Cisco SD-Access | SD-WAN *Integrated* Domain Pairwise Integration

Prescriptive Deployment Guide

October 2021

First Publish: 30 September 2021
Last Update: 12 October 2021

Contents

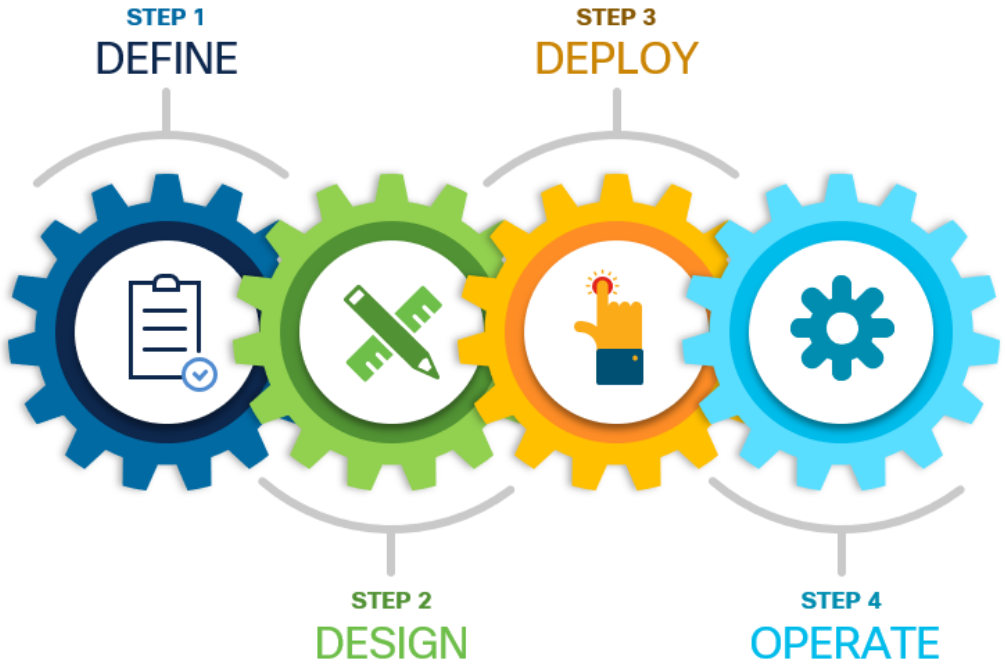
Hardware and Software Version Summary 3
About This Guide 4
Define 7
Cisco Software-Defined Wide Area Network Solution Overview 7
Cisco Software-Defined Access Overview 8
Protocol Operational Planes Overview 10
Cisco SD-Access | Cisco SD-WAN Pairwise Integration Overview 12
Integrated Domain Protocol Integrations 13
Design 16
Integrated Domain Design Considerations 21
Deploy 28
Process 1: Verifying Prerequisites for Integrated Domain 31
Process 2: Associate IOS-XE WAN Edge device with Service VPN 36
Process 3: Integrate the domain controllers 46
Process 4: Configuring LAN Segment manually 63
Process 5: Configuring LAN Segment with LAN Automation 81
Process 6: Provision Cisco SD-Access Fabric Site(s) 89
Process 7: Defining Group-Based Access Control Policies 121
Operate 126
Process 1: Monitoring and Assuring the Cisco SD-Access Infrastructure 126
Process 2: Validating Policy Enforcement 132
Process 3: Monitoring SD-WAN Edge device 133
Appendix A: Hardware and Software Versions 136
Appendix B: References Used in This Guide 140
Appendix C: Acronym Glossary 141
Appendix D: Recommended for You 147
Feedback 148

Hardware and Software Version Summary

Table 1. Hardware and Software Version Summary

Product	Software version
Cisco DNA Center Appliance	2.2.2.5 (System 1.6.424)
Cisco Identity Services Engine	3.0 Patch 2
Cisco SD-WAN Controllers	20.3.4
Cisco IOS XE WAN Edge Devices	IOS XE 17.3.4a
Cisco SD-Access Devices	IOS XE 17.3.4

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

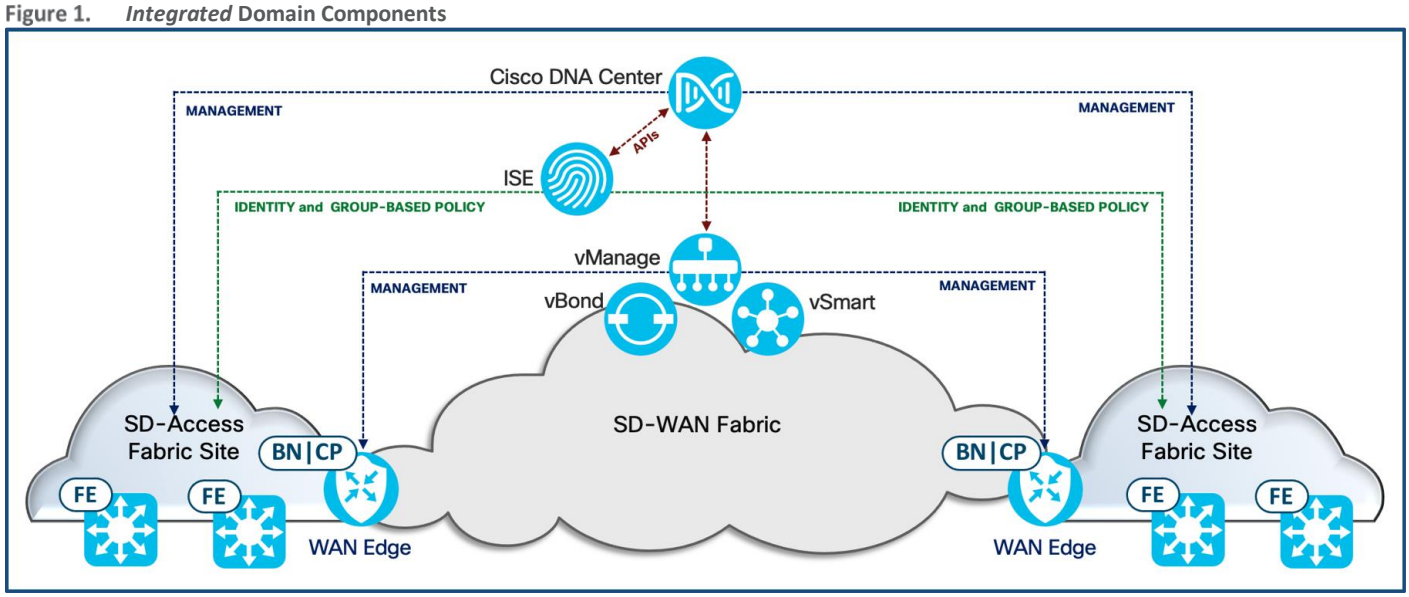
This guide provides design and deployment steps to use the Cisco SD-Access and Cisco SD-WAN solutions to achieve end-to-end segmentation and consistent policy across enterprise and branch. The guide focuses on the design considerations, best practices, and the step-by-step procedures needed to integrate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

The Cisco SD-Access | Cisco SD-WAN *Integrated* Domain and *Independent* 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. ***Integrated*** **Domain Components**



The guide focuses on the *Integrated* Domain deployment model where the SD-WAN controllers and Cisco DNA Center are integrated. In this approach, the WAN Edge devices perform both SD-WAN edge and SD-Access border and control plane functionality, managed and provisioned by the SD-WAN controllers. The SD-WAN vManage controller shares the WAN Edge devices to Cisco DNA Center. The SD-Access fabric components are managed and provisioned by the Cisco DNA Center.

Companion Resources

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

- SD-Access Solution Design Guide
- SD-Access and 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, 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 with the intent to maintain end-to-end automation, segmentation, and consistent group-based policy.

Define

This chapter is organized into the following sections:

Chapter	Section
Define	Cisco SD-WAN Solution Overview Cisco SD-Access Solution Overview Protocol Operational Planes Overview Cisco SD-Access | SD-WAN Pairwise Overview *Integrated* Domain Protocol Integrations

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

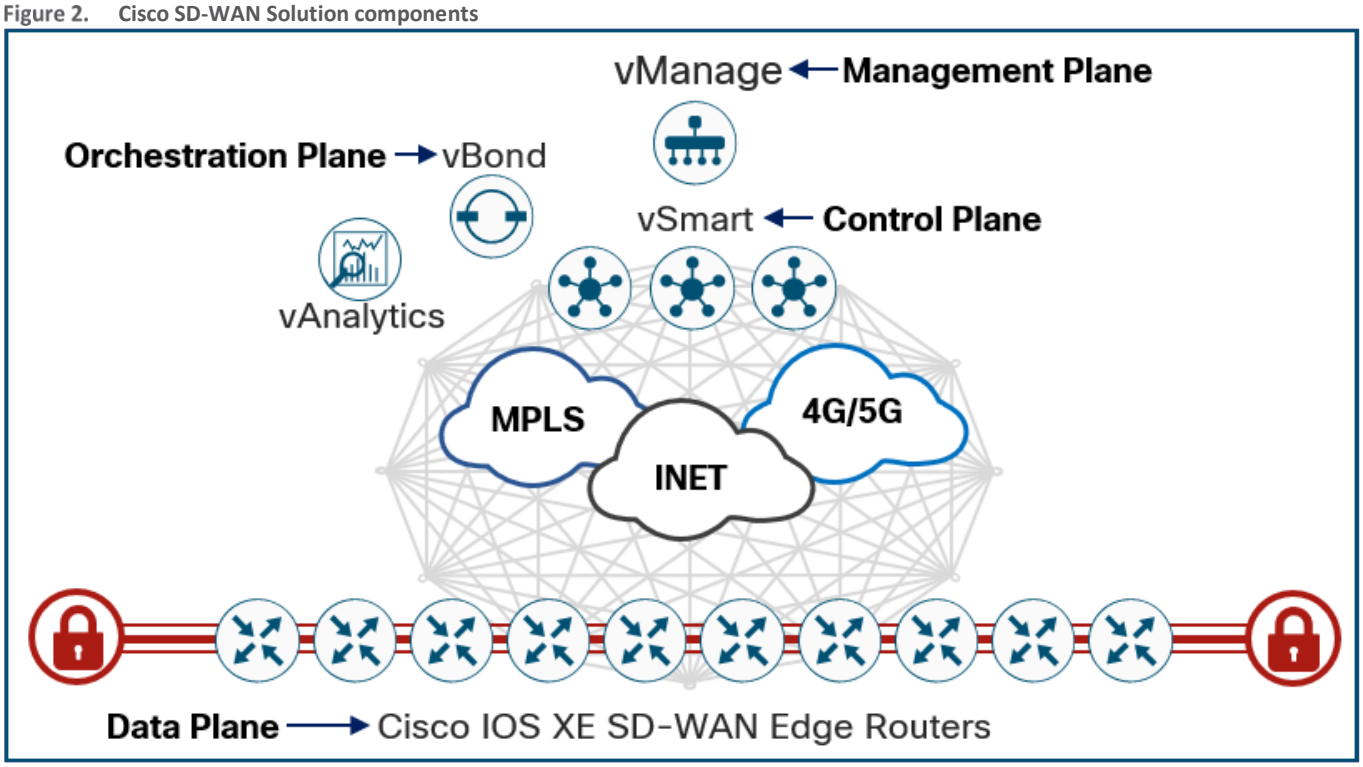
Management Plane Controller – Provides assurance, visibility, and management

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 drives 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 makes 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

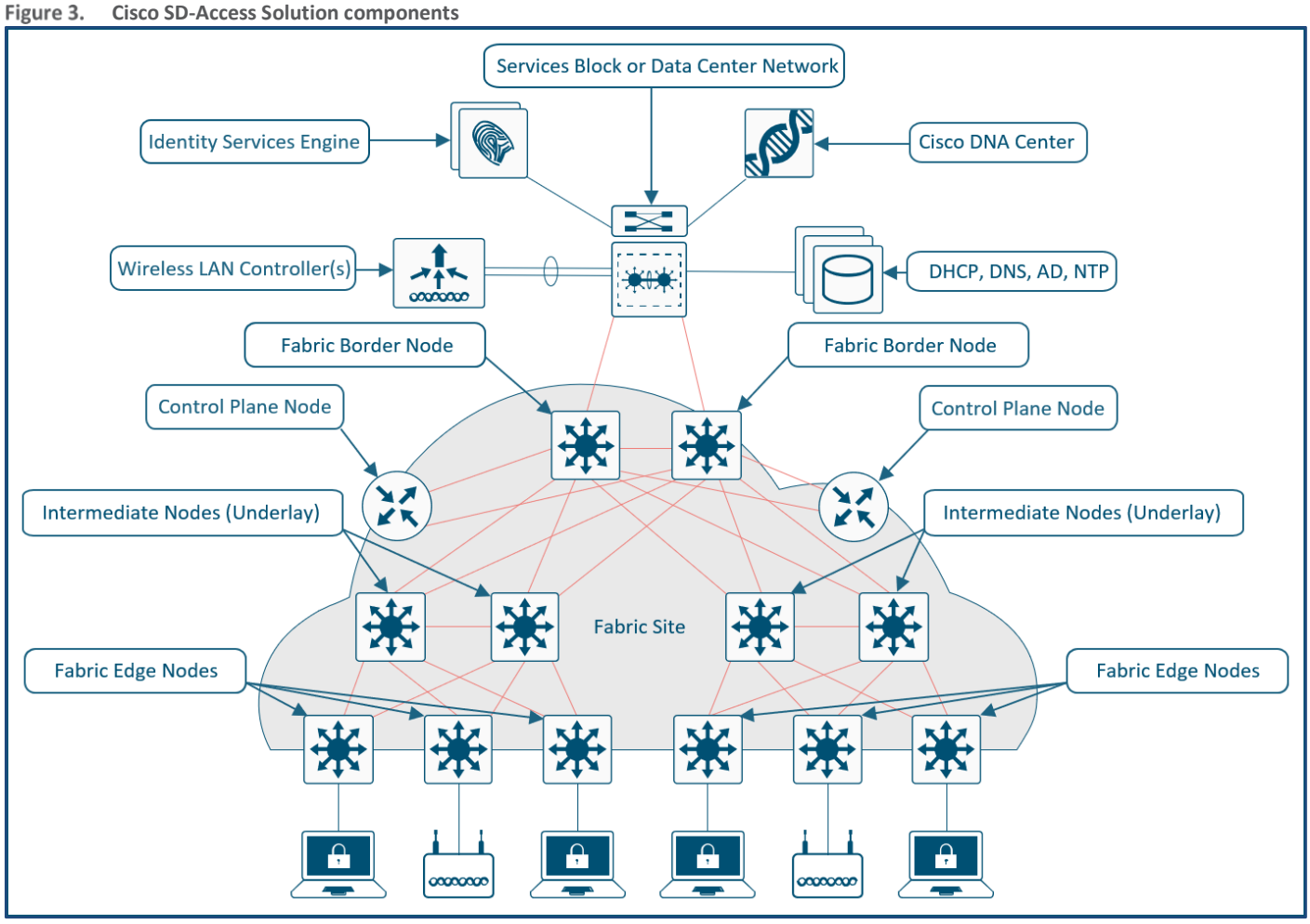
Cisco® Software-Defined Access (SD-Access) is the evolution from traditional campus designs to networks that directly implement the intent of an organization. SD-Access is a software application running on Cisco DNA Center hardware that is used to automate wired and wireless campus networks.

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® 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 – Independent fabric includes a control plane node, border node, edge node, and usually includes a Cisco Identity Services Engine (ISE) Policy Service Node (PSN) and fabric-mode Wireless LAN Controller (WLC).

Fabric Edge Nodes – This is 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 –This 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 access point (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 (ISE) – 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 Cisco 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 VN 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	Control Plane Protocols Data Plane Protocols Policy Plane Protocols

In SD-Access the control plane is based on Locator/ID Separation Protocol (LISP), the data plane is based on Virtual Extensible LAN (VXLAN), 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 Overlay Management Protocol (OMP), the data plane is based on IPSec/GRE, the policy plane is not limited to Layer 3 through Layer 7 information and can incorporate Service Level Agreements 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.

Tech tip
For additional details on the SD-Access protocols, see: SD-Access Operational Planes in the Cisco SD-Access Solution Design Guide.

Control Plane Protocols

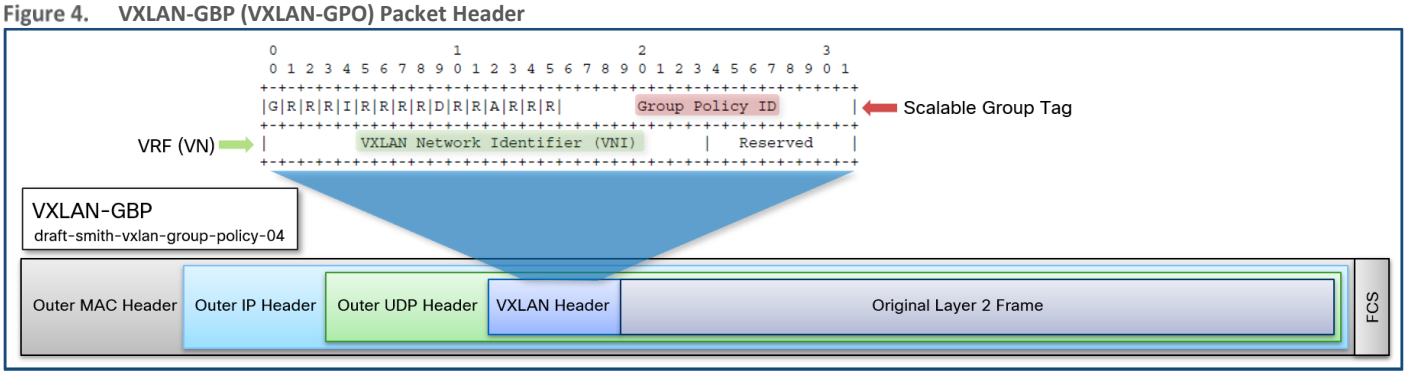
Cisco SD-Access leverages LISP control plane to communicate and exchange the endpoint's identity (EID) in relationship to its routing locator (RLOCs). The fabric devices query the control plane nodes to determine the RLOC information associated with the destination address (EID-to-RLOC mapping) and use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

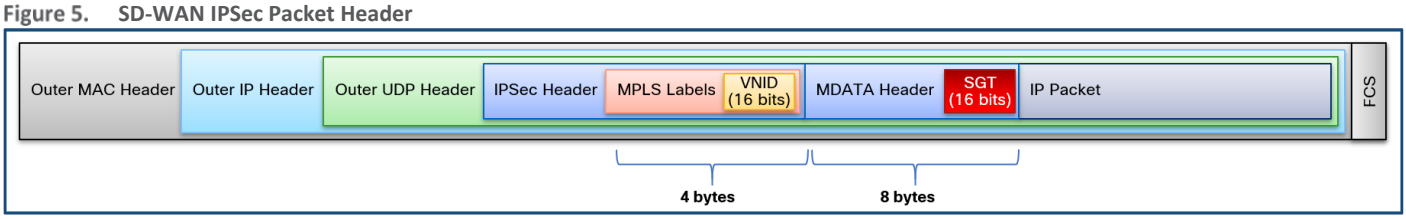


Cisco SD-WAN secures the data traffic with IPSec authentication and encryption. The secure data plane connection is established at the time of the WAN Edge onboarding process to ensure data plane integrity.

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 or MDATA, is used to carry the SGT in the WAN environment.

Figure 5. SD-WAN IPSec Packet Header



Policy Plane Protocols

The Cisco SD-Access solution leverages the 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 endpoints. 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.

Cisco SD-Access | Cisco SD-WAN Pairwise Integration Overview

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 three ways:

- *Integrated* Domain
- *Independent* Domain
- Both

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.

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 the vManage controller.

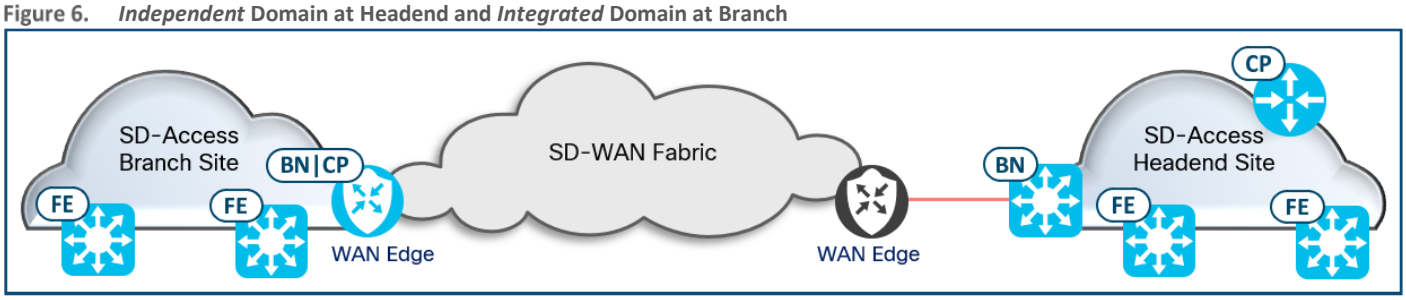
Cisco SD-Access | SD-WAN *Independent* Domain integration provide the capability of carrying end-to-end segmentation and policy with the flexibility of managing the domains independently. Using Inline tagging and 802.1Q tags, the segmentation constructs are carried across the *independent* domains.

Hybrid *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 networks.

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 6. *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.

Integrated Domain Protocol Integrations

This chapter is organized into the following sections:

Chapter	Section
Integrated Domain Protocol Integrations	Control Plane Integration Data Plane Integration Policy Plane Integration Putting It All Together

Control Plane Integrations – *Integrated* Domain

In the *Integrated Domain* Pairwise Integration, the WAN Edge device performs WAN Edge, colocated fabric Border and Control Plane functionality. SD-Access control plane protocol (LISP) is redistributed into SD-WAN control plane protocol (OMP) and vice versa to share routes across the sites. Each virtual network in the SD-Access environment is mapped to a dedicated service VPN in the SD-WAN environment. This ensures routes are shared across mapped segment and provide end-to-end segmentation across the WAN environment.

Data Plane Integrations – *Integrated* Domain

The data traffic in the SD-Access fabric site is VXLAN encapsulated. The VXLAN header carries the virtual network and scalable group tag from the Edge Node towards the Border Node or towards another Edge Node and vice-versa. The WAN Edge device, also the fabric Border Node, decapsulates the VXLAN packet and performs route lookup to determine the egress interface to reach the remote-site across the SD-WAN fabric in that segment. The VPN and SGT learnt from the SD-Access network is carried across the WAN transport to the remote site.

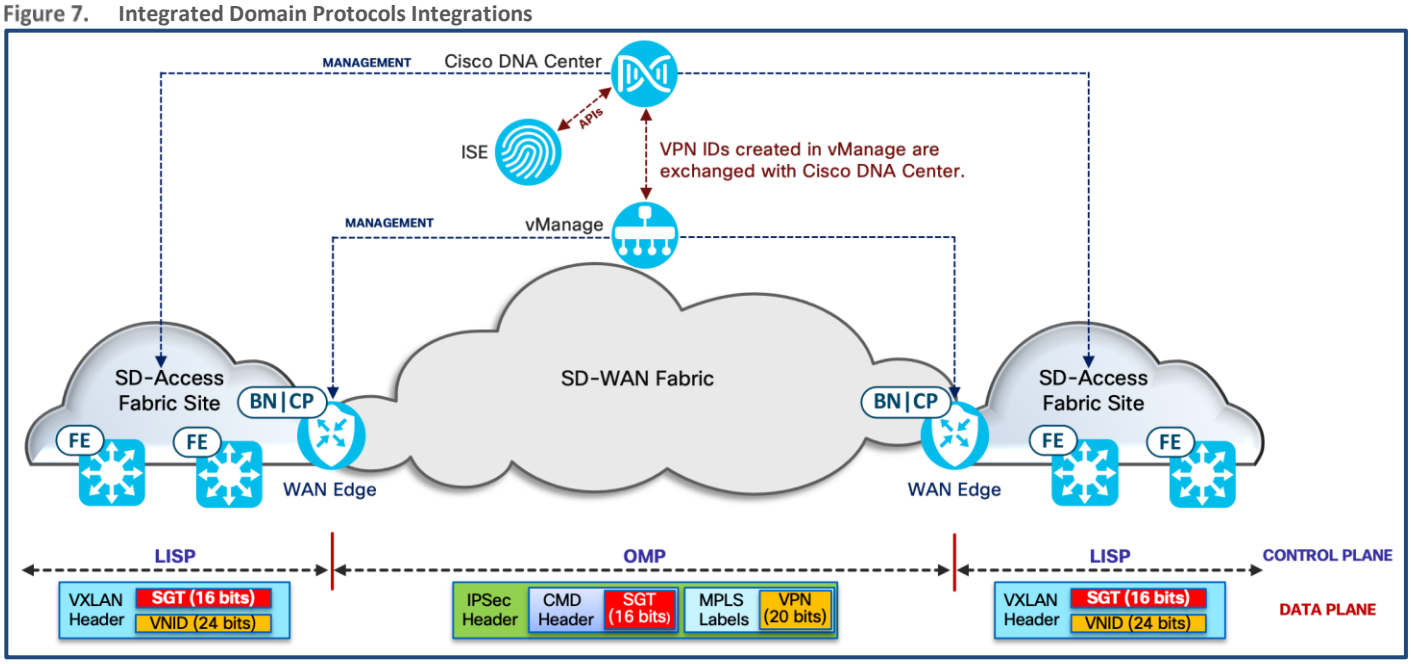
The remote-site WAN Edge device decapsulates the IPSec data packets. Based on the VPN ID information in the MPLS label header, the packet is forwarded into the appropriate SD-Access virtual network. The WAN Edge device copies the VPN and SGT in the IPSec header to the SD-Access VXLAN packet, before forwarding the data traffic at the SD-Access fabric segment, preserving the segment information in the data plane.

Policy Plane Integrations – *Integrated* Domain

In the *Integrated 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 IPSec packet. The Border Node, also the WAN Edge device, carries the SGT into the

IPSec CMD header. This allows the SGT to be carried across WAN transport 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 VXLAN header and carried in the fabric segment. This preserves the end-to-end segmentation in the policy plane.

Figure 7. Integrated 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 *Integrated* Domain deployment model, the domain controllers are integrated from the Cisco DNA-Center by providing SD-WAN vManage controller details.

The secure integration between the controllers allows to share information through RESTful API calls. The respective domain orchestrator owns the workflow and configuration generation:

- SD-WAN vManage controller owns the WAN configuration generation and provision.
- Cisco DNA Center owns the SD-Access configuration generation and provisioning to all LAN segment network devices with the exception of WAN Edge devices.
- Cisco DNA-Center builds and shares the required fabric configuration to the vManage SD-WAN controller to provision the WAN Edge with colocated Border and Control Plane functionality.

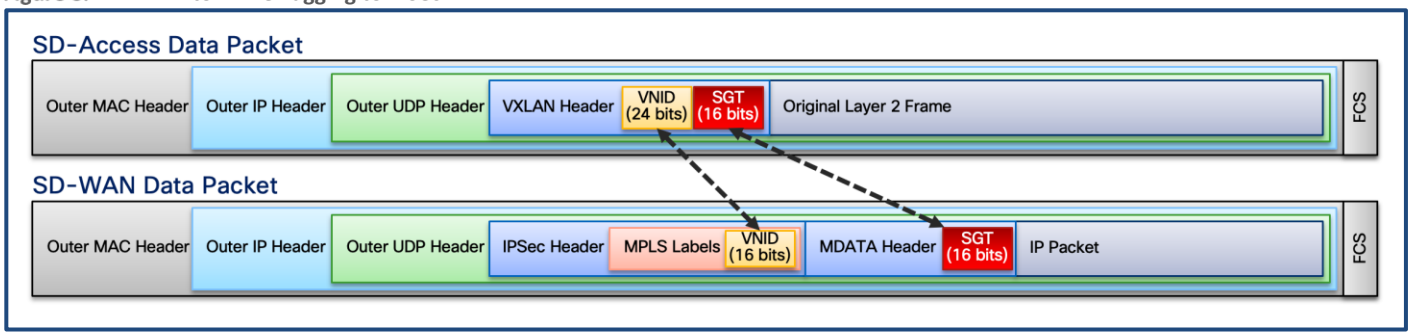
This provides enterprise deployments the flexibility to integrate the two domains together with the ability to securely onboard, provision the network devices and extend the benefits of Cisco SD-Access across sites, maintaining end-to-end segmentation and consistent policy across sites.

With the *Integrated 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 environment natively in the data plane.

- The WAN Edge device, also the fabric Border and Control Plane node, transfers the SGT data from the VXLAN into IPSec data packet header and carries it across the WAN environment, preserving the micro-segmentation.

Figure 8. VXLAN to Inline Tagging to IPSec



Design

This chapter is organized into the following sections:

Chapter	Section
Design	SD-WAN Flexible Topologies Overview SD-WAN High Availability Topologies SD-Access Flexible Topologies Overview Flexible Topologies Integration *Integrated* Domain Design Considerations

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 *Integrated* 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 the number of tunnels the router can support.

Based on the deployment requirements, the 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.

Refer to Cisco SD-WAN Design Guide for design recommendations and best practices to build SD-WAN infrastructure.

Figure 9. SD-WAN Hub-and-Spoke Deployment

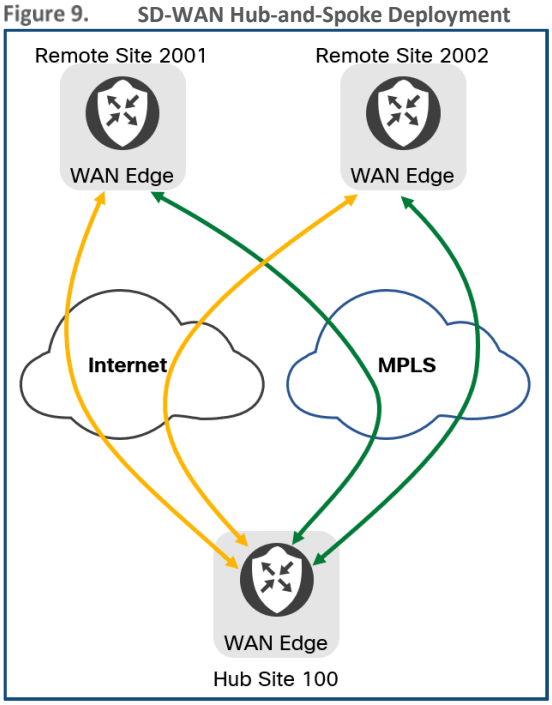


Figure 10. SD-WAN Partial-Mesh Deployment

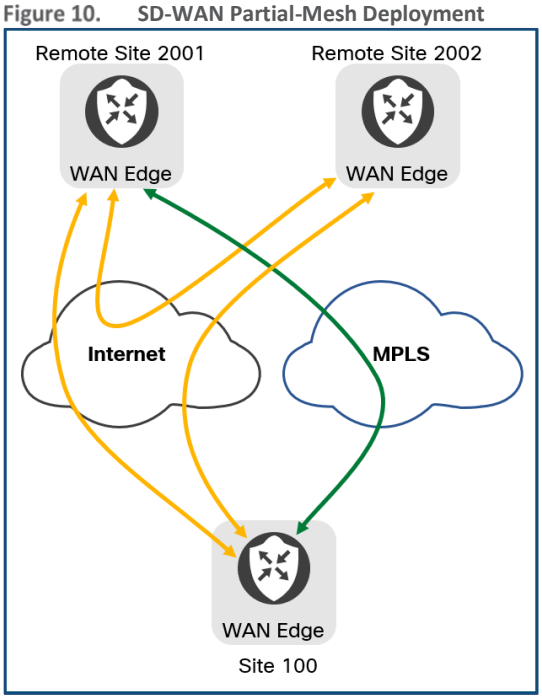
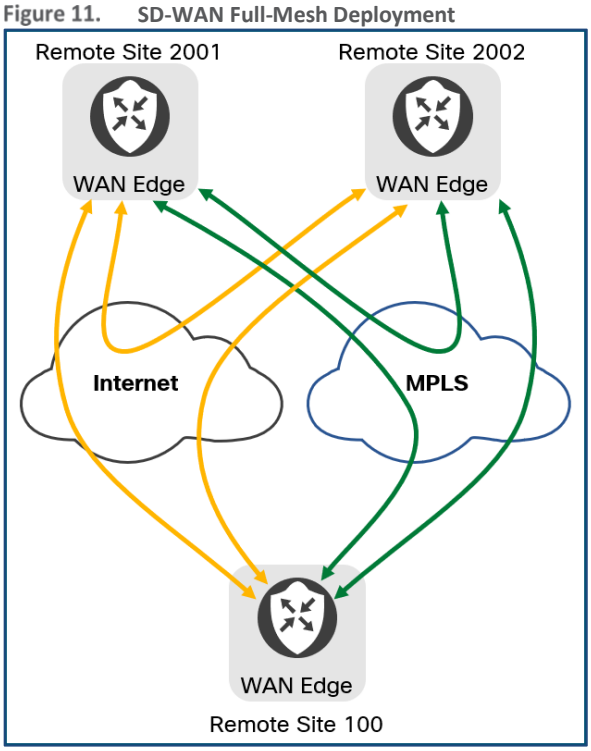


Figure 11. SD-WAN Full-Mesh Deployment



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 12. Single WAN Edge Dual Homed

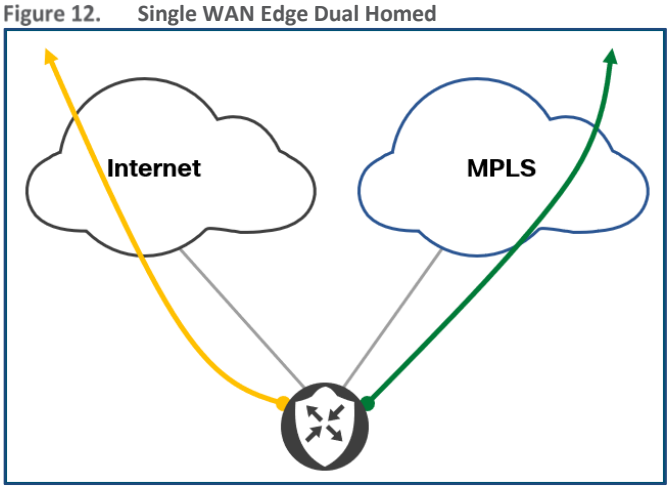


Figure 13. Two WAN Edge Devices Dual Multihomed

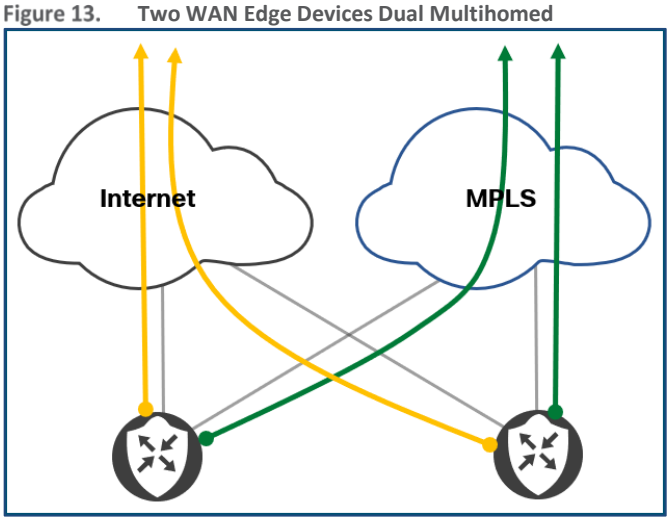
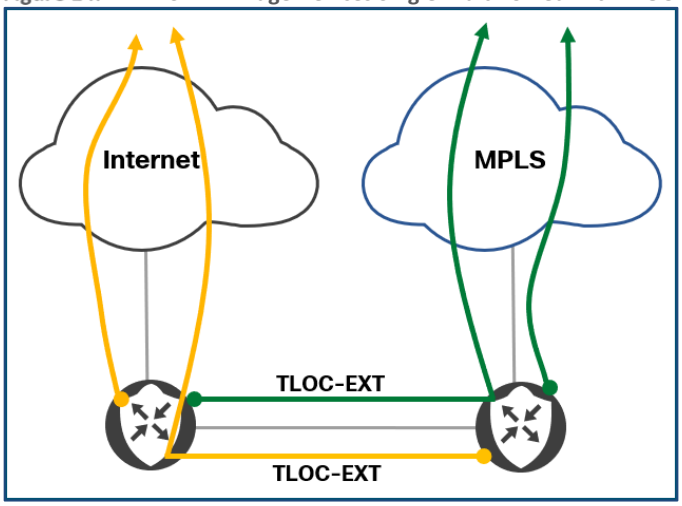


Figure 14. Two WAN Edge Devices Single Multihomed with TLOC Extension



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 it can be 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.

Refer to Cisco SD-Access Solution Design Guide - Underlay Network Design Chapter for design recommendations 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.

For *Integrated* Domain deployment, the SD-WAN WAN Edge device must be colocated with the SD-Access Border and Control Plane nodes functionality. This provides deployment flexibility for medium to small sites by co-locating the Border and Control Plane node and integrating embedded wireless on the Edge Node or with dedicated SD-Access Wireless Controller at the site for scaled environment. These solution deployment options provide flexibility to design a zero-trust, highly resilient, and always-available wired and wireless infrastructure, as shown in Figure 15.

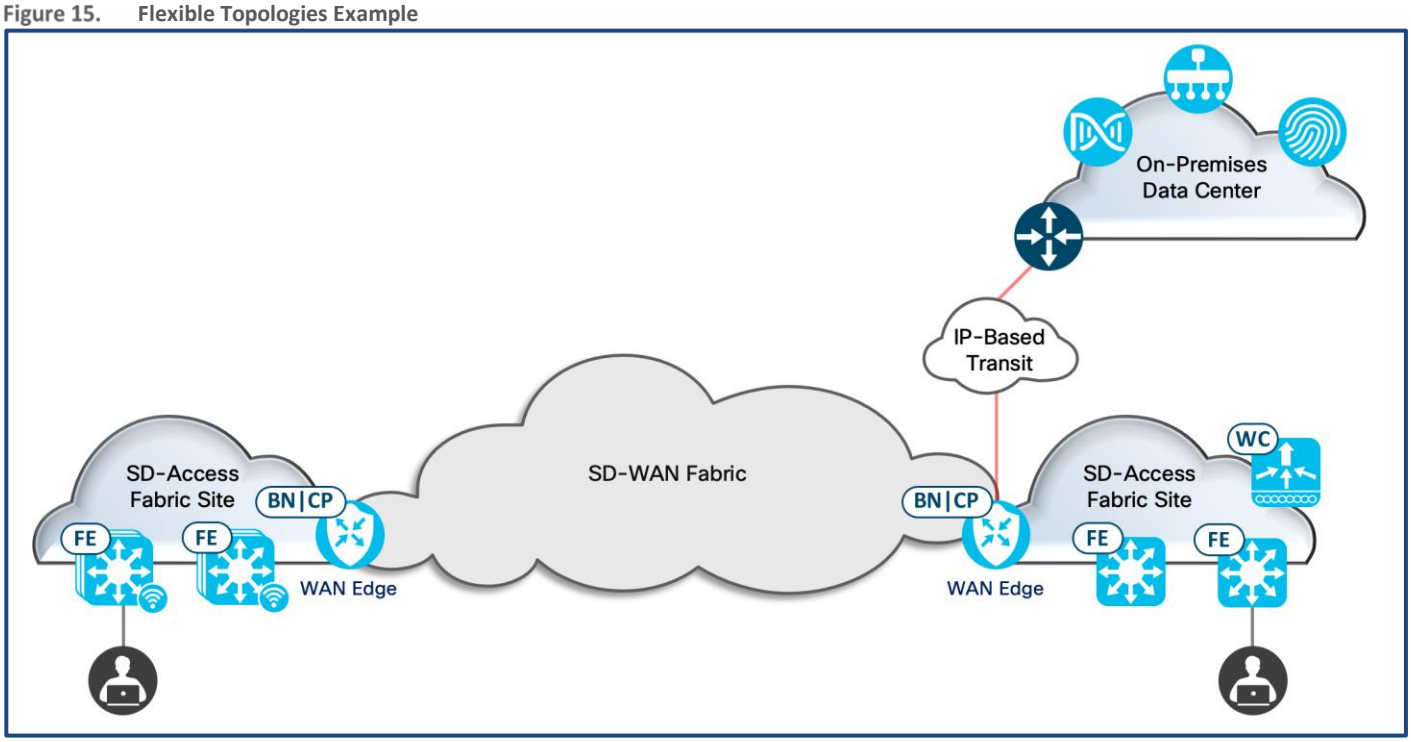
Refer to Cisco SD-Access Solution Design Guide for further design recommendations and best practices to build SD-Access infrastructure.

Flexible Topology Integration

With *Integrated* Domain SD-Access | SD-WAN Pairwise Integration, the SD-Access fabric sites must be new deployments. The SD-WAN WAN Edge routers at these locations can be new or existing network. *Integrated* Domain provides significant flexibility by integrating the two domains and 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 15. Flexible Topologies Example



Integrated Domain Design Considerations

This chapter is organized into the following sections:

Chapter	Section
Design Considerations	Service VPN and VN Considerations Underlay Infrastructure Considerations MTU Considerations Cisco SD-Access Fabric site considerations Macro-Segmentation considerations Micro-Segmentation Considerations Route-leaking Options SNMP and Syslog considerations Network Assurance and Visibility Latency Considerations Platform Requirements SD-Access Scale Considerations SD-WAN Edge SGT Forwarding Interoperability Deployment Limitations

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 that 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 device. This Fabric GRT Service VPN must be used at all sites to provide end-to-end IP reachability for the network devices.

Tech tip
The SD-WAN Global Routing Table uses VPN 0 to build the WAN fabric across WAN transports. 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. Mapping of SD-WAN Service VPN to Cisco SD-Access Virtual Network in DNA Center must be complete before SD-Access fabric site is created.

Underlay Infrastructure Considerations

Cisco SD-WAN Orchestrators take ownership of securely onboarding the WAN Edge devices and building resilient secure WAN network. The vManage controller integrated in Cisco DNA Center shares the selected WAN Edge devices part of the *Integrated* Domain integration with the Cisco DNA Center.

The shared WAN Edge devices can then be leveraged with Cisco DNA Center SD-Access workflow to build Fabric GRT infrastructure. The 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.

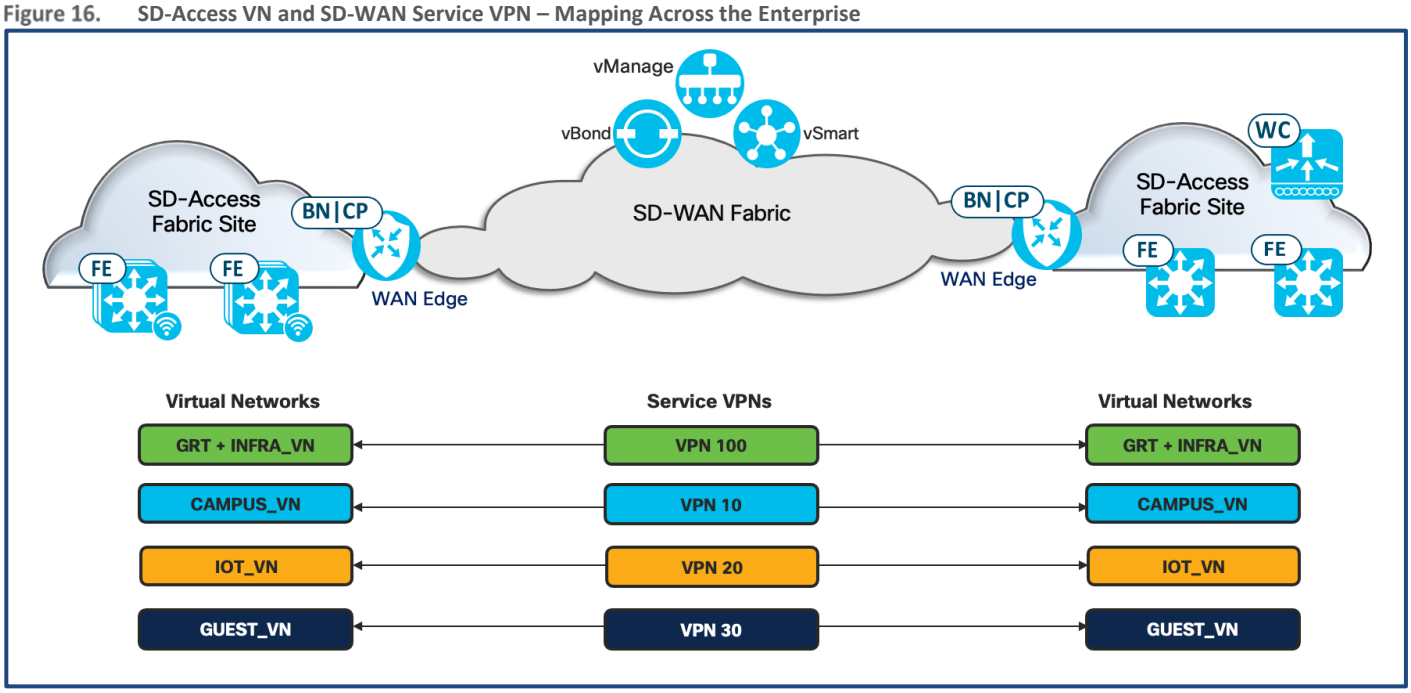
The WAN Edge device part of the *Integrated* domain integration can be configured as LAN Automation Seed devices to discover and configure the LAN segment network devices. LAN Automation provisions IS-IS routing protocol to provide Fabric GRT LAN connectivity at the site. Cisco DNA Center generated LAN Automation configuration for the WAN Edge device is shared with vManage orchestrator, to provision the WAN Edge device(s).

Alternatively, LAN segment can be manually configured and can leverage OSPF, EIGRP feature templates to build connectivity between the WAN Edge and the access layer.

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.

Tech tip
The WAN Edge device must be provisioned with /32 host mask ip address for Loopback 0 interface and should be part of Fabric GRT Service VPN. The WAN Edge interfaces that connect to the LAN segment should be associated to the Fabric GRT Service VPN.

Figure 16. SD-Access VN and SD-WAN Service VPN – Mapping Across the Enterprise



MTU Considerations

Cisco SD-Access VXLAN header adds an additional 50 bytes, and optionally 54 bytes, of encapsulation overhead. On switching platforms in SD-Access, the MTU is increased at the system level with the '*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.

Cisco SD-WAN Edge devices use the default MTU of 1500 bytes on the physical interface and this can be increased to a maximum MTU of 2000 bytes on the LAN-segment interfaces. To accommodate ethernet jumbo packets across the LAN segment, configure the WAN Edge device interface with MTU of 2000 bytes in the Cisco VPN Interface Ethernet feature template.

Tech tip
Fabric GRT network devices discovered and configured with Cisco DNA Center LAN Automation workflow will be provisioned higher MTU of 9100 bytes. The Seed device, WAN Edge device interface connecting the fabric site LAN segment is provisioned with MTU of 9100 bytes along with the system-mtu of 9100 bytes on the discovered switches.

MTU within the SD-WAN environment is addressed using Bidirectional Forwarding Detection (BFD) packets. These packets are used to periodically probe each WAN transport 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.

Cisco SD-Access Fabric Site Considerations

Before SD-Access fabric site is created, the following must be completed in Cisco DNA Center:

- Service VPN is associated to Virtual Network
- Network devices, including the SD-WAN WAN Edge devices are discovered with loopback 0 interface
- Network devices are provisioned to a site.

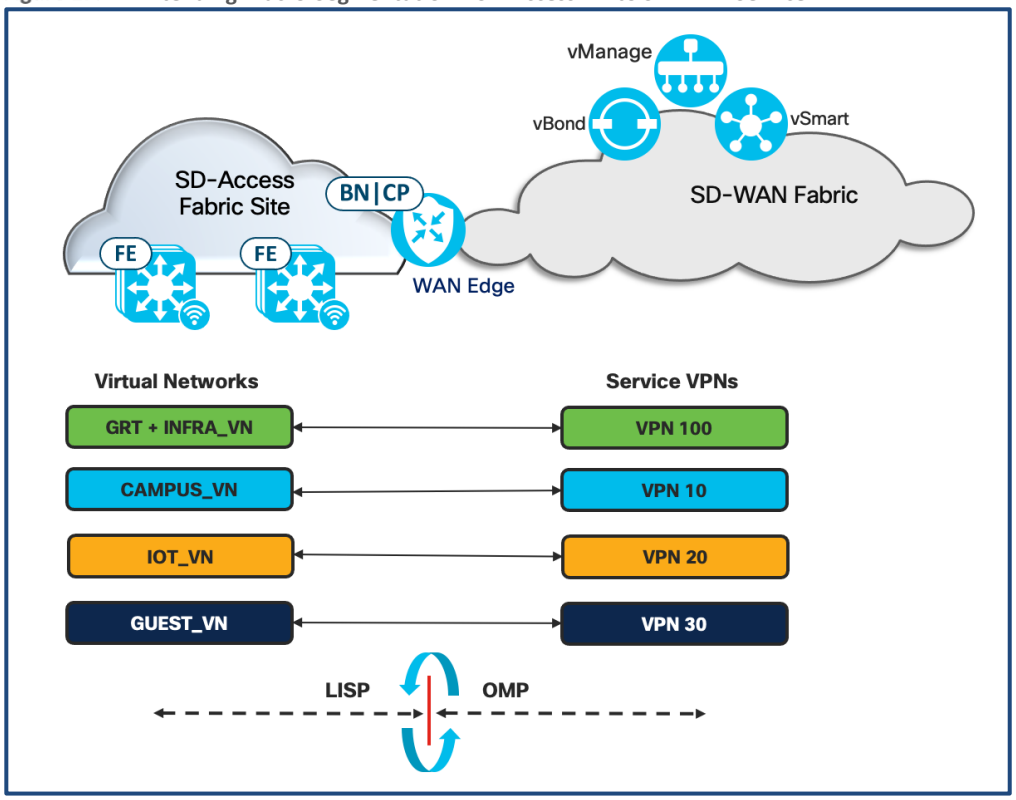
With the completion of the above, create fabric Site, associate fabric roles and connect IP-Transit or SD-WAN Transit or both. Note that the SD-WAN Transit is created in Cisco DNA Center on successful integration between the domain controllers. The WAN Edge part for the *Integrated* Domain integration is required to be associated with colocated Border and Control Plane Node functionality.

Macro-Segmentation Considerations

Cisco SD-Access overlay prefixes for each virtual network, advertised in LISP, is redistributed to corresponding Service-VPN SD-WAN control plane (OMP). This ensures control plane separation from one domain to another across the WAN environment.

By default, the WAN Edge device advertise /32 host prefixes from the fabric site LISP database to the SD-WAN OMP routing protocol. This can be modified by adding the overlay client prefixes in the Advertise OMP section of the Cisco VPN templates for each Service-VPN and advertise aggregate only for each virtual network.

Figure 17. Extending Macro-Segmentation – SD-Access VN to SD-WAN Service VPN



Micro-Segmentation Considerations

The WAN Edge device, also the fabric Border, terminates the VXLAN encapsulated packets from the LAN segment fabric nodes. The device copies the scalable group value from the VXLAN header into the IPSec CMD header for traffic destinated to remote-sites connected through the SD-WAN WAN environment.

At the remote-site the WAN Edge device copies the scalable group value form the IPSec CMD header to the VXLAN header before forwarding the traffic to the SD-Access fabric environment. This ensures the micro-segmentation information is carried natively in the data-plane across the domains.

SNMP and Syslog Considerations

SNMP and Syslog statistics on the WAN Edge router and LAN network devices are collected by Cisco DNA Center. It is recommended to leverage Cisco DNA Center, Network Setting > Device Credentials workflow to configure the device credentials, SNMPv2/SNMPv3 and Syslog parameters to the network devices across the enterprise infrastructure.

Network Assurance and Visibility

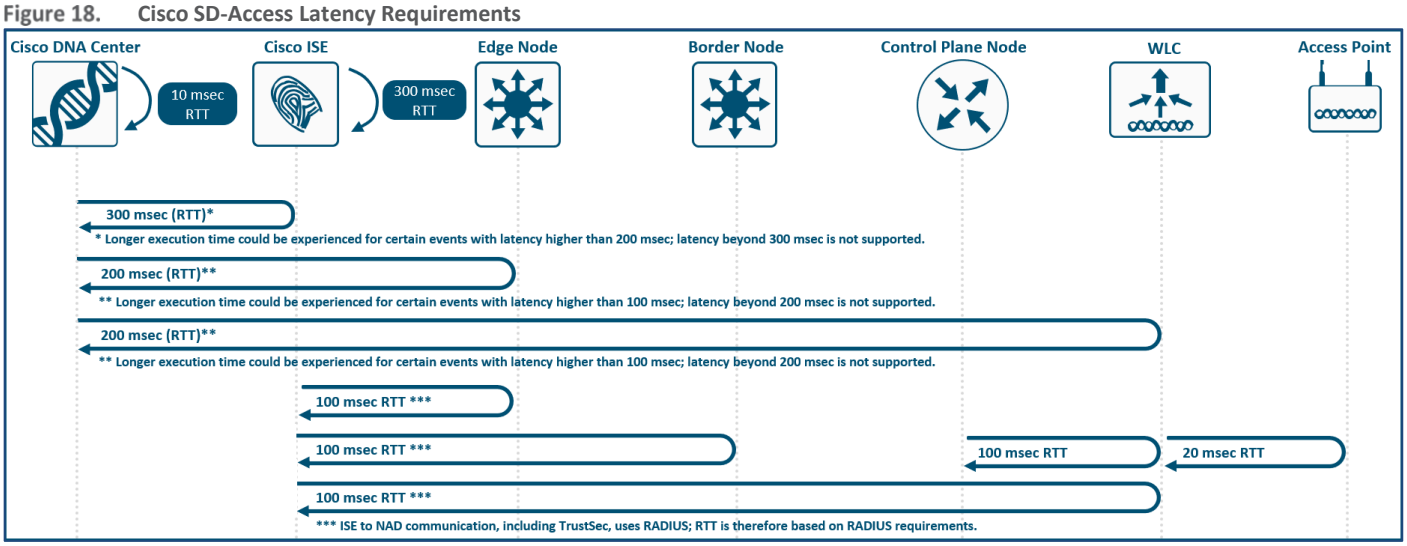
Visibility of SD-WAN WAN Edge device health, WAN transport health and Application statistics across the WAN transports are monitored in the SD-WAN vManage controller. Network Assurance from the fabric nodes are monitored in Cisco DNA Center. In the *Integrated* Domain integration

- SNMP and Syslog statistics for the WAN Edge are destined to Cisco DNA Center.
- Cisco DNA Center provides Site-level Topology, Network health, Network level Issues and Events, Device 360 and Client 360 visibility
- SD-WAN vManage provides WAN Edge device-level visibility into Inventory, Control Status, Site Health, Device Health, Transport Health and Events.

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 200 ms RTT. Latency between 100 ms and 200 ms 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



Platform Requirements

Cisco SD-Access | SD-WAN *Integrated Domain* Integration requires the network device to perform SD-WAN WAN Edge functionality and SD-Access colocated Border and Control Plane functionality.

Tables 1 list the supported hardware devices.

Table 1. Integrated Domain SD-WAN Edge Supported Platforms

Supported Cisco hardware	Additional details
ISR 4331 Series Routers	≥ 8G Memory
ISR 4351Series Routers	≥ 8G Memory
ISR 4400 Series Routers	≥ 8G Memory
ASR 1001-X Series Routers	≥ 8G Memory
ASR 1002-X Series Routers	≥ 8G Memory
ASR 1001-HX Series Routers	≥ 8G Memory
ASR 1002-HX Series Routers	≥ 8G Memory
Cisco Catalyst® 8300 Series Edge Platforms	≥ 8G Memory Cisco DNA Center ≥2.1.2.6 IOS XE ≥17.3.3

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, consult the SD-Access Platform Scale, Appliance Scale, and fabric VN Scale Tables in the Cisco DNA Center data sheet.

Table 2 list the scaling numbers for the WAN Edge platforms that are part of the *Integrated* Domain integration

Table 2. *Integrated* Domain WAN Edge platform scale numbers

Platform	Virtual Networks (VNs)	Max EID per VN	Max EID Entries
ASR Series Routers	10	5,000	50,000
ISR Series Routers	10	1,000	10,000

SD-WAN Edge SGT Forwarding Interoperability

The 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 ≥17.3.2a.

Table 3 shows the interoperability behavior for various WAN Edge platforms and their corresponding software version with respect to carrying SGTs in the data plane.

Table 3. SD-WAN Traffic Forwarding Interoperability

From \ To	≥IOS XE 17.3.x SD-WAN (Cisco TrustSec enabled)	≥IOS XE 17.3.x SD-WAN (Cisco TrustSec not enabled)	<IOS XE 17.2.x SD-WAN	Colocated SD-Access IOS XE WAN Edge	vEdge Router
≥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
≥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

Deployment Limitations

Integrated Domain integrates Cisco SD-Access and SD-WAN solution natively on the same WAN Edge device. This integration model is ideal, but not limited, for remote-branch deployment. The ability to fully automate the WAN and the LAN segment at remote sites, provides business the ability to deploy Zero-Trust Branch site faster, securely and provide consistent user experience.

Below lists the design constrains before considering the *Integrated* Domain deployment approach:

- Cisco SD-WAN WAN fabric infrastructure is built first followed by SD-Access network.
- Cisco IOS-XE WAN Edge device must be in vManage mode.
- Cisco SD-Access Border and Control Plane functions must be colocated on the IOS-XE SD-WAN WAN Edge router.
- A maximum of 2x colocated SD-Access | IOS XE WAN Edge devices are supported per SD-Access fabric site.
- Cisco SD-Access Border node should be configured as External-Only node.
- Group-Based policy enforcement is not supported on the IOS-XE WAN Edge devices.

- The following features are not supported on the colocated SD-Access | IOS-XE WAN Edge device:
    - Multicast
    - IPv6
    - Layer 2 Flooding
    - Layer 2 Border Handoff
    - SD-Access Transit
    - MultiSite Remote Border

Deploy

This chapter is organized into the following sections:

Chapter	Section
Deploy	Deployment Topology Overview Deployment Prerequisites Deployment Steps

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

Deployment Topology Overview

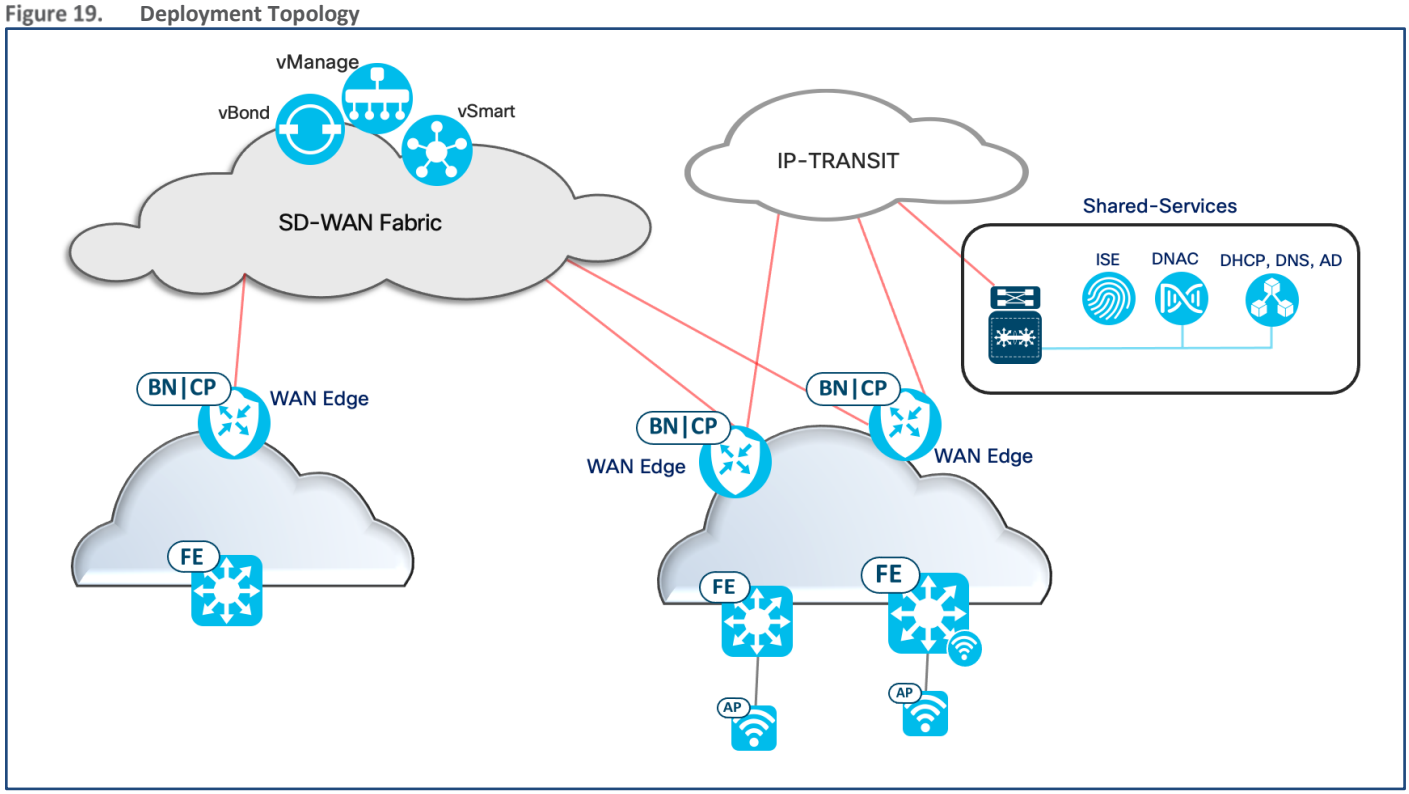
The validation topology has two SD-Access fabric sites connected via a Cisco SD-WAN fabric, representing multiple locations. The Cisco SD-WAN controllers are deployed in the enterprise private cloud. The WAN Edge routers are connected to SD-WAN fabric across public-internet and MPLS WAN transports.

At branch site, the single WAN Edge device part of the *Integrated* Domain deployment is directly connected to fabric Edge and to WAN transports.

At the headend location, the two WAN Edge devices are connected to fabric Edge devices, WAN transports and also the IP-Transit for reachability to shared-services network. At this site, embedded-wireless on Catalyst 9000 is deployed.

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 IP-Transit.

Figure 19. 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.
- 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 (optional).

Deployment Steps

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

Process	Procedure
Verifying Prerequisites for *Integrated* Domain	Verify the SD-WAN infrastructure Verify the WAN Edge secure data plane connections Verify Cisco DNA Center is installed with SD-Access Application Verify Cisco DNA Center is integrated with ISE Verify Cisco DNA Center design application configuration
Associating IOS-XE WAN Edge device with Service VPN	Configuring Service VPN Configuring ethernet interface for loopback 0 Associate VPN and ethernet template to the WAN Edge device
Integrating the domain controllers	Integrating vManage in Cisco DNA Center Associating IOS-XE WAN Edge devices to participate in the *Integrated*-Domain integration Provision the IOS-XE WAN Edge devices to participate in the *Integrated*-Domain integration Mapping Service VPN to Virtual Network in Cisco DNA Center Associate Scalable Groups to Virtual Networks
Configuring LAN Segment manually	Creating Interface template connecting to the LAN segment Configuring routing protocol template to form LAN segment routing adjacencies Associating interface, routing protocol templates on the IOS-XE WAN Edge device Discover and Provision the network devices to a site
Configuring LAN Segment with LAN Automation	Initiate LAN automation
Provision Cisco SD-Access Fabric Site(s)	Provision the network devices to a site (Optional) Provision IP - Transit Network Provision Fabric – Create Fabric Site Provision Fabric – Configure Host Onboarding Configure WAN Edge to advertise aggregate-summary routes for associated IP Address Pool (Optional) Provision Fabric – Port Assignment
Defining Group-Based Access Control Policies	Configure Group-Based Access Control policies

Process 1: Verifying Prerequisites for *Integrated* Domain

Before beginning the *Integrated* Domain deployment, the SD-WAN and SD-Access controllers must be deployed.

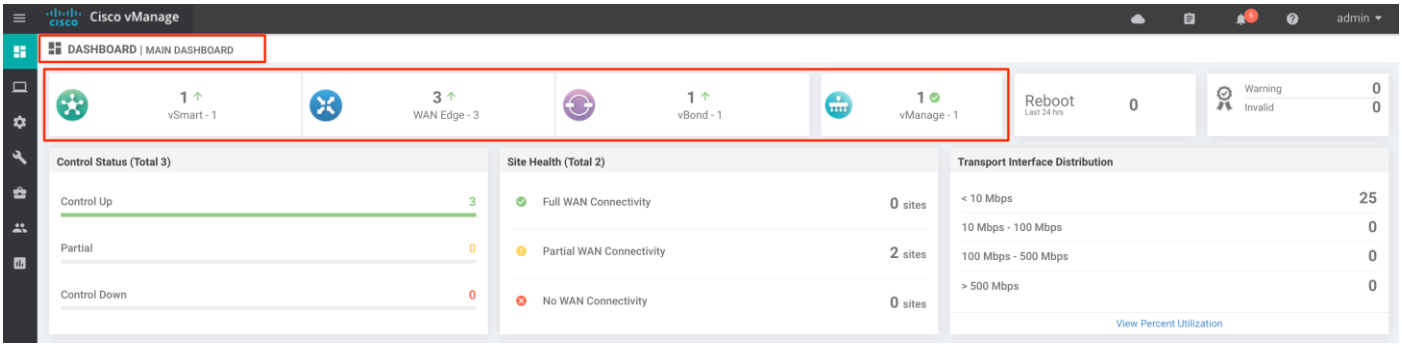
Procedure 1. Verify the SD-WAN infrastructure

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

Step 1. Log in to vManage and navigate to **Dashboard > Main Dashboard**.

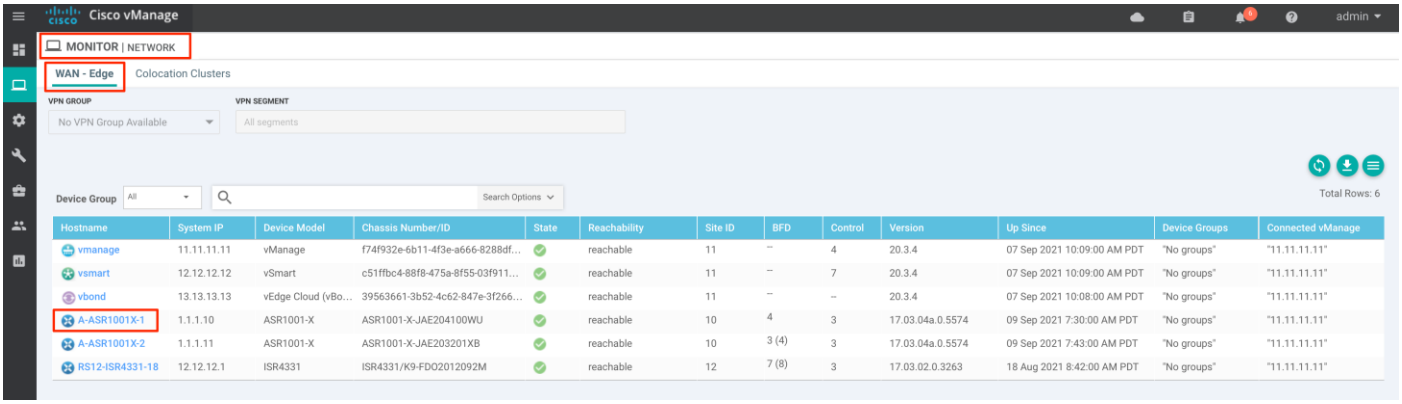
Step 2. Verify the state of vManage, vBond, vSmart, and the WAN Edge devices.

The ↑ green up arrow indicates a healthy, onboarded state.



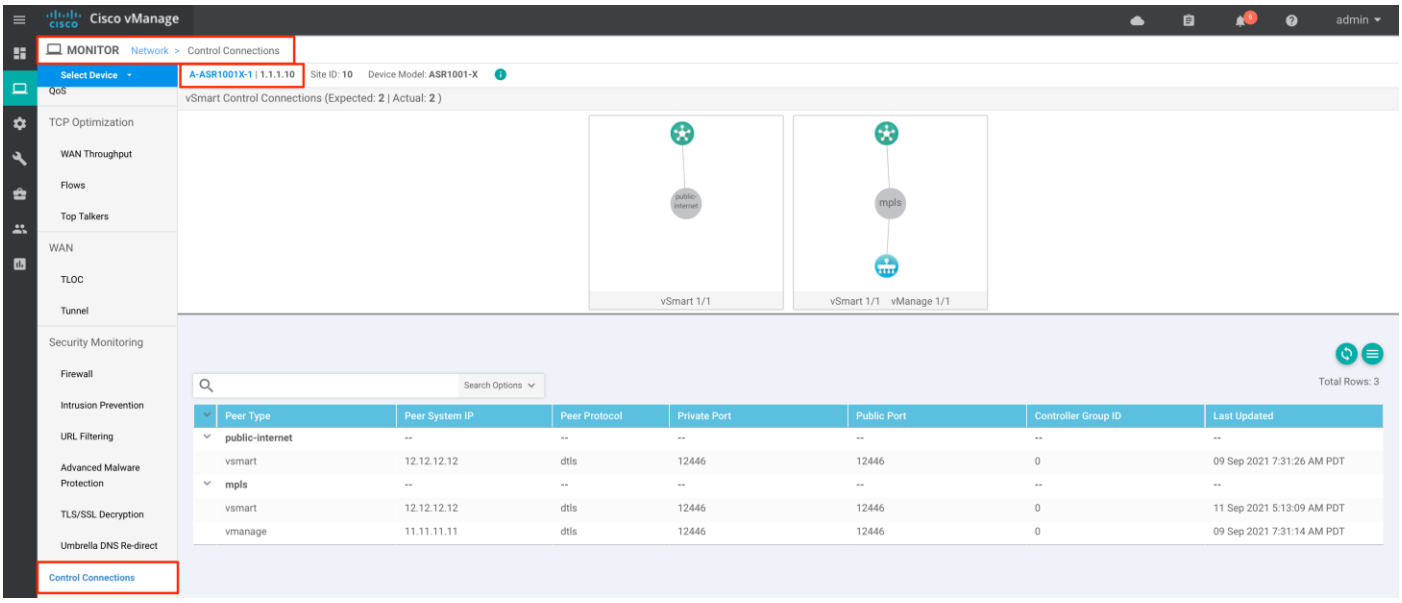
Step 3. In vManage, navigate to **Monitor > Network**.

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



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

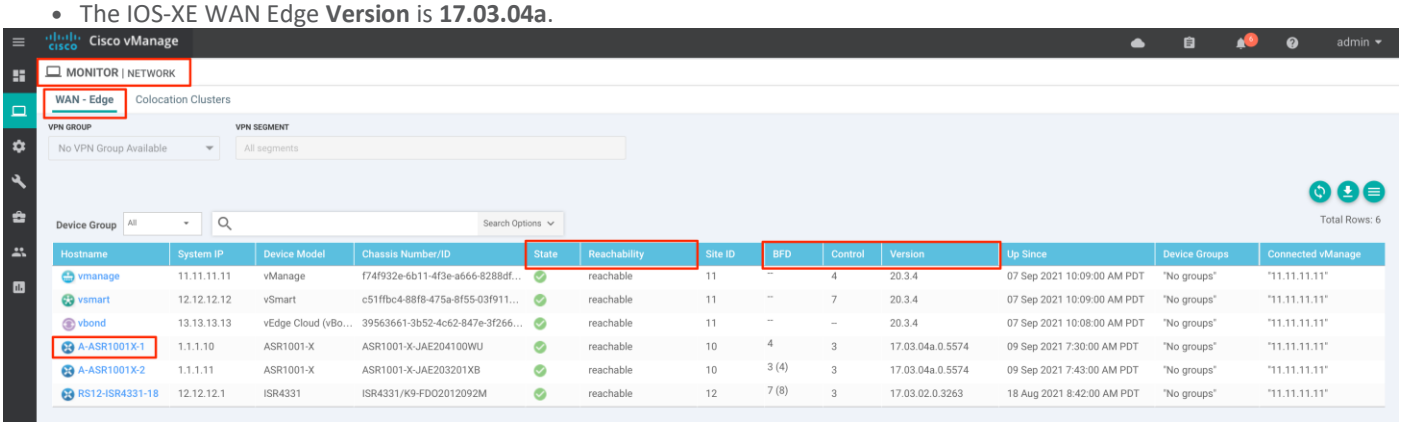
Verify the DTLS sessions are established with the SD-WAN controllers across the available WAN transport connections.



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 IOS-XE WAN Edge **Version** is **17.03.04a**.



Procedure 2. Verify the WAN Edge secure data plane connections

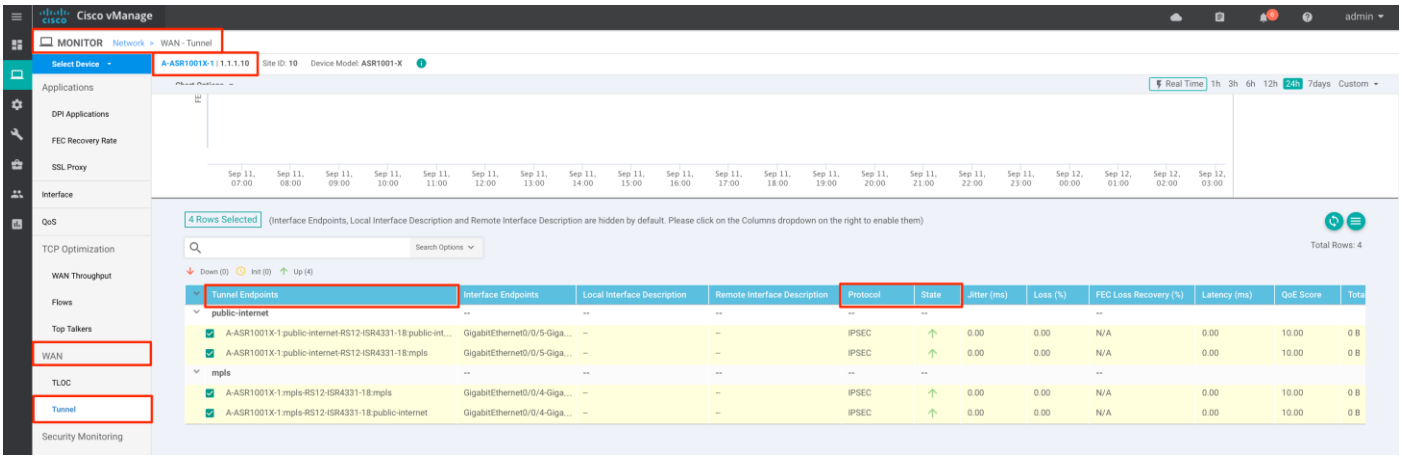
Step 1. In vManage, navigate to **Monitor > Network**.

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**.

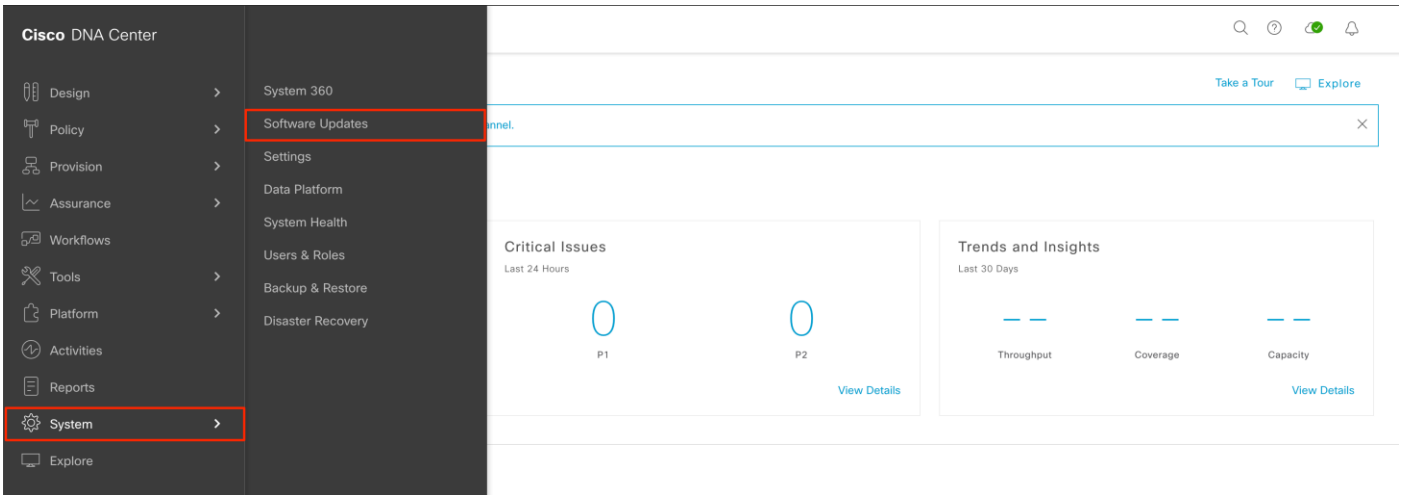


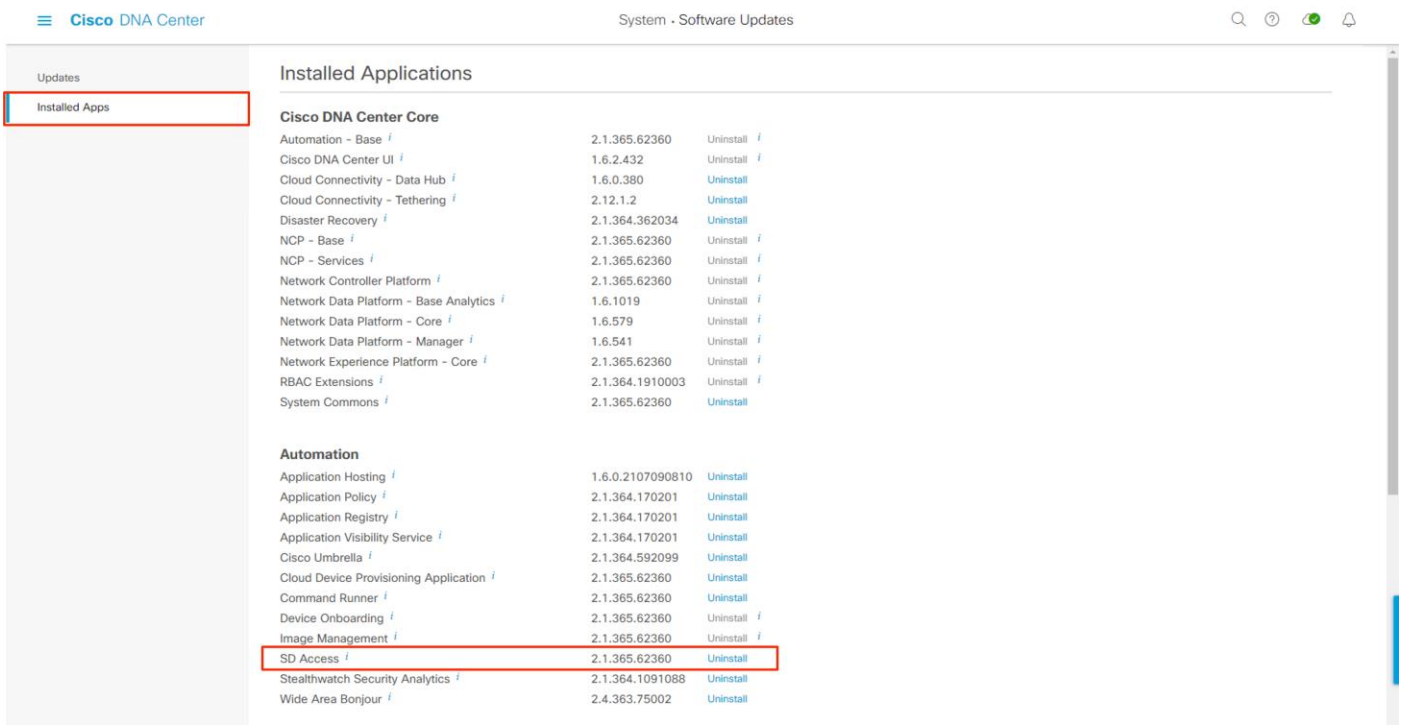
Procedure 3. Verify Cisco DNA Center is installed with the SD-Access application

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.



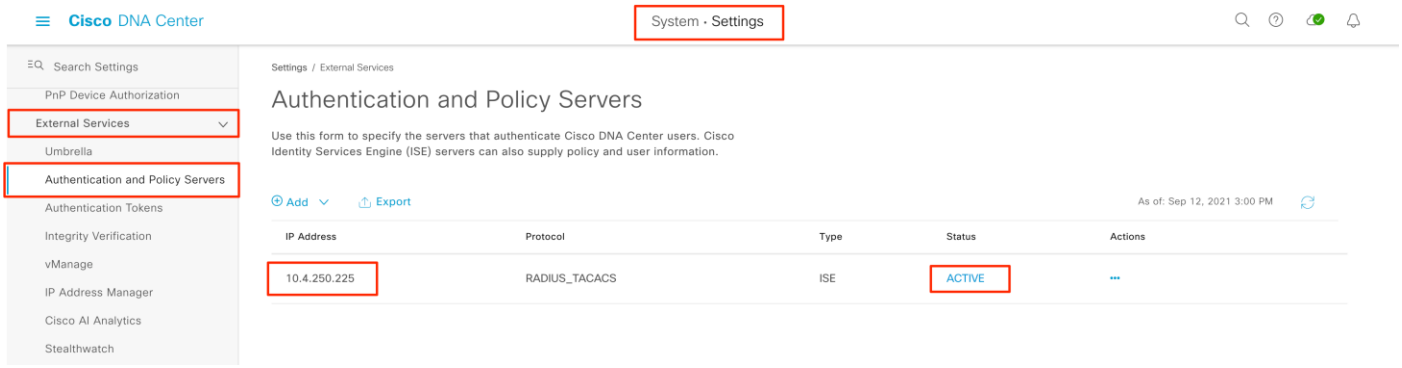


Procedure 4. Verify Cisco DNA Center is integrated with the Identity Services Engine

Step 1. In Cisco DNA Center, navigate to **System > Settings**.

