



# CLI Templates For Cisco IOS XE Catalyst SD-WAN Devices

- [CLI templates for Cisco IOS XE Catalyst SD-WAN devices, on page 1](#)
- [Benefits of CLI templates, on page 2](#)
- [Limitations of CLI templates, on page 2](#)
- [CLI templates in Cisco SD-WAN Manager, on page 3](#)
- [Sample configurations for CLI templates, on page 6](#)

## CLI templates for Cisco IOS XE Catalyst SD-WAN devices

**Table 1: Feature History Table**

| Feature Name                             | Release Information  | Description   |
|--|--|---|
| Device Configuration CLI Templates       | Cisco IOS XE Catalyst SD-WAN Release 17.2.1r<br>Cisco vManage 20.1.1 | The CLI Templates feature has been updated to support device configuration-based CLIs. You can use these templates to push the device configuration (yang-cli) to devices directly. |
| CLI Template for Cisco XE SD-WAN Routers | Cisco IOS XE Release 16.11.1a<br>Cisco SD-WAN release 19.1           | The CLI Templates for Cisco IOS XE Catalyst SD-WAN device features allow to you configure intent-based CLI templates for Cisco XE SD-WAN routers using Cisco SD-WAN Manager.        |
| VRF Configuration                        | Cisco IOS XE Catalyst SD-WAN Release 17.2.1r                         | Support for VRF configuration increased from a total of 100 to a total of 300 VRFs.<br><br>Supported on: Cisco ASR 1001-HX and Cisco ASR 1002-HX                                    |

You can configure CLI templates for Cisco IOS XE Catalyst SD-WAN devices in the following ways:

- [Device Configuration-Based CLI Templates for Cisco IOS XE Catalyst SD-WAN Devices](#)
- [Intent-Based CLI Templates for Cisco IOS XE Catalyst SD-WAN Devices](#)




---

**Note** If you generate a CLI template in a higher version of Cisco SD-WAN Manager and then try to apply it in a lower version, it may not be supported depending on the configuration. In this case, Cisco SD-WAN Manager might also deny access and generate an error message. It is recommended that you use a CLI template generated in an earlier version of Cisco SD-WAN Manager. For example, if you are using Cisco vManage Release 20.7.x, you can use a CLI template generated in Cisco vManage Release 20.6.x and earlier releases.

---

## Benefits of CLI templates

- You can reuse any Cisco vEdge-specific Cisco SD-WAN Manager feature templates for Cisco IOS XE Routers. When you create a device template using Cisco XE SDWAN Feature Templates, Cisco SD-WAN Manager displays the intent-based configuration (vEdge CLI syntax) and the corresponding device-based (Cisco XE SDWAN Routers) configuration. You can examine the intent-based configuration and repurpose that to create a separate CLI template for XE SDWAN routers.
- You can make multiple changes to a CLI template in a single edit.
- You can use a single configuration across multiple devices of the same device models. Variables can be used for rapid bulk configuration rollout with unique per-device settings. Common configurations like system-IP, site-id, hostname, IP addresses, and so on, can be defined as editable variables in the template and the same template can be attached to multiple devices.
- You can define custom length for variables in CLI Templates.
- You can use any existing IOS-XE device intent configuration as input for CLI template.
- Content of a CLI template can be used across multiple IOS-XE device types (common CLIs like VPN, VPN interface, BGP, OSPF and so on).

## Limitations of CLI templates

**Auxiliary ports:** When using a CLI template for Cisco Integrated Services Routers that have an auxiliary port, do not include commands for auxiliary ports, such as `line aux 0`. Doing so results in an error. These commands may be executed directly on the device.

When you import the CLI template configuration using the command, `show sdwan running-config`, you need to add quotes manually for the CLI template on the Cisco SD-WAN Manager.

From Cisco IOS XE Catalyst SD-WAN Release 17.12.x, policies configured using a Cisco Catalyst SD-WAN Controller template are ignored. To configure policies, navigate to **Configuration > Policies > Custom Options > CLI Policy**, add the policy and activate it for Cisco Catalyst SD-WAN Controller.

# CLI templates in Cisco SD-WAN Manager

You can configure CLI templates in Cisco SD-WAN Manager using these two methods:

- [Device configuration-based CLI templates for Cisco IOS XE Catalyst SD-WAN devices](#)
- [Intent-based CLI templates for Cisco IOS XE Catalyst SD-WAN devices](#)

## Device configuration-based CLI templates for Cisco IOS XE Catalyst SD-WAN devices

A device configuration-based CLI Template for Cisco IOS XE Catalyst SD-WAN devices is a configuration management tool that:

- enables Cisco SD-WAN Manager (vManage 20.1.1 and later) to specify CLI templates using yang-cli,
- pushes only the difference between device and template configurations to Cisco IOS XE Catalyst SD-WAN devices, and
- provides a preview of configuration changes before deployment.

