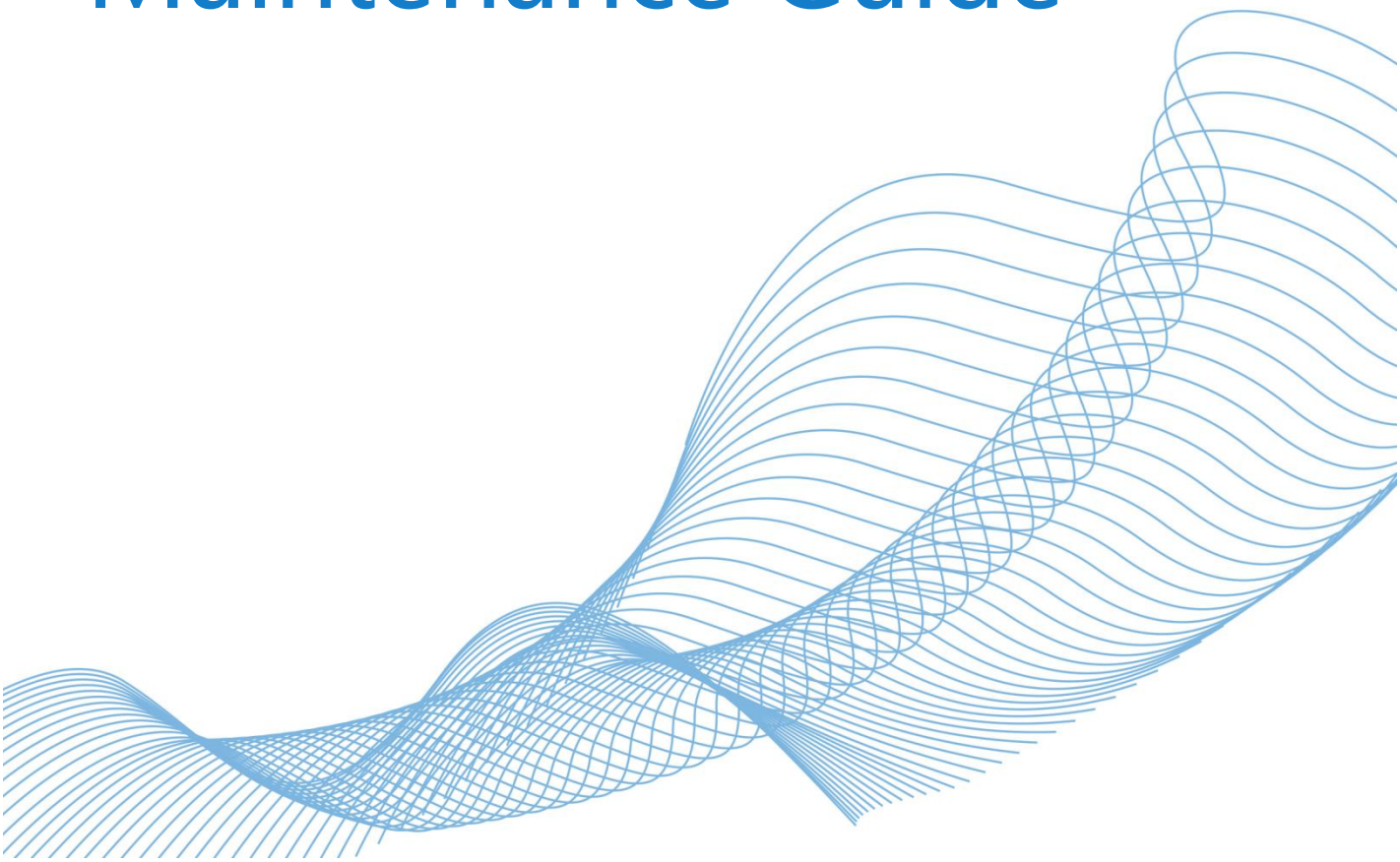
联软科技
LEAGSOFT

LeagSoft UniVPN Client

Maintenance Guide



Contents

1 Troubleshooting:SSLVPN

1.1 Overview

This document describes the most common solutions to SSL VPN faults, including SecoClient dialup faults, browser dialup faults, as well as FAQs. It helps you troubleshoot faults before contacting Huawei technical support.

1.2 Precautions

- It is recommended that you learn about the basic SSL VPN configurations of Huawei firewalls before using them.
- This document uses Huawei USG6000 series V5 firewalls as an example. The implementation may vary according to products and versions.
- In this document, FW is short for firewall.
- The public IP addresses used in this document are for reference only and have no substantial meanings.

1.3 List of SSL VPNs

1.3.1 SSL VPN Access Mode

Access Mode	Description
UniVPN	The UniVPN is client software provided by Leagsoft for remote VPN access. It provides secure and convenient access services for mobile office users to remotely access an enterprise network. SSL VPN provides web proxy, port forwarding, file sharing, and network extension services. The UniVPN client supports only network extension services.

1.4 Troubleshooting Guidelines for SSL VPN Dial-up Failures on UniVPN_V500R005C20 & V600R007C20

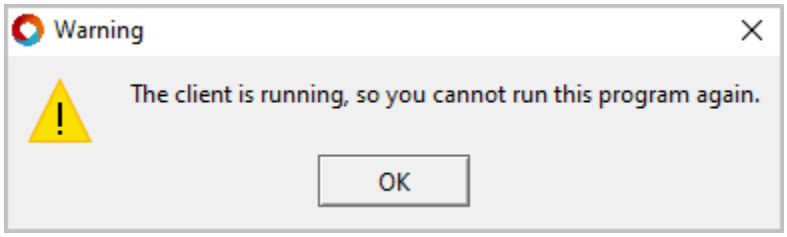
This chapter introduces the troubleshooting methods for dialing SSL VPN when UniVPN clients access firewall devices V500R005C20, V600R007C20, and later versions.

1.4.1 Troubleshooting Guidelines for Warnings Displayed on the UniVPN

1.4.1.1 Warning: The client is running, so you cannot run this program again.

Symptom

Warning: The client is running, so you cannot run this program again.

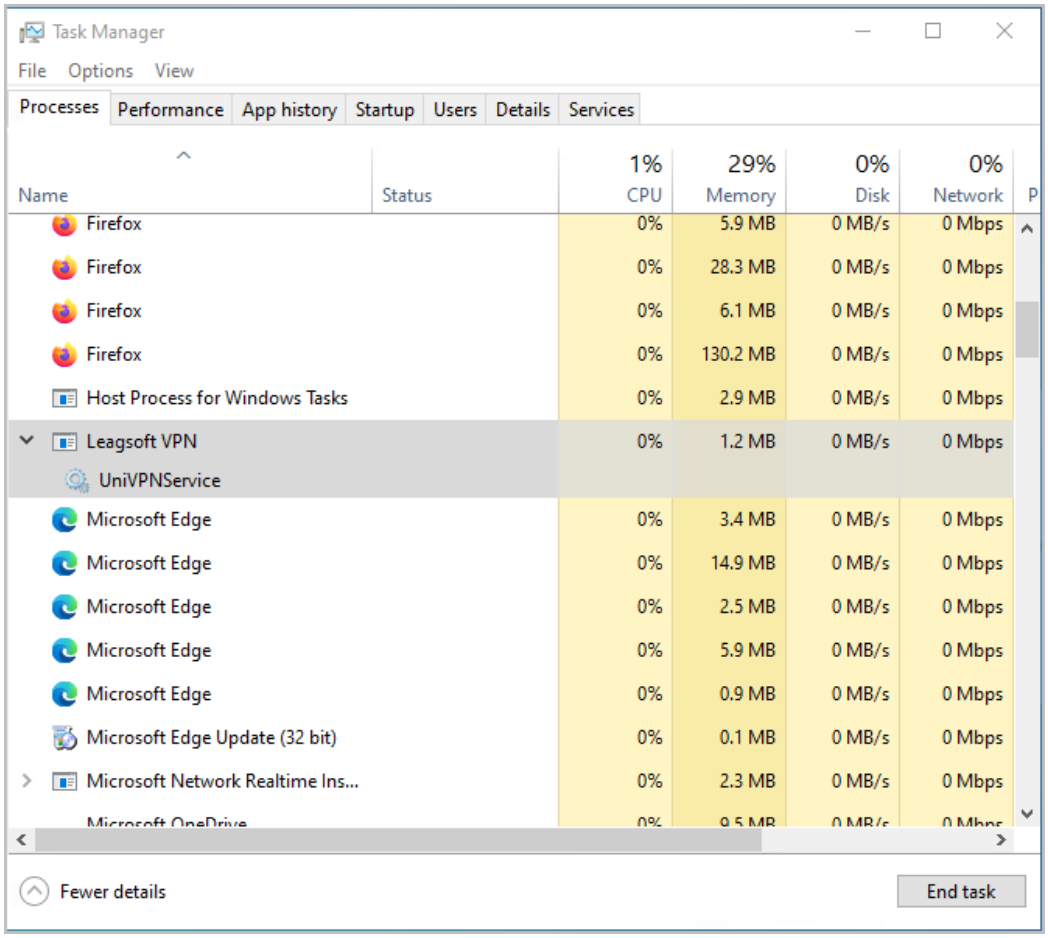


Possible Causes

The UniVPN is running.

Procedure

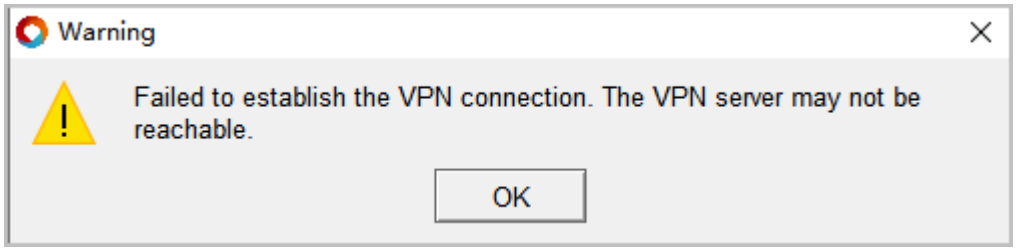
Close the existing UniVPN program and the browser that uses the SSL VPN service, and check whether the UniVPN.exe process in the task manager is disabled.



1.4.1.2 Warning: Failed to establish the VPN connection. The VPN server may not be unreachable.

Symptom

When the VPN gateway is connected, the system displays "Failed to establish the VPN connection. The VPN server may not be unreachable."



Possible Causes

1. The UniVPN is unreachable to the VPN gateway.
2. The IP address or port number of the VPN gateway on the UniVPN is incorrect.
3. The UniVPN version does not match the VPN gateway version.

4. When a device accesses the Internet through a proxy server (for example, 192.168.253.188), the VPN gateway of the public network is not configured for the UniVPN.

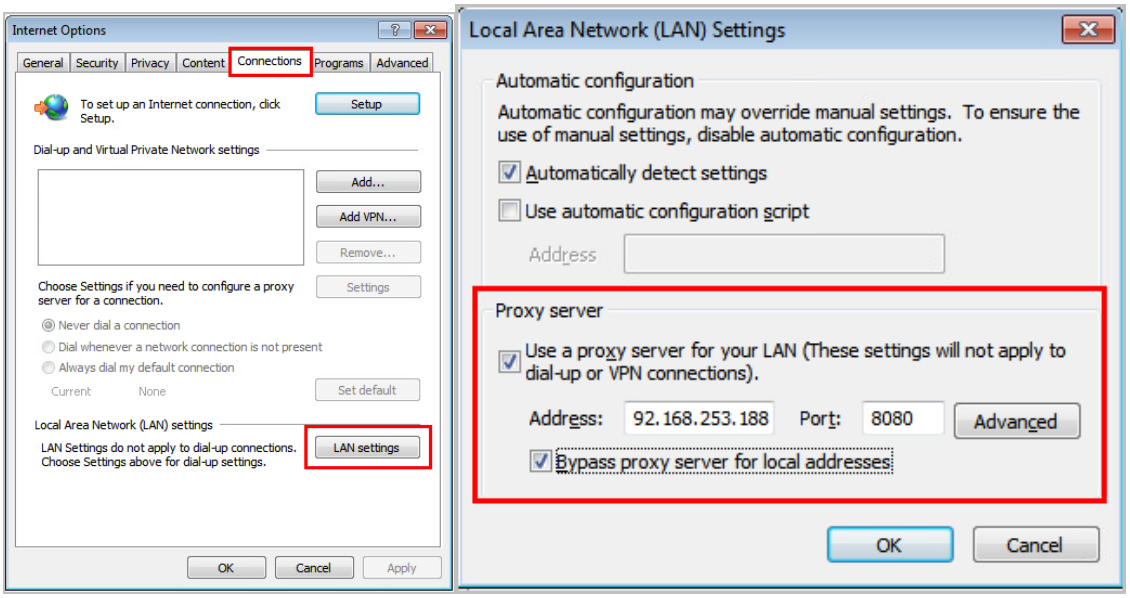
Procedure

- Fault location and troubleshooting for cause 1
  1. On the device where the UniVPN is installed, check whether the IP address of the VPN gateway can be pinged.
  2. If the route is unreachable, configure a route from the UniVPN to the VPN gateway. If the route is reachable, analyze cause 2.
- Fault location and troubleshooting for cause 2

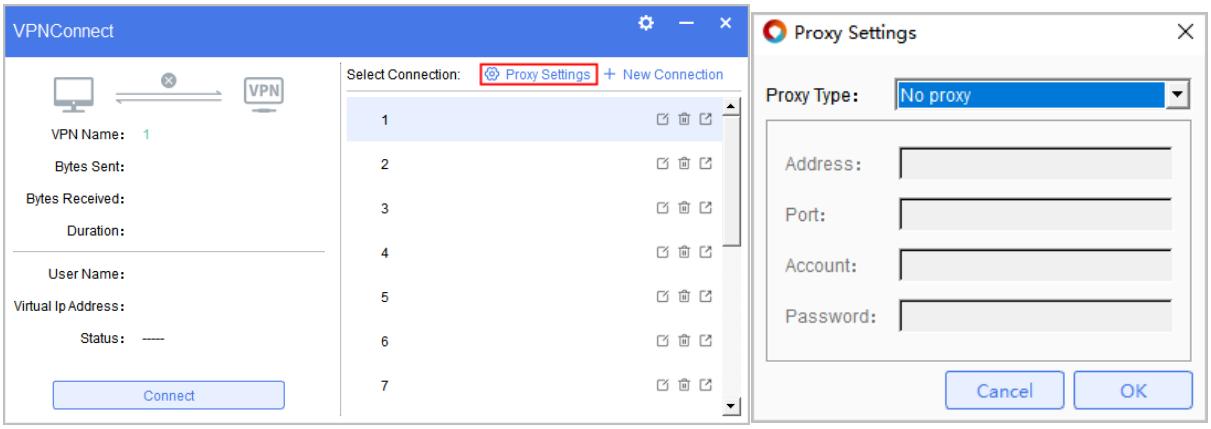
  Check whether the IP address and port number of the VPN gateway configured on the UniVPN are the same as those configured on the VPN gateway.
- Fault location and troubleshooting for cause 3

  Currently, the VPN gateway software versions that match the UniVPN are FW V500R001C20, FWV100R001C30SPC900, SVN V200R003C10SPC900, and their later versions.
- Fault location and troubleshooting for cause 4

  Check whether the device accesses the Internet through the proxy server.



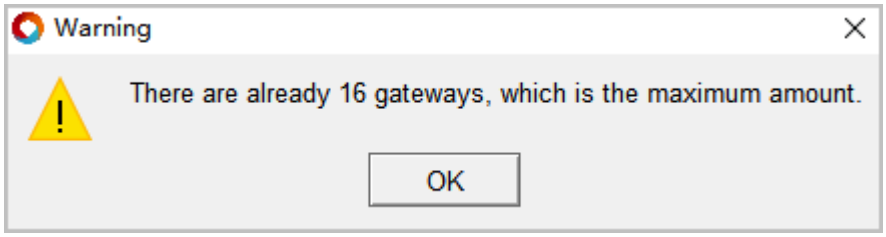
If yes, set proxy parameters on the UniVPN, as shown in the following figure.



1.4.1.3 Warning: There are already 16 gateways, which is the maximum amount.

Symptom

On the new connection page of the UniVPN, after 16 gateway addresses are entered in the remote gateway text box and **Add** is clicked, the system displays "Warning: There are already 16 gateways, which is the maximum amount."



Possible Causes

On the new connection page of the client, 16 remote gateways have been added, reaching the maximum number of allowed gateways.

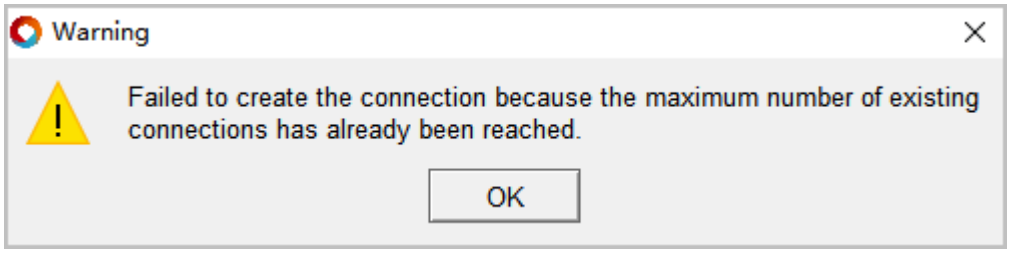
Procedure

After the number of remote gateways reaches 16, do not add any gateway address.

1.4.1.4 Warning: Failed to create the connection because the maximum number of existing connections has already been reached.

Symptom

On the UniVPN home page, add 16 VPN connections and click **+**. The system displays "Warning: Failed to create the connection because the maximum number of existing connections has already been reached."



Possible Causes

On the home page of the client, 16 connections have been added, reaching the maximum number of allowed connections.

Procedure

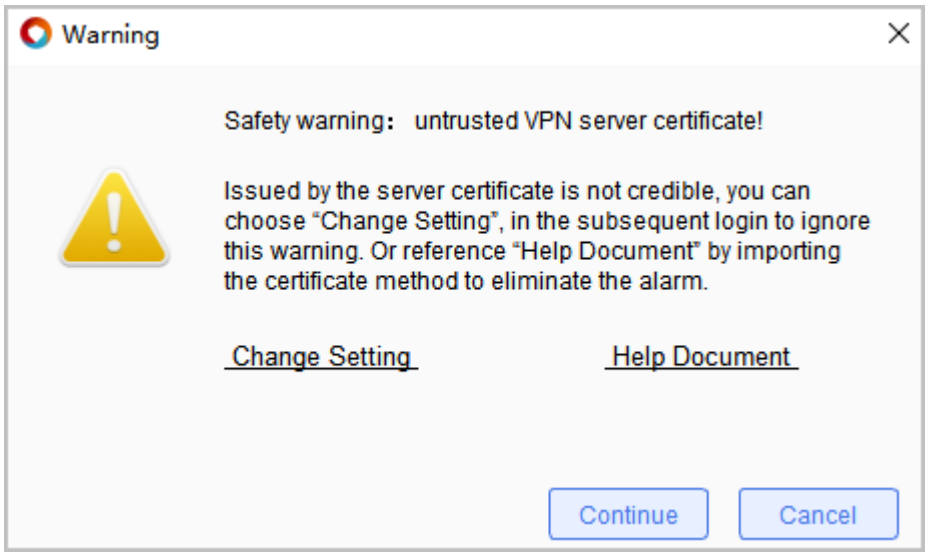
After 16 connections are added, do not add any connection.

1.4.2 Troubleshooting Guidelines for Warnings Displayed During User Name/Password-based Login

1.4.2.1 Warning: untrusted VPN server certificate

Symptom

When you use the UniVPN to log in to the SSL VPN virtual network through the SSL VPN tunnel, the following information is displayed:



Possible Causes

The CA certificate for authenticating the virtual gateway is unavailable on the UniVPN.

Procedure

To clear the warning, use either of the following operation methods:

- Click Change Setting and deselect Block connections to untrusted servers.

  This method can be used when you are sure about the authenticity of the virtual gateway.
- Issue certificates for the UniVPN and virtual gateway.

  This method is recommended when you are not sure about the authenticity of the virtual gateway.

Create two certificates. Place one device certificate on the virtual gateway, and place the other CA certificate on the host where the UniVPN resides. If your enterprise has a certificate system, you can use your own system to create certificates. If no certificate system is available, you can use XCA software to create certificates.

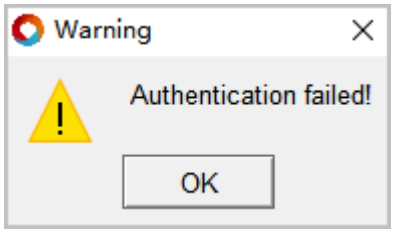
When you use the UniVPN to log in to a virtual gateway through an SSL VPN tunnel, the virtual gateway pushes the device certificate to the UniVPN. The system will not prompt certificate invalidity if the CA certificate on the UniVPN identifies the device certificate of the virtual gateway.

For details about how to create a certificate, How Do I Use XCA to Create Device Certificates and User Certificates?.

1.4.2.2 Warning: Authentication failed

Symptom

After you enter the user name and password and click Login on the UniVPN login page, the system displays "Authentication failed."



Possible Causes

1. The user name or password is incorrect, the user account expires, or the user is locked out.
2. The virtual gateway is bound to an incorrect authentication domain.
3. SSL VPN access is not enabled for authentication domains.
4. The network extension feature is not enabled on the virtual gateway.
5. The SSL VPN login device is in a dual standby state (HRP_S), but SSL VPN does not support login on the standby device.
6. The SSL VPN virtual gateway is not exclusive but shared.
7. The authentication server is configured for the authentication domain, and Prohibit new user login is selected for the new user authentication option, but the user does not exist locally.

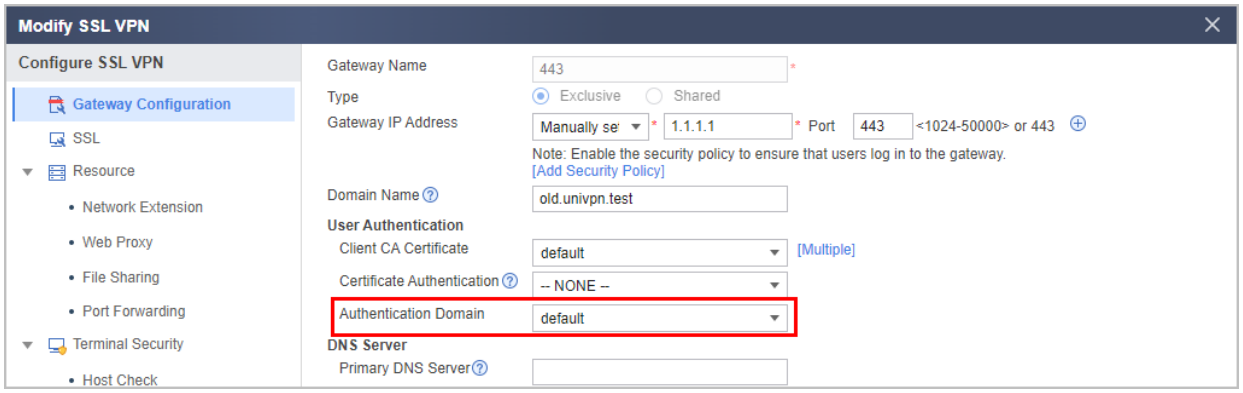
8. The AD/LDAP authentication server is configured for the authentication domain, and Force Password Change upon First Login is enabled on the server.
9. The metric value (hop count) of the route from the client to the server exceeds 1024.

Procedure

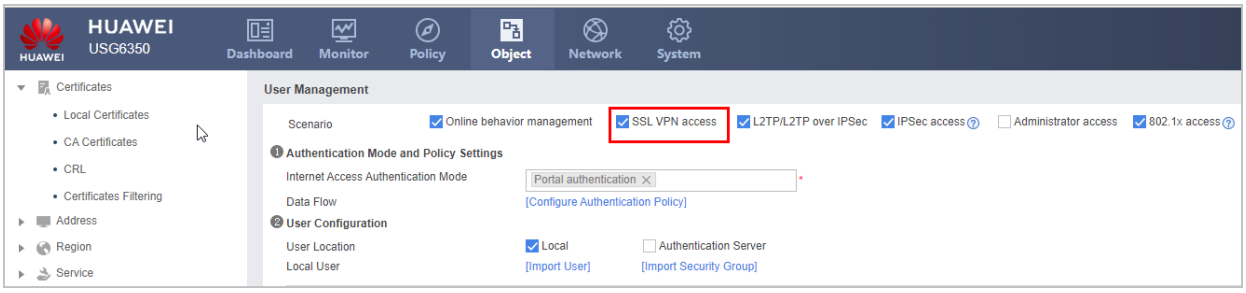
1. Log in to the device and check that the user name and password are correct and that the user does not expire or is not locked.

```
[sysname]display user-manage user verbose name user001
 2021-03-30 14:51:04.970 +08:00
 Current total number: 1
 --------------------------------------------------------------------------------
   User Name              : user001
   Password Config        : Yes
   Password               : OW7Q30GlNMDu2NS8ufuBIAAAAAALKhc4
   Parent Group           : /default
   Bind Mode              : Unidirectional     State                : Locked
   Expiration Time        : Unlimited
   Multi-IP Login         : Enabled
   User Type              : Created By Manager
   Vsys                   : public
 --------------------------------------------------------------------------------
 [sysname]
```

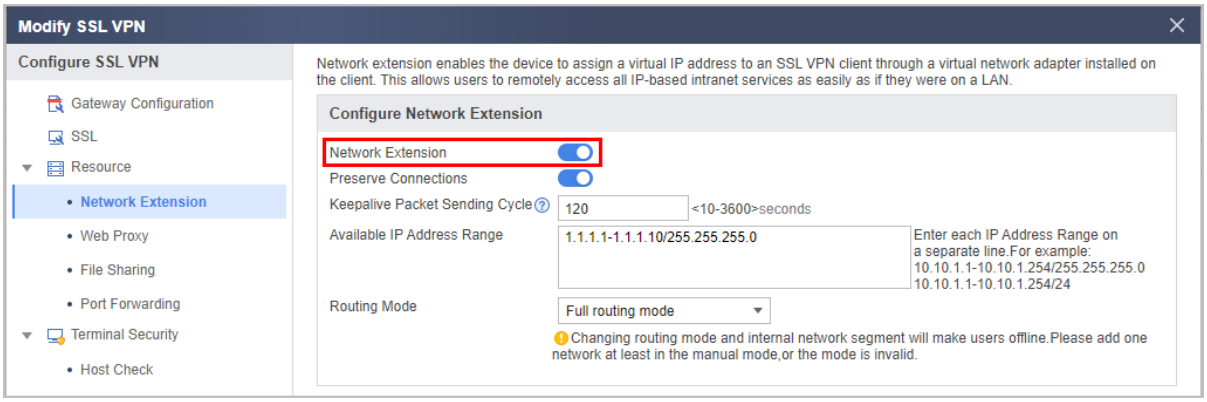
2. Check whether the correct authentication domain is bound to the virtual gateway.



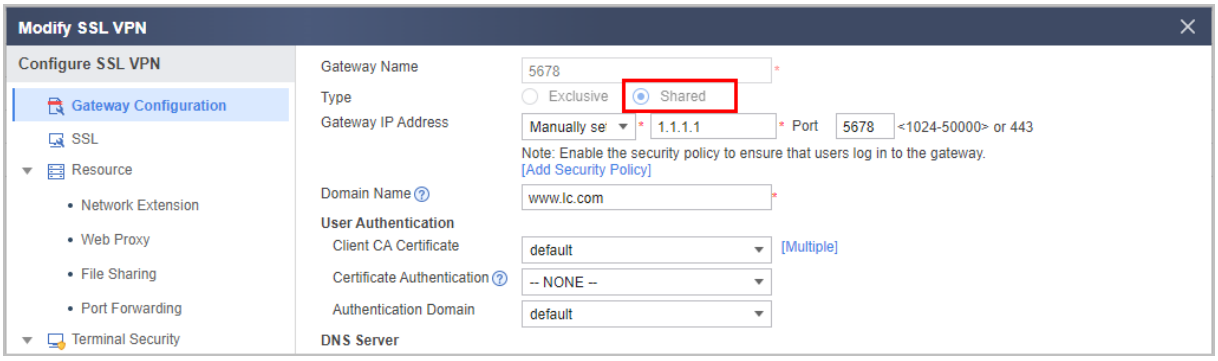
3. Check whether SSL VPN access is enabled in the authentication domain.



4. Check whether the network extension service of the virtual gateway is enabled.



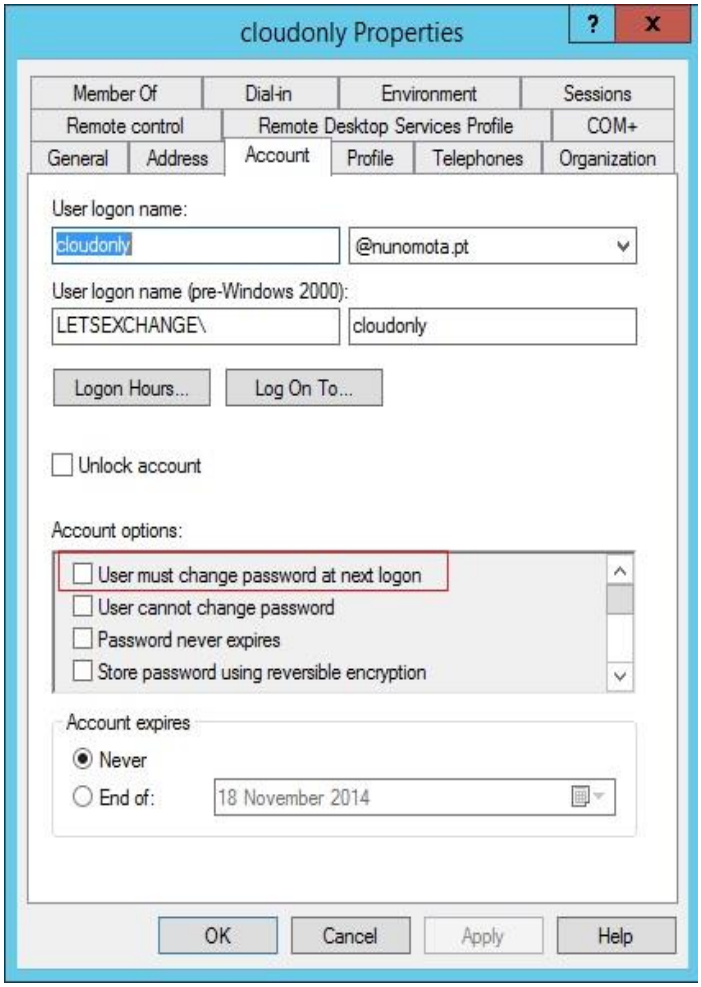
5. SSL VPN cannot be applied in load-balancing networking. Modify the configuration or networking to ensure that the SSL VPN login device is in the HRP_M state.
6. Check whether the SSL VPN virtual gateway must be shared. If not, delete the virtual gateway and create an exclusive virtual gateway.



7. Click the CLI console and enter the AAA authentication domain view. Run the display this command to check whether the new-user deny-authentication configuration exists in the authentication domain. If yes, run the undo new-user command to delete the configuration.

```
[sysname]aaa
[sysname-aaa]domain default
Info: The domain default is for common users.
[sysname-aaa-domain-default]dis this
2021-04-12 15:05:35.600 +8:00
#
domain default
service-scheme webServerScheme1530599131778
service-type internetaccess ssl-vpn
internet-access mode single-sign-on
reference user current-domain
new-user deny-authentication
#
return
[sysname-aaa-domain default]
```

8. Log in to the AD/LDAP server and check whether Force Password Change upon First Login is enabled. If yes, select Disable.



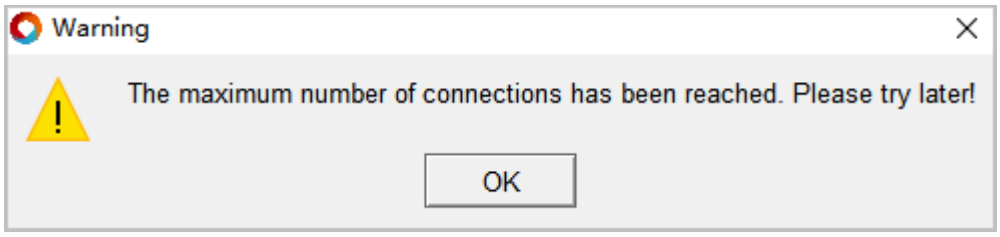
9. Check whether the metric value of the route to the server exceeds 1024. If yes, change the metric value of the route.

```
sugon@sugon-os:~/桌面$ route -n
内核 IP 路由表
目标            网关            子网掩码        标志  跃点   引用  使用 接口
0.0.0.0         10.18.11.254    0.0.0.0         UG    13392  0        0 enp1s0
10.18.11.0      0.0.0.0         255.255.255.0   U     100    0        0 enp1s0
10.20.2.96      10.18.11.254    255.255.255.255 UGH   100    0        0 enp1s0
169.254.0.0     0.0.0.0         255.255.0.0     U     1000   0        0 enp1s0
sugon@sugon-os:~/桌面$ sudo route del default gw 10.18.11.254
sugon@sugon-os:~/桌面$ sudo route add -net 0.0.0.0 gw 10.18.11.254 netmask 0.0.0.0  metric 0 enp1s0
sugon@sugon-os:~/桌面$ route -n
内核 IP 路由表
目标            网关            子网掩码        标志  跃点   引用  使用 接口
0.0.0.0         10.18.11.254    0.0.0.0         UG    0      0        0 enp1s0
10.18.11.0      0.0.0.0         255.255.255.0   U     100    0        0 enp1s0
10.20.2.96      10.18.11.254    255.255.255.255 UGH   100    0        0 enp1s0
169.254.0.0     0.0.0.0         255.255.0.0     U     1000   0        0 enp1s0
sugon@sugon-os:~/桌面$
```

1.4.2.3 Warning: The maximum number of connections has been reached. Please try later.

Symptom

After you enter the user name and password and click Login on the UniVPN login page, the system displays "The maximum number of connections has been reached. Please try later."



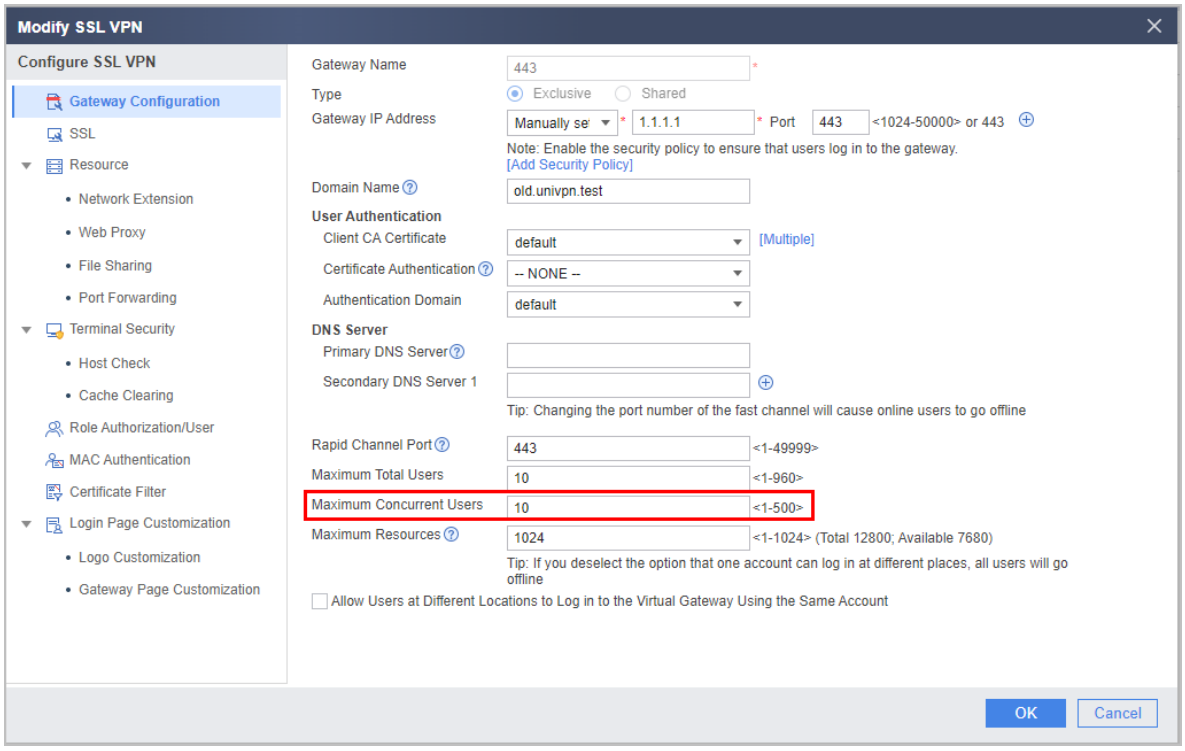
Possible Causes

1. The number of online SSL VPN users has reached the upper limit configured on the virtual gateway.
2. The public account function is enabled on the virtual gateway, and the number of online users using this account has reached the upper limit.

Procedure

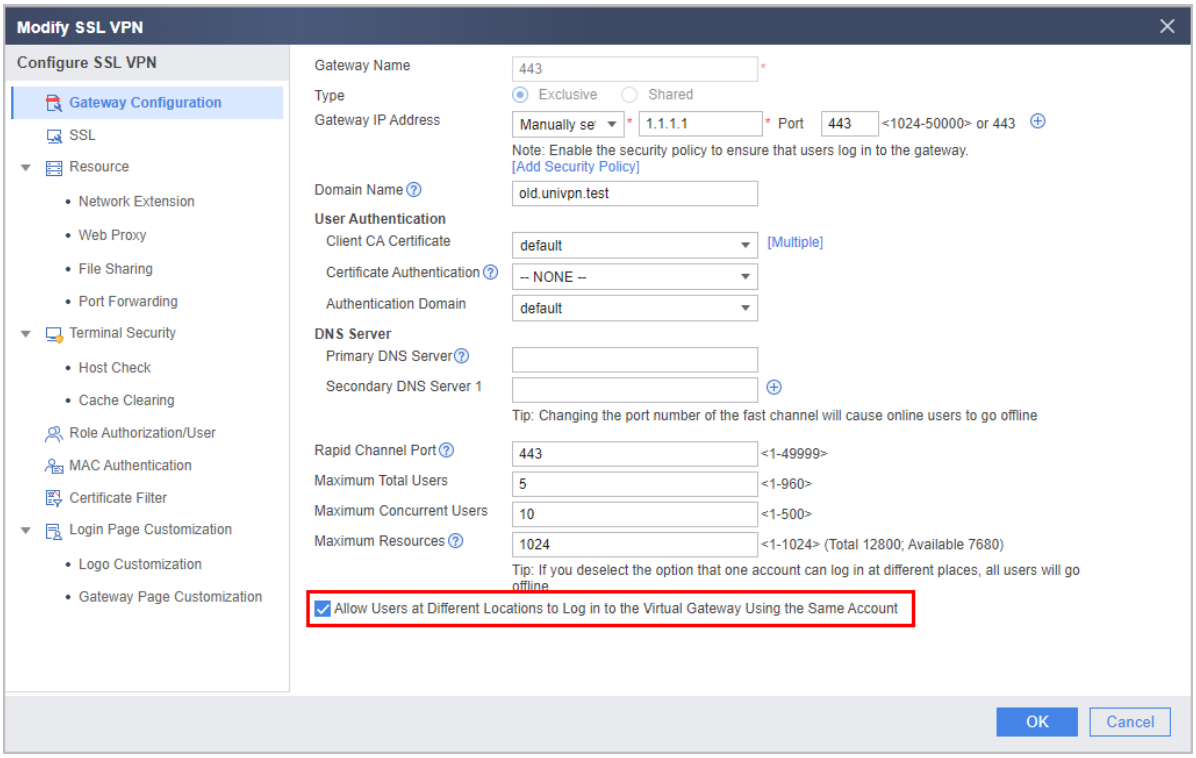
- Fault location and troubleshooting for cause 1

  Log in to the virtual gateway. Choose Network > SSL VPN > SSL VPN, and click the name of the virtual gateway. Check whether the maximum number of concurrent users allocated to the virtual gateway is proper. If not, modify the configuration.Fault location and troubleshooting for cause 1



- Fault location and troubleshooting for cause 2

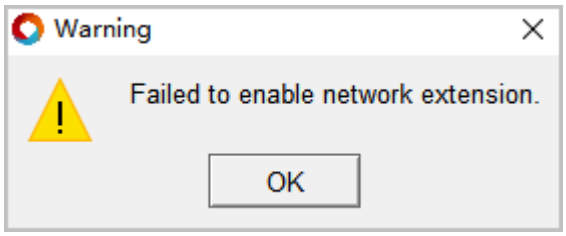
  Check the maximum number of online users. If the login request is normal, increase the maximum number of online users.



1.4.2.4 Warning: Failed to enable network extension

Symptom

After you enter the user name and password and click Login on the UniVPN login page, the system displays "Failed to enable network extension."



Possible Causes

1. The IP addresses in the network extension address pool of the virtual gateway have been used up.
2. The network extension client IP address of the virtual gateway is obtained from the external server, but Third-party server authorization scheme is not configured for the authentication domain.

Procedure

1. Start the CLI console, enter the service view of the virtual gateway, and run the display network-extension [ip] command to check the configuration and allocation of the network extension address pool. If all IP addresses in the address pool have been allocated, increase the number of addresses in the address pool based on service requirements.

```
[sysname-sslvpn-service] display network-extension  VG Network Extension Information
---------------------------                                  Network Extension State:
enable                                          Keep Alive State:          enable
Keep Alive Interval:          120(seconds)                                  Log State:
disable                                         Point to Point State:      disable
VIP Method:                   net pool assign   default net pool:          3.3.3.100
Route Mode:                   manual   Intranet IP/Mask:                   3.3.3.0/255.255.255.0   Intranet
IP/Mask:                192.168.1.0/255.255.255.0                          ----------------------------
Virtual IP Pool:                                                           NO.          Start-IP
End-IP                  Mask                  Alias
------------------------------------------------------------------------   1          3.3.3.100          3.3.3.200
255.255.255.0           3.3.3.100  ------------------------------------------------------------------------   ----End
[sysname-sslvpn-service] display network-extension ip                                  Client IP
Allocation                                                                 --------------------
NO.     User                                IP              Time of fetching IP
------------------------------------------------------------------------   1          usur002
3.3.3.101          2021-04-16 09:31:56  ------------------------------------------------------------------------
Virtual Gateway:sslvpn
```

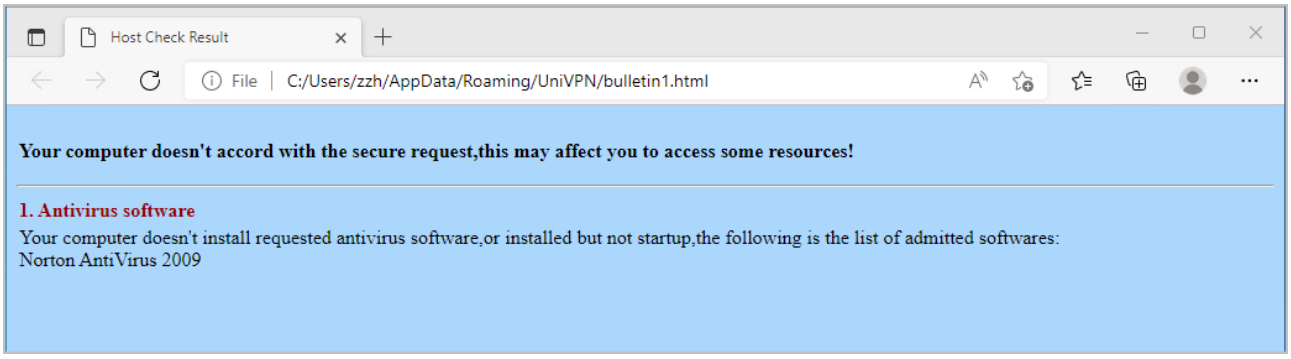
2. Configure a RADIUS authorization scheme if the authentication domain is set to Radius Server Authentication and network extension clients are configured to obtain IP addresses from external servers (network-extension external-server).

```
[sysname-sslvpn-service] display network-extension VG Network Extension Information
---------------------------- Network Extension State:
enable Keep Alive State: enable
Keep Alive Interval: 120(seconds) Log State:
disable Point to Point State: disable
VIP Method: external server assign default net pool: 3.3.3.100
Route Mode: manual Intranet IP/Mask: 3.3.3.0/255.255.255.0 Intranet
IP/Mask: 192.168.1.0/255.255.255.0
----End[sysname-sslvpn-service]
 [sysname-aaa] authorization-scheme radius [sysname-aaa-author-radius] dis this 2021-04-16
10:05:35.720 +8:00 # authorization-scheme radius authorization-mode radius # return
[sysname-aaa-author-radius] domain default Info: The domain default is for common users.
[sysname-aaa-domain-default] dis this 2021-04-12 15:15:35.360 +8:00 # domain default
authentication-scheme admin_radius authorization-scheme radius service-scheme
webServerScheme1530599131778 radius-server radius service-type internetaccess ssl-vpn
internet-access mode single-sign-on reference user current-domain # return [sysname-aaa-domain
default]
```

1.4.2.5 Warning: Host check failed

Symptom

After you enter the user name and password and click Login on the UniVPN login page, the system displays "Host check failed."



