Policy Groups Configuration Guide, Cisco IOS XE Catalyst SD-WAN Release 17.x

First Published: 2023-08-15

Last Modified: 2024-08-27

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

CONTENTS

Full Cisco Trademarks with Software License ?

CHAPTER 1 **Read Me First** 1

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

CHAPTER 3 **Policy Groups** 5

- Policy Groups 5
- Information About Policy Groups 6
  - Overview of Policy Groups 6
  - Overview of Policy Group Workflows 6
  - Benefits of Policy Groups 7
  - Information About Color Preference 7
- Supported Devices for Policy Groups 9
- Prerequisites for Policy Groups 10
- Restrictions for Policy Groups 11
- Group of Interest - Policy 11
- Add Policy Group 17
- Application Priority and SLA 18

CHAPTER 4 **Security Policy Using Policy Groups** 25

- Security Policy Using Policy Groups 25
- Information About Security Policy 26
- Enable RBAC for Security Policy 26
- Restrictions for Security Policy 27
- Configure a Security Policy Using a Policy Group 27

Configure a Group of Interest for a Security Policy 27
Configure Embedded Security 37
Configure an Embedded Security Sub-Policy 38
Configure Embedded Security Additional Settings 40
Configure a Secure Internet Gateway 46
Configure a Secure Service Edge 53
Configure DNS Security 60

CHAPTER 5 **Application Catalog** 61
Information About Application Catalog 62
Prerequisites for Application Catalog 62
Configure SD-AVC 63
Configure Cloud Connection 63
Restrictions for Application Catalog 63
Application Catalog Overview 64
View Applications 64
Configure Custom Applications 65
Configure Application List 67
Benefits of Kubernetes Clusters and Kubernetes Services 67
Benefits of Cloud SaaS Feeds 68
Configure, Discover Kubernetes Clusters and Kubernetes Services 68
Configure Cloud SaaS Feed Using Cisco SD-WAN Manager 69
Monitor Kubernetes Clusters and Kubernetes Services 69
Monitor Cloud SaaS Feed 70

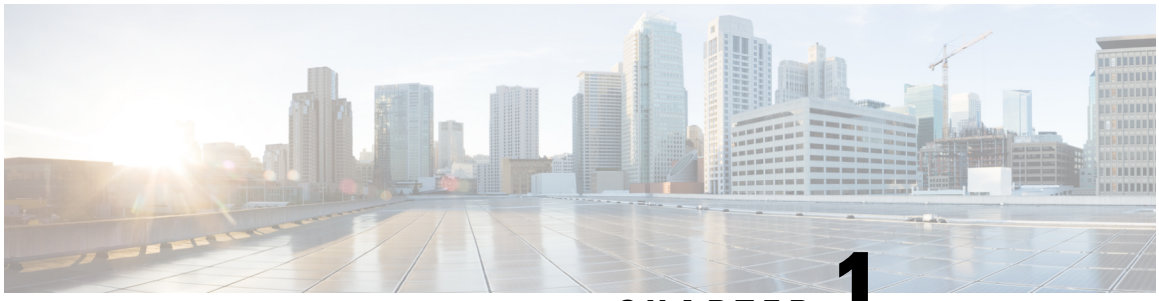
CHAPTER 6 **Policy Compliance** 71
Policy Compliance 71
Information About Policy Compliance 71
Restrictions for the Policy Compliance Check 72
View and Resolve Policy Compliance Issues 72

CHAPTER 7 **Topology** 75
Topology 75
Information About Topology 75

Prerequisites for Topology 76

Create Topology 76

Activate the Topology 81



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

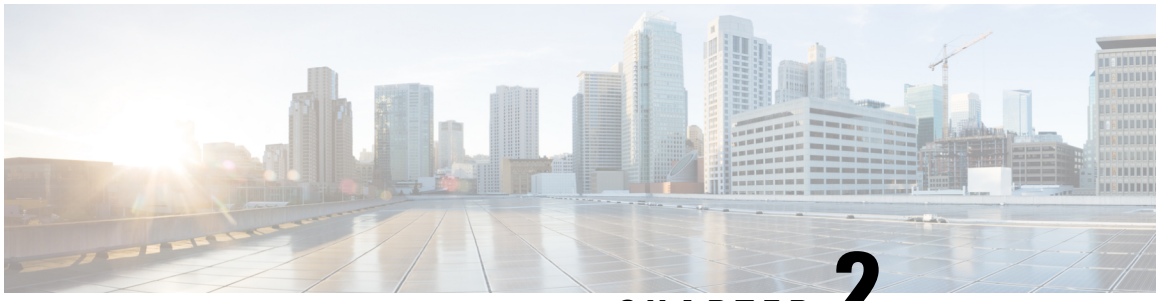
- User Documentation for Cisco IOS XE Catalyst SD-WAN Release 17

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

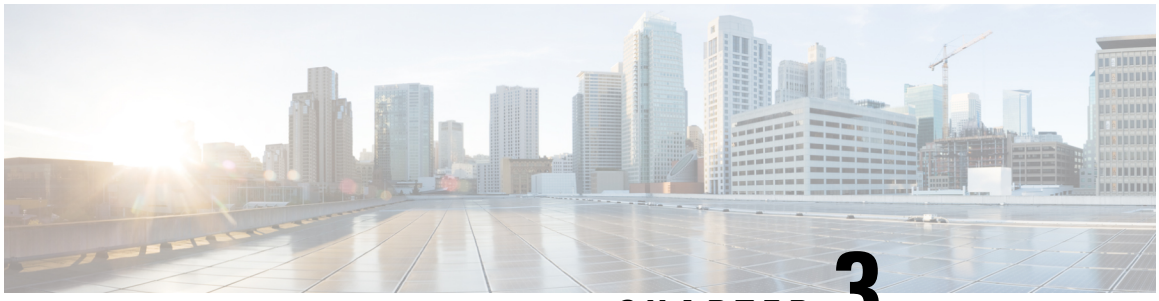
To provide feedback about Cisco technical documentation use the feedback form available in the right pane of every online document.



CHAPTER 2

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

What's New in Cisco IOS XE Catalyst SD-WAN Release 17.x



CHAPTER 3

Policy Groups

- Policy Groups, on page 5
- Information About Policy Groups, on page 6
- Supported Devices for Policy Groups, on page 9
- Prerequisites for Policy Groups, on page 10
- Restrictions for Policy Groups, on page 11
- Group of Interest - Policy, on page 11
- Add Policy Group, on page 17
- Application Priority and SLA, on page 18

Policy Groups

Table 1: Feature History

Feature Name	Release Information	Description
Policy Groups	Cisco IOS XE Catalyst SD-WAN Release 17.12.1a Cisco Catalyst SD-WAN Manager Release 20.12.1	This feature provides a simple, reusable, and structured approach for configuring policies in Cisco Catalyst SD-WAN. You can create a policy group, that is, a logical grouping of policies that is applied to one or more sites or devices at the site in the network. To deploy the policy group to devices, the devices must be managed by a configuration group in Cisco Catalyst SD-WAN. You can configure policies based on features that are required, recommended, or uniquely used, and then combine them to complete a policy configuration. The Deploy Policy Group workflow in Cisco Catalyst SD-WAN provides a guided method to select previously created policy groups and deploy them to sites or devices at the site that is managed by configuration groups.

Feature Name	Release Information	Description
Configure Traffic and Flow Visibility for Application Priority and SLA Policy	Cisco IOS XE Catalyst SD-WAN Release 17.13.1a Cisco Catalyst SD-WAN Manager Release 20.13.1	You can configure settings to enable traffic and flow visibility for the application priority and SLA policy in Cisco Catalyst SD-WAN. This feature allows you to monitor application and traffic flow over IPv4, IPv6, or both networks at the global hierarchy level in Cisco SD-WAN Manager.
Preferred Remote Color in AAR Policy	Cisco IOS XE Catalyst SD-WAN Release 17.15.1a Cisco Catalyst SD-WAN Manager Release 20.15.1	You can set a remote preferred color in the AAR policy to control traffic routing based on the SLA criteria.

Information About Policy Groups

Policy groups simplify the experience of configuring and deploying various policies on Cisco IOS XE Catalyst SD-WAN devices. Policy groups are a collection of different policies that you can configure through workflows and associate with and deploy on different Cisco IOS XE Catalyst SD-WAN devices.

Overview of Policy Groups

Policy Groups provide a simple, reusable, and structured approach for configuring policies and policy objects in Cisco IOS XE Catalyst SD-WAN devices.

Policy groups are a collection of various policies and policy parameters that you can configure quickly through a simplified workflow. Policy groups allows you to configure the basic and necessary policies with defaults to get your systems up and running. The more advanced user can switch to the **Advanced** layout to take complete control and configure detailed policy parameters such as service-level agreement (SLA) class, Quality of Service (QoS) Maps, and Match-Action parameters pertaining to the traffic policy. After creating a policy group, you can associate it with one or more sites or a single device at the site in the network and deploy it on devices managed by configuration groups.

After you've configured a policy group, you can deploy it on Cisco IOS XE Catalyst SD-WAN devices by using the Overview of Policy Group Workflows.

For more information about Cisco Catalyst SD-WAN policy and policy architecture, see *Policy Overview*.

Overview of Policy Group Workflows

The policy group workflow guides you in creating a policy group for one or more sites or a single device at the site in the network that is managed by configuration groups in Cisco Catalyst SD-WAN. The workflow provides you with an improved configuration and troubleshooting experience. The workflow has the following features:

- You can review the various configuration values on a single page within the workflow.

- You can easily identify and fix incorrect values that appear highlighted in red. In addition, an asterisk that is adjacent to a field name helps you identify the mandatory values within the workflow.

Deploy Policy Group Workflow

You can access the workflow by choosing **Workflows** > **Deploy Policy Group** menu in Cisco SD-WAN Manager.

The **Deploy Policy Group** workflow enables you to associate devices with a previously created policy group and deploy the policy group to the selected devices. You can review device configurations to further add Site IDs and other variables that must be provided as part of a policy group before deploying the policy group.

Note After you deploy a policy group, any change to the policy group is deployed to the Cisco SD-WAN Controller.

Benefits of Policy Groups

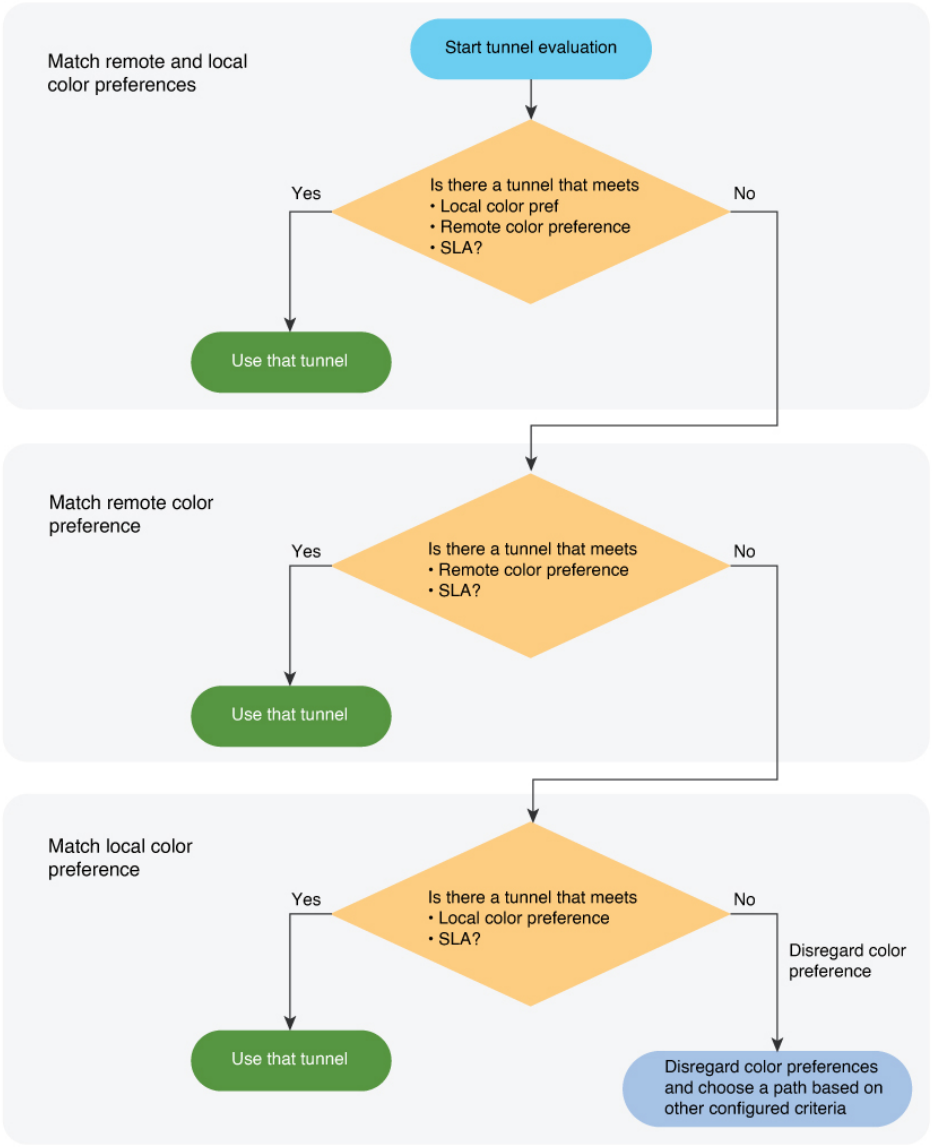
- Simplified user experience through an intuitive UI that allows you to quickly configure the basic policies that are required to get your Cisco Catalyst SD-WAN deployments up and running.
- Option to edit policy groups based on the changing needs of your network and save the configuration. You can choose to deploy these changes only when needed - during maintenance windows or in off-production hours.
- A **Preview CLI** option to preview the difference in configuration for relevant devices such as Cisco IOS XE Catalyst SD-WAN device and Cisco SD-WAN Controller in one location.
- Workflows to deploy policy groups.