These templates are used alongside feature templates and policies, including localized and security policies, in Cisco SD-WAN Manager.



- 
- Note** To configure features not accessible using Cisco SD-WAN Manager, we recommend doing the following:
1. Use the relevant feature template in addition to a CLI add-on feature template.
  2. For situations where the previous option is not sufficient, use the device configuration-based CLI templates as described in this section.
- 

## Configure device configuration-based CLI templates

### Procedure

---

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

**Note**

In Cisco SD-WAN Release 20.7.x and earlier releases, **Device Templates** is titled as **Device**.

**Step 2** From the **Create Template** drop-down list, select **CLI Template**.

**Step 3** From the **Device Model** drop-down list, select the type of device for which you are creating the template.

**Step 4** In the **Template Name** and **Template Description**, enter a name upto 128 alphanumeric characters and a description upto 2048 alphanumeric characters.

**Step 5** Choose **Device configuration**. Using this option, you can provide IOS-XE configuration commands that appear in the output of the `show sdwan running-config` command.

(Optional) To load the running config of a connected device, select it from the Load Running config from reachable device list and click **Search**.

**Step 6** In **CLI Configuration**, enter the configuration either by typing it, cutting and pasting it, or uploading a file.

**Step 7** To convert an actual configuration value to a variable, select the value and click **Create Variable**. Enter the variable name, and click **Create Variable**.

You can also type the variable name directly, in the format `{{variable-name}}`; for example, `{{hostname}}`.

These variables can be filled in device variables page per device after attaching the template. Values can be entered manually or can be uploaded via a csv file.

**Step 8** Click **Add** to save the feature template.

---

The new device template is displayed in the Device Template table.

## Intent-based CLI templates for Cisco IOS XE Catalyst SD-WAN devices

An intent-based CLI Template for Cisco IOS XE Catalyst SD-WAN devices is a configuration management tool that:

- allows Cisco SD-WAN Manager to configure CLI templates using intent-based commands,
- supports vEdge device syntax for command input, and
- pushes vEdge syntax-based commands to Cisco IOS XE Catalyst SD-WAN devices in IOS XE syntax.

Intent-based CLI templates enable configuration of Cisco IOS XE Catalyst SD-WAN devices using vEdge syntax via Cisco SD-WAN Manager.

With the support of device configuration-based CLI templates, the intent-based CLI templates will be deprecated. We recommend using the device configuration-based CLI templates as described in Device Configuration-Based CLI Templates for Cisco IOS XE Catalyst SD-WAN Devices.

Using Cisco SD-WAN Manager CLI templates significantly reduces the effort to configure feature templates.

## Configure intent-based CLI templates

### Procedure

---

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

#### Note

In Cisco SD-WAN Release 20.7.x and earlier releases, **Device Templates** is titled as **Device**.

**Step 2** From the **Create Template** drop-down list, select **CLI Template**.

**Step 3** From the **Device Model** drop-down list, select the type of device for which you are creating the template.

**Step 4** In the **Template Name** and **Template Description**, enter a name upto 128 alphanumeric characters and a description upto 2048 alphanumeric characters.

**Step 5** The configuration of the CLI template can either be intent-based or based on the device configuration:

- **Intent:** If you specify **Intent**, you specify commands in the Cisco vEdge format. If the device you've selected is a Cisco IOS XE Catalyst SD-WAN device, Cisco SD-WAN Manager converts the configuration for the device.
- **Device configuration:** This option is available from Cisco IOS XE Catalyst SD-WAN Release 17.2.1r and onwards and only for Cisco IOS XE Catalyst SD-WAN devices. For this option, you must specify the entire device configuration as it appears in `show sd-wan running config`.

**Note**

You can only use this feature with the qualified CLIs described in the *Cisco IOS XE Catalyst SD-WAN Qualified Command Reference Guide*.

**Example:**

You can upload a configuration file using **Select a File** or copy and paste the CLI configuration. Following is an example of an intent-based CLI with variables.

```
system

  host-name {{hostname}}
  system-ip {{system_ip}}
  domain-id 1

  site-id {{site_id}}
  port-offset      1
  admin-tech-on-failure
  organization-name "XYZ"
  logging
  disk
  enable

! !
```

These variables can be filled in device variables page per device after attaching the template. Values can be entered manually or can be uploaded via a csv file.

