



Verify and Monitor Cisco Catalyst SD-WAN Remote Access

- [Verify and Monitor SD-WAN Remote Access, on page 1](#)
- [Monitor Cisco Catalyst SD-WAN Remote Access Devices, on page 3](#)

Verify and Monitor SD-WAN Remote Access

On the Cisco IOS XE Catalyst SD-WAN device hosting the SD-WAN RA headend, use the following commands to verify that the remote access headend is configured and functioning.

Verification requires at least one remote user to be connected.

Client Connections in SD-WAN RA IPsec Mode

Use the **show crypto session** command and view the details in the “Interface: Virtual-Access” blocks in the command output. Each of these blocks corresponds to a connected client, and shows the IP address of the client and the details of the connection.

```
Device# show crypto session
...
Interface: Virtual-Access1
Profile: IKEV2_PROFILE
Session status: UP-ACTIVE
Peer: 10.0.12.40 port 500
  Session ID: 2
  IKEv2 SA: local 10.0.31.31/500 remote 10.0.12.40/500 Active
  IPSEC FLOW: permit ip 0.0.0.0/0.0.0.0 0.0.0.0/0.0.0.0
  Active SAs: 2, origin: crypto map
```

IKEv2 Sessions in SD-WAN RA IPsec Mode

Use the **show crypto ikev2 sa detailed** command to view the details of the IKEv2 session. For each connected client, the command output includes a block similar to the one in the following example. In the output, verify that the status is READY.

```
Device# show crypto ikev2 sa detailed
IPv4 Crypto IKEv2 SA

Tunnel-id Local Remote fvrf/ivrf Status
3 10.100.0.1/500 10.200.0.1/500 none/10 READY
Encr: AES-CBC, keysize: 256, PRF: SHA256, Hash: SHA256, DH Grp:19, Auth sign: RSA,
```

```

Auth verify: RSA
Life/Active Time: 86400/82405 sec
CE id: 0, Session-id: 3
Status Description: Negotiation done
Local spi: 0123456789ABCDEF      Remote spi: ABCDEF0123456789
Local id: example1@example.com
Remote id: example2@example.com
Local req msg id: 0                Remote req msg id: 50
Local next msg id: 0              Remote next msg id: 50
Local req queued: 0              Remote req queued: 50
Local window: 5                  Remote window: 5
DPD configured for 0 seconds, retry 0
Fragmentation not configured.
Dynamic Route Update: enabled
Extended Authentication not configured.
NAT-T is not detected
Cisco Trust Security SGT is disabled
Assigned host addr: 192.168.100.1
Initiator of SA : No

```

Client Connections in SD-WAN RA SSL (TLS) mode

Use the **show crypto ssl session** command to view the details of the clients connected.

```
Device# show crypto ssl session
```

```

SSL profile name: sslvpn_sdra_profile
Client_Login_Name  Client_IP_Address  No_of_Connections  Created  Last_Used
myssl              170.1.1.100        1                  11:29:49 11:29:49

```

```
Device# show crypto ssl session user myssl
```

```

Interface          : Virtual-Access1
Session Type       : Full Tunnel
Client User-Agent  : AnyConnect Windows 4.9.06037
Username           : myssl                      Num Connection : 1
Public IP          : 170.1.1.100
Profile            : sslvpn_sdra_profile
Policy             : sdra_sslvpn_policy
Last-Used          : 11:29:59                Created        : 23:35:52.695 UTC Sun Jul 16 2023
Tunnel IP          : 172.16.224.6                Netmask        : 0.0.0.0
Rx IP Packets      : 0                          Tx IP Packets  : 0

```

Route Information

Use the **show ip route vrf vrf** command to view route information. Specify the VRF assigned to a client. The command output shows information regarding the routes used in the VRF. Lines containing "Virtual-Access1" or similar indicate that a client is connected.

```
Device# show ip route vrf 10
```

```

Routing Table: 10
Codes: L - local, C - connected, S - static, R - RIP, M - mobile, B - BGP
D - EIGRP, EX - EIGRP external, O - OSPF, IA - OSPF inter area
N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
E1 - OSPF external type 1, E2 - OSPF external type 2, m - OMP
n - NAT, Ni - NAT inside, No - NAT outside, Nd - NAT DIA
i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1, L2 - IS-IS level-2
ia - IS-IS inter area, * - candidate default, U - per-user static route
H - NHRP, G - NHRP registered, g - NHRP registration summary
o - ODR, P - periodic downloaded static route, l - LISP
a - application route
+ - replicated route, % - next hop override, p - overrides from PFR
& - replicated local route overrides by connected

```

```
Gateway of last resort is not set

      10.0.0.0/8 is variably subnetted, 3 subnets, 2 masks
C       10.1.1.0/24 is directly connected, Loopback2
L       10.1.1.2/32 is directly connected, Loopback2
S       10.1.1.21/32 is directly connected, Virtual-Access1
      10.100.0.0/8 is variably subnetted, 4 subnets, 2 masks
m       10.100.7.0/24 [251/0] via 172.16.255.70, 2d23h, Sdwan-system-intf
m       10.100.17.0/24 [251/0] via 172.16.255.30, 02:29:17, Sdwan-system-intf
C       10.100.27.0/24 is directly connected, GigabitEthernet5
L       10.100.27.1/32 is directly connected, GigabitEthernet5
```

Monitor Cisco Catalyst SD-WAN Remote Access Devices

Minimum supported releases: Cisco IOS XE Catalyst SD-WAN Release 17.14.1a, Cisco Catalyst SD-WAN Manager Release 20.14.1

Cisco SD-WAN Manager can monitor devices in the overlay operating as remote access headends. To set up monitoring, add the following dashlets in the **Overview** dashboard:

- **Remote Access Headends:** Shows the total number of remote access headends in the network, organized by mode.
- **Remote Access Sessions:** Shows the number of remote access sessions in the network, categorized by client type. Also, lists the remote access headend devices that have the most remote access sessions (only top five devices are listed).

View Remote Access Session Information for Devices

To view remote access session details for each remote access headend, click **View Details** on the **Remote Access Headends** dashlet or **Remote Access Sessions** dashlet.

In the devices table, the following columns provide information about remote access sessions:

- **RA Session:** Total number of remote access sessions in the network.
- **RA Session Breakdown:** Type of remote access session or client.