Information About Color Preference

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.15.1a and Cisco Catalyst SD-WAN Manager Release 20.15.1

The AAR policy enables you to use TLOC color preferences to determine how a device chooses a tunnel for routing traffic. You can configure a preferred local TLOC color and a preferred remote TLOC color, referring to the local and remote TLOCs associated with a tunnel. When multiple tunnels are available, the device prioritizes tunnels according to the color preferences. This flowchart shows the logic.

Figure 1: Color Preference Logic



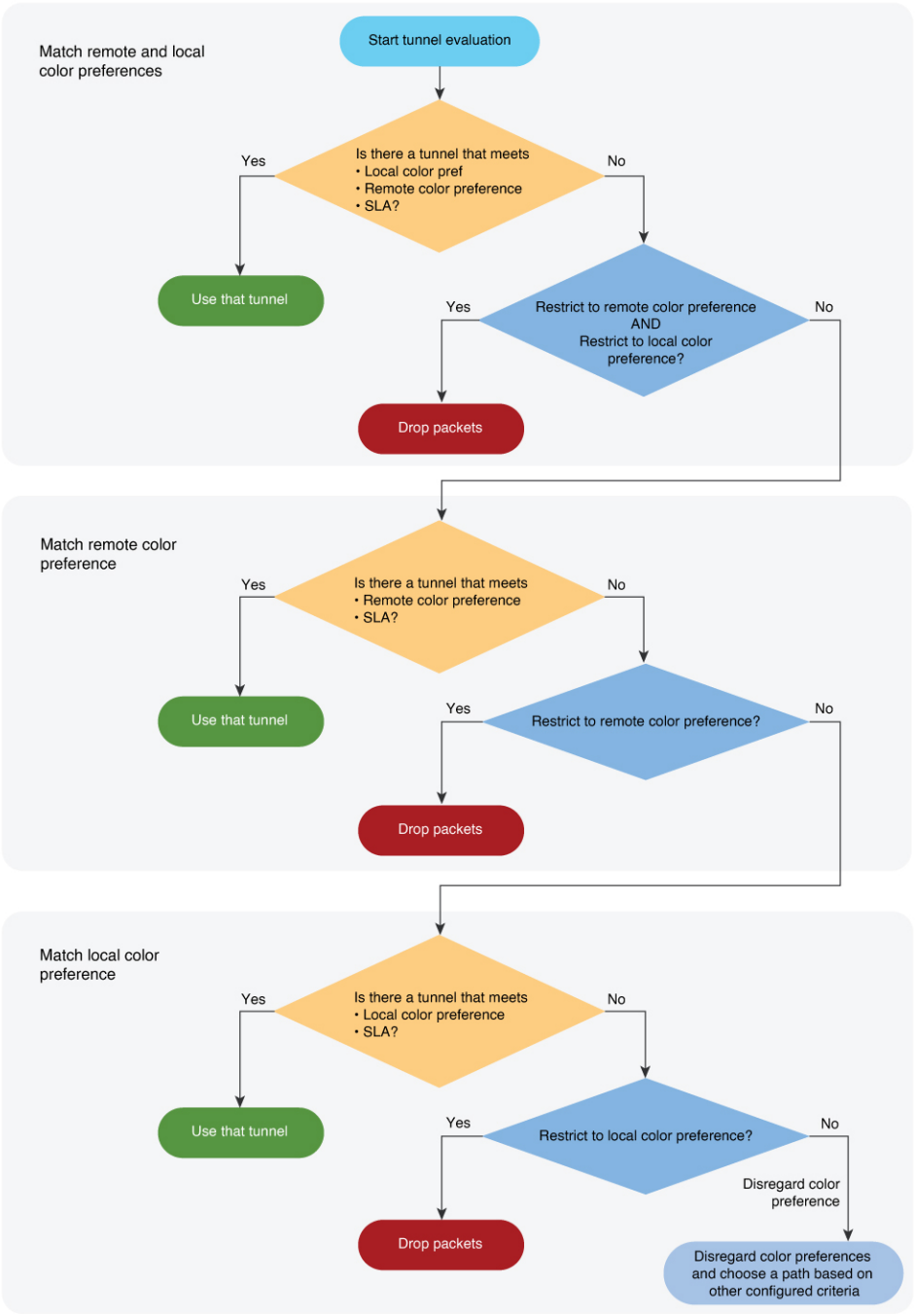
For more information, see Application Priority and SLA.

For configuring remote preferred color policies using **Configuration** > **Policies** see Configure Traffic Rules.

Restricting to a Color Preference

You can restrict the choice of a tunnel to include only tunnels that meet the configured color preferences. The options are **Restrict to Remote Color** and **Restrict to Preferred Color Group**. If no tunnels meet the criteria, the device drops the traffic. This flowchart shows the logic of choosing a tunnel when restricting to the color preferences.

Figure 2: Color Preference Logic, Restricting to Local or Remote Color



Supported Devices for Policy Groups

This feature is supported only on Cisco IOS XE Catalyst SD-WAN devices.

Prerequisites for Policy Groups

Before you begin configuring policy groups, ensure that the following requirements are met:

- Minimum software version for Cisco IOS XE Catalyst SD-WAN devices: Cisco IOS XE Catalyst SD-WAN Release 17.8.1a

  Minimum software version for Cisco SD-WAN Manager: Cisco Catalyst SD-WAN Manager Release 20.12.1

- Ensure that these devices are deployed and managed using a configurations group. For more information about creating configuration groups, see Configuration Groups and Feature Profiles.

Configure RBAC for policy groups

Ensure that the granular role-based access control (RBAC) for policy groups is specified by expanding it. With specific permissions to the usergroup, ensure that you are able to access policy groups from **Configuration** > **Policy Groups**.

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Manage Users** > **User Groups**.
2. Click **Add User Group**.
3. Enter **User Group Name**.
4. Select the **Read** or **Write** check box against the **Policy Group** and **Device** feature that you want to assign to a user group.
5. Click **Add**.

Configure RBAC for Application Priority Policy

Ensure that the granular RBAC for the application priority policy is specified by expanding it. With the set permissions to the usergroup, ensure that you are able to access the application priority policy from **Configuration** > **Policy Groups**.

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Manage Users** > **User Groups**.
2. Click **Add User Group**.
3. Enter **User Group Name**.
4. Select the **Read** or **Write** check box against the following features that you want to assign to a user group:
   - **Feature Profile** > **Application Priority** > **Qos Policy**
   - **Feature Profile** > **Application Priority** > **Traffic Policy**
   - **Feature Profile** > **Policy Object** > **App List**
   - **Feature Profile** > **Policy Object** > **SLA Class**
   - **Feature Profile** > **Policy Object** > **TLOC**
   - **Feature Profile** > **Policy Object** > **App Probe**
   - **Feature Profile** > **Policy Object** > **Preferred Color Group**

- **Feature Profile** > **Policy Object** > **Class**
- **Feature Profile** > **Policy Object** > **Data Prefix**
- **Feature Profile** > **Policy Object** > **Data Ipv6**
- **Feature Profile** > **Policy Object** > **Policer**

5. Click **Add**.

Restrictions for Policy Groups

- The Application Priority and SLA workflow does not support custom applications.
- You cannot deploy policy groups to devices that are not already managed by a configurations group.
- The forwarding class in localized policy is not supported.
- An error occurs when a duplicate parcel name (for example, Site27-VPN1) exists in another configuration group. Verify existing parcel names across all groups and modify the intended name to ensure exclusivity. Use descriptive naming conventions to prevent conflicts.

Group of Interest - Policy

Group of interest provides a list of related policy objects that you can configure and call in the match or action components of a policy. Click **Group of Interest** to create new objects for the policy group as described in the following sections:

Application

1. Click **Application**.
2. Click **Add Application** .
3. From the **Application/Application family list** drop-down, choose the required applications or application families.
4. Click **Save**.

A few application lists are preconfigured. You cannot edit or delete these lists.

Microsoft_Apps: Includes Microsoft applications, such as Excel, Skype, and Xbox. To display a full list of Microsoft applications, click the list in the **Entries** column.

Google_Apps: Includes Google applications, such as Gmail, Google Maps, and YouTube. To display a full list of Google applications, click the list in the **Entries** column.

App Probe Class

1. Click **Add App Probe Class**.
2. In the **App Probe** dialog box, specify the following:

Field	Description
Probe Class Name	Enter a name for the probe class.
Forwarding Class	Choose the forwarding class from the drop-down list.
Color	Choose the color from the drop-down list.
DSCP	Enter the DSCP value.

3. You can add more entries if needed by clicking on + icon.
4. Click **Save**.

Color

1. Click **Color**.
2. Click **New Color List** and specify the following:

Field	Description
Color List Name	Enter a name for the list.
Select Color	Choose one or more color lists types from the drop-down list.

3. Click **Add**.

To configure multiple colors in a single list, you can choose multiple colors from the drop-down list.

Community List

A community list is used to create groups of communities to use in a match clause of a route map. A community list can be used to control which routes are accepted, preferred, distributed, or advertised. You can also use a community list to set, append, or modify the communities of a route.

1. Click **Community List**.
2. Click **Add Community List** and specify the following:

Field	Description
Community List Name	Enter a name of the community list.

Field	Description
Add Community	Enter one or more communities separated by commas. • *aa*:*nn*: Autonomous System (AS) number and network number. Each number is a 2-byte value with a range from 1 to 65535. For example, 65526. • **internet**: Routes in this community are advertised to the internet community. This community comprises all BGP-speaking networking devices. • **local-as**: Routes in this community are not advertised outside the local AS number. • **no-advertise**: Attaches the NO_ADVERTISE community to routes. Routes in this community are not advertised to other BGP peers. • **no-export**: Attaches the NO_EXPORT community to routes. Routes in this community are not advertised outside the local AS or outside a BGP confederation boundary. To configure multiple BGP communities in a single list, include multiple **community** options, specifying one community in each option.

3. Click **Save**.

Data Prefix

1. Click **Data Prefix**.
2. Click **Add Data Prefix**.
3. In the **Data Prefix list** dialog box, specify the following:

Field	Description
Data Prefix List Name	Enter a name for the data prefix list.
Add Data Prefix	Enter one or more data prefixes separated by commas.

4. Click **Save**.

Data Prefix IPv6

1. Click **Data Prefix IPv6**.
2. Click **Add Data Prefix IPv6**.
3. In the **Data Prefix List** dialog box, specify the following:

Field	Description
Data Prefix List Name	Enter a name for the IPv6 data prefix list.
Add Data Prefix	Enter one or more IPv6 data prefixes separated by commas.

4. Click **Save**.

Expanded Community List

1. Click **Expanded Community List**.
2. Click **Add Expanded Community List** and specify the fiollowing:

Field	Description
Community List Name	Enter a name for the community list.
Add Community	Specify details of the expanded community list that is used to filter communities using a regular expression.

Forwarding Class

1. Click **Add Forwarding Class** and specify the following:

Field	Description
Forwarding Class	Enter a name for the forwarding class.
Queue	Choose a value for the queue from the drop-down list.

2. Click **Save**.

Policer

1. Click **Policer**.
2. Click **Add Policer** and specify the following:

Field	Description
Policer List Name	Enter a name for the policer list.
Burst (bytes)	Enter the maximum traffic burst size. The range is from 15,000 to 10,000,000 bytes.
Exceed	Choose the action to take when the burst size or traffic rate is exceeded. The options are: • Drop: sets the packet loss priority (PLP) to low • Remark: sets the packet loss priority (PLP) to high
Rate	Enter the maximum traffic rate, a value from 8 through 10^11 bits per second (bps).

3. Click **Save**.

Preferred Color Group

1. Click **Add Preferred Color Group**.
2. In the **Preferred Color Group Name** field, enter a name for the preferred color group.
3. Choose the color preference and path prefernce for the primary, secondary, and tertiary colors from the **Color Preference** and the **Path Preference** drop-down lists.

Field	Description
Preferred Color Group Name	Enter a name for the preferred color group.
Color Preference	Choose the color preference from the drop-down list. You can choose multiple colors.
Path Preference	Choose the path preference from the drop-down list. The options are: • Direct Path • Multi Hop Path • All Paths

4. Click **Save**.

Prefix List

1. Click **Prefix List**.
2. Click **Add Prefix List** and specify the following:

Field	Description
Prefix List Name	Enter a name for the IPv4 prefix list.
Add Prefix	Enter one or more IPv4 prefixes separated by commas.

3. Click **Save**.

Prefix List IPv6

1. Click **Prefix List IPv6**.
2. Click **Add Prefix List** and specify the following:

Field	Description
Prefix List Name	Enter a name for the IPv6 prefix list.
Add Prefix	Enter one or more IPv6 prefixes separated by commas.

3. Click **Save**.

SLA Class

1. Click **SLA Class**.
2. Click **Add SLA Class** and specify the following:

Field	Description
SLA Class List Name	Enter a name of the SLA class list.
Loss (%)	Enter the maximum packet loss on the connection, a value from 0 through 100.
Latency	Enter the maximum packet latency on the connection, a value from 1 through 1,000 milliseconds.
Jitter	Enter the maximum jitter on the connection, a value from 1 through 1,000 milliseconds.
App Probe Class	Choose the app probe class from the drop-down list or click **Create New** to create one.
Fallback Best Tunnel	Choose this option to enable the best tunnel criteria.

3. Click **Save**.

TLOC List

1. Click **TLOC List**.
2. Click **Add TLOC List** and specify the following:

Field	Description
List Name	Enter a name for the TLOC list.
TLOC IP	Specify the IP address for TLOC.
Color	Choose the color from the drop-down list.
Encapsulation	Choose the value from the drop-down list. The options are: • IPSec • GRE
Preference	Choose a preference to associate with the TLOC. The range is 0 to 4294967295.