**Step 6** To save the feature template, click **Add**.

---

## What to do next

# Sample configurations for CLI templates

## System level configuration

*Table 2: System level parameters*

| CLI Template Configuration  | Configuration on the Device   |
|---|---|
| <pre> system  host-name pm4  system-ip 172.16.255.14  overlay-id 1  site-id 400  control-session-pps 300  admin-tech-on-failure  sp-organization-name "XYZ Inc Regression" organization-name "XYZ Regression" console-baud-rate 115200 vbond 10.0.12.26 port 12346 </pre> | <pre> system  host-name pm4  system-ip 172.16.255.14  overlay-id 1  site-id 400  control-session-pps 300  admin-tech-on-failure  sp-organization-name "XYZ Inc Regression"  organization-name "XYZ Inc Regression"  console-baud-rate 11520  vbond 10.0.12.26 port 12346 </pre> |

### AAA Configuration - authentication, authorization, and accounting (AAA) with RADIUS and TACACS+

Table 3: AAA configuration

| CLI Template Configuration   | Configuration on the Device  |
|--|--|
| <pre> aaa auth- order local radius tacacs usergroup basic   task system read write   task interface read write ! usergroup netadmin ! usergroup operator task system read task interface read task policy read task routing read task security read ! user admin password  \$6\$nbblkA==\$ae/DO78l/wluPUohhBU2L6h/ Q.PLkurGvxjRlS9OWB9iTtFwSGNQcABV6F MW57vuEHvo3zp3qdYVinLmMIu/p/ secret \$9\$3/IL3/UF2F2F3E\$J9NBekLwrc9ExtHk6FSVAiDMOfD.QEAmM&amp;Dkz.c  !! radius server 10.99.144.200   source-interface GigabitEthernet0/0/1 exit server 10.99.144.201    source-interface GigabitEthernet0/1/0 exit ! tacacs server 10.0.1.1 auth-port 50 vpn 0 source-interface GigabitEthernet0/0/1 key 1 secret-key \$8\$Kcuva0CM871E8czESwV5g/YX4Q8pY1LSNk/+PIDrPcg=  exit ! ! </pre> | <pre> aaa group server tacacs+ server-10.0.1.1   server-private 10.0.1.1 timeout 5 key   \$8\$vs5hzVg/Z6EeuUdNHTzOwWPsUv9V/50xmcRfShWp3YI=    ip tacacs source-interface   GigabitEthernet0/0/1 ! aaa group server radius server-10.99.144.200   server-private 10.99.144.200 auth-port 1812   timeout 5 retransmit 3   ip radius source-interface   GigabitEthernet0/0/1 ! aaa group server radius server-10.99.144.201    server-private 10.99.144.201 auth-port 1812   timeout 5 retransmit 3   ip radius source-interface   GigabitEthernet0/1/0 ! aaa authentication login default local group radius group tacacs+ aaa authorization exec default local group radius group tacacs+ a aa session-id common --- added by default  username admin privilege 15 secret 9 \$9\$3/IL3/UF2F2F3E\$J9NBekLwrc9ExtHk6FSVAiDMOfD.QEAmM&amp;Dkz.c </pre> |

**Logging configuration - configures logging to either the local hard drive or a remote host****Table 4: Logging configuration**

| CLI Template Configuration   | Configuration on the Device  |
|--|--|
| <pre> logging   disk     enable     file size 12     file rotate 6   ! server 192.168.13.1   vpn          0   source-interface Loopback1   priority     alert exit !</pre> | <pre> logging   disk     enable   ! logging persistent size 75497472 filesize 12582912   logging buffered 512000 --- added by default  logging host 192.168.13.1 no logging rate-limit logging source-interface Loopback1 logging persistent</pre> |

**Switch port and VLAN configuration****Table 5: Switch port configuration**

| CLI Template Configuration   | Configuration on the Device   |
|--|---|
| <pre> interface GigabitEthernet0/1/4   switchport   mode trunk   access vlan vlan 10   access vlan name "DHCP Vlan"   trunk allowed vlan 10   !   no shutdown  vpn 10   name "DHCP VPN"   interface Vlan10     description "Vlan 10 Mgmt interface"     ip address 10.29.35.1/24     no shutdown   ! !</pre> | <pre> interface GigabitEthernet0/1/4   switchport ios-sw:mode trunk   switchport ios-sw:trunk allowed vlan 10   no shutdown   no ip address   exit  interface Vlan10   description Vlan 10 Mgmt interface   no shutdown   arp timeout 1200   vrf forwarding 10   ip address 10.29.35.1 255.255.255.0   ip mtu 1500   exit</pre> |

