Policy Configuration Tagging

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.

Table 1: Feature History

Feature Name	Release Information	Description
Support for Cisco Catalyst SD-WAN Policy Configuration Tagging Using the Cisco Catalyst SD-WAN Controller CLI Template	Cisco IOS XE Catalyst SD-WAN Release 17.9.1a Cisco vManage Release 20.9.1	This feature allows you to group multiple policy objects under a tag. The tag mechanism, when used in Cisco Catalyst SD-WAN centralized or localized policies, provides the following functionalities: • Controls the download speed of a policy between the Cisco Catalyst SD-WAN Controller and the Cisco IOS XE Catalyst SD-WAN devices. • Improves management of defined lists in the Cisco Catalyst SD-WAN Controller. • Better organizes the configurations of the intent-based network.

Supported Devices for Policy Configuration Tagging

Table 2: Supported Devices and Releases

Release	Supported Devices
Cisco IOS XE Catalyst SD-WAN Release 17.9.1a and later	• Cisco Catalyst 8500 Series Edge Platforms • Cisco Catalyst 8300 Series Edge Platforms • Cisco Catalyst 8200 Series Edge Platforms • Cisco Catalyst 8200 uCPE Series Edge Platforms • Cisco ASR 1000 Series Aggregation Services Routers • Cisco ISR 1000 and ISR 4000 Series Integrated Services Routers (ISRs) • Cisco ISR 1100 and ISR 1100X Series Integrated Services Routers (ISRs) • Cisco IR1101 Integrated Services Router Rugged • Cisco CSR 1000v Series Cloud Services Routers (CSR 1000V) • Cisco Catalyst 8000V Edge Software (Catalyst 8000V)

For details on supported models for each of these device families, refer to Cisco SD-WAN Device Compatibility page.

Restrictions for Policy Configuration Tagging

- Only data-prefix-lists, data-ipv6-prefix-lists, and app-lists tag members are supported.
- Configuration of both direction and direction-less tags within the same TAG is not supported.
- Configuration of tags using only Cisco SD-WAN Controller CLI templates is supported.
- Multi-tenancy is not supported.
- Configuration of number of tags is limited to maximum of 255.
- Configuration of objects per tag is limited to 64.

Information About Policy Configuration Tagging

The policy configuration tagging feature allows you to group policy objects and to assign tag values to various traffic flows by defining a policy. You can name the tags based on the functionality of the policy objects used to achieve the intent-based network configurations. These tags that are provisioned through the Cisco SD-WAN Controller are used in the policy rules for traffic classification.

You can assign unique tag IDs while creating each of the tags.

You can define members under a tag name, which are referenced directly under tag objects. The members can be directional or directionless. Supported tag member types are:

- Data-prefix-list
- Data-ipv6-prefix-list
- App-list

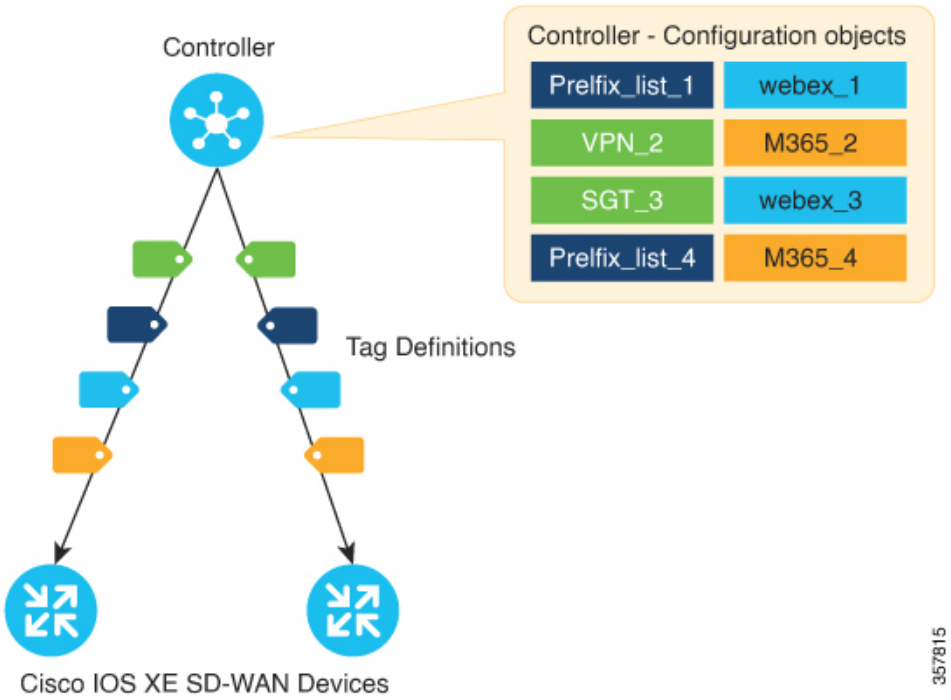
Data-prefix-list and data-ipv6-prefix-list are directional attributes, which are matched as source or destination keywords in the data-policy match statements. App-list is a directionless attribute. You can use directionless keyword such as application id in the app-list policy match statements. Directional and directionless attributes cannot be grouped under the same tag.

