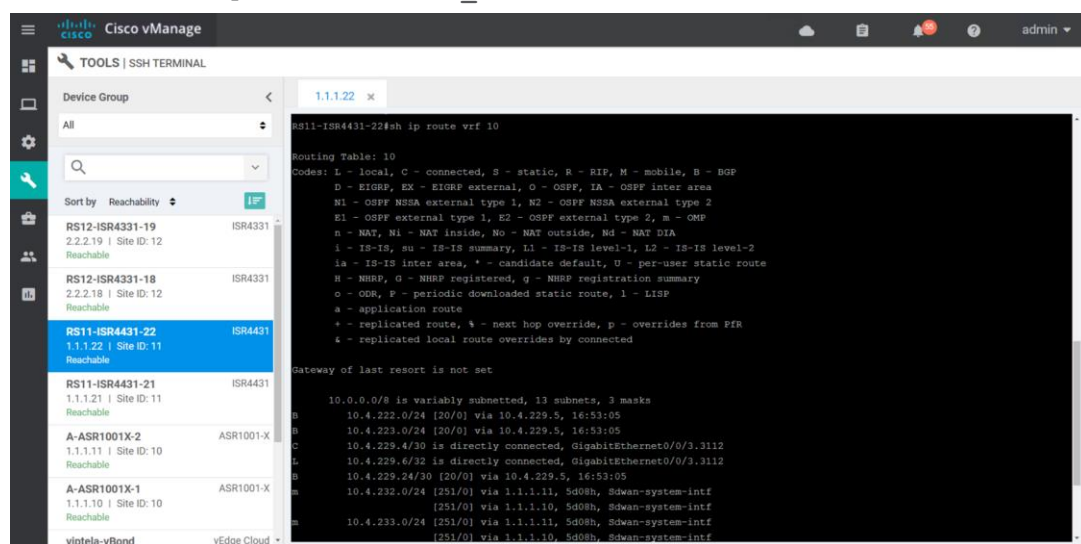
**Table 6.** BGP Verification – SD-WAN Edge Router

Command	Command Details
show vrf	Verifies the Service VPNs configured on the WAN Edge Router
show ip bgp vpnv4 all summary	Verifies BGP adjacencies for the Service VPNs configured with an IPv4 address-family.
show ip bgp vpnv6 unicast all summary	Verifies BGP adjacencies for the Service VPNs configured with an IPv6 address-family.



**Step 3.** Issue the following command to view routes being advertise in each Service VPN.

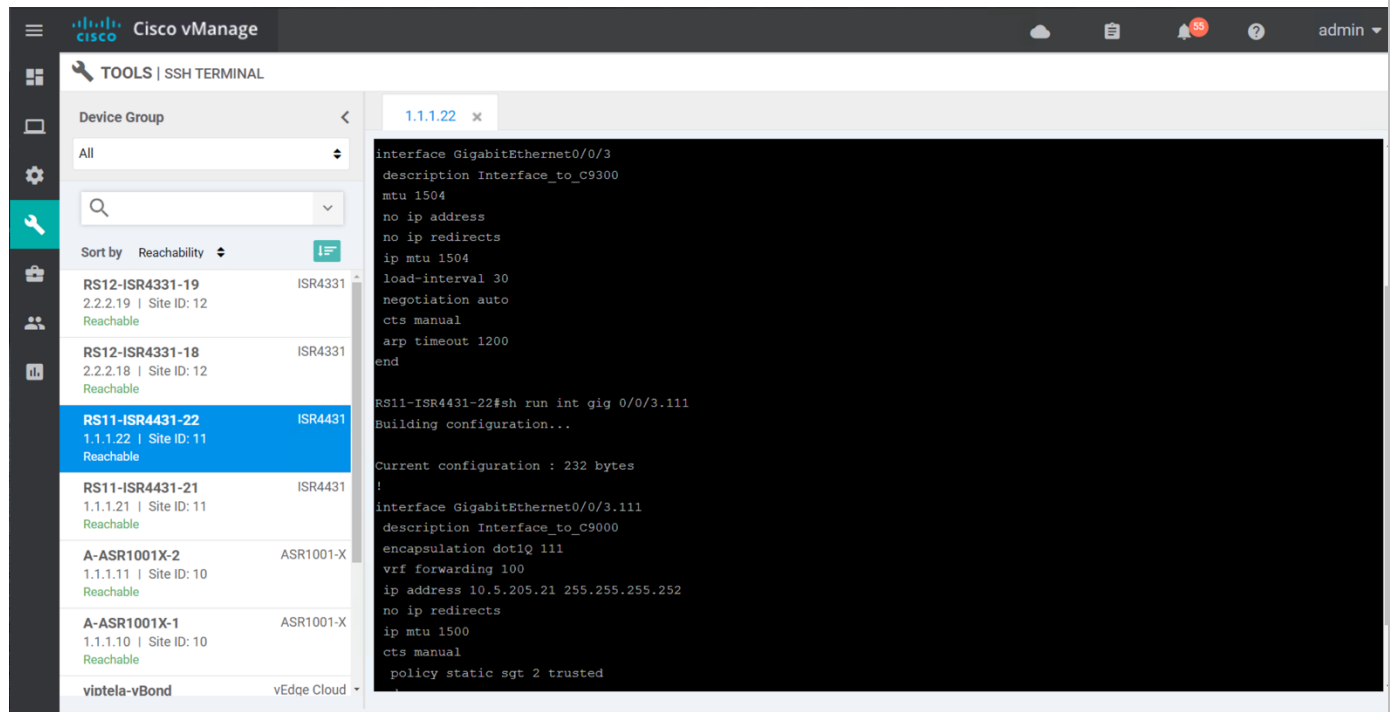
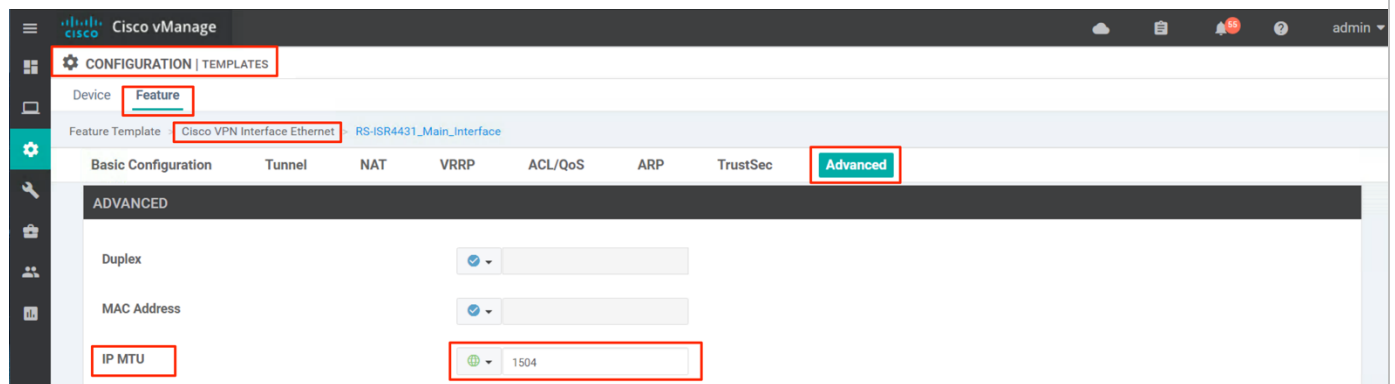
`show ip route vrf <VPN_number>`



## Tech tip

By default, Cisco IOS-XE WAN Edge devices are configured with IP MTU of 1500 bytes on each interface. The interface that connects the WAN Edge device to the border node is configured with sub-interfaces for each Service VPN. To accommodate the 4-byte 802.1Q encapsulation for the sub-interface, increase the IP MTU of the WAN Edge physical interface to 1504 bytes, and leave the default 1500-byte MTU on the sub-interfaces.

The IP MTU on the IOS-XE WAN Edge physical interface is defined under **Cisco VPN Interface Ethernet Feature Template > Advanced > IP MTU** in vManage.



## Process 2: Configuring Cisco TrustSec Inline Tagging

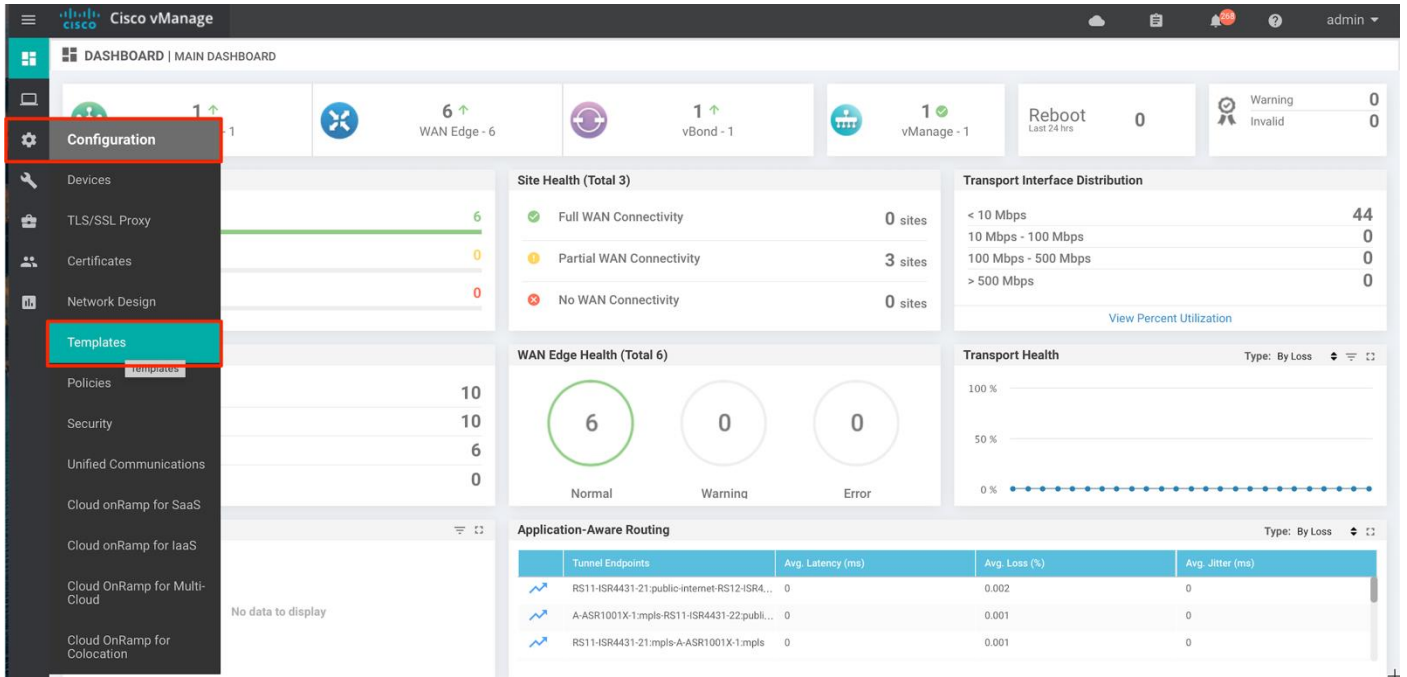
This section details the procedures to enable Cisco TrustSec Inline configuration on the IOS-XE WAN Edge device and SD-Access border node in order to carry the SGT micro-segmentation construct from one domain to the other.

### Procedure 1. Identify vManage Feature Templates Associated to Interfaces Connecting to the Border Node

Templates are used throughout vManage to configure the SD-WAN infrastructure. When a template that is associated to multiple WAN Edge devices is modified, the changes will be provisioned to all associated devices.

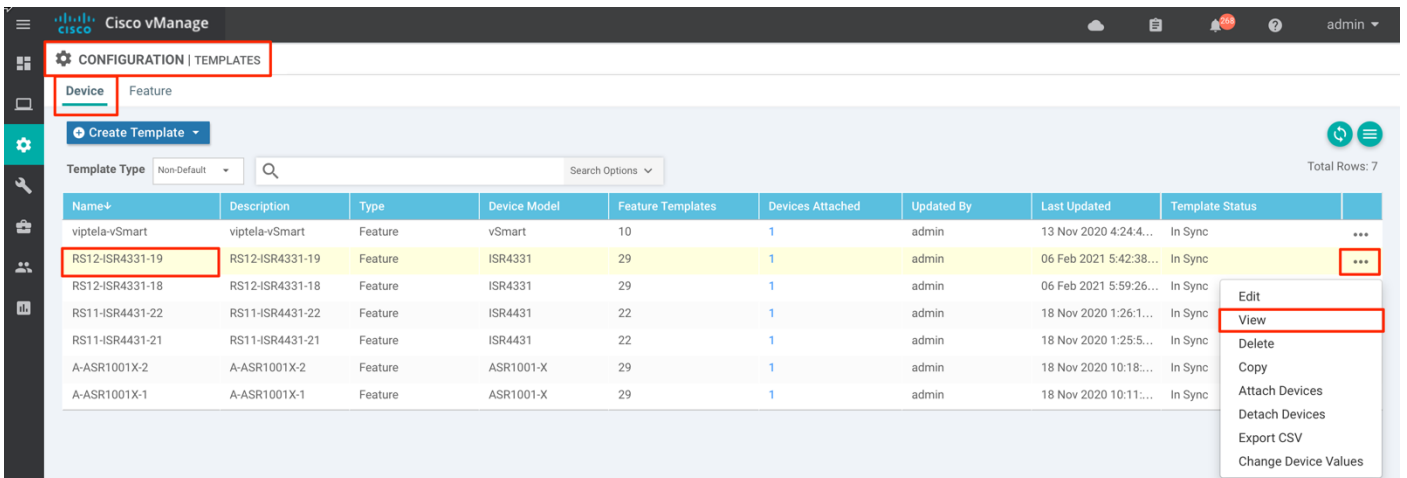
This procedure is used to identify physical interface and sub-interface Feature Templates that are provisioned on the WAN Edge devices which connect to Cisco SD-Access border node(s).

**Step 1.** Login into vManage, navigate to **Configuration > Templates**.

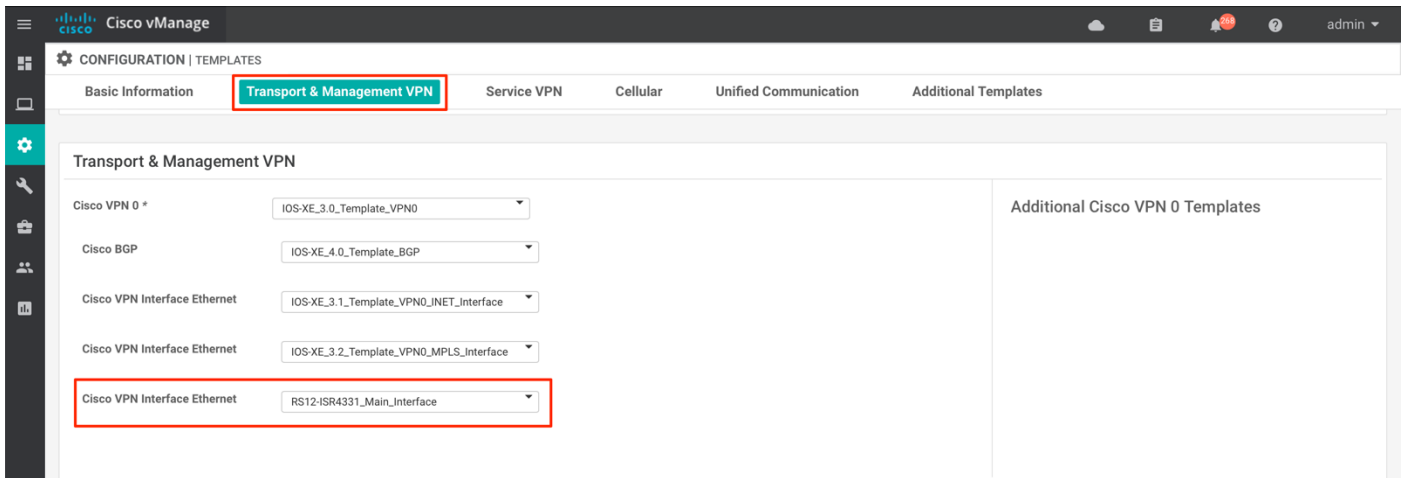


**Step 2.** Select the WAN Edge device from the **Device** list.

**Step 3.** View the feature templates associated to the device by clicking the three dots (...), and selecting the **View** option from the drop-down list.

