



VPN Monitoring and Troubleshooting in Security Cloud Control

- [Site-to-Site VPN Summary Page, on page 1](#)
- [Monitor Remote Access VPN Sessions, on page 1](#)
- [SD-WAN Summary Dashboard, on page 1](#)
- [System Messages, on page 5](#)
- [Debug Commands, on page 5](#)

Site-to-Site VPN Summary Page

You can use the Site-to-Site VPN Summary page to see consolidated information about VPN users, including the current status of users, device types, client applications, user geolocation information, and duration of connections. You can view details of the configured VPN topologies such as VPN interfaces, tunnel status, and so on.

For all VPN topologies, you can edit or delete the topology using the edit and delete buttons. For SASE topology VPNs, you have options to deploy, edit and delete any topology.

Monitor Remote Access VPN Sessions

The Security Cloud Control Remote Access Monitoring dashboard can be used to view consolidated information about RA VPN users, including the current status of users, device types, client applications, user geolocation information, and duration of connections. You can also disconnect RA VPN sessions as needed.

See [Monitor Remote Access Virtual Private Network Sessions](#) for more information.

SD-WAN Summary Dashboard

The SD-WAN Summary dashboard (**Overview > Dashboards > SD-WAN SummaryAnalysis > SD-WAN Summary**) provides a snapshot of your WAN devices and their interfaces. This dashboard helps you to:

- Identify issues with the underlay and overlay (VPN) topologies.

- Troubleshoot VPN issues using the existing **Health Monitoring**, **Device Management**, and **Site-to-Site Monitoring** pages.
- Monitor application performance metrics of WAN interfaces. The threat defense steers application traffic based on these metrics.

A WAN device must meet one of the following criteria:

- The device must be a VPN peer.
- The device must have WAN interface.

A WAN interface must meet one of the following criteria:

- The interface has IP address-based path monitoring enabled on it.
- The interface has a Policy Based Routing (PBR) policy with at least one application configured to monitor it.

For more information about PBR policy and path monitoring, see [Policy Based Routing](#).

Click **Uplink Decisions** to view the **VPN Troubleshooting** page. You can view syslogs with ID: 880001. These syslogs show the threat defense interfaces through which it steers traffic based on the configured PBR policy.

To view the above syslogs and to view the data on this dashboard, ensure that you review [Prerequisites for Using SD-WAN Summary Dashboard, on page 2](#).

For clusters, this dashboard displays application performance metrics of only the control node and not the data nodes.

Prerequisites for Using SD-WAN Summary Dashboard

- You must be an Admin, Security Analyst, or Maintenance user to view this dashboard. See [Secure Firewall Management Center and Cloud-delivered Firewall Management Center User Role Mapping](#) for more information.
- Threat defense devices must be Version 7.2 or later.
- Enable IP-based path monitoring and HTTP-based application monitoring on the WAN interfaces.
 1. Choose **Devices > Device Management**.
 2. Click the edit icon adjacent to the device that you want to edit.
 3. Click the edit icon adjacent to the interface that you want to edit.
 4. Click the **Path Monitoring** tab.
 5. Check the **Enable IP based Monitoring** check box.
 6. Check the **Enable HTTP based Application Monitoring** check box.
 7. Click **OK**.
- Configure a PBR policy with at least one application configured to monitor it:
 1. Choose **Devices > Device Management**.

2. Click the edit icon adjacent to the device that you want to edit.
 3. Click **Routing**.
 4. In the left pane, click **Policy Based Routing**.
 5. Click **Add**.
 6. From the **Ingress Interface** drop-down list, choose an interface.
 7. Click **Add** to configure a forwarding action.
 8. Configure the parameters.
 9. Click **Save**.
- To view syslogs when you click **Uplink Decisions**, you must:
 - Choose **Devices > Platform Settings** and create or edit a threat defense policy.
 - In the left pane, click **Syslog**.
 - Click the **Logging Setup** tab.
 - Check the **Enable Logging** check box to turn on the data plane system logging for the threat defense device.
 - Click the **All Logs** radio button to enable logging of all the troubleshooting syslog messages.
or
Click the **VPN Logs** radio button to enable logging of only the VPN troubleshooting messages.
 - Click **Save**.

