

System Profile

- Information about the System profile, on page 1
- AAA, on page 2
- BFD, on page 6
- Banner, on page 7
- Basic, on page 8
- Fabric Security , on page 12
- Flexible Port Speed, on page 16
- Global, on page 17
- Ignition Power Management, on page 20
- IPv4 Device Access Policy, on page 20
- IPv6 Device Access Policy, on page 21
- Logging, on page 22
- Multi-Region Fabric, on page 26
- NTP, on page 28
- OMP, on page 29
- Performance Monitoring, on page 34
- Remote Access, on page 34
- SNMP, on page 38

Information about the System profile

This section describes the features available in the System profile.

Note Some configurations and protocols are identified as insecure and is a security risk for Cisco devices. Existing deployments continue to function, but new installations require intentional enablement. For more information on remediation, refer to Resilient Infrastructure: Cisco Catalyst SD-WAN and Routing

AAA

The authentication, authorization, and accounting (AAA) feature configures authentication of users logging in to the Cisco Catalyst SD-WAN router, determines what permissions to give them, and performs accounting of their actions.

See Configure AAA Using a Configuration Group.

The following tables describe the options for configuring the AAA feature.

Local

Add users.

Table 1: Local

Field	Description
Enable AAA Authentication	Enable authentication parameters.
Accounting Group	Enable accounting parameters.
Add AAA User	
Name	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. The following usernames are reserved, so you cannot configure them: backup, basic, bin, daemon, games, gnats, irc, list, lp, mail, man, news, nobody, proxy, quagga, root, sshd, sync, sys, uucp, and www-data. Also, names that start with viptela-reserved are reserved.
Password	Enter a password for the user. The password is an MD5 digest string, and it can contain any characters, including tabs, carriage returns, and linefeeds. For more information, see Section 9.4 in RFC 7950, The YANG 1.1 Data Modeling Language. 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 recommended that you change this password.
Confirm Password	Re-enter the password for the user.

Field	Description
Privilege	Select between privilege level 1 or 15. • Level 1: User EXEC mode. Read-only, and access to limited commands, such as the ping command. • Level 15: Privileged EXEC mode. Full access to all commands, such as the reload command, and the ability to make configuration changes. By default, the EXEC commands at privilege level 15 are a superset of those available at privilege level 1.
Add Public Key Chain	
Key String*	Enter the authentication string for a key.
Key Type	Choose **ssh-rsa**.

RADIUS

Add RADIUS servers.

Table 2: RADIUS

Field	Description
Address*	Enter the IP address of the RADIUS server host.
Acct Port	Enter the UDP port to use to send 802.1X and 802.11i accounting information to the RADIUS server. Range: 1 - 65534. Default: 1813
Auth Port	Enter the UDP destination port to use for authentication requests to the RADIUS server. Default: 1812 Range: 1 - 65534
Retransmit	Enter the number of times the device transmits each RADIUS request to the server before giving up. Default: 3 Range: 0 - 100
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
Key*	Enter the key the Cisco IOS XE Catalyst SD-WAN device passes to the RADIUS server for authentication and encryption.

Field	Description
Key Type	Choose Protected Access Credential (PAC) key.

TrustSec

Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.18.1

Field	Description
CTS Authorization List	Specify a name of a list for authentication, authorization, and accounting (AAA) servers. The list name should be within 1-64 characters.
(Optional) **RADIUS Group**	Choose a RADIUS server.

TACACS Server

Add TACACS server.

Table 3: TACACS Server

Field	Description
Address*	Enter the IP address of the TACACS+ server host.
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: 49
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
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.

Accounting

Add accounting rules.

Table 4: Accounting

Field	Description
Rule Id*	Enter the accounting rule ID.

Field	Description
Method*	Specifies the accounting method list. Choose one of the following: • **commands**: Provides accounting information about specific, individual EXEC commands associated with a specific privilege level. • **exec**: Provides accounting records about user EXEC terminal sessions on the network access server, including username, date, and start and stop times. • **network**: Runs accounting for all network-related service requests. • **system**: Performs accounting for all system-level events not associated with users, such as reloads. **Note** When system accounting is used and the accounting server is unreachable at system startup time, the system will not be accessible for approximately two minutes.
Level	Choose the privilege level (1 or 15). Accounting records are generated only for commands entered by users with this privilege level.
Start Stop	Enable this option to if you want the system to send a start accounting notice at the beginning of an event and a stop record notice at the end of the event.
Use Server-group*	Choose a previously configured TACACS group. The parameters that this accounting rule defines are used by the TACACS servers that are associated with this group.

Authorization

Table 5: Authorization

Field	Description
Server Auth Order*	Choose the authentication order. It dictates the order in which authentication methods are tried when verifying user access to a Cisco IOS XE Catalyst SD-WAN device through an SSH session or a console port.
Authorization Console	Enable this option to perform authorization for console access commands.
Authorization Config Commands	Enable this option to perform authorization for configuration commands.
Add Authorization Rule	
Rule Id*	Enter the authorization rule ID.
Method*	Choose **Commands**, which causes commands that a user enters to be authorized.
Level	Choose the privilege level (1 or 15) for commands to be authorized. Authorization is provided for commands entered by users with this privilege level.

Field	Description
If Authenticated	Enable this option to apply the authorization rule parameters only to the authenticated users. If you do not enable this option, the rule is applied to all users.
Use Server-group*	Choose a previously configured TACACS group. The parameters that this authorization rule defines are used by the TACACS servers that are associated with this group.

BFD

Bidirectional Forwarding Detection (BFD) is a protocol that detects link failures as part of the Cisco Catalyst SD-WAN high-availability solution. This feature helps you configure options such as color, DSCP values, poll interval, multiplier for detection, and so on.

See Configure BFD using a configuration group.

The following tables describe the options for configuring the BFD feature.

Basic Configuration

Table 6: Basic Configuration

Field	Description
Poll Interval(In Millisecond)	Specify how often BFD polls all data plane tunnels on a router to collect packet latency, loss, and other statistics used by application-aware routing. Range: 1 through 4,294,967,296 ($2^{32} – 1$) milliseconds Default: 600,000 milliseconds (10 minutes)
Multiplier	Specify the value by which to multiply the poll interval, to set how often application-aware routing acts on the data plane tunnel statistics to figure out the loss and latency and to calculate new tunnels if the loss and latency times do not meet the configured SLAs. Range: 1 through 6 Default: 6
DSCP Values for BFD Packets(decimal)	Specify the Differentiated Services Code Point (DSCP) value of the BFD packets that is used in the DSCP control traffic. Range: 0-63 Default: 48

Color

Table 7: Color

Field	Description
Add Color	
Color*	Choose the color of the transport tunnel for data traffic moving between the devices. The color identifies a specific WAN transport provider. Values: 3g, biz-internet, blue, bronze, custom1, custom2, custom3, default, gold, green, lte, metro-ethernet, mpls, private1 through private6, public-internet, red, silver Default: default
Hello Interval (milliseconds)*	Specify how often BFD sends Hello packets on the transport tunnel. BFD uses these packets to detect the liveness of the tunnel connection and to detect faults on the tunnel. Range: 100 through 300000 milliseconds Default: 1000 milliseconds (1 second)
Multiplier*	Specify how many Hello packet intervals BFD waits before declaring that a tunnel has failed. BFD declares that the tunnel has failed when, during all these intervals, BFD has received no Hello packets on the tunnel. This interval is a multiplier of the Hello packet interval time. Range: 1 through 60 Default: 7
Path MTU Discovery*	Enable or disable path MTU discovery for the transport tunnel. When path MTU discovery is enabled, the path MTU for the tunnel connection is checked periodically, about once per minute, and it is updated dynamically. When path MTU discovery is disabled, the expected tunnel MTU is 1472 bytes, but the effective tunnel MTU is 1468 bytes. Default: Enabled
Default DSCP value for BFD packets*	Specify the Differentiated Services Code Point (DSCP) value of the BFD packets that is used in the DSCP control traffic. Range: 0-63 Default: 48

Banner

The Banner feature helps you to configure the system login banner.

