



Cisco Catalyst SD-WAN for Government Configuration Guide

First Published: 2020-08-17

Last Modified: 2025-11-19

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: <https://www.cisco.com/c/en/us/about/legal/trademarks.html>. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2020–2025 Cisco Systems, Inc. All rights reserved.



CONTENTS

CHAPTER 1	Read Me First	1
------------------	----------------------	----------

CHAPTER 2	What's New in Cisco IOS XE (Catalyst SD-WAN)	3
------------------	---	----------

CHAPTER 3	Introduction to Cisco Catalyst SD-WAN for Government	5
	Cisco Catalyst SD-WAN for Government Overview	5
	Supported Platforms	6
	Intended Audience	6
	Cisco Catalyst SD-WAN for Government Components	6
	Federal Boundary	8
	Customer Access to the Amazon Virtual Private Cloud	8
	Management Access to the Amazon Virtual Private Cloud	8
	Data Flow	9
	Data Collection Agent Configuration and Monitoring	9
	Incident Response	10
	Workflow for Using Cisco Catalyst SD-WAN for Government	11

CHAPTER 4	Cisco Catalyst SD-WAN Portal	13
	Overview of the Cisco Catalyst SD-WAN Portal	13
	Prerequisites for the Cisco Catalyst SD-WAN Portal	16
	Benefits of the Cisco Catalyst SD-WAN Portal	16
	Smart Accounts and Virtual Accounts	16

CHAPTER 5	Access the Cisco Catalyst SD-WAN Portal	19
	Workflow for Smart Account and Virtual Accounts for provisioning control components	19
	Create a Virtual Account associated with your Smart Account	20

Access the Cisco Catalyst SD-WAN Portal for the first time 20

Log in to the Cisco Catalyst SD-WAN Portal 21

CHAPTER 6 **Configure an Identity Provider for the Cisco Catalyst SD-WAN Portal 23**

Configure an identity provider for the Cisco Catalyst SD-WAN Portal 23

CHAPTER 7 **Manage Role-Based Access 25**

Configure Cisco Catalyst SD-WAN Portal roles for IdP users 25

Create additional roles 25

CHAPTER 8 **Manage fabrics 27**

Create a Cisco SD-WAN Cloud-Pro fabric 27

Configure advanced options for a Cisco SD-WAN Cloud-Pro fabric 31

Delete a fabric 35

Specify the allowed list of IP addresses for managing control component access 35

Create Predefined Inbound Rules 36

CHAPTER 9 **Use Cisco Catalyst 8000V as a Cloud Gateway for a fabric 39**

Information about Cisco Catalyst 8000V as a cloud gateway for a fabric 39

Use cases for Cisco Catalyst 8000V as a cloud gateway for a fabric 40

Prerequisites for Cisco Catalyst 8000V as a cloud gateway for a fabric 40

Restrictions for Cisco Catalyst 8000V as a cloud gateway for a fabric 40

Configure Cisco Catalyst 8000V as a cloud gateway for a fabric 40

CHAPTER 10 **Monitor fabrics 45**

Monitor control components and devices in fabrics 45

View fabric and control component details 45

View change window notifications 46

CHAPTER 11 **Manage account settings 49**

Information about predefined inbound rules 49

Benefits of predefined inbound rules 49

Manage predefined inbound rules 50

CHAPTER 12	Configuring system snapshots	53
	Information about system snapshots	53
	Take an on-demand snapshot	54
	View snapshots	55

CHAPTER 13	Configure webhooks	59
	Information about webhooks	59
	Configure a webhook	59
	Send a webhook notification	60

CHAPTER 14	Frequently Asked Questions	61
	Frequently Asked Questions	61
	How to	62
	Troubleshooting	62

CHAPTER 15	Configuration Conversion Tool	65
	Configuration Conversion Tool feature history	65
	Information about the Configuration Conversion Tool	65
	Restrictions for the Configuration Conversion Tool	66
	Prerequisites for the Configuration Conversion Tool	66
	Use the Configuration Conversion Tool	66

CHAPTER 16	Troubleshooting the Cisco Catalyst SD-WAN Portal	69
	Update an expired IdP certificate	69
	Reset a Misconfigured IdP	69
	Troubleshoot Smart Account issues	70
	Troubleshoot Virtual Account issues	70
	Troubleshoot browser security issues	71

CHAPTER 17	Set Up and Configure Cisco Catalyst SD-WAN Manager	73
	Configure the Network	73
	Bring-Up Sequence of Events	73

Summary of the User Portion of the Bring-Up Sequence	75
System and Interfaces Overview	76
Configure Single Sign-On Using Okta	81
Enable an Identity Provider in Cisco SD-WAN Manager	81
Configure SSO on the Okta Website	82
Assign Users to the Application on the Okta Website	85
Configure SSO for PingID	85
Configure SSO on the PingID Administration Portal	85
Configure Hardened Passwords	88
Enforce Strong Passwords	88
Password Requirements	88
Password Attempts Allowed	90
Password Change Policy	90
Reset a Locked User	90
Manage Users	91
Configure Users Using CLI	91
Configure User Login Options	92
Configure Account Lockout	94
Configure Unsuccessful Login Attempts Lockout	95
Configure Duo Multifactor Authentication	97
Configure Sessions in Cisco SD-WAN Manager	99
Set a Client Session Timeout in Cisco SD-WAN Manager	99
Set a Session Lifetime in Cisco SD-WAN Manager	99
Set the Server Session Timeout in Cisco SD-WAN Manager	100
Set the maximum sessions per user role	100
Configure NTP Addresses	101
NTP on Cisco Catalyst SD-WAN for Government Overlay Networks	101
Configure NTP Servers Using Cisco SD-WAN Manager	101
Configure Domain Name System Security Extensions	104
Overview of Domain Name System Security Extensions	104
Use Case for Domain Name System Security Extensions	105
Configure Domain Name System Security Extensions Using the CLI	105
Verify that FIPS is Enabled	105
Web Server Certificates	106

View Web Server Certificate Expiration Date	106
Renew Cisco Catalyst SD-WAN SSL Certificates for Controllers	106
Configure a Symantec Process Certificate	108
Install Enterprise Root Certificates	108
Secure Connections from Devices to Cisco SD-WAN Manager	109
Control Plane Security Overview	110
Data Plane Security Overview	111
Segmentation in Cisco Catalyst SD-WAN	112
VRFs Used in Cisco Catalyst SD-WAN Segmentation	113
Configure VRF Using Cisco SD-WAN Manager Templates	114

CHAPTER 18**Security Features 115**

Encrypt Communications	115
IPsec Pairwise Keys	116
Pairwise Keys	116
IPsec Security Association Rekey	116
Configure IPsec Pairwise Keys Using Cisco Catalyst SD-WAN Manager	117
Configure Pairwise Keys and Enable Rekeying on the CLI	117
Verify IPsec Pairwise Keys on a Cisco IOS XE Catalyst SD-WAN Device	118

CHAPTER 19**Software Development Life Cycle (SDLC) 121**

Architecture of Software Development Life Cycle Pipelines	121
Management VPC SDLC Pipeline	123
Checks for Regressions and Analysis of Code	123
Upgrade and Deploy Apps	124
Deploy to Cisco Catalyst SD-WAN for Government	124
Customer VPC SDLC Pipeline	124
Code Analysis Reporting	125



CHAPTER 1

Read Me First



Note To achieve simplification and consistency, the Cisco SD-WAN solution has been rebranded as Cisco Catalyst SD-WAN. In addition, from Cisco IOS XE SD-WAN Release 17.12.1a and Cisco Catalyst SD-WAN Release 20.12.1, the following component changes are applicable: **Cisco vManage to Cisco Catalyst SD-WAN Manager, Cisco vAnalytics to Cisco Catalyst SD-WAN Analytics, Cisco vBond to Cisco Catalyst SD-WAN Validator, Cisco vSmart to Cisco Catalyst SD-WAN Controller, and Cisco Controllers to Cisco Catalyst SD-WAN Control Components.** See the latest Release Notes for a comprehensive list of all the component brand name changes. While we transition to the new names, some inconsistencies might be present in the documentation set because of a phased approach to the user interface updates of the software product.

Related References

- [Cisco Catalyst SD-WAN Control Components Compatibility Matrix and Server Recommendations](#)
- [Cisco Catalyst SD-WAN Device Compatibility](#)

User Documentation

- [User Documentation for Cisco IOS XE Catalyst SD-WAN Release 17](#)

Communications, Services, and Additional Information

- Sign up for Cisco email newsletters and other communications at: [Cisco Profile Manager](#).
- For information on the latest technical, advanced, and remote services to increase the operational reliability of your network visit [Cisco Services](#).
- To browse and discover secure, validated enterprise-class apps, products, solutions, and services, visit [Cisco Devnet](#).
- To obtain general networking, training, and certification titles from Cisco Press Publishers, visit [Cisco Press](#).
- To find warranty information for a specific product or product family, visit [Cisco Warranty Finder](#).
- To view open and resolved bugs for a release, access the [Cisco Bug Search Tool](#).
- To submit a service request, visit [Cisco Support](#).

Documentation Feedback

To provide feedback about Cisco technical documentation use the feedback form available in the right pane of every online document.



CHAPTER 2

What's New in Cisco IOS XE (Catalyst SD-WAN)

[What's New in Cisco IOS XE Catalyst SD-WAN Release 17.x](#)

[What's New in Cisco SD-WAN \(vEdge\) Release 20.x](#)





CHAPTER 3

Introduction to Cisco Catalyst SD-WAN for Government

- [Cisco Catalyst SD-WAN for Government Overview, on page 5](#)
- [Supported Platforms, on page 6](#)
- [Intended Audience, on page 6](#)
- [Cisco Catalyst SD-WAN for Government Components, on page 6](#)
- [Federal Boundary, on page 8](#)
- [Customer Access to the Amazon Virtual Private Cloud, on page 8](#)
- [Management Access to the Amazon Virtual Private Cloud, on page 8](#)
- [Data Flow, on page 9](#)
- [Data Collection Agent Configuration and Monitoring, on page 9](#)
- [Incident Response, on page 10](#)
- [Workflow for Using Cisco Catalyst SD-WAN for Government, on page 11](#)

Cisco Catalyst SD-WAN for Government Overview

Security is a critical element of today's networking infrastructure. Network administrators and security officers are hard pressed to defend their network against attacks and breaches. As a result of hybrid clouds and remote employee connectivity, the security perimeter around networks is disappearing.

FedRAMP, the Federal Risk and Authorization Management Program, is a U.S.-government program that establishes a standardized approach for assessing, authorizing, and monitoring cloud service providers.

Cisco Catalyst SD-WAN for Government incorporates encryption and security at its core:

- Creates a restricted space called the federal boundary within the AWS GovCloud (U.S.).
- Restricts access to cleared personnel.
- Runs in Federal Information Processing Standard (FIPS) mode for all controllers.
- Ensures that all data and control connections are Secure Hash Algorithm 2 (SHA-2) compliant.
- Provides enhanced user session management.
- Performs a real-time audit at the controller level.
- Provides an automated Plan of Actions and Milestones (POA&M) report.

- Enables customers to have their own dedicated Amazon Virtual Private Cloud (Amazon VPC) that automatically denies all HTTP requests unless specifically authorized.
- Ensures protection by AWS services such as AWS Application Load Balancer (ALB), AWS Web Application Firewall (WAF), and AWS Shield. All the web services are behind the ALB and WAF for protection. They are also protected from distributed denial of service (DDoS) attacks by the AWS Shield. AWS Network Firewalls are employed to detect anomalous network activity.
- Uses a role-based access without local users for Cisco Federal Operations, a Cisco team that maintains and monitors the environment.

Cisco Catalyst SD-WAN for government conducts annual penetration testing through Third-Party Assessment Organizations (3PAOs). In addition to testing, Tenable Security Center performs daily penetration scanning. Tenable Security Center is a component of the management Amazon VPC. For more information, see [Cisco Catalyst SD-WAN components](#).

For more information on the general Cisco Catalyst SD-WAN security configuration, see the [Security Configuration Guide, Cisco IOS XE Release 17.x](#).

Supported Platforms

For a complete list of the supported platforms for Cisco Catalyst SD-WAN for government, see the [Supported Devices](#) section of the Release Notes document for Cisco IOS XE Catalyst SD-WAN devices.

To be FedRAMP-compliant, ensure that you run Cisco vManage Release 20.12.1.1 and Cisco IOS XE Catalyst SD-WAN Release 17.9.1a or later releases. Upgrade to major releases as they become available.



Note If you are using a hardware router, your device must be TAA-compliant. When ordering a device, ensure that the device's SKU is appended with ++. This indicates that the device is TAA-compliant. For more information, contact your Cisco sales representative.

Intended Audience

There are two types of users for Cisco Catalyst SD-WAN for Government:

- Customers, such as service providers, partners, and other end users.
- Cisco Catalyst SD-WAN Federal Operations (FedOps): A Cisco team that maintains and monitors Cisco Catalyst SD-WAN for Government.

Cisco Catalyst SD-WAN for Government Components

The Cisco Catalyst SD-WAN for government cloud boundary has a customer Amazon VPC and a management Amazon VPC. Individual customers have their own exclusive Amazon customer VPCs.

VPC	Components	User Access
Customer	Cisco Catalyst SD-WAN solution includes: Cisco SD-WAN Manager, Cisco SD-WAN Validator, Cisco SD-WAN Controller, Cisco IOS XE Catalyst SD-WAN devices, and other applications.	Customers
Management	<p>Cisco Catalyst SD-WAN Portal (SSP): Sets up and monitors Cisco Catalyst SD-WAN overlay networks.</p> <p>Cisco vMonitor: Monitors the system for health and failures.</p> <p>Cisco vOrchestrator: Assists Cisco Catalyst SD-WAN Portal in creating the customer VPC.</p> <p>Splunk Cloud server: Monitors data from the infrastructure FIM server client.</p> <p>Tenable Security Center: Handles vulnerability, compliance, and web application scans.</p> <p>Cisco Data Management Service (DMS): Provides data storage location services for Cisco SD-WAN Manager to send customer telemetry data, which is stored within the AWS Govcloud boundary in the S3 bucket.</p> <p>Cisco Data Collection Agent (DCA): Collects data regarding the health of the system. Pushes data to the Data Collection Service (DCS).</p> <p>Cisco Data Collection Service (DCS): Acts as the entry point for all telemetry data in the system.</p> <p>Jira (Atlassian): Refers to a hardened instance of Jira that automatically creates incidents for vulnerabilities found in the system.</p> <p>Amazon Web Services (AWS) Bastion host: Deployed within the AWS GovCloud boundary to provides a secure login mechanism for the Cisco FedOps Team to manage the backend servers.</p>	<p>Cisco FedOps</p> <p>Note: To manage their overlay networks, customers can access the Cisco Catalyst SD-WAN Portal that is hosted in the management VPC.</p>

In addition to the components listed in the table, to assist with the flow of data, the Cisco Catalyst SD-WAN for government solution uses Amazon Web Services' (AWS) Simple Queue Service (SQS), AWS Application Load Balancer (ALB), AWS Web Application Firewall (WAF), and the Amazon Aurora MySQL database. The network access control list (ACL) of the management Amazon VPC is managed using a Cisco Catalyst SD-WAN for government-approved instance of Okta.

Federal Boundary

The federal boundary for Cisco Catalyst SD-WAN for government contains a customer Amazon VPC and an Amazon management VPC. Individual customers have their own Amazon VPC.

The Cisco Catalyst SD-WAN for government's federal boundary is a restrictive environment that has these entry points for each customer:

- Customer Amazon VPC
- Management Amazon VPC
- Bastion Host VPC
- Analytics VPC

Customer Access to the Amazon Virtual Private Cloud

Only customers can access their customer Amazon VPC. They have application access to the SD-WAN overlay components and optionally, Catalyst SD-WAN virtual devices (such as Catalyst 8000v). They do not have access to the AWS boundary.

When customers set up their overlay network, it includes the following Cisco Catalyst SD-WAN components:

- Cisco SD-WAN Manager
- Cisco SD-WAN Controller
- Cisco SD-WAN Validator

How Customers Access their Customer Amazon VPC

To access their customer Amazon VPC, customers must allow the Cisco Catalyst SD-WAN Portal to allow trusted IP addresses to access their overlay network.

Management Access to the Amazon Virtual Private Cloud

The management Amazon VPC provides secure monitoring and end-to-end auditing of the Cisco Catalyst SD-WAN for government solution. An Amazon VPC is a secure location within the Amazon cloud with a set of allowed IP addresses and port numbers.

The only component that customers can access in the management Amazon VPC is the Cisco Catalyst SD-WAN Portal. The other components in the Cisco Catalyst SD-WAN Portal are only accessible to Cisco FedOps.

How Can Cisco FedOps Access the Management Amazon VPC

1. Connect to the Cisco network using the Cisco Secure Client.
2. Log in to the Cisco Catalyst SD-WAN Portal.

When a Cisco FedOps user logs in, the request goes through an AWS bastion host, which provides Secure Shell (SSH) access to all servers, including the management Amazon VPC.

3. Use a phishing-resistant security key, such as Yubikey with FIPS, for multi-factor authentication (MFA).
4. After the log in is authenticated, Cisco FedOps can connect to any device in the management Amazon VPC.

Data Flow

In the Cisco Catalyst SD-WAN for government solution, Cisco vMonitor collects data and logs from a variety of systems to check the health of the system and identify issues. Cisco vMonitor uses the following sources:

- Cisco Data Collection Agents (DCA): These agents are used to collect health data from Cisco Catalyst SD-WAN for government. Data from all these Cisco DCAs is then sent to the Cisco Data Collection Service (DCS).
- Splunk server: Monitors File Integrity Monitoring (FIM) on infrastructure servers. The controllers for the Cisco Catalyst SD-WAN for government solution have a built-in FIM server that collects audit logs and syslog changes. These changes are monitored by the Splunk server for vulnerability vectors. All the data is collected and the vulnerabilities are tagged and provided as POA&M reports.
- Okta: Splunk also polls the external Okta server that is used for MFA for Okta's logs on authentication and access attempts.
- Tenable Security Center: Performs vulnerability and compliance scans. This scanning is done weekly on the data in all VPCs except the customer VPC. The results of the scans are reported in the POA&M reports and remediated according to severity and SLA.

To ensure that data is secure, it is stored in AWS GovCloud. All the data (at rest and in transit) and control connections are SHA-2 compliant. The following types of data are stored:

- Domains accessed
- Private IP addresses
- Customers that have accessed the solution
- Any sniffing that occurs on the network

Data Collection Agent Configuration and Monitoring

The Cisco DCA is an agent that runs inside Cisco SD-WAN Manager, which can be hosted either on-premises or in the cloud. This Cisco DCA agent is used to report statistics, monitor, and provide telemetry data to Cisco Catalyst SD-WAN as long as the appropriate configurations are enabled.

To achieve this, the Cisco DCA contacts a service known as the Cisco DMS, which has relevant information regarding a customer's overlay network, for example, which region the network is located in, what are the data storage preferences, and so on. The Cisco DCA authenticates itself with the Cisco DMS using the custom OAuth credentials that are generated per customer overlay network (and communicated out of band to the customer). If the Cisco DMS is able to authenticate the Cisco DCA, the former gives the latter an authentication token and redirects the Cisco DCA to the appropriate Cisco DCS.

The Cisco DCS is the entry point for all telemetry data to get into Cisco Catalyst SD-WAN. There may be many instances of the Cisco DCS service depending on the public cloud, region, and so on. The Cisco DCA uses the token obtained in the prior flow to authenticate itself with the Cisco DCS and exchanges it for a regional Cisco DCS token. Thereafter, this token is used by the Cisco DCA when pushing all kinds of data to the Cisco DCS.

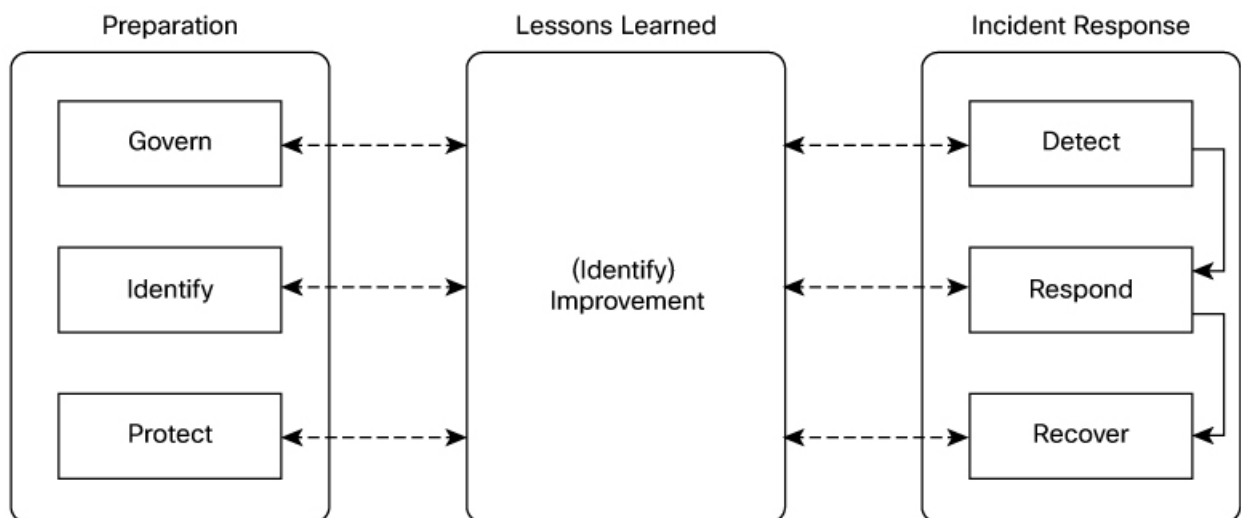
The Cisco DCA periodically collects data from its Cisco Catalyst SD-WAN localhost and pushes that data to the Cisco DCS. The Cisco DCS in turn, saves the data as JSON files in the S3 bucket. For every new JSON file that the S3 bucket receives, a new-object-created event is sent to an AWS Simple Notification Service (SNS) topic. Since Cisco vMonitor has already subscribed the topic with an HTTPS endpoint, Cisco vMonitor servers receive HTTPS requests from an AWS SNS for all the S3 new-object-created events. Cisco vMonitor servers validate the HTTPS request and use the metadata inside to fetch the actual files on S3 and update the database.

Incident Response

Incident response provides a consistently effective means of responding to and reporting on security incidents of the system. It encompasses all the actions taken to quickly restore normal information technology (IT) services and to minimize adverse impacts on business operations. Cisco Catalyst SD-WAN follows the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-61, Rev 3 definitions of an incident in determining when to activate the incident response team. The incident response plan coordinates with Cisco resources on an ongoing basis to remain prepared to identify, contain, eradicate, and recover from any incidents, if any, to the offering.

Responding to a security incident is not a single action, but an entire approach. This approach ensures that issues are detected and mitigated. The approach also has a step to recover from issues, if any, that were detected. It encompasses the following phases:

Figure 1: Incident Response Phases



Workflow for Using Cisco Catalyst SD-WAN for Government

To use Cisco Catalyst SD-WAN for government, you must do the following:

1. [Log in to the Cisco Catalyst SD-WAN Portal.](#)
2. [Create a Cisco Catalyst SD-WAN Cloud Hosted Fabric](#)
3. [Configure Cisco SD-WAN Manager.](#)
4. [Set up additional security features.](#)
5. [Monitor and manage your environment.](#)



CHAPTER 4

Cisco Catalyst SD-WAN Portal

- [Overview of the Cisco Catalyst SD-WAN Portal, on page 13](#)
- [Prerequisites for the Cisco Catalyst SD-WAN Portal, on page 16](#)
- [Benefits of the Cisco Catalyst SD-WAN Portal, on page 16](#)
- [Smart Accounts and Virtual Accounts, on page 16](#)

Overview of the Cisco Catalyst SD-WAN Portal

The Cisco Catalyst SD-WAN Portal is a cloud-infrastructure automation tool that: which

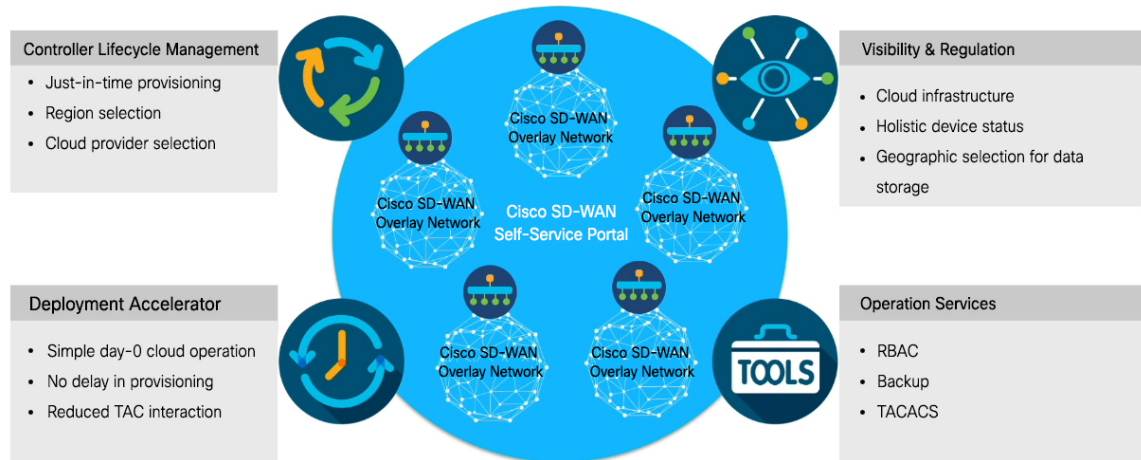
- is tailored for Cisco Catalyst SD-WAN,
- provides a quick way to provision, monitor, and maintain Cisco Catalyst SD-WAN control components on public cloud providers, and
- supports user authentication and granular access management for high security.