Step 2. Under **External Services,** select **Authentication and Policy Servers** from the left panel.

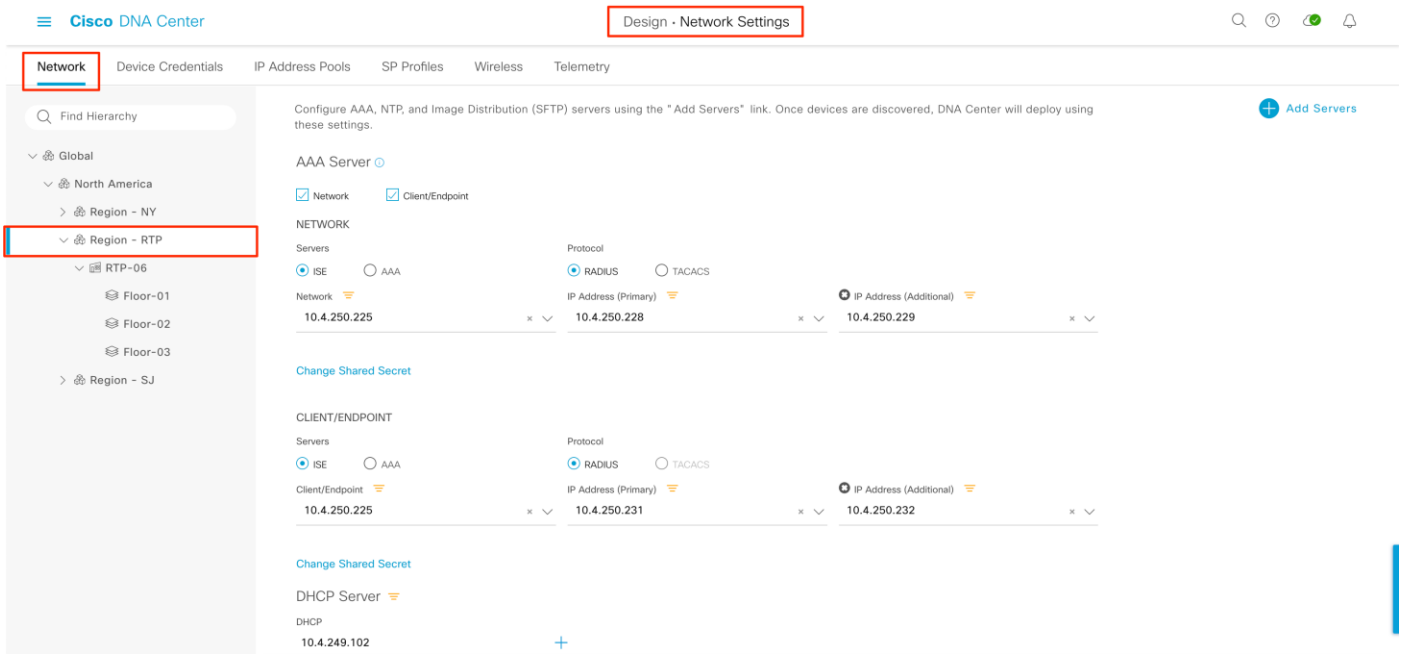
Step 3. Verify the ISE server is integrated and in **ACTIVE** state.



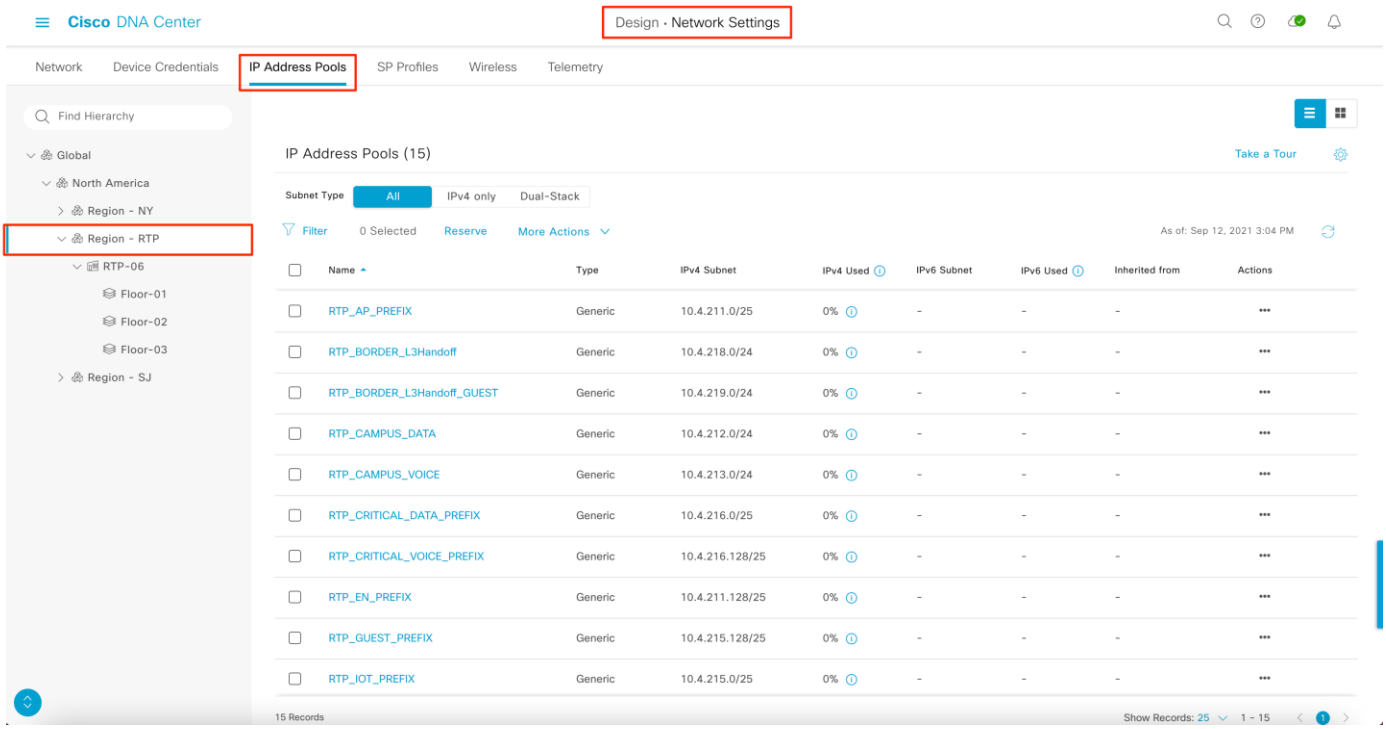
Procedure 5. Verify Cisco DNA Center design application configuration

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.

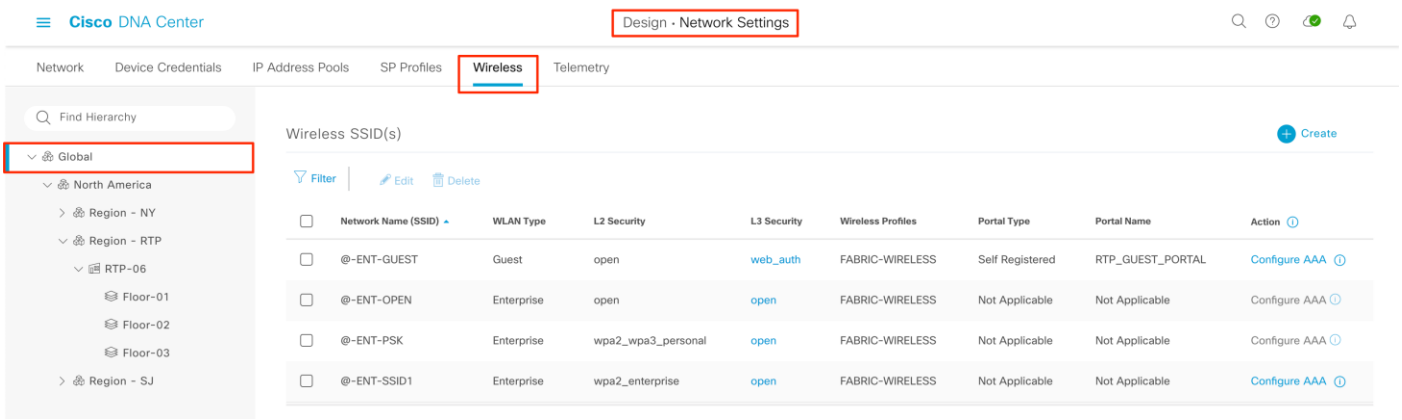


Step 3. Under **IP Address Pools** tab, make sure IP address are reserved appropriately for the site hierarchy.



Step 4. (Optional) Under the **Wireless** tab, select **Global** in the hierarchy.

Confirm the wireless Network SSID is configured and associated with Wireless Profile.



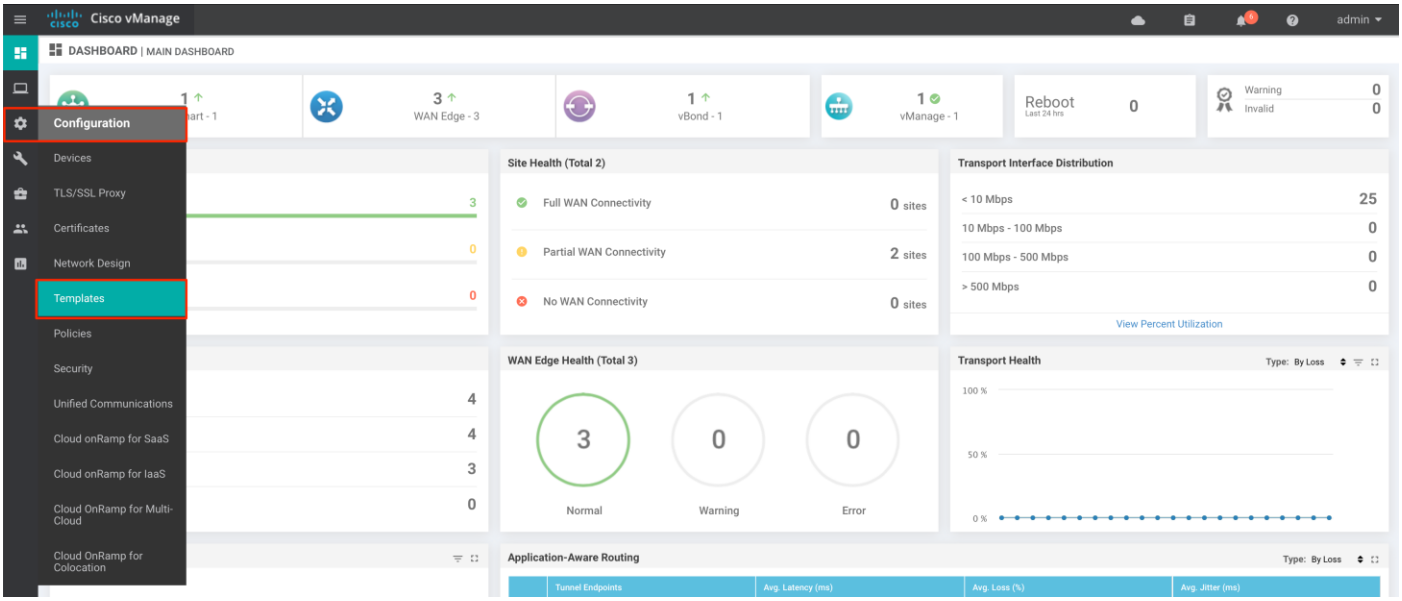
Process 2: Associate IOS-XE WAN Edge device with Service VPN

This section details the procedure to create service VPN templates and loopback 0 interface to the IOS-XE WAN Edge devices.

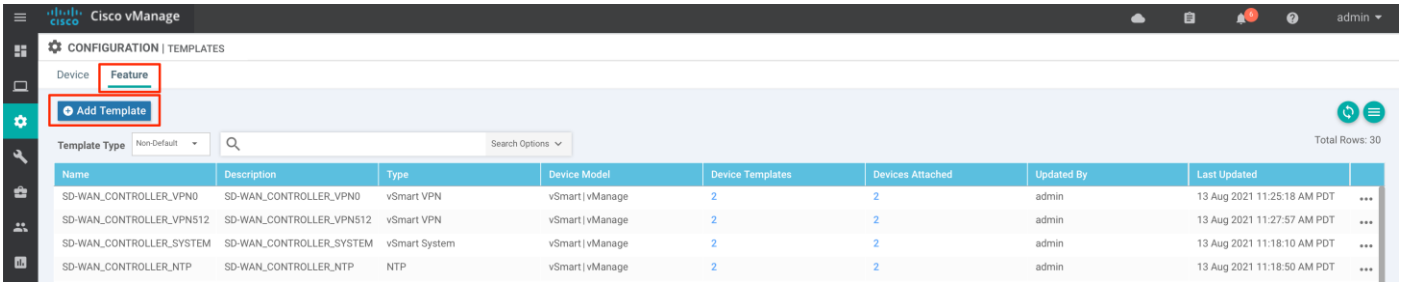
Procedure 1. Configuring Service VPN

In this procedure, lets create Service VPN – one dedicated for undelay reachability and others for multiple overlay networks.

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

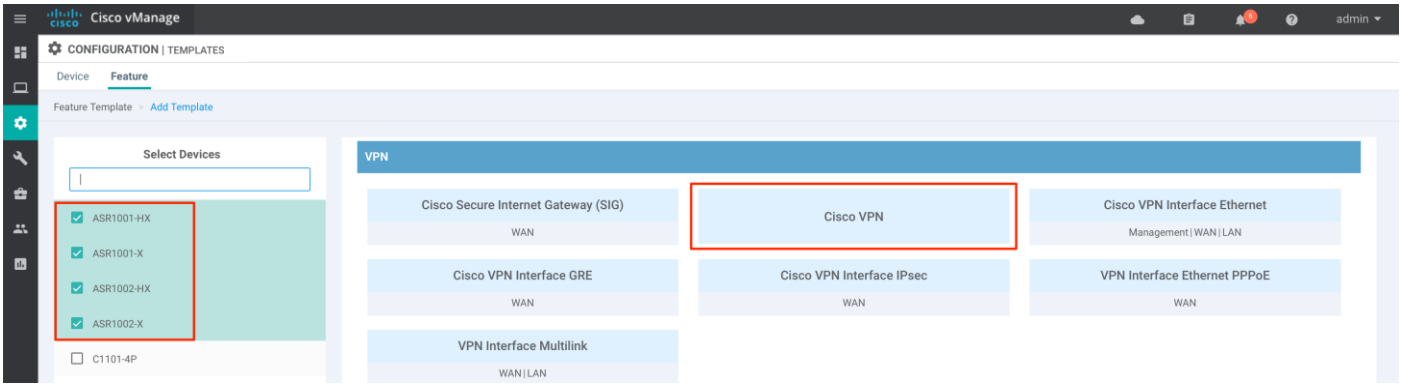


Step 2. Select **Feature** tab and select **Add Template**



Step 3. Choose all the WAN Edge devices.

under **VPN,** choose **Cisco VPN** template



Step 4. Input **Template Name**, **Description** for the template

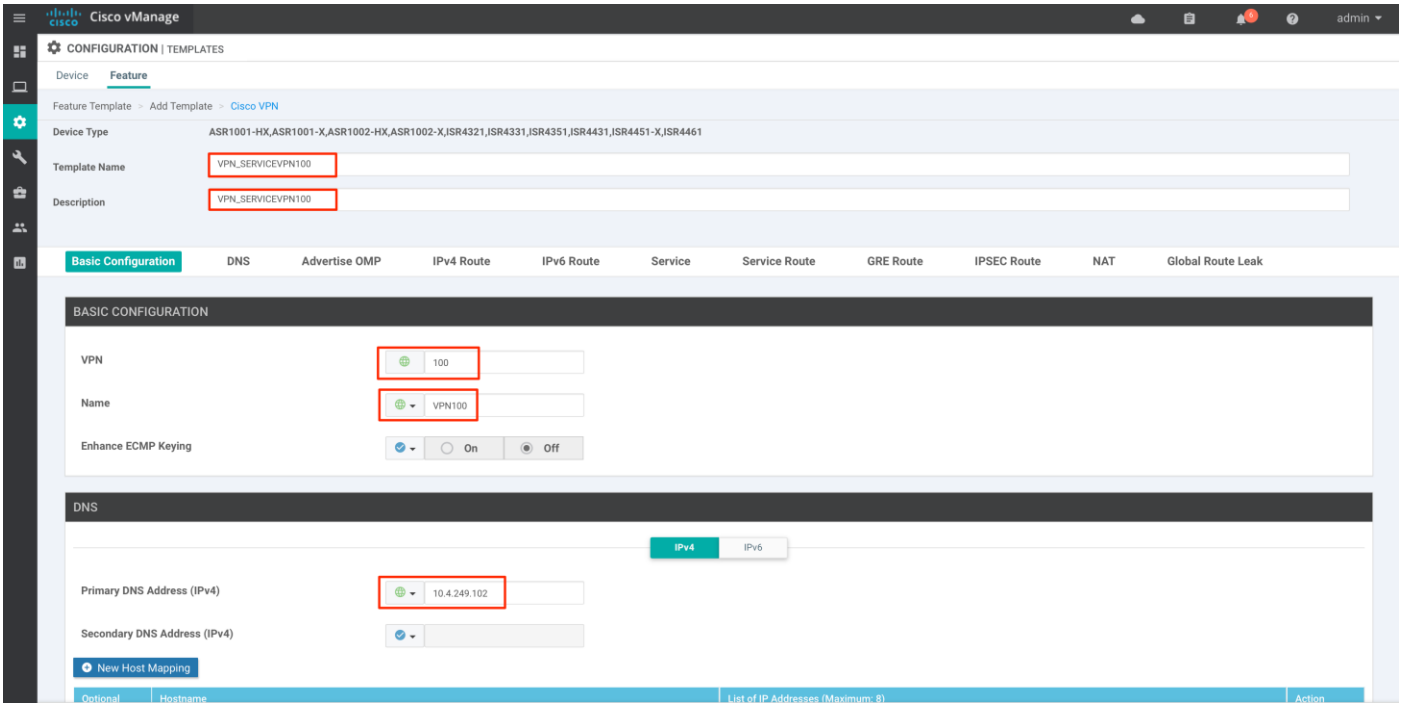
Under **Basic Configuration**, input **VPN**, **Name**

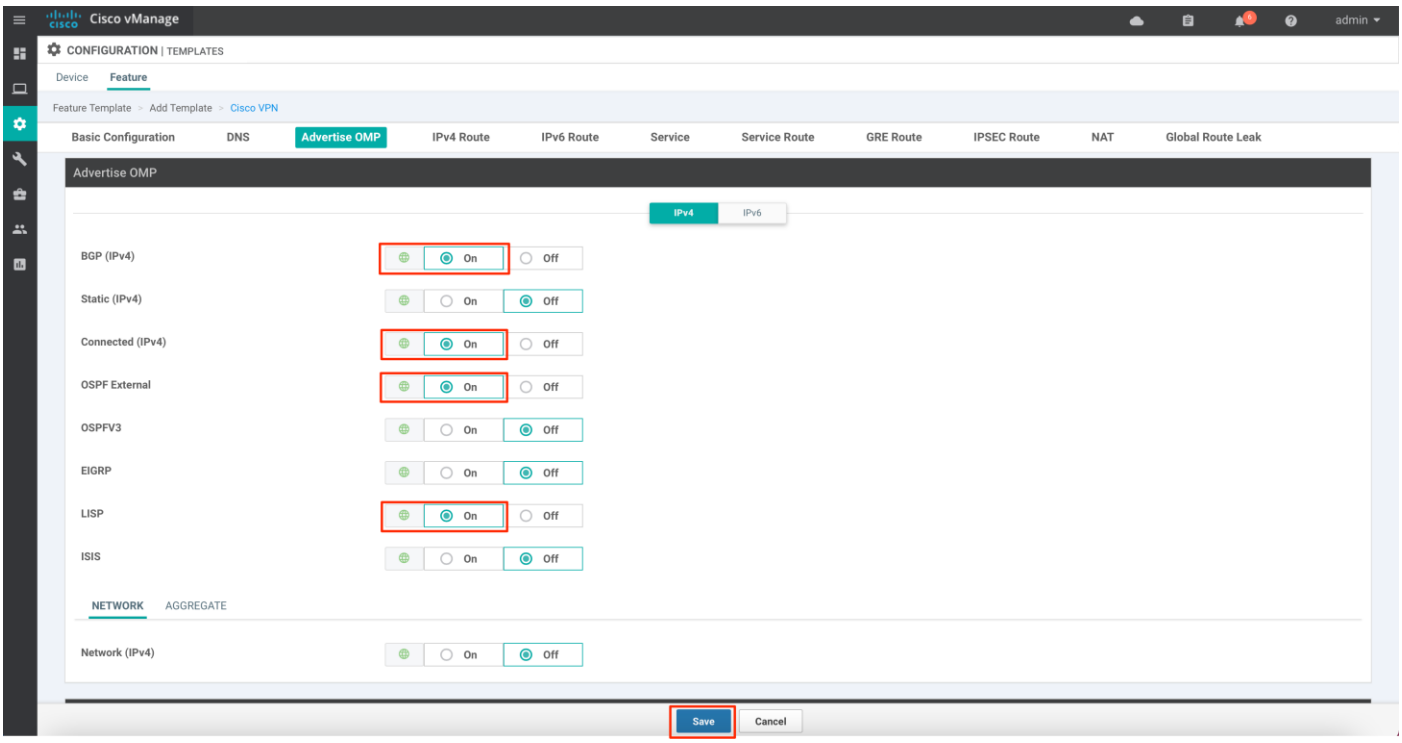
Under **DNS**, input **Primary DNS (IPv4)**

Under **Advertise OMP**, Enable **BGP (IPv4), Connected, OSPF External, LISP**

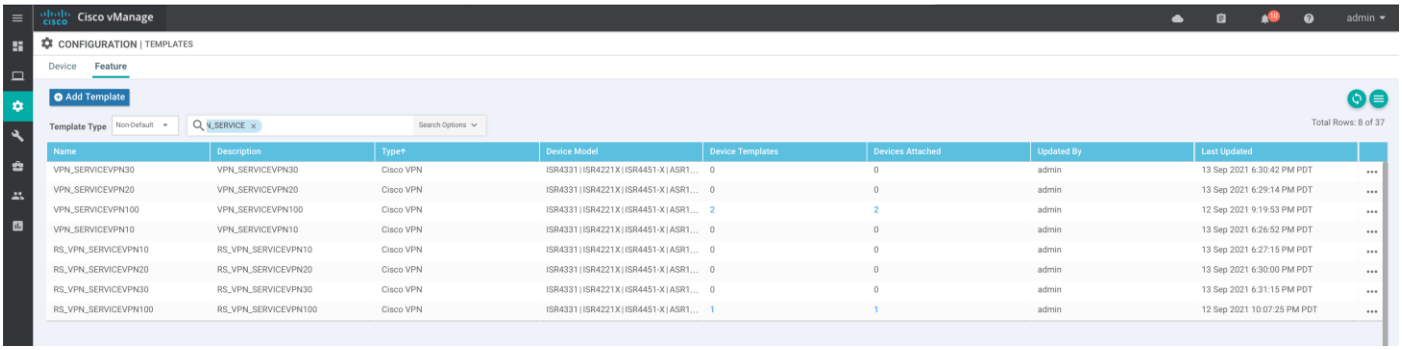
Tech tip
For sites connected to shared services in traditional IP network: • Enable BGP to be advertised in OMP ensuring remote-sites WAN Edge devices can reach the shared-services. • Enable LISP to be advertised in OMP to share the SD-Access INFRA_VN prefixes for Access Point, Extended/Policy-Extended nodes. • Enable Fabric GRT routing protocol (EIBGP/OSPF/ISIS) to be advertised in OMP to provide end-to-end reachability across all sites. • Enable Connected to be advertised in OMP For sites connected to SD-WAN Transit only: • Enable LISP to be advertised in OMP to share the SD-Access INFRA_VN prefixes for Access Point, Extended/Policy-Extended nodes. • Enable Fabric GRT routing protocol (EIBGP/OSPF/ISIS) to be advertised in OMP to provide end-to-end reachability across all sites. • Enable Connected to be advertised in OMP

Click **Save**





Step 5. Repeat steps in this Procedure to create additional Service VPN as needed



Tech tip
Each Virtual Network in Cisco SD-Access network should have a corresponding Service VPN in the SD-WAN environment.

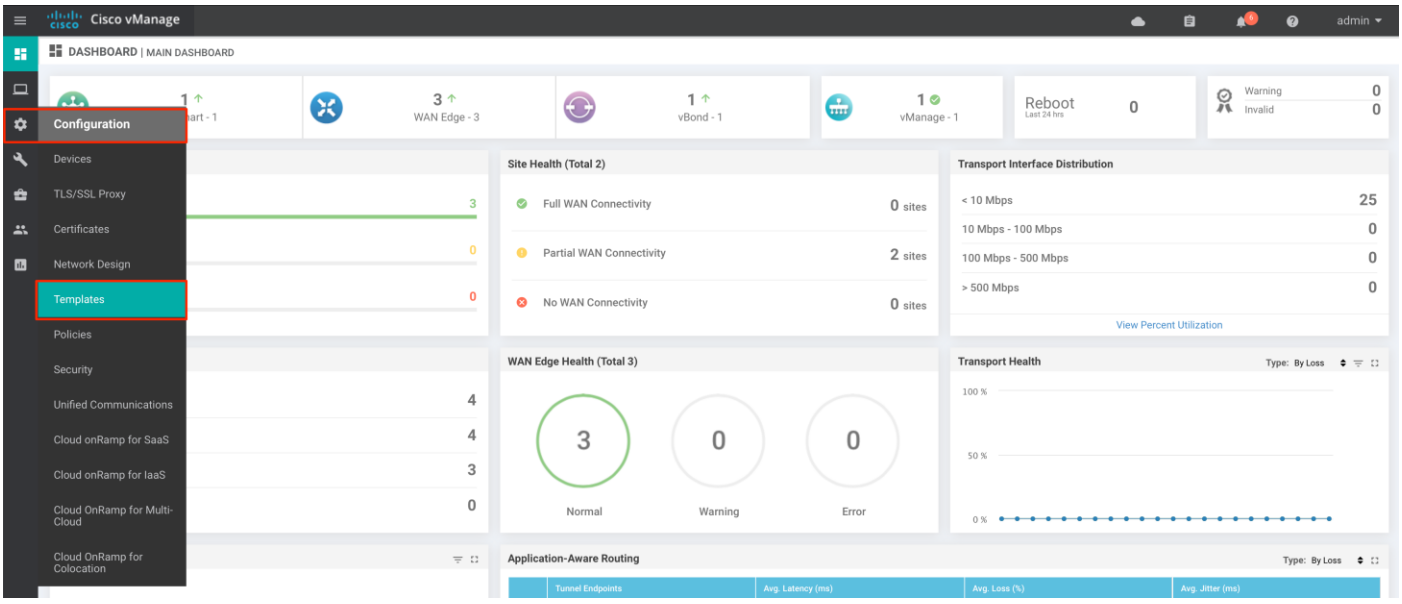
Procedure 2. Configuring ethernet interface for loopback 0

In this procedure, lets create Cisco VPN Interface Ethernet for interface loopback 0. This procedure is needed only when building the Fabric GRT manually.

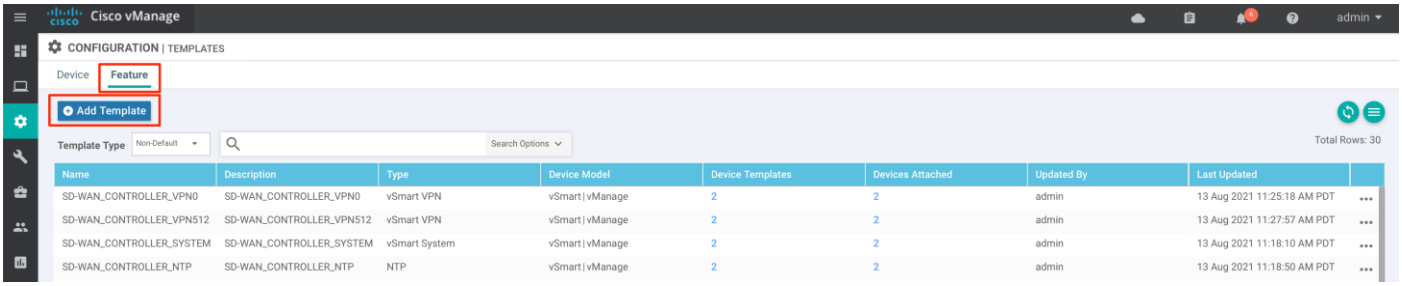
Skip the Procedure 2 and proceed to Procedure 3 if the deployment will leverage LAN Automation workflow to discover and provision the Fabric GRT network devices. As a part of the LAN Automation workflow, Cisco DNA Center will provision loopback 0 interface on the WAN Edge device.

Tech tip
Each Virtual Network in Cisco SD-Access network should have a corresponding Service VPN in the SD-WAN environment.

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

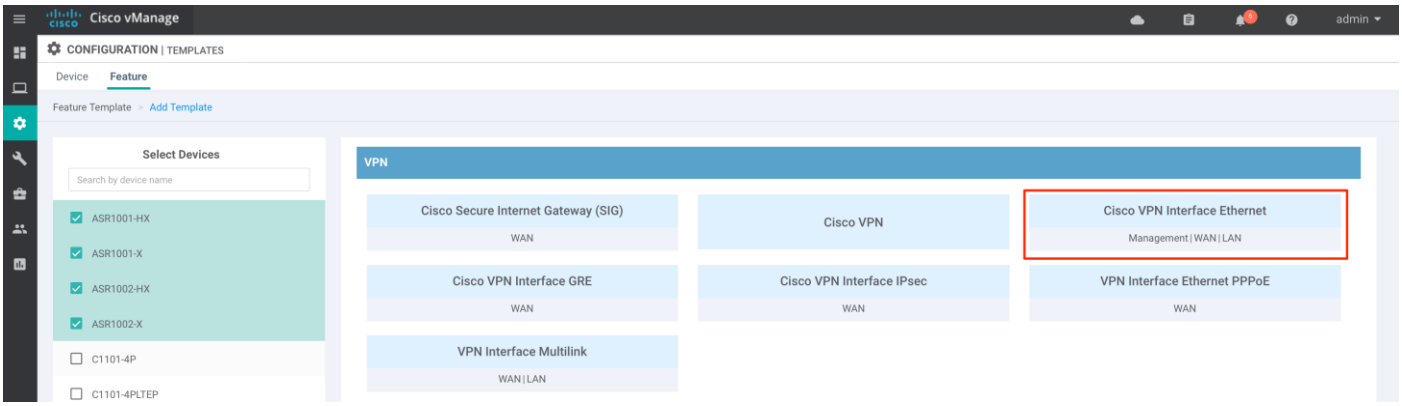


Step 2. Select **Feature** tab and select **Add Template**



Step 3. Choose all the WAN Edge devices.

under **VPN,** choose **Cisco VPN Interface Ethernet** template



Step 4. Input **Template Name**, **Description** for the template

Under **Basic Configuration**,

Shutdown, enable **No**

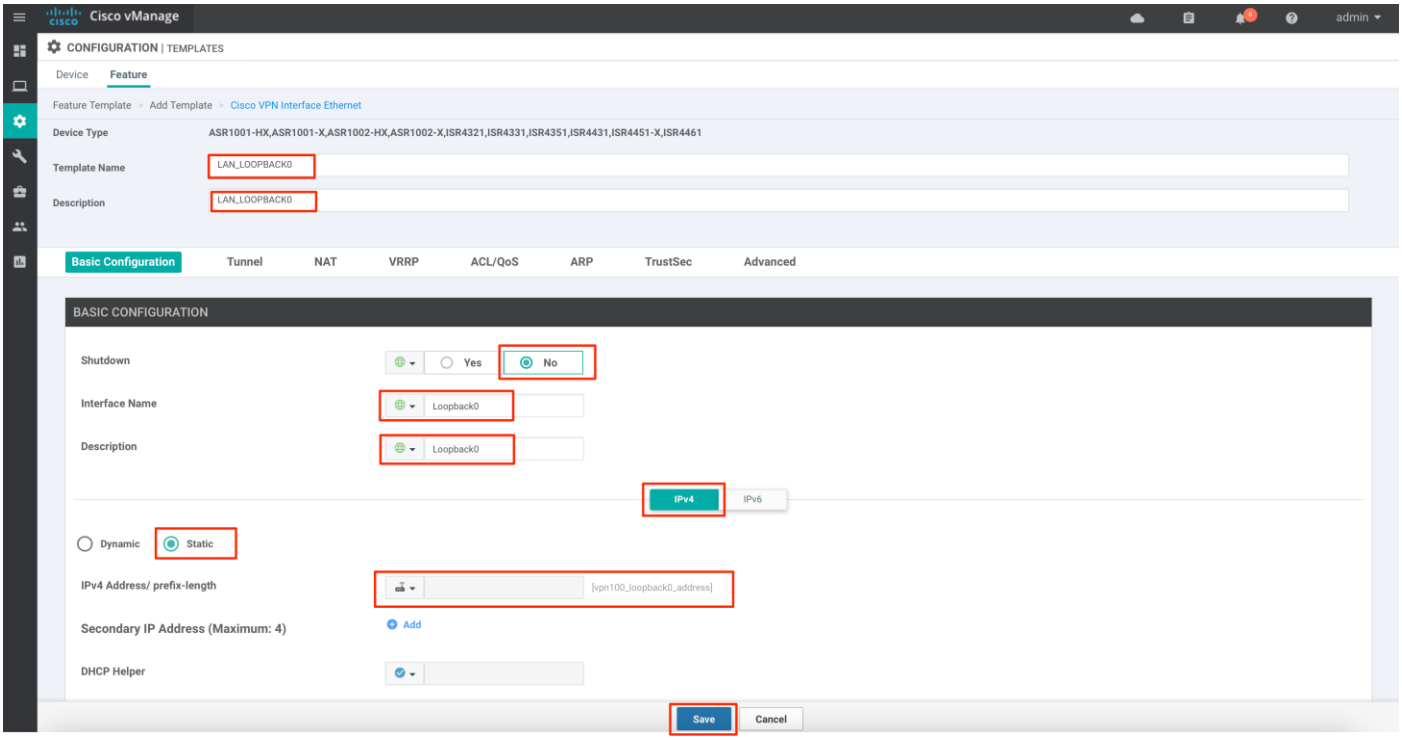
Input **Interface Name** - **Loopback0**

Input **Description** - **Loopback0**

Under **IPv4**, select **Static** option

Under **IPv4 Address / prefix-length**, create **Device Specific** variable '**vpn100_loopback0_address**'

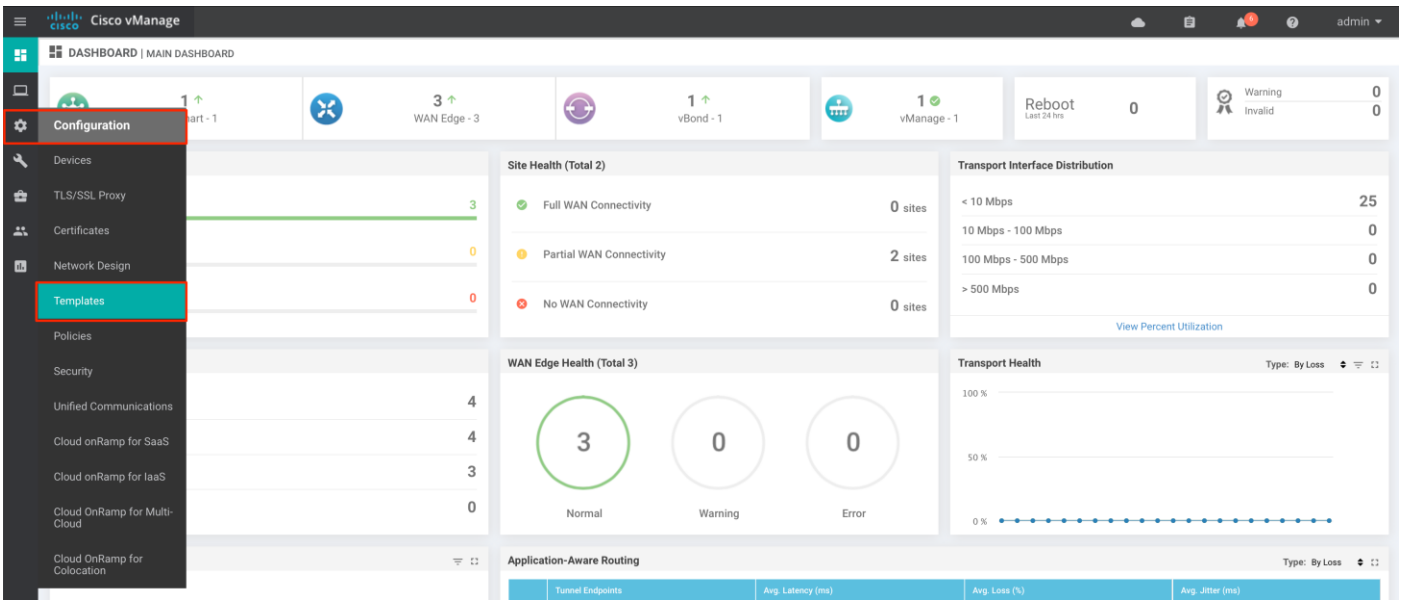
Click **Save**



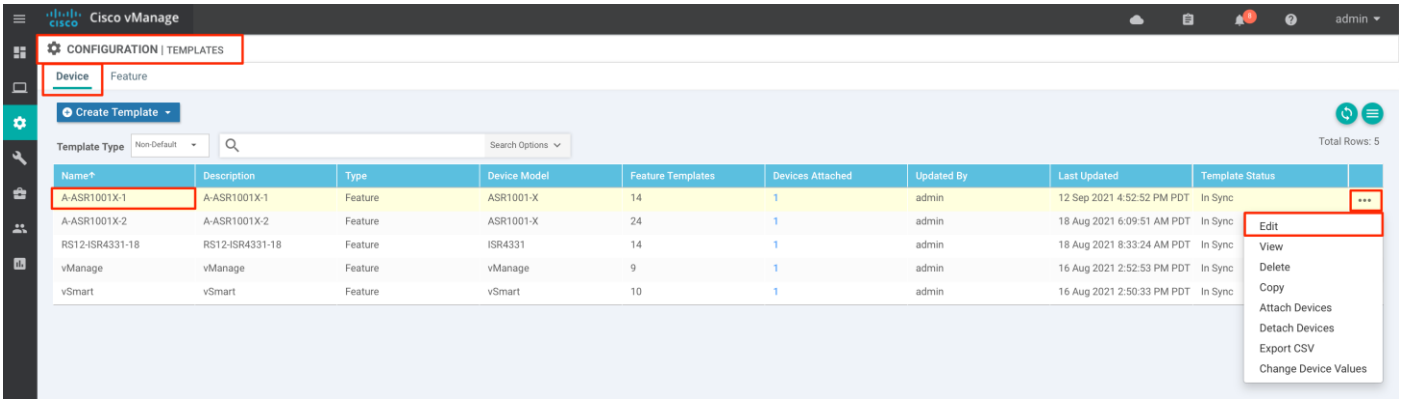
Procedure 3. Associate VPN and ethernet template to the WAN Edge device

This section details the procedure to associate cisco VPN and ethernet interface templates to the WAN Edge devices with the intent to provide end-to-end Fabric GRT reachability across the sites.

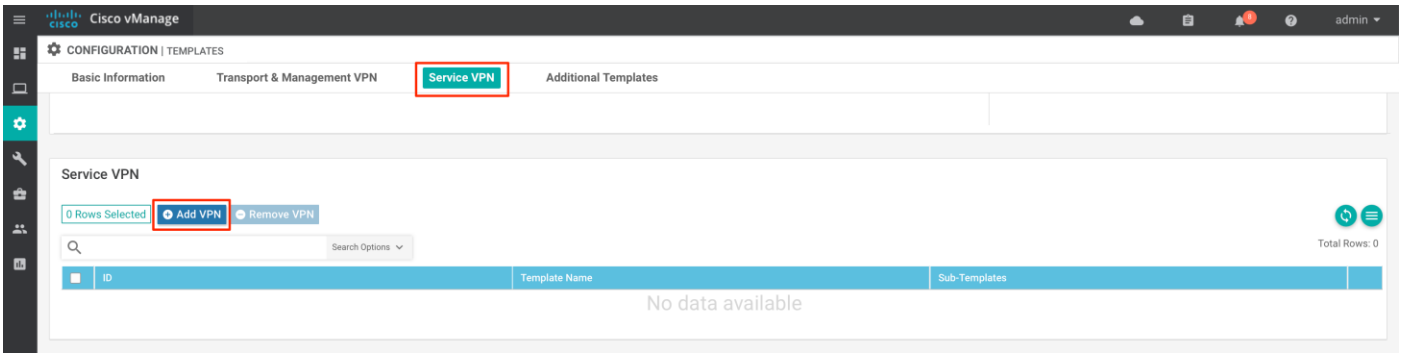
Step 1. Login into vManage, navigate to **Configuration** > **Templates**



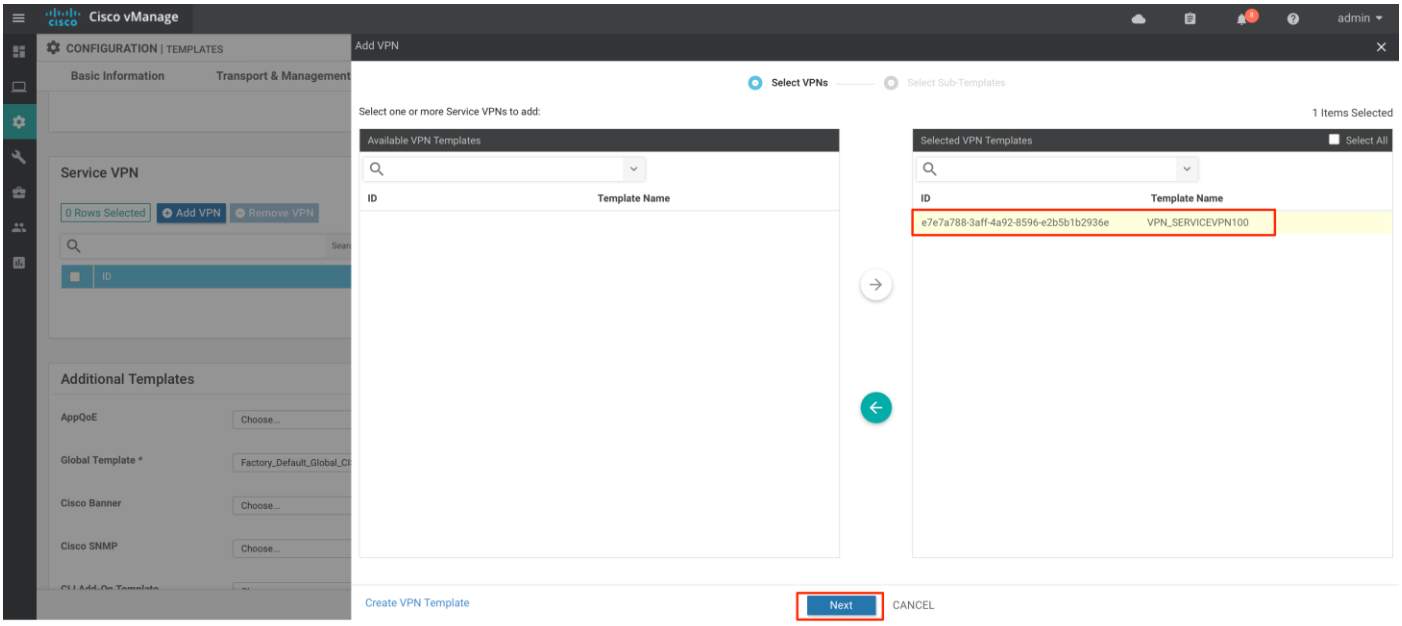
Step 2. Select the WAN Edge device from the list, click the three dots (**…**), and select **Edit** from the drop-down list.



Step 3. Select **Service VPN,** click **Add VPN**



Step 4. Select previously created Fabric GRT Service VPN, 'VPN_SERVICEVPN100' and move from **Available VPN Templates** to **Selected VPN Templates**. Click Next



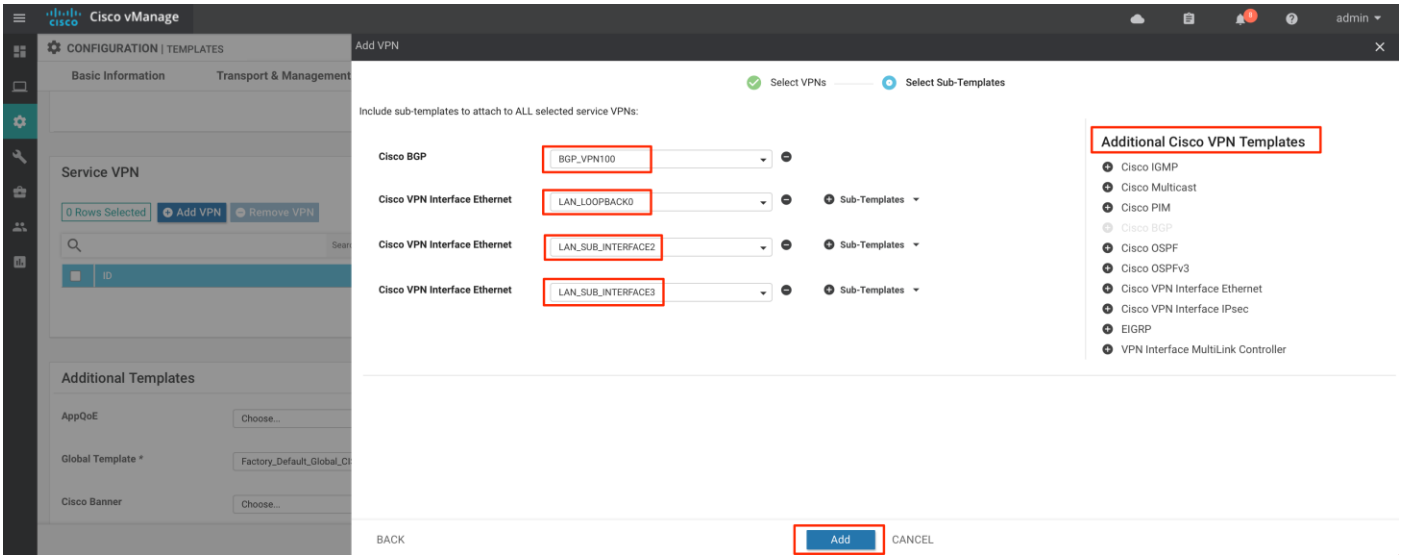
Step 5. This is required for deployments building manual Fabric GRT at the site.

Deployments using LAN Automation workflow to discover and provision Fabric GRT LAN segment, skip this step (Step 5) and proceed to next step (Step 6).

Select **Additional Cisco VPN Templates > Cisco VPN Interface Ethernet**.

Choose previously created ‘LAN_LOOPBACK0’ interface template and any additional interface to provide Fabric GRT connectivity.

Click **Add**

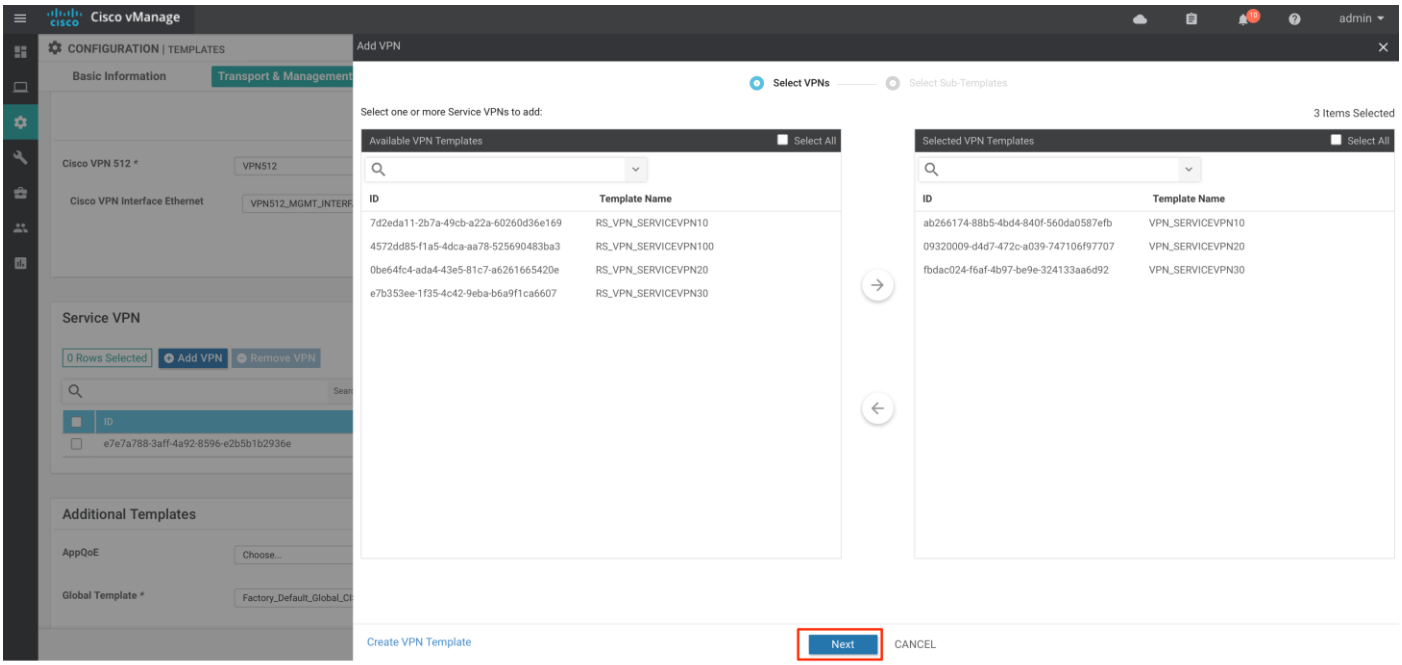


Step 6. Add additional Service VPN created.

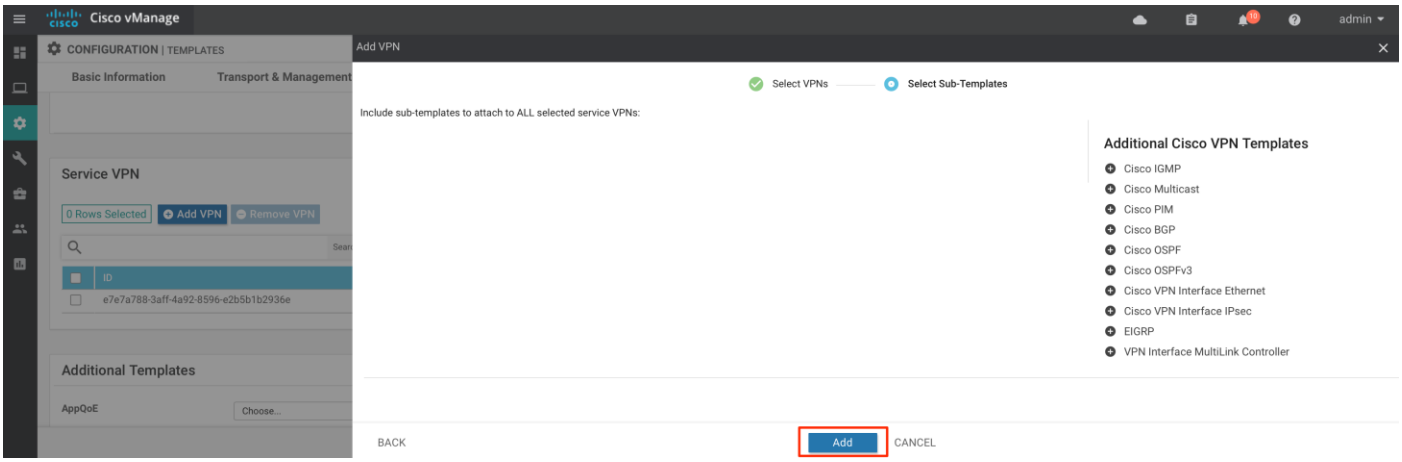
click **Add VPN**,

select VPNs and move from **Available VPN Templates to Selected VPN Templates**

click **Next**

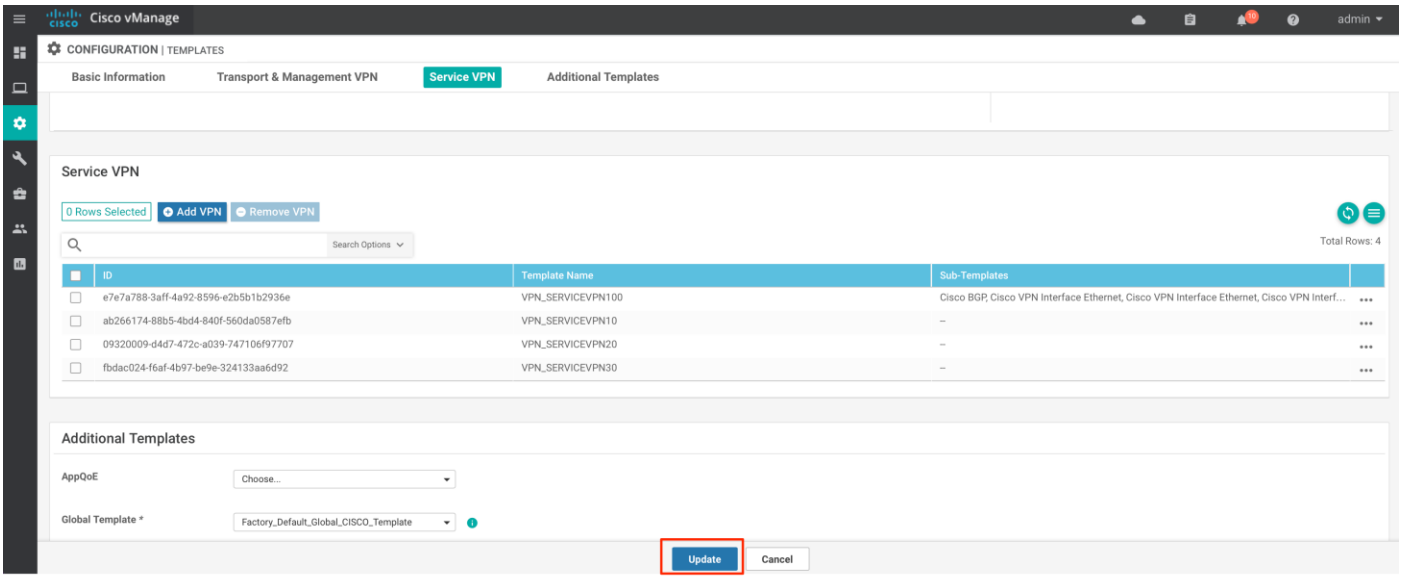


and Click **Add**

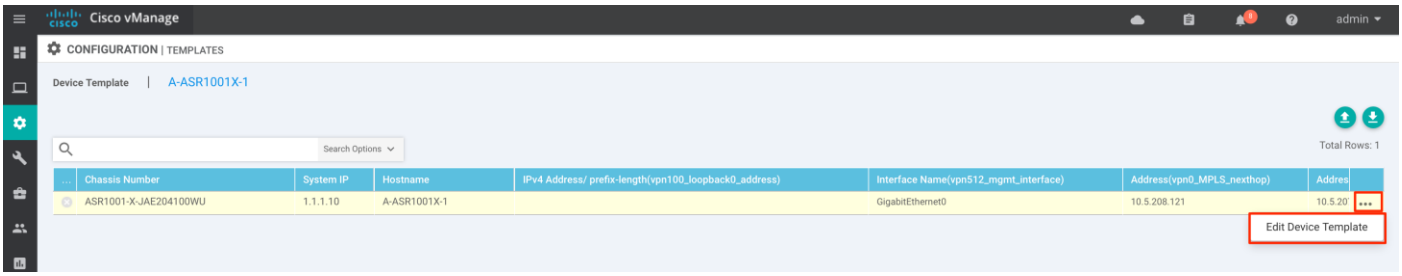


Tech tip
Associating Service VPN to the WAN Edge devices ensures these VPNs are shared with Cisco DNA Center, when the WAN Edge device is added part of the *Integrated* Domain deployment.

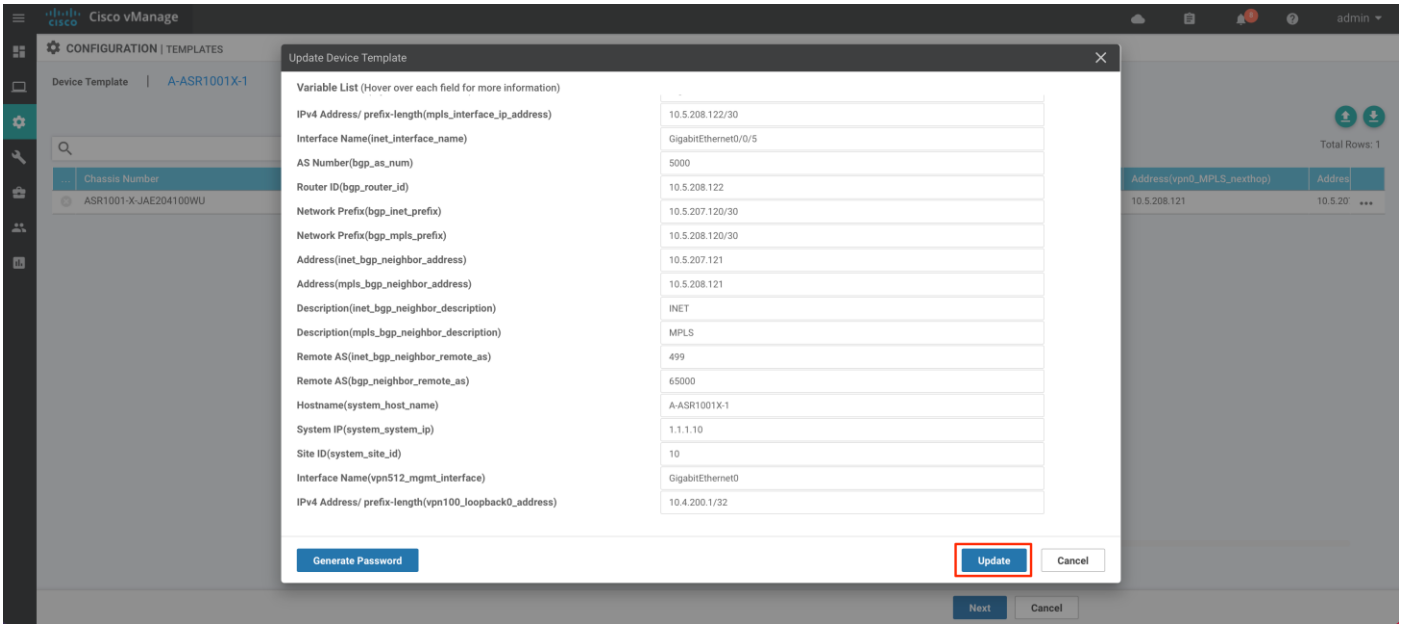
Step 7. Click **Update**

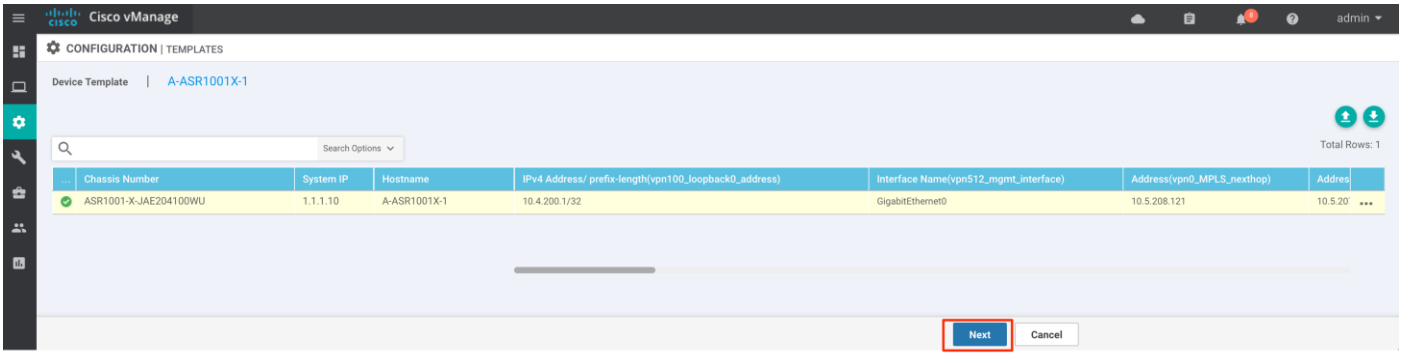


Step 8. click the three dots (**...**), select **Edit Device Template** from the drop-down list,



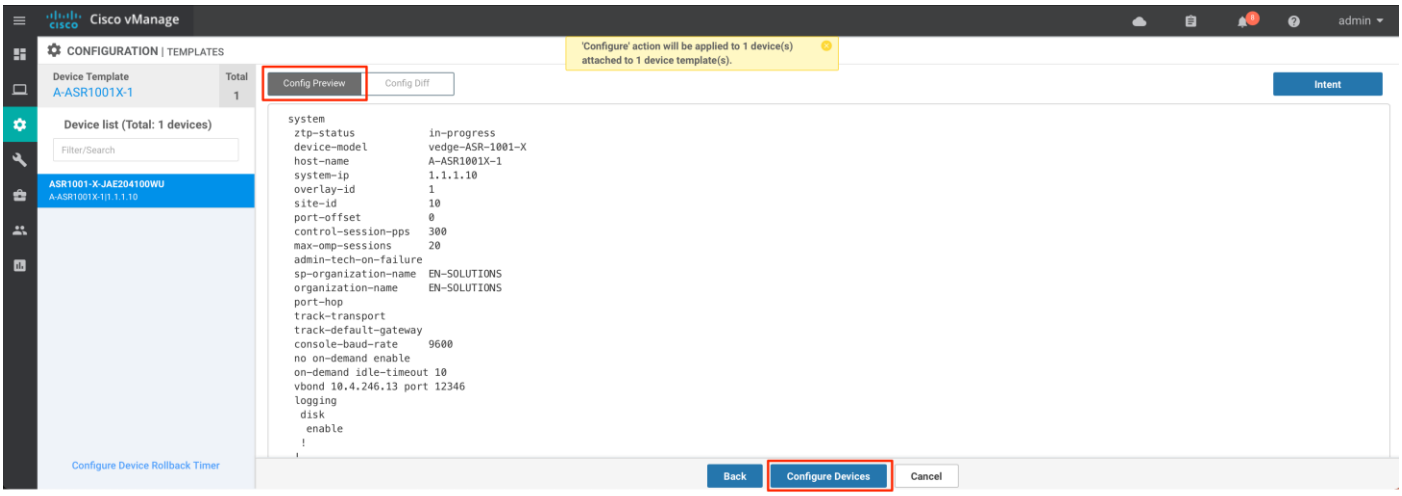
input Device-Specific variables and click **Update** and **Next**.

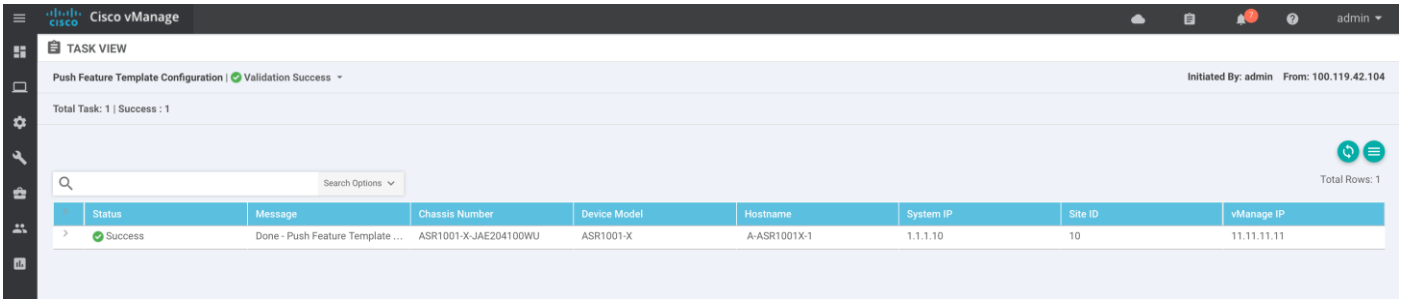




Click **Config Preview** to view the configuration being provisioned to WAN Edge device.

Click **Configure Devices**

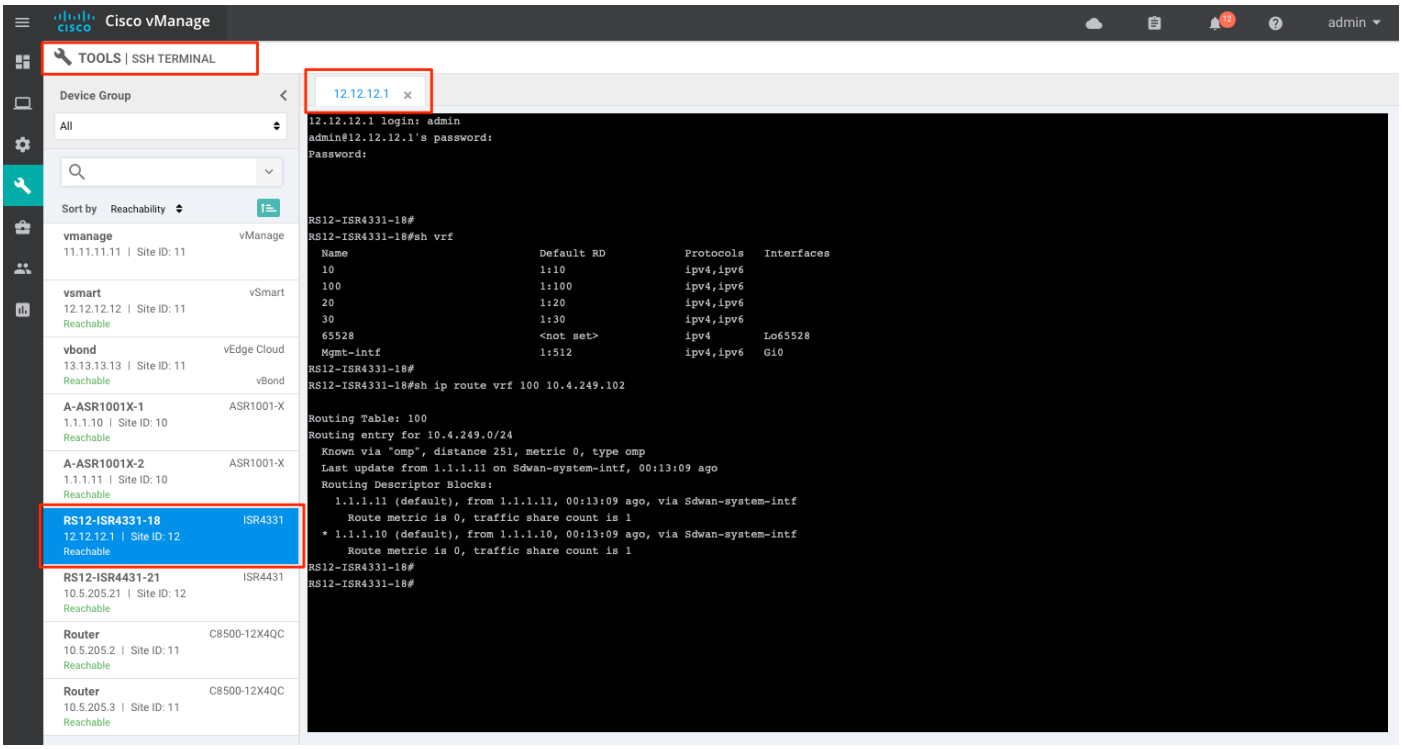




Step 9. Return to the Step1 of the Procedure and repeat for each WAN Edge device in the SD-WAN fabric.

Step 10. Verify the WAN Edge device have reachability to Cisco DNA Center from loopback 0 interface.

In vManage, navigate to **Tools > SSH Terminal**, select the **WAN Edge device** from the list. Login with the device credentials and execute the command '**show vrf**' and '**show ip route vrf 100 <DNA Center ip-address>**'



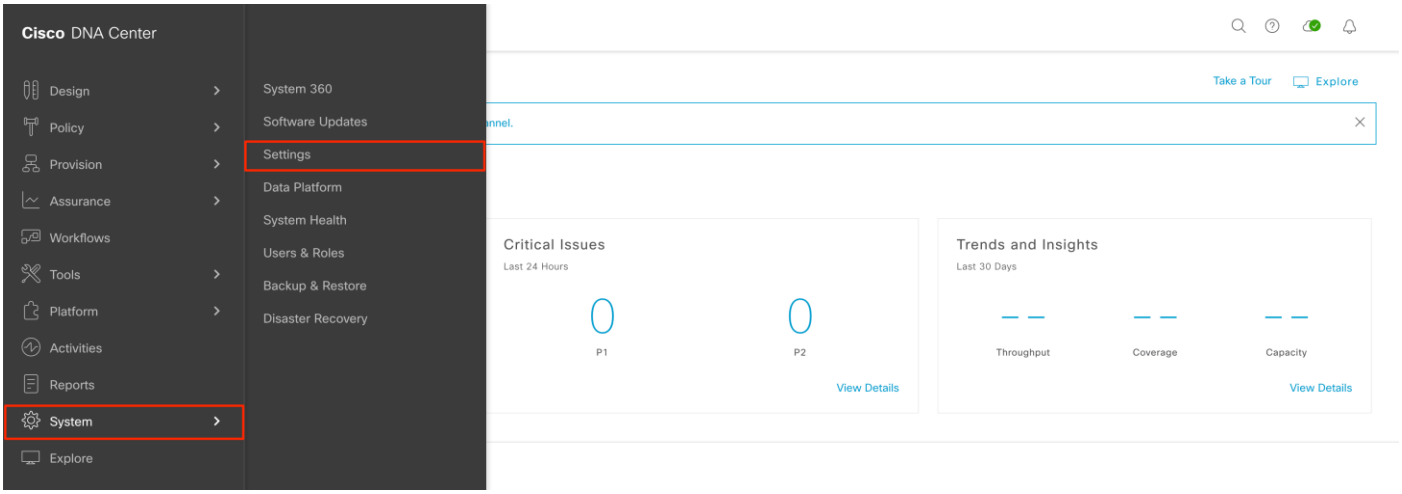
Process 3: Integrate the domain controllers

This section details the procedure to integrate SD-WAN vManage controller in Cisco DNA Center and share IOS-XE WAN Edge device(s) for the *Integrated* Domain integration.

Procedure 1. Integrating vManage in Cisco DNA Center

This section details the procedure to integrate vManage and DNA Center controllers together.

Step 1. Login into Cisco DNA Center, navigate to **System** > **Settings**

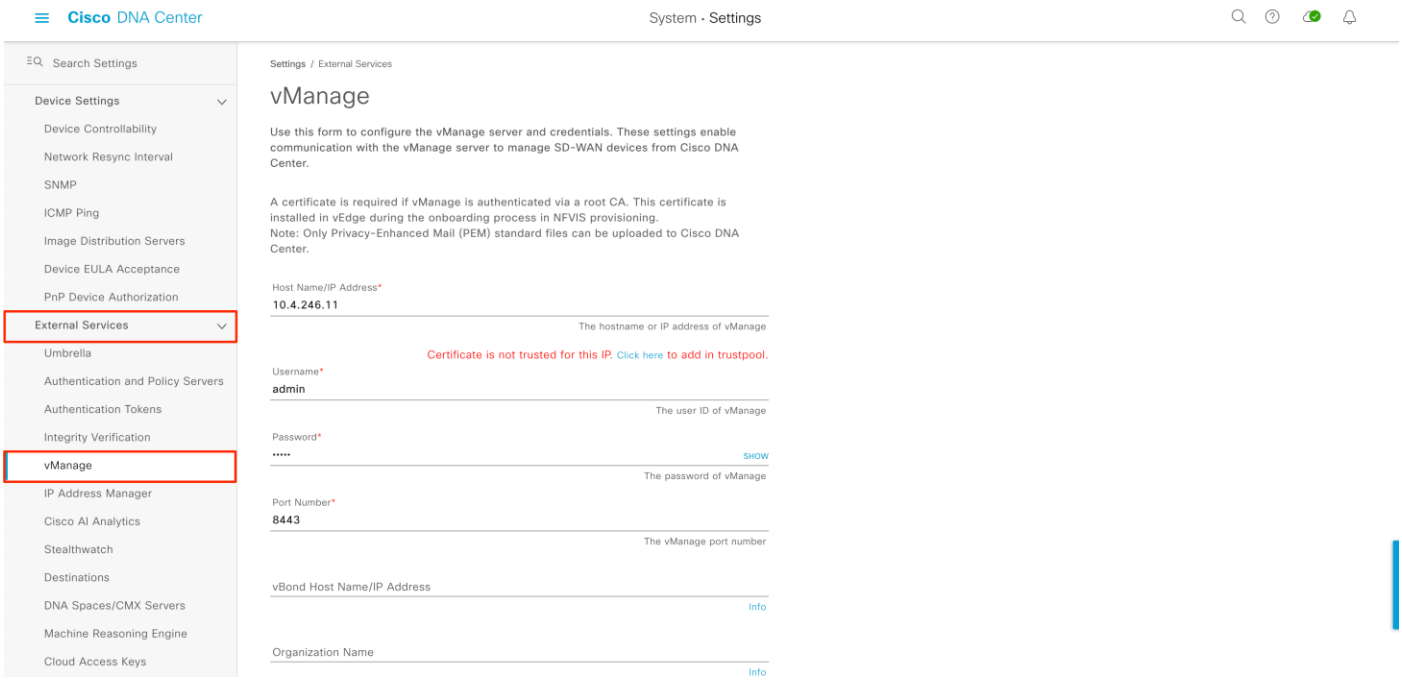


Step 2. Under **External Services**, click **vManage**

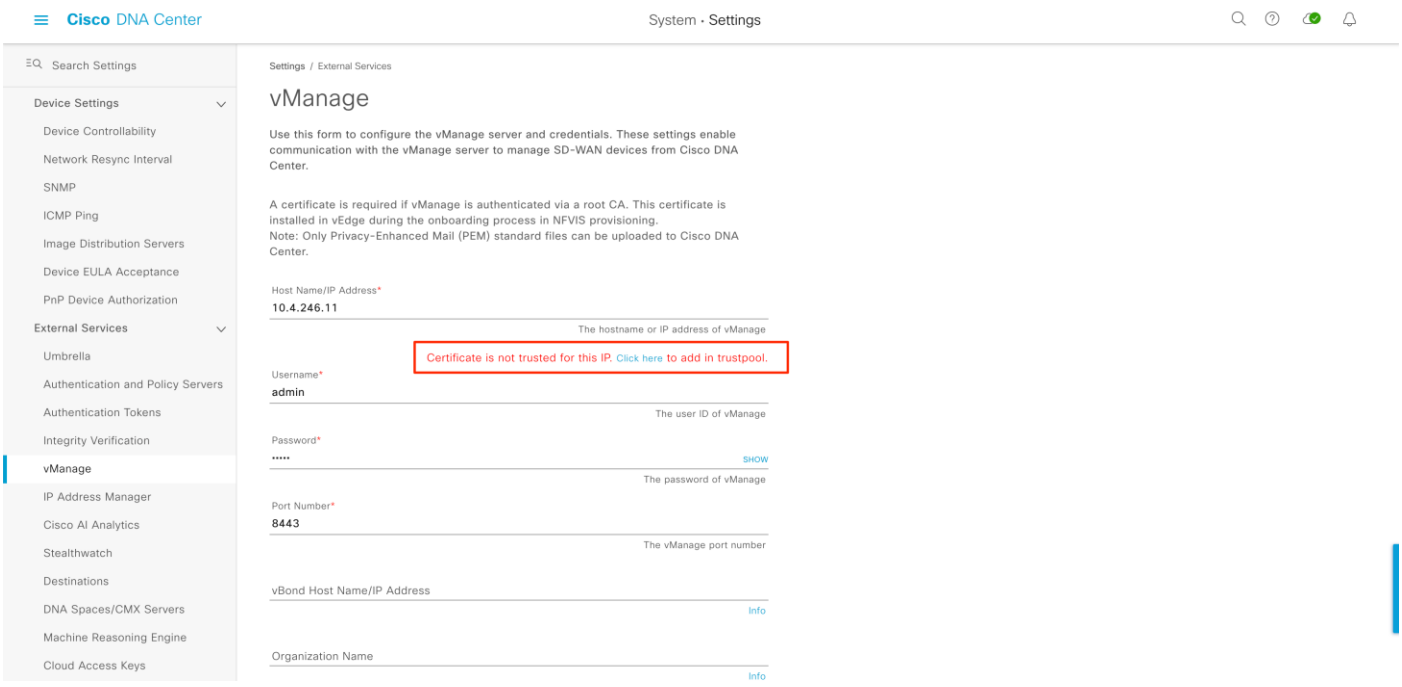
Input **Host Name/IP Address** of the VManage controller,

Credentials: user must be part of the netadmin user-group in vManage.