Possible Causes

The host check function is enabled on the virtual gateway, and the device does not meet security access requirements.

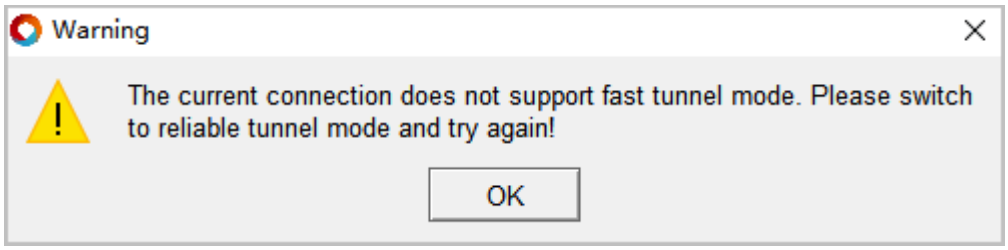
Procedure

Rectify the fault as prompted.

1.4.2.6 Warning: The current connection does not support fast tunnel mode. Please switch to reliable tunnel mode and try again!

Symptom

After you enter the user name and password and click **Login** on the UniVPN login page, the system displays "Warning: The current connection does not support fast tunnel mode. Please switch to reliable tunnel mode and try again!"

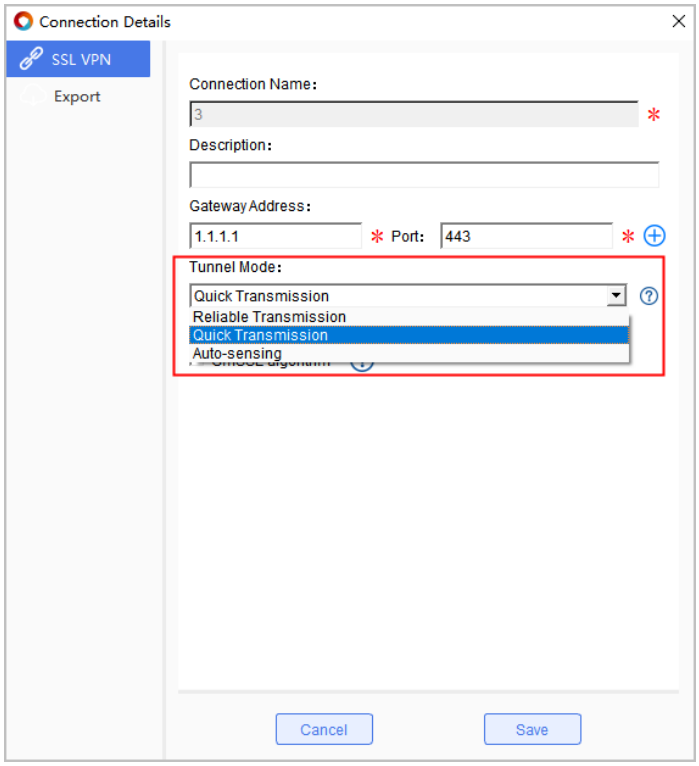


Possible Causes

During SSL VPN dialup, the device sends UDP detection packets to check whether fast tunnels can be established. If the device receives a response from the firewall, the fast tunnel can be established. The warning indicates that the UDP link is not reachable and that no fast tunnel can be established.

Procedure

1. Configure **Auto-sensing** on the UniVPN as a workaround. If the fast tunnel cannot be established, perform the following steps:



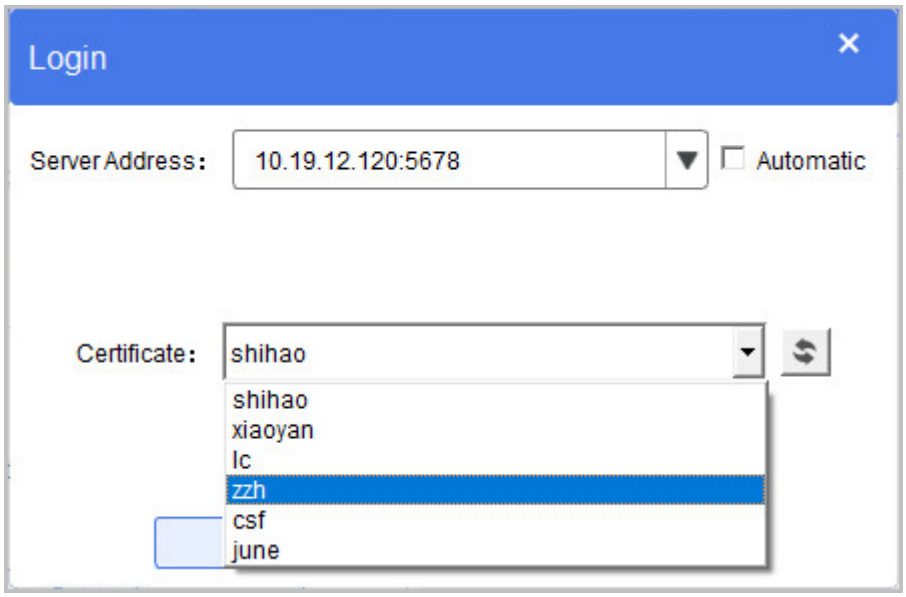
2. Check the firewall security policy to see if the data flow for establishing fast UDP links is permitted between the device and VPN gateway.
3. Check whether a NAT device is connected to the firewall. If yes, configure NAT for the TCP and UDP ports of the SSL VPN and modify the security policy to permit the fast link establishment flow. When NAT mapping is performed for UDP ports, the global port number must be the same as the inside port number.

1.4.3 Troubleshooting Guidelines for Warnings Displayed During Certificate-based Login

1.4.3.1 Failed to find the desired user certificate

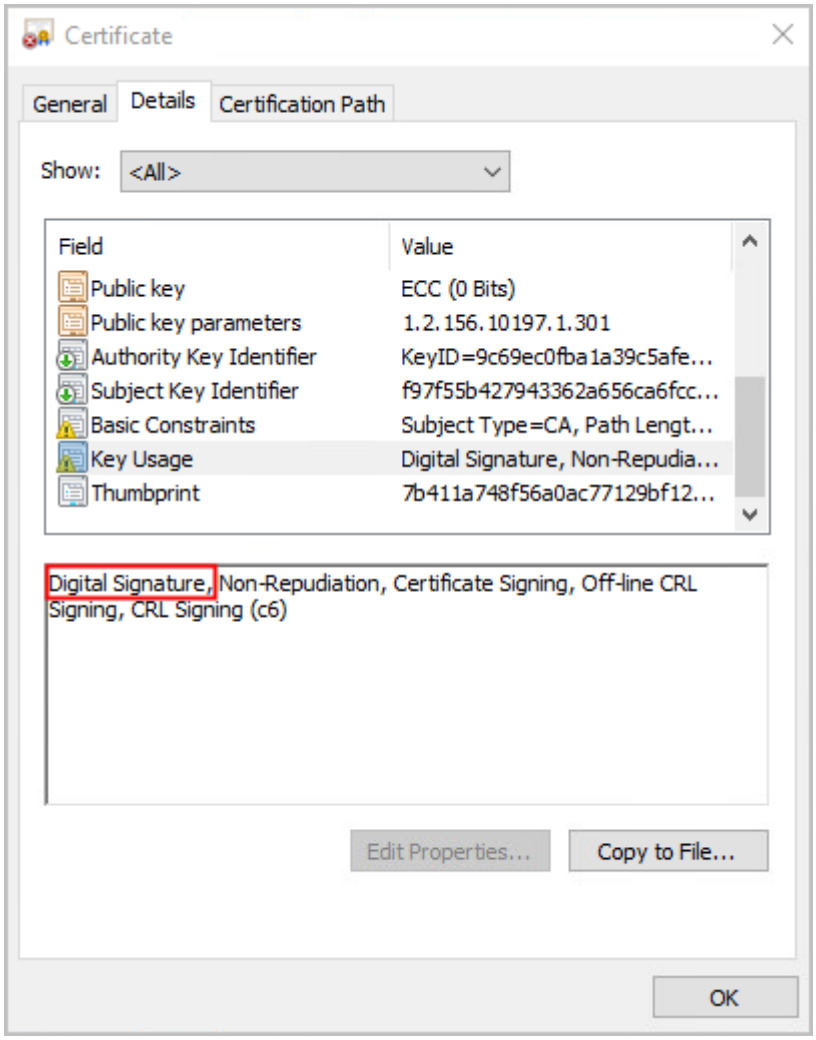
Symptom

The desired user certificate cannot be found on the SecoClient login page when you attempt to log in to the virtual gateway using certificate authentication.



Possible Causes

The Key Usage field of the user certificate does not contain Digital Signature.



Procedure

Create a user certificate with a digital signature carried in Key Usage.

NOTE

If the server does not support certificates without the digital signature capability, the client will not display such certificates.

If the server supports certificates without the digital signature capability, but the client does not display such certificates, the server may have the key usage enabled, which requires the digital signature capability.

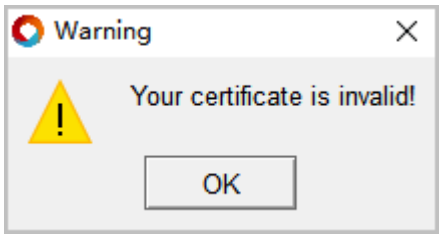
Product Name	Version	Support Authentication of Certificates Without the Digital Signature Capability (Y/N)
USG6000	V500R005C20SPC500 and later version	N

Product Name	Version	Support Authentication of Certificates Without the Digital Signature Capability (Y/N)
USG9500	V500R005C20SPC500 and later version	N
USG6000E	V600R007C20SPC300 and later version (except SPC301/SPC302)	N
Eudemon200E-N	V500R005C20SPC500 and later version	N
Eudemon200E-G	V600R007C20SPC300 and later version (except SPC301/SPC302)	N
Eudemon1000E-N	V500R005C20SPC500 and later version	N
Eudemon1000E-G	V600R007C20SPC300 and later version (except SPC301/SPC302)	N
Eudemon8000E-X	V500R005C20SPC500 and later version	N
SeMG9811	V500R005C20SPC500 and later version	N
NGFW Module	V500R005C20SPC500 and later version	N
USG12000	V600R021C10 and later version	Y
USG6000F	V600R021C10 and later version	Y
Eudemon9000E-X	V600R021C10 and later version	Y
Eudemon9000E-F	V600R021C10 and later version	Y
Eudemon1000E-F	V600R021C10 and later version	Y

1.4.3.2 Warning: Your certificate is invalid.

Symptom

When you select a user certificate and click Login on the SecoClient login page, the system displays "Your certificate is invalid."

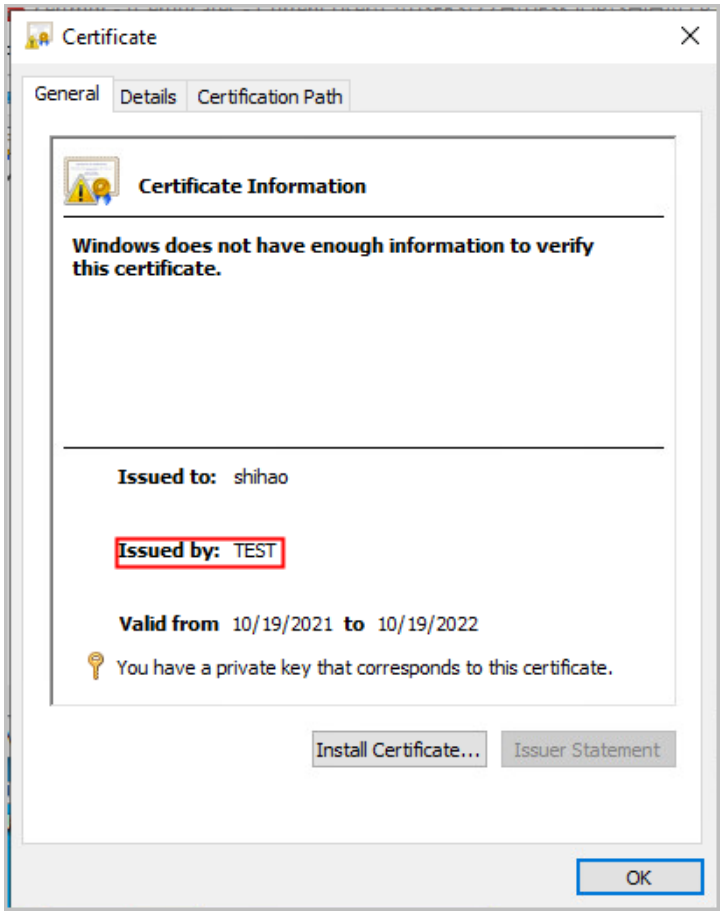


Possible Causes

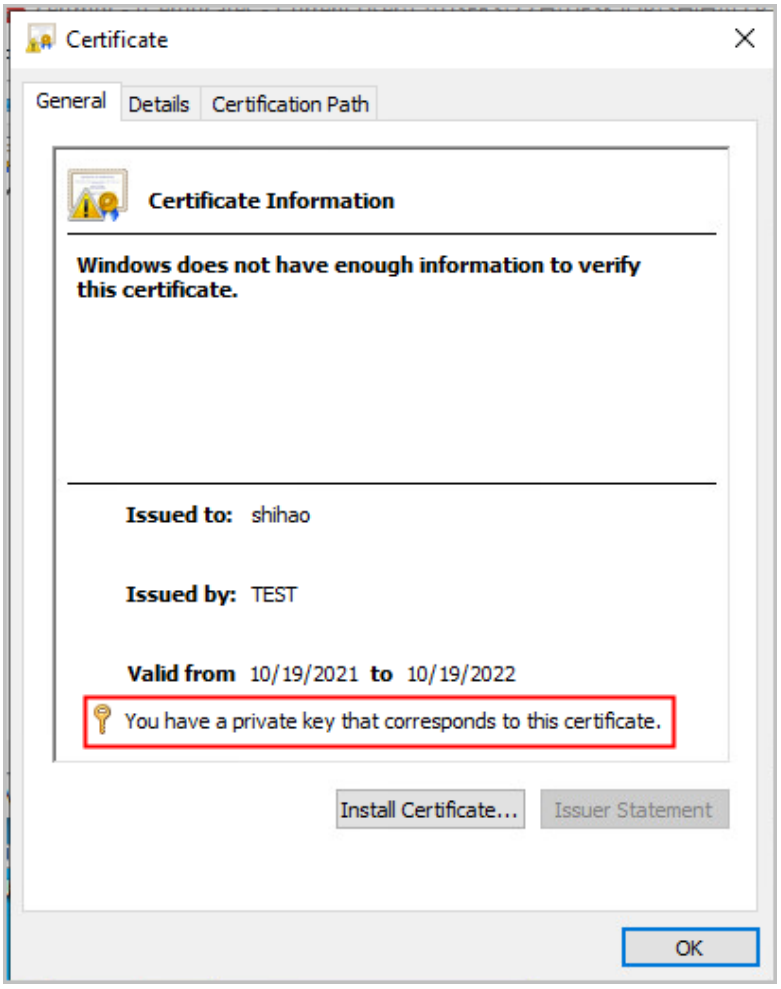
1. The user certificate is not issued using the root certificate signature of the CA certificate of the firewall virtual gateway client.
2. The user certificate installed on the device does not contain private key information.
3. The system time and time zone of the firewall are out of the scope of the user certificate.
4. The user certificate is revoked by the certificate revocation list (CRL) or online certificate status protocol (OCSP) configured on the firewall.

Procedure

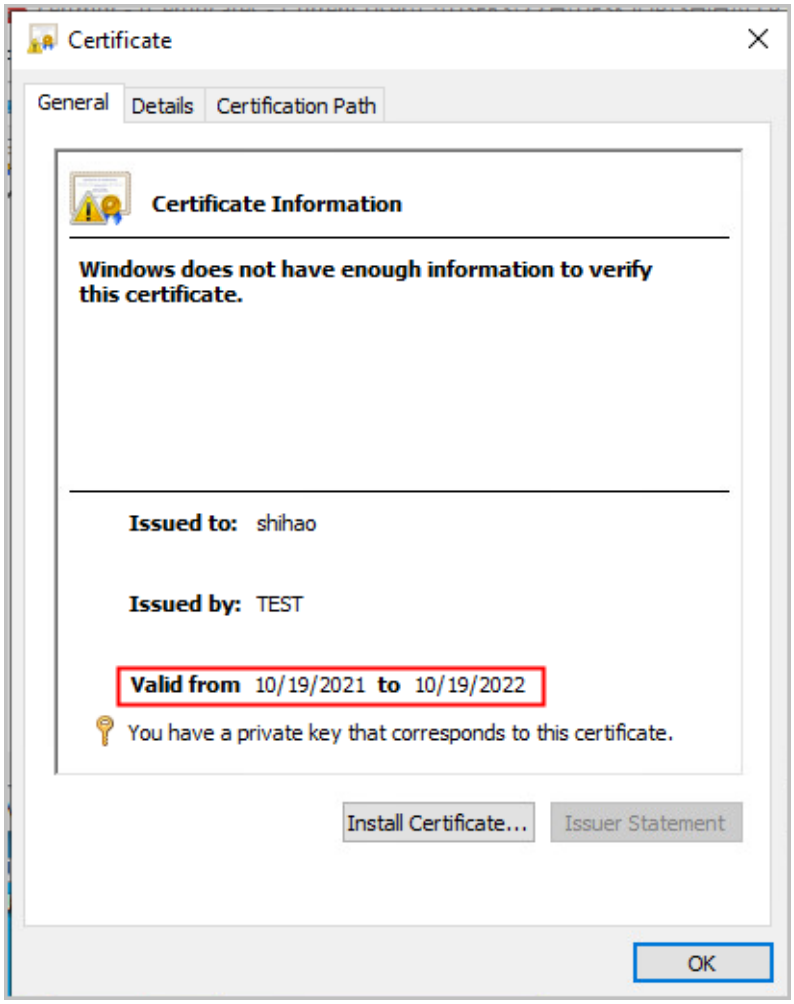
1. Check whether the Issued by field of the user certificate is the same as the Issued to field of the CA certificate on the firewall virtual gateway client.



2. Check whether the user certificate has a private key.



3. Check whether the system time and time zone of the firewall are within the scope of the user certificate.

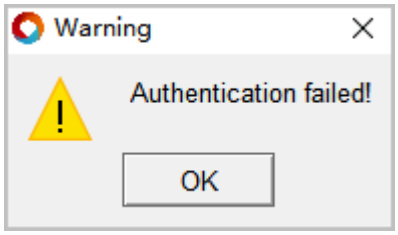


4. Check whether CRL or OCSP is configured on the firewall. If yes, undo the configuration and check the verification result.

1.4.3.3 Warning: Authentication failed

Symptom

Certificate challenge authentication is used by the virtual gateway. When you select a user certificate and click Login on the SecoClient login page, the system displays "Authentication failed."

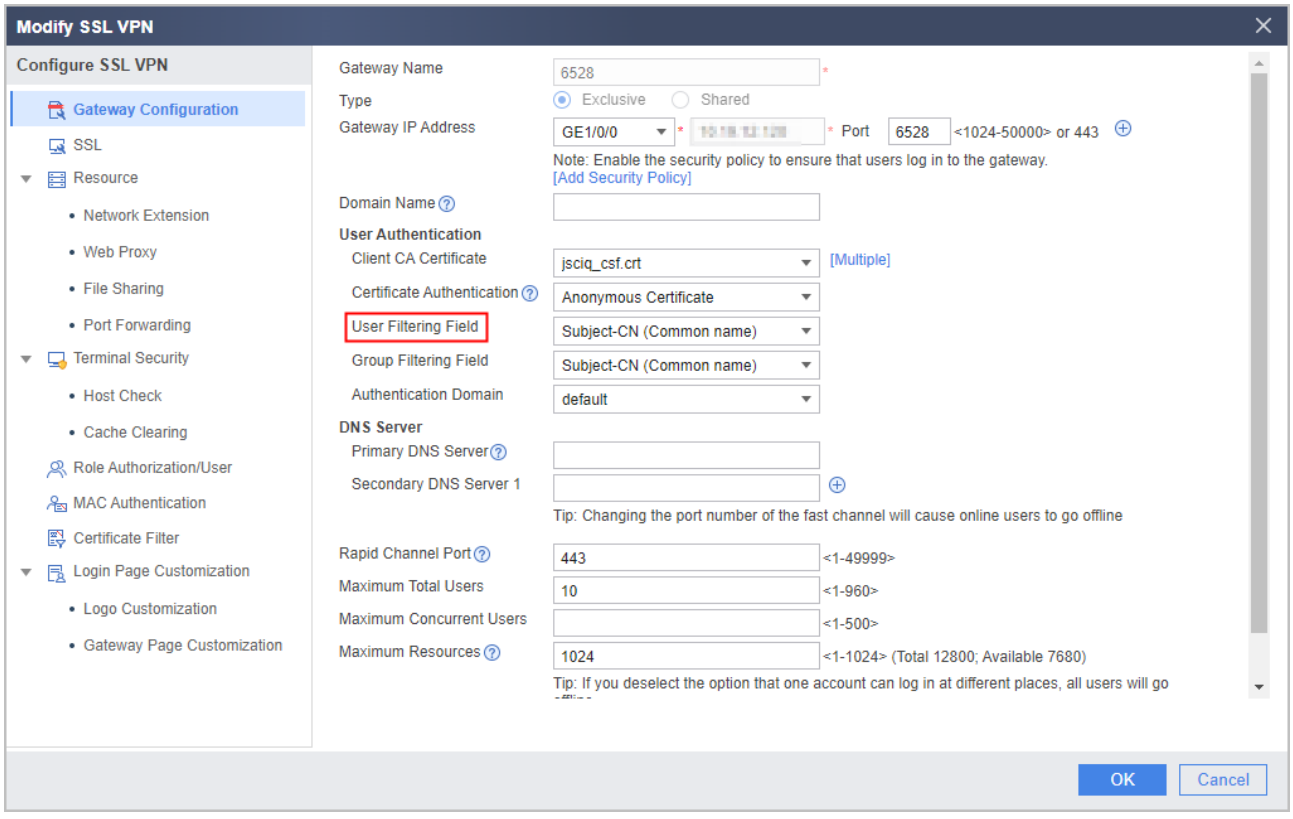


Possible Causes

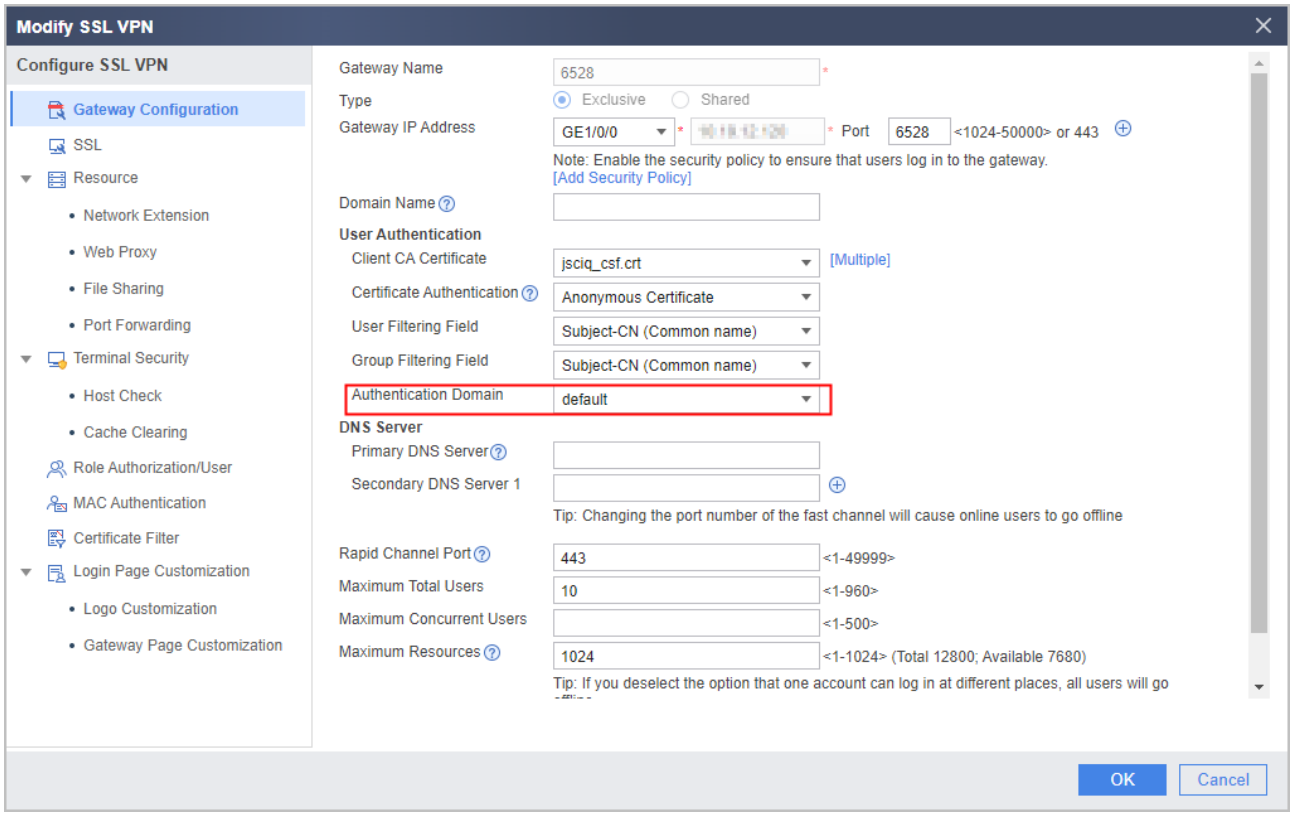
1. User Filtering Field configured for the virtual gateway certificate authentication is incorrect. As a result, the device obtains an incorrect user name from the user certificate when you log in to the device.
2. The virtual gateway is bound to an incorrect authentication domain.
3. SSL VPN access is not enabled for authentication domains.
4. The network extension feature is not enabled on the virtual gateway.
5. The SSL VPN login device is in a dual standby state (HRP_S), but SSL VPN does not support login on the standby device.
6. Expiration of certificate validity

Procedure

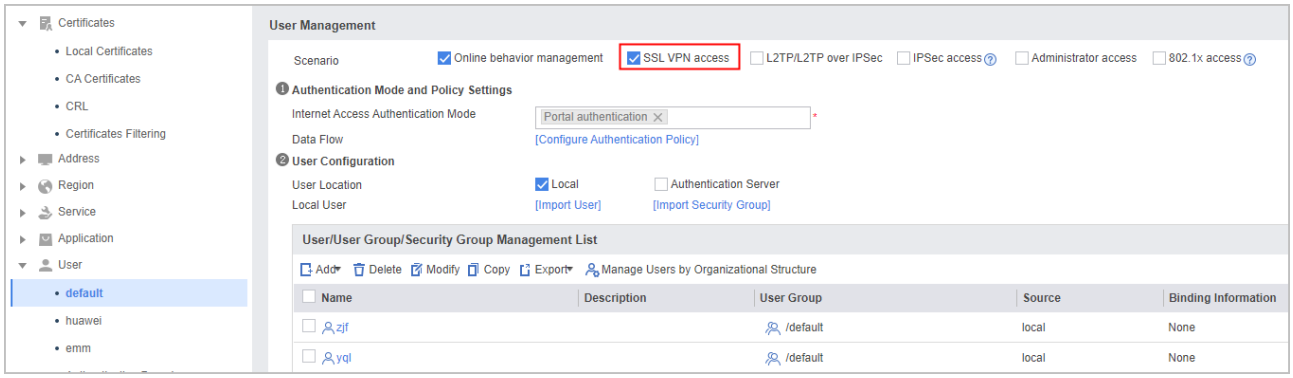
1. Log in to the device and check whether User Filtering Field configured in the virtual gateway certificate authentication matches the attribute name of the authentication field in the user certificate.



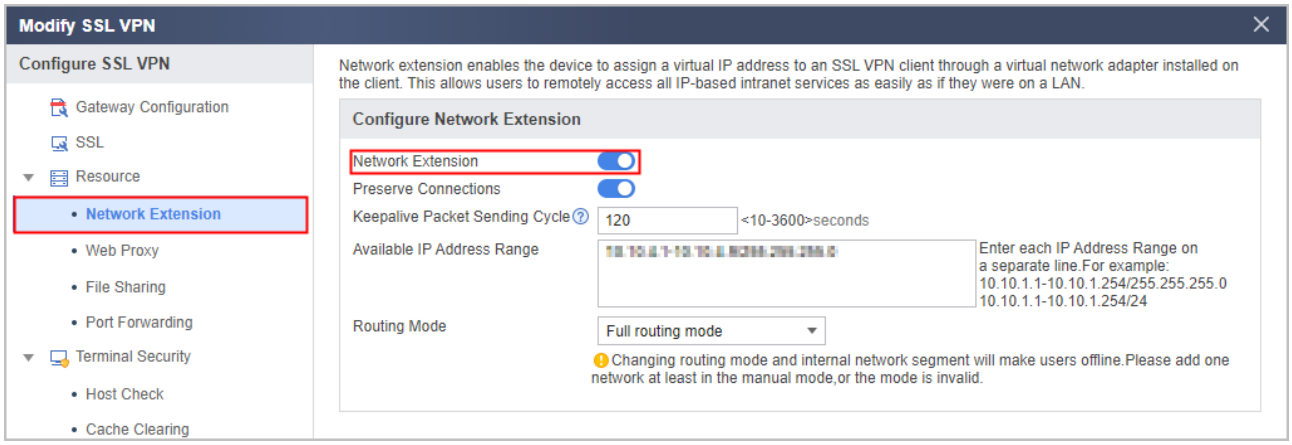
2. Check whether the correct authentication domain is bound to the virtual gateway.



3. Check whether SSL VPN access is enabled in the authentication domain.



4. Enable the network extension feature of the virtual gateway.



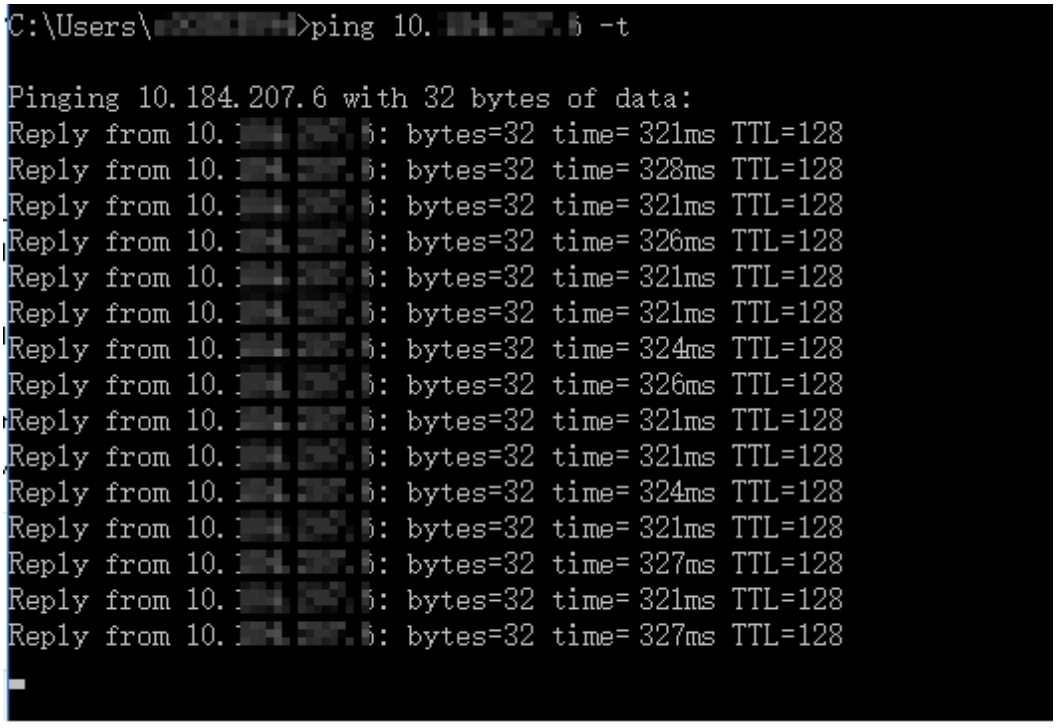
5. Modify the configuration or networking to ensure that the SSL VPN login device is in the HRP_M state.
6. Re import a new valid certificate after deleting the expired certificate

1.4.4 Troubleshooting Guidelines for Abnormal Services Encountered After Successful Login

1.4.4.1 Intranet Resource Access Is Stalled, and the Delay in Pinging the Intranet Is Long

Symptom

The SSL VPN dialup is successful, but access to intranet resources is stalled, and the delay in pinging the intranet is long. The test download rate is much lower than the download rate in NAT mapping.

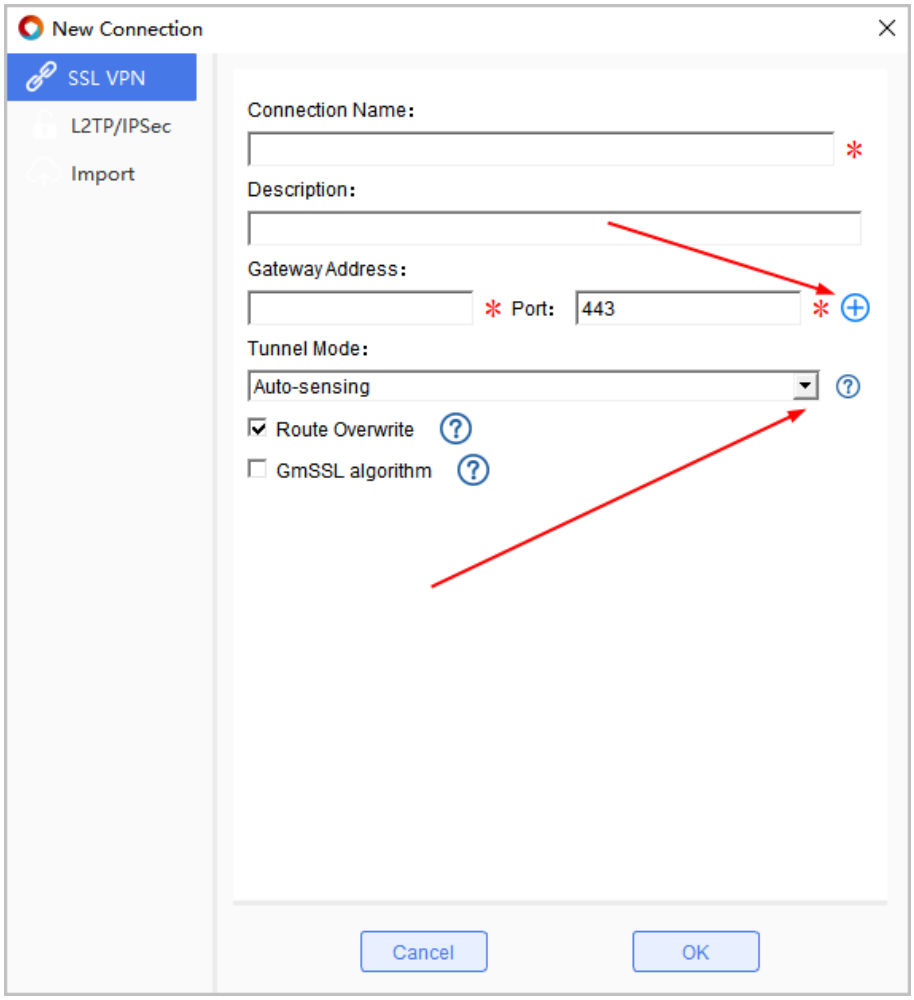


Possible Causes

NAT mapping only achieves address translation for packet headers, but the VPN technology encrypts and decrypts entire packets. Therefore, VPN requires more system resources and time than NAT mapping. This delay is more obvious if packets are transmitted over networks of different carriers.

Procedure

1. Select Quick Transmission or Auto-sensing from the Tunnel Mode drop-down list box. In quick transmission mode, the packet transmission rate is high. If Quick Transmission is selected, the interzone policy must be enabled between the Local zone and Untrust zone (assuming that the user is in the Untrust zone) on the firewall. In the policy, the service type is UDP, and the port number is 443. In auto-sensing mode, the SecoClient preferentially establishes an SSL VPN tunnel with the VPN gateway in quick transmission mode. If tunnel establishment fails, the SecoClient uses a reliable transmission mode to establish a VPN tunnel with the VPN gateway.
2. If an enterprise provides multiple SSL VPN gateways, enabling the automatic selection function on the SecoClient ensures that users can connect to the VPN gateway with the fastest response.



1.4.4.2 Failed to Access the Public Network After a Successful Login

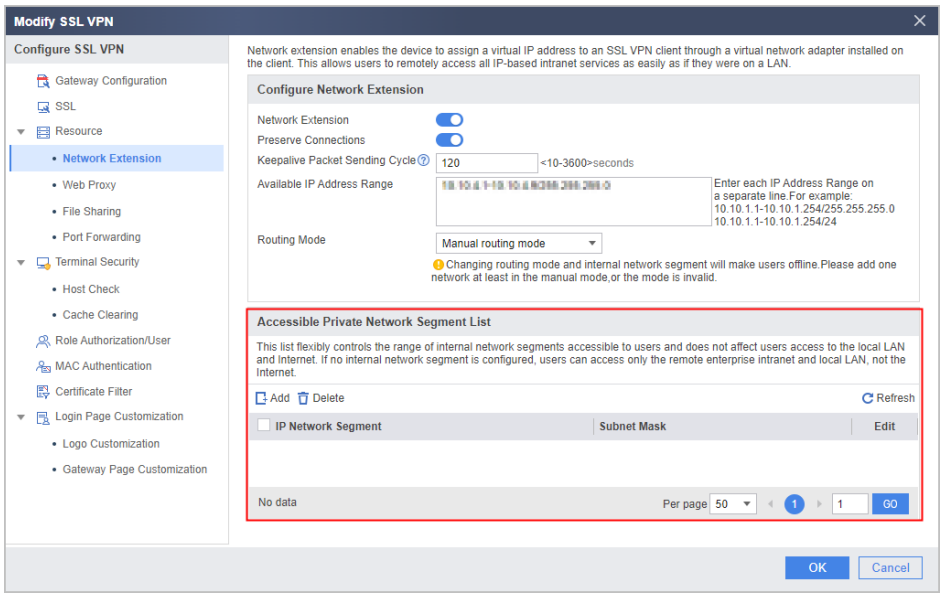
Symptom

The SSL VPN dialup is successful, but the public network cannot be accessed and the domain name cannot be pinged.

Possible Causes

The split or full routing mode is configured for the virtual gateway network extension service.

The network extension function is configured on the web page. If the accessible internal network segment list does not contain any network segment, the network extension routing mode is the split mode (network-extension mode split). If one or more network segments exist in the list, the network extension routing mode is the manual mode (network-extension mode manual). You can run the network-extension mode full command on the CLI console to set the full routing mode, but this mode cannot be configured using the web page. If the split or full routing mode is configured for network extension, the Internet is not accessible after SSL VPN dialup is used.



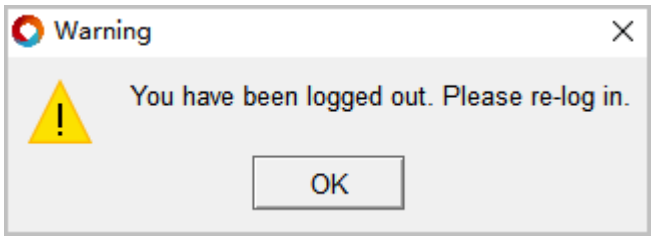
Procedure

Change the network extension routing mode to the manual mode. Enable the network extension function for devices so that VPN tunnels are used only when the devices access the specified VPNs on the intranet.

1.4.4.3 Warning: You have been logged out. Please re-log in.

Symptom

You are using the SecoClient service for a period after logging into the SecoClient, but the system displays "You have been logged out. Please re-log in."



Possible Causes

1. You are logged out by the administrator.
2. The aging time expires.

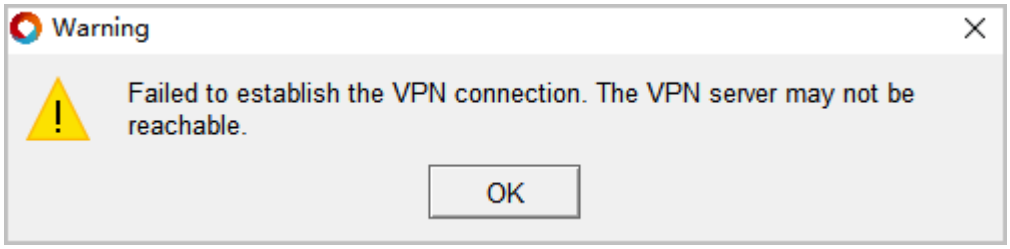
Procedure

1. Log in to the VPN gateway, and choose Monitor > System Logs. Check the firewall operation logs to see if the administrator has logged out you.
2. Check the session timeout interval configured on the virtual gateway and whether Preserve Connections is enabled.

1.4.4.4 Info: Failed to set up a VPN connection. The VPN server may be unreachable.

Symptom

After logging in to the UniVPN, the system displays "Info: Failed to set up a VPN connection. The VPN server may be unreachable."



Possible Causes

There is a high probability that the problem occurs because an encryption algorithm used by the client is different from that used by a gateway.

Procedure

Since V600R007C20SPC100, weak encryption algorithms are disabled on the virtual gateway by default. In this case, the cipher suite of the virtual gateway can only use

strong encryption algorithms. Only SecoClient running 7.0.2.26 or a later version can be used to log in to the virtual gateway.

For versions earlier than 7.0.2.26, you can run the v-gateway ssl weak-encryption enable command on the gateway to enable weak encryption algorithms of the virtual gateway.

1.4.4.5 After a Terminal Is Added to an AD Domain, SSL VPN Users Are Disconnected After Accessing the Network for a Period of Time

Symptom

After a terminal is added to an AD domain, SSL VPN users go offline unexpectedly after accessing the network for a period of time. When the terminal is not added to the AD domain, SSL VPN users do not go offline.

The fault symptoms are as follows.

- User logout records can be viewed on the firewall.

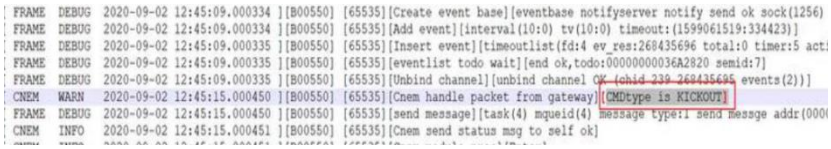
  Check user logout records on the active firewall. The following information is displayed.

```
HRP_M[HUAWEI] display aaa offline-record username user-name
2020-09-02 11:46:34.219 -03:00
--------------------------------------------------------------------------------
  User name             : test001@domain1
  Domain name           : domain1
  User MAC              : -
  User access type      : SSLVPN
  User IP address       : 10.0.91.89
  User IPV6 address     : -
  User ID               : 65915
  User login time       : 2020/09/02 11:44:27
  User offline time     : 2020/09/02 11:46:21
  User offline reason   : User request to offline
  User name to server   : test001
```

  Check user logout records on the standby firewall. The following information is displayed.

```
HRP_S[HUAWEI] display aaa offline-record username user-name
--------------------------------------------------------------------------------
  User name             : test001@domain1
  Domain name           : domain1
  User MAC              : -
  User access type      : SSLVPN
  User IP address       : 10.0.91.89
  User IPV6 address     : -
  User ID               : 65915
  User login time       : 2020/09/02 11:44:28
  User offline time     : 2020/09/02 11:46:21
  User offline reason   : Delete backup user
  User name to server   : test001
```

- SecoClient logs show that the gateway forces the user to go offline.



- Collect debug logs on the firewall. The LAM module generates the CUT_REQ event before the user goes offline.

```
HRP_M<HUAWEI-diagnose> debugging svm error
Sep 14 2020 13:15:49-03:00 FGSTHA00-01 CM/7/DEBUG:
[UCM-MSG] MSG Recv From: (taskName=LAM, Code=ESAP_SRV_MSG_CUT_REQ, Src=0, Dst=-1, Slot=0)WebAuth:0x0 Vrf:0Reason:29 Vlan:0 VPI/VCI:0/0 AccessType:0TimeoutMsg:0 Mac:0000-0000-0000 IPV6: IP:10.0.91.28.
Sep 14 2020 13:15:49-03:00 FGSTHA00-01 CM/7/DEBUG:
```

Possible Causes

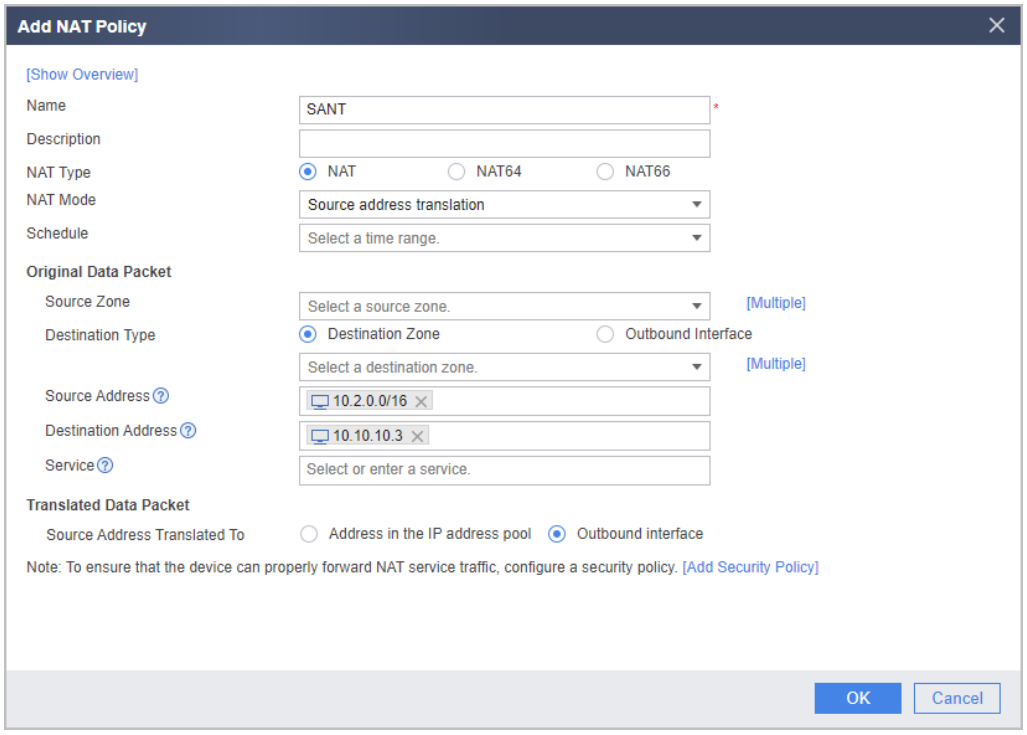
There is a high probability that the problem occurs because both SSL VPN and AD SSO (AD SSO is installed to query AD server security logs) are configured on the firewall.