You can provision these control components using the Cisco Catalyst SD-WAN Portal:

- Cisco SD-WAN Manager
- Cisco SD-WAN Validator
- Cisco SD-WAN Controller
- Optional virtual devices such as the Cisco Catalyst 8000v

Benefits and Functions

Figure 2: Cisco Catalyst SD-WAN Portal Benefits and Operations



The Cisco Catalyst SD-WAN Portal enforces multi-factor authentication (MFA) by default for the portal access. You can configure the Cisco Catalyst SD-WAN Portal to use an identity provider (IdP) that lets you connect any user with any application on any device, using single sign-on (SSO). The Cisco Catalyst SD-WAN Portal is modularized into separate web servers, backend servers, and database clusters to achieve software scalability.

Cisco vMonitor collects data on the cloud infrastructure and generates health notifications about the overlay infrastructure for the customer in a common database. The Cisco vOrchestrator web server is also accessible for advanced features and existing infrastructure-tier customizations, if any, that you use. The Cisco Catalyst SD-WAN Portal uses Cisco vMonitor and Cisco vOrchestrator by way of API calls to orchestrate actions and monitor the overlay.

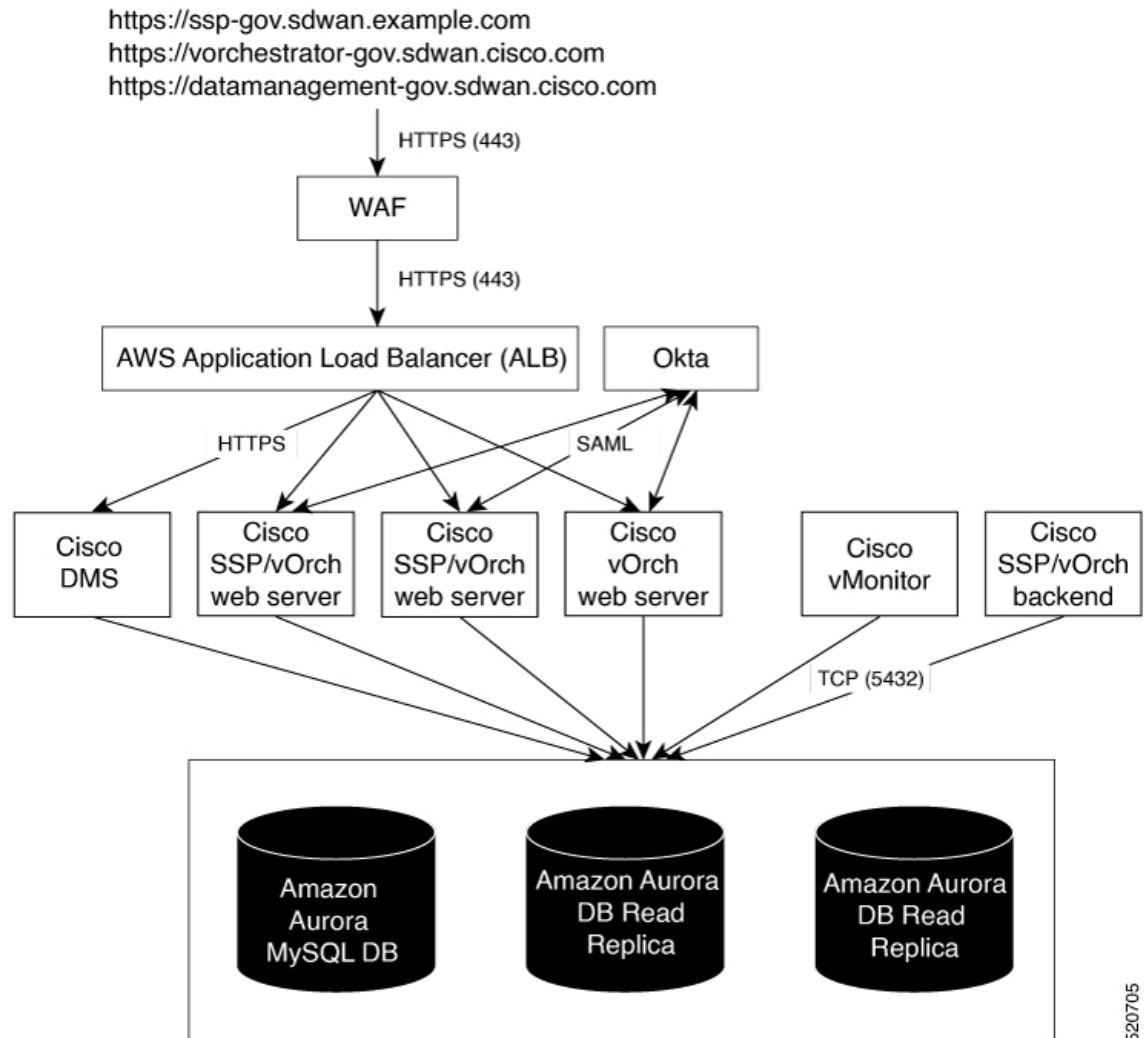


Note Cisco vMonitor and Cisco vOrchestrator can be accessed by Cisco FedOps only.

All three applications use a common global database that includes multiple read replicas for high availability and disaster recovery. The applications connect to the database using either Transport Layer Security (TLS) or Secure Sockets Layer (SSL).

Architecture (Government)

Figure 3: Cisco Catalyst SD-WAN Portal Architecture



520705

Audience

This document is intended for customers such as service providers, partners, and other end users.

There are two types of users for Cisco Catalyst SD-WAN Portal for Government:

- Customers, such as service providers, partners, and other end users.
- Cisco Catalyst SD-WAN Federal Operations (FedOps): A Cisco team that maintains and monitors Cisco Catalyst SD-WAN for Government.

Prerequisites for the Cisco Catalyst SD-WAN Portal

- Purchase a Cisco DNA subscription from the [Commerce Workspace](#).
- Create or open an existing Smart Account.
- Create a Virtual Account that is associated with your Smart Account.
- Add the device serial numbers on the Plug and Play Connect (PnP) portal.

For more information, see the [Network Plug and Play Connect Capability Overview](#).

Benefits of the Cisco Catalyst SD-WAN Portal

The Cisco Catalyst SD-WAN Portal:

- enables visibility into critical statistics like instance CPU utilization,
- provides a centralized dashboard for real-time monitoring of your Cisco Catalyst SD-WAN overlay networks,
- includes a wizard-driven interface that helps you easily navigate to tasks within the workflow,
- lets you select cloud providers and specify geographic locations for primary and secondary data storage,
- supports secure login using an identity provider (IdP) for single sign-on (SSO) with multi-factor authentication (MFA),
- supports role-based access control (RBAC),
- and supports provisioning new overlay networks with custom subnets that enable on-premises TACACS+ server connections.

Smart Accounts and Virtual Accounts

For more information, see [Workflow for Smart Account and Virtual Accounts for Provisioning the Controllers](#).

Smart Accounts

Smart Accounts are centralized, cloud-based data repositories that:

- contain the software licenses purchased by an organization,
- serve as a central hub for license management, and
- enable real-time enterprise-wide license management and compliance.

Use the Smart Account as a central repository to view software assets you have purchased, register and report software use, and manage licenses for your organization.

Using the Cisco Catalyst SD-WAN Portal, the Smart Account administrator can view and manage your control component infrastructure. Management tasks include viewing IP addresses for control components and

changing the control component IP access lists. To restrict access for other users, go to the Manage Smart Account section on [Cisco Software Central](#) and remove those users as Smart Account administrators. Alternatively, use the identity provider (IdP) onboarding feature to grant access to the Cisco Catalyst SD-WAN Portal based on trusted users in the IdP.

Virtual Accounts

Virtual Accounts are subaccounts within your Smart Account that:

- help you organize your Cisco assets in a way that aligns with your business,
- can be set up by department, product, geography, or another designation that suits your business model, and
- allow you to organize and manage your software licenses, devices, and users more granularly.

The system creates a default Virtual Account for you. Create an additional dedicated Virtual Account for Cisco Catalyst SD-WAN fabrics.

For more information, see [Create a Virtual Account Associated with Your Smart Account](#).

To provision a Cisco Catalyst SD-WAN control component, associate a Virtual Account with an offer attribute that is Cisco Catalyst SD-WAN-capable. An Cisco Catalyst SD-WAN-capable attribute is associated with a Virtual Account when ordering your Cisco DNA cloud license.



Note When you order DNA licenses using the enterprise agreement, the system does not automatically associate Virtual Accounts to an SD-WAN-capable attribute. Submit a cloud control component provisioning request form through the Enterprise Agreement Workspace for the CloudOps team to provision the control components. Contact Cisco Catalyst SD-WAN Technical Support to request access to the desired Virtual Account on the Cisco Catalyst SD-WAN Portal. After receiving access, you can provision the control components by providing the necessary enterprise agreement contract information.



CHAPTER 5

Access the Cisco Catalyst SD-WAN Portal

- [Workflow for Smart Account and Virtual Accounts for provisioning control components, on page 19](#)
- [Create a Virtual Account associated with your Smart Account, on page 20](#)
- [Access the Cisco Catalyst SD-WAN Portal for the first time, on page 20](#)
- [Log in to the Cisco Catalyst SD-WAN Portal, on page 21](#)

Workflow for Smart Account and Virtual Accounts for provisioning control components

This workflow describes how to create a Smart Account, create a Virtual Account, and associate the Cisco DNA subscription with your Virtual Account.

1. Open [Cisco Software Central](#) and create a Smart Account for your organization.
2. Create a Virtual Account associated with your Smart Account.
For instructions on how to create a Virtual Account, review [Virtual Accounts](#).
3. At the [Cisco Commerce Workspace](#), purchase a Cisco DNA subscription.



Note You must associate the Cisco DNA subscription with one Virtual Account within the respective Smart Account.

An account manager or sales representative usually places the order for the customer.

4. Choose the DNA cloud subscription product identification (PID) for your license.
Selecting the DNA cloud subscription PID automatically associates your Virtual Account with the SD-WAN-capable attribute for control component provisioning.
5. When the order is complete, the Virtual Account is available on the Cisco Catalyst SD-WAN Portal for control component provisioning.



Note The Virtual Account must include the device serial numbers that were added on the Cisco Plug and Play (PnP) portal. After creating the overlay through the Cisco Catalyst SD-WAN Portal, see the **Control Component Profile** tab on the Cisco PnP portal to view the mapping of the device serial numbers with their respective control components. This mapping provides the necessary information to add the devices to Cisco SD-WAN Manager or to perform zero-touch provisioning (ZTP). To confirm control component provisioning as part of the overlay creation process using the Cisco Catalyst SD-WAN Portal, view the **Control Component Profile** tab in the Cisco PnP portal.

For additional details, refer to [Cisco Network Plug and Play Connect Capability Overview](#).

Create a Virtual Account associated with your Smart Account

Before You Begin

Create a Smart Account for your organization using [Cisco Software Central](#).

For information on creating a Smart Account, refer to the documentation.

Create a Virtual Account

1. In [Cisco Software Central](#), choose **Manage account** under **Manage Smart Account**.
2. Click **Virtual Accounts**.
3. Click **Create Virtual Account**.
4. Click **Review Notice**, and after reviewing the notice, click **I Have Reviewed the Notice**.
5. Enter the required information in each field.



Note The **Parent Account** field is autopopulated with **At Top Level**. You may retain this selection.

6. Click **Next**.
7. (Optional) Assign users to the Virtual Account.
8. Click **Next**.
9. Click **Create Virtual Account**.

The newly created Virtual Account is listed in Virtual Accounts.

Access the Cisco Catalyst SD-WAN Portal for the first time

When you log in to the Cisco Catalyst SD-WAN Portal for the first time, you see a guided workflow. You can use this workflow to configure selected features and to create your first Cisco Catalyst SD-WAN overlay network.

Log in to the Cisco Catalyst SD-WAN Portal for the first time as a Smart Account administrator. If you do not use an identity provider (IdP), you must have Smart Account administrator privileges each time you log in.

If you use an IdP, you can access the Cisco Catalyst SD-WAN Portal with the permissions provided by the IdP.



Note You cannot use Virtual Account administrator-level access to log in to the Cisco Catalyst SD-WAN Portal, but you can use it with other portals, such as software.cisco.com. The Cisco Catalyst SD-WAN Portal does not accept Virtual Account administrator-level access.

Log in to the Cisco Catalyst SD-WAN Portal

1. For the commercial version of the Cisco Catalyst SD-WAN Portal, navigate to <https://ssp.sdwan.cisco.com/>. For the government version, log in at <https://ssp-gov.sdwangov.fedramp.cisco>
2. Enter your appropriate login credentials.
3. When prompted, set up or enter your multi-factor authentication (MFA) credentials. MFA is required for all users.



CHAPTER 6

Configure an Identity Provider for the Cisco Catalyst SD-WAN Portal

- [Configure an identity provider for the Cisco Catalyst SD-WAN Portal, on page 23](#)

Configure an identity provider for the Cisco Catalyst SD-WAN Portal

When you log in to the Cisco Catalyst SD-WAN Portal for the first time, you have the option to configure the Cisco Catalyst SD-WAN Portal to use the identity provider (IdP) of your organization, such as Okta Identity Management.



Note Configuring an IdP for the Cisco Catalyst SD-WAN Portal is optional.

After you configure your IdP and assign roles, you can log in using your organization's IdP instead of your account credentials on Cisco.com. For details on role configuration, refer to [Configure Cisco Catalyst SD-WAN Portal Roles for IdP Users](#).



Note When you set up an IdP in the Cisco Catalyst SD-WAN Portal, the issuer, login URL, and privacy-enhanced mail (PEM) key are not available from the IdP of your organization. This information is available after you set up the Assertion Consumer Service (ACS) URL and audience in your organization's IdP. When setting up your organization's IdP, we recommend that you add placeholder values for the ACS URL and audience. Later, you can configure the IdP on the Cisco Catalyst SD-WAN Portal and update your organization's IdP with the correct value of the ACS URL and audience Uniform Resource Identifier (URI) that is editable in the Cisco Catalyst SD-WAN Portal.

Before you begin

Before you configure an IdP in Cisco Catalyst SD-WAN Portal, create these variables on your organization's IdP. These variables are required for each user who logs in.

- `firstName`

- lastName
- email
- SSP_User_Role

For more information on roles, refer to [Configure Cisco Catalyst SD-WAN Portal Roles for IdP Users](#).

Configure an IdP for the Cisco Catalyst SD-WAN Portal

1. Specify the following information for your IdP.
 - Domain Name
 - IdP Issuer URL
 - IdP SSO URL
 - IdP Signature Certificate in PEM format
2. In federal environments only, check the **I acknowledge that this is a Federal IDP** check box.
3. To submit your IdP details, click **Submit Request**.
4. On your IdP site, confirm the IdP creation.



CHAPTER 7

Manage Role-Based Access

- [Configure Cisco Catalyst SD-WAN Portal roles for IdP users, on page 25](#)
- [Create additional roles, on page 25](#)

Configure Cisco Catalyst SD-WAN Portal roles for IdP users

Before you begin



Note Configuring Cisco Catalyst SD-WAN Portal roles for an identity provider (IdP) is optional.

Configure roles for IdP users

1. From the Cisco Catalyst SD-WAN Portal menu, choose **Manage Roles**.
2. Enter a name for the role.
3. For each of your virtual accounts, assign a role from this list:
 - **Monitor**: You can view and monitor all the overlay options in the Cisco Catalyst SD-WAN Portal.
 - **Overlay Management**: You can create, change, and monitor overlay networks.
 - **Administration**: You can perform the tasks defined by the monitor and overlay network roles, and onboard a secondary IdP.
4. Click **Add Role**.
5. After adding all the roles, click **Done**.
6. Log in to the Cisco Catalyst SD-WAN Portal again using your IdP credentials.

Create additional roles

To create an additional role, repeat the procedure described in the section.



CHAPTER 8

Manage fabrics

- [Create a Cisco SD-WAN Cloud-Pro fabric, on page 27](#)
- [Configure advanced options for a Cisco SD-WAN Cloud-Pro fabric, on page 31](#)
- [Delete a fabric, on page 35](#)
- [Specify the allowed list of IP addresses for managing control component access, on page 35](#)
- [Create Predefined Inbound Rules, on page 36](#)

Create a Cisco SD-WAN Cloud-Pro fabric

The Cisco Catalyst SD-WAN Portal provisions Cisco Catalyst SD-WAN fabrics using the information you provide during this procedure.

Before you begin


Ensure that you have these items:

- An active Cisco Smart Account.
- An active Cisco Virtual Account.
- The SA-Admin role for your Cisco Smart Account.
- A valid order for control components on Cisco Commerce (formerly CCW).

Create a Cisco SD-WAN Cloud-Pro fabric

1. Go to the URL that you received in the email from Cisco to access the Cisco Catalyst SD-WAN Portal, and log in.
2. From the Cisco Catalyst SD-WAN Portal menu, choose **Create Fabric**.
The **Create Cisco SD-WAN Fabric** page appears.
3. From the **Smart Account** drop-down list, choose the name of the Cisco Smart Account to which you want to associate the fabric.

**Note**

If your Cisco Smart Account is not listed in the drop-down, click  to refresh the list and search for your account by its domain ID.

4. From the **Virtual Account** drop-down list, choose the name of the Cisco Virtual Account to which you want to associate the fabric.
5. Select a Cisco SD-WAN Cloud or Cisco SD-WAN Cloud-Pro Fabric. See the Cisco SD-WAN Cloud Guide to create a Cisco SD-WAN Cloud fabric. If you select Cisco SD-WAN Cloud-Pro, a questionnaire dialog box appears. Provide the required details in the dialog box.
6. Check the appropriate boxes if you intend to use any of the listed features on the fabric. Select “None of the options” if you do not use any additional features. (required)
7. Enter the number of devices you plan to add to the fabric (required).
8. Enter the sales order number for any SD-WAN subscriptions you have (optional).
9. Click **Next**.

Based on your responses, you are directed to the Cisco SD-WAN Cloud or Cisco SD-WAN Cloud-Pro fabric creation workflow. See the Cisco SD-WAN Cloud to create a Cisco SD-WAN Cloud fabric. The remaining instructions apply to creating a Cisco SD-WAN Cloud-Pro fabric.

10. Click **Assign Control Components** and perform these actions in the **Assign Control Components** area:
 - a. Configure the options for the number of control component types in a Cisco SD-WAN Cloud-Pro fabric.

Option	Description
Assign (for the SD-WAN Manager control component type)	Enter the number of Cisco SD-WAN Manager control components in your deployment. Valid values are 1, 3, or 6 .
Assign (for the SD-WAN Validator control component type)	Enter the number of Cisco SD-WAN Validators in your deployment. The minimum value is 2 .
Assign (for the SD-WAN Controller control component type)	Enter the number of Cisco SD-WAN control components in your deployment. The minimum value is 2 .
Enable Cluster	Applies only if you choose a value of 3 or 6 for the number of Cisco SD-WAN Manager controllers. Turn on this option to create a Cisco SD-WAN Manager cluster.

Option	Description
Cluster Type	Applies only if you turn on the Enable Cluster option. Choose Single Tenant Cluster to enable a single tenant cluster.

b. Click **Assign**.

11. In the **Fabric** field, enter a name for your fabric.
12. Under **Cloud Provider**, choose **AWS** or **Azure** as the cloud provider at which you want the control components for your fabric to be hosted. Government sites use only Amazon Web Services (AWS).



Note IPv6 provisioning is only supported for Single Tenant fabrics hosted on AWS.

13. From the **SD-WAN Version** drop-down list, choose the version of Cisco Catalyst SD-WAN that you want to use on your control components.

Use the recommended version unless you require features that are offered only in another version. To see recommended versions, visit [Cisco Software Central](#).

Cisco Catalyst SD-WAN releases are described in the Cisco Catalyst SD-WAN Release Notes in the **Release Information** area in [User Documentation for Cisco IOS XE \(SD-WAN\) Release 17](#).
14. Under **Locations**, perform these actions:
 - a. From the **Primary Location** drop-down list, choose the geographical location where the Cisco SD-WAN Manager is provisioned.

We recommend that you choose a location that is relatively close to your network.
 - b. From the **Secondary Location** drop-down list, choose the geographical location for backed up data storage and load balancing. If you choose the same region for both primary and secondary, then the Cisco Catalyst SD-WAN Portal automatically places the instances in two different Zones within the same region.

We recommend that you choose the location that is closest to the primary location.
 - c. From the **Data Location** drop-down list, choose the geographical location for Cisco SD-WAN Analytics data storage.

We recommend that you choose the location that is closest to the primary location.
15. Enter this information under **Contacts**:
 - In the **Fabric Admins** field, enter one or more comma-separated email addresses or mailing list names to which the Cisco Catalyst SD-WAN Portal sends notifications about the fabric.
 - In the **Cisco Contact Email** field, enter the email address of a contact at Cisco that can be reached if there is an urgent issue and the administrator of the fabric cannot be reached.
 - In the **Enter Contract Number of Service** field, enter the number of your Cisco Catalyst SD-WAN Portal service contract.

- In the **Enter CCO ID of Service Requester** field, enter the Cisco Connection Online (CCO) ID of the person who created the ticket for your Cisco Catalyst SD-WAN Portal.

Alert Notifications: The Cisco Catalyst SD-WAN Portal generates alert notifications for various events, such as expiring subscriptions, maintenance windows, and feature changes. Notifications are sent to the registered Overlay Admin contact email addresses configured under Overlay Details. Keep your email addresses updated. You can register multiple email addresses. To update your registered email addresses, perform these steps:

- a. Log in to Cisco Catalyst SD-WAN Portal at <https://ssp.sdwan.cisco.com> for commercial sites or <https://ssp-gov.sdwan.gov.fedramp.cisco> for government sites. You must have PNP Smart Account Administrator role to be able to log in.

Alternatively, if your Smart Account Administrator has already set up an identity provider (IdP) on the Cisco Catalyst SD-WAN Portal, then you can log in with the role provided by your Administrator.

- b. Go to **Overlay Details > Description > Overlay Admin**
- c. Click on the pencil icon to edit.
- d. Type in your email address and hit **Tab**.
- e. Click on the check mark icon to save.

16. Configure the **Advanced Options** as needed.

For detailed information about these options, refer to [Configure Advanced Options for a Cisco SD-WAN Cloud-Pro Fabric](#).

- **Custom Subnets:** Configure private IP addresses for control component interfaces.
- **Custom Domain Settings:** Configure custom domains for accessing Cisco SD-WAN Validator and Cisco SD-WAN Manager.
- **Snapshot Settings:** Configure how often the system takes a snapshot of Cisco SD-WAN Manager instances in your deployment.
- **Custom Organization Name:** Configure a unique organization name to identify your network.
- **Compliance:** Select certification compliances for the fabric. Compliance is on by default in the government version of the Cisco Catalyst SD-WAN Portal.
- **Dual Stack:** Enable IPv6 dual stack.

17. Click **Click here to review and agree to Terms and Conditions before proceeding**. In the **Terms and Conditions** dialog box, review the displayed information and click **I Agree**.

18. Click **Create Fabric**.

Your request is submitted. Manual approval for a Cisco SD-WAN Cloud-Pro fabric can take up to 24 hours (1 day). You can view the progress of your request in the **Requests** area.

In addition, a password appears in the Cisco Catalyst SD-WAN Portal **Notification** page. Use this password to access the fabric for the first time.

After logging in, change this password immediately to secure your environment.



Note The system-provided control component password is no longer visible in the Cisco Catalyst SD-WAN Portal after seven days. We recommend that you keep a copy of the password if you want to retain it.

19. Once you receive a notification that your fabric is ready, follow these steps:
- Install control component certificates on your devices. For more details about certificate installation, refer to [Use Case: Cisco-Hosted Cloud Overlays with Software Version 19.x and Above](#).
 - Install web server certificates. For information about installing web server certificates, refer to [Web Server Certificates](#).

