联软科技
LEAGSOFT

LeagSoft UniVPN

User Access Guide

Contents

1 Document Information 1

2 Getting Started 3

3 Installing the Software 5

3.1 Installation Precautions 6
3.2 Obtaining the Software Installation Package 7
3.3 Installing the Software in the Windows System 8
3.4 Installing the Software in the Linux System 10
3.5 Installing the Software on a Mac Operating System 13

4 Configuring a VPN Connection 14

4.1 Configuring an SSL VPN Connection 15
4.2 Configuring an L2TP VPN Connection 18
4.3 Configuring an L2TP over IPSec VPN Connection 21
4.4 Configuring a VPN Connection by Importing a Configuration File 26

5 Establishing a VPN Connection 29

5.1 Initiating a VPN Connection 30
5.2 User Identity Authentication 31
5.2.1 User Name/Password Authentication 31
5.2.2 Authentication by Importing the PKI Digital Certificate 32
5.2.3 USB Key Authentication 34
5.2.4 Two-Factor Authentication 35

6 Optional Configurations 37

6.1 Uninstalling the UniVPN 37
6.2 Version Detection and Upgrade 38
6.3 Changing the Login Password 39
6.4 Other Configurations 39

7 Troubleshooting 42

7.1 Collecting Information for Troubleshooting 42

7.1.1 Collecting Error Reports.....42
7.1.2 Exporting a Configuration File.....45
7.2 Installation and Upgrade Faults.....45
7.3 Connection Faults.....46
7.4 Service Faults.....47

8 Appendix.....49

8.1 Using Commands to Configure the Client in the Linux System.....49
8.1.1 Starting the Client.....49
8.1.2 Configuring an SSL VPN Connection.....50
8.1.3 Configuring an L2TP VPN Connection.....52
8.1.4 Configuring an L2TP over IPSec VPN Connection.....54
8.2 VPN Configuration and Connection Templates.....57
8.2.1 SSL VPN Configuration and Connection Template.....57
8.2.2 L2TP VPN Configuration and Connection Template.....58
8.2.3 L2TP over IPSec VPN Configuration and Connection Template.....60

1 Document Information

Product Version

This document applies to the UniVPN products of 10781.02.266.1230 and later versions.

Intended Audience

This document is intended for mobile device users who need to establish VPN connections through the UniVPN. You can complete the VPN connection configuration on your mobile device by referring to 2 Getting Started to access resources on your enterprise network.

Products and Versions

Product Name	Version	Operating System
USG6000	V500R005C20SPC500 and later version	• Windows • Linux
USG9500	V500R005C20SPC500 and later version	• Windows • Linux
USG6000E	V600R007C20SPC300 and later version (except SPC301/SPC302)	• Windows • Linux
Eudemon200E-N	V500R005C20SPC500 and later version	• Windows • Linux
Eudemon200E-G	V600R007C20SPC300 and later version (except SPC301/SPC302)	• Windows • Linux

Product Name	Version	Operating System
Eudemon1000E-N	V500R005C20SPC500 and later version	• Windows • Linux
Eudemon1000E-G	V600R007C20SPC300 and later version (except SPC301/SPC302)	• Windows • Linux
Eudemon8000E-X	V500R005C20SPC500 and later version	• Windows • Linux
SeMG9811	V500R005C20SPC500 and later version	• Windows • Linux
NGFW Module	V500R005C20SPC500 and later version	• Windows • Linux
USG12000	V600R021C10 and later version	• Windows • Linux
USG6000F	V600R021C10 and later version	• Windows • Linux
Eudemon9000E-X	V600R021C10 and later version	• Windows • Linux
Eudemon9000E-F	V600R021C10 and later version	• Windows • Linux
Eudemon1000E-F	V600R021C10 and later version	• Windows • Linux

Change History

Issue 01 (2021-12-30)