After the terminal joins the AD domain, the SSL VPN user needs to connect to the AD domain controller for authentication (the AD domain controller records security logs at that time). After the authentication succeeds, the SSL VPN user successfully logs in to the network from the firewall. When the AD SSO server obtains security logs (containing the mapping between SSL VPN accounts and virtual IP addresses) from the AD domain controller, the server sends security logs to the firewall, and the firewall forces the user to go online again based on the security logs. In this scenario, the same user (the same account corresponds to the same virtual IP address) logs in to the network from the firewall twice. The first time is the SSL VPN user login process. After the SSL VPN user is authenticated, the user logs in to the network from the firewall. The second time is that the firewall parses the security logs sent by the AD SSO server and forces the user to go online.

However, the firewall does not support the preceding scenarios. When the firewall parses the security logs sent by the AD SSO server to force the user to go online, the firewall forces the existing online SSL VPN users to go offline.

Procedure

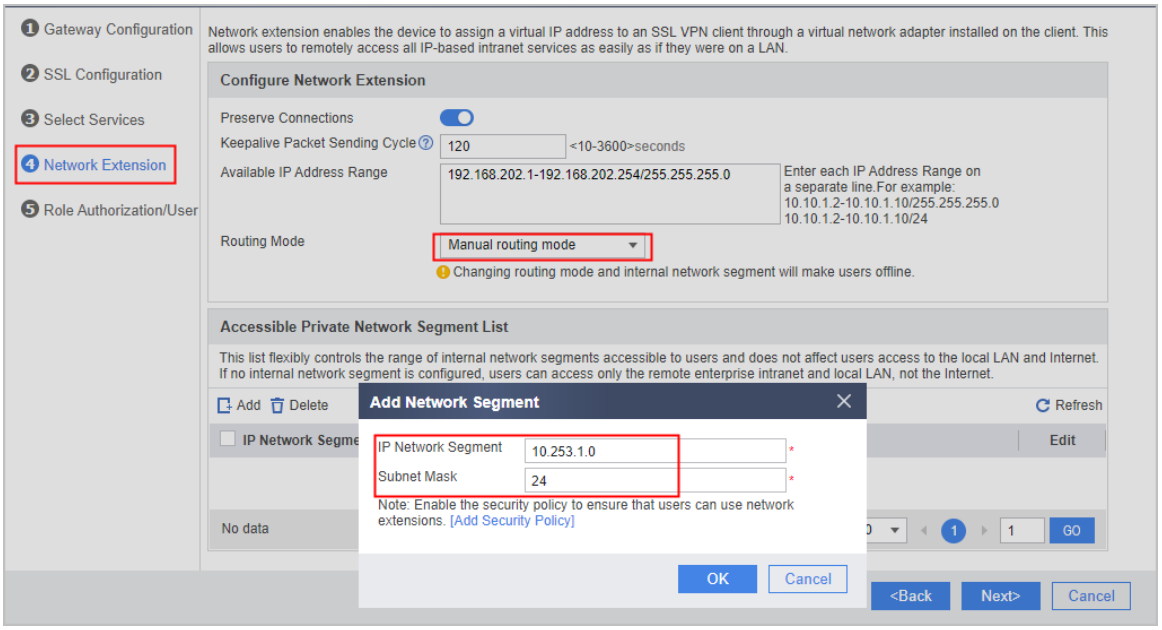
1. Check whether the AD SSO function (querying security logs on the AD server after AD SSO is installed) is configured on the firewall. If yes, go to the next step. If the AD SSO function is not configured, contact Huawei technical support.
2. Configure a source NAT policy on the firewall.
3. Configure a source NAT policy for the authentication data flow from SSL VPN users to the domain controller server. After the configuration, the SSL VPN user does not directly interact with the domain controller. In the security logs generated on the AD domain controller, the source IP address is not the virtual IP address obtained through SSL VPN dialup but is the IP address of the intranet interface of the firewall. In this way, when the firewall parses the security logs sent by the AD SSO server and forces the related user to go online, the firewall does not force the existing online SSL VPN users to go offline.
   a. Choose Policy > NAT Policy > NAT Policy from the main menu.
   b. Click Create and configure a source NAT policy.
   c. Assume that the virtual IP address of the SSL VPN user is 10.2.0.0/16 and the IP address of the AD domain controller is 10.10.10.3.



1.4.4.6 A User Cannot Access the New Network Segment After an SSL VPN Network-Extension Accessible Network Segment Is Added

Symptom

You choose Network Extension from the navigation pane. In the Configure Network Extension area, set Routing Mode to Manual routing mode. In the Accessible Private Network Segment List area, click Add. In the Add Network Segment dialog box, set IP Network Segment and Subnet Mask to 10.253.1.0 and 24, respectively. After a user goes offline and dials up again, the user cannot access the new network segment 10.253.1.0/24.



Possible Causes

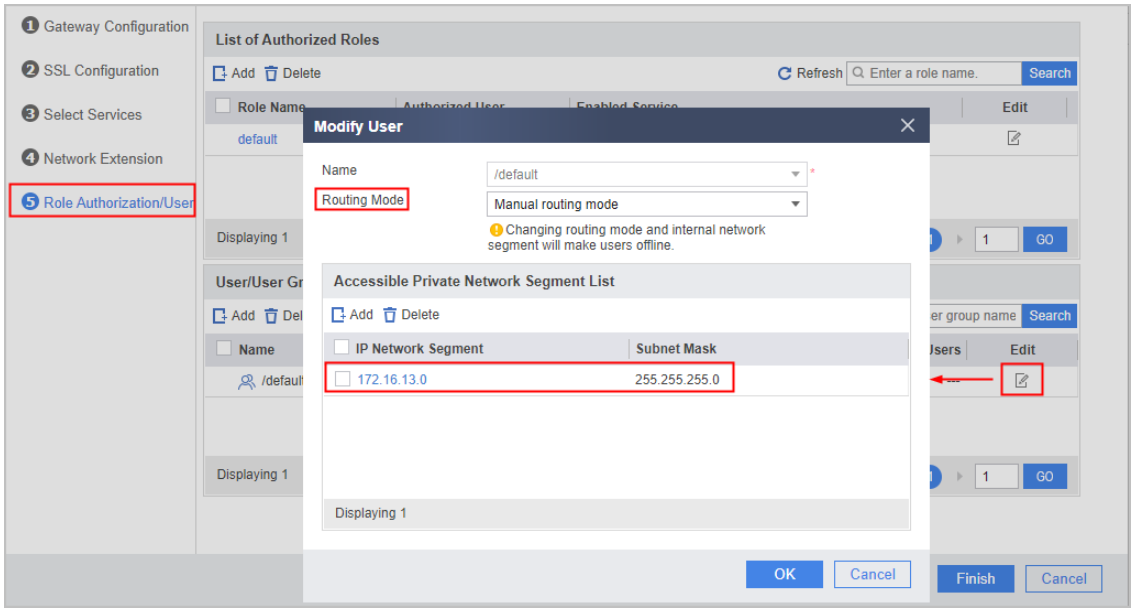
There is a high probability that the problem occurs because the device does not deliver the route destined for the new network segment to terminals.

Procedure

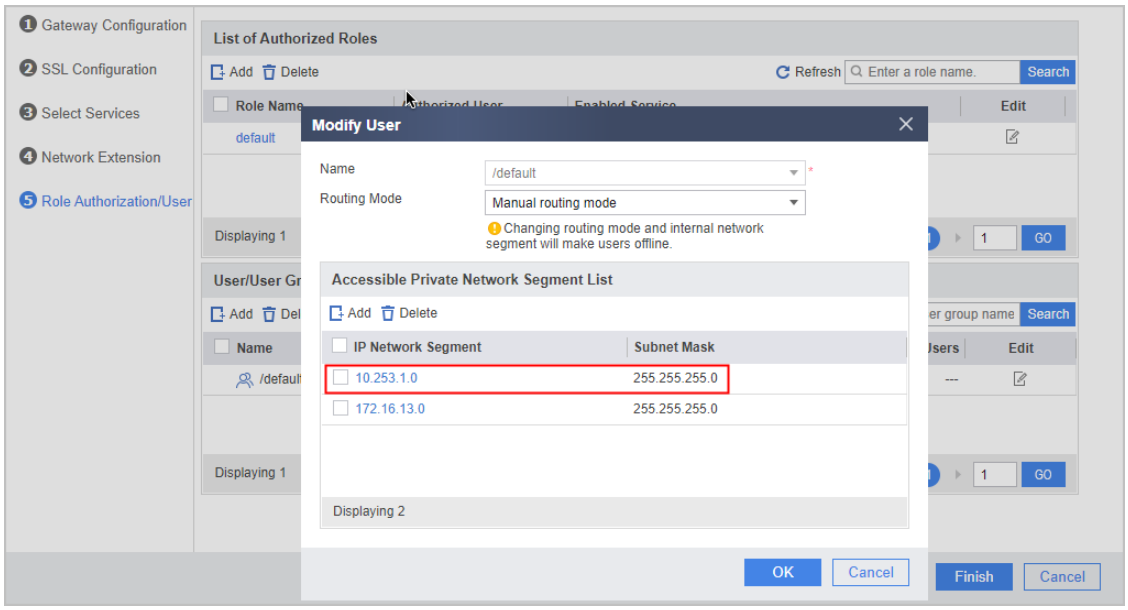
1. Run the route PRINT command on the terminal to check whether there is a route to the new network segment. If no, go to the next step. If yes, contact Huawei technical support.

```
C:\Users\XXX> route PRINT

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        NetMask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0    10.174.104.1   10.174.105.158      25
     10.174.104.0    255.255.252.0         On-link   10.174.105.158     281
   10.174.105.158  255.255.252.255         On-link   10.174.105.158     281
   10.174.105.255  255.255.252.255         On-link   10.174.105.158     281
```

2. Perform the following steps to check whether the user group has a routing mode specified and whether the new network segment is included in Accessible Private Network Segment List. If the user group has a routing mode and the new network segment is not included in Accessible Private Network Segment List, perform the following steps.
3. As shown in the following figure, a routing mode is configured for the user group, and the new network segment is not included in Accessible Private Network Segment List. If the routing mode is configured in the user group view, the routing mode configured in the network extension view does not take effect.



4. Add a network segment to Accessible Private Network Segment List for the user group.



5. After the user logs in again, check the local route. It is found that the new accessible intranet network segment of the user group has been delivered to the terminal, and the terminal user can access the resources on the network segment.

IPv4 routing table

==========

Active Routes:

Network Destination	NetMask	Gateway	Interface	Hops
0.0.0.0	0.0.0.0	90.x.x.x	90.x.x.x	281
0.0.0.0	0.0.0.0	17.1.1.1	17.1.1.2	271
10.253.1.0	**255.255.255.0**	**On-link**	**192.168.202.4**	**1**
10.253.1.255	255.255.255.255	On-link	192.168.202.4	257

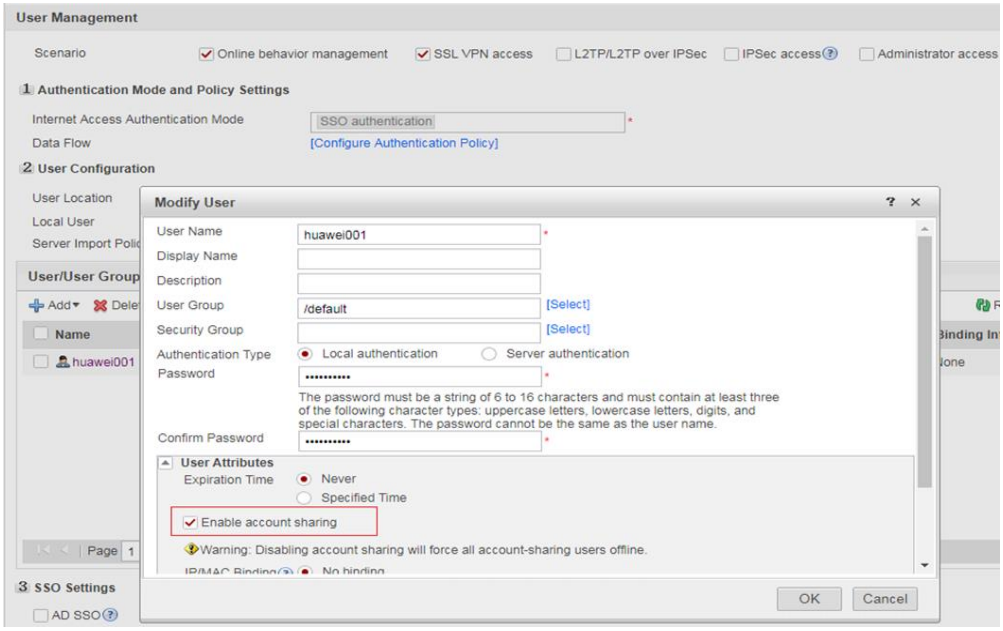
1.5 FAQs About SSL VPNs_V500R005C20 & V600R007C20

This chapter introduces the common consultation FAQs for UniVPN clients when accessing firewall devices V500R005C20, V600R007C20, and later versions.

1.5.1 How to Enable Different Users Using the Same Account to Log In to SSL VPN Simultaneously?

To enable different users using the same account to log in to SSL VPN at the same time, do as follows:

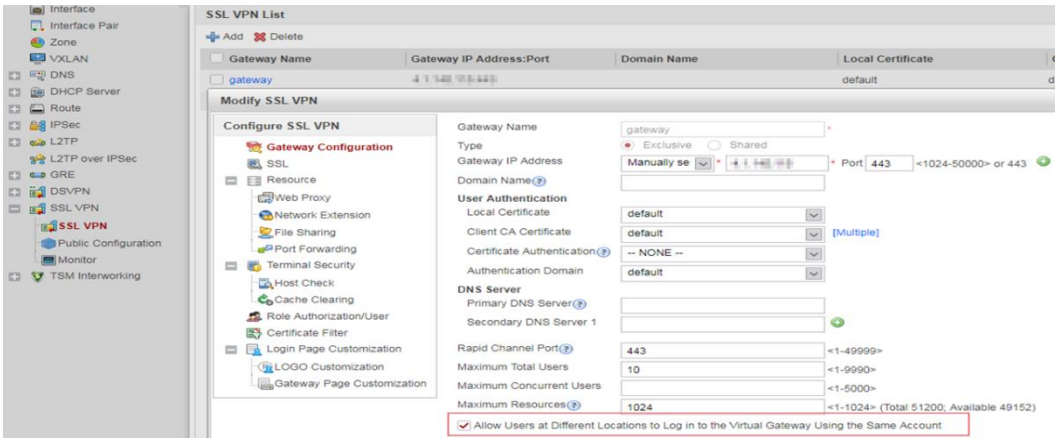
1. When you create a user account, select Enable account sharing.



2. CLI configuration method:

```
[sysname] user-manage user sslvpn
[sysname-localuser-sslvpn] multi-ip online enable
```

3. On the SSL VPN virtual gateway, select Allow Users at Different Locations to Log in to the Virtual Gateway Using the Same Account.



4. CLI configuration method:

```
[sysname] v-gateway test1
[sysname-test1] security
[sysname-test-security] public-user enable
```

1.5.2 Why Resources Cannot Be Accessed After the Connection Is Successful?

1. Functions vary when the client connects to different servers.
2. After the VPN connection is set up, the system determines whether to send packets through the tunnel based on the path delivered by the client. The firewall can be configured authorization resources. If the resources to be accessed enter the VPN tunnel according to the routing information but are not within the scope of the resources authorized by the role, the client intercepts and discards the packets.

1.5.3 What Is the Knowledge of SSL VPN Certificate Authentication?

1. Client CA certificates support the certificate chain. When configuring the certificate chain, select all the CA certificates on the chain.
2. You can select multiple client CA certificates that are not associated with each other so that the users holding certificates issued by different root certificates are allowed to access the network.
3. The user name field in the user certificate can contain spaces but must not contain any quotation marks (") or question marks (?).
4. In hot standby networking, certificates are not automatically backed up. You need to manually import client CA certificates to both active and standby devices.
5. If certificate-anonymous or certificate-challenge authentication is implemented for users, the client certificate needs to be installed on the client browser. The client certificate must be in .p12, .pem (including a key), or .pfx format.
6. In certificate-anonymous authentication mode, the device extracts fields from a user/device certificate to verify the identities of SSL VPN users. In certificate-challenge authentication mode, the device verifies the identities of SSL VPN users by extracting fields from a user/device certificate and also interworks with the local device or server to assist the authentication.

1.5.4 Does SSL VPN Support Binding Between Users and Devices

V100R001 and V500R001 do not support this function.

In V500R005C00, the virtual gateway can authenticate the MAC addresses of SSL VPN user devices. MAC address authentication is to permit only authorized devices to access the intranet, preventing external devices from imposing potential risks to the intranet.

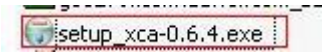
1.5.5 Does the High-End Firewall Support SSL VPN Services?

The USG9500 high-end firewall supports SSL VPN services starting from V500R001C50. The earlier versions (for example, V300R001) do not support SSL VPN services.

1.5.6 How Do I Use XCA to Create Device Certificates and User Certificates?

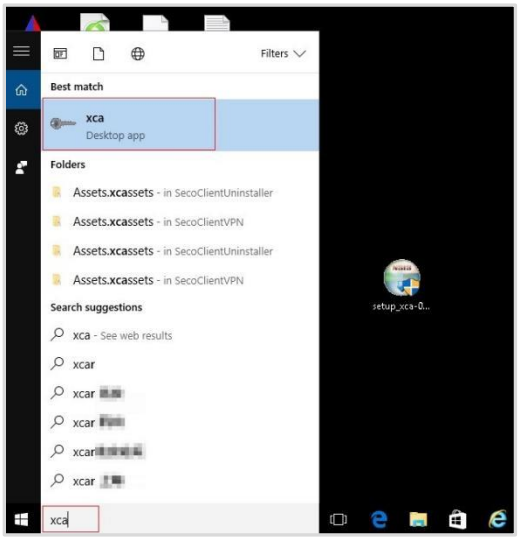
1. Install the XCA tool.

   Double-click setup_xca-0.6.4.exe and click Next until the installation is successful.

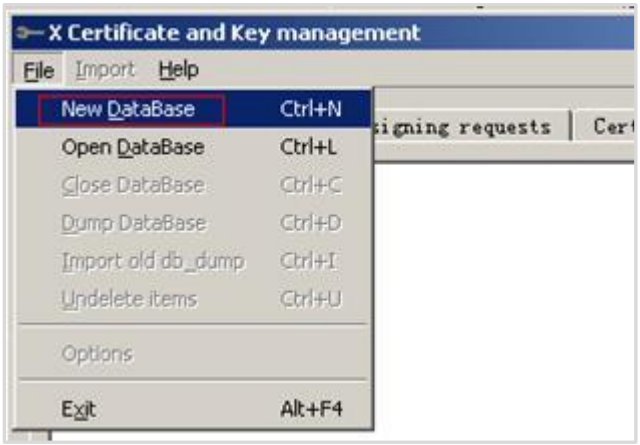


2. Run the program.

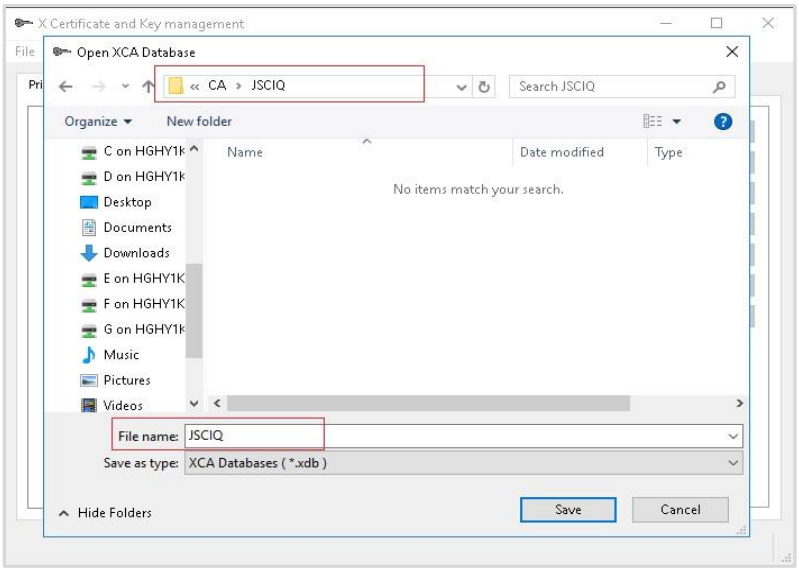
   a. Choose Start > Program > xca > xca.



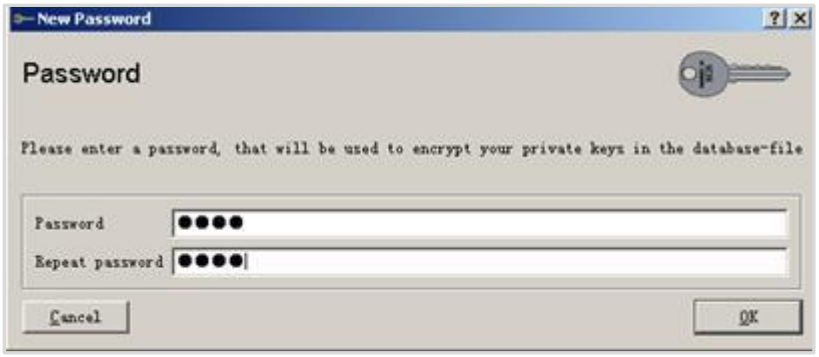
   b. Choose Start > Program > xca > xca.



c. Select a path for storing the database file, for example E:\ca\JSCIQ, name the file JSCIQ, and click Save.



d. In the displayed dialog box, enter a password and click OK.

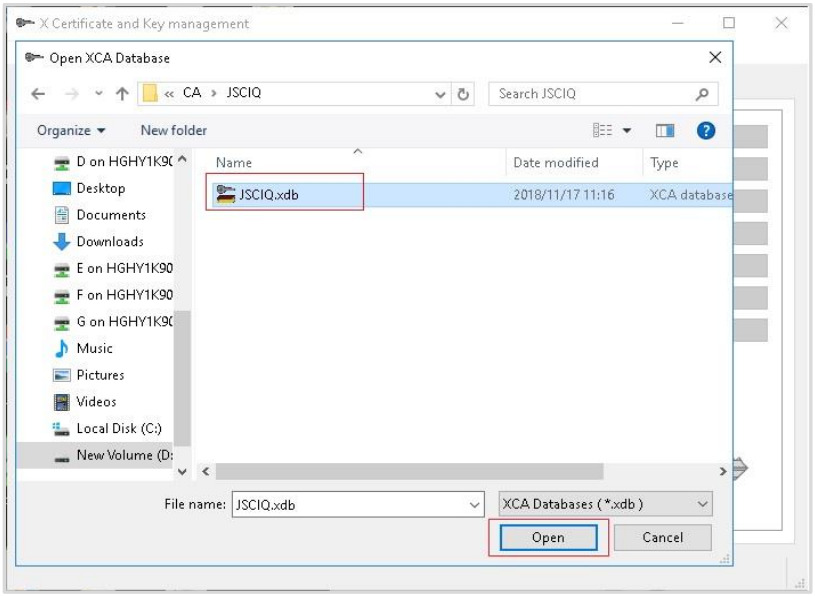


NOTE

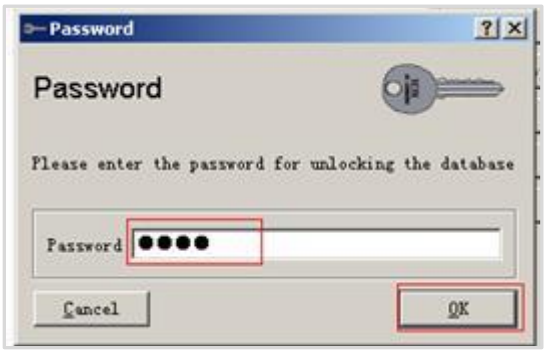
Remember this password because it is used when you start the database again.

3. Shut down and then start the xca tool.

a. Shut down and then start the xca tool.Start the database and choose **Open**.



b. Start the database and choose Open.



4. Create a root certificate.

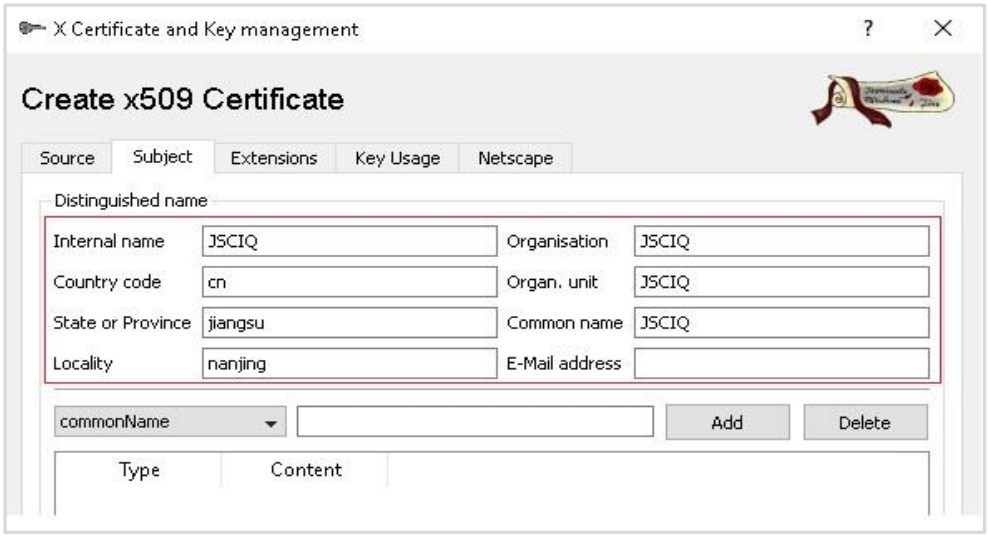
a. On the Certificates tab, click New Certificate.

b. In the Signing page of the Source tab, select SHA 1 from the Signature algorithm drop-down list box, select [default]CA from the Template drop-down list box, and click Apply.

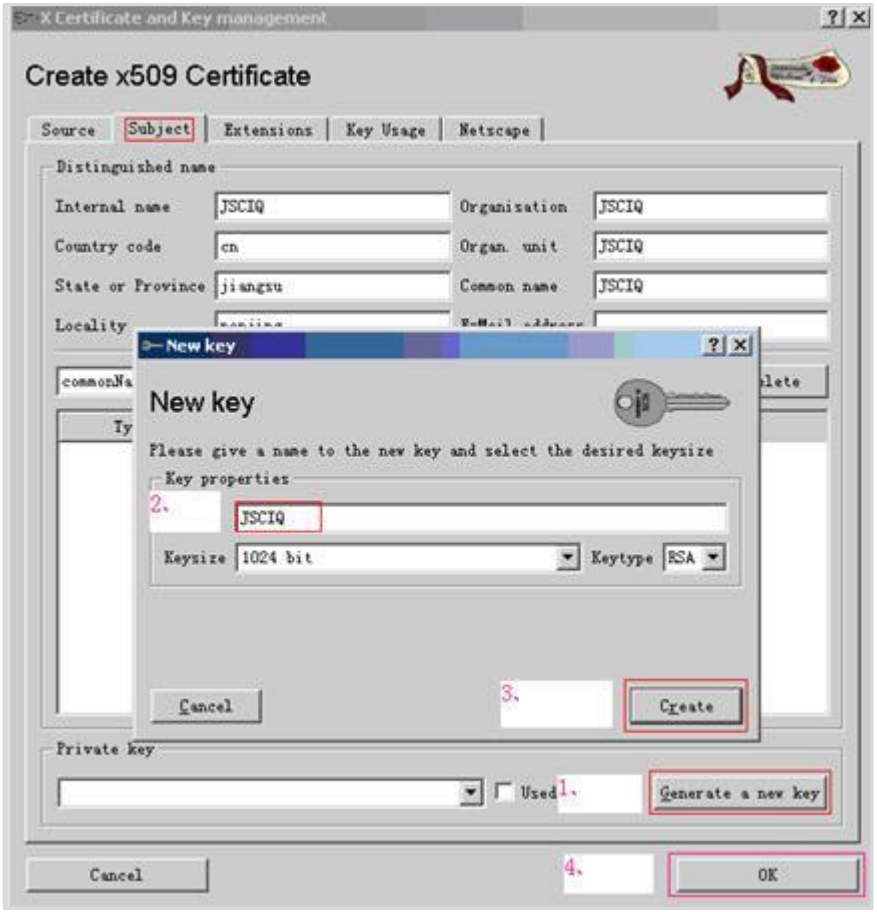
NOTE

Select SHA 1 as the signature algorithm, and click Apply.

c. On the Subject tab, enter name information.



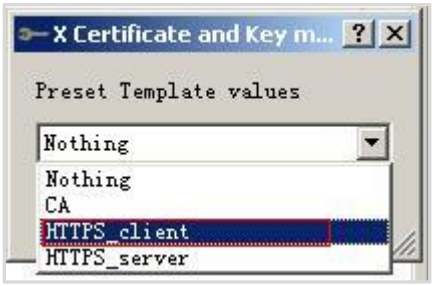
d. Click Generate a new key on the Subject tab. In the dialogue box displayed, set the key name to JSCIQ and click Create.



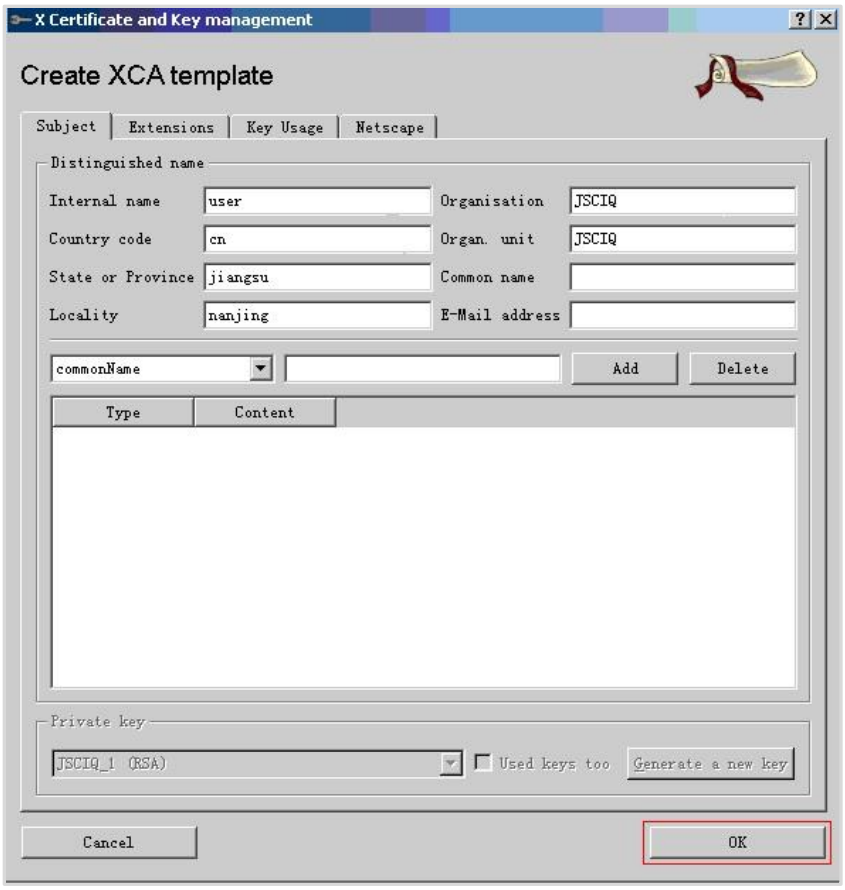
e. Click OK. The root certificate is generated.

5. Create a user certificate.
   - Create a user certificate template.
     a. Click Templates and then click New template to create a user certificate.

b. Click Templates and then click New template to create a user certificate.



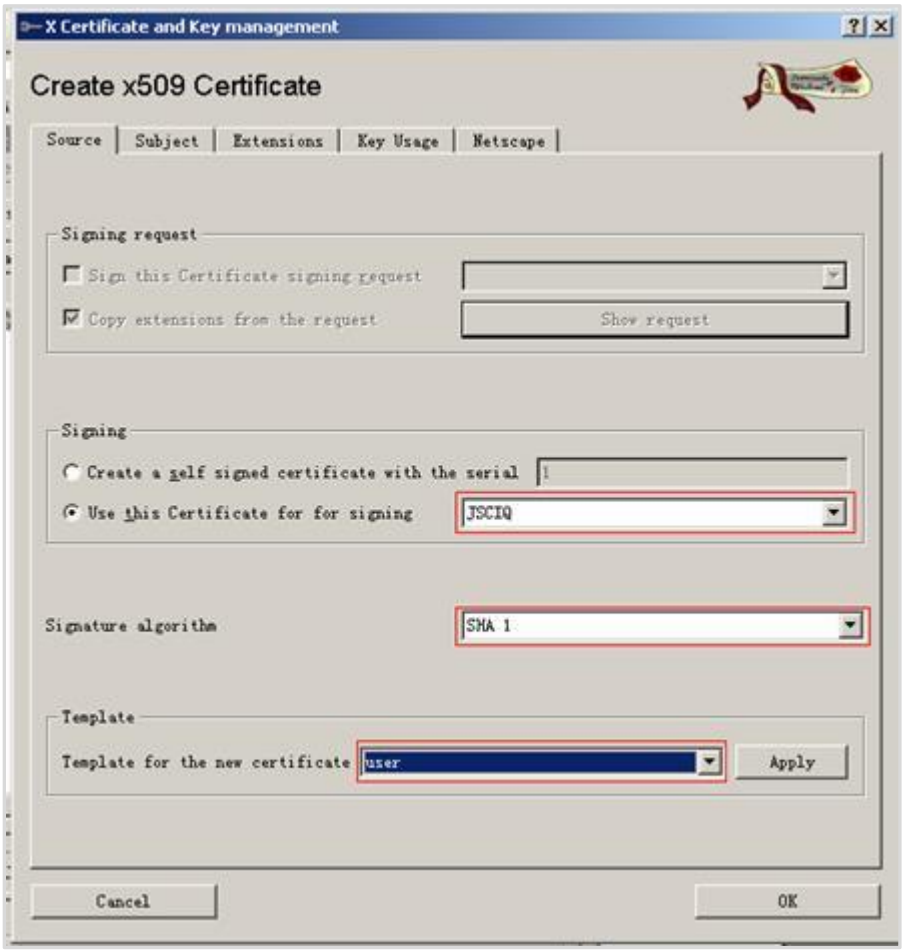
c. In the user template, set user parameters (do not set Common name because each user name is unique), and click OK.



- Create a user certificate.

  a. Click Certificate > New Certificate to create a user certificate.

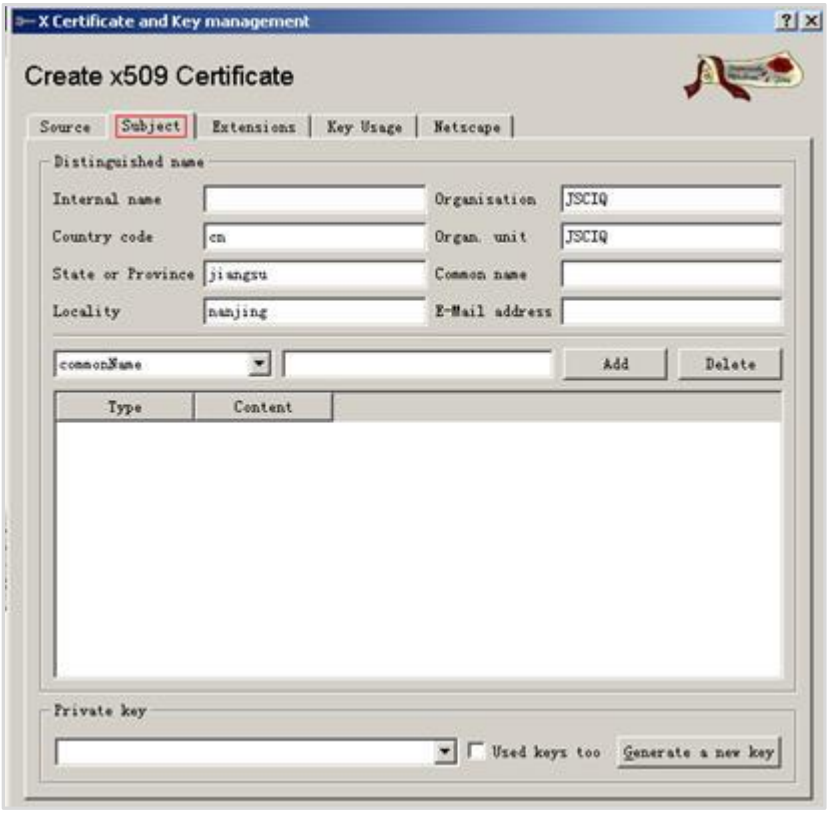
b. In the Signing pane, select JSCIQ from the Use this Certificate for signing drop-down list box, select SHA-1 from the Signature algorithm drop-down list box, and select user in the Template pane. Then click Apply.



NOTE

Select SHA 1 as the signature algorithm, and click Apply.

c. On the Subject tab page, template settings are displayed.



d. On the Subject tab page, template settings are displayed.
   (a) On the Subject tab, enter wangt in the Internal name text box.
   (b) Enter wangt in the Common name text box.
   (c) Click Generate a new key.
   (d) In the dialog box displayed, enter wangt.
   (e) Click Create.
   (f) Click OK.

e. The generated certificate is displayed.

6. Create a device certificate.

a. Choose Certificate > New Certificate to create a device certificate.

b. In the Signing pane, select JSCIQ from the Use this Certificate for signing drop-down list box, select SHA-1 from the Signature algorithm drop-down list box, and select [default] HTTPS_server in the Template pane. Then click Apply.

NOTE

Select SHA 1 as the signature algorithm, and click Apply.

c. On the Subject tab, perform the following operations:

(a) Enter 1.1.1.1 in the Internal name text box. (This address must be the IP address

(b) of the virtual gateway.)

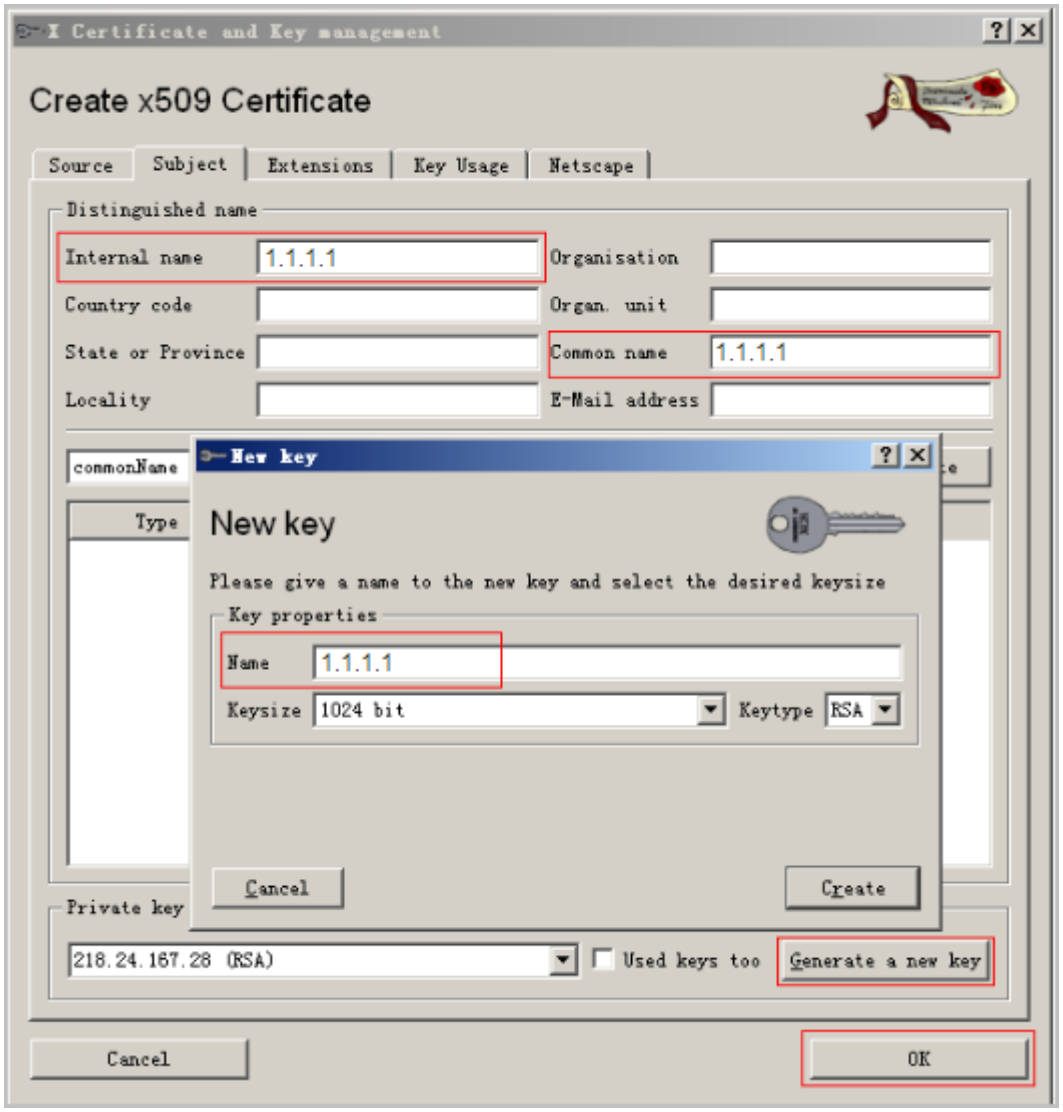
(c) Enter 1.1.1.1 in the Common name text box. (This address must be the IP address of the virtual gateway.)

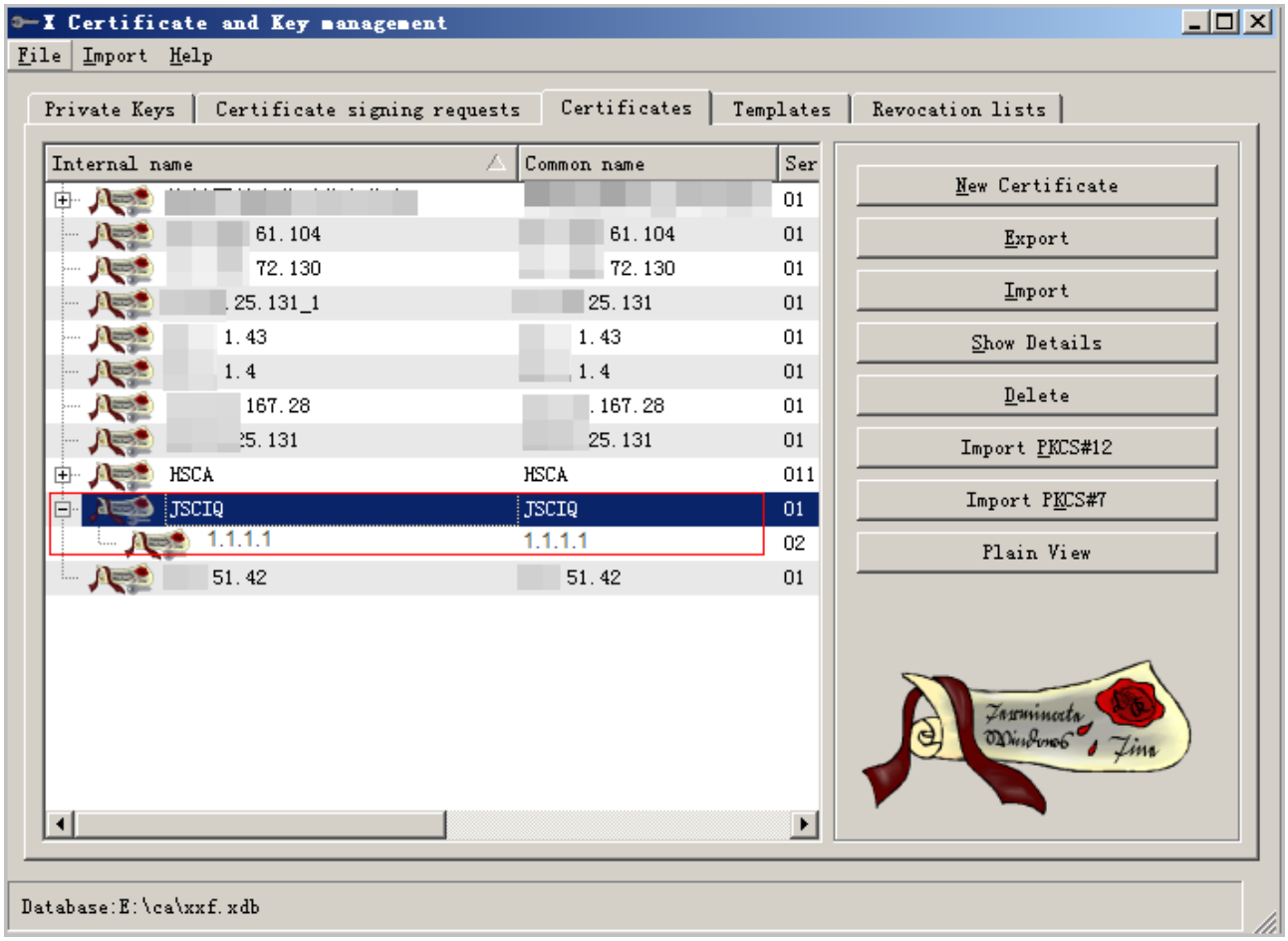
(d) Click Generate a new key.