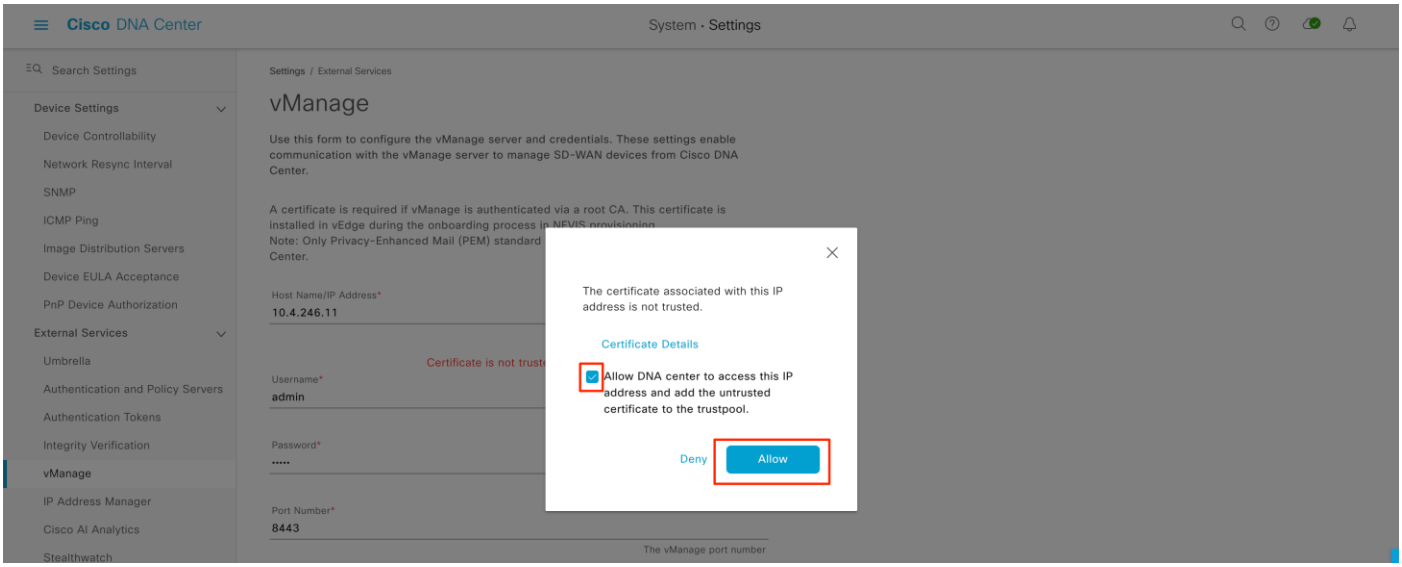
Port Numbers: 8443

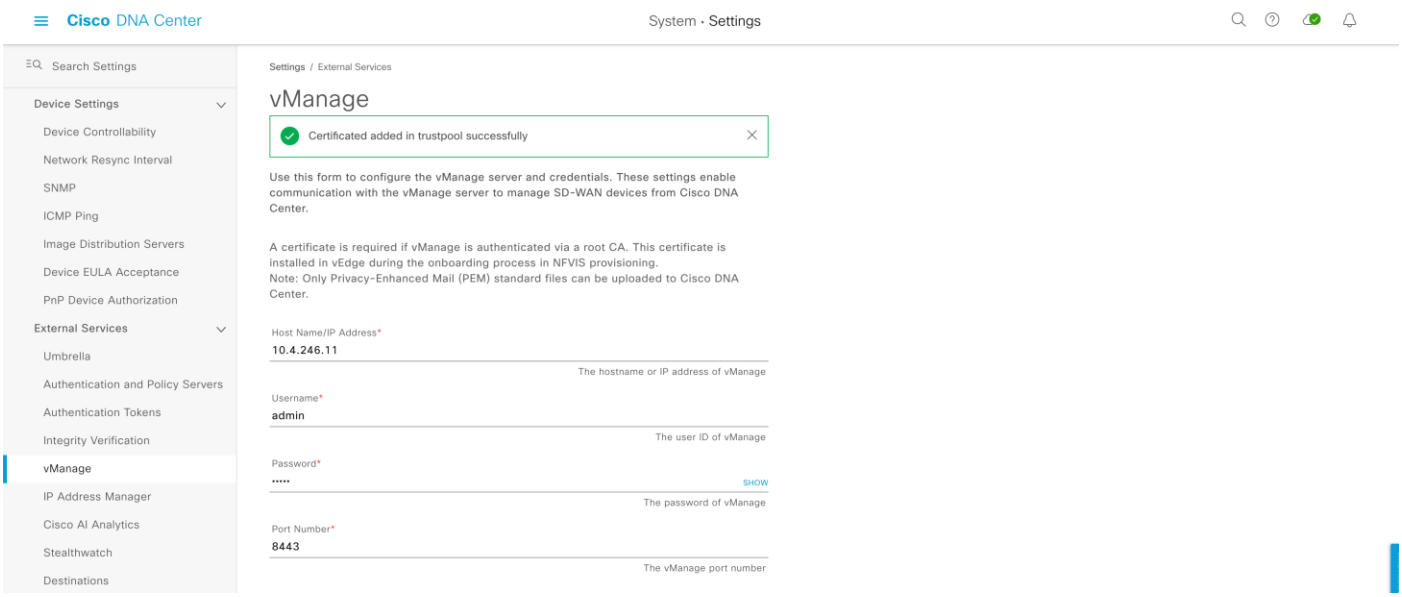


Step 3. Install the trustpool certificate, by clicking the **Click here** and allow the ip-address to be added to the trustpool

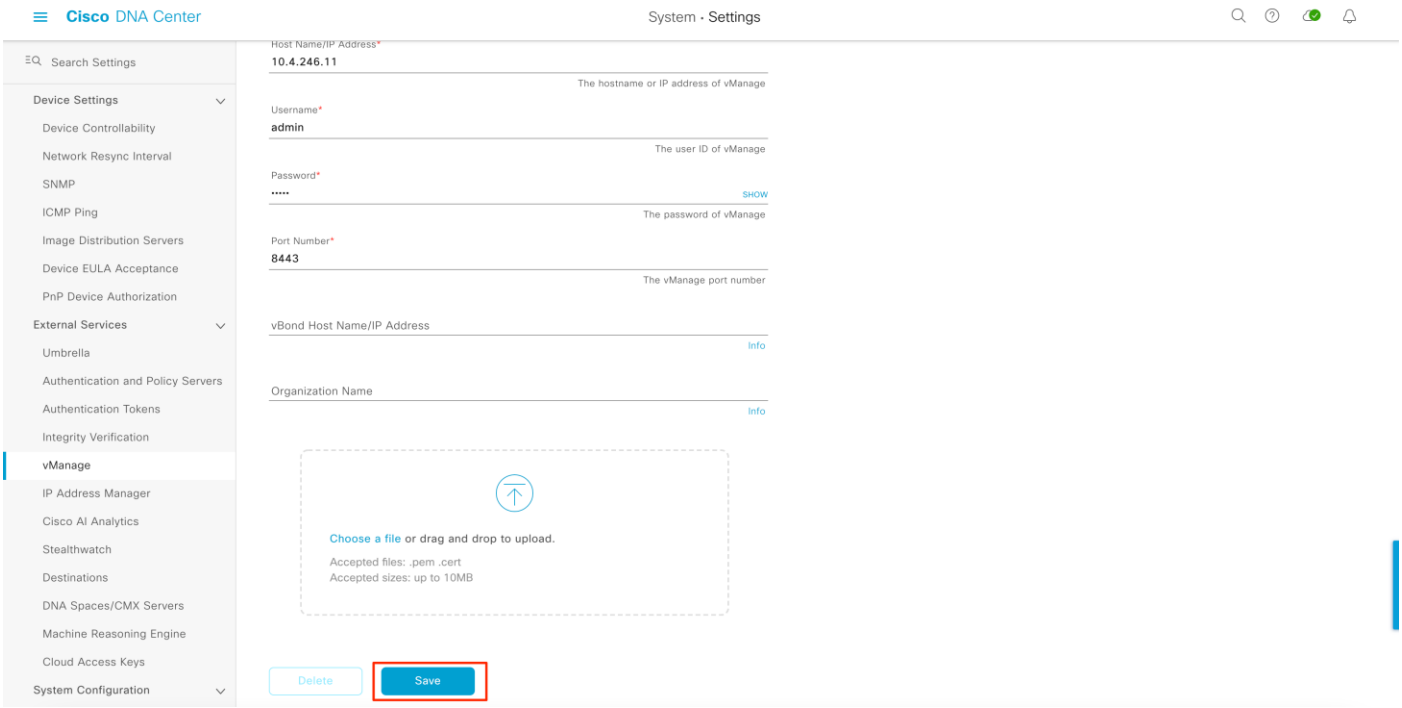


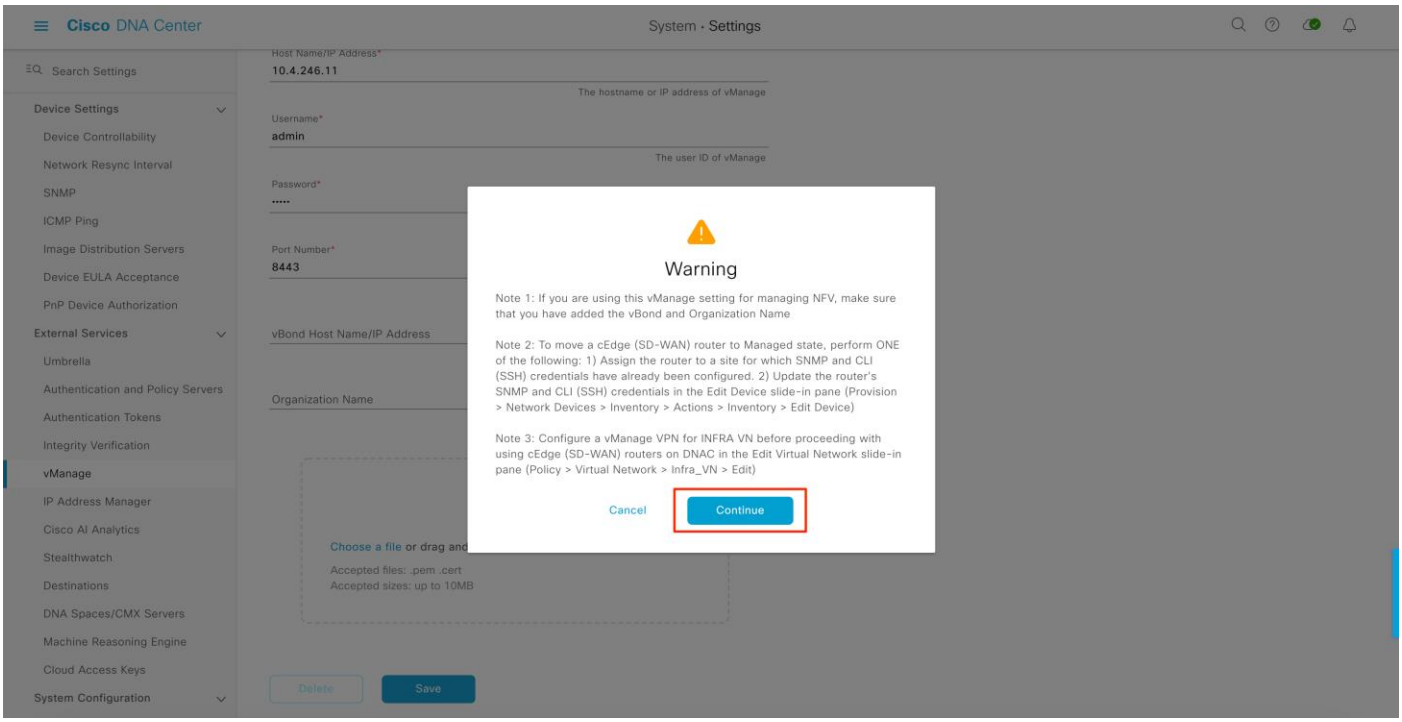
Tech tip
vBond Host Name/IP Address and ***Organization Name*** are optional for the *Integrated* Domain controller integrated but needed if the vManage is managing Enterprise NFV network devices.



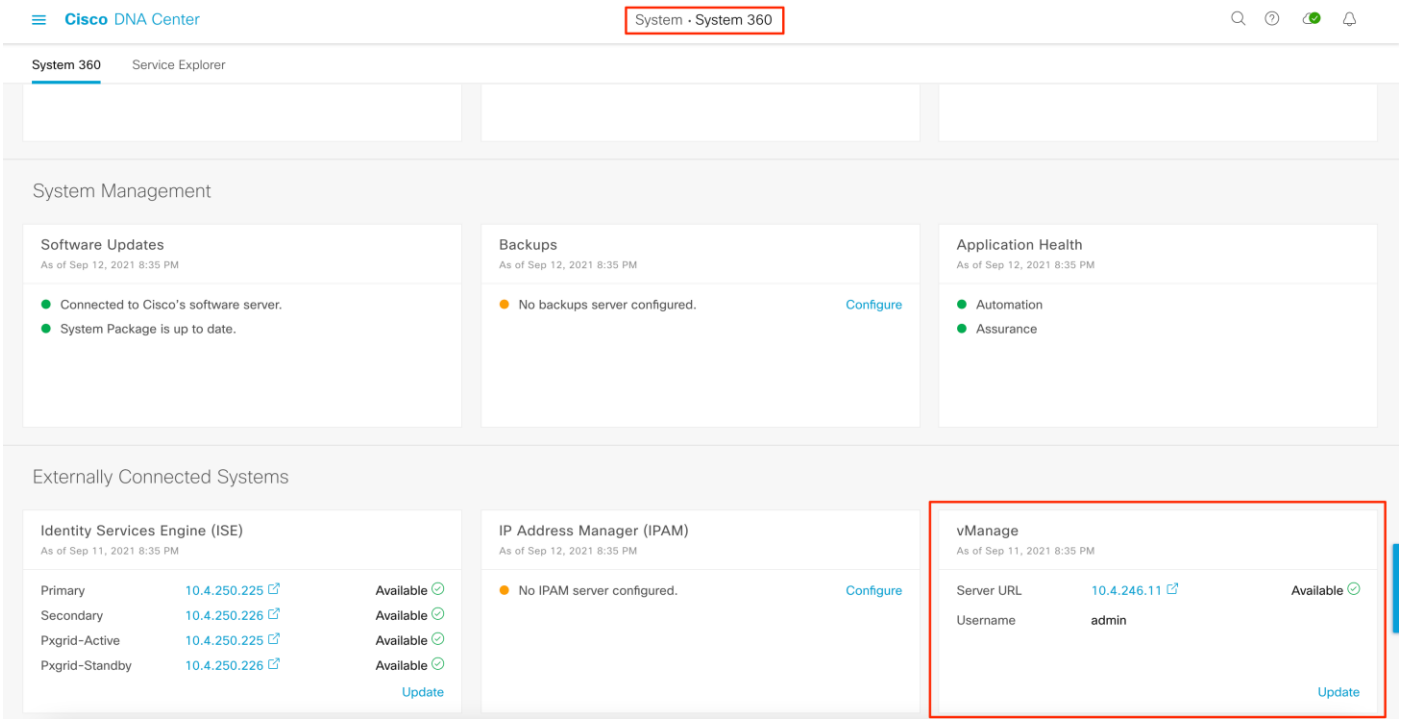


Step 4. Click **Save** and **Continue** in the pop-up **Warning** page.



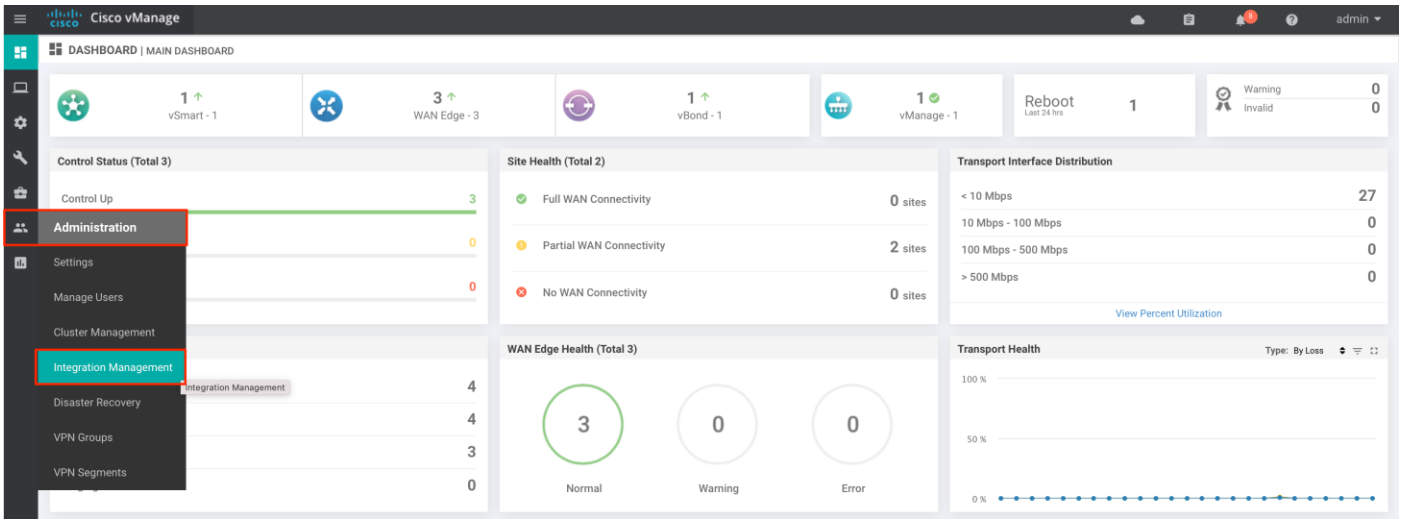


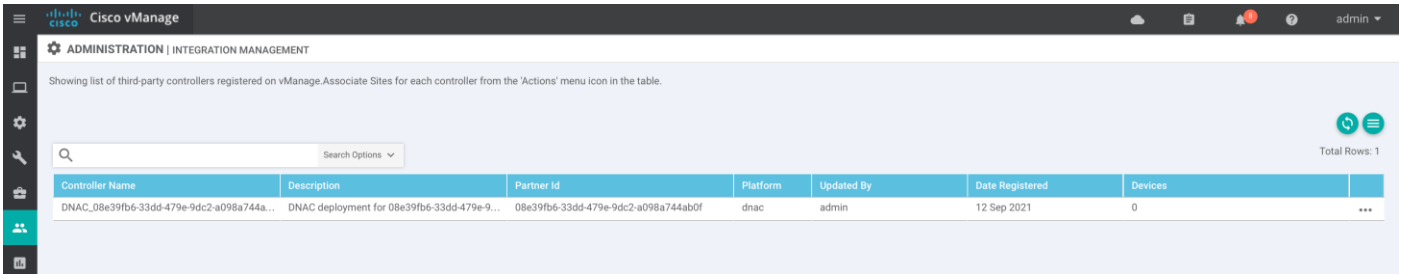
Step 5. Verify the controller integration health in **Cisco DNA Center > System 360**, scroll down to **External Connected Systems** section and view the **vManage** status



Step 6. On successfully integration a registered entry is created in SD-WAN vManage controller.

Login to vManage, navigate to **Administration > Integration Management**

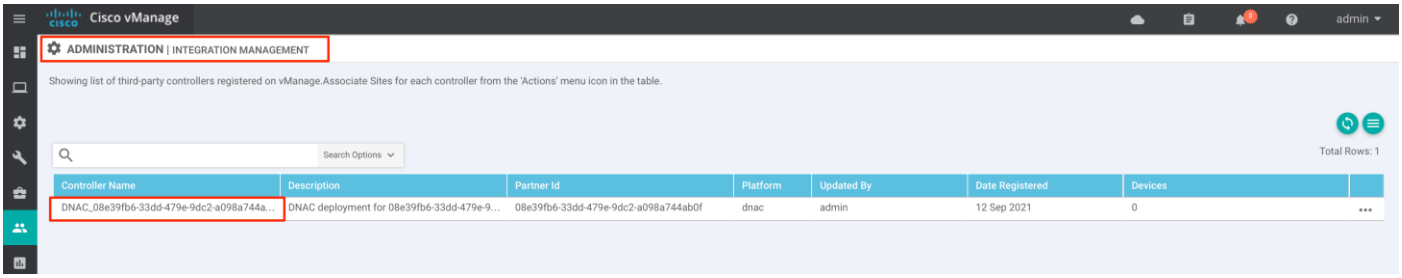




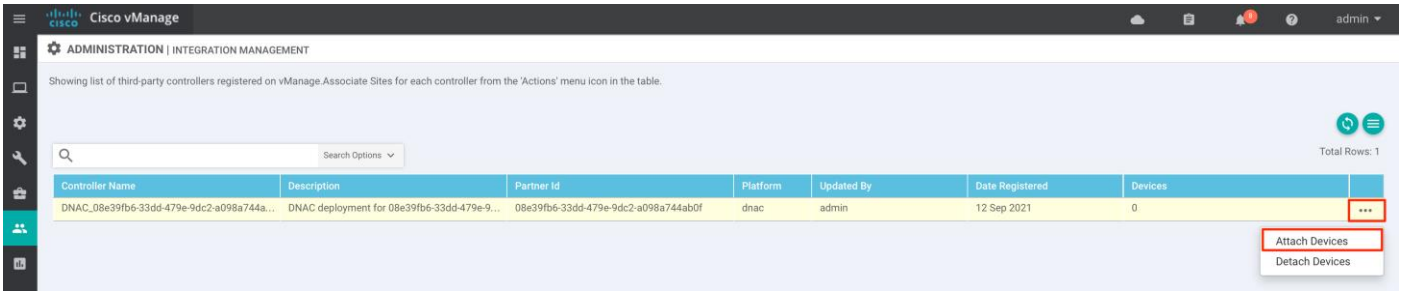
Procedure 2. Associating IOS-XE WAN Edge devices to participate in the *Integrated*-Domain integration

This section details the procedure to associate IOS-XE WAN Edge devices in vManage, share Service VPN and network devices to Cisco DNA Center that are part of the *Integrated* Domain deployment.

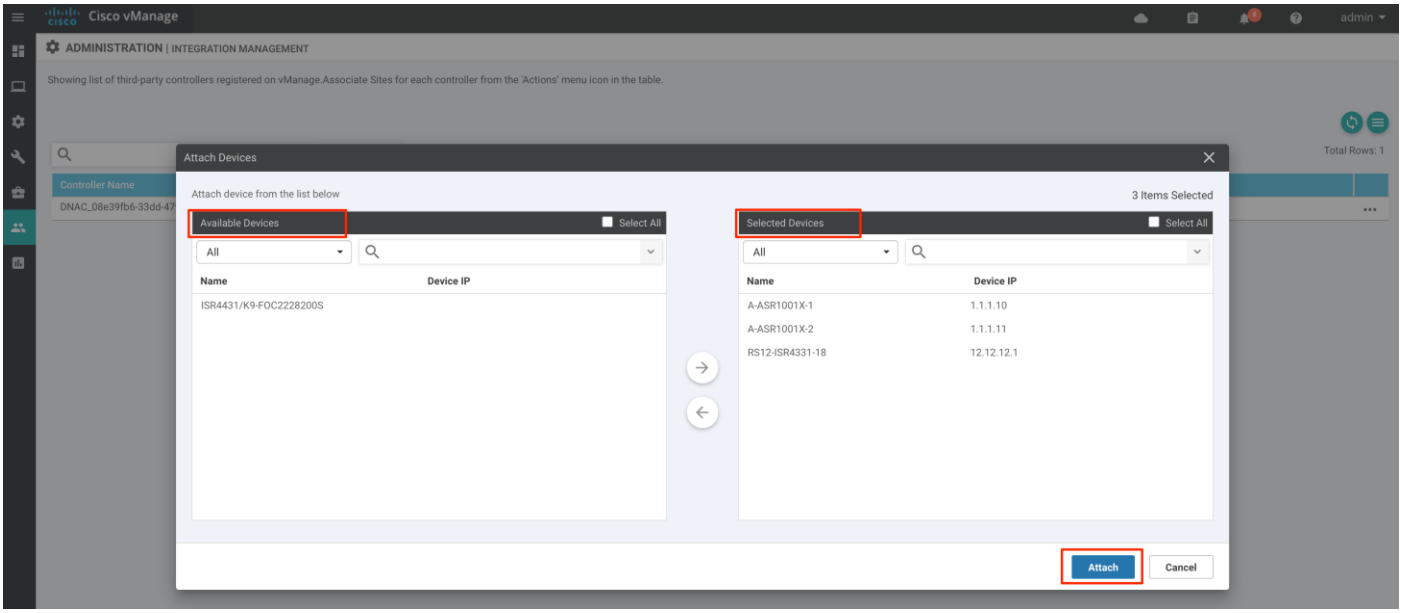
Step 1. Login to vManage, navigate to **Administration > Integration Management**

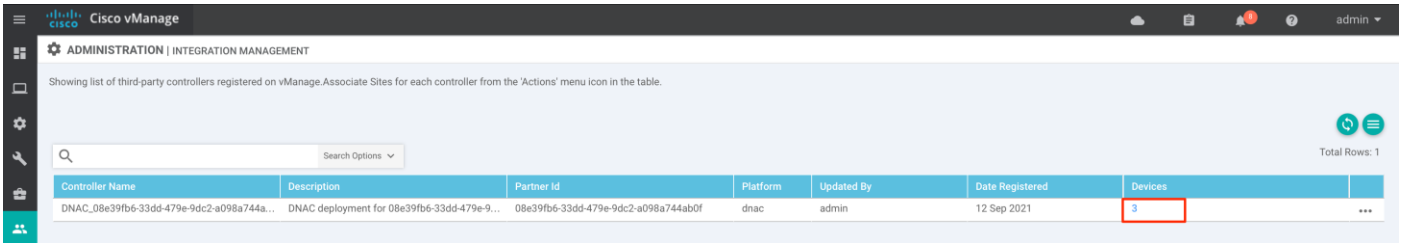


Step 2. Click the three dots (…) and select **Attach Devices** from the drop-down options

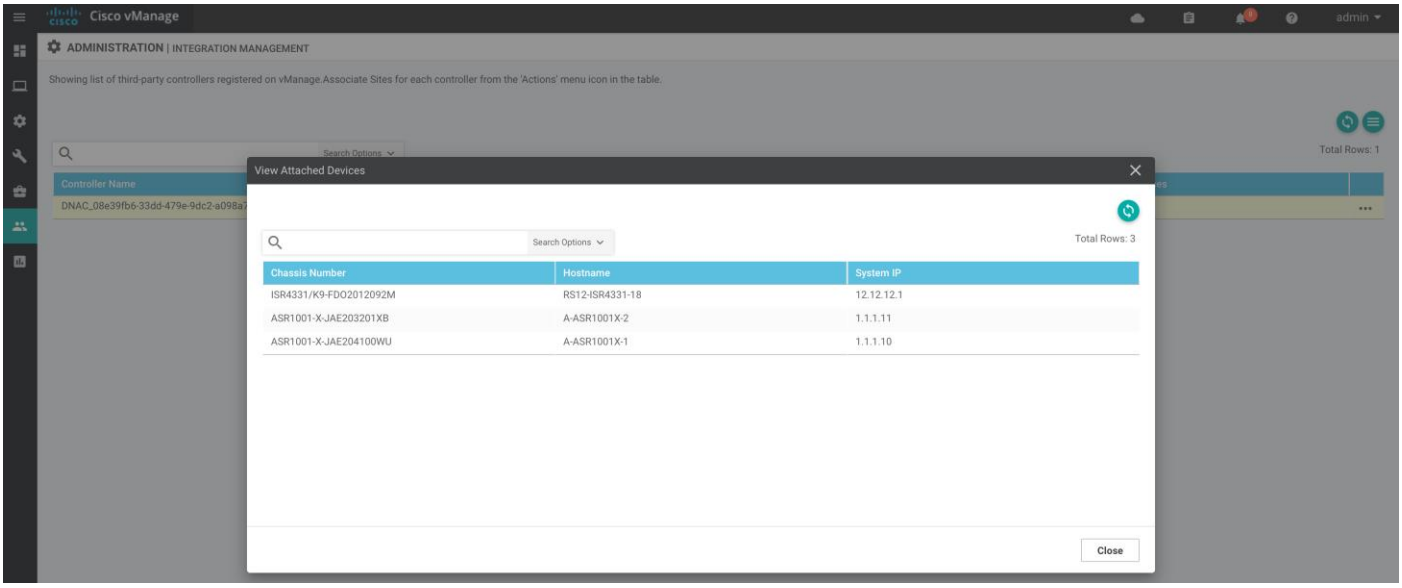


Step 3. Select IOS-XE WAN Edge devices from the **Available Devices** to move them to **Selected Devices** and click **Attach**





Select the value in the Devices column list the devices that are shared by vManage to Cisco DNA Center



Procedure 3. Provision the IOS-XE WAN Edge devices to participate in the *Integrated*-Domain integration

This section details the procedure to provision IOS-XE WAN Edge devices to a site in Cisco DNA Center.

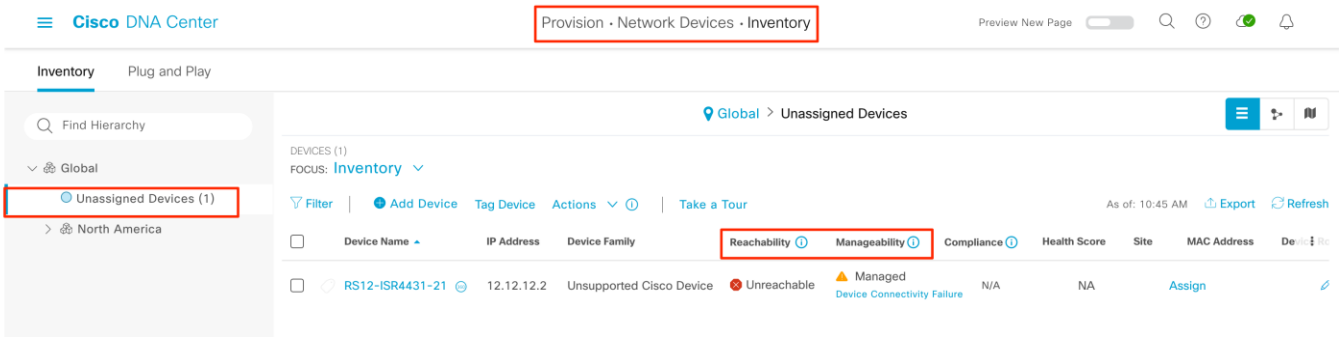
Step 1. Login to Cisco DNA Center, navigate to **Provision > Network Devices > Inventory.**

The WAN Edge device status in Cisco DNA Center is **Ping Reachable** with Manageability status as **Managed** with **SNMP Authentication Failure**. This is expected as the device has not been provisioned with site-specific parameters that contain SNMP configuration required to manage in network device in Cisco DNA Center.

Tech tip

The WAN Edge device status can also be in Reachability status as **Unreachable** and Manageability status as **Managed** with **Device Connectivity Failure**. This is expected as there is no loopback 0 ethernet interface configured on the WAN Edge device and the 'system-ip' address on the WAN Edge device is not reachable from Cisco DNA Center.

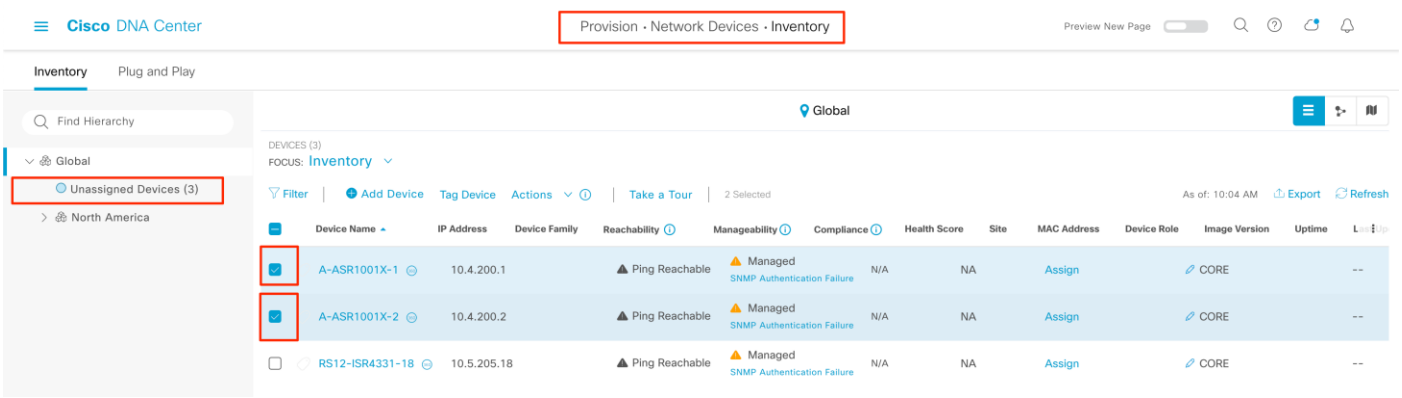
The Cisco DNA Center LAN Automation workflow to discover and provision the Fabric GRT network devices, will provision the required loopback 0 ethernet interface on the WAN Edge devices selected as Primary and Peer Seed device.

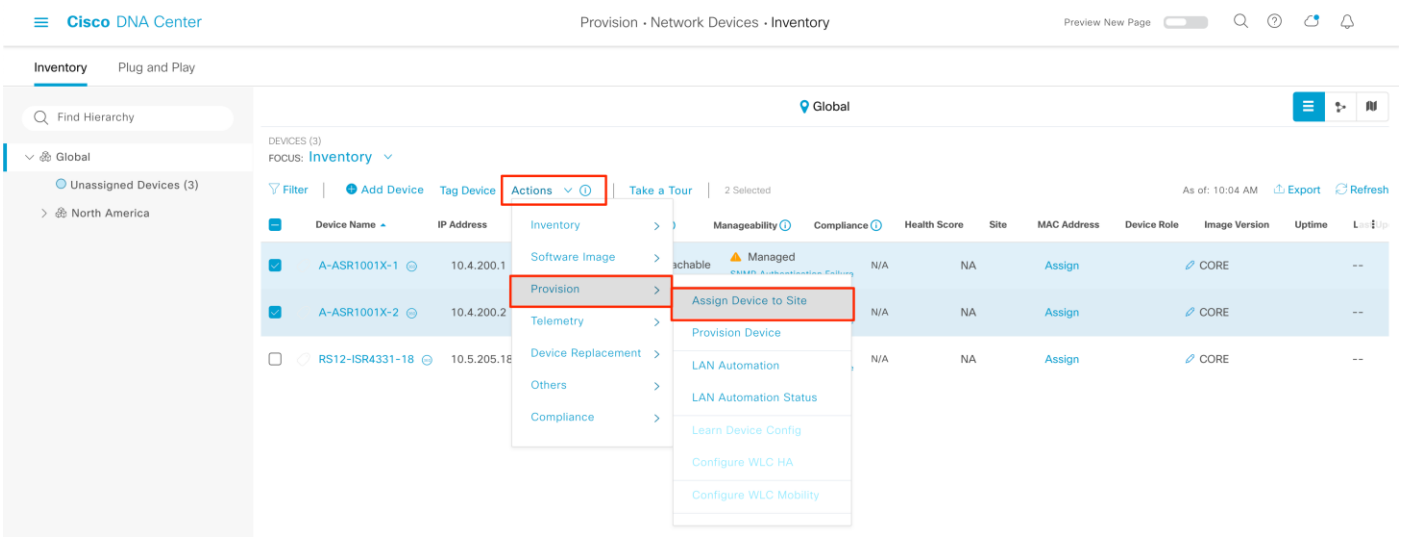


Continue with steps in this Procedure, even for the WAN Edge devices in the error state - **Unreachable, Managed** with **Device Connectivity Failure** status. Any DNA Center generated configuration is shared with vManage to provision it to the WAN Edge devices.

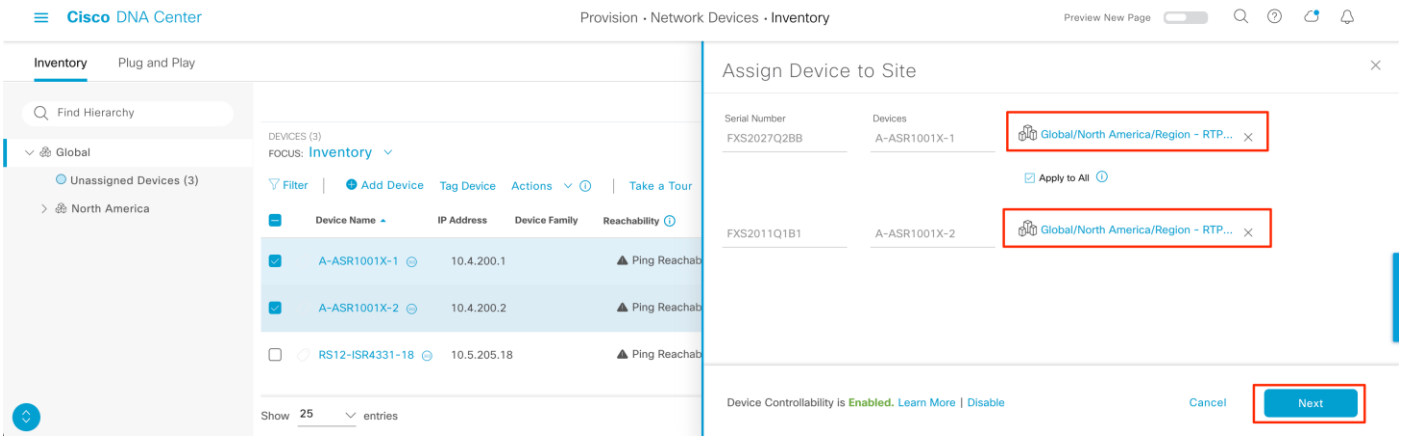
Step 2. With the WAN Edge devices in either Reachability and Manageability state, select the WAN Edge devices in the **Unassigned Devices** hierarchy

select **Actions > Provision > Assign Device to Site**

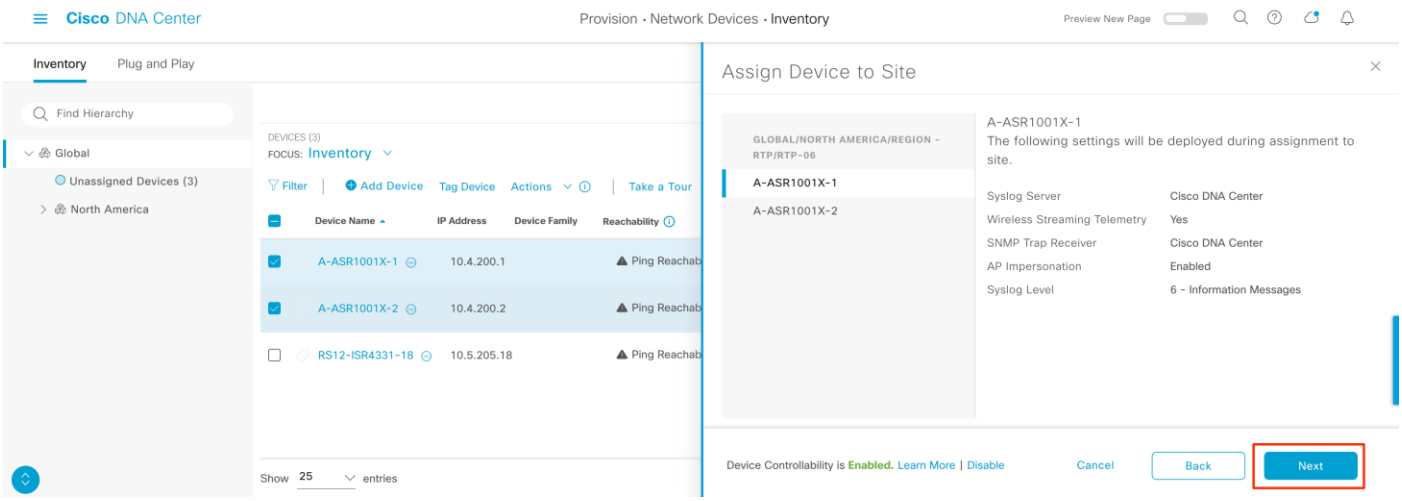




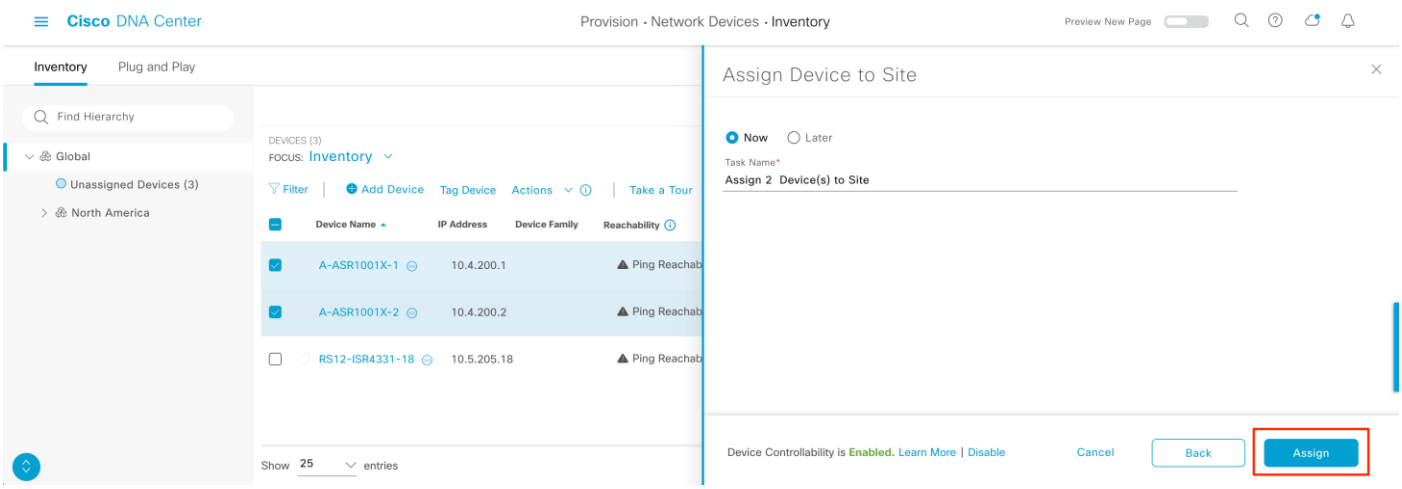
Step 3. In the slide-out page **Choose a Site** for each device and click **Next**



Step 4. View the parameters that gets provisioned to the device and click **Next**

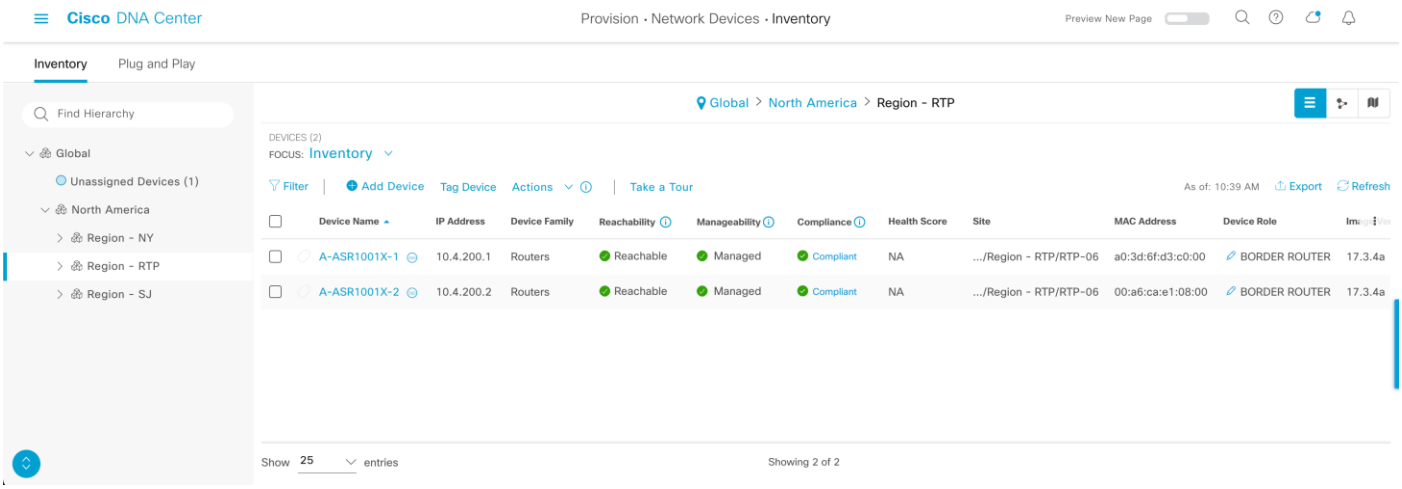


Click **Assign**

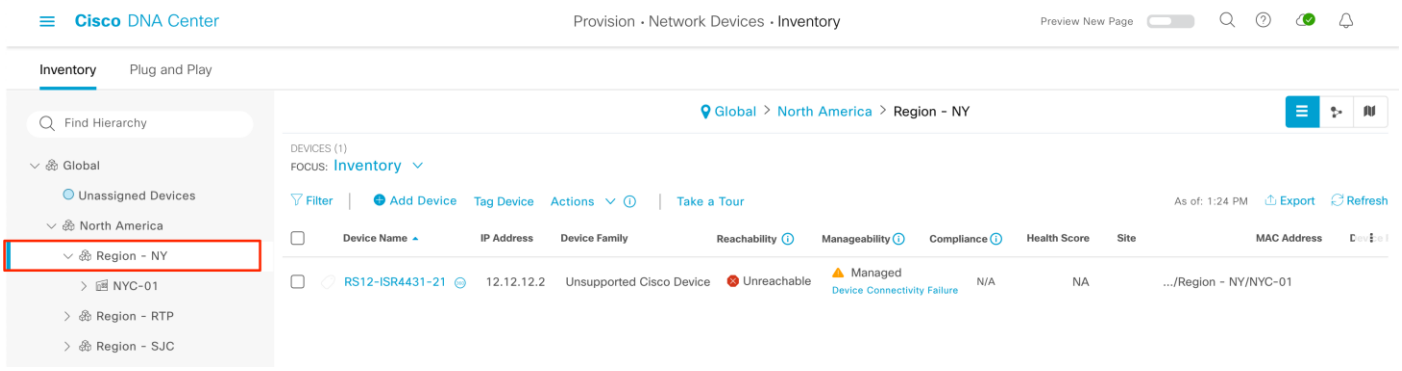


Step 5. Verify the devices are associated to the site.

For WAN Edge devices configured with Loopback 0 interface associated in the Fabric GRT Service VPN, Cisco DNA Center will use Loopback 0 IPv4 address to connect, perform SNMP polling and move the device to **Managed** state.



For WAN Edge devices with no Loopback 0 interface configured, Cisco DNA Center will not be able to connect. Devices will be in **Unreachable**, **Managed** with **Device Connectivity Failure** state but part of the site hierarchy.

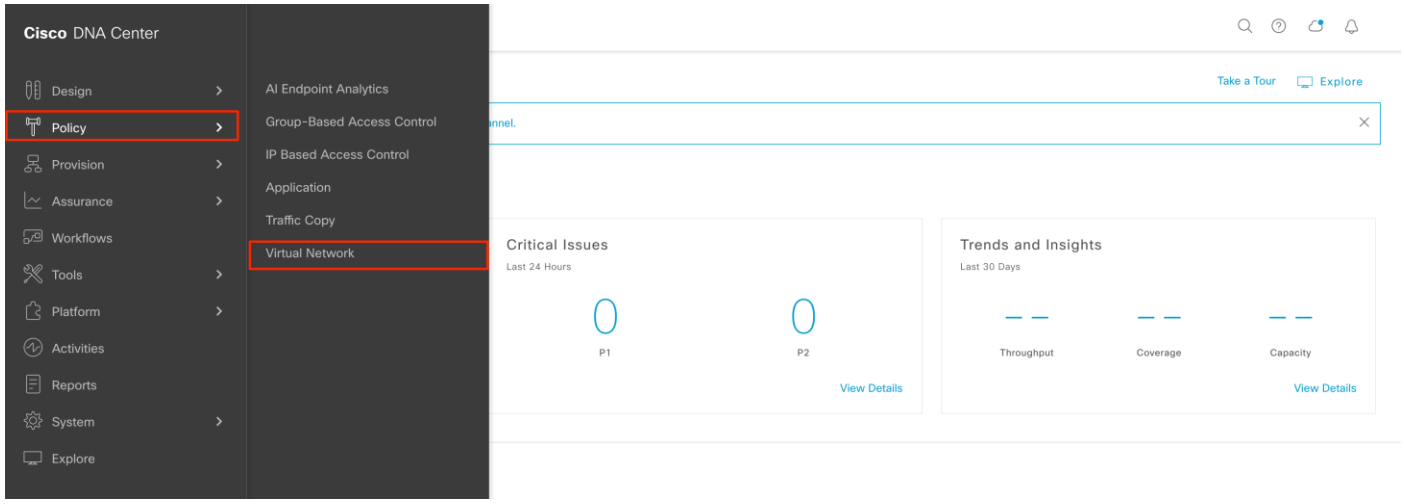


Tech Tip
The Cisco WAN Edge CLI credentials defined in the Cisco DNA Center network setting, must be configured on the network device. If needed, local user credentials can be configured on the WAN Edge device with Cisco AAA feature template from the vManage UI.

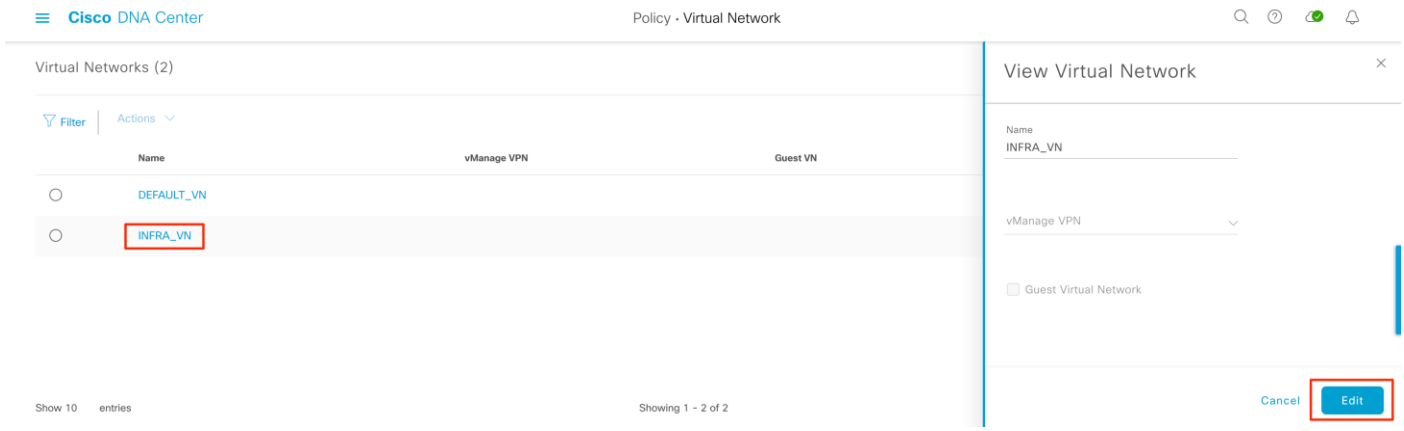
Procedure 4. Mapping Service VPN to Virtual Network in Cisco DNA Center

This section details the procedure of mapping Service VPN to Virtual Network in Cisco DNA Center.

Step 1. Login to Cisco DNA Center, navigate to **Policy > Virtual Networks**

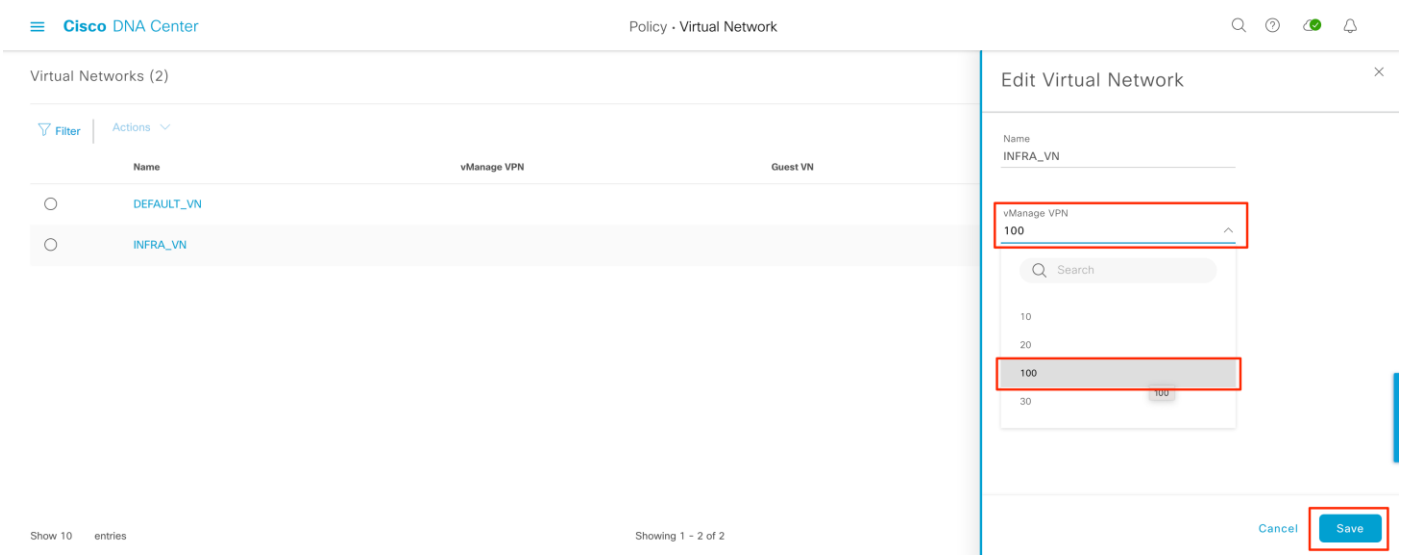


Step 2. Click in the Virtual Network name **INFRA_VN**, and click **Edit** in the slide-out page



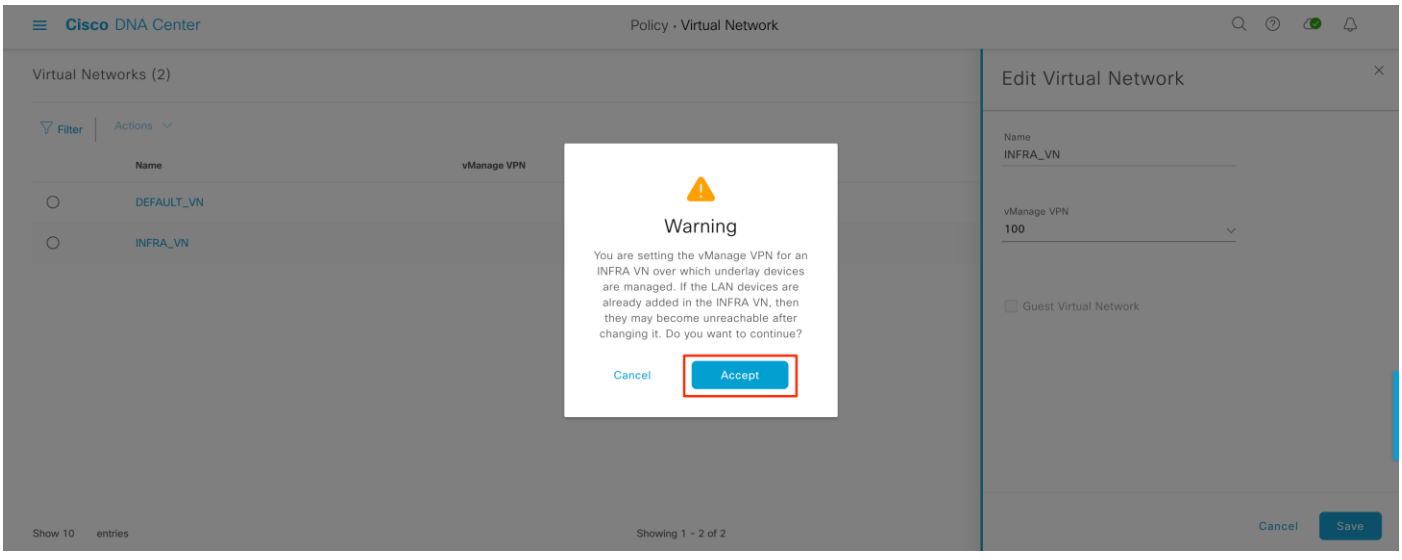
Choose the Fabric GRT Service VPN associated to the WAN Edge device in the vManage VPN drop-down option.

Click **Save**

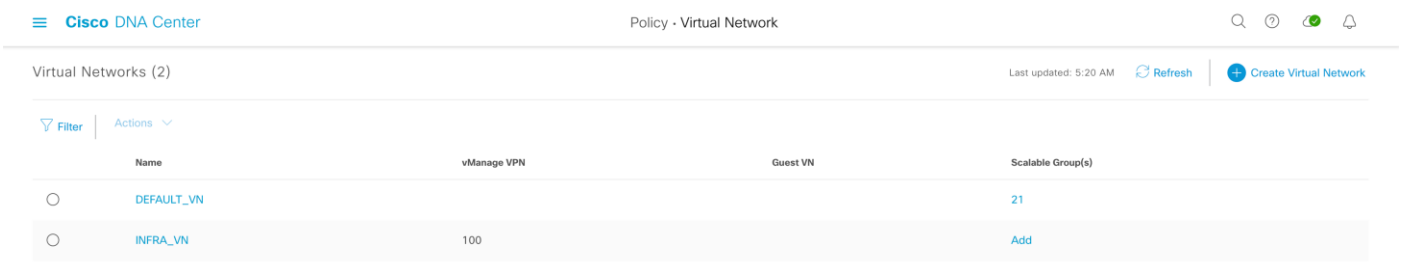


Tech tip
The vManage VPN lists all the user-configured Service VPNs that are created and associated to IOS-XE WAN Edge device that are part of the integration.

click **Accept**

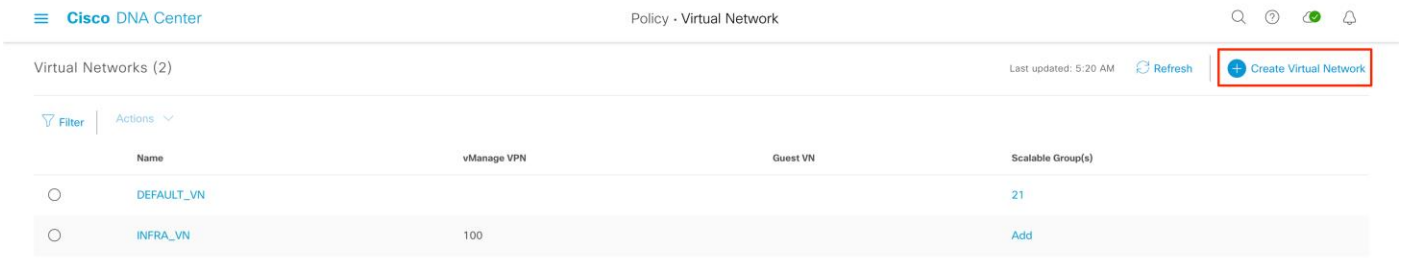


Step 3. Repeat the previous step, Step 2, for all Service VPN deployed in the SD-WAN fabric that has a corresponding Virtual Network already created.



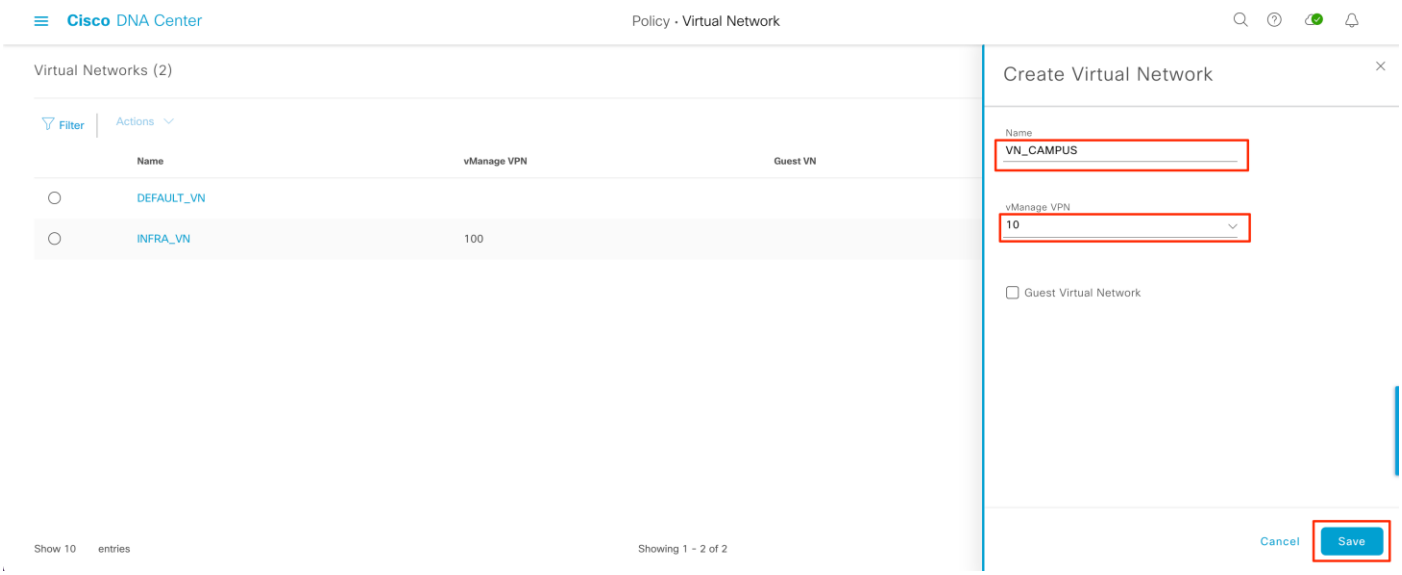
Step 4. Create a new SD-Access Virtual Network and map to Cisco SD-WAN Service-VPN to it.

Click **Create Virtual Network**

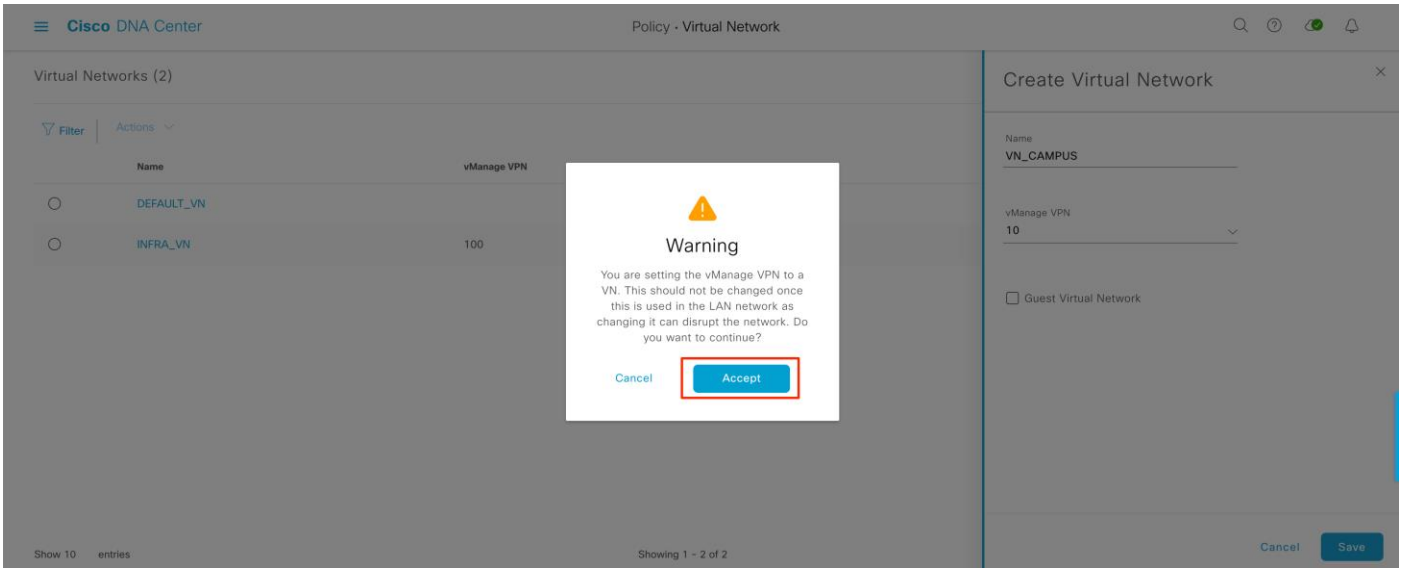


Input **Name** and choose the Service VPN that maps to the Virtual Network from the drop-down option

Click **Save**

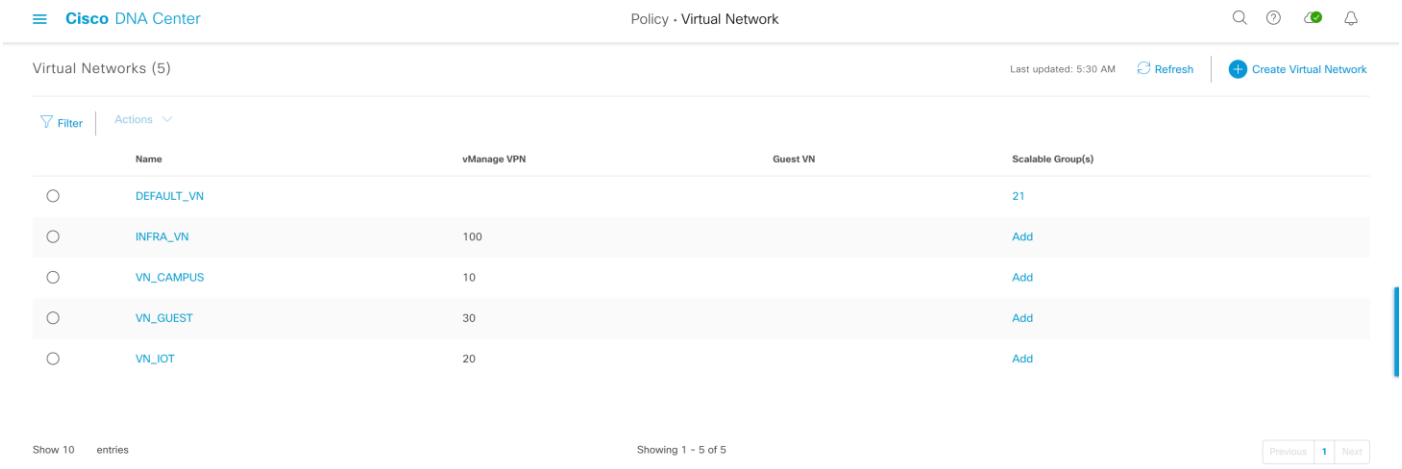


Select **Accept**



Step 5. Repeat the previous step, Step 4, for all Service VPN deployed in the SD-WAN WAN fabric and that requires corresponding Virtual Network in the Cisco SD-Access fabric.

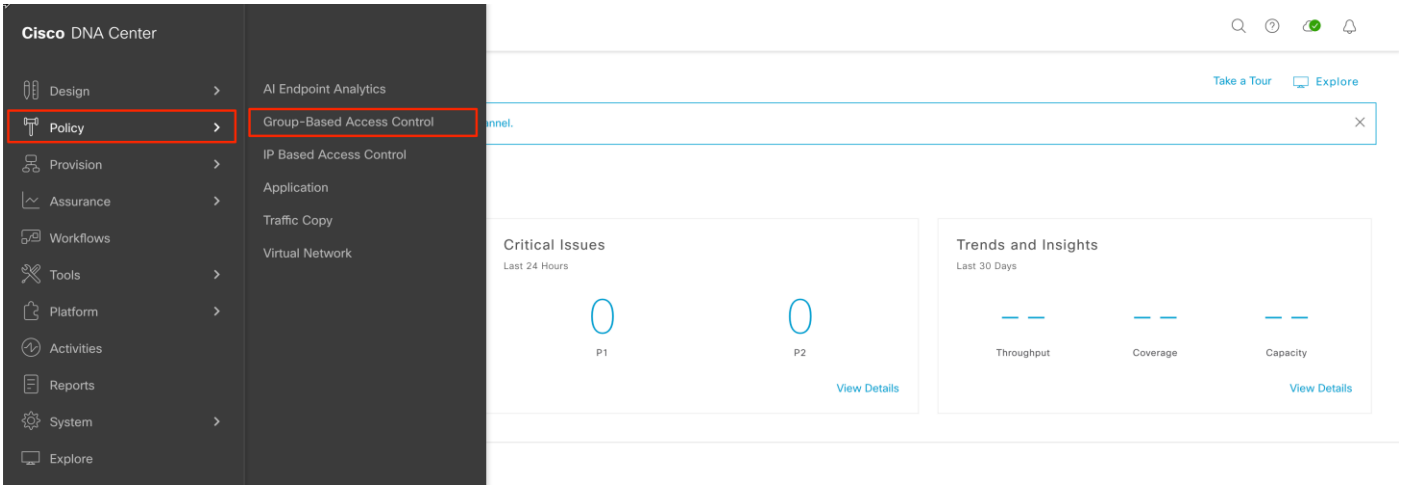
Step 6. Verify each Virtual Network is mapped to SD-WAN Service VPN extending the macro-segmentation from one domain to another.



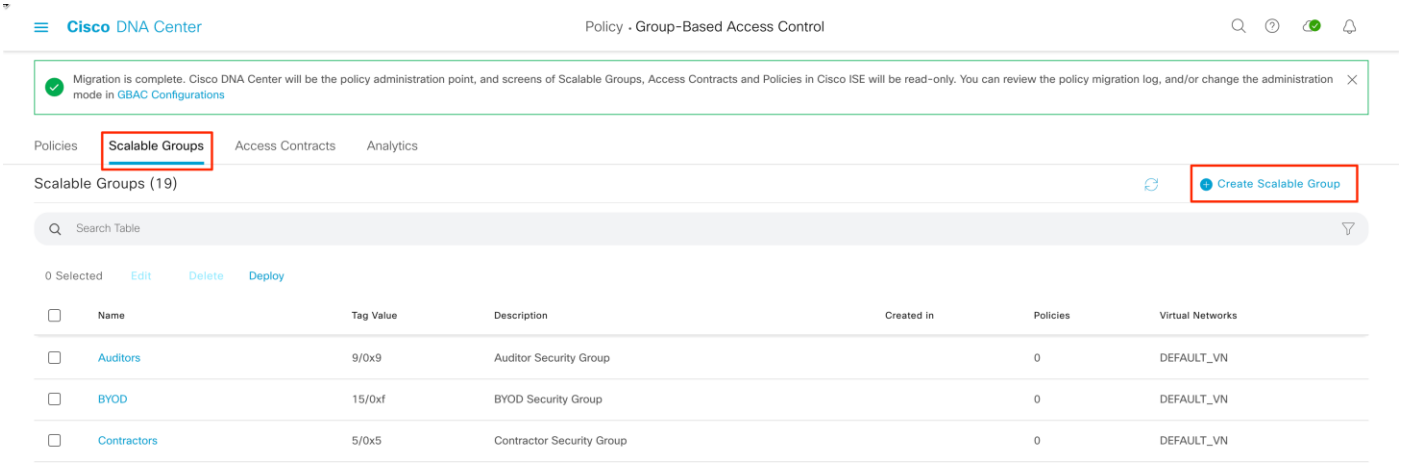
Procedure 5. Associate Scalable Groups to Virtual Networks

This section details the procedure to create Scalable groups and associate Scalable groups to Virtual Networks.

Step 1. In Cisco DNA Center, navigate to **Policy > Group-Based Access Control**

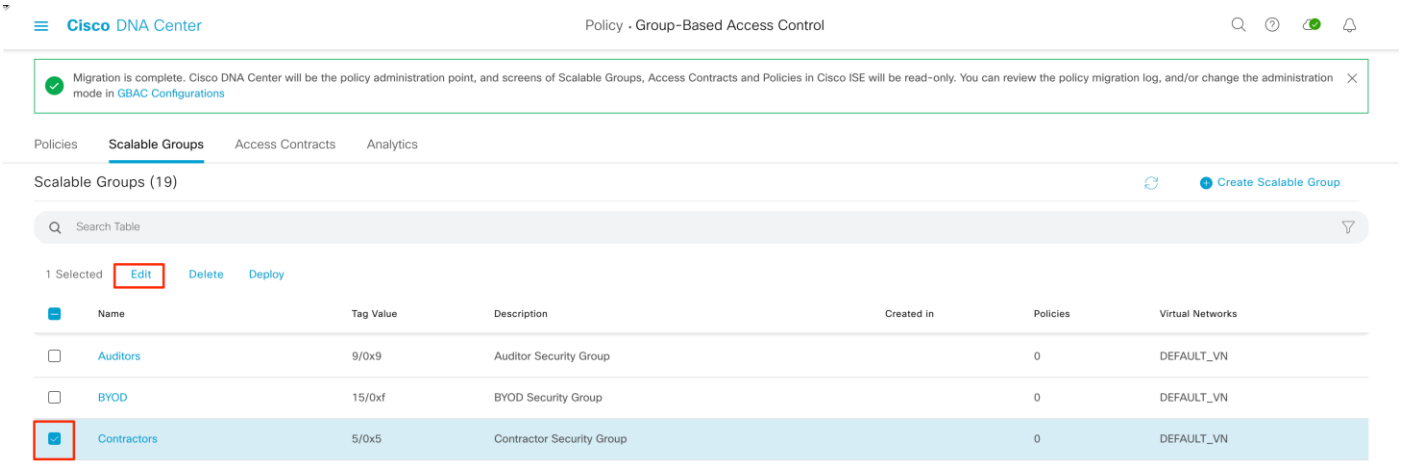


Step 2. Select **Scalable Groups** tab

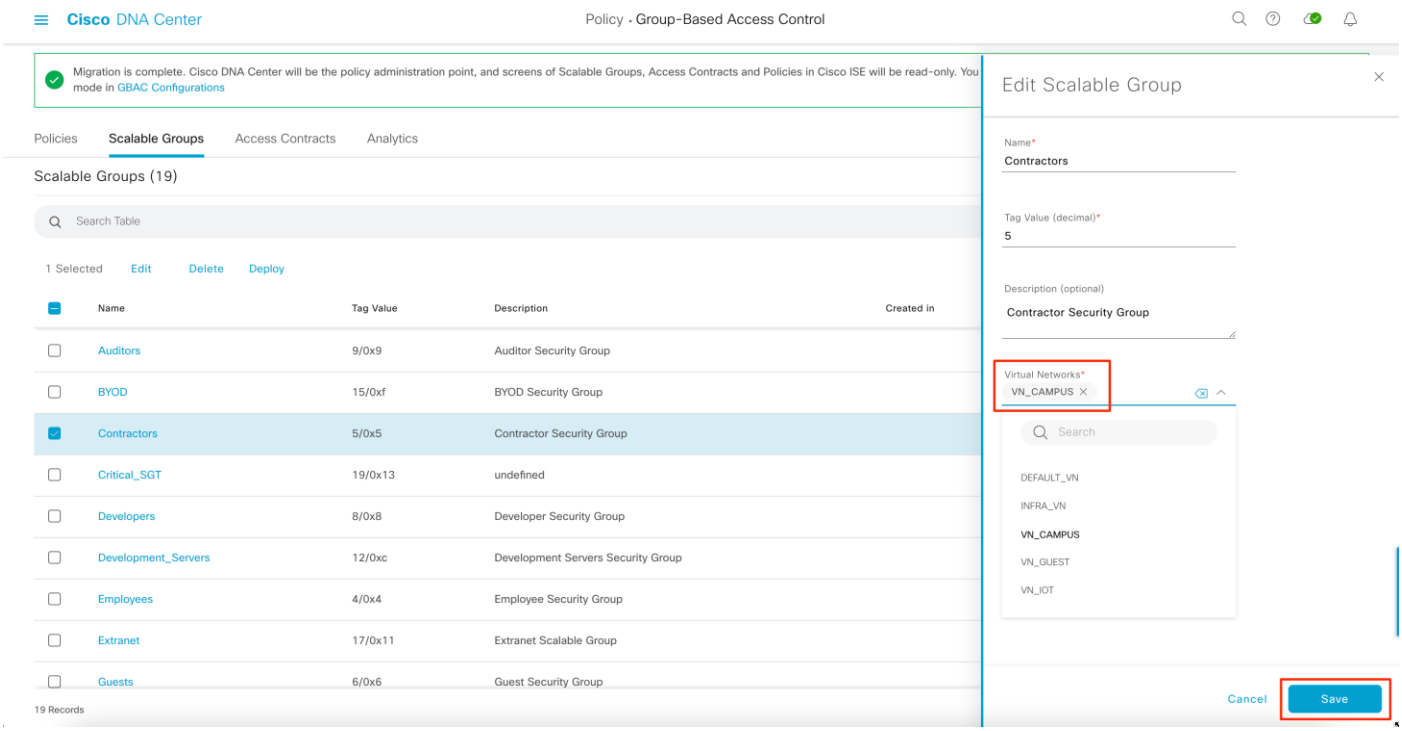


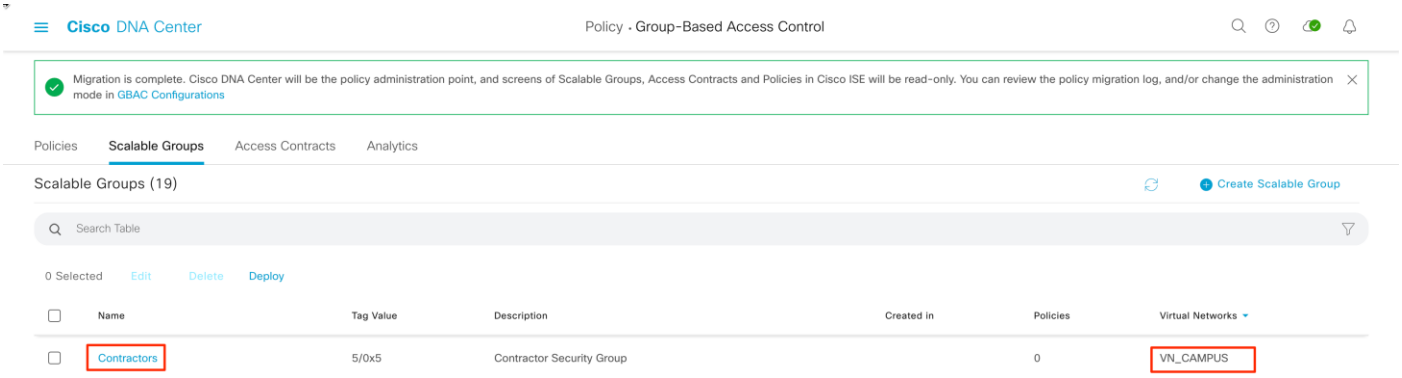
Note: By default, the Scalable Group learnt from ISE are associated to DEFAULT_VN

Step 3. To associate the Scalable Group to different Virtual Network, select the **Scalable Group** from the list and click **Edit**



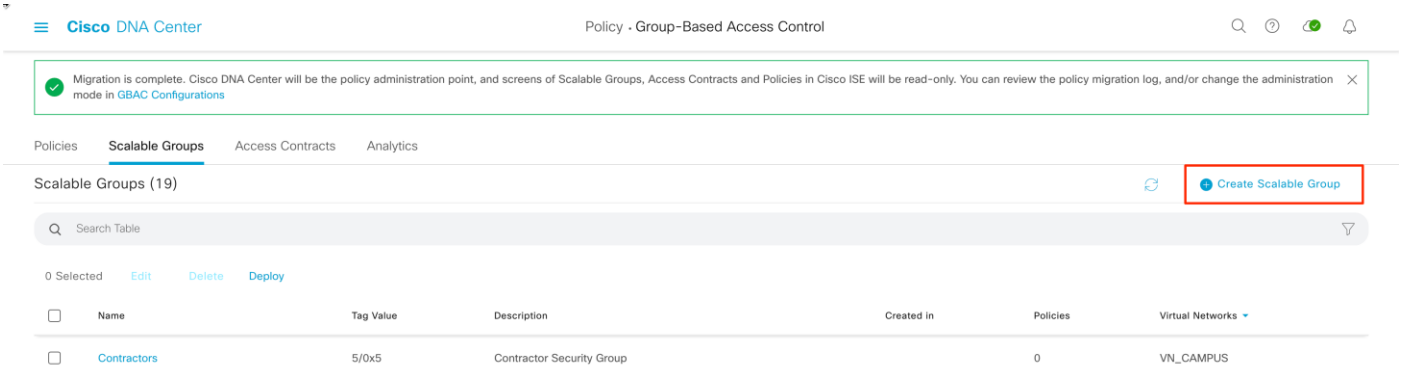
Select **the Virtual Networks** from the options and click **Save**



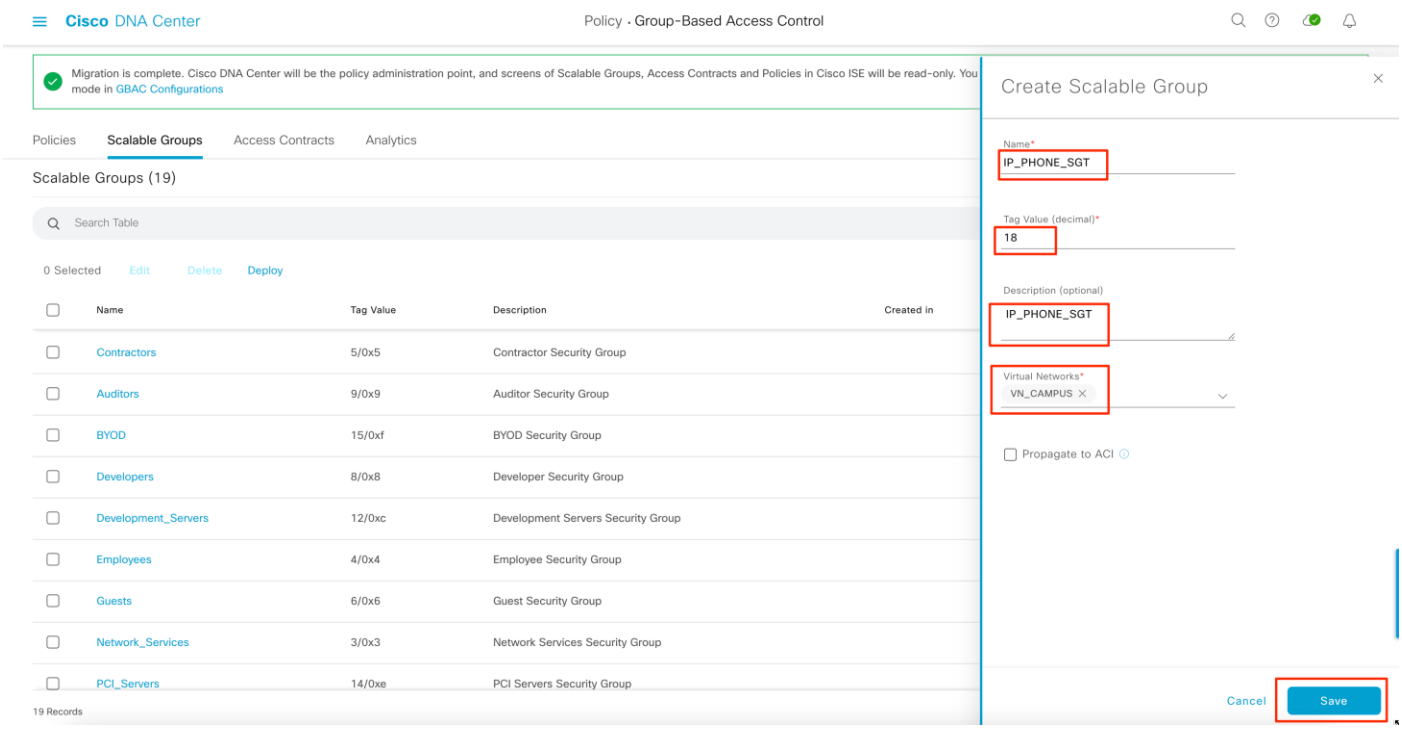


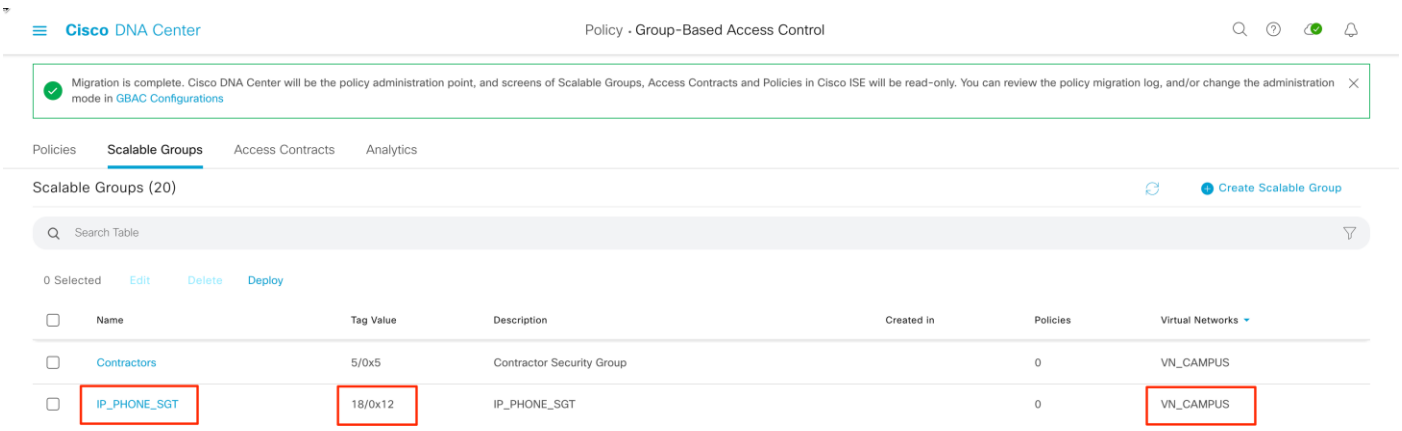
Step 4. Repeat Step 3, for other **Scalable Groups** being deployed at the site.