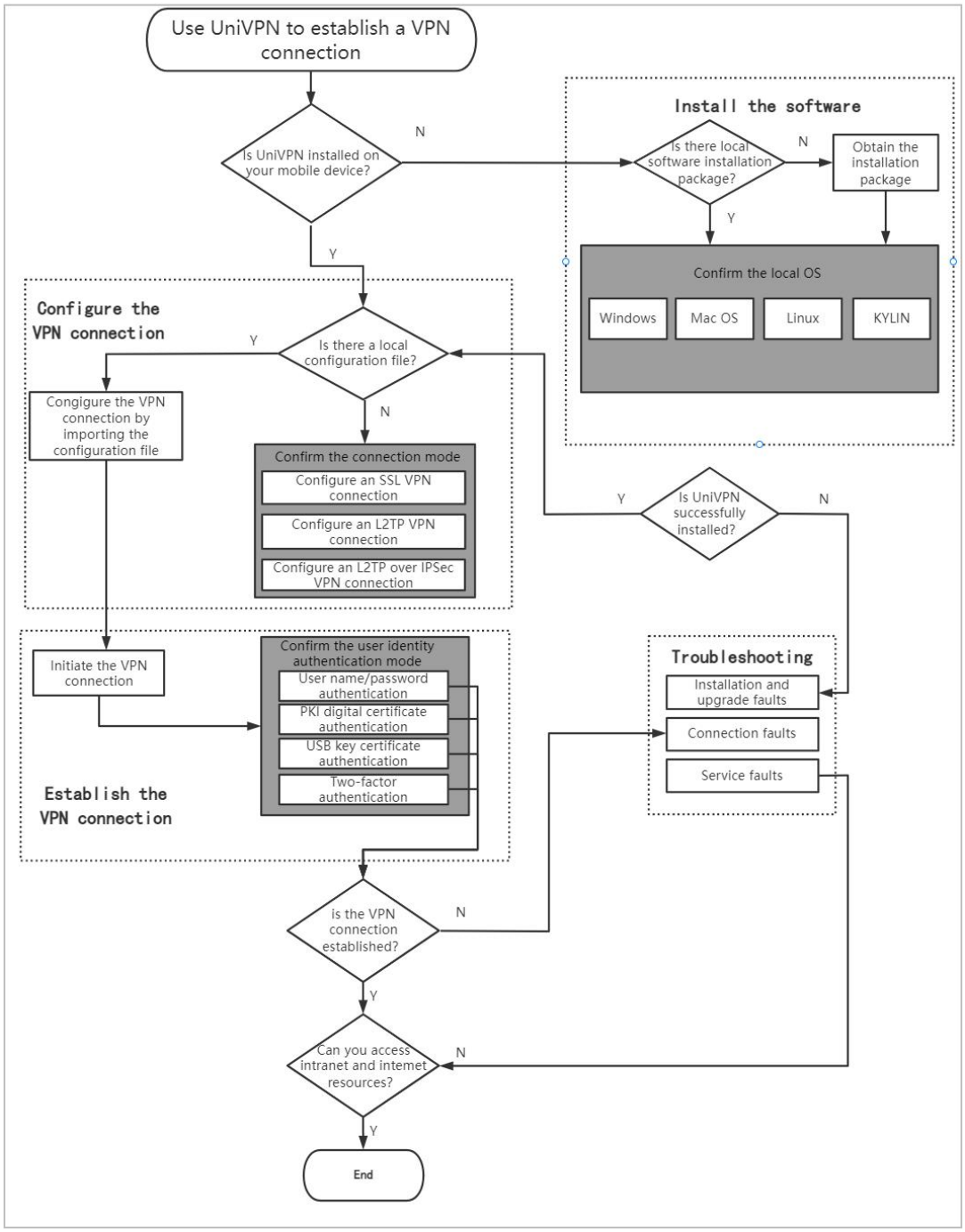
First official release, which matches UniVPN 10781.02.266.1230.

2 Getting Started

The UniVPN is VPN remote access client software provided by Shenzhen Leagsoft Technologies inc. It provides secure and convenient access services for mobile device users to remotely access resources on an enterprise network.

For users who use the software for the first time, refer to the task map in Figure 2-1 to complete the configuration operations required for establishing a VPN connection step by step.

Figure 2-1 Task map for mobile device users



3 Installing the Software

Before using the UniVPN to establish a VPN connection, ensure that the client software is completely and correctly installed on your mobile device. If the UniVPN has not been installed on your mobile device, do as follows to install it:

1. Before installing the software, read 3.1 Installation Precautions to understand the precautions and system configuration requirements for software installation.
2. If your mobile device does not have the UniVPN software installation package for the corresponding OS or the version of the installation package does not meet the requirement, obtain the software installation package by referring to 3.2 Obtaining the Software Installation Package.
3. Currently, the UniVPN supports two types of OSs (Windows and Linux), and different UniVPN software installation packages are provided for them. If you have obtained the software installation package that matches the OS of your mobile device, install the software by referring to the following steps:
   - **3.3** Installing the Software in the Windows System
   - **3.4** Installing the Software in the Linux System
   - **3.5** Installing the Software on a Mac Operating System

3.1 Installation Precautions

Before installing and using the UniVPN, read the following content carefully to understand the precautions for software installation and ensure that the system configuration of your mobile device meets the requirements.