## Cellular configuration

**Table 6: Cellular configuration - configures cellular controllers and cellular interfaces**

| CLI Template Configuration   | Configuration on the Device   |
|--|---|
| <pre> vpn 0  interface Cellular0/2/0    description "Cellular interface"    no shutdown  !   controller cellular 0/2/0    lte sim max-retry 1    lte failovertimer 7    profile id 1 apn Broadband  ! </pre> | <pre> interface Cellular0/2/0  description Cellular interface  no shutdown  ip address negotiated  ip mtu 1428  mtu          1500  exit   controller Cellular 0/2/0    lte sim max-retry 1    lte failovertimer 7    profile id 1 apn Broadband authentication  none pdn-type ipv4 </pre> |

**BGP, OSPF, and EIGRP - configures BGP, OSPF, and EIGRP routing protocols under transport or service VPN***Table 7: BGP, OSPF, and EIGRP configuration*

| CLI Template Configuration | Configuration on the Device |
|----------------------------|-----------------------------|
|----------------------------|-----------------------------|

| CLI Template Configuration  | Configuration on the Device |
|---|-----------------------------|
| <pre> vpn1   bgp 2     shutdown     distance external 30     distance internal 250     distance local 10     address-family ipv4-unicast       network 10.0.100.0/24       redistribute static route-policy     route_map       redistribute connected route-policy     route_map       !       neighbor 10.0.100.1       no shutdown       remote-as 3       timers         keepalive 12         holdtime 20         connect-retry 300         advertisement-interval 123       !       update-source GigabitEthernet0/0/1       ebgp-multihop 1       password \$8\$9pou4PH9b60B072hcw3MmSSdLCfJk8bVys12lLVb+08=       address-family ipv4-unicast  vpn 1   router     ospf       router-id 172.16.255.15       compatible rfc1583       timers spf 200 1000 10000       redistribute connected route-policy     route_map       max-metric router-lsa administrative       area 23       stub       interface GigabitEthernet0/0/1         cost 23         authentication type message-digest         authentication authentication-key key1        exit     exit   !  vpn 1   router     eigrp 1       af-interface GigabitEthernet0/0/2       no split-horizon       exit-af-interface     !     address-family ipv4 network 10.1.10.1/32     address-family ipv4 topology base     redistribute omp     exit-af-topology </pre> |                             |

| CLI Template Configuration | Configuration on the Device  |
|----------------------------|--|
|                            | <pre> router bgp 2   bgp log-neighbor-changes   distance bgp 30 250 10   address-family ipv4 unicast vrf 1     neighbor 10.0.100.1 remote-as 3     neighbor 10.0.100.1 activate     neighbor 10.0.100.1 ebgp-multihop 1     neighbor 10.0.100.1 maximum-prefix 2147483647 100     neighbor 10.0.100.1 password 0 password     neighbor 10.0.100.1 send-community both     neighbor 10.0.100.1 timers 12 20     neighbor 10.0.100.1 update-source GigabitEthernet0/0/1   network 10.0.100.0 mask 255.255.255.0   redistribute connected   redistribute static route-map route_map   exit-address-family ! timers bgp 60 180  router ospf 1 vrf 1   auto-cost reference-bandwidth 100   max-metric router-lsa   timers throttle spf 200 1000 10000   router-id 172.16.255.15   default-information originate   distance ospf external 110   distance ospf inter-area 110   distance ospf intra-area 110   redistribute connected subnets route-map route_map ! interface GigabitEthernet0/0/1   no shutdown   arp timeout 1200   vrf forwarding 1   ip address 10.1.100.14 255.255.255.0   ip redirects   ip mtu 1500   ip ospf 1 area 23   ip ospf network broadcast   mtu 1500   negotiation auto   exit ! router eigrp eigrp-name   address-family ipv4 vrf 1 autonomous-system 1   af-interface GigabitEthernet0/0/2   hello-interval 5   hold-time 15   no split-horizon exit-af-interface ! network 10.1.10.1 0.0.0.0   topology base   redistribute omp   exit-af-topology ! exit-address-family </pre> |

| CLI Template Configuration | Configuration on the Device |
|----------------------------|-----------------------------|
|                            | !<br>!                      |