Step 5. To create new Scalable Group, select **Create Scalable Group**

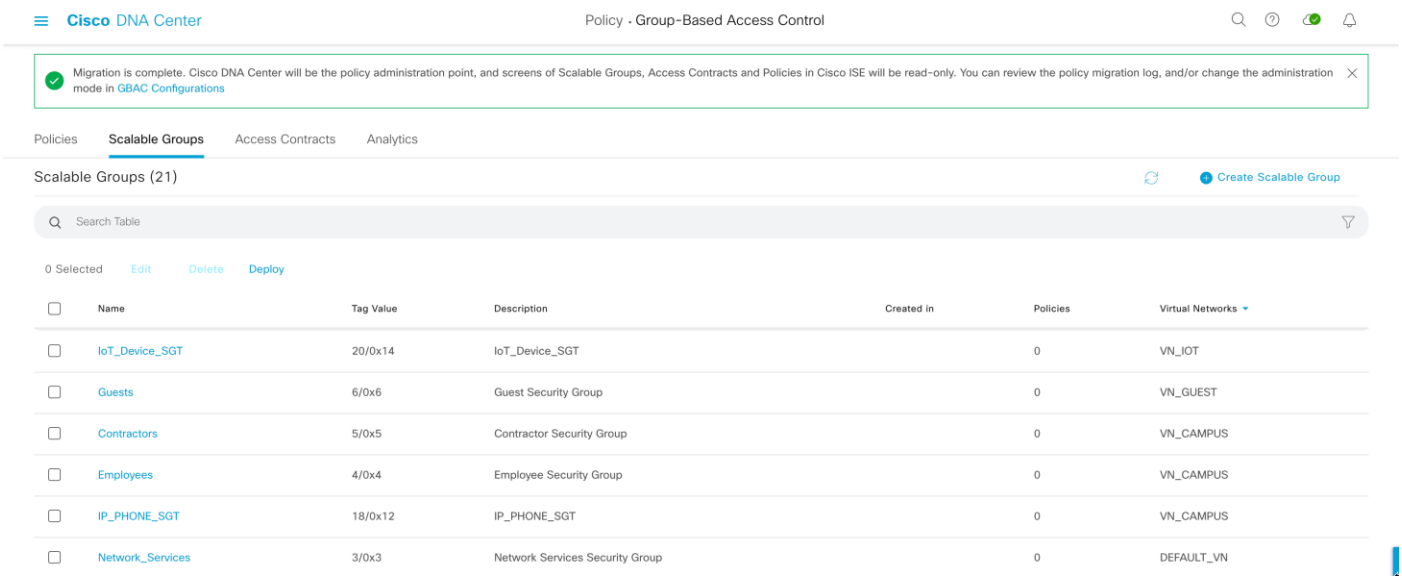


Input **Name**, **Tag Value** (optional), **Virtual Networks** and click **Save**





Step 6. Repeat the previous step, Step 5, to create additional **Scalable Group** and associate **Virtual Networks**.

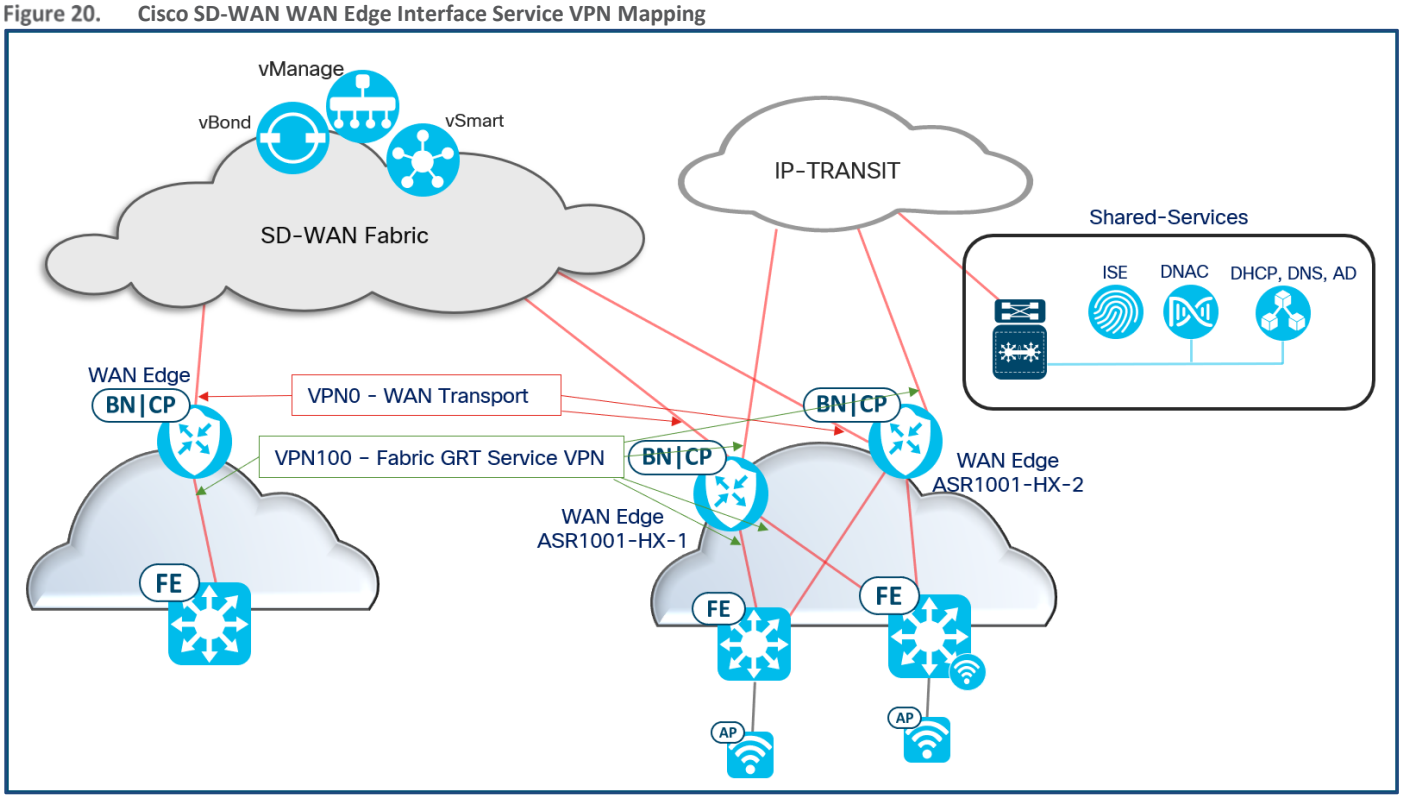


Process 4: Configuring LAN Segment manually

This section of the deployment guide provides detailed steps to manually configure the LAN segment with the intent to build Fabric GRT reachability at the site and also provide Fabric GRT reachability across sites.

WAN Edge device connectivity to LAN and WAN segment over different Service VPN.

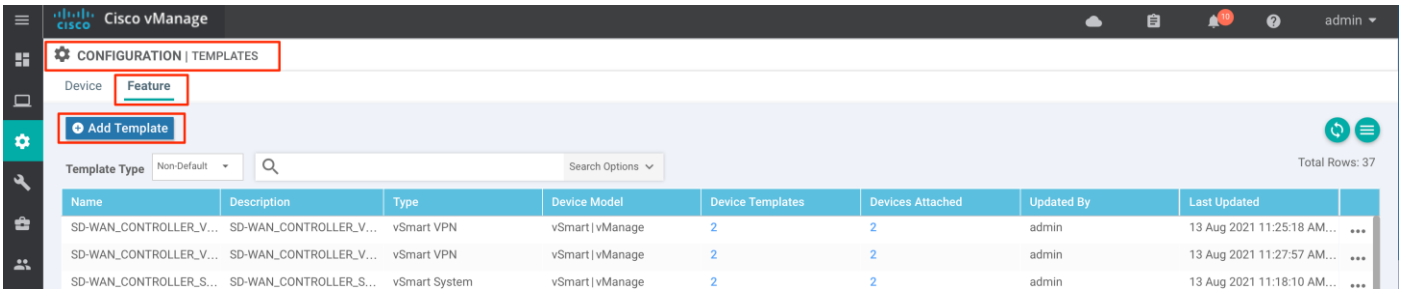
Figure 20. Cisco SD-WAN WAN Edge Interface Service VPN Mapping



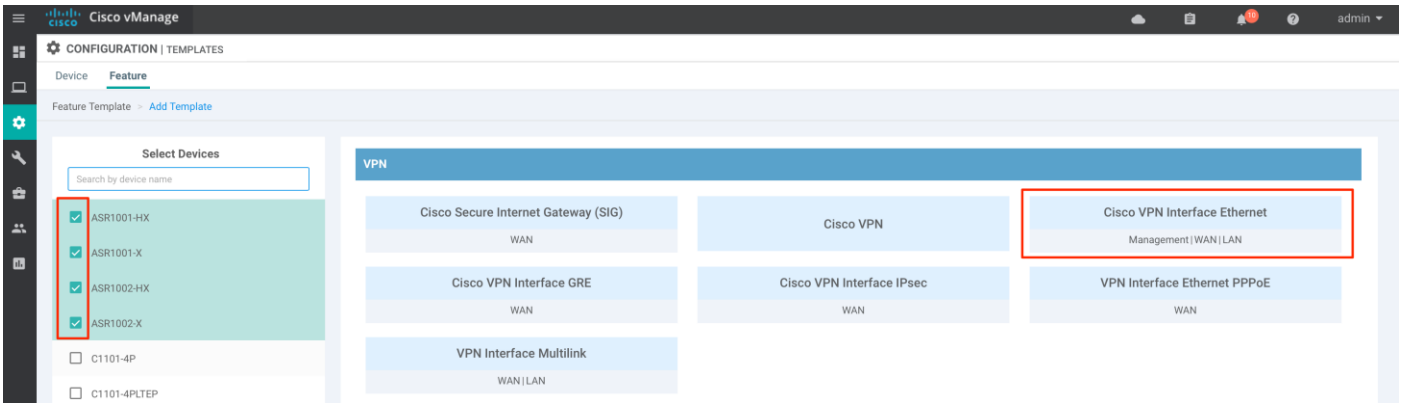
Procedure 1. Creating Interface template connecting to the LAN segment

This section details the procedure to create templates for Ethernet interface on the IOS-XE WAN Edge devices with the intent to connect to downstream LAN devices at the site.

Step 1. Login to vManage, navigate to **Configuration > Templates**, click **Feature** tab and **Add Template**



Step 2. Select the WAN Edge devices from the list and under **VPN** category, click **Cisco VPN Interface Ethernet** template



Step 3. Input **Template Name** and **Description** to reference the template**.**

Under **Basic Configuration** tab, select

Shutdown: **No**

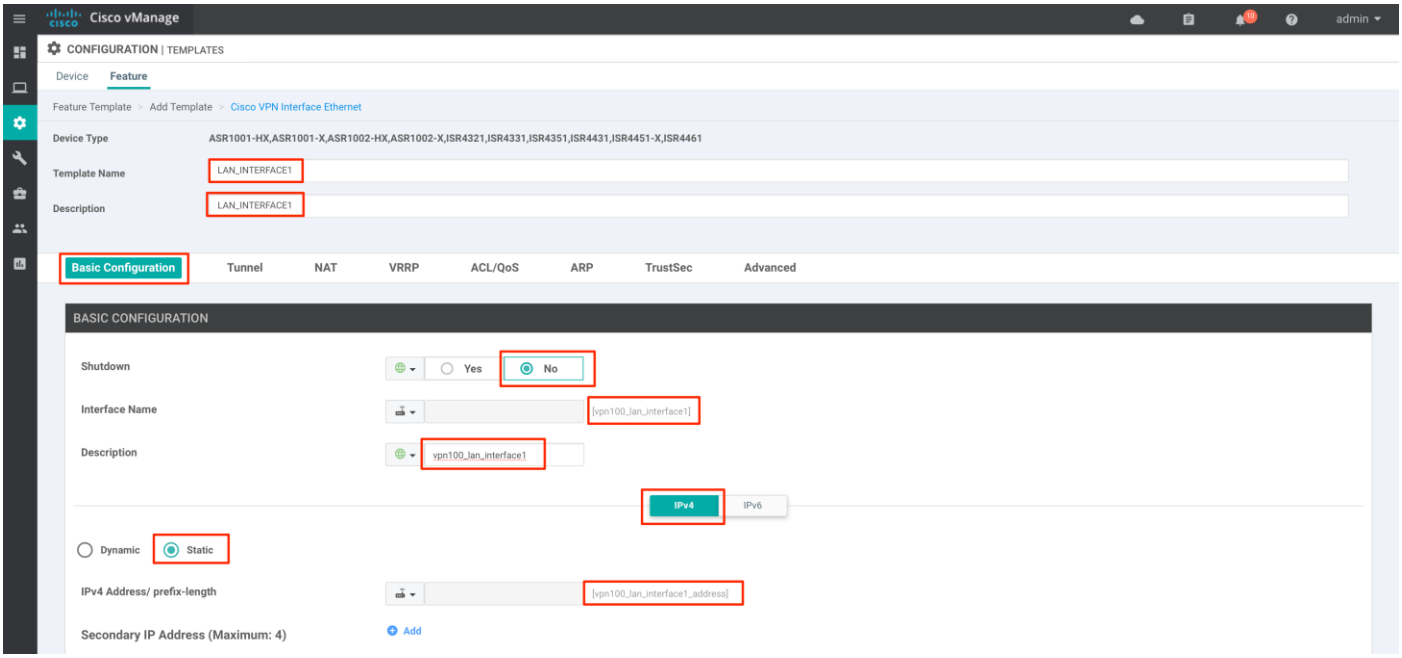
Interface Name: 'vpn100_lan_interface1'

Description: 'vpn100_lan_interface1'

Select **IPv4**

Select **Static**

IPv4 Address/prefix length: 'vpn100_lan_interface_address'

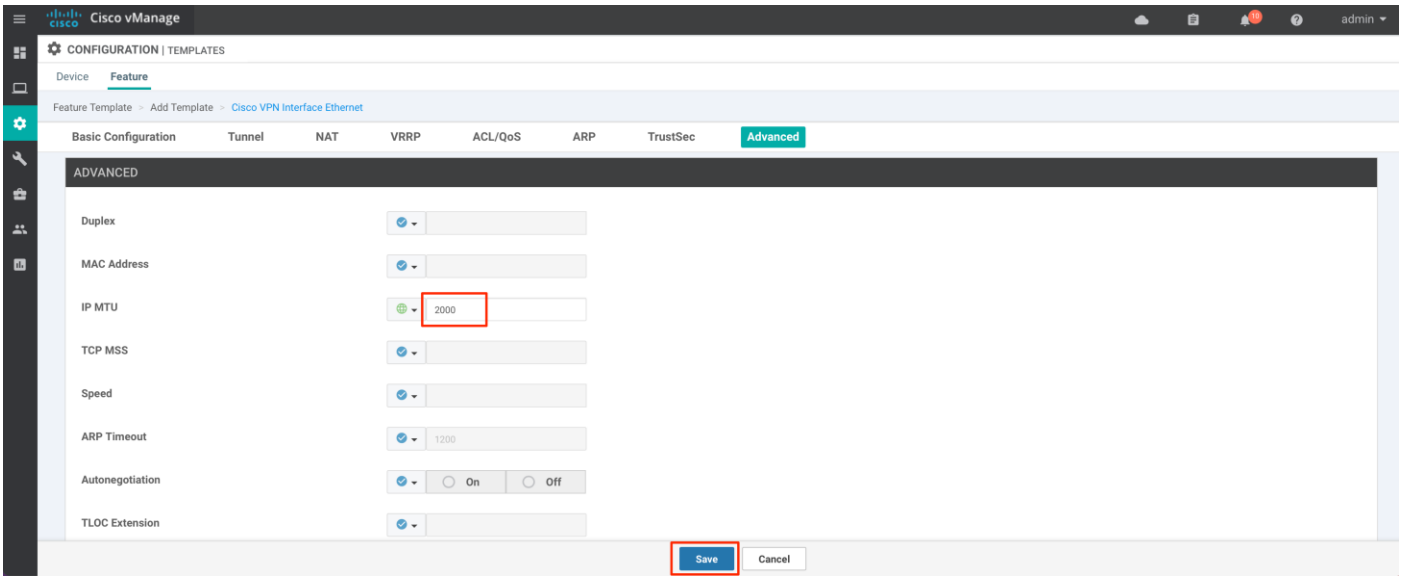


Under **Advanced** tab, input

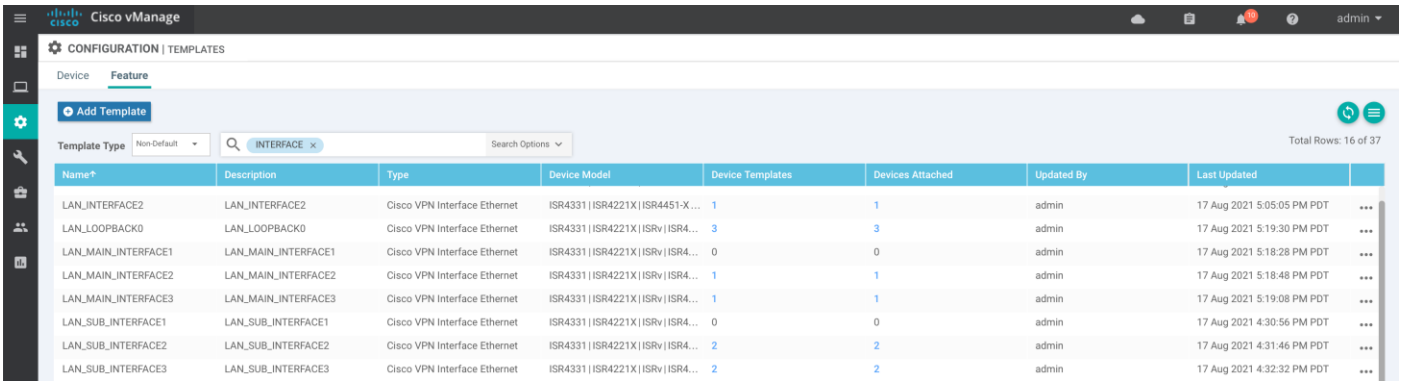
IP MTU: 2000

click **Save**

Tech tip
IP MTU for the interface connecting to the SD-Access LAN segment must be increased to more than 1550 to accommodate the VXLAN encapsulated packets. It is recommended to change the MTU size to highest supported value on the interface, which is 2000 bytes.



Step 4. Repeat this Procedure to add additional interface(s) that connects the IOS-XE WAN Edge devices to the Fabric GRT LAN segment.



Tech Tip

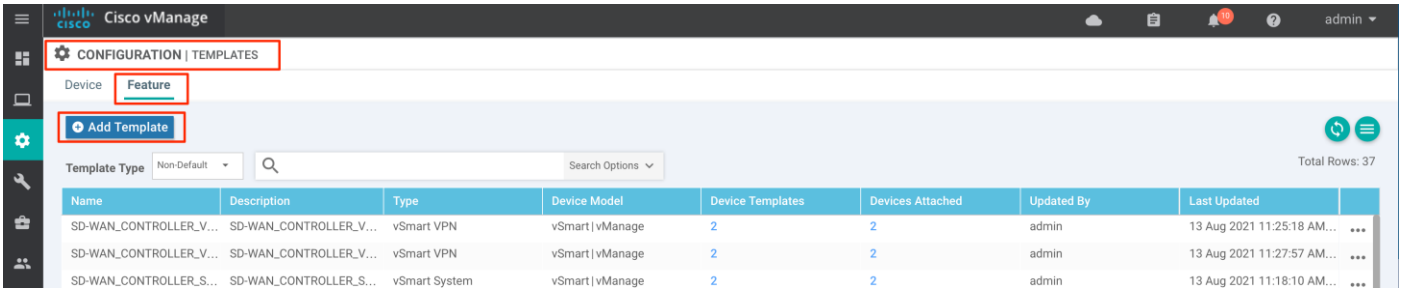
IOS-XE WAN Edge deployments with connection to peer-device, via IP-Transit, to reach the Shared-Services servers leverage sub-interfaces to accommodate Fabric GRT and overlay interface handoff. In such deployment, create the main-interface first with the **Cisco VPN Interface Ethernet** feature template and then add any additional interface template for each sub-interface with reduced IP MTU (1996) to accommodate the 4-bytes Dot1Q information.

Also, ensure all the Fabric GRT interface template are associated to the dedicated Fabric GRT Service VPN.

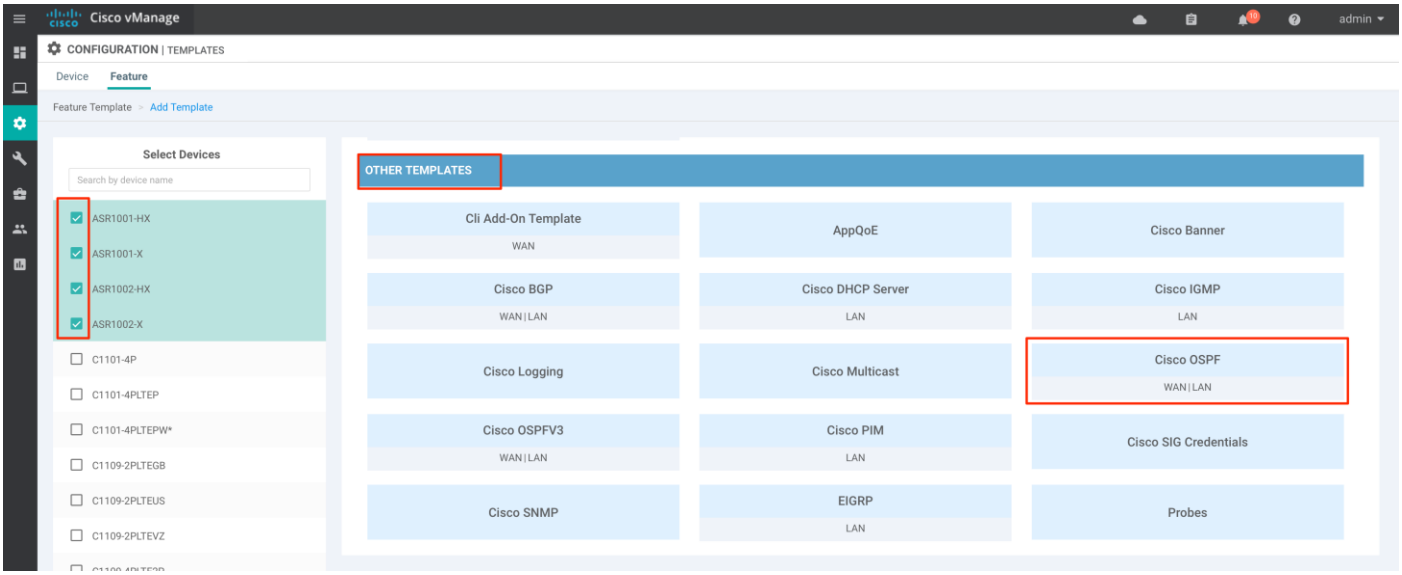
Procedure 2. Configuring routing protocol template to form LAN segment routing adjacencies

This section details the procedure to create routing protocol, OSPF, templates on the IOS-XE WAN Edge devices with the intent to form routing adjacencies to downstream LAN devices at the site.

Step 1. Login to vManage, navigate to **Configuration > Templates**, click **Feature** tab and **Add Template**



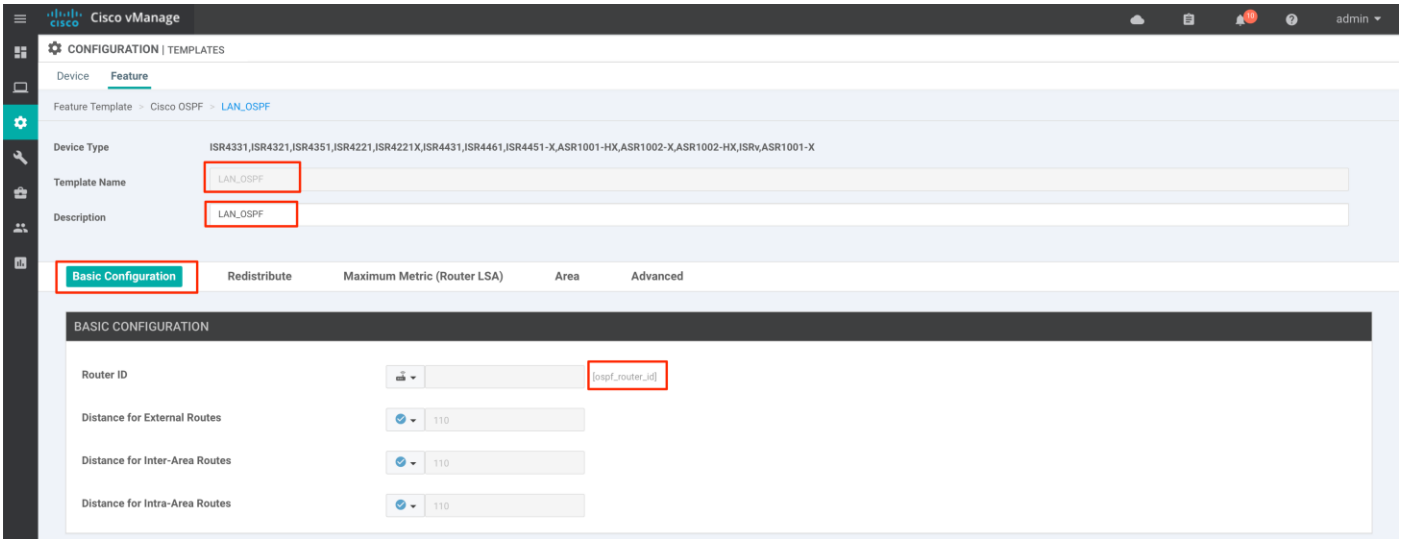
Step 2. Select the WAN Edge devices from the list and under **Other Templates** category, click **Cisco OSPF** template



Step 3. Input **Template Name** and **Description** to reference the template**.**

Under **Basic Configuration** tab, select

Router ID: 'ospf_router_id'

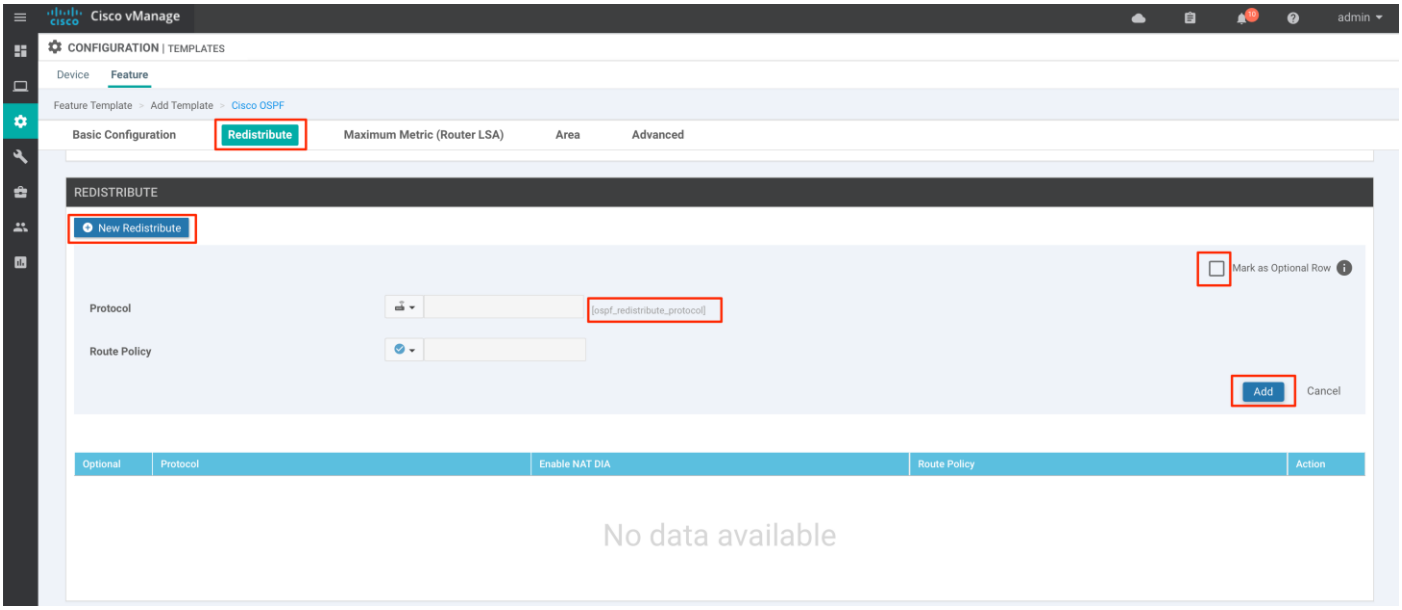


Step 4. Under **Redistribute** tab, click **New Redistribute and select**

Protocol: 'ospf_redistribute_protocol'

Enable **Mark as Optional Row**

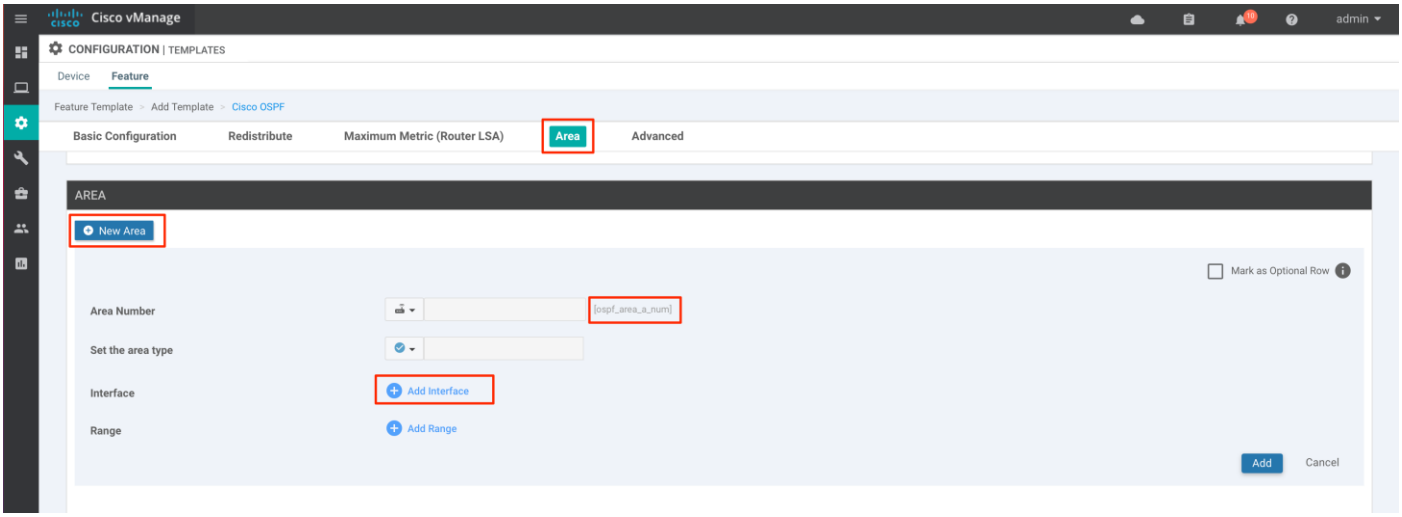
and click **Add**

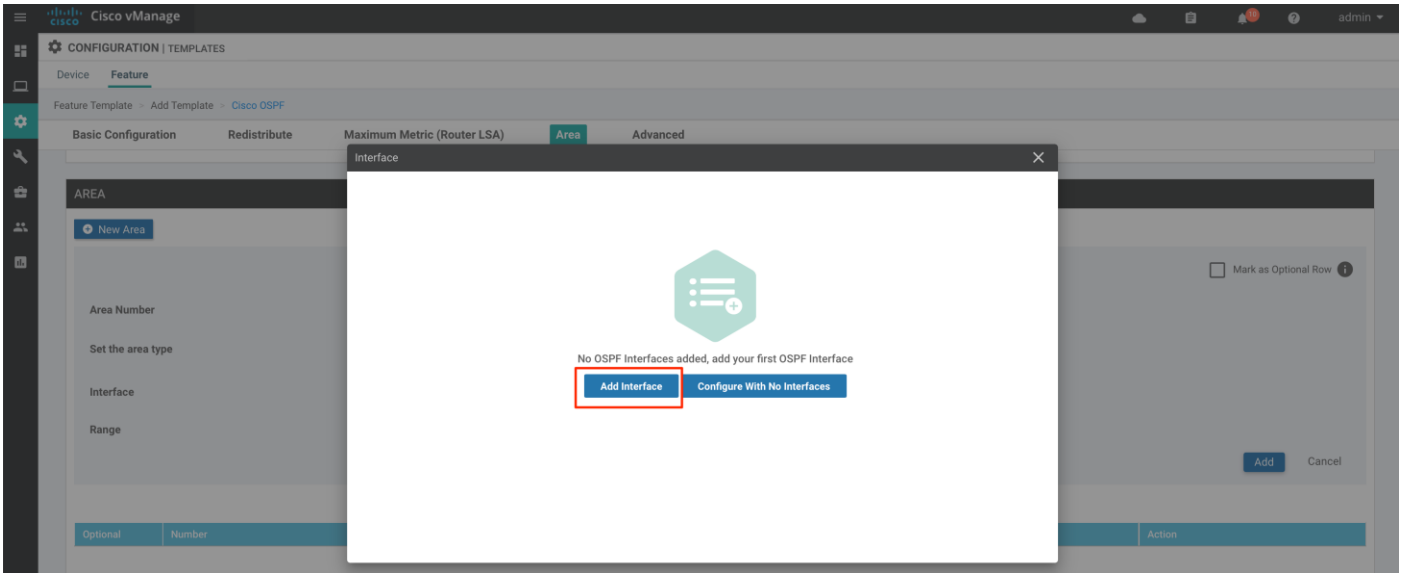


Step 5. Under **Area** tab, click **New Area** and input

Area Number: 'ospf_area_a_number'

Click **Add Interface** and click **Add Interface**

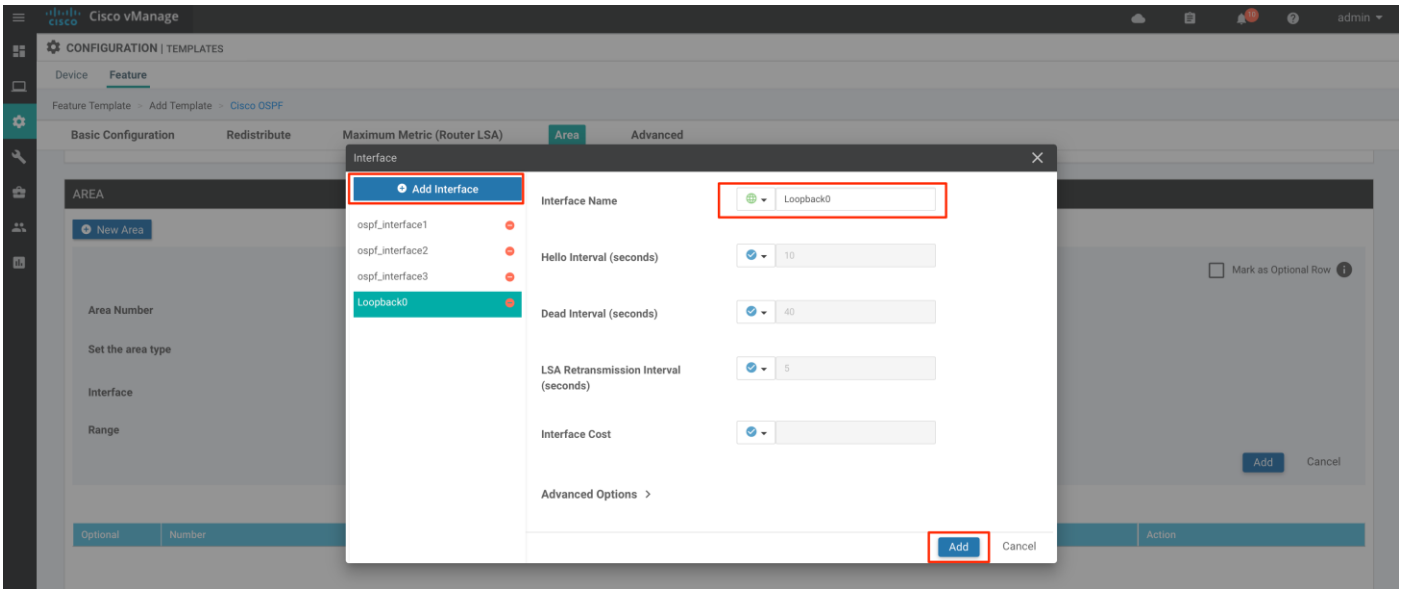




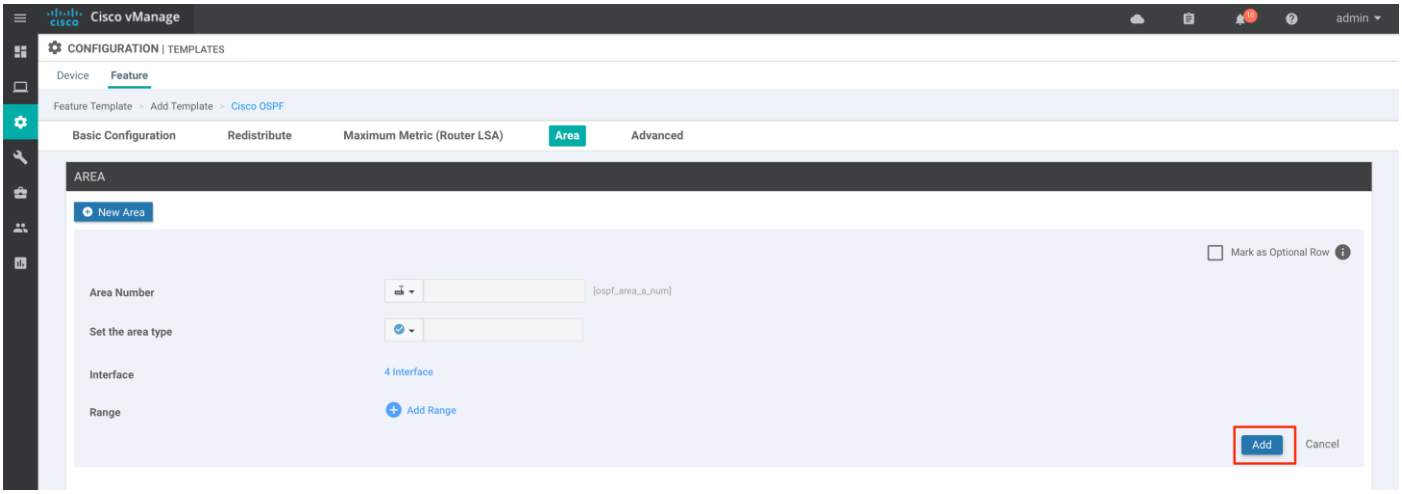
Input **Interface Name:** ‘ospf_inteface1’

Add additional interfaces as needed for the deployment by clicking **Add Interface**

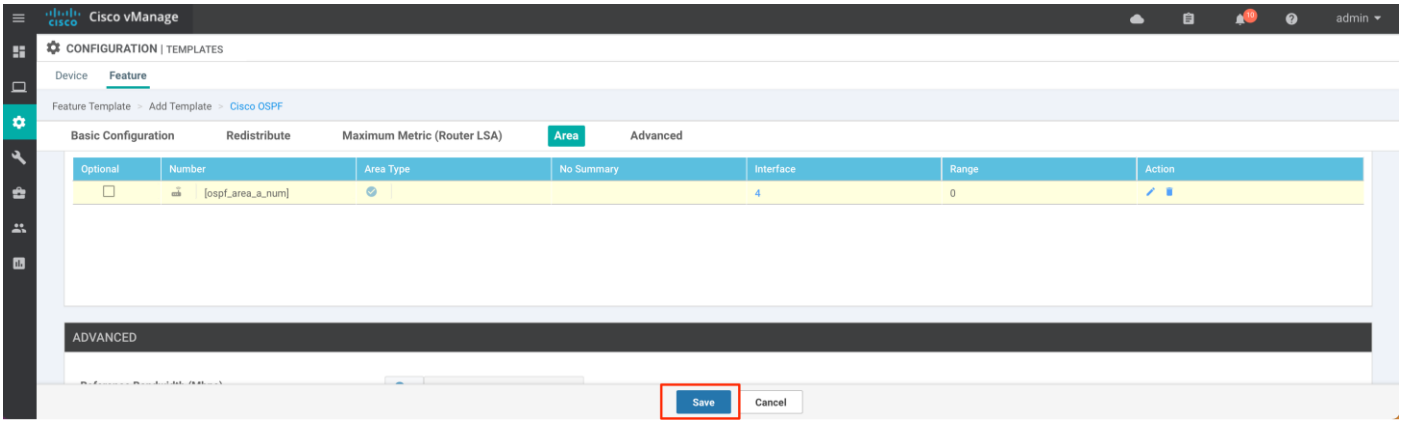
and then click **Add**

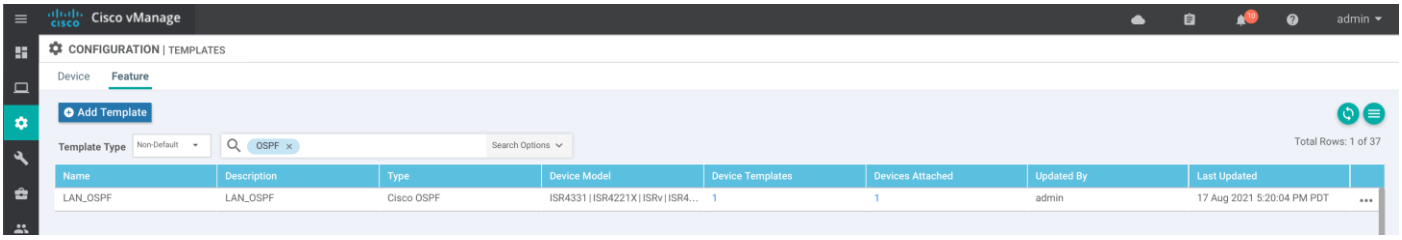


Click **Add**



Step 6. Click **Save** to save the routing protocol OSPF template

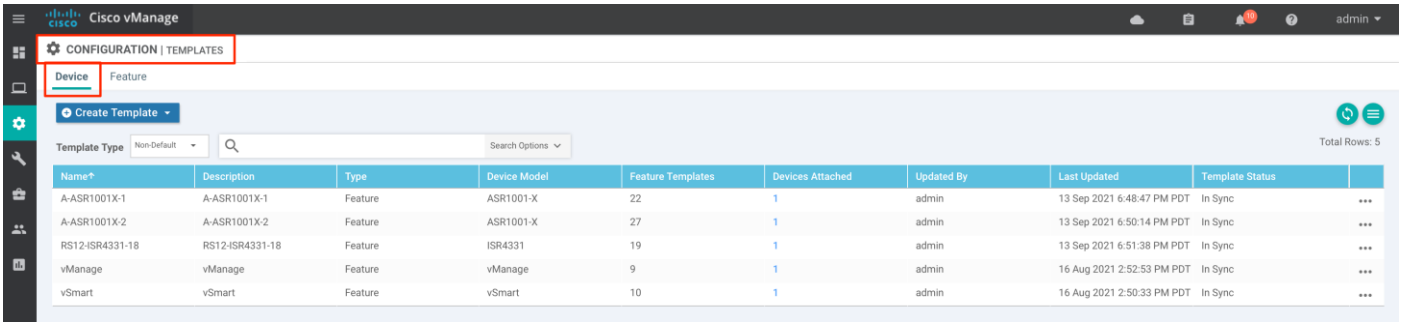




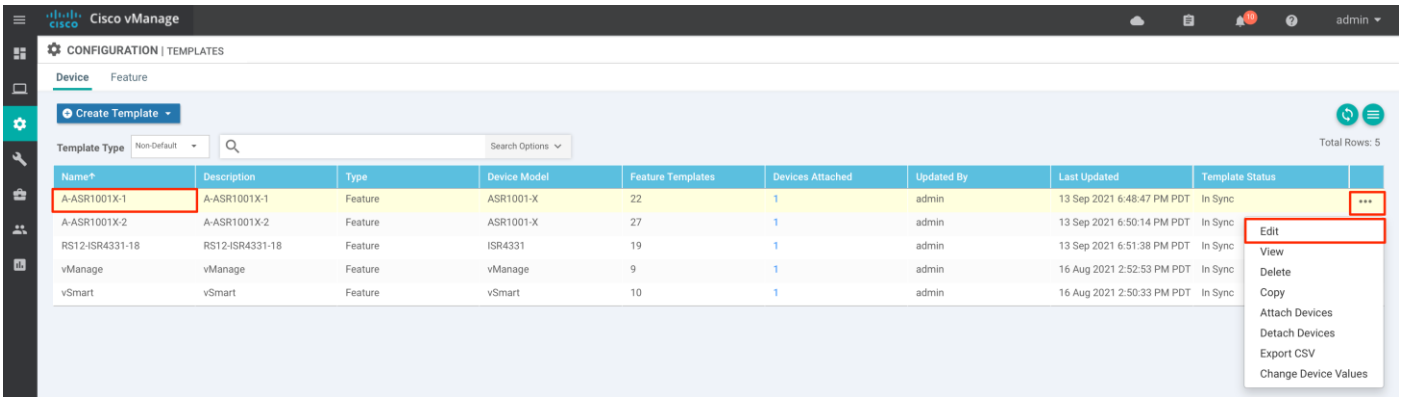
Procedure 3. Associating interface, routing protocol templates on the IOS-XE WAN Edge device

This section details the procedure to associate Cisco VPN Ethernet interface, routing protocol template with the intent to establish connectivity, establish routing adjacencies with network devices at the site and to provide end-to-end Fabric GRT connectivity across sites.

Step 1. Login to vManage, navigate to **Configuration > Templates**, click **Device** tab

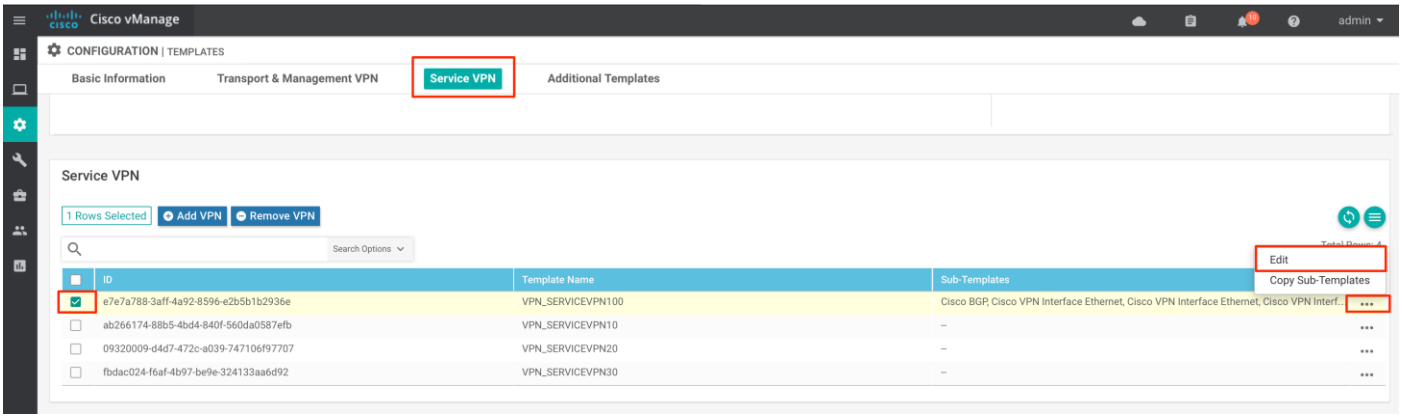


Step 2. Select the WAN Edge device from the list and click **three dots** (..) and select **Edit** from the drop-down options



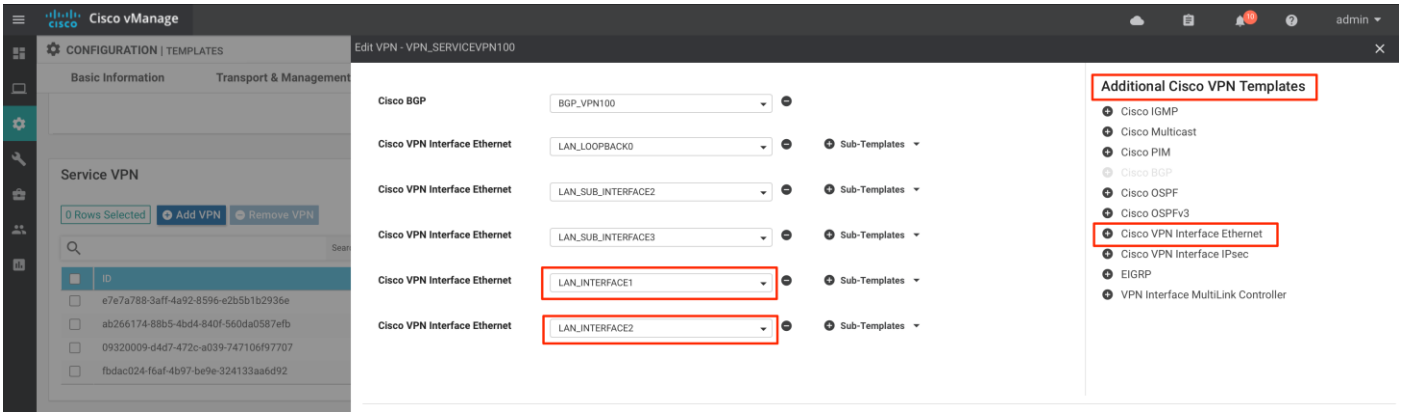
Step 3. Select **Service VPN** tab

click Fabric GRT Service **VPN** from the list and click **three dots** (…) and select **Edit** from the options



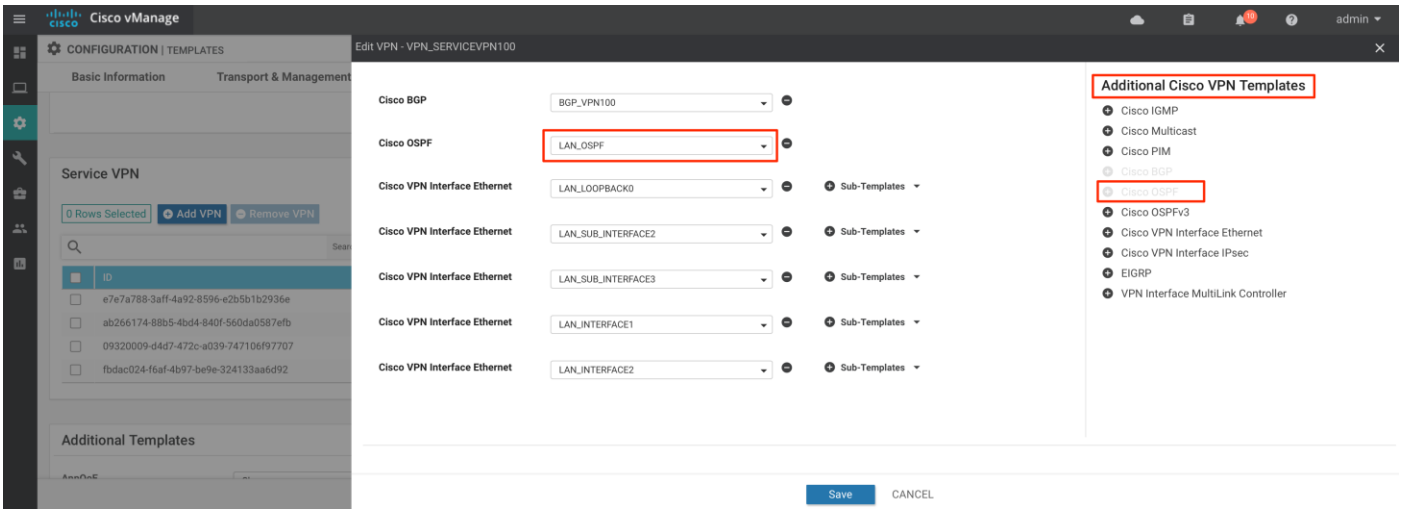
Step 4. Select interfaces that connects to the LAN segment, by selecting **Additional Cisco VPN Templates > Cisco VPN Interface Ethernet**

And select the interface template previously created.

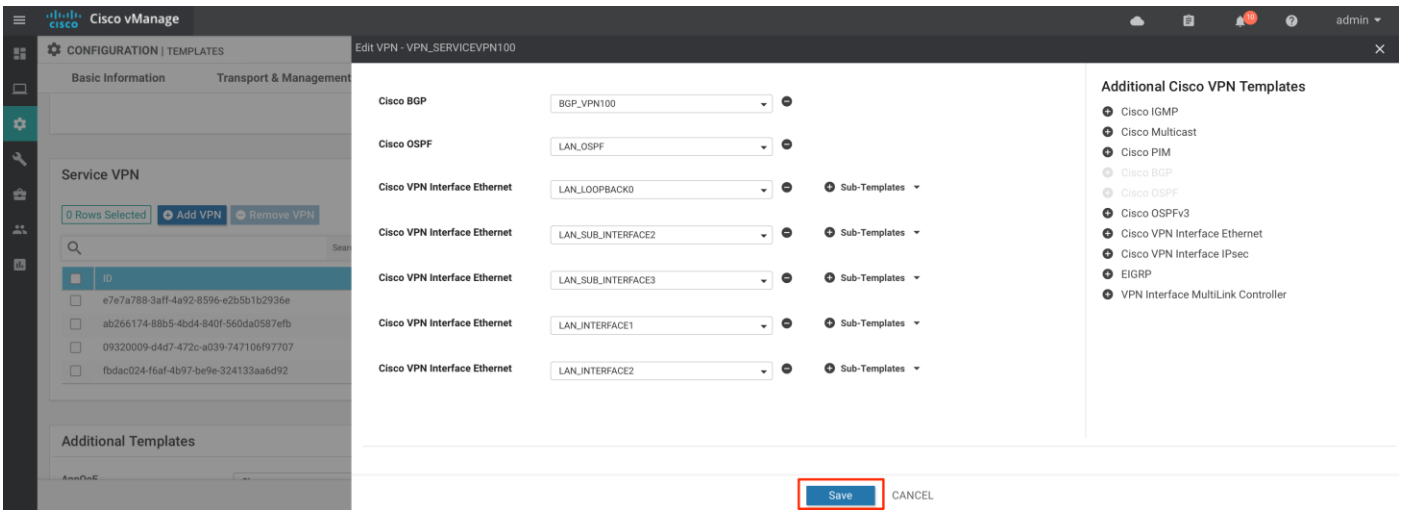


Step 5. Select routing protocol by selecting **Additional Cisco VPN Templates > Cisco OSPF**

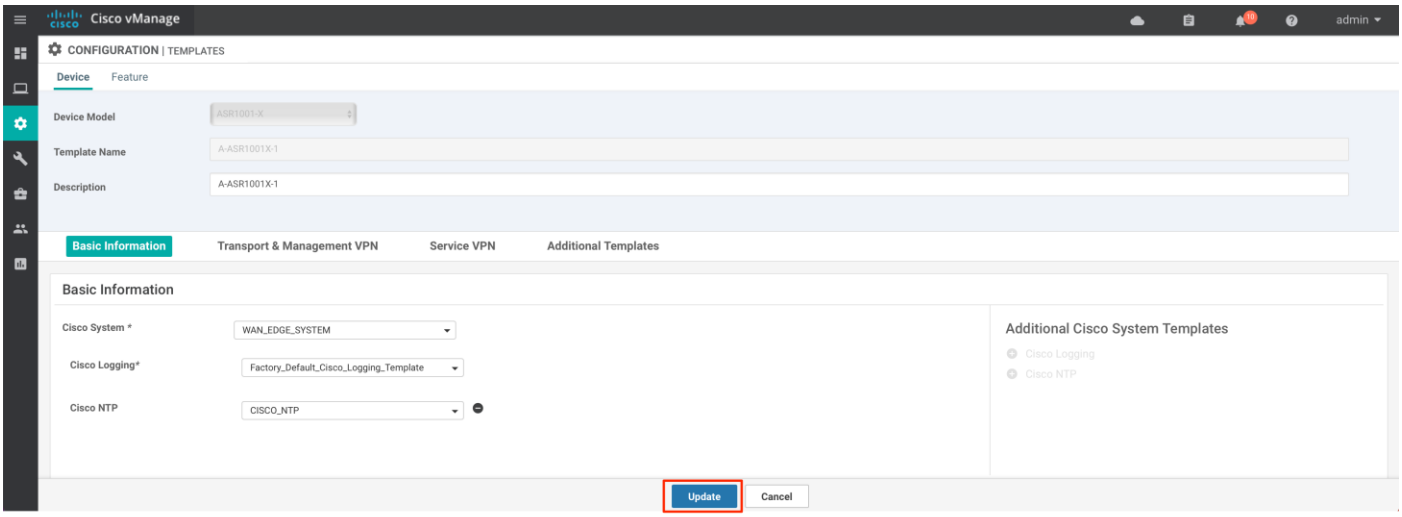
And select the routing protocol template previously created.



Step 6. Click **Save**.

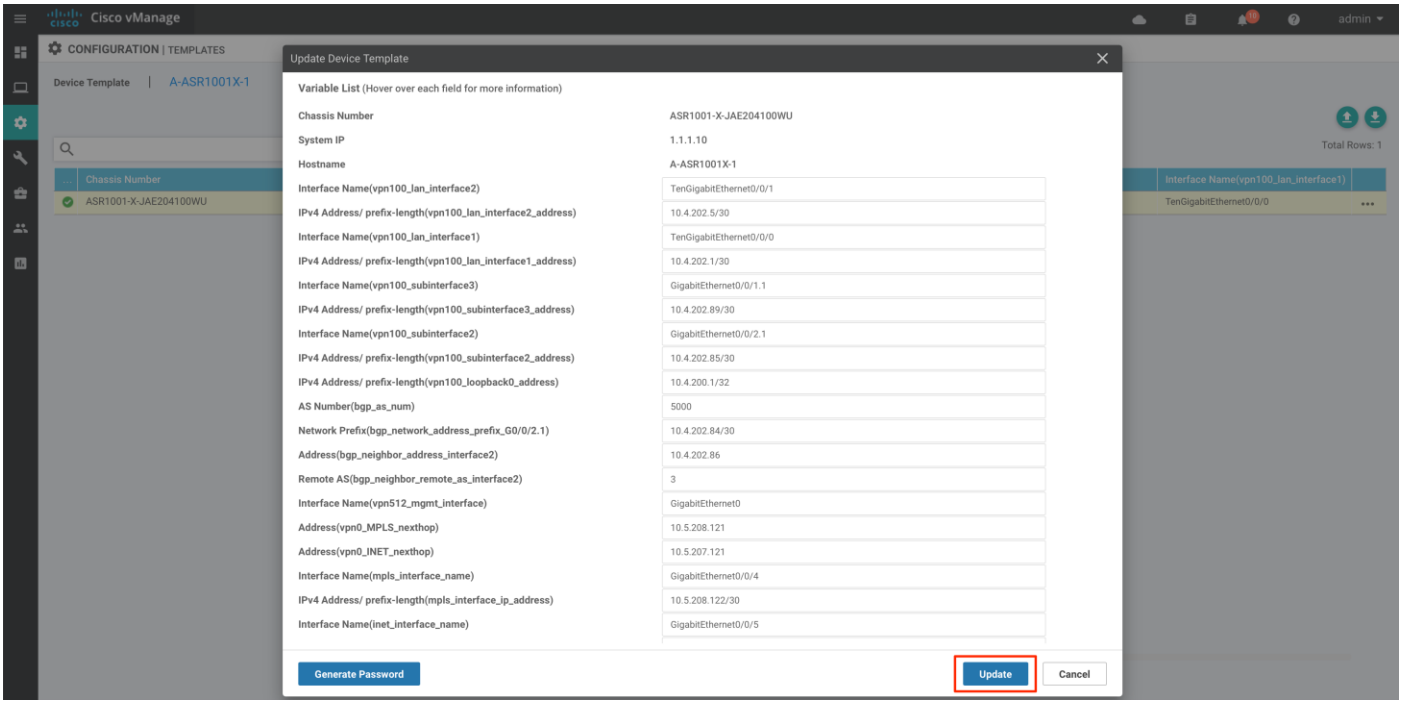


Step 7. Click **Update** to associate the templates to the WAN Edge device

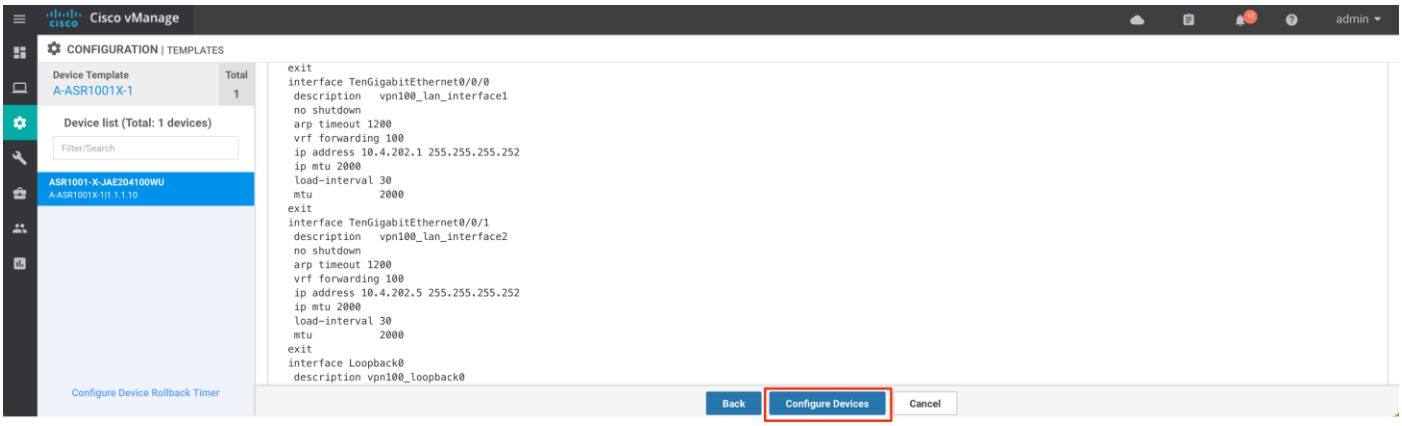


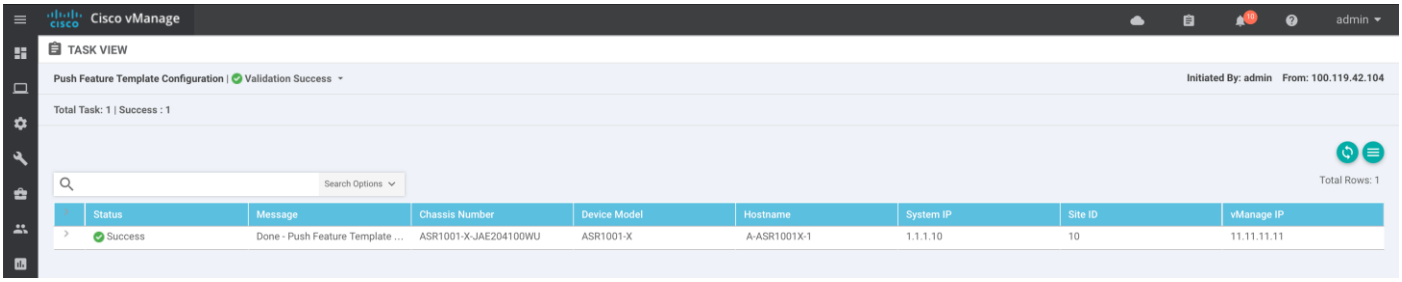
Step 8. Input values to device-specific variables, by clicking the **three dots** (…) and choose **Edit Device Template**

And click **Update**

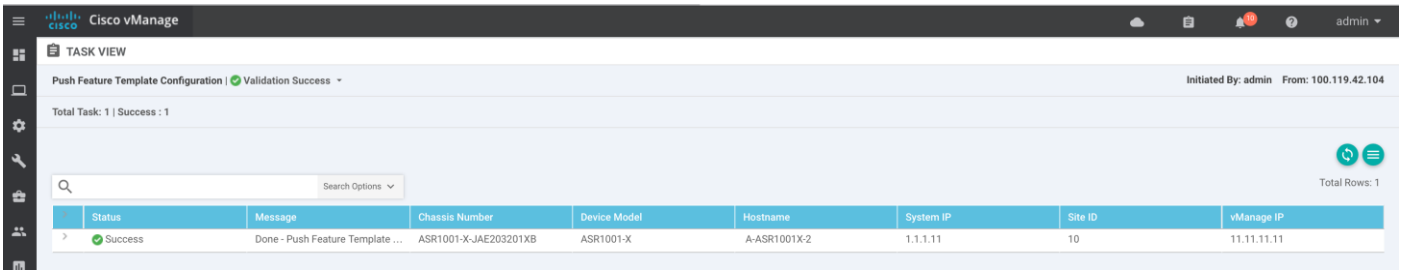


Step 9. Click **Next** and **Configure Devices**





Step 10. Repeat steps in this **Procedure** to establish resilient, highly available Fabric GRT connectivity on each IOS-XE WAN Edge device



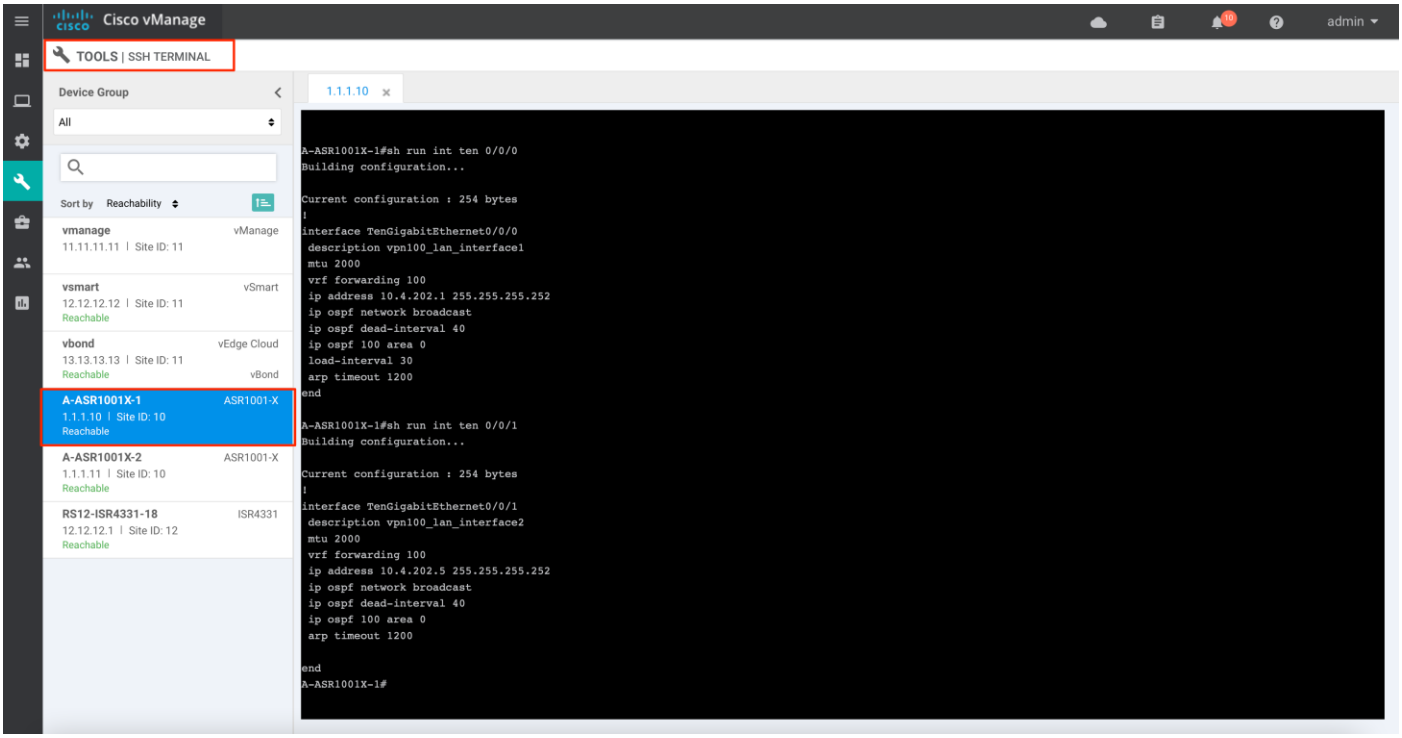
Step 11. Verify the Fabric GRT connectivity to the downstream devices

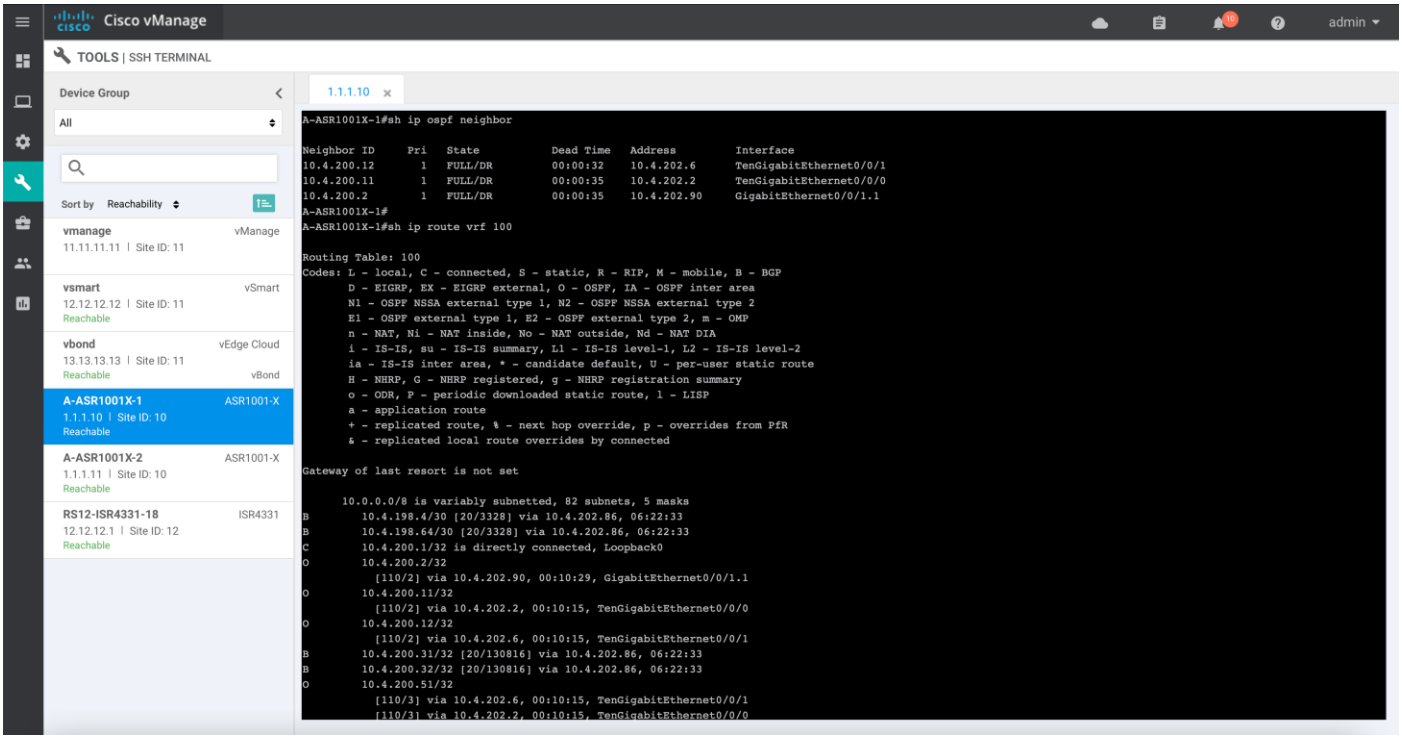
In vManage, navigate to **Tools > SSH Terminal**, select the WAN Edge device from the list. Login with the device credentials and execute the below command

'show run int <interface name>'

'show ip ospf neighbor'

'show ip route vrf <Fabric GRT Service VPN>'



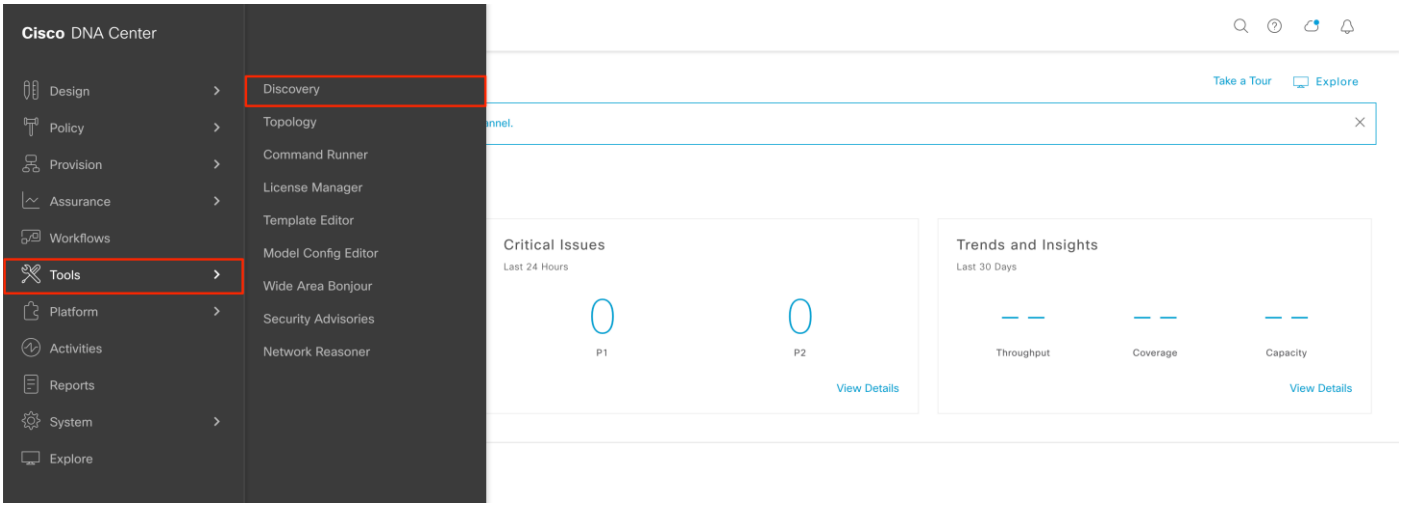


Procedure 4. Discover and Provision the network devices to a site

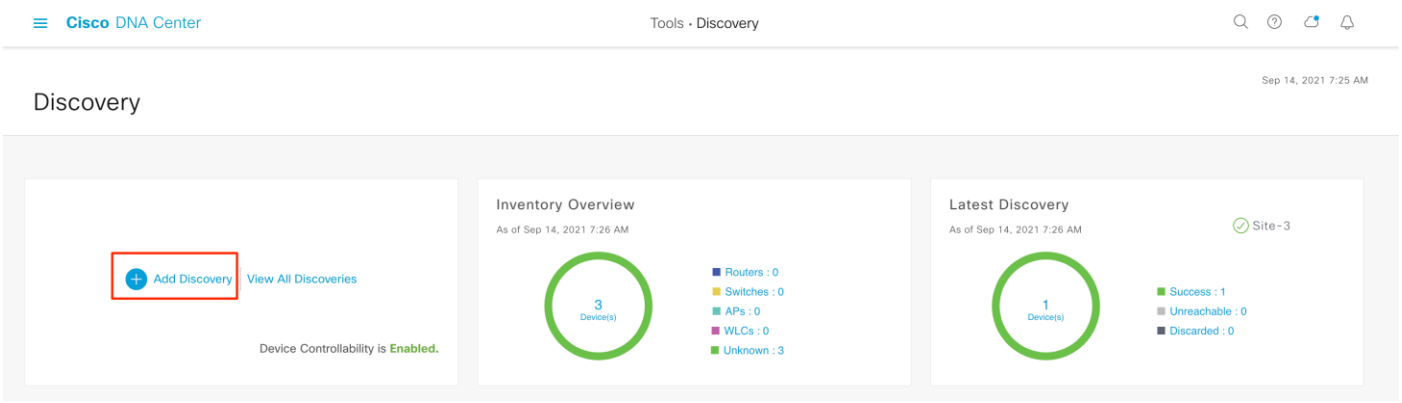
This section details the procedure to discover, provision the switches to a site with the intent to build Fabric GRT and prepare network devices to build Cisco SD-Access network.

Please refer Cisco SD-Access Design Guide for design recommendation band deployment best-practices to build resilient Fabric GRT network for Cisco SD-Access fabric site.