3. Click **Save**.

Add Policy Group

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Policy Groups** > **+ Add Policy Group**.
2. Enter a **Policy Group Name**, choose a **Solution** from the drop-down list and provide a description (optional).
3. Click **Create**.

Note If you have already created a policy group, click the policy group from the list of available policy groups to edit.

Table 2: Policy group parameters

Field	Description
Policy Group Name	Specify the name of the policy group. This field is mandatory and can contain only uppercase and lowercase letters, the digits 0 through 9, hyphens (–), and underscores (_). It cannot contain spaces or any other characters.
Description	Provide a description for the policy group. It can contain up to 2048 characters including spaces.
Policy	
Application Priority & SLA	Choose an application priority for the policy group from the drop-down list. Click **Create New** to create a new application priority.
Embedded Security	Choose an embedded security policy from the drop-down list. Click **Create New** to create a new embedded security policy by selecting a configuration group, creating firewall policies, and other configuration settings.
Secure Internet Gateway	Configure the Secure Internet Gateway (SIG) tunnels before you apply a data policy for redirecting application traffic to an SIG. Select a Secure Internet Gateway (SIG) policy from the drop-down list. Click **Create New** to create a new SIG policy.
DNS Security	Select a DNS Security policy from the drop-down list. Click **Create New** to create a new DNS Security policy.

1. Click **Save** to save your configuration.

2. Click the pencil icon to select or unselect devices to associate or dissociate with the policy group.

Note Starting from Cisco Catalyst SD-WAN Manager Release 20.15.1, click **+Add** adjacent to **Associated** field to select or unselect devices to assoicate or dissociate with the policy group. In the associate devices workflow, you can choose devices based on **Regions** and not just **Sites**.

3. Click **Deploy** to select sites and deploy the policy group..

To delete a policy group, select the ellipsis icon (**...**) to the right of the policy group and click **Delete**.

Application Priority and SLA

The application priority and SLA policies allows you to configure the app route policy, data policy, and QoS Map policies that route and prioritize traffic for best performance. All the basic information is preconfigured. You can specify a name and description for a policy group and configure the basic policy values. You can quickly configure the basic values to get started with the traffic policy. Configuring this policy provides the following benefits:

- Manage and customize bandwidth allocations.
- Prioritize applications based on their relevance to your business.

Create an Application Priority and SLA Policy

Click **+ Application priority & SLA policy** to create a policy and configure the values. To edit an existing policy, click the ellipsis icon (**...**) next to the application priority and SLA policy under **Action** and click **Edit**.

Choose one of the following options and configure the values that are based on the likely business relevance of the applications, and to give higher priority to business-relevant applications:

- **Gold** (Business-relevant): Likely to be important for business operations, for example, WebEx software.
- **Silver** (Default): No determination of relevance to business operations.
- **Bronze** (Business-irrelevant): Unlikely to be important for business operations, for example, gaming software.

Within each of the business-relevance categories, the workflow groups the applications into application lists, such as broadcast video, multimedia conferencing, VoIP telephony, and so on.

Table 3: Cisco Catalyst SD-WAN Fabric Traffic Policy

Field	Description
Preferred Path	To configure a preferred path, choose one or more colors of the data plane tunnel or tunnels from the drop-down list. Traffic is load-balanced across all the tunnels. If no tunnels match the SLA, data traffic is sent through any available tunnel. The preferences apply in order of priority to determine the path or color for forwarding traffic.
When SLA not met	Choose **Strict/Drop** to perform strict matching of the SLA class. If no data plane tunnel is available that satisfies the SLA criteria, traffic is dropped. Choose **Fallback to best path** to configure the best available tunnel to avoid a packet drop. This is the default. **Backup Path**: Path for traffic to use if the primary path fails.
Backup Path	To configure an alternate path for traffic flow, choose a path from the drop-down list.
Traffic Filtering	Click **Edit** to view and update app classification based on the business relevance. Choose a service provider class option and drag and drop the applications into different classes such as Gold or Bronze and click **Save** to update the configuration.
SLA	Add the SLA class in the traffic policy. Click **Edit** to configure the SLA class by adjusting the values for Loss (%), Latency (ms), or Jitter (ms) for the traffic policy.
QoS Queues	Click **Add QoS Policy** to add a QoS queue. Click **Edit** to configure the QoS Queues. Choose one of the following values for the QoS queuing model: • **4 Queues** • **5 Queues** • **6 Queues** • **8 Queues**

Table 4: Internet Offload Traffic

Field	Description
Secure Internet Gateway	Choose an application or application family list to tunnel traffic through a Secure Internet Gateway. Enable **Fallback to routing** for traffic to undergo normal routing if the SIG tunnels are down.
Direct Internet Access	Select an application or application family list to allow direct internet access. Enable **Fallback to routing** for traffic to undergo normal routing if Direct Internet Access (DIA) is not available.

Table 5: Apply Policy

Field	Description

Target	Configure the following parameters:
	• **Direction**: Choose the direction for applying the policy:
	  • **All**: Bidirection traffic flow
	  • **Service**: Incoming traffic from service.
	  • **Tunnel**: Incoming traffic from the tunnel.
	• **VPN**: Choose a target VPN from the drop-down list.
	• **Interface**: Specify a value or a variable for the Ethernet interface or DSL PPPoE interface type for applying the QoS policy.

Advanced Layout

The advanced view provides further options to configure the traffic policy along with rules, service level agreement (SLA) class, and QoS Map. Click the **Advanced** button on the top-right corner of the window to swtich to the advanced view.

Note If you make changes to the application priority and SLA policies and switch to the advanced layout, the changes are retained. You cannot switch back to the default view.

Based on the values you configure in the workflow, a policy profile and the relevant policy objects are created in the back-end when the workflow is completed. Similarly, you can configure traffic filtering and rules by creating the match and action conditions of a policy. You can also configure the app route policy SLA class and create customized QoS queues.

Table 6: Add Traffic Policy

Field	Description
Policy Name	Specify a name for the traffic policy.
VPN	Choose a VPN from the drop-down list.
Direction	• Choose the direction for applying the policy: • **All**: Bidirectional traffic flow • **Service**: Incoming traffic from service • **Tunnel**: Incoming traffic from tunnel

Table 7: Add Rules

Field	Description
Sequence	The sequence number of the rule.
Name	Specify a name for the rule.
Protocol	Choose a protocol from the drop-down list: • **IPv4** • **IPv6** • **Both**
Match	Choose a value for the match condition from the available options. For more information about match conditions, see the **Match Condition** table in the section *Configure Traffic Rules* in *Centralized Policy*.
Action	Choose a value for the action to take if the policy matches, from the available options. For more information about action values, see the **Action Condition** table in the section *Configure Traffic Rules* in *Centralized Policy*.
Base Action	Choose one of the following base actions for the packets based on the rules: • **Accept** • **Drop**

Table 8: Action Parameters on Policy Groups

Field	Description
Secure Service Edge	Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.13.1a and Cisco Catalyst SD-WAN Manager Release 20.13.1 Redirect application traffic to a Secure Service Edge instance. For more information on configuring Automatic tunnels on Cisco Secure Access, see Automatic Tunnels . Check the **Fallback to Routing** check box to route internet-bound traffic through the Cisco SD-WAN overlay when all Secure Service Edge tunnels are down.
Remote Preferred Color	Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.15.1a and Cisco Catalyst SD-WAN Manager Release 20.15.1 You can set a preferred remote color in the AAR policy to control traffic routing based on the application list. Use the **Restrict to Remote Color** option to drop traffic if the selected remote color does not meet the SLA.

To rearrange match–action pairs in the route policy, drag them to the desired position and click **Save Match and Actions**.

Table 9: SLA Class Components

Parameter	Description
jitter *milliseconds*	The maximum jitter on the connection Range: 1–1000 milliseconds
latency *milliseconds*	The maximum packet latency on the connection Range: 1–1000 milliseconds
loss *percentage*	The maximum packet loss on the connection Range: 1–100 percent

Starting from Cisco IOS XE Catalyst SD-WAN Release 17.14.1a, the SLA class loss, latency, and jitter values are as follows:

- Default values: Loss 5%, latency 500 ms, jitter 500 ms
- Business relevant values: Loss 2%, latency 300 ms, jitter 60 ms

- Business irrelevant values: Loss 10%, latency 600 ms, jitter 600 ms
- Bulk data values: Loss 5%, latency 500 ms, jitter 500 ms

For more information about SLA class and its components, see SLA Classes in *Application-Aware Routing*.

Table 10: QoS Queue

Field	Description
Queuing Model	Choose a value from the drop-down list for the queuing model.
Policy Name	Provide a name for the policy.
Interface	Specify a value for the interface.
Forwarding class	Choose a value for the forwarding class from the drop-down list.
Bandwidth %	Specify the maximum bandwidth. The range is 1–99.
Drops	Choose a value for the drop type from the following options: • **Random Early** • **Tail**
Scheduling type	Specify how to prioritize data packets for transmission to the destination by configuring the schedule type. The default is Weighted Round Robin (WRR).

For more information about QoS, see the section *Cisco Catalyst SD-WAN Forwarding and QoS Overview* in *Forwarding and QoS*.

Monitor traffic flow

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, Cisco Catalyst SD-WAN Manager Release 20.13.1.

You can configure collectors by clicking the **Additional Settings** tab, which provide options to monitor traffic flow on incoming packets in the LAN for application and flow visibility over IPv4, IPv6, or both network addresses.

Before you begin, ensure that you have configured Cflowd collector details in the Cisco SD-WAN Manager menu from **Configuration** > **Network Hierarchy** > **Collectors** > **Cflowd**.

Note The Cflowd configuration applies to the global level and not the site level.

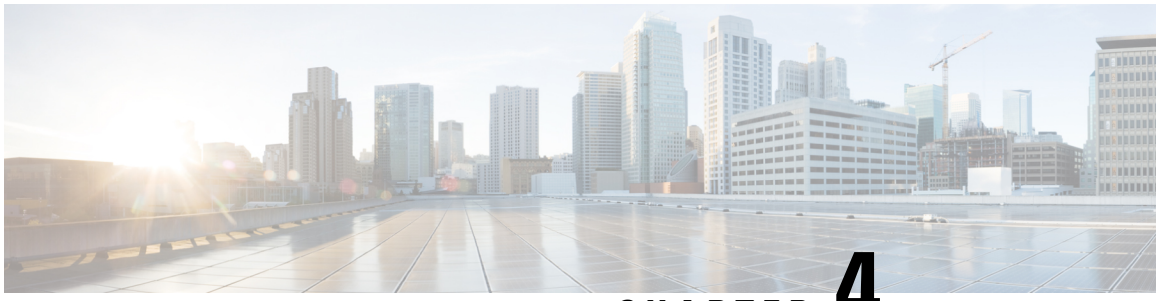
The additional settings that you configure are applied to the Cisco SD-WAN Controllers while deploying the application priority and SLA policy. For more information about configuring Cflowd, see the section Configure Cflowd in *Configure Collectors in a Network Hierarchy*.

Enable traffic flow monitoring

To enable traffic flow monitoring while configuring an application priority & SLA policy, click the **Additional Settings** tab in the top-right corner and configure the following values:

Table 11: Additional Settings

Field	Description
Application Visibility	Monitor all the applications running in all VPNs over IPv4, IPv6, or both networks in the LAN.
Flow Visibility	Monitor traffic flow over IPv4, IPv6, or both network addresses in the LAN.



CHAPTER 4

Security Policy Using Policy Groups

- Security Policy Using Policy Groups, on page 25
- Information About Security Policy, on page 26
- Enable RBAC for Security Policy, on page 26
- Restrictions for Security Policy, on page 27
- Configure a Security Policy Using a Policy Group, on page 27
- Configure a Group of Interest for a Security Policy, on page 27
- Configure Embedded Security, on page 37
- Configure an Embedded Security Sub-Policy, on page 38
- Configure Embedded Security Additional Settings, on page 40
- Configure a Secure Internet Gateway, on page 46
- Configure a Secure Service Edge, on page 53
- Configure DNS Security, on page 60

Security Policy Using Policy Groups

Table 12: Feature History

Feature Name	Release Information	Description
Security Policy Using Policy Groups	Cisco IOS XE Catalyst SD-WAN Release 17.12.1a Cisco Catalyst SD-WAN Manager Release 20.12.1	This feature provides a simple, reusable, and structured approach for configuring security policies in Cisco Catalyst SD-WAN. You can create a security policy, that is, a logical grouping of policies that is applied to one or more sites or a single device at a site in the network. To deploy the policy group to devices, the devices must be managed by a configuration group in Cisco Catalyst SD-WAN. The Deploy Policy Group workflow provides a guided method to choose previously created policy groups and deploy them to sites or a single device at a site that is managed by configuration groups.

Feature Name	Release Information	Description
Configure Secure Service Edge	Cisco IOS XE Catalyst SD-WAN Release 17.13.1a Cisco Catalyst SD-WAN Manager Release 20.13.1	With this feature you can configure a Secure Service Edge (SSE) profile using Cisco Secure Access as the provider. You can associate the SSE profile to a policy group to deploy to a device.

Information About Security Policy

Configuring security policies using policy groups simplifies the experience of configuring and deploying policies on Cisco IOS XE Catalyst SD-WAN devices. Use a workflow to configure policies and associate them with devices in the network.

The **Policy Groups** page includes the following:

- **Policy Group** (see Policy Group chapter)
- **Application Priority & SLA** (see Policy Group chapter)
- **Embedded Security**
- **Secure Internet Gateway (SIG)**
- **DNS Security**

Enable RBAC for Security Policy

To create a policy group and security feature profiles using configuration groups, role-based access control (RBAC) must provide read and write permissions on the following profiles to access each feature. Set the permissions of the user group to enable access to policy groups from **Configuration** > **Policy Groups**.

