Revised: October 30, 2026

AutoVPN for Cisco 8000 Series Secure Routers using Cisco Meraki Dashboard

Feature history for AutoVPN

The table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to www.cisco.com/go/cfn. An account on Cisco.com is not required.

Table 1: Feature information for AutoVPN

Feature name	Releases	Feature information
AutoVPN	Cisco IOS XE 26.1.1 Release	Auto VPN is a proprietary technology developed by Cisco Meraki that automates the creation and management of encrypted VPN tunnels between WAN routers in different network branches. From this release, Cisco 8000 Series Secure Routers can be configured for AutoVPN using Cisco Meraki Dashboard.
Post-Quantum Cryptography (PQC) for AutoVPN	Cisco IOS XE 26.2.1 Release	From this release, AutoVPN IKEv2 or IPsec tunnels supports a hybrid post-quantum key exchange based on ML-KEM-768. The Cisco Meraki Dashboard automatically includes the PQC configuration.
AutoVPN performance probing	Cisco IOS XE 26.2.1 Release	From this release, per-queue loss, latency, jitter, reachability, and SLA state across AutoVPN IPsec sessions are measured using active probes and passive metadata sampling.

AutoVPN for Cisco 8000 Series Secure Routers using Cisco Meraki Dashboard

AutoVPN is a proprietary technology developed by Cisco Meraki that automates the creation and management of encrypted VPN tunnels between WAN routers in different network branches. It simplifies the traditionally complex and time-consuming process of configuring site-to-site VPNs by leveraging cloud-based services and automation. All configurations are performed using the Cisco Meraki Dashboard, providing a centralized interface for setup and management.

PQC support

From Cisco IOS XE 26.2.1 release, AutoVPN IPsec tunnels use a hybrid post-quantum key exchange based on ML-KEM-768.

AutoVPN performance probing

AutoVPN performance probing measures the quality of active AutoVPN IPsec paths and supplements passive measurement of data traffic. The feature reports per-queue loss, round-trip latency, jitter, per-session reachability across IPsec tunnel sessions to support Site to Site VPN performance monitoring.

AutoVPN uses both passive sampling and active probes. Both methods update the same per-queue performance state. Active and passive measurements are processed within the AutoVPN data plane and do not require clock synchronization between peers.

Passive sampling samples client traffic every 100 ms and adds measurement metadata to selected packets already traversing the tunnel. This measures the performance experienced by live traffic.

Active probing sends synthetic probes at a 1-second interval on wired uplinks and a 10-second interval on cellular uplinks. Active probes maintain path measurements and per-session reachability when client traffic is insufficient or absent.

- Passive sampling operates every 100 ms on selected client traffic.
- Active probes operate every 1 second on wired uplinks and every 10 seconds on cellular uplinks.
- Latency, jitter, and packet loss are maintained independently per tunnel path and traffic queue.
- Loss and jitter are directional.
- Probe measurements do not require clock synchronization between peers.

AutoVPN continues to be configured and managed through the Cisco Meraki Dashboard. The Dashboard establishes the AutoVPN fabric, while IOS XE performs the data-plane measurements across the active IPsec sessions.

The AutoVPN path quality data is collected from the Cisco Secure routers and integrated with Cisco Meraki Dashboard for Site to Site VPN performance monitoring.

Supported routers

From Cisco IOS XE Release 26.1, AutoVPN can be configured using Cisco Meraki Dashboard on these Cisco 8000 Series Secure Routers. For more information, refer to Introduction to IOS XE Based Secure Routers Managed by Dashboard.

Restrictions

- Support for hub-to-hub tunnels and any features that rely on them is not available.
- Active backup functionality is not supported.

Configure AutoVPN

Use one of these methods to configure AutoVPN:

- AutoVPN configuration on Cisco Meraki Dashboard, on page 3
- AutoVPN configuration on Cisco Secure Routers

AutoVPN configuration on Cisco Meraki Dashboard

For information on Cisco Meraki AutoVPN, refer to Meraki Auto VPN - Configuration and Troubleshooting.