**VPN, Interface, and tunnel configuration for WAN and LAN interfaces**

*Table 8: VPN, Interface, and Tunnel configuration*

| CLI Template Configuration   | Configuration on the Device  |
|--|--|
| <pre> vpn 0   interface GigabitEthernet0/2/0     ip address 10.1.14.14/24   tunnel-interface     encapsulation ipsec     color lte     no allow-service bgp     allow-service dhcp     allow-service dns     allow-service icmp     no allow-service sshd     no allow-service netconf     no allow-service ntp     no allow-service ospf     no allow-service stun     allow-service https     !     autonegotiate     no shutdown     !     ip route 0.0.0.0/0 10.1.14.13  vpn 512 interface GigabitEthernet0   ip dhcp-client ipv6 dhcp-client autonegotiate no shutdown ! !                     </pre> | <pre> ip route 0.0.0.0 0.0.0.0 10.1.14.13 1  interface GigabitEthernet0/2/0   no shutdown   arp timeout 1200 - added by default   ip address 10.1.14.14 255.255.255.0   ip redirects --&gt; added by default   ip mtu 1500   mtu 1500   negotiation auto --&gt; added by default   exit  interface Tunnel20 ---&gt; based on the interface 0/2/0   no shutdown   ip unnumbered GigabitEthernet0/2/0   no ip redirects   ipv6 unnumbered GigabitEthernet0/2/0   no ipv6 redirects   tunnel source GigabitEthernet0/2/0   tunnel mode sdwan  sdwan   interface GigabitEthernet0/2/0     tunnel-interface       encapsulation ipsec weight 1       color lte       no last-resort-circuit       vmanage-connection-preference 5       no allow-service all       no allow-service bgp       allow-service dhcp       allow-service dns       allow-service icmp       no allow-service sshd       no allow-service netconf       no allow-service ntp       no allow-service ospf       no allow-service stun  interface GigabitEthernet0   no shutdown   arp timeout 1200   vrf forwarding Mgmt-intf   ip address dhcp client-id GigabitEthernet0 ip   redirects   ip dhcp client default-router distance 1 ip   mtu 1500   mtu 1500   negotiation auto                     </pre> |

## Network Address Translation (NAT) over Direct Internet Access (DIA)

Table 9: NAT over DIA

| CLI Template Configuration   | Configuration on the Device   |
|--|---|
| <pre> vpn 201   interface GigabitEthernet0/0/2.2901     description giga21     ip address 10.201.201.1/24     mtu 1496     no shutdown     vrrp 100       track-omp         ipv4 10.201.201.3     !   !   !   dhcp-server     address-pool 10.201.201.0/24     exclude 10.201.201.1-10.201.201.10     10.201.201.20-10.201.201.22     offer-time 600     lease-time 86400     admin-state up     options       default-gateway 10.201.201.1       dns-servers 10.99.139.201       tftp-servers 10.99.139.201     !   !   !   ip route 0.0.0.0/0 vpn 0   ! vpn 0   interface GigabitEthernet0/0/0     ip address 172.16.10.1/24     nat       udp-timeout 3       tcp-timeout 40       respond-to-ping     !   ! </pre> | <pre> interface GigabitEthernet0/0/2.2901   no shutdown   encapsulation dot1Q 2901   vrf forwarding 201   ip address 10.201.201.1 255.255.255.0   ip mtu 1496   vrrp 100 address-family ipv4     vrrpv2       address 10.201.201.3       priority 100       track omp shutdown   exit   exit  ip dhcp excluded-address vrf 201 10.201.201.1 10.201.201.10 ip dhcp excluded-address vrf 201 10.201.201.20 10.201.201.22 ip dhcp pool vrf-201-GigabitEthernet0/0/2.2901   option 150 ip 10.99.139.201   vrf 201   lease 1 0 0   default-router 10.201.201.1   dns-server 10.99.139.201   network 10.201.201.0 255.255.255.0   exit ip dhcp use hardware-address client-id no ip dhcp use class ip dhcp use vrf remote  ip nat inside source list nat-dia-vpn-hop-access-list interface GigabitEthernet0/0/0 overload   ip nat translation tcp-timeout 40   ip nat translation udp-timeout 3   ip nat route vrf 201 0.0.0.0 0.0.0.0 global  interface GigabitEthernet1/0/2   no shutdown   arp timeout 1200   ip address 10.1.15.15 255.255.255.0   ip nat outside   ip redirects   ip mtu 1500   mtu 1500   negotiation auto </pre> |

