

Virtual Private Network

Troubleshooting

Issue 01
Date 2026-04-23



Copyright © Huawei Technologies Co., Ltd. 2026. All rights reserved.

No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Technologies Co., Ltd.

Trademarks and Permissions



HUAWEI and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.

All other trademarks and trade names mentioned in this document are the property of their respective holders.

Notice

The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.

The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied.

Security Declaration

Vulnerability

Huawei's regulations on product vulnerability management are subject to the *Vul. Response Process*. For details about this process, visit the following web page:

<https://www.huawei.com/en/psirt/vul-response-process>

For vulnerability information, enterprise customers can visit the following web page:

<https://securitybulletin.huawei.com/enterprise/en/security-advisory>

1 The State of a VPN Connection Is Not connected

Symptom

On the **Enterprise – VPN Connections** page of the VPN console, the state of a VPN connection is displayed as **Not connected**.

Possible Causes

- The configurations at the two ends of the VPN connection are incorrect.
- The security group configuration on the Huawei Cloud management console or the ACL configuration on the customer gateway device is incorrect.
- The IPsec VPN connection negotiation fails or the connection is disconnected.

Procedure

1. Reset VPN connections.
If the problem persists, go to **2**.
2. Check the configurations at the two ends of the VPN connections.
 - a. Check whether the gateway IP addresses configured at the two ends of the VPN connection are reversed.
 - i. To check the active and standby EIPs of the VPN gateway, choose **Virtual Private Network > Enterprise – VPN Gateways** and view the IP addresses in the **Gateway IP Address** column.
 - ii. To check the IP address of the customer gateway, choose **Virtual Private Network > Enterprise – Customer Gateways** and view the IP address in the **Identifier** column.
 - If the gateway IP addresses at both ends are not reversed, modify the corresponding settings.
 - If the gateway IP addresses at both ends are reversed, go to **b**.
 - b. Check whether the IKE and IPsec policies at both ends are consistent. Choose **Virtual Private Network > Enterprise – VPN Connections**, locate the target VPN connection, and choose **More > Modify Policy Settings**. View the IKE and IPsec policy settings.

If the negotiation parameters in the IKE or IPsec policy at both ends are inconsistent, modify the corresponding policy.

If the negotiation parameters in the IKE and IPsec policies at both ends are consistent, go to **c**.

- c. Check whether the PSKs at both ends are the same.

The PSK cannot be checked on the VPN console. If you are not sure whether the PSK configured on the VPN console is correct, you are advised to change it to be the same as that configured on the customer gateway device.

To change the PSK on the VPN console, choose **Virtual Private Network > Enterprise – VPN Connections**, locate the target VPN connection, and choose **More > Reset PSK**.

- d. If the policy-based mode is used, check whether the source and destination CIDR blocks in the policy rules at the two ends of the VPN connection are reversed.

To check policy rules on the VPN console, choose **Virtual Private Network > Enterprise – VPN Connections**, locate the target VPN connection, and click **Modify VPN Connection**.

- e. If the static routing mode is used and the NQA function is enabled on the VPN console, check whether tunnel interface IP addresses are correctly configured on the customer gateway device.

- To check whether NQA is enabled on the VPN console, choose **Virtual Private Network > Enterprise – VPN Connections**, click the name of the target VPN connection, and view the value of **Link Detection** on the **Summary** tab page.

- To check the tunnel interface IP addresses configured on the VPN console, choose **Virtual Private Network > Enterprise – VPN Connections**, click **Modify VPN Connection**, and view the values of **Local Interface IP Address** and **Customer Interface IP Address**.

The local and remote interface IP addresses configured on the customer gateway device must be the same as the values of **Customer Interface IP Address** and **Local Interface IP Address** configured on the VPN console, respectively.

- f. If the BGP routing mode is used, check whether the BGP ASNs at the two ends of the VPN connection are reversed.

- To check the BGP ASN of the VPN gateway, choose **Virtual Private Network > Enterprise – VPN Gateways**, click the VPN gateway name, and view the BGP ASN in the **Basic Information** area.

- To check the BGP ASN of the customer gateway, choose **Virtual Private Network > Enterprise – Customer Gateways** and view the value in the **BGP ASN** column.

3. Check the security group configuration on the Huawei Cloud management console and the ACL configuration on the customer gateway device.

- a. Check whether the default security group on the Huawei Cloud management console permits the ports corresponding to the public IP addresses of the customer gateway.



- b. To check the default security group on the Huawei Cloud management console, perform the following steps:
 - i. Choose **Virtual Private Network > Enterprise – VPN Gateways**, and click the name of the VPC associated with the VPN gateway.
 - ii. On the **Virtual Private Cloud** page, click the number in the **Route Tables** column.
 - iii. On the **Route Tables** page, click the name of the route table.
 - iv. Locate and click the next hop of the active or standby EIP of the VPN gateway.
 - v. On the **Associated Security Groups** tab page, check whether the security group permits traffic of the ports.
 - c. Verify that an ACL on the customer gateway device permits the ports corresponding to the active and standby EIPs of the VPN gateway.
4. Check IPsec connection logs.
- a. Log in to the management console.
 - b. Click  in the upper left corner and select the desired region and project.
 - c. Click  in the upper left corner, and choose **Networking > Virtual Private Network**.
 - d. In the navigation pane on the left, choose **Virtual Private Network > Enterprise – VPN Connections**.
 - e. On the **VPN Connection** page, locate the target VPN connection, and click **View Logs** to view connection logs.
- Check IPsec connection logs, and locate the fault based on the log keywords and error codes listed in [Table 1-1](#).

Table 1-1 Common causes of VPN disconnection

Category	No.	Error Message	Description	Handling Procedure
IPsec VPN negotiation failure	1	phase1 proposal mismatch	IKE proposal parameters on both ends do not match. This message is available only on the initiator of the tunnel.	Check IKE proposal parameters at both ends of the tunnel, and ensure that the parameters are consistent at both ends.

Category	No.	Error Message	Description	Handling Procedure
	2	phase1 proposal encryption algorithm mismatch	The encryption algorithms in IKE proposals at both ends do not match. This message is available only on the responder of the tunnel.	
	3	phase1 proposal authentication method mismatch	The authentication methods in IKE proposals at both ends do not match. This message is available only on the responder of the tunnel.	
	4	phase1 proposal authentication algorithm mismatch	The authentication algorithms in IKE proposals at both ends do not match. This message is available only on the responder of the tunnel.	
	5	phase1 proposal dh mismatch	The DH groups in IKE proposals at both ends do not match. This message is available only on the responder of the tunnel.	
	6	phase1 proposal integrity algorithm mismatch	The integrity algorithms in IKE proposals at both ends do not match. This message is available only on the responder of the tunnel.	

Category	No.	Error Message	Description	Handling Procedure
	7	phase1 proposal prf mismatch	The PRF algorithms in IKE proposals at both ends do not match. This message is available only on the responder of the tunnel.	
	8	phase2 proposal or pfs mismatch	IPsec proposal parameters, PFS algorithms, or security ACLs on both ends do not match.	Check IPsec proposal parameters or PFS algorithms at both ends of the tunnel, and ensure that the parameters or algorithms are consistent at both ends.
	9	responder dh mismatch	The DH algorithm of the responder does not match that of the initiator.	Check DH algorithms at both ends of the tunnel, and ensure that the algorithms are consistent at both ends.
	10	initiator dh mismatch	The DH algorithm of the initiator does not match that of the responder.	
	11	encapsulation mode mismatch	Encapsulation modes on both ends do not match.	Contact technical support.
	12	flow mismatch	Security ACLs on both sides do not match.	Contact technical support.
	13	version mismatch	IKE versions on both ends do not match.	Contact technical support.
	14	peer address mismatch	IKE peer addresses on both ends do not match.	Check the IP addresses of IKE peers at both ends, and ensure that the IP addresses match each other.

Category	No.	Error Message	Description	Handling Procedure
	15	config ID mismatch	No IKE peer with the specified ID is found.	Contact technical support.
	16	exchange mode mismatch	Negotiation modes on both ends do not match.	Check the IKE negotiation modes at both ends, and ensure that the negotiation modes are consistent at both ends.
	17	authentication fail	The identity authentication fails.	Check IKE proposal parameters or IKE peer parameters at both ends of the tunnel, and ensure that the parameters are consistent at both ends.
	18	construct local ID fail	A local ID fails to be constructed.	Contact technical support.
	19	rekey no find old sa	The old SA fails to be found during renegotiation.	Contact technical support.
	20	rekey fail	The old SA is going offline during renegotiation.	Contact technical support.
	21	first packet limited	First packets are rate limited.	Contact technical support.
	22	unsupported version	The IKE version is not supported.	Contact technical support.
	23	malformed message	There is a malformed message.	Contact technical support.
	24	malformed payload	There is a malformed payload.	Contact technical support.

Category	No.	Error Message	Description	Handling Procedure
	25	malformed payload or psk mismatch	There are malformed payloads or the pre-shared keys at both ends are inconsistent.	Contact technical support.
	26	critical drop	The critical payload is not recognized.	Contact technical support.
	27	cookie mismatch	The cookies do not match.	Contact technical support.
	28	invalid cookie	The cookie is invalid.	Contact technical support.
	29	invalid length	The packet length is invalid.	Contact technical support.
	30	unknown exchange type	The negotiation mode is unknown.	Contact technical support.
	31	short packet	Packets are ultra-short.	Contact technical support.
	32	uncritical drop	The non-critical payload is not identified.	Contact technical support.
	33	route limit	The number of imported routes reaches the upper limit.	Replace the device with a device with higher route injection specifications, and properly plan the network.
	34	ip assigned fail	IP address assignment fails.	Ensure that the AAA and IPsec configurations, such as the IP address pools, AAA service schemes, and IP addresses assigned to IKE users, are correct.

Category	No.	Error Message	Description	Handling Procedure
	35	eap authentication timeout	EAP authentication times out.	Ensure that the client's user name and password as well as the user access configuration are correct.
	36	eap authentication fail	EAP authentication fails.	
	37	xauth authentication fail	XAUTH authentication fails.	
	38	xauth authentication timeout	XAUTH authentication times out.	
	39	license or specification limited	There is license control.	Contact technical support.
	40	local address mismatch	The local IP address and interface IP address in IKE negotiation do not match.	Check the local IP address and interface IP address used for IKE negotiation, and ensure that the addresses are consistent at both ends.
	41	dynamic peers number reaches limitation	The number of IKE peers reaches the upper limit.	Contact technical support.
	42	ipsec tunnel number reaches limitation	The number of IPsec tunnels reaches the upper limit.	Contact technical support.
	43	netmask mismatch	The mask does not match the configured one after the IPsec mask filtering function is enabled.	Contact technical support.
	44	flow conflict	A data flow conflict exists.	Contact technical support.

Category	No.	Error Message	Description	Handling Procedure
	45	proposal mismatch or use sm in ikev2	IPsec proposals on both ends do not match or IKEv2 uses an SM algorithm.	Check the algorithms used by IKEv2 in the IPsec proposals at both ends of the tunnel, and ensure that the algorithms are consistent at both ends.
	46	ikev2 not support sm in ipsec proposal ikev2	IKEv2 does not support the SM algorithm used in the IPsec proposal.	
	47	no policy applied on interface	No policy is applied to an interface.	Contact technical support.
	48	nat detection fail	NAT detection fails.	Contact technical support.
	49	fragment packet limit	The number of fragments exceeds the upper limit.	Contact technical support.
	50	fragment packet reassemble timeout	Fragment reassembly times out.	Ensure that the links at both ends are normal and the device status is normal.
	51	peer cert is expired	The peer certificate has expired.	Contact technical support.
	52	peer cert is revoked by CRL	The peer certificate is revoked.	Contact technical support.
	53	sa with same user exists	The SA is the same as that of another user.	Contact technical support.
	54	max transmit reached	The number of retransmitted packets reaches the maximum.	Contact technical support.

Category	No.	Error Message	Description	Handling Procedure
IPsec VPN connection disconnection	1	dpd timeout	DPD detection times out.	Perform a ping operation to check link reachability. If the link is unreachable, verify the link and network configuration.
	2	peer request	The peer device sends a message, asking the local device to tear down a tunnel.	Check log information of the peer end, and locate the cause of the IPsec tunnel fault.
	3	config modify or manual offline	The SA is automatically deleted due to configuration modification, or is manually deleted.	<ol style="list-style-type: none">1. Check whether an SA is reset manually. If so, no further action is required.2. Check whether the IPsec configuration modified on the local end is correct. If not, correct the IPsec configuration.3. Check whether the manual deletion of IPsec policies is appropriate. If not, reapply the IPsec policies to the interface.
	4	phase1 hard expiry	In phase 1, hard timeout (no new SA negotiation succeeds) occurs.	Check whether the IKE SA lifetime is proper. If not, modify the IKE SA lifetime.
	5	phase2 hard expiry	A hard timeout occurs in phase 2.	Check whether the IPsec SA lifetime is proper. If not, modify the IPsec SA lifetime.

Category	No.	Error Message	Description	Handling Procedure
	6	heartbeat timeout	Heartbeat detection times out.	Contact technical support.
	7	re-auth timeout	The SA is deleted because the re-authentication times out.	No action is required.
	8	aaa cut user	The SA is deleted because the AAA module logs out the user.	No action is required.
	9	ip address syn failed	IP addresses fail to be synchronized.	Ensure that the link is normal and the IPsec configurations are correct.
	10	hard expiry triggered by port mismatch	Hard timeout occurs due to a NAT port number mismatch.	Contact technical support.
	11	kick old sa with same flow	The old SA is deleted when the same flow is transmitted.	Contact technical support.
	12	cpu table updated	When an SPU is removed and inserted, the SAs of CPUs other than the one on the SPU are deleted.	No action is required.
	13	flow overlap	The IP address in the encrypted data flow conflicts with the peer IP address.	Check the security ACL configurations at both ends, and modify the conflicting ACL rules for traffic flows.
	14	spi conflict	An SPI conflict occurs.	No action is required.
	15	admin down	The VPN tunnel status is admin down.	Contact technical support.

Category	No.	Error Message	Description	Handling Procedure
	16	peer address switch	The peer address is changed.	Contact technical support.
	17	forward down	The fwd group goes down.	Contact technical support.
	18	sa with same user exists	The SA is the same as that of another user.	Contact technical support.
	19	reset sa by ike user	A user resets the SA.	Contact technical support.
	20	phase1 sa replace	A new IKE SA replaces the old one.	No action is required.
	21	phase2 sa replace	A new IPsec SA replaces the old one.	No action is required.
	22	manual offline	The connection is manually torn down.	Contact technical support.
	23	nhrp notify	The NHRP module notifies the device of SA deletion.	No action is required.
	24	receive backup delete info	The standby device receives an SA backup deletion message from the active device.	No action is required.
	25	eap delete old sa	When the peer device performs EAP authentication repeatedly, the local device deletes the old SA.	No action is required.
	26	receive invalid spi notify	The device receives an invalid SPI notification.	If the notification is frequently received, check whether the status and configurations of the peer device are abnormal.