See Configure a login banner using a configuration group.

The following table describes the options for configuring the Banner feature.

Table 8: Banner Basic Settings

Field	Description
Type	Choose a feature from the drop-down list.
Feature Name*	Enter a name for the feature.
Description	Enter a description of the feature. The description can contain any characters and spaces.
Login	Enter the text to display before the login prompt. The string can be up to 2048 characters long. To insert a line break, type \n.
Message of the Day	On a Cisco IOS XE Catalyst SD-WAN device, enter the message-of-the-day text to display before the login banner. The string can be up to 2048 characters long. To insert a line break, type \n.

Basic

The Basic feature helps you configure the basic system-wide functionality of the network devices, such as time zone, GPS location, baud rate of the console connection on the router, and so on.

See Configure Basic System Parameters Using a Configuration Group.

The following tables describe the options for configuring the Basic feature.

Basic Settings

Table 9: Basic Settings

Field	Description
Time Zone	Choose the time zone to use on the device.
Device Groups	Enter the names of one or more groups to which the device belongs, separated by commas.
Location	Enter a description of the location of the device. It can be up to 128 characters.
Description	Enter any additional descriptive information about the device.
Transport Gateway	(Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.13.1) Enable transport gateway functionality for the device. A transport gateway connects routers that may or may not have direct connectivity. One common use case for transport gateways is to provide connectivity between routers in disjoint networks, such as between public and private WANs. Another use case for transport gateway functionality is to use a transport gateway as the hub in a hub-and-spoke topology.

Controller Settings

Table 10: Controller Settings

Field	Description
Console Baud Rate(bps)	Choose the baud rate of the console connection on the router. Values: 1200, 2400, 4800, 9600, 19200, 38400, 57600, 115200 baud or bits per second (bps). Default: 9600
Overlay ID	Specifies the overlay ID of a device in the Cisco Catalyst SD-WAN overlay network. Range: 0 - 4294967295 ($2^{32} – 1$) Default: 1
Controller Group	List the Cisco Catalyst SD-WAN Controller groups to which the router belongs.
Max OMP Sessions	Set the maximum number of OMP sessions that a router can establish to a Cisco SD-WAN Controller. Range: 1 through 100
Affinity Group Number	(Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.13.1) Enter an affinity group number. Range: 1 through 63
Affinity Group Number for VRFs and **Range of VRFs**	(Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, Cisco Catalyst SD-WAN Manager Release 20.13.1) Enter an affinity group number for a specific range of VRFs. You can click + to configure an affinity group number for additional VRF ranges. Range for affinity group: 1 through 63 Range for VRFs: Range: 1 to 65525, excluding 512. For details see the VRF range behavior change described here.
Affinity Group Preference Auto	(Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, Cisco Catalyst SD-WAN Manager Release 20.13.1) Configure automatic affinity preference order. When you use this, a device prefers routes with a lower affinity group number. In this case affinity group numbers are not treated as arbitrary tags, but instead signify route priority, where a lower affinity group number means higher priority.

Field	Description
Affinity Group Preference	(Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.13.1a, Cisco Catalyst SD-WAN Manager Release 20.13.1) Enter a comma-separated list of affinity group numbers. In a Multi-Region Fabric scenario, this determines the order of preference for connecting to a gateway. Affinity group preference also used for path filtering when using the **filter route outbound affinity-group preference** command on a Cisco SD-WAN Controller. Range for affinity groups: 1 through 63

GPS

Table 11: GPS

Field	Description
GPS Latitude	Enter the latitude of the device, in the format decimal-degrees.
GPS Longitude	Enter the longitude of the device, in the format decimal-degrees.

Track Settings

Table 12: Track Settings

Field	Description
Track Transport	Enable this option to regularly check whether the DTLS connection between the device and a Cisco SD-WAN Validator is up. Default: Enabled
Track Default Gateway	Enable or disable tracking of default gateway. Gateway tracking determines, for static routes, whether the next hop is reachable before adding that route to the route table of the device. Default: Enabled
Track Interface Tag	Set the tag string to include in routes associated with a network that is connected to a non-operational interface. Range: 1 through 4294967295
Tracker DIA Stabilize Status	Enable this option to stabilize interface flaps by using the multiplier to update HTTP or ICMP tracker status from DOWN to UP.

Advanced

Table 13: Advanced

Field	Description
Port Hopping	Enable or disable port hopping. When a Cisco Catalyst SD-WAN device is behind a NAT, port hopping rotates through a pool of preselected OMP port numbers (called base ports) to establish DTLS connections with other Cisco Catalyst SD-WAN devices when a connection attempt is unsuccessful. The default base ports are 12346, 12366, 12386, 12406, and 12426. To modify the base ports, set a port offset value. Default: Enabled
Port Offset	Enter a number by which to offset the base port number. Configure this option when multiple Cisco Catalyst SD-WAN devices are behind a single NAT device, to ensure that each device uses a unique base port for DTLS connections. Values: 0 through 19
On Demand Tunnel	Enable dynamic on-demand tunnels between any two Cisco Catalyst SD-WAN spoke devices.
On Demand Tunnel Idle Timeout (In Minute)	Enter the on-demand tunnel idle timeout time. After the configured time, the tunnel between the spoke devices is removed. Range: 1 to 65535 minutes Default: 10 minutes
Control Session PPS	Enter a maximum rate of DTLS control session traffic to police the flow of control traffic. Range: 1 through 65535 pps Default: 300 pps
Multi Tenant	Enable this option to specify the device as multitenant.
Admin Tech On Failure	Enable this option to collect admin-tech information when the device reboots. Default: Enabled

Per packet load balancing

Table 14: Per packet load balancing fields

Field	Description
Local colors	Specify the WAN links (such as MPLS, Internet, and LTE) used to distribute traffic within the network.