**NAT64 configuration****Table 10: NAT64 configuration**

| CLI Template Configuration   | Configuration on the Device   |
|--|---|
| <pre> vpn 1  nat64    v4 pool pool1 start-address 10.1.1.10    v4 pool pool1 end-address 10.1.1.100  !  interface GigabitEthernet3  ip address 10.1.19.15/24  nat64  !  autonegotiate  no shutdown  ! </pre> | <pre> interface GigabitEthernet3  no shutdown  arp timeout 1200  vrf forwarding 1  ip address 10.1.19.15 255.255.255.0  negotiation auto  nat64 enable  nat64 prefix stateful 2001::F/64 vrf 1  nat64 v4 pool pool1 10.1.1.10 10.1.1.100 nat64 v6v4 list global-list pool pool1 vrf 1 nat64 translation timeout tcp 60 nat64 translation timeout udp 1 </pre> |

**Multilink and T1/E1 - configures T1/E1 controller and serial, multilink interfaces****Table 11: Configuring Multilink**

| CLI Template Configuration   | Configuration on the Device   |
|--|---|
| <pre> card type t1 0 2  controller T1 0/2/0    framing esf    clock source internal    linecode b8zs    cablelength long 0db    channel-group 1 timeslots 15    channel-group 2 timeslots 12    channel-group 3 timeslots 10    channel-group 4 timeslots 10  !  interface Multilink1  no shutdown  encapsulation ppp  ip address 10.1.10.30 255.255.255.0  ppp pap sent-username admin password admin  ppp authentication pap  ppp multilink  ppp multilink links minimum 1  ppp multilink fragment disable  ppp multilink group 1  exit  interface Serial0/2/0:1  no shutdown  encapsulation ppp  bandwidth 1536  no ip address  load-interval 30  ppp pap sent-username admin password admin  ppp authentication pap  ppp multilink  ppp multilink group 1  exit </pre> | <pre> interface Multilink1  ip address 10.1.10.30/24 shutdown  controller T1 0/2/0    linecode b8zs    channel-group 1    channel-group 3  !  ppp pap sent-username admin password admin  ppp authentication pap  ppp multilink  ppp multilink group 1 </pre> |

**Local QoS policy***Table 12: Local QoS policy*

| CLI Template Configuration | Configuration on the Device |
|----------------------------|-----------------------------|
|----------------------------|-----------------------------|

| CLI Template Configuration  | Configuration on the Device  |
|---|--|
| <pre> vpn 1  interface GigabitEthernet0/0/1    ip address 10.2.54.15/24    no shutdown    access-list MyACL in    ! policy  class-map  class best-effort queue 3  class bulk-data queue 2  class critical-data queue 1  class voice queue 0  ! access-list MyACL  sequence 10  match   dscp 46   !  action accept   class voice   !  !  sequence 20  match   source-ip      10.1.1.0/24   destination-ip 192.168.10.0/24   !  action accept   class bulk-data   set    dscp 32   !  !  !  sequence 30  match   destination-ip 192.168.20.0/24   !  action accept   class critical-data   set    dscp 22   !  !  !  sequence 40  action accept   class best-effort   set    dscp 0   !  !  !  default-action accept  ! qos-scheduler be-scheduler  class      best-effort  bandwidth-percent 20  buffer-percent 20  drops      red-drop  ! qos-scheduler bulk-scheduler </pre> | <pre> interface GigabitEthernet0/0/1  access-list MyACL in  exit class-map match-any best-effort  match qos-group 3  ! class-map match-any bulk-data  match qos-group 2  ! class-map match-any critical-data  match qos-group 1  ! class-map match-any voice  match qos-group 0  ! policy-map MyQoSMap  class best-effort   random-detect   bandwidth percent 20  !  class bulk-data   random-detect   bandwidth percent 20  !  class critical-data   random-detect   bandwidth percent 40  !  class voice   priority percent 20  !  ! policy  no app-visibility  no flow-visibility  no implicit-acl-logging  log-frequency      1000  class-map  class best-effort queue 3  class bulk-data queue 2  class critical-data queue 1  class voice queue 0  ! access-list MyACL  sequence 10  match   dscp 46   !  action accept   class voice   !  !  sequence 20  match   source-ip      10.1.1.0/24   destination-ip 192.168.10.0/24   !  action accept   class bulk-data   set    dscp 32   !  ! </pre> |

| CLI Template Configuration  | Configuration on the Device  |
|---|--|
| <pre> class          bulk-data bandwidth-percent 20 buffer-percent 20 drops          red-drop ! qos-scheduler critical-scheduler class          critical-data bandwidth-percent 40 buffer-percent 40 drops          red-drop ! qos-scheduler voice-scheduler class          voice bandwidth-percent 20 buffer-percent 20 scheduling    llq ! qos-map MyQoSMap qos-scheduler be-scheduler qos-scheduler bulk-scheduler qos-scheduler critical-scheduler qos-scheduler voice-scheduler ! ! ! ! </pre> | <pre> ! ! sequence 30 match   destination-ip 192.168.20.0/24 ! action accept class critical-data set   dscp 22 ! ! ! sequence 40 action accept class best-effort set   dscp 0 ! ! ! default-action accept ! ! ! ! </pre> |