1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Manage Users** > **User Groups**.
2. Click **Add User Group**.
3. Enter **User Group Name**.
4. Check a **Read** or **Write** check box for the **Policy Group**, **Device** and **Deploy** feature that you want to assign to a user group.
5. Check a **Read** or **Write** check box for the following features that you want to assign to a user group:
   - **Feature Profile** > **DNS Security** > **DNS Policy**
   - **Feature Profile** > **Sig Security** > **Sig Policy**
   - **Feature Profile** > **Embedded Security** > **Legacy Policy**
   - **Feature Profile** > **Embedded Security** > **NGFirewall**
   - **Feature Profile** > **Embedded Security** > **Policy**

- **Feature Profile** > **Policy Object** > **Advanced Inspection Profile**

  The **Advanced Inspection Profile** has the following subfeature profiles:

  - Advanced Malware Protection
  - Intrusion Prevention
  - SSL Decryption
  - SSL Decryption Profile
  - URL Filtering

6. Click **Add**.

Restrictions for Security Policy

From Cisco IOS XE Catalyst SD-WAN Release 17.14.1a and Cisco Catalyst SD-WAN Manager Release 20.14.1, security policy supports matching traffic using a custom application in a custom-defined application list. In earlier releases, this is not supported.

Configure a Security Policy Using a Policy Group

Using the **Create Security Policy** workflow, you can create a security policy, add sub-policy, add rules to existing sub-policies, and so on.

1. From the Cisco SD-WAN Manager menu, choose **Workflows** > **Workflow Library** > **Create Security Policy**. Alternatively, choose **Configuration** > **Policy Groups**.
2. Click **Embedded Security**.
3. On the **Embedded Security** page, click **Add Security Policy**. This launches the Security Policy workflow.
4. Enter **Policy Name** and **Description** and click **Next**.
5. On the **Select the optional Configuration Group to associate with the security policy** page, choose the configuration groups and click **Next**.
6. Click **Add Sub-Policy**. Refer to the steps used in the procedure, Configure an Embedded Security Sub-Policy, on page 38.
7. Click **Submit**.You can view the new security policy in the **Embedded Security** tab.

Configure a Group of Interest for a Security Policy

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Policy Groups** > **Group of Interest**.
2. Click the **Security** tab. The list of security objects and profiles appears.

Use the following tables to configure a different group of lists for security policy:

Application

Field	Description
Application List Name	Name of the application list. **Note** See the information about custom applications in Restrictions for Security Policy.
Applications	Choose one or more application types from the drop-down list. For example, Third Party Control, ABC News, Microsoft Teams, and so on. Choose one or more application family types from the drop-down list. For example, application-service, audio_video, authentication, behavioral, compression, database, encrypted, and so on.

Data Prefix

Field	Description
Data Prefix List Name	Name of the prefix list.
Data Prefix	The data prefix value.

Local Domain

Field	Description
Local Domain List Name	Name of the local domain list.
Local Domain	The local domain values separated by comma. For example, cisco.com.

FQDN (Fully Qualified Domain Name)

The FQDN is intended to be used for matching standalone servers in data centers or a private cloud. When matching public URLs, the recommended match action is **drop**. If you use **inspect** for public URLs, you must define all related sub URLs and redirect URLs.

Field	Description
FQDN List Name	Name of the FQDN list.
FQDN	The URL names separated by comma. For example, cisco.com.

Signature

The signature set blocks vulnerability with a Common Vulnerability Scoring System (CVSS) score that is greater than or equal to 9. It also blocks Common Vulnerabilities and Exposures (CVEs) published in the last two years and that have the rule categories: Malware CNC, Exploit Kits, SQL Injection or blocked list.

Field	Description
IPS Signature List Name	Name of the IPS signature list.
IPS Signature	The signatures in the format `Generator ID:Signature ID`, separated with commas. For example, 1234:5678. Range is 0 to 4294967295

URL Allow

List-based filtering allows the user to control access by permitting or denying access based on allowed or blocked lists. Here are some important points to note about these lists:

- URLs that are allowed are not subjected to any category-based filtering.
- If the same item is configured under both the allowed and blocked list, the traffic is allowed.
- If the traffic does not match either the allowed or blocked lists, then it is subjected to category-based and reputation-based filtering.

Field	Description
Allow URL List Name	Name of the Allow URL list.
Allow URL	The URLs to allow.

URL Block

List-based filtering allows the user to control access by permitting or denying access based on allowed or blocked lists.

Field	Description
Block URL List Name	Name of the Block URL list.
Block URL	The URLs to block.

Zone

Field	Description
Zone List Name	Name of the zone list.

Field	Description
VPN	Choose to configure zones with zone type as **VPN**. Add the VPNs to the zones from the drop-down list. The options are: • Payment Processing Network • Corporate Users • Local Internet for Guests • Physical Security Devices
Interface	Choose to configure zones with zone type as **Interface**. Add the interfaces to the zones from the **Add Interface** drop-down list. The options are: • Ethernet • FastEthernet • FiveGigabitEthernet • FortyGigabitEthernet • GigabitEthernet • HundredGigE

Port

Field	Description
Port List Name	Name of the port list.
Port	The port values separated by comma. The range is 0 to 65530.

Protocol

Field	Description
Protocol List Name	Name of the protocol list.
Protocols	Select one or more protocol names from the drop-down list. For example, snmp, tcp, udp, icmp, echo, telnet, and so on.

Geo Location

Field	Description
Geo Location List Name	Name of the geolocation list.
Geo Location	Select one or more geo locations from the drop-down list. For example, Africa, Antartic, Asia, Europe, and so on.

The security group of interest has the following profiles:

- Advanced Inspection Profile
- Intrusion Prevention Policy
- URL Filtering
- Advanced Malware Protection
- TLS/SSL Profile
- TLS/SSL Decryption

Advanced Inspection Profile

Field	Description
Profile Name	Name of the advanced inspection profile.
Description	The description of the profile.
Select an Intrusion Prevention	Choose an intrusion prevention option from the drop-down list.
Select an URL Filter	Choose a URL filter from the drop-down list.
Select an Advanced Malware Protection	Choose an advanced malware protection.
TLS Action	Choose the TLS action. The options are: • Decrypt • Pass Through • Do not Decrypt

Intrusion Prevention Policy

Field	Description
Profile Name	Name of the intrusion prevention policy.

Field	Description
Signature Set	Choose a signature set that defines the rules for an evaluating traffic from the **Signature Set** drop-down list. The following options are available. • **Balanced**: Provides protection without significant effect on system performance. • **Connectivity**: Less restrictive and provide better performance by imposing fewer rules. • **Security**: Provides more protection than Balanced but with an impact on performance.
Inspection Mode	Choose the inspection mode. The following options are available: • Detection: Choose this option for intrusion detection mode. • Protection: Choose this option for intrusion protection mode.
Custom Signature Set	Select one or more web categories from the drop-down list. The categories are: abortion, abused-drugs, auctions, and so on.
Select an Signature Allow List	Select a signature allow list.
Alerts Log Level	Choose the alert log level: • Error • Emergency • Alert • Critical • Warning • Notice • Info • Debug

URL Filtering Policy

Field	Description
Profile Name	Name of the URL filtering policy.
Web Category	Choose the web category. The options are Block and Allow.

Field	Description
Web Reputation	Choose the web reputation from the drop-down list. The reputation options are: • High Risk • Suspicious • Moderate Risk • Low Risk • Trustworthy
Select one or more web categories	Select one or more web categories from the drop-down list. The categories are: abortion, abused-drugs, auctions, and so on.
Select allow URL list	Select an allow URL list.
Select block URL list	Select a block URL list.
Block Page Server	Choose one of the options: • Block Page Content: Enter the default content header and content body. • Redirect URL: Enter the redirect URL.
Alerts and Logs	Choose the alert and log type: • Blocklist • Allowlist • Reputation/Category

Advanced Malware Protection Policy

Field	Description
Profile Name	Name of the advanced malware protection policy name.
Select AMP Cloud Region	Select AMT Cloud region. The options are: • NAM • EU • APJC

Field	Description
Alert Log Level	Choose the alert log level. The options are: • Critical • Warning • Info
File Analysis	Enable file analysis.
Select TG Cloud Region	Select TG Cloud region. The options are NAM and EU.
Select one or more file types	Select one or more file types. The options are, pdf, ms-exe, new-office, rtf, mdb, mscab, msole2, wri, xlw, flv, and swf.

TLS/SSL Profile

Field	Description
Profile Name	Name of the TLS/SSL profile.
Select Categories to assign action	Set the categories between the actions—Decrypt, No Decrypt, and Pass Through URL Categories. Alternatively, choose multiple categories and set the action.
Reputation	Enable reputation to choose the **Decrypt Threshold**. The decrypt threshold options are: • High Risk • Suspicious • Moderate Risk • Low Risk • Trustworthy
Advanced Options	
Select a Decrypt Domain list	Choose the decrypt domain list or click **Create New** to create a new decrypt domain list. 1. Enter **Decrypt Domain List Name**. 2. Enter **Decrypt Domain** 3. Click **Add**.

Field	Description
Select a No Decrypt Domain list	Choose the no decrypt domain list or click **Create New** to create a new no decrypt domain list. 1. Enter **No Decrypt Domain List Name**. 2. Enter **No Decrypt Domain** 3. Click **Add**.
Fail Decrypt	Enable the fail decrypt option, if decryption fails.

TLS/SSL Decryption

Field Name	Description
Policy Name	Name of the policy. The name can contain a maximum of 32 characters.
Server Certificate Checks	
Expired Certificate	Defines what the policy should do if the server certificate has expired. The options are: • **Drop**: Drop traffic • **Decrypt**: Decrypt traffic
Untrusted Certificate	Defines what the policy should do if the server certificate is not trusted. The options are: • **Drop**: Drop traffic • **Decrypt**: Decrypt traffic
Certificate Revocation Status	Defines whether the Online Certificate Status Protocol (OCSP) should be used to check the revocation status of the server certificate. The options are **Enabled** or **Disabled**.
Unknown Revocation Status	Defines what the policy does, if the OCSP revocation status is **unknown**. • **Drop**: Drop traffic • **Decrypt**: Decrypt traffic
Unsupported Mode Checks	

Field Name	Description
Unsupported Protocol Versions	Defines the unsupported protocol versions. • **Drop**: Drop the unsupported protocol versions. • **Decrypt**: Decrypt the unsupported protocol versions.
Unsupported Cipher Suites	Defines the unsupported cipher suites. • **Drop**: Drop the unsupported cipher suites. • **Decrypt**: Decrypt the unsupported cipher suites.
Failure Mode	Defines the failure mode. The options are close and open.
Certificate Bundle	Check the **Use default CA certificate bundle** checkbox to use the default CA.
Minimum TLS Version	Sets the minimum version of TLS that the proxy should support. The options are: • **TLS 1.0** • **TLS 1.1** • **TLS 1.2**
Proxy Certificate Attributes	
RSA Keypair Modules	Defines the Proxy Certificate RSA Key modules. The options are: • **1024 bit RSA** • **2048 bit RSA** • **4096 bit RSA**
Ec Key Type	Defines the key type. The options are: • **P256** • **P384** • **P521**
Certificate Lifetime (in Days)	Sets the lifetime of the proxy certificate, in days.

Configure Embedded Security

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

The Enterprise Firewall with Application Awareness uses a flexible and easily understood zone-based model for traffic inspection, compared to the older interface-based model.

A firewall policy is a type of localized security policy that allows stateful inspection of TCP, UDP, and ICMP data traffic flows. Traffic flows that originate in a given zone are allowed to proceed to another zone based on the policy between the two zones. A zone is a grouping of one or more VPNs. Grouping VPNs into zones allows you to establish security boundaries in your overlay network so that you can control all data traffic that passes between zones. For more information on Embedded Security, see Enterprise Firewall with Application Awareness.

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Policy Groups** > **Embedded Security**.
2. Choose a security policy and click **Edit**.
3. Click **Add Rule**.

Field	Description
Rule Name	The name of the rule.
Sequence	Specify the sequence.
Destination Zone	In the **Destination Zone** drop-down list, choose the zone to which data traffic is sent. The options are: • No-Zone • Corporate_Users • Local_Internet_for_Guests • Payment_Processing_Network • Physical_Security_Devices • Self • Untrusted Zones are created based on the VPNs in the configuration group selected in the create security policy workflow.

Field	Description

Match	Choose the desired match conditions from the **Add Conditions** drop-down list. The options are:
	• Applications
	• Protocol
	• Source
	  • Geo Location
	  • IPv4 Prefix
	  • Port
	• Destination
	  • FQDN
	  • Geo Location
	  • IPv4 Prefix
	  • Port
	
	When ISE is enabled, then SGT option is available in the **Source** and **Destination**. Identity User or User group is only supported for **Source**.

Action	Choose the desired action conditions. The options are: • Pass • Drop • Inspect • Log Events: Unified Logging for Inspect Action. Select **Advanced Inspection Profile** from the drop-down list.

Configure an Embedded Security Sub-Policy

1. From the **Configuration** > **Policy Groups**, choose **Embedded Security**.
2. Choose a security policy from the list and click **Edit**. and enter the following details.
3. Click **Add Sub-Policy** to add sub-policies for a security policy.

Field	Description
VPN / Interface	Specify the VPN or the interface.

Field	Description
Source Zone	Choose the zone that is the source of the data packets.
Zone List Name	The name of a zone list.
VPN	Choose to configure zones with zone type as **VPN**. Add the VPNs to the zones from the drop-down list. The options are: • Payment Processing Network • Corporate Users • Local Internet for Guests • Physical Security Devices
Interface	Choose to configure zones with zone type as **Interface**. Add the interfaces to the zones from the **Add Interface** drop-down list.
Rule Name	The name of the rule.
Sequence	Specify the sequence.
Destination Zone	Choose the zone to which data traffic is sent. The options are: • Any • Corporate_Users • Local_Internet_for_Guests • Payment_Processing_Network • Physical_Security_Devices • Self • Untrusted (VPN 0)

Field	Description

Match	Choose the desired match conditions from the **Add Conditions** drop-down list. The options are:
	• Applications
	• Protocol
	• Source
	  • Geo Location
	  • IPv4 Prefix
	  • Port
	• Destination
	  • FQDN
	  • Geo Location
	  • IPv4 Prefix
	  • Port

Action	Choose the desired action conditions. The options are: • Pass • Drop • Inspect • Log Events - Unified Logging for Inspect Action. Select **Advanced Inspection Profile** from the drop-down list.
User / User Group	An identity service engine has to be enabled to configure **User / User Group** sub policies. You can configure using **Administration** > **Integration Management** > **Identity Service Engine**.