Monitor WAN Devices and Interfaces Using the SD-WAN Summary Dashboard

The SD-WAN Summary dashboard has the following widgets :

- [WAN Connectivity, on page 3](#)
- [VPN Topology, on page 4](#)
- [Interface Throughput, on page 4](#)
- [Device Inventory, on page 4](#)
- [WAN Device Health, on page 4](#)

WAN Connectivity

This widget provides a summary of the WAN interfaces statuses. It shows the number of WAN interfaces that are in the **Online**, **Offline** or **No Data** states. Note that you cannot monitor subinterfaces using this widget.

Click **View All Interfaces** to view more details about the interfaces in the health monitor page.

If a WAN interface is in the **Offline** or **No Data** state, you can troubleshoot it from the health monitor page:

1. In the **Monitoring** pane, expand **Devices**.

2. Click the corresponding WAN device to view the device-specific health details.
3. Click the **Interface** tab to view the interface status and aggregate traffic statistics for a specific time.

Alternatively, you can click **View System & Troubleshoot Details**. The health monitor page is displayed with all the necessary details.

VPN Topology

This widget provides a summary of the site-to-site VPN tunnel statuses. It shows the number of **Active**, **Inactive**, and **No Active Data** VPN tunnels.

Click **View All Connections** to view the VPN tunnel details in the **Site-to-site VPN Monitoring** dashboard.

If the tunnels are in the **Inactive** or **No Active Data** state, you can troubleshoot using the **Site-to-site VPN Monitoring** dashboard. In the **Tunnel Status** widget, hover your cursor over a topology, click **View** (👁) and do one of the following:

- Click the **CLI Details** tab to view the details of the VPN tunnels.
- Click the **Packet Tracer** tab to use the packet tracer tool for the topology.

Interface Throughput

This widget monitors the average throughput of the WAN interfaces during the chosen time period.

The interface throughput is classified into four bands. These details aid in cost planning and resourcing. You can choose a time range for the widget data from the **Show Last** drop-down list. The range is from 15 minutes to two weeks.

Click **View Health Monitoring** to view more details about the interface in the health monitor page.

Device Inventory

This widget lists all the managed WAN devices and groups them according to the model.

Click **View Device Management** to view more details about the device in the **Device Management** page.

WAN Device Health

This widget displays the device count according to the health of the WAN devices. You can view the number of devices with errors, warnings, or those that are in **Disabled** state.

Click **View Health Monitoring** to view the alarms, and quickly identify, isolate, and resolve issues.

If the health of a device is affected, you can troubleshoot it from the health monitor page.

1. In the **Monitoring** pane, expand **Devices**.
2. Click the corresponding WAN device to view the device-specific health details.
3. Click **View System & Troubleshoot Details**. The health monitor page is displayed with all the necessary details.

A device can be in **Disabled** state for multiple reasons, including the following:

- Management interface is disabled.
- Device is powered off.

- Device is being upgraded.

Monitor Application Performance Metrics of WAN Interfaces Using the SD-WAN Summary Dashboard

Under the **Application Monitoring** tab, you can select a WAN device and view the application performance metrics for the corresponding WAN interfaces. These metrics include Jitter, Round Trip Time (RTT), Mean Opinion Score (MOS), and Packet Loss.

By default, the metrics data is refreshed every 5 minutes. You can change the refresh time; the range is from 5 to 30 minutes. You can view the metrics in tabular and graphical formats. For each WAN interface, the latest metric value appears in the table. For graphical data, you can choose a time interval of up to 24 hours to view the metrics data for the corresponding WAN interfaces.

System Messages

The Message Center is the place to start your troubleshooting. This feature allows you to view messages that are continually generated about system activities and status. To open the Message Center, click **System Status**, located to the immediate right of the **Deploy** button in the main menu.

Debug Commands

This section explains how you use debug commands to help you diagnose and resolve VPN-related problems. The commands described here are not exhaustive, this section include commands according to their usefulness in assisting you to diagnose VPN-related problems.

Usage Guidelines

Debug commands consume high-priority CPU resources, which can make the system unusable. Only use debug commands for specific troubleshooting or when instructed by Cisco TAC. To minimize impact, run these commands during periods of low network traffic.

You can view debug output in a CLI session only. Output is directly available when connected to the Console port, or when in the diagnostic CLI (enter **system support diagnostic-cli**). You can also view output from the device CLI with **show console-output** command.

