Control Components Settings on Cisco SD-WAN Manager

Cisco SD-WAN Control Components Settings on Cisco SD-WAN Manager

Table 1: Feature History

Feature Name	Release Information	Description
Cisco SD-WAN Control Components Settings on Cisco SD-WAN Manager	Cisco IOS XE Catalyst SD-WAN Release 17.18.1a Cisco Catalyst SD-WAN Manager Release 20.18.1	This feature simplifies the configuration of settings for Cisco SD-WAN Control Components.

Cisco SD-WAN Control Components Settings on Cisco SD-WAN Manager

Cisco SD-WAN Manager provides a simplified approach to manage the settings for Cisco SD-WAN Control Components. You can configure common settings or device specific settings for the Cisco SD-WAN Control Components.

To configure the common controller component settings navigate to **Configuration** > **Devices** > **Control Components** and then click **Common control components settings**.

Some settings like **Banner**, **Logging** and **SNMP** are disabled by default. You can enable them and then configure the settings.

The Cisco SD-WAN Control Components configurations can be seen in the column **Managed by**:

- templates, or
- settings.

Each unmanaged Cisco SD-WAN Control Components must be first deployed individually before bulk deploying the settings to all the Cisco SD-WAN Control Components.

To deploy individually to each Cisco SD-WAN Control Components, configure the device specific settings. Click **...** and select **Configure**.

Common Control Component Network Settings

NTP

Click **Add Server** and configure the following parameters.

Table 2: NTP

Field	Description
Hostname/IP address	Enter the IP address or FQDN of an NTP server.
VPN ID	Select the VPN that should be used to reach the NTP server, or the VPN in which the NTP server is located. If you have configured multiple NTP servers, they must all be located or be reachable in the same VPN.
Prefer	Enable if multiple NTP servers are at the same stratum level and you want one to be preferred. For servers at different stratum levels, the software chooses the one at the highest stratum level.

AAA

Table 3: AAA

Field	Description
Authentication order	From the drop-list choose the authentication order from **local**,**radius**, and **tacacs**.
Cisco TAC enable	For any Cisco SD-WAN Manager troubleshooting issues, enable **Read** and **Write** access.
Click **Add user** and configure the following parameters.	
Username	Enter a name for the user. It can be 1 to 128 characters long, and it must start with a letter. The name can contain only lowercase letters, the digits 0 through 9, hyphens (-), underscores (_), and periods (.). The name cannot contain any uppercase letters.

Field	Description
Password	Enter a password for the user. Each username must have a password. Users are allowed to change their own passwords. The default password for the admin user is admin. We strongly recommend that you change this password.
User group	Choose the user group from the drop-down menu. You can choose from: • **basic** • **operator** • **netadmin**

Table 4: Advanced

Field	Description
Disable audit logs	Click to disable the audit logs.
Disable netconf logs	Click to disable the netconf logs.
Authentication fallback	Enables authentication fallback.
Admin authentication order	Enables authentication order defined by the administrator.
User accounting	Enables user accounting.
Radius server	
Radius server list	Select the RADIUS server tag from the drop-down menu.
Timeout	Enter the number of seconds a device waits for a reply to a RADIUS request before retransmitting the request. Default: 5 seconds. Range: 1 through 1000
Retransmit	Enter the number of times the device transmits each RADIUS request to the server before giving up. Default: 5 seconds.
Click **Add server** and configure the following parameters.	
Tag	Enter a value for the server tag.

Field	Description
IP address	Enter the IP address of the RADIUS server host.
Authentication port	Enter the UDP destination port to use for authentication requests to the RADIUS server. If the server is not used for authentication, configure the port number to be 0. Default: Port 1812
Accounting port	Enter the UDP port to use to send 802.1X and 802.11i accounting information to the RADIUS server. Range: 0 through 65535. Default: 1813.
Secret key	Enter the key the Cisco IOS XE Catalyst SD-WAN device passes to the RADIUS server for authentication and encryption. You can type the key as a text string from 1 to 31 characters long, and it is immediately encrypted, or you can type an AES 128-bit encrypted key. The key must match the AES encryption key used on the RADIUS server.
VPN ID	Select the VPN ID from the drop-down list.
Priority	Set the priority of a RADIUS server, as a means of choosing or load balancing among multiple RADIUS servers, set a priority value for the server. The priority can be a value from 0 through 7. A server with a lower priority number is given priority over one with a higher number.
TACACS	
Timeout	Enter the number of seconds a device waits for a reply to a TACACS+ request before retransmitting the request. Default: 5 seconds. Range: 1 through 1000
Authentication	Choose the authentication from the drop-down list.
Click **Add server** and configure the following parameters.	
IP address	Enter the IP address of the TACACS server host.
Authentication port	Enter the UDP destination port to use for authentication requests to the TACACS server. If the server is not used for authentication, configure the port number to be 0. Default: Port 49