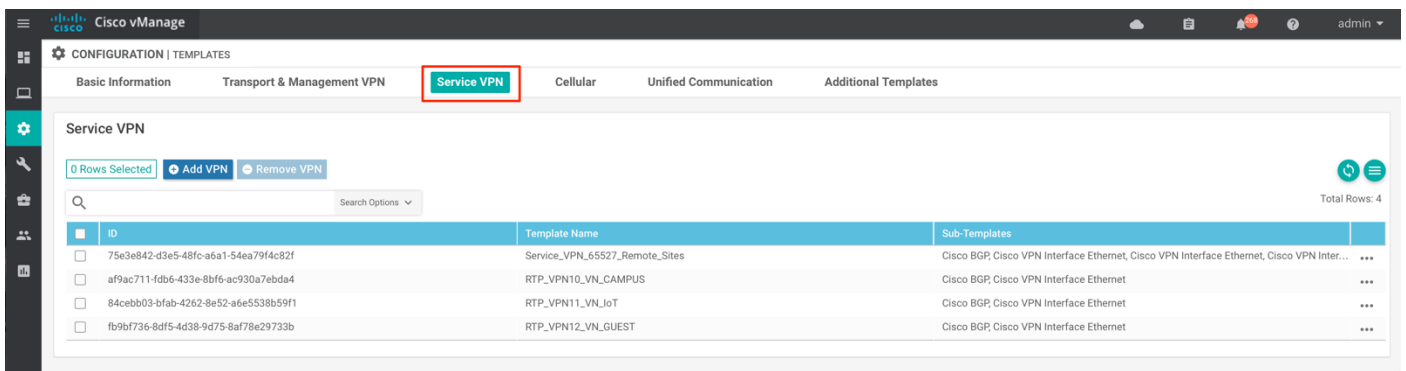


**Step 4.** Click on the **Transport & Management VPN** tab.

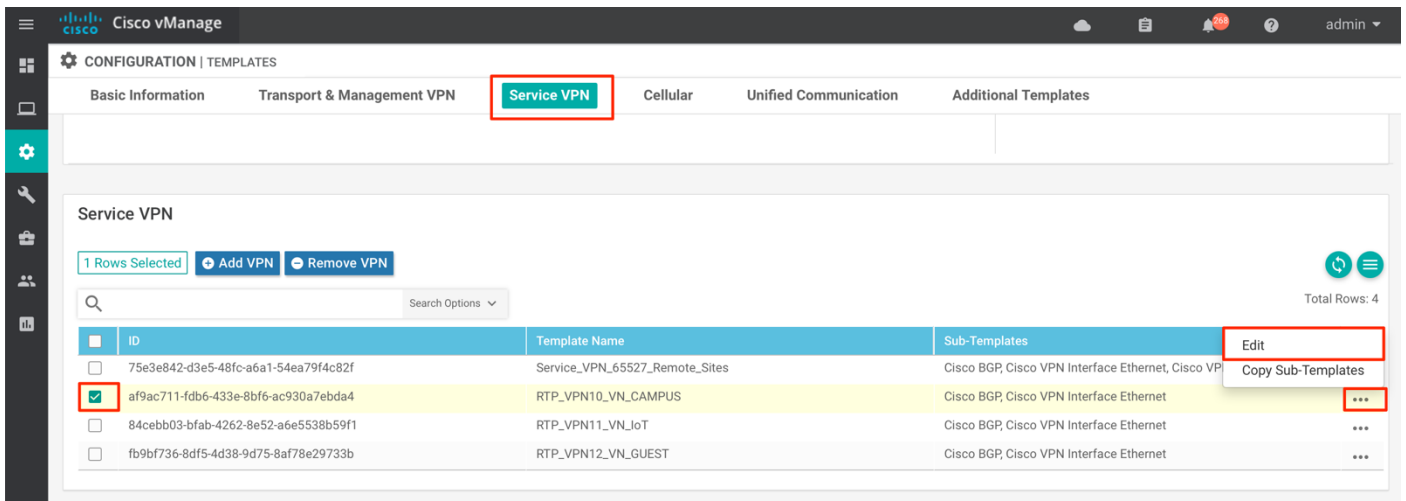


**Step 5.** Note down the **Cisco VPN Interface Ethernet** Feature Template name associated with the physical interface(s).

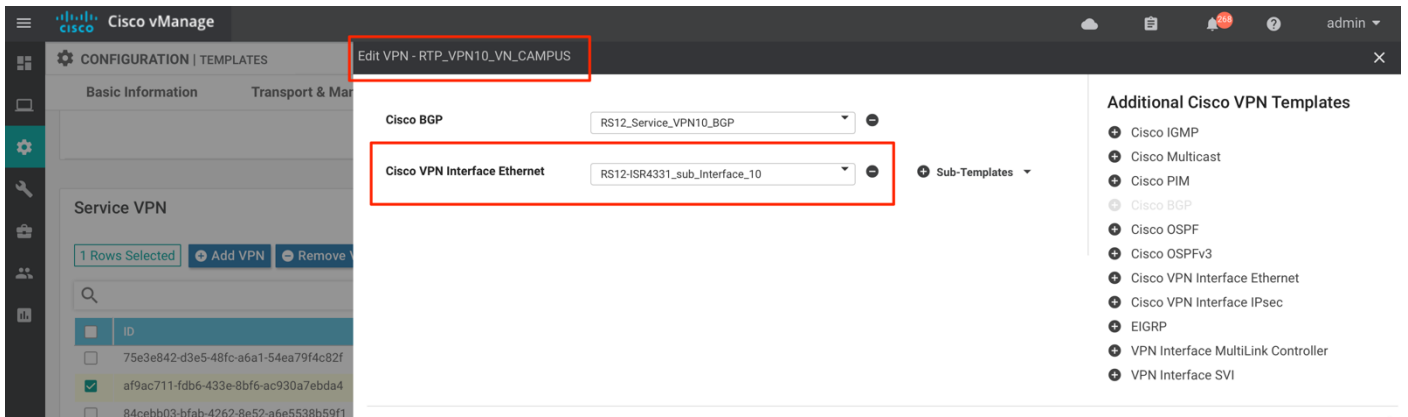
**Step 6.** Click the **Service VPN** tab.



**Step 7.** Select each Service VPN from the list, click the three dots (...), and select the **Edit** option to view the templates associated to the sub-interfaces on the device.



**Step 8.** Note down the **Cisco VPN Interface Ethernet** Feature Template name associated with the sub-interfaces.



**Step 9.** Return to [Step 1](#) and repeat for each WAN Edge device at the site.  
 Example Feature-Template-to-Interface associations are shown below.

**Table 7.** WAN Edge Router: **RS12-ISR4331-19**

Interface	Virtual Network	Service VPN	Feature Template
Physical	-	-	RS12-ISR4331_Main_Interface
Sub-interface	INFRA_VN	VPN 100	RS12-ISR4331_sub_Interface_100
Sub-interface	VN_CAMPUS	VPN 10	RS12-ISR4331_sub_Interface_10
Sub-interface	VN_IoT	VPN 11	RS12-ISR4331_sub_Interface_11
Sub-interface	VN_GUEST	VPN 12	RS12-ISR4331_sub_Interface_12

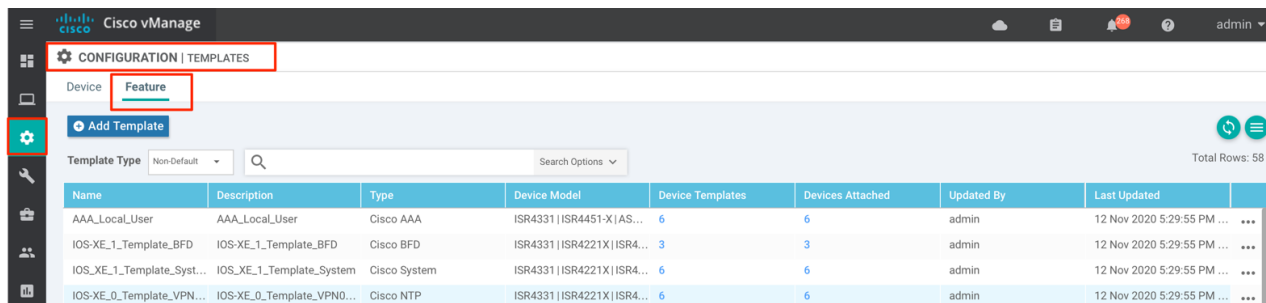
**Table 8.** WAN Edge Router: **RS12-ISR4331-18**

Interface	Virtual Network	Service VPN	Feature Template
Physical	-	-	RS12-ISR4331_Main_Interface
Sub-interface	INFRA_VN	VPN 100	RS12-ISR4331_sub_Interface_100
Sub-interface	VN_CAMPUS	VPN 10	RS12-ISR4331_sub_Interface_10
Sub-interface	VN_IoT	VPN 11	RS12-ISR4331_sub_Interface_11
Sub-interface	VN_GUEST	VPN 12	RS12-ISR4331_sub_Interface_12

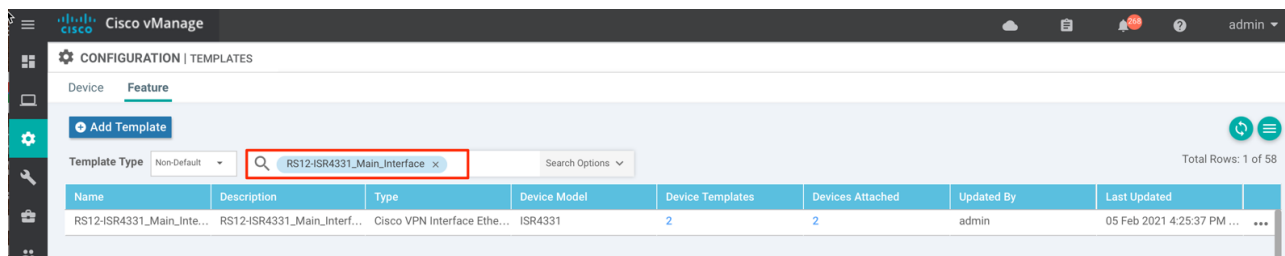
## Procedure 2. Configure CTS Inline Tagging on the SD-WAN Edge Physical Interface

This procedure describes the steps needed to enable TrustSec inline tagging on the physical interface.

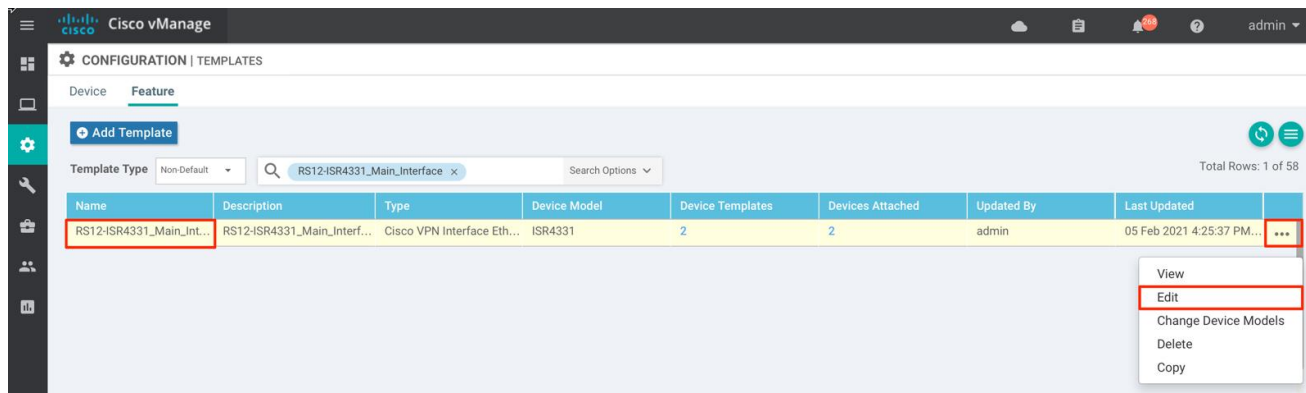
**Step 1.** In vManage, navigate to **Configuration > Templates**, and click the **Feature** tab.



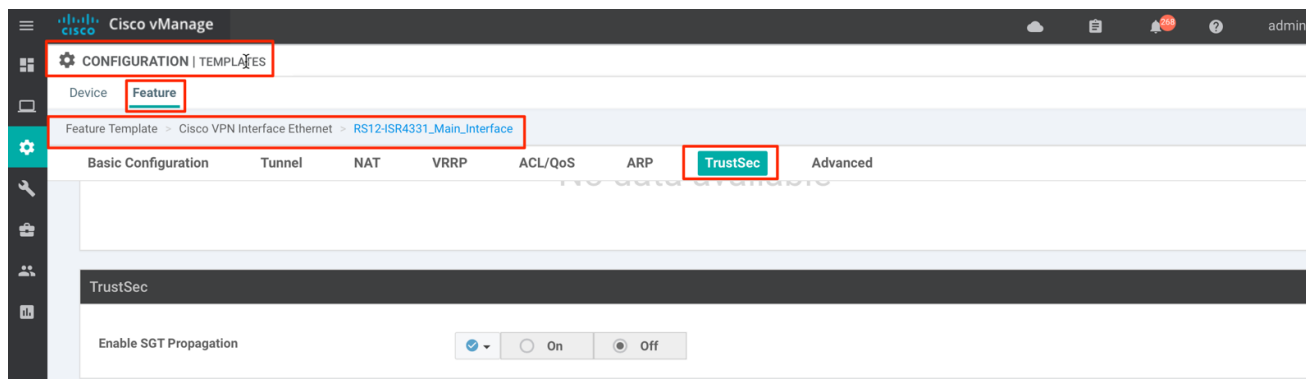
**Step 2.** Search for the Feature Template noted as a result of [Procedure 1](#): Identify vManage Feature Templates Associated to Interfaces Connecting to the Border Node.



**Step 3.** Select the Feature Template, click the three dots (...), and select **Edit** from the drop-down list.



**Step 4.** Select the **TrustSec** tab.



**Step 5.** Under **Enable SGT Propagation**, select the **ON** option.

Additional configuration options appear.

**Step 6.** To propagate the SGT, Under **Propagate**, select the **ON** option.

**Tech tip**

Both **Enable SGT Propagation** and **Propagate** must be enable for the *Independent* Domain deployment.

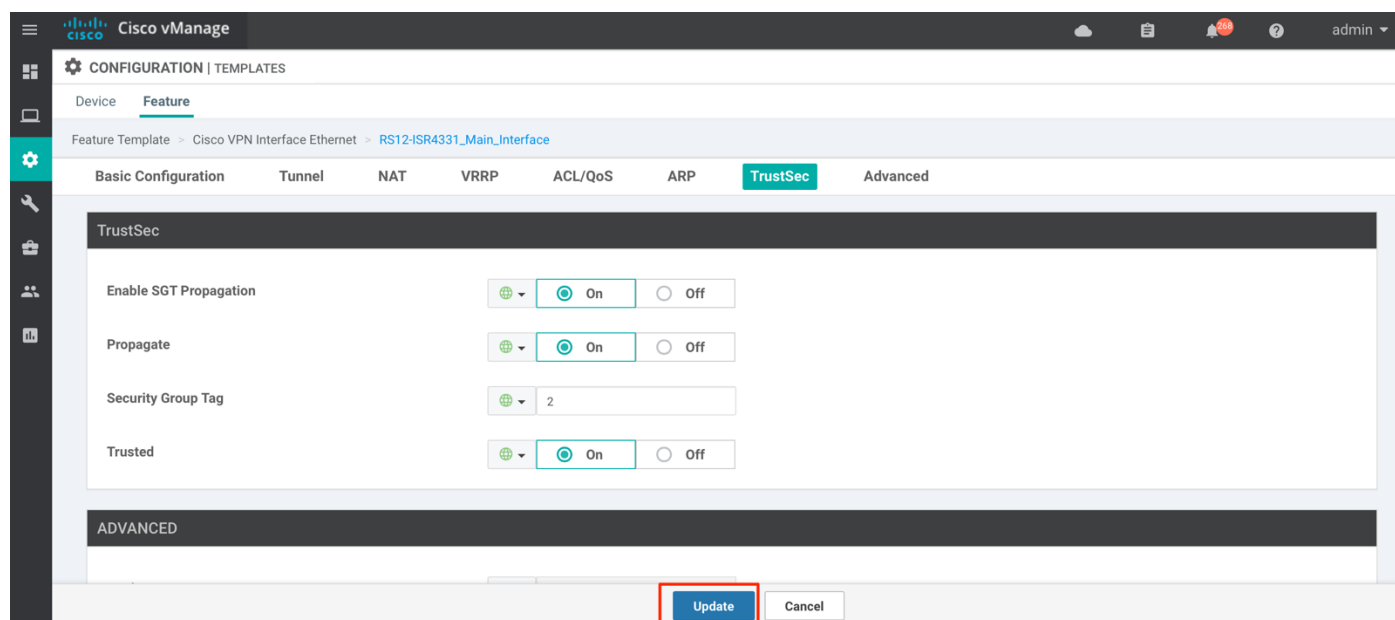
For details on the propagation behavior if other options are selected, please see the [SGT Propagations Options Table](#) in the Cisco SD-WAN Security Configuration Guide for IOS XE Release 17.x.