Step 1 From the Cisco Meraki Dashboard, choose **Security & SD-WAN** > **Configure** > **Site-to-site VPN**.

Step 2 Select **Hub** or **Spoke**.

Step 3 Click **Save**.

This enables site-to-site VPN between WAN appliances.

AutoVPN configuration on Cisco Secure Routers

Once routers are onboarded into the Cisco Meraki Dashboard, select the VPN role as Hub or Spoke and save the configurations.

Note

The router configurations are not manually set on the router, instead, all the configurations are automatically pushed from the Cisco Meraki cloud.

Cisco Meraki Dashboard manages the VPN registry, routing, key distribution, and tunnel brokering to enable immediate and seamless VPN connectivity upon configuration changes.

This command initiates the AutoVPN process to connect the device to the specified VPN configuration, enabling secure communication between sites.

Configuration block

```
crypto autovpn <autovpn-cfg>
vpn-registry server <addr1><port1><addr2><9350-9381>
local <device-num><device-id><is-hub><multi-uplink-tunnels><load-balance><uplink0-name><uplink1-name>
remote <device-num><device-id><is-hub><multi-uplink-tunnels><peer-psk>
```

Description

Table 2: CLI options

CLI options	Value	Description
<addr1><addr2>	IPv4 addresses	IPv4 addresses of the 2 VPN registry servers
<device-num>	4-byte decimal	Unique in an org
<device-id>	16-byte hex value	Unique in a cluster (multiple org)
<is-hub>	Boolean	local.. <is-hub> : remote.. <is-hub> :
<peer-psk>	String	Used by local device to verify the IKEv2 auth payload received in msg-4

CLI options	Value	Description
<multi-uplink-tunnels>	Boolean	True: create tunnels over all the uplinks False: single tunnel at any time Active tunnel between local/remote primary/secondary uplink based on link availability and remote <multi-tunnel> config.
<load-balance>	Boolean	This is applicable when <multi-tunnel> is TRUE. This indicates load-balancing (ECMP) of traffic when there are multiple tunnels between a device pair. True – ECMP False- Non-ECMP with tunnel preference based
<uplink0-name>	String	Name of the uplink-0 (example, Giga Ethernet 0/0)
<uplink1-name>	String	Name of the uplink-1 (example, Giga Ethernet 1/0)

Note

AutoVPN on IOS XE Devices leverages the existing IOS XE IKEv2/IPSec and MP-BGP configurations.

PQC configuration pushed by the Cisco Meraki Dashboard

```
crypto ikev2 proposal ikev2_proposal_autovpn
 encryption aes-gcm-256
 prf sha256
 group 21
 ! Enable PQC key exchange
 pqc mlkem768 optional
!
crypto ipsec profile ipsec_profile_autovpn
 set security-association lifetime seconds 14400
 set security-association replay window-size 1024
 set transform-set ts_autovpn
 ! Enable PQC PFS
 set pfs
 set ikev2-profile ikev2_profile_autovpn
!
```

Optional path-monitor CLI configuration

AutoVPN path monitoring is enabled automatically and uses product-defined default values. In normal deployments, no additional CLI configuration is required.

The following CLI is optional and can be used when an administrator needs to tune probe behavior for a specific deployment, WAN color, or network condition. These commands are configured under sla-policy path-monitor.

```
sla-policy
  path-monitor
  probe-interval <100-310000> [multiplier <1-60>]
```

```
  ignore-local-loss
  disable
  color <WAN1-WAN8>
   probe-interval <100-310000> [multiplier <1-60>]
   disable
```

This is an example of the CLI configuration:

```
sla-policy
  path-monitor
  probe-interval 2000 multiplier 5
  ignore-local-loss
  color WAN1
   probe-interval 5000
  color WAN2
   disable
```