Category	No.	Error Message	Description	Handling Procedure
	27	dns resolution status change	The DNS resolution status is changed.	<ol style="list-style-type: none">1. Ensure that the DNS server is working properly.2. Ensure that the configured domain name is correct. If the fault persists, contact technical support.
	28	ikev1 phase1-phase2 sa dependent offline	The device deletes the associated IPsec SA when deleting an IKEv1 SA.	Contact technical support.
	29	exchange timeout	Packet exchange times out.	Ensure that the link is normal and the IPsec configurations are correct.
	30	hash gene adjusted	The hash factor is adjusted, causing the IPsec tunnel to be deleted.	Contact technical support.
	31	ipsec tunnel recover	The tunnel is automatically recovered and re-established through a self-healing mechanism.	No action is required.
	32	hash except	The IPsec tunnel is deleted because the hash algorithm is adjusted.	Contact technical support.

If the fault persists after you verify the preceding configurations, contact Huawei engineers by [submitting a service ticket](#).

2 Ping Tests Between Cloud and On-premises Networks Fail

Symptom

- Servers in an on-premises data center cannot ping ECSs in a Huawei Cloud VPC.
- ECSs in a Huawei Cloud VPC cannot ping the servers in an on-premises data center.

Possible Causes

- The security group configuration on the Huawei Cloud management console is incorrect.
- The ACL rule associated with the interconnection subnet is incorrectly configured.
- The ACL configuration on the customer gateway device is incorrect.
- The route configuration on the customer gateway device is incorrect.

Procedure

1. Reset VPN connections.
If the problem persists, go to [2](#).
2. Check the security group configuration on the Huawei Cloud management console.
 - a. Verify that the default security group on the Huawei Cloud management console permits data flows destined for the customer subnet.
 - b. To check the default security group on the Huawei Cloud management console, perform the following steps:
 - i. Choose **Virtual Private Network > Enterprise – VPN Gateways**, and click the name of the VPC associated with the VPN gateway.
 - ii. Click the number of route tables corresponding to the VPC.
 - iii. On the **Route Tables** page, click the name of the route table.
 - iv. Locate and click the next hop of the active or standby EIP of the VPN gateway.

- v. On the **Associated Security Groups** tab page, check the ports permitted by the security group.
 - c. Verify that the default security group on the Huawei Cloud management console permits data flows originated from the customer subnet.
 - d. Verify that the default security group on the Huawei Cloud management console permits data flows destined for the local subnet.
 - e. Verify that the default security group on the Huawei Cloud management console permits data flows originated from the local subnet.
 - f. Verify that a security group permits data flows from the ECSs on Huawei Cloud to the customer subnet.
 - g. To check whether such a security group has been configured, choose **Compute > Elastic Cloud Server**, click an ECS name, click the **Security Groups** tab, and click **Manage Rule**.
 - h. Verify that a security group permits data flows from the customer subnet to the ECSs on Huawei Cloud.
3. The ACL rule associated with the interconnection subnet is incorrectly configured.
 - a. Check whether the ACL rule associated with the interconnection subnet permits the ports between all local and customer subnets.
 - i. Choose **Virtual Private Network > Enterprise – VPN Gateways**, and click the name of target VPN gateway.
 - ii. In the **Basic Information** area, check and record the interconnection subnet.
 - iii. In the **Basic Information** area, click the name of the associated VPC.
 - iv. On the **Summary** tab page of the VPC, click the number of subnets in the **Networking Components** area.
 - v. Find the interconnection subnet in the subnet list, and click the ACL name in the **Network ACL** column.
 - vi. Permit the ports between all local and customer subnets.
4. Check the ACL configuration on the customer gateway device.
 - a. Verify that an ACL rule on the customer gateway device permits data flows destined for the local subnet of the Huawei Cloud VPN gateway.
 - b. Verify that an ACL rule on the customer gateway device permits data flows originated from the local subnet of the Huawei Cloud VPN gateway.
5. To check the local subnet of the Huawei Cloud VPN gateway, choose **Virtual Private Network > Enterprise – VPN Gateways**, click the VPN gateway name, and view the value of **Local Subnet** in the **Basic Information** area.
6. Check the route configuration on the customer gateway device.
 - a. Verify that the public network route is correctly configured. That is, the destination address is an EIP of the Huawei Cloud VPN gateway, and the next hop is the egress interface address of the customer gateway device.
 - b. Verify that the private network route is correctly configured. That is, the destination address is the local subnet of the Huawei Cloud VPN gateway, and the next hop is the egress interface address of the customer gateway device.


- c. To check the local subnet of the Huawei Cloud VPN gateway, choose **Virtual Private Network > Enterprise - VPN Gateways**, click the VPN gateway name, and view the value of **Local Subnet** in the **Basic Information** area.

3 Packet Loss Occurs

Symptom

- Packet loss occurs when a server in an on-premises data center pings an ECS in a Huawei Cloud VPC.
- Packet loss occurs when an ECS in a Huawei Cloud VPC pings a server in an on-premises data center.

Procedure

- Check the customer-side networking and bandwidth.
 - Check whether the customer network has multiple egresses working in load balancing mode and whether traffic destined for Huawei Cloud is distributed to a non-VPN egress. Ensure that the traffic destined for Huawei Cloud is transmitted through the same egress.
 - Ping the IP address of the VPN gateway on Huawei Cloud and other public IP addresses (for example, 114.114.114.114) from the customer gateway to check the delay and packet loss rate on the public network. If the quality of the public network is poor, you are advised to seek help from the corresponding carrier.
 - Check whether traffic on the customer gateway device exceeds the bandwidth limit.
- Check the Huawei Cloud-side networking and bandwidth.
 - Check whether traffic exceeds the bandwidth of the Huawei Cloud VPN gateway.
 - i. Check the bandwidth of active and standby EIPs of the VPN gateway as follows: Choose **Virtual Private Network > Enterprise – VPN Gateways**, click the VPN gateway name, and check the value of **Bandwidth (Mbit/s)** in the **EIP** area.
 - ii. Check the actual bandwidth usage of the VPN gateway as follows: Choose **Virtual Private Network > Enterprise – VPN Gateways**, and click  corresponding to the active and standby EIPs in the **Gateway IP Address** column of the VPN gateway.

If traffic exceeds the bandwidth of the VPN gateway, increase the bandwidth.

- If the fault persists after you verify the preceding configurations, contact Huawei engineers by [submitting a service ticket](#).

4 Client Connection Failures

4.1 The Client Log Contains "Connection failed to establish within given time"

Applicable Client

Windows OpenVPN Connect

Symptom



A client cannot connect to a P2C VPN gateway, and the log contains the following error information:

Connection failed to establish within given time

Possible Causes

- The client device cannot access the Internet.
- After the server configuration is modified, the client configuration file is not downloaded again. As a result, the client configuration file in use is inconsistent with that on the **Server** tab page of the VPN gateway.

Procedure

1. On the client device, try to access other Internet services.
 - If the access also fails, contact your carrier to rectify the network connectivity fault.
 - If the access is successful, go to step 2.
2. Log in to the management console.
3. Click  in the upper left corner and select the desired region and project.
4. Click  in the upper left corner, and choose **Networking > Virtual Private Network**.
5. In the navigation pane on the left, choose **Virtual Private Network > Enterprise – VPN Gateways**.

6. Click the **P2C VPN Gateways** tab, locate the target VPN gateway, and click **View Server** in the **Operation** column.
7. On the **Server** tab page, view the server ID in the **Basic Information** area, and view the server port and protocol in the **Advanced Settings** area.
8. Check the **proto** and **remote** parameters in the client configuration file. An example is as follows:

```
...  
proto tcp # Protocol type  
remote XXX.XX.XX.XX XXX # Public IP address and port number of the server  
...
```

If the parameter settings in the client configuration file are inconsistent with the actual configuration of the server, use either of the following methods to rectify the fault:

- Method 1: Modify the server information.
 - i. On the **Server** tab page, modify the corresponding information.
 - ii. Download the new client configuration file.
The downloaded client configuration file is **client_config.zip**.
 - iii. Decompress **client_config.zip** to a specified directory, for example, **D:**.
After the decompression, the **client_config.ovpn** and **client_config.conf** files are generated.
 - iv. Open the **client_config.ovpn** file using Notepad or Notepad++.
 - v. Add the client certificate and private key to the file.
Enter the client certificate content and the corresponding private key in between `<cert></cert>` and `<key></key>` tags, respectively.

```
<cert>  
-----BEGIN CERTIFICATE-----  
Client certificate content  
-----END CERTIFICATE-----  
</cert>  
  
<key>  
-----BEGIN PRIVATE KEY-----  
Client private key  
-----END PRIVATE KEY-----  
</key>
```
 - vi. Save the .ovpn configuration file.
 - Method 2: Modify the client configuration file.
 - i. Open the **client_config.ovpn** file using Notepad or Notepad++.
 - ii. Modify the corresponding information in the client configuration file.
 - iii. Save the .ovpn configuration file.
9. Start the OpenVPN Connect client.
 10. Import the new client configuration file.
 11. Use the client to reconnect to the VPN gateway.
 12. Press **Win+R** and enter **cmd** to open the command window.
 - 13.

NOTE

XX.XX.XX.XX indicates the private IP address of the ECS to be connected. Replace it with the actual private IP address.

If information similar to the following is displayed, the client can communicate with the ECS:

```
64 bytes from XX.XX.XX.XX: icmp_seq=1 ttl=63 time=1.27 ms
64 bytes from XX.XX.XX.XX: icmp_seq=2 ttl=63 time=1.36 ms
64 bytes from XX.XX.XX.XX: icmp_seq=3 ttl=63 time=1.40 ms
64 bytes from XX.XX.XX.XX: icmp_seq=4 ttl=63 time=1.29 ms
64 bytes from XX.XX.XX.XX: icmp_seq=5 ttl=63 time=1.35 ms
64 bytes from XX.XX.XX.XX: icmp_seq=6 ttl=63 time=1.52 ms
```

4.2 The Client Log Contains "Cannot load CA certificate file [[INLINE]](no entries were read)"

Applicable Client

- Linux
- Windows OpenVPN GUI

Symptom

A client cannot connect to a P2C VPN gateway, and the log contains the following error information:

```
Cannot load CA certificate file [[INLINE]](no entries were read)
```

Possible Causes

There is no client certificate or private key in the client configuration file.

Procedure

1. Re-generate a client certificate and private key. For details, see [Using Easy-RSA to Issue Certificates \(Server and Client Sharing a CA Certificate\)](#). In this example, the generated client certificate and private key are **p2cclient.com.crt** and **p2cclient.com.key**, respectively.
2. Open the **client_config.ovpn**, **p2cclient.com.crt**, and **p2cclient.com.key** files using Notepad or Notepad++.
3. Copy the client certificate and private key to the **client_config.ovpn** file.

Enter the client certificate content and the corresponding private key in between `<cert></cert>` and `<key></key>` tags, respectively. An example is as follows:

```
<cert>
-----BEGIN CERTIFICATE-----
Client certificate content
-----END CERTIFICATE-----
</cert>

<key>
-----BEGIN PRIVATE KEY-----
Client private key
-----END PRIVATE KEY-----
</key>
```

4. Save the .ovpn configuration file.
5. Start the OpenVPN client.

6. Import the new client configuration file.
7. Use the client to reconnect to the VPN gateway.
8. On Windows, press **Win+R** and enter **cmd** to open the command window. On Linux, log in as the **root** user and open the command window.
- 9.

NOTE

XX.XX.XX.XX indicates the private IP address of the ECS to be connected. Replace it with the actual private IP address.

If information similar to the following is displayed, the client can communicate with the ECS:

```
64 bytes from XX.XX.XX.XX: icmp_seq=1 ttl=63 time=1.27 ms
64 bytes from XX.XX.XX.XX: icmp_seq=2 ttl=63 time=1.36 ms
64 bytes from XX.XX.XX.XX: icmp_seq=3 ttl=63 time=1.40 ms
64 bytes from XX.XX.XX.XX: icmp_seq=4 ttl=63 time=1.29 ms
64 bytes from XX.XX.XX.XX: icmp_seq=5 ttl=63 time=1.35 ms
64 bytes from XX.XX.XX.XX: icmp_seq=6 ttl=63 time=1.52 ms
```

NOTE

If you use a client on Linux, you need to upload the configuration file **client_config.conf** to the Linux system using Xftp. For details, see [Configuring a Client](#).

4.3 The Client Log Contains "error:068000A8:asn1 encoding routines:wrong tag"

Applicable Client

- Linux
- Windows OpenVPN GUI
- Windows OpenVPN Connect

Symptom

A client cannot connect to a P2C VPN gateway, and the log contains the following error information:

```
error:068000A8:asn1 encoding routines:wrong tag
```

Possible Causes

The client certificate and private key do not match.

Procedure

1. Open the **client_config.ovpn**, **p2cclient.com.crt**, and **p2cclient.com.key** files using Notepad or Notepad++.
In this example, **p2cclient.com.crt** is the client certificate, and **p2cclient.com.key** is the client private key.
2. Copy the client certificate and private key to the **client_config.ovpn** file.

Enter the client certificate content and the corresponding private key in between `<cert></cert>` and `<key></key>` tags, respectively. An example is as follows:

```
<cert>
-----BEGIN CERTIFICATE-----
Client certificate content
-----END CERTIFICATE-----
</cert>

<key>
-----BEGIN PRIVATE KEY-----
Client private key
-----END PRIVATE KEY-----
</key>
```

3. Save the .ovpn configuration file.
4. Start the OpenVPN client.
5. Import the new client configuration file.
6. Use the client to reconnect to the VPN gateway.
7. On Windows, press **Win+R** and enter **cmd** to open the command window. On Linux, log in as the **root** user and open the command window.
- 8.

NOTE

`XX.XX.XX.XX` indicates the private IP address of the ECS to be connected. Replace it with the actual private IP address.

If information similar to the following is displayed, the client can communicate with the ECS:

```
64 bytes from XX.XX.XX.XX: icmp_seq=1 ttl=63 time=1.27 ms
64 bytes from XX.XX.XX.XX: icmp_seq=2 ttl=63 time=1.36 ms
64 bytes from XX.XX.XX.XX: icmp_seq=3 ttl=63 time=1.40 ms
64 bytes from XX.XX.XX.XX: icmp_seq=4 ttl=63 time=1.29 ms
64 bytes from XX.XX.XX.XX: icmp_seq=5 ttl=63 time=1.35 ms
64 bytes from XX.XX.XX.XX: icmp_seq=6 ttl=63 time=1.52 ms
```

NOTE

If you use a client on Linux, you need to upload the configuration file **client_config.conf** to the Linux system using Xftp. For details, see [Configuring a Client](#).

