

Revised: July 25, 2025

# SD-Routing Solution Guide

## Introduction to SD-Routing

This solution guide provides an overview of the SD-Routing solution. It discusses the components, use cases, and various capabilities of Cisco Catalyst SD-WAN Manager and how it can be used to build your SD-Routing configuration.

### Intended audience

The audience for this document is anyone who wants a comprehensive understanding of the SD-Routing solution. This document is especially useful for technical support engineers who want to develop an end-to-end understanding of this solution's various capabilities and features to facilitate increased adoption in new customer segments.

### What is SD-Routing

SD-Routing is a capability to simplify and overcome the challenges of traditional routing deployments. This capability enables Cisco Catalyst SD-WAN Manager to manage traditional (non-SD-WAN) routing devices operating in autonomous mode and SD-WAN devices operating in controller mode through a single platform. This unified management platform offers many features such as device lifecycle management, DIA (Direct Internet Access), Cloud onRamp, monitoring, and troubleshooting tools.

### How to use SD-Routing

This section outlines the various ways in which SD-Routing can be used in your organization.

- **End-to-End lifecycle management driven by intent-based configuration:** Define intent in the form of features that are converted to configuration and security policies, which help manage all activities from initial planning and deployment, configuration, scheduling software upgrades, to monitoring and troubleshooting.
- **Modern monitoring and troubleshooting:** The solution offers a single-page, real-time user interface that shows a consolidated view of all monitoring components and services of the network. You can use Cisco Catalyst SD-WAN Manager to visualize the functioning of the devices using various states, statistics, dashlets, charts, and events. For more information, see [Monitoring Crypto VPN solutions on SD-Routing devices](#).

Figure 1: All the devices in the network with different states

Devices 15						
Q Search Table						
Hostname	Device Model	Site Name	System IP	Health ⓘ	Reachability	
Host 1	C1121-8PLTEPW*	Site 1	209.165.200.224	✖	↓	
Host 2	C8000v	Site 2	209.165.200.225	✖	↓	
Host 3	C8000v	Site 3	209.165.200.226	✖	↓	
Host 4	C8300-1N1S-6T (SD-Routing)	Site 4	209.165.200.227	✖	↓	
Host 5	C8000v	Site 5	209.165.200.228	✔	↑	
Host 6	ISR4331	Site 6	209.165.200.229	✖	↑	
Host 7	C1111-8PW*	Site 7	209.165.200.230	✔	↑	

- **Multicloud integration:** Extend your WAN network by using cloud services such as Microsoft Azure and Amazon Web Services (AWS) for efficient and secure connectivity between on-premises networks and cloud resources.
- **DIA with embedded security:** Improve the user experience for Software as a Service (SaaS) applications at remote sites by eliminating performance degradations caused by backhauling internet traffic to a central data center. DIA (Direct Internet Access) allows control of internet access on a per VPN basis. Security features are built directly into the DIA solution or its components in form of policies, rather than being separate software or hardware components.
- **Configuration support:** Provides support to configure features in the WAN branch and aggregation use case by using **Feature Parcels** support or by importing/loading configuration from onboarded devices.
- **Workflows for Security Policies:** Provides workflows for security policies such as Security Service Edge (SSE), Next-Generation Firewall (NGFW), Intrusion prevention, Advanced Malware Protection (AMP), and URL Filtering to ensure consistent security policies are applied across all branch deployments.

## What are the components of SD-Routing

SD-Routing consists of these components:

Component	Role
<b>Cisco Catalyst SD-WAN Manager</b>	<p>This centralized network management system is software-based and provides a Graphical User Interface (GUI) to easily monitor, configure, and maintain all onboarded devices and connected links in the underlay network.</p> <p>It provides a single pane of glass for Day 0, Day 1, and Day 2 operations.</p>
<b>Catalyst SD-WAN Validator</b>	<p>This software-based component performs the initial authentication of WAN Edge devices and orchestrates connectivity between Cisco Catalyst SD-WAN Manager and WAN Edge devices.</p> <p>It also has an important role in enabling the communication between devices that are located behind Network Address Translation (NAT).</p>
<b>Routing device</b>	<p>This is a traditional routing device operating in autonomous mode and is typically part of any network. This device, available as either a hardware appliance or as a software-based router, sits at a physical site, or in the cloud and provides secure data plane connectivity among the sites over one or more WAN transports.</p> <p>This device is responsible for traffic forwarding, security, encryption, quality of service (QoS), routing protocols such as Border Gateway Protocol (BGP), Open Shortest Path First (OSPF), and more.</p>

## Feature support

The SD-Routing solution broadly offers these features on various platforms.

**Figure 2: Supported features on different platforms**

Platform	Zero Touch Provisioning	Monitoring	Configuration	SWIM (Software image management)	Troubleshooting
Catalyst 8000 (C8500, C8300, C8200, C8KV)	✓	✓	✓	✓	✓
ISR 4000 (ISR4400, ISR4300, ISR4200)	✓	✓	✗	✓	✓
ISR 1000 (ISR1100, ISR1100x)	✓	✓	✓	✓	✓
ASR 1000 Series (ASR 1001-HX, ASR 1002-HX )	✓	✓	✗	✓	✓
Industrial Routers ( IR1101, IR1800, IR8100, IR8300, ESR6300)	✓	✓	✓	✓	✓

Support to configure features is not available on Cisco ASR 1001-HX, Cisco ASR 1002-HX, and Cisco ISR 4000 series platforms, but you can use these platforms for monitoring and troubleshooting devices.


## Getting started with SD-Routing

Before you get started with SD-Routing, make sure you have completed all prerequisites.

### General prerequisites

The general prerequisites include bringing up Cisco Catalyst SD-WAN Manager control components, validating device identity, setting up connectivity with Cisco Plug and Play (PnP) Connect server, and choosing the onboarding method best suited for your needs:

What	Why
<b>Boot up Cisco Catalyst SD-WAN Manager control components</b>	<p>You must boot Cisco Catalyst SD-WAN Manager control components and the Catalyst SD-WAN Manager in a specific sequence.</p> <p>See <a href="#">Cisco Catalyst SD-WAN Getting Started Guide</a> for details on bringing up the network.</p>
<b>Validate device identity</b>	<p>A device's identity is validated through certificates.</p> <ul style="list-style-type: none"> <li>• (Recommended): If your network uses the Cisco Public Key Infrastructure (PKI), you must upload any certificate. For understanding PKI, see <a href="#">Public Key Infrastructure</a> and the <a href="#">Cisco Catalyst SD-WAN Understanding and Planning a PKI</a> guide.</li> <li>• If your network is an enterprise network, upload a Root CA.</li> </ul> <p>See <a href="#">Catalyst SD-WAN Control Components Certificates and Authorized Serial Number File Deployment Guide</a> for information about enterprise certificates.</p>

<b>Onboarding methods</b>	Decide the best onboarding method for your requirements based on whether you have a m See <a href="#">Preferred Onboarding Options</a> .
<b>Provision with Cisco Plug and Play (PnP) Connect server</b>	<p>You must add the routing device to the Cisco Plug and Play (PnP) Connect server at <a href="#">Cisco</a> associate it with the Catalyst SD-WAN Validator controller profile. This ensures that the d SD-WAN Validator's allowed list of devices.</p> <p>You can download the allowed list <i>provision file</i> from the PnP portal and upload it to the SD-WAN Manager, or synchronize it with the Cisco Catalyst SD-WAN Manager through Account option. Cisco Catalyst SD-WAN Manager later distributes this allowed list to t</p> <p>Software routing devices deployed in virtual environment do not have chassis or serial num PnP server generates a unique serial number when the software device is added in the P</p> <p>See <a href="#">Add a Routing Device to Plug and Play Connect Portal</a> to know more about how to</p> <div>  <p><b>Note</b> Until Cisco IOS XE 17.16.1a release, the On-Prem PnP server does not support of routing devices.</p> </div>

## Device prerequisites

The device prerequisites include minimum software and device requirements for the autonomous device, and software requirements for Cisco Catalyst SD-WAN Manager.