Field	Description
Flow splitting	Specify how to divide traffic among the available tunnels. Packets: Sends a set number of packets (default: 1024) through one tunnel before switching to the next flowlet. This cycle repeats continuously to balance the network load. Packet gap: Switches tunnels based on the time interval between packets. If the time gap between bursts exceeds the maximum latency difference among tunnels, a new flowlet is sent on a different tunnel. This helps distribute traffic more effectively during natural pauses in data transmission.
Candidate tunnel group	Dynamically defines the group of tunnels used in a PPL network. All tunnels: All available tunnels become part of PPL network. Latency offset: Includes only those tunnels whose latency is within a configurable threshold of the lowest-latency tunnel. Adaptive cluster: Groups tunnels dynamically into clusters based on real-time loss and latency measurements. Tunnels with similar loss (primary factor) and latency (secondary factor) are grouped together for packet distribution.
Reorder	Enables packet reordering at the receiving end to reduce out-of-order delivery. If you disable this option, ensure that your application can independently handle packet reordering.

Fabric Security

Note Before the Cisco Catalyst SD-WAN Manager Release 20.12.1, Fabric Security was called Cisco Security.

Use this feature to configure security parameters for the data plane in the Cisco Catalyst SD-WAN overlay network.

The following tables describe the options for configuring the Fabric Security feature.

Basic Configuration

Field	Description
Rekey Time (seconds)	Specify how often a device changes the AES key. Before Cisco IOS XE Catalyst SD-WAN devices and Cisco vEdge devices can exchange data traffic, they set up a secure authenticated communications channel between them. The routers use IPSec tunnels between them as the channel, and the AES-256 cipher to perform encryption. Each router generates a new AES key for its data path periodically. Range: 10 through 63113904 seconds (730 days) Default: 86400 seconds (24 hours)
Extended AR Window	Enabling an extended AR window causes a router to add a time stamp to each packet using the IPsec tunnel. This prevents valid packets from being dropped if they arrive out of sequence. This option is turned off by default. Click **On** to enable it. Enabling the feature displays the **Extended Anti-Replay Window** field. Range: 10 ms to 2048 ms Default: 256 ms
Replay Window	Specify the size of the sliding replay window. Values: 64, 128, 256, 512, 1024, 2048, 4096, 8192 packets. Default: 512 packets
IPsec pairwise-keying	This option is turned off by default. Click **On** to enable it.
IKEV2	Select **IKEv2** to use IKEv2 to manage encryption keys for IPsec data-plane tunnels.
Post quantum encryption	Select the post-quantum encryption option to use: • **None**: Select **None** to use IKEv2 without enabling PQC or PPK. • **PQC**: Select **PQC** to use an ML-KEM algorithm during IKEv2 key negotiation. • **PPK**: Select **PPK** to use post-quantum preshared keys retrieved from an external SKIP or quantum-key-distribution key server.
Fallback to non pqc	Enable this field to allow the devices to use a classical algorithm if they cannot negotiate PQC. Disable it to require PQC.
Algorithm	Select the ML-KEM algorithm to use: **ML-KEM-512**, **ML-KEM-768**, or **ML-KEM-1024**.
Service VPN	Enter the service VPN identifier that provides connectivity to the external key server.
IP Address	Enter the IPv4 address of the external SKIP or quantum-key-distribution key server.

Field	Description
TCP Port	Enter the TCP port used to establish the secure SKIP connection to the external key server.
TLS PSK ID	Enter the identifier used for TLS preshared-key authentication between the device and the SKIP server.
TLS PSK Key	Enter the preshared key used to authenticate the device and encrypt the secure connection for retrieving and managing PPKs.

Authentication Type

Field	Description
Integrity Type	Choose one of the following integrity types: • **esp**: Enables Encapsulating Security Payload (ESP) encryption and integrity checking on the ESP header. • **ip-udp-esp**: Enables ESP encryption. In addition to the integrity checks on the ESP header and payload, the checks include the outer IP and UDP headers. • **ip-udp-esp-no-id**: Ignores the ID field in the IP header so that Cisco Catalyst SD-WAN can work with the non-Cisco devices. • **none**: Turns integrity checking off on IPSec packets. We don't recommend using this option.

Key Chain

Field	Description
Add Key Chain	
Key ID*	Select a key chain ID.
Key Chain Name*	Select a key chain name.

Key ID

Field	Description
Add Key ID	
ID*	Select a key chain ID.
Name*	Select a key chain name.

Field	Description
Include TCP Options	This field indicates whether a TCP option other than TCP Authentication Option (TCP-AO) is used to calculate Message Authentication Codes (MACs). A MAC is computed for a TCP segment using a configured MAC algorithm, relevant traffic keys, and the TCP segment data prefixed with a pseudoheader. When options are included, the content of all options is included in the MAC with TCP-AO's **MAC** field is filled with zeroes. When the options aren't included, all options other than TCP-AO are excluded from all MAC calculations.
Key String	Specify the master key for deriving the traffic keys. The master keys must be identical on both the peers. If the master keys do not match, authentication fails and segments may be rejected by the receiver. Range: 0 through 80 characters.
Receiver ID*	Specify the receive identifier for the key. Range: 0 through 255.
Send ID*	Specify the send identifier for the key. Range: 0 through 255.
TCP	Specify the algorithm to compute MACs for TCP segments. You can choose one of the following: • **aes-128-cmac** • **hmac-sha-1** • **hmac-sha-256**
Accept AO Mismatch	This field indicates whether the receiver must accept the segments for which the MAC in the incoming TCP-AO does not match the MAC that is generated on the receiver.
Accept Lifetime	The following fields appear when you click this field: • **Accept Local**: This option is disabled by default. Click **On** to enable it. • **Accept Start Epoch**: Specify the time in seconds that is entered in Cisco SD-WAN Manager for which the key to be accepted for TCP-AO authentication is valid. Specify the start time in the local time zone. By default, the start time corresponds to UTC time. • **End Time Format**: You can specify the end time in three ways—infinite (no expiry), duration (1 through 2147483646 sec), or exact (either UTC or local).

Field	Description
Send Lifetime	The following fields appear when you click this field: • **Send Local**: This option is disabled by default. Click **On** to enable it. • **Send Start Epoch**: Specify the time in seconds that is entered in Cisco SD-WAN Manager for which the key to be used in TCP-AO authentication is valid. Specify the start time in the local time zone. By default, the start time corresponds to UTC time. • **End Time Format**: You can specify the end time in three ways—infinite (no expiry), duration (1 through 2147483646 sec), or exact time (either UTC or local).

Flexible Port Speed

The Flexible Port Speed feature is applicable only to the Cisco Catalyst 8500-12X4QC router. Use this feature to configure interfaces to work as 100GE, 40GE, 10GE, or 1GE based on your requirement. Any changes made to the port type take effect only after applying the configuration group to devices.

Updating the port configuration using the Flexible Port Speed feature may enable some ports and disable others. For instance, by default , C8500-12X4QC operates Bay 1 in 10GE mode and Bay 2 in 40GE mode. The Bay 1 mode can be 10GE, 40GE, or 100GE. Setting Bay 1 to 100GE disables all ports of Bay 0. For more information, see Bay Configuration of the Cisco Catalyst 8500-12X4QC device.

Note In Cisco Catalyst SD-WAN Manager Release 20.13.1, you cannot update the Cisco Catalyst 8500-12X4QC port configuration to 2 ports of 100GE by using the Flexible Port Speed feature.

For more information about the Cisco Catalyst 8500-12X4QC platform's port options in each of its bays, see the C8500-12X4QC product overview in the *Cisco Catalyst 8500 Series Edge Platforms Data Sheet*.