4.4 The Client Log Contains "OpenSSL: error:0A000086:SSL routines::certificate verify failed"

Applicable Client

- Linux
- Windows OpenVPN GUI
- Windows OpenVPN Connect

Symptom

A client cannot connect to a P2C VPN gateway, and the log contains the following error information:

OpenSSL: error:0A000086:SSL routines::certificate verify failed

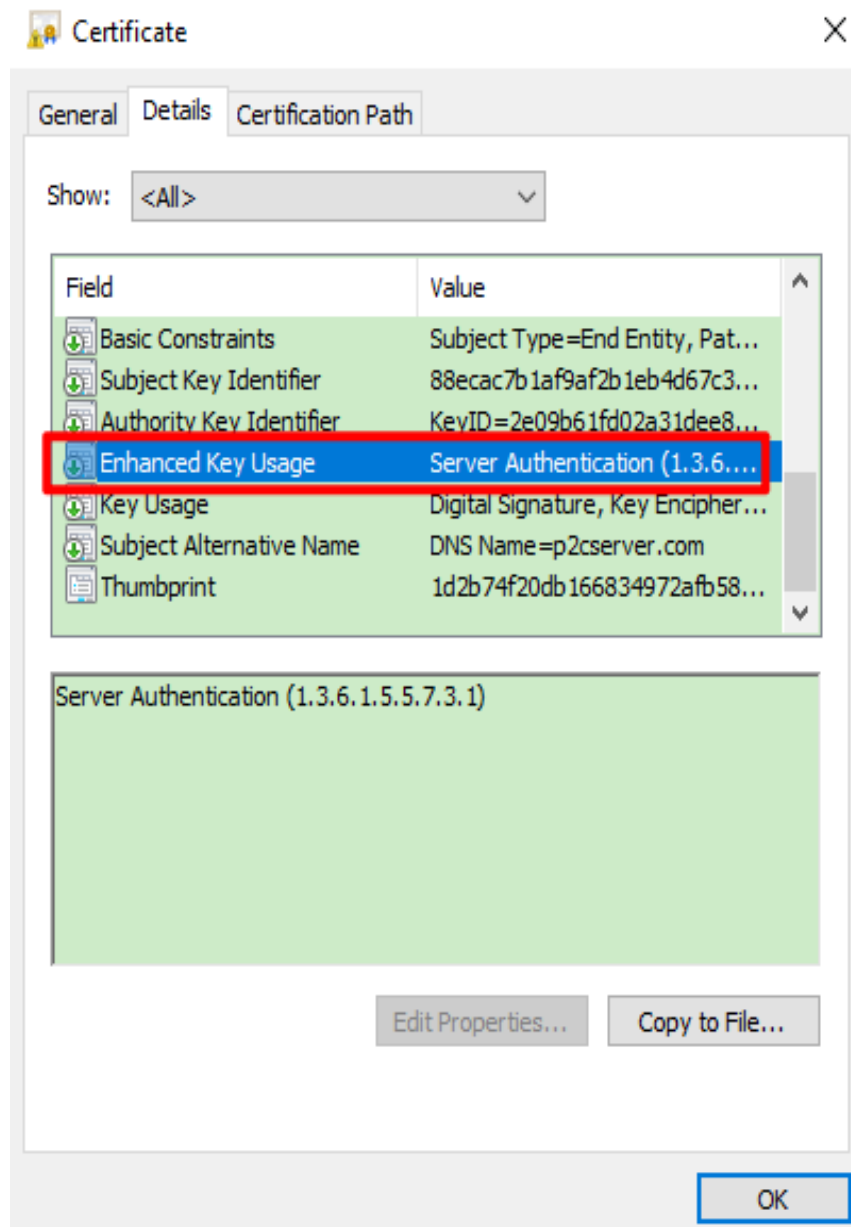
Possible Causes

The server certificate used by the VPN gateway does not contain the Server Authentication attribute. As a result, certificate verification fails.

Procedure

1. Double-click the target server certificate.
2. Click the **Details** tab, and check whether the certificate contains the Server Authentication attribute, as shown in [Figure 4-1](#).



Figure 4-1 Server certificate



If the certificate does not contain the Server Authentication attribute, re-generate a server certificate. For details, see [Using Easy-RSA to Issue Certificates \(Server and Client Sharing a CA Certificate\)](#).

A server certificate generated using OpenSSL does not contain the Server Authentication attribute. As such, you need to add **extendedKeyUsage = serverAuth** to the OpenSSL configuration file. The following is an example:

```
...
keyUsage = nonRepudiation, digitalSignature, keyEncipherment
extendedKeyUsage = serverAuth
...
```

3. Log in to the management console.
4. Click  in the upper left corner and select the desired region and project.
5. Click  in the upper left corner, and choose **Networking > Virtual Private Network**.
6. In the navigation pane on the left, choose **Virtual Private Network > Enterprise – VPN Gateways**.
7. Click the **P2C VPN Gateways** tab. In the P2C VPN gateway list, locate the target P2C VPN gateway, and click **View Server** in the **Operation** column.
8. On the **Server** tab page of the VPN gateway, click **Replace**.
9. In the displayed dialog box, click **Upload** in the drop-down list box.
Upload the new server certificate to CCM. For details, see [Using the CCM to Manage a Server Certificate](#).
10. Download the new client configuration file.
The downloaded client configuration file is **client_config.zip**.
11. Decompress **client_config.zip** to a specified directory, for example, **D:**.
After the decompression, the **client_config.ovpn** and **client_config.conf** files are generated.
12. Add the client certificate and private key to the file.
 - a. Open the **client_config.ovpn** file using Notepad or Notepad++.
 - b. Enter the client certificate content and the corresponding private key in between `<cert></cert>` and `<key></key>` tags, respectively.

```
<cert>
-----BEGIN CERTIFICATE-----
Client certificate content
-----END CERTIFICATE-----
</cert>

<key>
-----BEGIN PRIVATE KEY-----
Client private key
-----END PRIVATE KEY-----
</key>
```
 - c. Save the .ovpn configuration file.
13. Start the OpenVPN client.
14. Import the new client configuration file.
15. Use the client to reconnect to the VPN gateway.
16. On Windows, press **Win+R** and enter **cmd** to open the command window.
On Linux, log in as the **root** user and open the command window.

17.

 **NOTE**

XX.XX.XX.XX indicates the private IP address of the ECS to be connected. Replace it with the actual private IP address.

If information similar to the following is displayed, the client can communicate with the ECS:

```
64 bytes from XX.XX.XX.XX: icmp_seq=1 ttl=63 time=1.27 ms
64 bytes from XX.XX.XX.XX: icmp_seq=2 ttl=63 time=1.36 ms
64 bytes from XX.XX.XX.XX: icmp_seq=3 ttl=63 time=1.40 ms
64 bytes from XX.XX.XX.XX: icmp_seq=4 ttl=63 time=1.29 ms
64 bytes from XX.XX.XX.XX: icmp_seq=5 ttl=63 time=1.35 ms
64 bytes from XX.XX.XX.XX: icmp_seq=6 ttl=63 time=1.52 ms
```

 **NOTE**

If you use a client on Linux, you need to upload the configuration file `client_config.conf` to the Linux system using Xftp. For details, see [Configuring a Client](#).

If the problem persists, [submit a service ticket](#) to contact Huawei technical support.

4.5 The Client Log Contains "TLS Error: TLS handshake failed"

Applicable Client

- Linux
- Windows OpenVPN GUI

Symptom



A client cannot connect to a P2C VPN gateway, and the log contains the following error information:

```
TLS Error: TLS handshake failed
```

Possible Causes

The certificate and private key in the client configuration file do not match the client CA certificate imported on the **Server** tab page of the VPN gateway.

Procedure

1. Check whether the imported client CA certificate is correct.
 - a. Log in to the management console.
 - b. Click  in the upper left corner and select the desired region and project.
 - c. Click  in the upper left corner, and choose **Networking > Virtual Private Network**.
 - d. In the navigation pane on the left, choose **Virtual Private Network > Enterprise – VPN Gateways**.

- e. Click the **P2C VPN Gateways** tab. In the P2C VPN gateway list, locate the target P2C VPN gateway, and click **View Server** in the **Operation** column.
- f. On the **Server** tab page, view the issuer information of the client CA certificate.
- g. Double-click the target client CA certificate, click the **Details** tab, and view the issuer information.
 - If the issuer information on the client is consistent with that on the server, go to step 2.
 - If the issuer information on the client is inconsistent with that on the server, perform the following operations to import the client CA certificate again:
- i. On the **Server** tab page, choose **Certificate authentication** from the **Client Authentication Mode** drop-down list box, and click **Upload CA Certificate**.
- ii. Set parameters as prompted.

Table 4-1 Parameters for uploading a CA certificate

Parameter	Description	Example Value
Name	This parameter can be modified.	ca-cert-xxxx
Content	<p>Use a text editor (for example, Notepad++) to open the signature certificate file in PEM format, and copy the certificate content to this text box.</p> <p>NOTE</p> <ul style="list-style-type: none">It is recommended to use a certificate with a strong cryptographic algorithm, such as RSA-3072 or RSA-4096.Certificates using the RSA-2048 encryption algorithm have risks. Exercise caution when using such certificates.	<pre>-----BEGIN CERTIFICATE----- Certificate content -----END CERTIFICATE-----</pre>

- iii. Click **OK**.
- iv. Click **Delete** in the **Operation** column of the incorrect client CA certificate.
- v. In the **Delete CA Certificate** dialog box, click **OK**.
- h. Download the new client configuration file.

- i. The downloaded client configuration file is **client_config.zip**.
 - j. Decompress **client_config.zip** to a specified directory, for example, **D:**. After the decompression, the **client_config.ovpn** and **client_config.conf** files are generated.
 - k. Open the **client_config.ovpn** file using Notepad or Notepad++.
 - l. Add the client certificate and private key to the file.
Enter the client certificate content and the corresponding private key in between `<cert></cert>` and `<key></key>` tags, respectively.

```
<cert>
-----BEGIN CERTIFICATE-----
Client certificate content
-----END CERTIFICATE-----
</cert>

<key>
-----BEGIN PRIVATE KEY-----
Client private key
-----END PRIVATE KEY-----
</key>
```
 - m. Save the .ovpn configuration file.
 - n. Start the OpenVPN client.
 - o. Import the new client configuration file.
 - p. Use the client to reconnect to the VPN gateway.
2. Check whether the client certificate and private key in the configuration file match.

If the client CA certificate imported in step 1 is correct, the client certificate and private key in the configuration file do not match. In this case, copy the client certificate and private key to the client configuration file again.

- a. Open the **client_config.ovpn**, **p2client.com.crt**, and **p2client.com.key** files using Notepad or Notepad++. In this example, **p2client.com.crt** is the client certificate, and **p2client.com.key** is the client private key.
- b. Copy the client certificate and private key to the **client_config.ovpn** file.
Enter the client certificate content and the corresponding private key in between `<cert></cert>` and `<key></key>` tags, respectively. An example is as follows:

```
<cert>
-----BEGIN CERTIFICATE-----
Client certificate content
-----END CERTIFICATE-----
</cert>

<key>
-----BEGIN PRIVATE KEY-----
Client private key
-----END PRIVATE KEY-----
</key>
```

- c. Save the .ovpn configuration file.
- d. Start the OpenVPN client.
- e. Import the new client configuration file.
- f. Use the client to reconnect to the VPN gateway.
- g. On Windows, press **Win+R** and enter **cmd** to open the command window.

On Linux, log in as the **root** user and open the command window.

h.

NOTE

XX.XX.XX.XX indicates the private IP address of the ECS to be connected. Replace it with the actual private IP address.

If information similar to the following is displayed, the client can communicate with the ECS:

```
64 bytes from XX.XX.XX.XX: icmp_seq=1 ttl=63 time=1.27 ms
64 bytes from XX.XX.XX.XX: icmp_seq=2 ttl=63 time=1.36 ms
64 bytes from XX.XX.XX.XX: icmp_seq=3 ttl=63 time=1.40 ms
64 bytes from XX.XX.XX.XX: icmp_seq=4 ttl=63 time=1.29 ms
64 bytes from XX.XX.XX.XX: icmp_seq=5 ttl=63 time=1.35 ms
64 bytes from XX.XX.XX.XX: icmp_seq=6 ttl=63 time=1.52 ms
```

NOTE

If you use a client on Linux, you need to upload the configuration file **client_config.conf** to the Linux system using Xftp. For details, see [Configuring a Client](#).

If the problem persists, [submit a service ticket](#) to contact Huawei technical support.

4.6 The Client Log Contains "Options error: Unrecognized option or missing or extra parameter(s) in XXX: disable-dco"

Applicable Client

Linux

Symptom

A client cannot connect to a P2C VPN gateway, and the log contains the following error information:

```
Options error: Unrecognized option or missing or extra parameter(s) in XXX: disable-dco
```

Possible Causes

The OpenVPN client software version is 2.5 or earlier, which cannot identify the **disable-dco** configuration item.

Procedure

1. On Windows, open the **client_config.conf** file using Notepad or Notepad++.
2. Comment out **disable-dco**.
 - a. Press **Ctrl+F** to search for and locate **disable-dco**.
 - b. Enter **#** in front of the line where **disable-dco** is located to comment out the line.

```
...
...
```

```
# disable-dco
...
...
```

3. Save the .conf configuration file.
4. Upload the .conf configuration file to the Linux operating system using Xftp. In this example, the file is uploaded to the **/opt/** directory.
5. On Linux, run the following command to go to the directory where the client configuration file is stored:

```
cd /opt/
```

6. Run the following command to start the OpenVPN client and connect to the VPN gateway:

```
openvpn --config /opt/openvpn_config_user-01.conf
```

If the following information in bold is displayed, the OpenVPN connection is successfully established:

```
2025-02-27 19:22:41 Note: Kernel support for ovpn-dco missing, disabling data channel offload.
2025-02-27 19:22:41 OpenVPN 2.6.12 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL]
[PKCS11] [MH/PKTINFO] [AEAD] [DCO]
2025-02-27 19:22:41 library versions: OpenSSL 3.3.1 4 Jun 2024, LZO 2.10
...
...
...
2025-02-27 19:22:42 Initialization Sequence Completed
...
...
```

- 7.

NOTE

XX.XX.XX.XX indicates the private IP address of the ECS to be connected. Replace it with the actual private IP address.