You can apply the configured tags in a match criterion under localized and centralized policies. Devices process the tag configurations and apply the configurations to the data plane when the tag is referenced in the policy.

You can use the configuration type feature to tag objects in a configuration. The configuration tags are used in Cisco Catalyst SD-WAN centralized policy such as data policy, and app-aware routing policy and localized access-list policy. The following tag attributes are used in a policy match sequence statement:

- Source-tag-instance
- Destination-tag-instance
- Tag-instance

Figure 1: Policy Configuration Tagging in a Cisco Catalyst SD-WAN Network



As shown in the figure, at the Cisco SD-WAN Controller you can configure the tags using the policy objects with unique tag IDs. Once the tag IDs are assigned these tags are pushed to the Cisco IOS XE Catalyst SD-WAN devices in the network, which reference these tags. The devices then extract the policy list objects from the tags, which are used in the policy rules.

Features of Policy Configuration Tagging

- Supports only configuration type tag.
- Supports tagging a group of objects configuration.
- Supported tag members are data-prefix-lists, data-ipv6-prefix-lists, and app-lists.
- Supports defining configuration tags through a tag-centric model called **Defined Tag**.
- Supports adding configuration only through Cisco SD-WAN Controller CLI templates from Cisco SD-WAN Manager.

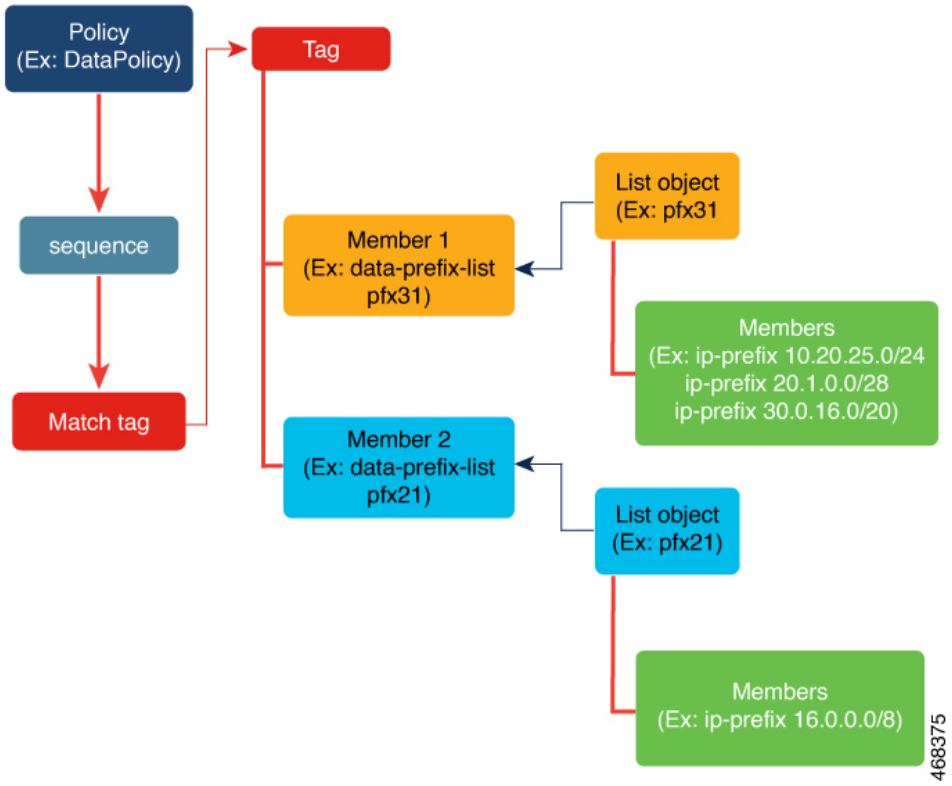
Tag Workflow

1. In Cisco SD-WAN Controller, create a tag that is based on the network intent.
2. Add the following policy list object members:
   - Data-prefix for each location
   - App-lists for applications

   The policy list objects can be defined anytime in the workflow, even after adding them in the tag instances.

3. Push these tags to the Cisco IOS XE Catalyst SD-WAN devices in the network.
4. Create a policy with multiple match sequences and include the tag objects in the Cisco Catalyst SD-WAN data-policy, app-aware-routing policy, and access-list policy.
5. If you add or remove a tag, the status is automatically reflected in the policy.
6. Update the policy to include new tag objects.