Some parameters have a scope drop-down list that enables you to choose **Global**, **Device Specific**, or **Default** for the parameter value. Choose one of the following options, as described in the table below:

Parameter Scope	Scope Description
Global (Indicated by a globe icon)	Enter a value for the parameter and apply that value to all devices. Examples of parameters that you might apply globally to a group of devices are DNS server, syslog server, and interface MTUs.
Device Specific (Indicated by a host icon)	Use a device-specific value for the parameter. Choose **Device Specific** to provide a value for the key in the field. The key is a unique string that helps identify the parameter. To change the default key, enter a new string in the field. Examples of device-specific parameters are system IP address, host name, GPS location, and site ID.

Parameter Scope	Scope Description
Default (indicated by a check mark)	The default value appears for parameters that have a default setting.

Basic Settings

Parameter Name	Description
Port Type	Choose from one of the following port combinations: • **12 ports of 1/10GE + 3 ports of 40GE** • **8 ports of 1/10GE + 4 ports of 40GE** • **2 ports of 100GE** • **12 ports of 1/10GE + 1 port of 100GE** • **8 ports of 1/10GE + 1 port of 40GE + 1 port of 100GE** • **3 ports of 40GE + 1 port of 100GE** Default is 12 ports of 1/10GE + 3 ports of 40GE.

Global

The Global feature helps you enable or disable various services on the devices such as HTTP, HTTPS, Telnet, IP domain lookup, and several other device settings.

The following tables describe the options for configuring the Global feature.

Services

Table 15: Services

Field	Description
HTTP Server	Enable or disable HTTP server.
HTTPS Server	Enable or disable secure HTTPS server.
FTP Passive	Enable or disable passive FTP.
Domain Lookup	Enable or disable Domain Name System (DNS) lookup.
ARP Proxy	Enable or disable proxy ARP.
RSH/RCP	Enable or disable remote shell (RSH) and remote copy (rcp) on the device.

Field	Description
Line Virtual Teletype (Configure Outbound Telnet)	Enable or disable outbound telnet.
Cisco Discovery Protocol (CDP)	Enable or disable Cisco Discovery Protocol (CDP).
Link Layer Discovery Protocol (LLDP)	Enable or disable Link Layer Discovery Protocol (LLDP).
Specify interface for source address	Enter the address of the source interface in all HTTPS client connections.

NAT 64

Table 16: NAT 64

Field	Description
UDP Timeout	Specify the NAT64 translation timeout for UDP. Range: 1 to 536870 (seconds) Default: 300 seconds (5 minutes)
TCP Timeout	Specify the NAT64 translation timeout for TCP. Range: 1 to 536870 (seconds) Default: 3600 seconds (1 hour)

BGP

Table 17: BGP

Field	Description
BGP Community New Format	Specify the new format for BGP community. Starting from Cisco IOS XE Catalyst SD-WAN Release 26.2.1, this field is enabled by default.

Authentication

Table 18: Authentication

Field	Description
HTTP Authentication	Choose the HTTP authentication mode. Accepted values: Local, AAA Default: Local

SSH Version

Table 19: SSH Version

Field	Description
SSH Version	Choose the SSH version. Default: Disabled

Other Settings

Table 20: Other Settings

Field	Description
TCP Keepalives (In)	Enable or disable generation of keepalive timers when incoming network connections are idle.
TCP Keepalives (Out)	Enable or disable generation of keepalive timers when outgoing network connections are idle.
TCP Small Servers	Enable or disable small TCP servers (for example, ECHO).
UDP Small Servers	Enable or disable small UDP servers (for example, ECHO).
Console Logging	Enable or disable console logging. By default, the router sends all log messages to its console port.
IP Source Routing	Enable or disable IP source routing. IP source routing is a feature that enables the originator of a packet to specify the path for the packet to use to get to the destination.
VTY Line Logging	Enable or disable the device to display log messages to a vty session in real time.
SNMP IFINDEX Persist	Enable or disable SNMP IFINDEX persistence, which provides an interface index (ifIndex) value that is retained and used when the device reboots.
Ignore BOOTP	Enable or disable BOOTP server. When enabled, the device listens for the BOOTP packet that comes in sourced from 0.0.0.0. When disabled, the device ignores these packets.
(optional) **Interface statistics per minute**	Minimum supported release: Cisco IOS XE Catalyst SD-WAN Release 26.1.1 Choose the time interval for interface statistics data collection: • **1 minute** • **5 minutes** (default)

Ignition Power Management

Using Cisco SD-WAN Manager, you can configure Ignition Power Management on Cisco IR1800 devices.

The following table describes the options for configuring the Ignition Power Management feature.

Table 21: Ignition Power Management

Field	Description
Name	Name for the ignition power management configuration.
Description	Description for the ignition power management configuration.
Enable	Enable or disable ignition power management.
Ignition Sense Enable	When ignition sense is enabled, it monitors the power supply voltage to detect whether ignition is on or off based on the configured thresholds. When ignition sense is disabled (on IR1835), it uses the ignition signal pin to detect whether ignition is on or off. **Note** Disabling ignition sense is supported only on IR 1835 routers.
Battery Type	Type of battery used.
Shutdown Timer	Timer (seconds) to delay shutdown after ignition is turned off.
Under voltage Threshold	Minimum voltage (in millivolts) for the device to operate before triggering an undervoltage event.
Sense voltage Threshold	Voltage threshold (in millivolts) for the device to sense ignition status. **Note** If the newly configured value is higher than the current input voltage, the router will shut down.

IPv4 Device Access Policy

Use the IPv4 device access policy to create a device configuration to handle both SSH and SNMP traffic directed towards the control plane.

Device access policies define the rules that traffic must meet to pass through an interface. When you define rules for incoming traffic, they are applied to the traffic before any other policies are applied. You can use access policies in routed and transparent firewall mode to control IP traffic.

The following tables describe the options for configuring the IPv4 device access policy.

Table 22: Basic Settings

Field	Description
Type	Choose a feature from the drop-down list.
Feature Name*	Enter a name for the feature. The name can be up to 128 characters and can contain only alphanumeric characters.
Description	Enter a description of the feature. The description can be up to 2048 characters and can contain only alphanumeric characters.

Table 23: ACL Sequence

Field	Description
ACL Sequence Name	Enter a name for the ACL Sequence.
Action Type	Choose one of the following actions for the ACL policy: • **Accept** • **Drop**
Default Action	The **Default Action** in the left pane is to drop the packets. Change the default action by clicking the ellipsis (**...**) icon.
Condition	• **Device Access Protocol (required)**: Choose a carrier from the drop-down list. For example, SNMP, SSH. • **Source Data Prefix**: Select an existing source data prefix or provide a source IP address. For example, 10.0.0.0/12. • **Source Port**: Enter the list of source ports when you have chosen SSH as the device access protocol. The range is 0 through 65535. • **Destination Data Prefix**: Select an existing destination data prefix or provide a destination IP address when you have chosen SSH as the device access protocol. For example, 10.0.0.0/12.

IPv6 Device Access Policy

Use the IPv6 device access policy to create a device configuration to handle both SSH and SNMP traffic directed towards the control plane.