Step 1. In Cisco DNA Center, navigate to **Tools > Discovery**



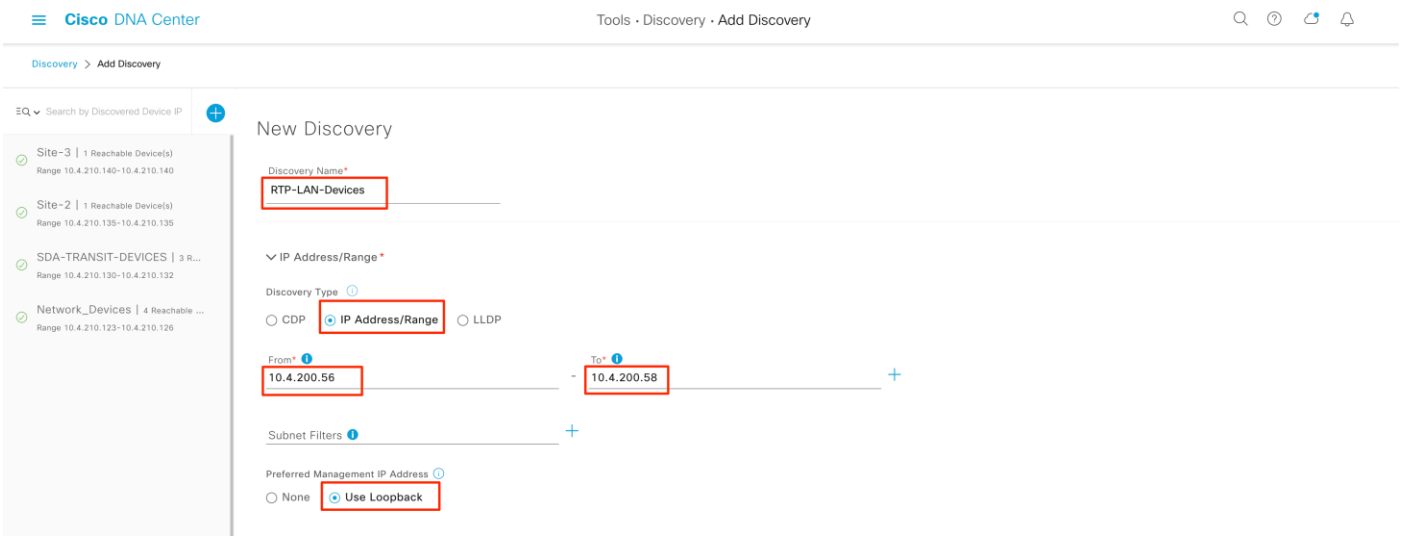
Step 2. Click Add **Discovery**



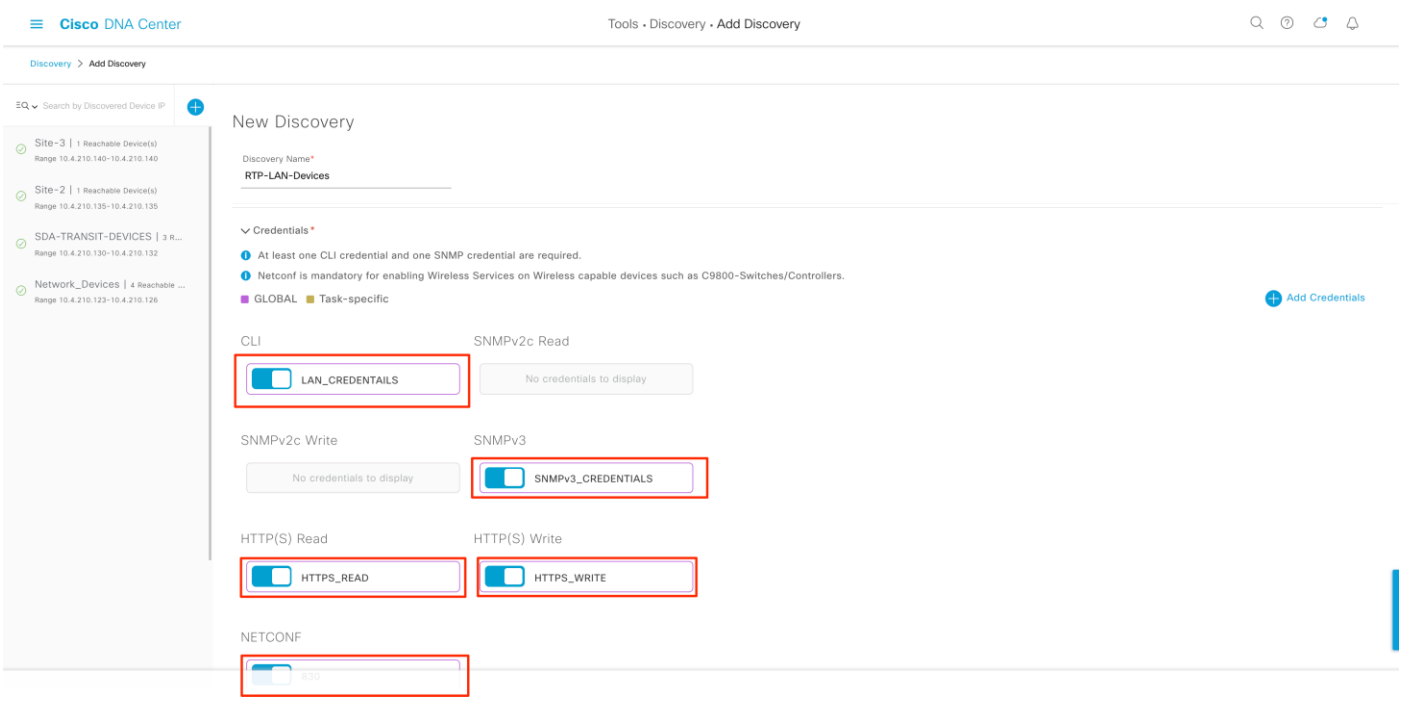
Step 3. Input **Discovery Name**

Select **Discovery Type: IP Address/Rage** and input IP Address of the devise to be discovered

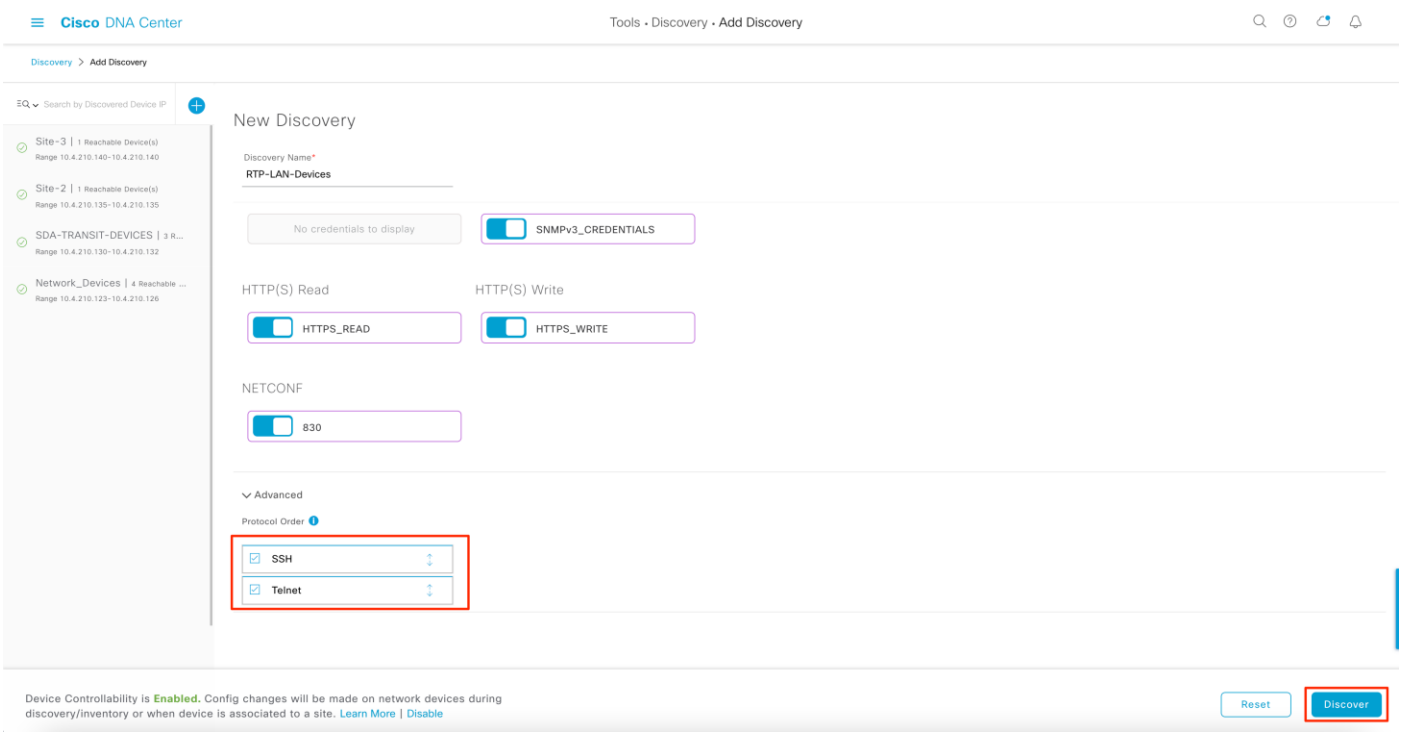
Select **Preferred Management IP Address: Use Loopback**



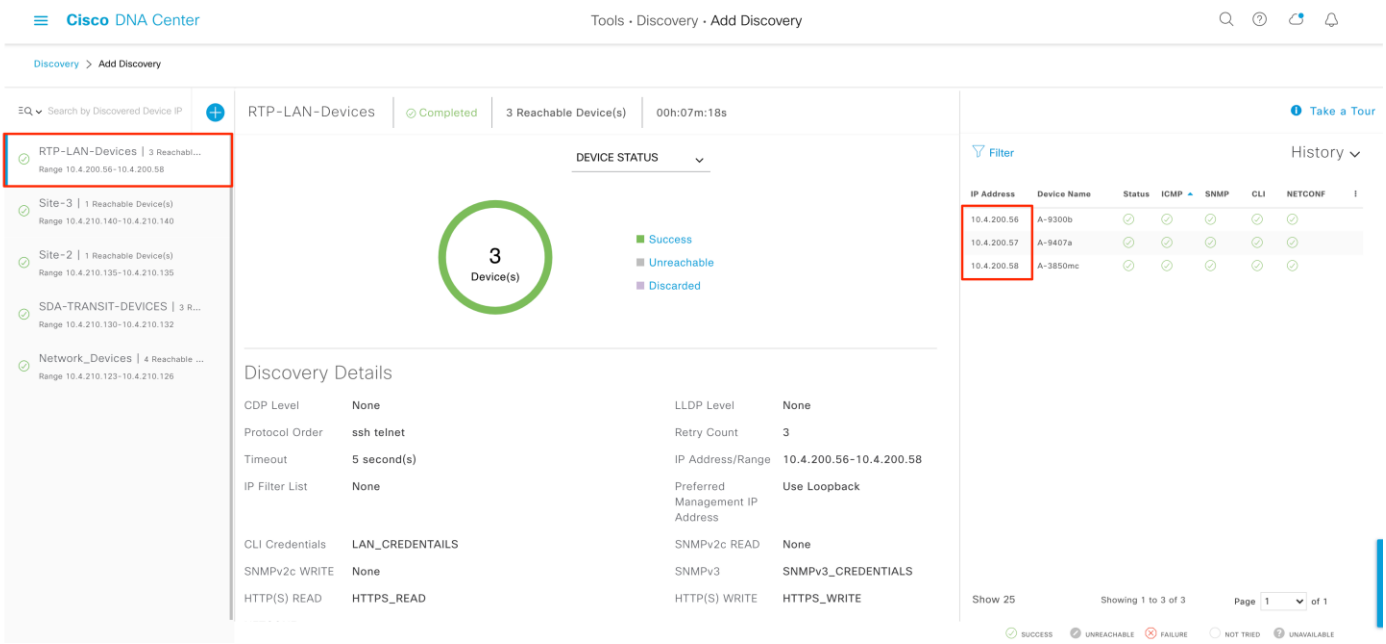
Under **Credentials** > select **CLI, SNMPv3, HTTP(s) Read, HTTP(s) Write, NETCONF** parameters



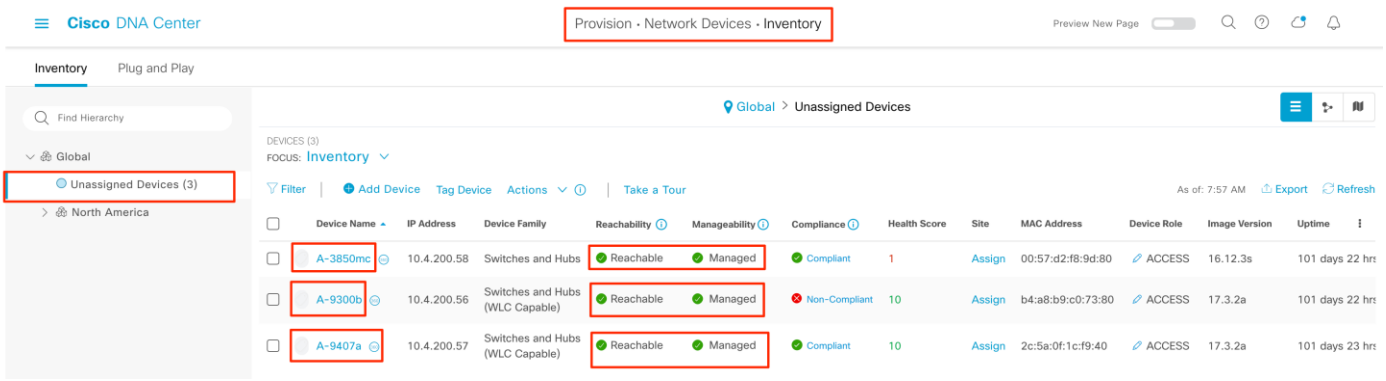
Step 4. Under Advanced > Protocol Order, select SSH, Telnet click **Discover**



Step 5. Verify the network devices are successfully discovered in Cisco DNA Center



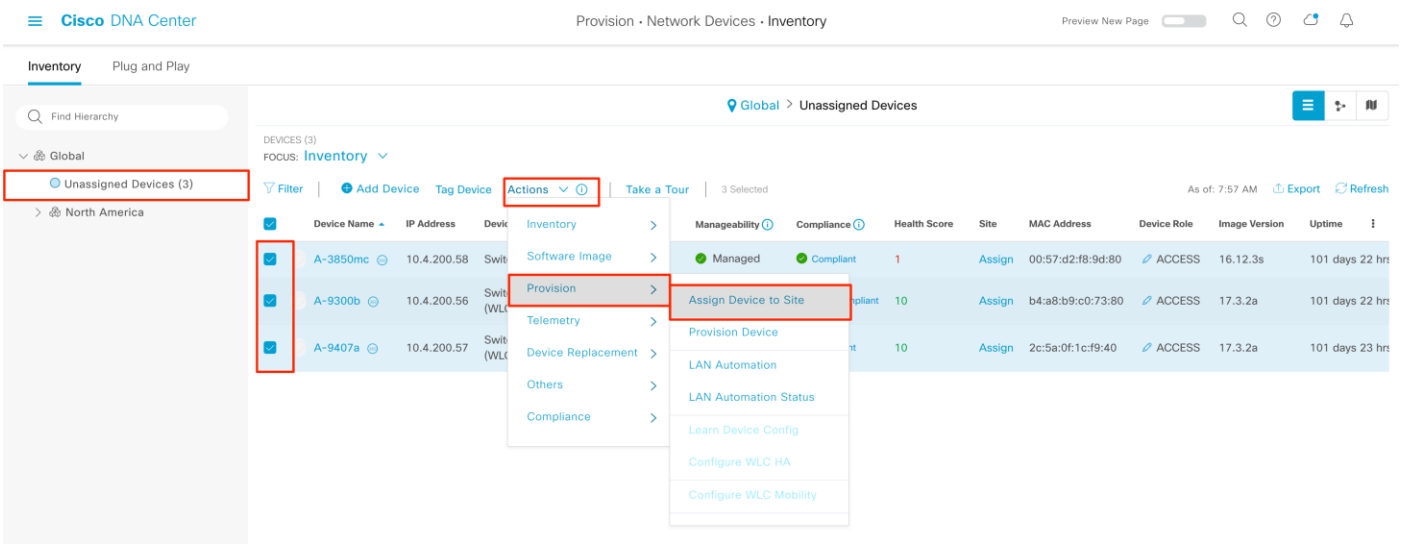
Step 6. Verify the network devices are in **Provision> Network Devices > Inventory > Unassigned Devices** hierarchy and devices are **Reachable** and in **Managed** state



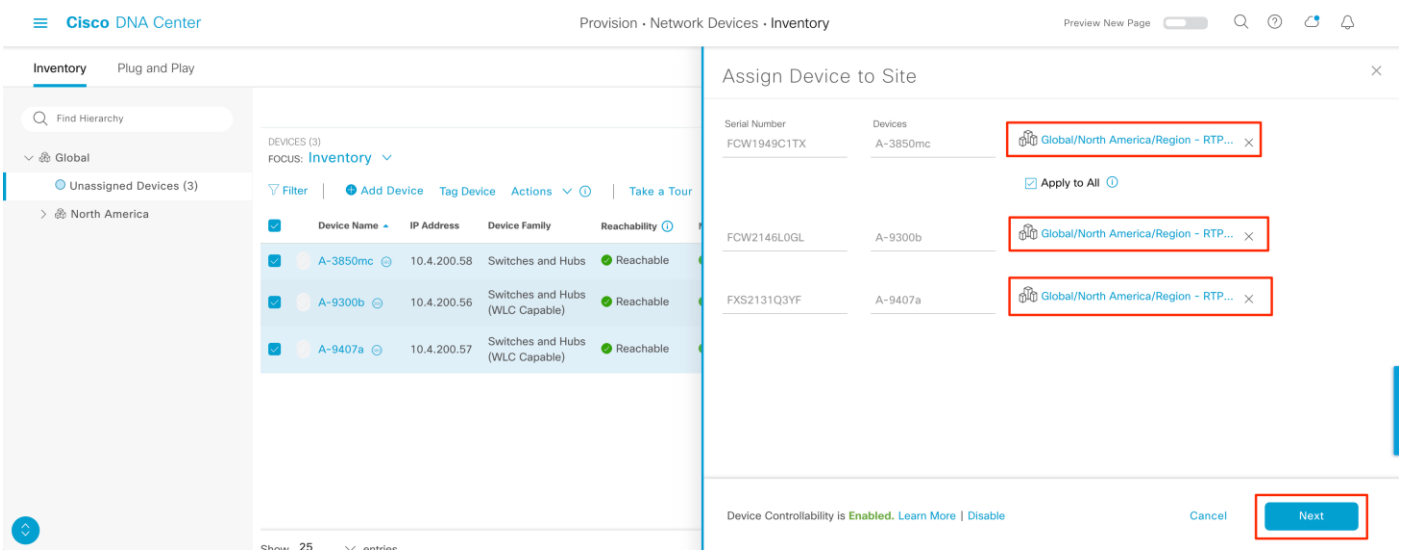
Step 7. Assign network devices to appropriate site.

Select network devices from the **Unassigned Devices** list

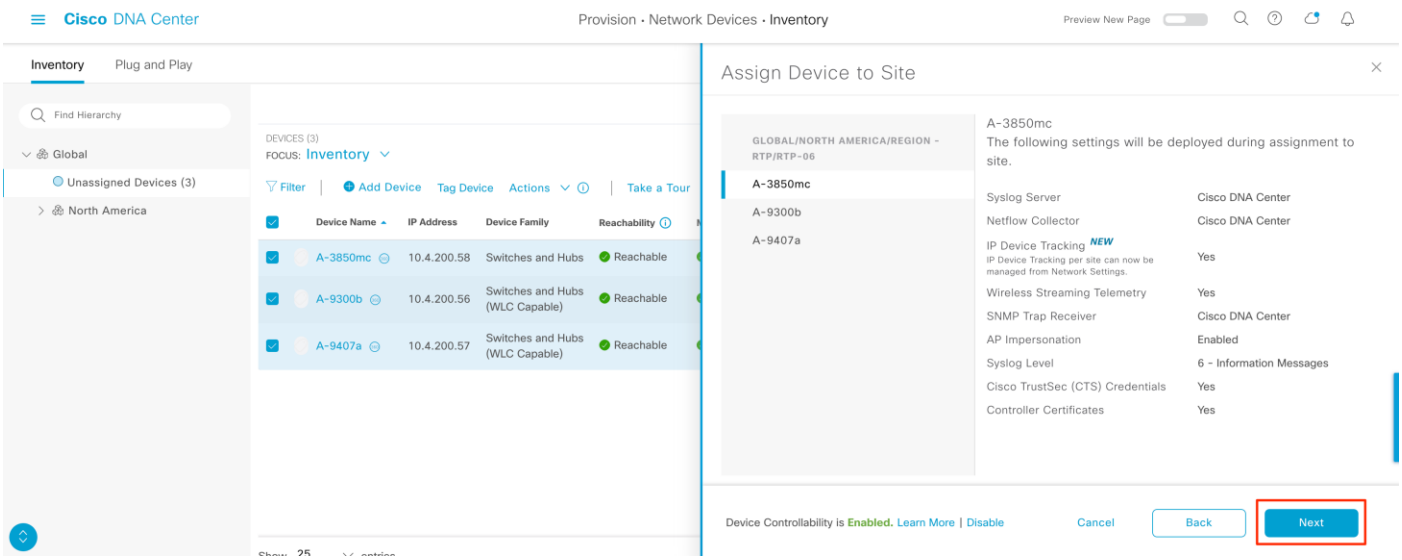
click **Actions > Provision > Assign Device to Site**



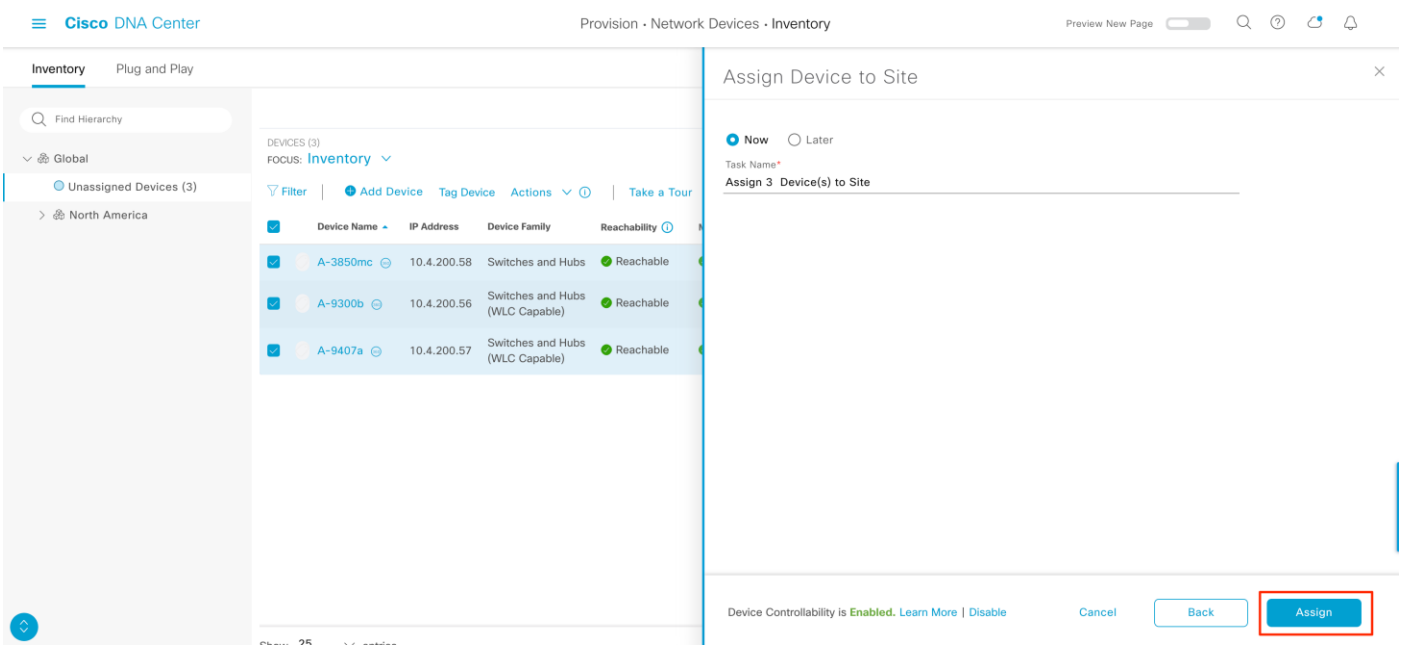
Choose the site for each device in the list and select **Next**



View the parameters that gets provisioned to the device and select **Next**

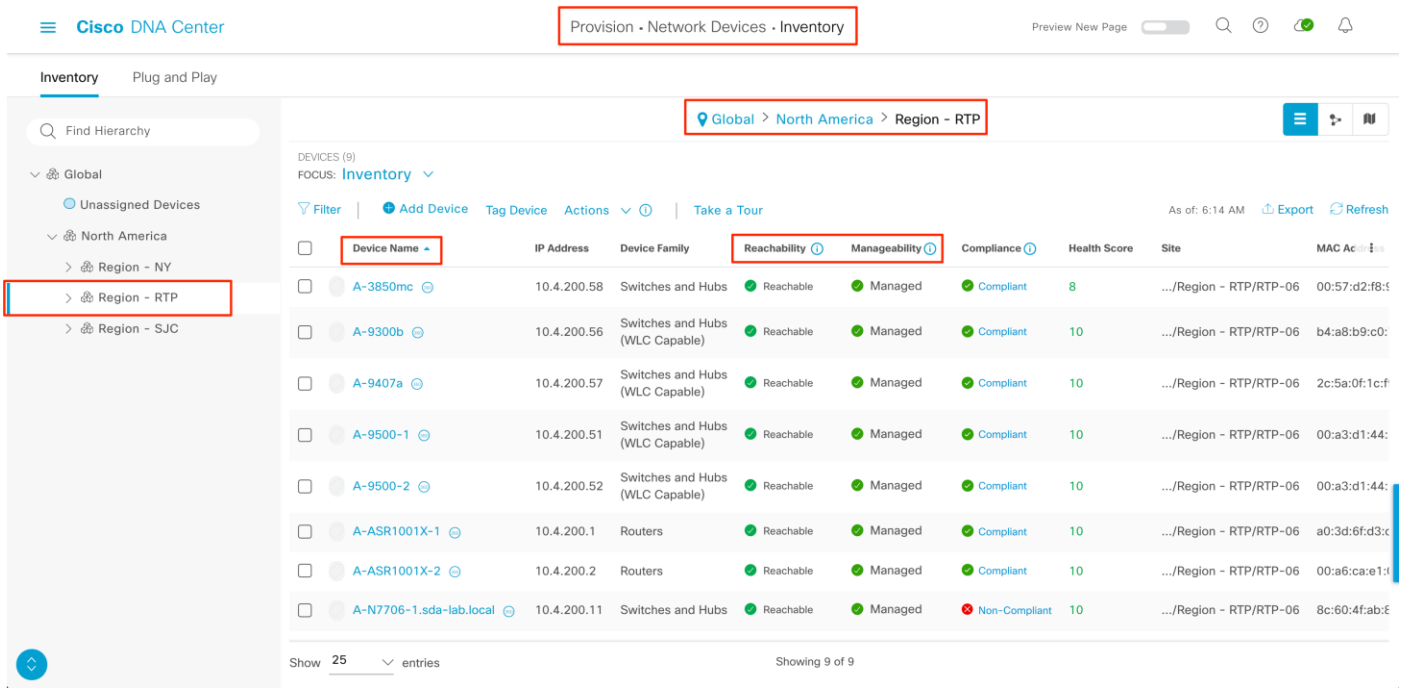


Click **Assign**



Step 8. Navigate to appropriate site **Hierarchy** and view the devices are assigned to the site.

Ensure the network devices are **Reachable** and in **Managed** state



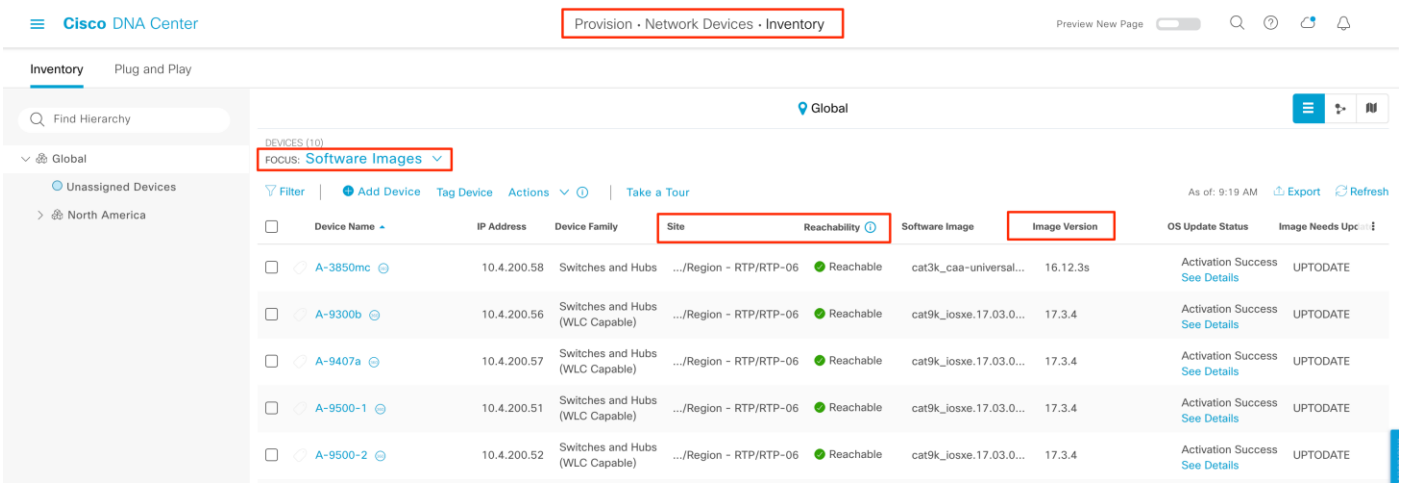
Step 9. If required, upgrade network device image.

Tech Tip

For network devices that require Image upgrade, refer to detailed steps documented in Campus Software Image Management (SWIM) using Cisco DNA Center Deployment Guide.

Image Management of IOS-XE SD-WAN WAN Edge devices is managed in SD-WAN vManage Controller, refer to detailed steps documented in 'Appendix B - Upgrading software on SD-WAN device' in Cisco SD-WAN:WAN Edge Onboarding Prescriptive Deployment Guide

Software Recommendation and Image location are available at Cisco Software-Defined Access Compatibility Matrix.

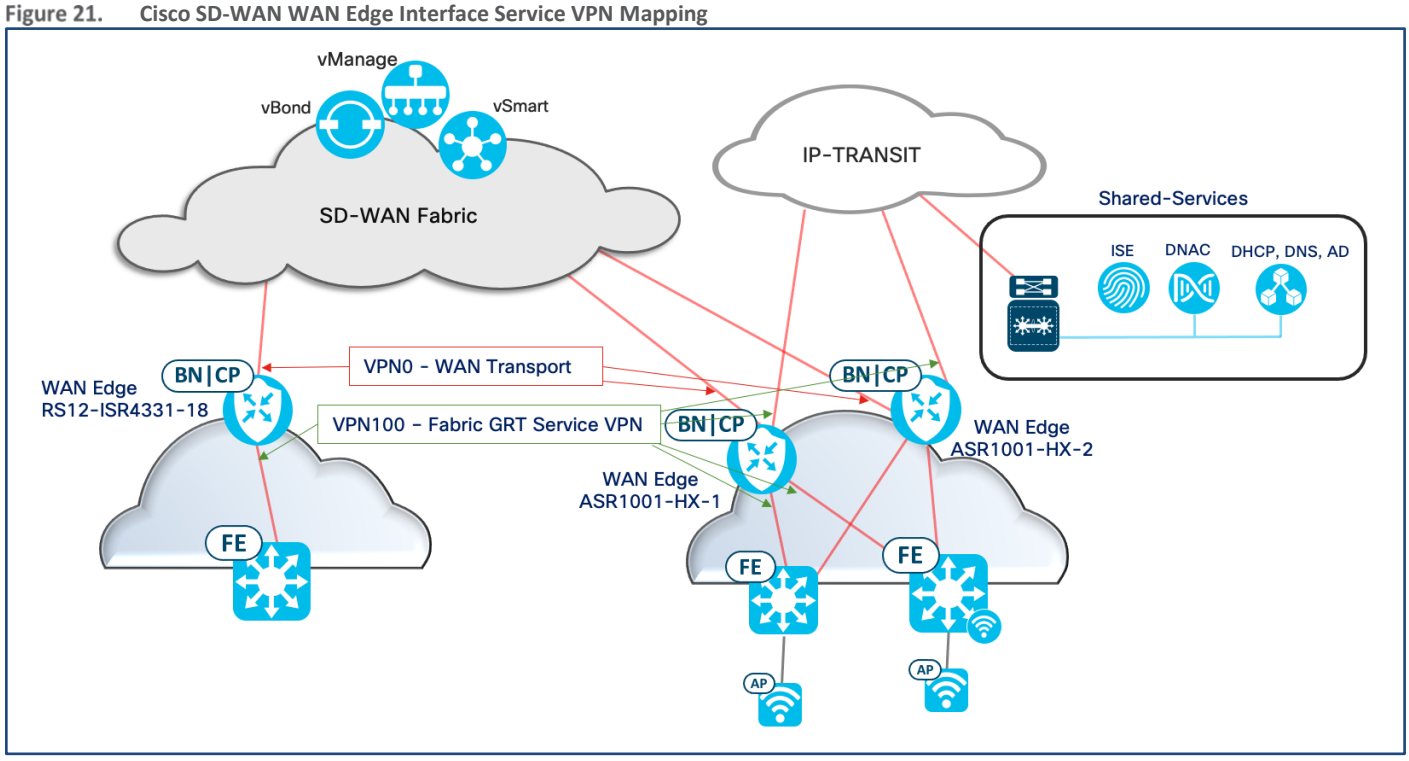


Process 5: Configuring LAN Segment with LAN Automation

This section of the deployment guide provides detailed steps to automate the LAN segment with LAN Automation, with the intent to build Fabric GRT reachability across sites. In this guide, we will leverage ISR4331 as seed device and onboard 9300 switch.

WAN Edge device connectivity to LAN and WAN segment over different Service VPN

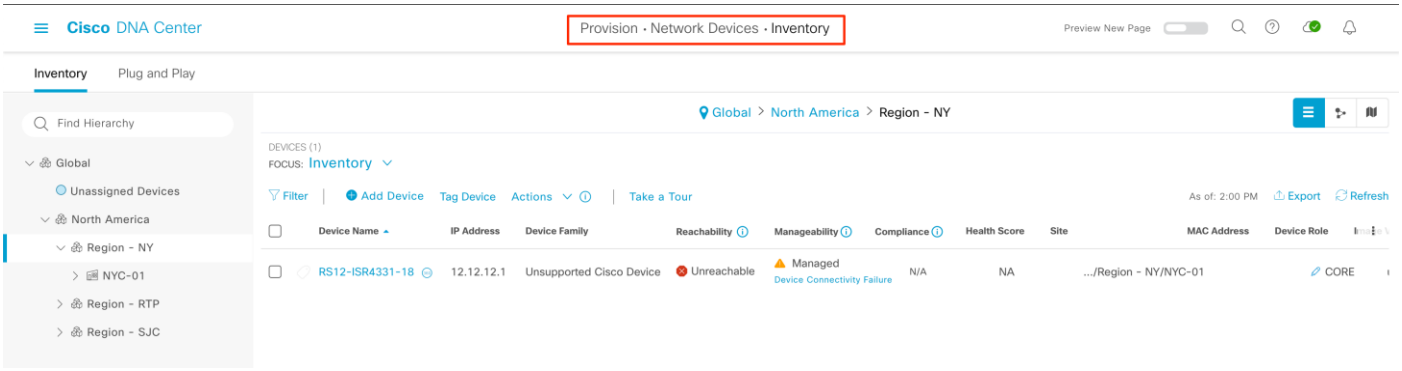
Figure 21. Cisco SD-WAN WAN Edge Interface Service VPN Mapping



Procedure 1. Initiate LAN Automation

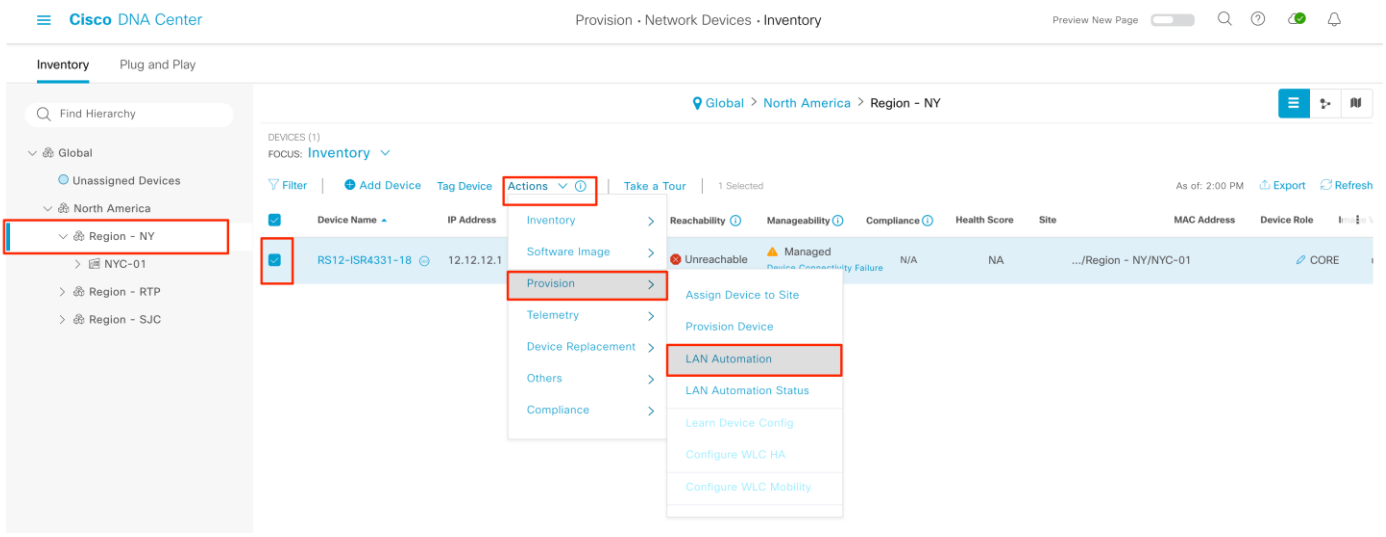
This section details the procedure to configure IOS-XE WAN Edge as seed device and discover network devices with the intent to build fabric site Fabric GRT connectivity.

Step 1. In Cisco DNA Center, navigate to **Provision > Network Devices > Inventory**



Step 2. Click the **Hierarchy** from the left panel, select the **WAN Edge** devices from the list of devices.

Click **Actions > Provision > LAN Automation** navigate to appropriate site



Step 3. In the slide-out **LAN Automation** page:

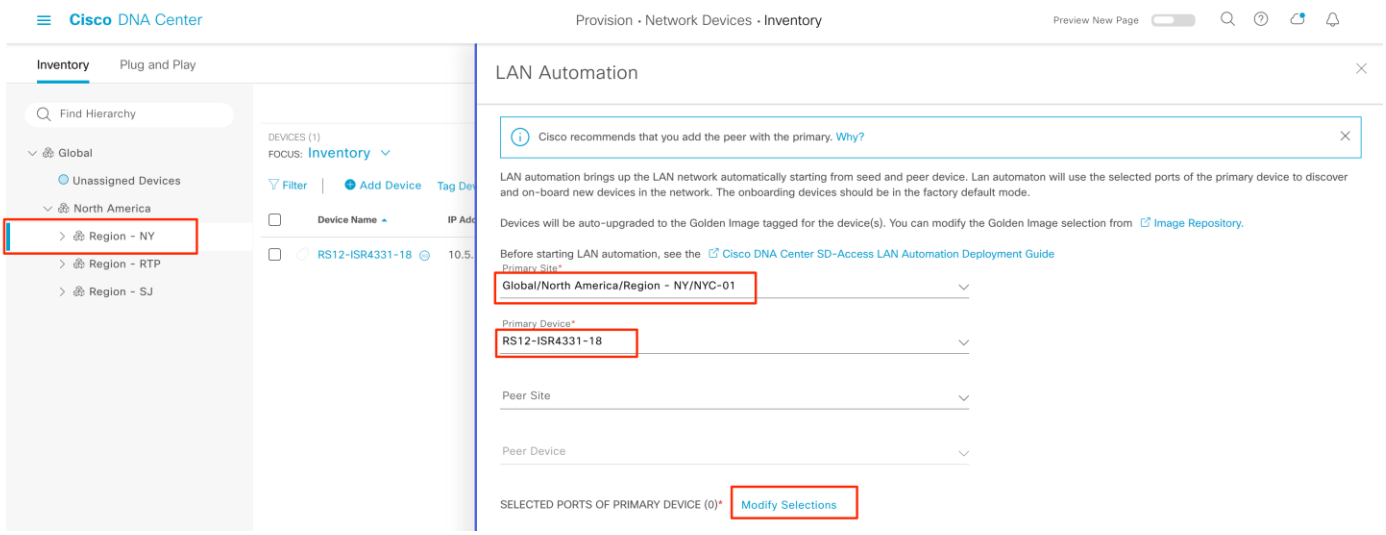
Select **Primary Site**

Select the **Primary Device**

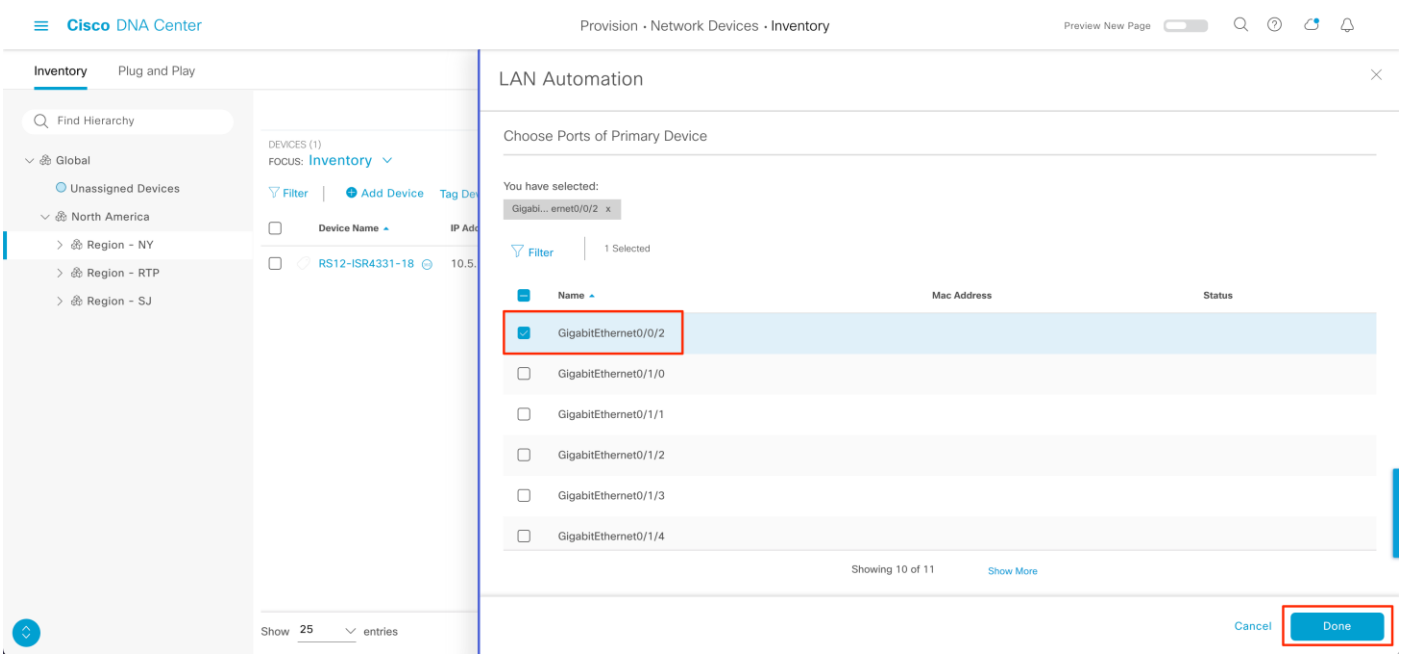
Select the **Peer Site** (if available)

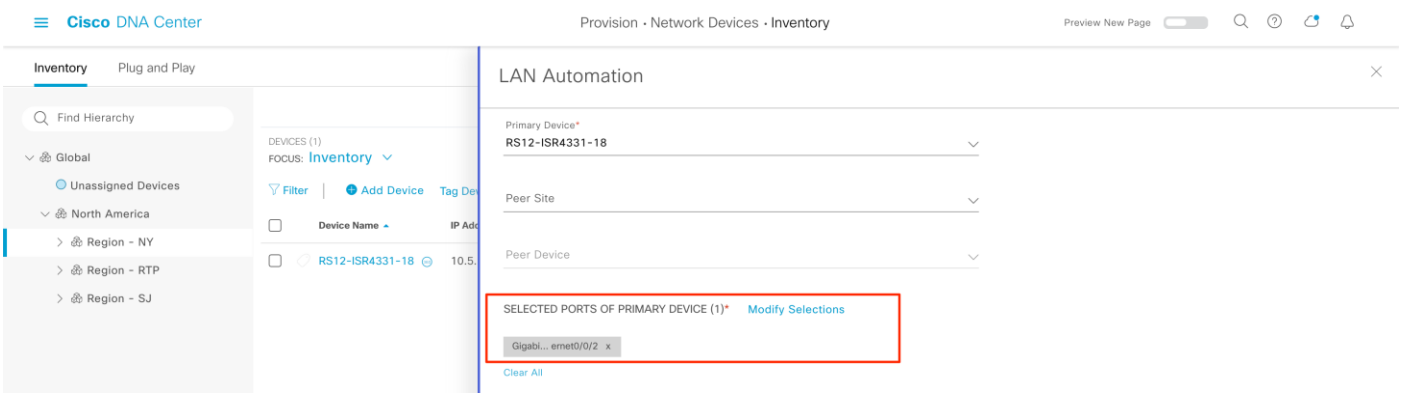
Select the **Peer Device** (if available)

Under **SELECTED PORTS OF PRIMARY DEVICE**, click **Modify selections**



Choose the interface(s) that connect to Fabric GRT switches at the site and click **Done.**





Under **Discovered Device Configuration** section,

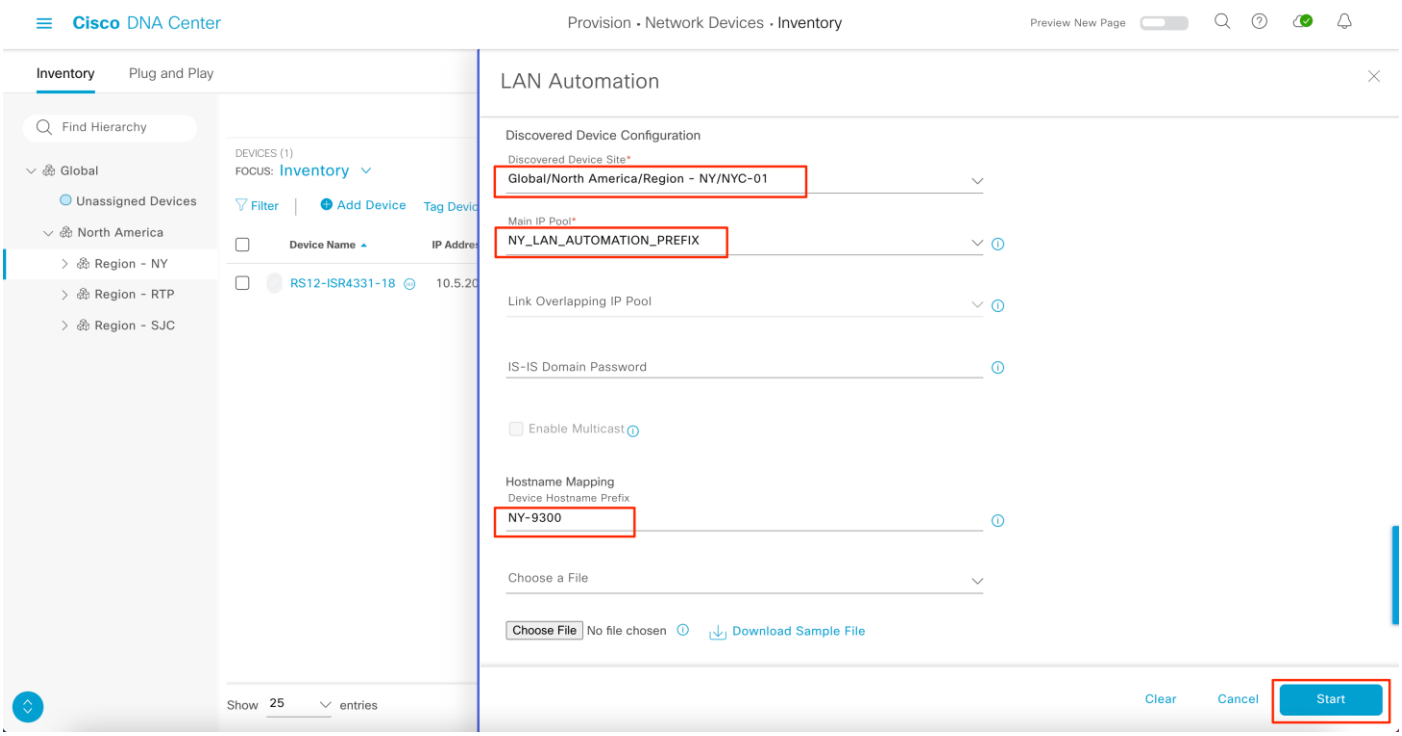
Input **Discovered Device Site:**

Input **Main IP Pool:**

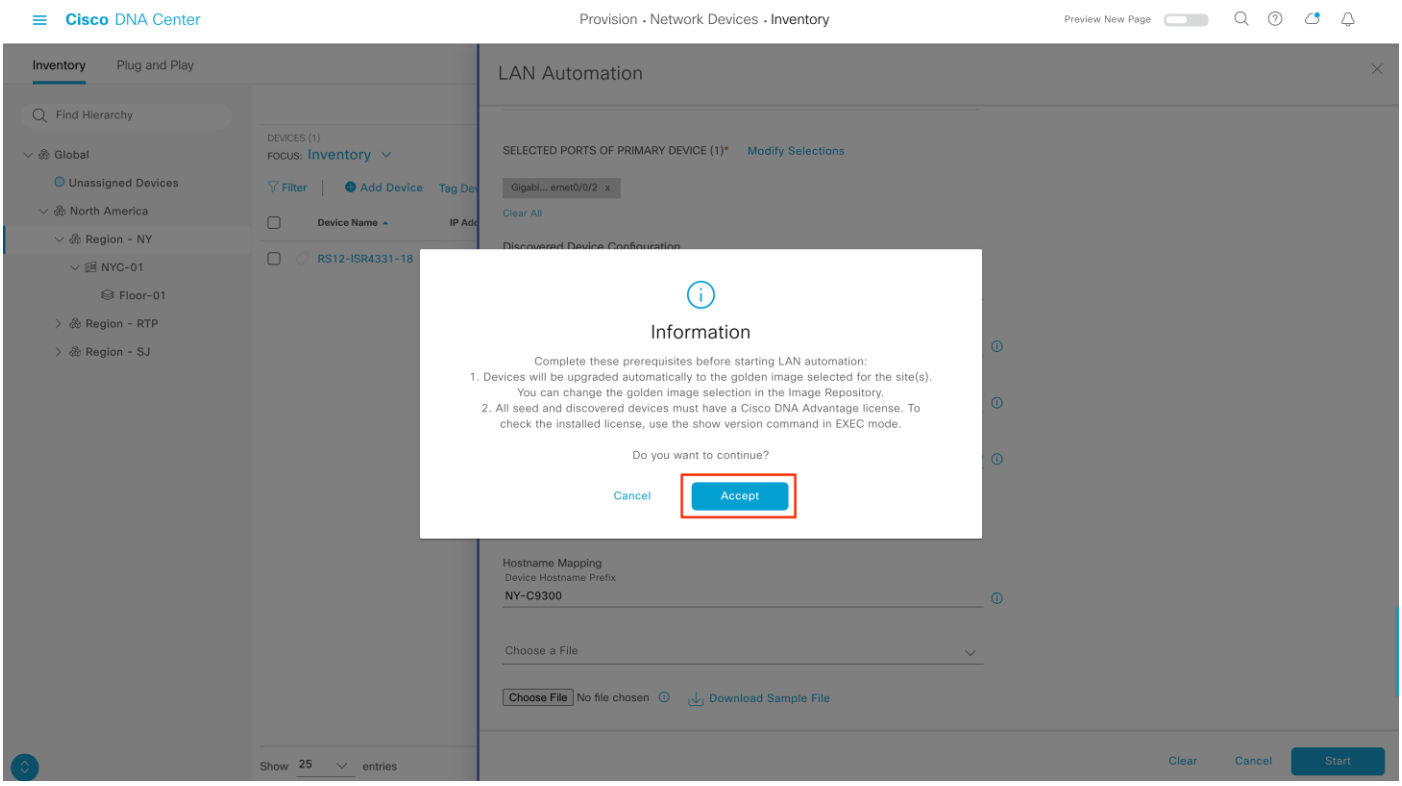
Under **Hostname Mapping,**

Input **Device Hostname Prefix:**

And click **Start**

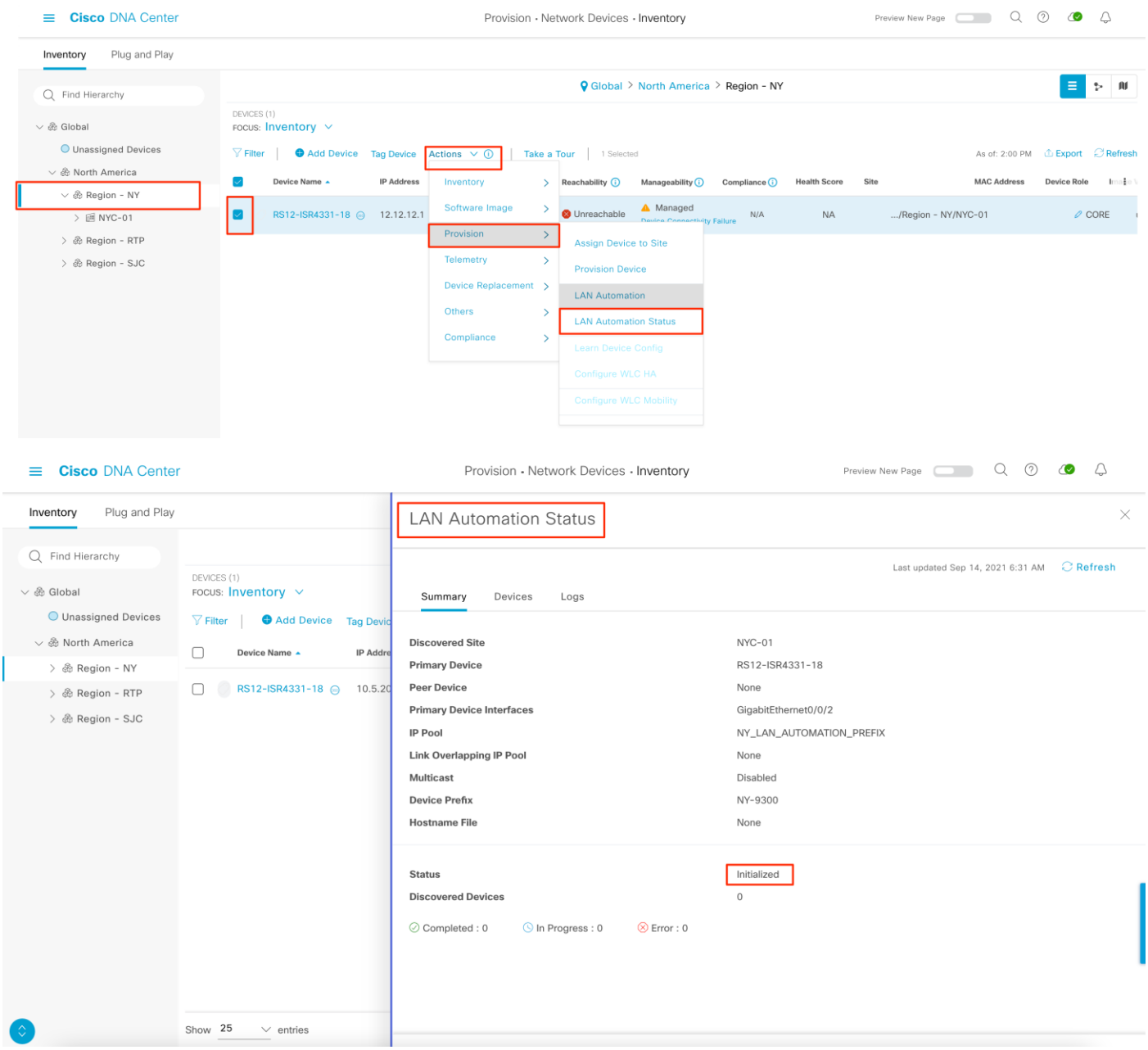


Step 4. Click **Accept** on the information pop-up page

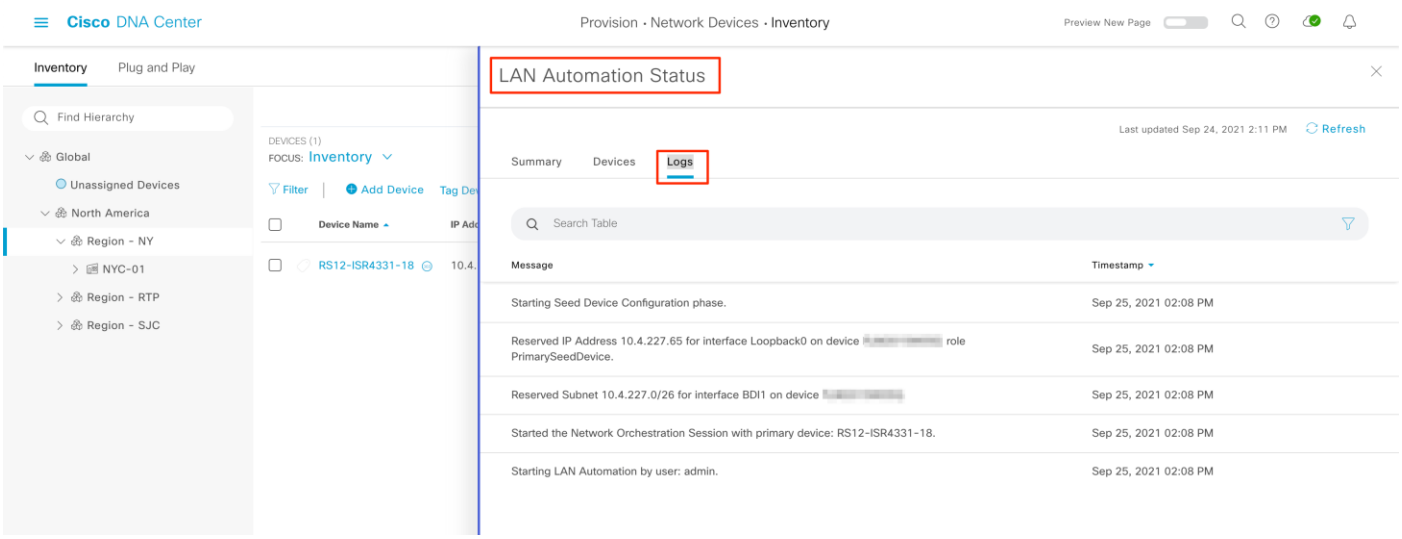


Step 5. View the LAN Automation status, navigate to **Provision > Network Devices > Inventory**.

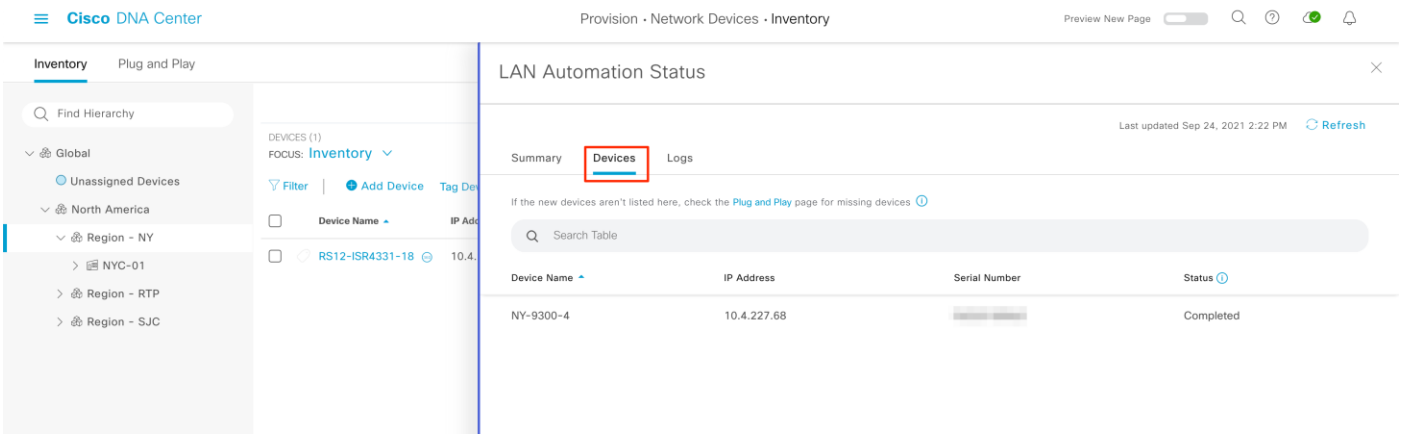
Select **Actions > Provision > LAN Automation Status**



View the LAN automation Status logs, by selecting the **Logs** tab.

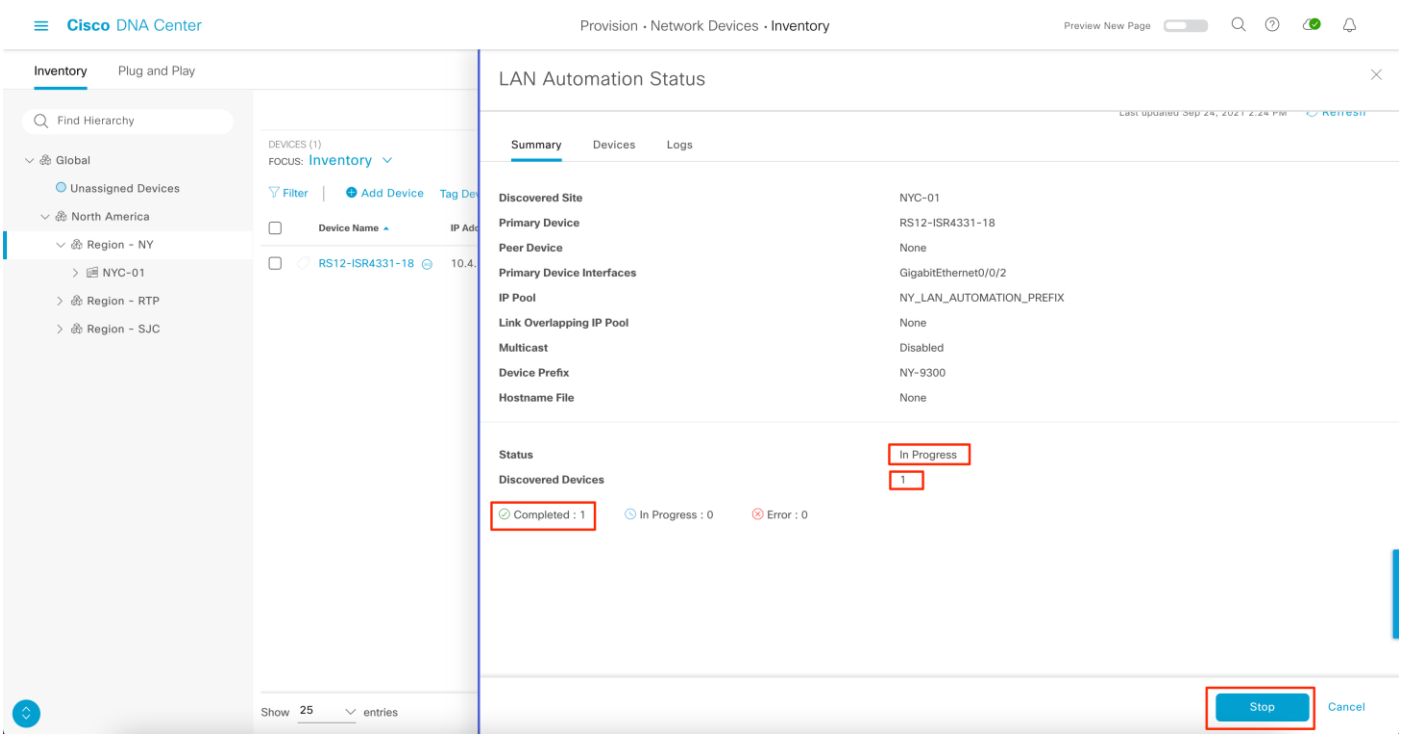


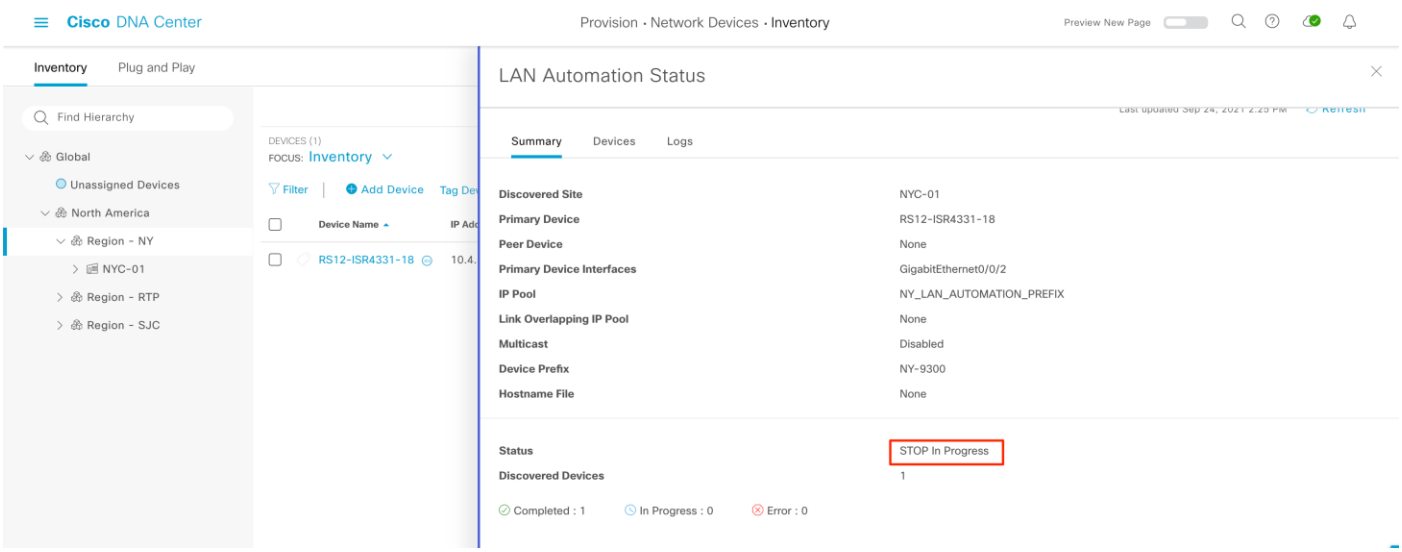
View the network devices discovered, by selecting the **Devices** tab

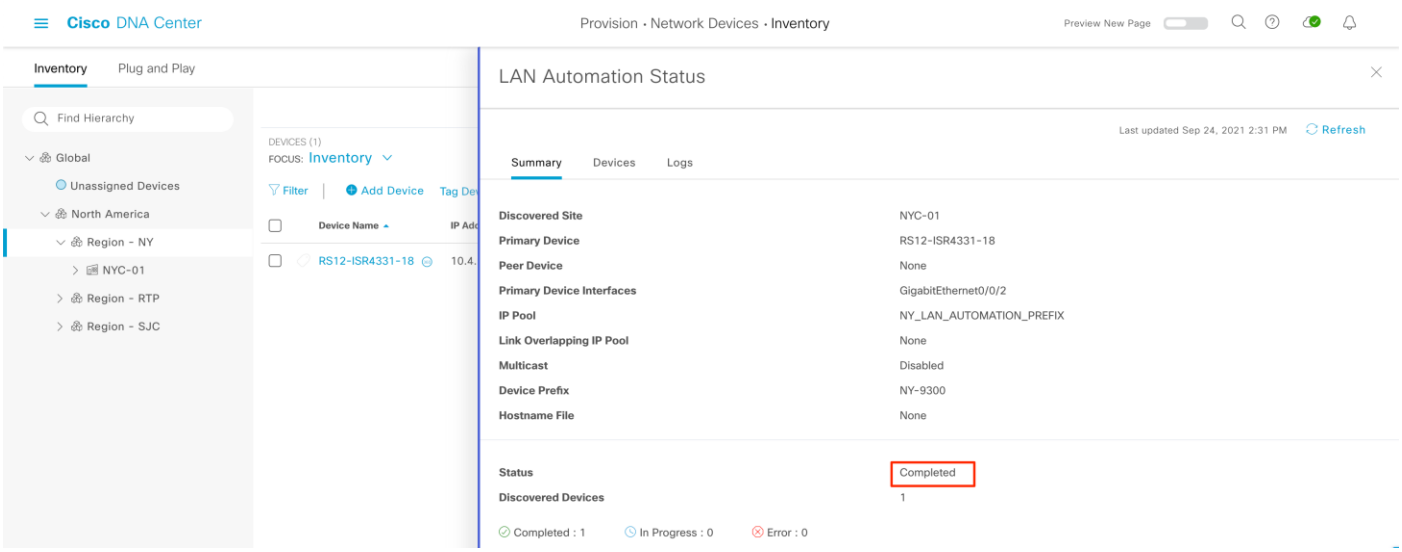


Step 6. Upon network devices being discovered, stop the LAN Automation to complete the onboarding process.

In the **LAN Automation Status > Summary tab** slide-out, click **Stop**



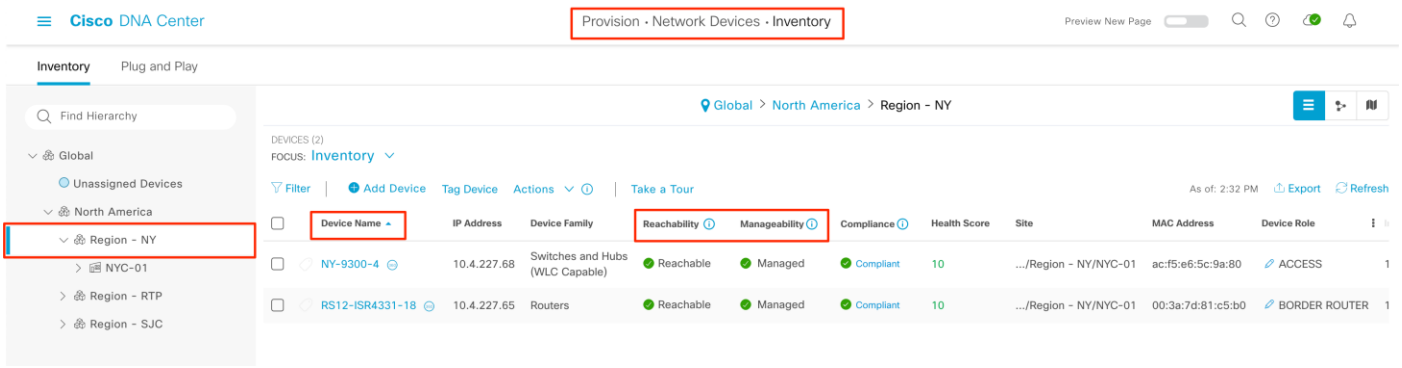




Step 7. View the discovered network devices in the DNA Center Inventory.

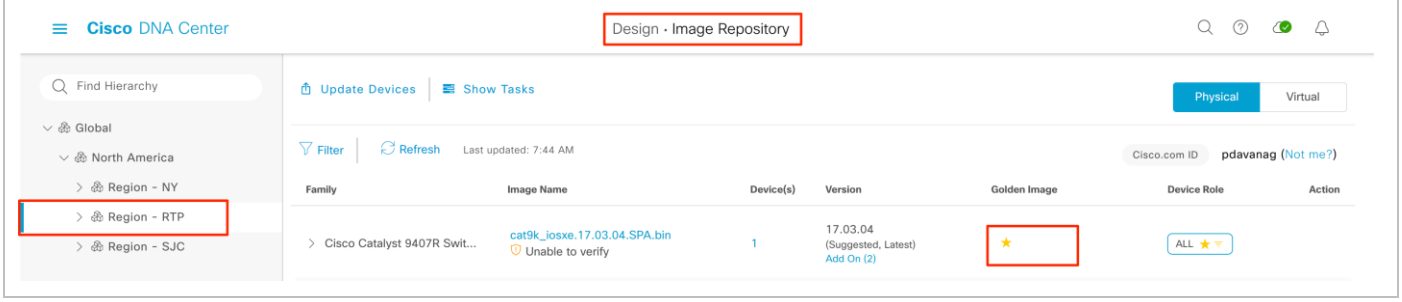
Navigate to Cisco DNA Center, **Provision > Network Devices > Inventory.**

select the site from the **Hierarchy** and verify the devices is **Reachable** and **Managed** state.



Tech Tip

Image Management for the discovered devices can be completed as a part of LAN Automation. This requires image to be available in Cisco DNA Center **Image Repository** and be tagged with **Golden** for the device family for the site.



Process 6: Provision Cisco SD-Access Fabric Site(s).

This section details the procedure to provision the network devices to a site, creating fabric site(s) and assigning fabric role to the devices.

Procedure 1. Provision the network devices to a site

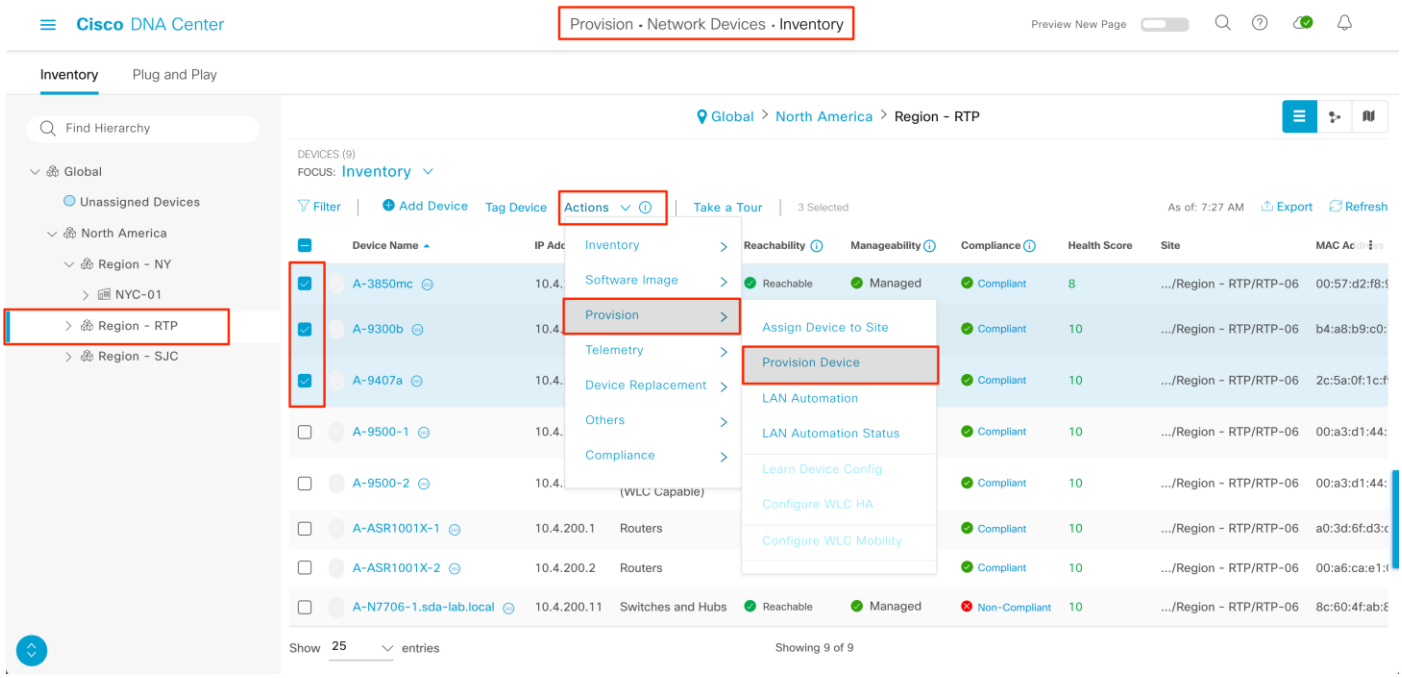
This section details the steps needed to provision the network devices to a site with the intent to configure network parameters such as AAA, DNS, NTP etc. defined in the Cisco DNA Center network setting.

Step 1. In Cisco DNA Center, navigate to **Provision > Network Devices > Inventory.**

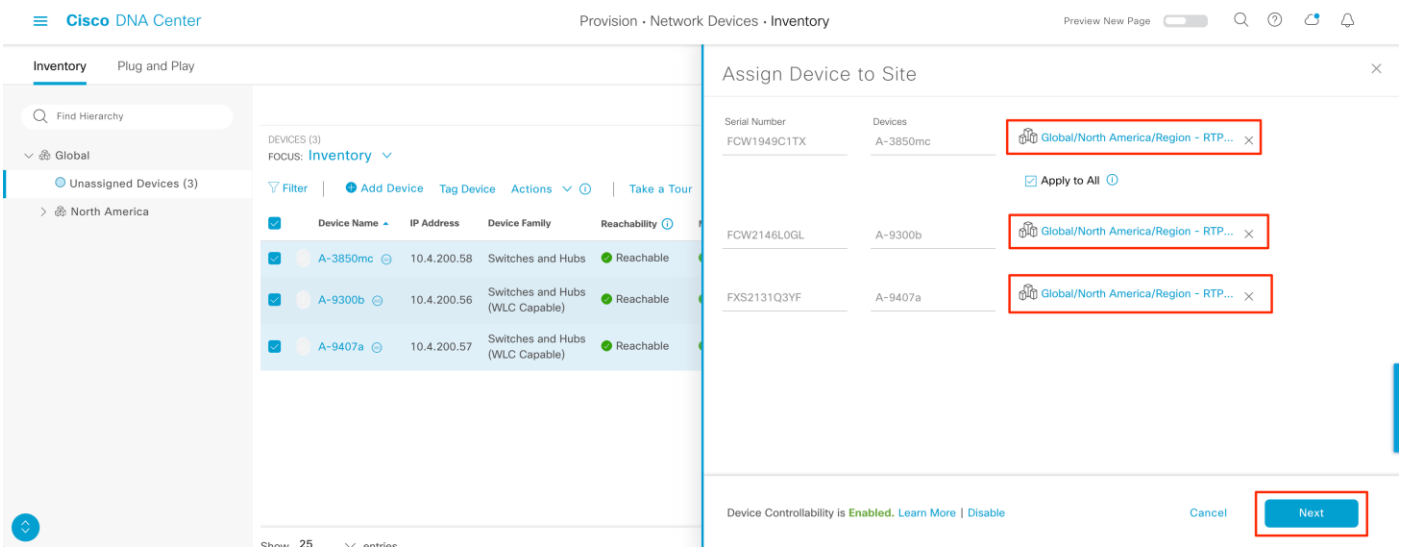
Select the site from **Hierarchy** and network devices from the **Devices** list

Click **Actions > Provision > Provision Device**

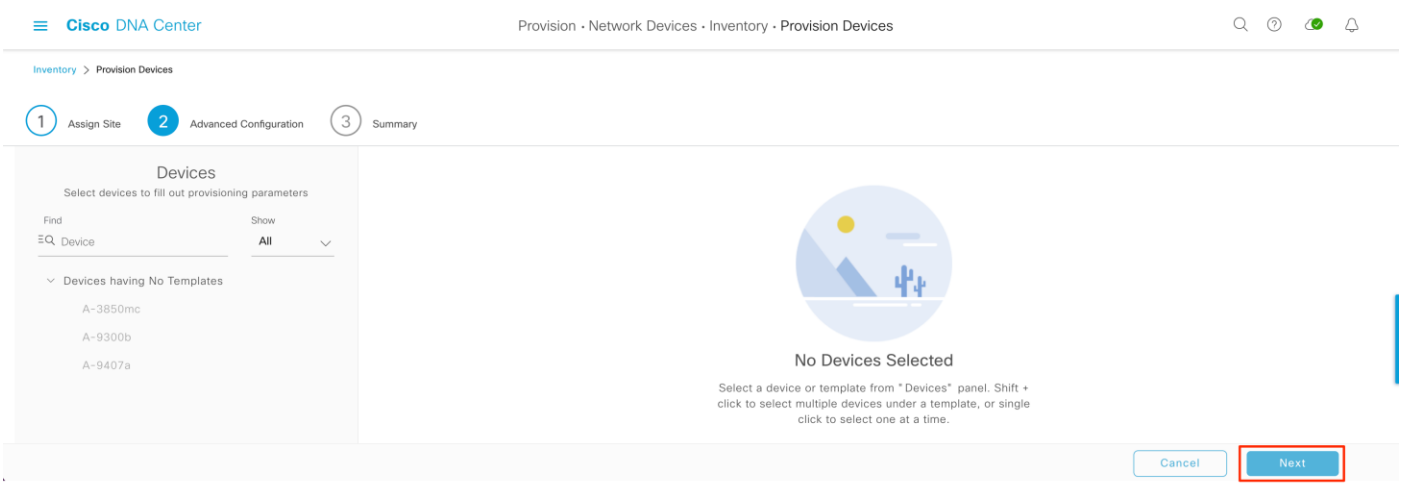
Tech tip
Similar network devices such as switches, routers can be grouped together and provisioned to a site together.