(e) In the dialog box displayed, enter 1.1.1.1.

(f) Click Create.

(g) Click OK.


X Certificate and Key management
Create x509 Certificate
Source
Subject
Extensions
Key Usage
Netscape
Distinguished name
Internal name
1.1.1.1
Organisation
Country code
Organ. unit
State or Province
Common name
1.1.1.1
Locality
E-Mail address
commonName
Type
New key
New key
Please give a name to the new key and select the desired keysize
Key properties
Name
1.1.1.1
Keysize
1024 bit
Keytype
RSA
Cancel
Create
Private key
218.24.167.28 (RSA)
Used keys too
Generate a new key
Cancel
OK



7. Export a certificate.
   - Export a root certificate.
     a. Select the root certificate JSCIQ and click Export.

b. The following dialog box is displayed.

c. Specify a path for saving the certificate and click OK.

NOTE

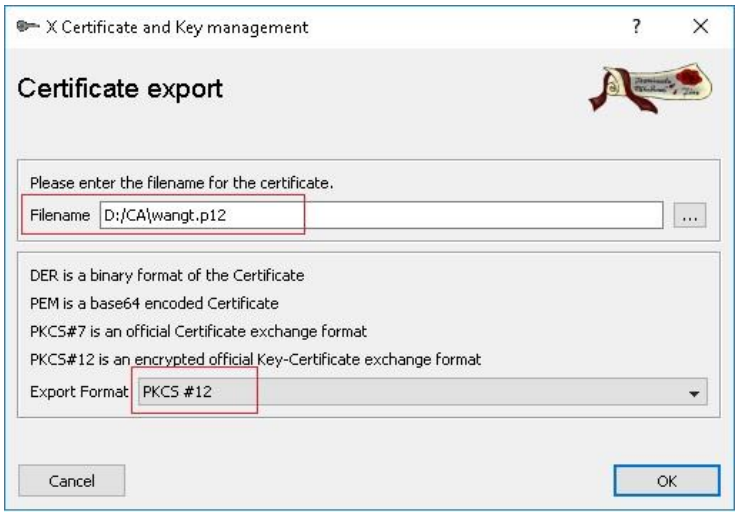
The path must not contain Chinese characters.

d. The JSCIQ.crt certificate is displayed in G:/ca.

- Export a user certificate.

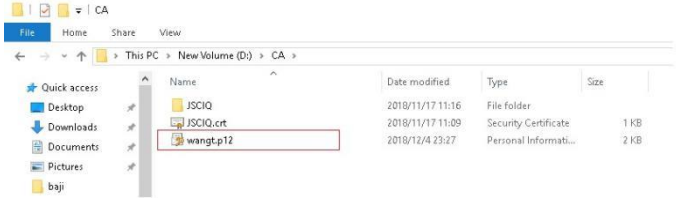
a. On the **Certificate** tab, select the user certificate **wangt** and click **Export**.

b. Specify a path for saving the user certificate, set the certificate format to PKCS #12, and click OK.



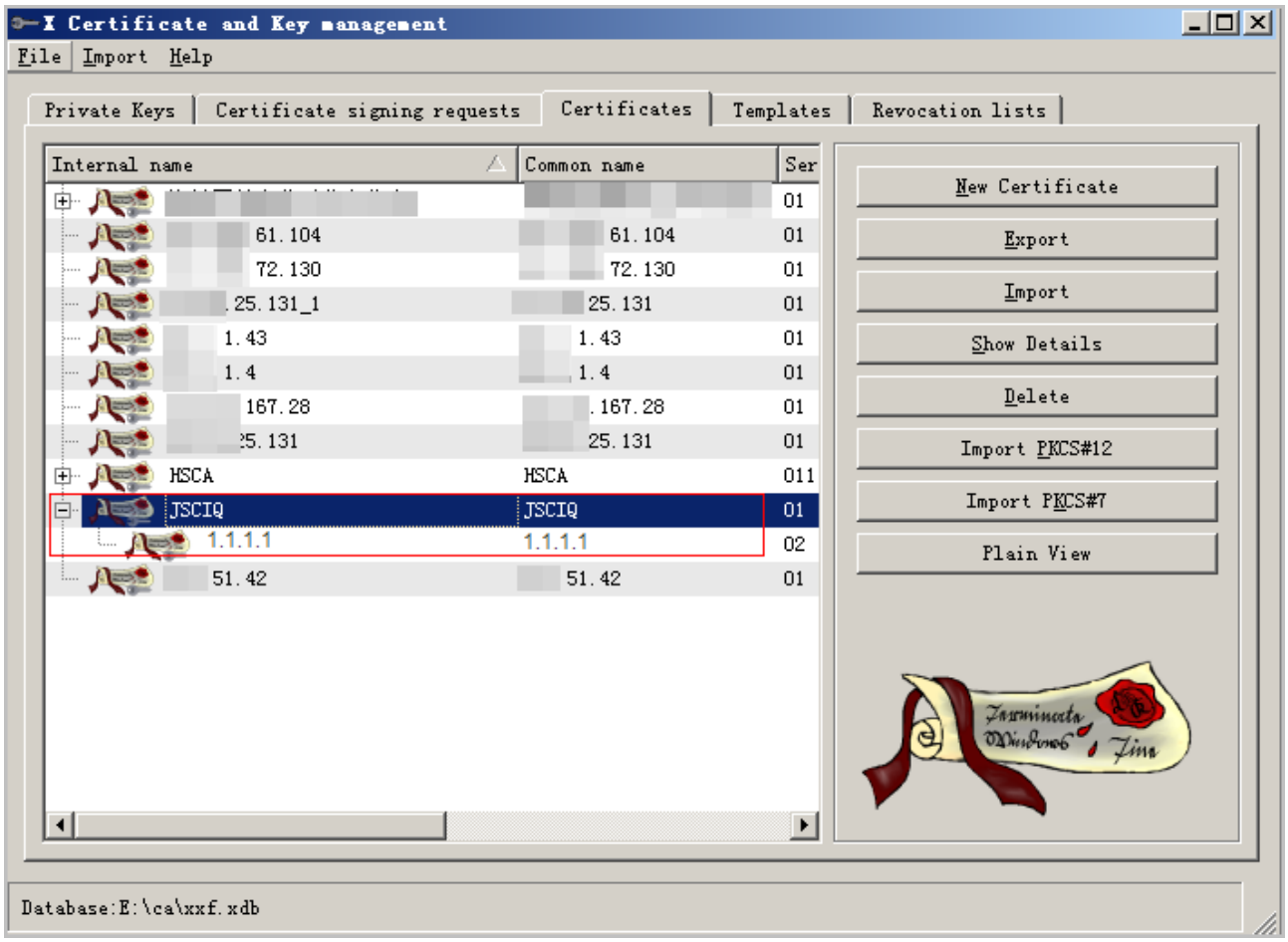
c. In the dialog box displayed, leave the password blank and click OK.

d. The certificate wangt is displayed in G:\ca.

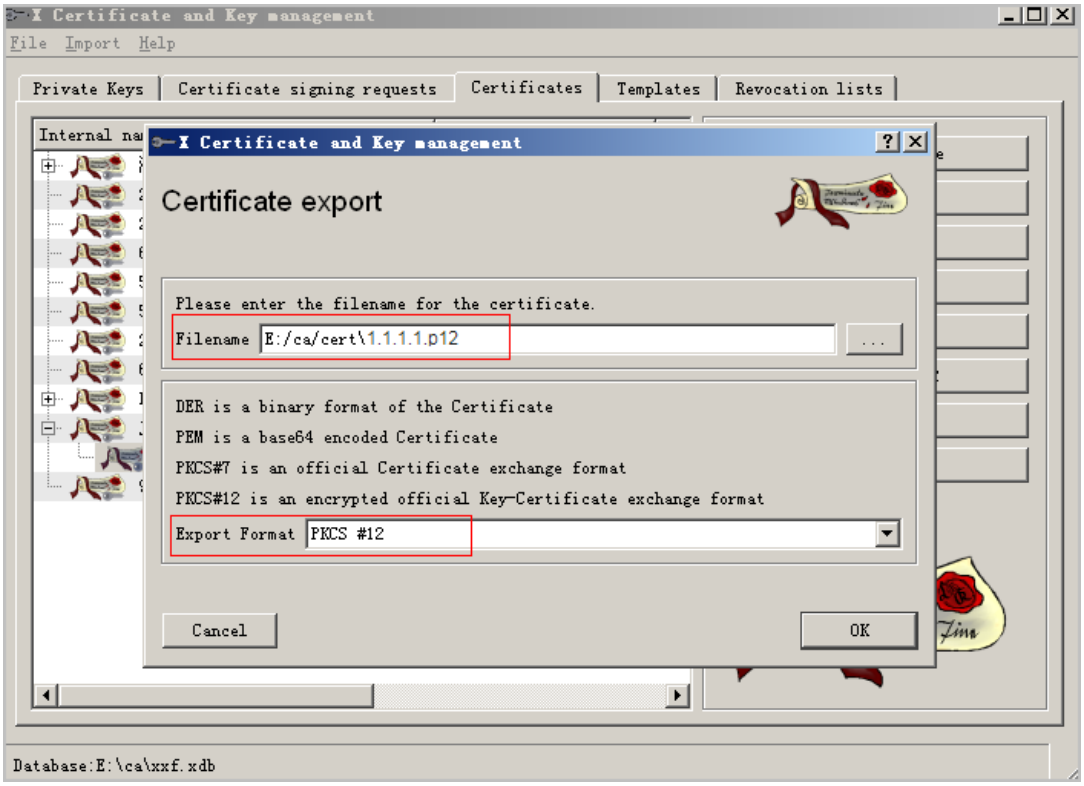


- Export a device certificate.

  a. On the Certificates tab, select the device certificate 1.1.1.1 and click Export



  b. Specify a path for saving the certificate, set the certificate format to PKCS #12, and click OK.



c. In the dialog box displayed, leave the password blank and click OK.

d. The certificate 1.1.1.1.p12 is displayed in E:\ca\cert.

1.5.7 Are Administrator Rights Required for Installing and Running the SecoClient?

To install the UniVPN, you must have the administrator rights.

To run the UniVPN, you do not need to have the administrator rights. Common users are allowed to run the UniVPN.

1.5.8 Can I Change the Account Password on the Terminal After the Dialup Is Successful on the SSL VPN Client?

Yes. Perform the following steps to modify the password.

1. Right-click the icon of the client from System Tray and choose Change Password from the shortcut menu.
2. In the Change Password dialog box, change the login password.

NOTE

The password can be changed only when a VPN connection has been established between UniVPN and a peer gateway.

After the password is changed successfully, the current VPN connection is disconnected. You need to use the new password to log in again.

1.5.9 Why Do I Need to Upload an ActiveX Control to a Device in Advance?

When a terminal user logs in to a virtual gateway through the Internet Explorer kernel browser to use the SSL VPN service, the user needs to download and install a related ActiveX control. The firewall of an earlier version packs the ActiveX control in the software package of the gateway. Therefore, you do not need to upload the ActiveX control in advance.

The ActiveX control is released separately for devices since the following versions. Therefore, you need to upload the ActiveX control to the device in advance.

- V600R007C00: For models excluding the USG6630E/6650E, USG6680E, USG6712E/6716E, an administrator needs to upload the ActiveX control to the device in advance.
- V600R007C20: For the versions earlier than V600R007C20SPC300 and the models except the USG6391E/6610E/6620E, USG6630E/6650E, USG6680E, USG6712E/6716E, an administrator needs to upload the ActiveX control to the device in advance. For V600R007C20SPC300 and later versions and all models, an administrator needs to upload the ActiveX control to the device in advances.
- V500R005C20: Only the USG9500 require an administrator to upload the ActiveX control to the device in advance.

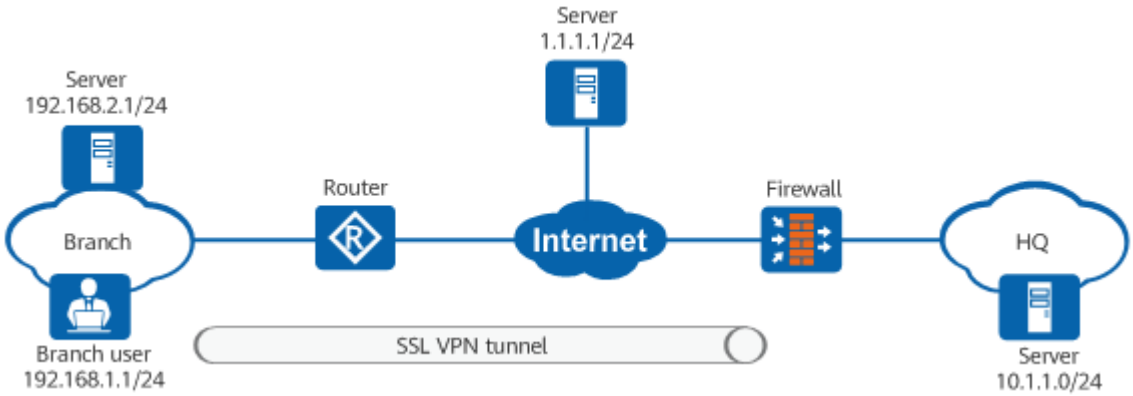
1.5.10 Which Network Extension Routing Mode Has a Higher Priority, in the Virtual Gateway Service View or Virtual Gateway User Group View?

If the routing mode is configured in both the virtual gateway service view and virtual gateway user group view, the routing mode configured in the latter view takes effect.

1.5.11 What Are the Differences Between the Routes Generated by the Terminal in the Three Routing Modes of SSL VPN Network Extension?

The network extension service of SSL VPN provides three routing modes: manual, split, and full routing.

After network extension is enabled, the firewall advertises routes to branch users based on the configured routing mode. The routing mode determines the range of resources that users can access.



Assume that the IP address obtained by the user from the firewall is 6.6.6.1/24 (IP address of the vNIC) and the next-hop IP address of the route is 192.168.1.2.

1.5.11.1 Manual Routing Mode

Routing Mode	Command	Routes Generated on the User Side	Access Service
Manual routing mode	network-extension mode manual network-extension manual-route 10.1.1.0 255.255.255.0 If the manual routing mode is selected, you must specify the Intranet network segment that users access.	Only the traffic destined for the headquarters (10.1.1.0/24) can pass through the vNIC 6.6.6.1 and enter the SSL VPN tunnel. The routes to the Internet and LAN remain unchanged.	Users can access all of the LAN, Internet, and enterprise intranet.

```
 IPv4 Route Table

===========================================================================
===========================
 Active Routes:
 Network Destination          Netmask          Gateway          Interface
Metric
      0.0.0.0            0.0.0.0     192.168.1.2      192.168.1.2      10
//Route for accessing the Internet
        6.6.6.1       255.255.255.255          On-link             6.6.6.1
257
       10.1.1.0         255.255.255.0          On-link             6.6.6.1        1
//Route for accessing the enterprise intranet
     10.1.1.255       255.255.255.255          On-link             6.6.6.1
257
   192.168.2.0       255.255.255.0     192.168.1.2      192.168.1.2      11
//Route for accessing the LAN

===========================================================================
===========================
```

1.5.11.2 Split Routing Mode

Routing Mode	Command	Routes Generated on the User Side	Access Service
Split routing mode	network-extension mode split	The IP address of the outbound interface of the default route is changed to the vNIC IP address. As a result, users cannot access the Internet. Users can still access the LAN because the route to the LAN remains unchanged.	Users can access only the LAN and enterprise intranet, but not the Internet.

```
 IPv4 Route Table

===========================================================================
===========================
 Active Routes:
 Network Destination          Netmask          Gateway          Interface
Metric
      0.0.0.0            0.0.0.0        On-link          6.6.6.1         1
//Route for accessing the enterprise intranet
        6.6.6.0         255.255.255.0         On-link             6.6.6.1
257
        6.6.6.1       255.255.255.255         On-link             6.6.6.1
257
      6.6.6.255       255.255.255.255         On-link             6.6.6.1
257
   192.168.2.0       255.255.255.0     192.168.1.2       192.168.1.2        11
//Route for accessing the LAN

===========================================================================
===========================
```

1.5.11.3 Full Routing Mode

Routing Mode	Command	Routes Generated on the User Side	Access Service
Full routing mode	network-extension mode full	The IP addresses of the outbound interfaces of almost all routes are changed to the vNIC IP address. This means that all traffic from users enters the SSL VPN tunnel. The route to 192.168.2.0 (local LAN) still exists in the routing table. The cost of the route is 11, but the cost of the route delivered by the firewall is 1. Therefore, the route to 192.168.2.0 does not take effect.	Users can access only the enterprise intranet, but not the LAN or Internet.

```
 IPv4 Route Table

===========================================================================
===========================================
 Active Routes:
 Network Destination                Netmask            Gateway
Interface        Metric
          0.0.0.0                0.0.0.0          On-link                6.6.6.1
1    //Route for accessing the enterprise intranet
          6.6.6.0          255.255.255.0          On-link                6.6.6.1
257    //Route for accessing the enterprise intranet
          6.6.6.1        255.255.255.255          On-link                6.6.6.1
257    //Route for accessing the enterprise intranet
        6.6.6.255        255.255.255.255          On-link                6.6.6.1
257    //Route for accessing the enterprise intranet
       192.168.2.0          255.255.255.0       192.168.1.2            192.168.1.2
11    //Route for accessing the enterprise intranet
       192.168.2.0          255.255.255.0          On-link                6.6.6.1
1    //Route for accessing the enterprise intranet
     192.168.2.255        255.255.255.255          On-link                6.6.6.1
257    //Route for accessing the enterprise intranet

===========================================================================
===========================================
```

The SSL VPN network extension service provides the following routing modes:

- In manual routing mode, the subnet of the headquarters network must be clearly defined and can be accessed through the SSL VPN vNIC. In addition, the intranet and Internet can be accessed when they are accessible.
- In split routing mode, the internal LAN continues to be accessible because the local LAN gateway is not changed. However, the Internet and HQ subnet can be accessed through the vNIC. This is why the SSL VPN client loses Internet access. You need to configure a proxy server in the HQ to provide Internet access for the SSL VPN client.
- In full routing mode, all traffic (destined for the Internet, intranet, and HQ subnet) is forwarded through the vNIC route of the SSL VPN. This is why only the HQ subnet can be accessed and the intranet and Internet cannot be accessed in this mode. (The Internet can provide the proxy server again at the HQ, for example, in the tunnel splitting scenario.).

NOTE

The routes delivered by the client in the same routing mode vary according to the operating system running on the client. The actual delivered route is used.

1.5.12 Does SSL VPN Support Two-Factor Authentication?

Yes. SSL VPN supports the following types of two-factor authentication:

1. RADIUS two-factor authentication: The firewall interworks with a RADIUS server to authenticate SSL VPN users. This authentication requires users to enter dynamic verification codes in addition to their user names and static PIN codes. The dynamic verification codes can be SMS verification codes or dynamic passwords generated by tokens.

2. Certificate-challenge authentication: combines client certificate authentication with local or server authentication.

1.5.13 What Can I Do If the vNIC Cannot Be Generated After I Log In to the Client Through Dialup?

Some drivers of SecoClient of an earlier version are incompatible with an operating system, which may cause this problem.Install the latest version of UniVPN.

1.5.14 Which SSL VPN Commands Can Be Used to Collect Debug Logs?

You are advised to run the debugging sslvpn-user allv-gateway-name user-name command to collect debug logs. This command can be used to enable the debug log function for all service accesses.

1.5.15 Do If the Delay of Pinging the Intranet Is Long After SSL VPN-based Access Is Performed?

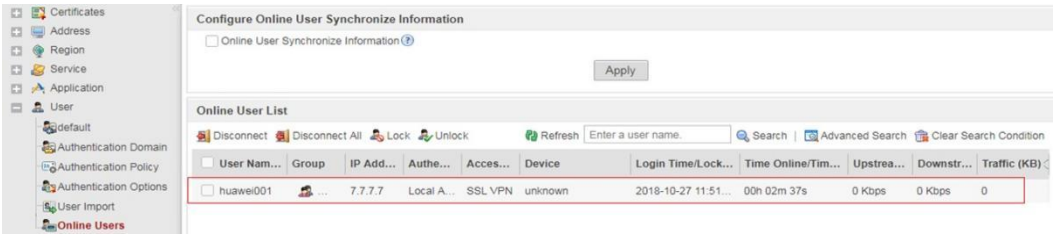
After a user accesses the intranet through the SSL VPN, the delay for pinging the intranet is long. The possible causes are as follows.

- A security policy configured on the firewall does not permit UDP packets of port 443 from the Untrust zone to the Local zone.When the terminal accesses the SSL VPN virtual gateway in fast transmission mode, UDP and its port 443 are used. As such, you need to configure a security policy on the firewall to permit UDP packets of port 443 from the Untrust zone to the Local zone. If the SSL VPN virtual gateway is deployed on the intranet and connected to a NAT device that is connected to the external network, configure a mapping entry containing UDP and its port 443 on the NAT device.
- HTTPS flood attack defense is configured on the firewall, and the threshold is too low.Run the display anti-ddos defend information system command to check whether HTTPS flood attack defense is enabled and view its threshold. You can run the anti-ddos https-flood source-detect alert-rate alert-rate command to change the threshold.

1.5.16 What Is the Correlation Between SSL VPN and User Management?

When the web proxy, port forwarding, or file sharing service is used, user information is not displayed in the online user list. Users get online and user information is displayed in the online user list only when a network extension service is used.

To view online SSL VPN users on the web page, choose User > Online Users or choose SSL VPN > Monitor.



You can also run CLI commands to view online users.

- Run the display onlineuser command in the basic view of the virtual gateway.
- Run the display user-manage online-user command in the system view.If you deregister a user in the online user list in user management or disconnect a user in SSL VPN monitoring, the user is forced to go offline.

1.5.17 What Is the Knowledge of SSL VPN Role Authorization?

The default role of the virtual gateway can only be edited but cannot be deleted. By default, this role is not allowed to access any intranet resources.

In USG6000 V100, the default role can access any intranet resources. Pay attention to this difference when you upgrade USG6000 V100 to V500.

A user logs in to the SSL VPN virtual gateway. If the user or user group is not added to any user-defined role, the default role applies.

If server authorization is configured for the authentication domain used for SSL VPN dialup, the authorization group is identified as follows:

1. If the user with the same user name already exists locally, the parent group of this user is used during authorization.
2. If the user with the same user name does not exist locally, check whether New User Authentication Options is configured.
   a. New User Authentication Options is not configured.

      The parent group of the user configured on the authorization server is used for authorization.
   b. New User Authentication Options is configured.

      If Prohibit New User Login is selected, the user login request is rejected, and the authorization process is terminated.

      If Add to User Group or Security Group is selected, the specified parent group is used for authorization.

      If Use It as a Temporary One and Do Not Add It to the Local User List is selected, the specified parent group is used for authorization.

1.5.18 How to Perform User-specific Permission Control After SSL VPN Authentication Is Successful?

Perform the following steps:

1. Configure an authentication-exempt policy for data flows that access intranet resources from the network extension address pool.
2. Bind the security policy to the user or user group.

1.5.19 How Do I Trace the Source of Unauthorized Operations After an SSL VPN User Accesses a Device?

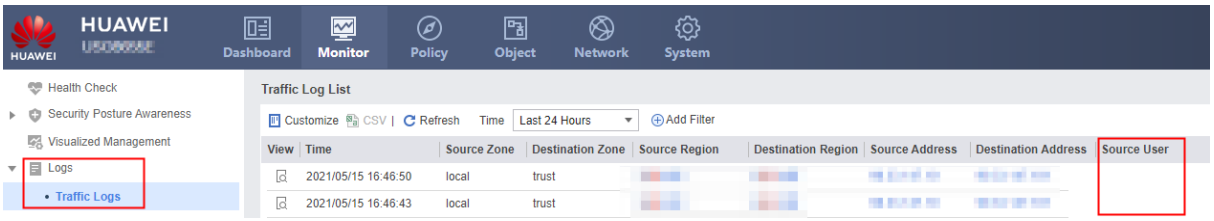
At a certain time, a user accesses the intranet through the SSL VPN, obtains a virtual IP address, and uses the virtual IP address to interact with the intranet server. If the SSL VPN user performs unauthorized operations on the intranet server, source tracing is required to locate the user.

Perform the following steps to trace the source.

1. View system logs to obtain the mapping between virtual IP addresses and user accounts.
   a. Choose Monitor > Logs > Traffic Logs from the main menu.
   b. Search for logs starting with USERS/5/NESRV. Information similar to the following is displayed.

```
Log information is recorded after the user logged in to the device successfully through the SSL VPN and enabled network extension:
%2000-04-02 01:35:41 USG6300 %%01USERS/5/NESRV(l): id=USG6320Eedemon time="2000-04-02 01:35:40" fw=USG6300 pri=5 vsys=root vpn=gateway user="huawei001" src=11.11.11.2 dst=11.11.11.1 duration=0s rcvd=0byte(s) sent=0byte(s) type=vpn service=1 msg="Network Extension: Service startup, the virtual IP address is 13.13.13.102."

Log information is recorded after the user logged in to the device successfully through the SSL VPN and disabled network extension:
%2000-04-02 01:35:59 USG6300 %%01USERS/5/NESRV(l): id=USG6320Eedemon time="2000-04-02 01:35:40" fw=USG6300 pri=5 vsys=root vpn=gateway user="huawei001" src=11.11.11.2 dst=11.11.11.1 duration=18s rcvd=0byte(s) sent=715byte(s) type=vpn service=1 msg="Network Extension: Service shutdown, the virtual IP address is 13.13.13.102."
```

2. Check whether an authentication policy is configured on the firewall. If an authentication-free policy is configured for the traffic of SSL VPN users accessing the intranet server, the traffic logs generated for such traffic contain user information.



1.5.20 What Are Authorization Rules in the SSL VPN Server Authentication Scenario?

Authorization rules in the server authentication scenario include local and server authorization rules.

Local Authorization

Assume that the local authorization configuration is as follows.

```
#
domain icf.local
```

```
 authentication-scheme admin_ldap
 authorization-scheme local
 service-scheme webServerScheme
 ldap-server ldapserver2
 service-type internetaccess ssl-vpn l2tp
 internet-access mode password
 reference user current-domain
#
```

If the test001@icf.local user exists, the authorization rules are as follows:

The virtual IP address is bound to the test001@icf.local user, which takes effect.

The test001@icf.local user is bound to a user-defined role. The user can match the role.

The direct parent group of the test001@icf.local user on the local device is bound to a user-defined role. The user can match the role.

The indirect parent group of the test001@icf.local user on the local device is bound to a user-defined role. The user does not match the role.

The direct parent group of the test001@icf.local user on the authentication server is bound to a user-defined role. The user does not match the role.

The indirect parent group to which the test001@icf.local user belongs on the authentication server is bound to a user-defined role. The user does not match the role.

If the test001@icf.local user does not exist, the authorization rules are as follows:

The direct parent group of the test001@icf.local user on the authentication server is bound to a user-defined role. The user does not match the role.

The indirect parent group to which the test001@icf.local user belongs on the authentication server is bound to a user-defined role. The user does not match the role.

Find the role bound to the icf.local root group. If no role is bound to the icf.local root group, the default role is matched.

Server Authorization

Assume that the server authorization configuration is as follows.

```
#
 domain icf.local
  authentication-scheme admin_ldap
  authorization-scheme ldap
  service-scheme webServerScheme
  ldap-server ldapserver2
  service-type internetaccess ssl-vpn l2tp
  internet-access mode password
  reference user current-domain
#
```

If the test001@icf.local user exists, the authorization rules are as follows:

The virtual IP address bound to the test001@icf.local user, which does not take effect.

The test001@icf.local user is bound to a user-defined role. The user does not match the role.

The direct parent group of the test001@icf.local user on the local device is bound to a user-defined role. The user can match the role.

The indirect parent group of the test001@icf.local user on the local device is bound to a user-defined role. The user does not match the role.

The direct parent group of the test001@icf.local user on the authentication server is bound to a user-defined role. The user does not match the role.

The indirect parent group to which the test001@icf.local user belongs on the authentication server is bound to a user-defined role. The user does not match the role.

If the test001@icf.local user does not exist, the authorization rules are as follows:

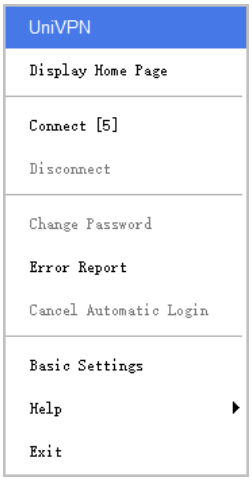
The direct parent group of the test001@icf.local user on the authentication server is bound to a user-defined role. The user can match the role.

The indirect parent group to which the test001@icf.local user belongs on the authentication server is bound to a user-defined role. The user does not match the role.

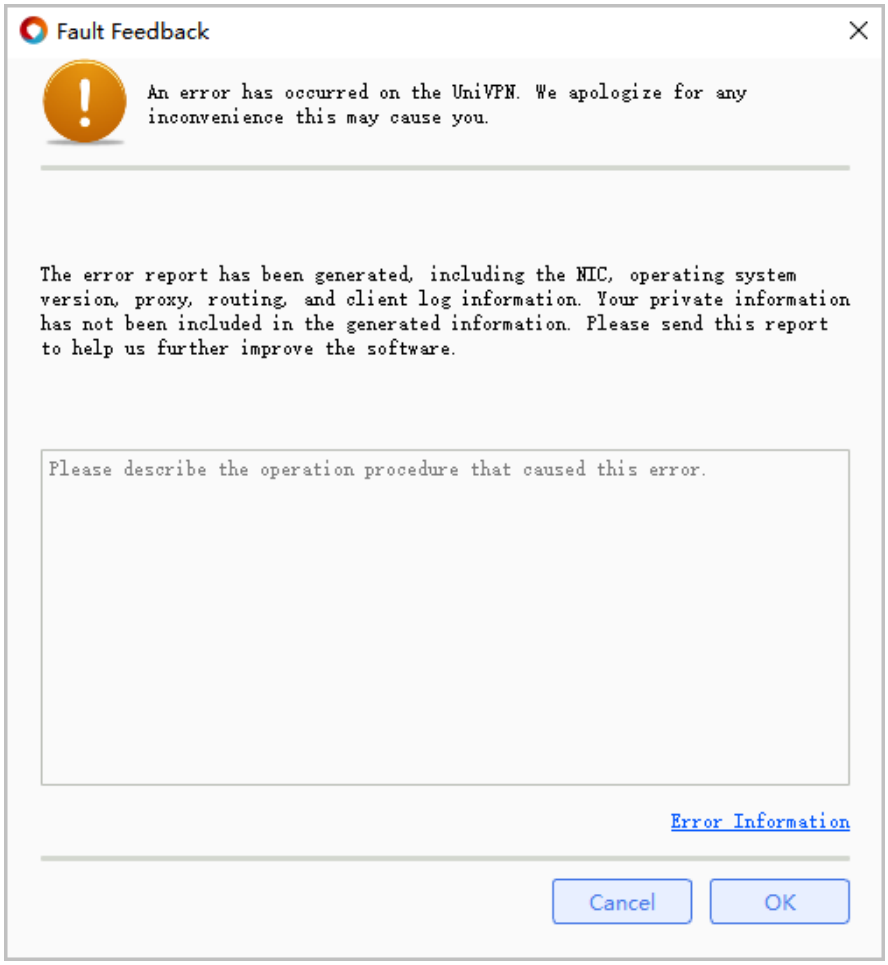
1.5.21 How to Collect UniVPN Logs?

Collection method on PCs

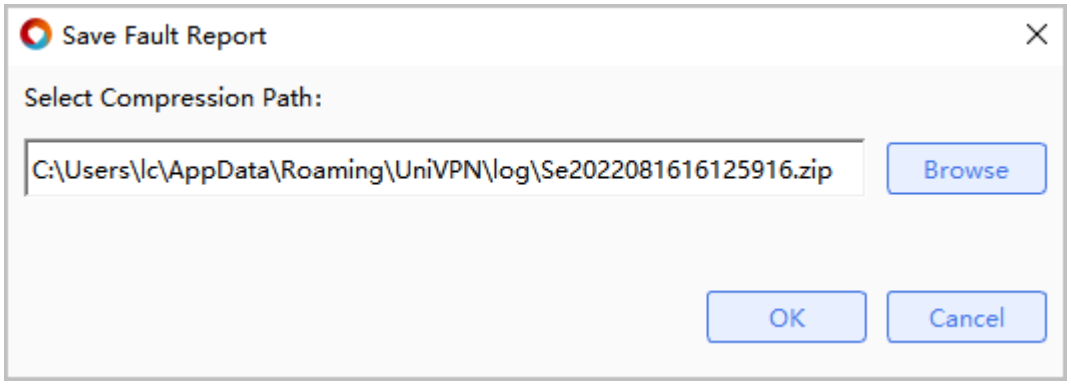
1. Right-click the UniVPN icon on the tray.



2. Select **Error Report**.



3. Enter the fault title and operation procedure as prompted.
4. Click **OK** and wait for the log package to be generated.



5. Click **Browse** to select the file save path.

The UniVPN collects client software usage information when generating error reports. Take proper measures to ensure that the following information is strictly protected:

- **error_detail.txt**: records the operation steps (manually input by a user) that cause an error, and the client version used.

- **netcard_info.txt**: records NIC information on the PC where the UniVPN is installed.
- **operate_system_info.txt**: records operating system information on the PC where the UniVPN is installed.
- **proxy_info.txt**: records proxy server information on the PC where the UniVPN is installed.
- **route_info.txt**: records routing information on the PC where the UniVPN is installed.
- **UniVPN_UniVPNCS_0.log**: records log information, such as login success or failure, VPN tunnel setup success or failure, generated during the UniVPN service configuration.
- **UniVPN_UniVPNUI_0.log**: records log information, such as VPN connection configuration and Chinese/English interface switching, generated on the UniVPN configuration page.
- **UniVPN_UniVPNPromoteService_0.log**: records log information about UniVPN service processes to ensure the normal running of the UniVPN.
- **Crash file**: is created when the UniVPN is terminated unexpectedly. The crash file name varies according to the exception cause. In the Windows system, the file name extension of a crash file is .dmp, while in the MAC operating system, the file name extension of a crash file is .core.

1.5.22 What Are Common SSL VPN Service Logs?

When a network exception occurs, the network administrator needs to locate the fault based on logs. The following lists common SSL VPN service logs:

Log recording SSL VPN login failures:

%2000-04-02 01:27:17 sysname %%01USERS/4/USRPWDERR(l): id=sysname time="2000-04-02 01:27:13" fw=sysname pri=4 vsys=root vpn=gateway user="huawei001" src=11.11.11.2 dst=0.0.0.0 duration=3s rcvd=0byte(s) sent=0byte(s) type=vpn service=5 msg="Session: huawei001 failed to login."

Log recording SSL VPN login successes:

%2000-04-02 01:35:34 sysname %%01USERS/5/LOGINSUC(l): id=sysname time="2000-04-02 01:35:33" fw=sysname pri=5 vsys=root vpn=gateway user="huawei001" src=11.11.11.2 dst=0.0.0.0 duration=0s rcvd=0byte(s) sent=0byte(s) type=vpn service=5 msg="Session: huawei001 logged in."

Log recording logout from the SSL VPN:

%2000-04-02 01:36:00 sysname %%01USERS/5/LOGOUT(l): id=sysname time="2000-04-02 01:35:59" fw=sysname pri=5 vsys=root vpn=gateway user="huawei001" src=11.11.11.2 dst=0.0.0.0 duration=26s rcvd=0byte(s) sent=715byte(s) type=vpn service=5 msg="Session: huawei001 logged out."

Log recording a user who succeeds in logging in to the SSL VPN and enabling network extension:

%2000-04-02 01:35:41 sysname %%01USERS/5/NESRV(l): id=sysname time="2000-04-02 01:35:40" fw=sysname pri=5 vsys=root vpn=gateway user="huawei001" src=11.11.11.2 dst=11.11.11.1 duration=0s rcvd=0byte(s) sent=0byte(s) type=vpn service=1 msg="Network Extension StartUp, The virtual IP adddress is 13.13.13.102."

Log recording a user who succeeds in logging in to the SSL VPN and disabling network extension:

%2000-04-02 01:35:59 sysname %%01USERS/5/NESRV(l): id=sysname time="2000-04-02 01:35:40" fw=sysname pri=5 vsys=root vpn=gateway user="huawei001" src=11.11.11.2 dst=11.11.11.1 duration=18s rcvd=0byte(s) sent=715byte(s) type=vpn service=1 msg="Network Extension: The virtual IP adddress is 13.13.13.102."

Log recording a user who succeeds in logging in to the SSL VPN login and changing the password:

%2000-04-02 01:35:21 sysname %%01USERS/5/CHGPWDKICK(l): id=sysname time="2000-04-02 01:35:20" fw=sysname pri=5 vsys=root vpn=gateway user="huawei001" src=11.11.11.2 dst=0.0.0.0 duration=36s rcvd=0byte(s) sent=636byte(s) type=vpn service=5 msg="User huawei001 was forcibly logged out, for the password was successfully modified."

Log recording that the network extension function is enabled by a user, who then logged out by the administrator:

%2000-04-02 01:36:00 sysname %%01USERS/5/LOGOUT(l): id=sysname time="2000-04-02 01:35:59" fw=sysname pri=5 vsys=root vpn=gateway user="huawei001" src=11.11.11.2 dst=0.0.0.0 duration=26s rcvd=0byte(s) sent=715byte(s) type=vpn service=5 msg="Session: huawei001 logged out with virtual IP address 13.13.13.102."

Log recording user logout due to session aging out:

%2000-04-02 02:10:00 sysname %%01USERS/5/EXPIREUSER (l): id=sysname time="2000-04-02 01:09:59" fw=sysname pri=5 vsys=root vpn=gateway user="huawei001" src=11.11.11.2 dst=0.0.0.0 duration=26s rcvd=0byte(s) sent=715byte(s) type=vpn service=5 msg="User huawei001 was forcibly logged out for the user ages."

Log recording resource access by SSL VPN users:

[sysname] v-gateway test

[sysname-test] service

Note: After the network extension log function is enabled, the gateway records a connection log each time the client establishes a TCP connection with the intranet server through network extension. If the TCP connection is frequently established, a great deal of log information is generated by the gateway, which affects query for other log information.

[sysname-test-service] network-extension log enable //Enable the network extension log function.

1.5.23 Are Users Forced to Log Out When SSL VPN Network Extension Settings Are Changed?

When the administrator adds, changes, or deletes a manual routing network segment for network extension services, online users of the virtual gateway are forced to log out.

When the administrator adds a network segment to the network extension address pool, online users of the virtual gateway are not logged out.

When the administrator deletes or modifies a network segment of the network extension address pool, the users whose IP addresses are allocated from this segment are forced to log out. The users whose IP addresses are not allocated from this segment are not logged out.

1.5.24 How Is the Interzone Relationship of SSL VPN Service Packets Determined?

SSL VPN provides web proxy, file sharing, port forwarding, and network extension services. The traffic of the web proxy, file sharing, and port forwarding services passes through the Local zone to the Trust zone. Trust indicates the security zone to which the firewall interface connected to the intranet belongs.

When an SSL VPN user accesses intranet resources using a network extension service, the firewall searches for the route to the public IP address of the user and finds an outbound interface. The security zone where the outbound interface resides is the source security zone for network extension service traffic. In the multi-egress scenario, multiple outbound interfaces may exist for the route. You need to configure the security zones where the outbound interfaces reside as the source security zones. The firewall searches for a route to the destination IP address of the network extension service traffic and uses the security zone where the outbound interface resides as the destination security zone.

1.5.25 Can I Access the Firewall Intranet Interface Address for Device Management After SSL VPN Login?

Yes.

Noted that in hot standby networking, you can use the intranet interface address of the active firewall for device management after logging in to the active firewall through SSL VPN dialup, but cannot manage the standby firewall in the same way. To manage the standby firewall, use the intranet bastion host or intermediate device to jump to the standby firewall.

If a management interface is bound to a VPN instance, the management interface cannot be accessed after the SSL VPN dialup connection is set up. In this case, you need to access the management interface through the intermediate device or access the intranet interface that is not bound to any VPN instance.

1.5.26 Which SSL VPN Configurations Can Be Backed Up in Hot Standby Networking?

Some SSL VPN configurations are displayed in Buildrun mode, and other configurations are saved in the database. For example, the maximum number of virtual gateway users, maximum number of virtual gateway resources, virtual gateway device certificate, and user/user group bound to the virtual gateway role, are not contained in the configuration file. You need to log in to the device to view these configurations.

In hot standby networking, SSL VPN configurations can be backed up, including adding users/user groups, creating roles, binding roles to users/user groups, unbinding roles from users/user groups, deleting roles, and deleting users/user groups in SSL VPN role authorization.

1.5.27 Does SSL VPN Support IPv6?

No.

1.5.28 What Are the Browsers Supported by SSL VPN Controls?

Currently, the mainstream browser kernels are as follows:

Trident kernel: Common browsers include Internet Explorer.

Gecko kernel: Common browsers include Mozilla Firefox.

Webkit kernel: Common browsers include Apple Safari(Win/Mac/iPhone/iPad)and Maxthon 3.

Blink kernel: Common browsers include Chrome and Opera.

Edge kernel: Common browsers include Edge.

Most of the new browsers in China are dual-core or even multi-core, including Trident and other kernels. Generally, other kernels are called quick mode, while the Trident kernel is called compatibility mode. Users can switch between the two modes.

360 Secure Browser (Trident+Blink)

360 Speed Browser (Trident+Blink)

Cheetah Safe Browser (Trident+Blink)

Maxthon Browser (Trident+Webkit)

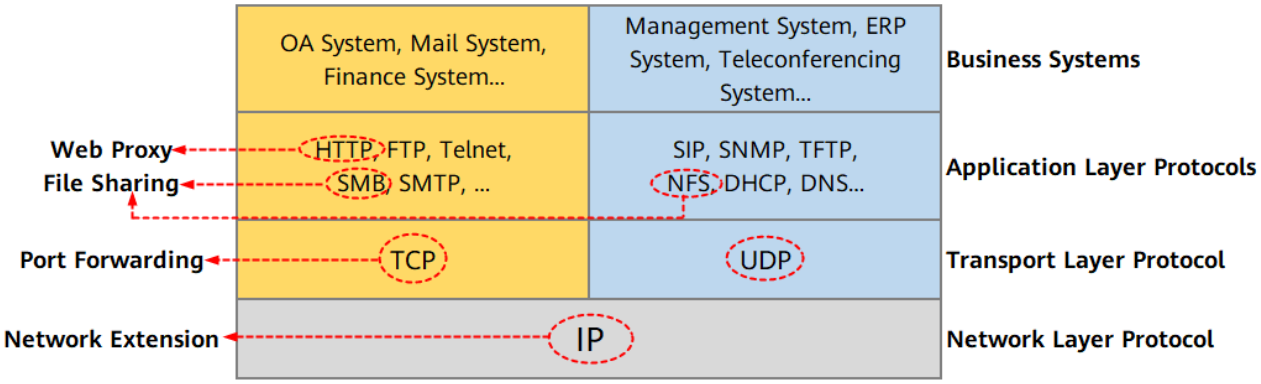
TheWorld Browser (Trident+Blink)

Sogou Browser (Trident+Webkit)

UC browser (Trident+Blink)

Currently, the SSL VPN features (web-link, port forwarding, network extension, and host check) are available only on the Internet Explorer kernel (that is, the Trident kernel) browser with ActiveX installed.

1.5.29 What Are the Application Scenarios of SSL VPN Features?



Web proxy: used to access intranet web resources.

File sharing: used to access shared resources of intranet system servers.

Port forwarding: used to access resources enabled on the TCP application server of the intranet.

Network extension: used to access all IP resources of the intranet.

1.5.30 Does SSL VPN Allow the VPN Clients from Other Vendors to Dial Up?

The SSL VPN private headers defined by each vendor are different. Therefore, the VPN clients of different vendors and the SSL VPN gateway cannot access each other.