**Step 7.** Under **Security Group Tag**, select the **Global Option**, and input tag value of **2**.

**Step 8.** Under **Trusted**, select the **ON** option.

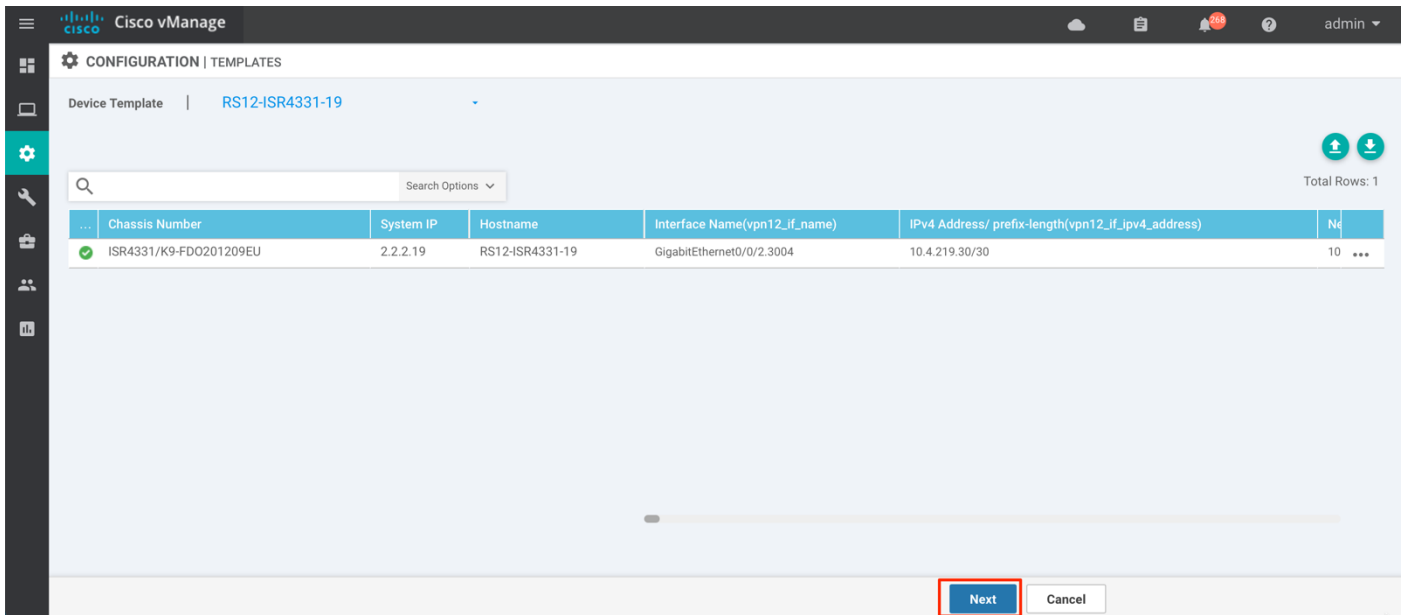
**Tech tip**

For further details on the conventions used for inline tagging, please see the [configuration conventions](#) section. For further and additional details along with a historical information and background, please see [Appendix E](#).



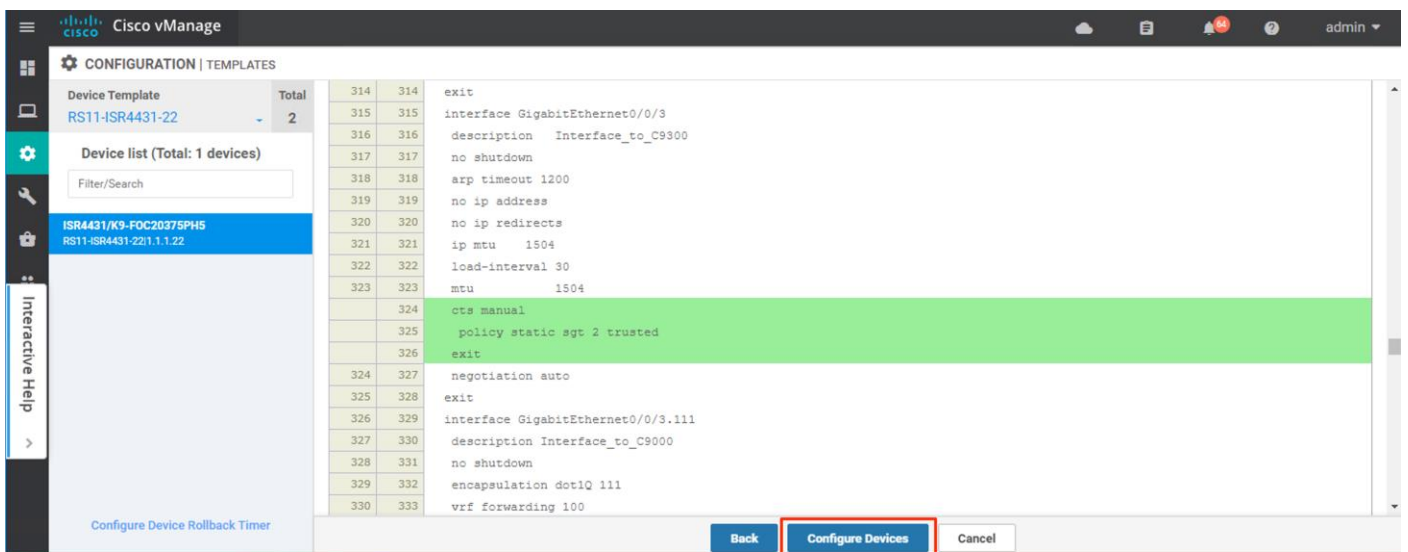
**Step 9.** Click **Update** at the bottom of the page.

**Step 10.** Click **Next**.



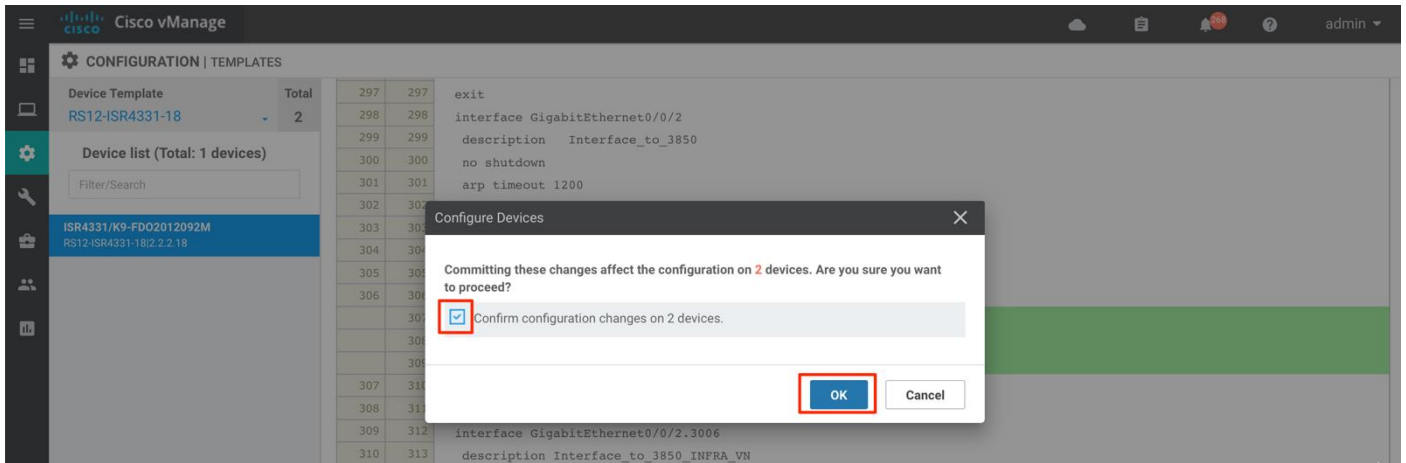
**Step 11.** View the configuration to be pushed to the devices that are associated with this Feature Template.

Click **Configure Devices**.

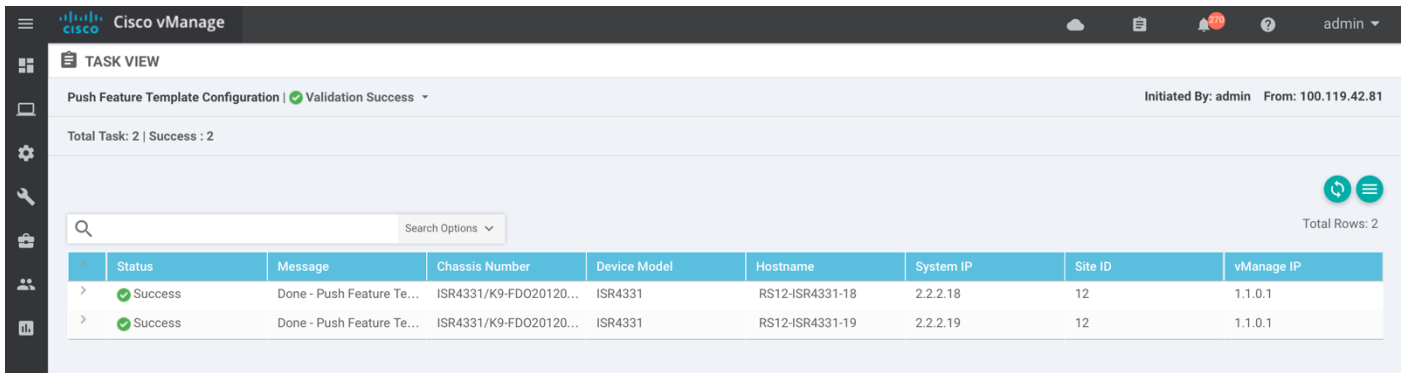


**Step 12.** Check the  **Confirm configuration changes** box, and click **OK**.





**Step 13.** View the **Status** of the provisioning along with the corresponding **Message**.



**Tech tip**

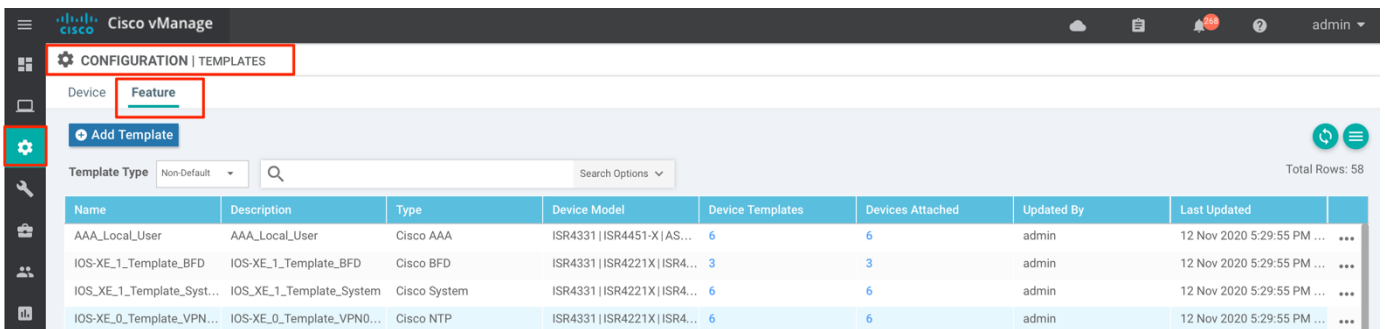
When TrustSec inline tagging feature is enabled on the physical interface, the interface will bounce resulting in momentary traffic loss.

**Step 14.** Return to [Step 1](#) and repeat these steps for all physical interfaces on the WAN Edge device(s) that connect to the SD-Access border node(s).

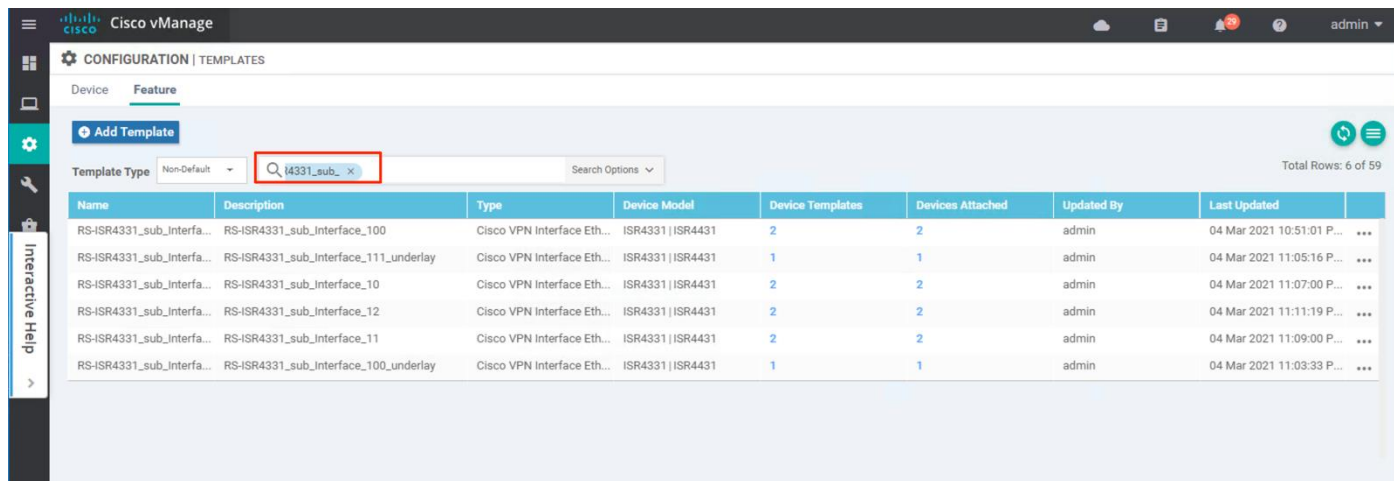
**Procedure 3.** Configure CTS Inline Tagging on the SD-WAN Edge Sub-interfaces

This procedure describes the steps needed to enable TrustSec inline tagging on the SD-WAN router sub-interface(s).

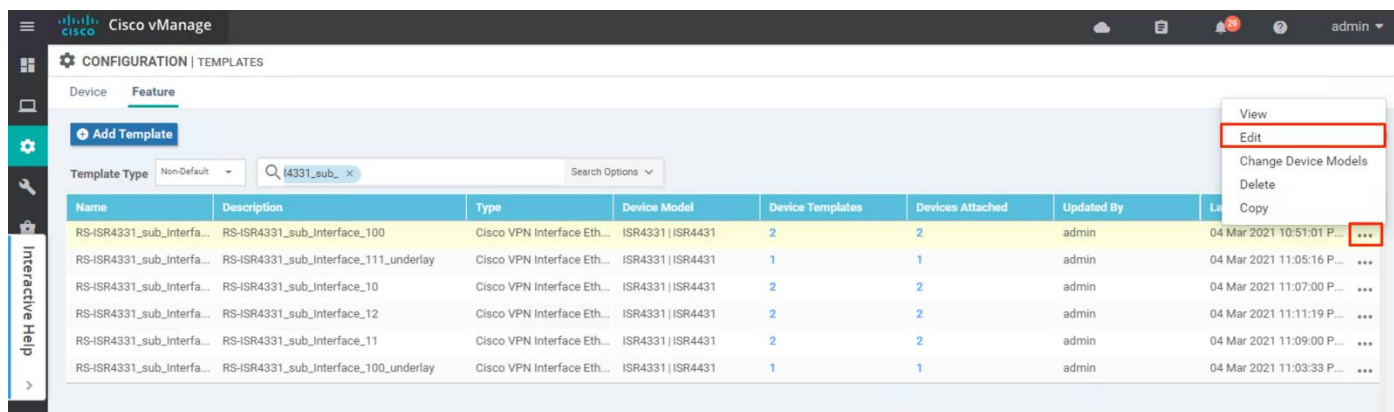
**Step 1.** In vManage, navigate to **Configuration > Templates**, and click the **Feature** tab.