Field	Description
Accounting port	Enter the UDP port to use to send 802.1X and 802.11i accounting information to the TACACS server. Range: 0 through 65535. Default: 49.
Secret key	Enter the key the Cisco IOS XE Catalyst SD-WAN device passes to the TACACS server for authentication and encryption. You can type the key as a text string from 1 to 31 characters long, and it is immediately encrypted, or you can type an AES 128-bit encrypted key. The key must match the AES encryption key used on the TACACS server.
VPN ID	Select the VPN ID from the drop-down list.
Priority	Set the priority of a TACACS server, as a means of choosing or load balancing among multiple TACACS servers, set a priority value for the server. The priority can be a value from 0 through 7. A server with a lower priority number is given priority over one with a higher number.

DNS

Table 5: DNS

Field	Description
Primary DNS	Enter the IPv4 or IPv6 address of the primary DNS server
Secondary DNS	Enter the IPv4 or IPv6 address of the primary DNS server
Click **Add host mapping** and configure the following parameters.	
Hostname	Enter the DNS name.
List of IP address	Enter a list of IP addresses seperated by comma.

Security

Table 6: Security

Field	Description
Control connection protocol	Choose the protocol to use on control plane connections: • **DTLS** (Datagram Transport Layer Security). This is the default. • **TLS** (Transport Layer Security)
TLS port	If you select TLS, configure the port number to use: Range: 1025 through 65535. Default: 23456

Controller

Table 7: Controller

Field	Description
Graceful Restart for OMP	Enables graceful restart. By default, graceful restart for OMP is enabled.
Graceful Restart Timer (seconds)	Specify how often the OMP information cache is flushed and refreshed. A timer value of 0 disables OMP graceful restart. Range: 0 to 31556952 seconds (365 days) Default: 43200 seconds (12 hours)
Number of Paths Advertised per Prefix	Specify the maximum number of equal-cost routes to advertise per prefix. s advertise routes to Cisco Catalyst SD-WAN Controllers, and the controllers redistributes the learned routes, advertising each route-TLOC tuple. A Cisco IOS XE Catalyst SD-WAN device can have up to eight TLOCs, and by default advertises each route-TLOC tuple to the Cisco Catalyst SD-WAN Controller. If a local site has two Cisco IOS XE Catalyst SD-WAN devices, a Cisco Catalyst SD-WAN Controller could potentially learn eight route-TLOC tuples for the same route. If the configured limit is lower than the number of route-TLOC tuples, the best route or routes are advertised. Range: 1 to 16 Default: 4

Field	Description
Send Backup Paths	Enable to have OMP advertise backup routes to Cisco IOS XE Catalyst SD-WAN devices. By default, OMP advertises only the best route or routes. If you configure to send backup paths, OMP also advertises the first non-best route in addition to the best route or routes.
Shutdown	Ensure that No is chosen to enable to the Cisco SD-WAN overlay network. Click Yes to disable OMP and disable the Cisco SD-WAN overlay network. OMP is enabled by default.
Hub & Spoke Topology	Enable to allow routes through hub and spoke topologies.
Click **Add Compatible TLOC color** and configure the following parameters.	
Primary color	Enter a primary TLOC color.
Secondary color	Enter a secondary TLOC color.
Click **Add incompatible TLOC color** and configure the following parameters.	
Primary color	Enter a primary TLOC color.
Secondary color	Enter a secondary TLOC color.

Table 8: Advanced settings

Field	Description
Discard Rejected Routes	Enable to have OMP discard routes that have been rejected on the basis of policy. By default, rejected routes aren’t discarded.
Enable Filtering Route Updates Based on Affinity	Enable filtering route updates based on affinity.
Enable Filtering Route Updates Based on TLOC-Color	Enable filtering route updates based on TLOC color.