1.5.31 What Are the Differences Between SSL VPN and SVN?

SSL VPN Category	SSL VPN Item	FW Model	SVN Model
Virtual gateway	License control over virtual gateway	The virtual gateway is not license controlled but is determined by device models.	The virtual gateway is license controlled. By default, one virtual gateway license is provided.
	Virtual gateway created in the public system	Supported	Not supported. All virtual gateways are created in the virtual system.

SSL VPN Category	SSL VPN Item	FW Model	SVN Model
Authentication and authorization	Multi-level authentication	Not supported	Supported. Three-level authentication is supported at most.
	Separated authorization and authentication.	Not supported	Supported
	Multiple authentication domains	Supported	Not supported
	Access control policy	Not supported	Supported
	Correlation between security policy and user/user group	Supported	Not supported
	Denying web login	Not supported	Supported
Auxiliary authentication	Device ID	Not supported	Supported
	Image verification code	Not supported	Supported
Desktop cloud	Load balancing gateway	Not supported	Supported
	Secure cloud gateway	Not supported	Supported
User lockout	Authentication mode in user lockout	Local user only	Local user or server user
	User lockout method	User name lockout only	User name or source IP address lockout

1.5.32 How Do I Advertise Routes Destined for the SSL VPN Service Address and Network Extension Address Pools in OSPF Networking?

Assume that the following information exists.

- Network extension address pools:

```
network-extension netpool 10.23.40.1 10.23.47.254 255.255.248.0
network-extension netpool 10.23.116.1 10.23.117.254 255.255.254.0
network-extension netpool 10.23.144.1 10.23.145.254 255.255.254.0
network-extension netpool 10.23.228.1 10.23.231.254 255.255.252.0
network-extension netpool 10.23.232.1 10.23.239.254 255.255.248.0
```

```
network-extension netpool 10.23.244.1 10.23.247.254 255.255.252.0
```

- Interface address for the interconnection between the firewall and intranet switch: 10.23.249.253
- Default route configured on the firewall: ip route-static 0.0.0.0 0.0.0.0 10.23.175.249
- Interface address for interconnection between the intranet switch and firewall: 10.23.249.254

To configure OSPF to advertise the network segment routes destined for the network extension address pools to the intranet switch, perform the following steps.

```
# Configure a route to each network extension address pool.
ip route-static 10.23.40.1 255.255.248.0 10.23.175.249
ip route-static 10.23.116.1 255.255.254.0 10.23.175.249
ip route-static 10.23.144.1 255.255.254.0 10.23.175.249
ip route-static 10.23.228.1 255.255.252.0 10.23.175.249
ip route-static 10.23.232.1 255.255.248.0 10.23.175.249
ip route-static 10.23.244.1 255.255.252.0 10.23.175.249

# Configure an IP prefix list, set the matching mode of the IP prefix list to permit, and set the IP address to be
filtered to the network segments of the network extension address pools.
ip ip-prefix prefix-a index 10 permit 10.23.40.1 21
ip ip-prefix prefix-a index 20 permit 10.23.116.1 23
ip ip-prefix prefix-a index 30 permit 10.23.144.1 23
ip ip-prefix prefix-a index 40 permit 10.23.228.1 22
ip ip-prefix prefix-a index 50 permit 10.23.232.1 21
ip ip-prefix prefix-a index 60 permit 10.23.244.1 22

# Configure a route-policy named sslvpn. Set the node number to 1 and the matching mode to permit.
route-policy sslvpn permit node 1
if-match ip-prefix prefix-a

# Configure a route-policy named sslvpn. Set the node number to 100 and the matching mode to deny.
route-policy sslvpn deny node 100

# Configure OSPF to import static routes.
ospf 23 router-id 10.23.249.253
bandwidth-reference 100000
import-route static route-policy sslvpn
area 0.0.0.23
#
To configure OSPF to advertise the route to the loopback address to the external network, perform the following
steps. The SSL VPN virtual gateway uses this loopback address.
# Configure a loopback address.
interface Loopback 10
ip address X.X.X.X 32

# Configure OSPF to import static routes.
ospf 23 router-id 10.23.249.253
bandwidth-reference 100000
import-route static route-policy sslvpn
area 0.0.0.23
network X.X.X.X 0.0.0.0

# Configure the SSL VPN virtual gateway to use the loopback address.
```

```
v-gateway ssl_vpn ip address X.X.X.X
```

1.5.33 Does the SSL VPN Support Hot Standby for Load Balancing Networking?

No. The SSL VPN function is not mutually exclusive with the hot standby function. Specifically, if the SSL VPN function is configured in hot standby mode, SSL VPN traffic is still processed only by the active device. SSL VPN traffic is not load balanced.

The configured active device refers to the device with the HRP_M prefix before the command-line prompt.

The configured standby device refers to the device with the prefix HRP_S before the command-line prompt.

1.5.34 Does the SSL VPN Support Hot Standby for Active/Standby Backup?

Yes. The active firewall automatically backs up the online session information about SSL VPN users to the standby firewall. This ensures that SSL VPN users are kept online during an active/standby switchover, thereby eliminating the need to dial up again.

1.5.35 Is Authentication-Exempt Supported for SSL VPN Users?

No.

1.5.36 Does UniVPN Support Mobile Phones as Terminals?

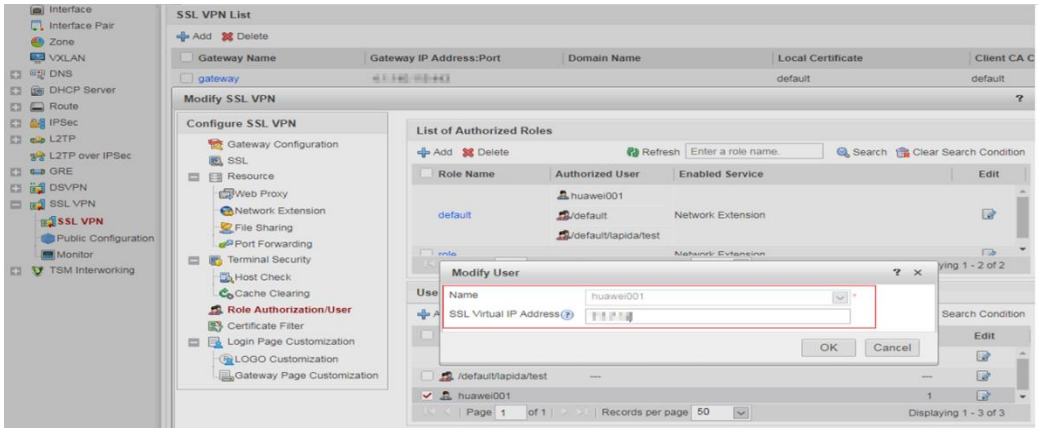
Supported.

The UniConnect client can be installed on terminals running iOS (10.0 or later) and Android (5.0 or later).

If system freezing occurs, try using a phone with a later version of the operating system.

1.5.37 How Does SSL VPN Bind Network Extension Virtual Addresses to Users?

Click Add under User/User Group List in Role Authorization/User, and then bind a virtual IP address to the user.



CLI configuration method:

[sysname] v-gateway test

[sysname-test] service

//1. Configure address pools.

[sysname-test-service] network-extension netpool 20.0.0.2 20.0.0.100 255.255.255.0

[sysname-test-service] network-extension netpool 10.0.100.2 10.0.100.200 255.255.255.0

[sysname-test] vpndb

//2.1 Add a user to the virtual gateway.

[sysname-test-vpndb] user abc

//2.2 Bind the user abc to the address 10.0.1000.100 so that when the user logs in, the IP address 10.0.100.100 is allocated to the user.

[sysname-test-vpndb] user abc virtual-ip 10.0.100.100

The firewall can also bind user groups and virtual address segments. However, the binding cannot be configured on the web page but can be configured only using CLIs.

//3.1 Add a user group to the virtual gateway.

[sysname-test-vpndb] group /default/huawei

//3.2 Bind an address pool to the user group. That is, IP addresses are allocated from the address pool 20.0.0.2-20.0.0.100 to the users in the user group huawei.

[sysname-test-vpndb] group /default/huawei network-extension netpool 20.0.0.2

1.5.38 What Is the Rule of Allocating Virtual IP Addresses in SSL VPN Network Extension?

Virtual IP address allocation priorities are as follows:

If a user is bound only to a network extension virtual IP address, this address is allocated to the user.

If a user group is bound to a network extension virtual IP address pool, virtual IP addresses in the address pool are allocated to the users in the user group.

If a user group is bound to a network extension virtual IP address pool and the users in the user group are bound to network extension virtual IP addresses, the bound virtual IP addresses are preferentially allocated to the users in the user group.

If a user does not belong to any group or if the user group is not bound to a network extension virtual IP address pool, the virtual IP address allocated to the user is from the address pool configured in the virtual gateway network extension service.

If a user group is bound to a network extension virtual IP address pool but the addresses in this pool are used by users outside the user group, these users can still use the original bound IP addresses, which does not affect online users.

Unbinding an address pool from a user group does not affect the users and online users in the user group bound to fixed addresses.

1.5.39 What Are Common Debugging Logs of SSL VPN?

- The terminal fails to verify the device certificate, and a certificate security warning is displayed.

```
[ NETC INFO 2022-01-04 14:06:36.000399 ][Administrator] [2][SSL Create][SSLConnect errno: 1,
state: error,connectSSL:-1]
[ NETC WARN 2022-01-04 14:06:36.000400 ][Administrator] [2][SSL Create
failed][ErrorCode:20][reason:Verify first error,unable to get local issuer certificate]
[ NETC WARN 2022-01-04 14:06:36.000400 ][Administrator] [2]3[xcs SSLFree begin][reason:connect
ssl error connectfd, return number is -1 pstConInf->psSsl=3792750]
[ CAUTH WARN 2022-01-04 14:06:36.000514 ][Administrator] [2][CAUTH Auth SendToGateway
failed][reason:netc connect error, code 1]
[ NETC INFO 2022-01-04 14:06:36.000517 ][Administrator] [2]4[xcs SSLFree
begin][pstConInf->psSsl=0]
[ NETC WARN 2022-01-04 14:06:36.000517 ][Administrator] [2][Socket close failed][fd:7404,errorcode
is 10035] // The certificate fails to be verified.
[ CAUTH WARN 2022-01-04 14:06:36.000518 ][Administrator] [2][Master auth failed][reason:send auth
pack to gateway error]
[ CAUTH ERROR 2022-01-04 14:06:36.000519 ][Administrator] [2][Auth login process failed][auth
master error]
[ CADM INFO 2022-01-04 14:06:36.000520 ][Administrator] [2][Normal Msg][biztype is 3 ,msgtype is
3 ,msgcode is 0x3000b]
```

- When a user logs in, the system displays a message indicating that the authentication fails because the certificate name or password is incorrect.

```
[ CAUTH INFO 2022-01-04 13:35:35.000058 ][Administrator] [2][Auth send][auth package send to
gateway successful]
[ CAUTH INFO 2022-01-04 13:35:35.000058 ][Administrator] [2][Master auth][send auth message to
gateway ok]
[ CAUTH INFO 2022-01-04 13:35:35.000059 ][Administrator] [2][Auth login process][auth master ok]
[ CAUTH INFO 2022-01-04 13:35:35.000059 ][Administrator] [2][Auth receive][auth type 0]
[ CAUTH INFO 2022-01-04 13:35:35.000059 ][Administrator] [2]uiModule = 0 iSRejCode= -5
puiCRejCode = 196609 //The user fails to be authenticated.
[ CAUTH INFO 2022-01-04 13:35:35.000059 ][Administrator] [2][Auth recv][auth master failed][reason =
196609]
[ CAUTH INFO 2022-01-04 13:35:35.000060 ][Administrator] [2][auth master exit][authType = 0]
[ NETC INFO 2022-01-04 13:35:35.000060 ][Administrator] [2]4[xcs SSLFree
begin][pstConInf->psSsl=3792750]
[ CADM INFO 2022-01-04 13:35:35.000060 ][Administrator] [2][Normal Msg][biztype is 3 ,msgtype is
3 ,msgcode is 0x30001]
```

- When a user logs in, the system displays a message indicating that the authentication fails because the user account is locked.

```
[ CAUTH    INFO     2022-01-04 14:14:48.000939 ][Administrator] [2][Auth send][auth package send to gateway successful]
[ CAUTH    INFO     2022-01-04 14:14:48.000940 ][Administrator] [2][Master auth][send auth message to gateway ok]
[ CAUTH    INFO     2022-01-04 14:14:48.000940 ][Administrator] [2][Auth login process][auth master ok]
[ CAUTH    INFO     2022-01-04 14:14:48.000940 ][Administrator] [2][Auth receive][auth type 0]
[ CAUTH    INFO     2022-01-04 14:14:48.000940 ][Administrator] [2]uiModule = 0 iSRejCode= -16 puiCRejCode = 196609 //The user account is locked.
[ CAUTH    INFO     2022-01-04 14:14:48.000941 ][Administrator] [2][Auth recv][auth master failed][reason = 196609]
[ CAUTH    INFO     2022-01-04 14:14:48.000941 ][Administrator] [2][auth master exit][authType = 0]
[ NETC     INFO     2022-01-04 14:14:48.000941 ][Administrator] [2]4[xcs SSLFree begin][pstConInf->psSsl=37668b0]
[ CADM     INFO     2022-01-04 14:14:48.000941 ][Administrator] [2][Normal Msg][biztype is 3 ,msgtype is 3 ,msgcode is 0x30001]
```

- When a user logs in, the system displays a message indicating that the authentication fails because the user does not have the network extension permission.

```
[ CAUTH    INFO     2022-01-04 14:14:48.000939 ][Administrator] [2][Auth send][auth package send to gateway successful]
[ CAUTH    INFO     2022-01-04 14:14:48.000940 ][Administrator] [2][Master auth][send auth message to gateway ok]
[ CAUTH    INFO     2022-01-04 14:14:48.000940 ][Administrator] [2][Auth login process][auth master ok]
[ CAUTH    INFO     2022-01-04 14:14:48.000940 ][Administrator] [2][Auth receive][auth type 0]
[ CAUTH    INFO     2022-01-04 14:14:48.000940 ][Administrator] [2]uiModule = 0 iSRejCode= -16 puiCRejCode = 196609 //The user account is locked.
[ CAUTH    INFO     2022-01-04 14:14:48.000941 ][Administrator] [2][Auth recv][auth master failed][reason = 196609]
[ CAUTH    INFO     2022-01-04 14:14:48.000941 ][Administrator] [2][auth master exit][authType = 0]
[ NETC     INFO     2022-01-04 14:14:48.000941 ][Administrator] [2]4[xcs SSLFree begin][pstConInf->psSsl=37668b0]
[ CADM     INFO     2022-01-04 14:14:48.000941 ][Administrator] [2][Normal Msg][biztype is 3 ,msgtype is 3 ,msgcode is 0x30001]
```

- The terminal actively logs out.

```
[ CAUTH    INFO     2022-01-04 15:42:13.000259 ][Administrator] [2][Auth send][auth package send to gateway successful]
[ NETC     INFO     2022-01-04 15:42:13.000468 ][Administrator] [2]4[xcs SSLFree begin][pstConInf->psSsl=2b17840]
[ CADM     INFO     2022-01-04 15:42:13.000469 ][Administrator] [2][cadm bizctl process][entry bizctl proc srcbiz 3 and bizctl 40]
[ CADM     INFO     2022-01-04 15:42:13.000470 ][Administrator] [2][cadm bizctl process][the biz start to exit biztype 5]
[ CADM     INFO     2022-01-04 15:42:13.000471 ][Administrator] [2][cadm bizctl process][the biztype 5 exit msg is sending. notice_biz 20]
[ CNEM     INFO     2022-01-04 15:42:13.000472 ][Administrator] [8][Cnem module proc][Enter]
[ CADM     INFO     2022-01-04 15:42:13.000474 ][Administrator] [2][cadm bizctl process][the biz start to exit biztype 8]
[ CNEM     INFO     2022-01-04 15:42:13.000474 ][Administrator] [8][Cnem module proc][Cnem module stop]
[ CADM     INFO     2022-01-04 15:42:13.000476 ][Administrator] [2][cadm bizctl process][the biztype 8 exit msg is sending. notice_biz 120]
[ CEPS     INFO     2022-01-04 15:42:13.000476 ][Administrator] [7][hostcheck pro][ceps module stop start]
```

```
[ NETC    INFO    2022-01-04 15:42:13.000478 ][Administrator] [8]4[xcs SSLFree
begin][pstConInf->psSsl=2b010b0]
[ CADM    INFO    2022-01-04 15:42:13.000480 ][Administrator] [2][cadm bizctl process][the notice has
been send to src biz 3--EXIT WAIT]//The user proactively logs out.
[ NETC    WARN    2022-01-04 15:42:13.000481 ][Administrator] [8][Socket close failed][fd:2324,errorcode
is 10035]
[ ROUTE   INFO    2022-01-04 15:42:13.000483 ][Administrator] [8][Route Recovery][start]
[ ROUTE   INFO    2022-01-04 15:42:13.000495 ][Administrator] [8][Route Recovery][Finish]
```

- The device logs out a user.

```
[ CNEM    WARN    2022-01-04 15:47:32.000364 ][Administrator] [3][Cnem handle packet from
gateway][CMDtype is KICKOUT]//The request for logging out a user from a device is received.
[ CNEM    ERROR   2022-01-04 15:47:32.000366 ][Administrator] [3][Cnem handle packet from
gateway][NEM_CMD_KICKOUT]
[ CNEM    INFO    2022-01-04 15:47:32.000367 ][Administrator] [3][Cnem send status msg to self ok]
[ CNEM    INFO    2022-01-04 15:47:32.000368 ][Administrator] [8][Cnem module proc][Enter]
[ CNEM    INFO    2022-01-04 15:47:32.000370 ][Administrator] [8][Cnem AsyncMsg BizNem Proc][Enter]
[ CNEM    INFO    2022-01-04 15:47:32.000371 ][Administrator] [8][Cnem run][Enter]
[ CNEM    INFO    2022-01-04 15:47:32.000387 ][Administrator] [8][Cnem run][the current status 145 and
msgtype 13]
[ CNEM    ERROR   2022-01-04 15:47:32.000388 ][Administrator] [8][Cnem receive or send packet
failed][goto ERR Handle]
[ NETC    INFO    2022-01-04 15:47:32.000390 ][Administrator] [8]4[xcs SSLFree
begin][pstConInf->psSsl=2b010b0]
[ ROUTE   INFO    2022-01-04 15:47:32.000391 ][Administrator] [8][Route Recovery][start]
[ ROUTE   INFO    2022-01-04 15:47:32.000404 ][Administrator] [8][Route Recovery][Finish]
```

- Keepalive times out, reconnection fails, and the user logs out.

```
[ CNEM    ERROR   2022-01-04 16:01:48.000444 ][Administrator] [8][Cnem err handle][nem module
reconnect fail]
[ CADM    INFO    2022-01-04 16:01:48.000444 ][Administrator] [2][Emergency Msg][biztype:5 msgtype:11
msgcode:0xb0002]
[ CEPS    INFO    2022-01-04 16:01:48.000493 ][Administrator] [7][eps proc][CEPS HostCheck Proc start
type 10]
[ CEPS    INFO    2022-01-04 16:01:49.000713 ][Administrator] [7][cacheclean logout][eps start logout
cache clean check end]
[ CADM    INFO    2022-01-04 16:01:49.000714 ][Administrator] [2][Normal Msg][biztype is 8 ,msgtype is
5 ,msgcode is 0x50002]
[ CADM    INFO    2022-01-04 16:01:49.000714 ][Administrator]
[5][CSDK_Send_Thread][uiMsgSourceMark:0x4000000 ->
uiMsgDestMark:0x2000000][uiModuleID:0x8000000][uiMsgType:0x2000500][uiConnetType:0x1000000][ui
MsgLength:0x0]
[ CAUTH   INFO    2022-01-04 16:01:49.000718 ][Administrator] [2][CAUTH Module Proc][in to CAUTH
Module Proc]
[ CAUTH   WARN    2022-01-04 16:01:49.000719 ][Administrator] [2][Service cert
failed][pstCAuthCtx->uiServiceCertCheck =0]
[ CADM    INFO    2022-01-04 16:01:49.000720 ][Administrator] [2][CAUTH Auth SendToGateway][no
need to set certinfo]
[ CADM    INFO    2022-01-04 16:01:49.000721 ][Administrator] [2][CAUTH Auth SendToGateway][proxy
info :0, user name:, proxy type:0]
[ NETC    WARN    2022-01-04 16:01:54.000722 ][Administrator] [2][SSL Connect failed][reason:ssl time
out, reconnect]
[ NETC    WARN    2022-01-04 16:01:59.000723 ][Administrator] [2][SSL Connect failed][reason:ssl time
out, reconnect]
[ NETC    WARN    2022-01-04 16:02:04.000724 ][Administrator] [2][SSL Connect failed][reason:ssl time
out, reconnect] //Reconnection times out.
```

[NETC ERROR 2022-01-04 16:02:04.000725][Administrator] [2][SSL Connect failed][reason:reach max reconnect time Addr: 10.19.12.120,Port: 5678]

- Complete log: The user logs in to the SSL VPN successfully.

[CADM INFO 2022-01-06 13:36:53.000070][Administrator] [4][Proxy info][ConnectType is <1>,Proxy type is <0>]//**1** indicates SSL VPN, and **0** indicates no proxy.
[CADM INFO 2022-01-06 13:36:53.000071][Administrator] [4][Proxy info][proxy is :0, user name is , proxy type is 0]
[PREF INFO 2022-01-06 13:36:53.000072][Administrator] [2][SetPrefSiteFlag]
[PREF INFO 2022-01-06 13:36:53.000073][Administrator] [2][Site pref proc][Enter]
[PREF INFO 2022-01-06 13:36:53.000074][Administrator] [2][Site Pref Preprocess SiteInfo][aucGatewayIP:10.19.12.120][uiGatewayPort:6528]
[PREF INFO 2022-01-06 13:36:53.000075][Administrator] [2]Number of sites 1
[PREF INFO 2022-01-06 13:36:53.000077][Administrator] [2][Default getway Index in configuration file is 0]
[PREF INFO 2022-01-06 13:36:53.000078][Administrator] [2][Default getway Index is 0]
[PREF INFO 2022-01-06 13:36:53.000096][Administrator] [39][Site pref thread enter][Site order is 0]
[PREF INFO 2022-01-06 13:36:53.000097][Administrator] [39][Park RequestPack][pstFirstConnRequest->ucDomain][10.19.12.120]
[PREF INFO 2022-01-06 13:36:53.000098][Administrator] [39][SITE_FirstConn_RequestPack over]
[CAUTH INFO 2022-01-06 13:36:53.000099][Administrator]
[CAUTH INFO 2022-01-06 13:36:53.000099][Administrator] [39][cauth][get the gateway ip is 10.19.12.120 and port is 6528 from domain name]
[CAUTH INFO 2022-01-06 13:36:53.000099][Administrator] [39][Addr info][ip address is valid]
[CAUTH INFO 2022-01-06 13:36:53.000099][Administrator] [39][cauth][get the gateway ip is 10.19.12.120 and port is 6528 from domain name]
[CAUTH INFO 2022-01-06 13:36:53.000100][Administrator]
[CAUTH INFO 2022-01-06 13:36:53.000100][Administrator] [39][cauth][get the gateway ip is 10.19.12.120 and port is 6528 from domain name]
[CAUTH INFO 2022-01-06 13:36:53.000100][Administrator] [39][Addr info][ip address is valid]
[PREF INFO 2022-01-06 13:36:53.000100][Administrator] [39][SITE FirstConn SendAndRecv][aucDomainName:10.19.12.120:6528]
[PREF INFO 2022-01-06 13:36:53.000100][Administrator] [39][SITE FirstConn SendAndRecv][aucDstDomain:10.19.12.120:6528]
[PREF INFO 2022-01-06 13:36:53.000101][Administrator] [39][SITE FirstConn SendAndRecv][!!!!!!!!!]
[PREF INFO 2022-01-06 13:36:53.000101][Administrator] [39][SITE FirstConn SendAndRecv][conn->aucHostName:10.19.12.120]
[PREF INFO 2022-01-06 13:36:53.000101][Administrator] [39][NETC_Socket_Connect] Begin!
[NETC INFO 2022-01-06 13:36:53.000102][Administrator] [39][SSL Create][Success]// SSL handshake is successful.
[NETC INFO 2022-01-06 13:36:54.000704][Administrator] [2][NETC SSL Create][connect][connectSSL == -1]
[NETC WARN 2022-01-06 13:36:54.000705][Administrator] [2][SSL Create][SSL_ERROR_WANT_READ continue][retry 19999]
[NETC INFO 2022-01-06 13:36:54.000706][Administrator] [2][SSL Create][SSLConnect errno: 1, state: error,connectSSL:-1]
[NETC WARN 2022-01-06 13:36:54.000706][Administrator] [2][SSL Create failed][ErrorCode:19][reason:Verify first error,self signed certificate in certificate chain]
[NETC WARN 2022-01-06 13:36:54.000706][Administrator] [2]3[xcs SSLFree begin][reason:connect ssl error connectfd, return number is -1 pstConInf->psSsl=2b5b3e0]
[CAUTH WARN 2022-01-06 13:36:54.000706][Administrator] [2][CAUTH Auth SendToGateway failed][reason:netc connect error, code 3]
[NETC INFO 2022-01-06 13:36:54.000706][Administrator] [2]4[xcs SSLFree begin][pstConInf->psSsl=0]
[NETC WARN 2022-01-06 13:36:54.000707][Administrator] [2][Socket close failed][fd:3668,errorcode is 10035]// Certificate verification fails, and a certificate security warning is displayed.

[CADM INFO 2022-01-06 13:36:54.000707][Administrator] [2][Normal Msg][biztype is 3 ,msgtype is 3 ,msgcode is 0x3000b]
[CADM INFO 2022-01-06 13:36:54.000708][Administrator] [5][CSDK_Send_Thread][uiMsgSourceMark:0x4000000 -> uiMsgDestMark:0x2000000][uiModuleID:0x3000000][uiMsgType:0xB000300][uiConnetType:0x1000000][uiMsgLength:0x0]
[CADM INFO 2022-01-06 13:37:15.000450][Administrator] [4][Proxy info][ConnectType is <1>,Proxy type is <0>]
[CADM INFO 2022-01-06 13:37:15.000450][Administrator] [4][Proxy info][proxy is :0, user name is , proxy type is 0]
[PREF INFO 2022-01-06 13:37:15.000450][Administrator] [2][Link pref proc][Enter]
[PREF INFO 2022-01-06 13:37:15.000451][Administrator] [2][Link backup not open][Return choice site] //Link backup is not enabled.

[CAUTH INFO 2022-01-06 13:37:15.000551][Administrator] [2][Auth send][auth package send to gateway successful]
[CAUTH INFO 2022-01-06 13:37:15.000551][Administrator] [2][Master auth][send auth message to gateway ok]
[CAUTH INFO 2022-01-06 13:37:15.000551][Administrator] [2][Auth login process][auth master ok]//The primary authentication is successful.
[CAUTH INFO 2022-01-06 13:37:15.000552][Administrator] [2][Auth receive][auth type 0]
[CAUTH INFO 2022-01-06 13:37:15.000552][Administrator] [2][auth master exit][authType = 0]
[NETC INFO 2022-01-06 13:37:15.000552][Administrator] [2]4[xcs SSLFree begin][pstConInf->psSsl=2b5b3e0]
[CADM INFO 2022-01-06 13:37:15.000553][Administrator] [2][Normal Msg][biztype is 3 ,msgtype is 2 ,msgcode is 0x20000]
[CADM INFO 2022-01-06 13:37:15.000553][Administrator] [5][CSDK_Send_Thread][uiMsgSourceMark:0x4000000 -> uiMsgDestMark:0x2000000][uiModuleID:0x3000000][uiMsgType:0x200][uiConnetType:0x1000000][uiMsgLength:0x0]
[CADM INFO 2022-01-06 13:37:15.000554][Administrator] [4][SSL Start Nem][in to SSL_StartNem]// Enable the network extension service.
[VNIC INFO 2022-01-06 13:37:15.000556][Administrator] [8][Start VNIC][begin] // Enable the Virtual NIC.
[VNIC INFO 2022-01-06 13:37:15.000557][Administrator] [8][Find the VNIC][success]
[VNIC INFO 2022-01-06 13:37:15.000564][Administrator] [8][Nic Open][begin]
[VNIC INFO 2022-01-06 13:37:15.000570][Administrator] [8][Get VNIC name] [name: local connection].
[VNIC INFO 2022-01-06 13:37:15.000571][Administrator] [8][VNIC Start] [open cmd is interface set interface "local connection" admin=ENABLED]
[CNEM INFO 2022-01-06 13:37:15.000603][Administrator] [8][Cnem send status msg to self ok]
[CNEM INFO 2022-01-06 13:37:15.000604][Administrator] [8][Cnem Start OK]//The network extension is enabled.
[NETC INFO 2022-01-06 13:37:15.000608][Administrator] [8][NETC SSL Create][pstConInf->aucHostName][10.19.12.120]
[NETC INFO 2022-01-06 13:37:15.000608][Administrator] [8][NETC SSL Create][g_gatewayDomain][10.19.12.120]
[PREF INFO 2022-01-06 13:37:15.000608][Administrator] [8][GetPrefSiteFlag:0]
[CAUTH INFO 2022-01-06 13:37:15.000608][Administrator] [8][CAUTH_CheckIsDomain][pucDomain is 10.19.12.120]
[CAUTH INFO 2022-01-06 13:37:15.000609][Administrator] [8][CAUTH_CheckIsDomain][pucDomain is IP]
[NETC INFO 2022-01-06 13:37:15.000609][Administrator] [8][NETC SSL Create][connect]

[NETC INFO 2022-01-06 13:37:15.000619][Administrator] [8][NETC SSL Create][connect][connectSSL == 1]
[NETC INFO 2022-01-06 13:37:15.000619][Administrator] [8][SSL Create][Success] // The network extension succeeded in establishing an SSL connection to the gateway.
[CNEM INFO 2022-01-06 13:37:15.000620][Administrator] [8][Cnem SSL create ok][3656]
[CNEM INFO 2022-01-06 13:37:15.000620][Administrator] [8][Cnem SSL create][reason:channel bind success][sslChannelId<3656>]
[CNEM INFO 2022-01-06 13:37:15.000620][Administrator] [8][Cnem send status msg to self ok]
[CNEM INFO 2022-01-06 13:37:15.000621][Administrator] [8][Cnem module proc][Enter]
[CNEM INFO 2022-01-06 13:37:15.000621][Administrator] [8][Cnem AsyncMsg BizNem Proc][Enter]
[CNEM INFO 2022-01-06 13:37:15.000621][Administrator] [8][Cnem run][Enter]
[CNEM INFO 2022-01-06 13:37:15.000621][Administrator] [8][Cnem run][the current status 20 and msgtype 1]
[CNEM INFO 2022-01-06 13:37:15.000621][Administrator] [8][Cnem send acl request to gateway ok]// Send an ACL request to the gateway. (used for interaction with the SVN)
[CNEM INFO 2022-01-06 13:37:15.000622][Administrator] [3][Cnem send status msg to self ok]

[CNEM INFO 2022-01-06 13:37:15.000626][Administrator] [8][Cnem send vip request to gateway ok] // Send a VIP request to the VPN gateway.
[CNEM INFO 2022-01-06 13:37:15.000628][Administrator] [3][Cnem handle packet from gateway][CMDtype is REQVIP]
[CNEM INFO 2022-01-06 13:37:15.000628][Administrator] [3][Cnem parse new netcfginfo][Enter]
[CNEM INFO 2022-01-06 13:37:15.000628][Administrator] [3][Cnem parse new netcfginfo][DNS Server IP Nums is 1]// Obtain one DNS server address from the device.
[CNEM INFO 2022-01-06 13:37:15.000628][Administrator] [3][Cnem parse vip info from gateway ok] // Obtain the VIP information from the device.
[VNIC INFO 2022-01-06 13:37:15.000632][Administrator] [8][Get VNIC iofd][handle is 2648]
[VNIC INFO 2022-01-06 13:37:15.000632][Administrator] [8][Get VNIC Handle][success]
[VNIC INFO 2022-01-06 13:37:15.000632][Administrator] [8][Active VNIC][begin]
[VNIC INFO 2022-01-06 13:37:15.000632][Administrator] [8][Active VNIC][success]
[VNIC INFO 2022-01-06 13:37:15.000633][Administrator] [8][Set IP and MASK][begin]
[VNIC INFO 2022-01-06 13:37:15.000633][Administrator] [8][VNIC IP is 10.19.15.36]// Virtual IP address information.
[VNIC INFO 2022-01-06 13:37:15.000633][Administrator] [8][VNIC mask is 255.255.255.0]// Subnet mask of the virtual IP address.
[VNIC INFO 2022-01-06 13:37:15.000675][Administrator] [8][Set IP and MASK][success]// Set the IP address for a virtual NIC.
[VNIC INFO 2022-01-06 13:37:15.000676][Administrator] [8][Set DNS Server IP][begin]
[VNIC INFO 2022-01-06 13:37:15.000745][Administrator] [8][VNIC Init][set DNS success]// Set the DNS for a virtual NIC.
[ROUTE INFO 2022-01-06 13:37:19.000059][Administrator] [41][Route set][Begin]:[70]
[ROUTE INFO 2022-01-06 13:37:19.000059][Administrator] [41][Route set][Before set route print the routetable:]//Print the routing table before VPN routes are injected.
[ROUTE INFO 2022-01-06 13:37:19.000060][Administrator] [41][Route print begin==========
[ROUTE INFO 2022-01-06 13:37:19.000068][Administrator] [41][Get best route info][Ip :10.19.28.254 Mask :0x00000000 Nic index :10]
[ROUTE INFO 2022-01-06 13:37:19.000068][Administrator] [41][gateWay info][Ip :10.19.12.120]
[ROUTE INFO 2022-01-06 13:37:19.000069][Administrator] [41][BroadCast Route Judge ok][DestIP : 0xff0f130a]
[ROUTE INFO 2022-01-06 13:37:19.000069][Administrator] [41][Cleanup VNIC related route][Success]// Clear the old virtual NIC route.
[ROUTE INFO 2022-01-06 13:37:19.000084][Administrator] [41][manul inner route info][Dest:0x2e0c130a Mask:0xffffffff NextHop:0x240f130a IfIndex:13]

```
[ ROUTE   ERROR   2022-01-06 13:37:19.000096 ][Administrator] [41][Delete route Failed][ErrorCode:0]
[ ROUTE   ERROR   2022-01-06 13:37:19.000097 ][Administrator] [41][Delete Unsafe Route Failed][Line :787]
[ ROUTE   INFO    2022-01-06 13:37:19.000097 ][Administrator] [41][BroadCast Route Judge ok][DestIP : 0xff0f130a]
[ ROUTE   INFO    2022-01-06 13:37:19.000097 ][Administrator] [41][BroadCast Route Judge ok][DestIP : 0xff1c130a]
[ ROUTE   INFO    2022-01-06 13:37:19.000097 ][Administrator] [41][BroadCast Route Judge ok][DestIP : 0xff3f1fac]
[ ROUTE   INFO    2022-01-06 13:37:19.000110 ][Administrator] [41][Set manual mode route][Success]
[ ROUTE   INFO    2022-01-06 13:37:19.000110 ][Administrator] [41][After set route][Routetable:]//Print the routing table after VPN routes are injected.
[ ROUTE   INFO    2022-01-06 13:37:19.000110 ][Administrator] [41][Route print begin==========================================================================================
```

- By default, the UniVPN records only INFO, WARN, and ERROR logs. To record DEBUG logs, modify the UniVPN configuration file **sysconfig.ini**.

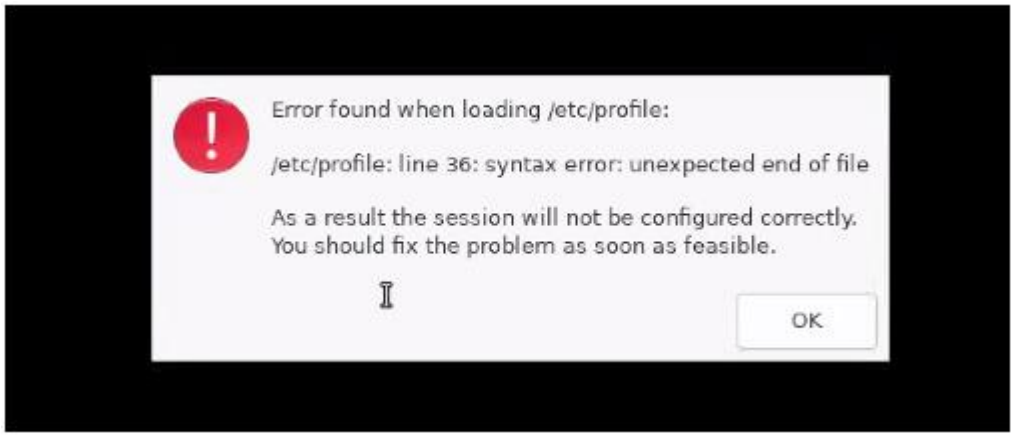
```
[GLOBAL]
ClientName = UniVPN
ClientVersion = 7.0.9.1
ClientCustomized = false
ClientLogLevel = 1 //Change the value to 0 so that DEBUG logs will be recorded.
```

1.5.40 Can the UniVPN and SecoClient Be Used Simultaneously?

No. If the SecoClient exists on the PC, it will be detected and uninstalled during UniVPN installation. If the SecoClient fails to be uninstalled, manually uninstall it to prevent UniVPN client problems.

1.5.41 Why the PC Reports an Error Before the UniVPN Is Started?

1. Localized Linux: If the following dialog box is displayed during startup, the VPN service cannot be automatically started. In this case, contact the administrator to restore the configuration file in the path **/etc/profile**.



2. After the VPN connection is set up successfully, if the program process exits unexpectedly (for example, the installation is overwritten or the computer is

powered off), the delivered routes may not be deleted. In this case, contact the administrator.

1.5.42 Whether to release some ports when using the client

Yes, the client will bind specific ports. Please allow the following ports to communicate.

Windows:

The promote service listens to port 29190. If it fails, the port is bound incrementally

CSDK listening port 19060

UI listener port 29192

Linux and MacOS platforms:

Promote service listening port 29191

Listening port 19060

UI listener port 29192

1.6 Troubleshooting Guidelines for SSL VPN Dial-up Failures on UniVPN_V600R21C10

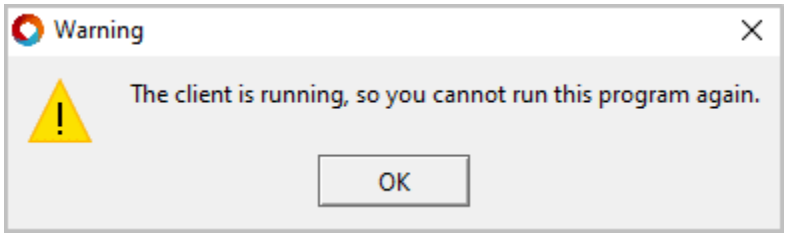
This chapter introduces the troubleshooting methods for dialing SSL VPN when UniVPN clients access firewall devices V500R005C20, V600R007C20, and later versions.

1.6.1 Troubleshooting Guidelines for Warnings Displayed on the UniVPN

1.6.1.1 Warning: The client is running, so you cannot run this program again.

Symptom

Warning: The client is running, so you cannot run this program again.

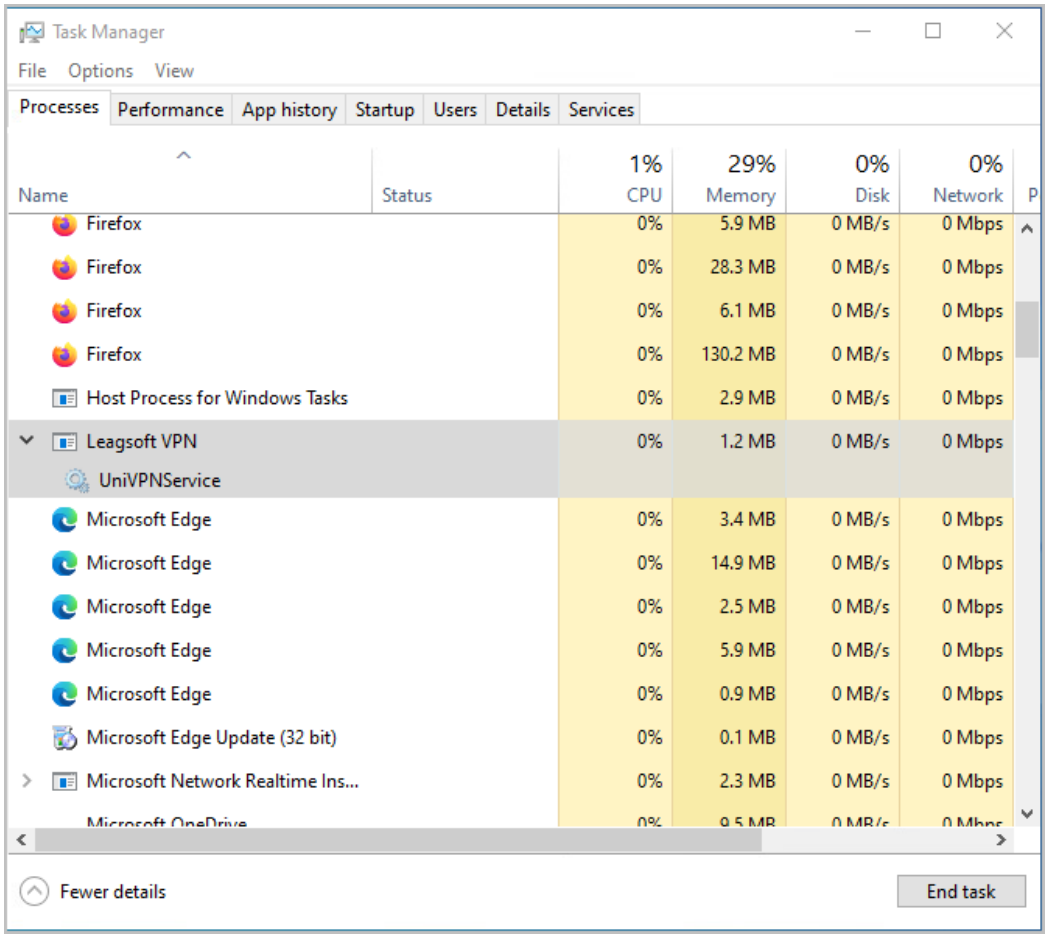


Possible Causes

The UniVPN is running.

Procedure

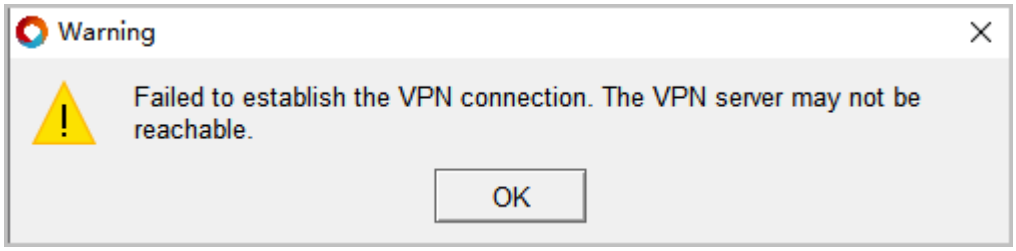
Close the existing UniVPN program and the browser that uses the SSL VPN service, and check whether the UniVPN.exe process in the task manager is disabled.



1.6.1.2 Warning: Failed to establish the VPN connection. The VPN server may not be unreachable.

Symptom

When the VPN gateway is connected, the system displays "Failed to establish the VPN connection. The VPN server may not be unreachable."



Possible Causes

1. The UniVPN is unreachable to the VPN gateway.
2. The IP address or port number of the VPN gateway on the UniVPN is incorrect.
3. The UniVPN version does not match the VPN gateway version.
4. When a device accesses the Internet through a proxy server (for example, 192.168.253.188), the VPN gateway of the public network is not configured for the UniVPN.

Procedure

- Fault location and troubleshooting for cause 1

  3. On the device where the UniVPN is installed, check whether the IP address of the VPN gateway can be pinged.
  4. If the route is unreachable, configure a route from the UniVPN to the VPN gateway. If the route is reachable, analyze cause 2.