To show debugging messages for a given feature, use the **debug** command. To disable the display of debug messages, use the **no** form of this command. Use **no debug all** to turn off all debugging commands.

```
debug feature [subfeature] [level]
no debug feature [subfeature]
```

Syntax Description

<i>feature</i>	Specifies the feature for which you want to enable debugging. To see the available features, use the debug ? command for CLI help.
<i>subfeature</i>	(Optional) Depending on the feature, you can enable debug messages for one or more subfeatures. Use ? to see the available subfeatures.
<i>level</i>	(Optional) Specifies the debugging level. Use ? to see the available levels.

Command Default The default debugging level is 1.

Example

With multiple sessions running on remote access VPN, troubleshooting can be difficult, given the size of the logs. You can use the **debug webvpn condition** command to set up filters to target your debug process more precisely.

debug webvpn condition {group name | p-ipaddress ip_address [{subnet subnet_mask | prefix length}] | reset | user name}

Where:

- **group name** filters on a group policy (not a tunnel group or connection profile).
- **p-ipaddress ip_address** [{subnet subnet_mask | prefix length}] filters on the public IP address of the client. The subnet mask (for IPv4) or prefix (for IPv6) is optional.
- **reset** resets all filters. You can use the **no debug webvpn condition** command to turn off a specific filter.
- **user name** filters by username.

If you configure more than one condition, the conditions are conjoined (ANDed), so that debugs appear only if all conditions are met.

After setting up the condition filter, use the base **debug webvpn** command to turn on the debug. Setting the conditions alone does not enable the debug. Use the **show debug** and **show webvpn debug-condition** commands to view the current state of debugging.

The following shows an example of enabling a conditional debug on the user jdoe.

```
firepower# debug webvpn condition user jdoe

firepower# show webvpn debug-condition
INFO: Webvpn conditional debug is turned ON
INFO: User name filters:
INFO: jdoe

firepower# debug webvpn
INFO: debug webvpn enabled at level 1.

firepower# show debug
debug webvpn enabled at level 1
INFO: Webvpn conditional debug is turned ON
INFO: User name filters:
INFO: jdoe
```

Related Commands

Command	Description
show debug	Shows the currently active debug settings.
undebug	Disables debugging for a feature. This command is a synonym for no debug .

debug aaa

See the following commands for debugging configurations or authentication, authorization, and accounting (AAA) settings.

debug aaa [*accounting* | *authentication* | *authorization* | *common* | *internal* | *shim* | *url-redirect*]

Syntax Description

<i>aaa</i>	Enables debugging for AAA. Use ? to see the available subfeatures.
<i>accounting</i>	(Optional) Enables AAA accounting debugging.
<i>authentication</i>	(Optional) Enables AAA authentication debugging.
<i>authorization</i>	(Optional) Enables AAA authorization debugging.
<i>common</i>	(Optional) Specifies the AAA common debug level. Use ? to see the available levels.
<i>internal</i>	(Optional) Enables AAA internal debugging.
<i>shim</i>	(Optional) Specifies the AAA shim debug level. Use ? to see the available levels.
<i>url-redirect</i>	(Optional) Enables AAA url-redirect debugging.

Command Default

The default debugging level is 1.

Related Commands

Command	Description
show debug aaa	Shows the currently active debug settings for AAA.
undebg aaa	Disables debugging for AAA. This command is a synonym for no debug aaa .

debug crypto

See the following commands for debugging configurations or settings associated with crypto.

debug crypto [*ca* | *condition* | *engine* | *ike-common* | *ikev1* | *ikev2* | *ipsec* | *ss-apic*]

Syntax Description

<i>crypto</i>	Enables debugging for <i>crypto</i> . Use ? to see the available subfeatures.
<i>ca</i>	(Optional) Specifies the PKI debug levels. Use ? to see the available subfeatures.
<i>condition</i>	(Optional) Specifies the IPsec/ISAKMP debug filters. Use ? to see the available filters.
<i>engine</i>	(Optional) Specifies the crypto engine debug levels. Use ? to see the available levels.
<i>ike-common</i>	(Optional) Specifies the IKE common debug levels. Use ? to see the available levels.

debug crypto ca

<i>ikev1</i>	(Optional) Specifies the IKE version 1 debug levels. Use ? to see the available levels.
<i>ikev2</i>	(Optional) Specifies the IKE version 2 debug levels. Use ? to see the available levels.
<i>ipsec</i>	(Optional) Specifies the IPsec debug levels. Use ? to see the available levels.
<i>condition</i>	(Optional) Specifies the Crypto Secure Socket API debug levels. Use ? to see the available levels.
<i>vpnclient</i>	(Optional) Specifies the EasyVPN client debug levels. Use ? to see the available levels.