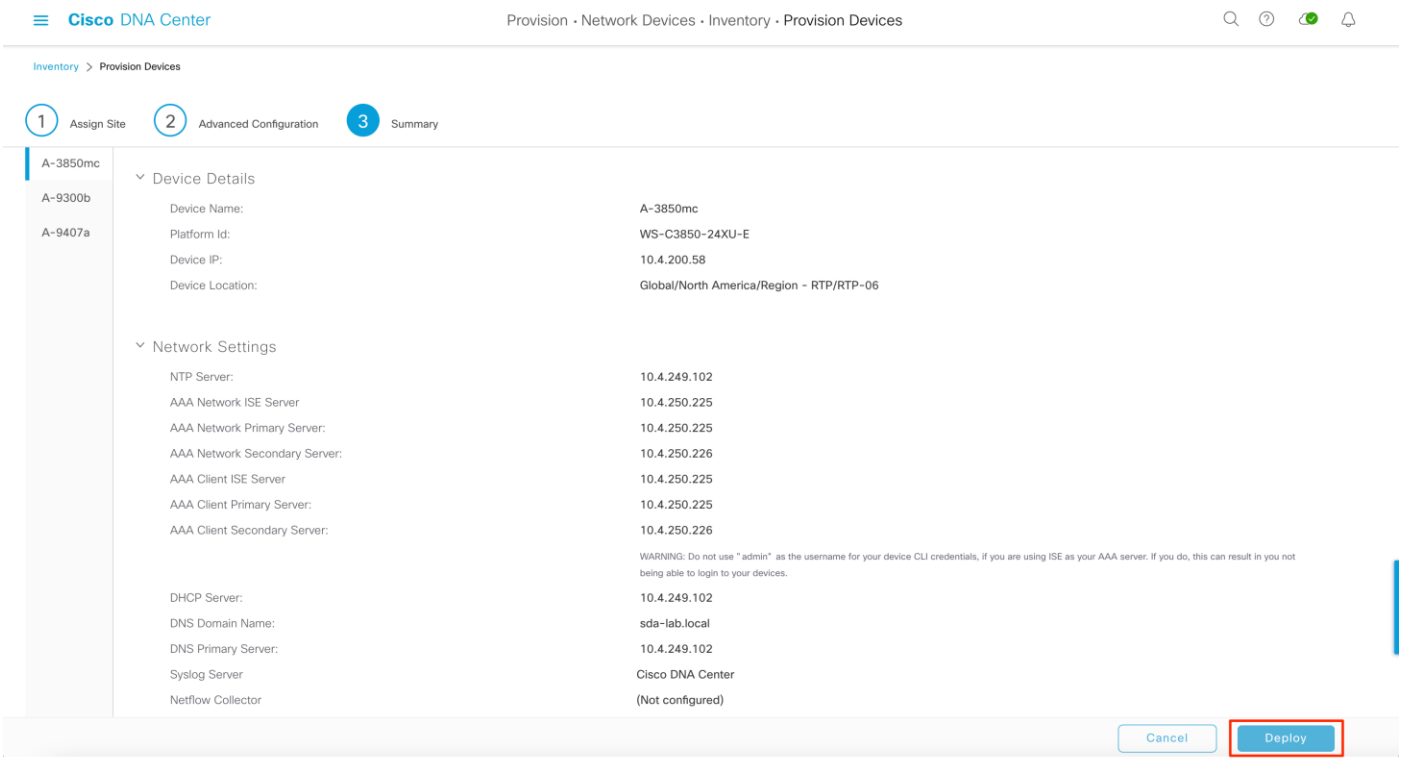
Step 2. **Choose the site** for each device in the list (the site auto) and select **Next.**



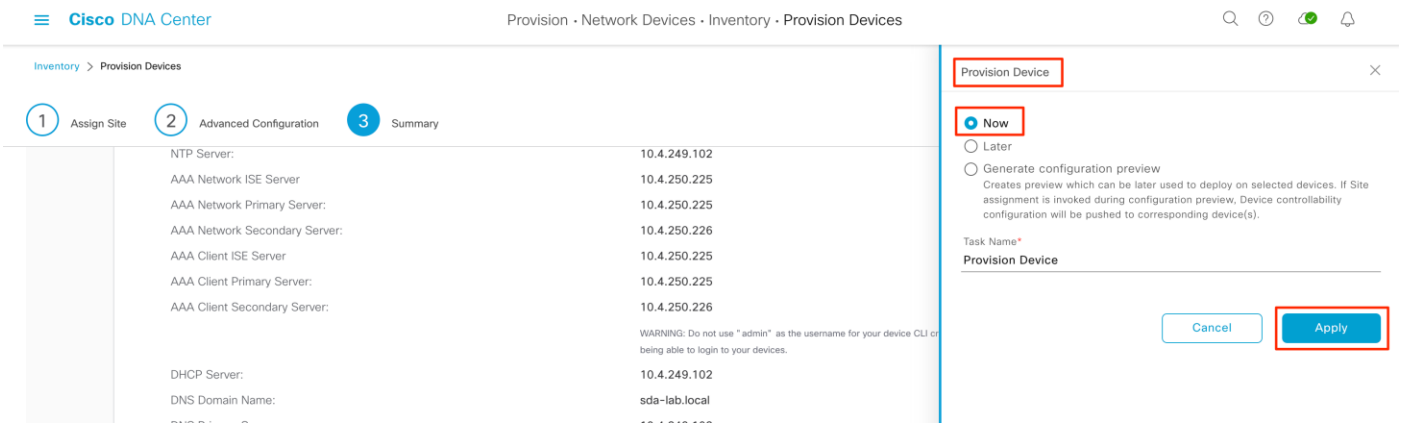
Click **Next**



View the parameters that gets provisioned on the device and select **Deploy**

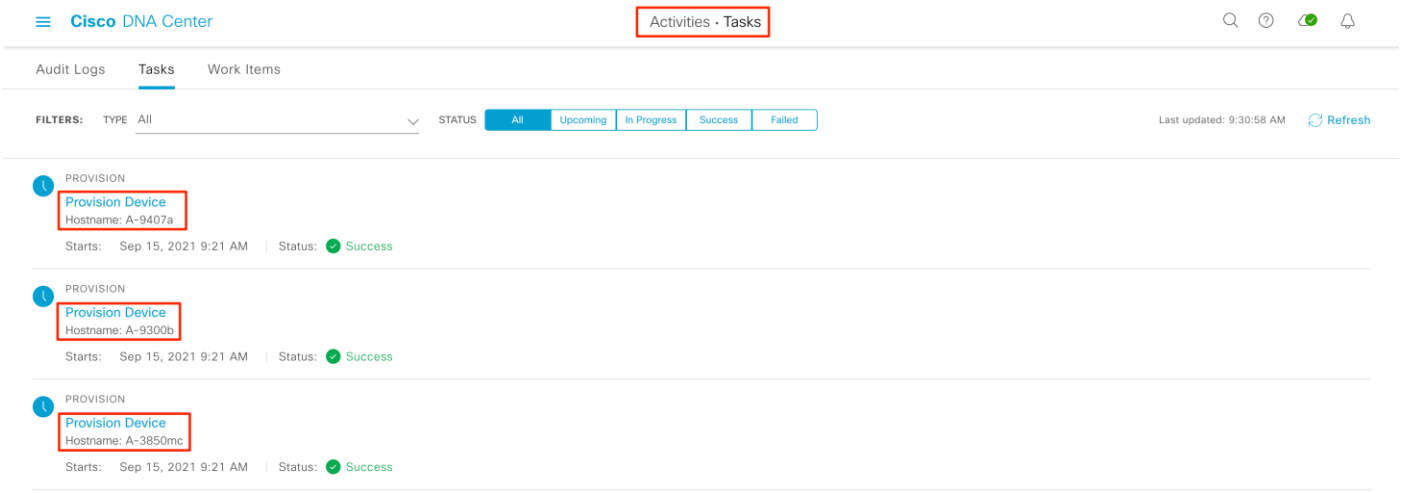


Under **Provision Device** slide-out page, select **Now** option and **Deploy**

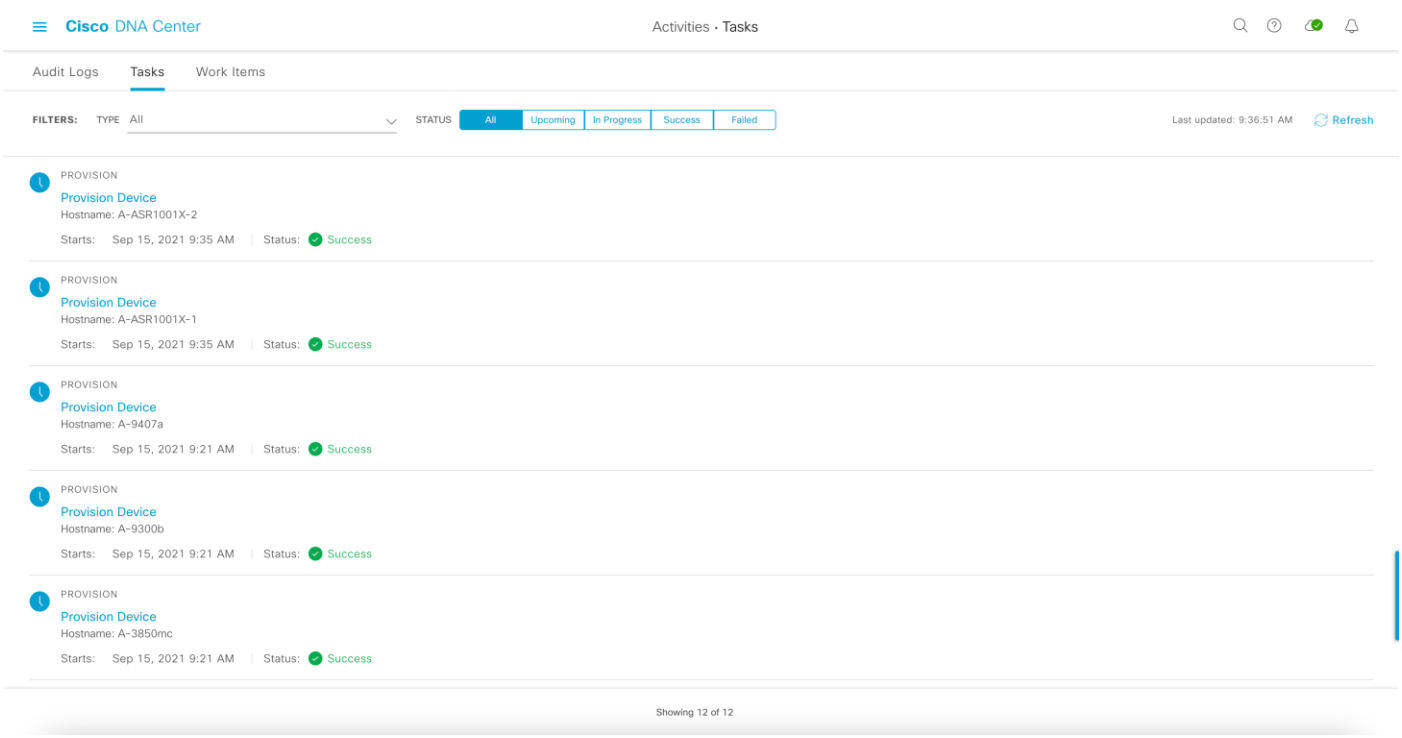


Step 3. View the status of the Provision task by navigating to

Cisco DNA Center > Activities > Tasks



Step 4. Repeat the steps in this Procedure to provision other network devices to a site, including the IOS-XE SD-WAN WAN Edge devices .

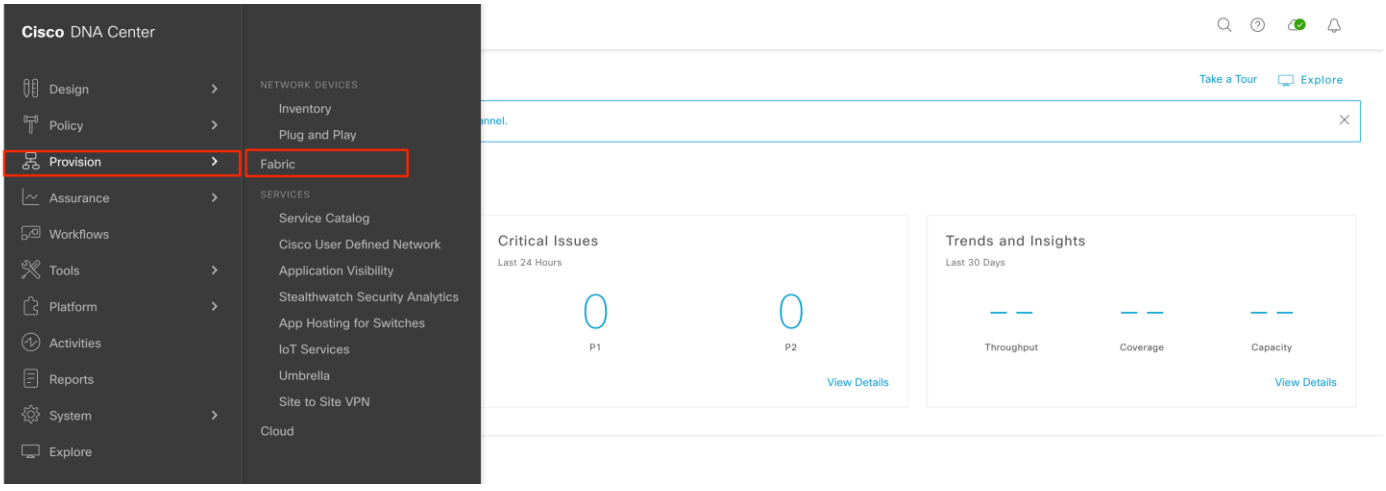


Procedure 2. (Optional) Provision IP-Transit Network

This section details the steps needed to create an IP-Transit network. This is needed only when the WAN Edge devices part of site has connectivity to shared services network through the IP network.

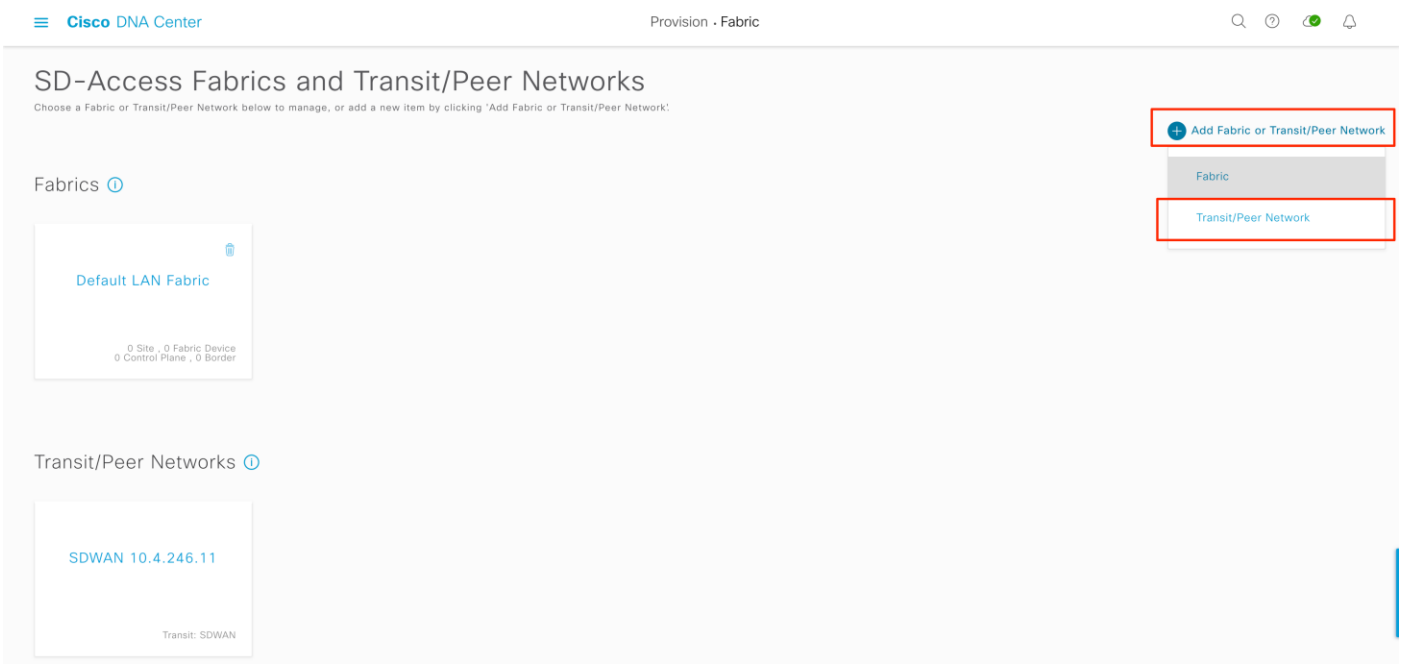
Skip this Procedure at remote sites, that requires connectivity to SD-WAN Transit only.

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



Step 2. Create IP-Transit

Click **Add Fabric or Transit/Peer Network** and Select **Transit/Peer Network** from the drop-down option



Tech Tip
Transit: SDWAN is created on successful integration between Cisco DNA Center and SD-WAN vManage controller.

Under, **Transit/Peer Network** slide out page:

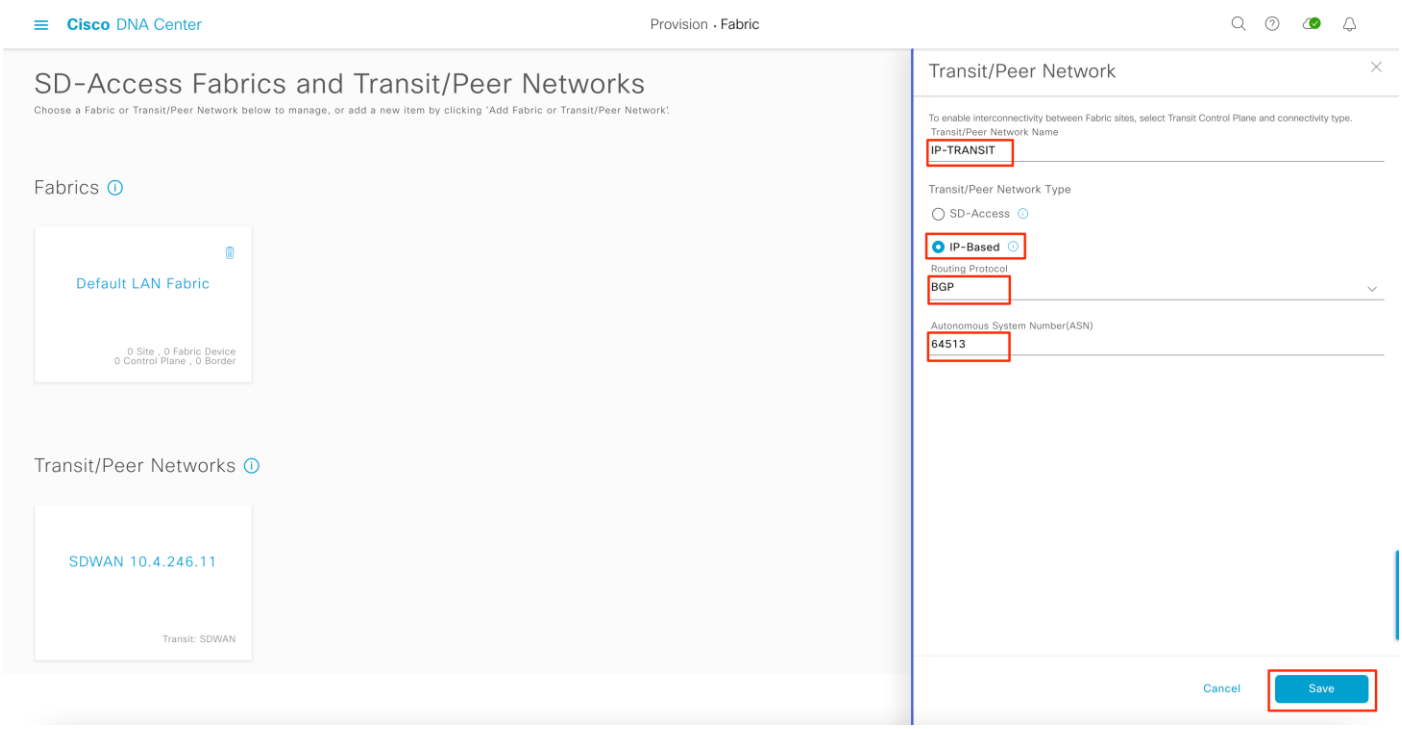
Input **Transit/Peer Network Name**

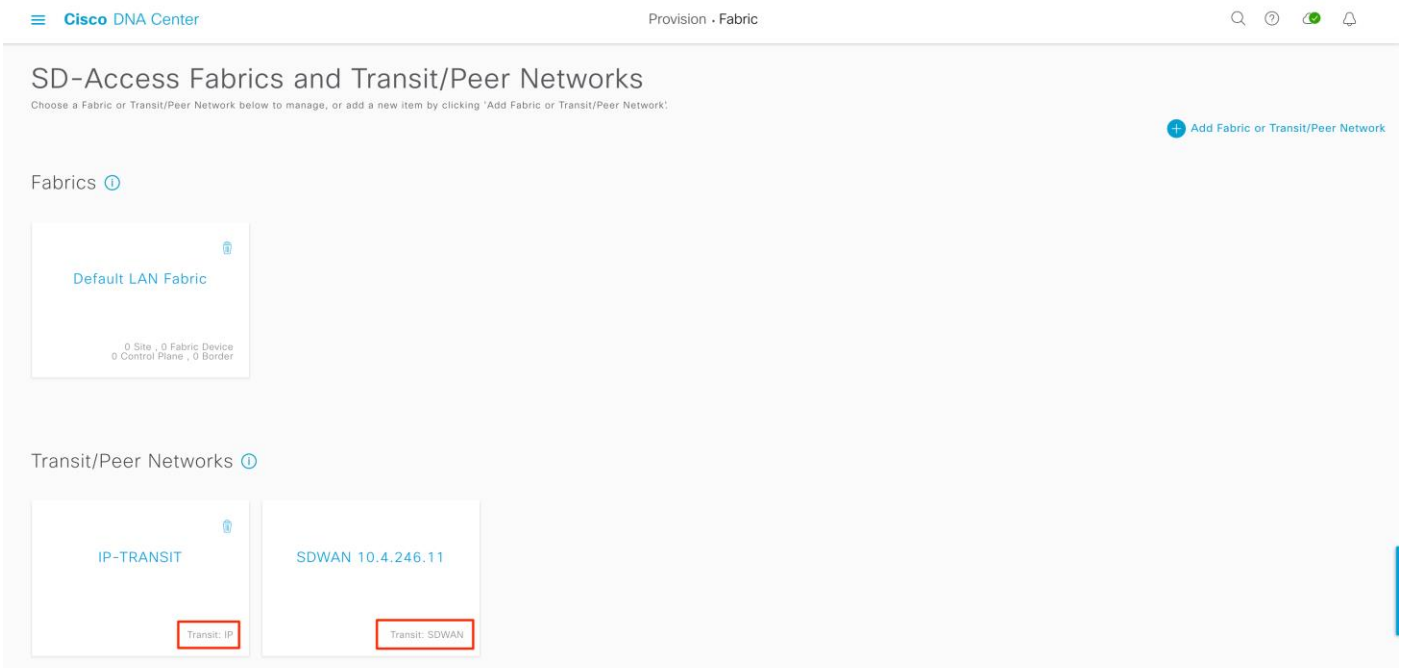
Select **Transit/Peer Network Type: IP-Based**

Select **Routing Protocol: BGP**

Input **Autonomous System Number (ASN):** peer network BGP AS number

Click **Save**





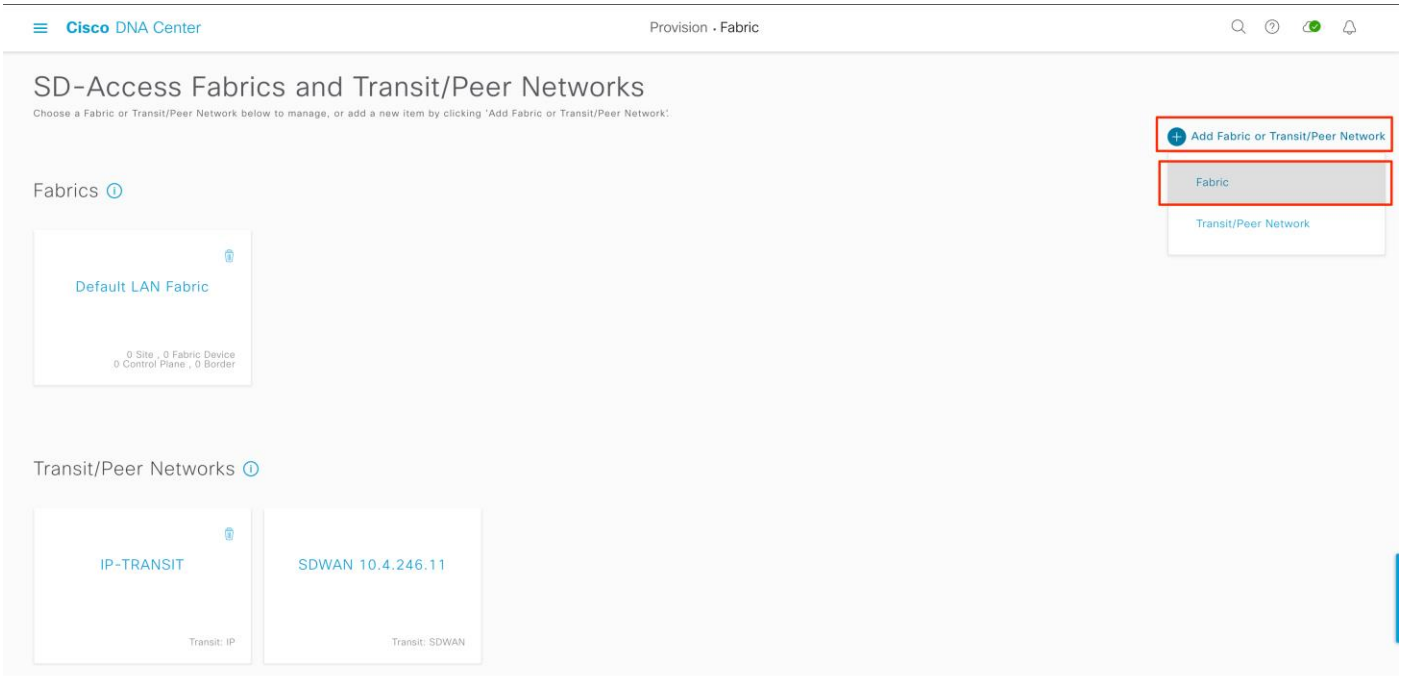
Procedure 3. Provision Fabric – Create Fabric Site

This section details the steps needed to create a Fabric site. The SD-Access fabric site is provisioned with IOS-XE WAN Edge device as colocated Fabric Border, Control Plane roles and connected SD-WAN Transit and IP-Transit. The access switches are associated with Fabric Edge role.

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

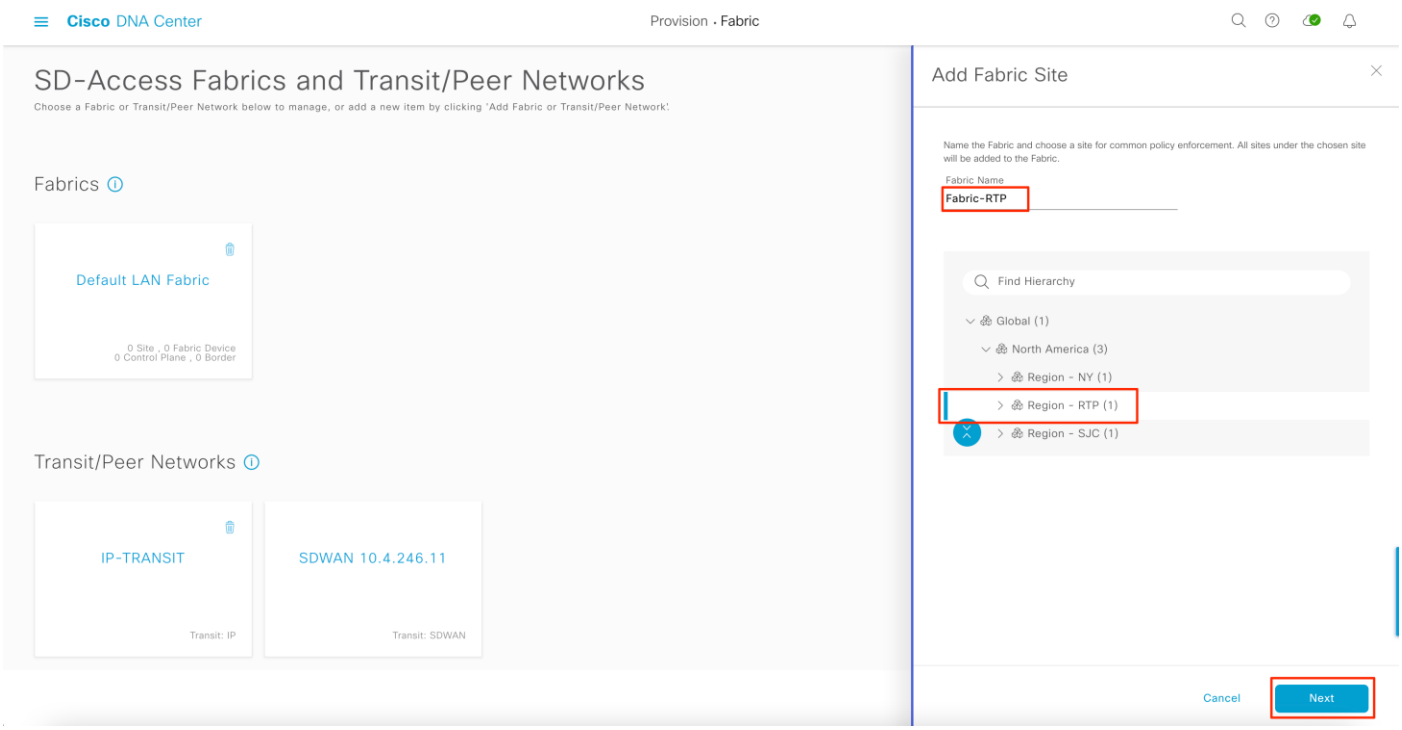
Create SD-Access fabric site, click **Add Fabric or Transit/Peer Network**

Select **Fabric** from the options



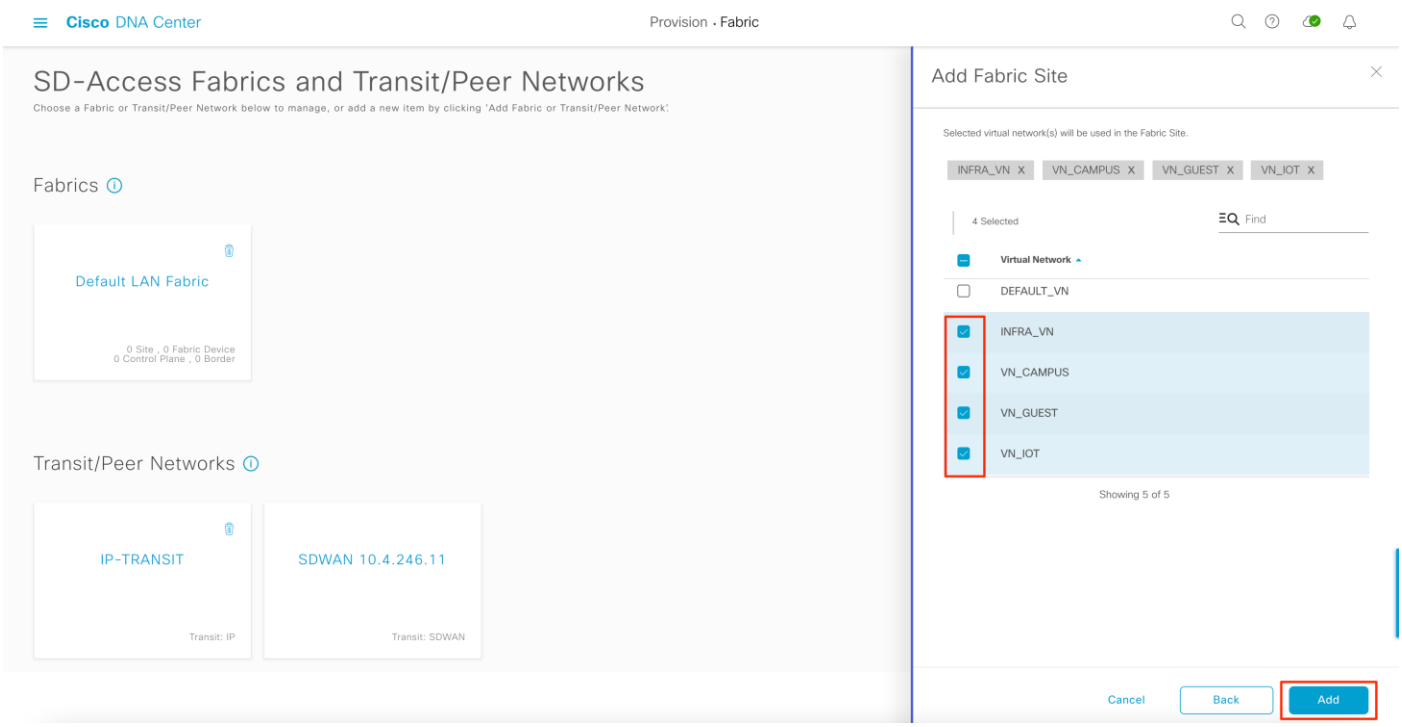
Step 2. Input **Fabric Name** and **location** by selecting the site from the hierarchy.

And click **Next**

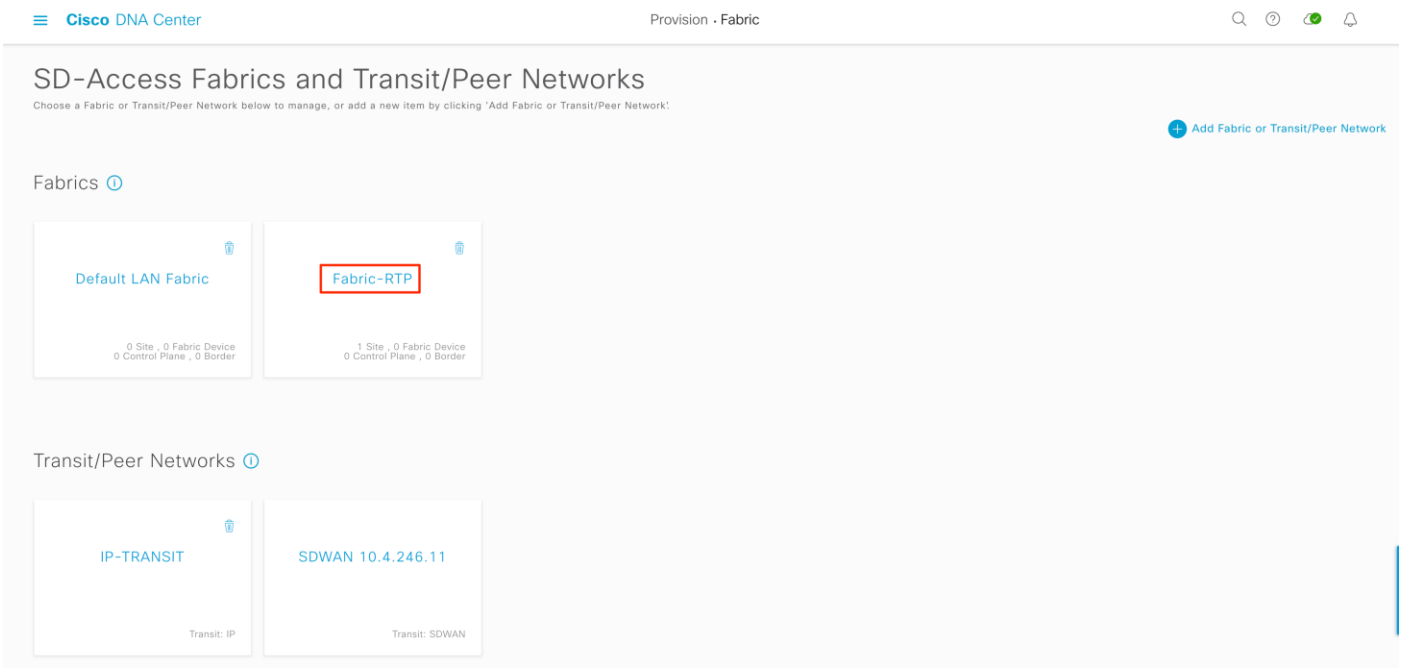


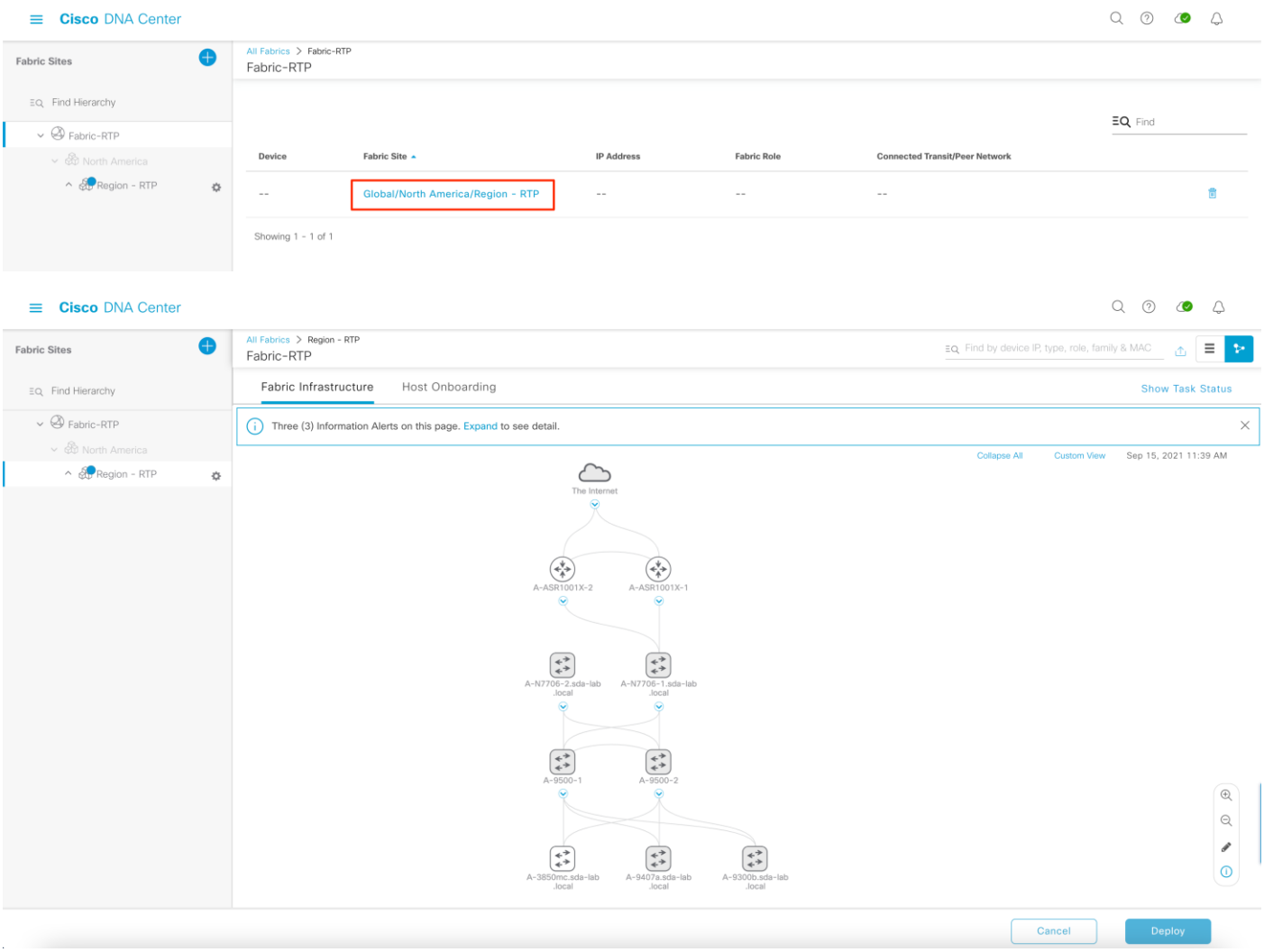
Step 3. Select all the **Virtual Network** from the list that needs to be provisioned at the site.

Click **Add**



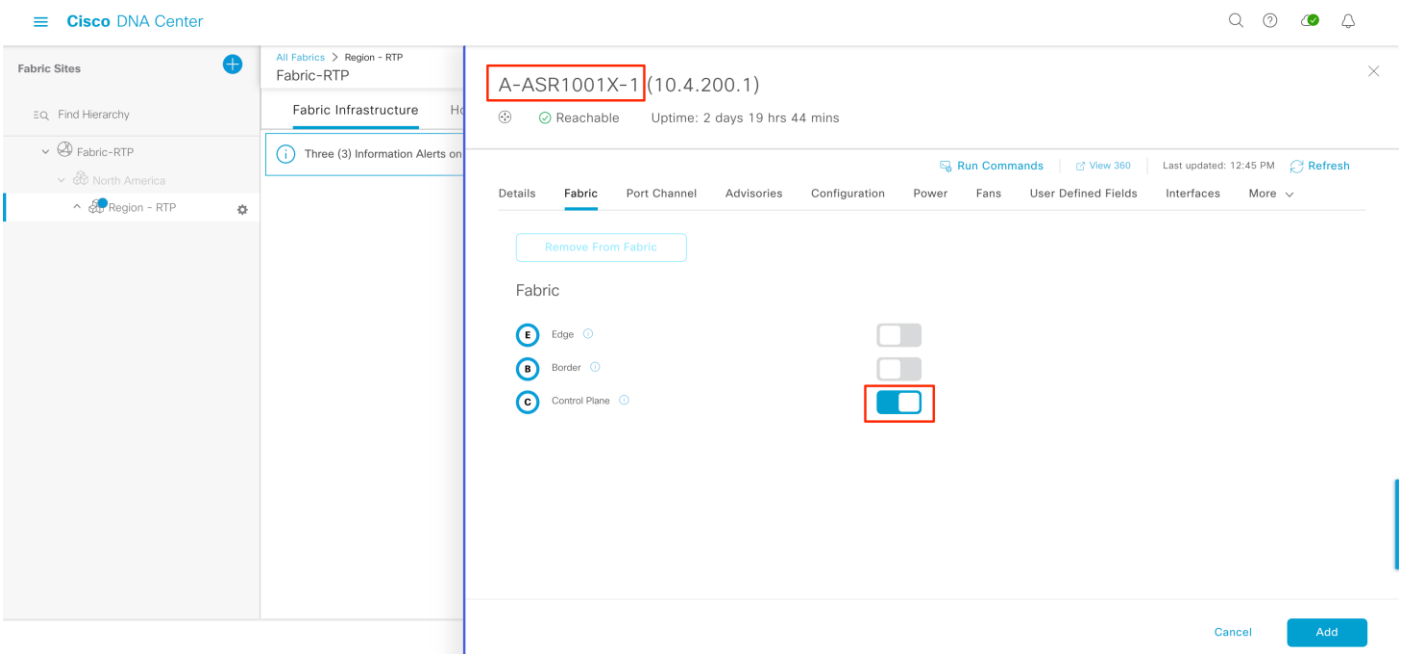
Step 4. Click on the fabric site ' **Fabric-RTP** ' card and select the site from the list





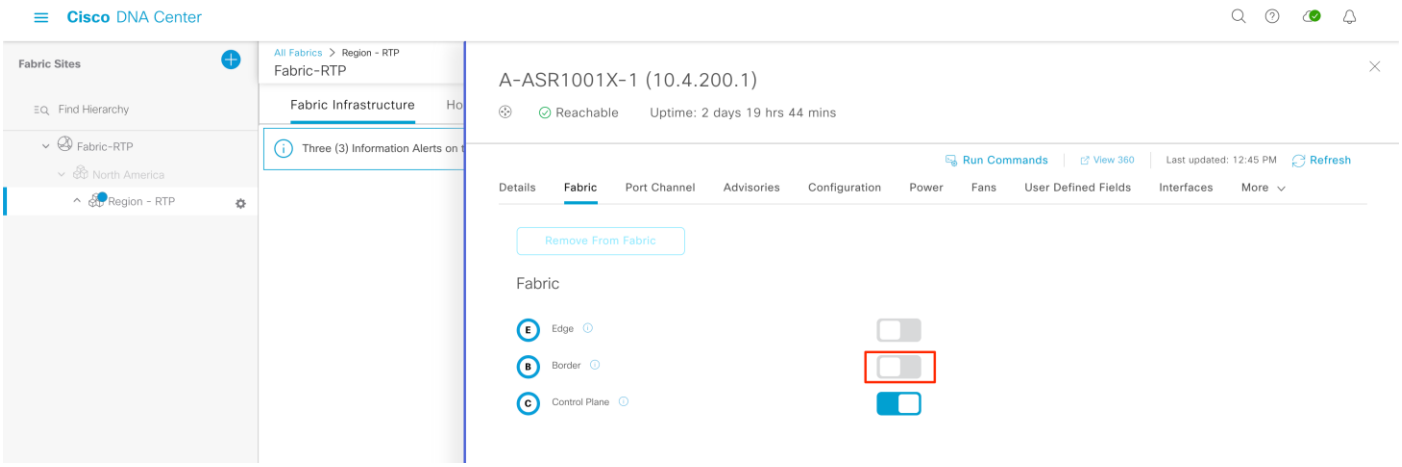
Step 5. Assign IOS-XE WAN Edge devices with Control Plane role.

Under **Fabric Infrastructure**, click the WAN Edge device and enable **Control Plane** functionality

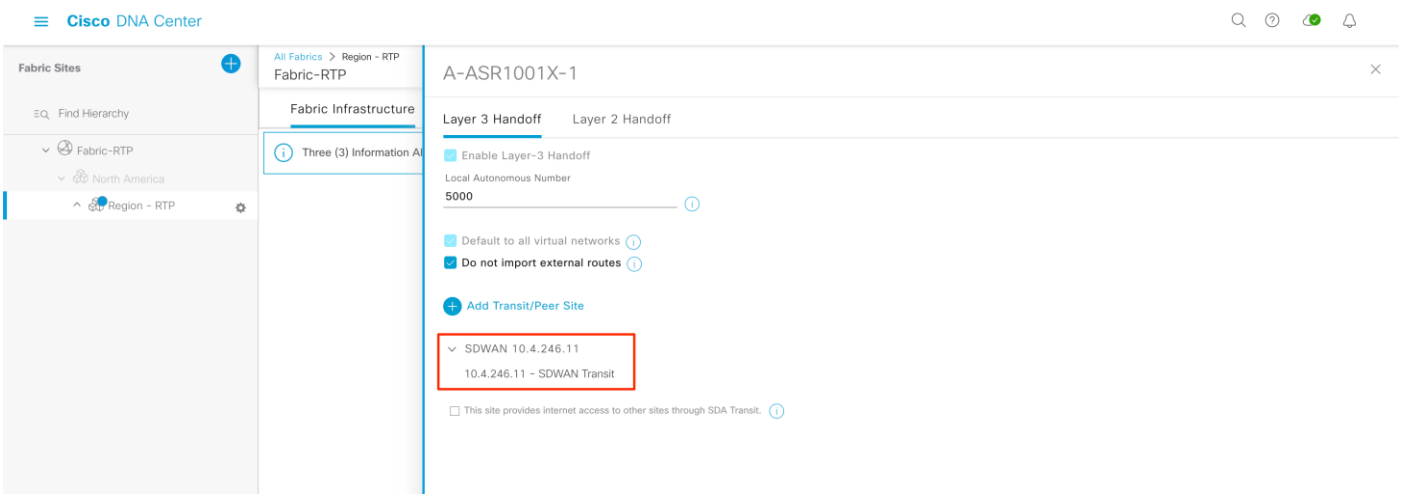


Step 6. Assign IOS-XE WAN Edge devices with **Border** functionality

Enable the **Border** role to the device



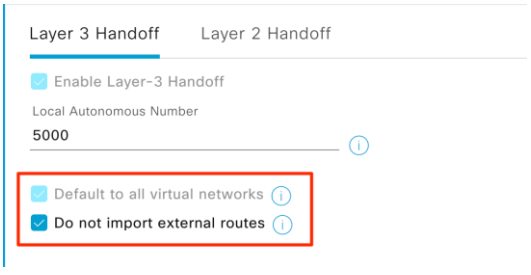
Transit: SDWAN is auto assigned to the IOS-XE WAN Edge device when selected as Border.



Tech tip

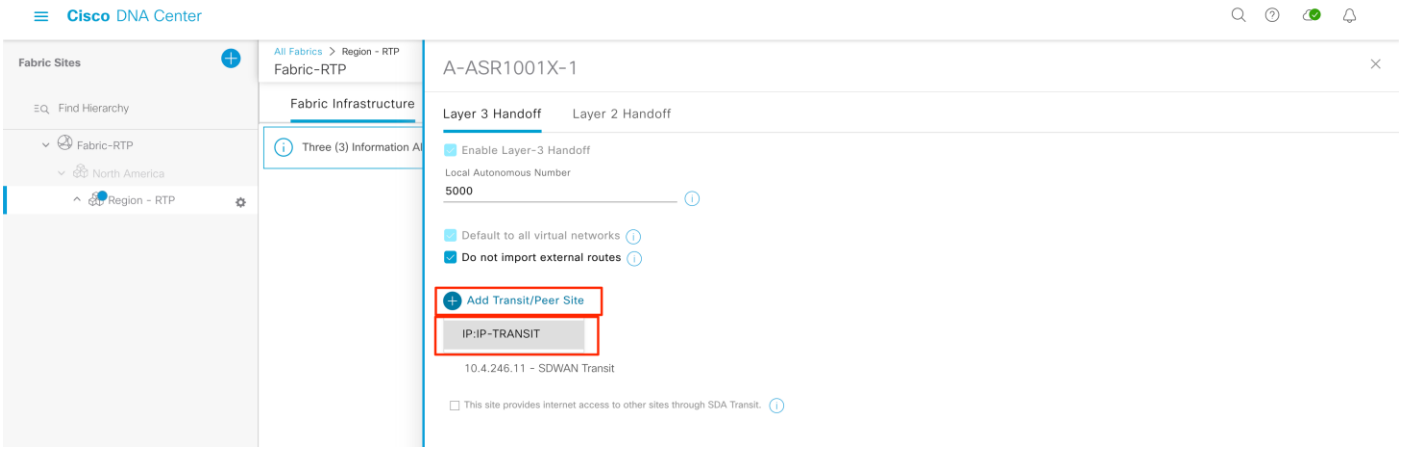
By default, Cisco SD-Access workflow chooses **External Border** as the Border type. For fabric sites that has connectivity to SDWAN Transit, leverage the default border type on the WAN Edge device.

WAN Edge learns routes to the rest of the network through SD-WAN infrastructure and for fabric site the WAN Edge device is the gateway of last resort implemented using LISP Proxy Tunnel Router (PxTR) functionality on fabric edge nodes.

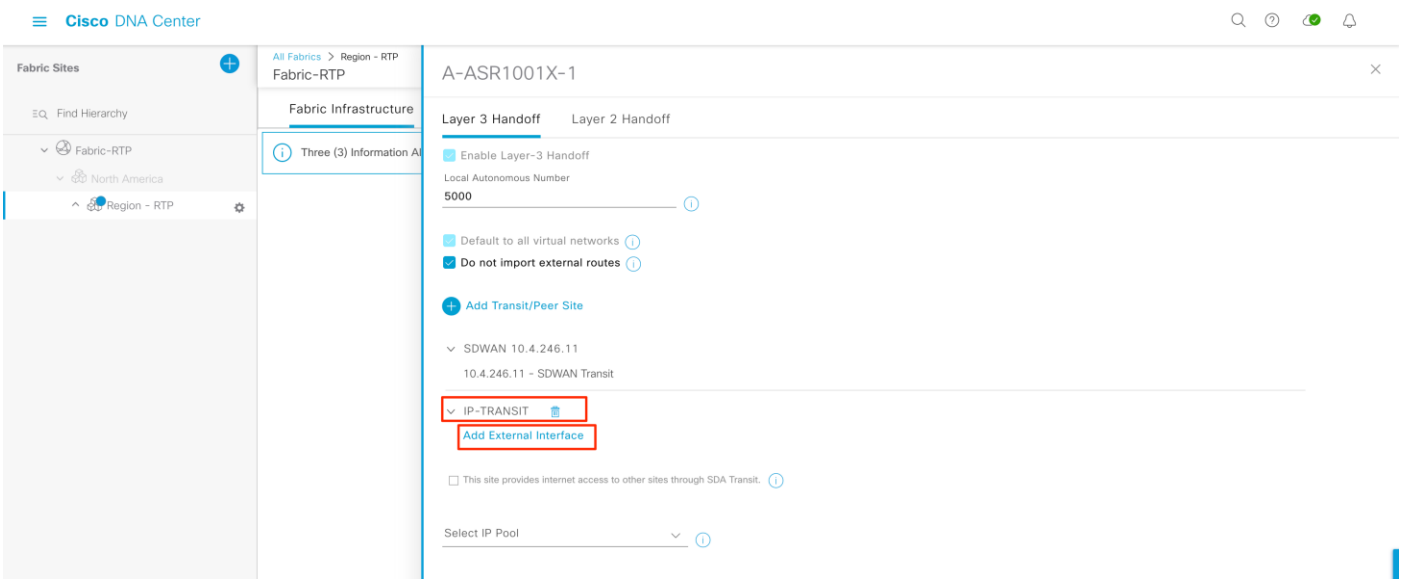


Step 7. For sites that requires IP-Transit to be associated to site.

Click **Layer 3 Handoff** > **Add Transit/Peer Site** and select previously created **IP-Transit** network.



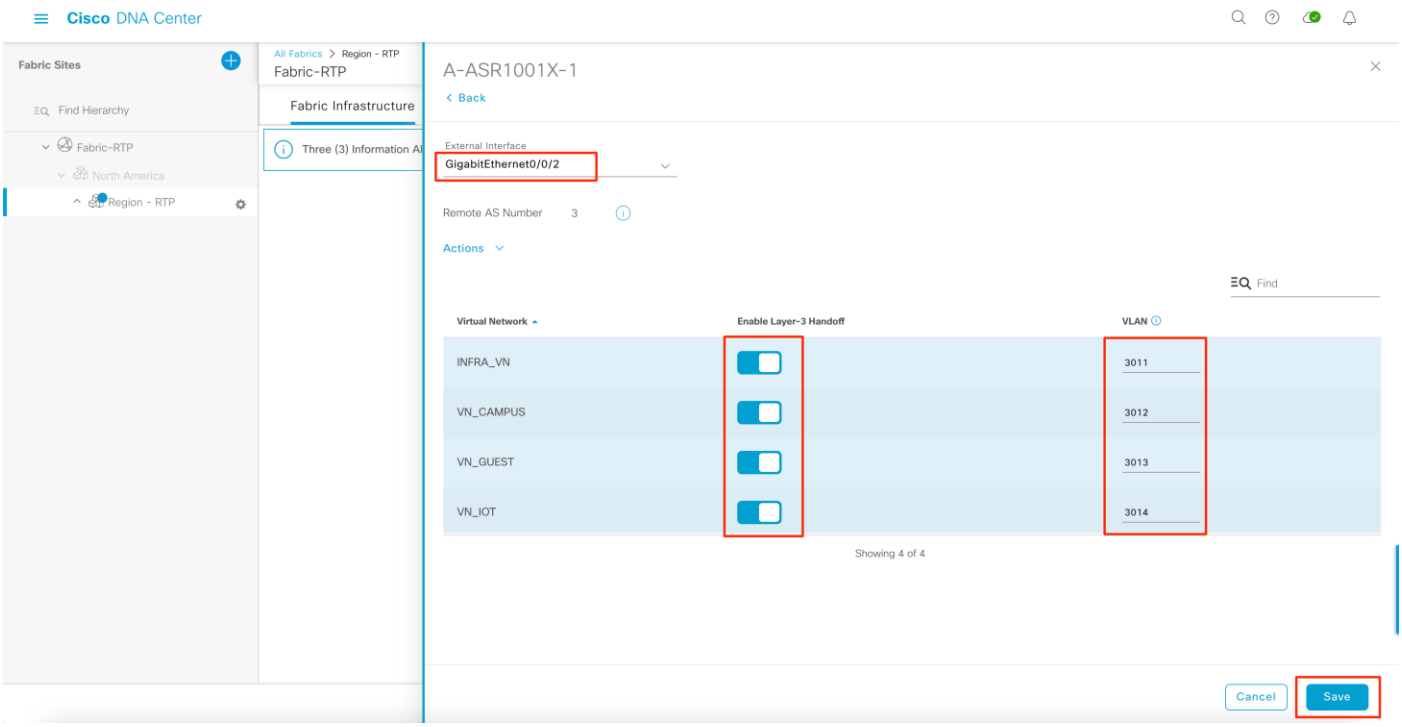
Under the selected **IP-Transit**, select the ports that connected to the peer device by clicking the **Add External Interface**



Select interface in the **External Interface** drop-down option

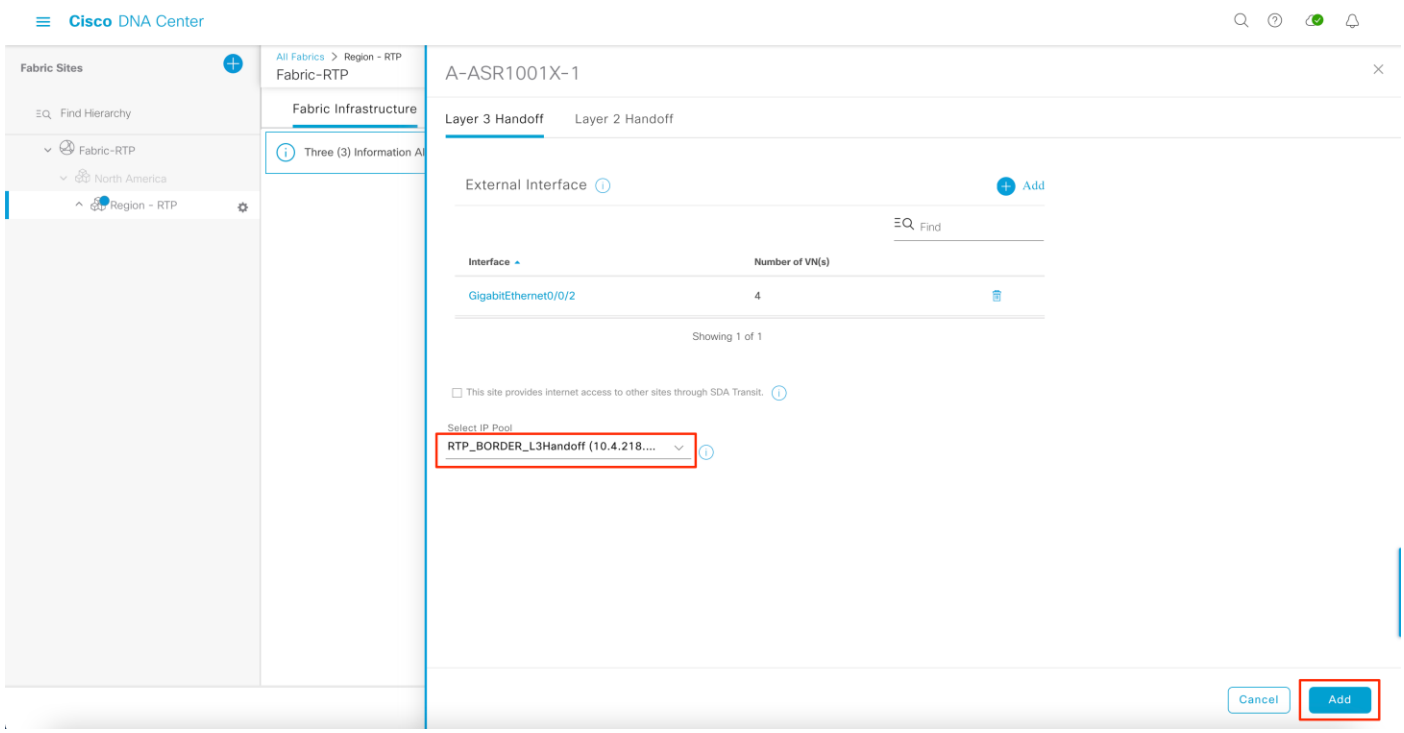
Select all the **Virtual Networks** that require IP-Transit handoff and assign a **vlan** number.

And click **Save**

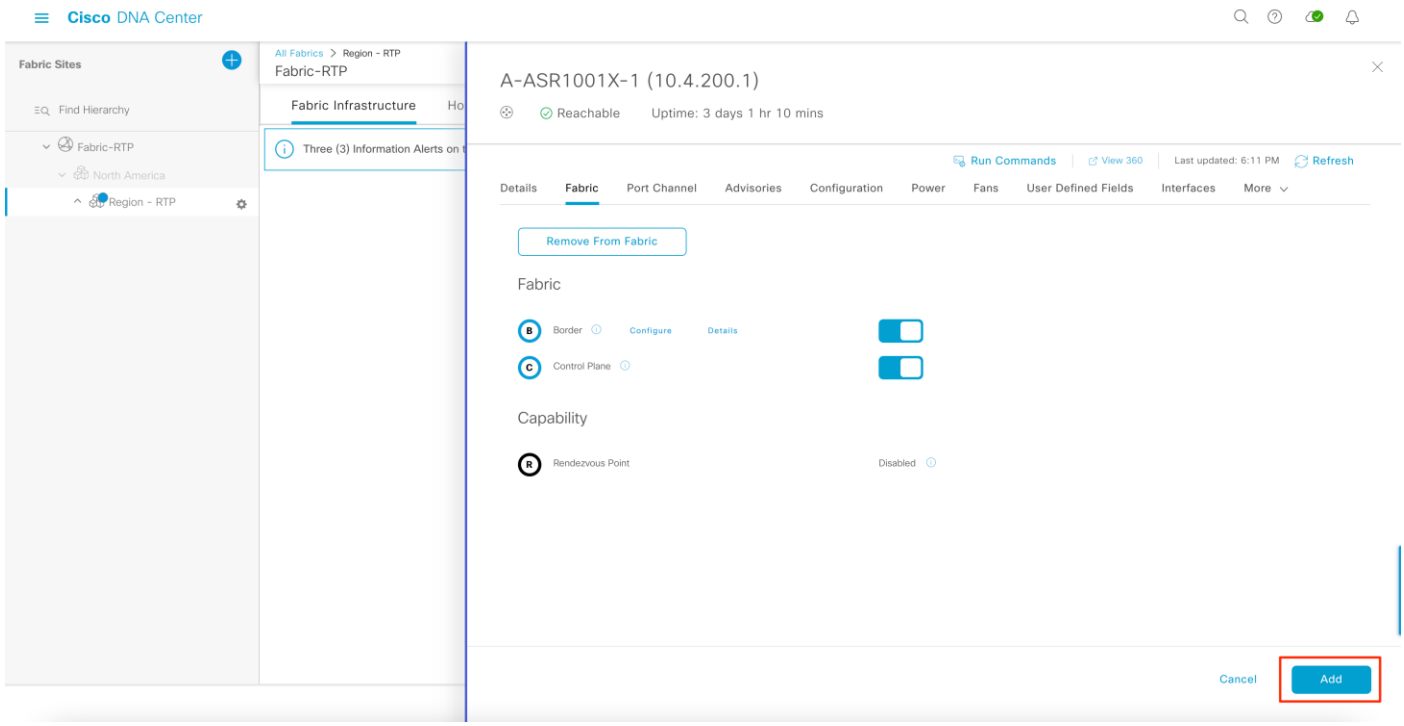


Under **Select IP Pool**, select the Border Handoff Pool

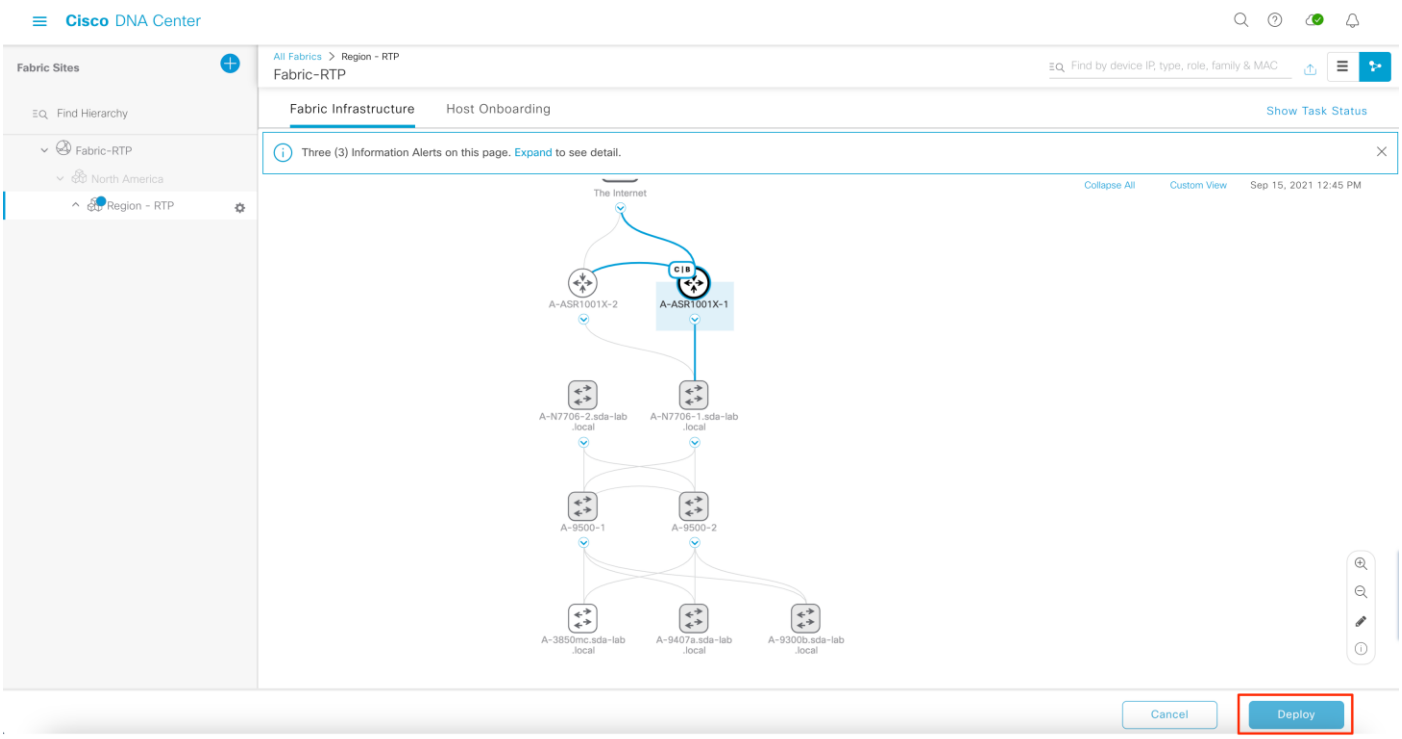
And click **Add**



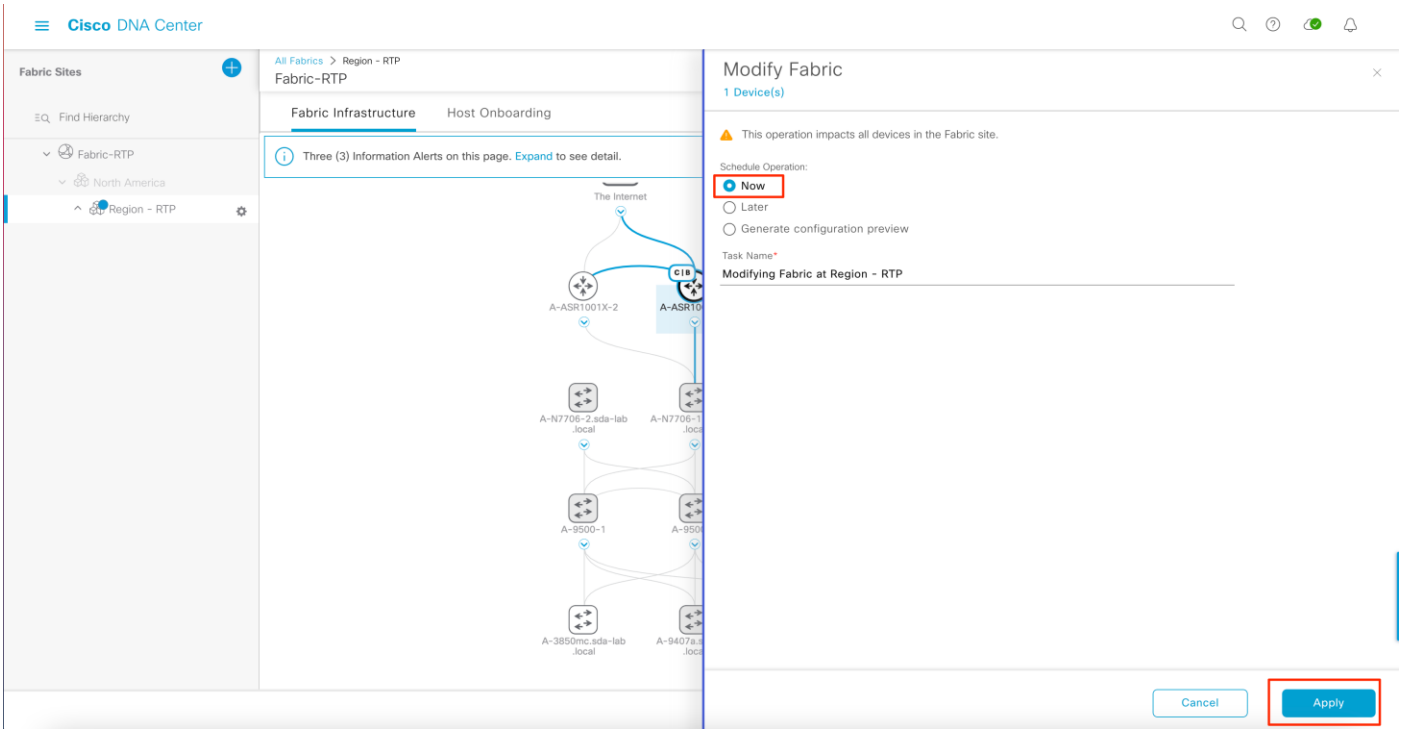
Step 8. Click **Add** to add Border and Control Plane role to the device



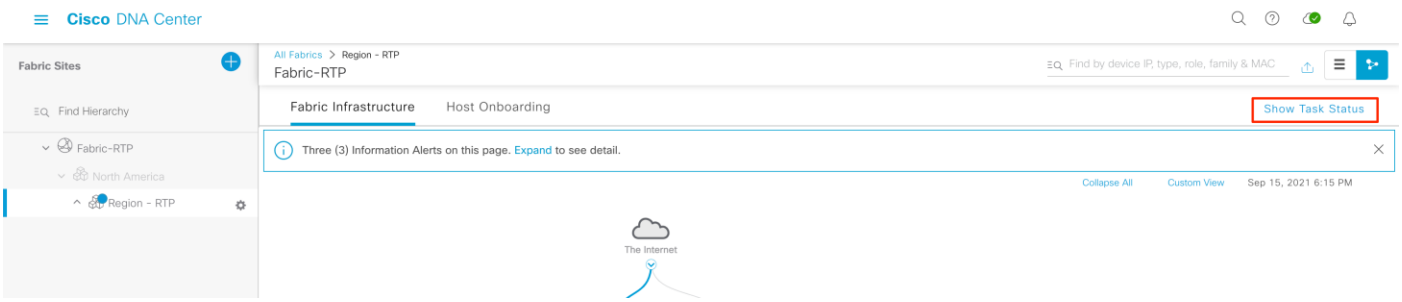
Step 9. Click **Deploy**

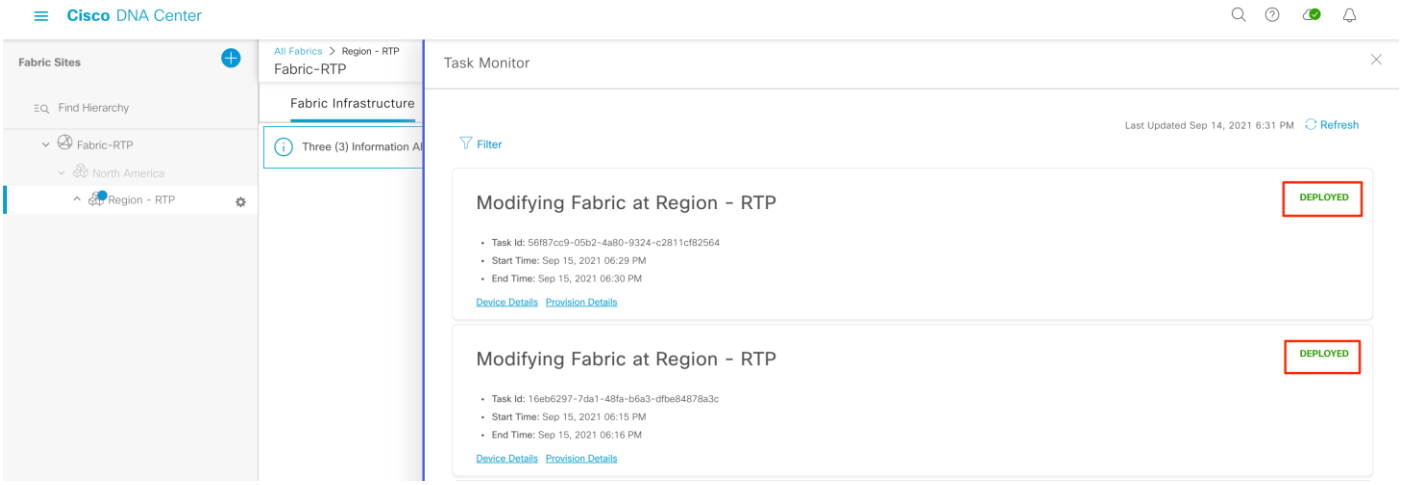


In the **Modify Fabric** slide out page, select **Schedule Operation: Now** and click **Apply**

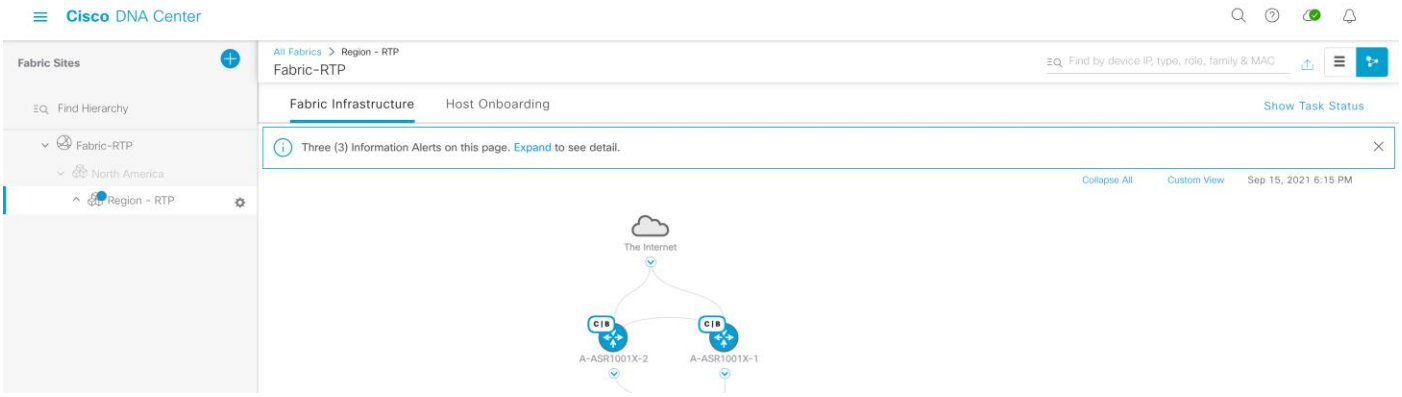


Step 10. View the status of the provision task by clicking **the Show Task Status**





Step 11. Repeat step 5 through step 10 to add any additional IOS-XE WAN Edge device at the site with Fabric Border and Control Plane functionality.



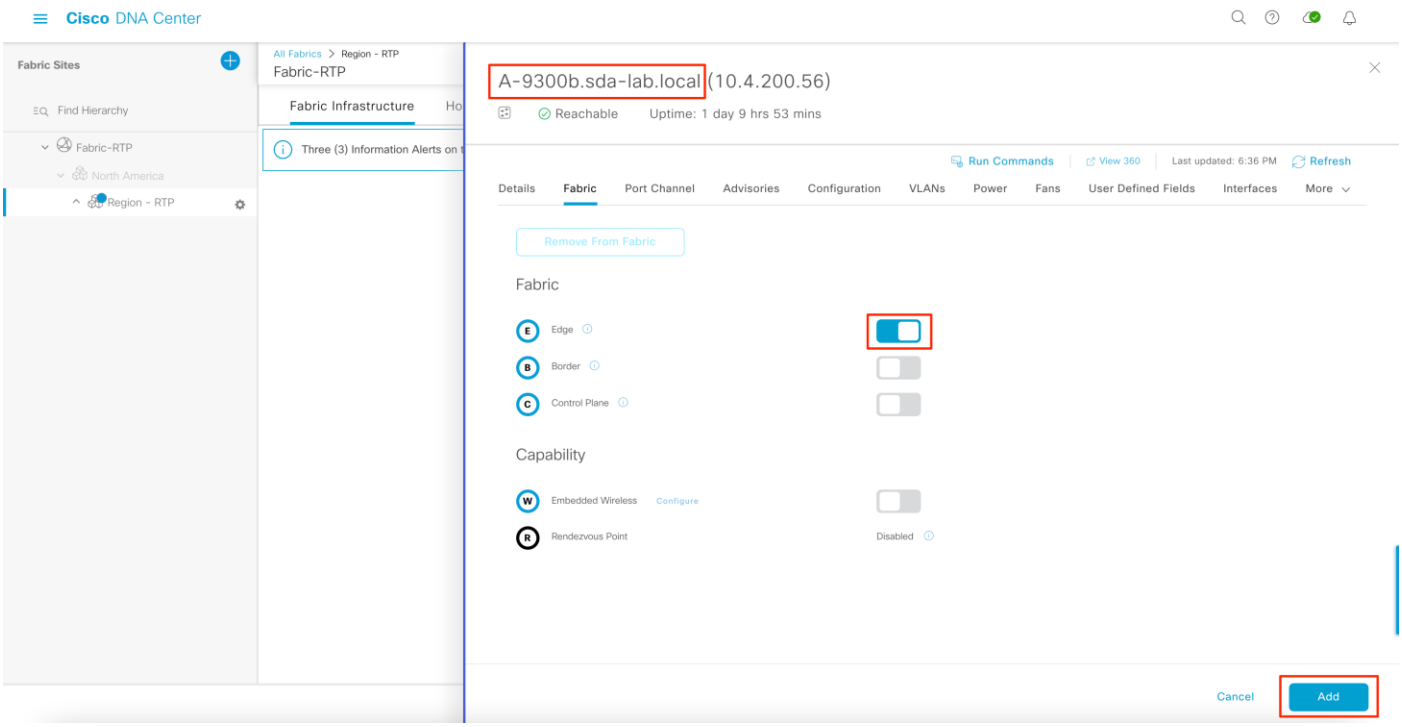
Tech tip
Cisco DNA Center automates the fabric border configuration with IP-based Layer 3 handoff. The IP Transit workflow provisions the fabric border with sub-interfaces for each VN extending the overlay segmentation to the peer-device, external-BGP neighborship is established to advertise prefixes from the fabric site and receive shared-services subnets from the peer-device. The peer-device, also commonly known as fusion device, takes cares of route-leaking between the extended overlay fabric site subnets and the global routing table containing the shared-service subnets. Please refer to Software-Defined Access Medium and Larger Site Fabric Provisioning guide on procedure to configure the peer-device.

It is also important to connect the two fabric site border nodes and configure internal-BGP session for each VN. This is needed for any Transit being deployed, either IP-Transit or SD-WAN transit, on the fabric Border Node. This would ensure the SD-Access LAN segment traffic is forwarded to other border in the case of uplink failures to both the WAN transport or to the peer device.

Step 12. Assign fabric Edge role to network devices

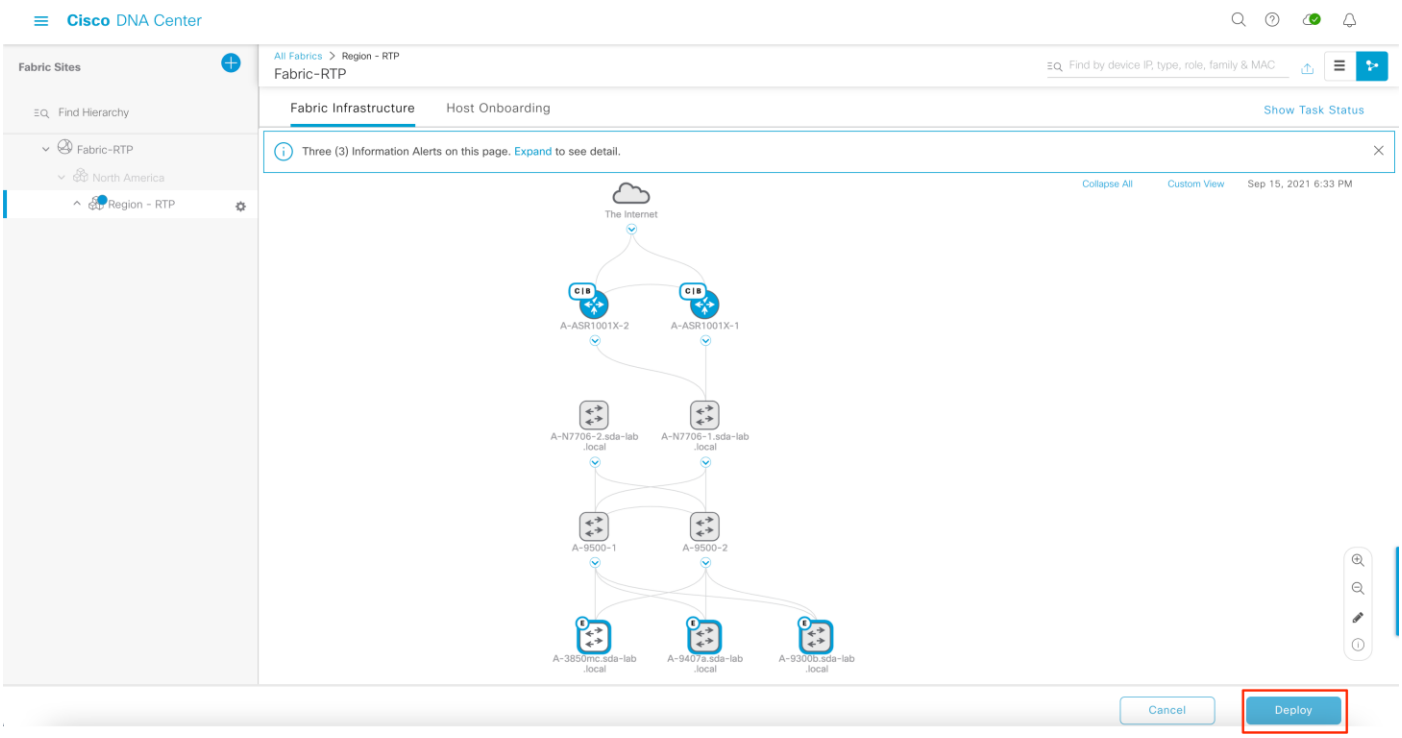
Click on the network device in the **Fabric Infrastructure** tab and select **Edge** role

Click **Add**

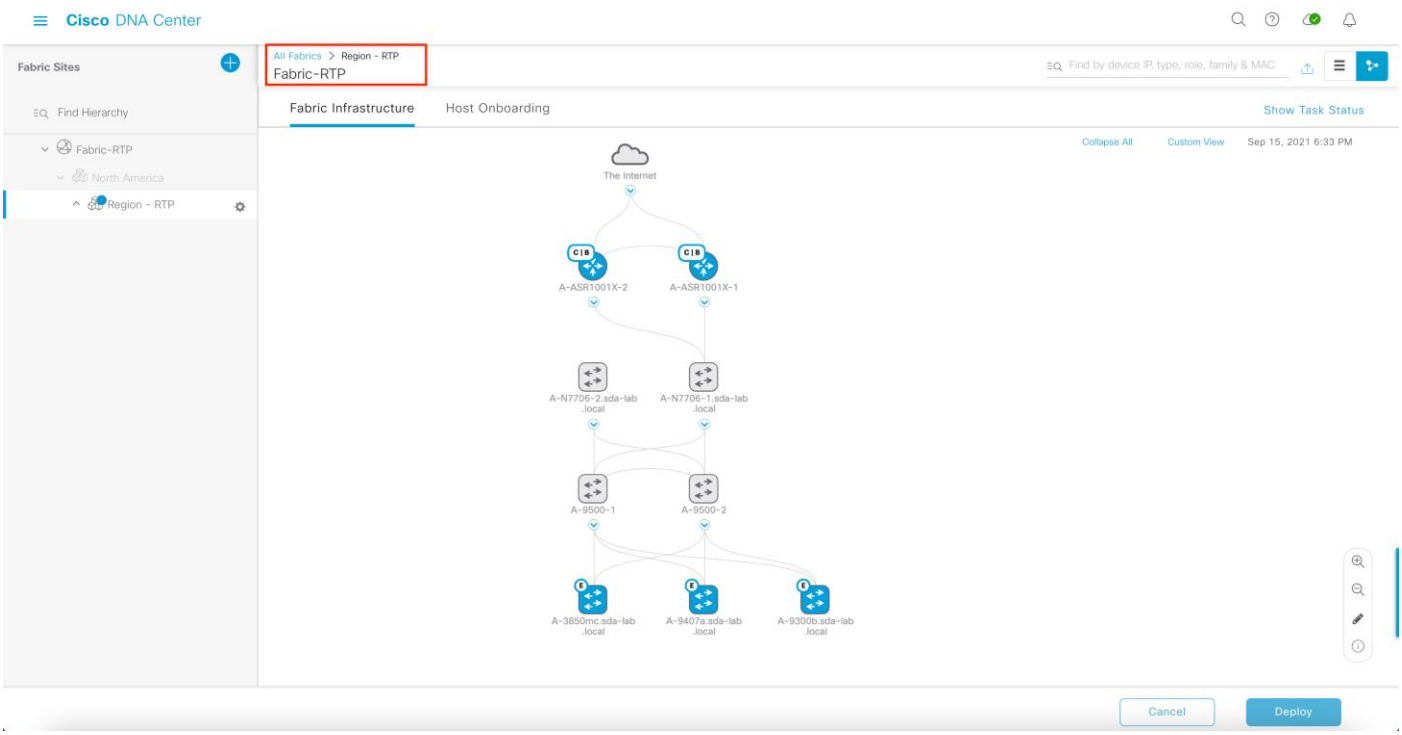


Repeat this step on other network devices that need to be provisioned with fabric **Edge** role

And click **Deploy**



In the **Modify Fabric** slide out page, select **Schedule Operation: Now** and click **Apply**



Tech Tip

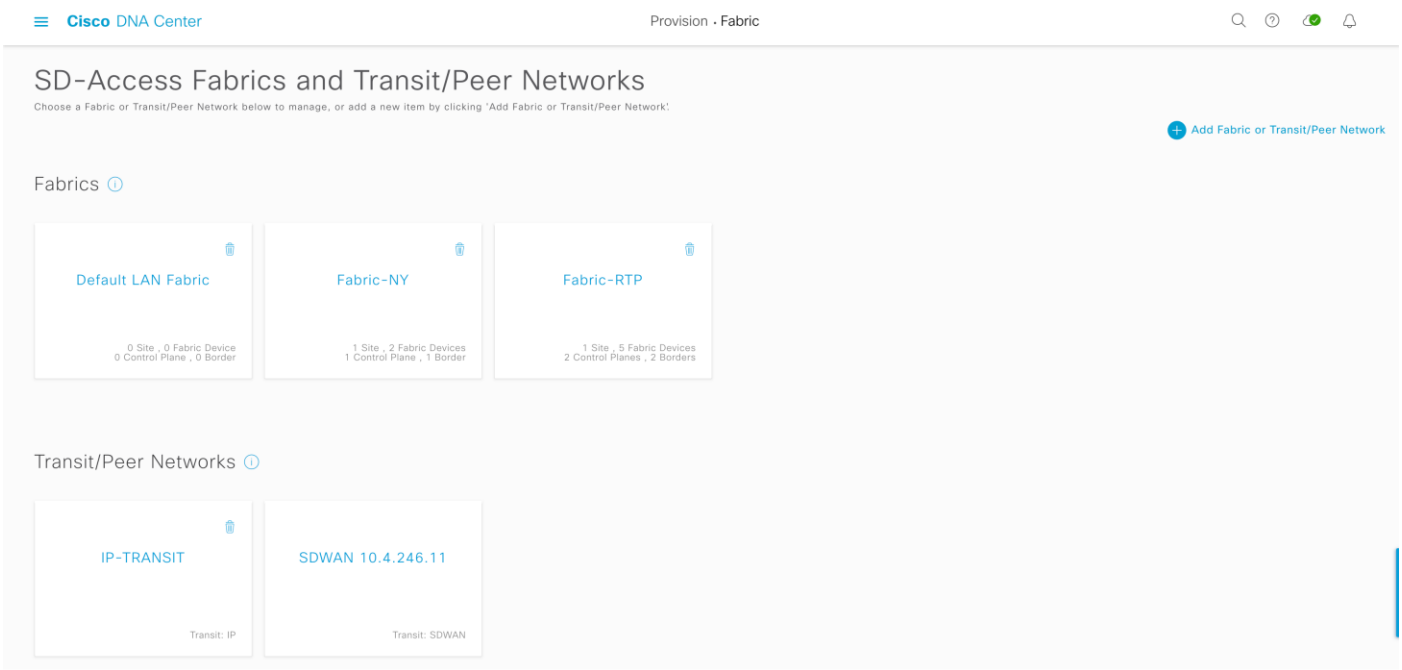
The Cisco SD-Access solution supports integration of wireless controller at each fabric site. The wireless controller can be either dedicated Wireless LAN Controller or Cisco Catalyst 9800 Embedded Wireless on Catalyst 9000 Series switch.