Table 3: CLI options

CLI options	Value	Description
probe-interval <value>	1000 ms non-cellular; 10000 ms cellular	Sets the interval between active probes in milliseconds. Range: 100–310000 ms. A per-color value overrides the global value. If local and peer intervals differ, AutoVPN uses the slower interval for that path; manual matching is not required.
multiplier <value>	7	Sets the number of consecutive unanswered probes before declaring the path unreachable. Range: 1–60.
ignore-local-loss	Disabled	Excludes locally generated QoS or queue drops from the WAN loss calculation.
disable	Enabled	Disables active path monitoring. When configured globally, it disables probing for all WAN colors; when configured under a WAN color, it affects only that color.
color WAN1 through color WAN8	No overrides	Enters the configuration context for a specific WAN color and allows per-color overrides.
no <option>	NA	Removes the configured option and restores the default or inherited behavior.

Verify the AutoVPN configuration

Use the command to verify the AutoVPN configuration on the device.

The **`show crypto autovpn session`** command was introduced in Cisco IOS XE Release 26.1.1. Use this command to troubleshoot and debug the AutoVPN configuration.

For Hub:

```
AutoVPN-HUB1#show crypto autovpn session
Local Information:
Device Number: 7111, ID: 70000000000000000000000000000111, Role: Hub

Local-WAN info learnt from VPN Registries:
Local-WAN Interface Private-IP:Port NAT-Type
------------------------------------------------------------------------------------
WAN-1 GigabitEthernet2 2.2.2.2:4500 Friendly
WAN-2 GigabitEthernet1 1.1.1.2:4500 Friendly

VPN Registry-1 10.126.71.240:9350
Local-WAN Status Public-IP:Port
-------------------------------------------------
WAN-1 Connected 10.126.71.245:5066
WAN-2 Connected 10.126.71.245:5062

VPN Registry-2 10.126.71.241:9351
Local-WAN Status Public-IP:Port
-------------------------------------------------
WAN-1 Connected 10.126.71.245:5066
WAN-2 Connected 10.126.71.245:5062

Peers learnt from VPN Registries:

Session Details:
Peer-No Local-IP:Port Peer-IP:Port Local-WAN# Peer-WAN# Session-Type State Interface Initiator
-----------------------------------------------------------------------------------------------
7333 2.2.2.2:4500 11.11.11.2:4500 1 1 Private Connected Vi4 No
7333 2.2.2.2:4500 12.12.12.2:4500 1 2 Private Connected Vi3 No
7333 1.1.1.2:4500 11.11.11.2:4500 2 1 Private Connected Vi1 No
7333 1.1.1.2:4500 12.12.12.2:4500 2 2 Private Connected Vi2 No
```

For Spoke:

```
AutoVPN_SPOKE1#show crypto autovpn session
Local Information:
Device Number: 7333, ID: 70000000000000000000000000000333, Role: Spoke

Local-WAN info learnt from VPN Registries:
Local-WAN Interface Private-IP:Port NAT-Type
------------------------------------------------------------------------------------
WAN-1 GigabitEthernet1 11.11.11.2:4500 Friendly
WAN-2 GigabitEthernet2 12.12.12.2:4500 Friendly

VPN Registry-1 10.126.71.240:9350
Local-WAN Status Public-IP:Port
-------------------------------------------------
WAN-1 Connected 10.126.71.245:5063
WAN-2 Connected 10.126.71.245:40000

VPN Registry-2 10.126.71.241:9351
Local-WAN Status Public-IP:Port
-------------------------------------------------
WAN-1 Connected 10.126.71.245:5063
WAN-2 Connected 10.126.71.245:40000

Peers learnt from VPN Registries:

Peer Number: 7111, ID: 70000000000000000000000000000111, Role:Hub
Peer-WAN Priv-IP:port(From Reg1) Priv-IP:port(From Reg2) Pub-IP:port(From Reg1) Pub-IP:port(From Reg2)
-----------------------------------------------------------------------------------------------------
WAN-1 2.2.2.2:4500 2.2.2.2:4500 10.126.71.245:5066 10.126.71.245:5066
WAN-2 1.1.1.2:4500 1.1.1.2:4500 10.126.71.245:5062 10.126.71.245:5062
```

```
Session Details:
Peer-No Local-IP:Port Peer-IP:Port Local-WAN# Peer-WAN# Session-Type State Interface Initiator
-------------------------------------------------------------------------------------------------------------
7111 11.11.11.2:4500 2.2.2.2:4500 1 1 Private Connected Vi1 Yes
7111 11.11.11.2:4500 1.1.1.2:4500 1 2 Private Connected Vi2 Yes
7111 12.12.12.2:4500 2.2.2.2:4500 2 1 Private Connected Vi3 Yes
7111 12.12.12.2:4500 1.1.1.2:4500 2 2 Private Connected Vi4
```