Command Default The default debugging level is 1.

Related Commands	Command	Description
	show debug crypto	Shows the currently active debug settings for crypto.
	undebug crypto	Disables debugging for crypto. This command is a synonym for no debug crypto .

debug crypto ca

See the following commands for debugging configurations or settings associated with crypto ca.

debug *crypto ca* [*cluster* | *messages* | *periodic-authentication* | *scep-proxy* | *transactions* | *trustpool*] [*1-255*]

Syntax Description	<i>crypto ca</i>	Enables debugging for <i>crypto ca</i> . Use ? to see the available subfeatures.
	<i>cluster</i>	(Optional) Specifies the PKI cluster debug level. Use ? to see the available levels.
	<i>cmp</i>	(Optional) Specifies the CMP transactions debug level. Use ? to see the available levels.
	<i>messages</i>	(Optional) Specifies the PKI Input/Output message debug level. Use ? to see the available levels.
	<i>periodic-authentication</i>	(Optional) Specifies the PKI periodic-authentication debug level. Use ? to see the available levels.
	<i>scep-proxy</i>	(Optional) Specifies the SCEP proxy debug level. Use ? to see the available levels.
	<i>server</i>	(Optional) Specifies the local CA server debug level. Use ? to see the available levels.
	<i>transactions</i>	(Optional) Specifies the PKI transaction debug level. Use ? to see the available levels.
	<i>trustpool</i>	(Optional) Specifies the trustpool debug level. Use ? to see the available levels.

1-255	(Optional) Specifies the debugging level.
-------	---

Command Default

The default debugging level is 1.

Related Commands

Command	Description
show debug crypto ca	Shows the currently active debug settings for crypto ca.
undebug	Disables debugging for crypto ca. This command is a synonym for no debug crypto ca .

debug crypto ikev1

See the following commands for debugging configurations or settings associated with Internet Key Exchange version 1 (IKEv1).

debug *crypto ikev1* [*timers*] [*1-255*]

Syntax Description

<i>ikev1</i>	Enables debugging for <i>ikev1</i> . Use ? to see the available subfeatures.
<i>timers</i>	(Optional) Enables debugging for IKEv1 timers.
<i>1-255</i>	(Optional) Specifies the debugging level.

Command Default

The default debugging level is 1.

Related Commands

Command	Description
show debug crypto ikev1	Shows the currently active debug settings for IKEv1.
undebug crypto ikev1	Disables debugging for IKEv1. This command is a synonym for no debug crypto ikev1 .

debug crypto ikev2

See the following commands for debugging configurations or settings associated with Internet Key Exchange version 2 (IKEv2).

debug *crypto ikev2* [*ha* | *platform* | *protocol* | *timers*]

Syntax Description

<i>ikev2</i>	Enables debugging <i>ikev2</i> . Use ? to see the available subfeatures.
<i>ha</i>	(Optional) Specifies the IKEv2 HA debug level. Use ? to see the available levels.
<i>platform</i>	(Optional) Specifies the IKEv2 platform debug level. Use ? to see the available levels.
<i>protocol</i>	(Optional) Specifies the IKEv2 protocol debug level. Use ? to see the available levels.

debug crypto ipsec

<i>timers</i>	(Optional) Enables debugging for IKEv2 timers.
---------------	--

Command Default

The default debugging level is 1.

Related Commands

Command	Description
show debug crypto ikev2	Shows the currently active debug settings for IKEv2.
undebugcrypto ikev2	Disables debugging for IKEv2. This command is a synonym for no debug crypto ikev2 .

debug crypto ipsec

See the following commands for debugging configurations or settings associated with IPsec.

debug *crypto ipsec* [1-255]

Syntax Description

<i>ipsec</i>	Enables debugging for <i>ipsec</i> . Use ? to see the available subfeatures.
<i>1-255</i>	(Optional) Specifies the debugging level.

Command Default

The default debugging level is 1.

Related Commands

Command	Description
show debug crypto ipsec	Shows the currently active debug settings for IPsec.
undebugcrypto ipsec	Disables debugging for IPsec. This command is a synonym for no debug crypto ipsec .

debug ldap

See the following commands for debugging configurations or settings associated with LDAP (Lightweight Directory Access Protocol).

debug *ldap* [1-255]

Syntax Description

<i>ldap</i>	Enables debugging for LDAP. Use ? to see the available subfeatures.
<i>1-255</i>	(Optional) Specifies the debugging level.