Configure advanced options for a Cisco SD-WAN Cloud-Pro fabric

Advanced options allow you to configure various settings for your fabric if the default settings are not what you need.

To configure advanced options for your fabric, click **Advanced Options** on the Cisco Catalyst SD-WAN Portal, then configure options as described in these sections:

- [Custom Subnets](#)
- [Custom Domain Settings](#)
- [Snapshot Settings](#)
- [Custom Organization Name](#)
- [Compliance](#)
- [Dual Stack](#)

Custom Subnets

The **Custom Subnets** area includes options for configuring private IP addresses to be used for control component interface IP addresses.

For use cases such as connecting to an enterprise TACACS+, connecting to an authentication, authorization, and accounting (AAA) server, sending messages to a syslog server, or enabling management access to instances over the fabric, you may want to deploy the control components with private IP addresses in specific prefixes which are unique and are not used elsewhere within your fabric.

Option	Description
Primary Subnet	

Option	Description
VPC Subnet	<p>Enter a private IP address block for the VPC for the primary region, For example, 192.168.0.0/24.</p> <p>This IP address block must be reachable from your private network.</p>
Primary Location	Shows the primary region for the fabric.
Management Subnet	<p>Enter a private IP address block for the management subnet for the primary region.</p> <p>This address must be within the IP address block that you enter for the VPC.</p> <p>The minimum size of the IP address block is 16 bits.</p>
Control Subnet	<p>Enter a private IP address block for the control subnet for the primary region.</p> <p>This address must be within the IP address block that you entered for the VPC.</p> <p>The minimum size of the IP address block is 16 bits.</p>
Cluster Subnet	<p>Enter a private IP address block for the cluster subnet for the primary region.</p> <p>This address must be within the IP address block that you entered for the VPC.</p> <p>The minimum size of the IP address block is 16 bits.</p>
Secondary Subnet	
VPC Subnet	<p>Enter a private IP address block for the VPC for the secondary region, for example, 192.168.1.0/24.</p> <p>This IP address block must be reachable from your private network.</p>
Primary Location	Shows the secondary region for the fabric.
Management Subnet	<p>Enter a private IP address block for the management subnet for the secondary region.</p> <p>This address must be within the IP address block that you entered for the VPC.</p> <p>The minimum size of the IP address block is 16.</p>
Control Subnet	<p>Enter a private IP address block for the control subnet for the secondary region.</p> <p>This address must be within the IP address block that you entered for the VPC.</p> <p>The minimum size of the IP address block is 16.</p>

Option	Description
Cluster Subnet	<p>Enter a private IP address block for the cluster subnet for the secondary region.</p> <p>This address must be within the IP address block that you entered for the VPC.</p> <p>The minimum size of the IP address block is 16.</p>

Custom Domain Settings

The **Custom Domain Settings** area includes options for configuring custom domains for accessing Cisco SD-WAN Validator and Cisco SD-WAN Manager.



Note For government deployments, the default domain is `sdwangov.fedramp.cisco` and cannot be changed.

By default, the domain name for commercial deployments is `cisco.com`. You can specify another domain, if needed.

If you specify a custom domain, you must create your own domain name systems for the Cisco SD-WAN Validator and Cisco SD-WAN Manager because we do not have access to your domains.

After you configure a custom domain, make these mappings to allow control component certificates to come up:

- Map the Cisco SD-WAN Validator DNS to all VPN 0 IP addresses.
- Map the Cisco SD-WAN Manager DNS to all VPN 512 IP addresses.

Option	Description
SD-WAN Validator	Enter the name of the DNS for the Cisco SD-WAN Validator.
SD-WAN Manager	Enter the name of the DNS for the Cisco SD-WAN Manager.

Snapshot Settings

The **Snapshot Settings** area includes an option for configuring how often the system takes a snapshot of Cisco SD-WAN Manager instances in your deployment.

By default, the network overlay configuration is backed up once a day and seven snapshots are stored.

For more detailed information about snapshots, see [Information About Snapshots](#).

Option	Description
Frequency	Choose how often the system takes a snapshot of Cisco SD-WAN Manager instances: <ul style="list-style-type: none"> • Once a day • Once in 2 days • Once in 3 days • Once in 4 days

Custom Organization Name

The **Custom Organization Name** area includes an option for configuring a unique organization name to identify your network.

Option	Description
Custom Organization Name	Enter a unique name for your organization. You can enter a name of up to 56 characters. To ensure that each organization's name is unique, the Cisco Catalyst SD-WAN Portal automatically appends a hyphen and your virtual account ID at the end of the name you enter.

Certification Compliance Modes

The **Compliance Configuration** area includes certification compliance options for the fabric in commercial deployments only. These compliance modes are available:

Table 1: Supported Certifications

Option	Description
PCI-DSS	Payment Card Industry Data Security Standard, Service Provider, Level 1
SOC2	System and Organization Controls
ISO27001, ISO27017, ISO27018, ISO27701	International Organization for Standardization
C5	Cloud Computing Compliance Controls Catalog (Germany)
ENS	Esquema Nacional de Seguridad (Spain)
Tx-RAMP	Texas Risk and Authorization Management Program Level 2

Dual Stack

The **Dual Stack** area includes an option for enabling IPv6 for control components on AWS hosted fabrics. IPv6 provisioning is only supported for Single Tenant fabrics hosted on AWS.

Enabling this option is required if your enterprise network is configured with IPv6. After this option is enabled, the fabric subnets are configured with both IPv4 and IPv6. IPv6 addresses are assigned by your cloud service provider.



Note After this option is enabled for a fabric, it cannot be disabled.

Option	Description
IPv6 Dual Stack	Select the checkbox to enable IPv6 dual stack for control components.

Delete a fabric

You cannot delete a fabric. If you need assistance, contact Cisco Catalyst SD-WAN Technical Support.

Specify the allowed list of IP addresses for managing control component access

For Cisco SD-WAN Cloud-Pro fabrics, you can specify trusted IP addresses, including prefixes, from which you can manage access to control components. To enable management access, specify a rule type, protocol, port range, and the source IP (IP addresses and prefixes) for which you require access.



Note You do not need to add the IP addresses of WAN edge devices for them to join the fabric. Devices with any IP address can join the fabric, using Datagram Transport Layer Security (DTLS) or Transport Layer Security (TLS) tunnels, as long as Cisco SD-WAN Manager allows the device serial numbers.

- You can add up to 200 rules per fabric.
 - Each rule is uniformly applied to all Cisco SD-WAN Cloud-Pro control components within the fabric.
 - The same rules are automatically applied when new Cisco SD-WAN Cloud-Pro instances are added, or when existing instances are replaced. Each rule can specify either a single IP address or a larger IP prefix.
1. From the Cisco Catalyst SD-WAN Portal dashboard, navigate to your fabric.
 2. In the **List View** tab, click the name of your fabric.
 3. Click **Inbound Rules**.
 4. Click **Add Inbound Rule**.
 5. Specify the following parameters for your IP address or prefix:
 - **Rule type:** Choose a rule type: **All**, **SSH**, **HTTPS**, **Custom TCP rule**, or **Custom UDP rule**.
 - **Port range:** For custom TCP and UDP rules, specify a port range.

- **Source:** Specify one or more IP addresses or IP address prefixes. For multiple entries, press tab to enter the next IP address or prefix.
 - **Descriptions:** Enter a description of the inbound rule.
6. Click **Add Rule**.
 7. Click **Add New Inbound Rule** and add other IP addresses or IP address prefixes that you want to allow. (Optional)

Create Predefined Inbound Rules

Table 2: Feature History

Feature Name	Release Information	Description
Predefined Inbound Rules	March 2023 Release	With this feature you can specify trusted IP addresses. These IP addresses are applied to any new overlay that you create under the Smart Account for which you configure this feature. These IP addresses can also be applied to existing overlays under the Smart Account for which you configure this feature.

Information About Predefined Inbound Rules

With this feature you can create inbound rules, each of which specifies trusted IP addresses. These IP addresses are applied to any new overlay that you create under the Smart Account for which you configure this feature. These IP addresses can also be applied to existing overlays under the Smart Account for which you configure this feature.

An inbound rule includes the rule name, protocol and port range to which the rule applies, and source IP address or prefix information. You can create up to 200 inbound rules.

Use Cases for Predefined Inbound Rules

Predefined inbound rules provide a convenient way to add the same group of trusted IP addresses to existing and new overlays. By creating predefined inbound rules, you avoid having to configure trusted IP address for each overlay manually.

Configure Predefined Inbound Rules

1. From the Cisco Catalyst SD-WAN Portal menu, choose **Admin Settings**.
2. Click ... adjacent to the Smart Account for which you want to configure a predefined inbound rule and click **Manage Predefined Inbound Rules**.

A list of the inbound rules that have been configured appears.

3. Click **Add Predefined Inbound Rules**.
4. In the **Add Inbound Rule** area, perform these actions:
 - a. In the **Name** field, enter a unique name for the rule.
 - b. From the **Rule Type** drop-down list, choose the type of protocol to which the rule applies (**All**, **SSH**, **HTTPS**, **Custom TCP rule**, or **Custom UDP rule**).
 - c. If you choose a rule type of **Custom TCP rule** or **Custom UDP rule**, in the **Port Range** field, enter a port range to which the rule applies.
 - d. In the **Source** field, enter an IP address or IP address prefix.
 - e. In the **Description** field, enter a descriptions of the predefined inbound rule.
 - f. (Optional) Click **Automatically add this rule to ALL overlays** to add this new rule to existing overlays under this Smart Account, in addition to future overlays that are created under this Smart Account.
If you do not click this option, this rule is added to future overlays only.
 - g. Click **Add**.



CHAPTER 9

Use Cisco Catalyst 8000V as a Cloud Gateway for a fabric

- [Information about Cisco Catalyst 8000V as a cloud gateway for a fabric, on page 39](#)
- [Use cases for Cisco Catalyst 8000V as a cloud gateway for a fabric, on page 40](#)
- [Prerequisites for Cisco Catalyst 8000V as a cloud gateway for a fabric, on page 40](#)
- [Restrictions for Cisco Catalyst 8000V as a cloud gateway for a fabric, on page 40](#)
- [Configure Cisco Catalyst 8000V as a cloud gateway for a fabric, on page 40](#)

Information about Cisco Catalyst 8000V as a cloud gateway for a fabric

Table 3: Feature History

Feature Name	Release Information	Description
Cisco Catalyst 8000V as a cloud gateway for a fabric	SD-WAN Portal: 2023-05 Cisco Catalyst SD-WAN Control Components Release 20.6.1	This feature lets you configure a Cisco Catalyst 8000V device as the cloud gateway for connecting a virtual private cloud with a private data center.

The Cisco Catalyst 8000V serves as the cloud gateway for connecting a virtual private cloud (VPC) with a private data center.

You can configure a Cisco Catalyst 8000V device as a cloud gateway in these ways, depending on your requirements:

- Create a new fabric and add a Cisco Catalyst 8000V device as the cloud gateway for each region in the fabric.
- Add a Cisco Catalyst 8000V device to each region in an existing fabric.
- Replace Cisco vEdge Cloud in an existing fabric with a Cisco Catalyst 8000V device.

Use cases for Cisco Catalyst 8000V as a cloud gateway for a fabric

You can use Cisco Catalyst 8000V as a cloud gateway in these scenarios:

- Integrating your fabric with a TACACS or RADIUS server for AAA (authentication, authorization, and accounting) when the server resides in a private data center that you access through a VPN.
- Sending syslog information to a private data center that you access through a VPN.

Prerequisites for Cisco Catalyst 8000V as a cloud gateway for a fabric

Before deploying the 8000V as a gateway, confirm these requirements:

- You must have a Cisco SD-WAN Manager administrator username and password.
- You must have a Smart Account administrator username and password.
- You must know the serial number of the 8000V that you are adding to a fabric.

Restrictions for Cisco Catalyst 8000V as a cloud gateway for a fabric

You can use the 8000V as a cloud gateway only in Cisco SD-WAN Cloud-Pro environments.

Configure Cisco Catalyst 8000V as a cloud gateway for a fabric

Before you begin

Obtain the serial number of each 8000V device that you are configuring. Go to [Cisco Software Central](#). In the **Smart Licensing** area, click **Manage Devices** under **Network Plug and Play**.

Configuration procedures

Use this table to find the steps for configuring an 8000V device as a cloud gateway in various scenarios. Choose the scenario that corresponds to your requirements. For each scenario, the table provides the general steps and links to more detailed information.

Scenario	General Steps	Reference
Create a new fabric and add an 8000V device as the cloud gateway for every region in the fabric.	Step 1: In the Cisco Catalyst SD-WAN Portal, create a new fabric.	See Create a Cisco Catalyst SD-WAN Cloud Hosted Fabric .
	Step 2: In the Cisco Catalyst SD-WAN Portal, configure a cloud gateway.	See Configure a cloud gateway in the Cisco Catalyst SD-WAN Portal , on page 41.
Add an 8000V device to every region in an existing fabric.	In the Cisco Catalyst SD-WAN Portal, configure a cloud gateway.	See Configure a cloud gateway in the Cisco Catalyst SD-WAN Portal , on page 41.
Replace Cisco vEdge Cloud with an 8000V device in an existing fabric.	Step 1: In the Cisco Catalyst SD-WAN Portal, configure a cloud gateway.	See Configure a cloud gateway in the Cisco Catalyst SD-WAN Portal , on page 41.
	Step 2: You can open a support case to request that the existing vEdge Cloud be removed.	See Open a support case for a fabric update , on page 43.

Configure a cloud gateway in the Cisco Catalyst SD-WAN Portal

1. Log in to the Cisco Catalyst SD-WAN Portal with administrator credentials.
2. Click the fabric for which you want to configure a cloud gateway.
3. From the **Actions** drop-down menu, choose **Add Cloud Gateways**.
4. Configure the fields listed in this table.



Note The Cisco Catalyst SD-WAN Portal does not save the usernames and passwords that you enter in these fields.

Field	Description
vManage Admin Credentials	
Username	Enter your Cisco SD-WAN Manager administrator username.
Password	Enter your Cisco SD-WAN Manager administrator password.
Smart Account Admin Credentials	
Username	Enter your Cisco Smart Account administrator username.
Password	Enter your Cisco Smart Account administrator password.

Field	Description
Cloud Gateway Serials	
Serial	<p>The number of fields that appear equals the number of regions in your fabric.</p> <p>Enter the serial number of the Cisco 8000V in each Serial field to designate it as a cloud gateway for each region.</p> <p>Ensure that each serial number you enter is unique.</p>
Custom IPs	
System IPs	<p>The number of System IPs fields equals the number of regions in your fabric.</p> <p>Optionally, enter an IP address in each field to configure a system interface for the cloud gateway that you are adding.</p> <p>A system interface IP address is persistent and identifies the device. It works like a router ID, which identifies the router from which packets originate.</p> <p>Specify a system IP address using decimal four-part dotted notation as an IPv4 address. Enter only the address because the prefix length (/32) is implicit.</p> <p>Select any IPv4 address except for 0.0.0.0/8, 127.0.0.0/8, and 224.0.0.0/4, or 240.0.0.0/4 and later.</p> <p>If you do not specify a system IP address, the Cisco Catalyst SD-WAN Portal assigns a random IP address. This address might duplicate the IP address of another device.</p> <p>Ensure that the IP address you enter is unused in the existing fabric. This prevents conflicts when provisioning the cloud gateway.</p>

Field	Description
Enable Webhook via Cloud Gateway	<p>This option applies only when Amazon Web Services (AWS) is the cloud provider for a dedicated fabric.</p> <p>To route webhook messages from Cisco SD-WAN Manager through a cloud gateway, select this option.</p> <p>Enabling this option is useful when your webhook server is hosted in your private network and no internet traffic is forwarded to this server. When this option is enabled, a connection is provisioned between your SD-WAN fabric and your private network.</p> <p>Once you enable this option, add a routing table entry on the server to forward network traffic to the webhook server through the cloud gateway. Refer to the email that you receive after the cloud gateway is provisioned for instructions.</p>

5. Click **Submit**.

Open a support case for a fabric update

To open a support case for a fabric update, go to Cisco [Support Case Manager](#), log in with your Cisco credentials, and click **Open New Case**.



CHAPTER 10

Monitor fabrics

You can monitor the Cisco Catalyst SD-WAN control components and devices in the fabrics. You can also view the Plan of Actions and Milestones report.

- [Monitor control components and devices in fabrics, on page 45](#)
- [View fabric and control component details, on page 45](#)
- [View change window notifications, on page 46](#)

Monitor control components and devices in fabrics

1. From the Cisco Catalyst SD-WAN Portal dashboard, click the **List View** tab.
The list of fabrics appears.
2. Select your fabric.
3. In the **Controller View** area, click the control component that you want to monitor—**SD-WAN Manager**, **SD-WAN Validator**, **SD-WAN Controller**, **Cloud Gateways**, or **vEdge**.
4. In the **Control Components** window, you can filter by network usage, CPU usage, or duration. Filter by state, type, version, or region to further narrow the list.



Note To align with Cisco Catalyst SD-WAN rebranding, the **Controllers** tab is renamed as the **Control Components** tab from Cisco IOS XE Catalyst SD-WAN Release 17.13.1a.

View fabric and control component details

1. From the Cisco Catalyst SD-WAN Portal dashboard, click the **List View** tab.
The list of fabrics appears.
2. Click the name of the fabric.
The **Dashboard > Overlays > Details** page displays detailed information for your fabric.

View change window notifications

Table 4: Feature History

Feature Name	Release Information	Description
Change Window Notifications	2021-02 Release	<p>Change window notifications let you view when your Cisco Catalyst SD-WAN fabric maintenance events start or end. You can also access details about the scheduled change notification and the planned maintenance operation.</p> <p>Cisco Catalyst SD-WAN Portal customers can only view change window notifications. A CloudOps user needs to schedule or start a change window notification.</p>

Change window notifications let you view the start and end times of your Cisco Catalyst SD-WAN fabric maintenance events. You can also access details about the scheduled change notification and the planned maintenance operation.

Banner alerts are displayed for notifications scheduled to start or that begin within 10 days. If a notification is completed or scheduled to start in more than 10 days, banner alerts are not displayed on the Cisco Catalyst SD-WAN Portal dashboard.

If a change notification has started, it shows as ongoing in the banner alert.

If a change notification is scheduled, it shows as started in the banner alert.

Before you begin

Cisco Catalyst SD-WAN Portal customers can only view change window notifications.

Only a CloudOps user can schedule or start a change window notification.

View change window notifications for all fabrics

1. From the Cisco Catalyst SD-WAN Portal dashboard, under **Change Window Notifications**, click a fabric that is scheduled or started.

The **Dashboard > Change Window Notifications** page is displayed with the list of fabrics.

A banner alert is displayed for every change window notification.

View all change window notifications for your fabrics on this page.

2. Optionally, filter by status to change the number of fabrics displayed.
3. Click **Change Window Notifications** to display all change window notifications and view their descriptions in the details column.

The **Dashboard > Overlays > Details > Change Window Notifications** page displays.

View change window notifications for specific fabrics

1. To view a change notification for a specific fabric, from the Cisco Catalyst SD-WAN Portal dashboard, click a fabric that has a scheduled or started change notification.

The **Dashboard > Overlays > Details** page is displayed.

2. Click an overlay that has a scheduled or started change window notification.

For change window notifications specific to a fabric, the banner alert is displayed without the fabric name because you are already viewing it.

On this page, view change window notifications for the selected fabric.

View the list of change window notifications

1. From the Cisco Catalyst SD-WAN Portal dashboard, click the fabric for which you have a scheduled or started change window notification.

The **Dashboard > Overlays** page displays.

2. Click the fabric name.

The **Dashboard > Overlays > Details** page displays.

3. In **Change Window Notifications**, choose the scheduled or started change window notification.

The **Dashboard > Overlays > Details > Change Window Notifications** page displays where you can view detailed information about your change notification event.



CHAPTER 11

Manage account settings

The table lists the feature history for managing account settings.

Table 5: Feature History

Feature Name	Release Information	Description
Support for managing predefined inbound rules	2022-11 Release	This feature enables you to specify trusted IP addresses and prefixes to manage control component access. You can also apply predefined inbound rules to all fabrics.

- [Information about predefined inbound rules, on page 49](#)
- [Benefits of predefined inbound rules, on page 49](#)
- [Manage predefined inbound rules, on page 50](#)

Information about predefined inbound rules

You can specify predefined inbound rules for allowing trusted IP addresses, including prefixes, to manage control component access. The predefined rules apply to any existing or new fabric created with the associated Smart Account.

You can add up to two hundred rules per fabric.

Benefits of predefined inbound rules

With predefined inbound rules, you can:

- automatically apply rules to any overlay that you create with the associated Smart Account, and
- support audit log entries for allowed IP addresses.

Manage predefined inbound rules

Before you begin

1. Create a Smart Account.

For more information on creating a Smart Account, see [Workflow for Smart Account and Virtual Accounts for Provisioning the Controllers](#).

2. Create a fabric.

For more information on creating a Cisco SD-WAN Cloud-Pro fabric, see [Create a Cisco SD-WAN Cloud-Pro Overlay Network](#).

Manage predefined inbound rules

1. From the Cisco Catalyst SD-WAN Portal menu, choose **Admin Settings**.
2. Under **Actions**, click . . . and choose **Manage Predefined Inbound Rules** from the drop-down list.
3. Click **Add Predefined Inbound Rules** to add a predefined inbound rule.
4. Configure the following fields:

Field	Description
Name	Enter a name for the predefined inbound rule.
Rule Type	Choose one of the available options from the drop-down list. <ul style="list-style-type: none"> • All • SSH • HTTPS • Custom TCP rule • Custom UDP rule
Protocol	Protocol is automatically populated depending on which Rule Type you choose.
Port Range	Enter a port range. If you chose Custom TCP rule or Custom UDP rule , the port range was automatically populated.
Source	Enter an IP address or an IP address prefix.
Description	Enter a description for the predefined inbound rule.

Field	Description
Automatically add this rule to ALL fabrics	Select this option to apply the predefined rules to all the fabrics associated with your Smart Account. If you do not select this option, the rule is not added to your existing fabrics.

5. Click **Add**.



CHAPTER 12

Configuring system snapshots

- [Information about system snapshots, on page 53](#)
- [Take an on-demand snapshot, on page 54](#)
- [View snapshots, on page 55](#)

Information about system snapshots

A Cisco SD-WAN Manager snapshot is a saved state of a Cisco SD-WAN Manager instance. Snapshots provide recovery points that the CloudOps team can use to restore your system. The SD-WAN Portal automatically saves the snapshots.

By contrast, you do not need to create snapshots for SD-WAN Controllers or SD-WAN Validators because they are stateless.

Which Cisco Catalyst SD-WAN installations store snapshots?

In Cisco SD-WAN Cloud and Cisco SD-WAN Cloud-Pro environments, the SD-WAN Portal manages saving snapshots of SD-WAN Manager, which are saved to cloud storage managed by Cisco. The system stores snapshots in the primary region that you select when you set up the SD-WAN fabric.

Viewing snapshot details

You can view details of the saved snapshots in the SD-WAN Portal. You cannot download the snapshots themselves.

Snapshot types

This table describes the available snapshot types.

Table 6: Snapshot types

Snapshot type	Description	When they are taken	How many are retained	How long they are retained
On-demand	<p>You can take an on-demand snapshot at any time, such as before a major change to your Cisco SD-WAN Manager configuration. Before the change window, freeze configuration changes and allocate up to eight hours (480 minutes) to create and save the on-demand snapshot.</p> <p>See Take an On-Demand Snapshot.</p>	On-demand	1	15 days. If you take another on-demand snapshot, retention ends sooner.
Regular	<p>Regular snapshots are saved at a configurable interval of one to four days. The snapshot typically occurs at midnight in the region of SD-WAN Manager.</p> <p>Set the interval during fabric creation:</p> <p>Advanced Options > Edit > Snapshot Settings</p> <p>See Create a Cisco SD-WAN Cloud-Pro Overlay Network.</p> <p>For an existing fabric, you can edit the snapshot interval in the SD-WAN Portal:</p> <p>View details > Snapshots > Actions > Edit snapshot frequency</p>	Interval you define: one to four days.	7	<p>The oldest of seven is discarded when a new snapshot is created.</p> <p>The retention duration is:</p> <p>(7 * use config interval) which is seven to 28 days.</p>
Golden	<p>You can mark a single regular or on-demand snapshot as Golden to save it for a longer period. Use this when SD-WAN Manager is in an ideal state for a long-term recovery point.</p> <p>Marking a new snapshot as Golden removes the Golden designation from the previous Golden snapshot. The previous Golden snapshot is then subject to removal according to its expiration schedule.</p>	This is an existing regular or on-demand snapshot manually marked as Golden.	1	90 days

Take an on-demand snapshot

You can take an on-demand snapshot of Cisco SD-WAN Manager configuration when needed. We recommend that you take a snapshot before any major change window.

When you take an on-demand snapshot, freeze configuration changes. Allocate up to 8 hours before the change window to ensure the snapshot is completed.