Configure Embedded Security Additional Settings

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Policy Groups**, choose **Embedded Security**.
2. Choose a security policy from the list and click **Edit** and enter the following details.
3. Click **Additional Settings** to configure additional settings for a security policy.

Field	Description
TCP SYN Flood Limit	Specify the threshold of SYN flood packets per second for each destination address.
Max Incomplete	Specify the timeout limits for the firewall policy. A **Max Incomplete** timeout limit protects firewall resources and keeps these resources from being used up.
TCP Limit	Specify the maximum TCP half-open sessions allowed on a device.
UDP Limit	Specify the maximum UDP half-open sessions allowed on a device.
ICMP Limit	Specify the maximum ICMP half-open sessions allowed on a device.
Audit Trail	Enable the **Audit Trail** option. This option is only applicable for rules with an inspect action.
Unified Logging	Enable the unified logging feature.
Optimized Policy	Enable the optimized policy option.
Session Reclassify Allow	Allow re-classification of traffic on policy change.
ICMP Unreachable Allow	Allow ICMP unreachable packets to pass through.
Advanced Inspection Profile	Attach a global advanced inspection profile (AIP) at a device level. All the rules in the device that match the traffic to be inspected are inspected using the advance inspection profile.

4. Choose the profile from the **Advanced Inspection Profile** drop-down list or click **Create New**.

Field	Description
Profile Name	The name of the profile.
Description	The description of the profile.
Select an Intrusion Prevention	Specify the maximum TCP half-open sessions allowed on a device.
UDP Limit	Specify the maximum UDP half-open sessions allowed on a device.
ICMP Limit	Specify the maximum ICMP half-open sessions allowed on a device.
Audit Trail	Enable the **Audit Trail** option. This option is only applicable for rules with an inspect action.

Field	Description
Unified Logging	Enable the unified logging feature.
Optimized Policy	Enable the optimized policy option.
Session Reclassify Allow	Allow re-classification of traffic on policy change.
ICMP Unreachable Allow	Allow ICMP unreachable packets to pass through.

5. Choose the intrusion prevention from the **Select an Intrusion Prevention** drop-down list or click **Create New**.

Field	Description
Profile Name	The name of the profile. The name can have a maximum of 32 characters.
Signature Set	Specify the signature set. The options are: • Balanced • Connectivity • Security
Inspection Mode	Specify the inspection mode. The options are: • Detection • Protection
Advanced	
Customer Signature Set	Enable customer signature set to add a new global custom signature. In the **Add New Global Custom Signature** window, choose **Download From** the following options: • Remote Server • Local Server (Not Recommended)
Select an Signature Allow List	Select an allowed signature list or **Create New** to create a new IPS signature list.

Field	Description
Alert Log Level	Choose the alert log level: • Error • Emergency • Alert • Critical • Warning • Notice • Info • Debug

6. Click **Add**.

7. Choose the advanced malware protection profile from the **Select an Advanced Malware Protection** drop-down list or click **Create New**.

Field	Description
Profile Name	The name of the profile. The name can have a maximum of 32 characters.
Select AMP Cloud Region	Choose the AMP cloud region. The options are: • NAM • EU • APJC
Inspection Mode	Specify the inspection mode. The options are: • Detection • Protection
Alert Log Level	Choose the alert log level: • Critical • Warning • Info
File Analaysis	Enable file analysis.

Field	Description
Select TG Cloud Region	Choose the cloud region from the drop-down list. The options are: • NAM • EU
Alert Log Level	Choose the alert log level: • Critical • Warning • Info
Select one or more file types	Choose one or more file type from the drop-down list: • All • pdf • ms-exe • new-office • rtf • mdb • mscab • msole2 • wri • xlw • flv • swf

8. Click **Add**.
9. Choose a URL filter from the **URL Filter** drop-down list or **Create New**.

Field	Description
Profile Name	The name of the profile. The name can have a maximum of 32 characters.
Web Category	Choose the web category from the drop-down list. The options are: • Block • Allow

Field	Description
Select one or more web categories	Choose one or more web categories from the drop-down list. The options are: abortion, abused-drugs and so on.
Web Reputation	Choose the web reputation from the drop-down list. The reputation options are: • High Risk • Suspicious • Moderate Risk • Low Risk • Trustworthy
Advanced	
Select allow url list	Select an allowed URL list or **Create New** to create a new allow URL list.
Select block url list	Select a blocked URL list or **Create New** to create a new block URL list.
Block Page Server	Choose the block page server from the drop-down list. The options are: • Block Page Content • Redirect URL: Specify the redirect URL
Alerts And Logs	Choose one or more file type from the drop-down list: • Blocklist • Allowlist • Reputation/Category

10. Click **Add**.
11. Choose **TLS Action**.

Field	Description
TLS Action	Choose the web category from the drop-down list. The options are: • Decrypt • Pass Through • Do not Decrypt

Field	Description
Select an TLS/SSL Decryption	Choose the TLS/SSL decryption profile from the drop-down list or **Create New** profile.

Configure a Secure Internet Gateway

Cisco Catalyst SD-WAN edge devices support routing, security, and other LAN access features that can be managed centrally. On high-end devices, you can enable all these features while providing the scale and performance required by large enterprises. However, on lower-end devices, enabling all the security features simultaneously can degrade performance. To avoid the performance degradation, integrate lower-end devices with Secure Internet Gateways (SIG) that do most of the processing to secure enterprise traffic. When you integrate a Cisco Catalyst SD-WAN edge device with a SIG, all client internet traffic, based on routing or policy, is forwarded to the SIG.

Access Umbrella credentials from **Administration** > **Settings** > **Cloud Provider Credentials**.

To configure a secure internet gateway:

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Policy Groups** > **Secure Internet Gateway**.
2. Click **Add Secure Internet Gateway**.
3. Choose **SIG Provider**. The options are:
   - Umbrella
   - Zscaler
   - Generic

Umbrella Configuration

Table 13: Cisco Umbrella Credentials

Field	Description
Organization ID	Enter the Cisco Umbrella organization ID (Org ID) for your organization. For more information, see the *Cisco Umbrella SIG User Guide*.
SIG Umbrella API Key	Enter the Umbrella Management API Key. Management API keys are used in SIG is **Secure Internet Gateway (SIG) - (Management)**. For more information, see the Cloud Security API documentation on the Cisco DevNet portal.
SIG Umbrella API Secret	Enter the Umbrella Management API Secret. For more information, see the Cloud Security API documentation on the Cisco DevNet portal.

Zscaler Configuration

You can access Zscaler credentials from **Administration** > **Settings** > **Cloud Provider Credentials**.

Table 14: Zscaler Credentials

Field	Description
Organization	Name of the organization in Zscaler cloud.
Partner base URI	This is the base URI that Cisco SD-WAN Manager uses in REST API calls. To find this information on the Zscaler portal, see the *ZIA Help* > *ZIA API* > *API Developer & Reference Guide* > *Getting Started*.
Username	Username of the Cisco Catalyst SD-WAN partner account.
Password	Password of the Cisco Catalyst SD-WAN partner account.
Partner API key	Partner API key. To find the key in Zscaler, see Managing SD-WAN Partner Keys.

Generic Configuration

To create tunnels, click **Configuration** and do the following:

Parameter Scope	Scope Description
Device Specific (indicated by a host icon)	Use device-specific value for the parameter. For device-specific parameters, you cannot enter value in the feature template. Enter the value when you add a device to the configuration group. To change the default key, type a new string and move the cursor out of the **Enter Key** box.
Global (indicated by a globe icon)	Enter value for the parameter, and apply that value to all devices.

1. Click **Add Tunnel**.
2. In the **Add Tunnel** dialog box, under **Basic Settings** configure the following:

Table 15: Basic Settings

Field	Description
Tunnel Type	Umbrella: (Read only) **ipsec** Zscaler: Click **ipsec** or **gre**. Generic: Click **ipsec** or **gre**.
Interface Name (1..255)	Name of the interface.
Description	Description for the interface.
Tracker	By default, a tracker is attached to monitor the health of tunnels.

Field	Description
Tunnel Source Interface	Name of the source interface of the tunnel. This interface should be an egress interface and is typically the internet-facing interface.
Source Public IP	(Automatic GRE tunnels to Zscaler only) Public IP address of the tunnel source interface that is required to create the GRE tunnel to Zscaler. Default: Auto We recommend that you use the default configuration. With the default configuration, the Cisco IOS XE SD-WAN device finds the public IP address assigned to the tunnel source interface using a DNS query. If the DNS query fails, the device notifies Cisco SD-WAN Manager of the failure. Enter the public IP address only if the DNS query fails.
Data-Center	For a primary data center, click **Primary**, or for a secondary data center, click **Secondary**. Tunnels to the primary data center serve as active tunnels, and tunnels to the secondary data center serve as back-up tunnels.
Tunnel Destination IP Address/FQDN	(Manual tunnels only) The IP address of the SIG provider endpoint. The configuration of FQDN for Tunnel Destination IP address is not supported.
Preshared Key	(Manual tunnels only) This field is displayed only if you choose **ipsec** as the **Tunnel Type**. Enter the password to use with the preshared key.
Advanced Options	
Shutdown	Click **No** to enable the interface; click **Yes** to disable. Default: No
IP MTU	Specify the maximum MTU size of packets on the interface. Range: 576 to 2000 bytes Default: 1400 bytes
TCP MSS	Specify the maximum segment size (MSS) of TPC SYN packets. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented. Range: 500 to 1460 bytes Default: None
DPD Interval	Specify the interval for IKE to send Hello packets on the connection. Range: 10 to 3600 seconds Default: 10

Field	Description
DPD Retries	Specify the number of seconds between DPD retry messages if the DPD retry message is missed by the peer. After one DPD message is missed by the peer, the router changes the state and sends a DPD retry message at a faster retry interval, which is the number of seconds between DPD retries if the DPD message is missed by the peer. The default DPD retry message is sent every 2 seconds. Five DPD retry messages can be missed before the tunnel is marked as down. Range: 2 to 60 seconds Default: 3
IKE	
IKE Rekey Interval	Specify the interval for refreshing IKE keys. Range: 3600 to 1209600 seconds (1 hour to 14 days) Default: 14400 seconds
IKE Cipher Suite	Specify the type of authentication and encryption to use during IKE key exchange. Choose one of the following: • AES 256 CBC SHA1 • AES 256 CBC SHA2 • AES 128 CBC SHA1 • AES 128 CBC SHA2 The IPsec Cipher Suite defaults vary by the type of the SIG: • Umbrella: AES 256 GCM • Zscaler: None • Generic: NULL SHA 512

Field	Description
IKE Diffie-Hellman Group	Specify the Diffie-Hellman group to use in IKE key exchange, whether IKEv1 or IKEv2. • 2 1024-bit modulus • 14 2048-bit modulus • 15 3072-bit modulus • 16 4096-bit modulus The IKE group defaults vary by the type of the SIG: • Umbrella: 14 2048-bit modulus • Zscaler: 2 1024-bit modulus • Generic: 16 4096-bit modulus
IPSec	
IPsec Rekey Interval	Specify the interval for refreshing IPsec keys. Range: 3600 to 1209600 seconds (1 hour to 14 days) Default: 3600 seconds
IPsec Replay Window	Specify the replay window size for the IPsec tunnel. Options: 64, 128, 256, 512, 1024, 2048, 4096. Default: 512
IPsec Cipher Suite	Specify the authentication and encryption to use on the IPsec tunnel. Options: • AES 256 CBC SHA1 • AES 256 CBC SHA 384 • AES 256 CBC SHA 256 • AES 256 CBC SHA 512 • AES 256 GCM • NULL SHA1 • NULL SHA 384 • NULL SHA 256 • NULL SHA 512 Default: AES 256 GCM

Field	Description
Perfect Forward Secrecy	Specify the PFS settings to use on the IPsec tunnel. Choose one of the following Diffie-Hellman prime modulus groups: • Group-2 1024-bit modulus • Group-14 2048-bit modulus • Group-15 3072-bit modulus • Group-16 4096-bit modulus • None: disable PFS The Perfect Forward Secrecy defaults vary by the type of the SIG: • Umbrella: None • Zscaler: None • Generic: Group 16

3. Click **Add**.

Note When a security policy associated with Zscaler is removed from a device and a new configuration group is deployed, the corresponding tunnel entry sometimes fails to be deleted from Zscaler's cloud services. As a result, attempting to establish a new tunnel may result in a DUPLICATE_ITEM error due to the presence of the existing entry. To resolve this issue, manually delete the stale tunnel entry from the Zscaler cloud whenever a security policy is removed from a device.

Tracker Configuration

To create one or more trackers to monitor tunnel health, click **Tracker** and do the following:

1. **Source IP Address**: Enter a source IP address for the probe packets.
2. Click **Add Tracker**.
3. In the **Add Tracker** dialog box, configure the following:

Table 16: Tracker Parameters

Field	Description
Name	Name of the tracker. The name can be up to 128 alphanumeric characters.
API url of endpoint	Specify the API URL for the SIG endpoint of the tunnel.