If information similar to the following is displayed, the client can communicate with the ECS:

```
64 bytes from XX.XX.XX.XX: icmp_seq=1 ttl=63 time=1.27 ms
64 bytes from XX.XX.XX.XX: icmp_seq=2 ttl=63 time=1.36 ms
64 bytes from XX.XX.XX.XX: icmp_seq=3 ttl=63 time=1.40 ms
64 bytes from XX.XX.XX.XX: icmp_seq=4 ttl=63 time=1.29 ms
64 bytes from XX.XX.XX.XX: icmp_seq=5 ttl=63 time=1.35 ms
64 bytes from XX.XX.XX.XX: icmp_seq=6 ttl=63 time=1.52 ms
```

4.7 The Client Log Contains "TCP: connect to [AF_INET] *.*.*.*:**** failed: Unknown error"

Applicable Client

- Linux
- Windows OpenVPN GUI

Symptom



A client cannot connect to a P2C VPN gateway, and the log contains the following error information:

```
TCP: connect to [AF_INET] *.*.*.*:**** failed: Unknown error
```

Possible Causes

- The client device cannot access the Internet.
- The protocol or port number in the client configuration file is different from that configured on the **Server** tab page of the VPN gateway.

Procedure

1. On the client device, try to access other Internet services.
 - If the access also fails, contact your carrier to rectify the network connectivity fault.
 - If the access is successful, go to step 2.
2. Log in to the management console.
3. Click  in the upper left corner and select the desired region and project.
4. Click  in the upper left corner, and choose **Networking** > **Virtual Private Network**.
5. In the navigation pane on the left, choose **Virtual Private Network** > **Enterprise – VPN Gateways**.
6. Click the **P2C VPN Gateways** tab, locate the target VPN gateway, and click **View Server** in the **Operation** column.
7. On the **Server** tab page, view the server ID in the **Basic Information** area, and view the server port and protocol in the **Advanced Settings** area.
8. Check the **proto** and **remote** parameters in the client configuration file. An example is as follows:

```
...
proto tcp # Protocol type
remote XXX.XX.XX.XX XXX # Public IP address and port number of the server
...
```

If the parameter settings in the client configuration file are inconsistent with the actual configuration of the server, use either of the following methods to rectify the fault:

- Method 1: Modify the server information.
 - i. On the **Server** tab page, modify the corresponding information.
 - ii. Download the new client configuration file.
 - iii. The downloaded client configuration file is **client_config.zip**.
 - iv. Decompress **client_config.zip** to a specified directory, for example, **D:**.
 - v. After the decompression, the **client_config.ovpn** and **client_config.conf** files are generated.
 - vi. Open the **client_config.ovpn** file using Notepad or Notepad++.
 - vii. Add the client certificate and private key to the file.

Enter the client certificate content and the corresponding private key in between <cert></cert> and <key></key> tags, respectively.

```
<cert>
-----BEGIN CERTIFICATE-----
Client certificate content
-----END CERTIFICATE-----
</cert>
```

```
<key>  
-----BEGIN PRIVATE KEY-----  
Client private key  
-----END PRIVATE KEY-----  
</key>
```

- viii. Save the .ovpn configuration file.
- Method 2: Modify the client configuration file.
 - i. Open the **client_config.ovpn** file using Notepad or Notepad++.
 - ii. Modify the corresponding information in the client configuration file.
 - iii. Save the .ovpn configuration file.
9. Start the OpenVPN Connect client.
10. Import the new client configuration file.
11. Use the client to reconnect to the VPN gateway.
12. On Windows, press **Win+R** and enter **cmd** to open the command window.
On Linux, log in as the **root** user and open the command window.
- 13.

NOTE

XX.XX.XX.XX indicates the private IP address of the ECS to be connected. Replace it with the actual private IP address.

If information similar to the following is displayed, the client can communicate with the ECS:

```
64 bytes from XX.XX.XX.XX: icmp_seq=1 ttl=63 time=1.27 ms  
64 bytes from XX.XX.XX.XX: icmp_seq=2 ttl=63 time=1.36 ms  
64 bytes from XX.XX.XX.XX: icmp_seq=3 ttl=63 time=1.40 ms  
64 bytes from XX.XX.XX.XX: icmp_seq=4 ttl=63 time=1.29 ms  
64 bytes from XX.XX.XX.XX: icmp_seq=5 ttl=63 time=1.35 ms  
64 bytes from XX.XX.XX.XX: icmp_seq=6 ttl=63 time=1.52 ms
```

NOTE

If you use a client on Linux, you need to upload the configuration file **client_config.conf** to the Linux system using Xftp. For details, see [Configuring a Client](#).

4.8 The Client Log Contains "AUTH: Received control message: AUTH_FAILED"

Applicable Client

- Linux
- Windows OpenVPN GUI

Symptom



A client cannot connect to a P2C VPN gateway, and the log contains the following error information:

```
AUTH: Received control message: AUTH_FAILED
```

Possible Causes

- If a static IP address has been configured for the user, the client can set up only one connection.
- The user entered incorrect passwords for five consecutive times, and the user account is locked.
- The username and password did not match.



Procedure

1. Check whether a static IP address is configured for the user.
 - a. Log in to the management console.
 - b. Click  in the upper left corner and select the desired region and project.
 - c. Click  in the upper left corner, and choose **Networking > Virtual Private Network**.
 - d. In the navigation pane on the left, choose **Virtual Private Network > Enterprise – VPN Gateways**.
 - e. Click the **P2C VPN Gateways** tab, locate the target VPN gateway, and click **View Server** in the **Operation** column.
 - f. Choose **User Management > Users**, and check whether a static IP address is configured for the user.
 - If no static IP address is configured, go to step 2.
 - If a static IP address is configured but it is occupied by another user, disconnect the client and reconnect it.
2. Check whether the user account is locked due to multiple incorrect password attempts.

If not, go to step 3.

If so, log in to the client again 5 minutes later.
3. Check whether the username and password for logging in to the client match.

If not, reset the password as follows, and use the new password for login:

 - a. Log in to the management console.
 - b. Click  in the upper left corner and select the desired region and project.
 - c. Click  in the upper left corner, and choose **Networking > Virtual Private Network**.
 - d. In the navigation pane on the left, choose **Virtual Private Network > Enterprise – VPN Gateways**.
 - e. Click the **P2C VPN Gateways** tab, locate the target VPN gateway, and click **View Server** in the **Operation** column.
 - f. Choose **User Management > Users**, and click **Reset Password** in the **Operation** column of the target user.
 - g. Set a new password and click **OK**.

If the problem persists, [submit a service ticket](#) to contact Huawei technical support.

4.9 The Client Log Contains "AUTH_FAILED"

Applicable Client

Windows OpenVPN Connect

Symptom



A client cannot connect to a P2C VPN gateway, and the log contains the following error information:

```
AUTH_FAILED
```

Possible Causes

- If a static IP address has been configured for the user, the client can set up only one connection.
- The user entered incorrect passwords for five consecutive times, and the user account is locked.
- The username and password did not match.
- The certificate and private key in the client configuration file do not match the client CA certificate imported on the **Server** tab page of the VPN gateway.

Procedure

- If password authentication is used, perform the following operations:
 - a. Check whether a static IP address is configured for the user.
 - i. Log in to the management console.
 - ii. Click  in the upper left corner and select the desired region and project.
 - iii. Click  in the upper left corner, and choose **Networking > Virtual Private Network**.
 - iv. In the navigation pane on the left, choose **Virtual Private Network > Enterprise – VPN Gateways**.
 - v. Click the **P2C VPN Gateways** tab, locate the target VPN gateway, and click **View Server** in the **Operation** column.
 - vi. Choose **User Management > Users**, and check whether a static IP address is configured for the user.
 - If no static IP address is configured, go to step [2](#).
 - If a static IP address is configured but it is occupied by another user, disconnect the client and reconnect it.
 - b. Check whether the user account is locked due to multiple incorrect password attempts.
If not, go to step [3](#).





- If so, log in to the client again 5 minutes later.
- c. Check whether the username and password for logging in to the client match.
If not, reset the password as follows, and use the new password for login:
 - i. Log in to the management console.
 - ii. Click  in the upper left corner and select the desired region and project.
 - iii. Click  in the upper left corner, and choose **Networking > Virtual Private Network**.
 - iv. In the navigation pane on the left, choose **Virtual Private Network > Enterprise – VPN Gateways**.
 - v. Click the **P2C VPN Gateways** tab, locate the target VPN gateway, and click **View Server** in the **Operation** column.
 - vi. Choose **User Management > Users**, and click **Reset Password** in the **Operation** column of the target user.
 - vii. Set a new password and click **OK**.
 - If certificate authentication is used, perform the following operations:
 - a. Check whether the imported client CA certificate is correct.
 - i. Log in to the management console.
 - ii. Click  in the upper left corner and select the desired region and project.
 - iii. Click  in the upper left corner, and choose **Networking > Virtual Private Network**.
 - iv. In the navigation pane on the left, choose **Virtual Private Network > Enterprise – VPN Gateways**.
 - v. Click the **P2C VPN Gateways** tab. In the P2C VPN gateway list, locate the target P2C VPN gateway, and click **View Server** in the **Operation** column.
 - vi. On the **Server** tab page, view the issuer information of the client CA certificate.
 - vii. Double-click the target client CA certificate, click the **Details** tab, and view the issuer information.
If the issuer information on the client is consistent with that on the server, go to step 2.
If the issuer information on the client is inconsistent with that on the server, perform the following operations to import the client CA certificate again:
 - 1) On the **Server** tab page, choose **Certificate authentication** from the **Client Authentication Mode** drop-down list box, and click **Upload CA Certificate**.
 - 2) Set parameters as prompted.

Table 4-2 Parameters for uploading a CA certificate

Parameter	Description	Example Value
Name	This parameter can be modified.	ca-cert-xxxx
Content	<p>Use a text editor (for example, Notepad++) to open the signature certificate file in PEM format, and copy the certificate content to this text box.</p> <p>NOTE</p> <ul style="list-style-type: none"> It is recommended to use a certificate with a strong cryptographic algorithm, such as RSA-3072 or RSA-4096. Certificates using the RSA-2048 encryption algorithm have risks. Exercise caution when using such certificates. 	<pre>-----BEGIN CERTIFICATE----- Certificate content -----END CERTIFICATE-----</pre>

- 3) Click **OK**.
- 4) Click **Delete** in the **Operation** column of the incorrect client CA certificate.
- 5) In the **Delete CA Certificate** dialog box, click **OK**.
- 6) Download the new client configuration file.
- 7) The downloaded client configuration file is **client_config.zip**.
- 8) Decompress **client_config.zip** to a specified directory, for example, **D:**.

After the decompression, the **client_config.ovpn** and **client_config.conf** files are generated.

- 9) Open the **client_config.ovpn** file using Notepad or Notepad++.
- 10) Add the client certificate and private key to the file.

Enter the client certificate content and the corresponding private key in between `<cert></cert>` and `<key></key>` tags, respectively.

```
<cert>
-----BEGIN CERTIFICATE-----
Client certificate content
-----END CERTIFICATE-----
</cert>

<key>
-----BEGIN PRIVATE KEY-----
Client private key
-----END PRIVATE KEY-----
</key>
```

- 11) Save the .ovpn configuration file.
 - 12) Start the OpenVPN client.
 - 13) Import the new client configuration file.
 - 14) Use the client to reconnect to the VPN gateway.
- b. Check whether the client certificate and private key in the configuration file match.

If not, copy the correct client certificate and private key to the client configuration file as follows:

- i. Open the **client_config.ovpn** file, client certificate, and client private key using Notepad or Notepad++.
- ii. Copy the client certificate and private key to the **client_config.ovpn** file.

Enter the client certificate content and the corresponding private key in between `<cert></cert>` and `<key></key>` tags, respectively. An example is as follows:

```
<cert>
-----BEGIN CERTIFICATE-----
Client certificate content
-----END CERTIFICATE-----
</cert>

<key>
-----BEGIN PRIVATE KEY-----
Client private key
-----END PRIVATE KEY-----
</key>
```

- iii. Save the .ovpn configuration file.
- iv. Start the OpenVPN client.
- v. Import the new client configuration file.
- vi. Use the client to reconnect to the VPN gateway.

If the problem persists, [submit a service ticket](#) to contact Huawei technical support.

4.10 The Client Log Contains "error=unable to get issuer certificate:".

Applicable Client

Windows OpenVPN GUI

Symptom

The client cannot connect to the P2C VPN gateway. The client log contains the following error information:

```
error=unable to get issuer certificate:
```

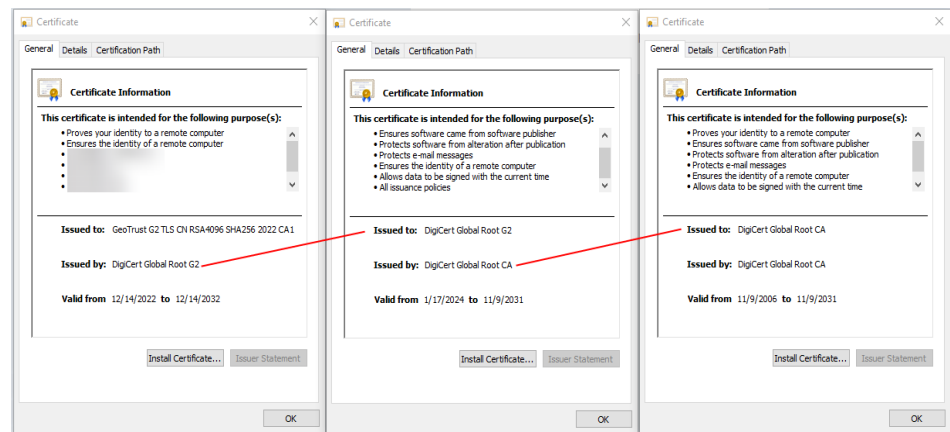
Possible Causes

The certificate chain of server certificates is incomplete. As a result, the client cannot verify the validity of the CA certificates in the configuration file.

Procedure

1. Open the **client_config.ovpn** file using Notepad or Notepad++.
2. Check the number of CA certificates in the client configuration file.
3. Double-click each CA certificate in client configuration file, click the **Certification Path** tab, and check whether the issuers and subjects of the certificates form a complete certificate chain.
 - If the issuer and subject of the top-level certificate are the same, the certificate chain is complete, as shown in **Figure 4-2**.

Figure 4-2 Complete CA certificate chain



- If the issuer and subject of the top-level certificate are different, the certificate chain is incomplete. Perform the following operations to supplement the certificate chain information:
 - a. Create a Notepad file.
 - b. Copy the CA certificate content in **client_config.ovpn** to the new Notepad file. The format of the certificate content is as follows:

```
<ca>
-----BEGIN CERTIFICATE-----
CA certificate
-----END CERTIFICATE-----
</ca>
```
 - c. Save the file and name it **ca.crt**.
 - d. Export the upper-level certificate of the CA certificate in use.
 - i. Double-click the CA certificate, click the **Certification Path** tab, and view the upper-level certificate of the CA certificate.
 - ii. Select the upper-level certificate, and click **View Certificate**. A new window containing the upper-level certificate is displayed.
 - iii. Click the **Details** tab, and click **Copy to File**.
 - iv. Click **Next**.
 - v. Select **Base-64 encoded** and click **Next**.