3.2 Obtaining the Software Installation Package

This section describes how to obtain the UniVPN client software installation package. In an actual task scenario, the enterprise network administrator is responsible for planning and deploying the software installation package and informing mobile device users.

3.3 Installing the Software in the Windows System

The UniVPN provides separate software installation packages for 32-bit and 64-bit Windows OSs. Select the correct installation package based on the OS environment of your mobile device.

3.4 Installing the Software in the Linux System

The UniVPN client supports only 64-bit Ubuntu 20.04.operating systems.

3.5 Installing the Software on a Mac Operating System_ZH-CN_TOPIC_0181901712

The UniVPN client supports only 64-bit Mac operating systems.

3.1 Installation Precautions

Before installing and using the UniVPN, read the following content carefully to understand the precautions for software installation and ensure that the system configuration of your mobile device meets the requirements.

Precautions

- When installing or uninstalling the software, use the user name and password with the administrator permission to log in to the OS.
- Do not install or use multiple VPN dial-up software programs on one mobile device. Otherwise, the VPN dial-up software or OS may not work properly.
- If the UniVPN already exists on your mobile device, a message is displayed during installation to prompt you to uninstall the UniVPN. You can delete the installed client software of the earlier version as prompted and run the installation program again to install the client software of the new version on your hard disk.

System Configuration Requirements

Table 3-1 System Configuration Requirements of the UniVPN

System Configuration	Requirement		
OS	Windows	Linux	Mac OS
OS version	• Windows 7 (32-bit/64-bit) • Windows 8 (32-bit/64-bit) • Windows 8.1 (32-bit/64-bit) • Windows 10 (32-bit/64-bit) • Windows Server 2008 (32-bit/64-bit) • Windows Server 2012 (64-bit)	• Ubuntu-20.04 (64-bit)	• OS X 10.11.x (64-bit) • OS X 10.12.x (64-bit) • OS X 10.13.x (64-bit) • OS X 10.14.x (64-bit) • OS X 10.15.x (64-bit) • OS X 11.x.x (64-bit) • OS X 12.x.x (64-bit)
Hardware resources	The UniVPN has no special requirements for software and hardware resources such as memory, hard disk, and CPU resources of the OS.		

3.2 Obtaining the Software Installation Package

This section describes how to obtain the UniVPN client software installation package. In an actual task scenario, the enterprise network administrator is responsible for planning and deploying the software installation package and informing mobile device users.

Before You Start

Before obtaining the software installation package, ensure that the OS environment and version of your mobile device comply with the system configuration requirements described in **3.1** Installation Precautions and obtain the software installation package that matches your OS environment.

Common Methods for Obtaining the Software Installation Package

- Obtain the software installation package from the administrator of your enterprise network and upload it to your mobile device.
- You can also log in to https://www.leagsoft.com/?u=/doc/article/103197.html .Click the link at the bottom of the UniVPN introduction page to download the software installation package of the required version.

NOTE

Because there are multiple SSL VPN user authentication modes, the obtained user login information and operations vary. Confirm the user authentication mode with your enterprise network administrator.

- Local authentication and server authentication: Obtain the user name and password.
- Certificate-anonymous authentication: Obtain and install the client certificate.
- Certificate-challenge authentication: Obtain the client certificate and password and install the client certificate.

Follow-Up Procedure

Currently, the UniVPN supports only three types of OSs (Windows, Linux, and Mac), and different UniVPN software installation packages are provided for them. If you have obtained the software installation package that matches the OS of your mobile device, install the software by referring to the following steps:

- **3.3** Installing the Software in the Windows System
- **3.4** Installing the Software in the Linux System
- **3.5** Installing the Software on a Mac Operating System

You can also go back to **2** Getting Started and perform subsequent configurations by referring to the task map.

3.3 Installing the Software in the Windows System

The UniVPN provides separate software installation packages for 32-bit and 64-bit Windows OSs. Select the correct installation package based on the OS environment of your mobile device.

Before You Start

Before installing the software, ensure that the OS environment and version of your mobile device comply with the system configuration requirements described in **3.1** Installation Precautions.

Procedure

Step 1 Log in to the OS using an account that has the administrator permission.

Step 2 Double-click the downloaded installation package. The installation wizard is displayed.

Step 3 The installation wizard prompts you to complete the installation task step by step.

NOTE

- By default, the UniVPN is installed in the system disk. For example, if the system is installed in drive C, the default installation path of the UniVPN is **C:\Program Files (x86)\UniVPN**.
- When you install the UniVPN client for the first time, a message is displayed, prompting you to install the network adapter driver. Follow the installation wizard to complete the installation.