- Fault location and troubleshooting for cause 2

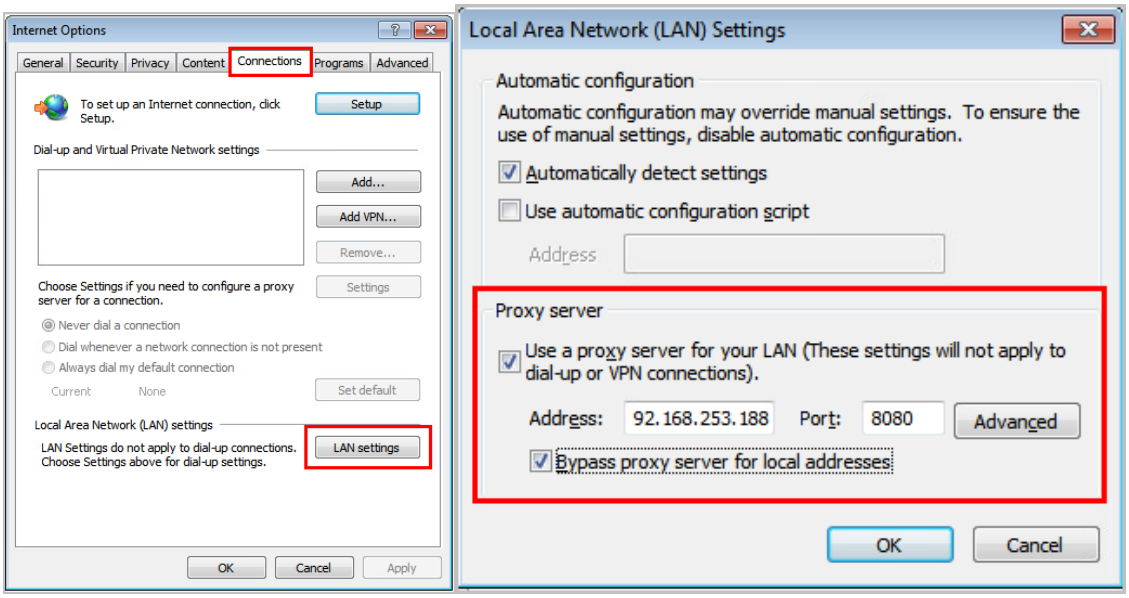
  Check whether the IP address and port number of the VPN gateway configured on the UniVPN are the same as those configured on the VPN gateway.

- Fault location and troubleshooting for cause 3

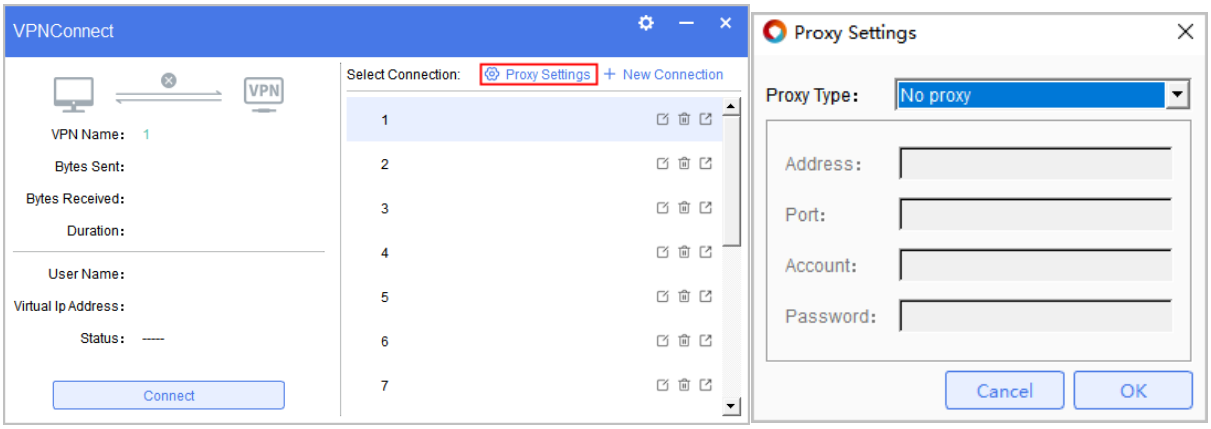
  Currently, the VPN gateway software versions that match the UniVPN are FW V500R001C20, FWV100R001C30SPC900, SVN V200R003C10SPC900, and their later versions.

- Fault location and troubleshooting for cause 4

  Check whether the device accesses the Internet through the proxy server.



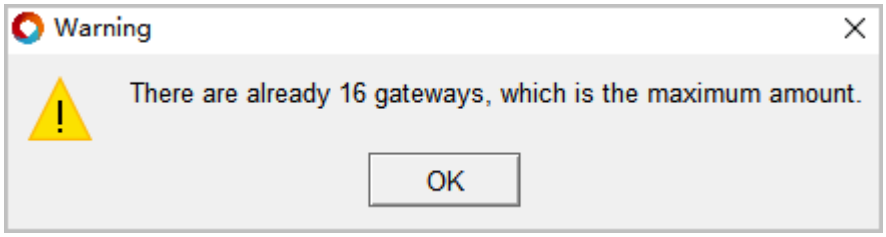
If yes, set proxy parameters on the UniVPN, as shown in the following figure.



1.6.1.3 Warning: There are already 16 gateways, which is the maximum amount.

Symptom

On the new connection page of the UniVPN, after 16 gateway addresses are entered in the remote gateway text box and **Add** is clicked, the system displays "Warning: There are already 16 gateways, which is the maximum amount."



Possible Causes

On the new connection page of the client, 16 remote gateways have been added, reaching the maximum number of allowed gateways.

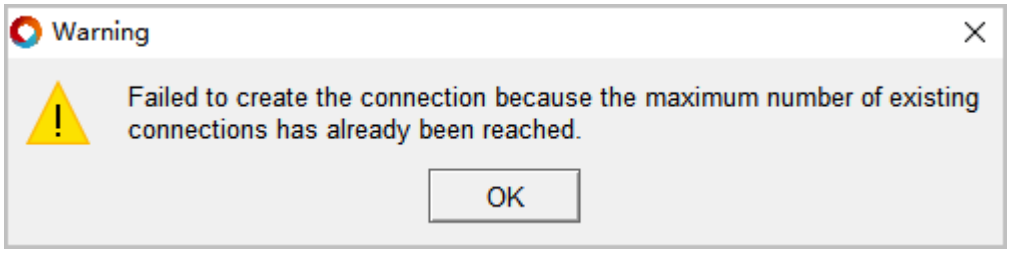
Procedure

After the number of remote gateways reaches 16, do not add any gateway address.

1.6.1.4 Warning: Failed to create the connection because the maximum number of existing connections has already been reached.

Symptom

On the UniVPN home page, add 16 VPN connections and click **+**. The system displays "Warning: Failed to create the connection because the maximum number of existing connections has already been reached."



Possible Causes

On the home page of the client, 16 connections have been added, reaching the maximum number of allowed connections.

Procedure

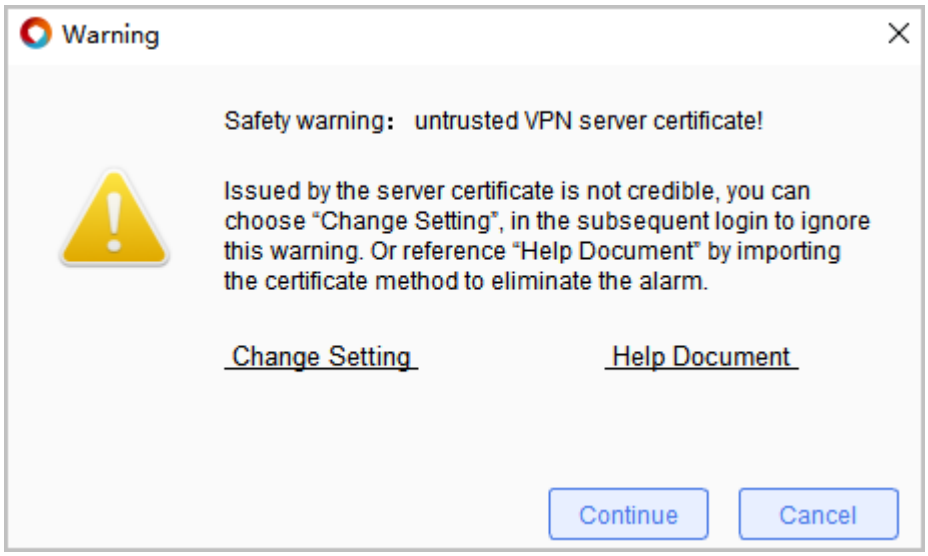
After 16 connections are added, do not add any connection.

1.6.2 Troubleshooting Guidelines for Warnings Displayed During User Name/Password-based Login

1.6.2.1 Warning: untrusted VPN server certificate

Symptom

When you use the UniVPN to log in to the SSL VPN virtual network through the SSL VPN tunnel, the following information is displayed:



Possible Causes

The CA certificate for authenticating the virtual gateway is unavailable on the UniVPN.

Procedure

To clear the warning, use either of the following operation methods:

- Click Change Setting and deselect Block connections to untrusted servers.

  This method can be used when you are sure about the authenticity of the virtual gateway.
- Issue certificates for the UniVPN and virtual gateway.

  This method is recommended when you are not sure about the authenticity of the virtual gateway.

Create two certificates. Place one device certificate on the virtual gateway, and place the other CA certificate on the host where the UniVPN resides. If your enterprise has a certificate system, you can use your own system to create certificates. If no certificate system is available, you can use XCA software to create certificates.

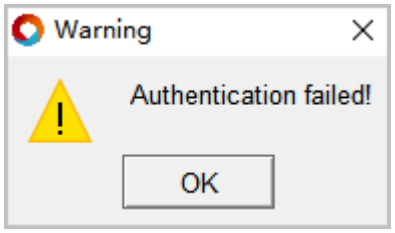
When you use the UniVPN to log in to a virtual gateway through an SSL VPN tunnel, the virtual gateway pushes the device certificate to the UniVPN. The system will not prompt certificate invalidity if the CA certificate on the UniVPN identifies the device certificate of the virtual gateway.

For details about how to create a certificate, How Do I Use XCA to Create Device Certificates and User Certificates?.

1.6.2.2 Warning: Authentication failed

Symptom

After you enter the user name and password and click Login on the UniVPN login page, the system displays "Authentication failed."



Possible Causes

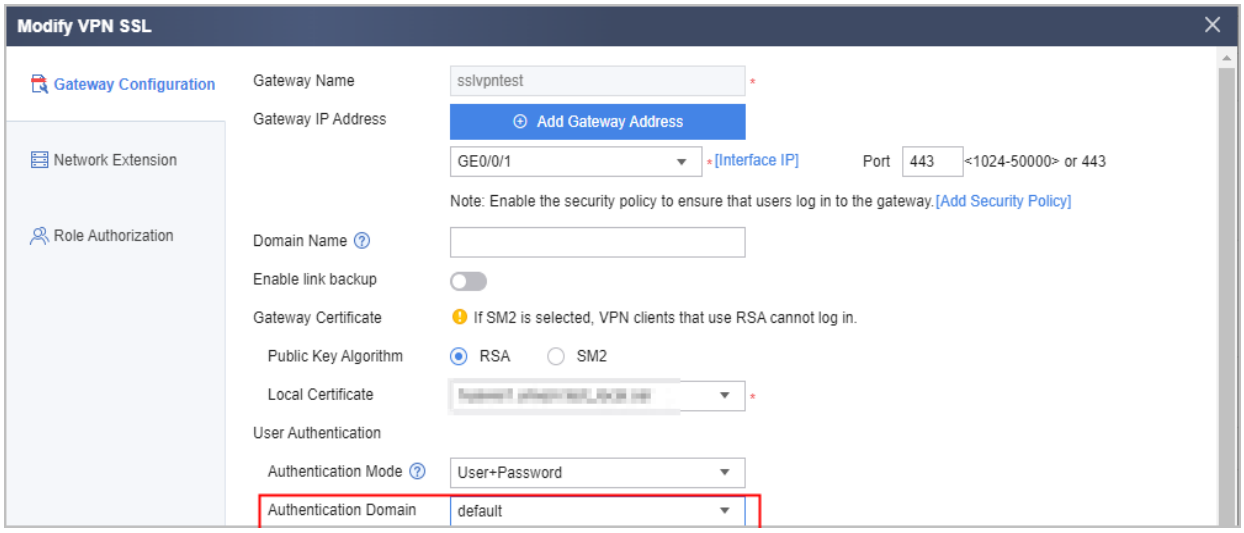
1. The user name or password is incorrect, the user account expires, or the user is locked out.
2. The virtual gateway is bound to an incorrect authentication domain.
3. SSL VPN access is not enabled for authentication domains.
4. The network extension feature is not enabled on the virtual gateway.
5. The SSL VPN login device is in a dual standby state (HRP_S), but SSL VPN does not support login on the standby device.
6. The AD/LDAP authentication server is configured for the authentication domain, and Force Password Change upon First Login is enabled on the server.
7. The metric value (hop count) of the route from the client to the server exceeds 1024.

Procedure

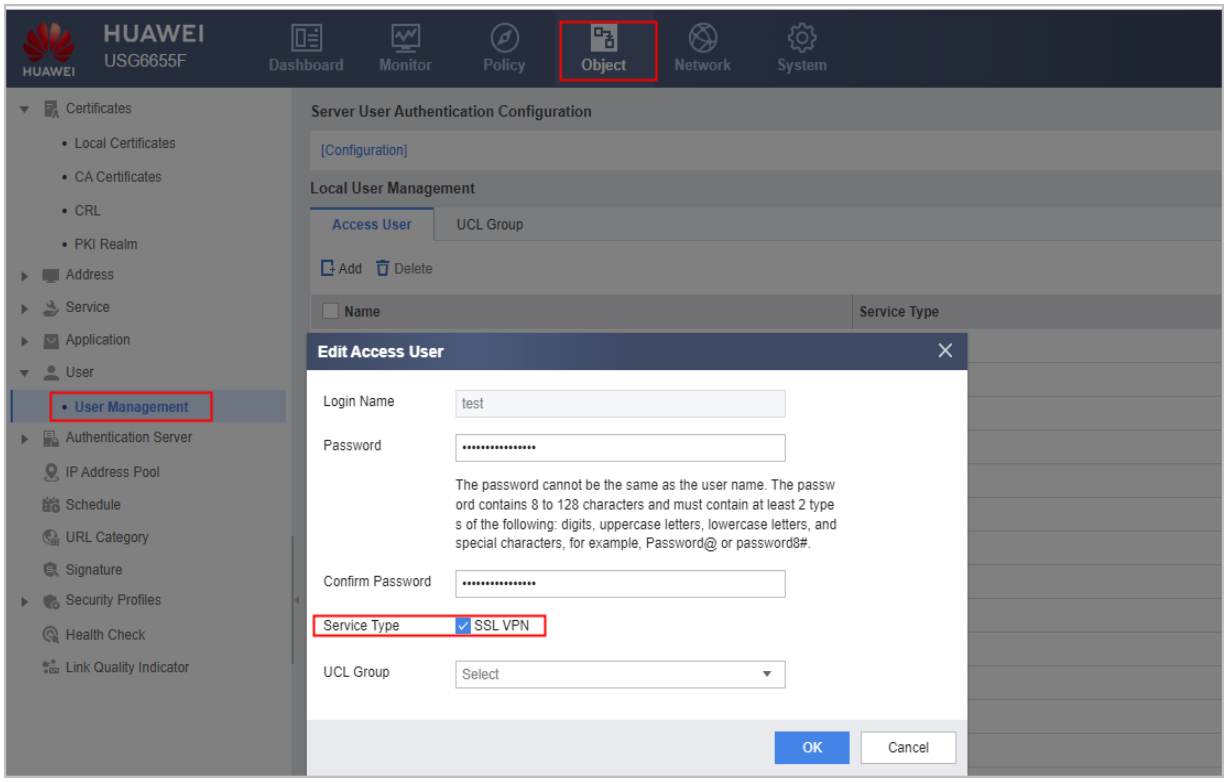
1. Log in to the device and check that the user name and password are correct and that the user does not expire or is not locked.

```
[HUAWEI-aaa]display local-access-user username user001
2023-04-13 08:58:05.793 +08:00
  The contents of local access user(s):
  Password                 : ****************
  State                    : block
  Service-type-mask        : V
  Access-limit             : Yes
  Access-limit-max         : 4294967295
  Accessed-num             : 0
  Block-time-left          : 2 Min(s)
  Original-password        : No
  Password-set-time        : 2023-02-23 20:01:17+08:00
  Password-expired         : Yes
  Password-expire-time     : 2023-03-15 20:01:17+08:00
  Account-expire-time      : -
  Local Access User ID     : 17
  Service-scheme           : -
  UCL group(s)             : -
```

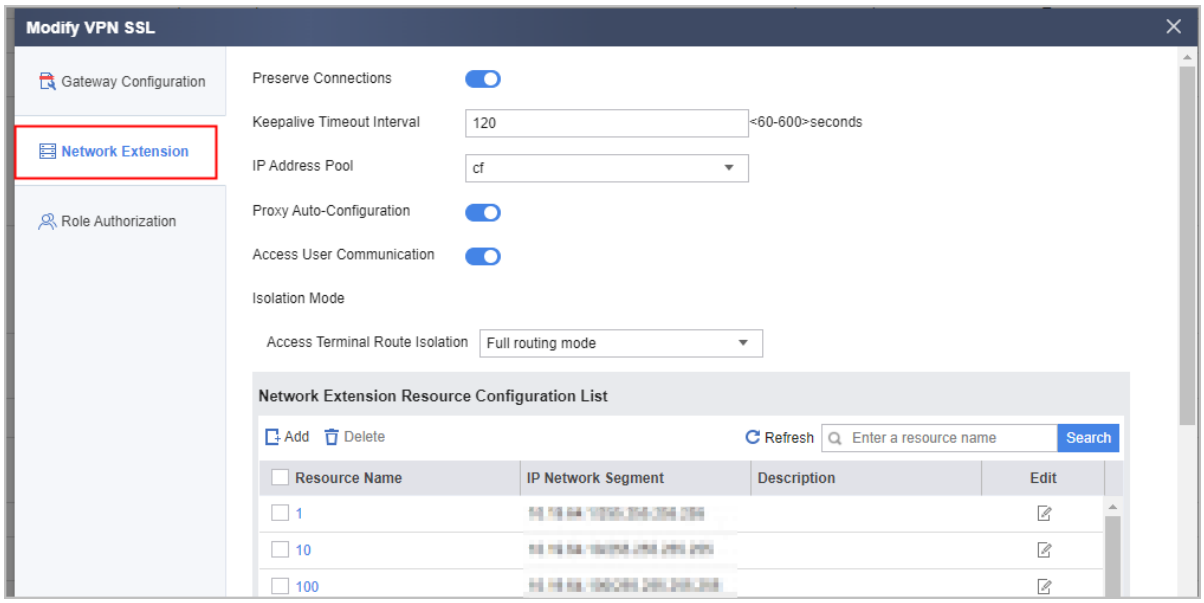
2. Check whether the correct authentication domain is bound to the virtual gateway.



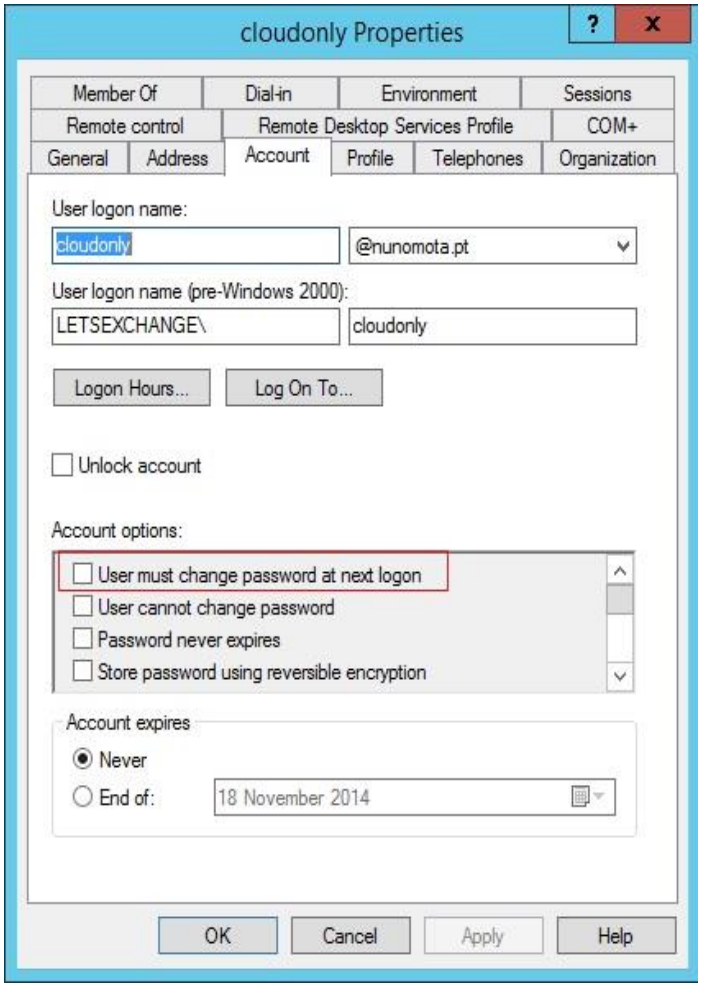
3. Check whether SSL VPN access is enabled in the authentication domain.



4. Check whether the network extension service of the virtual gateway is enabled.



5. SSL VPN cannot be applied in load-balancing networking. Modify the configuration or networking to ensure that the SSL VPN login device is in the HRP_M state.
6. Log in to the AD/LDAP server and check whether Force Password Change upon First Login is enabled. If yes, select Disable.



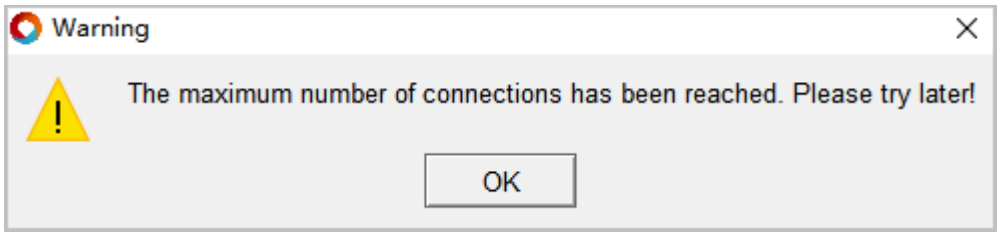
7. Check whether the metric value of the route to the server exceeds 1024. If yes, change the metric value of the route.

```
sugon@sugon-os:~/桌面$ route -n
内核 IP 路由表
目标            网关            子网掩码        标志  跃点   引用  使用 接口
0.0.0.0         10.18.11.254    0.0.0.0         UG    13392  0        0 enp1s0
10.18.11.0      0.0.0.0         255.255.255.0   U     100    0        0 enp1s0
10.20.2.96      10.18.11.254    255.255.255.255 UGH   100    0        0 enp1s0
169.254.0.0     0.0.0.0         255.255.0.0     U     1000   0        0 enp1s0
sugon@sugon-os:~/桌面$ sudo route del default gw 10.18.11.254
sugon@sugon-os:~/桌面$ sudo route add -net 0.0.0.0 gw 10.18.11.254 netmask 0.0.0.0  metric 0 enp1s0
sugon@sugon-os:~/桌面$ route -n
内核 IP 路由表
目标            网关            子网掩码        标志  跃点   引用  使用 接口
0.0.0.0         10.18.11.254    0.0.0.0         UG    0      0        0 enp1s0
10.18.11.0      0.0.0.0         255.255.255.0   U     100    0        0 enp1s0
10.20.2.96      10.18.11.254    255.255.255.255 UGH   100    0        0 enp1s0
169.254.0.0     0.0.0.0         255.255.0.0     U     1000   0        0 enp1s0
sugon@sugon-os:~/桌面$
```

1.6.2.3 Warning: The maximum number of connections has been reached. Please try later.

Symptom

After you enter the user name and password and click Login on the UniVPN login page, the system displays "The maximum number of connections has been reached. Please try later."



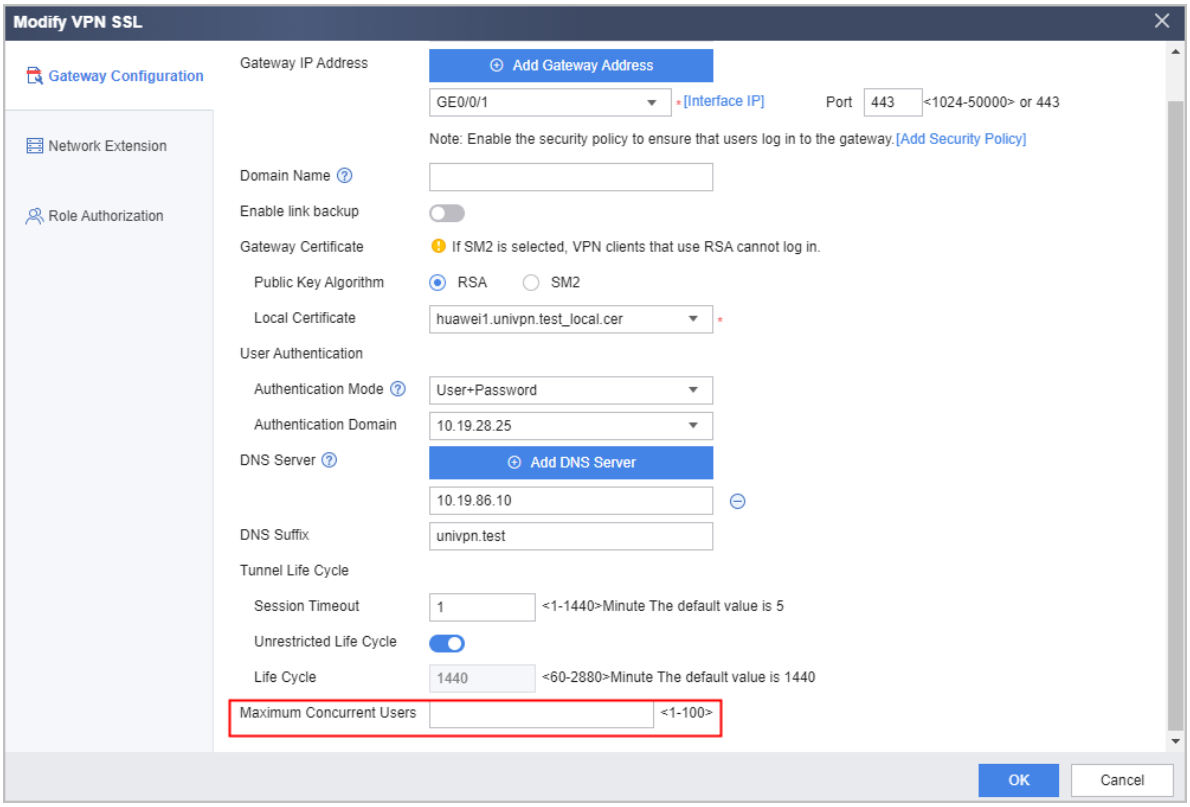
Possible Causes

1. The number of online SSL VPN users has reached the upper limit configured on the virtual gateway.
2. The public account function is enabled on the virtual gateway, and the number of online users using this account has reached the upper limit.

Procedure

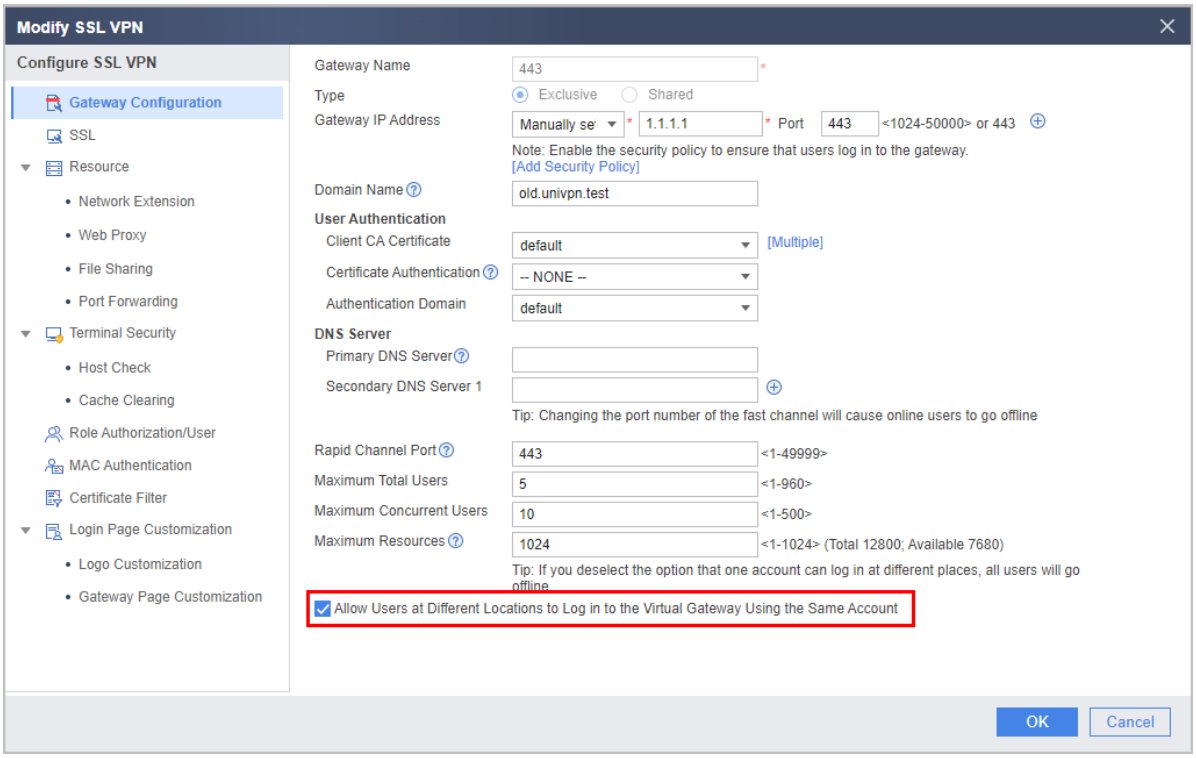
- Fault location and troubleshooting for cause 1

  Log in to the virtual gateway. Choose Network > SSL VPN > SSL VPN, and click the name of the virtual gateway. Check whether the maximum number of concurrent users allocated to the virtual gateway is proper. If not, modify the configuration.Fault location and troubleshooting for cause 1



- Fault location and troubleshooting for cause 2

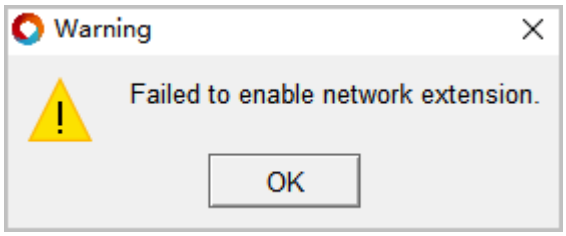
  Check the maximum number of online users. If the login request is normal, increase the maximum number of online users.



1.6.2.4 Warning: Failed to enable network extension

Symptom

After you enter the user name and password and click Login on the UniVPN login page, the system displays "Failed to enable network extension."



Possible Causes

1. The IP addresses in the network extension address pool of the virtual gateway have been used up.
2. The client's virtual network card is abnormal or the client does not have permission to operate the virtual network card.

Procedure

1. Start the CLI console, enter the service view of the virtual gateway, and run the display network-extension [ip] command to check the configuration and allocation of the network extension address pool. If all IP addresses in the address pool have been allocated, increase the number of addresses in the address pool based on service requirements.

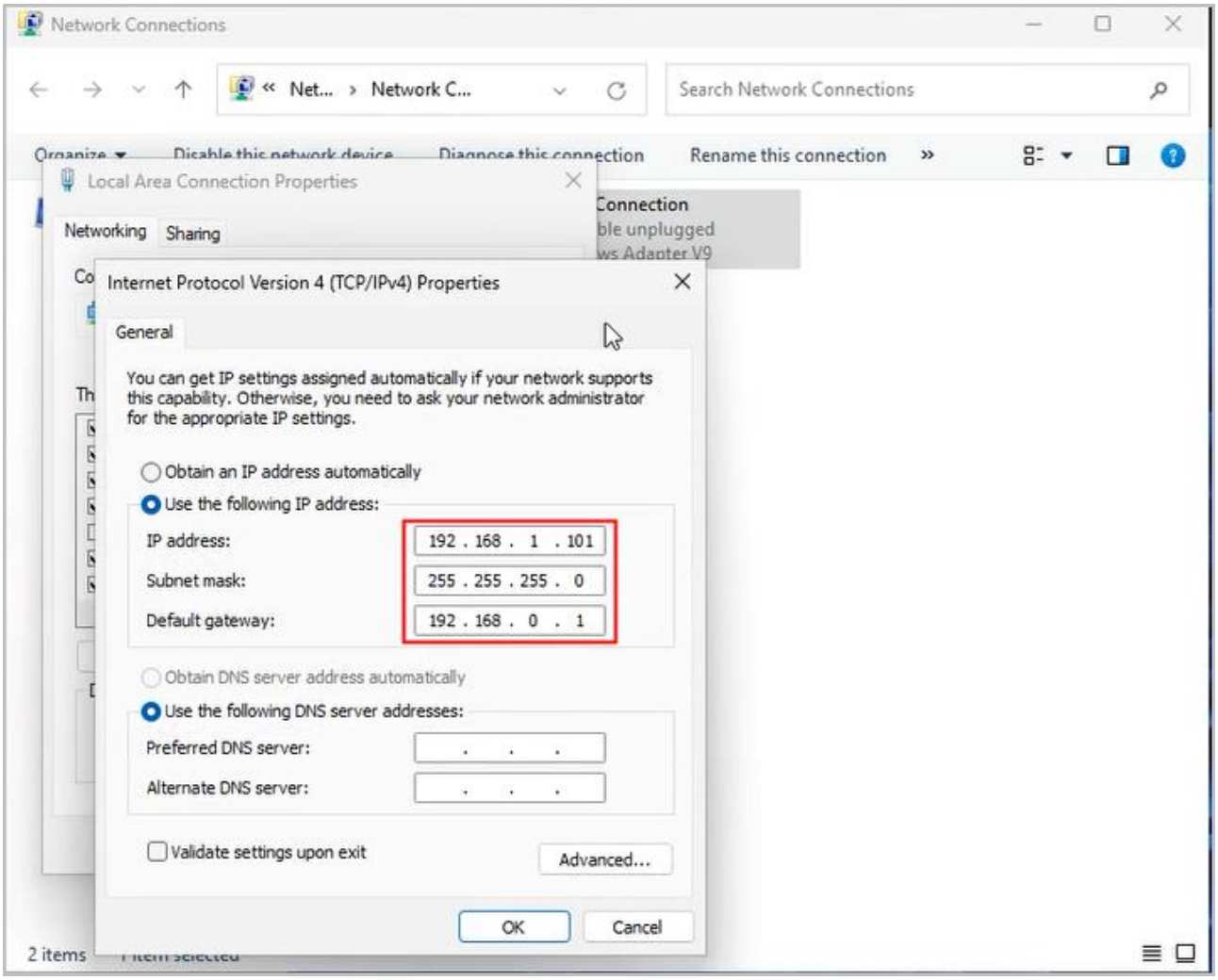
```
<HUAWEI>display ip pool name test
2023-04-21 16:41:26.551 +08:00

  Pool-name            : test
  Pool-No              : 0
  Lease                : 1 Days 0 Hours 0 Minutes
  Domain-name          : -
  DNS-server0          : -
  NBNS-server0         : -
  Netbios-type         : -
  Position             : Local
  Status               : Unlocked
  Gateway-0            : -
  Network              : -
  Mask                 : -
  VPN instance         : --
  Logging              : Disable
  Conflicted address recycle interval: -
  Address Statistic: Total          :100          Used           :0
                     Idle           :100          Expired        :0
                     Conflict       :0            Disabled       :0

 ------------------------------------------------------------------------------
  Section ID: 0
```

```
        Start           End          Total     Used Idle(Expired) Conflict Disabled
 ------------------------------------------------------------------------------
       100.1.1.1     100.1.1.100     100       0        100(0)       0        0
 ------------------------------------------------------------------------------
<HUAWEI>
```

Check if the system network adapter is correctly installed with the virtual network card. If the virtual network card is abnormal, please try uninstalling and reinstalling it;

2. Test whether the virtual network card can be operated normally under the current user, and execute the following three commands: disable, enable, and set IP to see if the virtual network card can be set correctly. If it cannot be set correctly, please check if there is a policy that prohibits clients from operating virtual network cards.

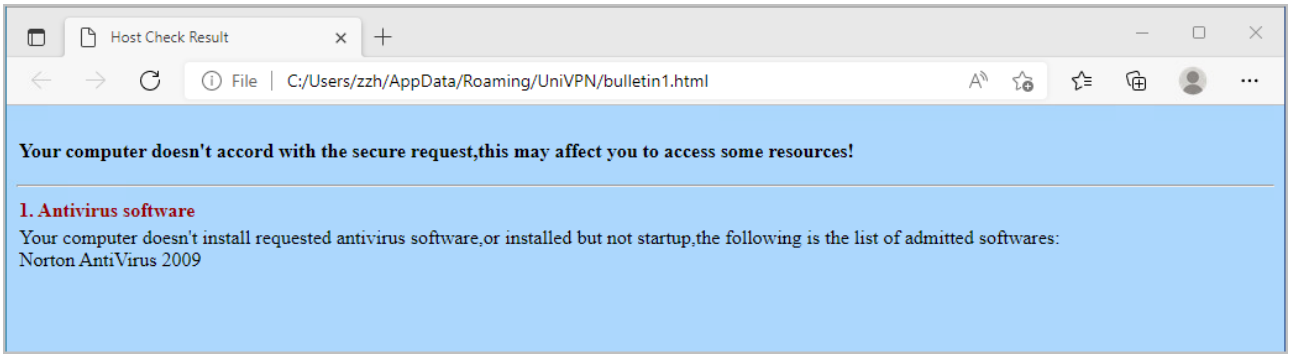
```
C:\Windows\System32>netsh.exe interface set interface "Local Area Connection" admin=DISABLED

C:\Windows\System32>netsh.exe interface set interface "Local Area Connection" admin=ENABLED

C:\Windows\System32>netsh interface ip set address "Local Area Connection" static 192.168.1.101 255.255.255.0
 192.168.0.1 1

C:\Windows\System32>
```



1.6.2.5 Warning: Host check failed

Symptom

After you enter the user name and password and click Login on the UniVPN login page, the system displays "Host check failed."



Possible Causes

The host check function is enabled on the virtual gateway, and the device does not meet security access requirements.

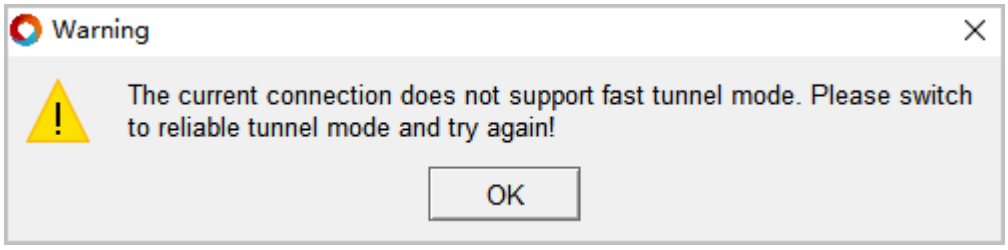
Procedure

Rectify the fault as prompted.

1.6.2.6 Warning: The current connection does not support fast tunnel mode. Please switch to reliable tunnel mode and try again!

Symptom

After you enter the user name and password and click **Login** on the UniVPN login page, the system displays "Warning: The current connection does not support fast tunnel mode. Please switch to reliable tunnel mode and try again!"

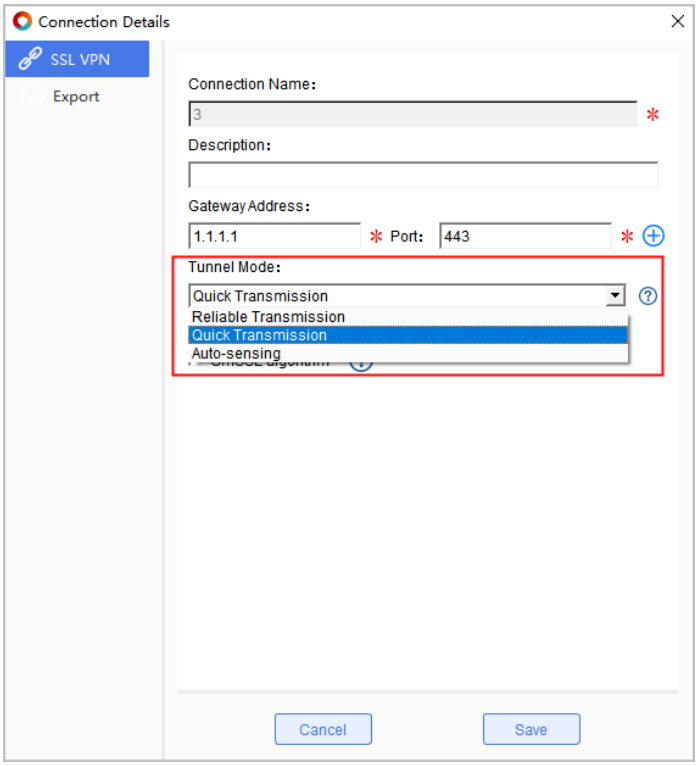


Possible Causes

During SSL VPN dialup, the device sends UDP detection packets to check whether fast tunnels can be established. If the device receives a response from the firewall, the fast tunnel can be established. The warning indicates that the UDP link is not reachable and that no fast tunnel can be established.

Procedure

1. Configure **Auto-sensing** on the UniVPN as a workaround. If the fast tunnel cannot be established, perform the following steps:



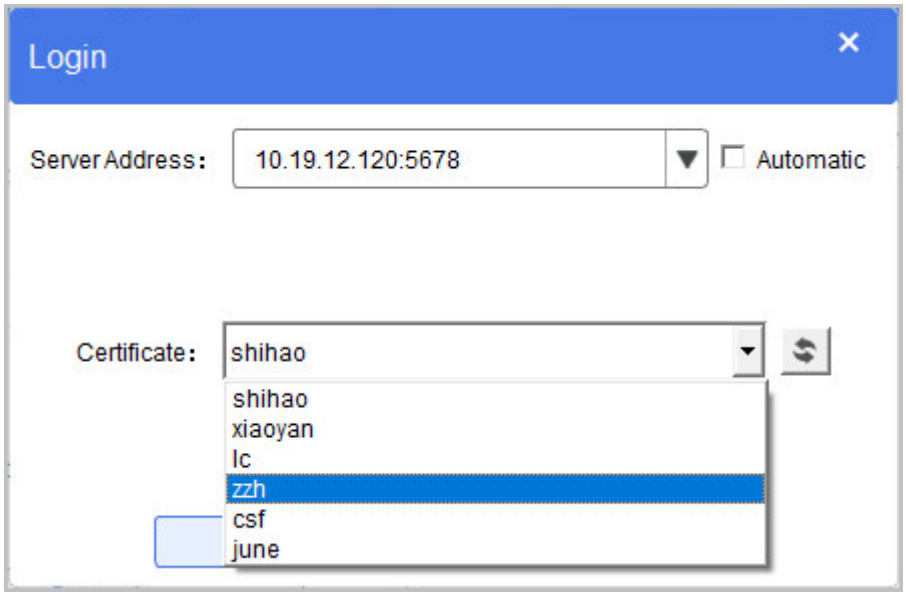
2. Check the firewall security policy to see if the data flow for establishing fast UDP links is permitted between the device and VPN gateway.
3. Check whether a NAT device is connected to the firewall. If yes, configure NAT for the TCP and UDP ports of the SSL VPN and modify the security policy to permit the fast link establishment flow. When NAT mapping is performed for UDP ports, the global port number must be the same as the inside port number.

1.6.3 Troubleshooting Guidelines for Warnings Displayed During Certificate-based Login

1.6.3.1 Failed to find the desired user certificate

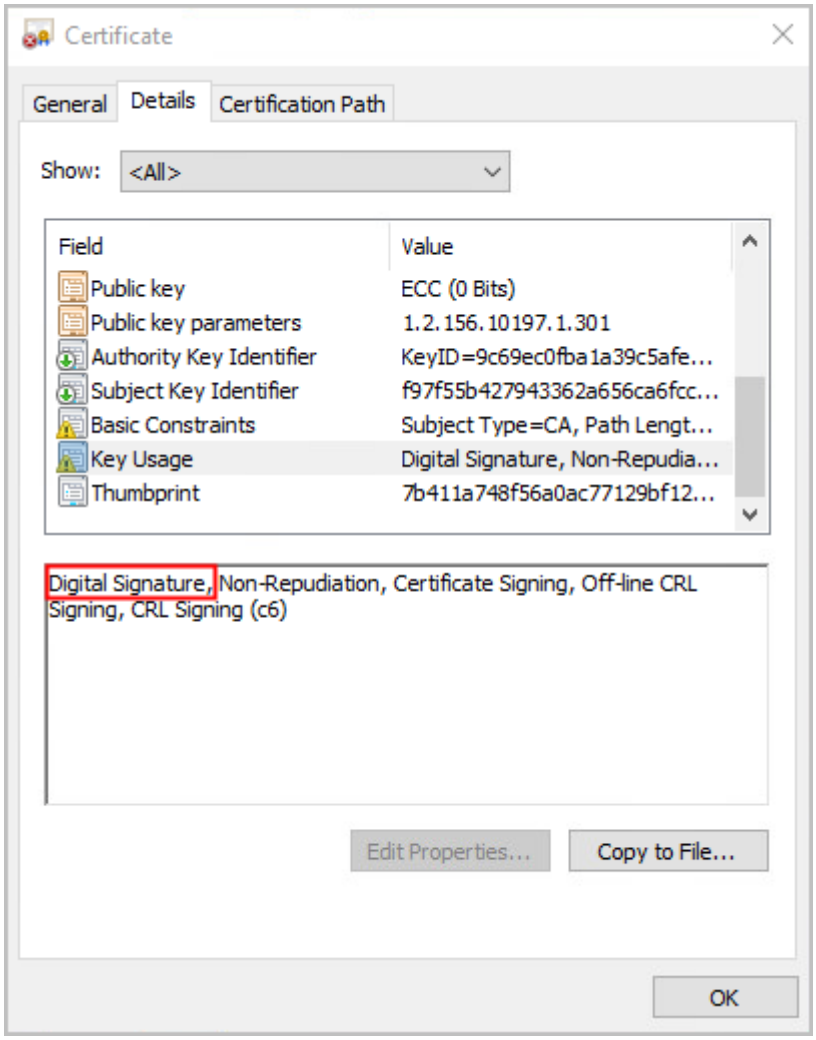
Symptom

The desired user certificate cannot be found on the SecoClient login page when you attempt to log in to the virtual gateway using certificate authentication.