<b>Minimum release version</b>	<p><b>Routing device:</b></p> <p>The autonomous routing device should have a minimum software version of Cisco IOS XE 17.15.1a and must be in Install Mode to boot the device.</p> <p><b>Cisco Catalyst SD-WAN Manager:</b></p> <p>The Cisco Catalyst SD-WAN Manager should have a minimum software version of 20.15 and should be equal to or greater than the IOS XE software version of the routing device.</p> <p>If you are using a hardware device that is running a version earlier than Cisco IOS XE 17.15.1a, use the <a href="#">Seamless Upgrade</a> feature to first upgrade your device and then onboard it into the Cisco Catalyst SD-WAN Manager.</p> <p><b>Configuration Groups:</b></p> <p>To use <b>Configuration Groups</b> for configuring any feature supported on SD-Routing devices, the minimum version of Cisco IOS XE software and Cisco Catalyst SD-WAN Manager is IOS XE 17.15.1a.</p>
--------------------------------	--

<b>Routing device</b>	<p>The factory default routing device should be able to resolve FQDN devicehelper.cisco.com and reach the Cisco cloud-hosted PnP Connect server to retrieve the Catalyst SD-WAN Validator controller information, organization name, and enterprise root CA certificates (if using enterprise root CA certificates)</p> <p>The details required are:</p> <ul style="list-style-type: none"> <li>• Site ID</li> <li>• Organization-name</li> <li>• Catalyst SD-WAN Validator information (IP address or FQDN of Catalyst SD-WAN Validator server)</li> <li>• Interface for connection to Cisco Catalyst SD-WAN Manager (Physical, Sub-interface, and Loopback)</li> </ul> <p><b>System IP :</b></p> <p>The System IP address provides a fixed location for the device in the network and is unique across all SD-Routing devices in the network. The system IP is used as the device's loopback address in the Global VRF. This address cannot be used for another interface in Global VRF.</p>
-----------------------	--

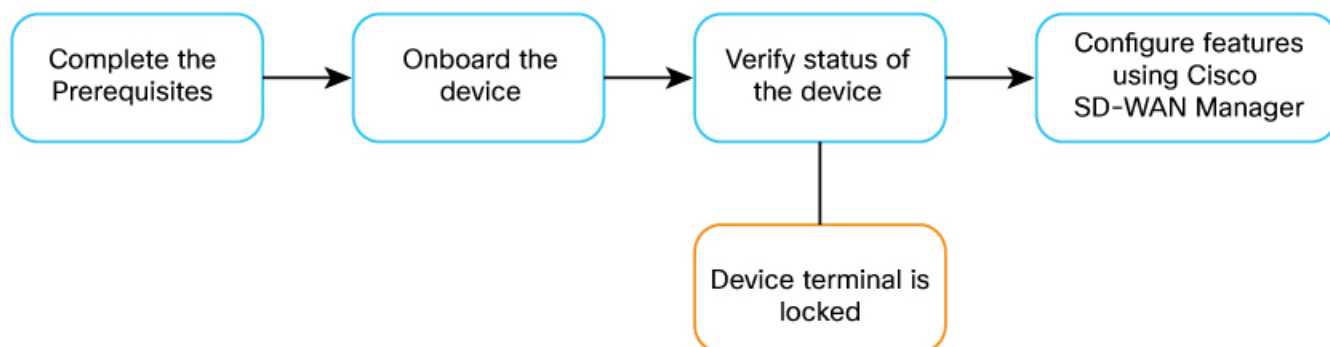
## Onboard a device

After you have reviewed the general and device prerequisites, onboard the autonomous device to Cisco Catalyst SD-WAN Manager using the onboarding method prescribed for your environment. See, [Onboard Routing Devices to Cisco Catalyst SD-WAN Manager](#).

After onboarding, verify the status of control connections using [Monitoring dashboard](#) in Cisco Catalyst SD-WAN Manager.

After the device is successfully onboarded and initial configuration is complete, the device terminal locks and is no longer available for configuration purposes. All feature configurations must be performed using Cisco Catalyst SD-WAN Manager.

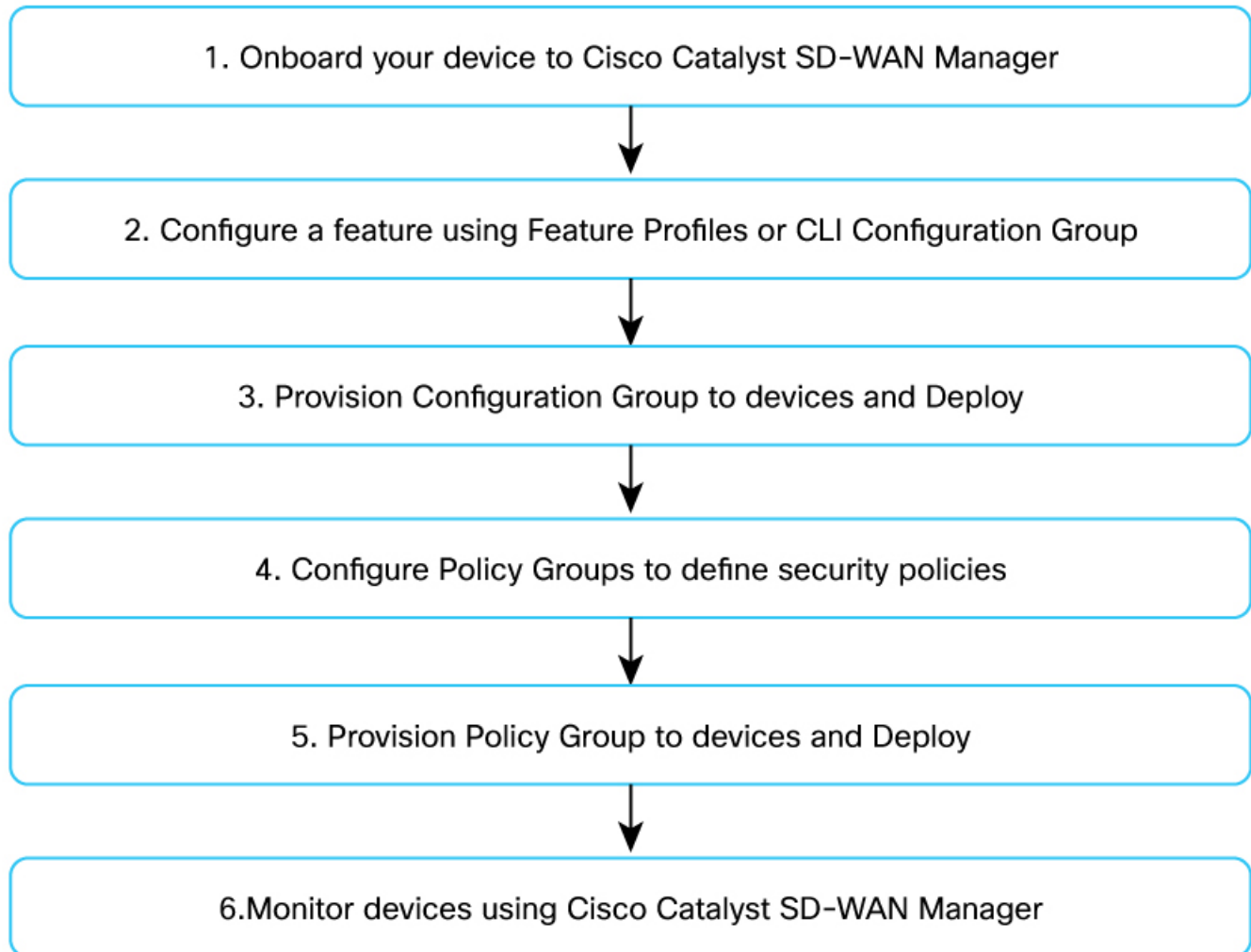
**Figure 3: Process of onboarding a device**



## Workflow to configure and monitor SD-Routing devices

This figure outlines the high-level steps involved in configuring and monitoring the SD-Routing solution. More details about each of the steps are provided in the subsequent section.