Device access policies define the rules that traffic must meet to pass through an interface. When you define rules for incoming traffic, they are applied to the traffic before any other policies are applied. You can use access policies in routed and transparent firewall mode to control IP traffic.

The following tables describe the options for configuring the IPv6 device access policy.

Table 24: IPv6 Device Access Policy

Field	Description
Add ACL Sequence	
ACL Sequence Name	Enter a name for the ACL Sequence.
Action Type	Choose one of the following actions for the ACL policy: • **Accept** • **Drop**
Default Action	The **Default Action** in the left pane is to drop the packets. Change the default action by clicking the ellipsis (**...**) icon.
Condition	• **Device Access Protocol (required)**: Choose a carrier from the drop-down list. For example, SNMP, SSH. • **Source Data Prefix**: Select an existing source data prefix or provide a source IP address. For example, 10.0.0.0/12. • **Source Port**: Enter the list of source ports when you have chosen SSH as the device access protocol. The range is 0 through 65535. • **Destination Data Prefix**: Select an existing destination data prefix or provide a destination IP address when you have chosen SSH as the device access protocol. For example, 10.0.0.0/12.

Logging

The Logging feature helps you configure logging to either the local hard drive or a remote host.

The following tables describe the options for configuring the Logging feature.

Table 25: Disk

Field	Description
Enable Disc	Enable this option to allow syslog messages to be saved in a file on the local hard disk, or disable this option to disallow it. By default, logging to a local disk file is enabled on all Cisco IOS XE Catalyst SD-WAN devices.

Field	Description
Max File Size(In Megabytes)	Enter the maximum size of syslog files. The syslog files are rotated on an hourly basis based on the file size. When the file size exceeds the configured value, the file is rotated and the syslog process is notified. Range: 1 to 20 MB Default: 10 MB
Rotations	Enter the number of syslog files to create before discarding the oldest files. Range: 1 to 10 Default: 10

Table 26: TLS Profile

Field	Description
Add TLS Profile	
TLS Profile Name*	Enter the name of the TLS profile.
TLS Version	Choose a TLS version: • **TLSv1.1** • **TLSv1.2**
Authentication Type*	Choose **Server**.

Field	Description
Cipher Suite List	Choose groups of cipher suites (encryption algorithm) based on the TLS version. Cipher suites: • **aes-128-cbc-sha**: Encryption type tls_rsa_with_aes_cbc_128_sha • **aes-256-cbc-sha**: Encryption type tls_rsa_with_aes_cbc_256_sha • **dhe-aes-cbc-sha2**: Encryption type tls_dhe_rsa_with_aes_cbc_sha2 (TLS1.2 and above) • **dhe-aes-gcm-sha2**: Encryption type tls_dhe_rsa_with_aes_gcm_sha2 (TLS1.2 and above) • **ecdhe-ecdsa-aes-gcm-sha2**: Encryption type tls_ecdhe_ecdsa_aes_gcm_sha2 (TLS1.2 and above) SuiteB • **ecdhe-rsa-aes-cbc-sha2**: Encryption type tls_ecdhe_rsa_aes_cbc_sha2 (TLS1.2 and above) • **ecdhe-rsa-aes-gcm-sha2**: Encryption type tls_ecdhe_rsa_aes_gcm_sha2 (TLS1.2 and above) • **rsa-aes-cbc-sha2**: Encryption type tls_rsa_with_aes_cbc_sha2 (TLS1.2 and above) • **rsa-aes-gcm-sha2**: Encryption type tls_rsa_with_aes_gcm_sha2 (TLS1.2 and above)

Note Some configurations and protocols are identified as insecure and is a security risk for Cisco devices. Existing deployments continue to function, but new installations require intentional enablement. For more information on remediation, refer to Resilient Infrastructure: Cisco Catalyst SD-WAN and Routing

Table 27: Server

Field	Description
Add Server	
Hostname/IPv4 Address*	Enter the DNS name, hostname, or IP address of the system on which to store syslog messages. To add another syslog server, click the plus sign (+). To delete a syslog server, click the trash icon to the right of the entry.
VPN*	Enter the identifier of the VPN in which the syslog server is located or through which the syslog server can be reached. Range: 1 to 65525, excluding 512. For details see the VRF range behavior change described here.

Field	Description
Source Interface	Enter the specific interface to use for outgoing system log messages. The interface must be located in the same VPN as the syslog server. Otherwise, the configuration is ignored. If you configure multiple syslog servers, the source interface must be the same for all of them.
Priority	Select the severity of the syslog message to save. The severity indicates the seriousness of the event that generated the message. Priority can be one of these: • **informational**: Routine condition (the default) (corresponds to syslog severity 6) • **debugging**: Prints additional logs to help debugging the issue. • **notice**: A normal, but significant condition (corresponds to syslog severity 5) • **warn**: A minor error condition (corresponds to syslog severity 4) • **error**: An error condition that does not fully impair system usability (corresponds to syslog severity 3) • **critical**: A serious condition (corresponds to syslog severity 2) • **alert**: Action must be taken immediately (corresponds to syslog severity 1) • **emergency**: System is unusable (corresponds to syslog severity 0)
TLS Enable*	Enable this option to allow syslog over TLS. When you enable this option, these fields appear: **TLS Properties Custom Profile**: Enable this option to choose a TLS profile. When you enable this option, the following field appears: **TLS Properties Profile**: Choose a TLS profile that you have created for server or mutual authentication in the IPv4 server configuration.
Add IPv6 Server	
Hostname/IPv6 Address*	Enter the DNS name, hostname, or IP address of the system on which to store syslog messages. To add another syslog server, click the plus sign (+). To delete a syslog server, click the trash icon to the right of the entry.
VPN*	Enter the identifier of the VPN in which the syslog server is located or through which the syslog server can be reached. Range: 1 to 65525, excluding 512. For details see the VRF range behavior change described here.
Source Interface	Enter the specific interface to use for outgoing system log messages. The interface must be located in the same VPN as the syslog server. Otherwise, the configuration is ignored. If you configure multiple syslog servers, the source interface must be the same for all of them.

Field	Description
Priority	Select the severity of the syslog message to save. The severity indicates the seriousness of the event that generated the message. Priority can be one of these: • **informational**: Routine condition (the default) (corresponds to syslog severity 6) • **debugging**: Prints additional logs to help debugging the issue. • **notice**: A normal, but significant condition (corresponds to syslog severity 5) • **warn**: A minor error condition (corresponds to syslog severity 4) • **error**: An error condition that does not fully impair system usability (corresponds to syslog severity 3) • **critical**: A serious condition (corresponds to syslog severity 2) • **alert**: Action must be taken immediately (corresponds to syslog severity 1) • **emergency**: System is unusable (corresponds to syslog severity 0)
TLS Enable*	Enable this option to allow syslog over TLS.
TLS Properties Custom Profile*	Enable this option to choose a TLS profile.
TLS Properties Profile	Choose a TLS profile that you have created for server or mutual authentication in the IPv6 server configuration.