**Security policy (ZBFW, IPS/IDS, URL-Filtering) configuration****Table 13: Security policy (ZBFW, IPS/IDS, URL-Filtering)**

| CLI Template Configuration   | Configuration on the Device |
|--|-----------------------------|
| <pre> policy   zone internet     vpn 0     !   zone zone1     vpn 1     !   zone zone2     vpn 2     !   zone-pair ZP_zone1_internet_fw_policy     source-zone    zone1     destination-zone internet     zone-policy    fw_policy     !   zone-pair ZP_zone1_zone2_fw_policy     source-zone    zone1     destination-zone zone2     zone-policy    fw_policy     !   zone-based-policy fw_policy     sequence 1     match       source-data-prefix-list subnet1       !     action inspect     !     !     default-action pass     !   zone-to-nozone-internet deny   lists     data-prefix-list subnet1     ip-prefix 10.0.10.0/24     !     !   url-filtering url_filter     web-category-action block     web-categories    games     block-threshold    moderate-risk     block text     "&lt;![CDATA[&amp;lt;h3&amp;gt;Access" to the requested     page has been denied]]&gt;"     target-vpns    1     !   intrusion-prevention intrusion_policy     security-level connectivity     inspection-mode protection     log-level      err     target-vpns    1     !     failure-mode    open   ! ! ! </pre> |                             |

| CLI Template Configuration | Configuration on the Device  |
|----------------------------|--|
|                            | <pre> ip access-list extended fw_policy-seq-1-acl_   11 permit object-group fw-policy-seq-1-service-og_ object-group subnet1 any ! ip access-list extended utd-nat-acl   10 permit ip any any ! class-map type inspect match-all fw_policy-seq-1-cm_   match access-group name fw_policy-seq-1-acl_ ! policy-map type inspect fw_policy   class fw_policy-seq-1-cm_     inspect ! class class-default   pass ! ! object-group service fw_policy-seq-1-service-og_   ip ! parameter-map type inspect-global   alert on   log dropped-packets   multi-tenancy   vpn zone security ! parameter-map type umbrella global   token A5EA676087BF66A42DC4F722C2AFD10D00256274   dnscrypt   vrf 1   dns-resolver          umbrella   match-local-domain-to-bypass ! ! zone security internet   vpn 0 ! zone security zone1   vpn 1 ! zone security zone2   vpn 2 ! zone-pair security ZP_zone1_internet_fw_policy source zone1 destination internet   service-policy type inspect fw_policy ! zone-pair security ZP_zone1_zone2_fw_policy source zone1 destination zone2   service-policy type inspect fw_policy ! app-hosting appid utd   app-resource package-profile cloud-low   app-vnic gateway0 virtualportgroup 0 guest-interface 0 </pre> |

| CLI Template Configuration | Configuration on the Device   |
|----------------------------|---|
|                            | <pre> guest-ipaddress 192.168.1.2 netmask 255.255.255.252 ! app-vnic gateway1 virtualportgroup 1 guest-interface 1 guest-ipaddress 192.0.2.2 netmask 255.255.255.252 ! start ! utd multi-tenancy utd engine standard multi-tenancy web-filter block page profile block-url_filter text &lt;\![CDATA[&amp;lt;h3&gt;Access to the requested page has been denied&amp;lt;/h3&gt;&amp;lt;p&gt;Please contact your Network Administrator&amp;lt;/p&gt;]]&gt; ! web-filter url profile url_filter categories block games ! block page-profile block-url_filter log level error reputation block-threshold moderate-risk ! ! threat-inspection profile intrusion_policy  threat protection policy connectivity logging level err ! utd global ! policy utd-policy-vrf-1 all-interfaces vrf 1 threat-inspection profile intrusion_policy  web-filter url profile url_filter exit ! </pre> |