- vi. Enter a file name, for example, **root-ca.cer**.
- vii. Click **Next** and then **Finish**.
If the configuration file contains two CA certificates, export the upper-level certificates of the two CA certificates.
- e. Copy the content of the upper-level certificate **root-ca.cer** to the client configuration file.
 - i. Open the **root-ca.cer** and **client_config.ovpn** files using Notepad or Notepad++.
 - ii. Copy the content of the upper-level certificate below the existing CA certificate in the **client_config.ovpn** file.
The format of the certificate content is as follows:

```
-----BEGIN CERTIFICATE-----  
Existing CA certificate  
-----END CERTIFICATE-----  
-----BEGIN CERTIFICATE-----  
Upper-level CA certificate  
-----END CERTIFICATE-----
```
 - iii. Save the .ovpn configuration file.
- f. Start the OpenVPN client.
- g. Import the new client configuration file.
- h. Use the client to reconnect to the VPN gateway.
- i. Press **Win+R** and enter **cmd** to open the command window.
- j.

NOTE

XX.XX.XX.XX indicates the private IP address of the ECS to be connected. Replace it with the actual private IP address.

If information similar to the following is displayed, the client can communicate with the ECS:

```
64 bytes from XX.XX.XX.XX: icmp_seq=1 ttl=63 time=1.27 ms  
64 bytes from XX.XX.XX.XX: icmp_seq=2 ttl=63 time=1.36 ms  
64 bytes from XX.XX.XX.XX: icmp_seq=3 ttl=63 time=1.40 ms  
64 bytes from XX.XX.XX.XX: icmp_seq=4 ttl=63 time=1.29 ms  
64 bytes from XX.XX.XX.XX: icmp_seq=5 ttl=63 time=1.35 ms  
64 bytes from XX.XX.XX.XX: icmp_seq=6 ttl=63 time=1.52 ms
```

If the problem persists, [submit a service ticket](#) to contact Huawei technical support.

4.11 The Client Log Contains "peer Certificate Verification Failure"

Applicable Client

Windows OpenVPN Connect

Symptom

A client cannot connect to a P2C VPN gateway, and the log contains the following error information:

peer certificate verification failure

Possible Causes

- The certificate chain of the server certificate is incomplete. As a result, the client cannot verify the validity of the CA certificate in the configuration file.
- The length of the CA certificate chain in the client configuration exceeds 3.

Procedure



1. Check whether the length of the CA certificate chain in the client configuration is too long.
 - a. Open the **client_config.ovpn** file using Notepad or Notepad++.
 - b. Check the number of CA certificates in the client configuration file.
 - If the number of CA certificates does not exceed 3, go to step 2.
 - If the number of CA certificates exceeds 3, the certificate chain length is too long and you need to generate new CA certificates. For details, see [Using Easy-RSA to Issue Certificates \(Server and Client Sharing a CA Certificate\)](#).
 - c. Log in to the management console.
 - d. Click  in the upper left corner and select the desired region and project.
 - e. Click  in the upper left corner, and choose **Networking > Virtual Private Network**.
 - f. In the navigation pane on the left, choose **Virtual Private Network > Enterprise – VPN Gateways**.
 - g. Click the **P2C VPN Gateways** tab, locate the target VPN gateway, and click **View Server** in the **Operation** column.
 - h. Upload a CA certificate.
 - i. On the **Server** tab page, choose **Certificate authentication** from the **Client Authentication Mode** drop-down list box, and click **Upload CA Certificate**.
 - ii. Set parameters as prompted.

Table 4-3 Parameters for uploading a CA certificate

Parameter	Description	Example Value
Name	This parameter can be modified.	ca-cert-xxxx

Parameter	Description	Example Value
Content	<p>Use a text editor (for example, Notepad++) to open the signature certificate file in PEM format, and copy the certificate content to this text box.</p> <p>NOTE</p> <ul style="list-style-type: none"> It is recommended to use a certificate with a strong cryptographic algorithm, such as RSA-3072 or RSA-4096. Certificates using the RSA-2048 encryption algorithm have risks. Exercise caution when using such certificates. 	<pre>-----BEGIN CERTIFICATE----- <i>Certificate content</i> -----END CERTIFICATE-----</pre>

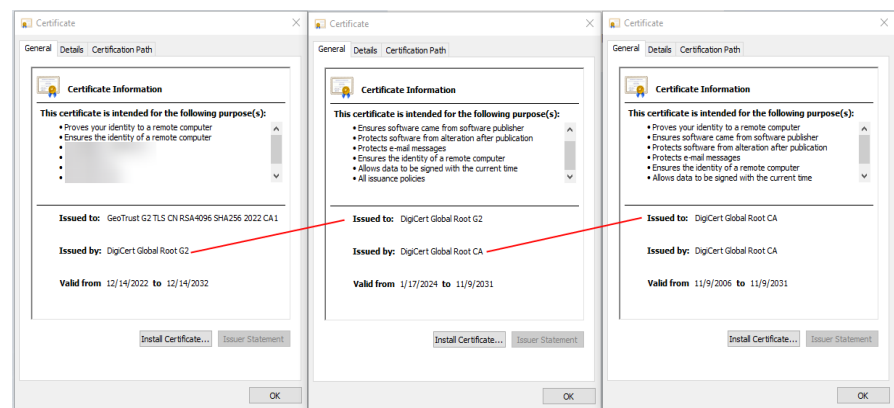
- iii. Click **OK**.
- i. Delete the incorrect CA certificate.
 - i. On the **Server** tab page, click **Delete** in the **Operation** column of the incorrect client CA certificate.
 - ii. In the **Delete CA Certificate** dialog box, click **OK**.
- j. Download the new client configuration file.
The downloaded client configuration file is **client_config.zip**.
- k. Decompress **client_config.zip** to a specified directory, for example, **D:**.
After the decompression, the **client_config.ovpn** and **client_config.conf** files are generated.
- l. Open the **client_config.ovpn** file using Notepad or Notepad++.
- m. Add the client certificate and private key to the file.
Enter the client certificate content and the corresponding private key in between `<cert></cert>` and `<key></key>` tags, respectively. An example is as follows:

```
<cert>
-----BEGIN CERTIFICATE-----
Client certificate content
-----END CERTIFICATE-----
</cert>

<key>
-----BEGIN PRIVATE KEY-----
Client private key
-----END PRIVATE KEY-----
</key>
```
- n. Save the .ovpn configuration file.
- o. Start the OpenVPN client.
- p. Import the new client configuration file.

- q. Use the client to reconnect to the VPN gateway.
2. Check whether the server certificate chain is complete.
 - a. Open the **client_config.ovpn** file using Notepad or Notepad++.
 - b. Check the number of CA certificates in the client configuration file.
 - c. Double-click each CA certificate in client configuration file, click the **Certification Path** tab, and check whether the issuers and subjects of the certificates form a complete certificate chain.
 - If the issuer and subject of the top-level certificate are the same, the certificate chain is complete, as shown in **Figure 4-3**.

Figure 4-3 Complete CA certificate chain



- If the issuer and subject of the top-level certificate are different, the certificate chain is incomplete. Perform the following operations to supplement the certificate chain information:
 - i. Create a Notepad file.
 - ii. Copy the CA certificate content in **client_config.ovpn** to the new Notepad file. The format of the certificate content is as follows:


```
<ca>
-----BEGIN CERTIFICATE-----
CA certificate
-----END CERTIFICATE-----
</ca>
```
 - iii. Save the file and name it **ca.crt**.
 - iv. Double-click the CA certificate, click the **Certification Path** tab, and view the upper-level certificate of the CA certificate.
 - v. Select the upper-level certificate, and click **View Certificate**. A new window containing the upper-level certificate is displayed.
 - vi. Click the **Details** tab, and click **Copy to File**.
 - vii. Click **Next**.
 - viii. Select **Base-64 encoded** and click **Next**.
 - ix. Enter a file name, for example, **root-ca.cer**.
 - x. Click **Next** and then **Finish**.

If the configuration file contains two CA certificates, export the upper-level certificates of the two CA certificates.

- xi. Open the **root-ca.cer** and **client_config.ovpn** files using Notepad or Notepad++.
- xii. Copy the content of the upper-level certificate below the existing CA certificate in the **client_config.ovpn** file.

The format of the certificate content is as follows:

```
-----BEGIN CERTIFICATE-----  
Existing CA certificate  
-----END CERTIFICATE-----  
-----BEGIN CERTIFICATE-----  
Upper-level CA certificate  
-----END CERTIFICATE-----
```

- xiii. Save the .cer certificate file.
- xiv. Start the OpenVPN client.
- xv. Import the new client configuration file.
- xvi. Use the client to reconnect to the VPN gateway.
- xvii. Press **Win+R** and enter **cmd** to open the command window.
- xviii.

NOTE

XX.XX.XX.XX indicates the private IP address of the ECS to be connected.
Replace it with the actual private IP address.

If information similar to the following is displayed, the client can communicate with the ECS:

```
64 bytes from XX.XX.XX.XX: icmp_seq=1 ttl=63 time=1.27 ms  
64 bytes from XX.XX.XX.XX: icmp_seq=2 ttl=63 time=1.36 ms  
64 bytes from XX.XX.XX.XX: icmp_seq=3 ttl=63 time=1.40 ms  
64 bytes from XX.XX.XX.XX: icmp_seq=4 ttl=63 time=1.29 ms  
64 bytes from XX.XX.XX.XX: icmp_seq=5 ttl=63 time=1.35 ms  
64 bytes from XX.XX.XX.XX: icmp_seq=6 ttl=63 time=1.52 ms
```

If the problem persists, [submit a service ticket](#) to contact Huawei technical support.

4.12 The Client Log Contains "error=path length constraint exceeded"

Applicable Client

Windows OpenVPN GUI

Symptom

A client cannot connect to a P2C VPN gateway, and the log contains the following error information:

```
error=path length constraint exceeded
```

Possible Causes

The length of the CA certificate chain in the client configuration exceeds 3.

Procedure



1. Re-generate CA certificates. For details, see [Using Easy-RSA to Issue Certificates \(Server and Client Sharing a CA Certificate\)](#).
2. Log in to the management console.
3. Click  in the upper left corner and select the desired region and project.
4. Click  in the upper left corner, and choose **Networking > Virtual Private Network**.
5. In the navigation pane on the left, choose **Virtual Private Network > Enterprise - VPN Gateways**.
6. Click the **P2C VPN Gateways** tab. In the P2C VPN gateway list, locate the target P2C VPN gateway, and click **View Server** in the **Operation** column.
7. Upload CA certificates.
 - a. On the **Server** tab page, choose **Certificate authentication** from the **Client Authentication Mode** drop-down list box, and click **Upload CA Certificate**.
 - b. Set parameters as prompted.

Table 4-4 Parameters for uploading a CA certificate

Parameter	Description	Example Value
Name	This parameter can be modified.	ca-cert-xxxx
Content	Use a text editor (for example, Notepad++) to open the signature certificate file in PEM format, and copy the certificate content to this text box. NOTE <ul style="list-style-type: none">• It is recommended to use a certificate with a strong cryptographic algorithm, such as RSA-3072 or RSA-4096.• Certificates using the RSA-2048 encryption algorithm have risks. Exercise caution when using such certificates.	-----BEGIN CERTIFICATE----- <i>Certificate content</i> -----END CERTIFICATE-----

- c. Click **OK**.
8. Delete the incorrect CA certificate.
 - a. On the **Server** tab page, click **Delete** in the **Operation** column of the incorrect client CA certificate.

- b. In the **Delete CA Certificate** dialog box, click **OK**.
9. Download the new client configuration file.
The downloaded client configuration file is **client_config.zip**.
10. Decompress **client_config.zip** to a specified directory, for example, **D:**.
After the decompression, the **client_config.ovpn** and **client_config.conf** files are generated.
11. Open the **client_config.ovpn** file using Notepad or Notepad++.
12. Add the client certificate and private key to the file.
Enter the client certificate content and the corresponding private key in between `<cert></cert>` and `<key></key>` tags, respectively. An example is as follows:

```
<cert>
-----BEGIN CERTIFICATE-----
Client certificate content
-----END CERTIFICATE-----
</cert>

<key>
-----BEGIN PRIVATE KEY-----
Client private key
-----END PRIVATE KEY-----
</key>
```
13. Save the .ovpn configuration file.
14. Start the OpenVPN client.
15. Import the new client configuration file.
16. Use the client to reconnect to the VPN gateway.
17. Press **Win+R** and enter **cmd** to open the command window.
- 18.

NOTE

XX.XX.XX.XX indicates the private IP address of the ECS to be connected. Replace it with the actual private IP address.

If information similar to the following is displayed, the client can communicate with the ECS:

```
64 bytes from XX.XX.XX.XX: icmp_seq=1 ttl=63 time=1.27 ms
64 bytes from XX.XX.XX.XX: icmp_seq=2 ttl=63 time=1.36 ms
64 bytes from XX.XX.XX.XX: icmp_seq=3 ttl=63 time=1.40 ms
64 bytes from XX.XX.XX.XX: icmp_seq=4 ttl=63 time=1.29 ms
64 bytes from XX.XX.XX.XX: icmp_seq=5 ttl=63 time=1.35 ms
64 bytes from XX.XX.XX.XX: icmp_seq=6 ttl=63 time=1.52 ms
```

If the problem persists, [submit a service ticket](#) to contact Huawei technical support.

4.13 The Client Log Contains "Certificate does not have key usage extension"

Applicable Client

Windows OpenVPN GUI

Symptom

A client cannot connect to a P2C VPN gateway, and the log contains the following error information:

Certificate does not have key usage extension

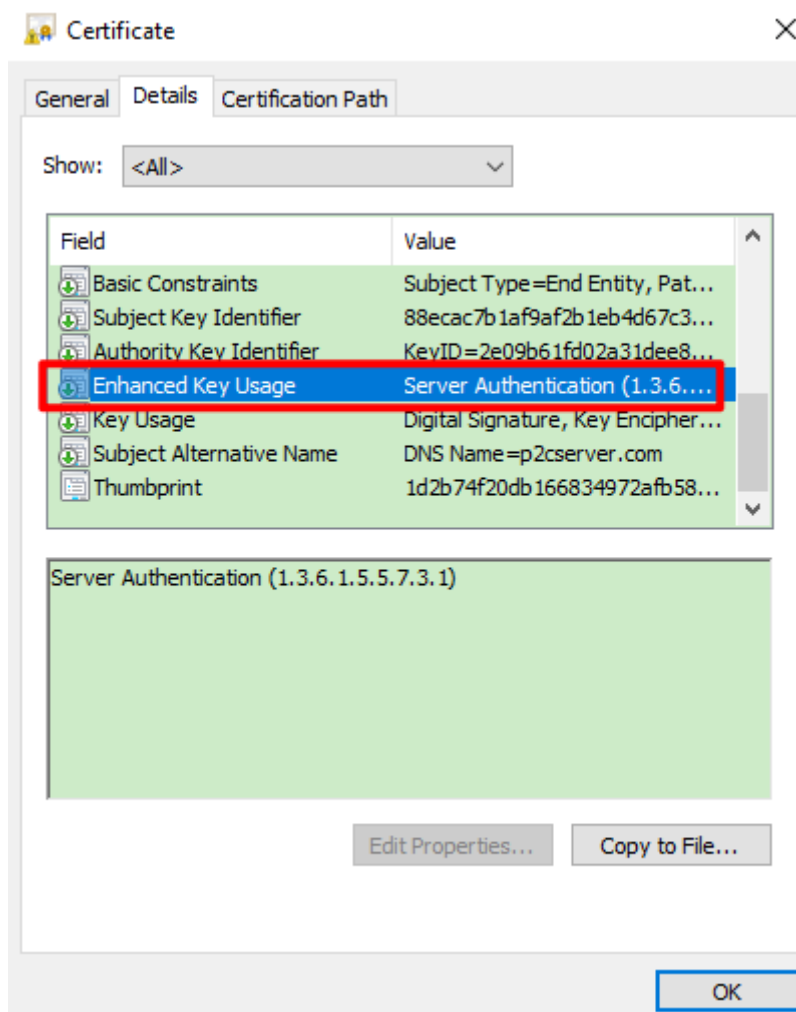
Possible Causes

The server certificate used by the VPN gateway does not contain the Server Authentication attribute. As a result, certificate verification fails.