Command Default

The default debugging level is 1.

Related Commands

Command	Description
show debug ldap	Shows the currently active debug settings for LDAP.
undebugldap	Disables debugging for LDAP. This command is a synonym for no debug ldap .

debug ssl

See the following commands for debugging configurations or settings associated with SSL sessions.

debug *ssl* [*cipher* | *device*] [*1-255*]

Syntax Description	<i>ssl</i>	Enables debugging for SSL. Use ? to see the available subfeatures.
	<i>cipher</i>	(Optional) Specifies the SSL cipher debug level. Use ? to see the available levels.
	<i>device</i>	(Optional) Specifies the SSL device debug level. Use ? to see the available levels.
	<i>1-255</i>	(Optional) Specifies the debugging level.

Command Default The default debugging level is 1.

Related Commands	Command	Description
	show debug ssl	Shows the currently active debug settings for SSL.
	undebug ssl	Disables debugging for SSL. This command is a synonym for no debug ssl .

debug webvpn

See the following commands for debugging configurations or settings associated with WebVPN.

debug *webvpn* [*anyconnect* | *chunk* | *cifs* | *citrix* | *compression* | *condition* | *cstp-auth* | *customization* | *failover* | *html* | *javascript* | *kcd* | *listener* | *mus* | *nfs* | *request* | *response* | *saml* | *session* | *task* | *transformation* | *url* | *util* | *xml*]

Syntax Description	<i>webvpn</i>	Enables debugging for WebVPN. Use ? to see the available subfeatures.
	<i>anyconnect</i>	(Optional) Specifies the WebVPN Secure Client debug level. Use ? to see the available levels.
	<i>chunk</i>	(Optional) Specifies the WebVPN chunk debug level. Use ? to see the available levels.
	<i>cifs</i>	(Optional) Specifies the WebVPN CIFS debug level. Use ? to see the available levels.
	<i>citrix</i>	(Optional) Specifies the WebVPN Citrix debug level. Use ? to see the available levels.
	<i>compression</i>	(Optional) Specifies the WebVPN compression debug level. Use ? to see the available levels.
	<i>condition</i>	(Optional) Specifies the WebVPN filter conditions debug level. Use ? to see the available levels.

<i>cstp-auth</i>	(Optional) Specifies the WebVPN CSTP authentication debug level. Use ? to see the available levels.
<i>customization</i>	(Optional) Specifies the WebVPN customization debug level. Use ? to see the available levels.
<i>failover</i>	(Optional) Specifies the WebVPN failover debug level. Use ? to see the available levels.
<i>html</i>	(Optional) Specifies the WebVPN HTML debug level. Use ? to see the available levels.
<i>javascript</i>	(Optional) Specifies the WebVPN Javascript debug level. Use ? to see the available levels.
<i>kcd</i>	(Optional) Specifies the WebVPN KCD debug level. Use ? to see the available levels.
<i>listener</i>	(Optional) Specifies the WebVPN listener debug level. Use ? to see the available levels.
<i>mus</i>	(Optional) Specifies the WebVPN MUS debug level. Use ? to see the available levels.
<i>nfs</i>	(Optional) Specifies the WebVPN NFS debug level. Use ? to see the available levels.
<i>request</i>	(Optional) Specifies the WebVPN request debug level. Use ? to see the available levels.
<i>response</i>	(Optional) Specifies the WebVPN response debug level. Use ? to see the available levels.
<i>saml</i>	(Optional) Specifies the WebVPN SAML debug level. Use ? to see the available levels.
<i>session</i>	(Optional) Specifies the WebVPN session debug level. Use ? to see the available levels.
<i>task</i>	(Optional) Specifies the WebVPN task debug level. Use ? to see the available levels.
<i>transformation</i>	(Optional) Specifies the WebVPN transformation debug level. Use ? to see the available levels.
<i>url</i>	(Optional) Specifies the WebVPN URL debug level. Use ? to see the available levels.
<i>util</i>	(Optional) Specifies the WebVPN utility debug level. Use ? to see the available levels.
<i>xml</i>	(Optional) Specifies the WebVPN XML debug level. Use ? to see the available levels.

Command Default

The default debugging level is 1.

Related Commands

Command	Description
show debug webvpn	Shows the currently active debug settings for WebVPN.
undebug webvpn	Disables debugging for WebVPN. This command is a synonym for no debug webvpn .

 `debug webvpn`