An on-demand snapshot is stored for 15 days after its creation, then it is deleted automatically. Only one on-demand snapshot is retained at any given time, as a new on-demand snapshot replaces the existing stored snapshot.



Note On-demand snapshots are not available for shared tenants.

1. From the Cisco Catalyst SD-WAN Portal, navigate to the list of available overlays.
The **Dashboard > Overlays** page appears.
2. Click the name of the fabric for which you want to take a snapshot.
3. From the **Dashboard > Cisco Hosted Overlays > Details** page, click the **Snapshot** tile.
4. From the **Actions** drop-down menu, choose **On-Demand Snapshot**.
5. In the **On-Demand Snapshot** area, turn on the switch for the Cisco SD-WAN Manager instance for which you want to take the snapshot.

For a Cisco SD-WAN Manager cluster, turn on the switches for each Cisco SD-WAN Manager instance in the cluster.

6. Click **Submit**.

Snapshot creation starts. Completing the snapshot can take up to 8 hours to complete, depending on the amount of data in Cisco SD-WAN Manager.

View snapshots

Before you begin

To view snapshot details, ensure that your overlay is associated with a Cisco SD-WAN Cloud-Pro controller.

For more information, see [Create a Cisco SD-WAN Cloud-Pro Overlay Network](#).

For more information on snapshots, see [Information About Snapshots](#).

View snapshots

1. From the Cisco Catalyst SD-WAN Portal dashboard, navigate to the list of available overlays.
The **Dashboard > Overlays** page displays.
2. Click the name of an overlay for which you want to view a snapshot.
3. From the **Dashboard > Cisco Hosted Overlays > Details** page, click on the tile for **Snapshot**.
The **Dashboard > Cisco Hosted Overlays > Details > Snapshots** page displays.

Table 7: Snapshot Fields

Field	Description
Snapshot ID (*denotes golden snapshot)	Specifies the snapshot ID. If a snapshot is a golden snapshot, it is denoted by an asterisk.
Name	Specifies the name of the snapshot.
Version	Specifies the version number of the Cisco SD-WAN Manager software.
Progress	Specifies the progress of the snapshot creation process.
Duration	Specifies the duration of the snapshot creation process.
State	Specifies the state of the snapshot creation process.
Device	Specifies the disk on Cisco SD-WAN Manager for which the snapshot was taken. There are either two or three disks on the Cisco SD-WAN Manager instance, depending on which version the device was originally provisioned on. Snapshots of all disks, taken at the same time, enable recovery and reconstruction of the Cisco SD-WAN Manager instance during disaster recovery.
Golden	Specifies if the snapshot is a golden snapshot. Available values are as follows: <ul style="list-style-type: none"> • false • true
Region	Specifies the region where this snapshot is stored.
Type	Specifies the type of snapshot. Available values include: <ul style="list-style-type: none"> • REGULAR, • ON-DEMAND, and • GOLDEN.
Overlay ID	Specifies the overlay ID.
Overlay	Specifies the overlay name and an ID.

Field	Description
Instance ID	Specifies the Cisco SD-WAN Manager instance ID.
Instance	Specifies the Cisco SD-WAN Manager instance name and ID.
Actions	To mark a specific date snapshot as golden, click Make Golden Snapshot .



CHAPTER 13

Configure webhooks

- [Information about webhooks, on page 59](#)
- [Configure a webhook, on page 59](#)
- [Send a webhook notification, on page 60](#)

Information about webhooks

A webhook is a method that enables HTTP communication between two systems and is initiated by a specified event. The SD-WAN Portal uses webhooks to send event notifications about the fabric. You can configure and manage webhooks through a tab in the **Administration Settings** area of the SD-WAN Portal.

Configure a webhook

Procedure

- Step 1** From the SD-WAN Portal menu, click **Administration** and select **Admin Settings**.
- Step 2** Select the **Webhooks** tab.
- Step 3** Click **Configure Webhook**.
- Step 4** Enter or select this information:
- Smart Account name
 - Virtual Account name
 - URL of webhook endpoint (must begin with https://)
 - Authorization type (choose Basic [username/password] or None).
- Step 5** Click **Add**.
The system displays a table of defined webhooks.
-

Send a webhook notification

Procedure

- Step 1** Right-click the webhook you want to edit in the table of defined webhooks, then choose **Send**.
- Step 2** Enter the plaintext notification for the webhook. Click **Send** to send the notification to the webhook server.
-



CHAPTER 14

Frequently Asked Questions

- [Frequently Asked Questions, on page 61](#)
- [How to, on page 62](#)
- [Troubleshooting, on page 62](#)

Frequently Asked Questions

What types of Cisco Catalyst SD-WAN deployments are supported on the Cisco Catalyst SD-WAN Portal?

You can deploy the following types of Cisco Catalyst SD-WAN on the Cisco Catalyst SD-WAN Portal:

- [Cisco SD-WAN Cloud](#)
- Cisco SD-WAN Cloud-Pro

See more details in [Types of Fabric Network in Cisco Catalyst SD-WAN](#).

What cloud providers are supported to provision SD-WAN control components in the Cisco Catalyst SD-WAN Portal?

The supported cloud providers for provisioning SD-WAN Control Components in the Cisco Catalyst SD-WAN Portal are Amazon Web Services (AWS) and Microsoft Azure.

What is the role of a Virtual Account in Cisco Catalyst SD-WAN Portal controller provisioning?

The Cisco Catalyst SD-WAN Portal uses SD-WAN subscriptions linked to a Virtual Account to determine which cloud SD-WAN Control Component entitlements are available and to facilitate SD-WAN Control Component provisioning. This information shows whether your Virtual Account supports SD-WAN. Provide a Virtual Account when you order an SD-WAN license to ensure successful provisioning through the Catalyst SD-WAN Portal.

How to

How do I access the Cisco Catalyst SD-WAN Portal?

Use the instructions in [Access the Cisco Catalyst SD-WAN Portal for the First Time](#) to access the Cisco Catalyst SD-WAN Portal.

If you want to use an identity provider (IdP) to access the portal, refer to [Configure an IdP for the Cisco Catalyst SD-WAN Portal](#).

How do I configure role-based access in the Cisco Catalyst SD-WAN Portal?

The role-based access control feature in the Cisco Catalyst SD-WAN Portal allows users to be assigned specific roles (Monitor, Overlay Management, or Administration) within designated virtual accounts. This process ensures granular visibility and streamlines provisioning and monitoring of new overlays. To configure role-based access, refer to the instructions provided in [Manage role-based access](#).

How do I set up multifactor authentication (MFA)?

The Cisco Catalyst SD-WAN Portal supports MFA by default, and it is mandatory for users. These one-time password generation options are available:

- Google Authenticator
- Email Authenticator
- Fingerprint sensor on supported computers (such as Apple MacBook)

For more information, refer to [Configure Additional MFA Options or Update an Existing MFA Option](#).

How do I move SD-WAN Control Component SKUs from one Virtual Account to another Virtual Account?

To reassign an order containing SD-WAN Control Component SKUs to a different Virtual Account, open a support case as described in [Troubleshooting, on page 62](#).

How do I add IP addresses to an allow list for managing fabric access through the Cisco Catalyst SD-WAN Portal?

To add IP addresses to an allow list through the Cisco Catalyst SD-WAN Portal, refer to the instructions in [Specify the Allowed List of IP Addresses for Managing Controller Access](#).

Troubleshooting

How do I get support for Cisco Catalyst SD-WAN Portal?

Follow these steps to open a Cisco support case for Catalyst SD-WAN Portal.

1. Go to <https://mycase.cloudapps.cisco.com/case>.
2. Select **Open New Case > Products & Services > Open Case**.

3. Enter the appropriate entitlement information. You typically need to include the serial number of a WAN edge device.
4. Click **Next**.
5. Enter your case details.
6. Select **Technology** and search for the appropriate Sub Tech keyword. For Cisco Catalyst SD-WAN Portal issues, select these keywords:
 - Technology: SDWAN - Cisco-Hosted
 - SubTechnology: SDWAN Cloud Infra



CHAPTER 15

Configuration Conversion Tool

- [Configuration Conversion Tool feature history, on page 65](#)
- [Information about the Configuration Conversion Tool, on page 65](#)
- [Restrictions for the Configuration Conversion Tool, on page 66](#)
- [Prerequisites for the Configuration Conversion Tool, on page 66](#)
- [Use the Configuration Conversion Tool, on page 66](#)

Configuration Conversion Tool feature history

Table 8: Feature History

Feature Name	Release Information	Description
Configuration Conversion Tool	April 2025	The Configuration Conversion Tool converts templates and policies to configuration groups, policy groups, and topology groups.

Information about the Configuration Conversion Tool

Use the Catalyst SD-WAN Configuration Conversion Tool to collect templates and policies from your SD-WAN Manager instance, convert them, and create new configuration groups, policy groups, and topology groups in a new SD-WAN Manager instance.

Conversion details

The Configuration Conversion Tool:

- converts device templates to configuration groups,
- converts policies into policy groups and topology groups where applicable, and
- transfers global device values and variable names.

Restrictions for the Configuration Conversion Tool

- The Configuration Conversion Tool is considered to be in beta.
- The Configuration Conversion Tool does not convert features that do not have a configuration group or policy group equivalent.

Prerequisites for the Configuration Conversion Tool

- Your site must be using Cisco Catalyst SD-WAN Manager Release 20.12.x or later.
- Your network firewall must accept incoming traffic from 74.207.103.254.

Use the Configuration Conversion Tool

Procedure

- Step 1** For the commercial version of the Cisco Catalyst SD-WAN Portal, navigate to <https://ssp.sdwan.cisco.com/>. For the government version, log in at <https://ssp-gov.sdwan.gov.fedramp.cisco>.
- Step 2** Launch the Configuration Conversion Tool. If you do not have full access to the Cisco Catalyst SD-WAN Portal, a message with a link for limited access appears. Click the displayed link to open the Configuration Conversion Tool.
- Step 3** Enter your SD-WAN Manager IP address or URL along with user credentials. Port and subdomain fields are optional.
- Step 4** Click **Collect** to retrieve all legacy constructs, including device templates, feature templates, policies, and associated constructs, from SD-WAN Manager.
- When the collection is complete, download the JSON file containing all configurations. Use this file to repeat the process later without collecting the data again from SD-WAN Manager.
- Step 5** Click **Templates** and select the device templates you want to convert to their new equivalents.
- The tool converts the device templates and associated feature templates.
- Step 6** If you need to convert policies, click **Policies** and select the option to enable policy conversion. This action converts all defined policies referenced by device templates.
- Step 7** Click **Convert** to convert the selected items.
- The **Converted Configurations** page displays all the newly converted constructs.
- Step 8** Confirm the list and click **Upload** to add the configurations to SD-WAN Manager.
- You can cancel an upload in progress.
- After the upload is complete, a summary of the configurations that were uploaded appears.
- If needed, you can click **Rollback** to remove all the constructs added to SD-WAN Manager during this session.
-

The new constructs are now ready to use.

What to do next

To migrate your devices to the newly converted configuration groups, complete the steps in the [Existing Deployments](#) section of the *Quick Start Guide - Catalyst SD-WAN Simplified Configuration and Policies*.



CHAPTER 16

Troubleshooting the Cisco Catalyst SD-WAN Portal

- [Update an expired IdP certificate, on page 69](#)
- [Reset a Misconfigured IdP, on page 69](#)
- [Troubleshoot Smart Account issues, on page 70](#)
- [Troubleshoot Virtual Account issues, on page 70](#)
- [Troubleshoot browser security issues, on page 71](#)

Update an expired IdP certificate

To update an expired identity provider (IdP) certificate, use the **Need help signing in** link in the Cisco Catalyst SD-WAN Portal **Sign In** window.

1. Navigate to the Cisco Catalyst SD-WAN Portal URL.
2. Click the **Need help signing in** link.
3. Click the **Need to reset IdP** link.
You are redirected to your Cisco account.
4. Enter your Cisco login credentials.
5. When prompted, set up or enter your MFA credentials.

Reset a Misconfigured IdP

If your identity provider (IdP) is misconfigured and you cannot log in, you can configure a new IdP.

1. Go to the Cisco Catalyst SD-WAN Portal URL.
2. Click **Need help signing in**.
3. Click **Need to reset IdP**.
You are redirected to your account.
4. Enter your login credentials.

5. When prompted, set up or enter your multifactor authentication (MFA) credentials.

Delete an IdP

1. Go to the Cisco Catalyst SD-WAN Portal URL.
2. Click **Need help signing in**.
3. Click the **Need to reset IdP**.
4. You are redirected to your account.
5. Enter your login credentials.
6. When prompted, set up or enter your MFA credentials.
7. Select **IdP details** > **Actions** and delete the IDP.



Note Only the IdP administrator is able to delete an IdP from Cisco Catalyst SD-WAN Portal. If you are not the IdP administrator or the administrator is no longer active, open a TAC case.

Troubleshoot Smart Account issues

Problem

A Smart Account is not visible in the **Smart Account** drop-down list after logging in to the Cisco Catalyst SD-WAN Portal. This can occur when there is no SD-WAN-capable attribute associated with the Smart Account.

Solution

Associate your DNA subscription with your Smart Account and Virtual Account.

For more information, see [Access the Cisco Catalyst SD-WAN Portal, on page 19](#).

Contact Technical Support to have your Smart Account associated with your DNA cloud subscription.

Troubleshoot Virtual Account issues

Problem

The Cisco Catalyst SD-WAN Portal displays an error that the Virtual Account is not SD-WAN capable.

This error indicates that a DNA subscription is not associated with the Virtual Account.

Solution

If you have an enterprise agreement, you cannot automatically associate Virtual Accounts to an SD-WAN-capable attribute.

As an enterprise customer, complete these steps to associate a Virtual Account with your DNA subscription:

1. Submit a cloud-controller provisioning request form through the Enterprise Agreement Workspace for the CloudOps team to provision the controllers.
2. Contact Cisco Catalyst SD-WAN Technical Support to request that the desired Virtual Account become available on the Cisco Catalyst SD-WAN Portal.
3. After the desired Virtual Account is available on the Cisco Catalyst SD-WAN Portal, provide the necessary enterprise agreement contract information to provision the controllers.

For more information, see .

For more information, see .

If you are unable to associate your Virtual Account with your DNA subscription, contact Technical Support to associate the Virtual Account with your DNA cloud subscription.

Troubleshoot browser security issues

Problem

You see this error:

```
CSRF Failed: CSRF token missing or incorrect
```

You see a cross-site request forgery (CSRF) token mismatch when the browser is unable to create a secure cookie or to access the cookie required for you to log in.

Solution

This error appears because of certain security settings in your web browser.

Clear the cache on your browser, or try another browser.



CHAPTER 17

Set Up and Configure Cisco Catalyst SD-WAN Manager

- [Configure the Network](#), on page 73
- [Configure Single Sign-On Using Okta](#), on page 81
- [Configure SSO for PingID](#), on page 85
- [Configure Hardened Passwords](#), on page 88
- [Configure User Login Options](#), on page 92
- [Configure Sessions in Cisco SD-WAN Manager](#), on page 99
- [Configure NTP Addresses](#), on page 101
- [Configure Domain Name System Security Extensions](#), on page 104
- [Verify that FIPS is Enabled](#), on page 105
- [Web Server Certificates](#), on page 106
- [Secure Connections from Devices to Cisco SD-WAN Manager](#), on page 109

Configure the Network

The topics in this section describe how to configure your network.

Bring-Up Sequence of Events

The bring-up process for edge devices—which includes authenticating and validating all the devices and establishing a functional overlay network—occurs with only minimal user input. From a conceptual point of view, the bring-up process can be divided into two parts, one that requires user input and one that happens automatically:

1. In the first part, you design the network, create virtual machine (VM) instances for cloud routers, and install and boot hardware routers. Then, in Cisco SD-WAN Manager, you add the routers to the network and create configurations for each router. This process is described in the Summary of the User Portion of the Bring-Up Sequence.
2. The second part of the bring-up process occurs automatically, orchestrated by the Cisco Catalyst SD-WAN software. As routers join the overlay network, they validate and authenticate themselves automatically, and they establish secure communication channels between each other. For Cisco SD-WAN Validators and Cisco SD-WAN Controllers, a network administrator must download the necessary authentication-related files from Cisco SD-WAN Manager, and then these Cisco SD-WAN Controllers

and Cisco SD-WAN Validators automatically receive their configurations from Cisco SD-WAN Manager. After Cisco hardware routers start, they are authenticated on the network and receive their configurations automatically from Cisco SD-WAN Manager through a process called zero-touch provisioning (ZTP). This process is described in the [Automatic Portions of the Bring-Up Sequence](#).

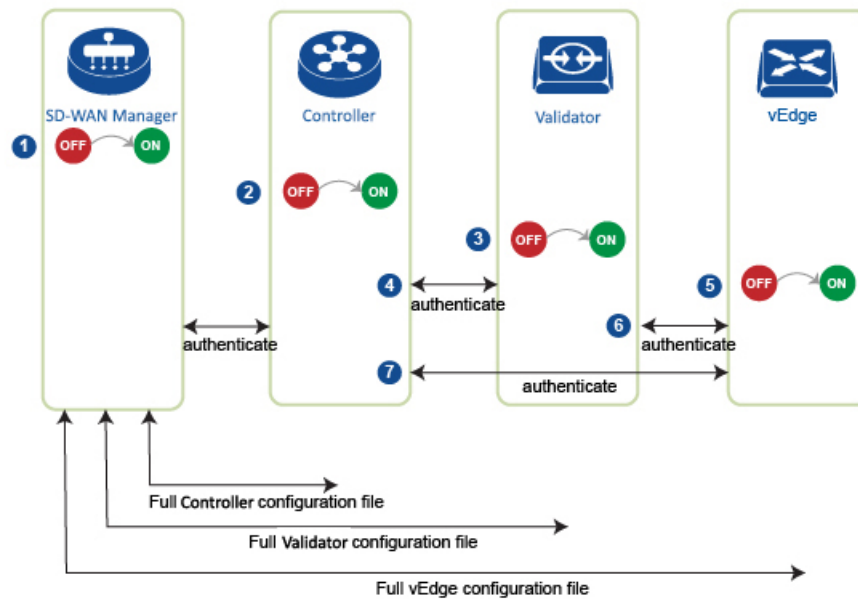
The end result of this two-part process is an operational overlay network.

This topic describes the sequence of events that occurs during the bring-up process, starting with the user portion and then explaining how automatic authentication and device validation occur.

Sequence of Events of the Bring-Up Process

From a functional point of view, the task of bringing up the routers in the overlay network occurs in the following sequence:

Figure 4: Bring-Up Sequence of Events



368439

1. The Cisco SD-WAN Manager software starts on a server in the data center.
2. The Cisco SD-WAN Validator starts on a server in the DMZ.
3. The Cisco SD-WAN Controller starts on a server in the data center.
4. Cisco SD-WAN Manager and the Cisco SD-WAN Validator authenticate each other, Cisco SD-WAN Manager and the Cisco SD-WAN Controller authenticate each other, and the Cisco SD-WAN Controller and the Cisco SD-WAN Validator securely authenticate each other.
5. Cisco SD-WAN Manager sends configurations to the Cisco SD-WAN Controller and the Cisco SD-WAN Validator.
6. The routers start in the network.
7. The routers authenticate themselves with the Cisco SD-WAN Validator.
8. The routers authenticate themselves with Cisco SD-WAN Manager.

9. The routers authenticate themselves with the Cisco SD-WAN Controller.
10. Cisco SD-WAN Manager sends configurations to the routers.

Before you start the bring-up process, note the following:

- To provide the highest level of security, only authenticated and authorized routers can access and participation in the Cisco Catalyst SD-WAN overlay network. To this end, the Cisco SD-WAN Controller performs automatic authentication on all the routers before they can send data traffic over the network.
- After the routers are authenticated, data traffic flows, regardless of whether the routers are in a private address space (behind a NAT gateway) or in a public address space.

To bring up the hardware and software components in a Cisco Catalyst SD-WAN overlay network, a transport network (also called a transport cloud), which connects all the routers and other network hardware components, must be available. Typically, these components are in data centers and branch offices. The only purpose of the transport network is to connect all the network devices in the domain. The Cisco Catalyst SD-WAN solution is agnostic with regards to the transport network, and, therefore, can be any type, including the internet, Multiprotocol Label Switching (MPLS), Layer 2 switching, Layer 3 routing, and Long-Term Evolution (LTE), or any mixture of transports.

For hardware routers, you can use the Cisco Catalyst SD-WAN zero-touch provisioning (ZTP) SaaS to bring up the routers. For more information on automatic process to bring-up hardware in the overlay network, see [Prepare Routers for ZTP](#).



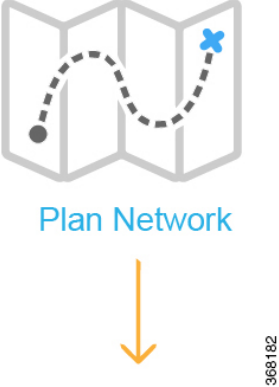
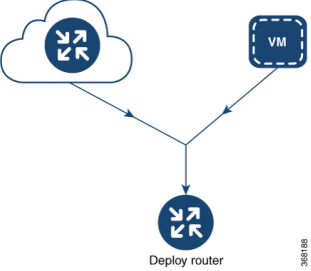
Note Starting from Cisco vManage Release 20.3.1, if you assign Cisco SD-WAN Manager VPN0 IP address in the 172.17.0.0/16 subnet, it cannot form control connections to edge devices (IOS XE SD-WAN and SD-routing).

Summary of the User Portion of the Bring-Up Sequence

In a general sense, what you do to bring up the Cisco Catalyst SD-WAN overlay network is what you would do to bring up any network—you plan out the network, create device configurations, and then deploy the network hardware and software components. These components include all the Cisco IOS XE Catalyst SD-WAN devices, all the traditional routers that participate in the overlay network, and all the network devices that provide shared services across the overlay network, such as firewalls, load balancers, and identity provider (IdP) systems.

The following table summarizes the steps for the user portion of the Cisco Catalyst SD-WAN overlay network bring-up sequence. The details of each step are provided in the links listed in the **Procedure** column. While you can bring up the Cisco IOS XE Catalyst SD-WAN devices in any order, we recommend that you deploy them in the order listed in the table, which is the functional order in which the devices verify and authenticate themselves.

Table 9: Workflow for the Bring-Up Sequence

Workflow	Procedure
<p data-bbox="349 346 365 367">1</p> 	<p data-bbox="706 346 1039 367">Plan out your overlay network.</p>
<p data-bbox="349 793 365 814">2</p> 	<p data-bbox="706 793 1429 840">Deploy the Cisco IOS XE Catalyst SD-WAN devices in the overlay network:</p> <ol data-bbox="706 871 1477 1218" style="list-style-type: none"> 1. For the cloud routers, create a VM instance, either on an AWS server, an ESXi, or a KVM hypervisor. 2. From Cisco SD-WAN Manager, send the serial numbers of all Cisco IOS XE Catalyst SD-WAN devices to the Cisco SD-WAN Controllers and Cisco SD-WAN Validators in the overlay network. 3. Create a full configuration for the Cisco IOS XE Catalyst SD-WAN devices by creating configuration templates on Cisco SD-WAN Manager. When Cisco SD-WAN Manager discovers a device in the overlay network, it pushes the appropriate configuration template to the device.

System and Interfaces Overview

Setting up the basic system-wide functionality of network devices is a simple and straightforward process. Basic parameters include defining host properties, such as name and IP address; setting time properties, including NTP; setting up user access to the devices; and defining system log (syslog) parameters.

In addition, the Cisco Catalyst SD-WAN software provides a number of management interfaces for accessing the Cisco Catalyst SD-WAN devices in the overlay network.

Host Properties

All devices have basic system-wide properties that specify information that the Cisco Catalyst SD-WAN software uses to construct a view of the network topology. Each device has a system IP address that provides a fixed location of the device in the overlay network. This address, which functions the same way as a router ID on a router, is independent of any of the interfaces and interface IP addresses on the device. The system IP address is one of the four components of the Transport Location (TLOC) property of each device.

A second host property that must be set on all devices is the IP address of the Cisco SD-WAN Validator for the network domain, or a Domain Name System (DNS) name that resolves to one or more IP addresses for

Cisco SD-WAN Validators. A Cisco SD-WAN Validator automatically orchestrates the process of bringing up the overlay network, admitting a new device into the overlay, and providing the introductions that allow the device and Cisco SD-WAN Controllers to locate each other.

Two other system-wide host properties are required on all devices, except for the Cisco SD-WAN Validators, to allow the Cisco Catalyst SD-WAN software to construct a view of the topology—the domain identifier and the site identifier.

To configure the host properties, see [Cisco Catalyst SD-WAN Overlay Network Bring-Up Process](#).