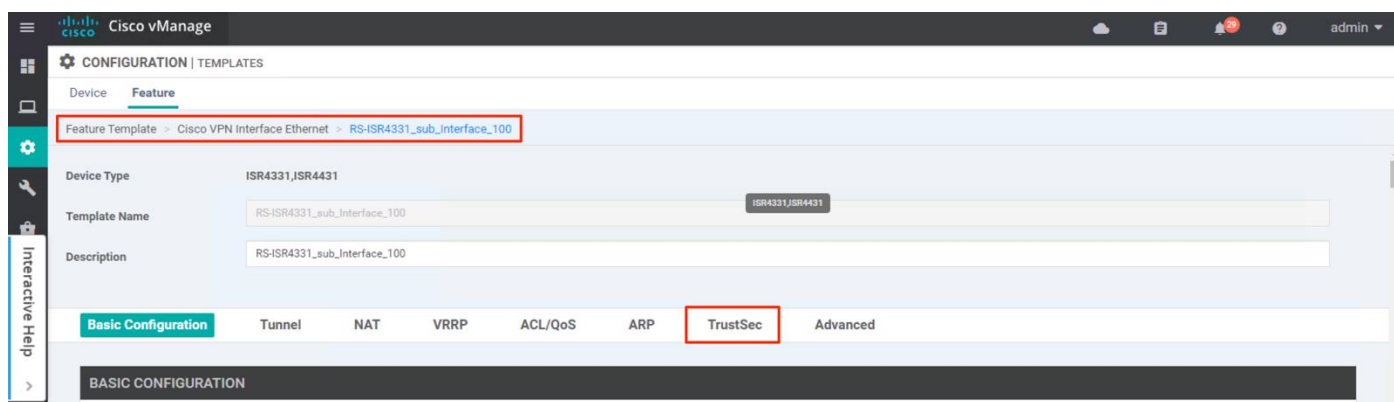
**Step 2.** Search for the Feature Template determined as a result of [Procedure 1](#): Identify vManage Feature Templates Associated to Interfaces Connecting to the Border Node.



**Step 3.** Select the Feature Template, click the three dots (...), and select **Edit** from the drop-down list.



**Step 4.** Select the **TrustSec** tab.

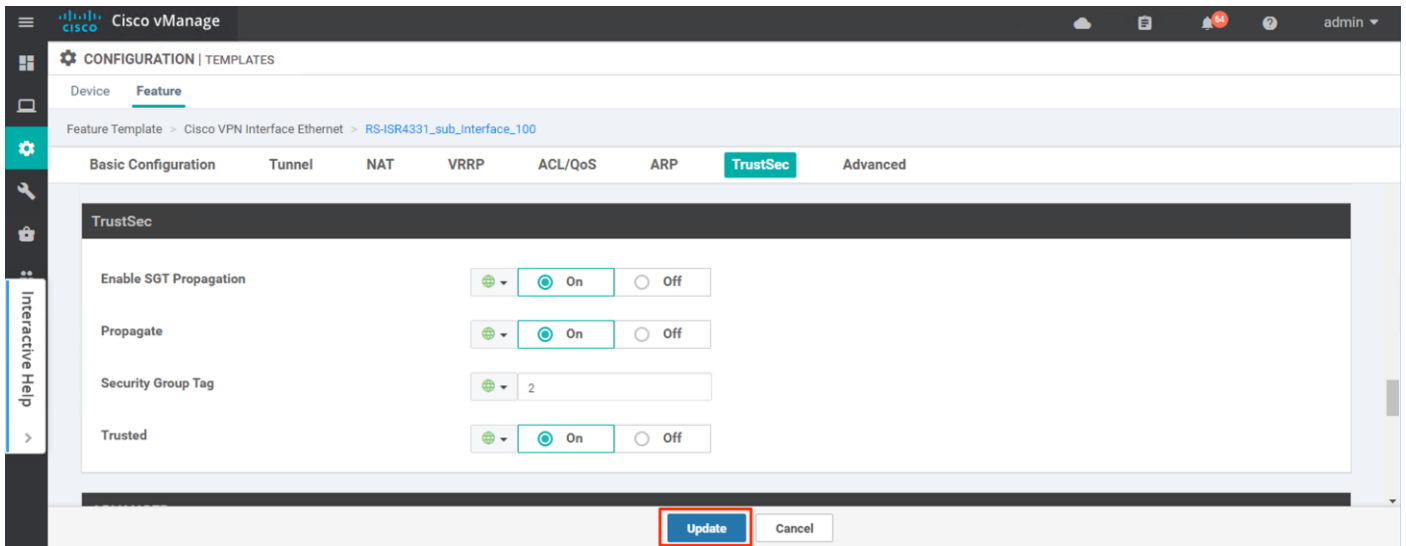


**Step 5.** Under **Enable SGT Propagation**, select the **ON** option

**Step 6.** Under **Propagate**, select the **ON** option

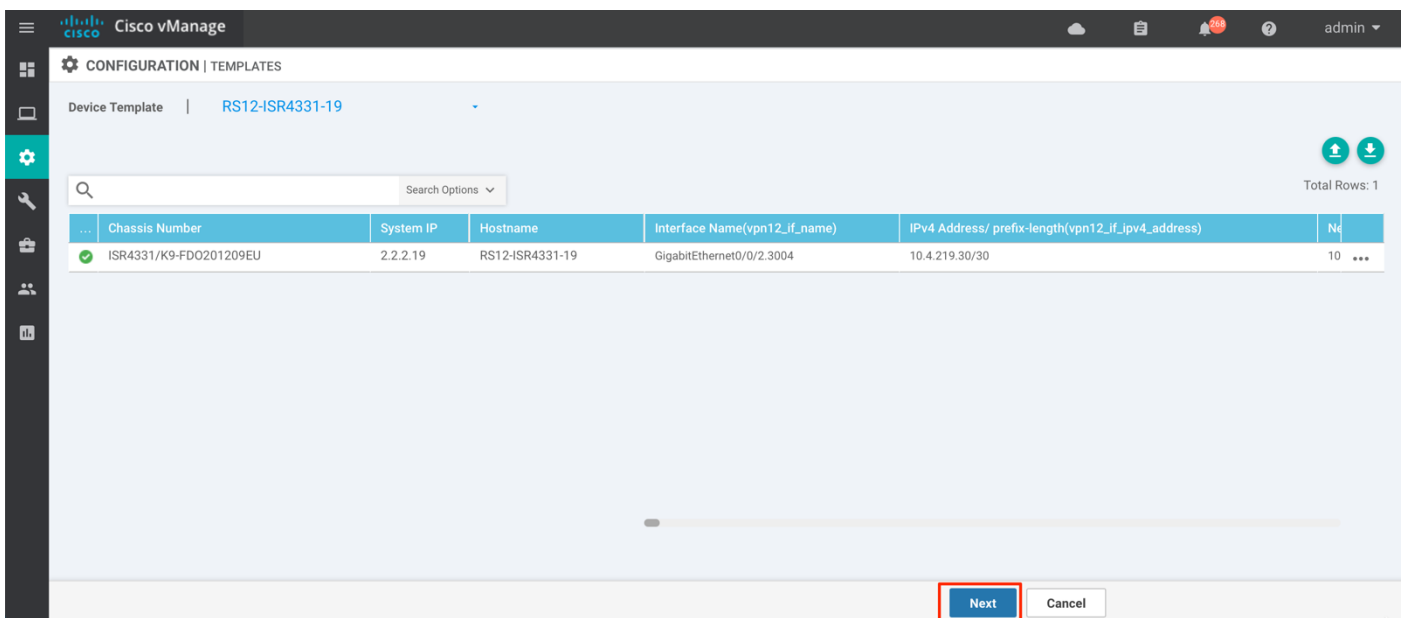
**Step 7.** Under **Security Group Tag**, select the **Global Option**, and input tag value of **2**.

**Step 8.** Under **Trusted**, select the **ON** option.

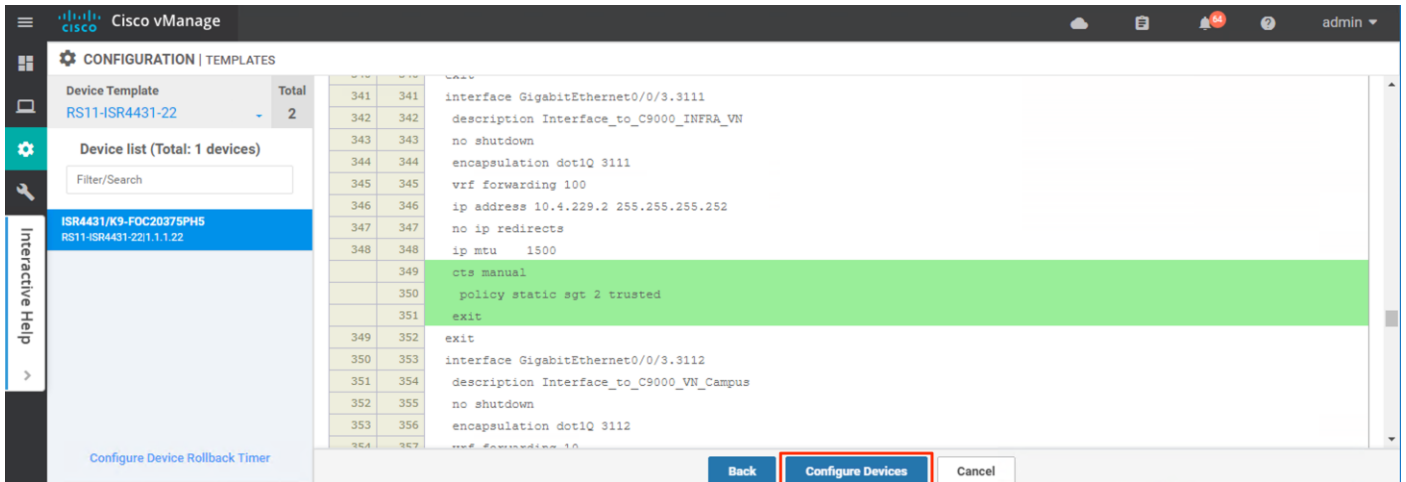


**Step 9.** Click **Update** at the bottom of the page.

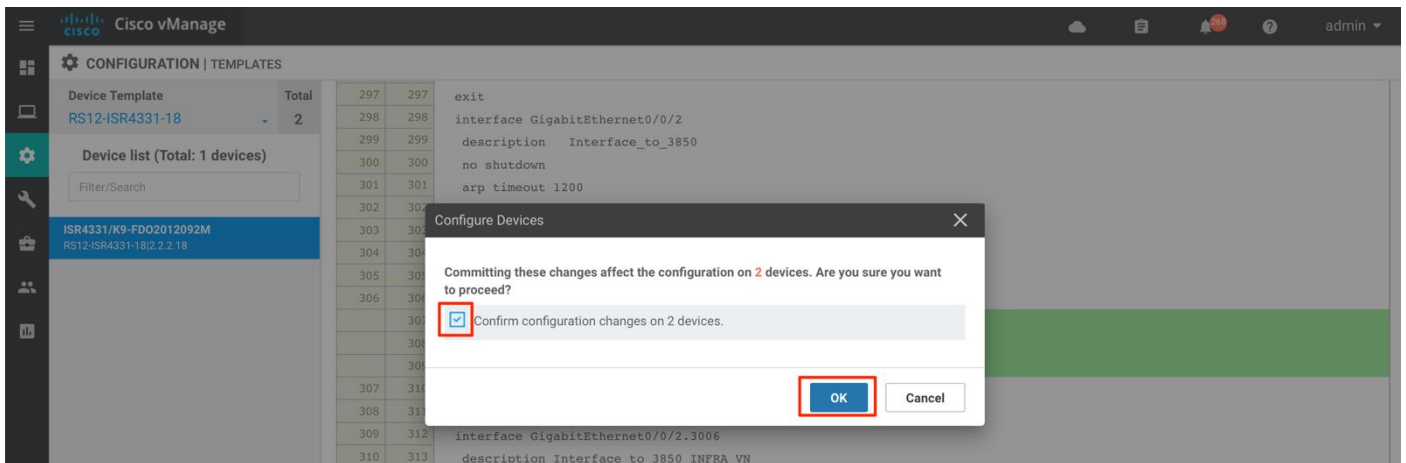
**Step 10.** Click **Next**.



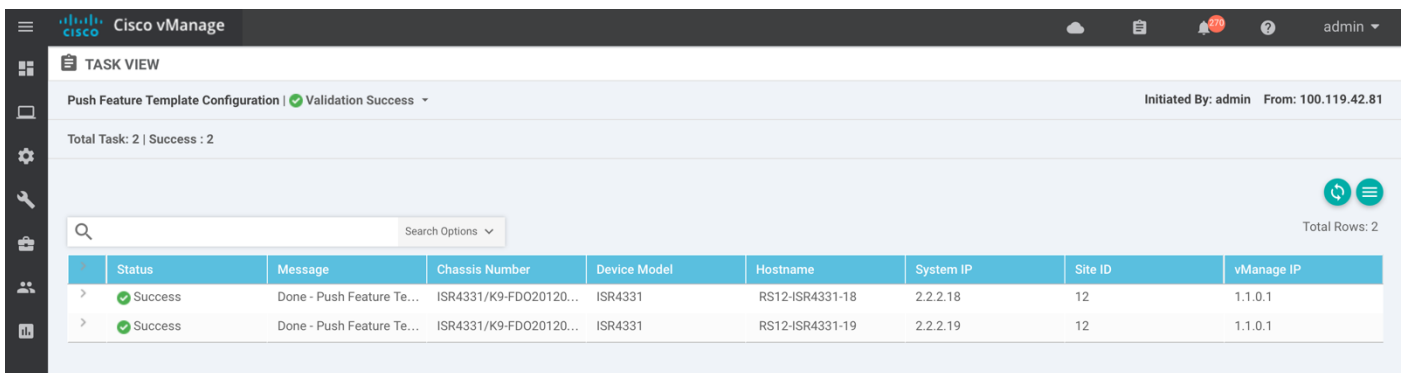
**Step 11.** View the configuration to be pushed to the devices that are associated with this Feature Template.  
Click **Configure Devices**.



**Step 12.** Check the  Confirm configuration changes box and click OK.



**Step 13.** View the status of the configuration provisioning on the WAN Edge devices.



### Tech tip

When inline tagging is enabled on an IOS XE SD-WAN router sub-interface, it will bounce resulting in a brief moment of traffic loss and routing protocol reconvergence.

**Step 14.** Return to [Step 1](#) and repeat these steps for all sub-interfaces on the WAN Edge device(s) the connect to the SD-Access border node(s).

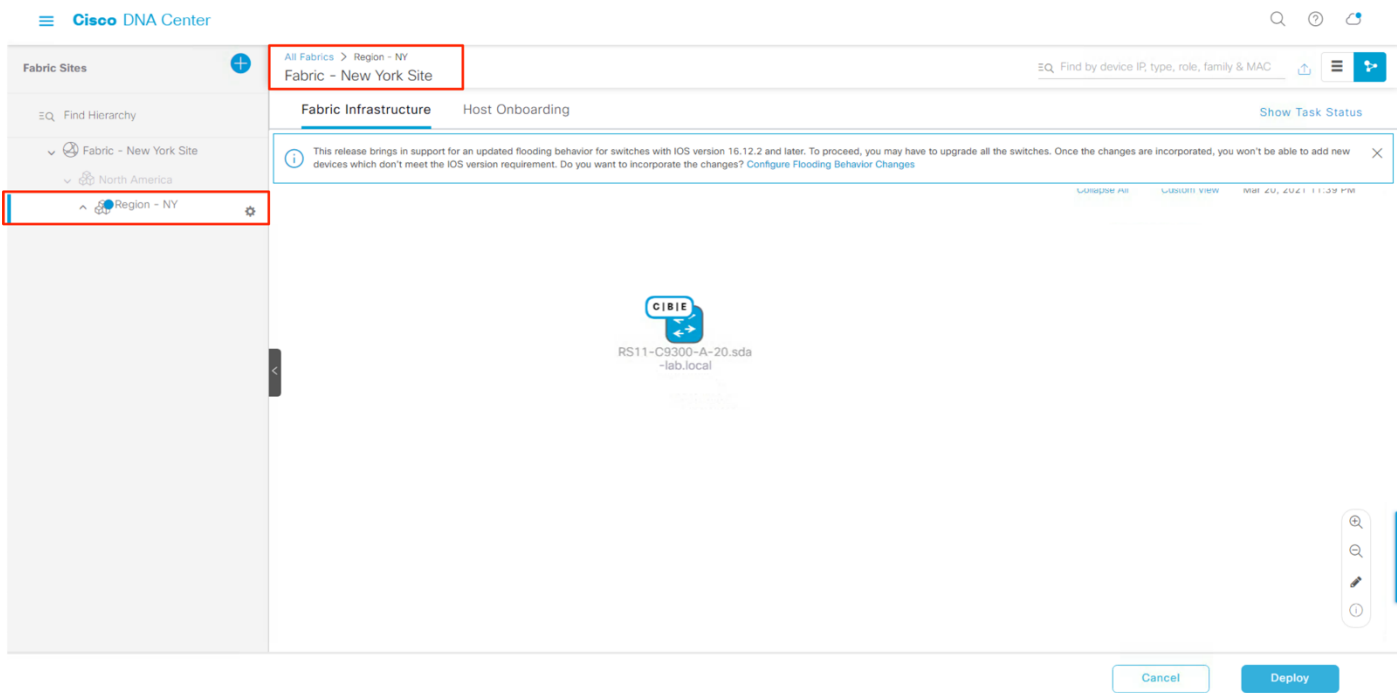
**Procedure 4. Configure Cisco TrustSec Inline Tagging on the Border Node**

In this procedure, the interface connecting to the IOS-XE WAN Edge device is configured with TrustSec inline tagging.