### Configuring NTP

Table 14: Configuring NTP

| CLI Template Configuration  | Configuration on the Device  |
|---|--|
| <pre> ntp server 10.29.43.1 source-interface GigabitEthernet1 version 4 exit ! ! </pre> | <pre> ntp server 198.51.241.229 source GigabitEthernet1 version 4 </pre> |

## IPv6 configuration

**Table 15: IPv6 configuration**

| CLI Template Configuration   | Configuration on the Device   |
|--|---|
| <pre>vpn 1   interface GigabitEthernet3     ipv6 address 2671:123A::1/128     shutdown   ! !</pre> | <pre>interface GigabitEthernet3   shutdown   arp timeout 1200   vrf forwarding 1   no ip address   ip redirects   ip mtu 1500   ipv6 address 2671:123A::1/128   ipv6 redirects   mtu 1500   negotiation auto exit vrf definition 1   rd 1:1   address-family ipv4   exit-address-family   !   address-family ipv6   exit-address-family   ! !</pre> |

## Service configuration

In Cisco IOS XE Catalyst SD-WAN Release 17.7.1a and earlier, only the following configurations under **service** can be configured via CLI templates:

```
service pad
service config
service tcp-keepalives-in
service tcp-keepalives-out
service tcp-small-servers
service udp-small-servers
```

## VRF configuration

Configure up to 300 VRFs, with a corresponding subinterface for each VRF. The example configures two VRFs.




---

**Warning** Do not configure VLAN 1. It is reserved for the native VLAN.

---

Table 16: VRF configuration

| CLI Template Configuration  | Configuration on the Device |
|---|-----------------------------|
| <pre> ! vpn 2 router bgp 1000   address-family ipv4-unicast     redistribute omp   address-family ipv6-unicast     redistribute omp   !   neighbor 192.0.2.2     no shutdown     remote-as 2   !   ipv6-neighbor 2001:DB8:2::2     remote-as 2   ! ! interface GigabitEthernet0/0/0.2   ip address 192.0.2.1/24   ipv6 address 2001: DB8:2::1/64   mtu 1496   no shutdown ! ! vpn 3 router bgp 1000   address-family ipv4-unicast     redistribute omp   address-family ipv6-unicast     redistribute omp   !   neighbor 192.0.3.2     no shutdown     remote-as 3   !   ipv6-neighbor 2001: DB8:3::2     remote-as 3   ! ! interface GigabitEthernet0/0/0.3   ip address 192.0.3.1/24   ipv6 address 2001: DB8:3::1/64   mtu 1496   no shutdown ! </pre> |                             |

| CLI Template Configuration | Configuration on the Device   |
|----------------------------|---|
|                            | <pre> vrf definition 2 rd 1:2 address-family ipv4   route-target export 1000:2   route-target import 1000:2   exit-address-family ! address-family ipv6   exit-address-family ! ! router bgp 1000   bgp log-neighbor-changes   distance bgp 20 200 20 ! address-family ipv4 vrf 2   redistribute omp   neighbor 192.0.2.2 remote-as 2   neighbor 192.0.2.2 activate   neighbor 192.0.2.2 send-community both   exit-address-family ! address-family ipv6 vrf 2   redistribute omp   neighbor 2001:DB8:2::2 remote-as 2   neighbor 2001:DB8:2::2 activate   neighbor 2001:DB8:2::2 send-community both   exit-address-family ! interface GigabitEthernet0/0/0.2   encapsulation dot1q 2   vrf forwarding 2   ip address 192.0.2.1 255.255.255.0   ip mtu 1496   ipv6 address 2001:DB8:2::1/64 end  vrf definition 3 rd 1:3 address-family ipv4   route-target export 1000:3   route-target import 1000:3   exit-address-family ! address-family ipv6   exit-address-family ! ! router bgp 1000   bgp log-neighbor-changes   distance bgp 20 200 20 ! address-family ipv4 vrf 3   redistribute omp   neighbor 192.0.3.2 remote-as 3   neighbor 192.0.3.2 activate   neighbor 192.0.3.2 send-community both   exit-address-family ! address-family ipv6 vrf 3   redistribute omp   neighbor 2001:DB8:3::2 remote-as 3 </pre> |

| CLI Template Configuration | Configuration on the Device  |
|----------------------------|--|
|                            | <pre>neighbor 2001: DB8:3::2 activate neighbor 2001: DB8:3::2 send-community both exit-address-family ! interface GigabitEthernet0/0/0.3 encapsulation dot1Q 3 vrf forwarding 3 ip address 192.0.3.1 255.255.255.0 ip mtu 1496 ipv6 address 2001:DB8:3::1/64 end</pre> |