Time and NTP

The Cisco Catalyst SD-WAN software implements the Network Time Protocol (NTP) to synchronize and coordinate time distribution across the Cisco Catalyst SD-WAN overlay network. NTP uses a intersection algorithm to select the applicable time servers and avoid issues caused due to network latency. The servers can also redistribute reference time using local routing algorithms and time daemons. NTP is defined in [RFC 5905, Network Time Protocol Version 4: Protocol and Algorithms Specification](#).

User Authentication and Access with AAA, RADIUS, and TACACS+

The Cisco Catalyst SD-WAN software uses Authentication, Authorization, and Accounting (AAA) to provide security for the devices on a network. AAA, in combination with RADIUS and Terminal Access Controller Access-Control System (TACACS+) user authentication, controls which users are allowed access to devices, and what operations they are authorized to perform after they are logged in or connected to the devices.

Authentication refers to the process by which users trying to access the devices are authenticated. To access devices, users log in with a username and a password. The local device can authenticate users. Alternatively, authentication can be performed by a remote device, either a RADIUS server or a TACACS+ server, or both in a sequence.

Authorization determines whether a user is authorized to perform a given activity on a device. In the Cisco Catalyst SD-WAN software, authorization is implemented using role-based access. Access is based on groups that are configured on the devices. A user can be a member of one or more groups. User-defined groups are considered when performing authorization, that is, the Cisco Catalyst SD-WAN software uses group names received from RADIUS or TACACS+ servers to check the authorization level of a user. Each group is assigned privileges that authorize the group members to perform specific functions on the corresponding device. These privileges correspond to specific hierarchies of the configuration commands and the corresponding hierarchies of operational commands that members of the group are allowed to view or modify.

Beginning in Cisco IOS XE Catalyst SD-WAN Release 17.5.1a, accounting generates a record of commands that a user executes on a device. Accounting is performed by a TACACS+ server.

For more information, see [Role-Based Access with AAA](#).

Authentication for WANs and WLANs

For wired networks (WANs), Cisco Catalyst SD-WAN devices can run IEEE 802.1X software to prevent unauthorized network devices from gaining access to the WAN. IEEE 802.1X is a port-based network access control (PNAC) protocol that uses a client-server mechanism to provide authentication for devices wishing to connect to the network.

IEEE 802.1X authentication requires three components:

- Requester: Client device, such as a laptop, that requests access to the Wide-Area Network (WAN). In the Cisco Catalyst SD-WAN overlay network, a supplicant is any service-side device that is running 802.1X-compliant software. These devices send network access requests to the router.

- **Authenticator:** A network device that provides a barrier to the WAN. In the overlay network, you can configure an interface device to act as an 802.1X authenticator. The device supports both controlled and uncontrolled ports. For controlled ports, the Cisco Catalyst SD-WAN device acts as an 802.1X port access entity (PAE), allowing authorized network traffic and preventing unauthorized network traffic ingressing to and egressing from the controlled port. For uncontrolled ports, Cisco Catalyst SD-WAN, acting as an 802.1X PAE, transmits and receives Extensible Authentication Protocol over IEEE 802 (EAP over LAN, or EAPOL) frames.
- **Authentication server:** Host that is running authentication software that validates and authenticates requesters that want to connect to the WAN. In the overlay network, this host is an external RADIUS server. This RADIUS server authenticates each client connected to the 802.1X port interface Cisco Catalyst SD-WAN device and assigns the interface to a virtual LAN (VLAN) before the client is allowed to access any of the services offered by the router or by the LAN.

For wireless LANs (WLANs), routers can run IEEE 802.11i to prevent unauthorized network devices from gaining access to the WLANs. IEEE 802.11i implements Wi-Fi Protected Access (WPA) and Wi-Fi Protected Access II (WPA2) to provide authentication and encryption for devices that want to connect to a WLAN. WPA authenticates individual users on the WLAN using a username and a password. WPA uses the Temporal Key Integrity Protocol (TKIP), which is based on the RC4 cipher. WPA2 implements the NIST FIPS 140-2-compliant AES encryption algorithm along with IEEE 802.1X-based authentication, to enhance user access security over WPA. WPA2 uses the Counter Mode Cipher Block Chaining Message Authentication Code Protocol (CCMP), which is based on the AES cipher. Authentication is done by either using preshared keys or through RADIUS authentication.

Network Segmentation

The Layer 3 network segmentation in Cisco Catalyst SD-WAN is achieved through VRFs on Cisco IOS XE Catalyst SD-WAN devices. When you configure the network segmentation on a Cisco IOS XE Catalyst SD-WAN device using Cisco SD-WAN Manager, the system automatically maps the VPN configurations to VRF configurations.

Network Interfaces

In the Cisco Catalyst SD-WAN overlay network design, interfaces are associated with VPNs that translate to VRFs. The interfaces that participate in a VPN are configured and enabled in that VPN. Each interface can be present only in a single VPN.



Note Cisco IOS XE Catalyst SD-WAN devices use VRFs in place of VPNs. When you complete the configuration on Cisco SD-WAN Manager, the system automatically maps the VPN configurations to VRF configurations.

The overlay network has the following types of VPNs/VRFs:

- **VPN 0: Transport VPN**, that carries control traffic using the configured WAN transport interfaces. Initially, VPN 0 contains all the interfaces on a device except for the management interface, and all the interfaces are disabled. This is the global VRF on Cisco IOS XE Catalyst SD-WAN software.
- **VPN 512: Management VPN**, that carries out-of-band network management traffic among the Cisco Catalyst SD-WAN devices in the overlay network. The interface used for management traffic resides in VPN 512. By default, VPN 512 is configured and enabled on all Cisco Catalyst SD-WAN devices. For controller devices, by default, VPN 512 is not configured. On Cisco IOS XE Catalyst SD-WAN devices, the management VPN is converted to VRF Mgmt-Intf.

For each network interface, you can configure a number of interface-specific properties, such as DHCP clients and servers, VRRP, interface MTU and speed, and Point-to-Point Protocol over Ethernet (PPPoE). At a high level, for an interface to be operational, you must configure an IP address for the interface and mark it as operational (no shutdown). In practice, you always configure additional parameters for each interface.

Management and Monitoring Options

There are various ways in which you can manage and monitor a router. Management interfaces provide access to devices in the Cisco Catalyst SD-WAN overlay network, allowing you to collect information from the devices in an out-of-band fashion and to perform operations on the devices, such as configuring and rebooting them.

The following management interfaces are available:

- CLI
- IP Flow Information Export (IPFIX)
- RESTful API
- SNMP
- System logging (syslog) messages
- Cisco SD-WAN Manager

CLI

You can access a CLI on each device, and from the CLI, you configure overlay network features on the local device and gather operational status and information regarding that device. Using an available CLI, we strongly recommend that you configure and monitor all the Cisco Catalyst SD-WAN network devices from Cisco SD-WAN Manager, which provides views of network-wide operations and device status, including detailed operational and status data. In addition, Cisco SD-WAN Manager provides straightforward tools for bringing up and configuring overlay network devices, including bulk operations for setting up multiple devices simultaneously.

You can access the CLI by establishing an SSH session to a Cisco Catalyst SD-WAN device.

For a Cisco Catalyst SD-WAN device that is being managed by Cisco SD-WAN Manager, if you create or modify the configuration from the CLI, the changes are overwritten by the configuration that is stored in the Cisco SD-WAN Manager configuration database.

IPFIX

The IP Flow Information Export (IPFIX) protocol, also called cflowd, is a tool for monitoring the traffic flowing through Cisco Catalyst SD-WAN devices in the overlay network and exporting information about the traffic to a flow collector. The exported information is sent in template reports, that contain both information about the flow and the data extracted from the IP headers of the packets in the flow.

Cisco Catalyst SD-WAN cflowd performs 1:1 traffic sampling. Information about all the flows is aggregated in the cflowd records; flows are not sampled.



Note Cisco Catalyst SD-WAN devices do not cache any of the records that are exported to a collector.

The Cisco Catalyst SD-WAN cflowd software implements cflowd Version 10, as specified in RFC 7011 and RFC 7012.

For a list of elements exported by IPFIX, see [Traffic Flow Monitoring with Cflowd](#).

To enable the collection of traffic flow information, you must create data policies that identify the traffic of interest, and then direct that traffic to a cflowd collector. For more information, see [Traffic Flow Monitoring with Cflowd](#).

You can also enable cflowd visibility directly on Cisco Catalyst SD-WAN devices without configuring a data policy, so that you can perform traffic flow monitoring on the traffic coming to the device from all the VPNs in the LAN. You can then monitor the traffic from Cisco SD-WAN Manager or from the device's CLI.

RESTful API

The Cisco Catalyst SD-WAN software provides a RESTful API, which is a programmatic interface for controlling, configuring, and monitoring the Cisco Catalyst SD-WAN devices in an overlay network. You can access the RESTful API through Cisco SD-WAN Manager.

The Cisco Catalyst SD-WAN RESTful API calls expose the functionality of the Cisco Catalyst SD-WAN software and hardware to an application program. Such functionality includes the normal operations you perform to maintain the devices and the overlay network itself.

SNMP

The Simple Network Management Protocol (SNMP) allows you to manage all the Cisco Catalyst SD-WAN devices in the overlay network. The Cisco Catalyst SD-WAN software supports SNMP v2c.

You can configure basic SNMP properties—device name, location, contact, and community—that allow the device to be monitored by an SNMP Network Management System (NMS).

You can configure trap groups and SNMP servers to receive traps.

The object identifier (OID) for the internet port of the SNMP MIB is 1.3.6.1.

SNMP traps are asynchronous notifications that a Cisco Catalyst SD-WAN device sends to an SNMP management server. Traps notify the management server of events, whether normal or significant, that occur on the Cisco Catalyst SD-WAN device. By default, SNMP traps are not sent to an SNMP server. Note that for SNMPv3, the PDU type for notifications, is either SNMPv2c inform (InformRequest-PDU) or trap (Trapv2-PDU).

Syslog Messages

System logging operations use a mechanism that is similar to the UNIX **syslog** command to record system-wide, high-level operations that occur on the Cisco Catalyst SD-WAN devices in the overlay network. The log levels (priorities) of the messages are the same as those in standard UNIX commands, and you can configure the priority of the syslog messages that should be logged. Messages can be logged to files on the Cisco Catalyst SD-WAN device or to a remote host.

Cisco SD-WAN Manager

Cisco SD-WAN Manager is a centralized network management system that allows configuration and management of all the Cisco Catalyst SD-WAN devices in the overlay network, and provides a dashboard displaying the operations of the entire network and of individual devices in the network. Three or more Cisco SD-WAN Manager servers are consolidated into a Cisco SD-WAN Manager cluster to provide scalability

and management support for up to 6,000 Cisco Catalyst SD-WAN devices, to distribute Cisco SD-WAN Manager functions across multiple devices, and to provide redundancy of network management operations.

Configure Single Sign-On Using Okta

Okta provides a secure identity management service that lets you connect any person with any application on any device using single sign-on (SSO).



Note The procedure for configuring SSO using Okta is same for tenant environments and providers.



Note Beginning with Cisco vManage Release 20.3.1, Cisco SD-WAN Manager no longer supports MD5 or SHA-1. All x.509 certificates handled by Cisco SD-WAN Manager need to use at least SHA-256 or a higher encryption algorithm.

Perform the following procedures to configure SSO.

Enable an Identity Provider in Cisco SD-WAN Manager

To configure Okta SSO, use Cisco SD-WAN Manager to enable an identity provider and generate a Security Assertion Markup Language (SAML) metadata file.

From Cisco vManage Release 20.10.1, you can use **Add New IDP Settings** to configure up to three IdPs. For more information on integrating with multiple IdPs, see the chapter [Configure Multiple IdPs](#).

1. From the Cisco SD-WAN Manager menu, choose **Administration > Settings**.
2. Click **Identity Provider Settings** and then click **Edit**.
3. Click **Enabled**.
4. Click **Click here to download the SAML metadata** and save the contents in a text file. This data is used for configuring Okta.
5. From the metadata that is displayed, make a note of the following information that you need for configuring Okta with Cisco SD-WAN Manager:
 - **Entity ID**
 - **Signing certificate**
 - **Encryption certificate**
 - **Logout URL**
 - **Login URL**



Note Administrators can set up SSO using a single **Entity ID** only. Cisco SD-WAN Manager doesn't support more than one **Entity ID** while setting up SSO.

6. In the **Upload Identity Provider Metadata** section, click **Select a File** to upload the IdP metadata file.
7. Click **Save**.

Configure SSO on the Okta Website



Note This procedure involves a third-party website. The details are subject to change.

To configure SSO on the Okta website:

1. Log in to the Okta website.



Note Each IdP application gets a customized URL from Okta for logging in to the Okta website.

2. Create a username using your email address.
3. To add Cisco SD-WAN Manager as an SSO application, from the Cisco SD-WAN Manager menu, click **Admin**.
4. Check the upper-left corner to ensure that it shows the **Classic UI** view on Okta.
5. If it shows **Developer Console**, click the down triangle to choose the **Classic UI**.
6. Click **Add Application** under **Shortcuts** to the right to go to the next window, and then click **Create New Application** on the pop-up window.
7. Choose **Web** for the platform, and choose **SAML 2.0** as the **Sign on Method**.
8. Click **Create**.
9. Enter a string as **Application name**.
10. (Optional): Upload a logo, and then click **Next**.
11. On the **SAML Settings for Single sign on URL** section, set the value to the **samlLoginResponse URL** from the downloaded metadata from Cisco SD-WAN Manager.
12. Check the **Use this for Recipient URL and Destination URL** check box.
13. Copy the **entityID** string and paste it in the **Audience URI (SP Entity ID)** field.
The value can be an IP address or the name of the Cisco SD-WAN Manager site.
14. For **Default RelayState**, leave empty.
15. For **Name ID format**, choose **EmailAddress**.

16. For **Application username**, choose **Okta username**.
17. For **Show Advanced Settings**, enter the fields as indicated below.

Table 10: Fields for Show Advanced Settings

Component	Value	Configuration
Response	Signed	Not applicable
Assertion Signature	Signed	Not applicable
Signature Algorithm	RSA-SHA256	Not applicable
Digest Algorithm	SHA256	Not applicable
Assertion Encryption	Encrypted	Not applicable
Encryption Algorithm	AES256-CBC	Not applicable
Key Transport Algorithm	RSA-OAEP	Not applicable
Encryption Certificate	Not applicable	<p>a. Copy the encryption certificate from the metadata you downloaded.</p> <p>b. Go to www.samltool.com and click X.509 CERTS, paste there. Click Format X.509 Certificate.</p> <p>c. Ensure to remove the last empty line and then save the output (X.509.cert with header) into a text file encryption.cer.</p> <p>d. Upload the file. Mozilla Firefox may not allow you to do the upload. Instead, you can use Google Chrome. You should see the certificate information after uploading to Okta.</p>
Enable Single Logout		Ensure that this is checked.
Single Logout URL		Get from the metadata.
Service provider Issuer		Use the entityID from the metadata.
Signature Certificate		<p>a. Obtain from the metadata. Format the signature certificate using www.samltool.com as described.</p> <p>b. Save to a file, for example, signing.cer and upload.</p>
Authentication context class	X.509 Certificate	Not applicable

Component	Value	Configuration
Honor Force Authentication	Yes	Not applicable
SAML issuer ID string	SAML issuer ID string	Not applicable
Attribute Statements	Field: Name	Value: <i>Username</i>
	Field: Name format (optional)	Value: Unspecified
	Field: Value	Value: <i>user.login</i>
Group Attribute Statements	Field: Name	Value: Groups
	Field: Name format (optional)	Value: Unspecified
	Field: Matches regex	Value: .* Note Matches regex with value * matches all user groups in Okta which may cause SSO slowness and that value "netadmin operator basic" is preferred to limit the number of unrelated user groups. You can add the custom groups to the regex with an OR operator. For example, netadmin operator basic <custom>.



Note It is mandatory to use the two strings, Username and Groups, exactly as shown above. Otherwise, you may be logged in with the default group of Basic.

18. Click **Next**.
19. For **Application Type**, check **This is an internal app that we have created** (optional).
20. Click **Finish**. This brings you to the Okta application window.
21. Click **View Setup Instructions**.
22. Copy the IdP metadata.
23. In Cisco SD-WAN Manager, navigate to **Identity Provider Settings > Upload Identity Provider Metadata**, paste the IdP metadata, and click **Save**.
24. In addition to copy-and-pasting the contents of a file with IdP metadata, you can also upload a file directly using the **Select a file** option.

Assign Users to the Application on the Okta Website



Note This procedure involves a third-party website. The details are subject to change.

To assign users to the application on the Okta website:

1. On the Okta application window, navigate to **Assignments > People > Assign**.
2. Choose **Assign to people** from the drop-down menu.
3. Click **Assign** next to the user(s) you chose and click **Done**.
4. To add a user, click **Directory > Add Person**.
5. Click **Save**.

Configure SSO for PingID

Cisco SD-WAN Manager supports PingID as an IdP. PingID is an identity management service for authenticating user identities with applications for SSO.

The configuration of Cisco SD-WAN Manager to use PingID as an IdP involves the following steps:

- Import (upload) IdP metadata from PingID to Cisco SD-WAN Manager.
- Download the Cisco SD-WAN Manager SAML metadata file to export to PingID.

Prerequisites:

1. In Cisco SD-WAN Manager, ensure that identity provider settings (**Administration Settings > Identity Provider Settings**) are set to **Enabled**.
2. Download the Cisco SD-WAN Manager SAML metadata file to export to PingID.
For more information on these procedures, see [Enable an Identity Provider in Cisco SD-WAN Manager](#). The steps are the same as for configuring Okta as an IdP.

Perform the following steps for configuring PingID.

Configure SSO on the PingID Administration Portal



Note This procedure involves a third-party website. The details are subject to change.

To configure PingID:

1. Log in to the [PingID administration portal](#).
2. Create a username using your email address.
3. Click the **Applications**.

4. Click **Add Application** and choose **New SAML Application**.

In the **Application Details** section, **Application Name**, **Application Description**, and **Category** are all required fields.

For logos and icons, PNG is the only accepted graphics format.

5. Click **Continue to Next Step**.

The **Application Configuration** section appears.

6. Make sure that you choose **I have the SAML configuration**.

7. Under the **You will need to download this SAML metadata to configure the application** section, configure the following fields:

- a. For **Signing Certificate**, use the drop-down menu, **PingOne Account Origination Certificate**.
- b. Click **Download** next to **SAML Metadata** to save the PingOne IdP metadata into a file.
- c. Later, you need to import the PingOne IdP metadata file into Cisco SD-WAN Manager to complete the SSO configuration.
 1. From the Cisco SD-WAN Manager menu, choose **Administration > Settings**.
 2. Click **Identity Provider Settings > Upload Identity Provider Metadata** to import the saved PingOne IdP metadata file into Cisco SD-WAN Manager.
 3. Click **Save**.

8. Under the **Provide SAML details about the application you are connecting to** section, configure the following fields:

- a. For **Protocol Version**, click **SAMLv2.0**.
- b. On **Upload Metadata**, click **Select File** to upload the saved Cisco SD-WAN Manager SAML metadata file to PingID.

PingID should be able to decode the metadata file and fill in the other fields.

- c. Verify that the following fields and values are entered correctly.

Field	Value
Assertion Consumer Service (ACS)	<Cisco SD-WAN Manager_URL>/samlLoginResponse
Entity ID	IP address of Cisco SD-WAN Manager
Single Logout Endpoint	<Cisco SD-WAN Manager_URL>/samlLogoutResponse
Single Logout Binding Type	Redirect
Primary Verification Certificate	Name of the certificate

Field	Value
Encrypt Assertion	(Optional) If you do not encrypt the assertion, you might be prone to assertion replay attacks and other vulnerabilities.
Encryption Certification	Name of the certificate
Encryption Algorithm	(Optional) AES_256
Transport Algorithm	RSA_OAEP
Signing Algorithm	RSA_SHA256
Force Re-authentication	False

9. Click **Continue to Next Step**.
10. In the **SSO Attribute Mapping** section, configure the following fields:
 - a. Click **Add new attribute** to add the following attributes:
 1. Add **Application Attribute** as **Username**.
 2. Set **Identity Bridge Attribute or Literal Value Value** to **Email**.
 3. Check the **Required** box.
 4. Add another **Application Attribute** as **Groups**.
 5. Check the **Required** check box, and then click on **Advanced**.
 6. In the **IDP Attribute Name or Literal Value** section, click **memberOf**, and in **Function**, click **GetLocalPartFromEmail**.
 - b. Click **Save**.
11. Click **Continue to Next Step** to configure the **Group Access**.
12. Click **Continue to Next Step**.
13. Before clicking **Finish**, ensure that the settings are all correct.

Configure Hardened Passwords

Table 11: Feature History

Feature Name	Release Information	Description
Hardened Passwords	Cisco IOS XE Catalyst SD-WAN Release 17.3.1a Cisco vManage Release 20.3.1	This feature enables password policy rules in Cisco SD-WAN Manager. After password policy rules are enabled, Cisco SD-WAN Manager enforces the use of strong passwords.
	Cisco IOS XE Catalyst SD-WAN Release 17.9.1a Cisco vManage Release 20.9.1	This feature lets you configure Cisco SD-WAN Manager to enforce predefined-medium security or high-security password criteria.

Enforce Strong Passwords

We recommend the use of strong passwords. You must enable password policy rules in Cisco SD-WAN Manager to enforce use of strong passwords.

After you enable a password policy rule, the passwords that are created for new users must meet the requirements that the rule defines. In addition, for releases from Cisco vManage Release 20.9.1, you are prompted to change your password the next time you log in if your existing password does not meet the requirements that the rule defines.

1. From the Cisco SD-WAN Manager menu, choose **Administration > Settings**.
2. Click **Password Policy**.
3. Perform one of these actions, based on your Cisco SD-WAN Manager release:
 - For releases before Cisco vManage Release 20.9.1, click **Enabled**.
 - For releases from Cisco vManage Release 20.9.1 click **Medium Security** or **High Security** to choose the password criteria.

By default, **Password Policy** is set to **Disabled**.

4. Click **Save**.

Password Requirements

Cisco SD-WAN Manager enforces the following password requirements after you have enabled the password policy rules:

- The following password requirements apply to releases before Cisco vManage Release 20.9.1:
 - Must contain a minimum of eight characters, and a maximum of 32 characters.

- Must contain at least one uppercase character.
 - Must contain at least one lowercase character.
 - Must contain at least one numeric character.
 - Must contain at least one of the following special characters: # ? ! @ \$ % ^ & * - .
 - Must not contain the full name or username of the user.
 - Must not reuse a previously used password.
 - Must contain different characters in at least four positions in the password.
- Minimum releases: Cisco IOS XE Catalyst SD-WAN Release 17.9.1a, Cisco vManage Release 20.9.1:

Password Criteria	Requirements
Medium Security	<ul style="list-style-type: none"> • Must contain a minimum of 8 characters • Must contain no more than 32 characters • Must contain at least 1 lowercase character • Must contain at least 1 uppercase character • Must contain at least 1 numeric character • Must contain at least 1 of the following special characters: # ? ! @ \$ % ^ & * - . • Must not be identical to any of the last 5 passwords used • Must not contain the full name or username of the user
High Security	<ul style="list-style-type: none"> • Must contain a minimum of 15 characters • Must contain no more than 32 characters • Must contain at least 1 lowercase character • Must contain at least 1 uppercase character • Must contain at least 1 numeric character • Must contain at least 1 of the following special characters: # ? ! @ \$ % ^ & * - . • Must not be identical to any of the last 5 passwords used • Must not contain the full name or username of the user • Must have at least eight characters that are not in the same position they were in the old password

Password Attempts Allowed

You are allowed five consecutive password attempts before your account is locked. After six failed password attempts, you are locked out for 15 minutes. If you enter an incorrect password on the seventh attempt, you are not allowed to log in, and the 15-minute lock timer starts again.

If your account is locked, wait for 15 minutes for the account to automatically be unlocked. Alternatively, reach out to an administrator to reset the password, or have an administrator unlock your account.



Note Your account gets locked even if no password is entered multiple times. When you do not enter anything in the password field, it is considered as invalid or wrong password.

Password Change Policy



Note You must have enabled password policy rules first for strong passwords to take effect. For more information, see [Enforce Strong Passwords, on page 88](#).

When resetting your password, you must set a new password. You cannot reset a password using an old password.



Note In Cisco vManage Release 20.6.4, Cisco vManage Release 20.9.1 and later releases, a user that is logged out, or a user whose password has been changed locally or on the remote TACACS server cannot log in using their old password. The user can log in only using their new password.

Reset a Locked User

If a user is locked out after multiple password attempts or unsuccessful login attempts, an administrator with the required rights can update passwords for this user.

There are two ways to unlock a user account, by changing the password or by getting the user account unlocked.



Note Only a **netadmin** user or a user with the User Management Write role can perform this operation.

To reset the password of a user who has been locked out:

1. In **Users (Administration > Manage Users)**, choose the user in the list whose account you want to unlock.
2. Click **...** and choose **Reset Locked User**.
3. Click **OK** to confirm that you want to reset the password of the locked user. Note that this operation cannot be undone.