Multi-Region Fabric

Multi-Region Fabric provides the ability to divide the architecture of the Cisco Catalyst SD-WAN overlay network into the following:

- A core overlay network: This network, called region 0, consists of border routers that connect to regional overlays (called access regions) and connect to each other. Each border router serves a single access region. Configure each border router with the "border-router" role and with the number of the access region that the border router serves.
- One or more regional overlay networks, called access regions: Each access region consists of edge routers that connect to other edge routers within the same region, and can connect to core region border routers that are assigned to the region. Configure each edge router with the "edge-router" role and an access region number.

See Configure Multi-Region Fabric Using Configuration Groups.

Basic Settings

Table 28: Basic Settings

Parameter Name	Description
Role	• Border routers: Use **border-router**. • Edge routers: Use **edge-router**.
Secondary Region ID	Secondary regions provide another layer to the Multi-Region Fabric architecture. A secondary region contains only edge routers and enables direct tunnel connections between edge routers in different primary regions. When you add an edge router to a secondary region, the router effectively operates in two regions simultaneously, and has different paths available through its primary and secondary regions. Range: 1 to 63

Advanced

Parameter Name	Description
Management Region	Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.13.1 Enable a management region in a Multi-Region Fabric scenario.
Management VPN	Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.13.1 Enter a VPN in which devices can connect to a management gateway. Range: 1 through 65531
Enable as Management Gateway	Enable management gateway functionality for the device. A management gateway is a device that other devices in the overlay (including edge devices and border routers, and devices enabled as transport gateways) connect to. All these devices establish direct tunnels with the management gateway.
Enable Migration Mode to Multi-Region Fabric	Use this parameter when migrating devices from a non-Multi-Region Fabric architecture to Multi-Region Fabric. To prepare for migration, do the following: • Use the **enabled** option for devices that will function as edge routers after migration. • Use the **enabled-from-bgp-core** option for Cisco Catalyst SD-WAN gateway routers that will function as border routers after migration.

NTP

Network Time Protocol (NTP) is a protocol that allows a distributed network of servers and clients to synchronize the timekeeping across the network. The NTP feature helps you configure NTP settings on the Cisco Catalyst SD-WAN network.

See Configure NTP Servers Using a Configuration Group

These tables describe the options for configuring the NTP feature.

Server

Table 29: Server

Field	Description
Add Server	
Hostname/IP address*	Enter the IP address of an NTP server, or a DNS server that knows how to reach the NTP server.
VPN to reach NTP Server*	Enter the number of 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. Range: 1 to 65525, excluding 512. For details see the VRF range behavior change described here.
Set authentication key for the server	Specify the MD5 key associated with the NTP server, to enable MD5 authentication. For the key to work, you must mark it as trusted in the **Trusted Key** field under **Authentication**.
Set NTP version*	Enter the version number of the NTP protocol software. Range: 1 to 4 Default: 4
Set interface to use to reach NTP server	Enter the name of a specific interface to use for outgoing NTP packets. The interface must be located in the same VPN as the NTP server. If it is not, the configuration is ignored.
Prefer this NTP server*	Enable this option if multiple NTP servers are at the same stratum level and you want one to be preferred. For servers at different stratum levels, Cisco Catalyst SD-WAN chooses the one at the highest stratum level.

Authentication

Table 30: Authentication

Field	Description
Add Authentication Keys	
Key Id*	Enter an MD5 authentication key ID. Range: 1 to 65535
MD5 Value*	Enter an MD5 authentication key. Enter either a cleartext key or an AES-encrypted key.
Trusted Key	Enter the MD5 authentication key to designate the key as trustworthy. To associate this key with a server, enter the same value that you entered for the **Set authentication key for the server** field under **Server**.

Advanced

Table 31: Advanced

Field	Description
Authoritative NTP Server	Choose **Global** from the drop-down list, and enable this option if you want to configure one or more supported routers as a primary NTP router.
Stratum	Enter the stratum value for the primary NTP router. The stratum value defines the hierarchical distance of the router from its reference clock. Valid values: Integers 1 to 15. If you do not enter a value, the system uses the router internal clock default stratum value, which is 8.
Source Interface	Enter the name of the exit interface for NTP communication. If configured, the system sends NTP traffic to this interface. For example, enter **`GigabitEthernet1`** or **`Loopback0`**.

OMP

This feature helps you configure the Overlay Management Protocol (OMP) parameters.

See Configure OMP Using a Configuration Group

The following tables describe the options for configuring the OMP feature.

Basic Configuration

Table 32: Basic Configuration

Field	Description
Graceful Restart Enable	Enable graceful restart. By default, the graceful restart for OMP is enabled.
Paths Advertised Per Prefix	Specify the maximum number of equal-cost routes to advertise per prefix. A Cisco IOS XE Catalyst SD-WAN device advertises routes to Cisco Catalyst SD-WAN Controllers, and the controllers redistribute the learned routes, advertising each route-TLOC tuple. A Cisco IOS XE Catalyst SD-WAN device can have up to four 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 through 16 Default: 4
BGP AS Path Auto-Translation	Enables automatic translation of the BGP as path length into the OMP preference value for BGP-learned routes. When this option is enabled, routes with shorter BGP aspaths are assigned a higher OMP preference. Specifically, the OMP preference for a BGP-learned route starts at 255 and is decremented by 1 for each AS in the BGP aspath. As a result, routes with fewer AS hops receive a higher preference within OMP route selection.
ECMP Limit	Specify the maximum number of OMP paths received from the Cisco Catalyst SD-WAN Controller that can be installed in the local route table of the Cisco IOS XE Catalyst SD-WAN device. By default, a Cisco IOS XE Catalyst SD-WAN device installs a maximum of four unique OMP paths into its route table. Range: 1 through 16 Default: 4
Advertisement Interval (In Second)	Specify the time between OMP update packets. Range: 0 through 65535 seconds Default: 1 second We recommend you to configure 5 seconds on edge devices and 20 seconds on vSmart.

Field	Description
Hold Time(In Second)	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 through 65535 seconds Defaults, by Cisco Catalyst SD-WAN Control Components release: • 20.18.x and later: 300 seconds • 20.16.x: 5400 seconds • 20.12.1 to 20.15.x: 300 seconds • Before 20.12.1: 60 seconds Defaults, by Cisco IOS XE Catalyst SD-WAN release: • 17.18.1 and later: 300 seconds • 17.16.x: 5400 seconds
EOR Timer(In Second)	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 through 3600 seconds (1 hour) Default: 300 seconds (5 minutes)
Overlay AS	Specify a BGP AS number that OMP advertises to the BGP neighbors of the router.
Shutdown	Enable this option to disable OMP and disable the Cisco Catalyst SD-WAN overlay network. OMP is enabled by default.
OMP Admin Distance Ipv4	To advertise a route over OMP, configure the OMP administrative distance for the IPv4 address lower than the leaked route administrative distance. Range: 1 through 255
OMP Admin Distance Ipv6	To advertise a route over OMP, configure the OMP administrative distance for the IPv6 address lower than the leaked route administrative distance. Range: 1 through 255

Timers

Table 33: Timers

Field	Description
Graceful Restart(In Second)	Specify how often the OMP information cache is flushed and refreshed. A timer value of 0 disables OMP graceful restart. Range: 0 through 604800 seconds (168 hours, or 7 days) Default: 43200 seconds (12 hours)