*Figure 4: Process to configure an SD-Routing device*



*Figure 5: Process to monitor an SD-Routing device*

You can use an onboarded device only for monitoring and troubleshooting purpose without using **Configuration Groups** to configure any features.

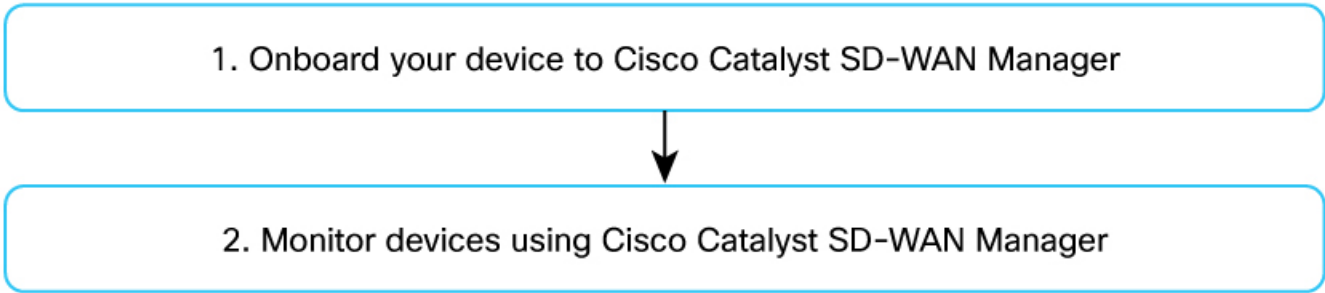


Table 1: Configure and monitor an SD-Routing device

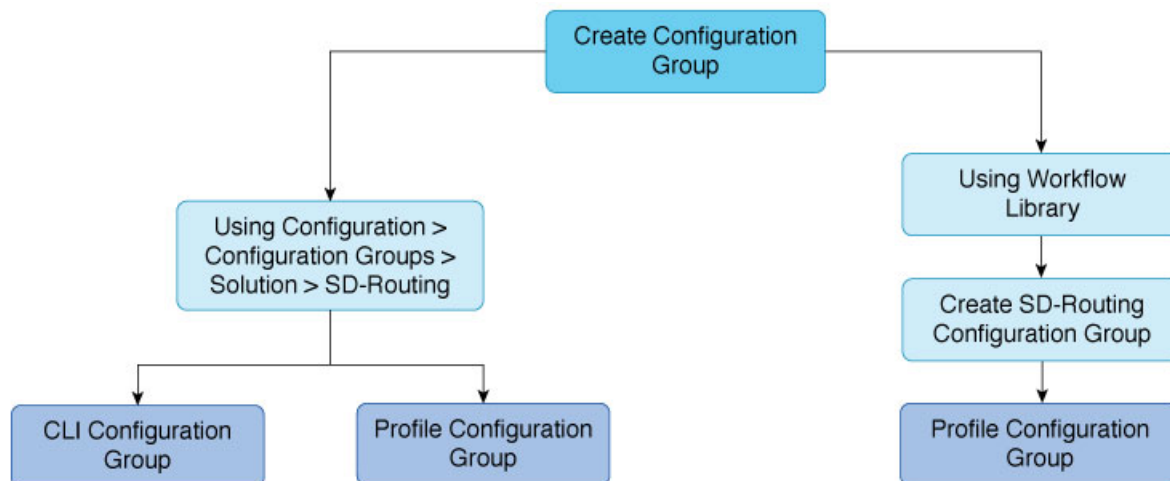
Step	What	Why	How
1	Onboard the device	To set up control connections to Cisco Catalyst SD-WAN Manager and therefore simplify management and configuration.	<a href="#">Onboard routing devices to Cisco Catalyst SD-WAN Manager</a>
2	Configure a feature using Configuration Groups	To build the configuration using <b>Feature Profiles</b> .	<a href="#">Configuration Groups for SD-Routing devices</a>
3	Deploy Configuration Group	To apply the configuration to one or more devices and deploy the changes.	<a href="#">Associate and deploy the Configuration Group to an SD-Routing device</a>
4	Configure Policy Groups	To configure policy and policy objects to translate business intent to control and manage traffic.	<a href="#">Using Policy Groups for SD-Routing devices</a>
5	Deploy Policy Groups	To apply the policy configuration to one or more devices and deploy the changes.	<a href="#">Using Policy Groups for SD-Routing devices</a>
6	Monitor devices	To monitor, track various aspects of device functioning and traffic flow.	<a href="#">SD-Routing Collection Page &gt; Monitor</a>

## Configuration management

**Configuration Groups** manage configuration on SD-Routing devices using user intent. This section describes the various methods to input user intent.



Figure 6: Different methods to configure user intent



## Configuration Group

A **Configuration Group** is a logical grouping of features or configurations that can be applied to one or more devices in the network, allowing for simplified and reusable configuration across different devices or locations. You can also create profiles based on features that are required, recommended, or uniquely used, and then combine the profiles to complete a device configuration.

The configuration group workflow in Cisco Catalyst SD-WAN Manager provides a guided method to create configuration groups and feature profiles. See [Configuration Groups for SD-Routing devices](#).

The different ways to apply configuration using **Configuration Groups** to SD-Routing devices are:

- [Feature Profiles](#)
- [CLI Configuration Group](#)

## Feature Profiles

A **Feature Profile** is a pre-defined set of configurations or features that can be applied to one or more devices, forming a logical grouping for deployment and management. For a list of features that have corresponding **Feature Parcels**, see [Appendix: Different Feature Parcels in Cisco Catalyst SD-WAN Manager](#).

### How to use a Feature Parcel

**Feature Parcels** are bundles designed to address common use cases and simplify deployment by providing a pre-packaged set of features. For example, you can configure a DMVPN solution for SD-Routing devices using the **Feature Parcels** in Cisco Catalyst SD-WAN Manager. See [Configure Cisco DMVPN for SD-Routing Devices](#).

## CLI Configuration Group

SD-Routing provides support to configure features in the WAN branch and aggregation use case. In case the feature you are configuring does not have support for [Feature Parcels](#), you can use **CLI Configuration Group** and configure a feature by using only commands.

The configuration you input in the **CLI Configuration Group** should include end-to-end details for the feature to be successfully deployed. For example, VRF, NAT, and so on.

## When to use a CLI Configuration Group

To decide when to use a **CLI Configuration Group** to configure features and functionalities on devices, review these points:

- **Configure an existing SD-Routing device :**

If you have existing SD-Routing devices that you want to bring into the network, the **CLI Configuration Group** allows you to load the device's existing running configuration, modify it, and deploy it back to these devices. You can also build a configuration file offline and import this file to deploy the configuration on devices.