Alternatively, you can click **Cancel** to cancel the operation.

Manage Users

From the Cisco SD-WAN Manager menu, choose **Administration** > **Manage Users** to add, edit, view, or delete users and user groups.

Please note the following:

- Only a user logged in as the **admin** user or a user who has Manage Users write permission can add, edit, or delete users and user groups from Cisco SD-WAN Manager.
- Each user group can have read or write permission for the features listed in this section. Write permission includes Read permission.
- All user groups, regardless of the read or write permissions selected, can view the information displayed in the Cisco SD-WAN Manager Dashboard.

Table 12: User Group Permissions for Different Device Types

Permissions	See This Section
User group permissions related to Cisco IOS XE Catalyst SD-WAN device configuration.	User Group Permissions: Cisco IOS XE Catalyst SD-WAN Devices
User group permissions related to Cisco Catalyst Wireless Gateway device configuration.	User Group Permissions: Cisco Catalyst Wireless Gateway Devices

Configure Users Using CLI

You can use the CLI to configure user credentials on each device. This way, you can create additional users and give them access to specific devices. The credentials that you create for a user by using the CLI can be different from the Cisco SD-WAN Manager credentials for the user. In addition, you can create different credentials for a user on each device. All Cisco IOS XE Catalyst SD-WAN device users with the **netadmin** privilege can create a new user.

To create a user account, configure the username and password, and place the user in a group:

This example, shows the addition of user, Bob, to an existing group:

```
Device(config)# system aaa user bob group basic
```

This example, shows the addition of user, Alice, to a new group `test-group`:

```
Device(config)# system aaa user test-group
Device(config)# system aaa user alice group test-group
```

The Username can be 1 to 128 characters long, and it must start with a letter. The name can contain only lowercase letters, the digits 0 through 9, hyphens (-), underscores (_), and periods (.). The name cannot contain any uppercase letters. Because some usernames are reserved, you cannot configure them. For a list of reserved usernames, see the **aaa** configuration command in the Cisco Catalyst SD-WAN Command Reference Guide.

The Password is the password for a user. Each username must have a password, and users are allowed to change their own password. The CLI immediately encrypts the string and does not display a readable version of the password. When a user logs in to a Cisco IOS XE Catalyst SD-WAN device, they have five chances to enter the correct password. After the fifth incorrect attempt, the user is locked out of the device, and must wait for 15 minutes before attempting to log in again.



Note Enclose any user passwords that contain the special character ! in double quotation marks (“”). If a double quotation is not included for the entire password, the config database (?) treats the special character as a space and ignores the rest of the password.

For example, if the password is C!sc0, use “C!sc0”.

Group name is the name of a standard Cisco Catalyst SD-WAN group (**basic**, **netadmin**, or **operator**) or of a group configured with the **usergroup** command (discussed below). If an admin user changes the permission of a user by changing their group, and if that user is currently logged in to the device, the user is logged out and must log back in again.

The factory-default password for the admin username is admin. We strongly recommend that you modify this password the first time you configure a Cisco IOS XE Catalyst SD-WAN device:

```
Device(config)# username admin password
$9$3/IL3/UF2F2F3E$J9NKBek1Wrq9ExmHk6F5VAiDMOFQfD.QPAmMxDdxz.c
```

Configure the password as an ASCII string. The CLI immediately encrypts the string and does not display a readable version of the password, for example:

```
Device# show run | sec username
username admin privilege 15 secret 9
$9$3F2M212G2/UM3U$TGe2kqoIibdIRDEj4cOVKbVFP/o4vn1FAwWnmzx1rRE
username appnav privilege 15 secret 9
$9$312L2V.F2VIM1k$P3MBAyBtGxKf/yBGnUSHQ1g/aelQhfIbieg28buJJGI
username eft secret 9 $9$3FMJ3/UD2VEL2E$d.ke4.an41v7wEhrQc6k5wIfE9M9WkNAJxUvbbempS.
username lab privilege 15 secret 9
$9$31.J3FUD2F.E2.$/AiVn9PmLCpgr6ExVrE7dH979Wu8nbdAfbzUtfysg.
username test secret 9 $9$112J316D3/QL3k$7PZOXJAJOIlos5UI763G3XcpVhXlqcwJ.qEmgmX4X9g
username vbonagir privilege 15 secret 9
$9$3/2K2UwF21QF3U$VbdQ5bq18590rRthF/NnNnOsw.dw1/EViMTFZ5.ctus
Device#
```

If you are using RADIUS to perform AAA authentication, you can configure a specific RADIUS server to verify the password:

```
Device(config)# radius server tag
```

The tag is a string that you defined with the **radius server tag** command, as described in the Cisco Catalyst SD-WAN Command Reference Guide.

Configure User Login Options

Table 13: Feature History

Feature Name	Release Information	Description
Inactivity Lockout	Cisco Catalyst SD-WAN Manager Release 20.12.1 Cisco SD-WAN Manager Release 20.9.3 and Releases 20.12.1 and later	This feature lets you configure Cisco SD-WAN Manager to lock out users who have not logged in for a designated number of consecutive days.

Feature Name	Release Information	Description
Unsuccessful Login Attempts Lockout	Cisco Catalyst SD-WAN Manager Release 20.12.1 Cisco SD-WAN Manager Release 20.9.3 and Releases 20.12.1 and later	This feature lets you configure Cisco SD-WAN Manager to lock out users who have made a designated number of consecutive unsuccessful login attempts within a designated period.
Duo Multifactor Authentication Support	Cisco Catalyst SD-WAN Manager Release 20.12.1 Cisco SD-WAN Manager Release 20.9.3 and Releases 20.12.1 and later	This feature lets you configure Cisco SD-WAN Manager to require Duo multifactor authentication (MFA) to verify the identity of users before they can log in to Cisco SD-WAN Manager.

Beginning with Cisco Catalyst SD-WAN Manager Release 20.12.1, a netadmin user can enable the following Cisco SD-WAN Manager user login features:

Beginning with Cisco IOS XE Catalyst SD-WAN Release 17.12.1a, you can access Cisco SD-WAN Manager with basic privileges even if TACACS user is not mapped to a group. Prior to Cisco IOS XE Catalyst SD-WAN Release 17.12.1a, the access to Cisco SD-WAN Manager was denied.

With Cisco SD-WAN Manager Release 20.9.3 and Releases 20.12.1 and later, a netadmin user can enable the following Cisco SD-WAN Manager user login features:

- **Inactivity lockout:** You can configure Cisco SD-WAN Manager to lock out users who have not logged in for a designated number of consecutive days. Locked out users cannot log in to Cisco SD-WAN Manager until an administrator unlocks their accounts.

See [Configure Account Lockout](#), on page 94.

- **Unsuccessful login lockout:** You can configure Cisco SD-WAN Manager to prevent users who make a designated number of consecutive unsuccessful login attempts within a designated time period from logging in to Cisco SD-WAN Manager until a configured amount of time passes or an administrator unlocks their user accounts.

By default, Cisco SD-WAN Manager locks out users for 15 minutes after five consecutive unsuccessful login attempts within 15 minutes. After a lockout period expires, a user can log in with the correct user name and password.

See [Configure Unsuccessful Login Attempts Lockout](#), on page 95.

- **Duo multifactor authentication:** You can configure Cisco SD-WAN Manager to require the use of Duo multifactor authentication to verify identity before users can log in. Users must confirm a login attempt by using Duo multifactor authentication on their mobile devices.

See [Configure Duo Multifactor Authentication](#), on page 97.

Configure Account Lockout

Before You Begin

Beginning with Cisco Catalyst SD-WAN Manager Release 20.12.1, you can configure Cisco SD-WAN Manager to lock out users who have not logged in for a designated number of consecutive days.

With Cisco vManage Release 20.9.3 and Cisco Catalyst SD-WAN Manager Release 20.12.1 and later, you can configure Cisco SD-WAN Manager to lock out users who have not logged in for a designated number of consecutive days.

Cisco SD-WAN Manager marks locked out users as inactive, and they cannot log in again until an administrator unlocks their accounts in Cisco SD-WAN Manager.



Note To unlock a user account, see [Reset a Locked User](#).

Configure Account Lockout

1. From the Cisco SD-WAN Manager menu, choose **Administration > Settings**.
2. Click **Account Lockout** and enable the **Inactive days before locked out** option.
(In Cisco Catalyst SD-WAN Manager Release 20.12.x, locate the **Account Lockout**, click **Edit**, and enable **Inactive days before locked out**.)
3. Configure the following options:

Field	Description
Inactive days before account locked out	<p>Enable this option and enter the number of consecutive inactive days after which Cisco SD-WAN Manager locks out a user.</p> <p>An inactive day is defined as a day on which a user does not log in to Cisco SD-WAN Manager.</p> <p>Valid values are 2 through 90.</p>
Number of failed login attempts before lockout	<p>Enter the number of failed login attempts after which Cisco SD-WAN Manager locks out a user.</p> <p>Possible values: 1 through 3600</p> <p>Default: 3600</p>

Field	Description
Duration within which the failed attempts are counted (minutes)	<p>Enter the period, in minutes, during which the system counts consecutive unsuccessful login attempts.</p> <p>For example, if you set this period to 10 minutes, and set the number of failed login attempts before lockout to 5, Cisco SD-WAN Manager locks out a user if the user makes 5 consecutive unsuccessful login attempts within 10 minutes.</p> <p>Possible values: 1 through 60</p> <p>Default: 60</p>
Cooldown or Lockout period	<p>This option controls whether Cisco SD-WAN Manager automatically resets a user who is locked because of unsuccessful login attempts.</p> <p>This option is enabled by default. If you disable it, an administrator must manually unlock the account of a locked-out user.</p> <p>a. Click Enabled adjacent to Cooldown or Lockout period.</p> <p>b. In the Lockout Interval (minutes) field, enter the number of minutes after which Cisco SD-WAN Manager automatically resets a locked out user.</p> <p>Possible values: 1 through 60</p> <p>Default: 15</p>

4. Click **Save**.

Configure Unsuccessful Login Attempts Lockout

Before You Begin

Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.12.1



Note From Cisco Catalyst SD-WAN Manager Release 20.13.1 or later, use the procedure described in [Configure Account Lockout](#), on page 94.

You can configure Cisco SD-WAN Manager to lock out users who have made a designated number of consecutive unsuccessful login attempts within a period of time.

With Cisco SD-WAN Manager Release 20.9.3 and Releases 20.12.1 and later, you can configure Cisco SD-WAN Manager to lock out users who have made a designated number of consecutive unsuccessful login attempts within a period of time.

Cisco SD-WAN Manager prevents locked out users from logging in again until a configured amount of time has passed or an administrator unlocks their accounts in Cisco SD-WAN Manager.



Note To unlock a user account, see [Reset a Locked User](#).

Configure Unsuccessful Login Attempts Lockout

1. From the Cisco SD-WAN Manager menu, choose **Administration > Settings**.
2. Click **Account Lockout**
3. In the **Lockout on failed login attempts** row, click **Edit**.
4. Configure the following options:

Field	Description
Number of failed login attempts before lockout	Enter the number of failed login attempts after which Cisco SD-WAN Manager locks out a user. Possible values: 1 through 3600 Default: 3600
Duration within which the failed attempts are counted (minutes)	Enter the period, in minutes, during which the system counts consecutive unsuccessful login attempts. For example, if you set this period to 10 minutes, and set the number of failed login attempts before lockout to 5, Cisco SD-WAN Manager locks out a user if the user makes 5 consecutive unsuccessful login attempts within 10 minutes. Possible values: 1 through 60 Default: 60

Field	Description
Cooldown or Lockout period	<p>This option controls whether Cisco SD-WAN Manager automatically resets a user who is locked because of unsuccessful login attempts.</p> <p>This option is enabled by default. If you disable it, an administrator must manually unlock the account of a locked-out user.</p> <p>a. Click Enabled adjacent to Cooldown or Lockout period.</p> <p>b. In the Lockout Interval (minutes) field, enter the number of minutes after which Cisco SD-WAN Manager automatically resets a locked out user.</p> <p>Possible values: 1 through 60</p> <p>Default: 15</p>

5. Click **Save**.

Configure Duo Multifactor Authentication

Beginning with Cisco Catalyst SD-WAN Manager Release 20.12.1, you can configure Cisco SD-WAN Manager to require Duo multifactor authentication (MFA) to verify the identity of users before they can log in to Cisco SD-WAN Manager and other controllers. When you configure this feature, users are prompted on their mobile devices to authenticate with Duo after they enter a username and password and click **Log In** on the Cisco SD-WAN Manager **Login** screen.

With Cisco vManage Release 20.9.3 and Releases 20.12.1 and later, you can configure Cisco SD-WAN Manager to require Duo multifactor authentication (MFA) to verify the identity of users before they can log in to Cisco SD-WAN Manager and other controllers. When you configure this feature, users are prompted on their mobile devices to authenticate with Duo after they enter a username and password and click **Log In** on the Cisco SD-WAN Manager **Login** screen.

This feature requires that you have a Duo account with local users created on that account.



Note

- Duo MFA does not apply to the admin user by default. To enable Duo MFA for the admin user, enable the **DUO MFA Configuration** option, and then enter the [admin-auth-order](#) command from the CLI.
- Users do not see a message in Cisco SD-WAN Manager that an MFA request has been sent to a mobile device.

1. Log into the Duo Admin Panel.
2. Create an Auth API application.

This provides the Duo integration key, secret key, and API hostname information required to complete Duo MFA configuration. Read more about [Duo Auth API](#).

3. From the Cisco SD-WAN Manager menu, choose **Administration > Settings**.
4. Click **DUO MFA Configuration**. (If you are using Cisco Catalyst SD-WAN Manager Release 20.12.x or earlier, click **Edit**.)
5. Click **Enabled**.
6. Configure the following options:

Field	Description
Integration Key	Enter the integration key (Ikey) for your Duo account.
Secret Key	Enter the secret key (Skey) for your Duo account.
API Hostname	Enter the API hostname (api-hostname) for your Duo account.
Server proxy	<p>(Read only) Shows the server proxy that is used to access the Duo server if Cisco SD-WAN Manager is behind a firewall. Set this server proxy with the system http proxy or the system https proxy command.</p> <p>Note If Cisco SD-WAN Manager is deployed on a cloud that can be reached by an external network, a server proxy should not be set.</p>

7. Click **Save**.
8. If a Cisco SD-WAN Validator or a Cisco SD-WAN Controller does not have internet access, use the following commands in the CLI or the device template of the device to provide access to the Duo MFA feature.

These commands configure the device with proxy information about the device on which Duo MFA is enabled.

```
vm# config
vm(config)# system aaa
vm(config-aaa)# multi-factor-auth
vm(config-multi-factor-auth)# duo
vm(config-duo)# api-hostname name
vm(config-duo)# secret-key key
vm(config-duo)# integration-key key
vm(config-duo)# proxy proxy_url
vm(config-duo)# commit
```

Configure Sessions in Cisco SD-WAN Manager

Table 14: Feature History

Feature History	Release Information	Description
Configure Sessions in Cisco SD-WAN Manager	Cisco IOS XE Catalyst SD-WAN Release 17.3.1a Cisco vManage Release 20.3.1	This feature lets you see all the HTTP sessions that are open within Cisco SD-WAN Manager. It gives you details about the username, source IP address, domain of the user, and other information. A user with User Management Write access, or a netadmin user can trigger a log out of any suspicious user's session.

Set a Client Session Timeout in Cisco SD-WAN Manager

You can set a client session timeout in Cisco SD-WAN Manager. When a timeout is set, such as no keyboard or keystroke activity, the client is automatically logged out of the system.



Note You can edit Client Session Timeout in a multitenant environment only if you have a Provider access.

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings**.
2. Click **User Sessions**.
3. Under **Client Session Timeout**, click **Session Timeout**.
4. Specify the timeout value, in minutes.
5. Click **Save**.

Set a Session Lifetime in Cisco SD-WAN Manager

You can specify how long to keep your session active by setting the session lifetime, in minutes. A session lifetime indicates the amount of time for which a session can be active. If you keep a session active without letting the session expire, you will be logged out of the session in 24 hours, which is the default session timeout value.

The default session lifetime is 1440 minutes or 24 hours.



Note You can edit Session Lifetime in a multitenant environment only if you have a Provider access.

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Settings**.

2. Click **User Sessions**.
3. In the **SessionLifeTime Timeout (minutes) field**, specify the session timeout value, in minutes, from the drop-down list.
4. Click **Save**.

Set the Server Session Timeout in Cisco SD-WAN Manager

You can configure the server session timeout in Cisco SD-WAN Manager. The server session timeout indicates how long the server should keep a session running before it expires due to inactivity. The default server session timeout is 30 minutes.



Note Server Session Timeout is not available in a multitenant environment even if you have a Provider access or a Tenant access.

1. From the Cisco SD-WAN Manager menu, choose **Administration > Settings**.
2. Click **User Sessions**.
3. In **Server Session Timeout Timeout(minutes) field**, specify the timeout value, in minutes.
4. Click **Save**.

Set the maximum sessions per user role

You can configure the maximum number of concurrent login sessions for each configured user role. This maximum value applies to all users assigned to that role.

For example, if the “Max user sessions” value for the netadmin role is set to 3, then each user assigned to the netadmin role can have up to 3 concurrent login sessions across the platform. If a fourth session is initiated by one of those users, an error message appears.

Range for “Max user sessions”: 1 to 255. Default: If undefined, there is no limit on the number of concurrent sessions for that role. For government installations, recommended values are 3 sessions for administrative roles and 2 sessions for conventional roles.

The value also applies to CLI sessions.

Change maximum sessions value for a user role

1. From the Cisco SD-WAN Manager menu, choose **Administration > Users and Access > Roles**.
The “Max user sessions value” is displayed for each defined role, including both default and custom roles.
2. Click the role name, edit the **Max user sessions** value, and click **Update**.



Note As of Release 20.18.1, the previous method for changing this value in **Settings > Trust and Privacy** is no longer supported. If a “Max user sessions” value has been defined on your system by that method, that value serves as the maximum value for all user roles until changed.

Configure NTP Addresses

The topics in this section describe how to configure Network Time Protocol (NTP) addresses.

NTP on Cisco Catalyst SD-WAN for Government Overlay Networks

When the Cisco Catalyst SD-WAN Portal creates a Cisco Catalyst SD-WAN overlay network, it automatically configures the NTP server for the overlay network. The server that is configured is a National Institute of Standards and Technology-authenticated (NIST-authenticated) NTP server. When you view logs, the timestamp of a log corresponds to these NTP servers.

The Cisco Catalyst SD-WAN Portal determines the NTP server based on the location that you select for your overlay network as follows:

- **US Gov West (California)**: Colorado NTP server
- **US Gov East (Maryland)**: Maryland NTP server

All management virtual private clouds (VPCs) are hosted in **US Government Cloud West**. Therefore, the NTP server configured for these VPCs is the Colorado NTP server.

Optionally, you can configure the NTP server as described in the following section.

Configure NTP Servers Using Cisco SD-WAN Manager

Configure NTP servers on your devices in order to synchronize time across all the devices in the Cisco overlay network. You can configure up to four NTP servers, and they must all be located or reachable in the same VPN.

Other devices are allowed to ask a Cisco Catalyst SD-WAN device for the time, but no devices are allowed to use a Cisco Catalyst SD-WAN device as an NTP server.



Note For the NTP to properly function when using Global VRF on the Cisco IOS XE Catalyst SD-WAN devices, you must configure **allow-service ntp** for the tunnel interface on the Cisco VPN Interface Ethernet template.

To configure an NTP server using Cisco SD-WAN Manager templates:

1. Create an NTP feature template to configure NTP parameters, as described in this section.
2. Configure the timezone in the System template.

Name the Template

1. From the Cisco SD-WAN Manager menu, choose **Configuration > Templates**.
2. Click **Device Templates**.



Note In Cisco vManage Release 20.7.x and earlier releases, **Device Templates** is titled **Device**.

3. From the **Create Template** drop-down list, choose **From Feature Template**.
4. From the **Device Model** drop-down list, choose the type of device for which you wish to create the template.
5. Click **Basic Information**.
6. From **Additional Cisco System Templates**, click **NTP**.
7. From the **NTP** drop-down list, choose **Create Template**.

The **Cisco NTP** template form is displayed. This form contains fields for naming the template, and fields for defining NTP parameters.

8. In **Template Name**, enter a name for the template.
The name can be up to 128 characters and can contain only alphanumeric characters.
9. In **Template Description**, enter a description of the template. The description can be up to 2048 characters and can contain only alphanumeric characters.

When you first open a feature template, for each parameter that has a default value, the scope is set to Default (indicated by a check mark), and the default setting or value is shown. To change the default value or to enter a value, click the scope drop-down list to the left of the parameter field and select one of the following:

Table 15: Setting Parameter Scope

Parameter Scope	Scope Description
Device Specific (indicated by a host icon)	<p>Use a device-specific value for the parameter. For device-specific parameters, you cannot enter a value in the feature template. You enter the value when you attach a device to a device template.</p> <p>When you click Device Specific, the Enter Key box opens. This box displays a key, which is a unique string that identifies the parameter in a CSV file that you create. This file is an Excel spreadsheet that contains one column for each key. The header row contains the key names (one key per column), and each row after that corresponds to a device and defines the values of the keys for that device. You upload the CSV file when you attach a device to a device template. For more information, see Create a Template Variables Spreadsheet.</p> <p>To change the default key, type a new string and move the cursor out of the Enter Key box.</p> <p>Examples of device-specific parameters are system IP address, hostname, GPS location, and site ID.</p>

Parameter Scope	Scope Description
Global (indicated by a globe icon)	Enter a value for the parameter, and apply that value to all devices. Examples of parameters that you might apply globally to a group of devices are DNS server, syslog server, and interface MTUs.

Configure an NTP Server

To configure an NTP server, click **Server**, and click **Add New Server**, and configure the following parameters. Parameters marked with an asterisk are required to configure an NTP server.

Table 16: Parameters for Configuring an NTP Server

Parameter Name	Description
Hostname/IP Address*	Enter the IP address of an NTP server, or a DNS server that knows how to reach the NTP server.
Authentication Key ID*	Specify the MD5 authentication key associated with the NTP server, to enable authentication. For the key to work, you must mark it as trusted in the Trusted Keys field, under Authentication . Note From Cisco Catalyst SD-WAN Control Components Release 20.14.1, you can use CMAC-AES authentication when configuring NTP servers for Cisco SD-WAN Control Components. This requires configuration using a CLI template.
VPN ID*	Enter the number of the VPN that should be used to reach the NTP server, or the VPN in which the NTP server is located. If you have configured multiple NTP servers, they must all be located or be reachable in the same VPN. Range: Range: 1 to 65525, excluding 512. For details see the VRF range behavior change described here .
Version*	Enter the version number of the NTP protocol software. The range is from 1 through 4. The default is 4.
Source Interface	Enter the name of a specific interface to use for outgoing NTP packets. The interface must be located in the same VPN as the NTP server. If it is not, the configuration is ignored.
Prefer	Click On if multiple NTP servers are at the same stratum level and you want one to be preferred. For servers at different stratum levels, the software chooses the one at the highest stratum level.

To add an NTP server, click **Add**.

To add another NTP server, click **Add New Server**. You can configure up to four NTP servers. The Cisco Catalyst SD-WAN software uses the server at the highest stratum level.

To edit an NTP server, click the pencil icon to the right of the entry.

To delete an NTP server, click the trash icon to the right of the entry.

To save the feature template, click **Save**.

Configure NTP Authentication Keys

To configure the authentication keys used to authenticate NTP servers, click **Authentication**, and then the **Authentication Key**. Then click **New Authentication Key**, and configure the following parameters. Parameters marked with an asterisk are required to configure the authentication keys.

Table 17: Parameters for Configuring NTP Authentication Keys

Parameter Name	Description
Authentication Key ID*	Enter the following values: <ul style="list-style-type: none"> • Authentication Key: Enter an authentication key ID. Valid range is from 1 to 65535. • Authentication Value: Enter either a cleartext key or an AES-encrypted key.
Authentication Value*	Enter an authentication key. For this key to be used, you must designate it as trusted. To associate a key with a server, enter the same value that you entered in the Authentication Key ID field under Server .

To configure the trusted keys used to authenticate NTP servers, under **Authentication**, click **Trusted Key**, and configure the following parameters.

Table 18: Parameters for Configuring Trusted Keys

Parameter Name	Description
Trusted Keys*	Enter the authentication key to designate the key as trustworthy. To associate this key with a server, enter the same value that you entered for the Authentication Key ID field under Server .

Configure Domain Name System Security Extensions

The topics in this section describe how to configure Domain Name System Security Extensions (DNSSEC).

Overview of Domain Name System Security Extensions

Cisco SD-WAN Manager performs DNSSEC validation using Unbound, an open-source project developed by NLnet Labs. Unbound is a secure Domain Name System (DNS) resolver that is easy to use and configure.