Advertise

Table 34: Advertise

Field	Description
Advertise Ipv4 BGP	Enable this option to advertise BGP routes to OMP. By default, BGP routes are not advertised to OMP.
Advertise Ipv4 OSPF	Enable this option to advertise external OSPF routes to OMP. By default, external OSPF routes are not advertised to OMP.
Advertise Ipv4 OSPF v3	Enable this option to advertise external OSPFv3 routes to OMP. By default, external OSPFv3 routes are not advertised to OMP.
Advertise Ipv4 Connected	Enable this option to advertise connected routes to OMP. By default, connected routes are not advertised to OMP.
Advertise Ipv4 Static	Enable this option to advertise static routes to OMP. By default static routes are not advertised to OMP.
Advertise Ipv4 LISP	Enable this option to advertise LISP routes to OMP. By default, LISP routes are not advertised to OMP.
Advertise Ipv4 ISIS	Enable this option to advertise IS-IS routes to OMP. By default, IS-IS routes are not advertised to OMP.
Advertise Ipv4 EIGRP	Enable this option to advertise EIGRP routes to OMP. By default, EIGRP routes are not advertised to OMP.
Advertise Ipv6 BGP	Enable this option to advertise BGP routes to OMP. By default, BGP routes are not advertised to OMP.
Advertise Ipv6 OSPF	Enable this option to advertise external OSPF routes to OMP. By default, external OSPF routes are not advertised to OMP.
Advertise Ipv6 Connected	Enable this option to advertise connected routes to OMP. By default, connected routes are not advertised to OMP.
Advertise Ipv6 Static	Enable this option to advertise static routes to OMP. By default static routes are not advertised to OMP.

Field	Description
Advertise Ipv6 LISP	Enable this option to advertise LISP routes to OMP. By default, LISP routes are not advertised to OMP.
Advertise Ipv6 ISIS	Enable this option to advertise IS-IS routes to OMP. By default, IS-IS routes are not advertised to OMP.
Advertise Ipv6 EIGRP	Enable this option to advertise EIGRP routes to OMP. By default, EIGRP routes are not advertised to OMP.

Best Path

Table 35: Best Path

Field	Description
Treat Hierarchical and Direct Paths Equally	(Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.13.1) In a Multi-Region Fabric scenario, if using secondary regions, enable this option to enable packets to use all available paths rather than only direct paths. By default, when a direct path is available to reach a destination, the overlay management protocol (OMP) enables only the direct path to the routing forwarding layer because the direct path uses fewer hops. This logic is part of route optimization. The result is that the forwarding layer, which includes application-aware routing policy, can only use the direct path. **Treat Hierarchical and Direct Paths Equally** disables this comparison of the number of hops so that traffic can use either the direct secondary-region path (fewer hops) or the primary-region path (more hops). When you disable the comparison of the number of hops, OMP applies equal-cost multi-path routing (ECMP) to all routes, and packets can use all available paths.
Transport Gateway Path Behavior	(Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.13.1) Choose one of the following: • **Prefer Transport Gateway Path**: For devices that can connect through a transport gateway, use only the transport gateway paths, even if other paths are available. • **Do ECMP Between Direct and Transport Gateway Paths**: For devices that can connect through a transport gateway and through direct paths, apply ECMP to all available paths.
Site Type	(Minimum supported release: Cisco Catalyst SD-WAN Manager Release 20.13.1) If you configure a value for **Transport Gateway Path Behavior**, this field appears. Optionally, choose one or more site types to apply the transport gateway path behavior only to those site types.

Performance Monitoring

Using Cisco SD-WAN Manager, you can monitor the performance of applications.

The following tables describe the options for configuring the Performance Monitoring feature.

Application Performance Monitoring

Table 36: Monitoring

Field	Description
Monitoring	To enable monitoring, check the check box. You can enable monitoring only in Global mode. Enabling monitoring displays a list of application groups. Fourteen application groups are enabled by default. You can disable or enable more applications based on your requirements. Check the check box adjacent to an application group to enable monitoring.

Table 37: Underlay Measurement Track Service

Field	Description
Monitoring	Click **Monitoring** drop-down list, and choose **Global** to trace tunnel paths regularly according to a configured time interval. Click the toggle button to enable the continuous monitoring option in UMTS.
Monitoring Interval (Minutes)	In the **Monitoring Interval (Minutes)** field, choose a time. This option enables you to monitor exact path at a specific time period.
Event Driven	Click the **Event Driven** drop-down list, and choose **Global** to trace tunnel paths when triggered by one of the events as per the event type.
Event Type	Click the **Event Type** drop-down list, and choose an event type. The event types are: • **SLA Change**: Change in the service-level agreement (SLA) parameter for the tunnel. • **PMTU Change**: Change in the Path MTU (PMTU) parameter for the tunnel.

To save the configuration, click **Save**.

Remote Access

The following table describes options to specify the name and description for the remote access feature.

See Configure Cisco Catalyst SD-WAN Remote Access Using a Configuration Group

Table 38: Remote Access Settings

Field	Description
Type	Choose Remote Access feature from the drop-down list.
Feature Name*	Enter a name for the feature.
Description	Enter a description of the feature. The description can contain any characters and spaces.
Connection Type	Choose the connection type from the following: • **IPsec** • **SSL-VPN** By default, IPsec is selected. We recommend using IPsec mode. SSL-VPN mode is supported only on Cisco Catalyst 8000v Edge Software with limited features.

For each parameter of the feature that has a default value, the scope is set to Default (indicated by a check mark), and the default setting or value is shown.

Private IP-Pool

The **Private IP-Pool** pane allows you to specify the size of the private IP pool to allocate to a device from the global IP pool for the remote access defined in the network hierarchy. The device uses the private IP pool to assign an IP address to each remote access client.

If you enable the remote access feature through the Create Configuration Group workflow, the workflow creates a global IPv4 pool in Network Hierarchy for remote access use. In Cisco vManage Release 20.11.1, if you want to enable the IPv6 pool for the remote access feature, you must create IPv6 pool manually in the network hierarchy. You can edit the remote access feature in a configuration groups to update the pool size.

To release the IP pool allocated to a device, remove the remote access feature, disable remote access in the service VPN, and successfully deploy the configuration group to the device. Then the IPv4 and IPv6 pools allocated to a device are returned to the global IPv4 and IPv6 pool for remote access, in the network hierarchy. The global remote access pools reflect the latest capacity.

Table 39: Private IP-Pool

Field	Description
Maximum Number of Clients	Enter the maximum number of remote access clients that can connect to a remote access headend device. This number determines the size of the IPv4 pool allocated to the device. If a global IPv6 pool is defined for remote access in the network hierarchy, each SD-WAN RA headend device will be allocated an IPv6 pool sufficient for the maximum number of remote access clients (8000).