Field	Description
Hold Time (seconds)	Specify how long to wait before closing the OMP connection to a peer. If the peer doesn't receive three consecutive keepalive messages within the hold time, the OMP connection to the peer is closed. Range: 0 to 65535 seconds Default: • Cisco Catalyst SD-WAN Control Components Release 20.16.x: 5400 seconds • From Cisco Catalyst SD-WAN Control Components Release 20.12.1 to Cisco Catalyst SD-WAN Control Components Release 20.15.x: 300 seconds • Before Cisco Catalyst SD-WAN Control Components Release 20.12.1: 60 seconds
Advertisement Interval (seconds)	Specify the time between OMP Update packets. Range: 0 to 65535 seconds Default: 1 second We recommend you to configure 5 seconds on edge devices and 20 seconds on Cisco SD-WAN Controller.
EOR Timer (Seconds)	Specify how long to wait after an OMP session has gone down and then come back up to send an end-of-RIB (EOR) marker. After this marker is sent, any routes that weren't refreshed after the OMP session came back up are considered to be stale and are deleted from the route table. Range: 1 to 3600 seconds (1 hour) Default: 300 seconds (5 minutes)

Banner

Table 9: Banner

Field	Description
Login message	Enter text to display before the login prompt. The string can be up to 2048 characters long. To insert a line break, type **\n**.
MOTD message	On a Cisco IOS XE Catalyst SD-WAN device enter message-of-the-day text to display prior to the login banner. The string can be up to 2048 characters long. To insert a line break, type **\n**.

Logging

Table 10: Logging

Field	Description
Hostname	Enter the DNS name, hostname, or IPv4, IPv6 address of the system on which to store syslog messages.
VPN ID	Enter the identifier of the VPN in which the syslog server is located or through which the syslog server can be reached. VPN ID Range: 0 and 512

SNMP

Table 11: SNMP

Field	Description
Version	Select SNMP version as v2 or v3.
Name for Device	Enter a name for the device.
Contact person	Enter the name of the network management contact person in charge of managing the Cisco IOS XE Catalyst SD-WAN device or a Cisco vEdge device. It can be a maximum of 255 characters.
Location of device	Enter a description of the location of the device. It can be a maximum of 255 characters.
Click **Add view** and configure the following parameters.	
Name	Enter a name for the view. A view specifies the MIB objects that the SNMP manager can access. The view name can be a maximum of 32 characters. You must add a view name for all views before adding a community.

Field	Description
Object Identifiers	Click **Add OID** and configure the following parameters: • **Object Identifiers**: Enter the OID of the object. For example, to view the Internet portion of the SNMP MIB, enter the OID 1.3.6.1. To view the private portion of the MIB, enter the OID 1.3.6.1.4.1.41916. Use the asterisk wildcard (*) in any position of the OID subtree to match any value at that position rather than matching a specific type or name. • **Exclude OID**: On/Off—Click Off to include the OID in the view or click On to exclude the OID from the view. To save the object identifiers, click Save. To remove an OID from the list, click the trash can icon next to the entry.
Click **Add group** and configure the following parameters.	
Name	Enter a name for the trap group. It can be from 1 to 32 characters long.
Security level	Choose the authentication to use for the group. • **no-auth-no-priv**: Authenticate based on a username. When you configure this authentication, you do not need to configure authentication or privacy credentials. • **auth-priv**: Authenticate using the selected authentication algorithm. When you configure this authentication, users in this group must be configured with an authentication and an authentication password and a privacy and privacy password.
View	Choose an SNMP view that the group can access.
Click **Add user** and configure the following parameters.	
Name	Enter a name of the SNMP user. It can be 1 to 32 alphanumeric characters.
Group	Choose the name of an SNMP group.
Authentication password	Enter the authentication password either in cleartext or as an AES-encrypted key.