DNSSEC adds a layer of security to DNS, which is used to translate domain names to internet addresses.

Unbound is integrated into Cisco SD-WAN Manager as a daemonized local DNS server.

Unbound performs the following tasks:

- Forwards DNS queries from local applications to DNS servers.
- Validates replies from DNS servers and answers queries from applications.

- Caches the DNS server resolution results.

To validate DNSSEC responses, a DNSSEC server (a local Unbound server running on Cisco SD-WAN Manager) needs to be configured with certain keys to trust.

DNS entries are signed by a DNS server with a private key, and the public key is returned by that server as a DNSKEY Resource Record (RR). The DNSKEY RR is hashed, and the parent zone's DNS server stores the hash and publishes it as a Delegation Signer-RR.

By default, the Unbound Domain Name System can be configured to automatically download and trust the root Delegation Signer and DNSKEY RR, as well as keep the root Delegation Signer and DNSKEY RR up to date using the auto-trust-anchor-file configuration option.



Note Configure DNSSEC validation using the Cisco Catalyst SD-WAN RESTful APIs.

Use Case for Domain Name System Security Extensions

Many government agencies have their own Identity Provider (IdP) or single sign-on (SSO) mechanism to authenticate users trying to log in to Cisco SD-WAN Manager. For example, let us consider a social security instance, `sso.ssa.gov`. The domain name needs to be resolved by a configured private DNS server, which is also DNSSEC-aware. This prevents a potential DDoS attack of Cisco SD-WAN Manager by spoofing for name server requests. If the private DNS server is compromised, then the response signature does not match, and hence the forwarding does not occur.

Configure Domain Name System Security Extensions Using the CLI

To enable DNSSEC validation, use the **request dnssec start** CLI command. To disable DNSSEC validation, use the **request dnssec stop** CLI command.

You can also restart or check the status of the DNSSEC server using the **restart** or the **status** commands as shown below.

```
vmanage# request dnssec ?
Description: Enable or disable DNSSEC server
Possible completions:
  restart  restart the unbound server
  start    start the unbound server
  status   show unbound server status information
  stop     stop the unbound server
```



Note You may have to disable DNSSEC for cloud environments, such as Amazon Web Services (AWS), where AWS is already DNSSEC-aware.

Verify that FIPS is Enabled

Run the following command on the vshell of Cisco SD-WAN Manager to verify that Federal Information Processing Standards (FIPS) is enabled:

```
openssl version -a
```

You can also run the following command from the Cisco SD-WAN Manager CLI to also show if FIPS is enabled or not:

```
show system status
```

Web Server Certificates

Cisco does not issue web certificates for Cisco SD-WAN Manager. We recommend that you generate the Certificate Signing Request (CSR) and get it signed by your Certificate Authority (CA) for your Domain Name System (DNS) name. Then, you may either add an A entry in your DNS server for the IP, or a CNAME to the `.viptela.net` / `.sdwan.cisco.com` Cisco SD-WAN Manager DNS name for commercial deployments or `.sdwangov.fedramp.cisco` for government deployments.



Note The controller certificates issued by Cisco are for the controllers to use internally. You cannot use these certificates to issue web server certificates.

For more information, see the [Web Server Certificates](#) section in the Cisco Catalyst SD-WAN Getting Started Guide.

View Web Server Certificate Expiration Date

When you establish a secure connection between your web browser and the Cisco SD-WAN Manager server using authentication certificates, you configure the time period for which the certification is valid (in Step 8 in the previous section). At the end of this time period, the certificate expires. The **Web Server Certificate** bar in the window shows the expiration date and time.

Starting 60 days before the certificate expires, the Cisco SD-WAN Manager Dashboard displays a notification indicating that the certificate is about to expire. This notification is then redisplayed 30, 15, and 7 days before the expiration date, and then daily.

Renew Cisco Catalyst SD-WAN SSL Certificates for Controllers

Signed certificates are used to authenticate devices in the overlay network. After being authenticated, devices can establish secure sessions between each other.



Note The certificate renewal process is applicable only if you have a Cisco SD-WAN Cloud-Pro single tenant or multi-tenant controller overlay. This process is not applicable if you have a shared tenant overlay.

You can generate the Certificate Signing Request (CSR) as well as install the signed certificates, using Cisco SD-WAN Manager. There are 3 options for Certificate Root CA:

1. Cisco Root CA bundle (already present on controllers with software version 19.2.3 and above, Cisco Catalyst SD-WAN devices with software version 19.2.3 and above, Cisco IOS XE Catalyst SD-WAN devices with software versions 16.12.3+ or 16.10.4+ or 17.x+.

2. Symantec/Digicert Root CA (already present on all controllers, Cisco Catalyst SD-WAN devices and Cisco IOS XE Catalyst SD-WAN devices).
3. Your own Enterprise Root CA.



Note Select the certificate-generation method only once. The method you select is automatically applied each time you add a device to the overlay network.

To renew the controller certificates, you need to follow the appropriate process based on your deployment type and certificate type:

- The controller certification authorization settings configure the certification- generation process for all controller devices. For more information, see [Cisco Catalyst SD-WAN Controller Certificates](#).
- Note that since the certificate renewal involves an entire control plane flap, you are required to follow the instructions as per above, to renew the certificates, even for Cisco SD-WAN Cloud-Pro controllers.
- The Cisco CloudOps team does not automatically renew the certificates for the customers.
- On the Cisco SD-WAN Manager **Settings** page, there is an option for **Symantec Automated** or **Cisco Automated** where automated refers to automatic submission of CSRs and retrieval of certificates. The option does include automation of certain steps of the process, compared to the manual option. However, the step to trigger the generation of CSRs for each controller is still manual, to be done by you, to initiate the renewal process.
- Note that the Cisco SD-WAN Manager Dashboard shows a warning 6 months in advance that the certificates are about to expire.
- You can view the expiry date at any time at by choosing **Configuration > Certificates > Controllers** from the Cisco SD-WAN Manager menu.



Note Starting from Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, the **Controllers** tab is renamed as the **Control Components** tab to stay consistent with Cisco Catalyst SD-WAN rebranding.

- The Cisco CloudOps team sends email notifications 30/15/5 day prior to expiry, to the registered email address contact for the overlay in your system as well.
- You can open a case with us anytime to request the current registered email address or change it. We recommend that customers help keep the owner email address updated for all Cisco CloudOps notifications. We recommend keeping us updated with the customer contact email address for alert notifications, preferably a team mailer address instead of an individual user email address.
- Also, we recommend being aware of the controller certificate expiry dates and plan for renewal at least 1 month before expiry.

Configure a Symantec Process Certificate

Use the following steps to configure a Symantec signing server to automatically generate, sign, and install certificates on each controller device:

1. From the Cisco SD-WAN Manager menu, choose **Administration > Settings**.
2. Click **Edit** to the right of the **Controller Certificate Authorization** bar.
3. Click **Symantec Automated**. This is the recommended method for handling controller-signed certificates.
4. Enter the first and last name of the certificate requestor.
5. Enter the email address of the certificate requestor. This address is required because the signed certificate and a confirmation email are sent to the requestor using email. The signed certificate and the confirmation email are also available on the customer portal.
6. Specify the validity period for the certificate. It can be one, two, or three years.
7. Enter a challenge phrase. The challenge phrase is your certificate password and is required when you renew or revoke your certificate.



Note A challenge phrase is used to encode a certificate. If you lose the certificate, you can retrieve that specific certificate from Symantec's DigiCert portal using the challenge phrase. You can renew the certificates using the Symantec Automated or Manual method.

For the automated method, enter the name, email address, and the challenge phrase in Cisco SD-WAN Manager **Administration > Settings**. When the CSR is generated, this information is used to include in the Symantec portal and then to receive and install the approved certificates from Symantec, automatically.

For the manual method, enter the name, email address, and the challenge phrase in Symantec's DigiCert portal.

8. Confirm your challenge phrase.
9. In the Certificate Retrieve Interval field, specify how often the Cisco SD-WAN Manager server checks if the Symantec signing server has sent the certificate.
10. Click **Save**.

Install Enterprise Root Certificates

You can install enterprise root certificates on the Cisco SD-WAN Validator, Cisco SD-WAN Manager, and Cisco SD-WAN Controllers.

By default, the enterprise root certificate has the following properties:

- Country: United States
- State: California
- City: San Jose
- Organizational Unit: ENB
- Organization: CISCO

- Domain Name: cisco.com
- Email: cisco-cloudops-sdwan@cisco.com

To view this information, use the **show certificate signing-request decoded** command on a controller device, and check the output in the Subject line, for example:

```
vSmart# show certificate signing-request decoded
.
.
.
Subject: C=US, ST=California, L=San Jose, OU=vIPtela Inc Regression, O=vIPtela Inc,
CN=vsmart-uuid.viptela.com/emailAddress=support@viptela.com
.
.
.
```

To install an enterprise root certificate:

1. From the Cisco SD-WAN Manager menu, choose **Administration > Settings**.
2. Click **Edit** to the right of the **Controller Certificate Authorization** bar.
3. Click **Enterprise Root Certificate**.
4. In the **Certificate** field, either paste the enterprise root certificate, or click **Select a file** and upload the file that contains the certificate.
5. To change one or more of the default CSR properties:
 - a. Click **Set CSR Properties**.
 - b. Enter the domain name to include in the CSR. This domain name is appended to the certificate number (CN).
 - c. Enter the organizational unit (OU) to be included in the CSR.
 - d. Enter the organization (O) to be included in the CSR.
 - e. Enter the city (L), state (ST), and two-letter country code (C) to be included in the CSR.
 - f. Enter the email address (emailAddress) of the certificate requestor.
 - g. Specify the validity period for the certificate. It can be one, two, or three years.
6. Click **Import & Save**.

**Note**

Cisco does not issue web certificates for Cisco SD-WAN Manager as of today. We recommend that you generate a CSR and get it signed by your own CA for your Domain Name System (DNS) name. You should either add an A entry in your DNS server for the IP, or a CNAME to the Cisco SD-WAN Manager DNS name.

Secure Connections from Devices to Cisco SD-WAN Manager

The topics in this section describe how to secure the connections from devices to Cisco SD-WAN Manager.

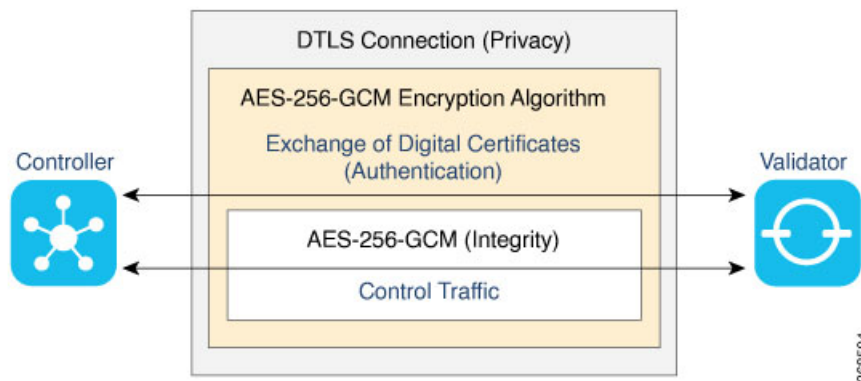
Control Plane Security Overview

The control plane of any network determines the network topology and defines how to direct packets. In a traditional network, the control plane operations of building and maintaining routing and forwarding tables and directing packets towards their destination are handled by routing and switching protocols, which typically offer few or no mechanisms for authenticating devices or for encrypting routing updates and other control information. In addition, the traditional methods of providing security are manual and do not scale. For example, certificates are typically installed manually rather than in an automated fashion, and using preshared keys is not a secure approach for providing device security.

The Cisco Catalyst SD-WAN control plane has been designed with network and device security in mind. The foundation of the control plane is one of two security protocols derived from Secure Sockets Layer (SSL)—the Datagram Transport Layer Security (DTLS) protocol and the Transport Layer Security (TLS) protocol. The Cisco SD-WAN Controller, which is the centralized brain of the Cisco Catalyst SD-WAN solution, establishes and maintains DTLS or TLS connections to all Cisco Catalyst SD-WAN devices in the overlay network—to the routers, the Cisco SD-WAN Validator, to Cisco SD-WAN Manager, and to other Cisco SD-WAN Controllers. These connections carry control plane traffic. DTLS or TLS provides communication privacy between Cisco Catalyst SD-WAN devices in the network, using the Advanced Encryption Standard (AES-256) encryption algorithm to encrypt all the control traffic sent over the connections. For information about how Cisco SD-WAN Manager communicates with devices and controllers, see [Cisco Catalyst SD-WAN Manager](#) in the *Cisco Catalyst SD-WAN Getting Started Guide*.

The privacy and encryption in the control plane, which is offered by DTLS and TLS, provide a safe and secure foundation for the other two security components, that is, authentication and integrity. To perform authentication, the Cisco Catalyst SD-WAN devices exchange digital certificates. These certificates, which are either installed by the software or hard-coded into the hardware, depending on the device, identify the device and allow the devices themselves to automatically determine which ones belong in the network and which are imposters. For integrity, the DTLS or TLS connections run AES-256-GCM, an authenticated encryption with associated data (AEAD) that provides encryption and integrity, which ensures that all the control and data traffic sent over the connections has not been tampered with.

Figure 5: Cisco Catalyst SD-WAN Control Plane Overview



The following are the control plane security components, which function in the privacy provided by DTLS or TLS connections:

- AES-256-GCM: This algorithm provides encryption services.
- Digital certificates: These are used for authentication.
- AES-256-GCM: This is responsible for ensuring integrity.

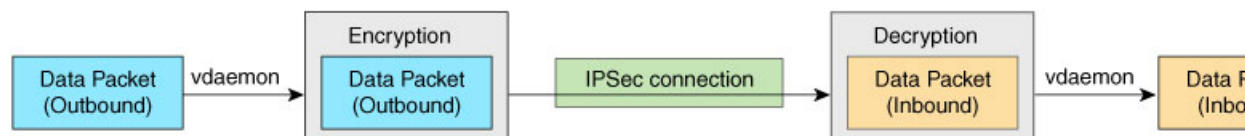
Data Plane Security Overview

The data plane of any network is responsible for handling data packets that are transported across the network. The data plane is also sometimes called the forwarding plane. In a traditional network, data packets are typically sent directly over the Internet or another type of public IP cloud, or they could be sent through MPLS tunnels. If the routers in the Cisco Catalyst SD-WAN overlay network were to send traffic over a public IP cloud, the transmission would be insecure. Anyone can sniff the traffic, and implement various types of attacks, including man-in-the-middle (MITM) attacks.

The underlying foundation for security in the Cisco Catalyst SD-WAN data plane is the security of the control plane. Because the control plane is secure—all the devices are validated, and control traffic is encrypted and cannot be tampered with—you can be confident about using routes and other information learned from the control plane, to create and maintain secure data paths throughout a network of routers.

The data plane provides the infrastructure for sending data traffic among the routers in the Cisco Catalyst SD-WAN overlay network. Data plane traffic travels within secure Internet Security (IPsec) connections. The Cisco Catalyst SD-WAN data plane implements the key security components of authentication, encryption, and integrity, as shown in the figure, and described below.

Figure 6: Cisco Catalyst SD-WAN Data Plane Overview



- **Authentication:** As mentioned, the Cisco Catalyst SD-WAN control plane contributes the underlying infrastructure for data plane security. In addition, authentication is enforced by two other mechanisms:
 - In the traditional key exchange model, the Cisco Catalyst SD-WAN Controller sends IPsec encryption keys to each edge device.
 - In the pairwise keys model, the Cisco SD-WAN Controller sends Diffie-Hellman public values to the edge devices, and they generate pairwise IPsec encryption keys using Elliptic-curve Diffie-Hellman (ECDH) and a P-384 curve. For more information, see [Pairwise Keys, on page 116](#).
 - By default, IPsec tunnel connections use an enhanced version of the Encapsulating Security Payload (ESP) protocol for authentication on IPsec tunnels.
- **Encryption:** An enhanced version of ESP protects a data packet's payload. This version of the protocol also checks the outer IP and UDP headers. Hence, this option supports an integrity check of the packet, which is similar to the Authentication Header (AH) protocol. Data encryption is done using the AES-GCM-256 cipher.
- **Integrity:** To guarantee that data traffic is transmitted across the network without being tampered with, the data plane implements several mechanisms from the IPsec security protocol suite:
 - An enhanced version of the ESP protocol encapsulates the payload of data packets.
 - The enhanced version of ESP uses an AH-like mechanism to check the integrity of the outer IP and UDP headers. You can configure the integrity methods supported on each router, and this information is exchanged in the router's TLOC properties. If two peers advertise different authentication types, they negotiate the type to use, choosing the strongest method.
 - The anti-replay scheme protects against attacks in which an attacker duplicates encrypted packets.

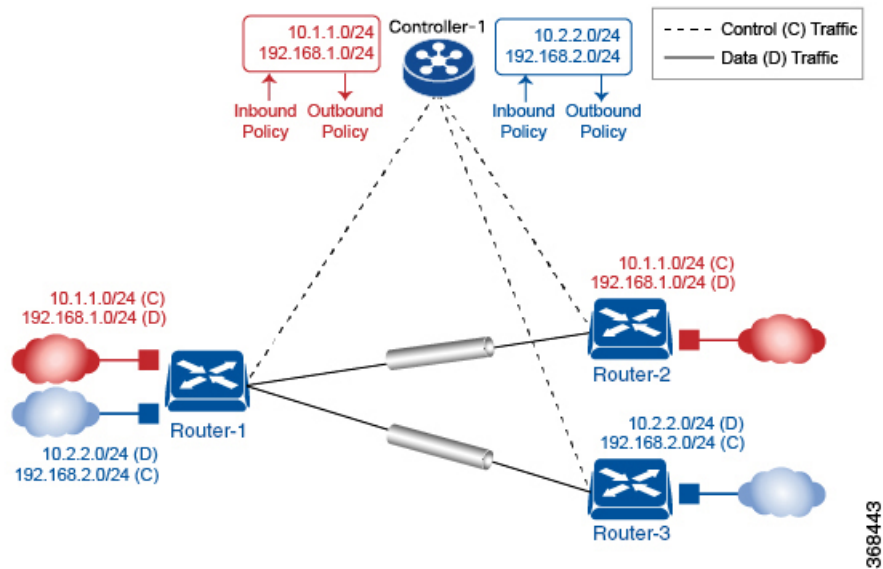
Segmentation in Cisco Catalyst SD-WAN

In the Cisco Catalyst SD-WAN overlay network, VRFs divide the network into different segments.

Cisco Catalyst SD-WAN employs the more prevalent and scalable model of creating segments. Essentially, segmentation is done at the edges of a router, and the segmentation information is carried in the packets in the form of an identifier.

The figure shows the propagation of routing information inside a VRF.

Figure 7: Propagation of Routing Information Inside a VRF



In this figure:

- Router-1 subscribes to two VRFs, red and blue.
 - The red VRF caters to the prefix 10.1.1.0/24 (either directly through a connected interface or learned using the IGP or BGP).
 - The blue VRF caters to the prefix 10.2.2.0/24 (either directly through a connected interface or learned using the IGP or BGP).
- Router-2 subscribes to the red VRF.
 - This VRF caters to the prefix 192.168.1.0/24 (either directly through a connected interface or learned using the IGP or BGP).
- Router-3 subscribes to the blue VRF.
 - This VRF caters to the prefix 192.168.2.0/24 (either directly through a connected interface or learned using the IGP or BGP).

Because each router has an Overlay Management Protocol (OMP) connection over a TLS tunnel to a Cisco SD-WAN Controller, it propagates its routing information to the Cisco SD-WAN Controller. On the Cisco SD-WAN Controller, the network administrator can enforce policies to drop routes, to change TLOCs, which

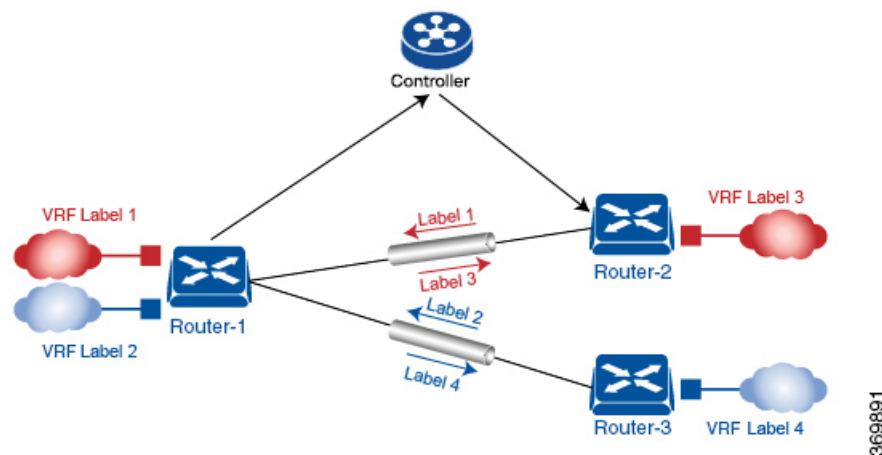
are overlay next hops, for traffic engineering or service chaining. A network administrator can apply these policies as inbound and outbound policies on the Cisco SD-WAN Controller.

All the prefixes belonging to a single VRF are kept in a separate route table. This provides the Layer 3 isolation required for the various segments in the network. So, Router-1 has two VRF route tables, and Router-2 and Router-3 each have one route table. In addition, the Cisco SD-WAN Controller maintains the VRF context of each prefix.

Separate route tables provide isolation on a single node. So how is routing information propagated across the network?

In the Cisco Catalyst SD-WAN solution, this is done using VRF identifiers, as shown in the figure below. A VRF ID, which is carried in a packet, identifies each VRF on a link. When you configure a VRF on a router, the VRF has a label associated with it. The router sends the label, along with the VRF ID, to the Cisco SD-WAN Controller. The Cisco SD-WAN Controller propagates this router-to-VRF ID mapping information to the other routers in the domain. The remote routers then use this label to send traffic to the appropriate VRF. The local routers, on receiving the data with the VRF ID label, use the label to demultiplex the data traffic. This is similar to how MPLS labels are used. This design is based on standard RFCs and is compliant with regulatory procedures such as PCI and HIPAA.

Figure 8: VRF Identifiers



Note The transport network that connects the routers is completely unaware of the VRFs. Only the routers know about VRFs; the rest of the network follows standard IP routing.

VRFs Used in Cisco Catalyst SD-WAN Segmentation

The Cisco Catalyst SD-WAN solution involves the use of VRFs to separate traffic.

Global VRF

The global VRF is used for transport. To enforce the inherent separation between services (such as prefixes that belong to the enterprise) and transport (the network that connects the routers), all the transport interfaces, that is, all the TLOCs, are kept in the global VRF. This ensures that the transport network cannot reach the service network by default. Multiple transport interfaces can belong to the same VRF, and packets can be forwarded to and from transport interfaces.

A global VRF contains all the interfaces for a device, except the management interface, and all the interfaces are disabled. For the control plane to establish itself so that the overlay network can function, you must configure tunnel interfaces in a global VRF. For each interface in a global VRF, you must set an IP address, and create a tunnel connection that sets the color and encapsulation for the WAN transport connection. (The encapsulation is used for the transmission of data traffic.) These three parameters—IP address, color, and encapsulation—define a TLOC (transport location) on the router. The OMP session running on each tunnel sends the TLOC to the Cisco SD-WAN Controllers so that they can learn the overlay network topology.

Dual-Stack Support on Transport VPNs

In the global VRF, Cisco IOS XE Catalyst SD-WAN devices and Cisco SD-WAN Controller support dual stack. To enable dual stack, configure an IPv4 address and an IPv6 address on the tunnel interface. The router learns from a Cisco SD-WAN Controller whether a destination supports IPv4 or IPv6 addresses. When forwarding traffic, a router chooses either the IPv4 or the IPv6 TLOC, based on the destination address. But IPv4 is always preferred when configured.

Management VRF

Mgmt-Intf is the management VRF on Cisco IOS XE Catalyst SD-WAN devices. It is configured and enabled by default. It carries out-of-band network management traffic among the devices in the overlay network. You can modify this configuration, if required.

Configure VRF Using Cisco SD-WAN Manager Templates

In Cisco SD-WAN Manager, use a CLI template to configure VRFs for a device. For each VRF, configure a subinterface and link the subinterface to the VRF. You can configure up to 300 VRFs.

Starting from Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, you can configure up to 2,000 VRFs in the overlay network and up to 500 VRFs for a single device. Each VRF deals with fewer routes than before, making the distribution of routes across the network more efficient and easier to scale.

When you push a CLI template to a device, Cisco SD-WAN Manager overwrites existing configuration on the device and loads the configuration defined in the CLI template. Consequently, the template cannot only provide the new content being configured, such as VRFs. The CLI template must include all the configuration details required by the device. To display the relevant configuration details on a device, use the **show sdwan running-config** command.