Authentication

Table 40: Authentication

Field	Description
Radius Group Name	Choose an existing RADIUS group or create a new RADIUS group. Click **Add Radius Group** to add a RADIUS server and group to the AAA feature profile in the System Profile.
Pre-Shared Key (PSK) Authentication	Enable Pre-Shared Key (PSK) authentication. • **AAA-based-PSK**: Choose this option to fetch the pre-shared keys from the RADIUS server. This option allows configuring a pre-shared key on the RADIUS server that is unique per remote access client or a group of remote access clients. • **Groups PSK**: Choose this option to configure a common pre-shared key for all remote access clients connecting to a device. **Note** **Pre-Shared Key (PSK) Authentication** is applicable only for connection-type IPsec and not for SSL-VPN.
CA Server Setup	Choose a CA server for certificate-based authentication. The certificate from the selected CA is used by the device to authenticate the remote access clients. Before choosing a CA server, configure the CA server from **Configuration** > **Certificate Authority**.
User Authentication	Choose the user authentication option for AnyConnect Extensible Authentication Protocol (EAP) authentication used by remote access client. **Note** The **User Authentication** setting is applicable only for the IPsec connection type and not for SSL-VPN.
User & Device Authentication	Choose the user and device authentication option for AnyConnect EAP authentication used by remote access client. The **User & Device Authentication** setting is applicable only for the IPsec connection type and not for SSL-VPN.
Enable Profile Download	Enable download of an AnyConnect profile XML file to Cisco AnyConnect clients from the remote access headend devices. In the **Upload Profile XML File** pane, choose an XML file or drag and drop to upload. The maximum file size is 20 KB.

AAA Policy

Table 41: AAA Policy

Field	Description
Specify Name	Choose this option to specify the name of the policy to look up on the RADIUS server. In the **Policy Name** field, which appears only for the **Specify Name** option, enter the name of the policy.
Derive Name from Peer Identity	Choose this option to use the identity of the peer as the name of the policy to lookup on the RADIUS server. **Note** This setting is applicable only for the IPsec connection type and not for SSL-VPN.
Derive Name from Peer Identity Domain	Choose this option to use the domain portion of the identity of the peer as the name of the policy to look up on the RADIUS server. **Note** This setting is applicable only for the IPsec connection type and not for SSL-VPN.
Policy Password	Enter the policy password.
Enable Accounting	Enable accounting.

Note The IKEv2 and IPsec settings are applicable only for the IPsec connection type and not for SSL-VPN.

IKEv2 and IPsec Settings

Table 42: IKEv2 and IPsec Settings

Field	Description
Local IKE Identity Type	Enter the local IKEv2 identity type. The options are: • IPv4 Address or IPv6 Address • Email • FQDN • Key-ID
Local IKE Identity Value*	Enter the value of the local IKEv2 identity based on the identity type selected.

Field	Description
Security Association (SA) Lifetime	Enter the lifetime in seconds for the IKEv2 security association. The range is from 3600 to 86400. The default lifetime is 86400 seconds.
Enable Anti - Denial of Service (DOS) Check	Enable an Anti-Denial of Service (DOS) check.
Anti-DOS Threshold	Enter the Anti-DOS threshold value. Range: 10 to 1000. Default: 100.

SNMP

The application-layer Simple Network Management Protocol (SNMP) provides a communication standard for interaction between SNMP managers and agents. The protocol defines a standardized language that is commonly used for monitoring and managing devices in a network. The SNMP feature helps you configure the SNMP functionality on the Cisco IOS XE Catalyst SD-WAN devices.

See Configure SNMP using a Configuration Group

The following tables describe the options for configuring the SNMP feature.

SNMP Basic Settings

Table 43: SNMP Version

Field	Description
SNMP Version	Choose one of the following SNMP versions: • **SNMP v2** • **SNMP v3**
SNMP v2: Add View	
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 255 characters. You must add a view name for all views before adding a community.

Field	Description
Add OID	Click this option to add object identifiers (OID) and configure the following parameters: • **Id***: 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 Cisco Catalyst SD-WAN 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**: Enable this option to include the OID in the view or disable this option to exclude the OID from the view.
SNMP v2: Add Community	
Name*	Enter a name for the community. The name can be from 1 through 32 characters and can include angle brackets (< and >).
User Label*	(Minimum release: Cisco vManage Release 20.9.2) Enter a label or identifier for the community name. It helps you distinguish or update a community name when there are multiple community names for an SNMP target.
View*	Choose a view to apply to the community. The view specifies the portion of the MIB tree that the community can access.
Authorization*	Choose **read-only** from the drop-down list. The MIBs supported by Cisco Catalyst SD-WAN do not allow write operations, so you can configure only read-only authorization.
SNMP v2: Add Target	
VPN ID*	Enter the number of the VPN to use to reach the trap server. Range: 1 to 65525, excluding 512. For details see the VRF range behavior change described here.
IPv4/IPv6 address of SNMP server*	Enter the IP address of the SNMP server.
UDP port number to connect to SNMP server*	Enter the UDP port number for connecting to the SNMP server. Range: 1 though 65535
Community Name*	Choose the name of a community that was configured under **Add Community**. This field is applicable only to Cisco vManage Release 20.9.1 and earlier releases.
User Label*	(Minimum release: Cisco vManage Release 20.9.2) Choose a user label that was configured under **Add Community**.
Source interface for outgoing SNMP trap*	Enter the interface to use to send traps to the SNMP server that is receiving the trap information.
SNMP v3: Add View	

Field	Description
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 255 characters.
Add OID	Click this option to add object identifiers (OID) and configure the following parameters: • **Id***: 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 Cisco Catalyst SD-WAN 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**: Enable this option to include the OID in the view or disable this option to exclude the OID from the view.
SNMP v3: Add Group	
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-no-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. **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 trap group can access.
SNMP v3: Add User	
Name*	Enter a name of the SNMP user. It can be 1 to 32 alphanumeric characters.
Authentication Protocol	Choose the authentication mechanism for the user: • **md5** • **sha**
Authentication Password	Enter the authentication password either in cleartext or as an AES-encrypted key.

Field	Description
Privacy Protocol	Choose the privacy type for the user. • **aes-cfb-128**: Use Advanced Encryption Standard cipher algorithm used in cipher feedback mode, with a 128-bit key. This is a SHA-1 authentication protocol. • **aes-256-cfb-258**: Use Advanced Encryption Standard cipher algorithm used in cipher feedback mode, with a 256-bit key. This is a SHA-256 authentication protocol. Starting from Cisco Catalyst SD-WAN Manager Release 20.15.4, only **aes-256-cfb-258** is supported.
Privacy Password	Enter the privacy password either in cleartext or as an AES-encrypted key.
Group*	Choose the name of an SNMPv3 group.
SNMP v3: Add Target	
VPN ID*	Enter the number of the VPN to use to reach the trap server. Range: 1 to 65525, excluding 512. For details see the VRF range behavior change described here.
IPv4/IPv6 address of SNMP server*	Enter the IP address of the SNMP server.
UDP port number to connect to SNMP server*	Enter the UDP port number for connecting to the SNMP server. Range: 1 though 65535
User*	Choose the name of a user that was configured under **Add User**.
Source interface for outgoing SNMP trap*	Enter the interface to use to send traps to the SNMP server that is receiving the trap information.

SNMP Advanced Settings

Table 44: Advanced Settings

Field	Description
Shutdown	By default, SNMP is enabled.
Contact Person	Enter the name of the network management contact person in charge of managing the Cisco IOS XE Catalyst SD-WAN 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.