Field	Description
Privacy password	Enter the privacy password either in cleartext or as an AES-encrypted key.
Click **Add trap group** and configure the following parameters.	
Name	Enter a name for the trap group. It can be from 1 to 32 characters long.
Trap Type Modules	Click the group number, and configure the following parameters: In **Severity Levels**, select one or more severity levels for the trap—**critical**, **major**, or **minor**. In **Module Name**, select the type of traps to include in the trap group: • **all**: All trap types. • **app-route**: Traps generated by application-aware routing. • **bfd**: Traps generated by BFD and BFD sessions. • **control**: Traps generated by DTLS and TLS sessions. • **dhcp**: Traps generated by DHCP. • **hardware**: Traps generated by hardware. • **omp**: Traps generated by OMP. • **routing**: Traps generated by BGP, OSPF, and PIM. • **security**: Trap generated by certificates, Cisco Catalyst SD-WAN Controller and vEdge serial number files, and IPsec. • **system**: Traps generated by system-wide functions. • **vpn**: Traps generated by VPN-specific functions, including interfaces and VRRP. • **bridge**: Traps generated to notify about events on a network bridge. • **wwan**: Traps generated from wireless network devices. • **policy**: Traps generated to notify about specific events or errors for policies that are defined for the device.

Field	Description
Click **Add trap target** and configure the following parameters.	
VPN ID	Enter the number of the VPN to use to reach the trap server. The only supported VPN ID's are 0 and 512.
IP address	Enter the IP address of the SNMP server.
UDP port	Enter the UDP port number for connecting to the SNMP server.*Range:* 1 though 65535
Trap group name	Select the name of a trap group that was configured under Group.
User name	Enter the username. The username can be a string from 1 to 32 characters.

Configure device specific control component network settings

Load running configuration

When you configure the settings for Cisco SD-WAN Control Components for the first time, Cisco SD-WAN Manager automatically loads the device specific settings from the running configuration of the device. The configurations include system parameters, VPN 0 and VPN 512 static routes, and interface configurations. You can also click **Load running config** to overwrite the existing settings.

System

Field	Description
Hostname	Enter a name for the Cisco Catalyst SD-WAN device. It can be up to 32 characters.
Site ID	Enter the identifier of the site in the Cisco Catalyst SD-WAN overlay network domain in which the device resides, such as a branch, campus, or data center. The site ID must be the same for all Cisco Catalyst SD-WAN devices that reside in the same site.*Range:* 1 through 4294967295 ($2^{32} – 1$)
System IP	Enter the system IP address for the Cisco Catalyst SD-WAN device, in decimal four-part dotted notation. The system IP address provides a fixed location of the device in the overlay network and is a component of the device's TLOC address. It is used as the device's loopback address in the transport VPN (VPN 0). You cannot use this same address for another interface in VPN 0.

Field	Description
Description	Enter any additional descriptive information about the device.
Location	Enter a description of the location of the device. It can be up to 128 characters.
Timezone	Select the timezone to use on the device.
Latitude	Enter the latitude of the device, in the format *decimal-degrees*.
Longitude	Enter the longitude of the device, in the format *decimal-degrees*.
Device groups	Enter the names of one or more groups to which the device belongs, separated by commas.
Dual stack IPv6 default	This option is available only if you select Cisco SD-WAN Manager and Cisco SD-WAN Controller. Enable to make dual stack IPv6 as the default.
Validator Address	This option is available only if you select Cisco SD-WAN Validator. Enter the IP address of the Cisco SD-WAN Validator.
Controller group ID	This option is available only if you select Cisco SD-WAN Controller. Enter the Cisco SD-WAN Controller groups to which the router belongs.
Overlay ID	This option is available only if you select Cisco SD-WAN Controller. Enter the identifier of the site in the Cisco Catalyst SD-WAN overlay network in which the device resides.
MRF region list	This option is available only if you select Cisco SD-WAN Controller and if you have enabled Multi-Region Fabric. Enter the MRF regions.

VPN and interface

Table 12: VPN 0

Field	Description
Click **Add interface** and configure the following parameters.	