Figure 2: Tagging Workflow with Examples



Benefits of Policy Configuration Tagging

The benefits of using policy configuration tagging are:

- Enables reusability of policy objects.
- Enables faster policy download on a device with reduced configuration size and sequences.
- Tag sharing across different policies is supported.
- Enables visibility or corelation across the network in a user-defined intent.
- Controls the policy configuration download speed between the Cisco SD-WAN Controller and the Cisco IOS XE Catalyst SD-WAN devices.
- Improves management of the defined lists in the controller.

- Better organization of the configurations for the intent-based network.

Configure Policy Configuration Tagging Using a CLI Template

Before You Begin

Ensure that the controllers and the edge devices are all updated to the latest versions—Cisco Catalyst SD-WAN Control Components Release 20.9.x, Cisco vManage Release 20.9.1, and Cisco IOS XE Catalyst SD-WAN Release 17.9.1a.

Configure Policy Configuration Tagging Using a CLI Template

For more information about using CLI templates, see CLI Add-On Feature Templates and CLI Templates.

Note By default, CLI templates execute commands in global config mode.

This section provides example CLI configurations to configure tag-instances and centralized policy using Cisco SD-WAN Controller CLI templates.

Creating Policy Configuration Tagging

1. Configure a new object tag-instance on Cisco SD-WAN Controller:

   tag-instances [tag-instance] [lists]

2. Create tag-instance with member attributes such as app-lists, data-ipv6-prefix-list, and data-prefix-list. Configure tag instances with a global unique ID for each of the tag names. The tag configuration is pushed to only those devices which reference these TAGs:

   tag-instance *tag-instance-name* [**id** *global-unique-id*][**app-list** *app-list-name*] [**data-prefix-list** *prefix-list-name*] [**data-ipv6-prefix-list** *ipv6-prefix-list-name*]

3. Configure tag-instance lists:

   lists[**app-list** *app-list-name*] [**data-prefix-list** *prefix-list-name*] [**data-ipv6-prefix-list** *ipv6-prefix-list-name*]

Adding Tag-Instances in a policy match criteria

1. Configure localized access-list policy (ACLs and IPv6 ACLs) to include destination or source tag instances in matching attributes:

   match [**destination-tag-instance** *dest-tag-name* | **source-tag-instance** *src-tag-name*]

2. Configure centralized data policy to include destination-tag-instance, source-tag-instance, or tag-instance in matching attributes:

   match [**destination-tag-instance** *dest-tag-name* | **source-tag-instance** *src-tag-name* | **tag-instance** *tag-name*]

3. Configure centralized Application Aware Route (AAR) policy to include destination-tag-instance, source-tag-instance, or tag-instance in matching attributes:

match[**destination-tag-instance** *dest-tag-name* | **source-tag-instance** *src-tag-name* | **tag-instance** *tag-name*]

Here's the complete configuration example for creating tag-instances, including the tag instances as matching attribute in localized and centralized policies:

```
****Tag Configuration*****
tag-instances
 tag-instance blue
  id  2000
  data-ipv6-prefix-list v6_pfx1 v6_pfx2
 !
 tag-instance orange
  id  3000
  app-list appl1 appl2
 !
 lists
  data-prefix-list pfx1
   ip-prefix 10.0.0.1/32
  !
  data-ipv6-prefix-list v6_pfx1
   ipv6-prefix 2001::1/128
  !
  app-list appl1
   app amazon
  !
 !
!
****Localized Policy****
policy
 lists
  data-prefix-list pfx1
   ip-prefix 10.20.24.0/24
  !
 !
 access-list acl
  sequence 10
   match
    source-tag-instance blue
   !
   action accept
    count acl_input_wc
   !
  !
  default-action drop
 !
!
****Centralized Policy *****
policy
data-policy DP1
  vpn-list vpn1
   sequence 100
    match
     tag-instance orange
    !
    action accept
    !
   !
   sequence 200
    match
     source-tag-instance blue
    !
```

```
   action drop
    count count1
   !
  !
  sequence 300
   match
    destination-tag-instance blue
   !
   action accept
   !
```