Field	Description
Threshold	Enter the wait time for the probe to return a response before declaring that the configured endpoint is down. Range: 100 to 1000 milliseconds Default: 300 milliseconds
Probe Interval	Enter the time interval between probes to determine the status of the configured endpoint. Range: 20 to 600 seconds Default: 60 seconds
Multiplier	Enter the number of times to resend probes before determining that a tunnel is down. Range: 1 to 10 Default: 3

4. Click **Add**.

High Availability Configuration

To designate active and back-up tunnels and distribute traffic among tunnels, click **High Availability** and do the following:

1. Click **Add Interface Pair**.
2. In the **Add Interface Pair** dialog box, configure the following:

Field	Description
Active Interface	Choose a tunnel that connects to the primary data center.
Active Interface Weight	Enter weight (weight range 1 to 255) for load balancing. Load balancing helps in distributing traffic over multiple tunnels and this helps increase the network bandwidth. If you enter the same weights, you can achieve ECMP load balancing across the tunnels. However, if you enter a higher weight for a tunnel, that tunnel has higher priority for traffic flow. For example, if you set up two active tunnels, where the first tunnel is configured with weight of 10, and the second tunnel with weight configured as 20, then the traffic is load-balanced between the tunnels in a 10:20 ratio.
Backup Interface	To designate a back-up tunnel, choose a tunnel that connects to the secondary data center. To omit designating a back-up tunnel, choose **None**.

Field	Description
Backup Interface Weight	Enter weight (weight range 1 to 255) for load balancing. Load balancing helps in distributing traffic over multiple tunnels and this helps increase the network bandwidth. If you enter the same weights, you can achieve ECMP load balancing across the tunnels. However, if you enter a higher weight for a tunnel, that tunnel has higher priority for traffic flow. For example, if you set up two back-up tunnels, where the first tunnel is configured with weight of 10, and the second tunnel with weight configured as 20, then the traffic is load-balanced between the tunnels in a 10:20 ratio.

3. Click **Add**.

Configure a Secure Service Edge

Before You Begin

Create the Cisco SSE credentials from **Administration** > **Settings** > **Cloud Credentials**.

Configure a Secure Service Edge

Choose the **SSE Provider**. The options are:

- Cisco Secure Access
- (Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.14.1) Zscaler

Configure a Tracker

While creating automatic tunnels, Cisco SD-WAN Manager creates and attaches a default tracker endpoint with default values for failover parameters. However, you can also create customized trackers with failover parameters that suit your requirements.

1. In the **Source IP Address** field, enter a source IP address without a subnet mask.
2. Click **Add Tracker**.
3. In the **Add Tracker** pop-up window, configure the following:

Table 17: Tracker Parameters

Field	Description
Name	Name of the tracker. The name can be up to 128 alphanumeric characters.
API url of endpoint	Specify the API URL for the Secure Service Edge endpoint of the tunnel. Default: service.sig.umbrella.com

Field	Description
Threshold	Enter the wait time for the probe to return a response before declaring that the configured endpoint is down. Range: 100 to 1000 milliseconds Default: 300 milliseconds
Probe Interval	Enter the time interval between probes to determine the status of the configured endpoint. Range: 20 to 600 seconds Default: 60 seconds
Multiplier	Enter the number of times to resend probes before determining that a tunnel is up or down. Range: 1 to 10 Default: 3

4. Click **Add**.

Configure Tunnels

To create tunnels, click **Configuration** and do the following:

1. Click **Add Tunnel**.
2. In the **Add Tunnel** pop-up window, under **Basic Settings**, configure the following:

Table 18: Basic Settings

Field	Description
Tunnel Type	• Cisco Secure Access: (Read only) **ipsec** • (Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.14.1) Zscaler: **ipsec** or **gre**
Interface Name (1..255)	Name of the interface.
Description	Enter a description for the interface.
Tracker	By default, a tracker is attached to monitor the health of tunnels.
Tunnel Source Interface	Name of the source interface of the tunnel. This interface should be an egress interface and is typically the internet-facing interface. The tunnel source interface supports loopback.

Field	Description
Source Public IP	(Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.14.1) Public IP address of the tunnel source interface that is required to create the GRE tunnel to Zscaler. Default: Auto. We recommend that you use the default configuration. With the default configuration, the Cisco IOS XE Catalyst SD-WAN device finds the public IP address assigned to the tunnel source interface using a DNS query. If the DNS query fails, the device notifies Cisco SD-WAN Manager of the failure. Enter the public IP address only if the DNS query fails.
Data-Center	For a primary data center, click **Primary**, or for a secondary data center, click **Secondary**. Tunnels to the primary data center serve as active tunnels, and tunnels to the secondary data center serve as back-up tunnels.
Advanced Options (Optional)	
Shutdown	Click the radio button to enable this option. Default: Disabled
Enable Tracker	Click the radio button to enable this option.
IP MTU	Specify the maximum MTU size of packets on the interface. Range: 576 to 2000 bytes Default: 1400 bytes
TCP MSS	Specify the maximum segment size (MSS) of TPC SYN packets. By default, the MSS is dynamically adjusted based on the interface or tunnel MTU such that TCP SYN packets are never fragmented. Range: 500 to 1460 bytes Default: None
DPD Interval	Specify the interval for Internet Key Exchange (IKE) to send Hello packets on the connection. Range: 10 to 3600 seconds Default: 10

Field	Description
DPD Retries	Specify the number of seconds between Dead Peer Detection (DPD) retry messages if the DPD retry message is missed by the peer. If a peer misses a DPD message, the router changes the state and sends a DPD retry message. The message is sent at a faster retry interval, which is the number of seconds between DPD retries. The default DPD retry message is sent every 2 seconds. The tunnel is marked as down after five DPD retry messages are missed. Range: 2 to 60 seconds Default: 3
IKE	
IKE Rekey Interval	Specify the interval for refreshing IKE keys. Range: 3600 to 1209600 seconds (1 hour to 14 days) Default: 14400 seconds
IKE Cipher Suite	Specify the type of authentication and encryption to use during IKE key exchange. Choose one of the following: • AES 256 CBC SHA1 • AES 256 CBC SHA2 • AES 128 CBC SHA1 • AES 128 CBC SHA2 Default: AES 256 CBC SHA1
IKE Diffie-Hellman Group	Specify the Diffie-Hellman group to use in IKE key exchange, whether IKEv1 or IKEv2.
IPSec	
IPsec Rekey Interval	Specify the interval for refreshing IPsec keys. Range: 3600 to 1209600 seconds (1 hour to 14 days) Default: 3600 seconds
IPsec Replay Window	Specify the replay window size for the IPsec tunnel. Options: 64, 128, 256, 512, 1024, 2048, or 4096 packets. Default: 512

Field	Description
IPsec Cipher Suite	Specify the authentication and encryption to use on the IPsec tunnel. Options: • AES 256 CBC SHA1 • AES 256 CBC SHA 384 • AES 256 CBC SHA 256 • AES 256 CBC SHA 512 • AES 256 GCM Default: AEM 256 GCM
Perfect Forward Secrecy	Specify the Perfect Forward Secrecy (PFS) settings to use on the IPsec tunnel. Choose one of the following Diffie-Hellman prime modulus groups: • Group-2 1024-bit modulus • Group-14 2048-bit modulus • Group-15 3072-bit modulus • Group-16 4096-bit modulus • None: disable PFS

3. Click **Add**.

Applicable only to Cisco Secure Access:

Region: When you choose the region, a pair of primary and secondary region is selected. Choose the primary region that Cisco Secure Service Edge provides from the drop-down list and the secondary region is auto-selected in Cisco SD-WAN Manager. If the primary region with a unicast IP address is not reachable then the secondary region with a unicast IP address is reachable and vice versa. Cisco Secure Access ensures that both the regions are reachable at all times.

Note You can configure any DNS server on the device which connects to HTTPS to get the public IP address. To configure a source interface for HTTPS, use the **ip http client source-interface** command on Cisco SD-WAN Manager.

Configure High Availability

To designate active and back-up tunnels and distribute traffic among tunnels, click **High Availability** and do the following:

1. Click **Add Interface Pair**.
2. In the **Add Interface Pair** pop-up window, configure the following:

Field	Description
Active Interface	Choose a tunnel that connects to the primary data center.
Active Interface Weight	Enter weight (weight range 1 to 255) for load balancing. Load balancing helps in distributing traffic over multiple tunnels and this helps increase the network bandwidth. If you enter the same weights to both the tunnels, you can achieve ECMP load balancing across the tunnels. However, if you enter a higher weight for a tunnel, that tunnel has higher priority for traffic flow. For example, if you set up two active tunnels, where the first tunnel is configured with weight of 10, and the second tunnel with weight configured as 20, then the traffic is load-balanced between the tunnels in a 10:20 ratio.
Backup Interface	To designate a back-up tunnel, choose a tunnel that connects to the secondary data center. To omit designating a back-up tunnel, choose **None**.
Backup Interface Weight	Enter weight (weight range 1 to 255) for load balancing. Load balancing helps in distributing traffic over multiple tunnels and this helps increase the network bandwidth. If you enter the same weights, you can achieve ECMP load balancing across the tunnels. However, if you enter a higher weight for a tunnel, that tunnel has higher priority for traffic flow. For example, if you set up two back-up tunnels, where the first tunnel is configured with weight of 10, and the second tunnel with weight configured as 20, then the traffic is load-balanced between the tunnels in a 10:20 ratio.

3. Click **Add**.

Advanced Settings

(Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.14.1)

Applicable only to Zscaler:

Field	Description
Primary Datacenter	Cisco SD-WAN Manager automatically selects the primary data center closest to the WAN edge device. To route traffic to a specific Zscaler data center, choose the data center from the drop-down list.
Secondary Datacenter	Cisco SD-WAN Manager automatically selects the secondary data center closest to the WAN edge device. To route traffic to a specific Zscaler data center, choose the data center from the drop-down list.

Zscaler Location

Field	Description
Zscaler Location	Enter the name of a location that is configured on the ZIA Admin Portal. If you do not enter a location name, the Zscaler service detects the location based on the received traffic. For more information about locations, see *ZIA Help > Traffic Forwarding > Location Management > About Locations*.
Country	You can enable or disable this option only if either primary or secondary data center is set to Auto. When you choose Auto, the data center selected is within the country of the device.

Gateway Options

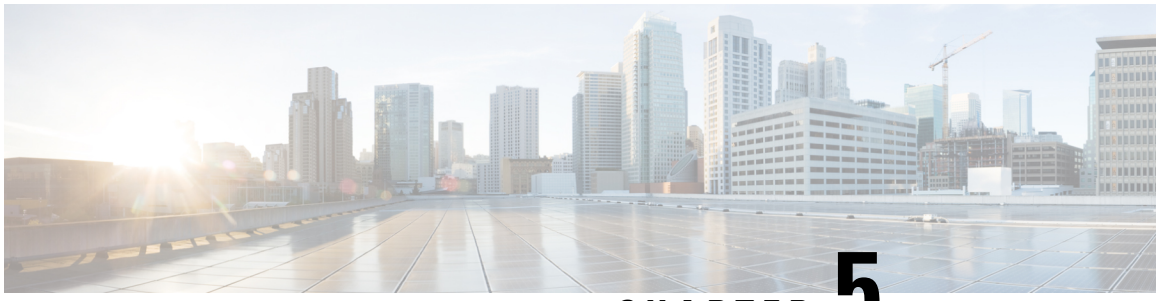
Field	Description
Authentication Required	See *ZIA Help > Traffic Forwarding > Location Management > Configuring Locations*. Default: Off
Enable Caution	See *ZIA Help > Traffic Forwarding > Location Management > Configuring Locations*. Default: Off
Enable AUP	See *ZIA Help > Traffic Forwarding > Location Management > Configuring Locations*. Default: Off
XFF Forwarding	See *ZIA Help > Traffic Forwarding > Location Management > Configuring Locations*. Default: Off
Enable IPS Control	See *ZIA Help > Traffic Forwarding > Location Management > Configuring Locations*. Default: Off
Enable Firewall	See *ZIA Help > Traffic Forwarding > Location Management > Configuring Locations*. Default: Off

Configure DNS Security

The Cisco Catalyst SD-WAN Umbrella Integration feature enables the cloud-based security service by inspecting the Domain Name System (DNS) query that is sent to the DNS server through the device. The security administrator configures policies on the Umbrella portal to either allow or deny traffic toward the fully qualified domain name (FQDN). The router acts as a DNS forwarder on the network edge, transparently intercepts DNS traffic, and forwards the DNS queries to the Umbrella cloud.

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Policy Groups** > **DNS Security**.
2. Click **Add DNS Security Policy**.

Field	Description
Add DNS Security Policy	From the **Add DNS Security Policy** drop-down list, select **Create New** to create a new DNS Security Policy policy.
Create New	Displays the DNS Security Policy wizard.
Policy Name	Enter a name for the policy.
Umbrella Registration Status	Displays the status of the API Token configuration.
Manage Umbrella Registration	Click **Manage Umbrella Registration** to add Cisco Umbrella Registration Key and Secret. Specific network-devices keys are used in DNS. • Enter **Organization ID**. • Enter **Registration Key**. • Enter **Secret**. You can edit the umbrella credentials from **Administration** > **Settings** > **Cloud Provider**.
Match All VPN	Click **Match All VPN** to keep the same configuration for all the available VPNs.
Custom VPN Configuration	choose **Custom VPN Configuration** to input the specific VPNs.
Local Domain Bypass List	Choose the domain bypass.
DNS Server IP	Configure **DNS Server IP** from the following options: • **Umbrella Default** • **Custom DNS**
DNSCrypt	Enable or disable the DNSCrypt.