Field	Description
Interface name	Enter a name for the interface. Spell out the interface names completely (for example, eth1). Configure all the interfaces of the router, even if you are not using them, so that they are configured in the shutdown state and so that all default values for them are configured.
Shutdown	Enable or disable the interface.
IPv4 type	Configure an IPv4 address assign type. • **Dynamic**: Choose Dynamic to set the interface as a Dynamic Host Configuration Protocol (DHCP) client so that the interface receives its IP address from a DHCP server. • **Static**: Choose Static to enter an IP address that doesn't change. • **None**: Choosing this option means that IPv4 address is not configured.
IPv4 CIDR	Enter an IPv4 address.
IPv4 DHCP distance	Enter an administrative distance value for routes learned from a DHCP server. This option is available when you choose **Dynamic**. Default: 1
IPv6 type	Configure an IPv6 address assign type. • **Dynamic**: Choose Dynamic to set the interface as a Dynamic Host Configuration Protocol (DHCP) client so that the interface receives its IP address from a DHCP server. • **Static**: Choose Static to enter an IP address that doesn't change. • **None**: Choosing this option means that IPv6 address is not configured.
IPv6 CIDR	Enter an IPv6 IP address.
IPv6 DHCP distance	Enter an administrative distance value for routes learned from a DHCP server. This option is available when you choose **Dynamic**. Default: 1
IPv6 DHCP rapid con	Enable DHCP rapid commit, to speed up the assignment of IP addresses.

Field	Description
Tunnel	This option is not available for Cisco SD-WAN Validator. Enable this option to create a tunnel interface.
Tunnel color	Choose a color for the TLOC.
Allow Service	Allow the following services on the interface: • **All** • **DHCP** • **NTP** • **DNS** • **ICMP** • **SSHD** • **STUN** • **NETCONF**

Table 13: IPv4 Static route

Field	Description
Click **Add IPv4 static route** and configure the following parameters.	
IPv4 prefix	Enter the IPv4 address or prefix, in decimal four-point-dotted notation, and the prefix length of the IPv4 static route to configure in the VPN.
IPv4 next hop	When you click the next hop, the following fields appear: • **IPv4 Address**: Enter the next-hop IPv4 address. • **Distance**: Enter the administrative distance for the route.

Table 14: IPv6 Static route

Field	Description
Click **Add IPv6 static route** and configure the following parameters.	
IPv6 prefix	Enter the IPv6 address or prefix, in decimal four-point-dotted notation, and the prefix length of the IPv6 static route to configure in the VPN.

Field	Description
IPv6 next hop	When you click the next hop, the following fields appear: • **IPv6 Address**: Enter the next-hop IPv4 address. • **Distance**: Enter the administrative distance for the route.

Table 15: VPN 512

Field	Description
Click **Add interface** and configure the following parameters.	
Interface name	Enter a name for the interface. Spell out the interface names completely (for example, eth1). Configure all the interfaces of the router, even if you are not using them, so that they are configured in the shutdown state and so that all default values for them are configured.
Shutdown	Enable or disable the interface.
IPv4 type	Configure an IPv4 VPN interface. • **Dynamic**: Choose Dynamic to set the interface as a Dynamic Host Configuration Protocol (DHCP) client so that the interface receives its IP address from a DHCP server. • **Static**: Choose Static to enter an IP address that doesn't change. • **None**
IPv4 CIDR	Enter an IPv4 IP address.
IPv4 DHCP distance	Enter an administrative distance value for routes learned from a DHCP server. This option is available when you choose **Dynamic**. Default: 1
IPv6 type	
IPv6 CIDR	Enter an IPv6 IP address.
IPv6 DHCP distance	Enter an administrative distance value for routes learned from a DHCP server. This option is available when you choose **Dynamic**. Default: 1

Field	Description
IPv6 DHCP rapid con	Enable DHCP rapid commit, to speed up the assignment of IP addresses.

Table 16: IPv4 Static route

Field	Description
Click **Add IPv4 static route** and configure the following parameters.	
IPv4 prefix	Enter the IPv4 address or prefix, in decimal four-point-dotted notation, and the prefix length of the IPv4 static route to configure in the VPN.
IPv4 next hop	When you click the next hop, the following fields appear: • **IPv4 Address**: Enter the next-hop IPv4 address. • **Distance**: Enter the administrative distance for the route. • **None**

Table 17: IPv6 Static route

Field	Description
Click **Add IPv6 static route** and configure the following parameters.	
IPv6 prefix	Enter the IPv6 address or prefix, in decimal four-point-dotted notation, and the prefix length of the IPv6 static route to configure in the VPN.
IPv6 next hop	When you click the next hop, the following fields appear: • **IPv6 Address**: Enter the next-hop IPv4 address. • **Distance**: Enter the administrative distance for the route. • **None**