Verify Tag-Instances Configuration Using the CLI

The following is a sample output from the **show sdwan tag-instances from-vsmart** command displaying the downloaded tags from Cisco SD-WAN Controller on Cisco IOS XE Catalyst SD-WAN device:

```
Device# show sdwan tag-instances from-vsmart
tag-instances-from-vsmart
 tag-instance APP_facebook_TAG9
  id       60000
  app-list apps_facebook
 tag-instance APP_office_TAG10
  id       70000
  app-list apps_ms apps_zoom
 tag-instance APP_webex_TAG8
  id       50000
  app-list apps_webex
 lists data-prefix-list multicast_pfx
  ip-prefix 10.10.20.30/8
 lists data-prefix-list pfx1
  ip-prefix 10.20.24.0/24
 lists data-prefix-list pfx21
  ip-prefix 172.16.10.10/8
 lists data-prefix-list pfx22
  ip-prefix 172.16.20.20/16
  ip-prefix 192.168.10.20/8
 lists data-ipv6-prefix-list v6_pfx1
  ipv6-prefix 2001::/64
 lists data-ipv6-prefix-list v6_pfx21
  ipv6-prefix 2001::1/128
  ipv6-prefix 2001::/64
 lists app-list apps_facebook
  app dns
  app facebook
 lists app-list apps_ms
  app ms-office-365
  app ms-office-web-apps
  app ms-services
  app ms-teams
  app pop3
 lists app-list apps_webex
  app sip
  app webex-audio
  app webex-control
  app webex-media
  app webex-meeting
  app webex-video
 lists app-list apps_zoom
  app zoom-meetings
```

The following is a sample output from the **show sdwan policy from-vsmart** command displaying the policy that is downloaded from the Cisco SD-WAN Controller on Cisco IOS XE Catalyst SD-WAN device:

```
Device# show sdwan policy from-vsmart
from-vsmart sla-class SLA1
 latency 100
from-vsmart data-policy DATA_POLICY
 direction from-service
 vpn-list vpn_1
  sequence 11
   match
    destination-port         5060
    protocol                 17
    source-tag-instance      DP_V4_TAG1
    destination-tag-instance DP_V4_TAG3
   action accept
    count src_dst_legacy_v4
  sequence 21
   match
    source-tag-instance DP_V4_TAG1
   action drop
    count src_v4
  sequence 31
   match
    source-tag-instance      DP_V4_TAG2
    destination-tag-instance DP_V4_TAG3
    tag-instance             APP_webex_TAG8
   action drop
    count src_dst_app_v4
  sequence 41
   match
    source-tag-instance      DP_V4_TAG1
    destination-tag-instance DP_V4_TAG3
    tag-instance             APP_facebook_TAG9
   action accept
    count src_dst_app2_v4
```

The following is a sample output from the **show platform software common-classification** command displaying the tag information from a forwarding manager on a forwarding plane (FMAN-FP):

```
Device# show platform software common-classification F0 tag all
Total Number of TAGs: 9
tag id       tag name              tag type     num clients  num sets     num member types
  total members
-------------------------------------------------------------------------------------------------
900          special_TAG7          Per Type OR  0            2            1
  2
10000        DP_V4_TAG1            Per Type OR  1            1            1
  1
11000        DP_V4_TAG2            Per Type OR  1            2            1
  2
12000        DP_V4_TAG3            Per Type OR  1            6            1
  6
20000        DP_V6_TAG4            Per Type OR  1            1            1
  1
21000        DP_V6_TAG5            Per Type OR  1            2            1
  2
50000        APP_webex_TAG8        Per Type OR  1            1            1
  1
60000        APP_facebook_TAG9     Per Type OR  1            1            1
  1
70000        APP_office_TAG10      Per Type OR  1            2            1
  2
```

```
Device# show platform software common-classification f0 tag 1 summary
TAG ID: 1
TAG TYPE: Per Type OR
TAG Name: net1
Is Dummy: F

client data:
  client id     client name
  ----------------------------------
  166           SDWAN

member data:
  Prefix List           6
  App List              3
```

```
Device# show platform software common-classification f0 tag 1 prefixList
 member details:
  member detail type    member id     member data
  ------------------------------------------------
  IPv4 Prefix List      65537         100
  IPv6 Prefix List      65538         101
  IPv4 Prefix List      65540         103
  IPv6 Prefix List      65541         104
  IPv6 Prefix List      65544         107
  IPv4 Prefix List      65546         109
```

```
Device# show platform software common-classification f0 tag 1 appList
 member details:
  member detail type    member id     member data
  ------------------------------------------------
  App List              65539         102
  App List              65542         105
  App List              65545         108
```

```
Device# show platform software common-classification f0 tag 1 set
Total Number of SETs: 18
  Set ID        member detail type    member id     member data
  ------------------------------------------------------------
  1             IPv4 Prefix List      65537         100
  1             App List              65539         102
  2             IPv4 Prefix List      65537         100
  2             App List              65542         105
  3             IPv4 Prefix List      65537         100
  3             App List              65545         108
  4             IPv6 Prefix List      65538         101
  4             App List              65539         102
  5             IPv6 Prefix List      65538         101
```