Procedure

1. Right-click the target server certificate, and choose **Properties** from the shortcut menu.
2. Click the **Details** tab, and check whether the certificate contains the Server Authentication attribute, as shown in [Figure 4-4](#).



Figure 4-4 Server certificate



If the certificate does not contain the Server Authentication attribute, re-generate a server certificate. For details, see [Using Easy-RSA to Issue Certificates \(Server and Client Sharing a CA Certificate\)](#).

A server certificate generated using OpenSSL does not contain the **Server Authentication** attribute. As such, you need to add **extendedKeyUsage = serverAuth** to the OpenSSL configuration file. The following is an example:

```
...  
keyUsage = nonRepudiation, digitalSignature, keyEncipherment  
extendedKeyUsage = serverAuth  
...
```

3. Log in to the management console.
4. Click  in the upper left corner and select the desired region and project.
5. Click  in the upper left corner, and choose **Networking > Virtual Private Network**.
6. In the navigation pane on the left, choose **Virtual Private Network > Enterprise – VPN Gateways**.
7. Click the **P2C VPN Gateways** tab. In the P2C VPN gateway list, locate the target P2C VPN gateway, and click **View Server** in the **Operation** column.
8. On the **Server** tab page of the VPN gateway, click **Replace**.
9. In the displayed dialog box, click **Upload** in the drop-down list box.
Upload the new server certificate to CCM. For details, see [Uploading a Server Certificate](#).
10. Download the new client configuration file.
The downloaded client configuration file is **client_config.zip**.
11. Decompress **client_config.zip** to a specified directory, for example, **D:**.
After the decompression, the **client_config.ovpn** and **client_config.conf** files are generated.
12. Add the client certificate and private key to the file.
 - a. Open the **client_config.ovpn** file using Notepad or Notepad++.
 - b. Enter the client certificate content and the corresponding private key in between `<cert></cert>` and `<key></key>` tags, respectively.

```
<cert>  
-----BEGIN CERTIFICATE-----  
Client certificate content  
-----END CERTIFICATE-----  
</cert>  
  
<key>  
-----BEGIN PRIVATE KEY-----  
Client private key  
-----END PRIVATE KEY-----  
</key>
```
 - c. Save the .ovpn configuration file.
13. Start the OpenVPN client.
14. Import the new client configuration file.
15. Use the client to reconnect to the VPN gateway.
16. Press **Win+R** and enter **cmd** to open the command window.
- 17.

 **NOTE**

`XX.XX.XX.XX` indicates the private IP address of the ECS to be connected. Replace it with the actual private IP address.

If information similar to the following is displayed, the client can communicate with the ECS:

```
64 bytes from XX.XX.XX.XX: icmp_seq=1 ttl=63 time=1.27 ms
64 bytes from XX.XX.XX.XX: icmp_seq=2 ttl=63 time=1.36 ms
64 bytes from XX.XX.XX.XX: icmp_seq=3 ttl=63 time=1.40 ms
64 bytes from XX.XX.XX.XX: icmp_seq=4 ttl=63 time=1.29 ms
64 bytes from XX.XX.XX.XX: icmp_seq=5 ttl=63 time=1.35 ms
64 bytes from XX.XX.XX.XX: icmp_seq=6 ttl=63 time=1.52 ms
```

If the problem persists, [submit a service ticket](#) to contact Huawei technical support.

4.14 The Client Log Contains "Error message: ovpnagent:request error"

Applicable Client

Windows OpenVPN Connect

Symptom

A client cannot connect to a P2C VPN gateway, and the log contains the following error information:

```
Error message: ovpnagent:request error
```

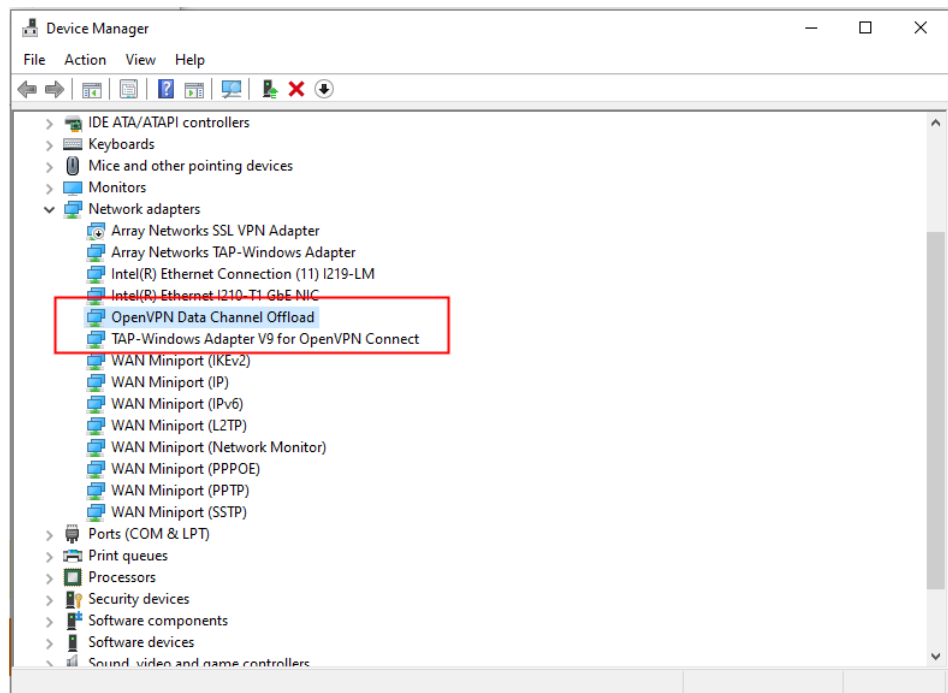
Possible Causes

The OpenVPN client software is not running properly.

Procedure

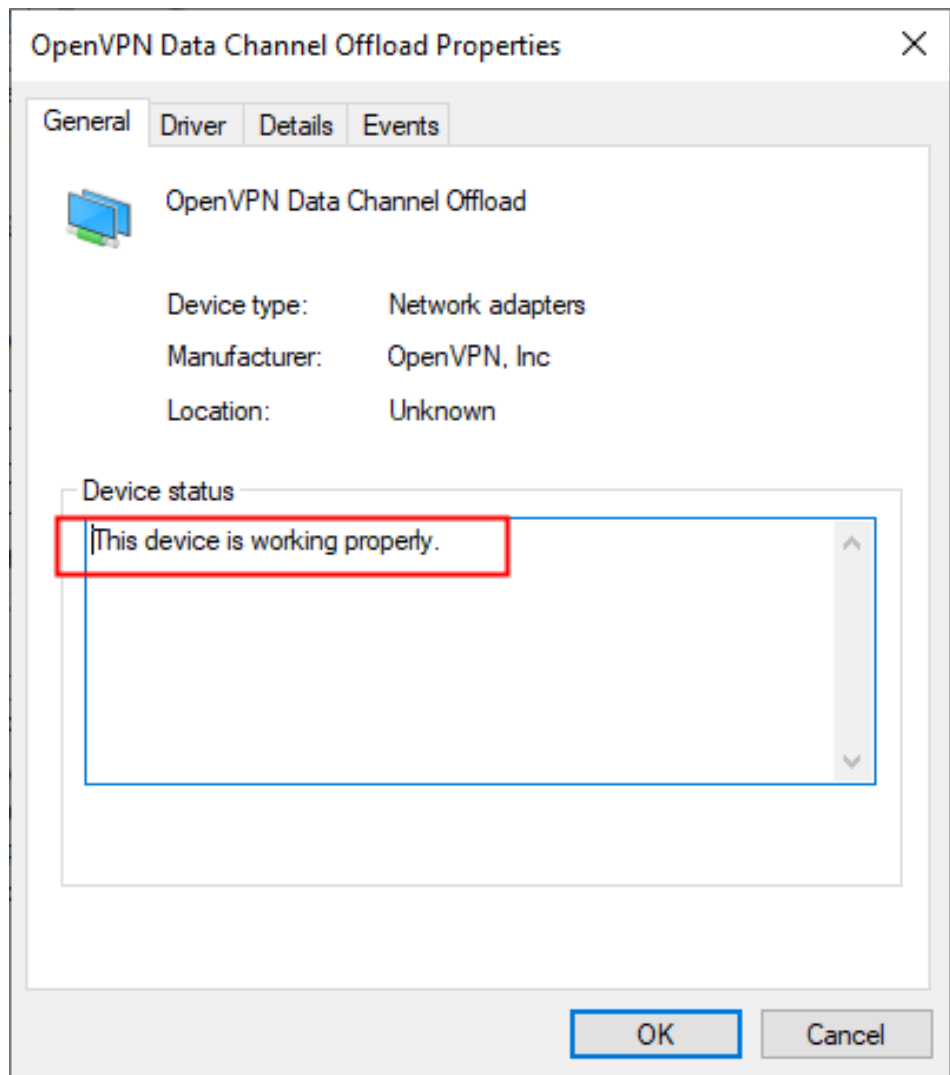
1. Check OpenVPN network adapters.
 - a. Press **Win+R**, enter **devmgmt.msc**, and press **Enter** to open the Device Manager.
 - b. Click **Network adapters**, and find **TAP-Windows Adapter V9 for OpenVPN Connect** and **OpenVPN Data Channel Offload**, as shown in [Figure 4-5](#).

Figure 4-5 Device Manager



- c. Right-click each of the preceding network adapter, choose **Properties**, and check the device status, as shown in [Figure 4-6](#).

Figure 4-6 Checking the device status

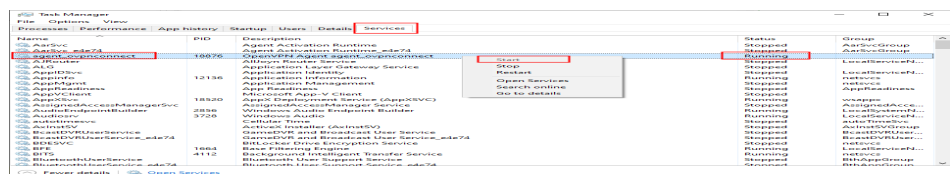


If the device status is normal, uninstall OpenVPN Connect and reinstall it.

2. Check whether the agent_ovpnconnect service is running properly.
 - a. Enter **Task Manager** in the taskbar search box, and click **Task Manager** to open it.
 - b. Click the **Services** tab, and find the agent_ovpnconnect service.

If the service status is **Stopped**, right-click the service and choose **Start** from the shortcut menu, as shown in **Figure 4-7**.

Figure 4-7 Task Manager



3. Reconnect to the client to the VPN gateway.

4. Press **Win+R** and enter **cmd** to open the command window.
- 5.

NOTE

XX.XX.XX.XX indicates the private IP address of the ECS to be connected. Replace it with the actual private IP address.

If information similar to the following is displayed, the client can communicate with the ECS:

```
64 bytes from XX.XX.XX.XX: icmp_seq=1 ttl=63 time=1.27 ms
64 bytes from XX.XX.XX.XX: icmp_seq=2 ttl=63 time=1.36 ms
64 bytes from XX.XX.XX.XX: icmp_seq=3 ttl=63 time=1.40 ms
64 bytes from XX.XX.XX.XX: icmp_seq=4 ttl=63 time=1.29 ms
64 bytes from XX.XX.XX.XX: icmp_seq=5 ttl=63 time=1.35 ms
64 bytes from XX.XX.XX.XX: icmp_seq=6 ttl=63 time=1.52 ms
```

4.15 The Client Log Contains "X509::parse_pem: error in cert::error:0480006C:PEM routines::no start line"

Applicable Client

- Linux
- Windows OpenVPN GUI

Symptom

A client cannot connect to a P2C VPN gateway, and the log contains the following error information:

```
X509::parse_pem: error in cert::error:0480006C:PEM routines::no start line
```

Possible Causes

In certificate authentication mode, the client configuration file does not contain the client certificate or private key.

Procedure

1. Re-generate a client certificate and private key. For details, see [Using Easy-RSA to Issue Certificates \(Server and Client Sharing a CA Certificate\)](#). In this example, the generated client certificate and private key are **p2cclient.com.crt** and **p2cclient.com.key**, respectively.
2. Open the **p2cclient.com.crt**, **p2cclient.com.key**, and **client_config.ovpn** files using Notepad or Notepad++.
3. Copy the generated client certificate and private key to the client configuration file.

Enter the client certificate content and the corresponding private key in between `<cert></cert>` and `<key></key>` tags, respectively. An example is as follows:

```
<cert>
-----BEGIN CERTIFICATE-----
Client certificate content
-----END CERTIFICATE-----
```

```
</cert>
<key>
-----BEGIN PRIVATE KEY-----
Client private key
-----END PRIVATE KEY-----
</key>
```

4. Save the .ovpn configuration file.
5. Start the OpenVPN client.
6. Import the new client configuration file.
7. Use the client to reconnect to the VPN gateway.
8. On Windows, press **Win+R** and enter **cmd** to open the command window.
On Linux, log in as the **root** user and open the command window.
- 9.

NOTE

XX.XX.XX.XX indicates the private IP address of the ECS to be connected. Replace it with the actual private IP address.