Possible Causes

The Key Usage field of the user certificate does not contain Digital Signature.



Procedure

Create a user certificate with a digital signature carried in Key Usage.

NOTE

If the server does not support certificates without the digital signature capability, the client will not display such certificates.

If the server supports certificates without the digital signature capability, but the client does not display such certificates, the server may have the key usage enabled, which requires the digital signature capability.

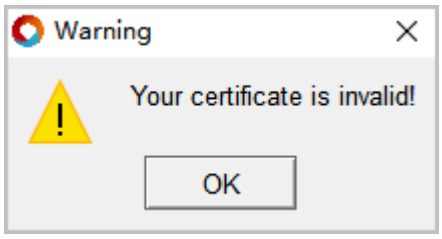
Product Name	Version	Support Authentication of Certificates Without the Digital Signature Capability (Y/N)
USG6000	V500R005C20SPC500 and later version	N

Product Name	Version	Support Authentication of Certificates Without the Digital Signature Capability (Y/N)
USG9500	V500R005C20SPC500 and later version	N
USG6000E	V600R007C20SPC300 and later version (except SPC301/SPC302)	N
Eudemon200E-N	V500R005C20SPC500 and later version	N
Eudemon200E-G	V600R007C20SPC300 and later version (except SPC301/SPC302)	N
Eudemon1000E-N	V500R005C20SPC500 and later version	N
Eudemon1000E-G	V600R007C20SPC300 and later version (except SPC301/SPC302)	N
Eudemon8000E-X	V500R005C20SPC500 and later version	N
SeMG9811	V500R005C20SPC500 and later version	N
NGFW Module	V500R005C20SPC500 and later version	N
USG12000	V600R021C10 and later version	Y
USG6000F	V600R021C10 and later version	Y
Eudemon9000E-X	V600R021C10 and later version	Y
Eudemon9000E-F	V600R021C10 and later version	Y
Eudemon1000E-F	V600R021C10 and later version	Y

1.6.3.2 Warning: Your certificate is invalid.

Symptom

When you select a user certificate and click Login on the SecoClient login page, the system displays "Your certificate is invalid."

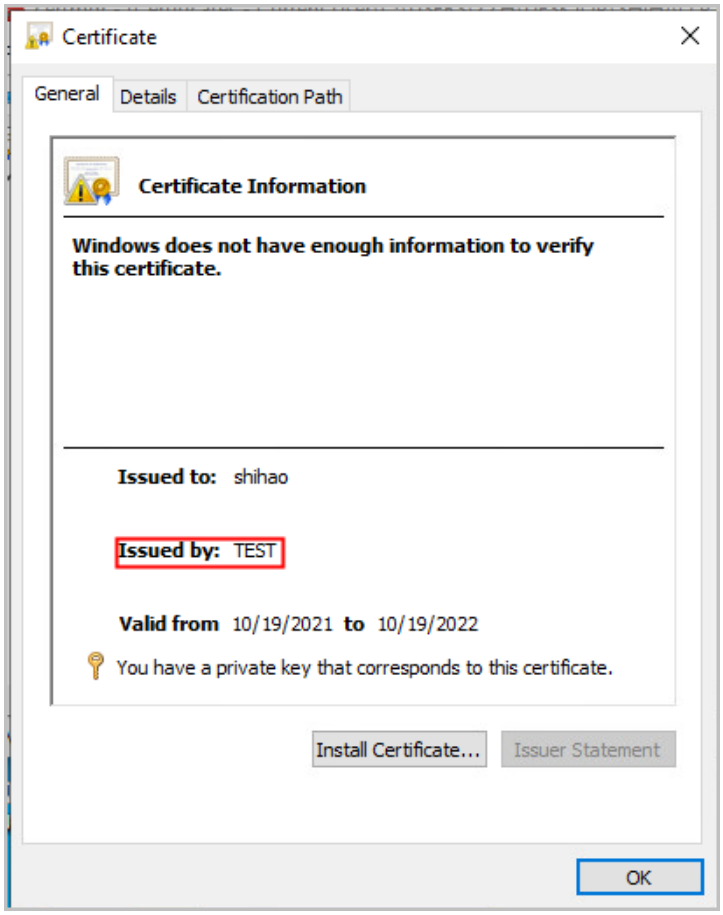


Possible Causes

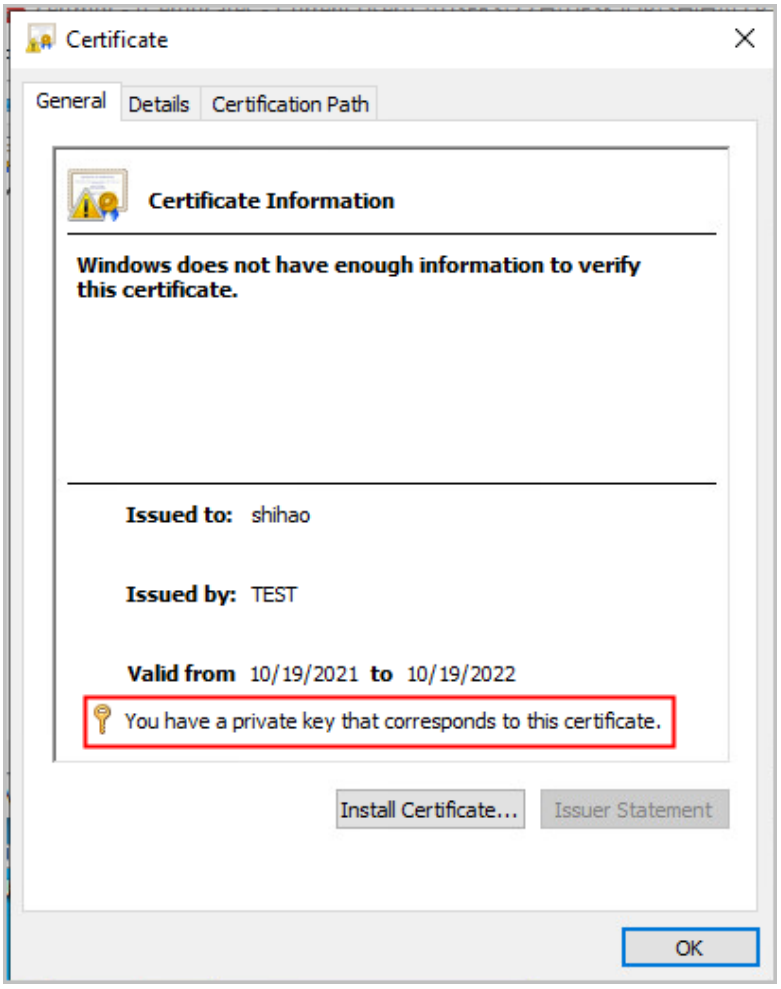
1. The user certificate is not issued using the root certificate signature of the CA certificate of the firewall virtual gateway client.
2. The user certificate installed on the device does not contain private key information.
3. The system time and time zone of the firewall are out of the scope of the user certificate.
4. The user certificate is revoked by the certificate revocation list (CRL) or online certificate status protocol (OCSP) configured on the firewall.

Procedure

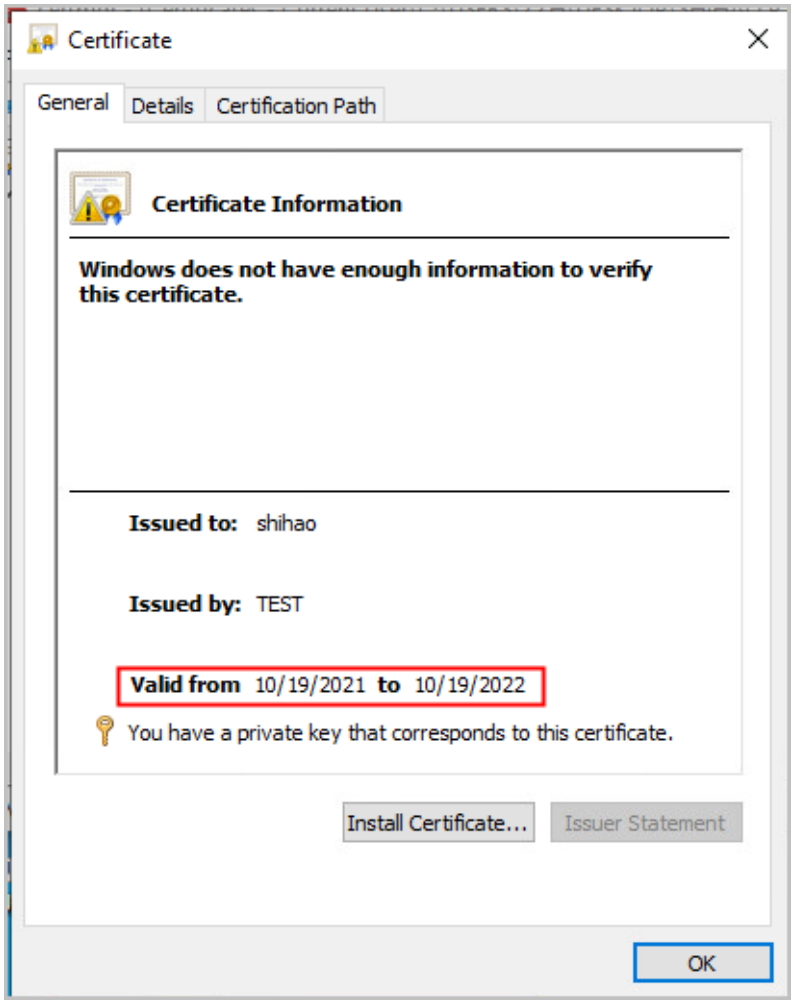
1. Check whether the Issued by field of the user certificate is the same as the Issued to field of the CA certificate on the firewall virtual gateway client.



2. Check whether the user certificate has a private key.



3. Check whether the system time and time zone of the firewall are within the scope of the user certificate.

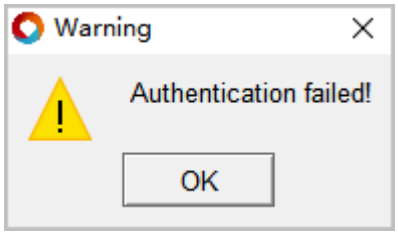


4. Check whether CRL or OCSP is configured on the firewall. If yes, undo the configuration and check the verification result.

1.6.3.3 Warning: Authentication failed

Symptom

Certificate challenge authentication is used by the virtual gateway. When you select a user certificate and click Login on the SecoClient login page, the system displays "Authentication failed."

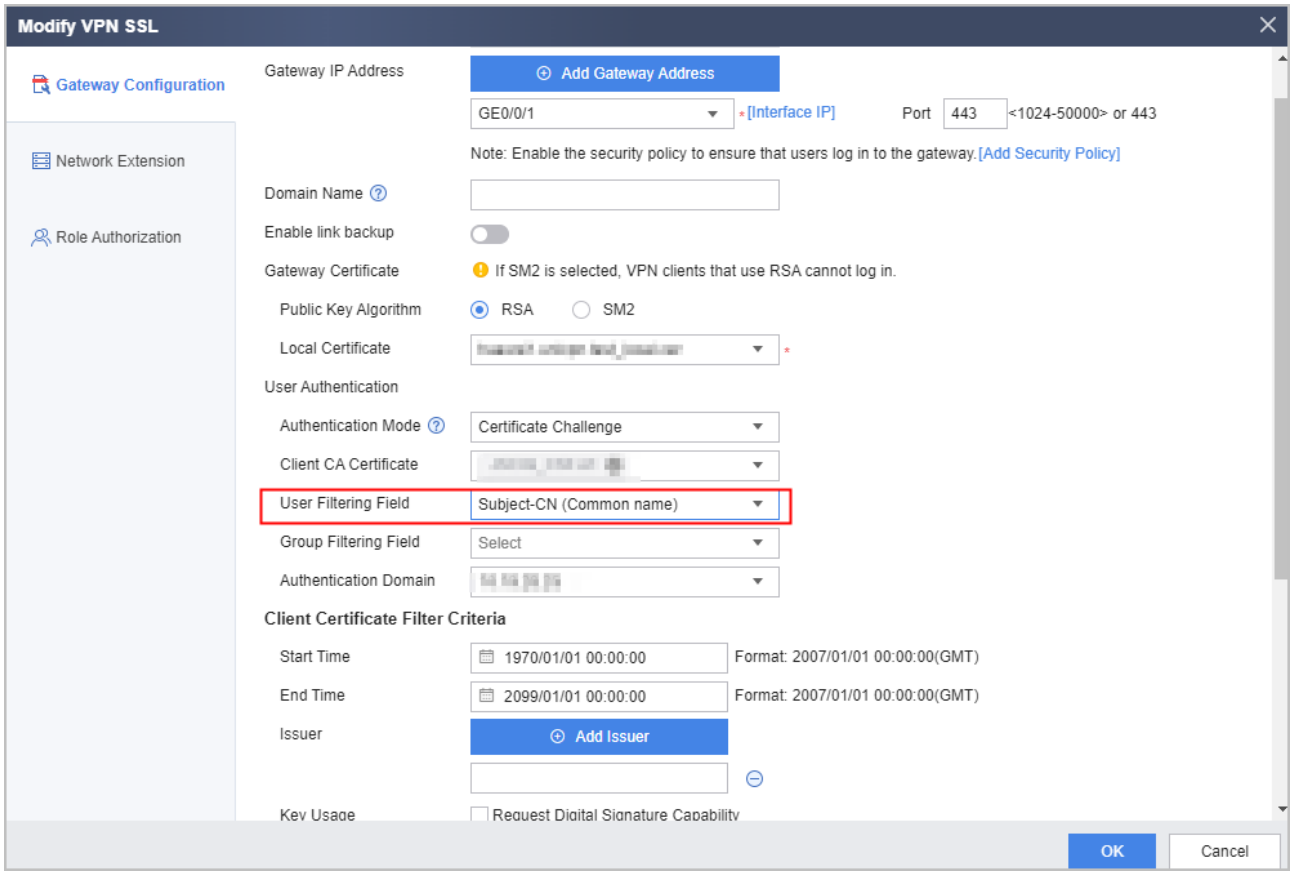


Possible Causes

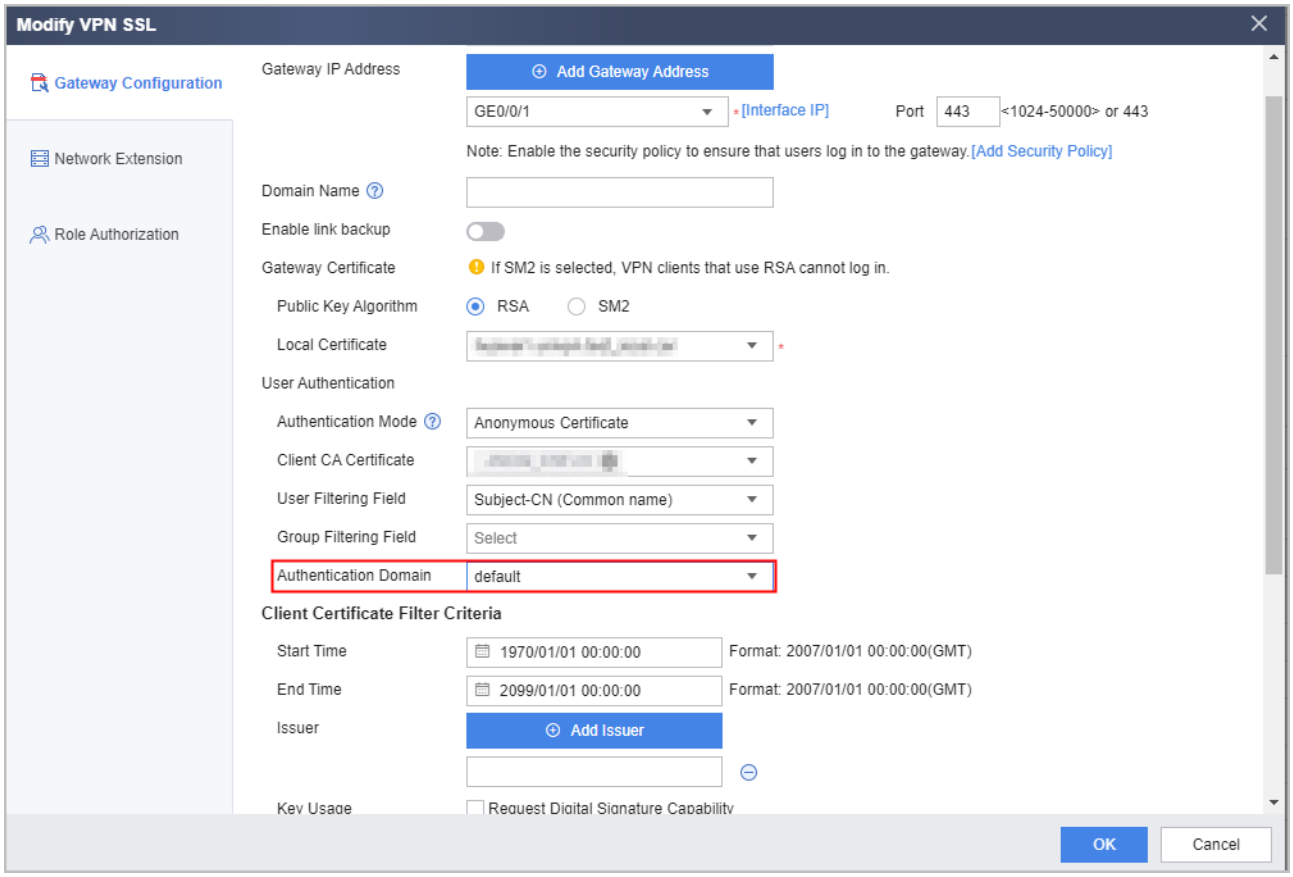
1. User Filtering Field configured for the virtual gateway certificate authentication is incorrect. As a result, the device obtains an incorrect user name from the user certificate when you log in to the device.
2. The virtual gateway is bound to an incorrect authentication domain.
3. SSL VPN access is not enabled for authentication domains.
4. The network extension feature is not enabled on the virtual gateway.
5. The SSL VPN login device is in a dual standby state (HRP_S), but SSL VPN does not support login on the standby device.
6. Expiration of certificate validity

Procedure

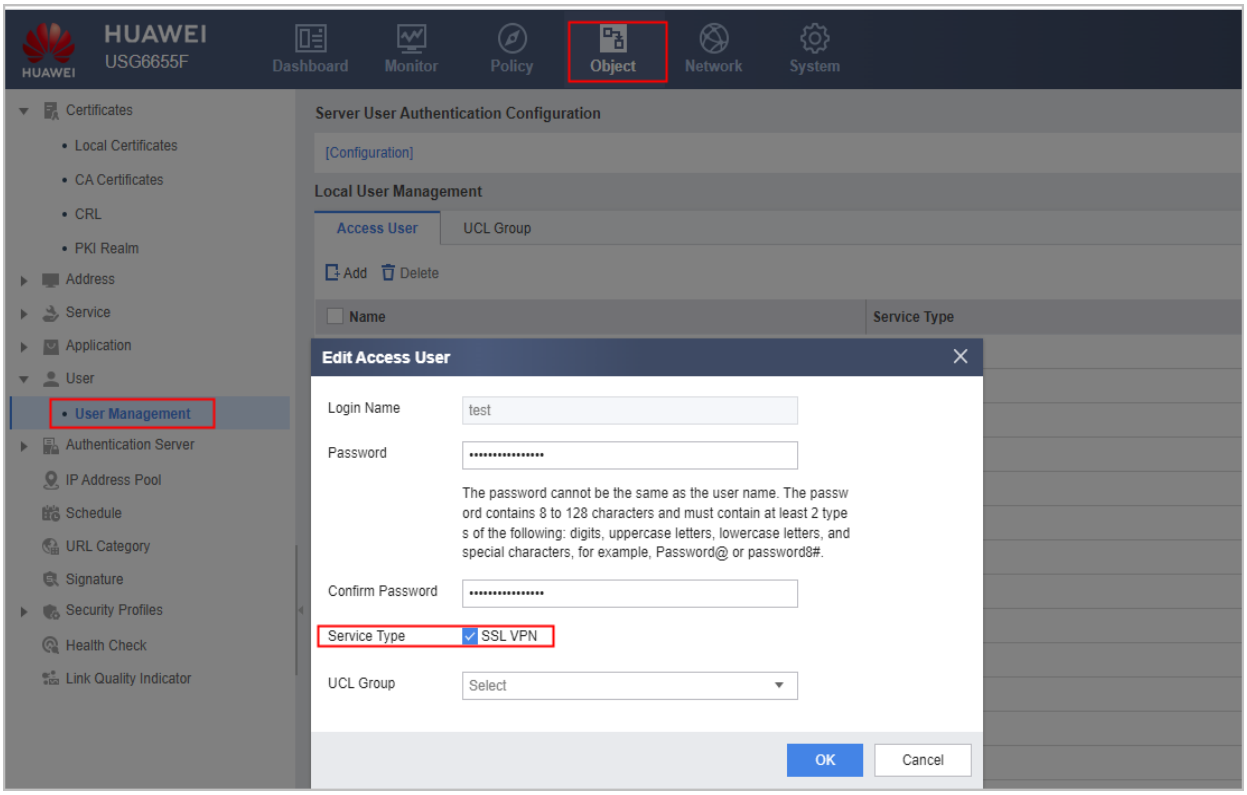
1. Log in to the device and check whether User Filtering Field configured in the virtual gateway certificate authentication matches the attribute name of the authentication field in the user certificate.



2. Check whether the correct authentication domain is bound to the virtual gateway.



3. Check whether SSL VPN access is enabled in the authentication domain.



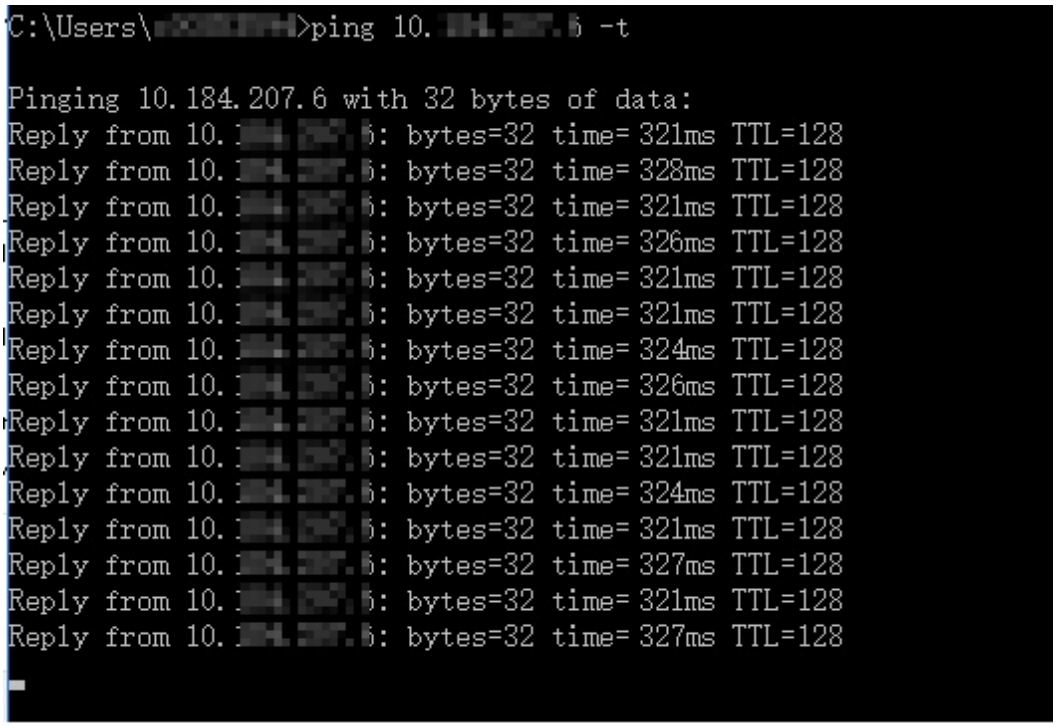
4. Enable the network extension feature of the virtual gateway.
5. Modify the configuration or networking to ensure that the SSL VPN login device is in the HRP_M state.
6. Re import a new valid certificate after deleting the expired certificate

1.6.4 Troubleshooting Guidelines for Abnormal Services Encountered After Successful Login

1.6.4.1 Intranet Resource Access Is Stalled, and the Delay in Pinging the Intranet Is Long

Symptom

The SSL VPN dialup is successful, but access to intranet resources is stalled, and the delay in pinging the intranet is long. The test download rate is much lower than the download rate in NAT mapping.

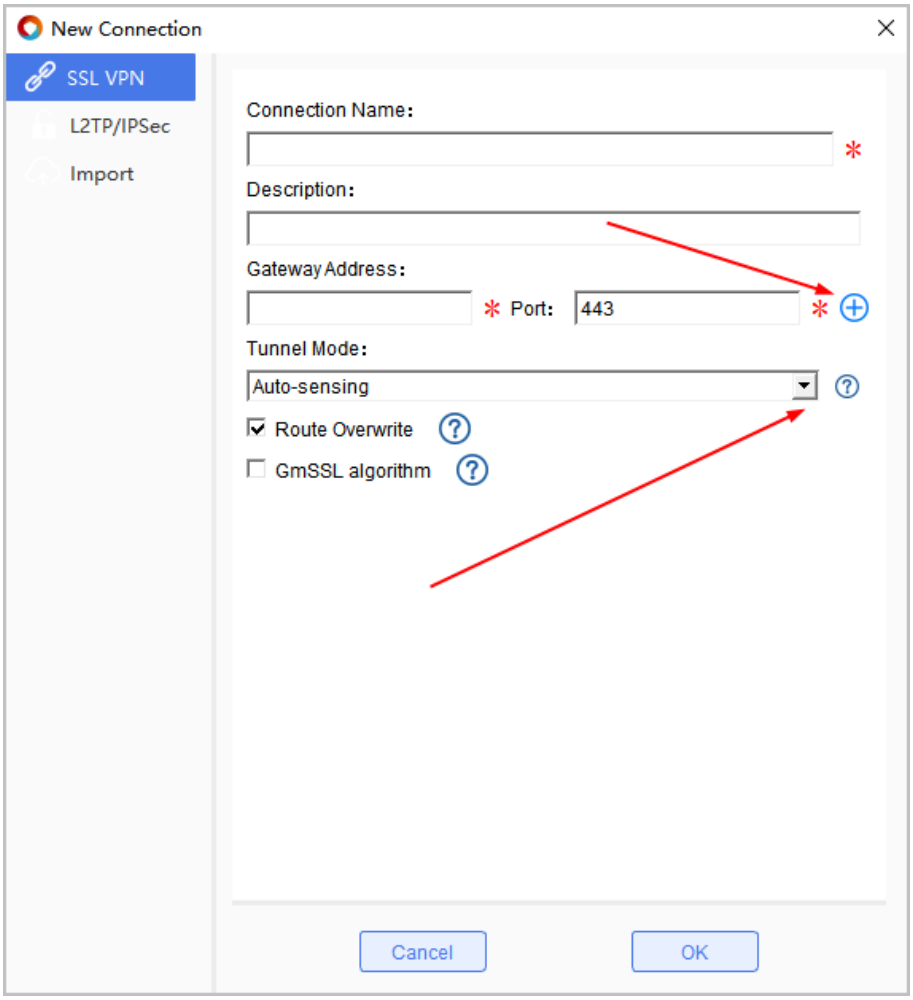


Possible Causes

NAT mapping only achieves address translation for packet headers, but the VPN technology encrypts and decrypts entire packets. Therefore, VPN requires more system resources and time than NAT mapping. This delay is more obvious if packets are transmitted over networks of different carriers.

Procedure

1. Select Quick Transmission or Auto-sensing from the Tunnel Mode drop-down list box. In quick transmission mode, the packet transmission rate is high. If Quick Transmission is selected, the interzone policy must be enabled between the Local zone and Untrust zone (assuming that the user is in the Untrust zone) on the firewall. In the policy, the service type is UDP, and the port number is 443. In auto-sensing mode, the SecoClient preferentially establishes an SSL VPN tunnel with the VPN gateway in quick transmission mode. If tunnel establishment fails, the SecoClient uses a reliable transmission mode to establish a VPN tunnel with the VPN gateway.
2. If an enterprise provides multiple SSL VPN gateways, enabling the automatic selection function on the SecoClient ensures that users can connect to the VPN gateway with the fastest response.



1.6.4.2 Failed to Access the Public Network After a Successful Login

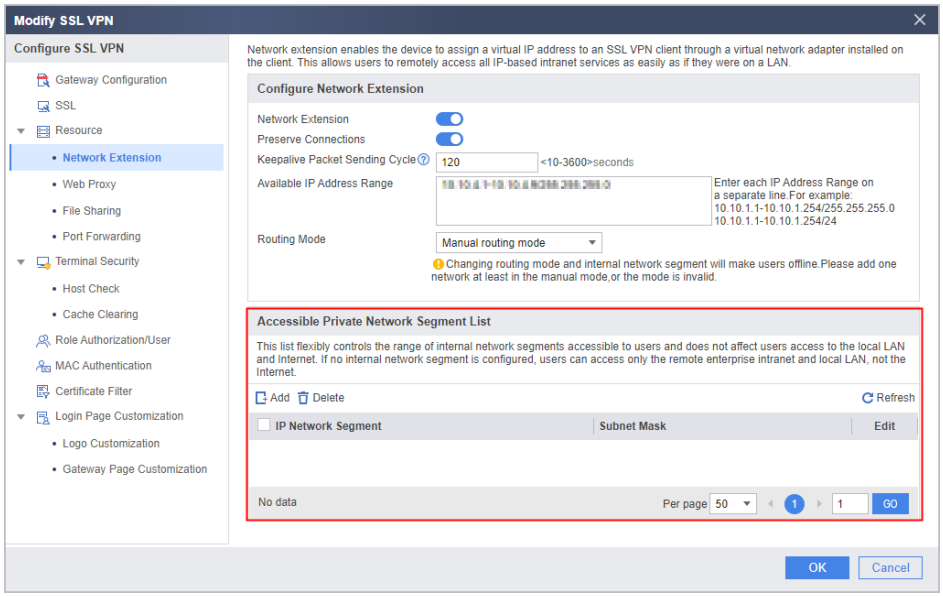
Symptom

The SSL VPN dialup is successful, but the public network cannot be accessed and the domain name cannot be pinged.

Possible Causes

The split or full routing mode is configured for the virtual gateway network extension service.

The network extension function is configured on the web page. If the accessible internal network segment list does not contain any network segment, the network extension routing mode is the split mode (network-extension mode split). If one or more network segments exist in the list, the network extension routing mode is the manual mode (network-extension mode manual). You can run the network-extension mode full command on the CLI console to set the full routing mode, but this mode cannot be configured using the web page. If the split or full routing mode is configured for network extension, the Internet is not accessible after SSL VPN dialup is used.



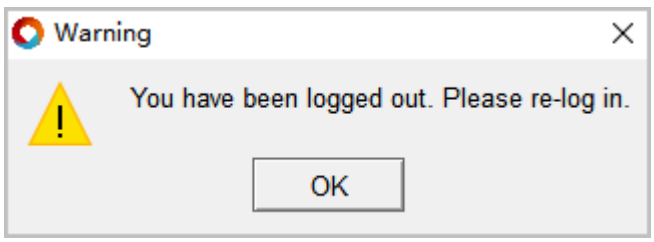
Procedure

Change the network extension routing mode to the manual mode. Enable the network extension function for devices so that VPN tunnels are used only when the devices access the specified VPNs on the intranet.

1.6.4.3 Warning: You have been logged out. Please re-log in.

Symptom

You are using the SecoClient service for a period after logging into the SecoClient, but the system displays "You have been logged out. Please re-log in."



Possible Causes

1. You are logged out by the administrator.
2. The aging time expires.

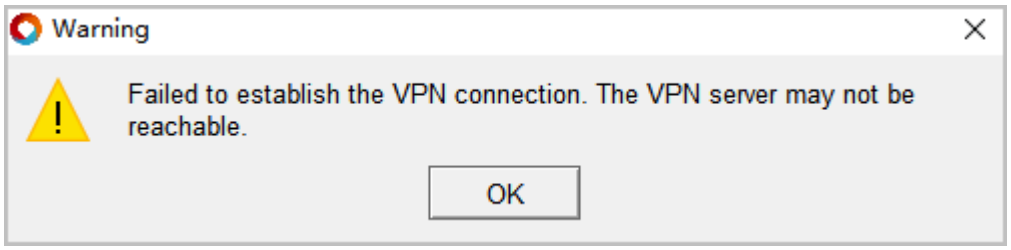
Procedure

3. Log in to the VPN gateway, and choose Monitor > System Logs. Check the firewall operation logs to see if the administrator has logged out you.
4. Check the session timeout interval configured on the virtual gateway and whether Preserve Connections is enabled.

1.6.4.4 Info: Failed to set up a VPN connection. The VPN server may be unreachable.

Symptom

After logging in to the UniVPN, the system displays "Info: Failed to set up a VPN connection. The VPN server may be unreachable."



Possible Causes

There is a high probability that the problem occurs because an encryption algorithm used by the client is different from that used by a gateway.

Procedure

Since V600R007C20SPC100, weak encryption algorithms are disabled on the virtual gateway by default. In this case, the cipher suite of the virtual gateway can only use strong encryption algorithms. Only SecoClient running 7.0.2.26 or a later version can be used to log in to the virtual gateway.

For versions earlier than 7.0.2.26, you can run the v-gateway ssl weak-encryption enable command on the gateway to enable weak encryption algorithms of the virtual gateway.

1.6.4.5 After a Terminal Is Added to an AD Domain, SSL VPN Users Are Disconnected After Accessing the Network for a Period of Time

Symptom

After a terminal is added to an AD domain, SSL VPN users go offline unexpectedly after accessing the network for a period of time. When the terminal is not added to the AD domain, SSL VPN users do not go offline.

The fault symptoms are as follows.

- User logout records can be viewed on the firewall.

  Check user logout records on the active firewall. The following information is displayed.

```
[HUAWEI]info-center source sslvpn channel logbuffer log level informational
Warning: There is security risk as all logs which level is not less than 6 will be output the logbuffer.
[HUAWEI]display logbuffer service-log
2023-04-23 11:43:46.314 +08:00
Logging buffer configuration and contents : enabled
Allowed max buffer size : 10240
Actual buffer size : 512
Channel number : 4 , Channel name : logbuffer
Dropped messages : 0
Overwritten messages : 1008
Current messages : 11

Apr 23 2023 11:39:02+08:00 HUAWEI %%01SSLVPN/6/USERLOGOUT(l):CID=0x814f0428;The user logged out. (User Name=csf, Vsys=pub
lic, VGName=sslvpntest, Virtual IP= [redacted], Client IP= [redacted] Obverse Packets=9, Obverse Bytes=1110, Reverse Pa
ckets= 76, Reverse Bytes=4596, Logout Reason=The user proactively goes offline.).
Apr 23 2023 11:38:28+08:00 HUAWEI %%01SSLVPN/6/USERLOGINSUCC(l):CID=0x814f0428;User login succeeded. (User Name=csf, Vsys
=public, VGName=sslvpntest, Virtual IP= [redacted] Client IP=[redacted]).
```

  Check user logout records on the standby firewall. The following information is displayed.

```
[HUAWEI]info-center source sslvpn channel logbuffer log level informational
Warning: There is security risk as all logs which level is not less than 6 will be output the logbuffer.
[HUAWEI]display logbuffer service-log
2023-04-23 11:43:46.314 +08:00
Logging buffer configuration and contents : enabled
Allowed max buffer size : 10240
Actual buffer size : 512
Channel number : 4 , Channel name : logbuffer
Dropped messages : 0
Overwritten messages : 1008
Current messages : 11

Apr 23 2023 11:39:02+08:00 HUAWEI %%01SSLVPN/6/USERLOGOUT(l):CID=0x814f0428;The user logged out. (User Name=csf, Vsys=pub
lic, VGName=sslvpntest, Virtual IP= [redacted], Client IP= [redacted] Obverse Packets=9, Obverse Bytes=1110, Reverse Pa
ckets= 76, Reverse Bytes=4596, Logout Reason=The user proactively goes offline.).
Apr 23 2023 11:38:28+08:00 HUAWEI %%01SSLVPN/6/USERLOGINSUCC(l):CID=0x814f0428;User login succeeded. (User Name=csf, Vsys
=public, VGName=sslvpntest, Virtual IP= [redacted] Client IP=[redacted]).
```

- SecoClient logs show that the gateway forces the user to go offline.

```
FRAME  DEBUG  2020-09-02 12:45:09.000334 ][B00550] [65535][Create event base][eventbase notifyserver notify send ok sock(1256)
FRAME  DEBUG  2020-09-02 12:45:09.000334 ][B00550] [65535][Add event][interval(10:0) tv(10:0) timeout:(1599061519:334423)]
FRAME  DEBUG  2020-09-02 12:45:09.000335 ][B00550] [65535][Insert event][timeoutlist(fd:4 ev_res:268435696 total:0 timer:5 act
FRAME  DEBUG  2020-09-02 12:45:09.000335 ][B00550] [65535][eventlist todo wait][end ok,todo:0000000036A2820 semid:7]
FRAME  DEBUG  2020-09-02 12:45:09.000335 ][B00550] [65535][Unbind channel][unbind channel OK (chid 239 268435695 events(2))]
CNEM   WARN   2020-09-02 12:45:15.000450 ][B00550] [65535][Cnem handle packet from gateway][CMDtype is KICKOUT]
FRAME  DEBUG  2020-09-02 12:45:15.000450 ][B00550] [65535][send message][task(4) mqueid(4) message type:1 send message addr(000
CNEM   INFO   2020-09-02 12:45:15.000451 ][B00550] [65535][Cnem send status msg to self ok]
```

- Collect debug logs on the firewall. The LAM module generates the CUT_REQ event before the user goes offline.

```
HRP_M<HUAWEI-diagnose> debugging swm error
Sep 14 2020 13:15:49-03:00 FGSTHA00-01 CM/7/DEBUG:
[UCM-MSG] MSG Recv From: (taskName=LAM, Code=ESAP_SRV_MSG_CUT_REQ, Src=0, Dst=-1, Slot=0)WebAuth: 0x0 Vrf: 0Reason: 29 Vlan: 0 VPI/VCI: 0/0 AccessType: 0TimeoutMsg: 0 Mac: 0000-0000-0000 IPV6: IP: 10.0.91.28.
Sep 14 2020 13:15:49-03:00 FGSTHA00-01 CM/7/DEBUG:
```

Possible Causes

There is a high probability that the problem occurs because both SSL VPN and AD SSO (AD SSO is installed to query AD server security logs) are configured on the firewall.

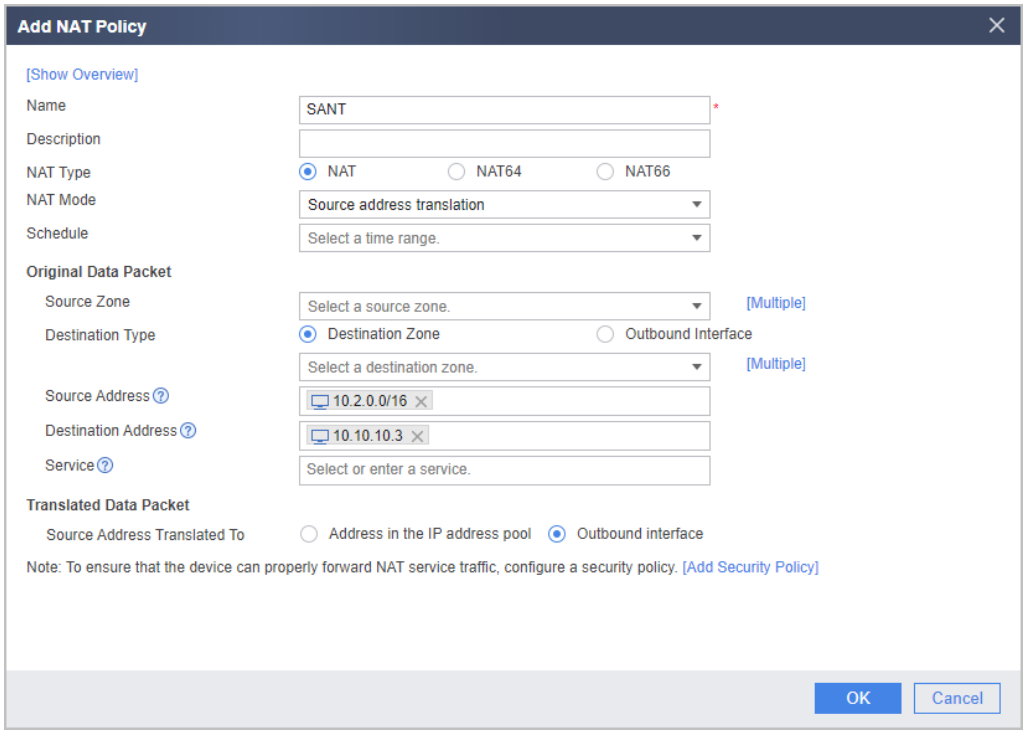
After the terminal joins the AD domain, the SSL VPN user needs to connect to the AD domain controller for authentication (the AD domain controller records security logs at

that time). After the authentication succeeds, the SSL VPN user successfully logs in to the network from the firewall. When the AD SSO server obtains security logs (containing the mapping between SSL VPN accounts and virtual IP addresses) from the AD domain controller, the server sends security logs to the firewall, and the firewall forces the user to go online again based on the security logs. In this scenario, the same user (the same account corresponds to the same virtual IP address) logs in to the network from the firewall twice. The first time is the SSL VPN user login process. After the SSL VPN user is authenticated, the user logs in to the network from the firewall. The second time is that the firewall parses the security logs sent by the AD SSO server and forces the user to go online.

However, the firewall does not support the preceding scenarios. When the firewall parses the security logs sent by the AD SSO server to force the user to go online, the firewall forces the existing online SSL VPN users to go offline.

Procedure

1. Check whether the AD SSO function (querying security logs on the AD server after AD SSO is installed) is configured on the firewall. If yes, go to the next step. If the AD SSO function is not configured, contact Huawei technical support.
2. Configure a source NAT policy on the firewall.
3. Configure a source NAT policy for the authentication data flow from SSL VPN users to the domain controller server. After the configuration, the SSL VPN user does not directly interact with the domain controller. In the security logs generated on the AD domain controller, the source IP address is not the virtual IP address obtained through SSL VPN dialup but is the IP address of the intranet interface of the firewall. In this way, when the firewall parses the security logs sent by the AD SSO server and forces the related user to go online, the firewall does not force the existing online SSL VPN users to go offline.
   d. Choose Policy > NAT Policy > NAT Policy from the main menu.
   e. Click Create and configure a source NAT policy.
   f. Assume that the virtual IP address of the SSL VPN user is 10.2.0.0/16 and the IP address of the AD domain controller is 10.10.10.3.



1.7 FAQs About the Mobile Client

In addition to the PC-based UniConnect client, Huawei also launches the iOS- and Android-based mobile clients.

How to Obtain

- **Obtaining the iOS mobile client**

  Method 1: Open the **App Store**, and search for **UniConnect** to download the latest version.

- **Obtaining the Android mobile client**

  Method 1: Download and open an AppGallery app, and search for **UniConnect** to download the latest version.

Specifications

Currently, the UniConnect mobile client supports only SSL VPN connections. The following table lists the supported models and operating systems:

Table 1-1 Supported models and operating systems

Operating System	iOS	Android
Supported Operating System Version	iOS 10.0 or later.	Android 5.0 or later.