----End

Follow-Up Procedure

- After installing the UniVPN, you can start **3.5** Installing the Software on a Mac Operating System

The UniVPN client supports only 64-bit Mac operating systems.

Before You Start

Before installing the software, ensure that the OS environment and version of your device comply with the system configuration requirements described in 3.1 "Installation Precautions."

Procedure

Step 1 Log in to the Mac operating system.

Step 2 Double-click the downloaded installation package to run the installation program.

Step 3 Complete the installation as prompted by the installation program.

Step 4 After the installation is complete, you can find the application in the application folder.

Step 5 Double-click **UniVPN** to start the program.

----End

Follow-up Procedure

- After installing the UniVPN, you can start 4 Configuring a VPN Connection.
- If an error occurs during the installation, rectify the fault by referring to 7.2 Installation and Upgrade Faults.
- You can go back to 2 Getting Started and perform subsequent configurations by referring to the task map.

- Configuring a VPN Connection.
- If an error occurs during the installation, rectify the fault by referring to **7.2** Installation and Upgrade Faults.
- You can also go back to **2** Getting Started and perform subsequent configurations by referring to the task map.

3.4 Installing the Software in the Linux System

A UniVPN installation package is available for the 64-bit Ubuntu 20.04 Linux operating system. Select the correct installation package based on your OS.

Before You Start

Before installing the software, ensure that the OS environment and version of your mobile device comply with the system configuration requirements described in **3.1** Installation Precautions.

Procedure

The following uses the Ubuntu 20.04 operating system as an example.

Step 1 Log in to the Linux system using an account that has the root permission.

Step 2 Save the downloaded installation package to the main folder (**root** > **home** > **UniVPN**).

Step 3 Start the **Terminal**. In the **home/UniVPN** directory, run the **./***installation package name***.run** command as the root user to install the UniVPN.

```
root@UniVPN-virtual-machine:~# cd /home/UniVPN/
root@uniVPN-virtual-machine:/home/UniVPN# ./UniVPN-xxxxx.xx.xxx.xxxx.run
/
install.sh
uninstall.sh
sysconfig.ini
qt.conf
bak/
component/
config/
driver/
image/
image/Customized/
image/Customized/customized.ini
image/UniVPN.desktop
image/UniVPNA.desktop
image/ICON.ico
language/
language/2052/
language/2052/l_UILabel.ini
```

Step 4 If the installation succeeds, the following information is displayed.

```
Starting UniVPNPromoteService daemon: UniVPNPromoteService.
*****The program has been installed in directory UniVPN of your home Directory!*****
*****Enjoy!*****
```

Step 5 Click the UniVPN icon on the desktop to start the program.

----End

Follow-Up Procedure

- After installing the UniVPN, you can start **3.5** Installing the Software on a Mac Operating System

The UniVPN client supports only 64-bit Mac operating systems.

Before You Start

Before installing the software, ensure that the OS environment and version of your device comply with the system configuration requirements described in 3.1 "Installation Precautions."

Procedure

Step 1 Log in to the Mac operating system.

Step 2 Double-click the downloaded installation package to run the installation program.

Step 3 Complete the installation as prompted by the installation program.

Step 4 After the installation is complete, you can find the application in the application folder.

Step 5 Double-click **UniVPN** to start the program.

----End

Follow-up Procedure

- After installing the UniVPN, you can start 4 Configuring a VPN Connection.
- If an error occurs during the installation, rectify the fault by referring to 7.2 Installation and Upgrade Faults.
- You can go back to 2 Getting Started and perform subsequent configurations by referring to the task map.

- Configuring a VPN Connection.
- If an error occurs during the installation, rectify the fault by referring to **7.2** Installation and Upgrade Faults.
- You can also go back to **2** Getting Started and perform subsequent configurations by referring to the task map.

3.5 Installing the Software on a Mac Operating System

The UniVPN client supports only 64-bit Mac operating systems.

Before You Start

Before installing the software, ensure that the OS environment and version of your device comply with the system configuration requirements described in 3.1 "Installation Precautions."

Procedure

Step 1 Log in to the Mac operating system.

Step 2 Double-click the downloaded installation package to run the installation program.

Step 3 Complete the installation as prompted by the installation program.

Step 4 After the installation is complete, you can find the application in the application folder.

Step 5 Double-click **UniVPN** to start the program.

----End

Follow-up Procedure

- After installing the UniVPN, you can start 4 Configuring a VPN Connection.
- If an error occurs during the installation, rectify the fault by referring to 7.2 Installation and Upgrade Faults.
- You can go back to 2 Getting Started and perform subsequent configurations by referring to the task map.