If information similar to the following is displayed, the client can communicate with the ECS:

```
64 bytes from XX.XX.XX.XX: icmp_seq=1 ttl=63 time=1.27 ms
64 bytes from XX.XX.XX.XX: icmp_seq=2 ttl=63 time=1.36 ms
64 bytes from XX.XX.XX.XX: icmp_seq=3 ttl=63 time=1.40 ms
64 bytes from XX.XX.XX.XX: icmp_seq=4 ttl=63 time=1.29 ms
64 bytes from XX.XX.XX.XX: icmp_seq=5 ttl=63 time=1.35 ms
64 bytes from XX.XX.XX.XX: icmp_seq=6 ttl=63 time=1.52 ms
```

NOTE

If you use a client on Linux, you need to upload the configuration file **client_config.conf** to the Linux system using Xftp. For details, see [Configuring a Client](#).

4.16 The Client Log Contains "certReadError"

Applicable Client

- Linux
- Windows OpenVPN GUI

Symptom

A client cannot connect to a P2C VPN gateway, and the log contains the following error information:

```
certReadError
```

Possible Causes

In certificate authentication mode, the client configuration file does not contain the client certificate or private key.

Procedure

1. Re-generate a client certificate and private key. For details, see [Using Easy-RSA to Issue Certificates \(Server and Client Sharing a CA Certificate\)](#). In this example, the generated client certificate and private key are **p2cclient.com.crt** and **p2cclient.com.key**, respectively.
2. Open the **p2cclient.com.crt**, **p2cclient.com.key**, and **client_config.ovpn** files using Notepad or Notepad++.
3. Copy the generated client certificate and private key to the client configuration file.

Enter the client certificate content and the corresponding private key in between `<cert></cert>` and `<key></key>` tags, respectively. An example is as follows:

```
<cert>
-----BEGIN CERTIFICATE-----
Client certificate content
-----END CERTIFICATE-----
</cert>

<key>
-----BEGIN PRIVATE KEY-----
Client private key
-----END PRIVATE KEY-----
</key>
```

4. Save the .ovpn configuration file.
5. Start the OpenVPN client.
6. Import the new client configuration file.
7. Use the client to reconnect to the VPN gateway.
8. On Windows, press **Win+R** and enter **cmd** to open the command window. On Linux, log in as the **root** user and open the command window.
- 9.

NOTE

XX.XX.XX.XX indicates the private IP address of the ECS to be connected. Replace it with the actual private IP address.

If information similar to the following is displayed, the client can communicate with the ECS:

```
64 bytes from XX.XX.XX.XX: icmp_seq=1 ttl=63 time=1.27 ms
64 bytes from XX.XX.XX.XX: icmp_seq=2 ttl=63 time=1.36 ms
64 bytes from XX.XX.XX.XX: icmp_seq=3 ttl=63 time=1.40 ms
64 bytes from XX.XX.XX.XX: icmp_seq=4 ttl=63 time=1.29 ms
64 bytes from XX.XX.XX.XX: icmp_seq=5 ttl=63 time=1.35 ms
64 bytes from XX.XX.XX.XX: icmp_seq=6 ttl=63 time=1.52 ms
```

NOTE

If you use a client on Linux, you need to upload the configuration file **client_config.conf** to the Linux system using Xftp. For details, see [Configuring a Client](#).

4.17 The Client Log Contains "OPTIONS ERROR:failed to negotiate cipher with server.Add the server's cipher('AES-XXX-GCM') to --data-ciphers(currently 'AES-XXX-GCM') if you want to connect to this server."

Applicable Client

Windows OpenVPN GUI

Symptom



A client cannot connect to the VPN gateway, and the client log contains the following error message:

```
OPTIONS ERROR:failed to negotiate cipher with server.Add the server's cipher('AES-XXX-GCM') to --data-ciphers(currently 'AES-XXX-GCM') if you want to connect to this server. # AES-XXX-GCM is the configured encryption algorithm.
```

Possible Causes


The cipher suite of the client does not match that of the server.

Procedure

1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. Click  in the upper left corner, and choose **Networking > Virtual Private Network**.
4. In the navigation pane on the left, choose **Virtual Private Network > Enterprise - VPN Gateways**.
5. Click the **P2C VPN Gateways** tab. In the P2C VPN gateway list, locate the target P2C VPN gateway, and click **View Server** in the **Operation** column.
6. On the **Server** tab page, view the encryption algorithm and authentication algorithm of the server in the **Advanced Settings** area.
7. Check the **data-ciphers** and **auth** parameters in the client configuration file. An example is as follows:

```
...  
data-ciphers AES-XXX-GCM # Encryption algorithm  
auth SHAXXX # Authentication algorithm  
...
```

If the parameter settings in the client configuration file are inconsistent with the actual configuration of the server, use either of the following methods to rectify the fault:

- Method 1: Change the encryption algorithm of the server.
 - i. On the **Server** tab page, click  next to **Advanced Settings**, and change the encryption algorithm.

- ii. Download the new client configuration file.
The downloaded client configuration file is **client_config.zip**.
 - iii. Decompress **client_config.zip** to a specified directory, for example, **D:**.
After the decompression, the **client_config.ovpn** and **client_config.conf** files are generated.
 - iv. Open the **client_config.ovpn** file using Notepad or Notepad++.
 - v. Add the client certificate and private key to the file.
Enter the client certificate content and the corresponding private key in between `<cert></cert>` and `<key></key>` tags, respectively. An example is as follows:

```
<cert>
-----BEGIN CERTIFICATE-----
Client certificate content
-----END CERTIFICATE-----
</cert>

<key>
-----BEGIN PRIVATE KEY-----
Client private key
-----END PRIVATE KEY-----
</key>
```
 - vi. Save the .ovpn configuration file.
- Method 2: Modify the client configuration file.
- i. Open the **client_config.ovpn** file using Notepad or Notepad++.
 - ii. Modify the **data-ciphers** and **auth** parameters.

```
...
data-ciphers AES-XXX-GCM # The configured encryption algorithm must be the same
as that of the server.
auth SHAXXX # The configured authentication algorithm must be the same as that
of the server.
...
```
 - iii. Save the .ovpn configuration file.
8. Start the OpenVPN Connect client.
 9. Import the new client configuration file.
 10. Use the client to reconnect to the VPN gateway.
 11. Press **Win+R** and enter **cmd** to open the command window.
 - 12.

 NOTE

XX.XX.XX.XX indicates the private IP address of the ECS to be connected. Replace it with the actual private IP address.

If information similar to the following is displayed, the client can communicate with the ECS:

```
64 bytes from XX.XX.XX.XX: icmp_seq=1 ttl=63 time=1.27 ms
64 bytes from XX.XX.XX.XX: icmp_seq=2 ttl=63 time=1.36 ms
64 bytes from XX.XX.XX.XX: icmp_seq=3 ttl=63 time=1.40 ms
64 bytes from XX.XX.XX.XX: icmp_seq=4 ttl=63 time=1.29 ms
64 bytes from XX.XX.XX.XX: icmp_seq=5 ttl=63 time=1.35 ms
64 bytes from XX.XX.XX.XX: icmp_seq=6 ttl=63 time=1.52 ms
```

If the problem persists, [submit a service ticket](#) to contact Huawei technical support.

4.18 The Client Log Contains "Session invalidated: DECRYPT_ERROR"

Applicable Client

Windows OpenVPN Connect

Symptom



The connection is successful but is interrupted within 1 second. This process repeats continuously, and the following error information is recorded in the client log:

```
Session invalidated: DECRYPT_ERROR
```

Possible Causes


The cipher suite of the client does not match that of the server.

Procedure

1. Log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. Click  in the upper left corner, and choose **Networking > Virtual Private Network**.
4. In the navigation pane on the left, choose **Virtual Private Network > Enterprise - VPN Gateways**.
5. Click the **P2C VPN Gateways** tab. In the P2C VPN gateway list, locate the target P2C VPN gateway, and click **View Server** in the **Operation** column.
6. On the **Server** tab page, view the encryption algorithm and authentication algorithm of the server in the **Advanced Settings** area.
7. Check the **data-ciphers** and **auth** parameters in the client configuration file. An example is as follows:

```
...  
data-ciphers AES-XXX-GCM # Encryption algorithm  
auth SHAXXX # Authentication algorithm  
...
```

If the parameter settings in the client configuration file are inconsistent with the actual configuration of the server, use either of the following methods to rectify the fault:

- Method 1: Change the encryption algorithm of the server.
 - i. On the **Server** tab page, click  next to **Advanced Settings**, and change the encryption algorithm.
 - ii. Download the new client configuration file.
The downloaded client configuration file is **client_config.zip**.
 - iii. Decompress **client_config.zip** to a specified directory, for example, **D:**.

After the decompression, the **client_config.ovpn** and **client_config.conf** files are generated.

- iv. Open the **client_config.ovpn** file using Notepad or Notepad++.
- v. Add the client certificate and private key to the file.

Enter the client certificate content and the corresponding private key in between `<cert></cert>` and `<key></key>` tags, respectively. An example is as follows:

```
<cert>
-----BEGIN CERTIFICATE-----
Client certificate content
-----END CERTIFICATE-----
</cert>

<key>
-----BEGIN PRIVATE KEY-----
Client private key
-----END PRIVATE KEY-----
</key>
```

- vi. Save the .ovpn configuration file.
- Method 2: Modify the client configuration file.
- i. Open the **client_config.ovpn** file using Notepad or Notepad++.
 - ii. Modify the **data-ciphers** and **auth** parameters.

```
...
data-ciphers AES-XXX-GCM # The configured encryption algorithm must be the same
as that of the server.
auth SHAXXX # The configured authentication algorithm must be the same as that
of the server.
...
```

- iii. Save the .ovpn configuration file.
8. Start the OpenVPN Connect client.
 9. Import the new client configuration file.
 10. Use the client to reconnect to the VPN gateway.
 11. Press **Win+R** and enter **cmd** to open the command window.
 - 12.

NOTE

`XX.XX.XX.XX` indicates the private IP address of the ECS to be connected. Replace it with the actual private IP address.

If information similar to the following is displayed, the client can communicate with the ECS:

```
64 bytes from XX.XX.XX.XX: icmp_seq=1 ttl=63 time=1.27 ms
64 bytes from XX.XX.XX.XX: icmp_seq=2 ttl=63 time=1.36 ms
64 bytes from XX.XX.XX.XX: icmp_seq=3 ttl=63 time=1.40 ms
64 bytes from XX.XX.XX.XX: icmp_seq=4 ttl=63 time=1.29 ms
64 bytes from XX.XX.XX.XX: icmp_seq=5 ttl=63 time=1.35 ms
64 bytes from XX.XX.XX.XX: icmp_seq=6 ttl=63 time=1.52 ms
```

If the problem persists, [submit a service ticket](#) to contact Huawei technical support.

4.19 The Client Log Contains "Unrecognized option or missing or extra parameter(s) in xxx.ovpn:108: data-ciphers (2.4.12)"

Applicable Client

Linux

Symptom



A client cannot connect to the VPN gateway, and the client log contains the following error message:

```
Unrecognized option or missing or extra parameter(s) in xxx.ovpn:108: data-ciphers (2.4.12)
```

Possible Causes

The client OpenVPN 2.4.12 cannot identify the configuration items **data-ciphers** and **disable-dco**.

Procedure

1. On Windows, log in to the management console.
2. Click  in the upper left corner and select the desired region and project.
3. Click  in the upper left corner, and choose **Networking > Virtual Private Network**.
4. In the navigation pane on the left, choose **Virtual Private Network > Enterprise – VPN Gateways**.
5. Click the **P2C VPN Gateways** tab, and click **Download Client Configuration** in the **Operation** column of the target VPN gateway.
The downloaded client configuration file is **client_config.zip**.
6. Decompress **client_config.zip** to a specified directory, for example, **D:**.
After the decompression, the **client_config.ovpn** and **client_config.conf** files are generated.
7. Open the **client_config.conf** file using Notepad or Notepad++.
8. Configure the client configuration file.
 - a. Add the client certificate and private key to the file.

Enter the client certificate content and the corresponding private key in between `<cert></cert>` and `<key></key>` tags, respectively. An example is as follows:

```
<cert>
-----BEGIN CERTIFICATE-----
Client certificate content
-----END CERTIFICATE-----
</cert>

<key>
```

```
-----BEGIN PRIVATE KEY-----
Client private key
-----END PRIVATE KEY-----
</key>
```

- b. Enter **#** in front of the lines where **data-ciphers** and **disable-dco** are located to comment out the lines.

```
...
...
# data-ciphers AES-XXX-XXX
...
...
# disable-dco
...
...
```

9. Save the .conf configuration file.
10. Upload the .conf configuration file to the Linux operating system using Xftp. In this example, the file is uploaded to the **/opt/** directory.
11. On Linux, run the following command to go to the directory where the client configuration file is stored:

```
cd /opt/
```

12. Run the following command to start the OpenVPN client and connect to the VPN gateway:

```
openvpn --config /opt/openvpn_config_user-01.conf
```

If the following information in bold is displayed, the OpenVPN connection is successfully established:

```
2025-02-27 19:22:41 Note: Kernel support for ovpn-dco missing, disabling data channel offload.
2025-02-27 19:22:41 OpenVPN 2.6.12 x86_64-pc-linux-gnu [SSL (OpenSSL)] [LZO] [LZ4] [EPOLL]
[PKCS11] [MH/PKTINFO] [AEAD] [DCO]
2025-02-27 19:22:41 library versions: OpenSSL 3.3.1 4 Jun 2024, LZO 2.10
...
...
...
2025-02-27 19:22:42 Initialization Sequence Completed
...
...
```

- 13.

 **NOTE**

XX.XX.XX.XX indicates the private IP address of the ECS to be connected. Replace it with the actual private IP address.

If information similar to the following is displayed, the client can communicate with the ECS:

```
64 bytes from XX.XX.XX.XX: icmp_seq=1 ttl=63 time=1.27 ms
64 bytes from XX.XX.XX.XX: icmp_seq=2 ttl=63 time=1.36 ms
64 bytes from XX.XX.XX.XX: icmp_seq=3 ttl=63 time=1.40 ms
64 bytes from XX.XX.XX.XX: icmp_seq=4 ttl=63 time=1.29 ms
64 bytes from XX.XX.XX.XX: icmp_seq=5 ttl=63 time=1.35 ms
64 bytes from XX.XX.XX.XX: icmp_seq=6 ttl=63 time=1.52 ms
```

4.20 When a User Uses a Federated Account to Log in to the Client, the Browser Displays the Error Message "The user does not have the vpn:system:loginP2cVpnBySSO permission. Contact the administrator to add the permission."

Symptom

When a user uses an existing federated account to log in to the client, the browser displays a message indicating that the authentication fails.



Error message: The user does not have the vpn:system:loginP2cVpnBySSO permission. Contact the administrator to add the permission.

Possible Causes

The current user does not have the vpn:system:loginP2cVpnBySSO permission.