CHAPTER 5

Application Catalog

Table 19: Feature History

Feature Name	Release Information	Description
Application Catalog	Cisco IOS XE Catalyst SD-WAN Release 17.13.1a Cisco Catalyst SD-WAN Manager Release 20.13.1	The **Application Catalog** feature provides control and visibility for applications running in your network environment. The application catalog is continuously updated as new applications are developed to ensure that your Cisco SD-WAN Manager environment adapts to changes in application use.
Discover and Monitor Kubernetes Clusters	Cisco IOS XE Catalyst SD-WAN Release 17.13.1a Cisco Catalyst SD-WAN Manager Release 20.13.1	The Cisco SD-WAN Manager integrates Kubernetes cluster discovery and monitoring to monitor your network infrastructure and your containerized applications from a single interface. The Kubernetes cluster management streamlines the network and applications while providing a visibility and control on the applications.
Cloud SaaS Feeds	Cisco IOS XE Catalyst SD-WAN Release 17.13.1a Cisco Catalyst SD-WAN Manager Release 20.13.1	Cloud SaaS (Software as a Service) feeds are information or data feed from SaaS applications that are hosted on the cloud. These applications can range from customer relationship management (CRM) tools to financial software, and Cisco SD-WAN Manager provides real-time data and updates as feeds from the SaaS applications.

- Information About Application Catalog, on page 62
- Prerequisites for Application Catalog, on page 62
- Restrictions for Application Catalog, on page 63
- Application Catalog Overview, on page 64
- View Applications, on page 64
- Configure Custom Applications, on page 65
- Configure Application List, on page 67
- Benefits of Kubernetes Clusters and Kubernetes Services, on page 67
- Benefits of Cloud SaaS Feeds, on page 68
- Configure, Discover Kubernetes Clusters and Kubernetes Services, on page 68

• Configure Cloud SaaS Feed Using Cisco SD-WAN Manager, on page 69
• Monitor Kubernetes Clusters and Kubernetes Services, on page 69
• Monitor Cloud SaaS Feed, on page 70

Information About Application Catalog

The application catalog in Cisco SD-WAN Manager provides visibility and control of applications running in your Cisco Catalyst SD-WAN environment powered by SD-AVC. For more information about SD-AVC, see Cisco SD-AVC User Guide. The application catalog includes applications ranging from business productivity apps like Office 365 or Google Workspace to social media platforms, cloud platforms, and customer-created applications.

The application catalog is a central place to take care of all operation tasks related to applications, capabilities like updating applications and cloud SaaS feeds from different sources, creating custom applications, viewing applications in different groups, creating an application list and many more. The feature optimizes network connectivity based on the specific requirements of different Kubernetes services.

Note You can use custom applications in the same way as any other protocol when configuring policies using policy groups or using centralized policies. For more information on configuring policies using Policy Groups, see, Group of Interest - Policy.

The **Application Catalog** tab has the following features:

- Overview
- Applications
- Application Source Settings
- Discovered Application
- Application List
- Configure SD-AVC
- Configure Cloud Connection

Prerequisites for Application Catalog

To fully utilize the capabilities of application catalog, the following conditions must be met:

- Enable SD-AVC on the **Administration** > **Settings** page.

Note For Cisco Cloud-hosted overlays provisioned in Cisco Catalyst SD-WAN Control Components Release 20.10.x and later releases, the SD-AVC service and Cloud Connector are enabled by default. For more information see, Cisco SD-AVC.

- Enable SD-AVC Cloud Connector to use SaaS feeds for enhanced application classification (Optional, but recommended).

Configure SD-AVC

1. Click **SD-AVC**.

   The **Cluster Management** page appears. The default tab is **Service Configuration**.
2. Click **Add Manager**.
3. In the **Add Manager** page, choose **Node Persona** from the following options:
   - Compute + Data (Up to 5 nodes each)
   - Compute (Up to 5 nodes)
   - Data (Up to 10s of nodes)
4. Enter the **Manager IP Address**, **Username** and **Password**.
5. Choose **Enable SD-AVC**.
6. Click **Add**.

Configure Cloud Connection

1. Click Configure Cloud Connection.

   The Administration Settings page appears.
2. Click SD-AVC.
3. Enable Cloud Connector in the Settings / System SD-AVC page.
4. Enter the OTP and the Cloud Gateway URL.
5. Click Save.

Note For more information on SD-AVC Connector, see Enable Cisco SD-AVC Cloud Connector.

Restrictions for Application Catalog

Restrictions for Kubernetes Clusters and Kubernetes Services

- Only Google Cloud and Amazon Web Services are supported as cloud providers.

Note AWS GovCloud is not supported.

Other cloud providers can utilize Kubernetes Clusters and Kubernetes Services feature using the manual upload option.

- Maximum number of custom applications: 1100
- Maximum number of L3/L4 rules: 20000
- Maximum number of server names: 50000

Application Catalog Overview

Applications in Registry

The Applications in Registry provide a visual representation of different types of applications in the system. It helps to understand the distribution and proportions of the applications based on their categories.

- Built in: Applications that are built-in or pre-installed in the system.
- Discovered: Applications that are discovered or detected by the system.
- Custom: Custom-built applications specifically developed for the system.

The chart segments represent the application categories, and the size of each segment indicates the relative proportion of applications in that category. Use this chart to gain insights into the application landscape and understand the composition of applications in the system. This chart illustrates the applications in the Cisco SD-WAN Manager Application registry. The device application registry is updated after pushing a configuration to the devices. For example, when a new custom application is created, it is not updated in the device application registry until a policy with that custom application is pushed to the device, however, it will be counted in the custom application on this chart since Cisco SD-WAN Manager already has the definition in its registry. All the custom applications created are seen in the Applications tab and in the chart as custom apps.

Top Applications Observed in Network

The **Applications Observed in Network** doughnut chart provides insights into the types of top applications observed within the network traffic. It displays the distribution and prevalence of different application categories.

Each segment in the chart represents a specific application category, and the size of the segment indicates the relative presence or frequency of that category within the observed network traffic. Use this chart to gain insights into the types of applications that are prominent within the network and understand the traffic composition. You can view the application details based on the timestamp. For example, Last 1 Hour, Last 3 Hours and so on. The maximum time period you can select is 24 hours.

View Applications

View the applications associated with your cloud account including the applications you create and the default applications on Cisco SD-WAN Manager.

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Application Catalog** > **Applications**.

   A list of applications associated with your Cisco SD-WAN Manager appears.

2. Choose an application attribute from the **Select Application Attributes** drop-down box. For example, **Application Source**.

   From the **Choose Filter** drop-down choose a filter to view only the relevant applications.

Configure Custom Applications

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Application Catalog** > **Applications** > **Custom Application**
2. Enter **Application name**.

   Configure the following:

Field	Description
Application Name	Enter a name for the application list.
Server Names	Enter the server names. The names specify the fully qualified domain names or regex starting with '*' but not ending with '*', or both separated by commas. For example, *.customapp.com, customapptest.com, *appcustom.
Application Family	Choose the application family. The options include instant messaging, game, mail, routing, and so on.
Application Group	Choose the application group. The options include flash-group, ipsec-group, concur-group, and so on.
Traffic Class	Choose the traffic class. The options include multimedia-conferencing, network-control, real-time-interactive, and so on. **Note** This attribute is used to categorize network traffic into different classes based on specific criteria like source and destination IP addresses, port numbers, etc. Traffic classes are crucial in the traffic matching process because they enable the Cisco Catalyst SD-WAN to identify and sort traffic, which helps in efficiently managing bandwidth and resources. When setting up the policy group workflow, different traffic classes can be allocated different priorities.

Field	Description
Business Relevance	Choose the business relevance from the drop-down list. The options are: • **Bronze** • **Gold** • **Silver** **Note** This attribute is used to specify the priority of network traffic based on its relevance to business operations. For example, traffic related to critical business applications can be assigned a higher relevance, and therefore, a higher priority. This ensures that important traffic gets the resources it needs for optimal performance.
IPv4 Address	Enter the IPv4 addresses separated by commas. Subnet prefix length is 24 to 32.
Ports	Enter the port number or range or both separated by a space. For example, 1 2 10-20.
L4 Protocol	Enter L4 protocol. The options are: • TCP • UDP • TCP-UDP

3. Click **Save**.

Export Application List

1. Click Export to export the application list.

   The **Applications.csv** file is downloaded to the local desktop.

   You can use custom applications in the same way as any other protocol when configuring Cisco Catalyst SD-WAN policies using policy groups or using centralized policies. For more information on configuring policies using Policy Groups, see, Group of Interest - Policy.

Configure Application List

Create Application List

1. From the **Configuration** > **Application Catalog** > **Application List**, click **Create Application List**.
2. Choose **Create New** to create a new application list, or choose **Existing** to update an existing application list.
3. Enter the **Application List** or choose an **Application List** from the drop-down list to update an existing application list.
4. Choose an application or application family from the **Application** or **Application Family** drop-down list.
5. Click **Save**.

   The application list is created.

To find application or application set, perform the following steps:

1. On the **Application Lists** page, you can find the existing application or application family by using the **Find Application/ Application Set** field.
2. Choose the **Default Application List** or **Custom Application List** from the **Show** drop-down list.

   The selected application list appears. You can filter the application or application family lists.

   The **Summary** pane displays the total, custom and default application lists.
3. Click **Create Application List** to create or edit an existing application list.

Note Application lists configured in the Application Catalog can only be used in the configuration of policies using Policy Groups.

Benefits of Kubernetes Clusters and Kubernetes Services

- Unified Network Management: Cisco SD-WAN Manager gives the ability to add Kubernetes clusters and it discovers any applications running on them.
- Enhanced Visibility: The Cisco SD-WAN Manager and Kubernetes clusters integration provides complete visibility over both network infrastructure and application definitions, making it easier to identify and resolve issues.
- Improved Performance: Cisco Catalyst SD-WAN's ability to optimize network traffic, combined with direct visibility over Kubernetes resources, results in improved application performance.
- Greater Efficiency: The network management based on application requirements and Kubernetes services leads to greater operational efficiency.

- Advanced Security: The Cisco SD-WAN Manager and Kubernetes clusters integration provides more robust security for both network and application layers.

Benefits of Cloud SaaS Feeds

- Cloud SaaS feeds provide real-time data on cloud application classification. Cisco SD-WAN Manager uses this information to make intelligent decisions about routing and optimizing traffic to ensure the best possible performance for these applications.
- The Application classification is enhanced and up-to-date with latest Cloud SaaS feeds.

Configure, Discover Kubernetes Clusters and Kubernetes Services

Enable Kubernetes Clusters for Cloud-based Deployment

1. From the Cisco SD-WAN Manager menu, click **Configuration** > **Application Catalog**.
2. Click the **Application Source Setttings** tab.
3. In the **Kubernetes Cluster** section, click **Cloud Account**.
4. Click **Add Account**.
5. Select a cloud account and click **Enable**.

   The **Kubernetes Cluster** table displays the cloud accounts with the Kubernetes discovery status in the **Status** column.

Note You'll see a list of cloud accounts appearing already in the **Kubernetes Cluster** cluster table if you've configured the cloud accounts using the Cloud OnRamp for Multicloud feature.

Enable Manual Discovery of Kubernetes Clusters

1. In the Cisco SD-WAN Manager menu, click **Configuration** > **Application Catalog**
2. Navigate to the **Application Source Setttings** tab.
3. In the **Kubernetes Cluster** section, click **Manually Upload**.
4. Choose or drag and drop a kubeconfig file and click **Add**.

Note Maximum file size: 10 MB

The **Kubernetes Cluster** table displays the cloud accounts, with the Kubernetes discovery status in the **Status** column.

Once you configured the Kubernetes cluster, navigate to the **Discovered Application** tab to view the services and applications discovered on those Kubernetes clusters and create custom applications if needed.

Configure Cloud SaaS Feed Using Cisco SD-WAN Manager

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Application Catalog** > **Application Source Settings**.
2. In the **Cloud SaaS Feeds** table, you see a list of cloud application feeds.

Note Only if you've enabled SD-AVC and Cloud connections, you'll see the list of cloud SaaS feeds.

3. In the **Actions** column, click the **...** icon adjacent to the respective cloud SaaS feed row.
4. Click **Enable** to view cloud SaaS feeds for the application of your choice.

Note Choose **Disable** so that the application classification doesn't use the Cloud SaaS feeds and instead uses NBAR classification logic.

Monitor Kubernetes Clusters and Kubernetes Services

Monitor Kubernetes Clusters

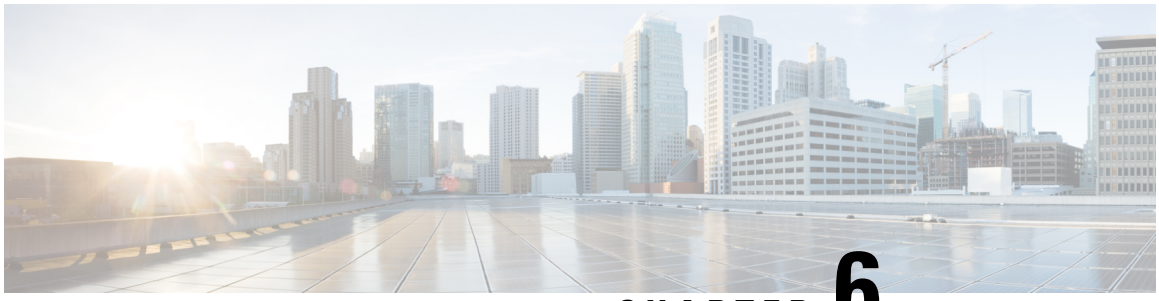
1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Application Catalog**.
2. Navigate to the **Application Source Settings** tab in the **Application Catalog** page.
3. The **Kubernetes Cluster** table displays the cluster details along with the Kubernetes cluster discovery status.

Monitor Applications

1. Navigate to the **Discovered application** tab in the **Application Catalog** page.
2. The **Kubernetes Services** table displays the discovered applications and the details to monitor the application status.

Monitor Cloud SaaS Feed

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Application Catalog** > **Application Source Settings**.
2. In the **Action** column, click **...** icon and choose **View Feeds**.
3. In the the **View Feeds** page, you see detailed information regarding the particular cloud SaaS feeds.