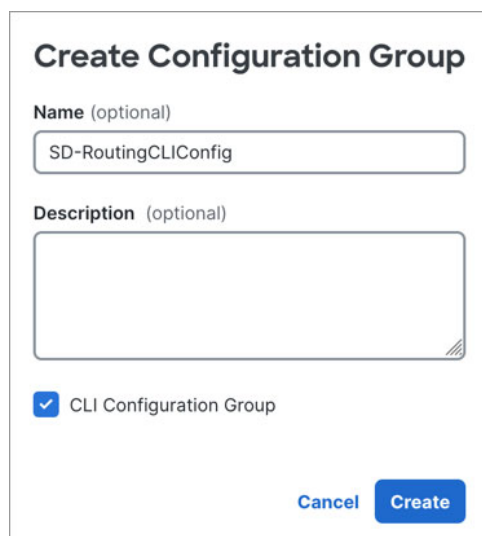
- **Deploy configuration as templates across other devices :**

If you have multiple devices connected to your WAN and you want to use the same **CLI Configuration Group** across all devices, you can define the configuration in one device and then use it as a template across any other device in the network. This saves effort, prevents configuration errors, and helps with quicker deployments.

## How to use a CLI Configuration Group

Let's assume a scenario where you want to deploy Cisco Group Encrypted Transport VPN (GETVPN) in your WAN environment. **Feature Parcel** support is currently not available to configure this solution. Instead, you can use **CLI Configuration Group** and input all commands that are required to configure this solution. The commands include all the deployment constructs such as Group Members, Key Servers, and so on.

*Figure 7: CLI Configuration Group in Cisco Catalyst SD-WAN Manager*



**Create Configuration Group**

Name (optional)  
SD-RoutingCLIConfig

Description (optional)

☒ CLI Configuration Group

Cancel Create

## Understand how CLI Configuration Group is processed

Let's assume you have built your configuration either by using **Load Running config** option from a reachable device or by using the **Import Config File** option. You now have all commands populated in the **CLI** pane.

As mentioned earlier, Cisco Catalyst SD-WAN Manager uses NETCONF or YANG models to configure and manage devices. A typical configuration may have a mix of YANG commands and non-YANG commands. Having a mix of these commands can disrupt the process of provisioning the configuration because Cisco Catalyst SD-WAN Manager processes YANG commands and non-YANG commands in different ways. Therefore, it is important to separate the YANG commands from the non-YANG commands and process them separately.

### Configuration contains only YANG commands


1. Populate configuration in the **CLI** pane by using **Load Running config** option. If there are no non-YANG commands, the **Classic CLI** pane is not displayed.
2. Click **Save**, and then **Done**. The Cisco Catalyst SD-WAN Manager will analyze the new configuration, compare it with the existing configuration on the device, and push the delta configuration to the device. After successfully deploying the configuration, the device terminal locks, and you can only perform any further configuration through the Cisco Catalyst SD-WAN Manager.

### Configuration contains YANG commands and non-YANG commands

Populate the configuration in the **CLI Pane** by using the **Load Running config** option. If the configuration contains non-YANG commands, an alert is displayed. You can choose to automatically move non-YANG commands to the **Classic CLI** pane or ignore the alert and manually update the configuration to separate the YANG commands from the non-YANG commands.

The Cisco Catalyst SD-WAN Manager processes the YANG commands first, then processes the non-YANG commands. Let's look at different error scenarios and how to resolve these errors.

Status as shown in Cisco Catalyst SD-WAN Manager	What is the reason	How is the configuration processed	What should you do
Successful	There is no error in the YANG commands and non-YANG commands. The configuration was processed successfully.	The Cisco Catalyst SD-WAN Manager processes the YANG commands first followed by the non-YANG commands.	No further action is needed.

<b>Partial success</b>	There is no error in the YANG commands but there is an error in the non-YANG commands.	<p>The YANG commands are processed first and successfully pushed to the device.</p> <p>The processing of non-YANG commands stops when an error is encountered.</p> <p>The non-YANG commands (Classic CLI) that are error-free before the error are successfully pushed to the device.</p>	<ol style="list-style-type: none"> <li>1. In <b>Configuration &gt; WAN Edges</b>, select <b>Template Log</b> to view log for the device.</li> <li>2. In <b>Configuration Groups</b> page, select the <b>CLI Configuration Group</b>. Click <b>Edit</b>. Correct the error and then deploy the configuration again.</li> </ol> <div data-bbox="1084 590 1130 642"></div> <p><b>Note</b> Cisco Catalyst SD-WAN Manager does not support rollback <b>Classic CLI</b> commands. To retain the previous device configurations, correct the errors manually using Cisco Catalyst SD-WAN Manager.</p>
<b>Failed</b>	There are errors in the YANG commands and non-YANG commands.	As the YANG commands have errors, processing stops completely and no configuration is deployed to the device.	<ol style="list-style-type: none"> <li>1. <b>Configuration &gt; WAN Edges</b> select <b>Template Log</b> to view log for the device.</li> <li>2. In <b>Configuration Groups</b> page, select the <b>CLI Configuration Group</b>. Click <b>Edit</b>. Correct the error and then deploy the configuration again.</li> </ol> <p>Check if there are any non-YANG commands in the <b>CLI</b> pane. If so, move it to <b>IOS CLI</b> pane.</p>

<b>Rollback</b>	The control connections have failed causing a rollback of the configuration to its previous working state.	No configuration is deployed to the device.	<ol style="list-style-type: none"> <li>1. In <b>Configuration &gt; WAN Edges</b>, review the <b>Reachability</b> column to view devices that are not active.</li> <li>2. If you encounter unknown errors, contact the TAC team for guidance.</li> </ol>
-----------------	--	---	---

## How is SD-Routing configuration processed

Cisco Catalyst SD-WAN Manager uses NETCONF or YANG models to configure and manage devices because the SD-Routing components understand YANG models.

This approach allows network administrators to quickly adapt and introduce new features and functionalities to the SD-Routing solution instead of configuring devices using command-line interfaces. When you configure a feature using **Feature Parcels** and provision the configuration, Cisco Catalyst SD-WAN Manager internally processes these configurations as YANG models.

Let us look at some scenarios to understand how Cisco Catalyst SD-WAN Manager processes configuration.

### Scenario 1: Configure a feature using Feature Profiles

The **Feature Profiles** in Cisco Catalyst SD-WAN Manager provide different profiles. Combine these profiles like building blocks to complete your device configuration. Configure your intent using the appropriate **Feature Profiles**.

#### Define user intent

The user intent is configured using various **Feature Profiles**.

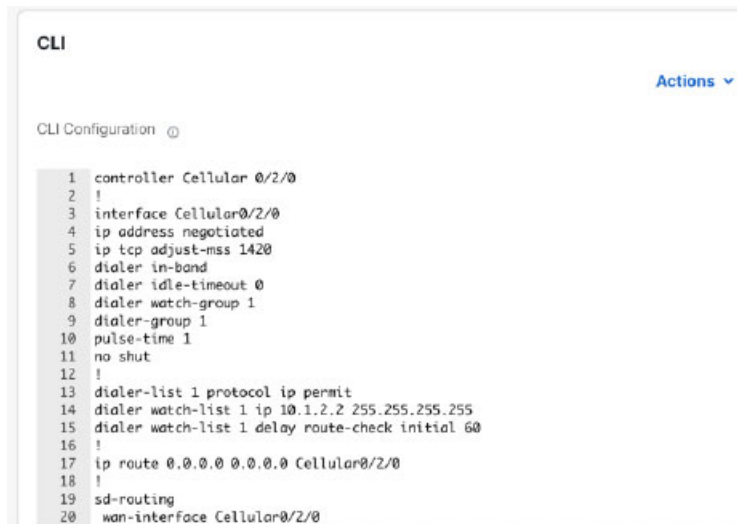
**Figure 8: Sample Feature Parcel in Transport and Management Profile**

The screenshot displays a configuration interface with three stacked sections, each with a title bar and a plus button in the top right corner:

- Global VRF:** Contains a dropdown menu with 'vrf' selected, an edit icon (pencil), and a plus button.
- Cellular Controller:** Contains a dropdown menu with 'Controller0/1/0' selected, an edit icon (pencil), a delete icon (trash), and a plus button.
- Cellular Controller:** Contains a dropdown menu with 'Controller0/3/0' selected, an edit icon (pencil), a delete icon (trash), and a plus button.