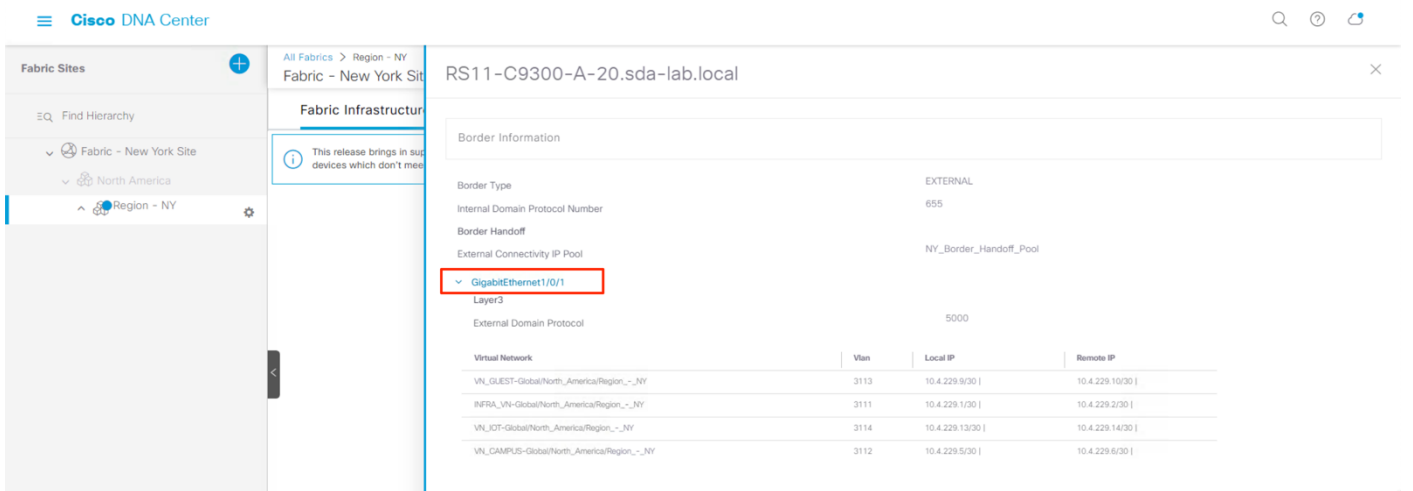
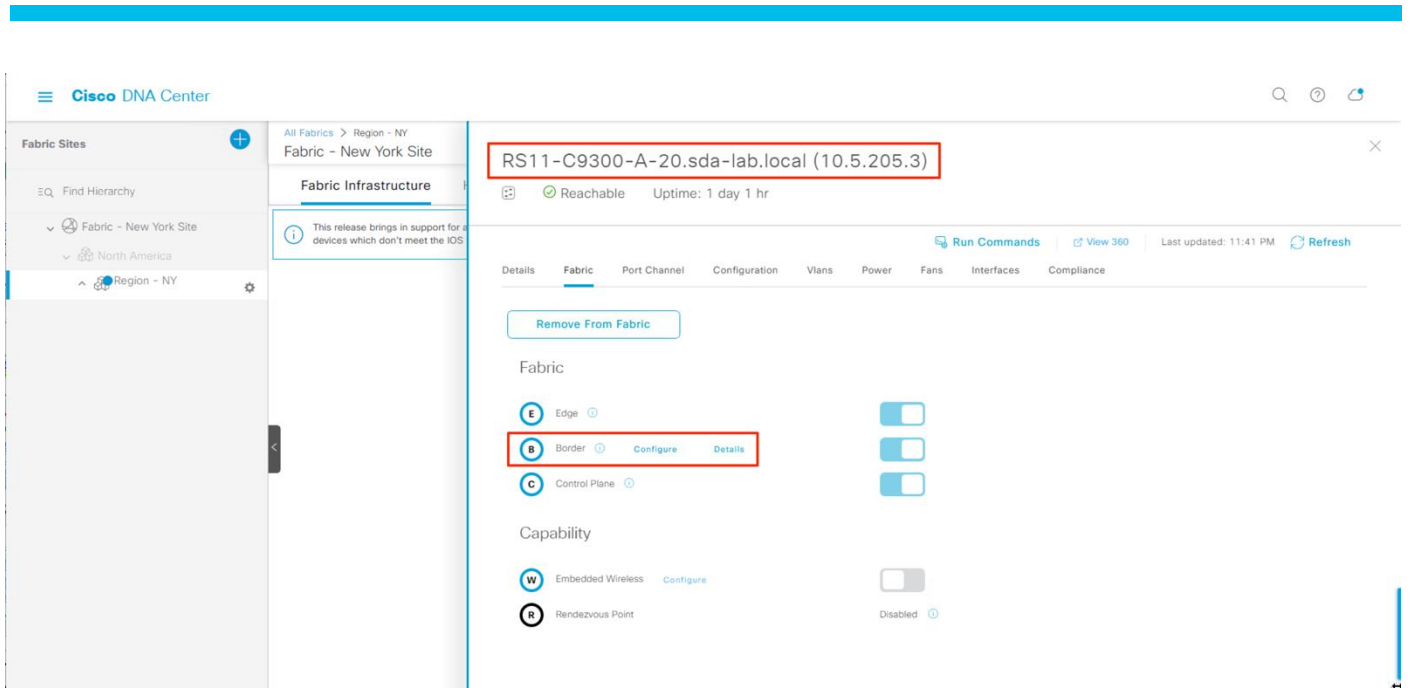
**Tech tip**

For routing platforms, inline tagging is configured on the physical interface and each sub-interfaces. On switching platforms, inline tagging is performed on the physical interface, and not on the SVIs.

- Step 1.** In Cisco DNA Center, navigate to **Provision > Fabric**.
- Step 2.** Select the Fabric site in the **Fabrics** section.
- Step 3.** Select the site from the hierarchy list in the left panel.



- Step 4.** Select **Fabric Infrastructure** to see the network topology view.  
Click on the border node device to open the slide out panel.
- Step 5.** Select the **Fabric** tab and click **Details** next to **Border**.  
Note the interface(s) used for the handoff.



**Step 6.** SSH into the border node through CLI and configure the following commands on the Layer 3 handoff physical interface connecting to the WAN Edge device.

When inline tagging is enabled on the physical interface, the interface will bounce resulting in a brief moment of traffic loss and routing protocol reconvergence.

```
interface <physical interfaces>
  cts manual
  propagate sgt
  policy static sgt 2 trusted
  exit
```

## Tech tip

When the border node is a routing platform, inline tagging must be configured on both physical and sub-interfaces that connect to the WAN Edge device.

```
interface <physical interfaces>
  cts manual
  propagate sgt
  policy static sgt 2 trusted
  exit
```

```
interface <sub-interfaces>
  cts manual
  propagate sgt
  policy static sgt 2 trusted
  exit
```

**Step 7.** Repeat [Step 6](#) on any additional handoff interfaces on the border node that connects to the WAN Edge router(s).

**Step 8.** Return to [Step 1](#) and repeat for each border node that connects to the WAN Edge router(s).

## Tech tip

For further details on the conventions used for inline tagging, please see the [configuration conventions](#) section. For further and additional details along with a historical information and background, please see [Appendix E](#).

## Process 3: Defining Group-Based Access Control Policies

This section details the procedure to configuring consistent group-based access control policies across multiple fabric sites connected via Cisco SD-WAN infrastructure and that are part of Cisco SD-Access | SD-WAN Pairwise Integration.

### Procedure 1. Configure Group-Based Access Control Policies

**Step 1.** Navigate to **Cisco DNA Center > Policy > Group-Based Access Control**.

The screenshot displays the Cisco DNA Center web interface. On the left, a dark sidebar contains a navigation menu with the following items: Design, Policy (highlighted with a red box), Provision, Assurance, Workflows, Tools, Platform, Activity, Reports, and System. To the right of the sidebar, a secondary menu lists: AI Endpoint Analytics, Group-Based Access Control (highlighted with a red box), IP Based Access Control, Application, Traffic Copy, and Virtual Network. The main content area shows a search bar with 'YouTube Channel.' and a 'Take a Tour' button. Below this, there are two summary cards: 'Issues' showing 0 for P1 and 1 for P2, and 'Trends and Insights' for the last 7 days, with metrics for Throughput, Coverage, and Capacity.

**Step 2.** Under **Policies** tab, click the appropriate **Source/Destination** matrix element.

The **Create Policy** slide-out panel appears.

The screenshot shows the Cisco DNA Center interface. At the top, there's a navigation bar with 'Cisco DNA Center' and 'Policy - Group-Based Access Control'. A notification banner at the top left states 'Migration is complete. Cisco DNA Center will be the policy administrator...'. The main area is split into two panels. The left panel, titled 'Policies (0)', has a 'Filter' button and a legend for 'Permit', 'Deny', 'Custom', and 'Default'. It features a matrix with 'Source' (Auditors, BYOD, Contractors, Developers, etc.) and 'Destination' (Auditors, BYOD, Contractors, etc.). The 'Employees' source and 'Contractors' destination cell is highlighted with a red box. A tooltip above it shows 'Employees > Default Policy > Contractors' and 'Contractors > Default Policy > Employees'. The right panel, titled 'Create Policy', shows 'Employees -> Contractors' selected, 'Policy Status' set to 'Enabled', and a 'Change Contract' link highlighted with a red box. At the bottom right of the panel are 'Cancel' and 'Save' buttons.

**Step 3.** Click **Change Contract** from the **Create Policy** slide-out panel to change from the default contract.

This screenshot is similar to the previous one, showing the 'Create Policy' slide-out panel. The 'Change Contract' link in the 'Contract' section is highlighted with a red box. The rest of the interface, including the 'Policies' tab and the matrix, remains the same.

**Step 4.** Select one of the existing or predefined contracts from the list.



Optionally, create a new custom contract by clicking the **Create Contract** by following Steps 5-8.

If using an existing or predefined contract, skip to [Step 9](#).

**Step 5.** If creating a new contract, click **Create Contract**.

The screenshot shows the Cisco DNA Center interface for managing Group-Based Access Control (GBAC) policies. A notification at the top left states: "Migration is complete. Cisco DNA Center will be the policy administration point, and the policy migration log, and/or change the administration mode in GBAC Configurations." The main area is titled "Change Contract" and features a "Filter" section and a table of existing contracts. A red box highlights the "Create Contract" button in the top right corner.

Name	Description	Policies Referencing	Created in
<input type="radio"/> Permit_IP_Log	Permit IP with logging	0	
<input type="radio"/> Permit IP	Permit IP SGACL	0	
<input type="radio"/> DenyRemoteServices	Sample contract to block Remote Access and telnet services	0	
<input type="radio"/> Deny_IP_Log	Deny IP with logging	0	
<input type="radio"/> Deny IP	Deny IP SGACL	0	
<input type="radio"/> DENY_ICMP	DENY_ICMP	0	
<input type="radio"/> AllowWeb	Sample contract to allow access to Web	0	
<input type="radio"/> AllowDHCPDNS	Sample contract to allow DHCP and DNS	0	

**Step 6.** Input a **Name** and **Description**.

**Step 7.** Define the applicable **Action**, **Application**, **Transport Protocol**, **Source / Destination**, **Port**, and optionally enable **Logging**.

**Step 8.** Click **Save**.

The screenshot shows the "Change Contract" interface with the "Name" field set to "EMPLOYEES\_CONTRACTORS\_LIMIT" and the "Description" field set to "Limited Communication between Employees and Contractors". Below these fields is a table titled "CONTRACT CONTENT (4)". A red box highlights the "Save" button at the bottom right.

#	Action *	Application *	Transport Protocol	Source / Destination	Port	Logging	Action
1	Deny	Advanced	ICMP	-	-	<input checked="" type="checkbox"/>	+ X
2	Deny	bitorrent	TCP	Destination	6881,6882,6883,68 ...	<input checked="" type="checkbox"/>	+ X
3	Deny	ftp	TCP	Destination	21,21000	<input checked="" type="checkbox"/>	+ X
4	Deny	Advanced	UDP	Destination Source	587 ANY	<input type="checkbox"/>	+ X

**Step 9.** Select the contract using the  radio button, and click **Change**.

Cisco DNA Center Policy · Group-Based Access Control

Migration is complete. Cisco DNA Center will be the policy administration point, and is now made in GBAC Configurations

**Change Contract**

Filter

Name	Description	Policies Referencing	Created in
<input type="radio"/> AllowDHCPDNS	Sample contract to allow DHCP and DNS	0	
<input type="radio"/> AllowWeb	Sample contract to allow access to Web	0	
<input type="radio"/> Deny IP	Deny IP SGACL	0	
<input type="radio"/> Deny_IP_Log	Deny IP with logging	0	
<input type="radio"/> DenyRemoteServices	Sample contract to block Remote Access and telnet services	0	
<input checked="" type="radio"/> EMPLOYEES_CONTRACTORS_LIMIT	Limited Communication between Employees and Contractors	0	

Show 10 entries Showing 1 - 8 of 8

Cancel **Change**

**Step 10.** In the Policy Status drop-down, selected **Enabled**.

**Step 11.** Click **Save**.

Cisco DNA Center Policy · Group-Based Access Control

Migration is complete. Cisco DNA Center will be the policy administration point, and is now made in GBAC Configurations

**Create Policy**

Contractors → Employees **Custom**

Policy Status **Enabled**

Contract: **Change Contract**

Name	Description	Policies Referencing
EMPLOYEES_CONTRACTORS_LIMIT	Limited Communication between Employees and Contractors	0

#	Action	Application	Protocol	Source / Destination	Port	Logging
1	DENY	advanced	ICMP	Source Destination		ON
2	DENY	bittorrent	TCP	Destination	6881,6882,6883,6884,6885,6886,6887,6888,6889	ON
3	DENY	ftp	TCP	Destination	21,21000	ON
4	DENY	advanced	UDP	Source Destination	587	ON

Default Action PERMIT Logging ON

Cancel **Save**

Cisco DNA Center Policy - Group-Based Access Control

Migration is complete. Cisco DNA Center will be the policy administration point, and screens of Scalable Groups, Access Contracts and Policies in Cisco ISE will be read-only. You can review the policy migration log, and/or change the administration mode in GBAC Configurations

Policies Scalable Groups Access Contracts

Policies (1) Enter full screen

GBAC Configuration Default: Permit IP Create Policies

Filter Deploy Refresh

Permit Deny Custom Default

Contractors > EMPLOYEES\_CONTRACTORS\_LIMIT > Employees  
Employees > Default Policy > Contractors

**Step 12.** If needed, return to [Step 1](#) to define additional contracts policies.

**Step 13.** Once complete, click **Deploy** to provision the policies.

Cisco DNA Center Policy - Group-Based Access Control

Migration is complete. Cisco DNA Center will be the policy administration point, and screens of Scalable Groups, Access Contracts and Policies in Cisco ISE will be read-only. You can review the policy migration log, and/or change the administration mode in GBAC Configurations

Policies Scalable Groups Access Contracts Analytics

Policies (1) Enter full screen

GBAC Configuration Default: Permit IP Create Policies

Filter **Deploy** Refresh

Permit Deny Custom Default

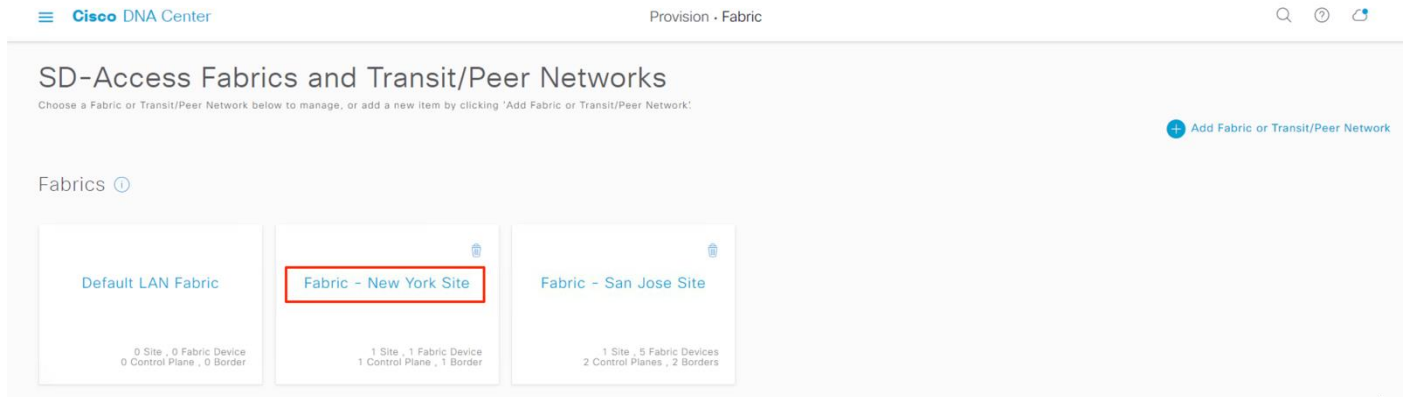
**Procedure 2.** (Optional) Provision Static Host Onboarding on the Edge Node

Endpoints connected to an edge node can be dynamically associated to a VLAN through an ISE Authorization policy upon successful authentication. The Authorization policy can include VLAN and SGT along with additional policy elements that are download to and enforced on the edge node.

