VPN Monitoring and Troubleshooting

This chapter describes threat defense VPN monitoring tools, parameters, and statistics information as well as troubleshooting.

VPN Summary Dashboard

System dashboards provide you with at-a-glance views of current system status, including data about the events collected and generated by the system. You can use the VPN dashboard 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.

Viewing the VPN Summary Dashboard

Remote access VPNs provide secure connections for remote users, such as mobile users or telecommuters. Monitoring these connections provides important indicators of connection and user session performance at a glance.

You must be an Admin user in a leaf domain to perform this task.

Procedure

Step 1 Choose **Overview** > **Dashboards** > **Access Controlled User Statistics** > **VPN**.

Step 2 View the Remote Access VPN information widgets:

- Current VPN Users by Duration.

- Current VPN Users by Client Application.
- Current VPN Users by Device.
- VPN Users by Data Transferred.
- VPN Users by Duration.
- VPN Users by Client Application.
- VPN Users by Client Country.

Remote Access VPN Dashboard

Remote Access Virtual Private Network (RA VPN) allows remote users to securely connect to your network. The RA VPN dashboard allows you to monitor real-time data from active RA VPN sessions on the devices. You can quickly determine problems related to user sessions and mitigate the problems for your network and users.

RA VPN dashboard (**Overview > Dashboards > Remote Access VPN**) provides a snapshot of the active RA VPN sessions on the threat defense devices managed by the management center.

The dashboard has the following widgets:

- Active Sessions (Tabular View)
- Active Sessions (Map view)
- Sessions
- Device Identity Certificates

Active Sessions (Tabular View)

This widget provides a tabular view of the active RA VPN users connected. You can view details of the active RA VPN sessions such as username, assigned IP, public IP, login time, VPN gateway (threat defense device), client application, client operating system, connection profile, and group policy. You can use the filter to narrow down your search based on the different criteria. You can also perform the following actions on the individual sessions:

- Terminate a session of a specific user.
- Terminate all sessions of a specific user connected to a specific VPN gateway.
- Terminate all sessions that are connected to a specific VPN gateway.

Active Sessions (Map View)

This widget shows an interactive heat map to visualize the location of the users connected through RA VPN sessions on the devices.

- Countries that have user sessions appear in shades of blue.
- Legend of the map provides a scale that indicates the correlation between the number of sessions in a country and the shade of blue for the country.

- Hover the mouse pointer over the map to view the country name and the total number of active user sessions.
- Zoom in, zoom out, and reset options are available.

Sessions

This widget allows you to monitor real-time data from active RA VPN sessions on the devices. You can filter and view the distribution of active RA VPN sessions according to:

- Device: Displays the number of sessions per device.
- Encryption Type: Displays the number of Secure Client SSL or IPsec sessions.
- Secure Client Version: Displays the sessions per Secure Client version.
- Operating System: Displays the sessions per operating systems. For example, Windows, Linux, Mac, Mobile OS, and so on.
- Connection Profile: Displays the sessions per connection profile.

Device Identity Certificates

This widget provides information about the identity certificate expiry of the RA VPN gateways. You can view expired certificates and certificates that are due for expiry within a month. Click **View Details** to view the certificates in the **Device > Certificates** page.

SD-WAN Summary Dashboard

The SD-WAN Summary dashboard (**Overview > Dashboards > 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.

Prerequisites for Using SD-WAN Summary Dashboard

- You must be an Admin, Security Analyst, or Maintenance user to view this dashboard.
- 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 the application performance metrics for the WAN interfaces, you must:
  - Threat defense devices must be Version 7.4.1.
  - Enable data collection from the SD-WAN module in the health policy.
    1. Choose **System > Policy**.
    2. Click the **Edit health policy** icon.
    3. In the **Health Modules** tab, under **SD-WAN**, click the **SD-WAN Monitoring** toggle button.
  - Configure applications for the PBR policies.

1. Choose **Objects > Object Management > Access List > Extended**.
2. Click the edit icon adjacent to the access list and add the applications for the PBR policy.