If you want to add any extra configuration that is not available as **Feature Parcels**, use the **CLI Add-on Profile** and input or import commands in the **CLI** pane.

**Figure 9: Sample CLI Add-on Profile**



The screenshot shows a web interface for configuring a CLI Configuration Group. At the top, there is a header 'CLI' and a button 'Actions' with a dropdown arrow. Below the header, the text 'CLI Configuration' is followed by a small icon. The main area displays a list of 20 CLI commands, numbered 1 through 20, in a monospaced font. The commands are as follows:

```
1 controller Cellular 0/2/0
2 !
3 interface Cellular0/2/0
4 ip address negotiated
5 ip tcp adjust-mss 1420
6 dialer in-band
7 dialer idle-timeout 0
8 dialer watch-group 1
9 dialer-group 1
10 pulse-time 1
11 no shut
12 !
13 dialer-list 1 protocol ip permit
14 dialer watch-list 1 ip 10.1.2.2 255.255.255.255
15 dialer watch-list 1 delay route-check initial 60
16 !
17 ip route 0.0.0.0 0.0.0.0 Cellular0/2/0
18 !
19 sd-routing
20 wan-interface Cellular0/2/0
```

## Process user intent

The Cisco Catalyst SD-WAN Manager maps all configurations to YANG models automatically. The administrator takes care of entering valid values so that there are no errors during provisioning. After you provision the device successfully, the system replaces the existing configuration with the configuration that you entered in Cisco Catalyst SD-WAN Manager.

## Status of the device after provisioning

After successfully provisioning the configuration to selected devices, the device terminal is locked. This means that any further configuration can only be done using Cisco Catalyst SD-WAN Manager and you cannot make any configuration changes through the device terminal.

If you need to add configuration to the device, detach the device from **Configuration** > **WAN Edges**. Click ..., select **Config Unlock**). You can now add configuration using the device terminal.

If you deploy the **Configuration Group** to the device, all the configuration is saved to the device and the device terminal is locked.

## Errors during provisioning

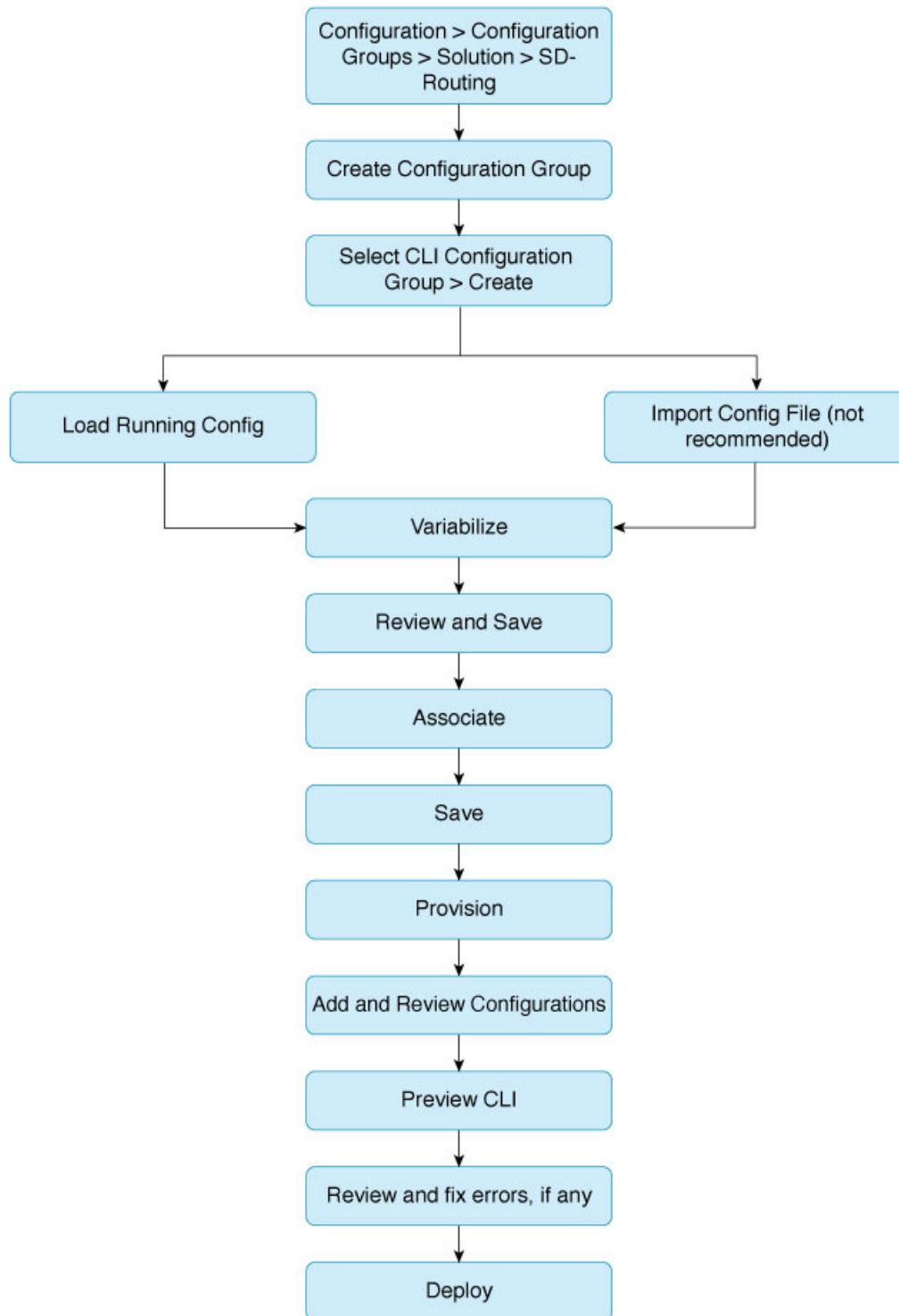
If the provisioning of configuration fails due to any errors, the configuration on the device is rolled back to the earlier working state.

## Scenario 2: Configure a feature using CLI Configuration Group

You can use the **CLI Configuration Group** to group and manage device configurations using only commands. A **CLI Configuration Group** is useful to configure features on devices when configurations are not fully supported through **Feature Parcels**.

This illustration shows how configuration in a **CLI Configuration Group** is processed. You will find more details in the next sections.

**Figure 10: How a CLI Configuration Group is processed**



## Define User Intent

You can use the **Load Running Configuration** option to load any existing configuration from an onboarded device. This provides a foundation for you to add additional configuration as needed. This option also has built-in logic to automatically detect any non-YANG commands and alert you of them.

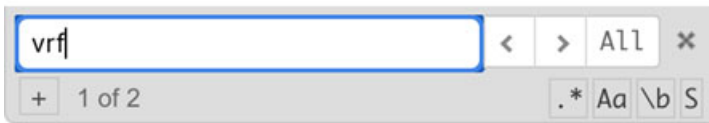
You can also choose to build your configuration file offline and then use the **Import Config File** option to load all the configuration. Both options help you streamline deployments, migrate configurations between Cisco Catalyst SD-WAN Manager instances, and apply standardized configurations across environments.