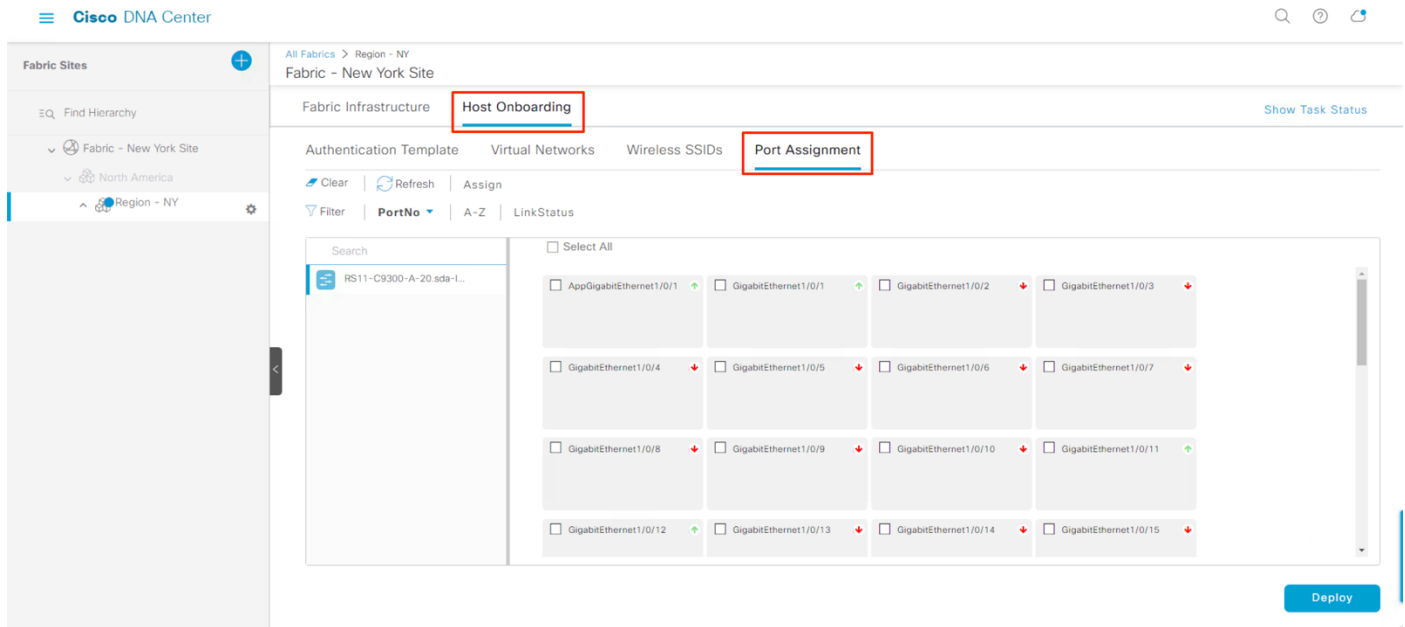
For endpoints without a supplicant, Cisco DNA Center provides a workflow to statically configure the edge node's port connecting to the endpoint with VLAN and SGT information. The steps below demonstrate this static procedure which configures an access port with static VLAN and SGT assignment.

This procedure is not needed if the VLAN and SGT is dynamically assigned via ISE Authorization policies.

- Step 1.** In Cisco DNA Center, navigate to **Provision > Fabric**.
- Step 2.** Select the Fabric site in the **Fabrics** section.
- Step 3.** Select the site from the hierarchy list in the left panel.



- Step 4.** Click the **Host Onboarding** tab, then click the **Port Assignment** tab.



- Step 5.** Select the Edge Node from the list.
  - Step 6.** Select the applicable port(s) and click the **Assign** button.
- The Port Assignment slide out panel appears.

The screenshot shows the Cisco DNA Center interface for Host Onboarding. The breadcrumb navigation is "All Fabrics > Region - NY > Fabric - New York Site". The main tabs are "Fabric Infrastructure", "Host Onboarding", and "Wireless SSIDs". Under "Host Onboarding", there are sub-tabs for "Authentication Template", "Virtual Networks", and "Port Assignment". The "Port Assignment" sub-tab is active. In the top left, there are buttons for "Clear", "Refresh", and "Assign" (highlighted with a red box). Below these are filter options: "Filter", "PortNo", "A-Z", and "LinkStatus". The main area displays a search bar and a grid of network interfaces. The selected interfaces are GigabitEthernet1/0/11 and GigabitEthernet1/0/12, both highlighted in blue. A "Deploy" button is located at the bottom right.

**Step 7.** In the slide out, use the drop-downs to assign the following.

- Connected Device Type
- VLAN Name / IP Address Pool (Data)
- Scalable Group
- VLAN Name / IP Address Pool (Voice) (If applicable)
- Authentication Template
- Description (Optional)

The screenshot shows the "Port Assignment" configuration slide-out in Cisco DNA Center. The title "Port Assignment" is highlighted with a red box. The "Selected Interfaces (2)" section lists GigabitEthernet1/0/11 and GigabitEthernet1/0/12. The configuration fields are as follows:
 

- Connected Device Type: User Devices (ip-phone,computer,laptop)
- VLAN Name / IP Address Pool (Data): DATA-VN\_CAMPUS / NY\_VN\_Campus\_Data\_Pool ( 10.4.222.0 | VN\_CAMP...)
- Scalable Group: IP\_Phones
- VLAN Name / IP Address Pool (Voice): VOICE-VN\_CAMPUS / NY\_VN\_Campus\_Voice\_Pool ( 10.4.223.0 | VN\_CAM...)
- Authentication Template: No Authentication
- Description: Static\_Assignemnt\_VLAN\_SGT

 At the bottom right, there are "Cancel" and "Update" buttons, with the "Update" button highlighted by a red box.

**Step 8.** Click **Update**.

**Step 9.** Repeat the above steps, if needed, to configure additional ports, and click **Deploy**,

The screenshot shows the Cisco DNA Center interface for configuring a fabric. The breadcrumb navigation is "All Fabrics > Region - NY > FABRIC NY". The main navigation bar includes "Fabric Infrastructure", "Host Onboarding", and "Show Task Status". The "Host Onboarding" section has tabs for "Authentication Template", "Virtual Networks", "Wireless SSIDs", and "Port Assignment". The "Port Assignment" tab is active, showing a search bar with "RS11-C9300-A-20.sda-L..." and a "Select All" checkbox. Below this is a grid of 20 GigabitEthernet ports, each with a checkbox and a status indicator (red down arrow for down, green up arrow for up). The ports are arranged in a 4x5 grid. The "Deploy" button is highlighted with a red border.

**Step 10.** Select the **Now** option, and click **Apply**.

## Operate

This section covers the steps used to monitor, manage, and troubleshoot various network components in this *Independent Domain* deployment.

It is organized into the following processes and procedures.

Process	Procedure
<a href="#">Monitoring and Assuring the Cisco SD-Access Infrastructure</a>	<a href="#">View the Cisco DNA Center and ISE Communication Status</a> <a href="#">View Cisco DNA Center Assurance Summary</a> <a href="#">View Cisco DNA Center Assurance Details</a> <a href="#">View Fabric Provisioning Details in Cisco DNA Center</a>
<a href="#">Monitoring SD-WAN Edge TrustSec Configuration</a>	<a href="#">View the WAN Network Health in Cisco vManage</a>
<a href="#">Validating Policy Enforcement</a>	<a href="#">View GBAC Policies and Access Contracts</a> <a href="#">Verify Policy Configuration on Edge Nodes</a>

### Process 1: Monitoring and Assuring the Cisco SD-Access Infrastructure

This process demonstrates how to monitor and assure the SD-Access Infrastructure using Cisco DNA Center Assurance.

#### Procedure 1. View the Cisco DNA Center and Cisco Identity Service Engine Communication Status

Similar to the [steps](#) in the prerequisites, this procedure verifies Cisco DNA Center and ISE integration. This procedure displays a list of the ISE Primary and Secondary Policy Administration Nodes (PAN) and ISE Primary and Secondary pxGrid Nodes and their communication status with Cisco DNA Center.

**Step 1.** Navigating to **Cisco DNA Center > System > System 360**.

**Step 2.** Under **Externally Connected Systems**, view the status of the Identity Service Engine (ISE).

The output will vary based on the deployment. At minimum, there should be two entries:

- Primary – Available ✓
- PxGrid – Available ✓

Cisco DNA Center System - System 360 🔍 🔄 🏠

### System Management

#### Software Updates

As of Feb 8, 2021 6:22 AM

- Connected to Cisco's software server.
- 29 Application Updates available. [View](#)

#### Backups

As of Feb 8, 2021 6:22 AM

- No backups server configured. [Configure](#)

#### Application Health

As of Feb 8, 2021 6:22 AM

- Automation
- Assurance

### Externally Connected Systems

#### Identity Services Engine (ISE)

As of Feb 7, 2021 6:22 AM

SECONDARY	10.4.250.201	Available <span>🟢</span>
PRIMARY	10.4.250.200	Available <span>🟢</span>
PXGRID-ACTIVE	10.4.250.201	Available <span>🟢</span>
PXGRID-STANDBY	10.4.250.200	Configured <span>🟢</span>

[Update](#)

#### IP Address Manager (IPAM)

As of Feb 8, 2021 6:22 AM

- No IPAM server configured. [Configure](#)

#### vManage

As of Feb 7, 2021 6:22 AM

- No vManage server configured. [Configure](#)

## Procedure 2. View Cisco DNA Center Assurance Summary

The main Cisco DNA Center provides a wealth of information regarding the state and status of the devices it manages along with details on configuration elements. These are each shown in different dashlets.

**Step 1.** To view the overall network health including the network devices, wireless clients, and wired clients, navigate to the main dashboard by clicking the Cisco DNA Center button in the top left corner.

**Step 2.** For further details and to navigate to the Assurance application, click [View Details](#) in a dashlet.

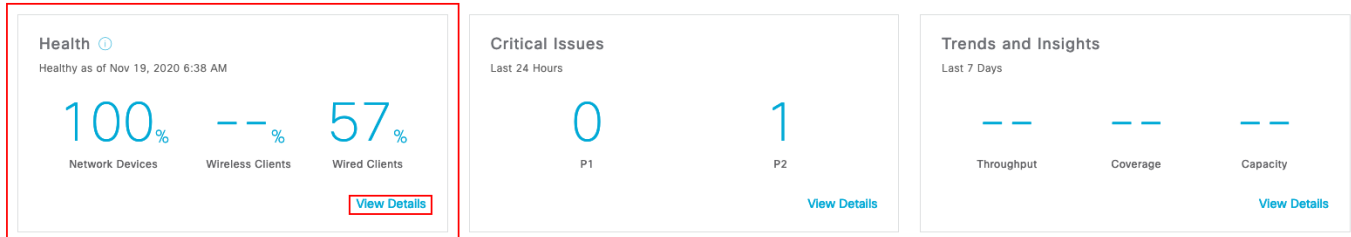


Welcome, admin

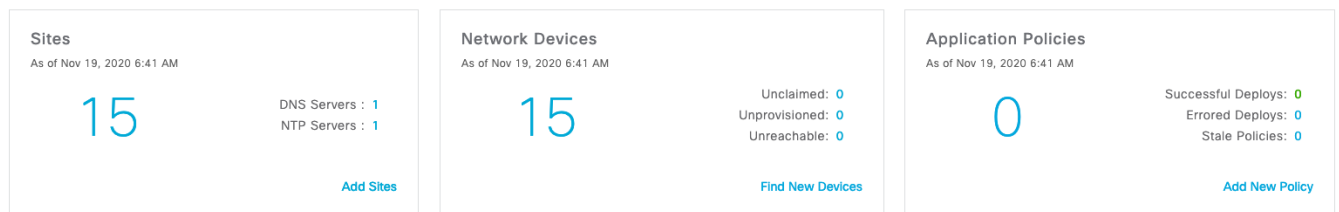
Take a Tour Learn More

Learn about new capabilities in this release on the Cisco DNA Center YouTube Channel.

Assurance Summary



Network Snapshot



**Procedure 3.** View Cisco DNA Center Assurance Details

The Cisco DNA Center Assurance application provides rich details and information that expands further on the summary data presented on the main dashboard.

**Step 1.** Navigate to **Cisco DNA Center > Assurance > Dashboards > Health.**

**Step 2.** Click the tabs for **Overall, Network, Client, Application** tabs to get respective detailed health information.

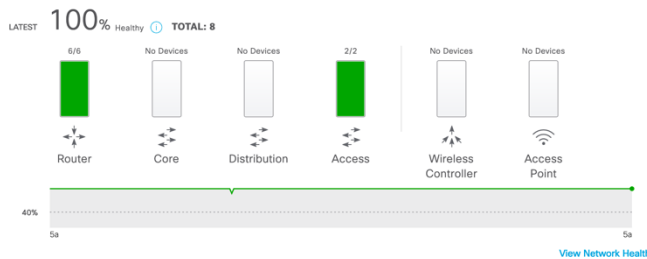
Tab	Details
Overall	Used to monitor and troubleshoot the overall health of your enterprise
Network	Displays global view of the network and is used to determine if there are potential network issues to address
Client	Displays global view of the health of all wired and wireless clients and is used to determine if there are potential client issues to address
Application	Displays global view of the applications is used to determine if there are application client issues to address

Overall **Network** Client Application

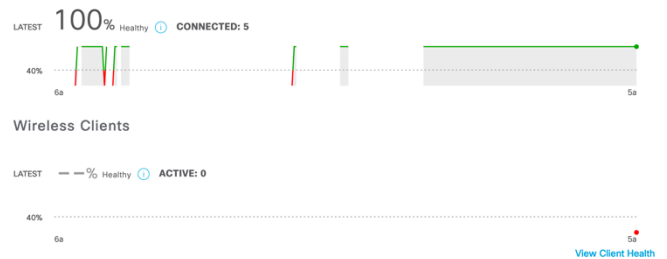
Global Last 24 Hours

Actions

### Network Devices



### Wired Clients



### Wireless Clients



### Top 10 Issue Types

Priority	Issue Type	Device Role	Category	Issue Count	Site Count (Area)	Device Count	Last Occurred Time
P2	Switch power failure	ACCESS	Device	1	1	1	Jun 21, 2020 12:40 PM
P3	Device time has drifted from Cisco DNA Center	BORDER ROUTER	Device	29	3	6	Jun 22, 2020 4:48 AM
P3	Device time has drifted from Cisco DNA Center	ACCESS	Device	13	2	2	Jun 22, 2020 2:41 AM
P3	Device time has drifted from Cisco DNA Center	UNKNOWN	Device	1	0	1	Jun 21, 2020 8:39 PM

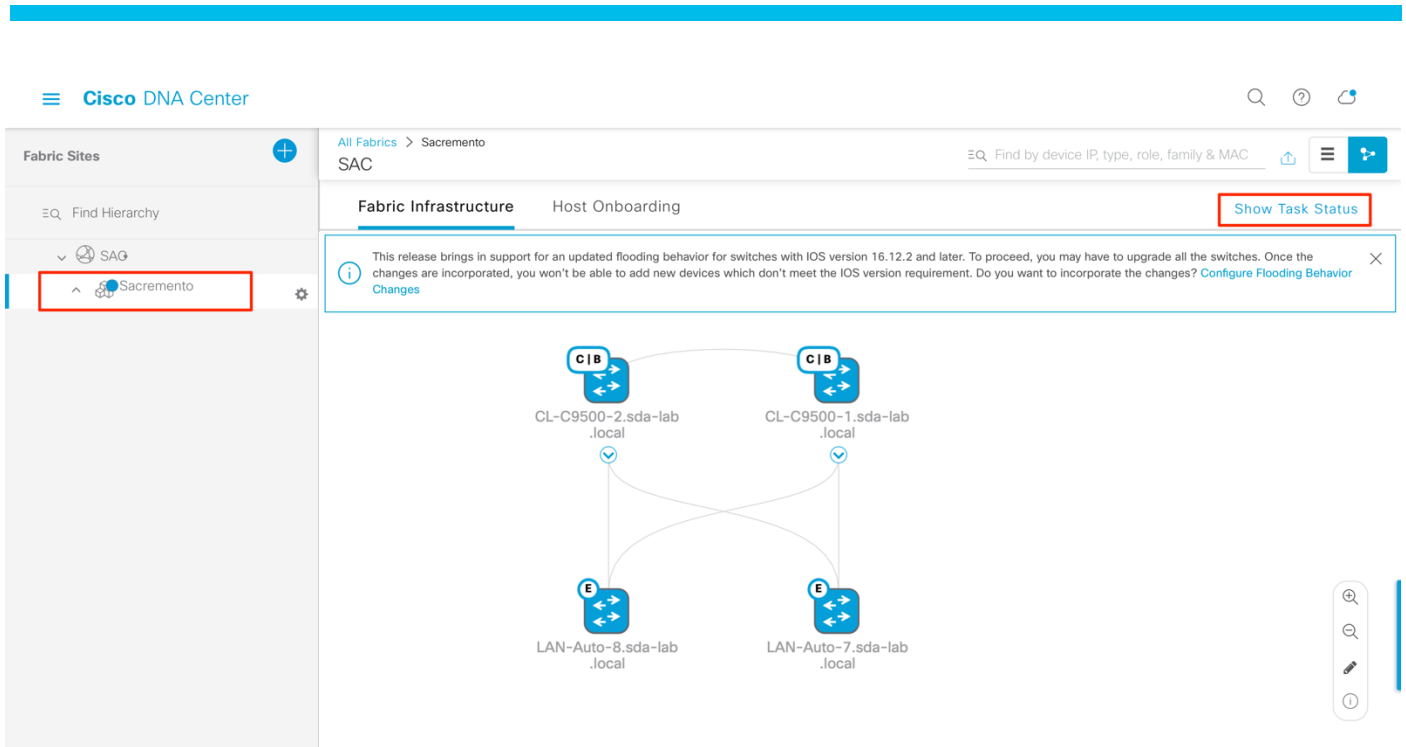
### Tech tip

For further details, please see the [Cisco DNA Center Assurance User Guide](#).