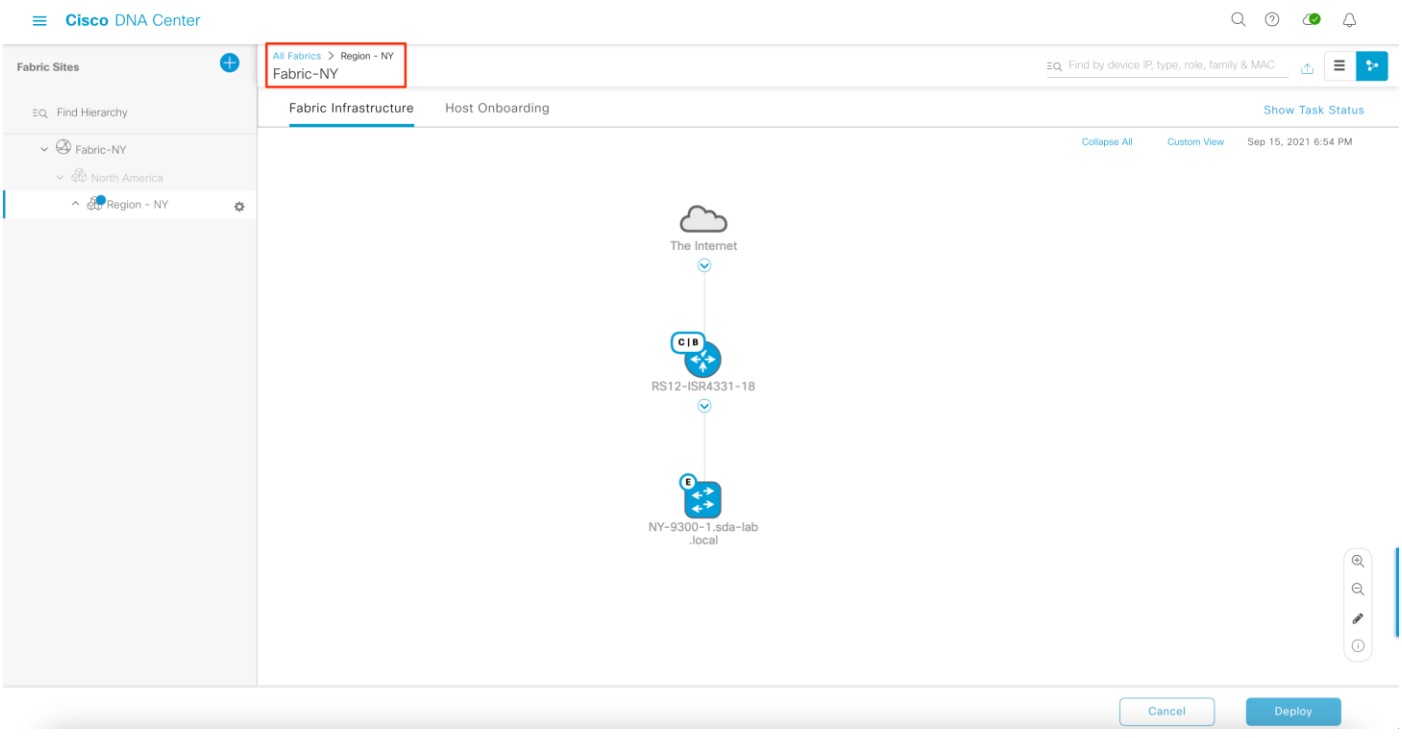
The Access Points (APs) within the fabric site need to establish a CAPWAP tunnel to WLC Management IP Address. APs associated in INFRA_VN must have IP reachability to the Management IP Address via the Global Routing Table within the fabric site. The WLC IP Address

reachability on the fabric edge node(s) must be through a more specific route and not through a default route. The management IP address of WLCs connect to or through the WAN Edge routers should be present in the Fabric GRT Service VPN.

Refer to Cisco SD-Access Design Guide and Cisco SD-Access Wireless Design and Deployment Guide for supported platform and detailed steps to implement fabric Wireless.

Step 13. Create additional **Fabric Sites** as necessary, with each fabric site connected to either **SDWAN Transit or IP-Transit or both**.

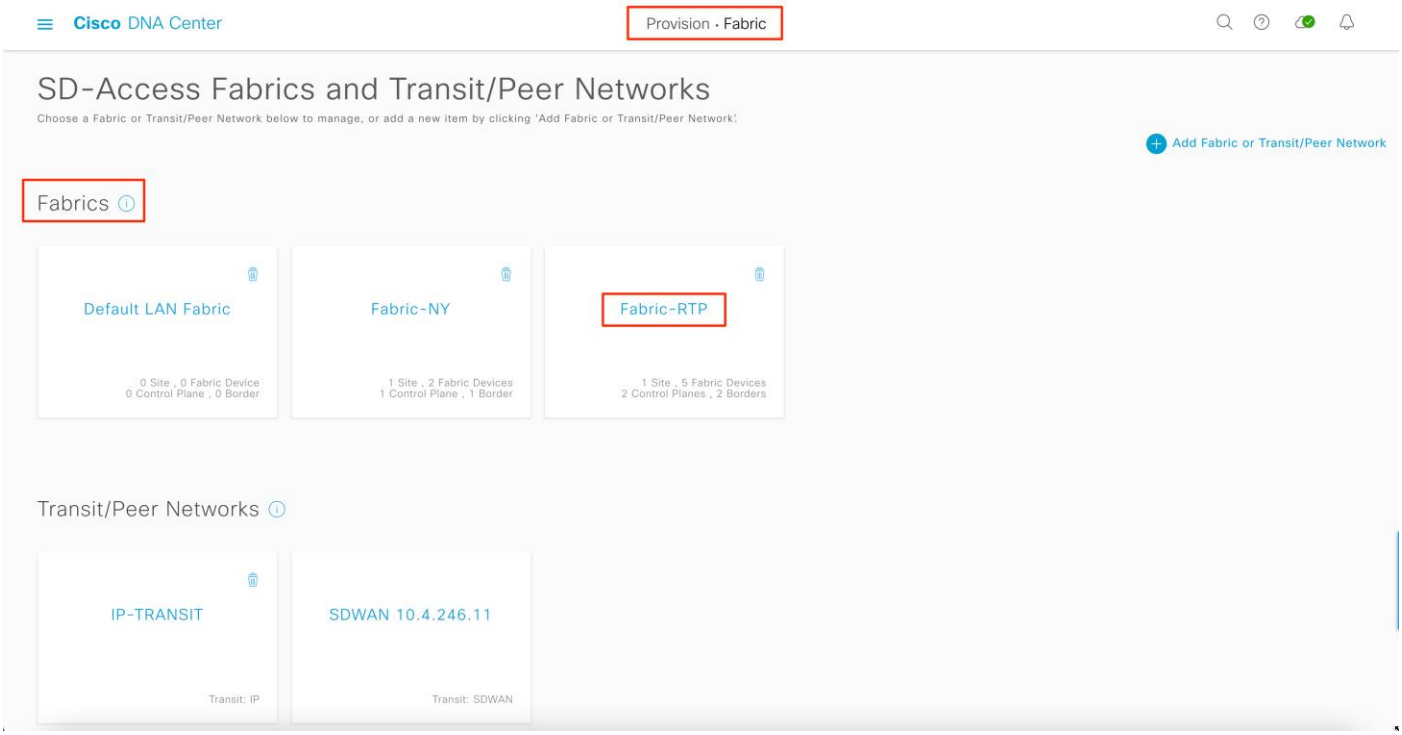




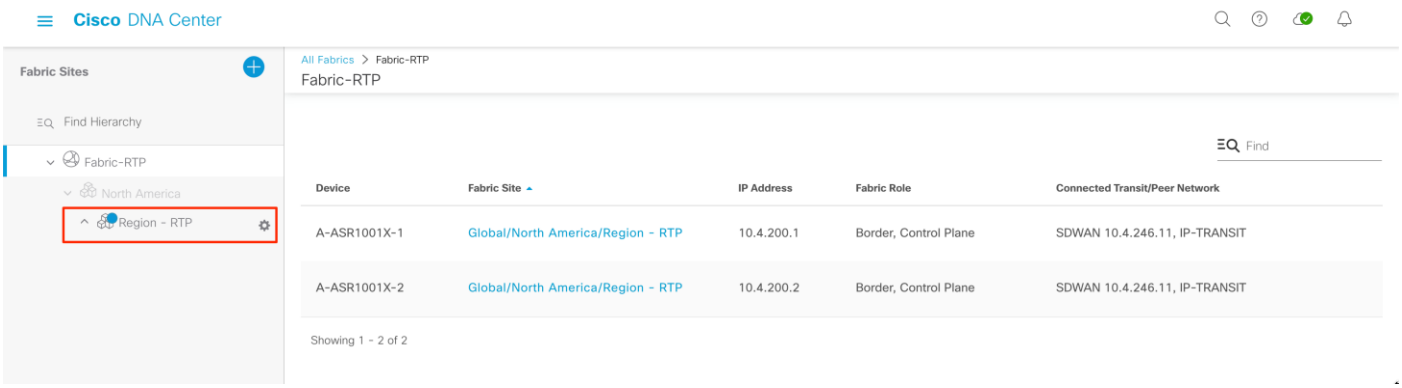
Procedure 4. Provision Fabric – Configure Host Onboarding

This section details the steps needed to select default Authentication Template for the site, associate IP Address pools to Virtual Networks and Wireless SSIDs and optionally configure Ports.

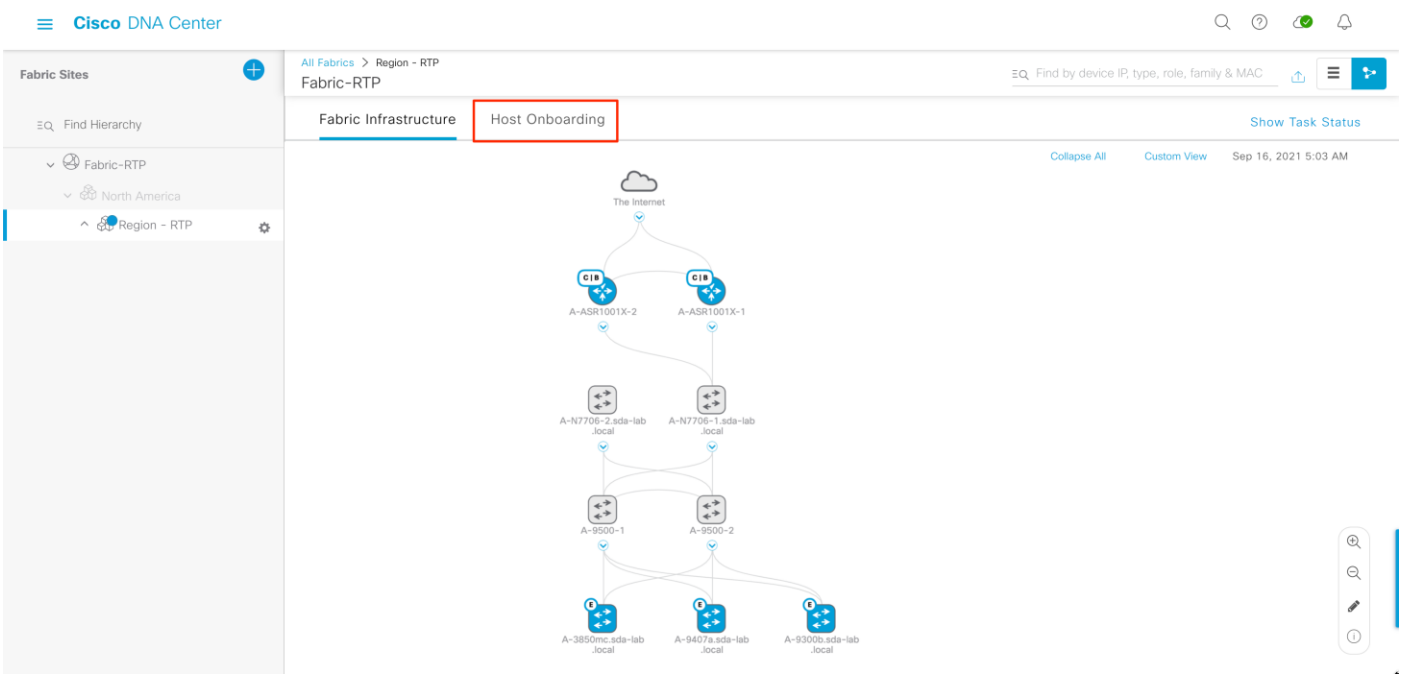
Step 1. In Cisco DNA Center, navigate to **Provision > Fabric**, select a **Fabric Site.**



Step 2. Select the site from the **Hierarchy**

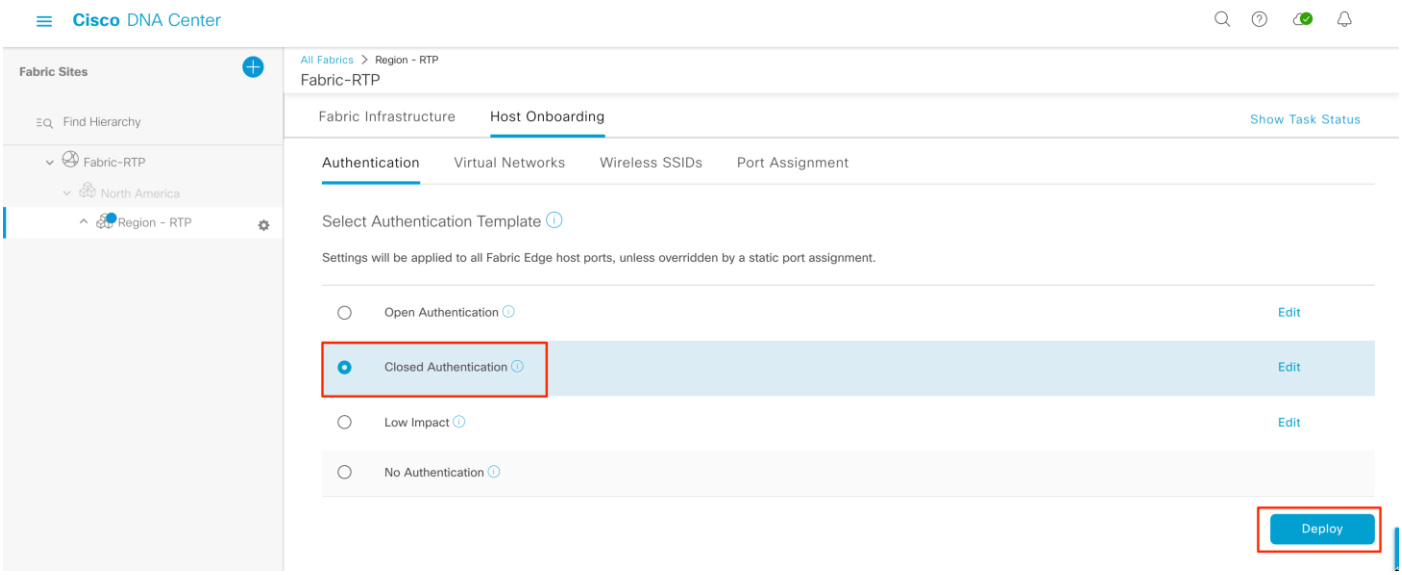


Step 3. Select **Host Onboarding** tab

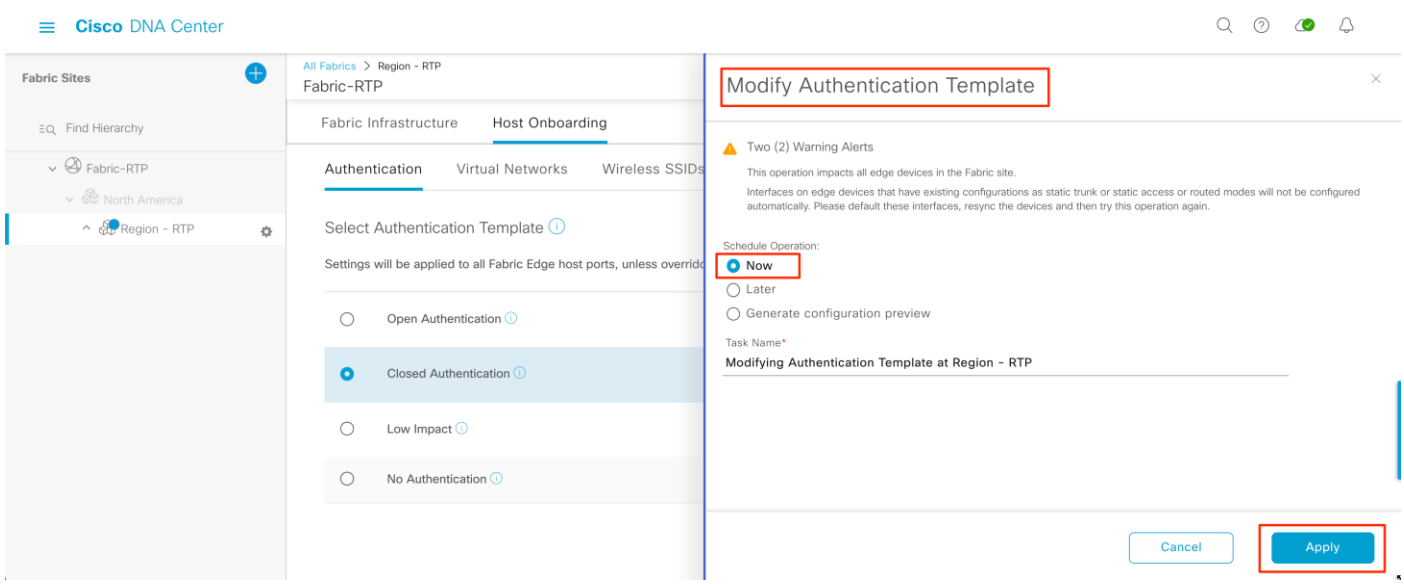


Step 4. Select the default **Authentication Template** for the fabric site

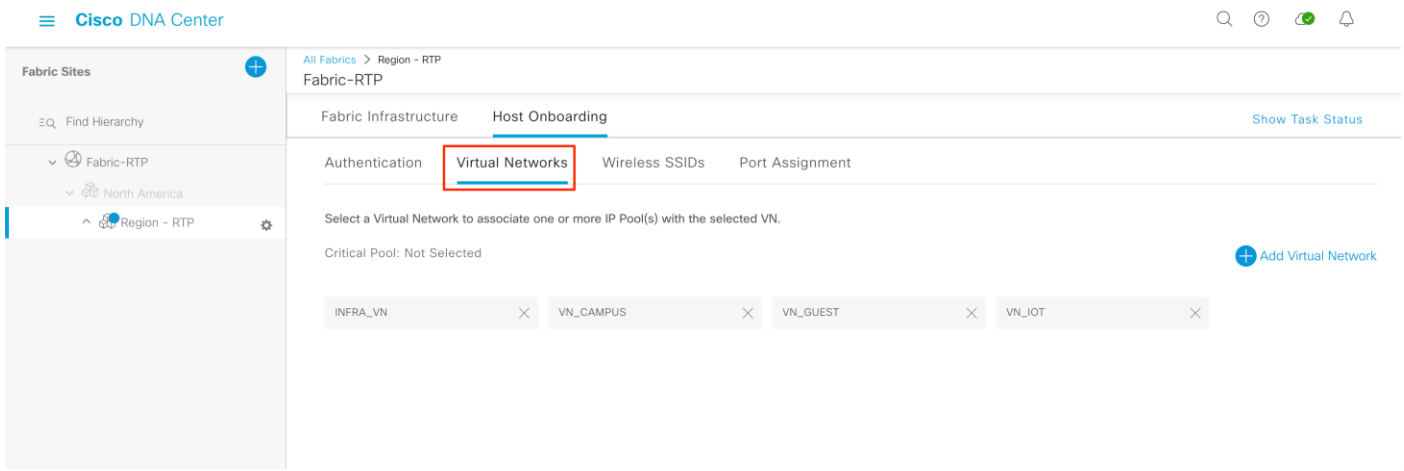
Click **Deploy**



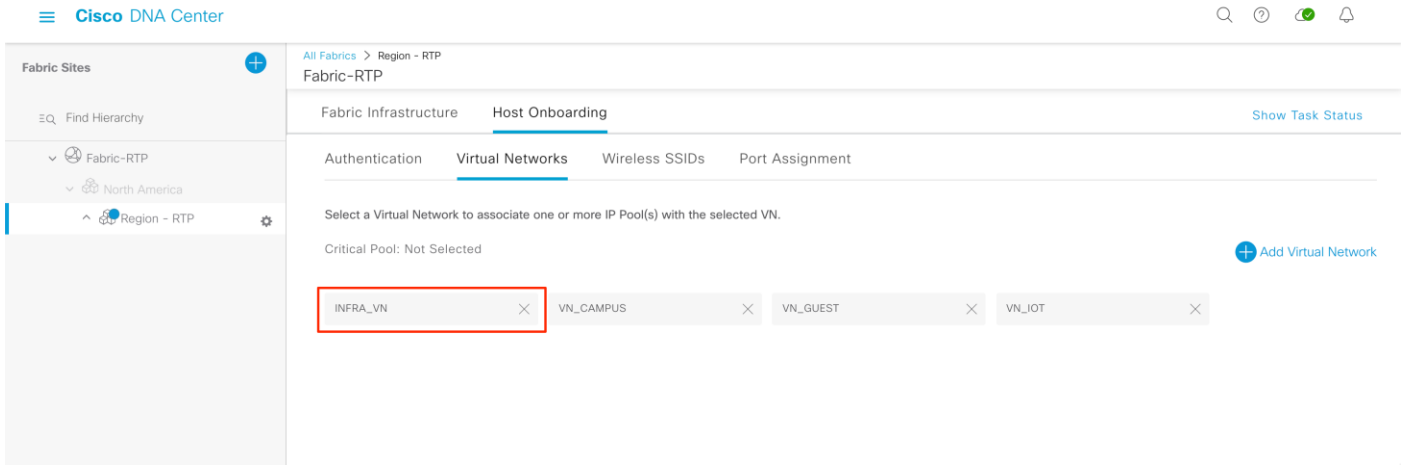
In the **Modify Authentication Template** slide-out page, select **Schedule Operation: Now** and click **Apply**



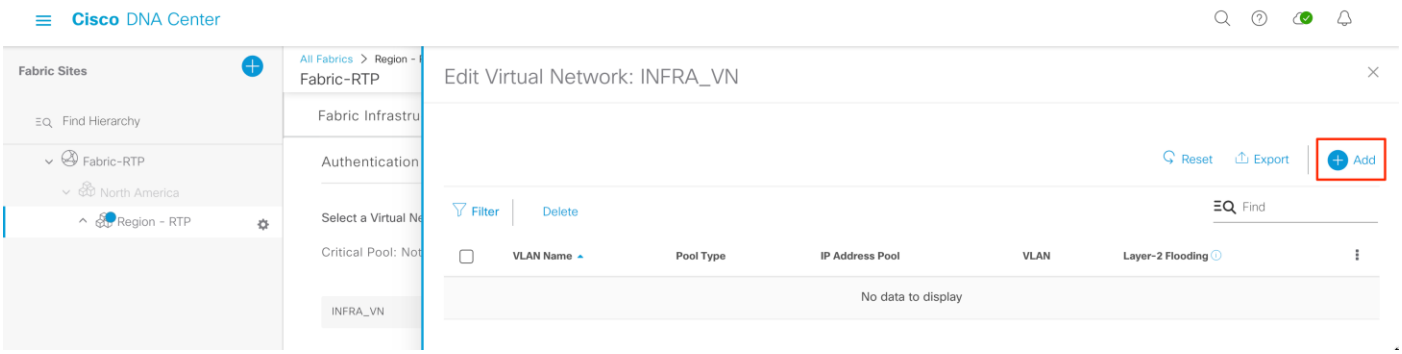
Step 5. Select **Virtual Networks** tab



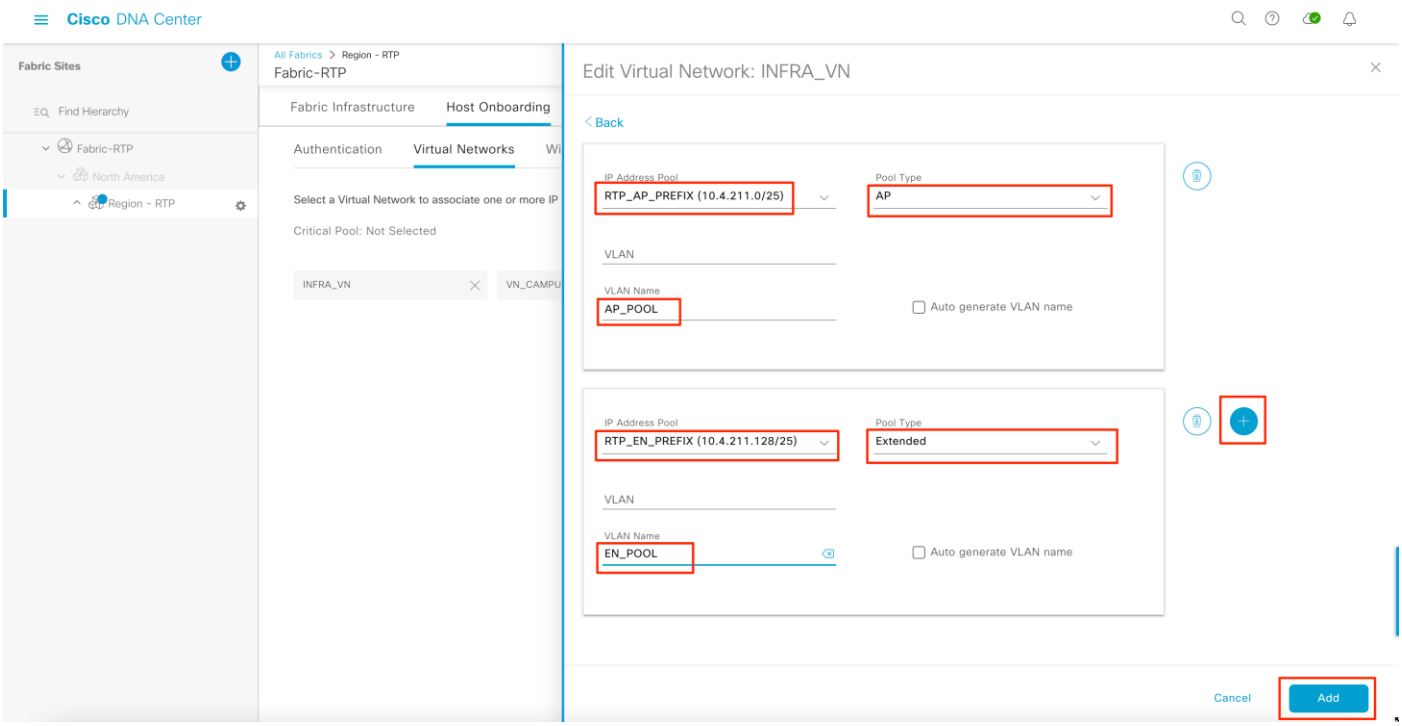
Select the **Virtual Network**



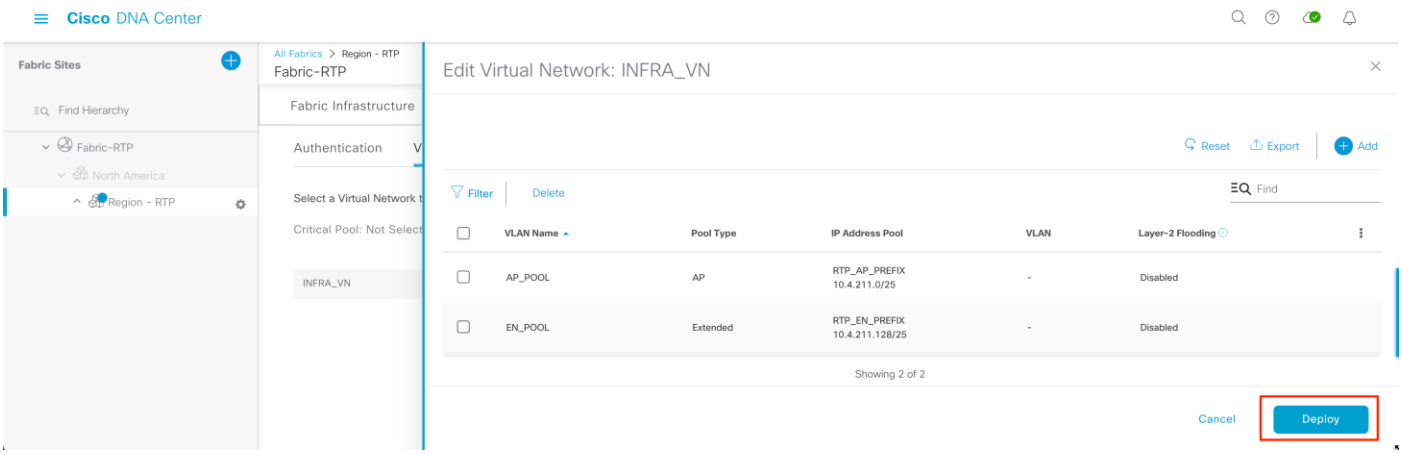
and click **Add**



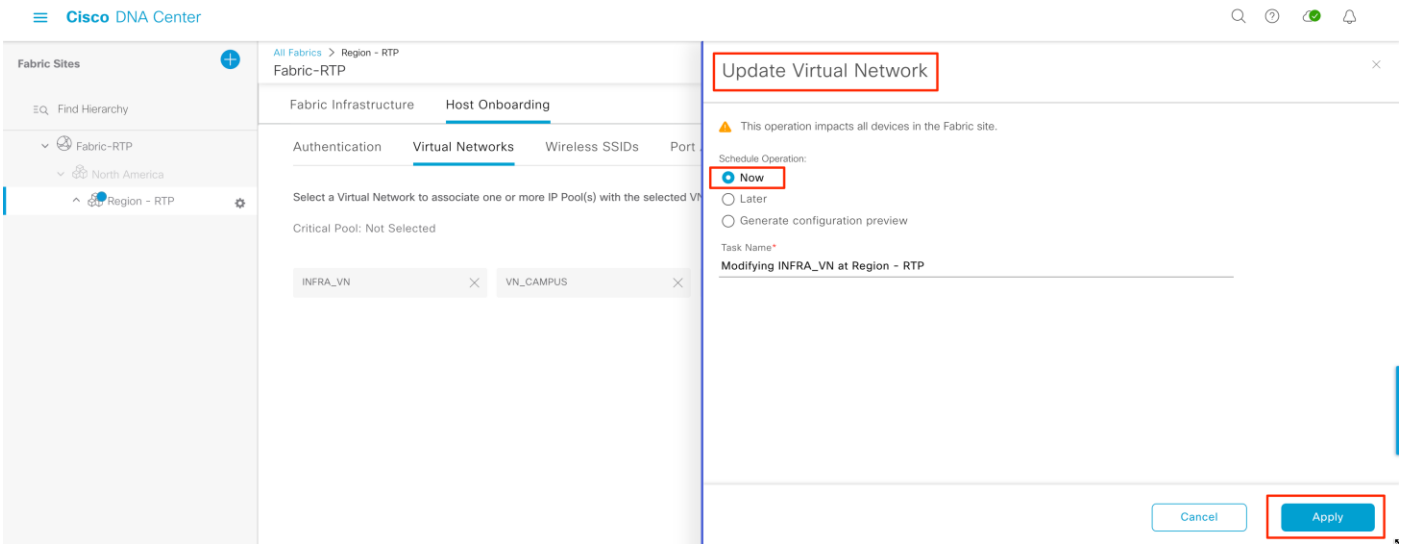
associate **IP Address Pool(s)** part of the Virtual Network and click **Add**

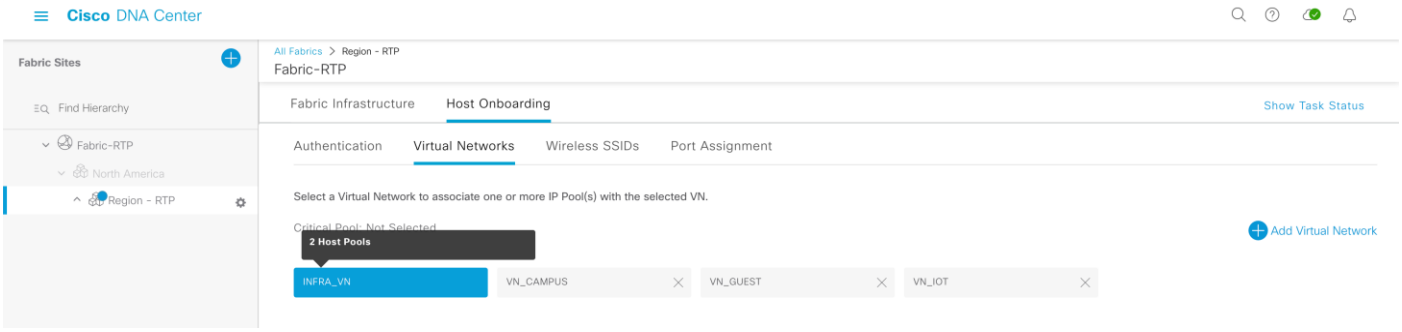


Verify the IP Address Pools and click **Deploy.**



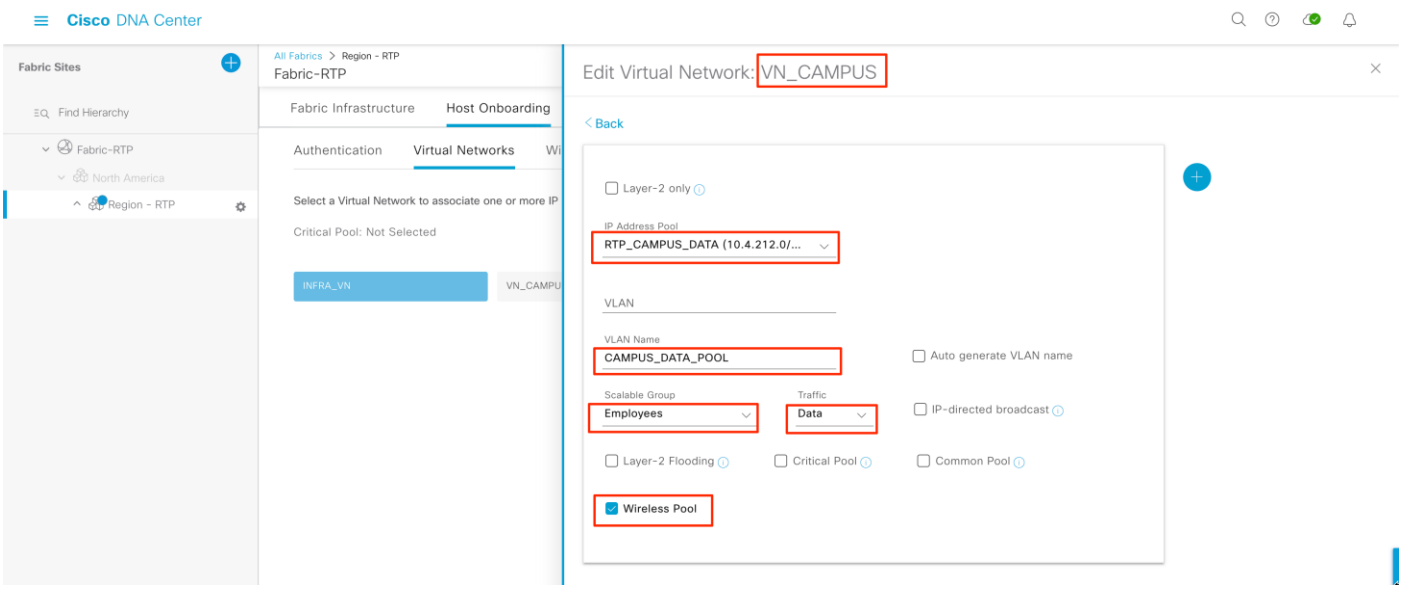
In the **Update Virtual Network** slide-out page, select **Schedule Operation: Now** and click **Apply**





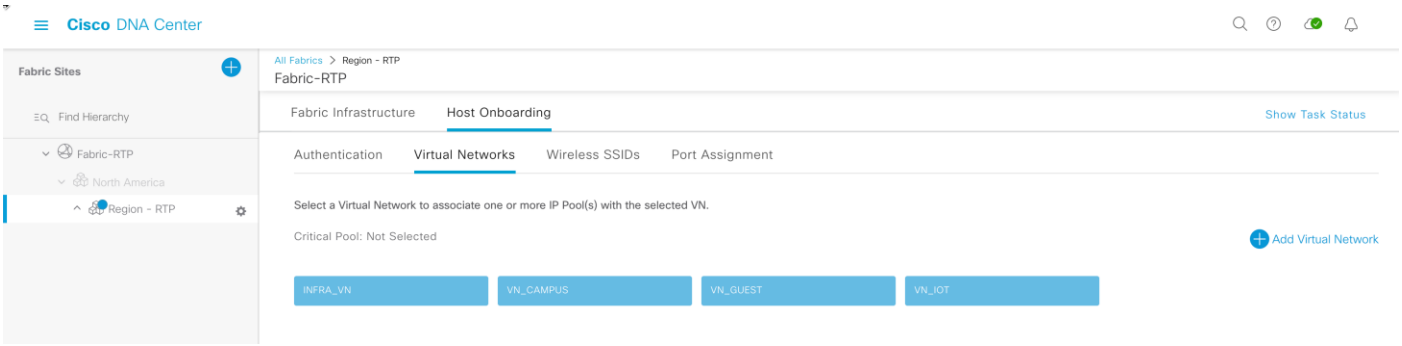
Step 6. Repeat the previous step, Step 5, to associate **IP Address Pools** to **Virtual Networks** for the site.

For Virtual Network (other than the INFRA_VN), configure **VLAN Name**, **Scalable Group**, **Traffic** and feature(s) that is required



Tech tip
Same VLAN Name can be used across multiple fabric sites with different IP Address Pool at each fabric site. This provides the simplicity to configure a single Authorization profile in Cisco ISE, that returns same VLAN name to the fabric edge on successful authenticated.

Step 7. View the Virtual Networks and associated IP Address Pool



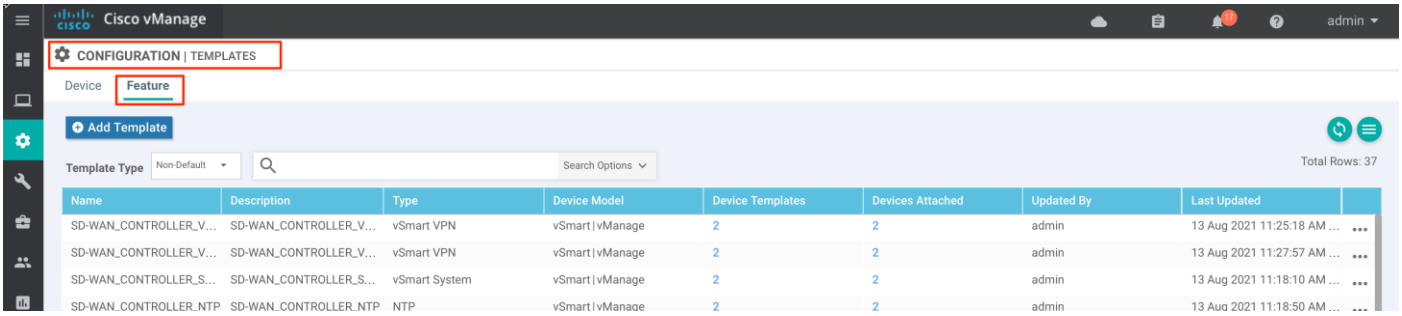
Procedure 5. Configure WAN Edge to advertise aggregate-summary routes for associated IP Address Pool

The IOS-XE SD-WAN WAN Edge device, which is colocated fabric Border, Control Plane node and WAN Edge device, is configured to re-distribute OMP to LISP and vice-versa. This will result in WAN Edge device advertising both the host prefixes and network subnet for each IP Address Pool associated to Virtual Network.

To optimize and avoid advertising the host entries to remote sites, configure corresponding vManage > Cisco VPN feature template to advertise aggregate-summary subnets for each IP Address pool configured in the Virtual Network.

This section details steps to configure Cisco VPN templates to advertise aggregate-summary routes

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



Step 2. Search Service VPN, **Cisco VPN** feature template that was previously created for each Virtual Network.

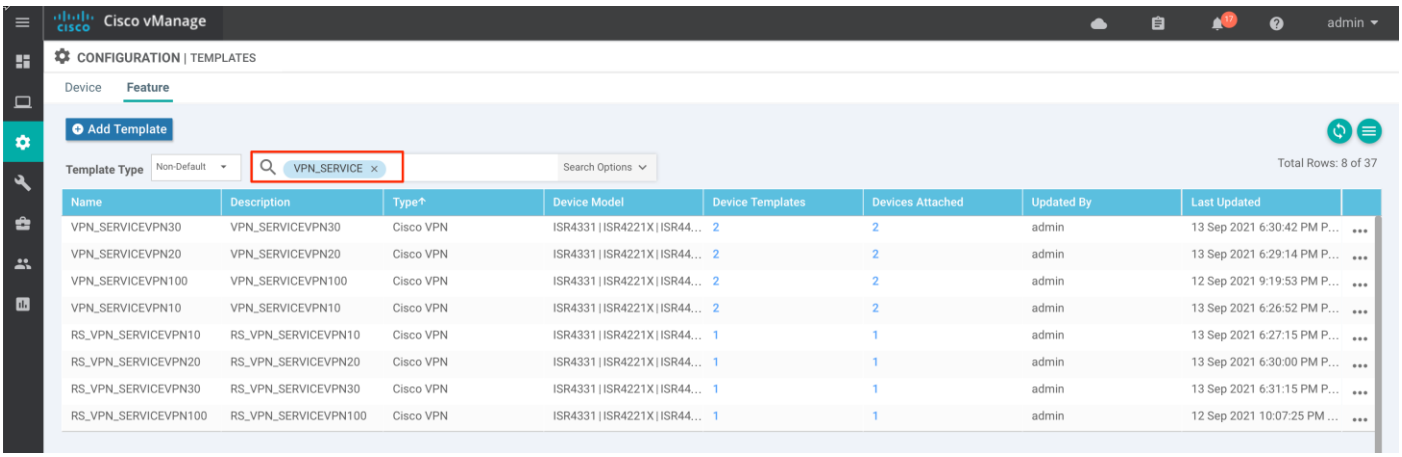
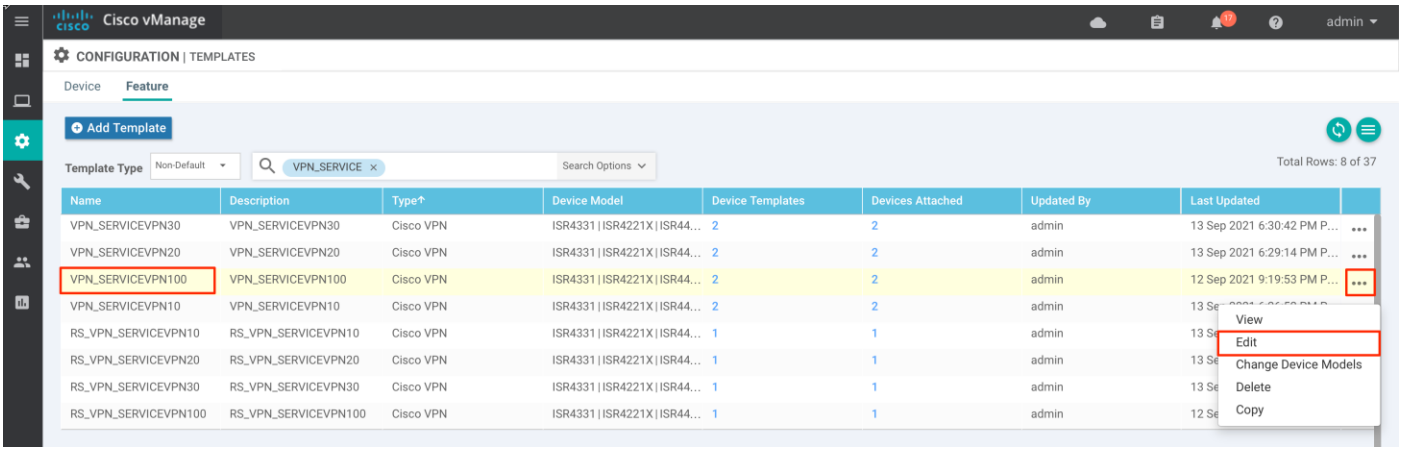


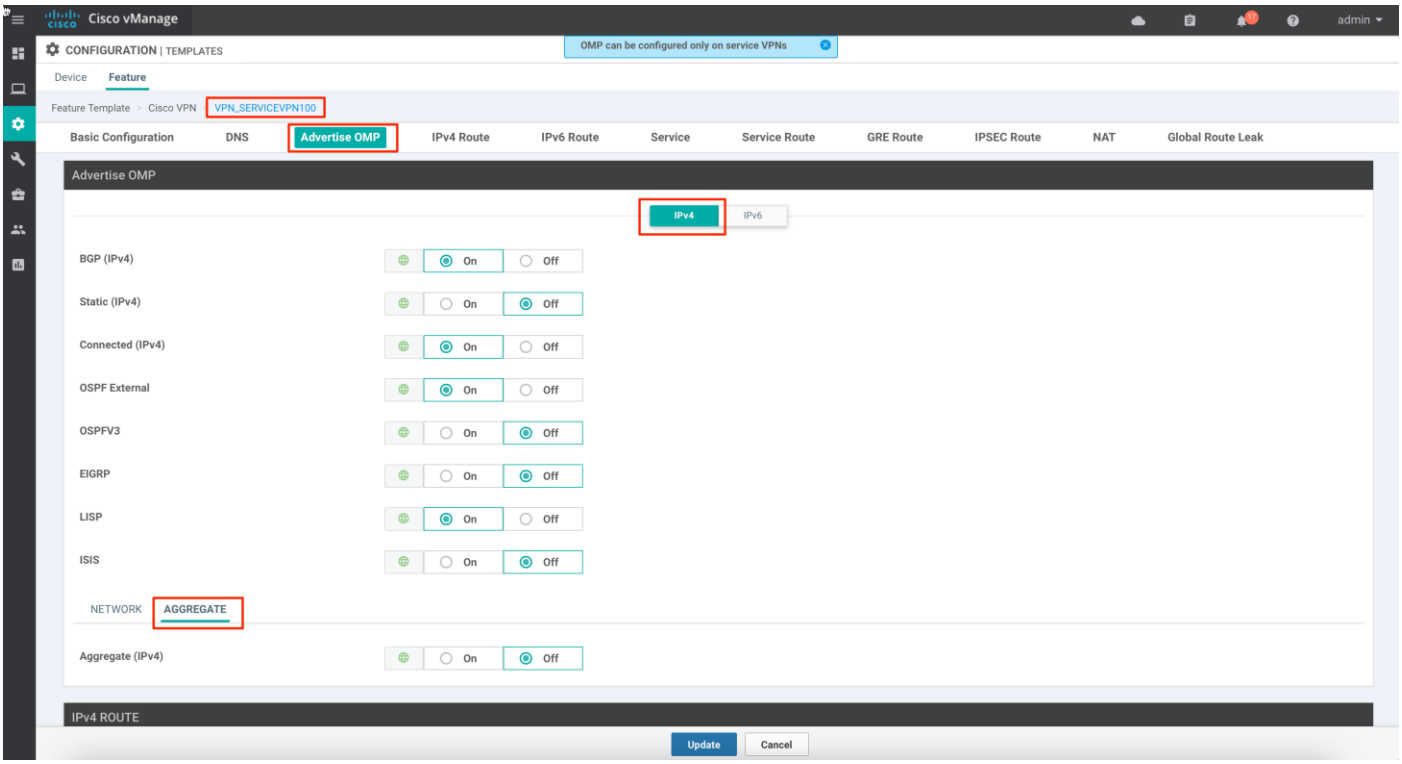
Table 4. Service VPN – Virtual Network mapping

Site	Virtual Network	Service VPN	Feature Template
Fabric-RTP	INFRA_VN + GRT	VPN 100	VPN_SERVICEVPN_100
	VN_CAMPUS	VPN 10	VPN_SERVICEVPN_10
	VN_IoT	VPN 20	VPN_SERVICEVPN_20
	VN_GUEST	VPN 30	VPN_SERVICEVPN_30
Fabric-NYC	INFRA_VN + GRT	VPN 100	RS_VPN_SERVICEVPN_100
	VN_CAMPUS	VPN 10	RS_VPN_SERVICEVPN_10
	VN_IoT	VPN 20	RS_VPN_SERVICEVPN_20
	VN_GUEST	VPN 30	RS_VPN_SERVICEVPN_30

Step 3. Select each Cisco VPN template, click three dots (…) and select **Edit**

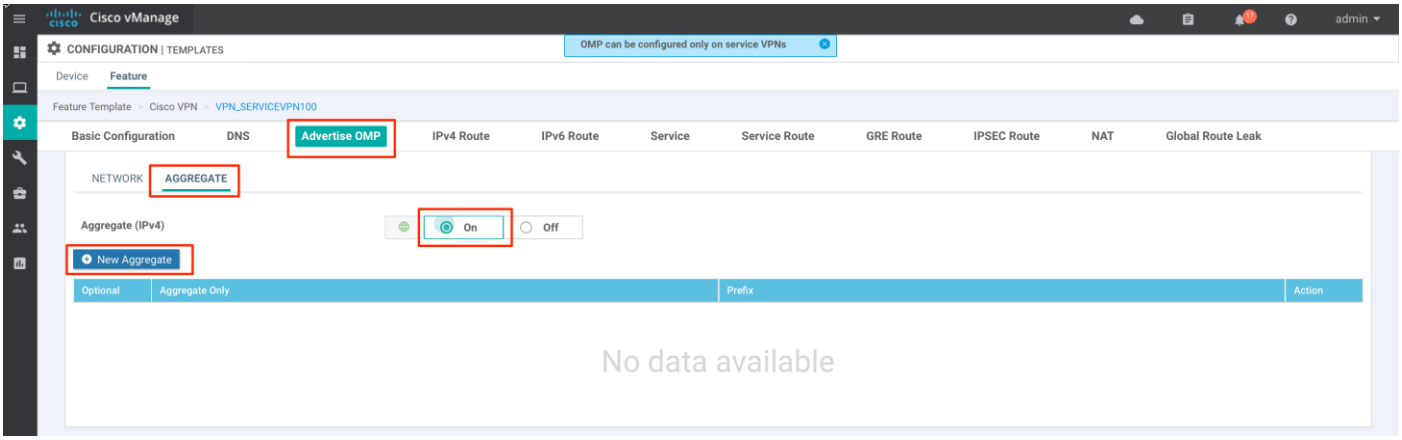


Step 4. Select **Advertise OMP**, under **IPv4** section select **Aggregate** tab



Step 5. Select **Aggregate (IPv4): On**

And select **Add Aggregate**

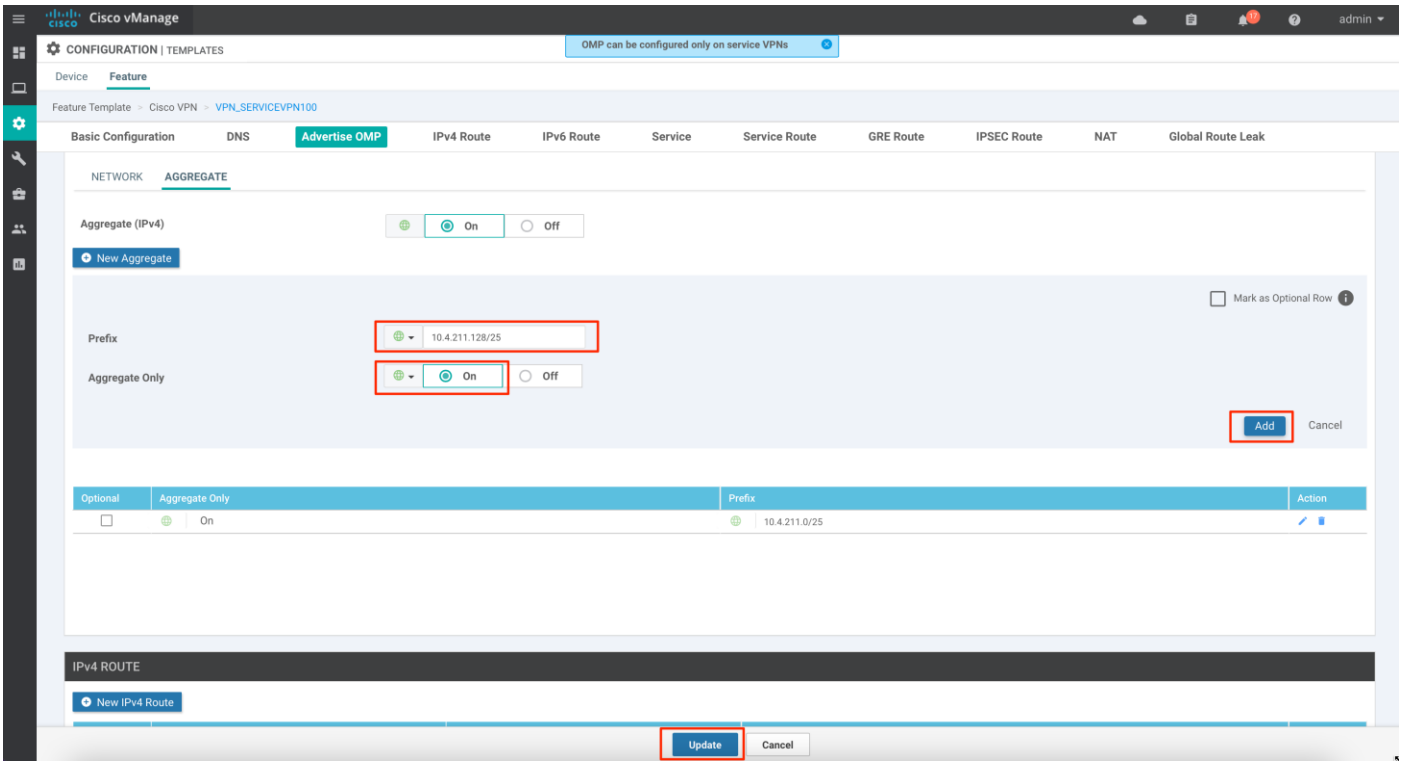


Input **Prefix**

Select **Aggregate Only: ON**

And **click Add**

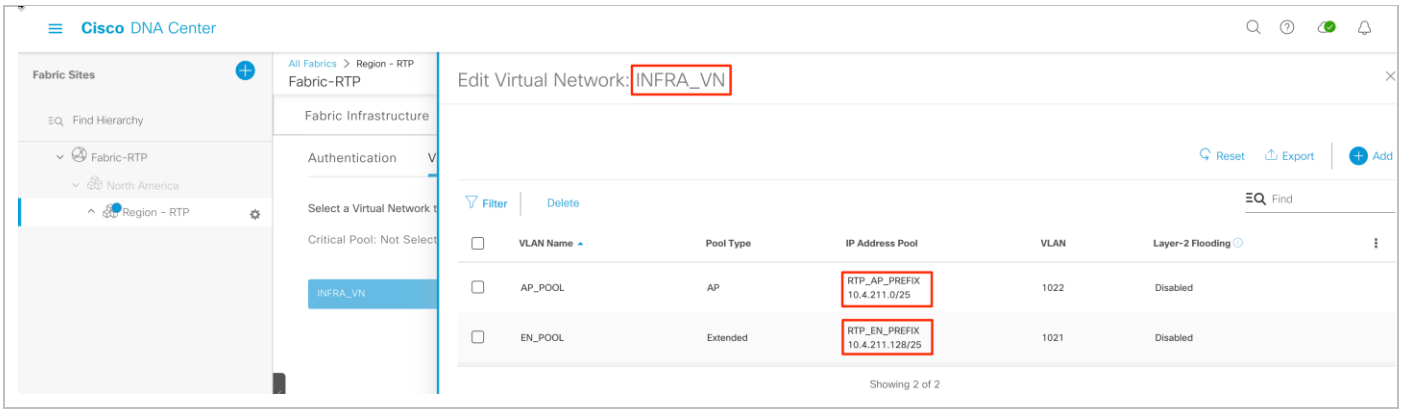
And select **Update** at the bottom of the page



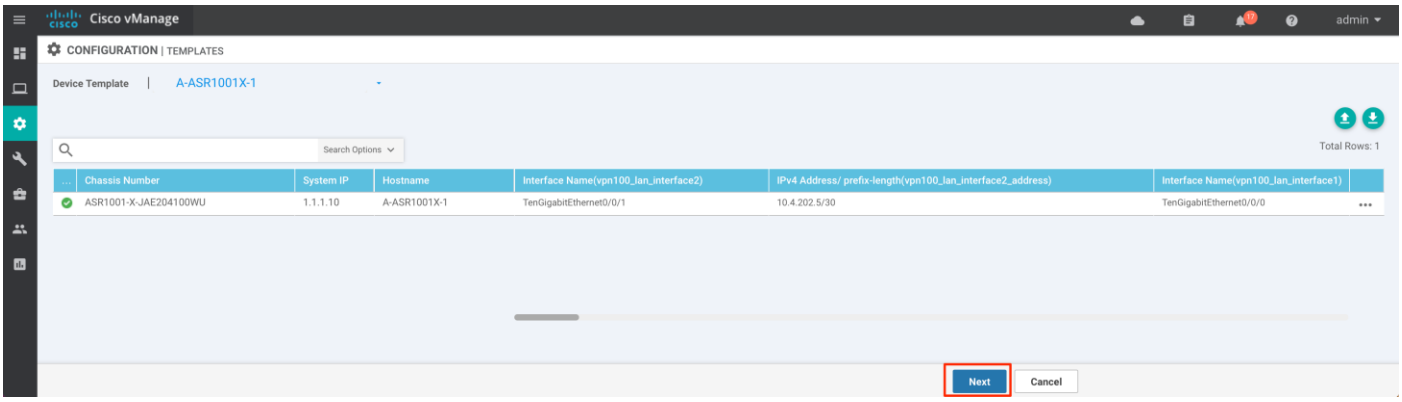
Tech Tip

The network IP Address prefix can be obtained from Cisco DNA Center. Navigate to **Provision > Fabric > Fabric Site > Fabric Site > Host Onboarding > Virtual Networks** tab. Click each **Virtual Network** to view the **IP Address Pool** provisioned. Configure the IP Address prefixes to corresponding **Service VPN** in vManage.

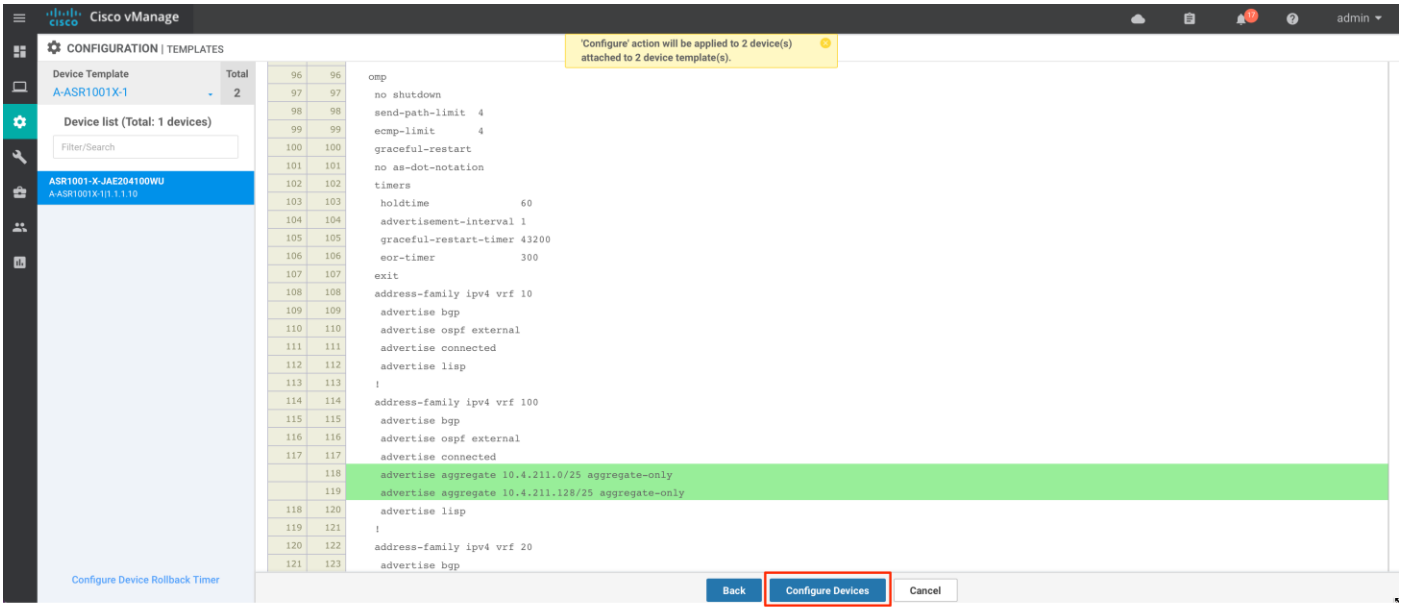
Please note the IP Address prefix in the *INFRA_VN* is mapped to Service VPN 100 (Fabric GRT Service VPN) in vManage.



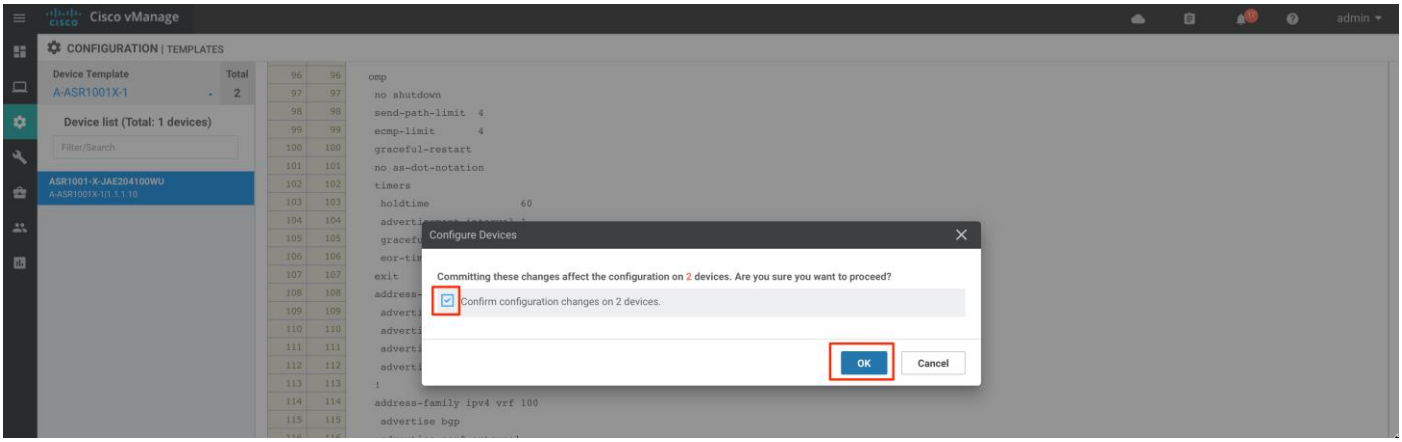
Step 6. Click **Next**

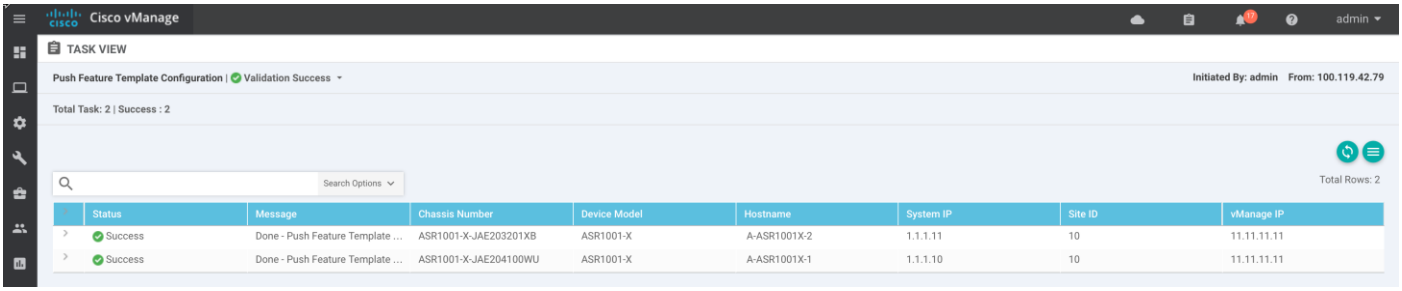


And select **Configure Devices**

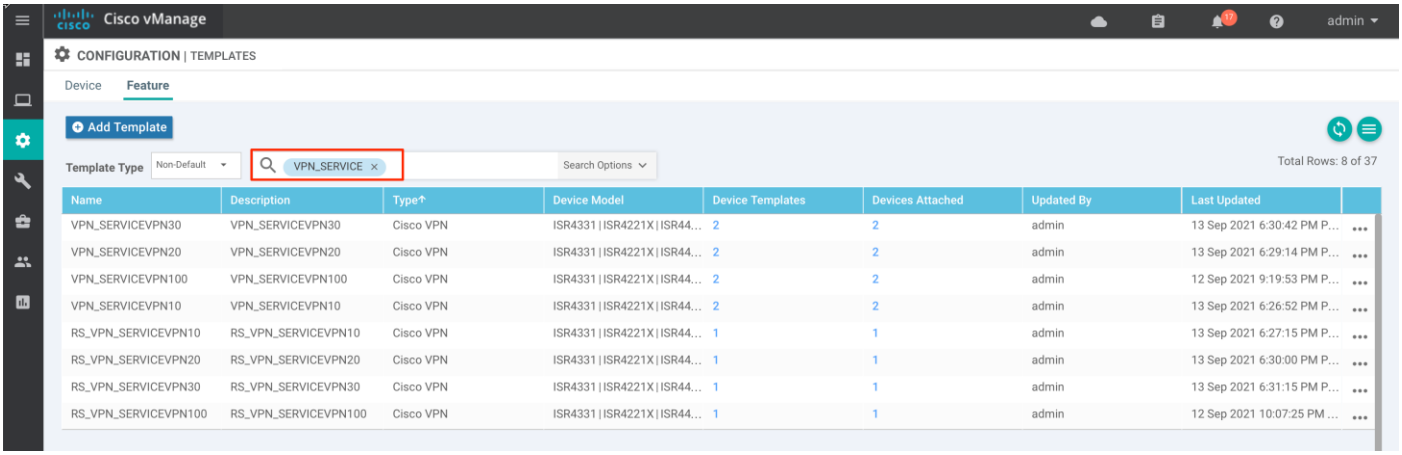


Enable the option to **Confirm Configuration changes** and click **OK**





Step 7. Repeat Step 3 through Step 6, for each Service VPN template to advertise only the aggregate routes in the OMP protocol across SD-WAN fabric to other sites.



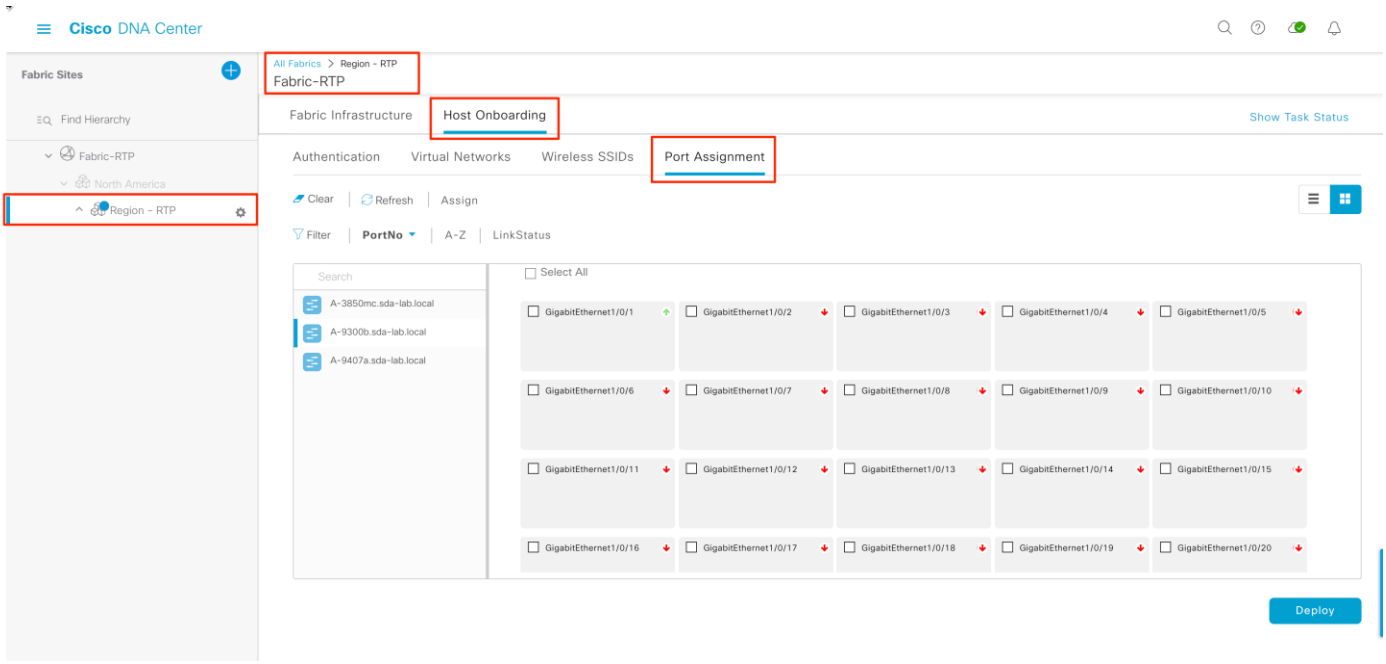
Procedure 6. (Optional) Provision Fabric – Port Assignment

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 downloaded 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 next steps 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 are dynamically assigned via ISE Authorization polices.