- Configure the forwarding action for the policy with one of the four application metrics.
  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 the edit icon adjacent to the policy that you want to edit.
  6. In the **Edit Policy Based Route** dialog box, click the edit icon adjacent to the corresponding ACL.
  7. In the **Edit Forwarding Actions** dialog box, from the **Interface Ordering** drop-down list, choose one of the following options:
     - **Minimal Jitter**
     - **Maximum Mean Opinion Score**
     - **Minimal Round-Trip Time**
     - **Minimal Packet Loss**

     If you choose **Interface Priority** or **Order**, application monitoring is not enabled on the interface.
- Configure ECMP 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 **Routing**.
  4. In the left pane, click **ECMP**.
  5. Click **Add** and specify a name for the ECMP zone.
  6. Click **Add** to move interfaces from **Available Interfaces** to **Selected Interfaces**.
  7. Click **OK**.
- Ensure that traffic passes through the interface.
- Enable DNS inspection on each WAN device so that the threat defense device can do DNS snooping, and configure the trusted DNS servers:
  1. Choose **Devices > Platform Settings**.
  2. Click the edit icon adjacent to the threat defense policy that you want to edit.
  3. In the left pane, click **DNS**.
  4. Click the **DNS Settings** tab.

5. Check the **Enable DNS name resolution by device** check box.
6. Click the **Trusted DNS Servers** tab.
7. Do one of the following:
   - Click the **Trust Any DNS server** toggle button.
   - Under **Specify DNS Servers**, click **Edit** to add trusted DNS servers.

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

The SD-WAN Summary dashboard has the following widgets under the **Overview** tab:

Top Applications

This widget displays the top 10 applications ranked according to throughput.

You can choose a time range for the widget data from the **Show Last** drop-down list. The range is 15 minutes to two weeks.

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 the View icon 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 throughput utilization of the WAN interfaces.

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.

VPN Session and User Information

The system generates events that communicate the details of user activity on your network, including VPN-related activity. The system monitoring capabilities enable you to determine quickly whether remote access VPN problems exist and where they exist. You can then apply this knowledge and use your network management tools to reduce or eliminate problems for your network and users. Optionally, you can log out remote access VPN users as needed.

Viewing Remote Access VPN Active Sessions

Analysis > **Users** > **Active Sessions**

Lets you view the currently logged-in VPN users at any given point in time with supporting information such as the user name, login duration, authentication type, assigned/public IP address, device details, client version, endpoint information, throughput, bandwidth consumed group policy, tunnel group and so on. The system allows you to filter current user information, log users out, and delete users from the summary list.

Note If you configure your VPN in a high-availability deployment, the device name displayed against active VPN sessions can be the primary or secondary device that identified the user session.

Viewing Remote Access VPN User Activity

Analysis > **Users** > **User Activity**

Lets you view the details of user activity on your network. The system logs historical events and includes VPN-related information such as connection profile information, IP address, geolocation information, connection duration, throughput, and device information.

Site to Site VPN Connection Event Monitoring

The site-to-site VPN connection event allows you to know if the VPN encrypts or do not encrypts the connection and helps you to troubleshoot connectivity issues, especially in multi-hop VPN deployments. The event dashboard of the management center displays the IP address of the VPN peer (peer's IKE address) which encrypts or decrypts the traffic and displays the VPN action as follows:

- If the connection is decrypted by the VPN, the column **Decrypt Peer** displays the IP address of the VPN peer which decrypts the traffic and displays **Decrypt** as the VPN action.
- If the connection is encrypted by the VPN, the column **Encrypt Peer** displays the IP address of the VPN peer which encrypts the traffic and displays **Encrypt** as the VPN action.

- If the VPN server cascades the connection, it gets decrypted on one tunnel and gets re-encrypted on another tunnel. In this case, both **Encrypt Peer** and **Decrypt Peer** IP addresses get appears in the event. The column **VPN Action** displays **VPN Routing** as the action to indicate that the connection transit through the VPN server.