For details about creating and applying CLI templates, and for an example of configuring VRFs, see the CLI Templates for Cisco IOS XE Catalyst SD-WAN Routers chapter of the [Systems and Interfaces Configuration Guide, Cisco IOS XE Release 17.x](#).

The following are the supported devices:

- Cisco ASR1001-HX
- ASR1002-HX
- C8500-12X
- C8500-12X4QC
- C8500L-8S4X
- C8500-20X6C



CHAPTER 18

Security Features



Note To achieve simplification and consistency, the Cisco SD-WAN solution has been rebranded as Cisco Catalyst SD-WAN. In addition, from Cisco IOS XE SD-WAN Release 17.12.1a and Cisco Catalyst SD-WAN Release 20.12.1, the following component changes are applicable: **Cisco vManage to Cisco Catalyst SD-WAN Manager, Cisco vAnalytics to Cisco Catalyst SD-WAN Analytics, Cisco vBond to Cisco Catalyst SD-WAN Validator, Cisco vSmart to Cisco Catalyst SD-WAN Controller, and Cisco Controllers to Cisco Catalyst SD-WAN Control Components.** See the latest Release Notes for a comprehensive list of all the component brand name changes. While we transition to the new names, some inconsistencies might be present in the documentation set because of a phased approach to the user interface updates of the software product.

- [Encrypt Communications, on page 115](#)
- [IPsec Pairwise Keys, on page 116](#)

Encrypt Communications

The U.S. federal government requires that all data at rest and in transit be encrypted.

To satisfy this requirement, Cisco uses the following forms of encryption:

- Transport Layer Security (TLS) 1.2 encryption.
- FIPS Object Module - a FIPS validated model that meets the FIPS 140-2 requirements, performs the FIPS-approved cryptographic functions, and is designed for use in conjunction with Cisco SSL distributions. FIPS mode is enabled by default in Cisco Catalyst SD-WAN for government.
For more information, see [Cisco FIPS Object Module](#).
- Cisco SSL is a Cisco-enhanced version of OpenSSL, which enables products to achieve FIPS compliance.
For more information, see [Cryptographic Module Validation Program CMVP](#).



Note All the virtual machines within the Cisco Catalyst SD-WAN for government boundary use the 7.x version of the Cisco SSL library, which runs in FIPS mode, thereby ensuring that all the data at rest and in transit are encrypted.

IPsec Pairwise Keys

Table 19: Feature History

Feature Name	Release Information	Description
Secure Communication Using Pairwise IPsec Keys	Cisco IOS XE Catalyst SD-WAN Release 16.12.1b	This feature allows you to create and install private pairwise IPsec session keys for secure communication between an IPsec device and its peers.

The IPsec pairwise keys feature implements controller-based key exchange protocol between a device and controller.

Controller-based key exchange protocol is used to create a Gateway-to-Gateway VPN (RFC7018) in either a full-mesh topology or dynamic full-mesh topology.

The network devices set up a protected control-plane connection to the controller. The controller distributes policies to network devices. The network devices, in turn, communicate with each other through a secure data plane.

A pair of IPsec session keys (one encryption key and one decryption key) are configured for each pair of local and remote transport locations (TLOC).

Pairwise Keys

Key exchange method combined with authentication policies facilitate pairwise key creation between two network devices. You use a controller to distribute keying material and policies between network devices. The devices generate private pairwise keys with each other.

IPsec devices share public keys from the Diffie-Hellman (DH) algorithm with the controllers. The controllers relay the DH public keys to authorized peers of the IPsec device as defined by the centralized policy.

Network devices create and install private pairwise IPsec session keys to secure communication with their peers.

IPsec Security Association Rekey

Every rekeying IPsec device generates a new Diffie-Hellman (DH) pair and new IPsec security association pairs for each peer with which it is communicating. The new security association pairs are generated as a combination of the new DH private key and the DH public key of each peer. The IPsec device distributes the new DH public value to the controller, which forwards it to its authorized peers. Each peer continues to transmit to the existing security association, and subsequently, to new security associations.

During a simultaneous rekey, up to four pairs of IPsec Security Associations (SAs) can be temporarily created. These four pairs converge on a single rekey of a device.

An IPsec device can initiate a rekey due to reasons such as the local time or a volume-based policy, or the counter result of a cipher counter mode initialization vector nearing completion.

When you configure a rekey on a local inbound security association, it triggers a peer outbound and inbound security association rekey. The local outbound security association rekey is initiated after the IPsec device receives the first packet with the new Security Parameter Index (SPI) from a peer.



-
- Note**
- A pairwise-key device can form IPsec sessions with both pairwise and nonpairwise devices.
 - The rekeying process requires higher control plane CPU usage, resulting in lower session scaling.
-

Configure IPsec Pairwise Keys Using Cisco Catalyst SD-WAN Manager

1. From the Cisco SD-WAN Manager menu, choose **Configuration > Templates**.
2. Click **Feature Templates** and then click **Add Template**.



Note In Cisco vManage Release 20.7.1 and earlier releases, **Feature Templates** is called **Feature**.

3. From the **Device Model** drop-down menu, choose the type of device for which you are creating the template.
4. From **Basic Information**, click **Cisco Security** feature template.
5. From **Basic Configuration**, click **On** or **Off** from the **IPsec pairwise-keying** field.
6. Alternatively, enter the pairwise key specific to the device in the **Enter Key** field.
7. Click **Save**.

Configure Pairwise Keys and Enable Rekeying on the CLI

A pair of IPsec session keys is configured for each pair of local and remote transport locations.

The keys use AES-GCM-256 (AES_256_CBC for multicast) cipher to perform encryption. By default, a key is valid for 3600 seconds.

Configure Pairwise Keys

Use the following command to configure pairwise keys:

```
Device(config)# security ipsec pairwise-keying
```



Note You must reboot the Cisco IOS XE Catalyst SD-WAN device for the private-key configuration to take effect.

Configure Rekeying for IPsec Pairwise Keys

Use the following command to configure rekeying for pairwise keys:

```
Device(config)# security ipsec pwk-sym-rekey
```

Verify IPsec Pairwise Keys on a Cisco IOS XE Catalyst SD-WAN Device

Use the following command to verify the outbound connections for pairwise keys:

```
Device# show sdwan ipsec pwk outbound-connections
```

SS	E-KEY	AH	REMOTE	SA	PKEY	NONCE	PKEY					
SOURCE IP	Source Port	SOURCE IP	DEST Port	LOCAL TLOC ADDRESS	REMOTE TLOC COLOR	PWK-SPI	INDEX	ID	REMOTE TLOC COLOR	TLOC HASH	TLOC HASH	TLOC HASH
REMOTE TLOC ADDRESS	REMOTE TLOC ADDRESS	REMOTE TLOC COLOR	PWK-SPI	INDEX	ID	HASH	HASH	HASH				
HASH	AUTH											
10.168.11.3	12346	192.168.90.3	12346	10.1.0.2					lte			
10.1.0.1		privatel	000000	202	0	6668			17B0	F5A5		
true												
10.168.11.3	12346	192.168.92.6	12346	10.1.0.2					lte			
10.1.0.6		default	00A001	52	10	0ED6	AF12	0A09	8030			
true												
10.168.12.3	12346	192.168.90.3	12346	10.1.0.2					blue			
10.1.0.1		privatel	000000	205	0	6668			17B0	F5A5		
true												
10.168.12.3	12346	192.168.92.6	12346	10.1.0.2					blue			
10.1.0.6		default	00A001	55	10	0ED6	AF12	B9B7	BE29			
true												

Use the following command to verify the inbound connections on IPsec pairwise keys:

```
Device# show sdwan ipsec pwk inbound-connections
```

DEST	LOCAL	LOCAL	SOURCE	REMOTE	REMOTE				
SA	PKEY	NONCE	PKEY	SS	D-KEY	AH	PORT	DEST IP	PWK-SPI
PORT	TLOC ADDRESS	TLOC ADDRESS	TLOC COLOR	TLOC ADDRESS	TLOC COLOR	AUTH	TLOC ADDRESS	TLOC COLOR	PWK-SPI
INDEX	ID	HASH	HASH	HASH	HASH				
192.168.90.3				12346			10.168.11.3		
12346	10.1.0.2		lte				10.1.0.1	privatel	000000
2	1	5605	70C7	17B0	F5A5	true			
192.168.92.6				12346			10.168.11.3		
12346	10.1.0.2		lte				10.1.0.6	default	00100B
52	1	5605	70C7	CCC2	C9E1	true			
192.168.90.3				12346			10.168.12.3		
12346	10.1.0.2		blue				10.1.0.1	privatel	000000
5	1	B9F9	5C75	17B0	F5A5	true			
192.168.92.6				12346			10.168.12.3		
12346	10.1.0.2		blue				10.1.0.6	default	00100B
55	1	B9F9	5C75	A0F8	7B6B	true			

```
Device# show sdwan ipsec pwk local-sa
```

PKEY	NONCE	PKEY	SA			
TLOC-ADDRESS	TLOC-COLOR	SOURCE-IP	SOURCE PORT	SPI	INDEX	ID
10.1.0.2	lte	10.168.11.3	12346	257	6	1 5605
70C7						
10.1.0.2	blue	10.168.12.3	12346	257	3	1 B9F9
5C75						

```
Device# show platform hardware qfp active feature ipsec da spi
```

g_hash_idx	Flow id	QFP SA hdl	source IP	dport	SA ptr	sport	dest IP
						crypto_hdl/old	

```

1541      3      11      192.168.90.3      12346 192.168.92.6
      12346 0x312b84f0 0x00000115/0x00000114
0x0000000031fbfa80/0x0000000031fbd520
6661      131     36      10.168.12.3      12346 192.168.92.6
      12346 0x312b9990 0x0000b001/0x0000a001
0x0000000031fbc380/0x0000000031fbc9a0
7429      117     6       10.168.11.3     12346 192.168.92.6
      12346 0x312b9300 0x0000b001/0x0000a001
0x0000000031fbd970/0x0000000031fbb580

```

```

      System id  Wan int Wan ip
Yubei-ledge    5102  Gi2.xxx Sub 10.168.xxx
Yubei-tsn      5108  Gi0/0/1 192.168.92.8
Yubei-ovld     5106  Gi0/0/0 192.168.92.6
Yubei-lng      5107  Gi0/0/0 192.168.92.7
Yubei-utah     5104  Gi0/0/0 192.168.92.4
Yubei-vedge    5101  ge0/0   192.168.90.3

```

Use the following command to display IPsec pairwise keys information on a Cisco IOS XE Catalyst SD-WAN device:

```
Device# show sdwan security-info
```

```

security-info authentication-type "AH_SHA1_HMAC SHA1_HMAC"
security-info rekey 86400
security-info replay-window 512
security-info encryption-supported "AES_GCM_256 (and AES_256_CBC for multicast)"
security-info fips-mode Enabled
security-info pairwise-keying Enabled

```

Debug Commands on Cisco IOS XE Catalyst SD-WAN Devices

Use the following **debug** commands for debugging issues related to IPsec pairwise keys:

```

debug plat soft sdwan ftm pwk [dump | log]
debug plat soft sdwan ttm pwk [dump | log]
debug plat soft sdwan vdaemon pwk [dump | log]

```




CHAPTER 19

Software Development Life Cycle (SDLC)



Note To achieve simplification and consistency, the Cisco SD-WAN solution has been rebranded as Cisco Catalyst SD-WAN. In addition, from Cisco IOS XE SD-WAN Release 17.12.1a and Cisco Catalyst SD-WAN Release 20.12.1, the following component changes are applicable: **Cisco vManage to Cisco Catalyst SD-WAN Manager, Cisco vAnalytics to Cisco Catalyst SD-WAN Analytics, Cisco vBond to Cisco Catalyst SD-WAN Validator, Cisco vSmart to Cisco Catalyst SD-WAN Controller, and Cisco Controllers to Cisco Catalyst SD-WAN Control Components.** See the latest Release Notes for a comprehensive list of all the component brand name changes. While we transition to the new names, some inconsistencies might be present in the documentation set because of a phased approach to the user interface updates of the software product.

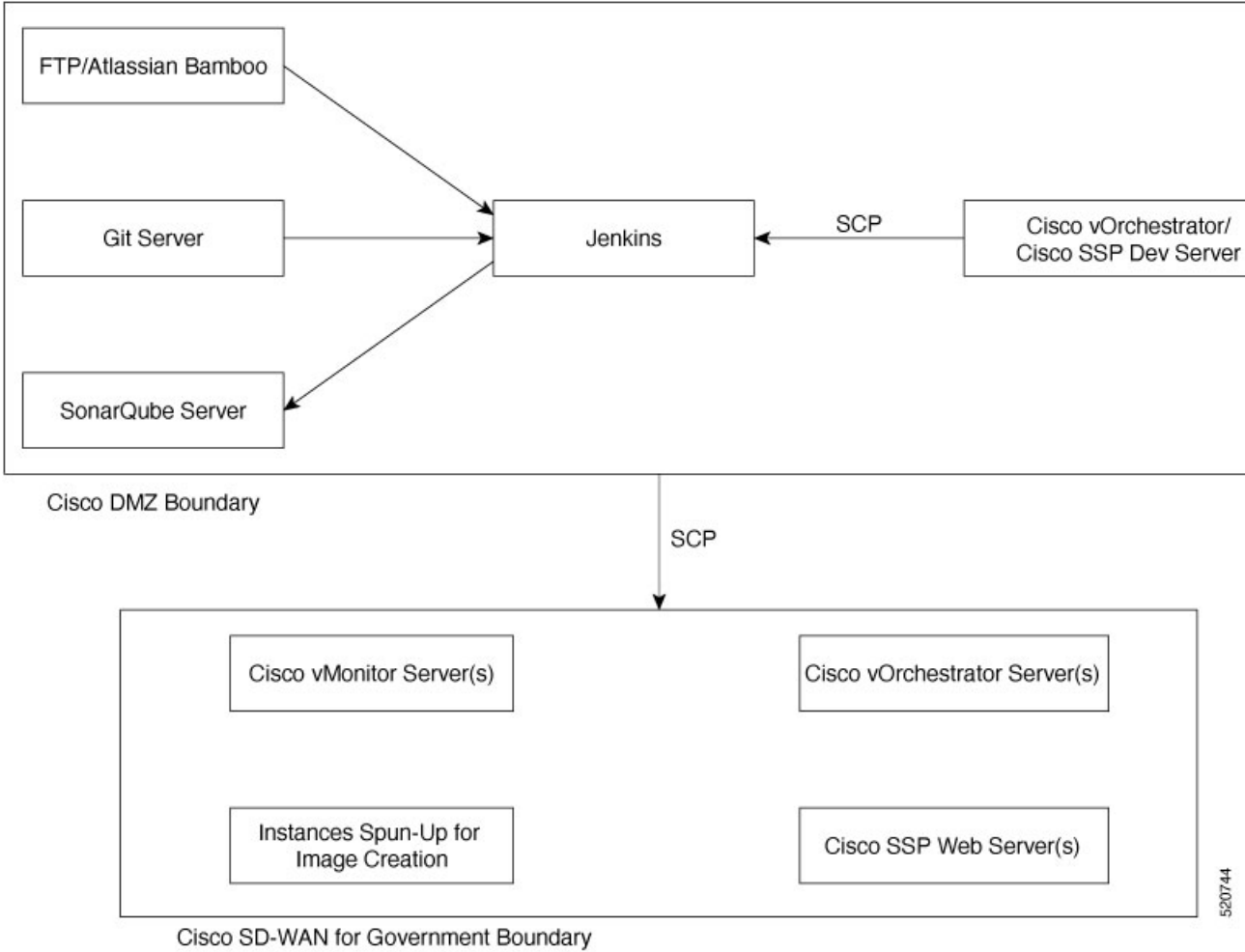
- [Architecture of Software Development Life Cycle Pipelines, on page 121](#)
- [Management VPC SDLC Pipeline, on page 123](#)
- [Customer VPC SDLC Pipeline, on page 124](#)
- [Code Analysis Reporting, on page 125](#)

Architecture of Software Development Life Cycle Pipelines

There are two Cisco Catalyst SD-WAN for government Software Development Life Cycle (SDLC) pipelines:

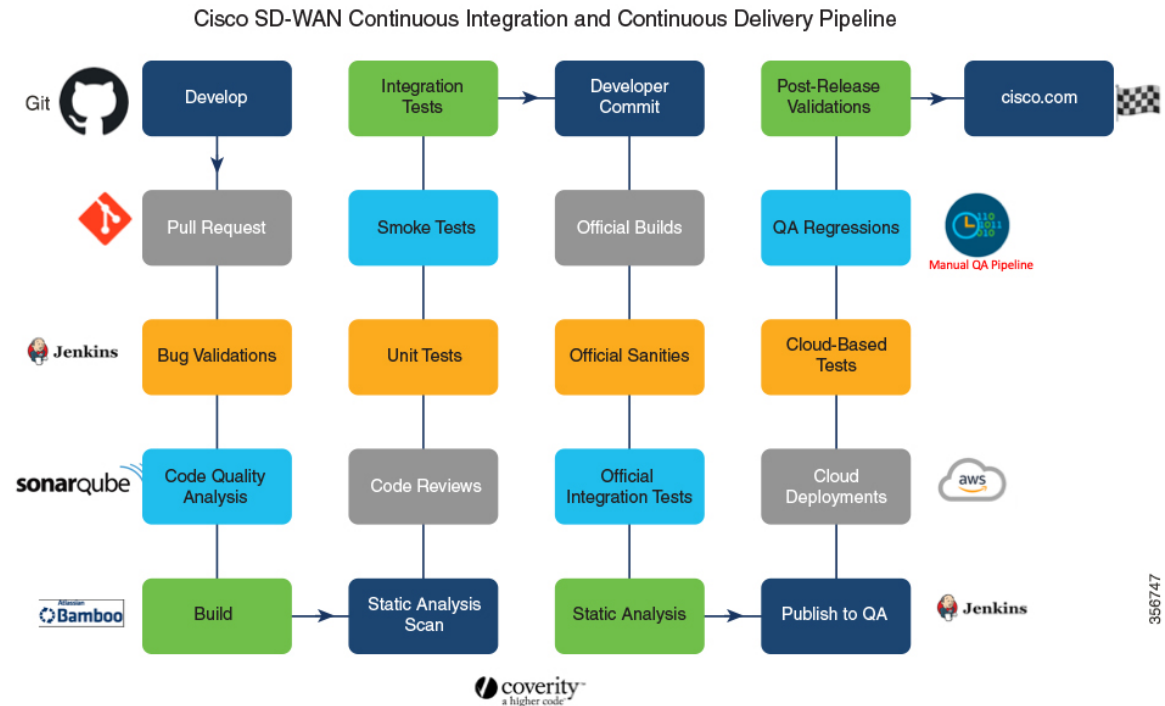
- Cisco vOrchestrator and Cisco vMonitor SDLC pipeline: The SDLC pipeline used to develop and deploy control components in the Amazon management VPC.
- Cisco Catalyst SD-WAN controllers and Cisco SD-WAN Manager SDLC pipeline: The SDLC pipeline used to develop and deploy control components in the Amazon customer VPC.

Figure 9: Cisco vOrchestrator and Cisco vMonitor SDLC pipeline



520744

Figure 10: Cisco SD-WAN Continuous Integration and Continuous Delivery Pipeline



356747

Management VPC SDLC Pipeline

Before the images are built and deployed to Cisco Catalyst SD-WAN for government, the code is first analyzed. After analysis, the code is pushed to a development server in the Cisco DMZ network.

The management VPC SDLC pipeline does the following:

Checks for Regressions and Analysis of Code

To check for regressions and analyze code, Cisco has created the following automated pipeline:

1. Jenkins pulls the code locally from Cisco's Git server.
2. Jenkins (open-source automation tool) securely copies the code to the development server using the scp (secure copy) utility.
3. On the development server, robot regressions are triggered. Regression reports are generated and stored locally on the Jenkins server.
4. The SonarQube scanner scans the local source code. The results of the scans are pushed to the SonarQube server.
5. Clears the local workspace.

Upgrade and Deploy Apps

To upgrade and deploy applications, Jenkins does the following:

1. Pulls the source code locally.
2. Copies the code using the scp utility to the appropriate server using the PEM key.
3. Performs the required steps to upgrade or deploy the servers.
4. Verifies that all the services are functioning.
5. Sends a notification email of the job status.
6. Clears the local workspace.

Deploy to Cisco Catalyst SD-WAN for Government

The pipeline creates instances that it uses to create encrypted Amazon Machine Images (AMI) of the new builds. These images are then copied to the federal government environment and added to the image database. The pipeline does this:

1. Pulls the appropriate build file (tar.gz) from the FTP server.
2. Creates instances in the GovCloud environment.
3. Uses these instances to create base images.
4. Using the scp utility, and securely copies the code to these instances.
5. Configures the instances to meet the requirements of each controller.
6. Creates base images using these instances.
7. Terminates the instances that were used for image creation.
8. Creates unencrypted copies of the new image.
9. Creates encrypted copies of the unencrypted images.
10. Tags the encrypted images.
11. Clears the build files from the local server.
12. Cisco vOrchestrator identifies the encrypted images using the tags.
13. Cisco vOrchestrator stores the AMI IDs in the database to use when creating an overlay network.

Customer VPC SDLC Pipeline

To develop and deploy code for Cisco Catalyst SD-WAN controllers, the following is done:

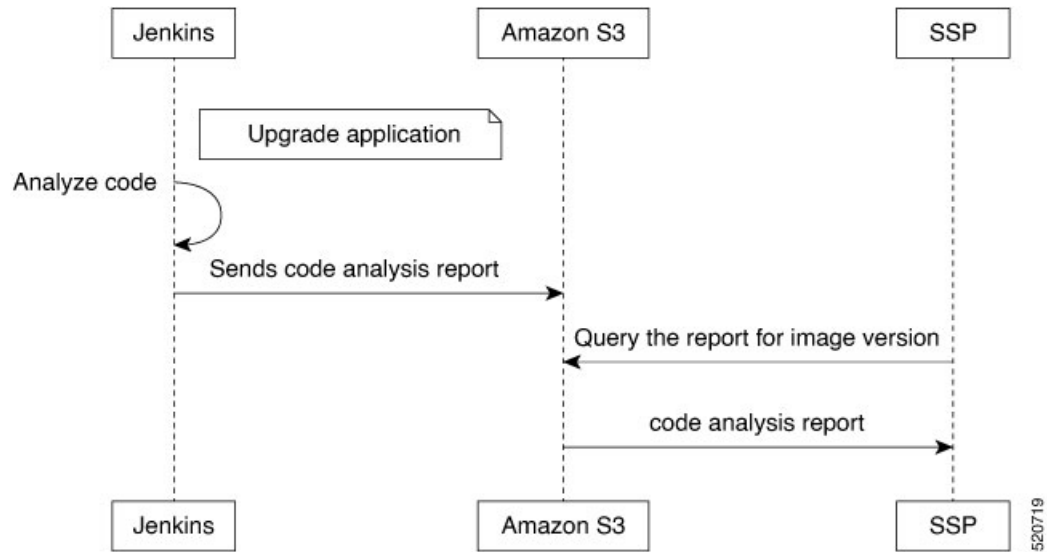
1. Developers write and integrate code:
 - a. Writes code and pushes to Git.
 - b. Jenkins validates the code for bugs.

- c. SonarQube analyzes the code for quality.
 - d. Atlassian Bamboo builds the code
 - e. A static analysis scan is performed.
 - f. Other developers review the code.
 - g. Other standard code tests such as unit, smoke, and integration tests are performed.
 - h. The developer commits the code.
 - i. An official build is generated.
 - j. Official sanity and integration tests are conducted.
 - k. Static analysis scans are run on the build.
 - l. The builds are published to Quality Assurance.
2. Quality Assurance tests the code:
 - a. Quality Assurance deploys the builds to cloud deployments.
 - b. Quality Assurance runs cloud-based tests.
 - c. Quality Assurance runs regression tests and other tests that are a part of the manual Quality Assurance pipeline.
 - d. Run postrelease validations.
 3. The build is published to Cisco.com.

Code Analysis Reporting

Whenever one of the Cisco cloud applications (Cisco vOrchestrator, Cisco vMonitor, Cisco Catalyst SD-WAN Portal, AWS bastion host, and Data Center Services [DCS]) applications are upgraded through Jenkins, a code analysis report is generated. The report is available on the Cisco Catalyst SD-WAN Portal. After every upgrade, a script pushes the report to AWS S3, and saves it based on its version. If there is a request from the Cisco Catalyst SD-WAN Portal, a report is downloaded to AWS S3 directly and served.

Figure 11: Code Analysis Reporting Workflow



Accessing the Build Report Using the Cisco Catalyst SD-WAN Portal

1. Log in to the Cisco Catalyst SD-WAN Portal.
2. Click the sidebar icon in the top left corner of the window.
3. Click **Build Reports**.
4. Download the code analysis reports.