Note

You can verify IKEv2/IPSec and MP-BGP connectivity using the existing standard commands.

To verify use of PQC encryption in IKEv2/IPsec tunnels use the **show crypto ikev2 sa detailed** command.

```
Router# show crypto ikev2 sa detailed

IPv4 Crypto IKEv2  SA
Tunnel-id Local                 Remote                fvrf/ivrf            Status

4         1.1.1.2/500           1.1.1.1/500           none/none            READY

Encr: AES-CBC, keysize: 256, PRF: SHA512, Hash: SHA512, DH Grp:21, Auth sign: PSK, Auth verify: PSK
PQC Key Exchange: ML-KEM-768
Life/Active Time: 86400/65905 sec
CE id: 0, Session-id: 1
Local spi: 828DC8848548B23C       Remote spi: D77638A21E177EF0
Status Description: Negotiation done
Local id: 1.1.1.2
Remote id: 1.1.1.1
Local req msg id:  44             Remote req msg id:  0
Local next msg id: 44             Remote next msg id: 0
Local req queued:  44             Remote req queued:  0
Local window:      20             Remote window:      20
DPD configured for 0 seconds, retry 0
Fragmentation not  configured.
Quantum-safe Encryption using PQC: ML-KEM-768
Dynamic Route Update: enabled
Extended Authentication not configured.
NAT-T is not detected
Cisco Trust Security SGT is disabled
Initiator of SA : Yes
PEER TYPE: IOS-XE
```

Use the following show commands to view the AutoVPN probes.

```
Router #show platform hardware qfp act feature cloud-mgmt datapath autovpn session
Src IP          Dst IP          Src Port Dst Port Sess ID  Adj ID       Jitter(us) Loss(%)  RTT(us)    State

--------------- --------------- -------- -------- -------- ------------ ---------- -------- ----------
------------
10.1.17.15      10.1.18.16      4500     4500     8        0xf8000206   59         0.00     260        Up

10.1.15.15      10.1.18.16      4500     4500     7        0xf80001f6   96         0.00     391        Up

10.1.15.15      10.1.16.16      4500     4500     5        0xf80001d6   52         3.19     200612     Up
```

```
10.1.17.15      10.1.16.16      4500     4500     6        0xf80001e6   183        0.00     376        Up


pm5#show platform software ndbman rp ac database record_get
//locations;fru=BINOS_FRU_FP;slot=0;bay=0;chassis=-1;node=0/services;serviceName=dp_qper/autovpn_pathmon;local_device_no=500;peer_no=600;local_uplink_no=1;remote_uplink_no=1;queue_id=1
NDBMAN DB show command default max records limit is 1000

URI =
//locations;fru=BINOS_FRU_FP;slot=0;bay=0;chassis=-1;node=0/services;serviceName=dp_qper/autovpn_pathmon;local_device_no=500;peer_no=600;local_uplink_no=1;remote_uplink_no=1;queue_id=0
cur_loss: '314'
cur_jitter: '0'
cur_latency: '200'
cur_mos: '30'
export_time: 'Fri, 31 Jul 2026 07:44:14 +0000'
local_device_no: '500'
peer_no: '600'
local_uplink_no: '1'
remote_uplink_no: '1'
queue_id: '0'


pm5#show platform hardware qfp act feature cloud-mgmt datapath autovpn session 5
Session ID              5
Source IP               10.1.15.15
Source Port             4500
Destination IP          10.1.16.16
Destination Port        4500
Adj ID                  0xf80001d6
PMTU                    1400
Local Probe Interval    1000
Peer Probe Interval     1000
Actual Probe Interval   1000
Probe Multiplier        7
State                   Up
Session Up(s)           53448
Session Up/Down Count   1/0
Ignore Local Loss       False
Echo       (Tx/Rx)      59386/59379
SLA        (Tx/Rx)      47509/47503

Pathmon stats
Queue DSCP Jitter(us) Loss(%) RTT(us) Sampled Tx      Sampled Rx      Tx              Rx
----- ---- ---------- ------- ------- --------------- --------------- --------------- ---------------
0     46   290        3.01    200634  31578           31500           339279          338984
1     26   62         2.71    200499  31592           31464           339274          338844
2     10   106        2.77    200324  31571           31521           337970          340216
3     0    62         2.96    200409  31591           31480           339271          340099

Pathmon loss window stats
Queue Base Send Pkts  Base Receive Pkts Current Send Pkts Current Receive Pkts StatAddr
----- --------------  ----------------- ----------------- -------------------- ----------
0     11270           10937             0                 0                    0xfffefcf4f260
1     11269           10962             0                 0                    0xfffefcf4f348
2     11268           10932             0                 0                    0xfffefcf4f430
3     11270           10922             0                 0                    0xfffefcf4f518
```