Step 1. In Cisco DNA Center, navigate to **Provision > Fabric**, select the appropriate **Fabric Site > Host Onboarding > Port Assignment** tab



Step 2. select the **Fabric Node** and click on the **Interface**

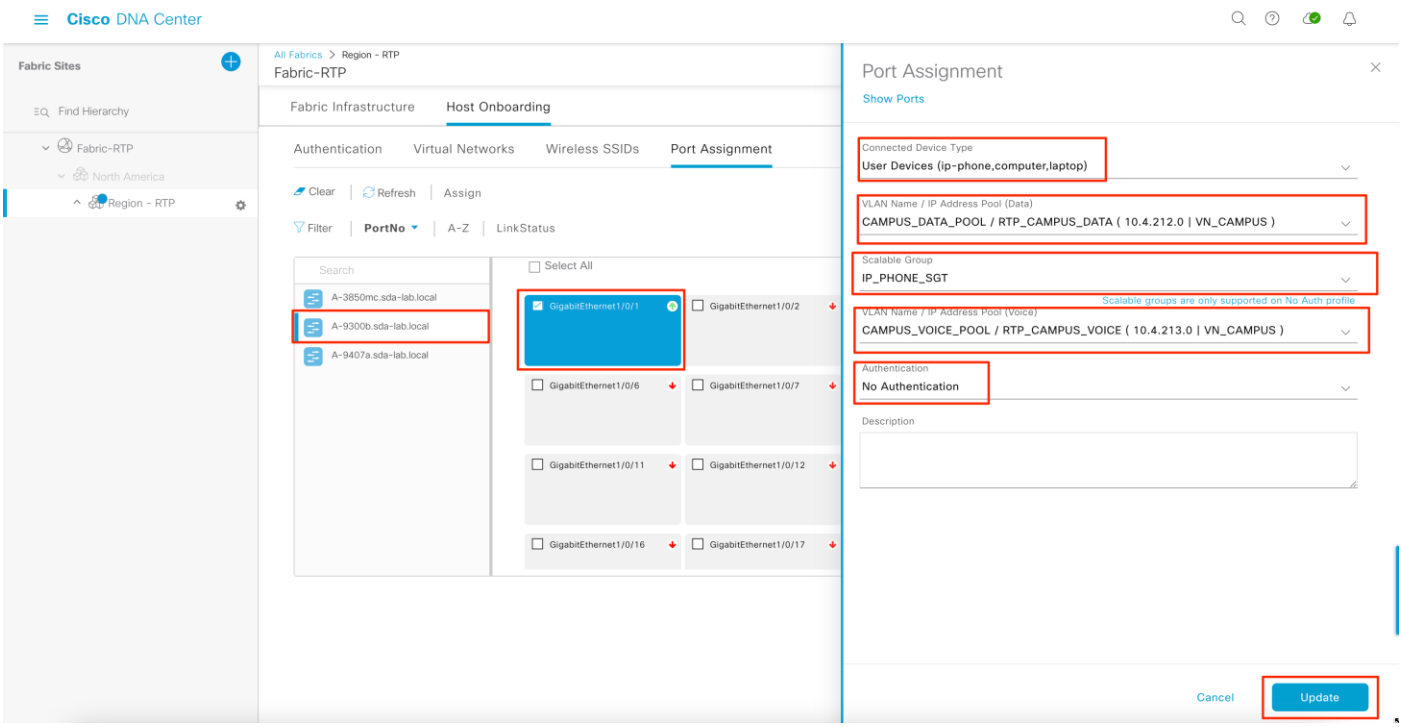
input **Connected Device Type: User Devices**

select the **IP Address Pool** from the drop-down options for **Voice** and/or **Data**

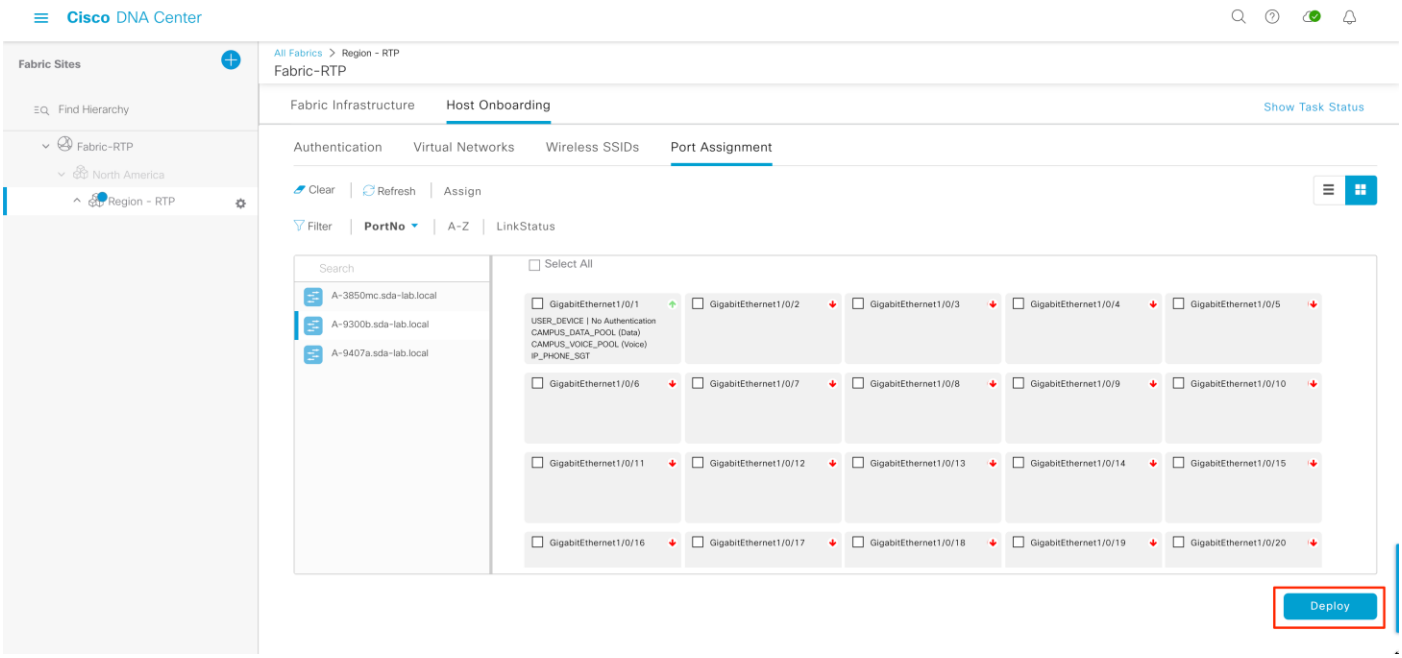
select the **Scalable Group** for endpoint connected to the interface

select **Authentication: No Authentication**

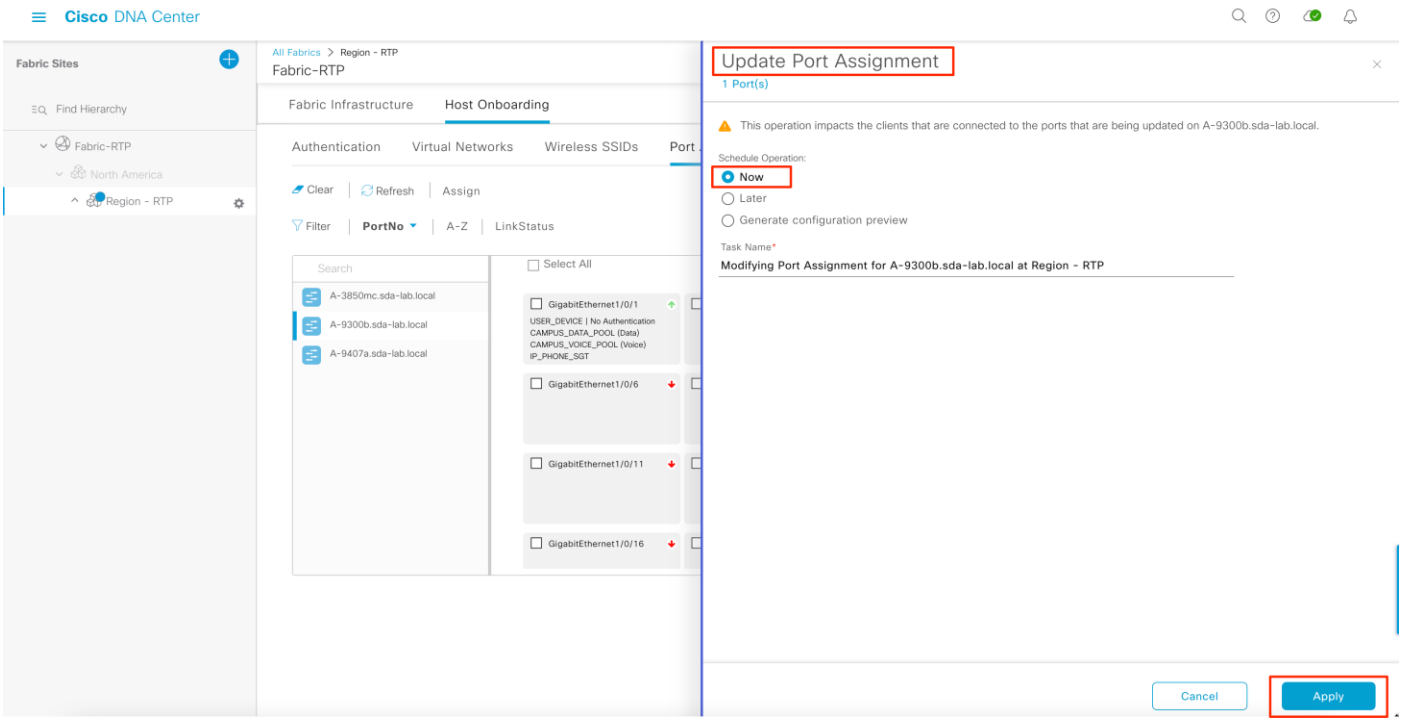
and click **Update**



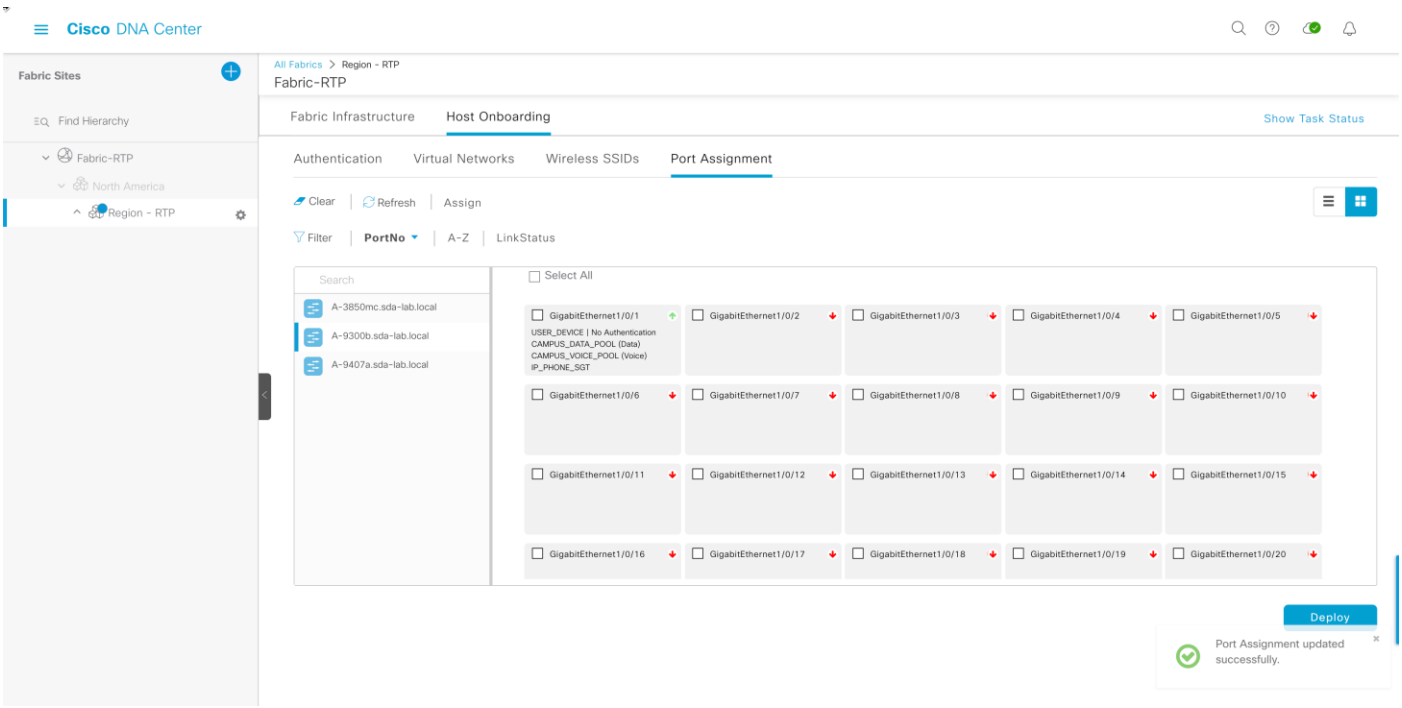
Step 3. Configure additional interfaces on the same fabric node and click **Deploy**



In the **Update Port Assignment** slide-out page, select **Schedule Operation: Now** and click **Apply**



Step 4. View the static Port Assignment for the device

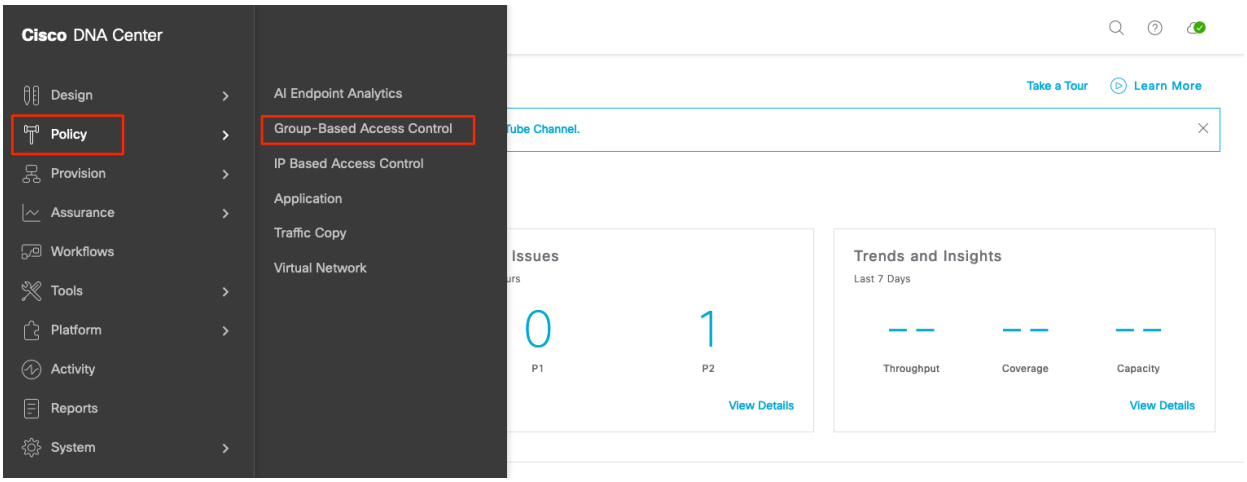


Process 7: Defining Group-Based Access Control Policies

This section details the procedure to configure 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.

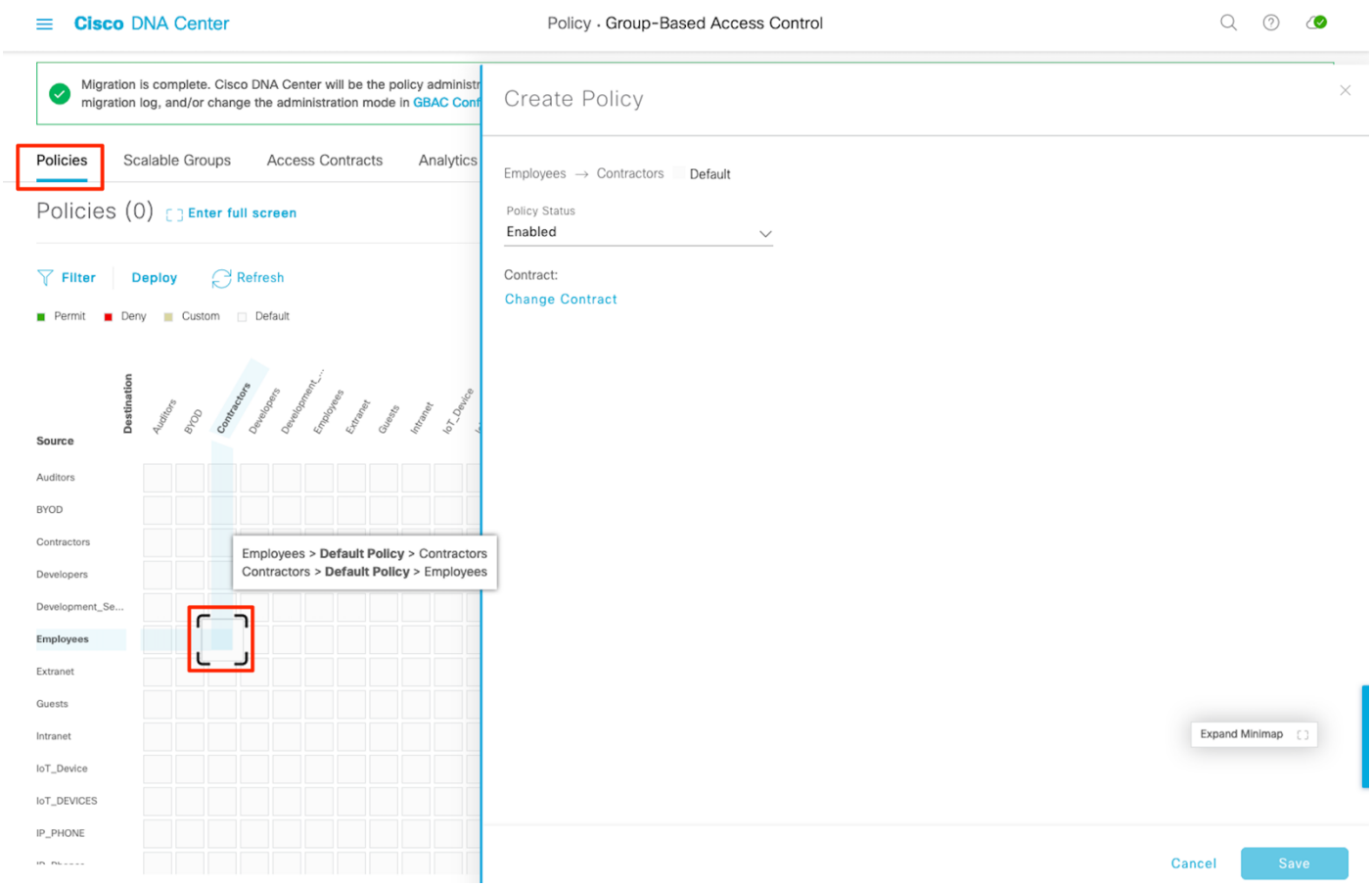
Procedure 1. Configure Group-Based Access Control policies

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

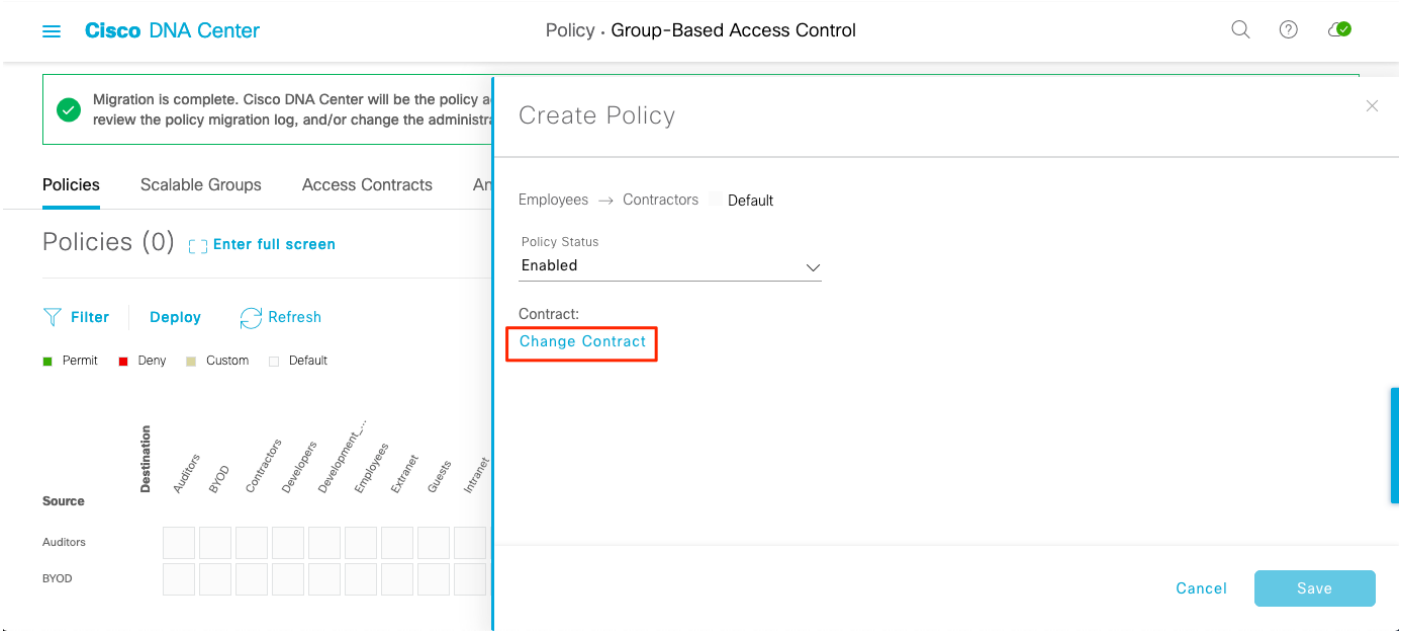


Step 2. Under **Policies** tab, click the appropriate **Source/Destination** matrix element.

The Create Policy slide-out panel appears.



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

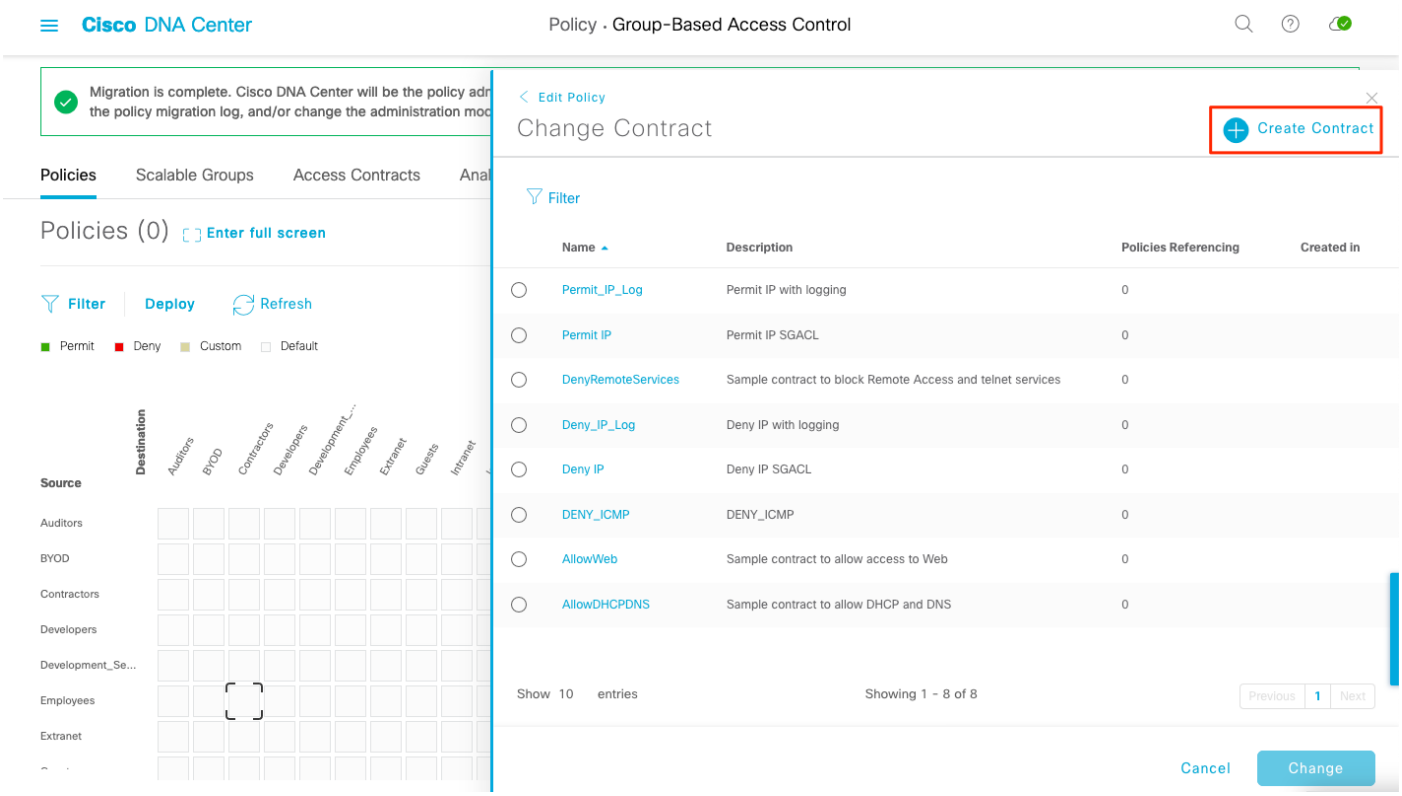


Step 4. Select one of the existing or predefined contracts from the list.

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.

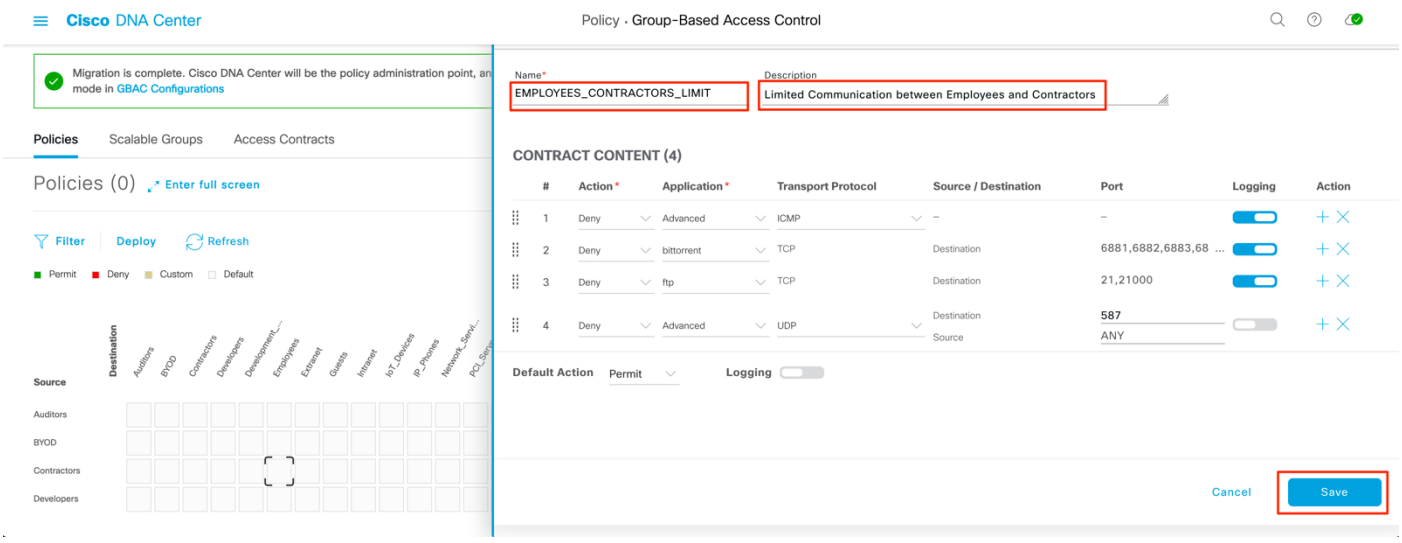
Step 5. If creating a new contract, click **Create Contract**.



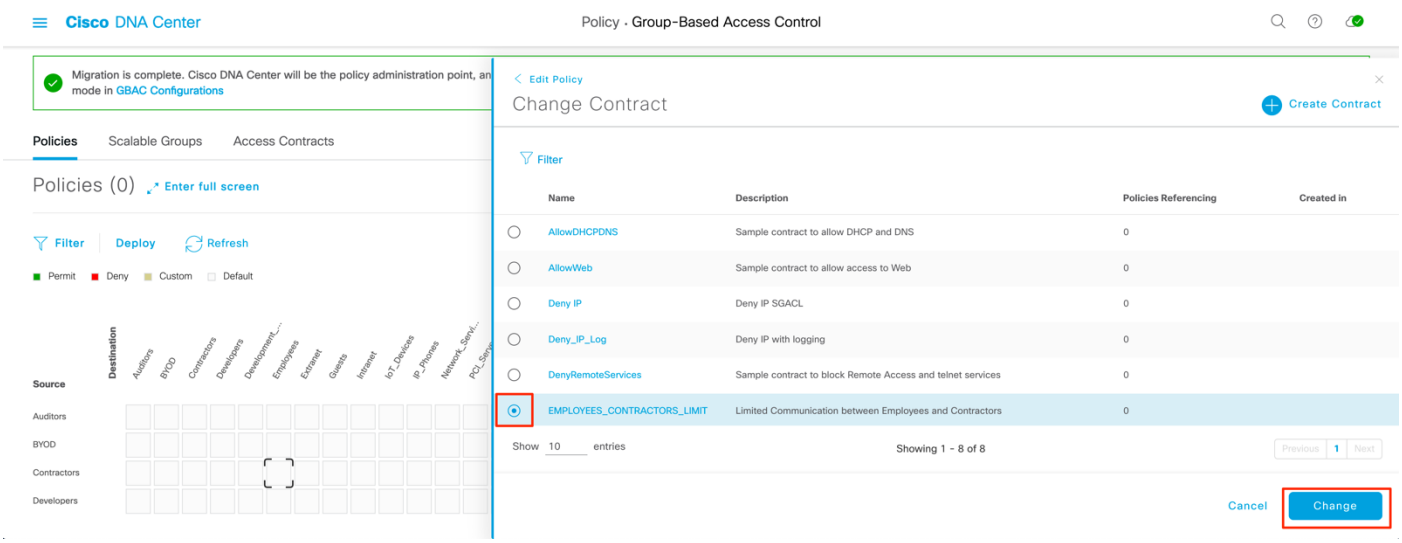
Step 6. Input a **Name** and **Description.**

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

Step 8. Click **Save**.

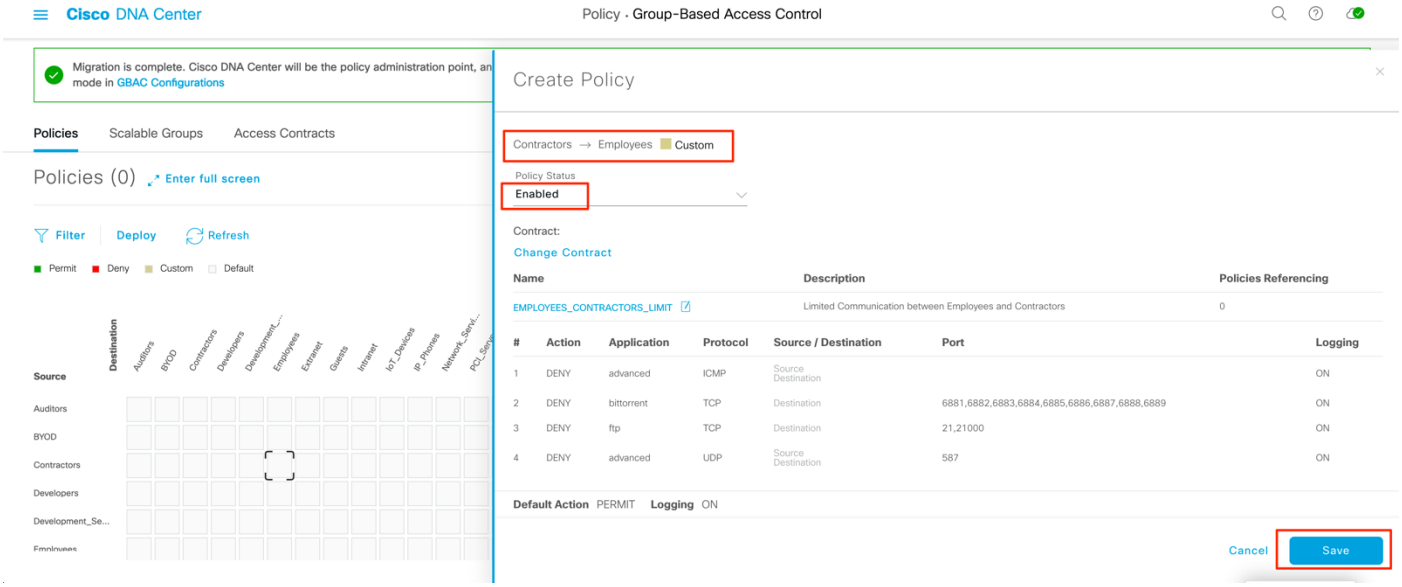


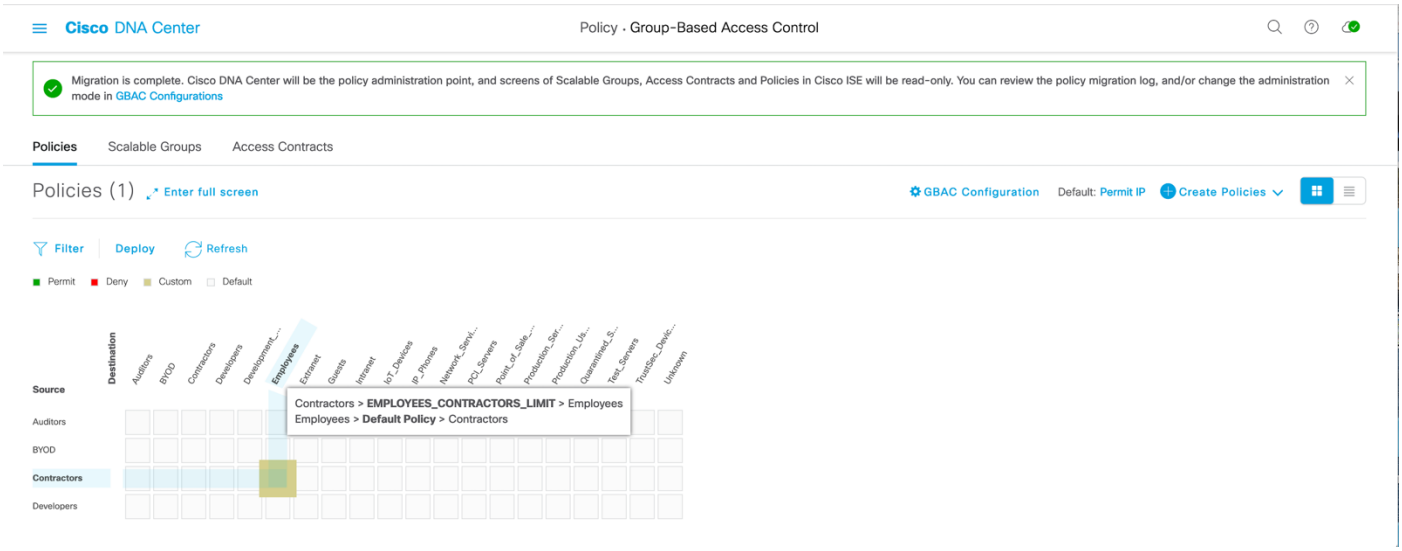
Step 9. Select the contract using the ⊙ radio button and click **Change.**



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

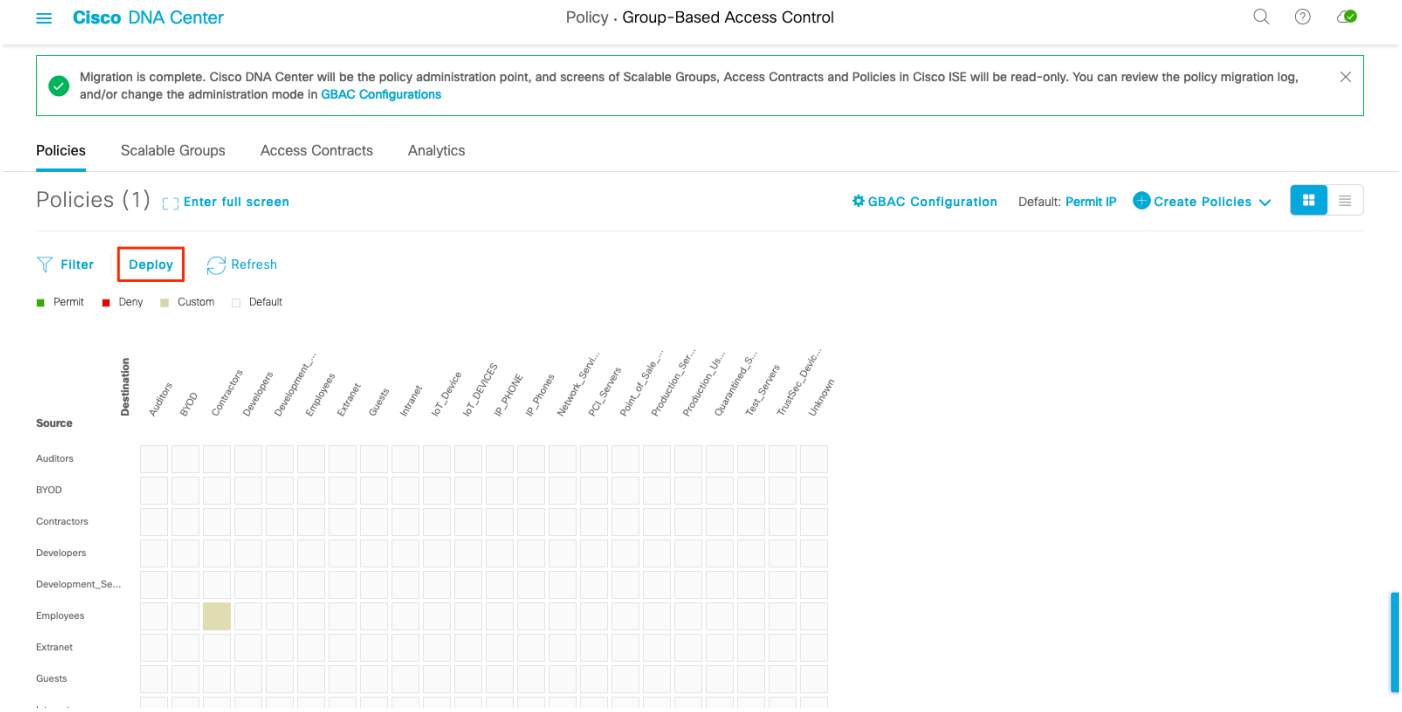
Step 11. Click **Save.**





Step 12. If needed, return to Step 1 to define additional contracts policies.

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



Operate

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

It is organized into the following processes and procedures:

Process	Procedure
Monitoring and Assuring the Cisco SD-Access Infrastructure	View Cisco DNA Center and ISE communication status View Cisco DNA Center Assurance summary View Cisco DNA Center Assurance details View Fabric provisioning details in Cisco DNA Center
Validating Policy enforcement	View Group-Based Access Control policies and access contracts Verify policy configuration on edge nodes
Monitoring SD-WAN Edge device health	Monitor IOS-XE WAN Edge router health and connection status View the Audit Logs in the SD-WAN vManage controller

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 Cisco DNA Center and Cisco Identity Service Engine communication status

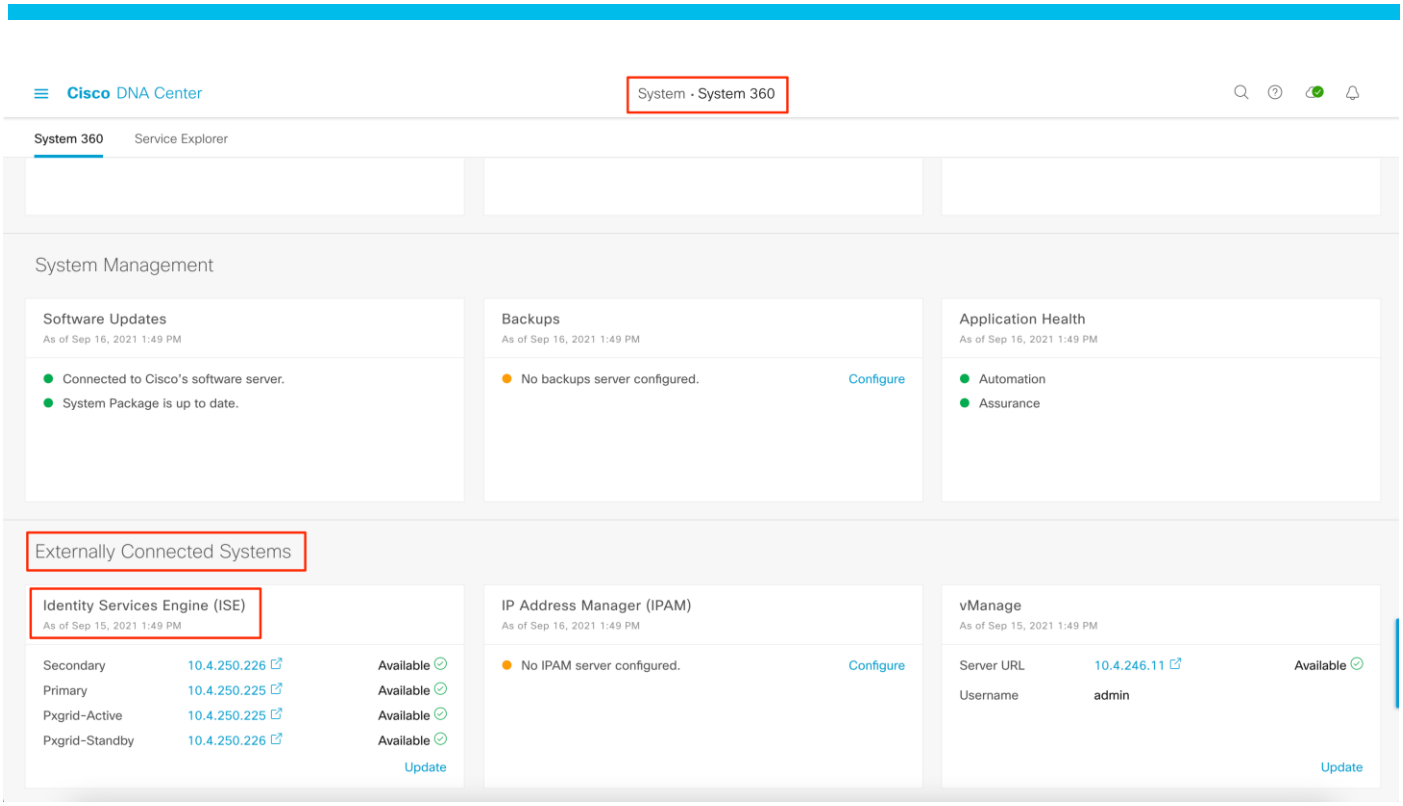
Similar to the steps in the prerequisites, this procedure verifies Cisco DNA Center and ISE integration. This procedure displays a list of the ISE Primary and Secondary Policy Administration Nodes (PAN) and ISE Primary and Secondary pxGrid Nodes and their communication status with Cisco DNA Center.

Step 1. Navigate 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 a minimum, there should be two entries:

- Primary – Available √
- PxGrid – Available √

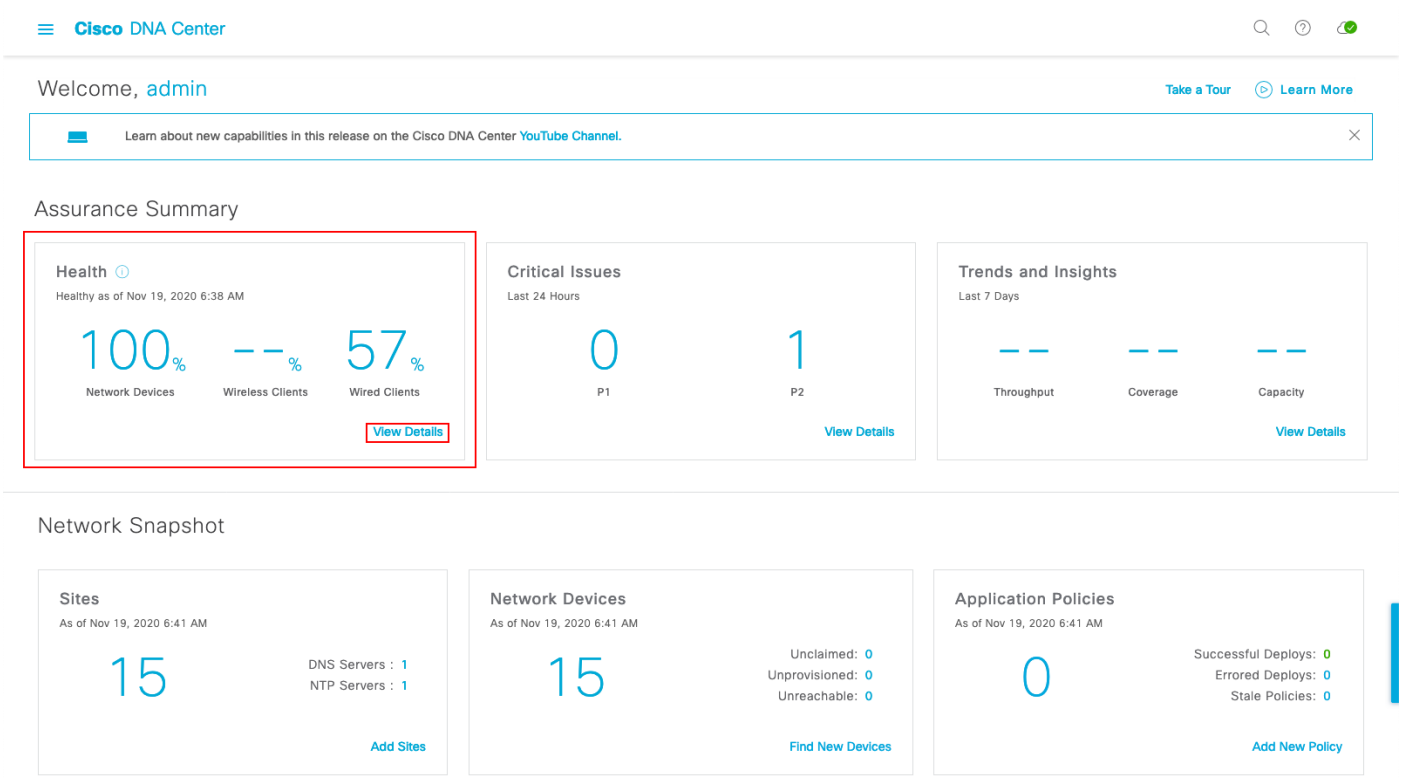


Procedure 2. View Cisco DNA Center Assurance summary

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.



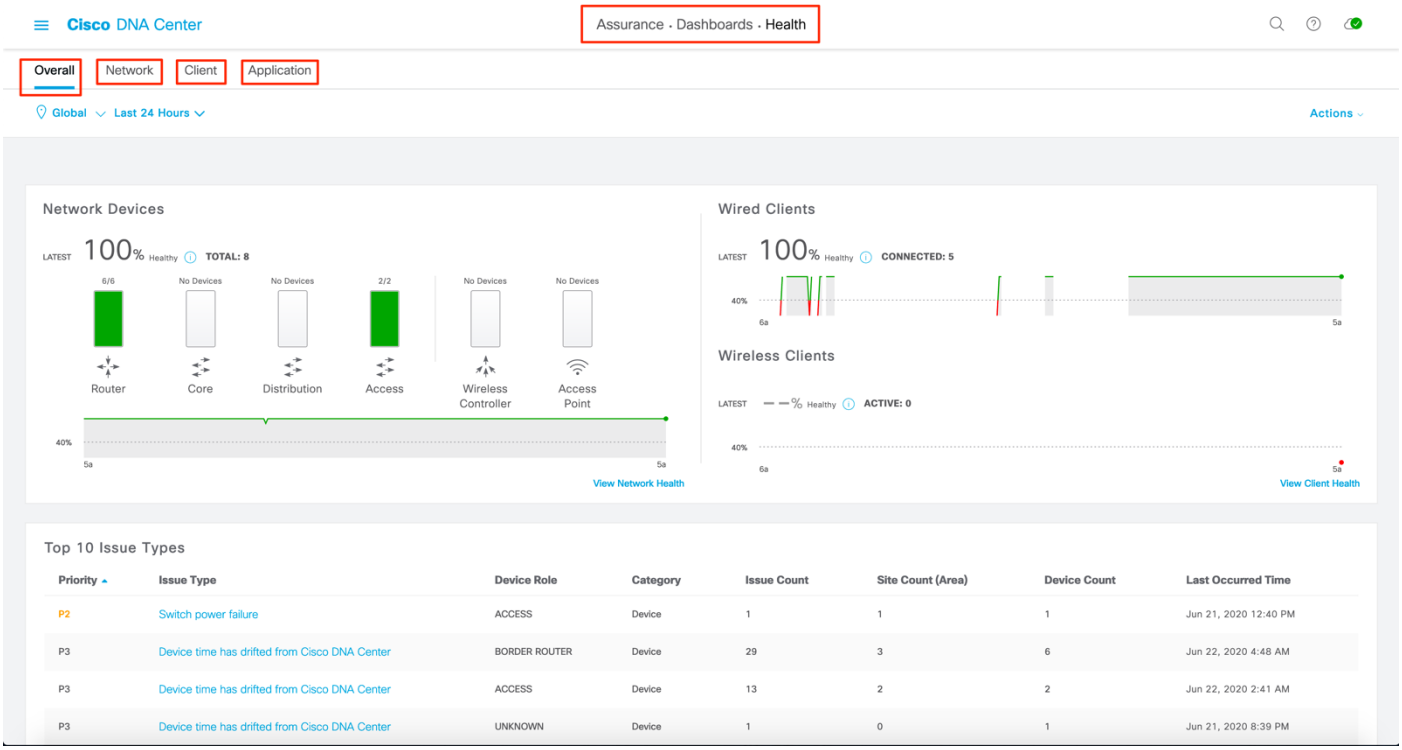
Procedure 3. View Cisco DNA Center Assurance details

The Cisco DNA Center Assurance application provides rich details and information that expand 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**, and **Application** to get respective detailed health information.

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



Tech tip
For further details, see the Cisco DNA Center Assurance User Guide.

Procedure 4. View Fabric provisioning details in the Cisco DNA Center task status

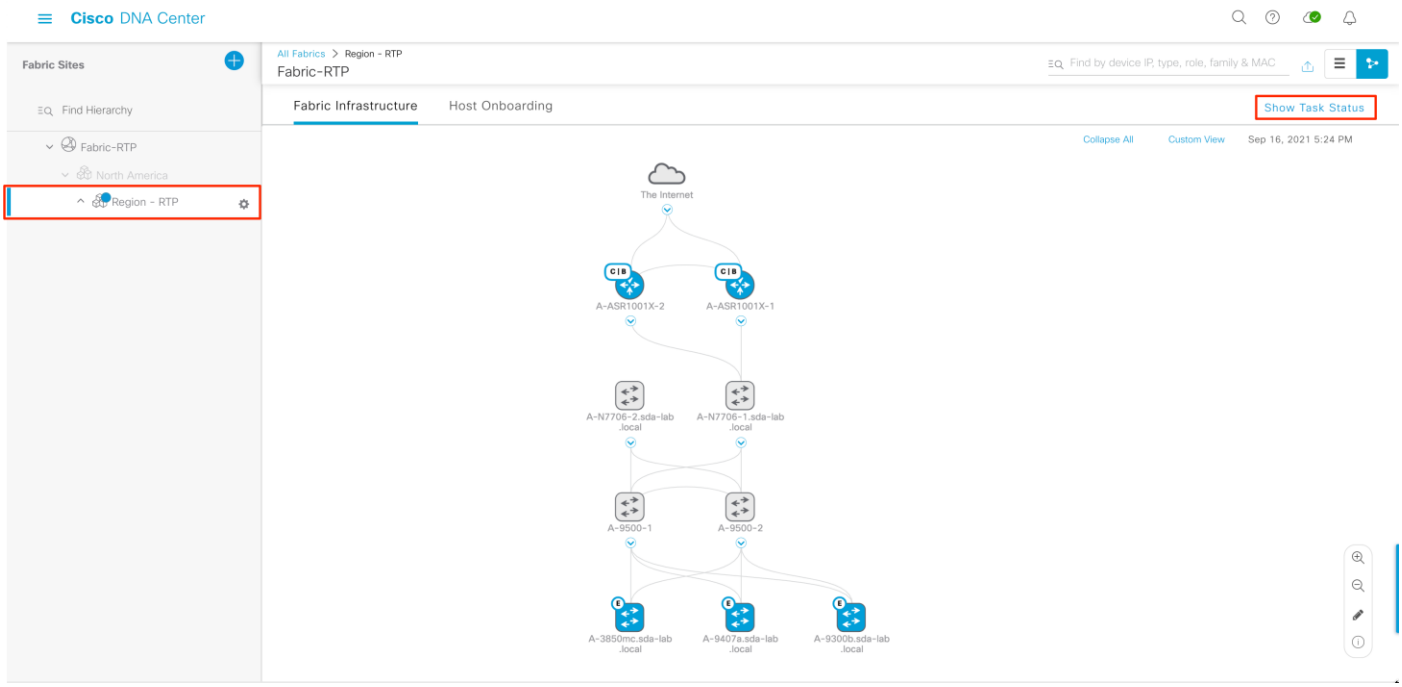
Use this procedure to verify the configuration that is deployed on the SD-Access devices.

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

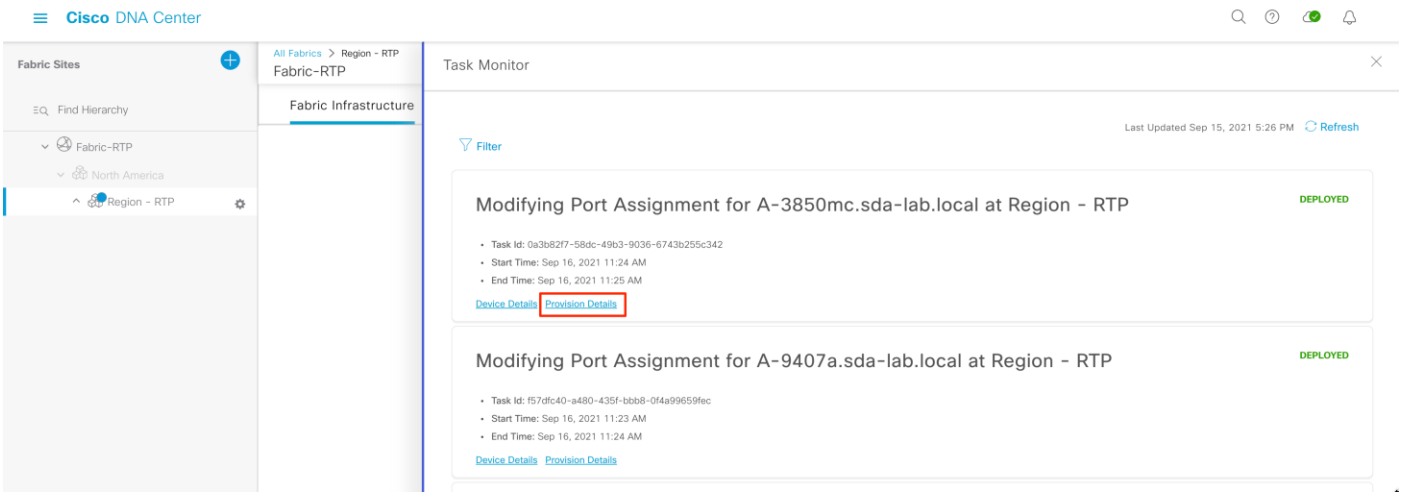
Step 2. Select the fabric site in the **Fabrics** section.

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

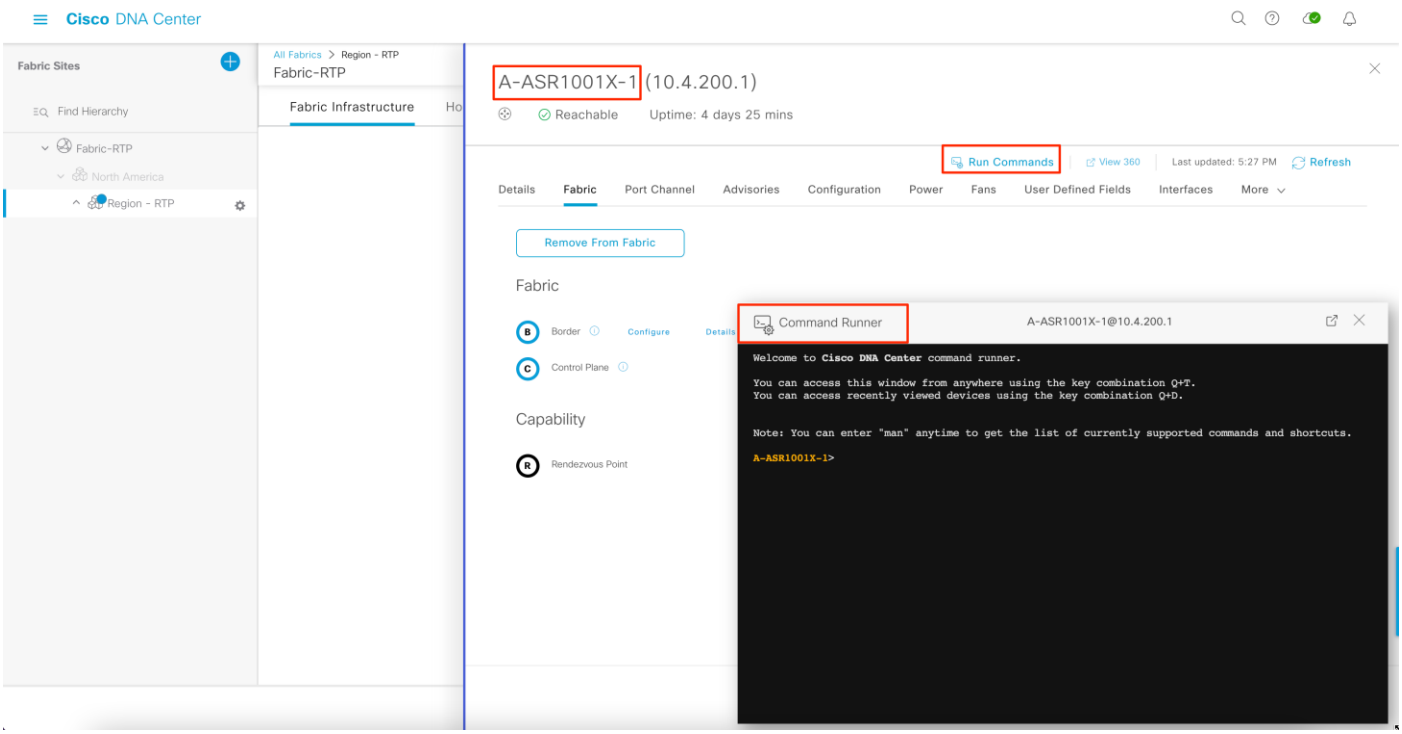
Step 4. Click **Show Task Status.**



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



Step 6. Click the network device in the **Fabric Infrastructure** tab, Select **Run Commands**



Step 7. In the **Command Runner** tab, issue the commands outlined in Table 5, Table 6 to view the fabric status.

Table 5. Verification Commands – SD-Access fabric Border, Control Plane

Command	Command Details
show lisp sessions	Displays the LISP control plane status to fabric Edge and Wireless Controller node.
Show ip bgp summary	Displays BGP neighborship state towards SD-WAN WAN transports.
Show ip bgp vpn4 all summary	Displays BGP neighborship state towards Peer Transit Networks for each Service VPN.
Show ip route vrf <Service_VPN>	Displays the routes learnt from the Peer Transit network device on specified Service VPN

Table 6. Verification Commands – SD-Access Edge

Command	Command Details
show lisp sessions	Displays the LISP control plane status to fabric Control Plane node
Show ip dhcp snooping binding	Displays DHCP snooping binding database table for all client connected on the edge node
Show authentication status	Displays authentication status for all clients connected to the edge port configured for authentication.
Show cts environment-data	Displays the Cisco Trustsec environment-data state downloaded from ISE.

Process 2: Validating Policy Enforcement

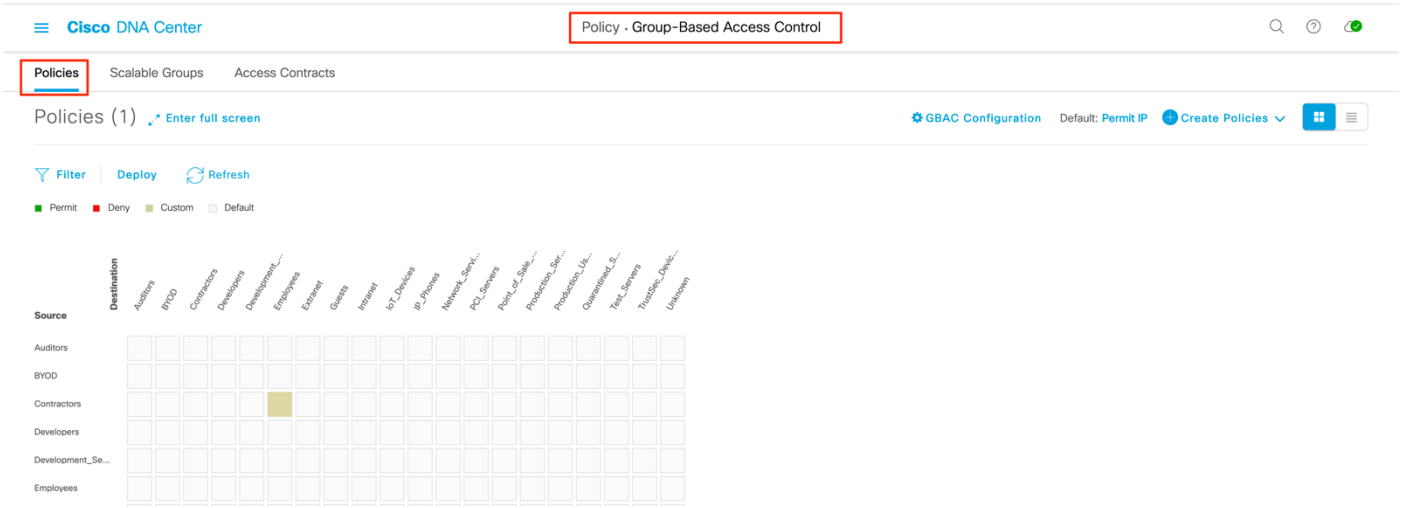
Use this process to view that TrustSec policy that has been defined in Cisco DNA Center and that it has been provisioned with the SD-Access fabric devices.

Procedure 1. View Group-Based Access Control policies and access contracts

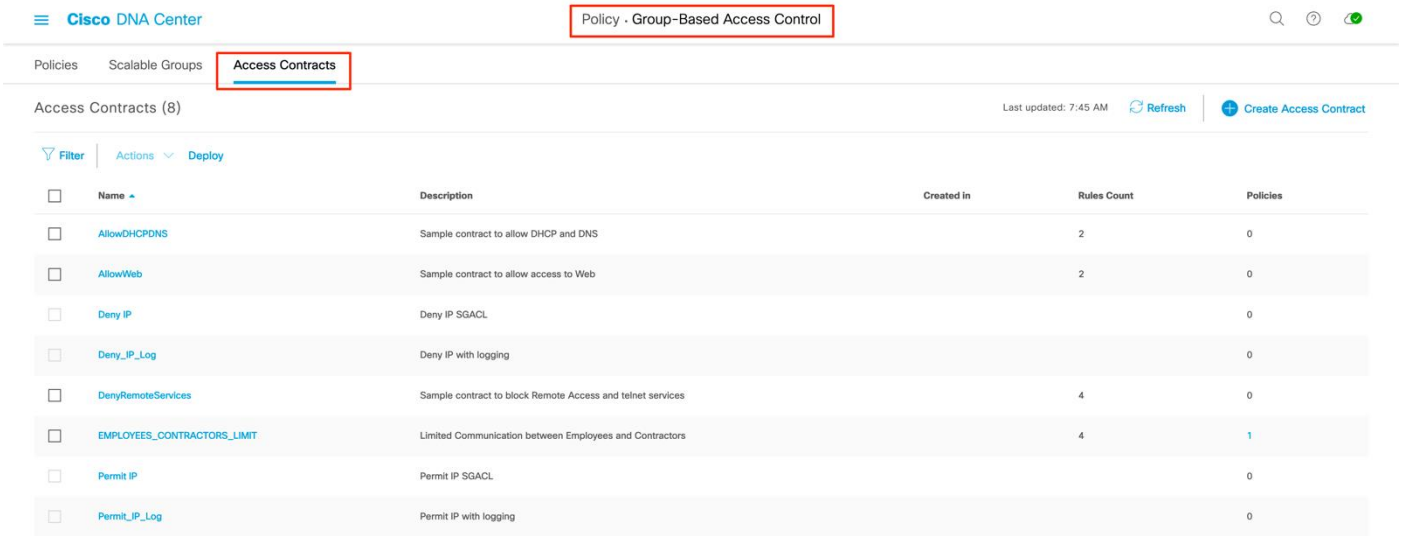
This procedure uses the Cisco DNA Center Policy Application to view the configuration of the TrustSec Policy Matrix and the defined access contracts.

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

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



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



Procedure 2. Verify policy configuration on edge nodes

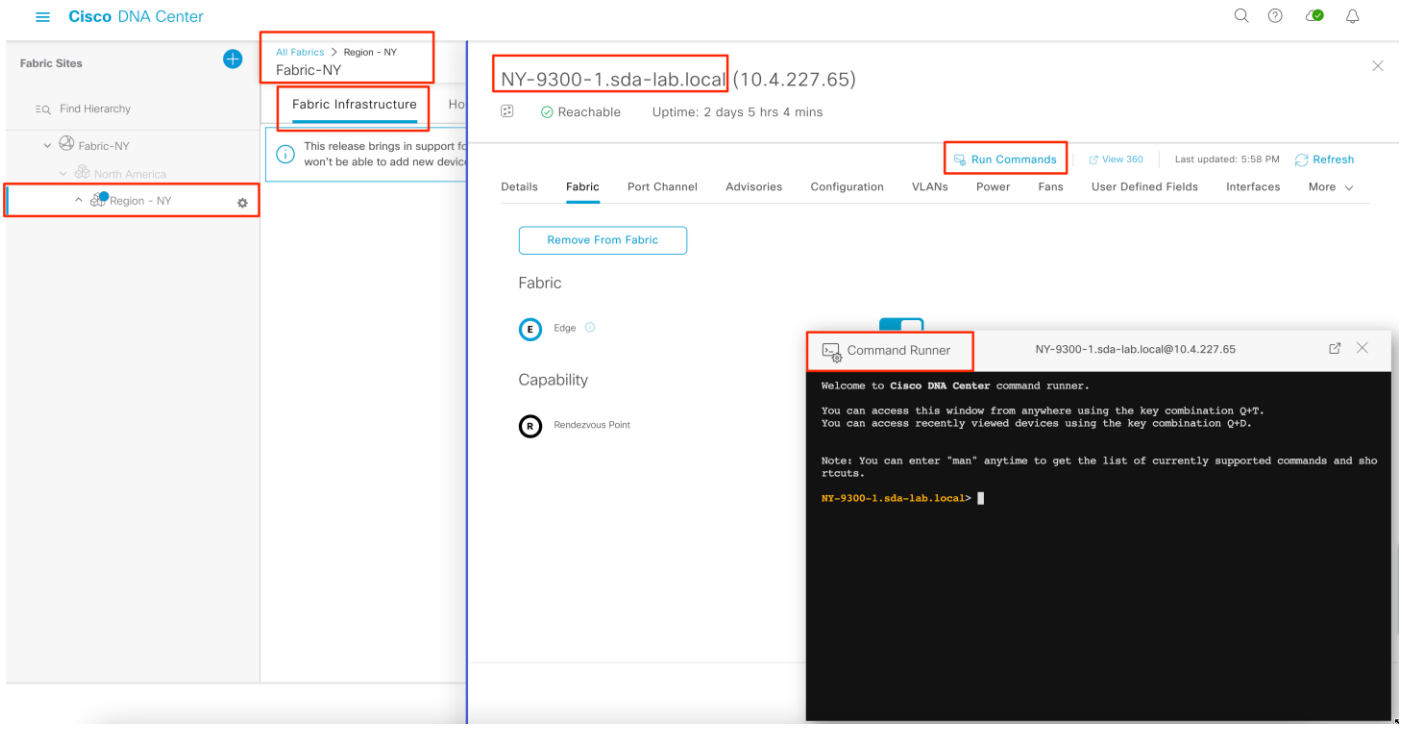
This procedure uses the Cisco DNA Center Command Runner functionality to verify the policy configuration on edge nodes.

Step 1. Navigate to **Cisco DNA Center** > **Provision** > **Fabric.**

Step 2. Select the fabric site in the **Fabrics** section.

Select the site from the hierarchy list in the left panel.

Select the **Fabric Infrastructure** tab and the **Fabric Edge** node



Step 3. In the **Command Runner** tab, issue the commands outlined in Table 7 to view the policy configuration status.

Table 7. 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

Process 3: Monitoring SD-WAN Edge device

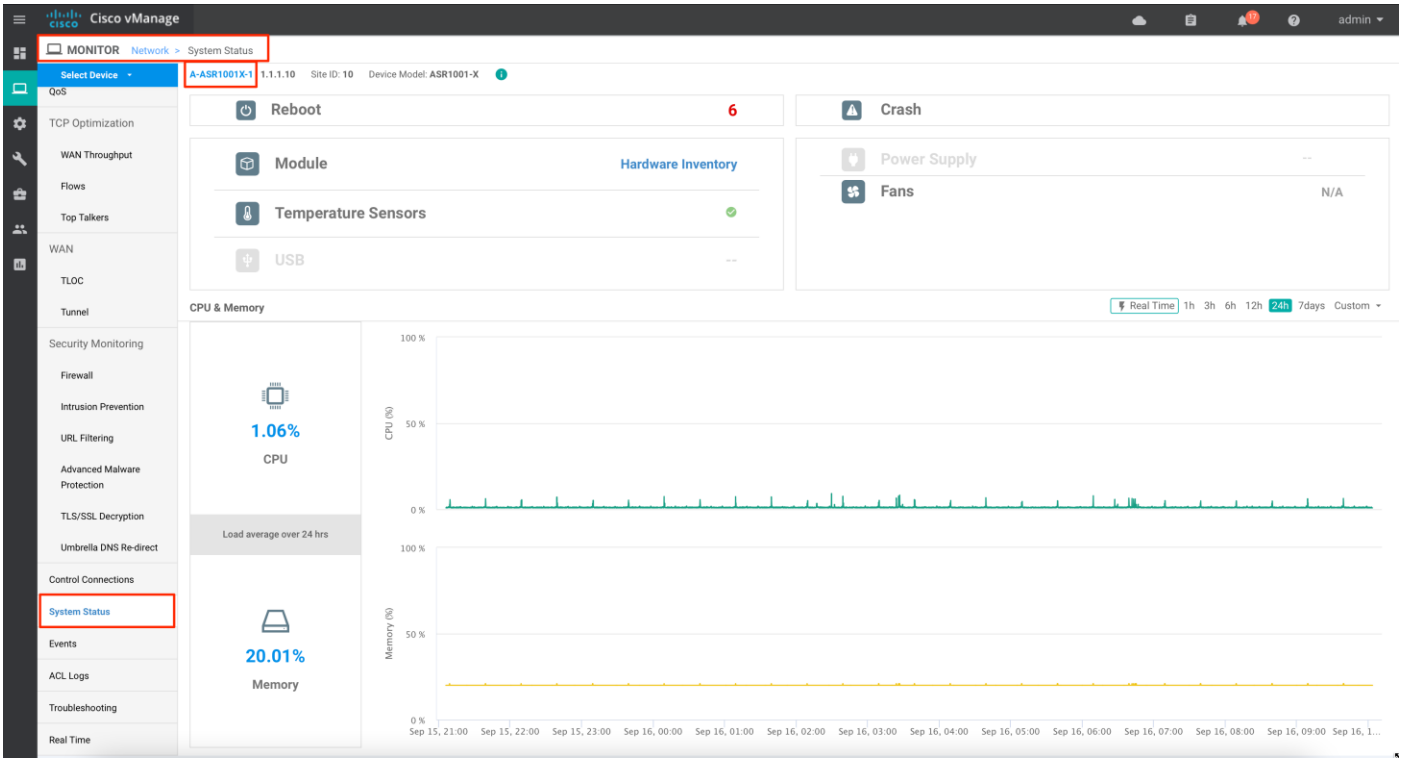
Use this process to view the status of the TrustSec configuration on the WAN Edge routers.

Procedure 1. Monitor IOS-XE WAN Edge router health and connection status

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

Step 2. Select the WAN Edge from the list.

Step 3. Select **System Status** option from the left panel



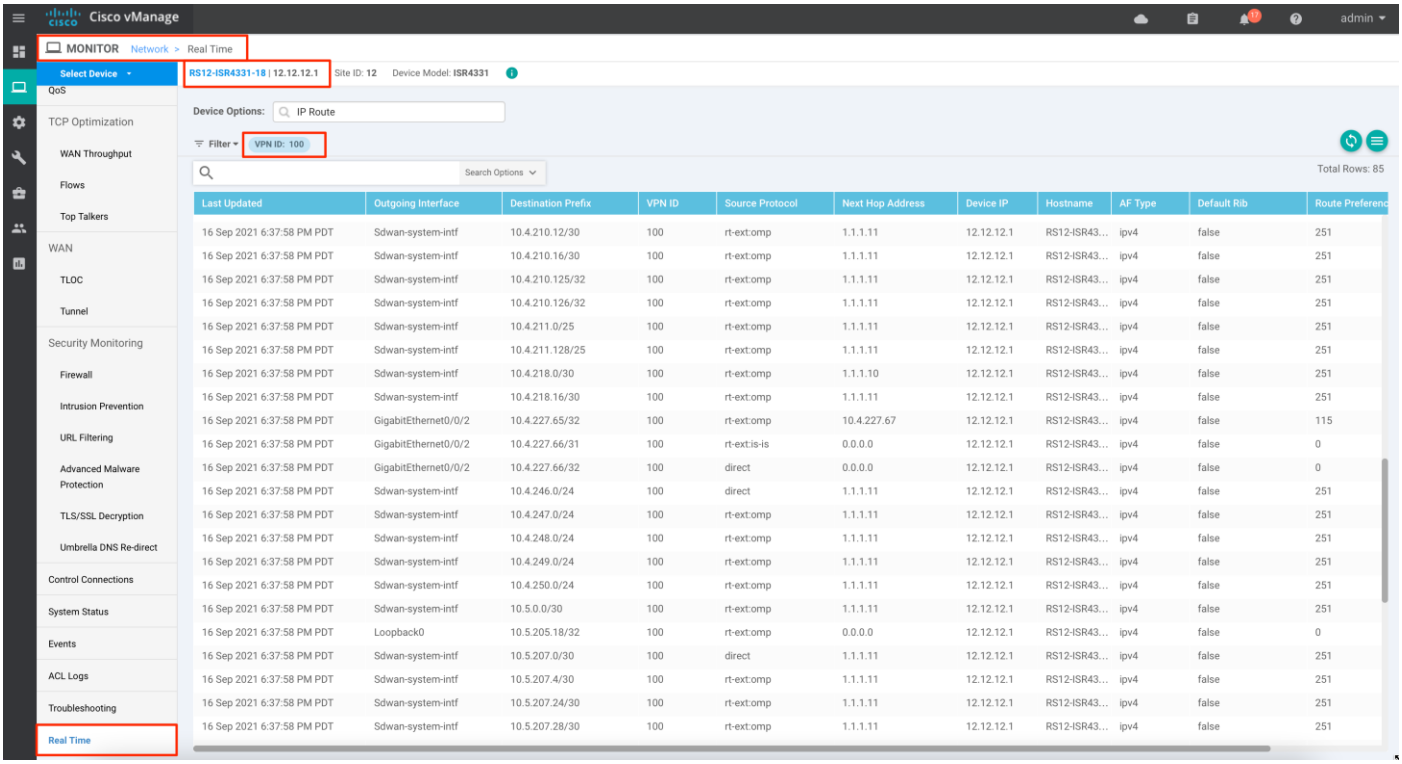
Step 4. Select the **Real Time** option from the left panel.

Step 5. In the **Device Options** box, search for the following:

IP Route and filter for certain Service VPN

Control Connections

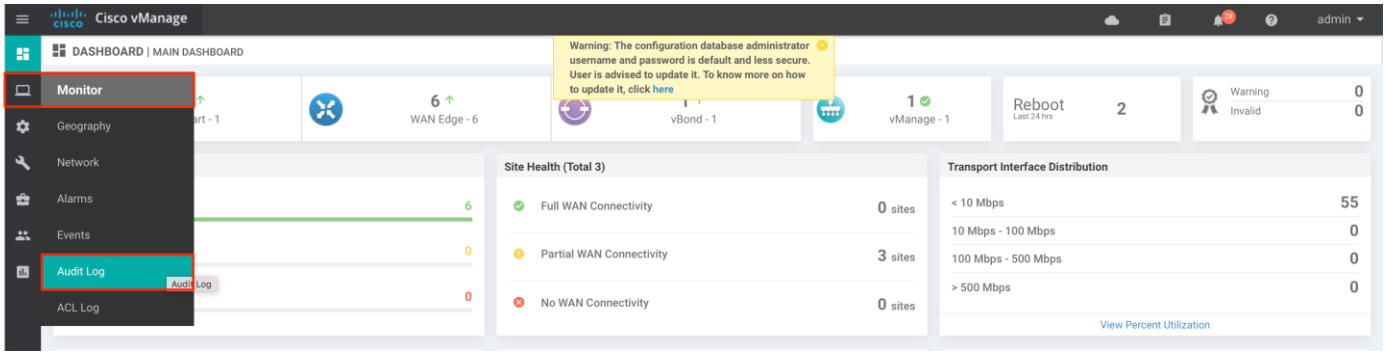
BFD Session



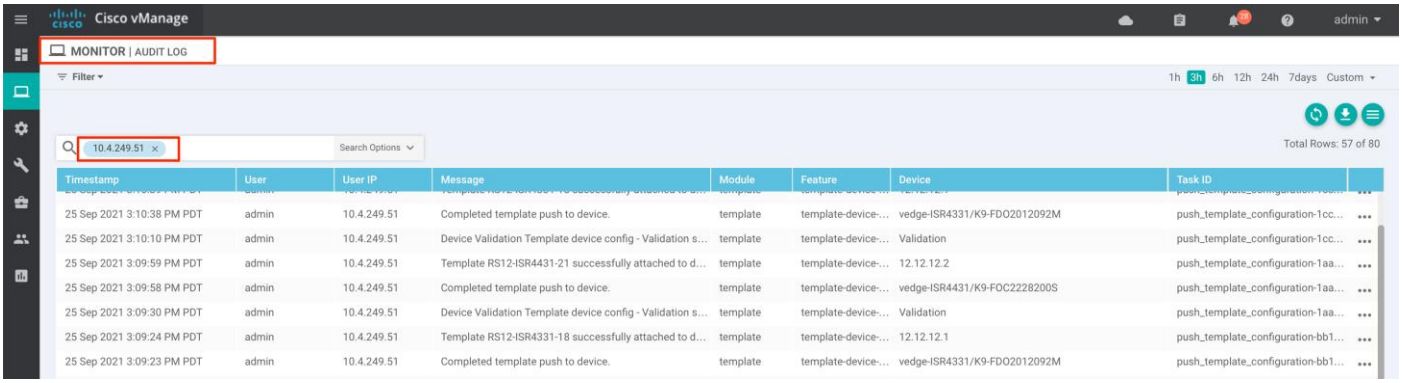
Procedure 2. View the Audit Logs in the SD-WAN vManage controller

Use this procedure to view Audit Logs, config shared by DNA Center to vManage to provision the WAN Edge device.

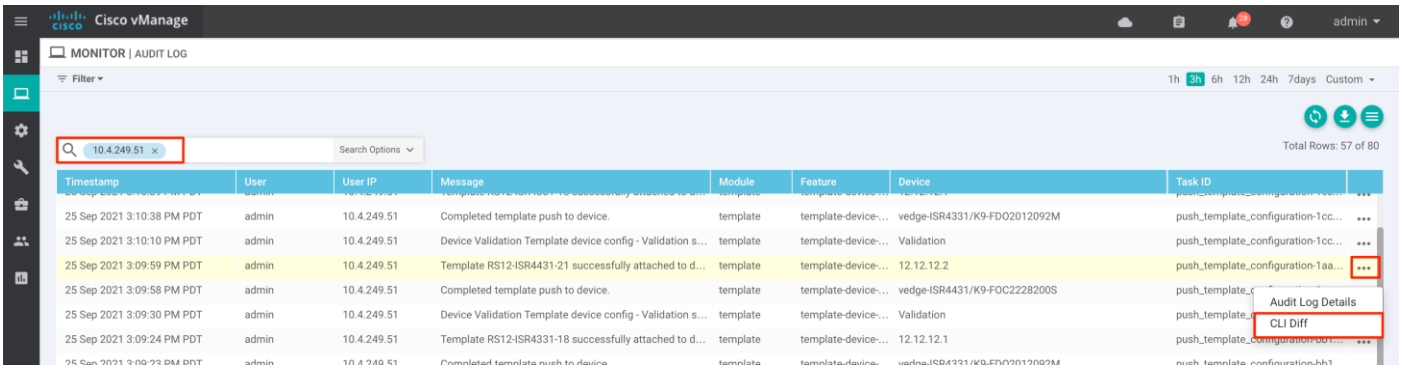
Step 1. In vManage, navigate to **Monitor > Audit Log**



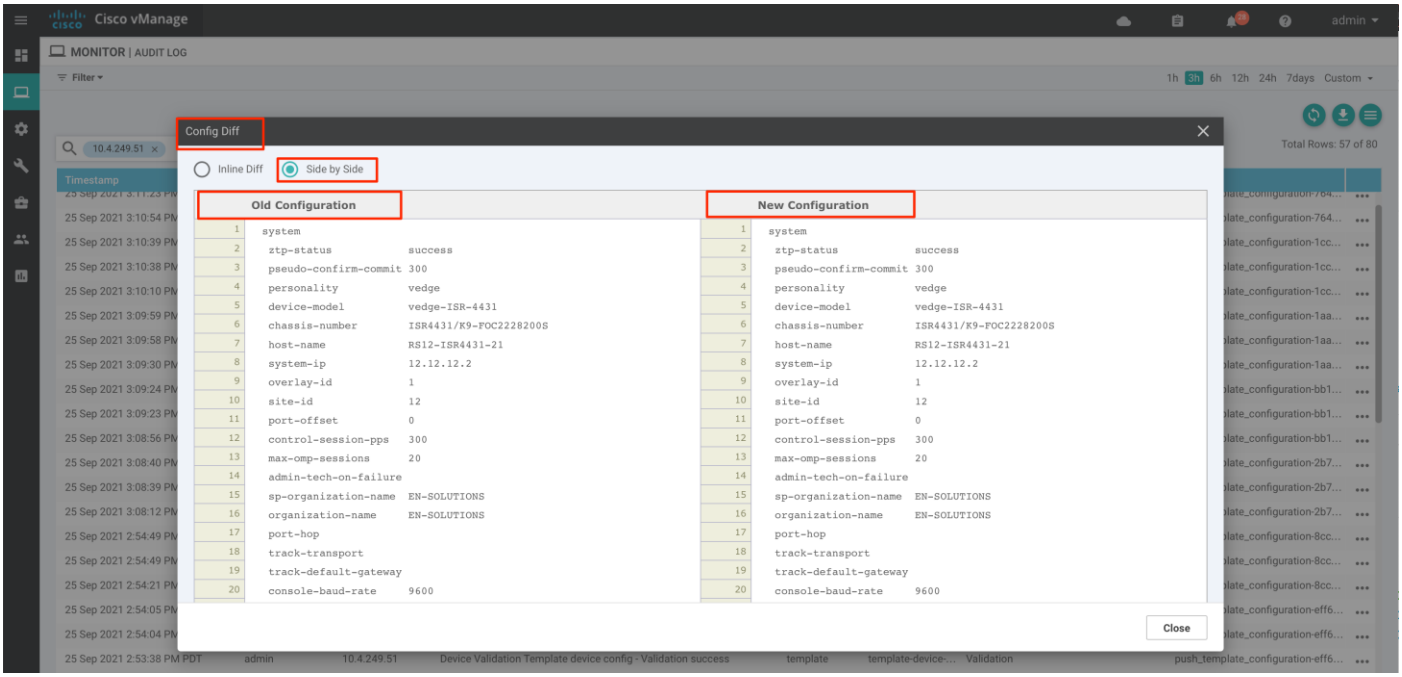
Step 2. In the search tab, input Cisco DNA Center **IP Address** to filter configuration that is shared and provisioned to the WAN Edge device by vManage controller.



Step 3. Select a **task** and click the three dots (…) to view the **Audit Log Details** or **CLI Diff**



In the **Config Diff** window, select **Side by Side** to view the **Old Configuration** and **the New Configuration**



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 8. Cisco SD-WAN Infrastructure

Product	Part number	Software version
Cisco vSmart	viptela-smart-20.3.4-genericx86-64.ova	20.3.4
Cisco vManage	viptela-vmanage-20.3.4-genericx86-64.ova	20.3.4
Cisco vBond	viptela-edge-20.3.4-genericx86-64.ova	20.3.4

Product	Part number	Software version
ASR 1001-X Series	ASR1001-X	17.3.4a
ISR 4300 Series	ISR4331/K9	17.3.4a

Table 9. Device Platform, Model, and Software Version

Platform	Model (PID)	Software code version
Cisco DNA Center	DN2-HW-APL-L	Cisco DNA Center 2.2.2.5
Identity Services Engine	R-ISE-VMS-K9	ISE 3.0 Patch 2
Catalyst 9300 Series	C9300-48U	17.3.4
Catalyst 9400 Series	C9400-48U	17.3.4
WLC 8540 Series	AIR-CT8540-K9	8.10.151.0
Cisco Catalyst 9800 Embedded Wireless on C9300, C9400, C9500 Series Switch	C9300 Embedded Wireless	17.3.4

Table 10. Cisco SD-Access fabric devices

Product	SD-Access fabric role
Catalyst 9300 Series Switches	Fabric Edge, Embedded Wireless
Cisco ASR 1000-X Series Aggregation Services Routers	Colocated Border and Control Plane Node
Catalyst 9300 Series Switches	Edge Nodes
Catalyst 9400 Series Switches	Edge Nodes

Table 11. Cisco DNA Center Package Versions

Package name - GUI	Software version
System	1.6.424
System Commons	2.1.365.62360
Access Control Application	2.1.365.62360
AI Endpoint Analytics	1.4.365
AI Network Analytics	2.6.9.453
Application Hosting	1.6.0.2107090810
Application Policy	2.1.364.170201
Application Registry	2.1.364.170201
Application Visibility Service	2.1.364.170201

Package name - GUI	Software version
Assurance - Base	2.2.2.411
Assurance - Sensor	2.2.2.404
Automation - Base	2.1.365.62360
Automation - Intelligent Capture	2.1.365.62360
Automation - Sensor	2.1.365.62360
Cisco DNA Center Global Search	1.5.0.362
Cisco DNA Center Platform	1.5.1.137
Cisco DNA Center UI	1.6.2.432
Cisco Umbrella	2.1.364.592099
Cloud Connectivity - Contextual Content	1.3.1.359
Cloud Connectivity - Data Hub	1.6.0.380
Cloud Connectivity - Tethering	2.12.1.2
Cloud Device Provisioning Application	2.1.365.62360
Command Runner	2.1.365.62360
Device Onboarding	2.1.365.62360
Disaster Recovery	2.1.364.362034
Group-Based Policy Analytics	2.2.1.226
Image Management	2.1.365.62360
Machine Reasoning	2.1.364.212034
NCP - Base	2.1.365.62360
NCP - Services	2.1.365.62360
Network Controller Platform	2.1.365.62360
Network Data Platform - Base Analytics	1.6.1019
Network Data Platform - Core	1.6.579
Network Data Platform - Manager	1.6.541
Network Experience Platform - Core	2.1.365.62360
Path Trace	2.1.365.62360
RBAC Extensions	2.1.364.1910003
Rogue and aWIPS	2.2.0.45

Package name - GUI	Software version
SD Access	2.1.365.62360
Stealthwatch Security Analytics	2.1.364.1091088
Wide Area Bonjour	2.4.363.75002

Appendix B: References Used in This Guide

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 and 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

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

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

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 Adaptative 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 Catalyst® 9300 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

Feedback

For comments and suggestions about this guide and related guides, join the discussion on Cisco Community 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**.