If you enable the bypass Access Control Policy for decrypted traffic (sysopt permit-vpn) option, the system bypasses the Access Control Policy and do not log events for decrypted traffic. This option is disabled by default and all decrypted traffic in the VPN tunnel undergoes ACL inspection.

View Site to Site VPN Connection Events

Access the connection event viewer of the management center to know if the VPN encrypts or do not encrypts the connection traffic and to retrieve the VPN peer details.

Before you begin

Ensure that you enable logging of connection events at the beginning of connection and at the end of connection in the access control rule.

Procedure

Step 1 Choose **Analysis** > **Connections** > **Events**.

Step 2 Go to **Table View of Connection Events** tab.

Step 3 In the table view of events, multiple fields are hidden by default. To change the fields that appear, click the **x** icon in any column name to display a field chooser.

Step 4 Choose the following columns:

- Decrypt Peer
- Encrypt Peer
- VPN Action

Step 5 Click **Apply**.

See *Connection and Security-Related Connection Events* in the Secure Firewall Management Center Administration Guide for more information on the connection events.

VPN Troubleshooting

This section describes VPN troubleshooting tools and debug information.

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.

VPN System Logs

You can enable logging of VPN troubleshoot syslogs for threat defense devices. Logging information can help you identify and isolate network or device configuration problems. When you enable VPN logging, the threat defense devices send VPN syslogs to the management center.

All VPN syslogs appear with a default severity level **errors** or a higher severity (unless changed). You can manage the VPN logging through threat defense platform settings. You can adjust the message severity level by editing the **VPN Logging Settings** in the threat defense platform settings policy for targeted devices. See Configure Syslog Logging for Threat Defense Devices for details on enabling VPN logging, configuring syslog servers, and viewing the system logs.

We recommend that you set the logging level of the VPN logs as level 3 (Errors). Setting the VPN logging level to level 4 and above (Warnings, Notifications, Informational or Debugging) could overload the management center.

Note When you configure a device with site-to-site or remote access VPN, it automatically enables sending VPN syslogs to the management center by default.

Viewing VPN System Logs

The system captures event information to help you to gather additional information about the source of your VPN problems. Any VPN syslogs that are displayed have a default severity level 'ERROR' or higher (unless changed). By default the rows are sorted by the **Time** column.

You must be an Admin user in a leaf domain to perform this task.

Before you begin

Enable VPN logging by checking the **Enable Logging to Secure Firewall Management Center** check boxselecting the **VPN Logs** radio button under the **Logging to Secure Firewall Management Center** setting in the threat defense platform settings (**Devices** > **Platform Settings** > **Syslog** > **Logging Setup**).

See Syslog for details on enabling VPN logging, configuring syslog servers, and viewing the system logs.

Procedure

Step 1 Choose **Devices** > **VPN** > **Troubleshooting**.

Step 2 You have the following options:

- Search—To filter current message information, click **Edit Search**.
- View—To view VPN details associated with the selected message in the view, click **View**.
- View All—To view VPN details for all messages in the view, click **View All**.

- Delete—To delete selected messages from the database, click **Delete** or click **Delete All** to delete all the messages.

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

Because debugging output is assigned high priority in the CPU process, it can render the system unusable. For this reason, use **debug** commands only to troubleshoot specific problems or during troubleshooting sessions with the Cisco Technical Assistance Center (TAC). Moreover, it is best to use **debug** commands during periods of lower network traffic and fewer users. Debugging during these periods decreases the likelihood that increased **debug** command processing overhead will affect system use.

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 regular Firepower Threat Defense CLI using the **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

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

aaa	Enables debugging for AAA. Use ? to see the available subfeatures.
accounting	(Optional) Enables AAA accounting debugging.
authentication	(Optional) Enables AAA authentication debugging.
authorization	(Optional) Enables AAA authorization debugging.