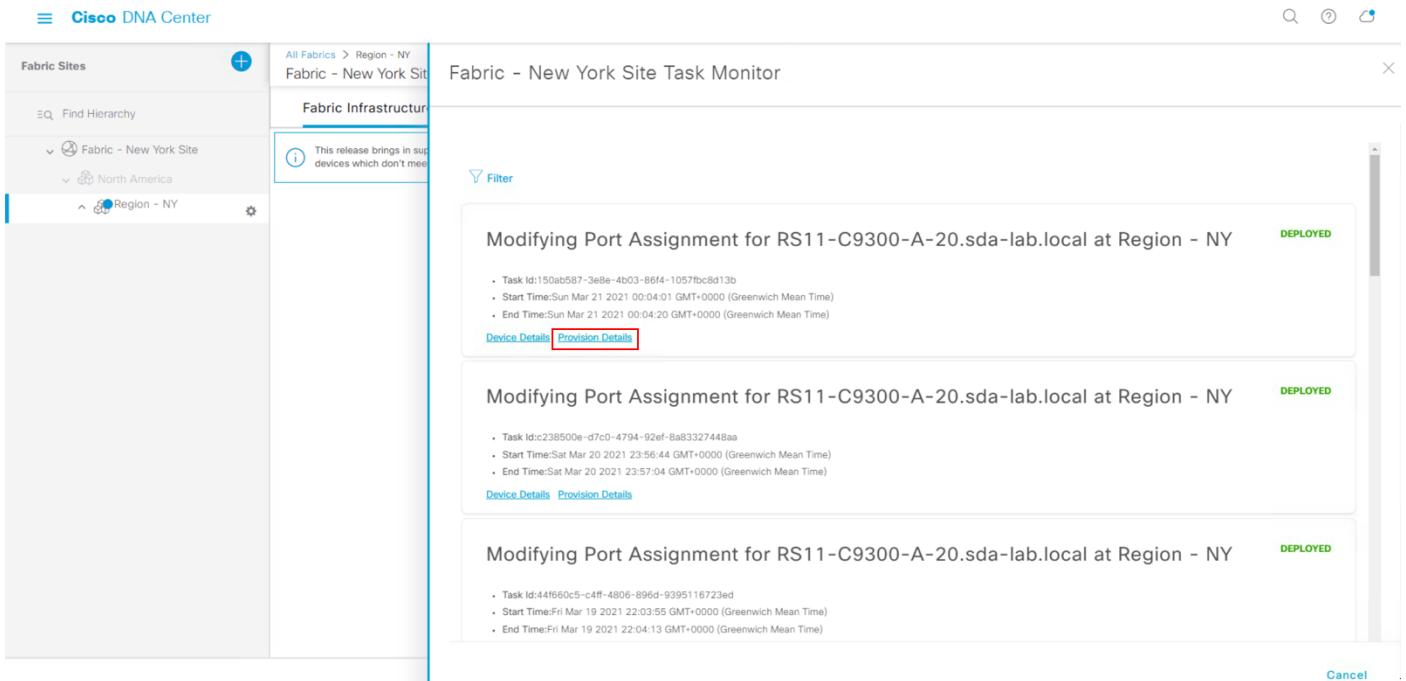
## Procedure 4. View Fabric Provisioning Details in Cisco DNA Center Task Status

Use this procedure to verify the configuration that is deployed on the SD-Access devices.

- Step 1.** In Cisco DNA Center, navigate to **Provision > Fabric**.
- Step 2.** Select the Fabric site in the **Fabricks** section.
- Step 3.** Select the site from the hierarchy list in the left panel.
- Step 4.** Click **Show Task Status**.



**Step 5.** Under a task, select **Provision Details** to view the details.



## Process 2: Monitoring SD-WAN Edge TrustSec Configuration

Use this process to view the status of the TrustSec configuration on the WAN Edge routers.

### Procedure 1. View the Cisco TrustSec Interface Details on the WAN Edge Router

**Step 1.** Navigate to **vManage > Monitor > Network**.

**Step 2.** Select the WAN Edge from the list.

**Step 3.** Select **Real Time** option from the left panel.

**Step 4.** In the **Device Options** box, search for the following: **Interface trustsec**

- The desired **mode** is **cts-ndac-mode-manual**.
- The desired **SGT propogate** is **cts-sgt-propogate-enabled**.
- The desired **SGT value** is **2**.
- The desired **SGT Assignment** is **cts-manual-trusted**.

### Tech tip

The SGT value should match the Trusted Value defined in [Step 7](#) of the inline tagging configuration of the sub-interfaces on the SD-WAN Edge Router.

The screenshot shows the Cisco vManage interface. The breadcrumb navigation is 'MONITOR Network > Real Time'. The selected device is 'RS12-ISR4331-19 | 2.2.2.19 | Site ID: 12 | Device Model: ISR4331'. The 'Device Options' search box contains 'Interface trustsec'. The table below shows the results of the search.

Interface Name	mode	SGT propagate	SGT	SGT Assignment
GigabitEthernet0/0/2	cts-ndac-mode-manual	cts-sgt-propagate-enabled	2	cts-manual-trusted
GigabitEthernet0/0/2.3001	cts-ndac-mode-manual	cts-sgt-propagate-enabled	2	cts-manual-trusted
GigabitEthernet0/0/2.3002	cts-ndac-mode-manual	cts-sgt-propagate-enabled	2	cts-manual-trusted
GigabitEthernet0/0/2.3003	cts-ndac-mode-manual	cts-sgt-propagate-enabled	2	cts-manual-trusted
GigabitEthernet0/0/2.3004	cts-ndac-mode-manual	cts-sgt-propagate-enabled	2	cts-manual-trusted
GigabitEthernet0/0/2.656	cts-ndac-mode-manual	cts-sgt-propagate-enabled	2	cts-manual-trusted

## Process 3: Validating Policy Enforcement

Use this process to view the TrustSec that has been defined in Cisco DNA Center and that has been provisioned the SD-Access Fabric devices.

### Procedure 1. View Group-Based Access Control Policies and Access Contracts

This procedure uses the Cisco DNA Center Policy Application to view the configuration of the TrustSec Policy Matrix and the defined Access Contracts.

**Step 1.** Navigate to **Cisco DNA Center > Policy > Group-Based Access Control.**

**Step 2.** Select the **Policies** to view the TrustSec Policy Matrix.

The screenshot shows the Cisco DNA Center interface for Policy - Group-Based Access Control. The 'Policies' tab is selected. The page displays a TrustSec Policy Matrix with the following columns for Destination: Auditors, BYOD, Contractors, Developers, Development\_Se..., Employees, External, Guests, Intranet, IPT\_Laptops, IP\_Printers, Internet\_Serv..., PD\_Servers, Public\_of\_Side..., Production\_Ser..., Production\_Ut..., Quarantine\_S..., Tel\_Servers, TrustSec\_Devel..., and Unknown. The rows for Source are Auditors, BYOD, Contractors, Developers, Development\_Se..., and Employees. A single yellow cell is visible at the intersection of the 'Contractors' source and 'Contractors' destination.

**Step 3.** Select the **Access Contracts** tab to view the predefined and custom Contracts.

The screenshot shows the Cisco DNA Center interface for Policy - Group-Based Access Control, with the 'Access Contracts' tab selected. It displays a table of 8 access contracts:

Name	Description	Created in	Rules Count	Policies
AllowDHCPDNS	Sample contract to allow DHCP and DNS		2	0
AllowWeb	Sample contract to allow access to Web		2	0
Deny IP	Deny IP SGACL			0
Deny_IP_Log	Deny IP with logging			0
DenyRemoteServices	Sample contract to block Remote Access and telnet services		4	0
EMPLOYEES_CONTRACTORS_LIMIT	Limited Communication between Employees and Contractors		4	1
Permit IP	Permit IP SGACL			0
Permit_IP_Log	Permit IP with logging			0

## Procedure 2. Verify Policy Configuration on Edge Nodes

This procedure uses the Cisco DNA Center Command Runner functionality to verify the policy configuration on edge nodes.

**Step 1.** Navigate to **Cisco DNA Center > Provision > Network Devices > Inventory.**

**Step 2.** Select an applicable edge node from the list.

A slide-out panel appears.

**Step 3.** Select **Run Commands.**

The screenshot displays the Cisco DNA Center interface. At the top, the breadcrumb navigation shows 'Provision - Network Devices - Inventory'. The main content area is titled 'RS11-C9300-A-20.sda-lab.local (10.5.205.3)'. On the left, a sidebar shows a list of devices, with 'RS11-C9300-A-20.sda-lab.local' selected. The main panel shows details for this device, including its name, IP address (10.5.205.3), location, and role (ACCESS). A 'Run Commands' button is highlighted. Below the details, there are sections for 'INVENTORY', 'SOFTWARE IMAGES', and 'PROVISION'. A 'Command Runner' window is open, displaying a welcome message and instructions for using the command runner interface.

**Step 4.** In the **Command Runner** tab, issue the following commands to view the policy configuration status.

**Table 9.** Policy Verification Commands – SD-Access Edge Node

Command	Command Details
show cts environment-data	Displays the Cisco TrustSec environment data downloaded from ISE
show authentication sessions interface <interface_id> details	Displays authentication details, associated authorization profile, SGT tag and associated security group-based policy for the endpoint connected on the interface
show cts role-based permissions	Displays the Security Group-Based policy downloaded from ISE for enforcement
show cts role-based counters	Displays the packets denied or permitted based on the defined Group-Based Access policy

## Appendix A: Hardware and Software Versions

The following products and software versions were included as part of validation in this deployment guide, and this validated set is not inclusive of all possibilities. Additional hardware options are listed in the associated [SD-Access Compatibility Matrix](#) and the [Cisco DNA Center data sheets](#). These documents may have guidance beyond what was tested as part of this guide. Updated Cisco DNA Center package files are regularly released and available within the packages and updates listing in the [release notes](#).

**Table 10.** Cisco SD-WAN Infrastructure

Product	Part number	Software Version
Cisco vSmart	viptela-smart-20.3.3-genericx86-64.ova	20.3.3
Cisco vManage	viptela-vmanage-20.3.3.1-genericx86-64.ova	20.3.3
Cisco vBond	viptela-edge-20.3.3-genericx86-64.ova	20.3.3

**Table 11.** Device Platform, Model, and Software Version

Platform	Model (PID)	Software Code Version
Cisco DNA Center	DN2-HW-APL-L	Cisco DNA Center 2.1.2.6
Identity Services Engine	R-ISE-VMS-K9	ISE 2.7 Patch 3
Catalyst 9300 Series	C9300-48U	17.3.3
ASR 1000x Series	ASR1002-X	17.3.3
WLC 8540 Series	AIR-CT8540-K9	8.10.151.0

**Table 12.** Cisco SD-Access Fabric Devices

Product	SD-Access Fabric Role
Catalyst 9500 Series Switches	Fabric in a Box
Cisco ASR 1000-X and 1000-HX Series Aggregation Services Routers	Colocated Border and Control Plane Node
Catalyst 9300 Series Switches	Edge Nodes

**Table 13.** Cisco DNA Center Package Versions

Package Name - GUI	Package Name - CLI	Software Version
System	system	1.5.279
System Commons	system-commons	2.1.266.62815
Access Control Application	access-control-application	2.1.266.62815
AI Endpoint Analytics	ai-endpoint-analytics	1.2.1.549

Package Name - GUI	Package Name - CLI	Software Version
AI Network Analytics	ai-network-analytics	2.4.26.0
Application Hosting	app-hosting	1.4.299.201120
Application Policy	application-policy	2.1.266.170289
Application Registry	application-registry	2.1.266.170289
Application Visibility	application-visibility-service	2.1.266.170289
Assurance - Base	assurance	2.1.2.500
Assurance - Sensor	sensor-assurance	2.1.2.496
Automation - Base	base-provision-core	2.1.266.62815
Automation - Intelligent Capture	icap-automation	2.1.266.62815
Automation - Sensor	sensor-automation	2.1.266.62815
Cisco AI Endpoint Analytics	endpoint-analytics	1.2.5.14
Cisco DNA Center Global Search	dnac-search	1.3.99.283
Cisco DNA Center Platform	dnac-platform	1.5.1.60
Cisco DNA Center UI	platform-ui	2.1.266.62815
Cisco SD-Access	sd-access	2.1.266.592420
Cisco Umbrella	umbrella	1.6.0.162
Cloud Connectivity - Data Hub	cloud-connectivity-data-hub	1.3.1.97
Cloud Connectivity - Tethering	cloud-connectivity-tethering	2.1.266.62815
Cloud Device Provisioning Application	cloud-provision-core	2.1.266.62815
Command Runner	command-runner	2.1.266.62815
Device Onboarding	device-onboarding	2.1.266.362261
Group Based Policy Analytics	group-based-policy-analytics	1.0.1.158
Image Management	image-management	2.1.266.62815
Machine Reasoning	machine-reasoning	2.1.266.215219
NCP - Base	ncp-system	2.1.266.62815
NCP - Services	automation-core	2.1.266.62815
Network Controller Platform	network-visibility	2.1.266.62815



Package Name - GUI	Package Name - CLI	Software Version
Network Data Platform - Base Analytics	ndp-base-analytics	1.5.1.187
Network Data Platform - Core	ndp-platform	1.5.1.805
Network Data Platform - Manager	ndp-ui	1.5.1.155
Path Trace	path-trace	2.1.266.62815
RBAC Extensions	rbac-extensions	2.1.266.1905024
Rogue Management	rogue-management	2.0.0.51
Stealthwatch Security Analytics	ssa	2.1.266.1095317
Wide Area Bonjour	wide-area-bonjour	2.4.265.75003

---

## Appendix B: References Used in This Guide

Cisco 4000 Series Integrated Services Router Gigabit Ethernet WAN Modules Data Sheet Cisco 4000 Series Integrated Services Router Gigabit Ethernet WAN Modules Data Sheet: <https://www.cisco.com/c/en/us/products/collateral/routers/4000-series-integrated-services-routers-isr/datasheet-c78-730527.html>

Cisco DNA Center Assurance User Guides: <https://www.cisco.com/c/en/us/support/cloud-systems-management/dna-center/products-user-guide-list.html>

Cisco SD-Access & Cisco DNA Center Management Infrastructure: <https://cs.co/sda-infra-pdg>

Cisco SD-Access Fabric Provisioning Prescriptive Deployment Guide: <https://cs.co/sda-fabric-pdg>

Cisco SD-Access for Distributed Campus Prescriptive Deployment Guide: <https://cs.co/sda-distrib-pdg>