Monitor and troubleshoot

This section details debug commands for troubleshooting and provides information on related connection syslog messages.

Table 4: Debug cammands

To debug	Use the command	Description
AutoVPN **Note** The AutoVPN debug commands are introduced in Cisco IOS XE 26.1.1 Release.	**debug crypto autovpn error**	Enables AutoVPN error debugs
	debug crypto autovpn event	Enables AutoVPN debugs related to events like session events
	debug crypto autovpn info	Enables AutoVPN info debugs
	debug crypto autovpn verbose	Enables VPN registry message send and receive events
IKEv2/IPSec	**debug crypto ikev2**	Enables IKEv2 debug messages
	debug crypto ikev2 error	Enables debugging for IKEv2 errors
	debug crypto ikev2 internal	Enables internal debugging for IKEv2
	debug crypto ikev2 packet	Shows IKEv2 packet-level send/receive details
	debug crypto ipsec	Displays IPsec events
	debug crypto ipsec error	Shows IPsec-specific errors
	debug crypto ipsec message	Shows IPsec operational messages
	debug crypto ipsec states	Shows IPsec SA state transitions
	debug tunnel protection	Shows tunnel-protection/IPsec-profile activity
MP-BGP	**debug ip bgp vpnv4 unicast updates**	Shows VPNv4 route updates
	debug ip bgp vpnv4 unicast updates <peer-ip> in	Shows VPNv4 routes received from one MP-BGP peer
	debug ip bgp vpnv4 unicast updates <peer-ip> out	Shows VPNv4 routes advertised to one MP-BGP peer

Syslog messages

AutoVPN session connection syslog message:

Event Type	Details
AUTOVPN_VPN_REG_SESS_DOWN	AutoVPN connection is DOWN from Local Interface IP: <IP address> to VPN registry IP:Port <port address>
AUTOVPN_VPN_REG_SESS_UP	AutoVPN connection is UP from Local Interface IP: <IP address> to VPN registry IP:Port <port address>

AutoVPN peer session connection syslog message:

Event Type	Details
AUTOVPN_PEER_SESS_DOWN	AutoVPN tunnel is DOWN between local IP: <IP address> and Peer IP:Port <port address>
AUTOVPN_PEER_SESS_UP	AutoVPN tunnel is UP between local IP: <IP address> and Peer IP:Port <port address>