When you use the **Import the configuration** option, Cisco Catalyst SD-WAN Manager does not validate the syntax or support configuration rollback in case of errors. It is the administrator's responsibility to validate the configuration before provisioning it. This is not the recommended method to build the configuration on your device.

## Search CLI

Typically configurations spans across multiple lines and when you are trying to build your configuration for a specific functionality you may need to review certain details. For example, VRF definition. In such a scenario, you can use the **Search CLI** option. **Search CLI** option is also helpful when you encounter an error during deployment and you have to look for the specific line to fix in the configuration.

*Figure 11: Search CLI pane in Cisco Catalyst SD-WAN Manager*



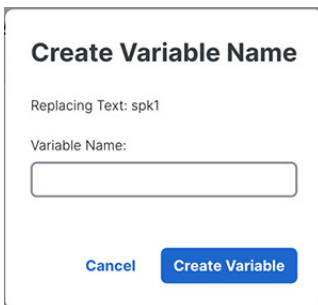
You can choose between wildcard search, case sensitive search, whole word search or search within a selection.

## Create Variable

The **Create Variable** functionality allows you to convert static configuration values into dynamic placeholders. This enables flexible and reusable configurations across multiple devices.

For example, you can introduce a variable for host name in the configuration. For each device where the configuration is deployed, the administrator only needs to enter the hostname for that device.

*Figure 12: Replace text in CLI configuration*



## Encrypt Type6

You can use **Encrypt Type 6** specifically when you need to secure sensitive information in a configuration, such as passwords or keys. This feature ensures the information is encrypted before it is deployed to devices. The encryption is done using a reversible 128-bit AES encryption algorithm.



## Classic CLI

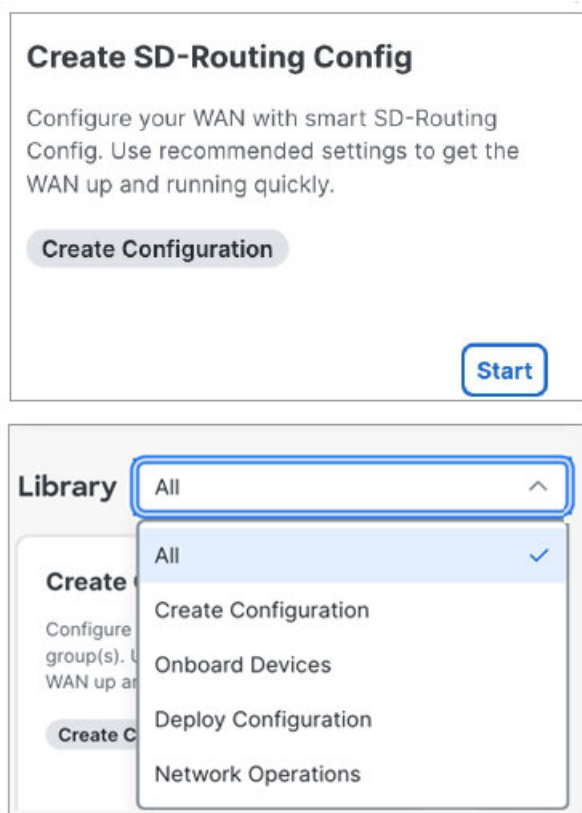
The **Classic CLI** option lets you separate the YANG commands from the commands without associated YANG models.

Use this option to launch a **Classic CLI** pane in which you can enter any non-YANG commands. It is the administrator's responsibility to ensure that the commands entered in the Classic CLI pane are validated and do not cause any network instability or service disruptions. See [Understand how CLI Configuration Group is processed, on page 10](#).

## Workflows

Workflows are pre-defined, guided processes that simplify common tasks, such as **Configuration Group** creation, upgrading software, and onboarding devices quickly.

*Figure 13: Creating a Workflow in Cisco Catalyst SD-WAN Manager*

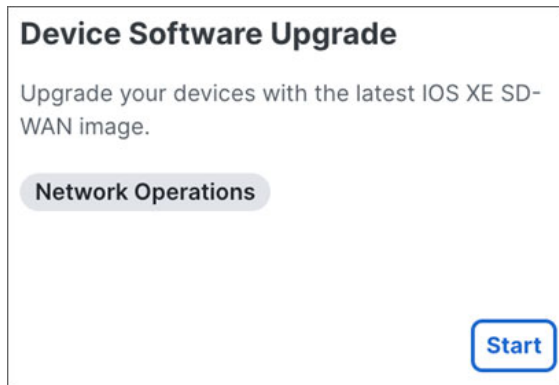


## How to use Workflows

Suppose the SD-Routing devices on your network use an older release of Cisco IOS XE software. All devices must be upgraded to the latest image.

To do this without manually upgrading each device, you can start a **Device Software Upgrade** workflow to upgrade all the devices together to the latest software image.

Figure 14: Schedule a software upgrade using Cisco Catalyst SD-WAN Manager workflows



## Policy Management

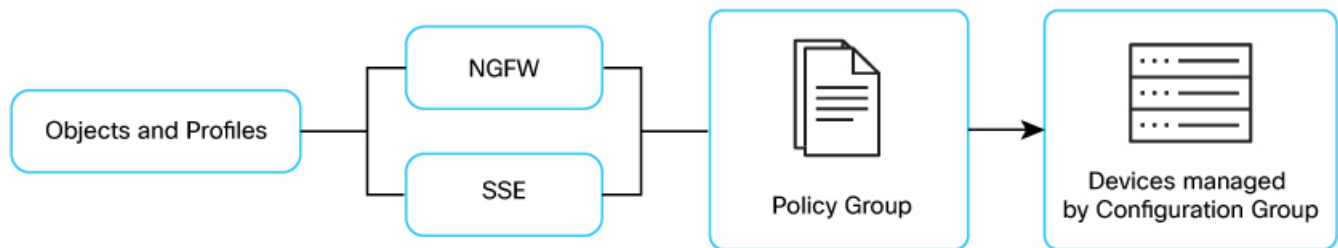
Policy management on SD-Routing devices is done using **Policy Groups**. A policy defines how the network should behave, influencing the flow of both data traffic and routing information.

### What is a Policy Group

A **Policy Group** is a collection of policies and parameters that you can configure and deploy together. These groups simplify policy management by letting you package multiple policy configurations into a single, manageable unit. Examples of policies you can configure include security, application priority, and traffic management.

After you create a **Policy Group**, you can associate it with one or more sites or with a single device at a site. After association, you can deploy it on devices that are managed by **Configuration Groups**. See [Use Policy Groups for SD-Routing Devices](#).