Cisco SD-Access Solution Design Guide: <https://cs.co/sda-cvd>

Cisco SD-Access Solution Design Guide, SD-Access Operational Planes Chapter: <https://www.cisco.com/c/en/us/td/docs/solutions/CVD/Campus/cisco-sda-design-guide.html#SDAccessOperationalPlanes>

Cisco SD-WAN Design Guide: <https://www.cisco.com/c/en/us/td/docs/solutions/CVD/SDWAN/cisco-sdwan-design-guide.html>

Cisco SD-WAN Edge Onboarding Prescriptive Deployment Guide: <https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/SDWAN/sd-wan-wan-edge-onboarding-deploy-guide-2020jan.pdf>

Cisco SD-WAN End-to-End Deployment Guide: <https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/SDWAN/SD-WAN-End-to-End-Deployment-Guide.pdf>

Cisco vManage How-Tos for Cisco IOS XE SD-WAN Devices, Chapter: What's New in Cisco vManage: [https://www.cisco.com/c/en/us/td/docs/routers/sdwan/vManage\\_How-Tos/vmanage-howto-xe-book/whats-new.html](https://www.cisco.com/c/en/us/td/docs/routers/sdwan/vManage_How-Tos/vmanage-howto-xe-book/whats-new.html)

Overview of TrustSec Guide, Configuring Native SGT Propagation (Tagging): [https://www.cisco.com/c/dam/en/us/solutions/collateral/borderless-networks/trustsec/C07-730151-00\\_overview\\_of\\_trustSec\\_og.pdf](https://www.cisco.com/c/dam/en/us/solutions/collateral/borderless-networks/trustsec/C07-730151-00_overview_of_trustSec_og.pdf)

Release Notes for Cisco IOS XE SD-WAN Devices, Cisco IOS XE Release Amsterdam 17.3.x: [https://www.cisco.com/c/en/us/td/docs/routers/sdwan/release/notes/xe-17-3/sd-wan-rel-notes-xe-17-3.html#concept\\_ecj\\_kyz\\_blb](https://www.cisco.com/c/en/us/td/docs/routers/sdwan/release/notes/xe-17-3/sd-wan-rel-notes-xe-17-3.html#concept_ecj_kyz_blb)

---

## Appendix C: Acronym Glossary

**AAA**—Authentication, Authorization, and Accounting

**ACP**—Access-Control Policy

**ACI**—Cisco Application Centric Infrastructure

**ACK**—Acknowledge or Acknowledgement

**ACL**—Access-Control List

**AD**—Microsoft Active Directory

**AFI**—Address Family Identifier

**AMP**—Cisco Advanced Malware Protection

**AP**—Access Point

**API**—Application Programming Interface

**APIC**—Cisco Application Policy Infrastructure Controller (ACI)

**ASA**—Cisco Adaptive Security Appliance

**ASM**—Any-Source Multicast (PIM)

**ASR**—Aggregation Services Router

**Auto-RP**—Cisco Automatic Rendezvous Point protocol (multicast)

**AVC**—Application Visibility and Control

**BFD**—Bidirectional Forwarding Detection

**BGP**—Border Gateway Protocol

**BMS**—Building Management System

**BSR**—Bootstrap Router (multicast)

**BYOD**—Bring Your Own Device

**CAPWAP**—Control and Provisioning of Wireless Access Points Protocol

**CDP**—Cisco Discovery Protocol

**CEF**—Cisco Express Forwarding

**CMD**—Cisco Meta Data

**CPU**—Central Processing Unit

**CSR**—Cloud Services Routers

**CTA**—Cognitive Threat Analytics

**CUWN**—Cisco Unified Wireless Network

---

**CVD**—Cisco Validated Design

**CYOD**—Choose Your Own Device

**DC**—Data Center

**DHCP**—Dynamic Host Configuration Protocol

**DM**—Dense-Mode (multicast)

**DMVPN**—Dynamic Multipoint Virtual Private Network

**DMZ**—Demilitarized Zone (firewall/networking construct)

**DNA**—Cisco Digital Network Architecture

**DNS**—Domain Name System

**DORA**—Discover, Offer, Request, ACK (DHCP Process)

**DWDM**—Dense Wavelength Division Multiplexing

**ECMP**—Equal Cost Multi Path

**EID**—Endpoint Identifier

**EIGRP**—Enhanced Interior Gateway Routing Protocol

**EMI**—Electromagnetic Interference

**ETR**—Egress Tunnel Router (LISP)

**EVPN**—Ethernet Virtual Private Network (BGP EVPN with VXLAN data plane)

**FHR**—First-Hop Router (multicast)

**FHRP**—First-Hop Redundancy Protocol

**FMC**—Cisco Firepower Management Center

**FTD**—Cisco Firepower Threat Defense

**GBAC**—Group-Based Access Control

**GbE**—Gigabit Ethernet

**Gbit/s**—Gigabits Per Second (interface/port speed reference)

**GRE**—Generic Routing Encapsulation

**GRT**—Global Routing Table

**HA**—High-Availability

**HQ**—Headquarters

**HSRP**—Cisco Hot-Standby Routing Protocol

**HTDB**—Host-tracking Database (SD-Access control plane node construct)

**IBNS**—Identity-Based Networking Services (IBNS 2.0 is the current version)

---

**ICMP**— Internet Control Message Protocol

**IDF**—Intermediate Distribution Frame; essentially a wiring closet.

**IEEE**—Institute of Electrical and Electronics Engineers

**IETF**—Internet Engineering Task Force

**IGP**—Interior Gateway Protocol

**IID**—Instance-ID (LISP)

**IOE**—Internet of Everything

**IoT**—Internet of Things

**IP**—Internet Protocol

**IPAM**—IP Address Management

**IPS**—Intrusion Prevention System

**IPSec**—Internet Protocol Security

**ISE**—Cisco Identity Services Engine

**ISR**—Integrated Services Router

**IS-IS**—Intermediate System to Intermediate System routing protocol

**ITR**—Ingress Tunnel Router (LISP)

**LACP**—Link Aggregation Control Protocol

**LAG**—Link Aggregation Group

**LAN**—Local Area Network

**L2 VNI**—Layer 2 Virtual Network Identifier; as used in SD-Access Fabric, a VLAN.

**L3 VNI**— Layer 3 Virtual Network Identifier; as used in SD-Access Fabric, a VRF.

**LHR**—Last-Hop Router (multicast)

**LISP**—Location Identifier Separation Protocol

**MAC**—Media Access Control Address (OSI Layer 2 Address)

**MAN**—Metro Area Network

**MEC**—Multichassis EtherChannel, sometimes referenced as **MCEC**

**MDF**—Main Distribution Frame; essentially the central wiring point of the network.

**MnT**—Monitoring and Troubleshooting Node (Cisco ISE persona)

**MOH**—Music on Hold

**MPLS**—Multiprotocol Label Switching

**MR**—Map-resolver (LISP)

---

**MS**—Map-server (LISP)

**MSDP**—Multicast Source Discovery Protocol (multicast)

**MTU**—Maximum Transmission Unit

**NAC**—Network Access Control

**NAD**—Network Access Device

**NAT**—Network Address Translation

**NBAR**—Cisco Network-Based Application Recognition (NBAR2 is the current version).

**NFV**—Network Functions Virtualization

**NSF**—Non-Stop Forwarding

**OMP**— Overlay Management Protocol

**OSI**—Open Systems Interconnection model

**OSPF**—Open Shortest Path First routing protocol

**OT**—Operational Technology

**PAgP**—Port Aggregation Protocol

**PAN**—Primary Administration Node (Cisco ISE persona)

**PCI DSS**—Payment Card Industry Data Security Standard

**PD**—Powered Devices (PoE)

**PETR**—Proxy-Egress Tunnel Router (LISP)

**PIM**—Protocol-Independent Multicast

**PITR**—Proxy-Ingress Tunnel Router (LISP)

**PnP**—Plug-n-Play

**PoE**—Power over Ethernet (Generic term, may also refer to IEEE 802.3af, 15.4W at PSE)

**PoE+**—Power over Ethernet Plus (IEEE 802.3at, 30W at PSE)

**PSE**—Power Sourcing Equipment (PoE)

**PSN**—Policy Service Node (Cisco ISE persona)

**pxGrid**—Platform Exchange Grid (Cisco ISE persona and publisher/subscriber service)

**PxTR**—Proxy-Tunnel Router (LISP – device operating as both a PETR and PITR)

**QoS**—Quality of Service

**RADIUS**—Remote Authentication Dial-In User Service

**REST**—Representational State Transfer

**RFC**—Request for Comments Document (IETF)

---

**RIB**—Routing Information Base

**RLOC**—Routing Locator (LISP)

**RP**—Rendezvous Point (multicast)

**RP**—Redundancy Port (WLC)

**RP**—Route Processer

**RPF**—Reverse Path Forwarding

**RR**—Route Reflector (BGP)

**RTT**—Round-Trip Time

**SA**—Source Active (multicast)

**SAFI**—Subsequent Address Family Identifiers (BGP)

**SD**—Software-Defined

**SDA**—Cisco Software Defined-Access

**SD-Access**—Cisco Software Defined-Access

**SDN**—Software-Defined Networking

**SD-WAN**—Cisco Software-Defined WAN

**SFP**—Small Form-Factor Pluggable (1 GbE transceiver)

**SFP+**— Small Form-Factor Pluggable (10 GbE transceiver)

**SGACL**—Security-Group ACL

**SGT**—Scalable Group Tag, sometimes reference as Security Group Tag

**SM**—Spare-mode (multicast)

**SNMP**—Simple Network Management Protocol

**SSID**—Service Set Identifier (wireless)

**SSM**—Source-Specific Multicast (PIM)

**SSO**—Stateful Switchover

**STP**—Spanning-tree protocol

**SVI**—Switched Virtual Interface

**SVL**—Cisco StackWise Virtual

**SWIM**—Software Image Management

**SXP**—Scalable Group Tag Exchange Protocol

**Syslog**—System Logging Protocol

**TACACS+**—Terminal Access Controller Access-Control System Plus

---

**TCP**—Transmission Control Protocol (OSI Layer 4)

**UCS**— Cisco Unified Computing System

**UDP**—User Datagram Protocol (OSI Layer 4)

**UPoE**—Cisco Universal Power Over Ethernet (60W at PSE)

**UPoE+**— Cisco Universal Power Over Ethernet Plus (90W at PSE)

**URL**—Uniform Resource Locator

**VLAN**—Virtual Local Area Network

**VN**—Virtual Network, analogous to a VRF in SD-Access

**VNI**—Virtual Network Identifier (VXLAN)

**vPC**—virtual PortChannel (Cisco Nexus)

**VPLS**—Virtual Private LAN Service

**VPN**—Virtual Private Network

**VPNv4**—BGP address family that consists of a Route-Distinguisher (RD) prepended to an IPv4 prefix

**VPWS**—Virtual Private Wire Service

**VRF**—Virtual Routing and Forwarding

**VSL**—Virtual Switch Link (Cisco VSS component)

**VSS**—Cisco Virtual Switching System

**VXLAN**—Virtual Extensible LAN

**WAN**—Wide-Area Network

**WLAN**—Wireless Local Area Network (generally synonymous with IEEE 802.11-based networks)

**WoL**—Wake-on-LAN

**xTR**—Tunnel Router (LISP – device operating as both an ETR and ITR)



---

## Appendix D: Recommended for You

Cisco IBNG / Enterprise Networking Validated Design and Deployment Guides: <https://cs.co/en-cvds>

Deploying SD-Access Embedded Wireless on Cat9300 switches: <https://community.cisco.com/t5/networking-documents/cisco-sd-access-embedded-wireless-on-catalyst-9300-deployment/ta-p/3886635>

Cisco SD-Access Segmentation Design Guide: <https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/SDWAN/CVD-SD-WAN-Design-2018OCT.pdf>

Cisco SD-WAN Design Guide: <https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/SDWAN/sd-wan-wan-edge-onboarding-deploy-guide-2019dec.pdf>

Cisco SD-WAN: WAN Edge Onboarding Deployment Guide:  
<https://www.cisco.com/c/dam/en/us/td/docs/solutions/CVD/SDWAN/sd-wan-wan-edge-onboarding-deploy-guide-2019dec.pdf>

Cisco SD-WAN Enabling Direct Internet Access Deployment Guide:  
<https://www.cisco.com/c/en/us/td/docs/solutions/CVD/SDWAN/CVD-SD-WAN-DIA-2019JUL.html>

Cisco SD-WAN Application-Aware Routing Deployment Guide:  
<https://www.cisco.com/c/en/us/td/docs/solutions/CVD/SDWAN/cisco-sdwan-application-aware-routing-deploy-guide.html>

---

## Appendix E: TrustSec Inline Tagging Syntax History and Explanation

### TrustSec Dynamic Peers Overview

Since its inception, Cisco TrustSec (CTS) has had two paradigms for trust establishment: dynamic and manual. Trust is necessary to understand if the TrustSec device should trust the SGT that is included in the frame or packet. Inclusive within that paradigm is the concept of dynamic peer authentication and authorization on an interface that uses inline tagging. This capability was enabled through the **cts dot1x** command in classic IOS software. In modern versions of Cisco software, IOS XE ≥16.x, this command is deprecated along with its capabilities. An explanation for that deprecation follows and is intended to clarify the current command structure used in manual trust.

The concept of dynamic trust via authentication and authorization was built before the IEEE 802.1AE MACsec standard and MKA (MACsec Key Agreement) were released. A pre-release proprietary method for key exchange was supported by certain devices. This proprietary method used the Security Association Protocol (SAP) for switch-to-switch authentication. The syntax for both MKA and SAP key exchange definitions were tightly coupled with the **cts** interface commands (**cts dot1x**, **cts manual**, etc) for the establishment of trust. In modern versions of software, MACsec and MKA configuration syntax are separate and decoupled from the **cts** interface commands.

Furthermore, **cts dot1x** dynamic peer authentication and authorization did not support a hitless failover method in the event that the ISE server was unavailable across all platforms. In addition, the **cts dot1x** commands were only available on switch interfaces resulting in a feature that was not widely deployed as it did not create the end-to-end automated trust environment through dynamic establishment. The reality of deployment and overlays (DMVPN, GETVPN, VXLAN, SD-WAN) established that SGT inline propagation and trust establishment was done exclusively with manual trust configuration. The result of these factors is that inline tagging is configured exclusively through the **cts manual** command and not the older methods.

### CTS Dynamic Peer SGT Overview

The intent of this dynamic peer authentication and authorization was to allow a form of plug and play and dynamic establishment of trust. When configuring the dynamic peer authentication and authorization elements (**cts dot1x**), an SGT value in ISE was assigned to the device via a process called Network Device Authorization Control (NDAC) and dynamically downloaded. This dynamic SGT value was used to apply policy to switch-to-switch traffic and corresponded to the device SGT of the peer device on the link. This SGT value also instructed the device to tag all untagged traffic with the corresponding value and instructed the peer device to use the SGT in the NDAC response for all traffic it sourced from itself. For the factors cited in the overview as well as operational considerations the use of this dynamic trust establishment was never widely deployed.

### Inline Tagging – Modern Configuration Conventions

Since the dynamic peer configuration was deprecated, a standard template and configuration convention has been used to ensure consistent behavior across platforms that support CTS inline tagging. This standard convention uses the SGT value of 2 as, by default in ISE, this SGT value is assigned to the **TrustSec\_Devices** Security Group (SG). This value is still assigned to devices for tagging sourced traffic via NDAC at the time of the device authentication and authorization in ISE though it is no longer used to authenticate and authorize peer devices. This manual trust establishment and templating is also compatible with modern Zero-Touch Provisioning (ZTP) and plug and play (PnP) solutions.

The SGT value that is assigned can technically be any value that is registered and defined in ISE, that has a human-readable, relevant name and description to the administrator, and that is not used for another purpose or assigned to another SG in the TrustSec domain.

The recommended practice in inline tagging is to assign a single SGT to all CTS network devices, to ensure that SGT value is assigned in ISE for **TrustSec\_Devices** SG devices, and to use the SGT value of 2. The value can be changed for policy reasons

---

though that practice calls for careful consideration. If changed, the corresponding SGT in ISE must be changed for full system continuity and integrity.

---

## Feedback

For comments and suggestions about this guide and related guides, join the discussion on [Cisco Community](https://cs.co/en-cvds) at <https://cs.co/en-cvds>.

### **Americas Headquarters**

Cisco Systems, Inc.  
San Jose, CA

### **Asia Pacific Headquarters**

Cisco Systems (USA) Pte. Ltd.  
Singapore

### **Europe Headquarters**

Cisco Systems International BV Amsterdam,  
The Netherlands

Cisco has more than 200 offices worldwide. Addresses, phone numbers, and fax numbers are listed on the Cisco Website at <https://www.cisco.com/go/offices>.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/go/trademarks>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)