CHAPTER 6

Policy Compliance

- Policy Compliance, on page 71
- Information About Policy Compliance, on page 71
- Restrictions for the Policy Compliance Check , on page 72
- View and Resolve Policy Compliance Issues , on page 72

Policy Compliance

Table 20: Feature History

Feature Name	Release Information	Description
Policy Compliance	Cisco IOS XE Catalyst SD-WAN Release 17.14.1a Cisco Catalyst SD-WAN Control Components Release 20.14.1	This feature analyzes application-aware policies to determine whether the updates to applications in a later Protocol Pack release change the operation of a policy. Any such change is considered a policy compliance issue. To ensure that the operation of each policy remains aligned to the policy intent, the feature flags any compliance issues to enable you to address them.

Information About Policy Compliance

Various types of policies specify application traffic to match by using application lists, which contain one or more applications. The applications in application lists may be from a Protocol Pack or may be user-defined custom applications. As new Protocol Packs are released, changes occur to the protocol set. These changes may include adding applications that provide more granular classification of existing applications, renaming applications, and so on.

For example, an earlier Protocol Pack may include an application that captures all traffic for a set of services. A later Protocol Pack may include separate applications for different components of the services to provide more granular classification of the traffic. To illustrate with a fictional example, an application x-media might be broken into x-audio and x-video for more granular classification.

If a policy matches traffic using an application list that includes the x-media application, the policy does not make use of the later, more granular classification as x-audio and x-video.

Check Policy Compliance

When checking the applications in a policy, Cisco SD-WAN Manager compares them with the applications in the Protocol Pack currently loaded in Cisco SD-WAN Manager. Cisco SD-WAN Manager checks policies for the following compliance issues:

- Checks existing policies to determine whether the policies match applications that have become classified in a more granular fashion in a later Protocol Pack release.
- Checks for renamed applications. For example, renaming application Skydrive to Onedrive.
- Checks for policies that match traffic broadly by transport protocol, such as http. When a policy matches traffic so broadly, it is difficult to anticipate which new applications, in later Protocol Packs, may be included in the match.

This check keeps the policy intent intact after new applications are added.

View Compliance Issues

If Cisco SD-WAN Manager detects a compliance issue with a policy, it displays the affected policies and relevant new applications. For information about viewing compliance issues, see View and Resolve Policy Compliance Issues , on page 72.

Restrictions for the Policy Compliance Check

- See the NBAR2 Protocol Pack Library for information about which Protocol Pack updates are available for each Cisco IOS XE release.
- Devices using a Cisco IOS XE release earlier than Cisco IOS XE Catalyst SD-WAN Release 17.14.1a support only policies that use applications that were available in the original built-in Protocol Pack release of the Cisco IOS XE release. They do not support policies that use applications added in subsequent Protocol Pack releases.

  For example, if the original built-in Protocol Pack release of the Cisco IOS XE release did not include application x, and a policy uses application x, then a router using a release earlier than Cisco IOS XE Catalyst SD-WAN Release 17.14.1a cannot support that policy. This is true even if you later upgrade the router to use a Protocol Pack that includes application x.

View and Resolve Policy Compliance Issues

1. From the Cisco SD-WAN Manager menu, choose **Configuration** > **Application Catalog** > **Compliance**.

   In the **Policy Compliance** area, the table shows the policies that do not comply with the application lists in the current Protocol Pack.

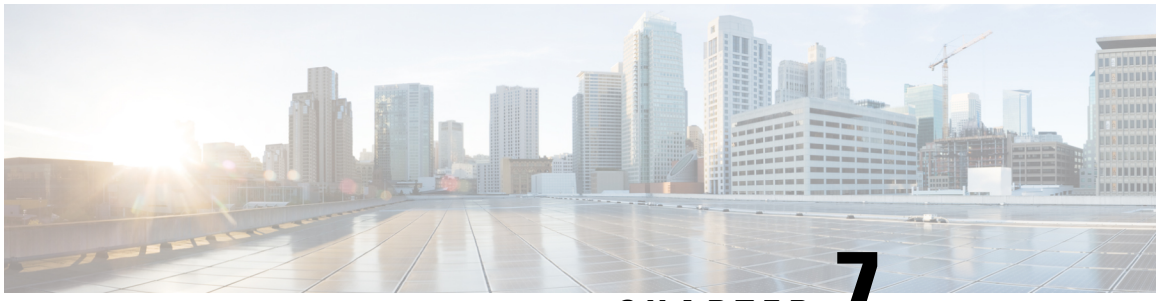
2. In the **Policy Compliance** area, click **...** in the **Actions** column adjacent to the policy you want to update and choose one of these:

   - **Update Application**: Automatically updates the relevant application lists used by affected policies to incorporate the new application or applications.

Note

- Ensure that all devices in the network are using Cisco IOS XE Catalyst SD-WAN Release 17.14.1a or later. If there are devices in the network using earlier releases, updating applications may cause a failure in employing a policy.
- For policies created using policy groups, this action does not deploy the policy to the devices. In this case, to update devices to use the adjusted policy, deploy the policy manually to the devices.

- **Change Policy**: Opens the policy to enable you to manually edit the policy and address the use of the affected application.



CHAPTER 7

Topology

- Topology, on page 75
- Information About Topology, on page 75
- Prerequisites for Topology , on page 76
- Create Topology, on page 76
- Activate the Topology, on page 81

Topology

Table 21: Feature History

Feature Name	Release Information	Description
Topology	Cisco IOS XE Catalyst SD-WAN Release 17.12.1a Cisco Catalyst SD-WAN Manager Release 20.12.1	This feature allows you to provision a **Mesh** or a **Hub and Spoke** topology policy which is applied to Cisco Catalyst SD-WAN Controllers. This allows exchange of data traffic between two or more Cisco IOS XE Catalyst SD-WAN devices.
Region Support for Topology	Cisco IOS XE Catalyst SD-WAN Release 17.15.1a Cisco Catalyst SD-WAN Manager Release 20.15.1	Apply advanced and custom topologies to a specific MRF region or a group of MRF regions. Create match conditions within custom topologies to match them with MRF region(s).

Information About Topology

Create the network structure to apply the policy group to, by configuring the topology so that all devices within a service VPN can communicate with each other. You can also edit existing topologies in this window. You can create the following types of topology and customize them:

- **Hub and Spoke**

- **Mesh**

Prerequisites for Topology

Before you begin configuring policy groups, ensure that the following requirements are met:

- Minimum software version for Cisco IOS XE Catalyst SD-WAN devices: Cisco IOS XE Catalyst SD-WAN Release 17.8.1a
- Ensure that granular RBAC for topology groups is specified by expanding it. With specific permissions to the usergroup, ensure that you are able to access policy groups from **Configuration** > **Topology**.
  1. From the Cisco SD-WAN Manager menu, choose **Administration** > **Manage Users** > **User Groups**.
  2. Click **Add User Group**.
  3. Enter **User Group Name**.
  4. Select the **Read** or **Write** check box against the topology group and device feature that you want to assign to a user group.
  5. Click **Add**.

Create Topology

To create a topology, click **Create Topology** and provide a name, and description and click **Create**. To edit an existing topology, click the ellipsis icon to the right of the topology under **Action** and click **Edit**. When you have created a topology, click **Add Topology** and select from the following options:

- **Hub and Spoke**
- **Mesh**

Hub and Spoke

In a hub and spoke configuration, devices at the branches and remote offices connect directly to specific devices and will not create tunnels to other devices. Communication is available through the configured VPN hubs.

Table 22: Hub and Spoke

Field	Description
Name	Enter a name for the Hub and Spoke topology. This field is mandatory.
VPN	Select a value for the VPN from the drop-down list. This field is mandatory.
Hub Sites	Click **Add hub sites** to select hub sites to add to the topology.

Field	Description
Spoke Sites	Click **Add Spoke Group** to select spoke sites to add to the topology. To add a spoke site, at least one hub site must be added.

Mesh

In a mesh configuration, devices at the branch or remote office are configured to connect directly to other devices in the organization that are also in mesh mode along with spoke devices that are configured to use as a hub.

Table 23: Mesh

Field	Description
Name	Enter a name for the Mesh topology.
VPN	Select a value for the VPN from the drop-down list.
Sites	[Optional] Click **Add sites** to add sites to the mesh topology.

Once you have created either a Hub and Spoke or Mesh topology, you can customize the topology by clicking **Customize Topology**. This migrates your current hub and spoke or mesh topology policy to a platform where you can customize the policy.

Custom Topology

This option allows you to configure Routes or TLOC policies, where you can specify the policy rules and match–action pairings to perform when a match occurs.

Table 24: Topology Attributes

Policy Type	Usage
Name	Name of the custom topology.
VPNs	The Used by data-policy and app-route-policy to list the VPNs for which the policy is applicable.
Level	Starting from Cisco Catalyst SD-WAN Manager Release 20.15.1, you can choose a **Level** for your topology and choose between **Sites** and **Regions**.
InBound Sites	[Optional] Specify the route advertisements that the Cisco Catalyst SD-WAN Controller receives from the devices.
OutBound Sites	[Optional] Specify the route advertisements that the Cisco Catalyst SD-WAN Controller sends to the devices.
Inbound Regions	When you choose **Level** as **Regions**, choose an inbound region from the list of regions.

Policy Type	Usage
Outbound Regions	When you choose **Level** as **Regions**, choose an outbound region from the list of regions.
Role	Choose between **Border** and **Edge** as a role for the router.

Click **Add Rules** to configure Route or TLOC policy match–action pairings that are numbered and are examined in sequential order. When a match occurs, the action is performed, and the policy analysis on that route or packet terminates. Some types of policy definitions apply only to specific VPNs.

You can configure more sequence rules, as needed and drag and drop to re-order them.

Table 25: Match

Match Condition	Description
Color	One or more colors. The available colors are: 3G, biz-internet, blue, bronze, custom1, custom2, custom3, default, gold, green, LTE, metro-ethernet, MPLS, private1 through private6, public-internet, red, and silver.
Community	Specify communities and community numbers.
Expanded Community	List of one or more BGP communities. In the **Community List** field, you can specify the following: • **aa:nn**: AS number and network number. Each number is a 2-byte value with a range from 1 to 65535. • **internet**: Routes in this community are advertised to the internet community. This community comprises all BGP-speaking networking devices. • **local-as**: Routes in this community are not advertised outside the local AS. • **no-advertise**: Attach the NO_ADVERTISE community to routes. Routes in this community are not advertised to other BGP peers. • **no-export**: Attach the NO_EXPORT community to routes. Routes in this community are not advertised outside the local AS or outside a BGP confederation boundary. To configure multiple BGP communities in a single list, include multiple **community** options, specifying one community in each option.

Match Condition	Description
OMP Tag	Tag value that is associated with the route or prefix in the routing database on the device. The range is 0 through 4294967295.
Origin	Protocol from which the route was learned.
Originator	IP address from which the route was learned.
Path Type	In a Hierarchical Cisco Catalyst SD-WAN architecture, match a route by its path type, which can be one of the following: • **Hierarchical Path**: A route that includes hops from an access region to a border router, through region 0, to another border router, then to an edge router in a different access region. • **Direct Path**: A direct path route from one edge router to another edge router. • **Transport Gateway Path**: A route that is reoriginated by a router that has transport gateway functionality enabled.
Preference	The preference value that the route or prefix has in the local site, that is, in the routing database on the device. A higher preference value is more preferred. The range is 0 through 255.
Prefix List	One or more prefixes. Specifies the name of a prefix list.
Region	Starting from Cisco Catalyst SD-WAN Manager Release 20.15.1, one or more region identifiers.
Site	One or more overlay network site identifiers.
TLOC	Individual TLOC address.
VPN	Individual VPN identifier. The range is 0 through 65535.

The **Reject** option is selected by default.

Table 26: Action

Match Condition	Description
Affinity	Specify the
Community	Specify communities and community numbers.

Match Condition	Description
Export To	Select a VPN list, or create a new one.
OMP Tag	Enter the OMP route tag. The range is 0 through 4294967295.
Preference	Enter the preference number for the route, a number between 0-4294967295.
Service	Enter the following information: **Type**: Select a service type from the following options: • **Firewall** • **Intrusion Detection Prevention** • **Intrusion Detection System** • **Net Service 1** • **Net Service 2** **VPN**: Enter the number of the Service VPN. **TLOC IP**: Enter the IP address of the Service TLOC. **Color**: Select a color type from the drop-down list. **Encapsulation**: Select **IPSEC** or **GRE** as the encapsulation type. **TLOC List**: Select a service TLOC list from the drop-down list, or create a new one.
TLOC	Individual TLOC address.

Match Condition	Description
TLOC Action	Select an action from the following option in the drop-down list: • **Strict**: Direct matching traffic only to the intermediate destination. With this action, if the intermediate destination is down, no traffic reaches the final destination. If you do not configure a set tloc-action action in a centralized control policy, strict is the default behavior. • **Primary**: First direct matching traffic to the intermediate destination. If that driver is not reachable, then direct it to the final destination. With this action, if the intermediate destination is down, all traffic reaches the final destination. • **Backup**: First direct matching traffic to the final destination. If that driver is not reachable, then direct it to the intermediate destination. With this action, if the source is unable to reach the final destination directly, it is possible for all traffic to reach the final destination via the intermediate destination. • **Equal Cost Multi-path**: Equally direct matching control traffic between the intermediate destination and the ultimate destination. With this action, if the intermediate destination is down, all traffic reaches the ultimate destination.

Click **Save Match and Actions** to commit your changes and click **Save** to add the customization.

Activate the Topology

When you have created a topology, you must activate the topology for it to take effect. By activating the topology, you create the new network structure, and as a result also deactivate any existing topology. .

1. To activate the topology, click the ellipsis icon to the right of the topology and click **Activate**
2. Click **Preview CLI** and select a device from the left pane to view the configuration difference.
3. Click **Deploy** to deploy the topology group to the Cisco SD-WAN Control Components.

To deactivate the topology, click the ellipsis icon next to the topology and click **Deactivate** and **Deploy**.

Note After you deploy a topology group, any change to the topology group is deployed to the Cisco SD-WAN Controller.