Figure 15: Policy Groups in Cisco Catalyst SD-WAN



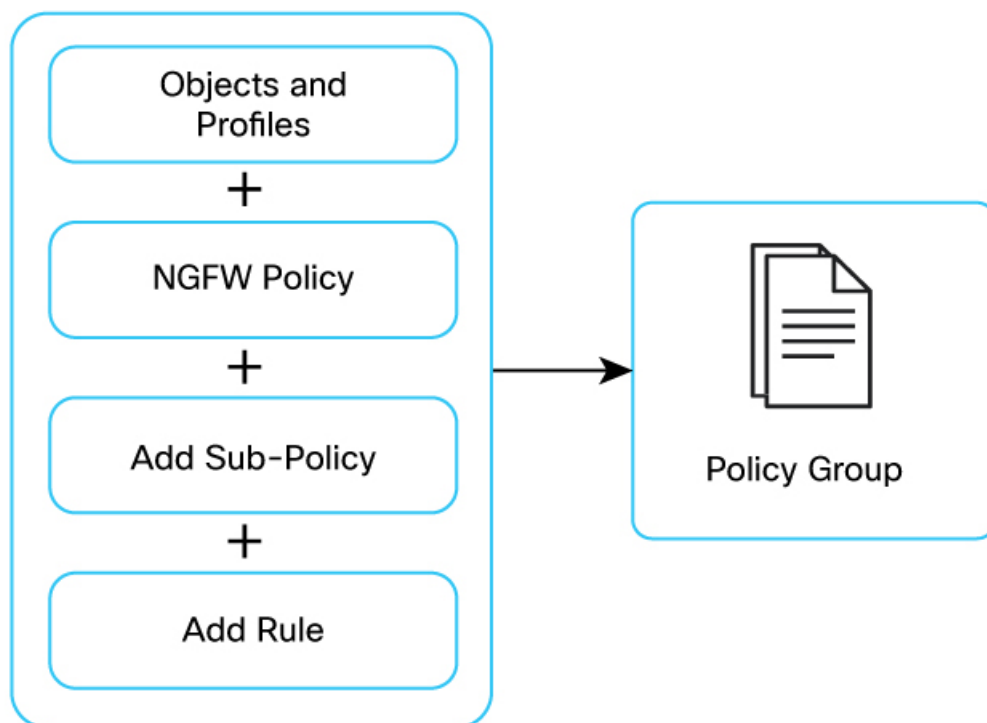
May

### Components of Policy Group

The **Policy Groups** feature consists of these components.

Component	Use	Example
<b>NGFW</b>	<p>Next-Generation Firewall (NGFW) policy offers workflow-based protection for enterprise networks, integrating features such as Application Firewall, IPS, URL Filtering, AMP, TLS Proxy, and DNS security.</p> <p>These policies enable organizations to create rules that manage traffic flow between defined zones.</p>	Create an NGFW policy to monitor and control network traffic from the head office in San Jose to the branch office in Bangalore. Use the policy to detect malicious activity and decrypt encrypted traffic.
<b>SSE</b>	Security Service Edge (SSE) is a cloud-delivered security framework that provides secure access to the internet, cloud services, and private applications, regardless of the user location.	You can configure secure internet access from the data center to a hybrid office.
<b>Objects and Profiles</b>	Objects and Profiles are reusable lists of network entities, such as sites or applications. You define these lists and use them within policies to match traffic or apply actions. This approach simplifies policy configuration and management.	<p>For example, you can create a group of sites. Then, use that group in a policy to match traffic originating from those sites.</p> <p>You can then define actions to take on that matched traffic, such as prioritizing it, routing it through a specific tunnel, or dropping it.</p>

**Figure 16: Policy Group building blocks**



## NGFW

NGFW (Next-Generation Firewall) is a security feature integrated into the SD-Routing solution. It provides enhanced protection beyond traditional firewalls.

NGFW offers capabilities like threat intelligence, application control, and deep packet inspection, along with Zero Trust access, to safeguard against modern cyber threats.

### How to use NGFW

You can set up policies to analyze the contents of network traffic, instead of only examining headers. This allows you to identify and block malicious activity.

## SSE

Cisco Secure Access is a cloud Security Service Edge (SSE) solution. It converges network security services delivered from the cloud to connect a hybrid workforce.

Cisco Catalyst SD-WAN Manager uses REST APIs to gather policy information from Cisco Secure Access and then shares this information with the SD-Routing devices. This solution provides users with seamless, transparent, and secure Direct Internet Access (DIA). It enables users to connect from any device and any location.

### How to use SSE

With an SSE solution, you can configure IPsec tunnels between your device and the SSE provider's network. The SSE provider's cloud platform then inspects your traffic for security before it reaches its destination.

You can configure trackers, such as HTTP probes, within the SSE policy to monitor the health and availability of the tunnels.

## Objects and Profiles

**Objects and Profiles** define and categorize specific values or objects for use within policies.

They act as building blocks for policies, allowing you to match or take actions based on these pre-defined groups. These groups can include parameters such as site **Data Prefix**, **TLOC List**, and other criteria.

### Network Objects

**Network Objects** are groups that when used in conjunction with other policy components define how traffic should be handled.

For example, you can create a *High Priority Applications* group. This group includes all applications that require the highest quality of service. You can use this group in a policy to prioritize traffic from these applications.

### Security Objects

**Security Objects** are groups that identify and categorize network traffic for policy enforcement.

Security objects can be used to define which users or groups have access to certain resources. They can also specify what permissions those users or groups have. Security groups are a common example of security objects, allowing administrators to assign permissions to a group of users rather than individually.

### Security Profiles

Using **Security Profiles** you can create a bundle of policies called **Advanced Inspection Profile**. The **Advanced Inspection Profile** can include sub-policies such as **Intrusion Prevention**, **Advanced Malware Protection**, **TLS Action**, **URL Filtering** and **TLS/SSL Decryption**.

Together, these policies create a unified security policy. You can deploy the unified policy on SD-Routing devices.

## How to use Objects and Profiles

Let us assume a scenario in which you want to prioritize video conferencing traffic from your branch offices.

You can create a **Data Prefix List** in **Objects and Profiles** containing the IP addresses of all your branch office devices. Then, you can create a policy that matches traffic from this list and applies a specific SLA class for video conferencing.

**Figure 17: Data Prefix List**

The image shows a web-based configuration form titled "Data Prefix List". It contains two input fields: "Data Prefix List Name" and "Add Data Prefix". Below the second field is a small text example: "Example: 10.X.X.X/12 separated by commas". At the bottom right of the form are two buttons: "Cancel" and "Save".

## Create an SD-Routing Policy Group

This section explains how to build a policy for your device. For detailed information about **Policy Groups**, see [Using Policy Groups for SD-Routing Devices](#).

When you create a **Policy Group**, it serves as a container for all policies and policy objects that can be configured and deployed to SD-Routing devices. This **Policy Group** can be applied to multiple devices (that are managed by **Configuration Groups**) and sites.

## Create an NGFW Policy

To create an NGFW policy, complete these steps:

- **Create a Sub Policy** to define the conditions that the data traffic flow from the source zone must match to allow the flow to continue to the destination zone.
- **Create a Rule** to specify what actions to take when the traffic inflow meets the criteria specified.
- **Create Additional Settings** to define how to manage firewall resources and perform security logging with minimal impact on packet processing.

See [Configure Firewall Policies for SD-Routing Devices](#). for information on creating an NGFW policy.

## Create an SSE Policy

An SSE (Security Service Edge) policy involves these steps:

- Set up a connection between Cisco Secure Access and the SD-Routing device
- Enable domain lookup for the device
- Configure DNS and NAT
- Configure these details on Cisco Catalyst SD-WAN Manager :
  - Set up cloud credentials.
  - Configure source interface address for loopback interface.

- Create a Tracker to monitor and manage the health and performance of tunnels created for Secure Service Edge (SSE) connections. This tracker helps track the status of IPsec tunnels established between SD-Routing devices and SSE cloud providers such as Cisco Secure Access.
- Create an IPsec tunnel that serves as a communication channel between the SD-Routing device and SSE.
- Create a Region, which specifies the geographical area where SSE services are deployed.
- Create an Interface Pair to configure multiple physical interfaces for a Secure Service Edge (SSE) connection. This allows for redundancy and load balancing.
- Configure traffic redirection.

For more information, see [Configure Secure Access for SD-Routing Devices](#).