Procedure

Contact the administrator to add the **VPN SSOAccessPolicy** permission. The procedure is as follows:

- Step 1** Log in to the management console.
- Step 2** Click  in the upper left corner and select the desired region and project.
- Step 3** Click  in the upper left corner of the page, and choose **Management & Governance > Identity and Access Management**.
- Step 4** Choose **User Groups** from the navigation pane.
- Step 5** Click **Authorize** in the **Operation** column of the created user group.
- Step 6** In the search box in the upper right corner, search for **VPN SSOAccessPolicy** and select it.
- Step 7** Click **Next** and select the authorization scope as required.
- Step 8** Click **OK**.

----End

5 Successful Client Connection but Unavailable Services

5.1 A Client Cannot Ping the Private IP Address of an ECS

Symptom

A client is connected to a P2C VPN gateway, but cannot ping the private IP address of an ECS.

Possible Causes

- Ping detection is disabled on the client device or ECS.
- Ping detection packets are denied by a security group of the ECS.
- The local CIDR block of the VPN gateway does not contain the private IP address of the ECS to be accessed.
- The user group to which the user belongs is not configured, or the user group is not configured with the corresponding access policy.
- After the specified IP address of a client is changed and the client automatically reconnects to the server, the route to the local subnet is not generated in the routing table on the Windows operating system.

Procedure

1. Check whether ping detection is disabled in an access control policy of the client device or ECS.
If so, modify the policy to permit ping detection. For the Windows operating system, you also need to modify the inbound rules of the firewall to permit ICMPv4-In.
2. Verify that the inbound and outbound rules in the ECS's security group permit ICMP packets.
3. Verify that the local CIDR block includes the private IP address of the ECS to be accessed.

- a. On the **Server** tab page of the VPN gateway, modify the local CIDR block.
- b. Disconnect the client and reconnect it.
- c. Check whether the client device can receive routes advertised by the VPN gateway.
 - On the Windows operating system, run the **route print** command.
 - On the Linux operating system, run the **ip route show all** command.
4. Ensure that the user group to which the user belongs and the access policy have been configured in user management.

The destination CIDR block of the access policy needs to include the private IP address of the ECS to be accessed.
5. Verify that the local CIDR block and client address pool configured on the server meet the following requirements:
 - Local CIDR block: 192.168.1.XX
 - Client address pool: 172.16.0.0
6. On the client, check whether the route to the local CIDR block is generated.
 - If the route is generated, the IP address assigned to the client is 172.16.0.5.

The command output is as follows:

IPv4 Routing Table

=====

Active Routes:

Network	Destination	Netmask	Gateway	Interface	Metric
192.168.1.XX	255.255.255.0	172.16.0.0	172.16.0.5	281	
192.168.2.XX	255.255.255.0	172.16.0.0	172.16.0.5	281	
192.168.3.XX	255.255.255.0	172.16.0.0	172.16.0.5	281	

=====

- If the route is not generated, disconnect the client and reconnect it.

If the problem persists, [submit a service ticket](#) to contact Huawei technical support.

5.2 Packet Loss Occurs During Service Access

Symptom

A client is connected to a P2C VPN gateway, but packet loss occurs during service access.

Possible Causes

- Service traffic bursts or continuously exceeds the bandwidth of the VPN gateway instance.
- The bandwidth of the EIP bound to the VPN gateway is insufficient.
- The quality of the Internet is poor.

Procedure

1. Go to the traffic monitoring view from the VPN gateway list page, and check whether traffic bursts or continuously approaches the bandwidth specification of the VPN gateway.

2. On the **Basic Information** page of the VPN gateway, view the EIP bandwidth, and check whether traffic exceeds the EIP bandwidth based on the traffic information in the traffic monitoring view.
If the traffic exceeds the EIP bandwidth, increase the EIP bandwidth.
3. Ping the public IP address of the VPN gateway from the client to detect the Internet link quality.
If the quality of the Internet link is poor, contact the carrier to resolve the problem.

5.3 Client Traffic Is Interrupted, and an Error Message Is Displayed During Connection Establishment

Applicable Client

OpenVPN GUI

Symptom

The client is successfully connected, but cannot ping the IP address of an ECS. When the OpenVPN GUI client is restarted, the following message is displayed: "OPENVPNServiceInteractive" is not started. The log contains the following error information:

```
ERROR: route addition failed using CreatelpForwardEntry: access denied
```

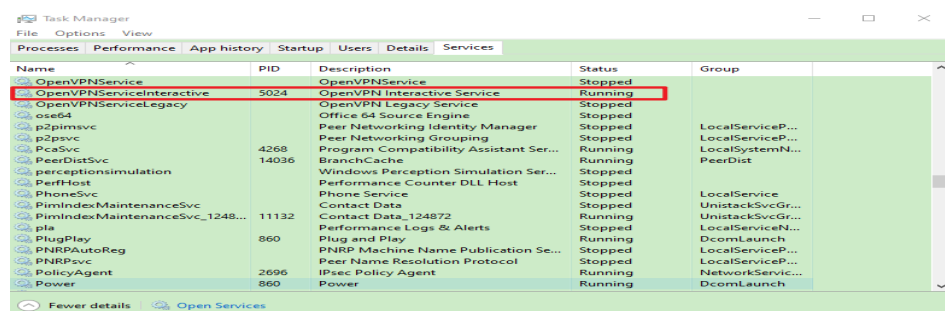
Possible Causes

The OpenVPN client software is not running properly.

Procedure

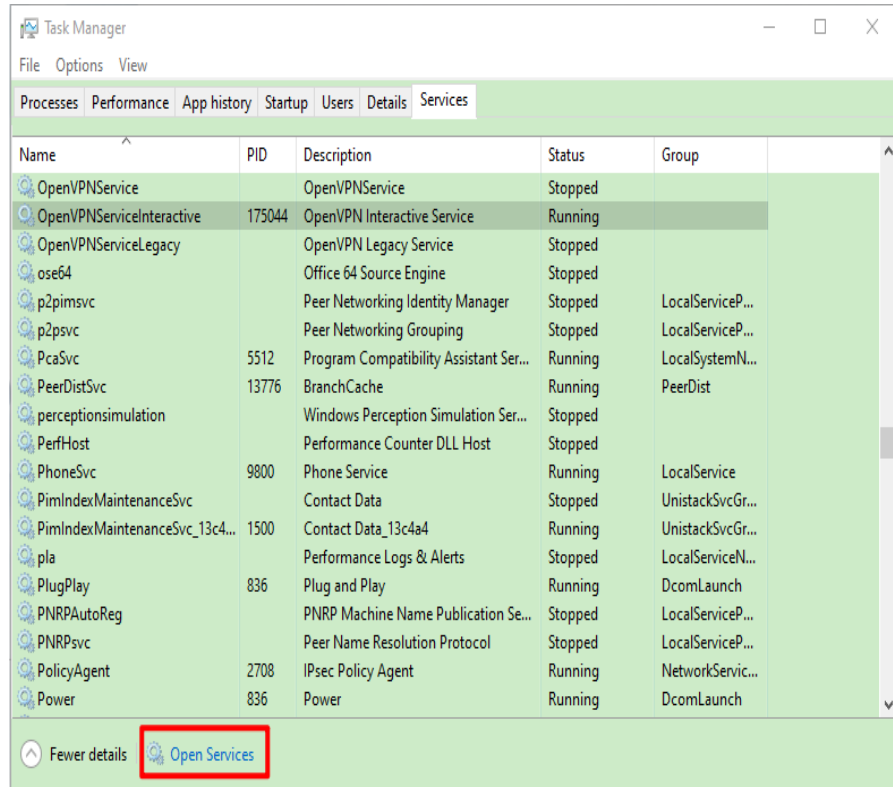
1. Enter **Task Manager** in the taskbar search box, and click **Task Manager** to open it.
2. Click the **Services** tab, find the OPENVPNServiceInteractive service, and check its running status, as shown in [Figure 5-1](#).

Figure 5-1 Task Manager



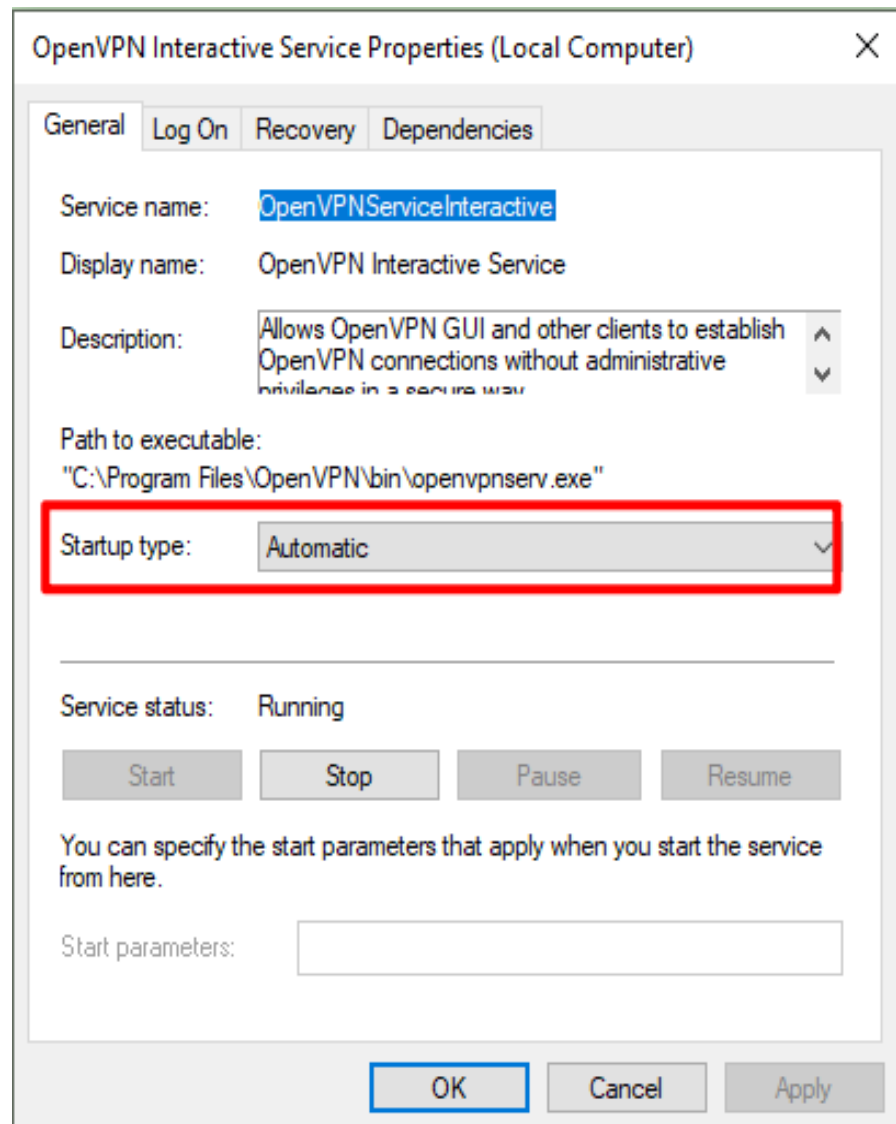
- If the service is running properly, go to step [3](#).

- If the service is stopped, perform the following operations to change the startup type of the service:
 - i. Right-click the service and choose **Start** to start the service.
 - ii. Click **Open Services** in the lower part of the Task Manager, as shown in [Figure 5-2](#).

Figure 5-2 Open Services

- iii. Find the OpenVPN Interactive Service, right-click it, and choose **Properties** from the shortcut menu.
- iv. Change the **Startup type** value of the service to **Automatic**, as shown in [Figure 5-3](#).

Figure 5-3 Changing the startup type



- v. Click **OK**.
3. Disconnect the OpenVPN GUI client and reconnect it.

6 S2C Classic VPN

6.1 Common Check Items

VPN connections or ping operations fail when configurations (such as the negotiation policy, firewall, route table, interzone policy, NAT configuration, and security group) are incorrect.

Check the following configurations.

- [Checking the Negotiation Information on Both Sides of a VPN Connection](#)
- [Checking the Firewall Configuration on Your Local Network and the Security Group Configuration on the Cloud](#)
- [Checking the Firewall Route Table](#)
- [Checking the Firewall Inter-zone Policy](#)
- [Checking the NAT Configurations on the Firewall](#)

Checking the Negotiation Information on Both Sides of a VPN Connection

- Ensure that the PSKs of the two sides are the same.
- Ensure the IKE policies and the IPsec policies of the two sides are the same.
- Local and remote subnets are matched pairs.

Checking the Firewall Configuration on Your Local Network and the Security Group Configuration on the Cloud

- Ensure that data packets from your network to the VPC subnet on Huawei Cloud are permitted.
- Ensure that data packets from the VPC subnet on Huawei Cloud to your network are permitted.

Checking the Firewall Route Table

Verify that there is a route to the VPC subnet on Huawei Cloud.

- Ensure that a route table contains a route to the target network on Huawei Cloud.

- Ensure that the forwarding table of the route works properly.

 **NOTE**

Incorrect route configurations:

1. The destination CIDR block is different from the VPC CIDR block. In this case, traffic destined for Huawei Cloud cannot be routed to the public network interface configured with the IPsec policy.
2. The outbound interface rather than the next hop is specified when configuring a static route.

On an Ethernet network, the outbound interface cannot learn the ARP entries from the remote side, leading to route forwarding failure.

3. The VPN gateway address on Huawei Cloud is specified as the next hop of the route.

Some third-party devices do not support automatic route recursion. VPN traffic is sent from the public network interface. Therefore, the next hop must be the gateway address provided by the carrier.

Checking the Firewall Inter-zone Policy

- From the Trust zone to the Untrust zone: Allows access from your local network to the VPC subnet on the cloud.
- From the Untrust zone to the Trust zone: Allows access from the VPC on the cloud to your local network.

Checking the NAT Configurations on the Firewall

Check whether the local VPN gateway is behind the NAT device (usually the border firewall). That is, the outbound interface of the VPN gateway uses a private IP address, and then it is translated into a public IP address by the NAT device.

This scenario is also called IPsec NAT traversal.

6.2 Common Configuration Issues and Solutions

- Inconsistent PSKs: PSK update takes effect in the next IKE negotiation. Ensure that the PSKs at both ends are the same.
- Inconsistent negotiation policies: Check the authentication algorithm, encryption algorithm, version, DH algorithm, and negotiation mode in the IKE policy, and the authentication algorithm, encryption algorithm, encapsulation format, and PFS algorithm in the IPsec policy. Ensure the PFSs at both ends are the same. By default, the PFS configuration is disabled on some devices.
- Interesting traffic: Check the ACL configurations at both ends. The actual IP address and mask must be used.
- NAT configuration: Do not perform NAT on the on-premises subnet that is used to access the cloud.
- Security policies: Allow all protocols used by the on-premises subnet to access the cloud subnet, and allow two public IP addresses to communicate on UDP port 500 and UDP port 4500 using ESP or AH.
- Route configurations: Set the outbound interface for accessing the cloud subnet to the tunnel interface or IPsec negotiation interface. Ensure that the next-hop ARP resolution of the outbound interface is reachable.

For more information, see [Connection or Ping Failure](#).