Operating System	iOS	Android
Supported Device Model	• iPhone X • iPhone 8/8 Plus • iPhone 7/7 Plus • iPhone 6s/6s Plus • iPhone 6/6 Plus • iPhone 5s • iPad Pro • iPad Air 1/2 • iPad 4 • iPad mini 2/3/4	-
Supported Device Screen Resolution	-	• 720*1280 • 1080*1920 • 1440*2560 • 2160*4096

The function specifications of the UniConnect mobile client are as follows:

Table 1-2 Function specifications

Function		iOS	Android
SSL VPN	Network extension	Supported	Supported
	Terminal security NOTE When the terminal security function is enabled on the gateway, the UniConnect mobile client can dial up successfully.	Supported	Supported
	Selecting the optimal gateway	Supported	Supported
	Reconnection upon disconnection	Supported	Supported

Function		iOS	Android
	Link backup NOTE When the link backup function is enabled on the gateway, the UniConnect mobile client can dial up successfully.	Supported	Supported
	Certificate authentication	Supported	Supported
	MAC address authentication	Not supported	Not supported
	Certificate filtering	Supported	Supported
	Two-factor authentication	Supported	Supported Perform two-factor authentication using an SMS verification code.
L2TP VPN		Not supported	Not supported
L2TP over IPsec VPN		Not supported	Not supported
NAT Traversal		Not supported	Not supported
Proxy Traversal		Not supported	Not supported
Tunnel Splitting		Supported	Supported
Basic Function	Automatic startup upon power-on	Not supported	Not supported
	GUI Language Switching NOTE Users can only switch between Chinese and English.	Supported	Supported
	Automatic login	Supported	Supported
Configuration File	Import	Not supported	Not supported
	Export	Not supported	Not supported
Fault Locating		Supported	Supported
Command Line Configuration		Not supported	Not supported
Non-administrator User Configuration		Supported	Supported

The performance specifications of the UniConnect mobile client are as follows:

Table 1-3 Performance specifications

Function	Specifications
Number of new VPN connections	16

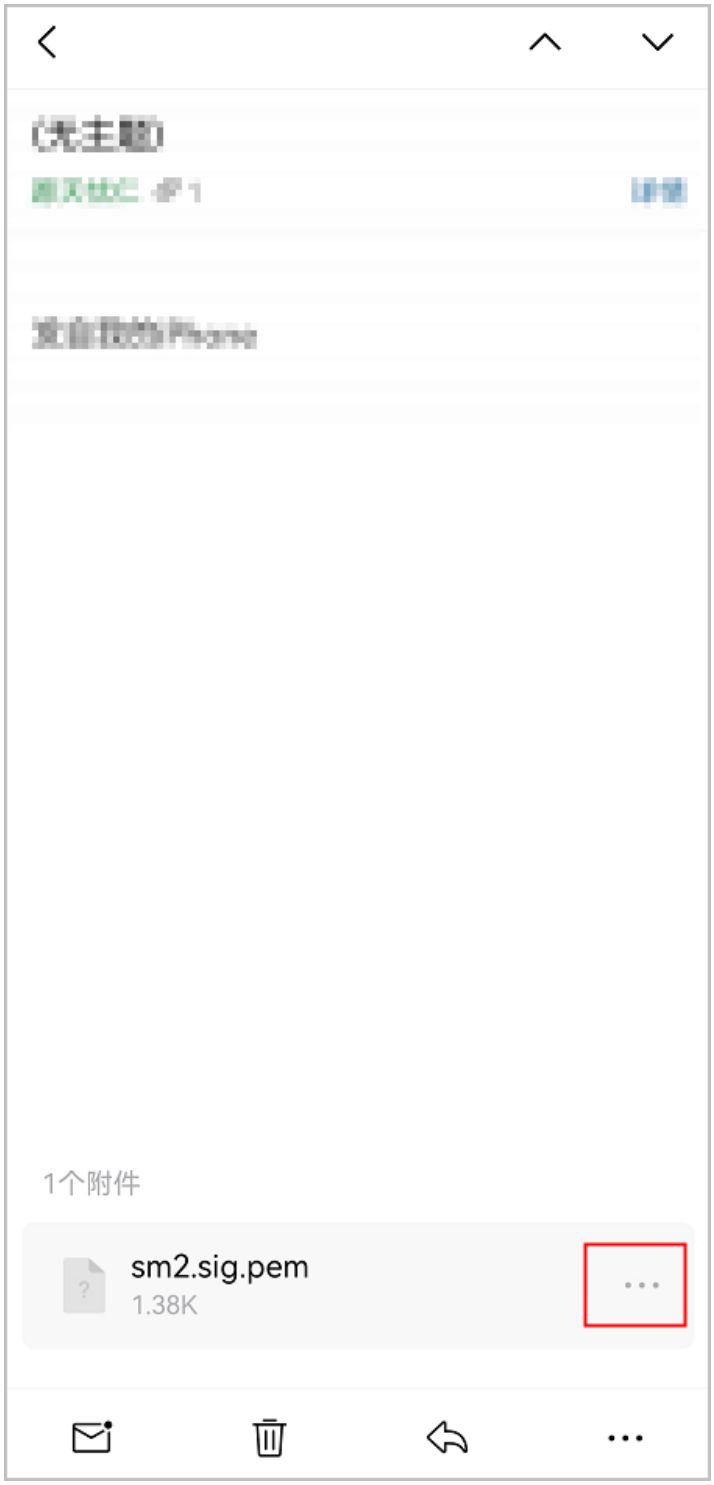
Operations

For details about how to use the UniConnect mobile client, choose  > **Help** in the app and view the online help.

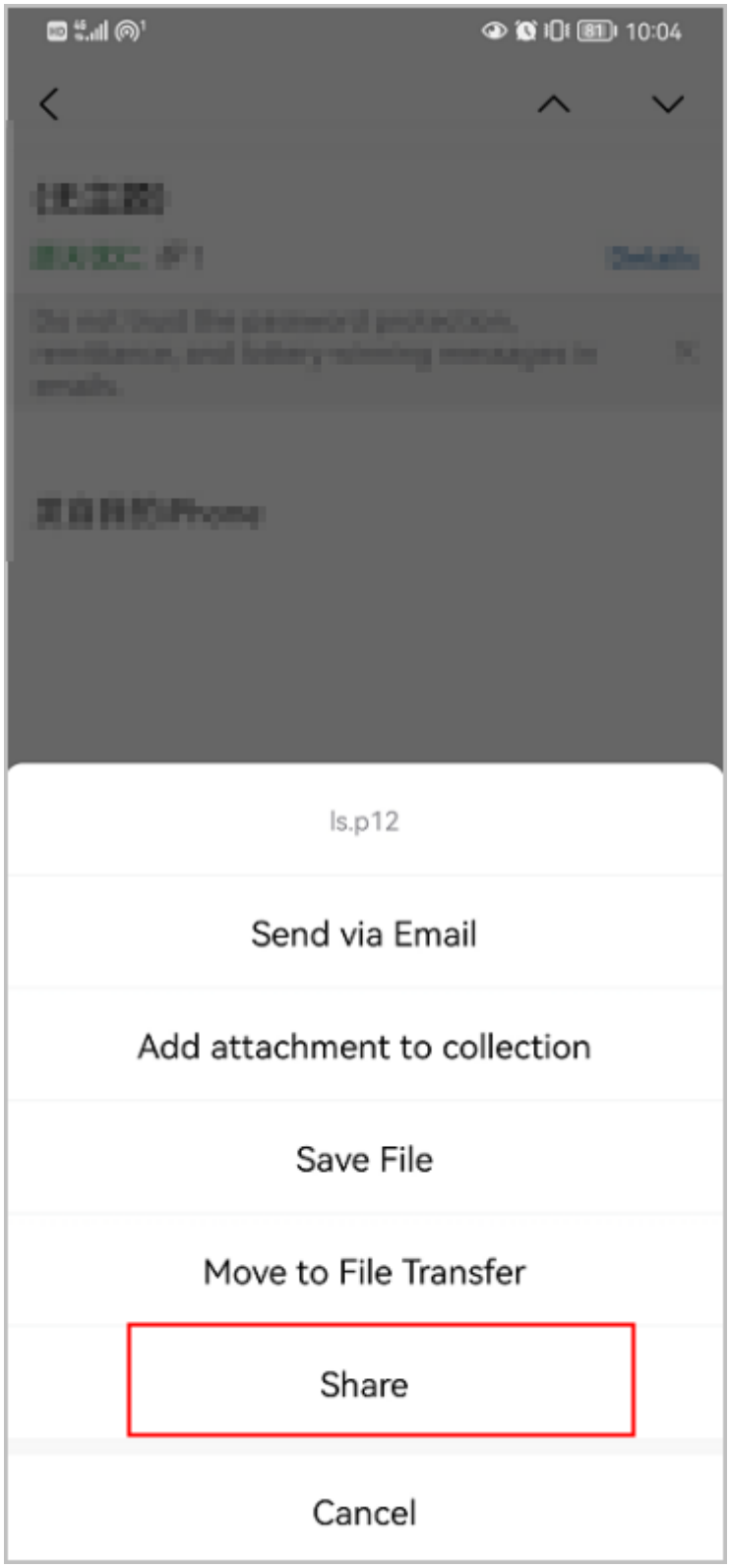
1.7.1 How Do I Import a Chinese Cryptographic Certificate?

The following describes how to import the Chinese cryptographic certificate into the UniConnect client, and the import method for a non-Chinese cryptographic certificate is the same.

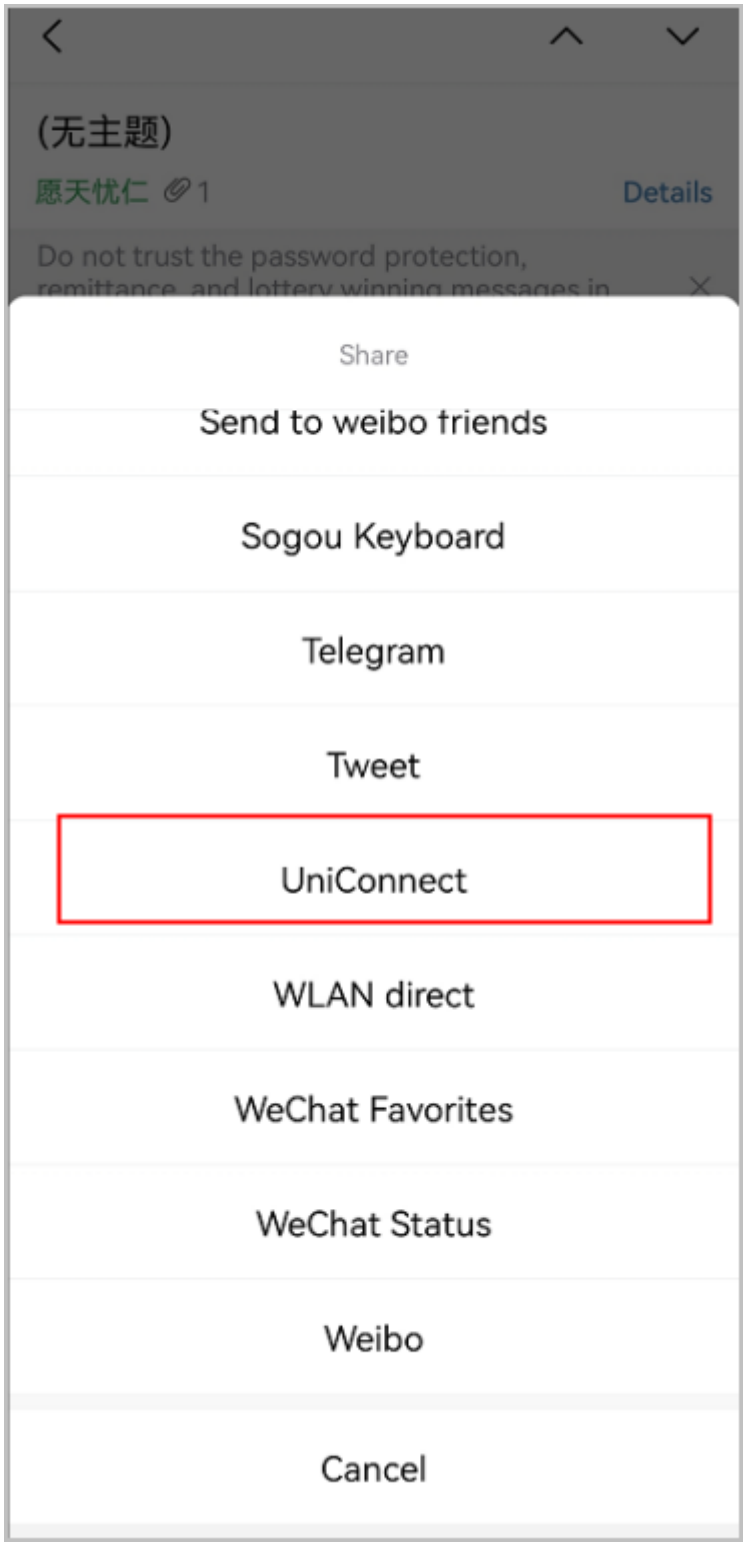
Step 1 Open your mailbox, find the certificate file, and click  in the lower right corner.



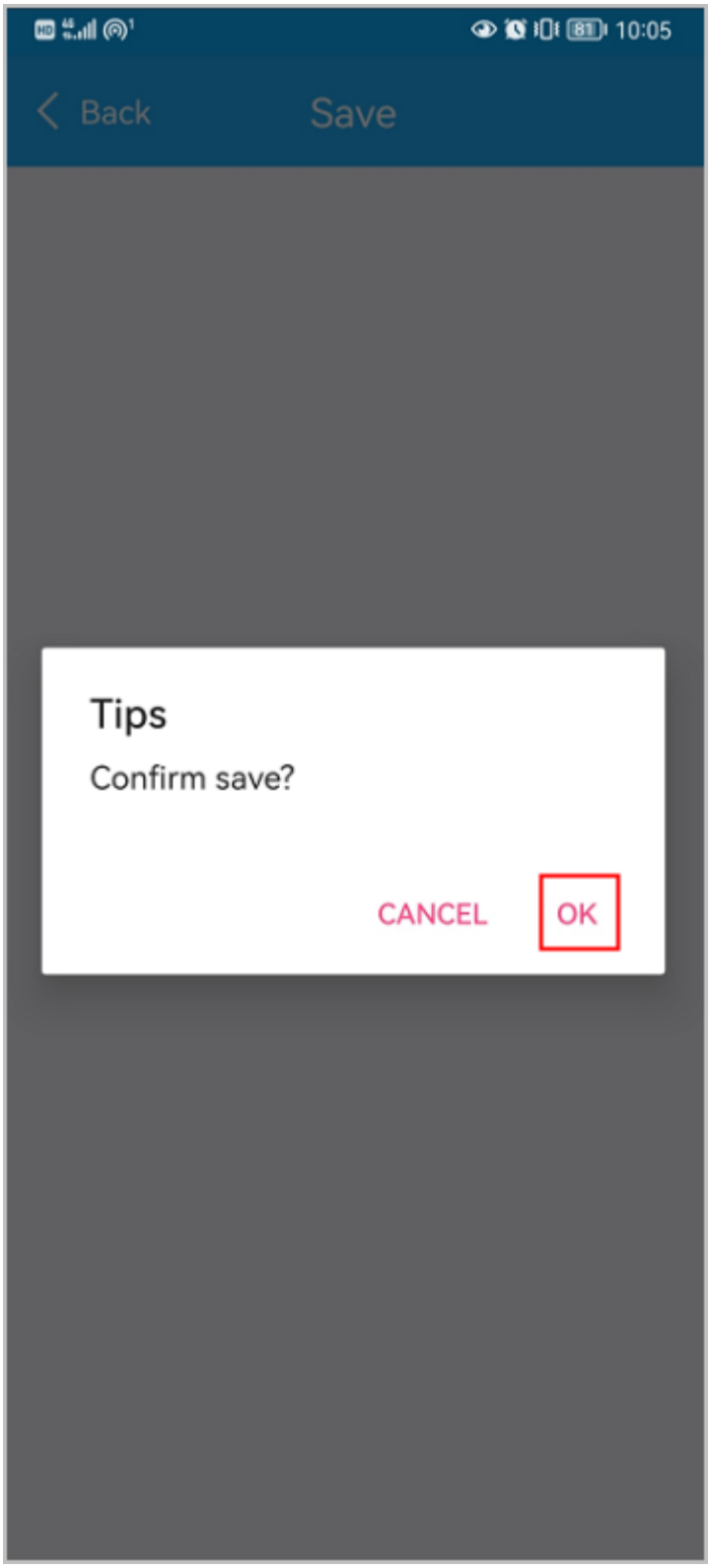
Step 2 Click the file (The download starts when the file is not downloaded) and click **Share**.


10:04
ls.p12
Send via Email
Add attachment to collection
Save File
Move to File Transfer
Share
Cancel

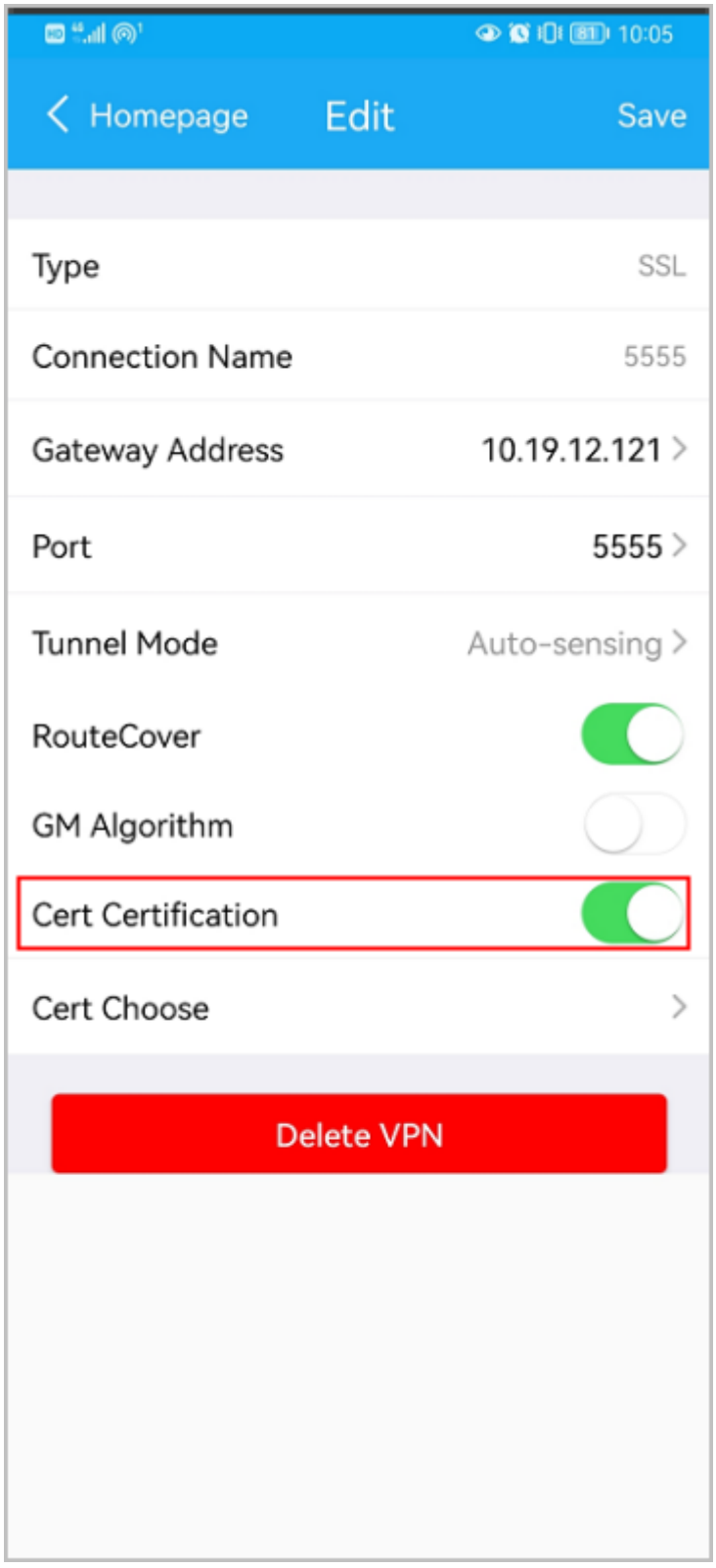
Step 3 Click **UniConnect**.



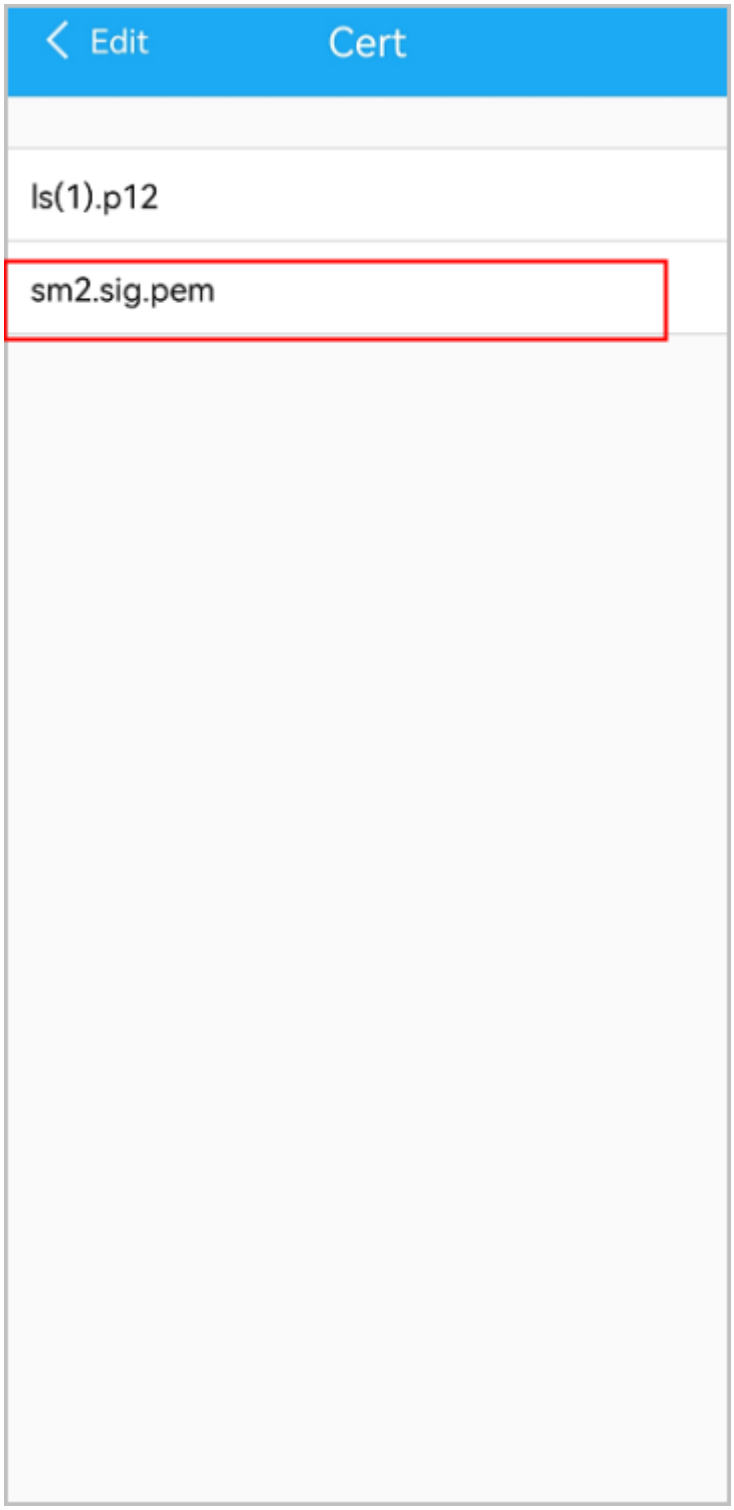
Step 4 Click **OK**.



Step 5 After the import is successful, enable **Cert Certification**.



Step 6 Click **Cert Choose** and select **sm2.sig.pem**.

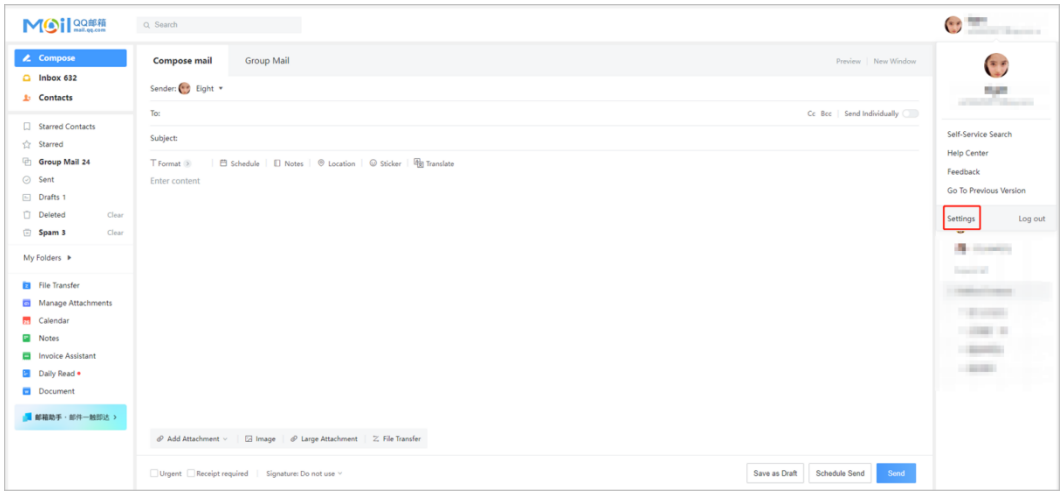


----End

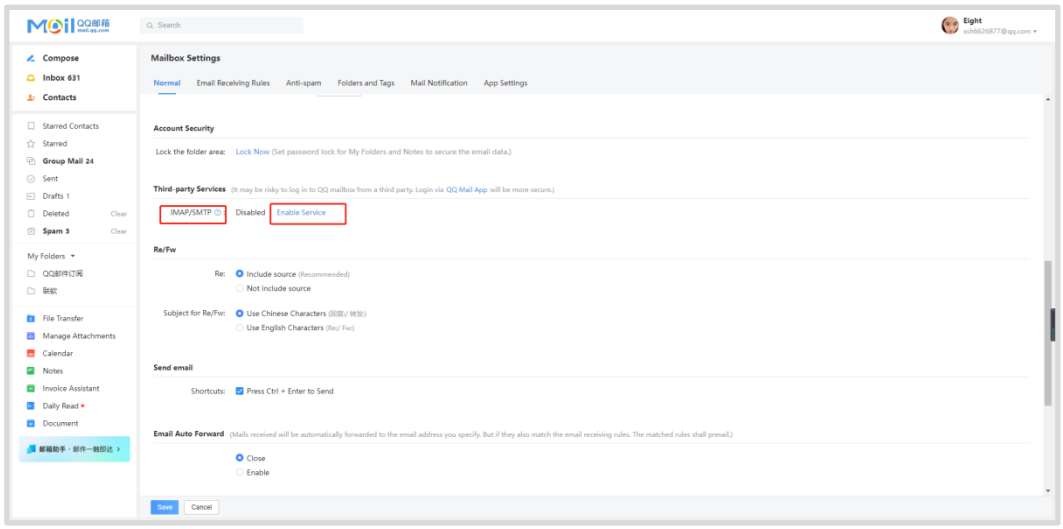
1.7.2 How Do I Report an iOS Clinet Problem?

Configuring the Mailbox

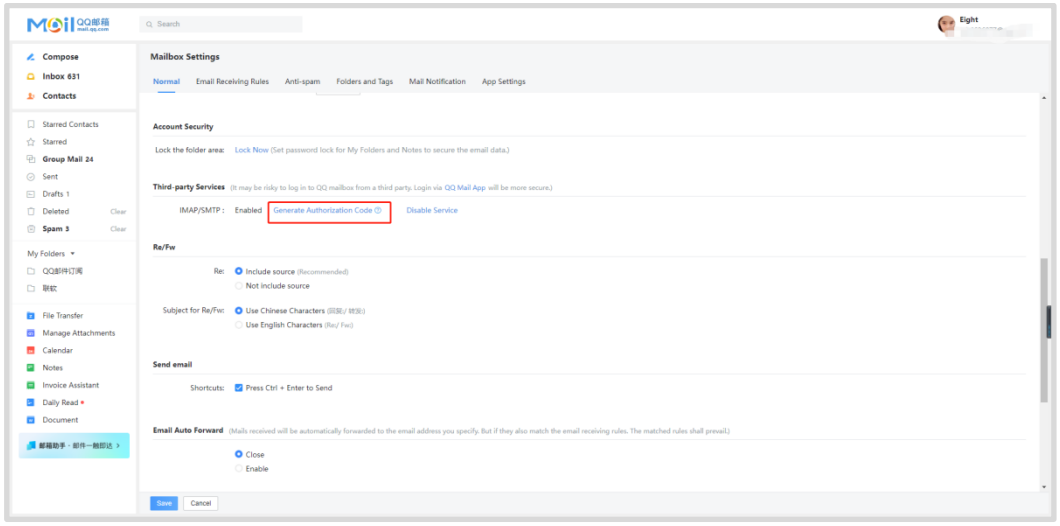
Step 1 Go to QQMail, click the user name in the upper right corner, and click **Settings**.

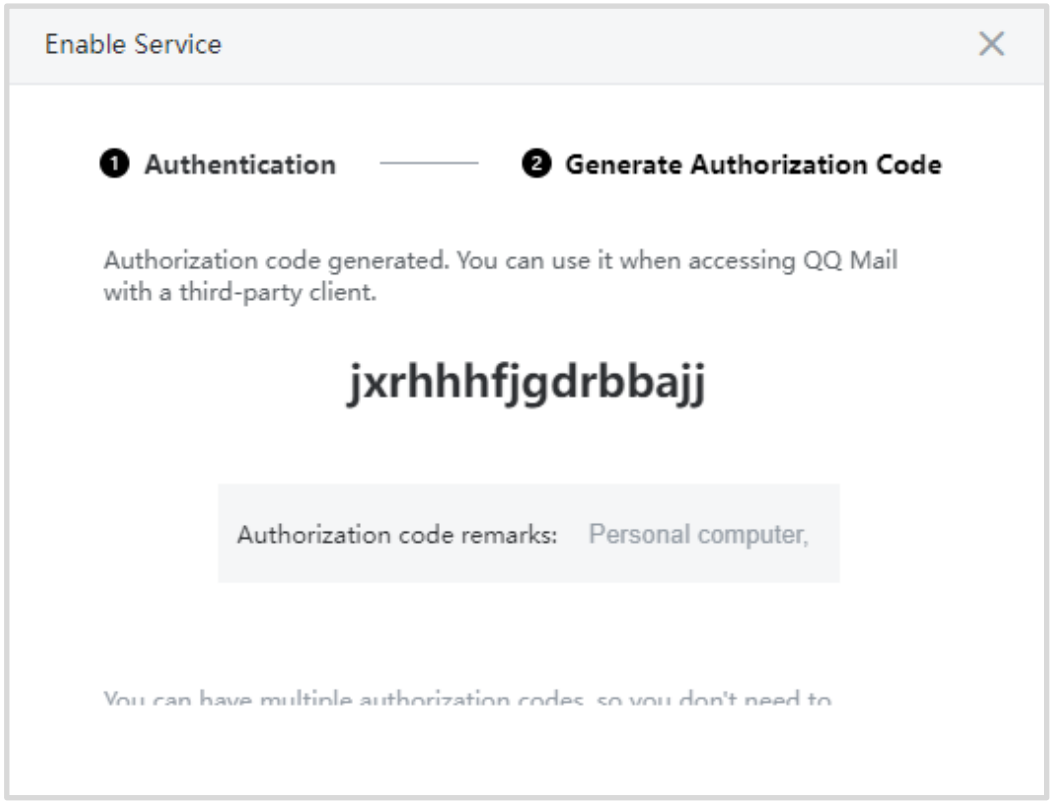


Step 2 On the **Normal** tab page, click **Enable Service** behind **IMAP/SMTP** to enable the IMAP service.



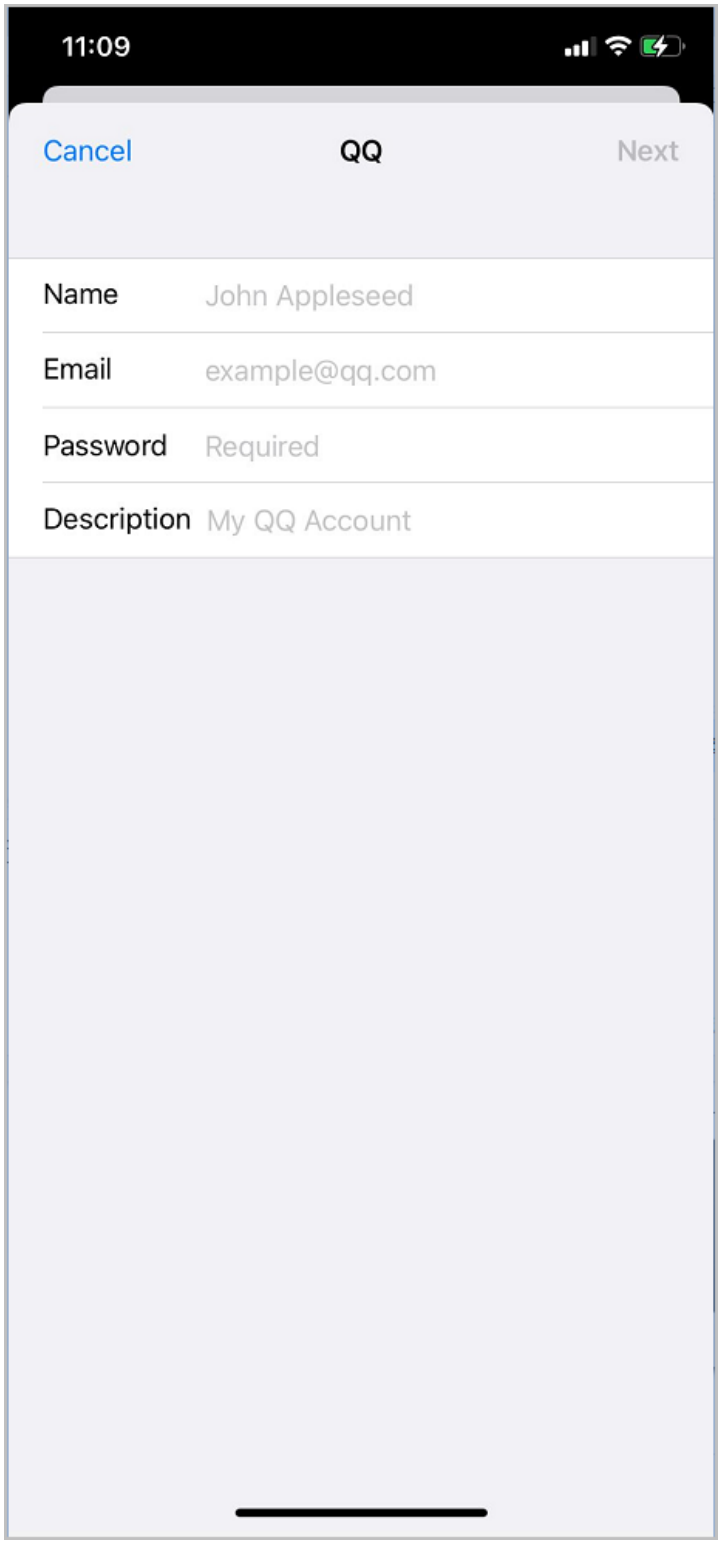
Step 3 Click **Generate Authorization Code** to obtain an authorization code.





Step 4 Open the mailbox app on the mobile phone. Select QQMail if it is available. Select **Other** if QQMail is unavailable.

Step 5 Set **Name**, **Email**, and **Password** (the authorization code displayed in the second figure in step 3).

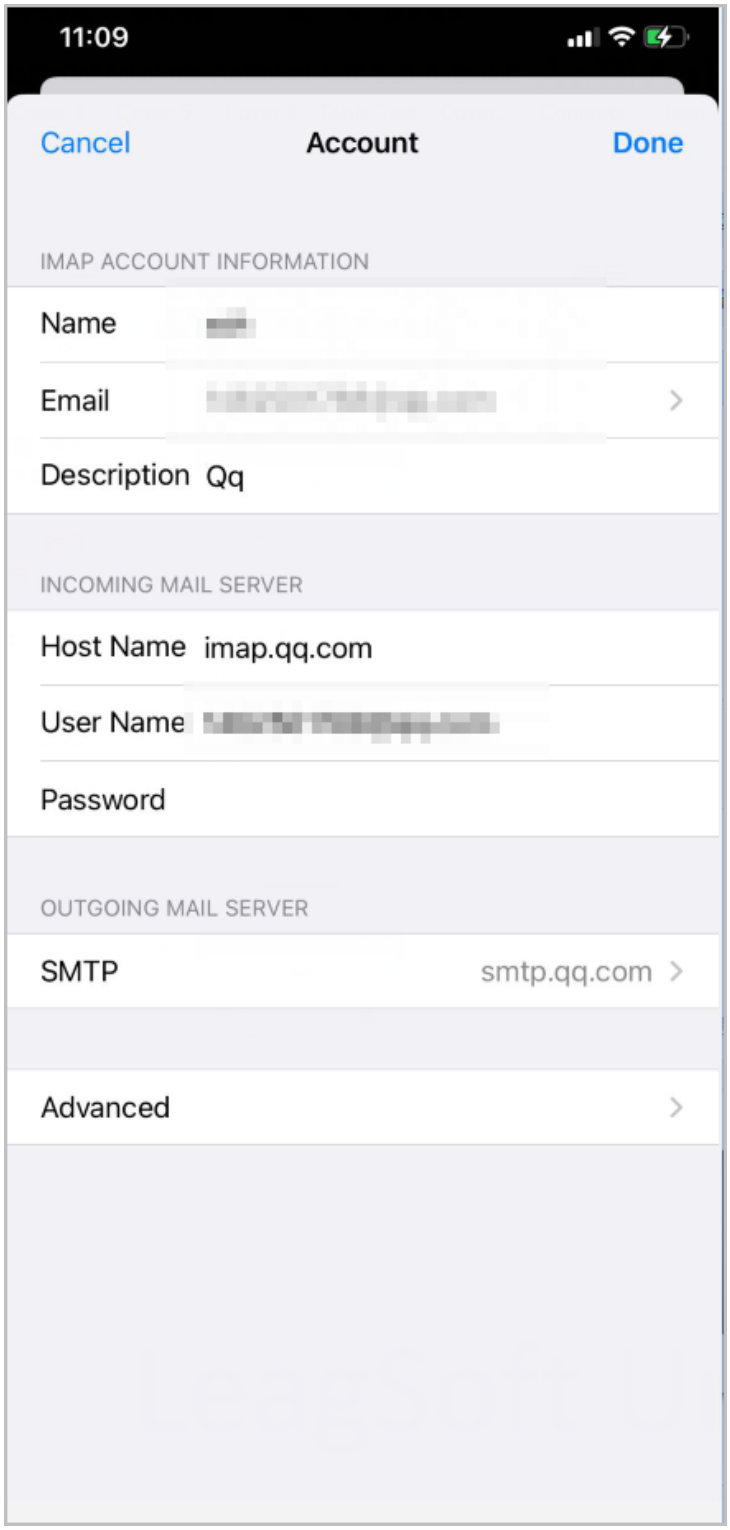


Step 6 Click **Next** in the upper right corner.

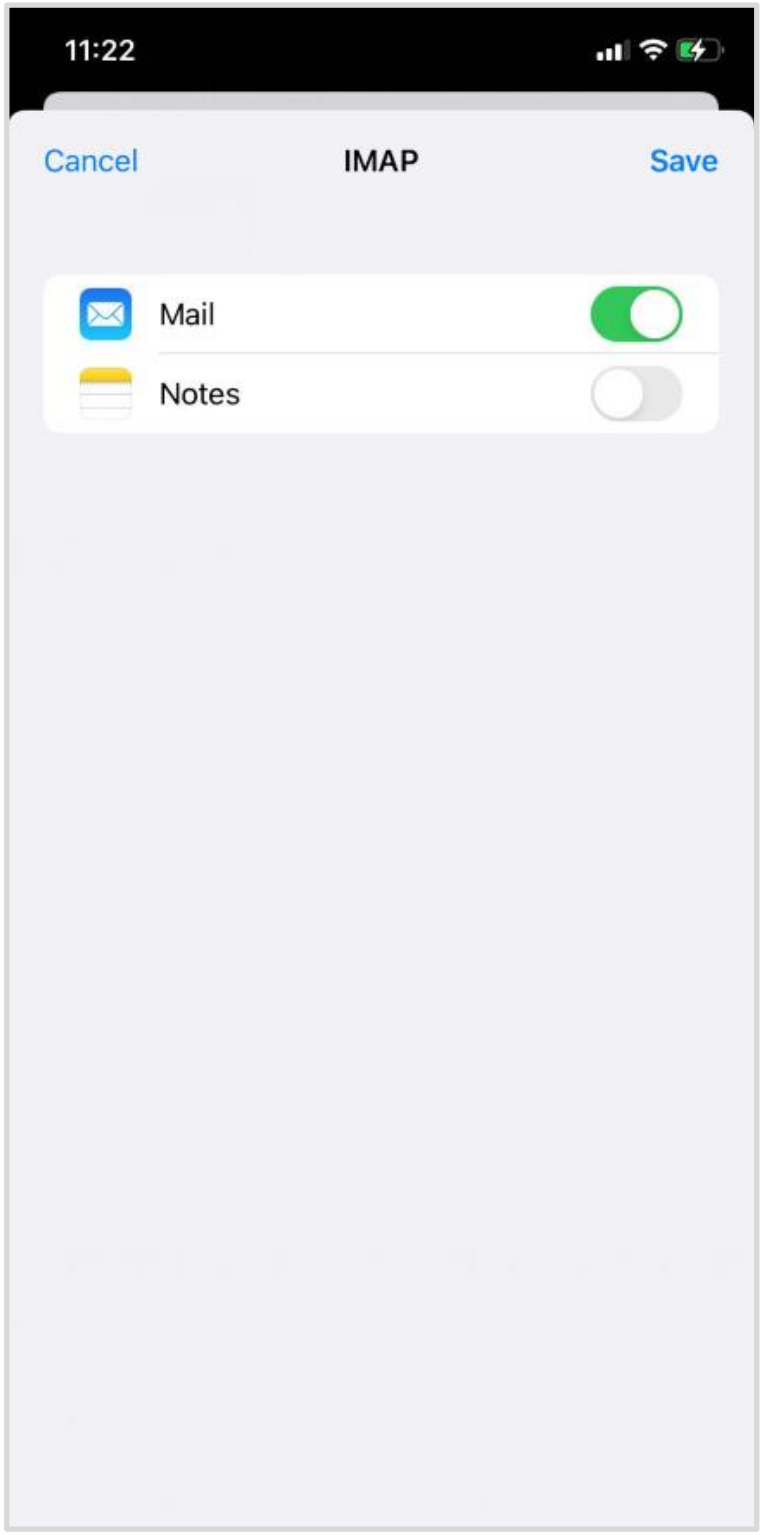
Step 7 In the **IMAP ACCOUNT INFORMATION** area, set **Name**, **Email**, and **Description**.

In the **INCOMING MAIL SERVER** area, set **Host Name**(imap.qq.com), **User Name** (email address), and **Password** (the authorization code displayed in the second figure in step 3).

The information entered for **OUTGOING MAIL SERVER** is the same as that entered for **INCOMING MAIL SERVER**. (The host name is smtp.qq.com and the password is the authorization code.)



Step 8 Click **Save**.



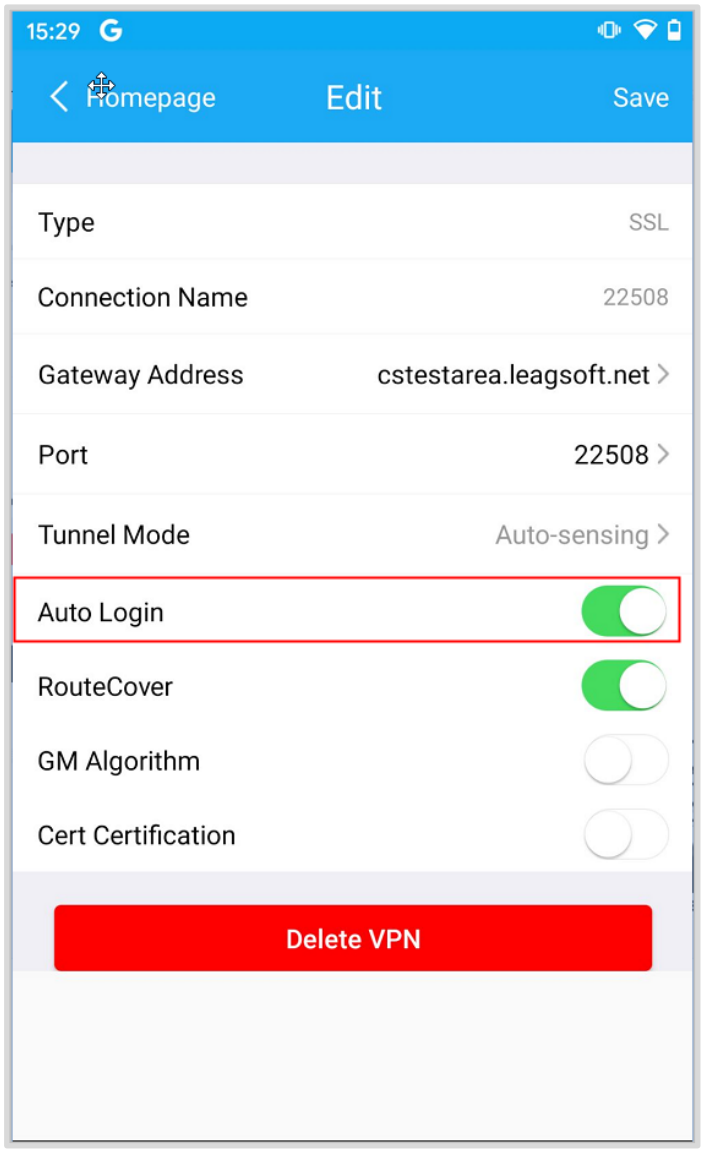
Step 9 After the configuration is successful, choose > **Feedback** on the login page of the UniVPN client to enable the feedback log function.

----End

1.7.3 How Do I Disable Automatic Login (Android)?

Step 1 Enable automatic login when the user password is entered for login, and the connection is successful.

Step 2 After disconnection, disable **Auto Login** in the **Edit** page of a connection. When you log in again, the automatic login is unavailable.



----End

1.7.4 What Can I Do If the iOS Client Freezes Abnormally?

If the iOS client is used for a long time or the version is too old, the client freezes abnormally. In this case, restart the client.