## Configure Objects and Profiles

Use **Objects and Profiles** to select policy objects that you can configure and then reference in the **match** or **action** components of a policy.

Think of **Objects and Profiles** as reusable building blocks for your network policies. You can enforce these policies across the entire network. For example, you can create a **URL List** that specifies which websites employees in your organization can access.

**Figure 18: Objects and Profiles**

← Policy Group						
Objects and Profiles						
Network Security objects Security profiles						
Application List						
Add Application List ⓘ						
	Name	Entries	References	Updated By	Last Updated	Action
App Probe Class	test1	audio-video, application-servi...	1	admin	Jun 19, 2023, 3:21:03 PM	<a href="#">✎</a> <a href="#">🗑</a>
Color	box_net_apps	box	0	system	May 27, 2024, 2:13:14 PM	<a href="#">✎</a> <a href="#">🗑</a>
Community list	REAL_TIME_APPS	sip, rtp, skinny, sipvicious	0	system	May 27, 2024, 2:19:34 PM	<a href="#">✎</a> <a href="#">🗑</a>
Data Prefix	sugar_crm_apps	sugarcrm	0	system	May 27, 2024, 2:13:22 PM	<a href="#">✎</a> <a href="#">🗑</a>
Data Prefix IPv6	Google_Apps	android-updates, bloqer, chro...	0	system	Mar 6, 2024, 2:01:03 PM	<a href="#">✎</a> <a href="#">🗑</a>
Expanded community list						
Forwarding Class						

## How is SD-Routing Policy configuration processed

Policy configurations are created using the **Policy Groups** wizard.

A policy is processed in this order:

1. All **match–action** clauses are processed in sequential order, starting from the lowest sequence number upwards.
2. When a **match occurs**, the configured action is performed. The sequential processing stops, and all other match-action pairings are skipped.
3. If a match **does not occur**, the configured entity is subject to the default action configured (by default it is **reject**).

The match conditions of each clause (such as source or destination IP, application, and protocol) are evaluated against the incoming traffic.

# Monitoring and troubleshooting

This section covers details of tools within Cisco Catalyst SD-WAN Manager to observe network performance, identify issues, and resolve problems.

## Understand monitoring and troubleshooting features

The monitoring and troubleshooting features in SD-Routing provide a centralized, streamlined approach to managing your network infrastructure. You can use Cisco Catalyst SD-WAN Manager to view alarms, events, and logs. You can also access built-in troubleshooting tools such as Ping, Traceroute, SSH, and packet capture.

### Monitoring

- **Alarms and Events** : SD-Routing allows you to monitor alarms and events across your network. You can group alarms and events by severity, such as Critical, Major, or Minor, and filter them by object, severity, type, and time.
- **Device Monitoring** : You can monitor device-specific attributes like CPU usage, memory, interface status, VPN, and interface statistics within the SD-WAN Manager.
- **Application Performance Monitoring** : Monitor application performance—such as ART and Media—on SD-Routing devices. Monitoring includes DMVPN tunnels with IKEv2 encryption. This optimizes application performance and reduces downtime.
- **Speed Test** : Utilize the speed test tool to verify network performance between devices.
- **Security dashboard**: Presents a centralized interface for managing and monitoring the security aspects of your Cisco Catalyst SD-WAN network. The dashboard provides a consolidated view of security policies, threat detections, and overall security posture.

### Troubleshooting

- **Built-in Tools** : Diagnostic tools such as Ping, Traceroute, SSH, and packet capture help you diagnose issues.
- **Network-Wide Path Insight (NWPI)** : A diagnostic tool that traces application traffic and analyzes network flows to identify network issues.

## Appendix

This section covers reference information such as FAQ and Feature Parcel details:

### Frequently asked questions

Question	Answer
If deployment fails, how long does it take for the configuration to be rolled back to the previous working state?	Cisco Catalyst SD-WAN Manager waits for five minutes to re-establish the control connection. If the connection is not restored within this time, rollback of the configuration is initiated.

Question	Answer
<b>What happens when new configuration is pushed to a device that has existing configuration?</b>	Cisco Catalyst SD-WAN Manager analyses the new configuration and compares it with existing configuration on the device and only pushes the delta configuration to the device. For example: IP MTU is configured on <i>Device abc</i> but this configuration is not included on <i>Device xyz</i> . Then the configuration on <i>Device xyz</i> is overwritten by the configuration you built using the <b>CLI Configuration</b> dialog. Therefore, IP MTU configuration is not added to <i>Device xyz</i> .
<b>What happens if you delete the configuration from the device after provisioning it?</b>	After provisioning the configuration to a device, if you delete the <b>CLI Configuration Group</b> or <b>CLI Add-On Profile</b> , you can manually add commands to the existing configuration using the SSH terminal. Adding the same <b>CLI Configuration Group</b> or <b>CLI Add-On Profile</b> to the device once again leads to the configuration being pushed for processing, once again.
<b>Why does Cisco Catalyst SD-WAN manager show the status of the device as Locked?</b>	After the device is successfully onboarded, the device terminal is locked and is no longer available for any configuration. Any configurations to be done have performed using Cisco Catalyst SD-WAN Manager. If you want to unlock the configuration, detach the device from the <b>Configuration Group</b> . Then the device terminal is available for configuration.

## Feature Parcels in Cisco Catalyst SD-WAN Manager



### Note

This list is valid till Cisco IOS XE 17.16.1a

Profile Name	Feature		Sub feature
<b>System Profile</b>	<ul style="list-style-type: none"> <li>• AAA</li> <li>• Banner</li> <li>• Global</li> <li>• Logging</li> <li>• NTP</li> </ul>		None
<b>Service Profile</b>	VRF	<ul style="list-style-type: none"> <li>• BGP Routing</li> <li>• OSPF Routing</li> <li>• EIGRP Routing</li> <li>• OSPFv3 IPV4 Routing</li> <li>• OSPFv3 IPV6 Routing</li> <li>• Ethernet Interface</li> <li>• IPSec Interface</li> <li>• DMVPN Tunnel</li> </ul>	<ul style="list-style-type: none"> <li>• Route Policy</li> <li>• ACL IPv4</li> <li>• Object Tracker</li> <li>• Object Tracker Group</li> </ul>



<b>Transport and Management Profile</b>	Global VRF	<ul style="list-style-type: none"> <li>• BGP Routing</li> <li>• OSPF Routing</li> <li>• OSPFv3 IPV4 Routing</li> <li>• OSPFv3 IPv6 Routing</li> <li>• Ethernet Interface</li> <li>• IPSEC Interface</li> <li>• Cellular Interface</li> </ul>	
	Management VRF	<ul style="list-style-type: none"> <li>• Object Tracker</li> <li>• Object Tracker Group</li> </ul>	
	Cellular Controller	<ul style="list-style-type: none"> <li>• Cellular Profile</li> <li>• GPS</li> <li>• Cellular Band Select</li> </ul>	
	VRF	<ul style="list-style-type: none"> <li>• BGP Routing</li> <li>• OSPF Routing</li> <li>• OSPFv3 IPV4 Routing</li> <li>• OSPFv3 IPv6 Routing</li> <li>• Ethernet Interface</li> <li>• IPSec Interface</li> </ul>	<ul style="list-style-type: none"> <li>• Route Policy</li> <li>• ACL IPv4</li> <li>• Object Tracker</li> <li>• Object Tracker Group</li> </ul>
<b>Policy Profile</b>	AS Path Class Map <ul style="list-style-type: none"> <li>• Data Prefix</li> <li>• Prefix</li> <li>• Expanded Community</li> <li>• Extended Community</li> <li>• Mirror</li> </ul> Policer Standard Community VPN		
<b>Other Profile</b>			