common	(Optional) Specifies the AAA common debug level. Use ? to see the available levels.
internal	(Optional) Enables AAA internal debugging.
shim	(Optional) Specifies the AAA shim debug level. Use ? to see the available levels.
url-redirect	(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.
undebug 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

crypto	Enables debugging for *crypto*. Use ? to see the available subfeatures.
ca	(Optional) Specifies the PKI debug levels. Use ? to see the available subfeatures.
condition	(Optional) Specifies the IPsec/ISAKMP debug filters. Use ? to see the available filters.
engine	(Optional) Specifies the crypto engine debug levels. Use ? to see the available levels.
ike-common	(Optional) Specifies the IKE common debug levels. Use ? to see the available levels.
ikev1	(Optional) Specifies the IKE version 1 debug levels. Use ? to see the available levels.
ikev2	(Optional) Specifies the IKE version 2 debug levels. Use ? to see the available levels.
ipsec	(Optional) Specifies the IPsec debug levels. Use ? to see the available levels.
condition	(Optional) Specifies the Crypto Secure Socket API debug levels. Use ? to see the available levels.
vpnclient	(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

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

ikev1	Enables debugging for *ikev1*. Use ? to see the available subfeatures.
timers	(Optional) Enables debugging for IKEv1 timers.
1-255	(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

ikev2	Enables debugging *ikev2*. Use ? to see the available subfeatures.
ha	(Optional) Specifies the IKEv2 HA debug level. Use ? to see the available levels.
platform	(Optional) Specifies the IKEv2 platform debug level. Use ? to see the available levels.
protocol	(Optional) Specifies the IKEv2 protocol debug level. Use ? to see the available levels.
timers	(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		
	ipsec	Enables debugging for *ipsec*. Use ? to see the available subfeatures.
	1-255	(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		
	ldap	Enables debugging for LDAP. Use ? to see the available subfeatures.
	1-255	(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		
	ssl	Enables debugging for SSL. Use ? to see the available subfeatures.
	cipher	(Optional) Specifies the SSL cipher debug level. Use ? to see the available levels.
	device	(Optional) Specifies the SSL device 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 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

webvpn	Enables debugging for WebVPN. Use ? to see the available subfeatures.
anyconnect	(Optional) Specifies the WebVPN Secure Client debug level. Use ? to see the available levels.
chunk	(Optional) Specifies the WebVPN chunk debug level. Use ? to see the available levels.
cifs	(Optional) Specifies the WebVPN CIFS debug level. Use ? to see the available levels.
citrix	(Optional) Specifies the WebVPN Citrix debug level. Use ? to see the available levels.
compression	(Optional) Specifies the WebVPN compression debug level. Use ? to see the available levels.
condition	(Optional) Specifies the WebVPN filter conditions debug level. Use ? to see the available levels.
cstp-auth	(Optional) Specifies the WebVPN CSTP authentication debug level. Use ? to see the available levels.
customization	(Optional) Specifies the WebVPN customization debug level. Use ? to see the available levels.
failover	(Optional) Specifies the WebVPN failover debug level. Use ? to see the available levels.
html	(Optional) Specifies the WebVPN HTML debug level. Use ? to see the available levels.
javascript	(Optional) Specifies the WebVPN Javascript debug level. Use ? to see the available levels.
kcd	(Optional) Specifies the WebVPN KCD debug level. Use ? to see the available levels.

listener	(Optional) Specifies the WebVPN listener debug level. Use ? to see the available levels.
mus	(Optional) Specifies the WebVPN MUS debug level. Use ? to see the available levels.
nfs	(Optional) Specifies the WebVPN NFS debug level. Use ? to see the available levels.
request	(Optional) Specifies the WebVPN request debug level. Use ? to see the available levels.
response	(Optional) Specifies the WebVPN response debug level. Use ? to see the available levels.
saml	(Optional) Specifies the WebVPN SAML debug level. Use ? to see the available levels.
session	(Optional) Specifies the WebVPN session debug level. Use ? to see the available levels.
task	(Optional) Specifies the WebVPN task debug level. Use ? to see the available levels.
transformation	(Optional) Specifies the WebVPN transformation debug level. Use ? to see the available levels.
url	(Optional) Specifies the WebVPN URL debug level. Use ? to see the available levels.
util	(Optional) Specifies the WebVPN utility debug level. Use ? to see the available levels.
xml	(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**.