4 Configuring a VPN Connection

The UniVPN supports two VPN connection configuration modes: manual mode and configuration file mode.

The configuration mode depends on whether your enterprise network administrator provides the VPN connection configuration file.

- If the administrator has provided the configuration file, you can directly import the configuration file to configure the VPN connection. For details, see **4.4** Configuring a VPN Connection by Importing a Configuration File.
- If you do not have the configuration file, you can **manually** configure a VPN connection on the UniVPN.

  When you manually configure a VPN connection, the connection parameters to be configured vary according to the type of the VPN to be connected. Therefore, you need to confirm the type of the VPN to be connected with your enterprise network administrator and obtain necessary connection parameters.

  After specifying the type of the VPN to be connected and obtaining necessary connection parameters, configure the VPN connection by referring to the following sections:
  - **4.1** Configuring an SSL VPN Connection
  - **4.2** Configuring an L2TP VPN Connection
  - **4.3** Configuring an L2TP over IPSec VPN Connection

The methods for configuring VPN connections using the UniVPN on the Windows and Linux operating systems are basically the same. The following uses the Windows operating system as an example.

4.1 Configuring an SSL VPN Connection

If you have confirmed with your enterprise network administrator that the type of the VPN to be connected is SSL VPN, perform the steps in this section to configure the VPN connection.

4.2 Configuring an L2TP VPN Connection

If you have confirmed with your enterprise network administrator that the type of the VPN to be connected is L2TP VPN, perform the following steps to configure the VPN connection.

4.3 Configuring an L2TP over IPSec VPN Connection

If you have confirmed with your enterprise network administrator that the type of the VPN to be connected is L2TP over IPSec VPN, perform the following steps to configure the VPN connection.

4.4 Configuring a VPN Connection by Importing a Configuration File

The configuration file is an .ini file generated by your enterprise network administrator using the configuration file export function of the UniVPN. The file contains all parameters required for creating a specific VPN connection. After obtaining the configuration file, you can import the configuration file to the UniVPN client to generate the configured VPN connection. This simplifies your configuration.

4.1 Configuring an SSL VPN Connection

If you have confirmed with your enterprise network administrator that the type of the VPN to be connected is SSL VPN, perform the steps in this section to configure the VPN connection.

Before You Start

Before the configuration, check the following table to ensure that you have obtained the connection parameters required for setting up an SSL VPN connection.

NOTE

You can also use the configuration and connection templates in **8** Appendix to check whether the obtained connection parameters are complete.

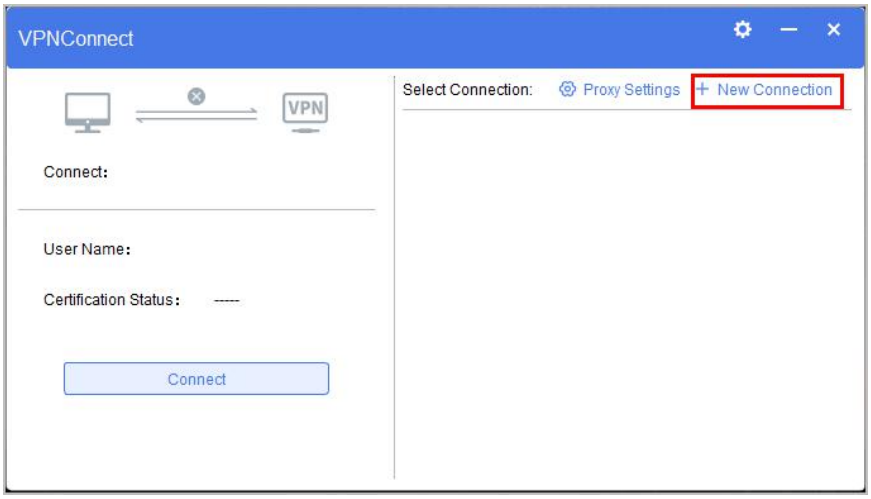
Table 4-1 SSL VPN connection parameters

Check Item		Remarks
Are Proxy Settings needed?	No	If you do not use any proxy server when accessing the Internet, Proxy Settings are unnecessary.
	Yes (Use the system proxy)	There are three proxy server scenarios. After selecting a proxy type, enter the address, port number, account, and password. You can obtain this information from your enterprise network administrator.
	Yes (Use Http/Https proxy)	
	Yes (Use the Socks5 proxy)	
Connection name		Identifies an SSL VPN connection. You can set it as required.
Description		Indicates information about the connection, such as the creator, creation time, and connection purpose. You can set the information as required.
Remote gateway		Specifies the IP address of an SSL VPN virtual gateway. Obtain this value from your enterprise network administrator.

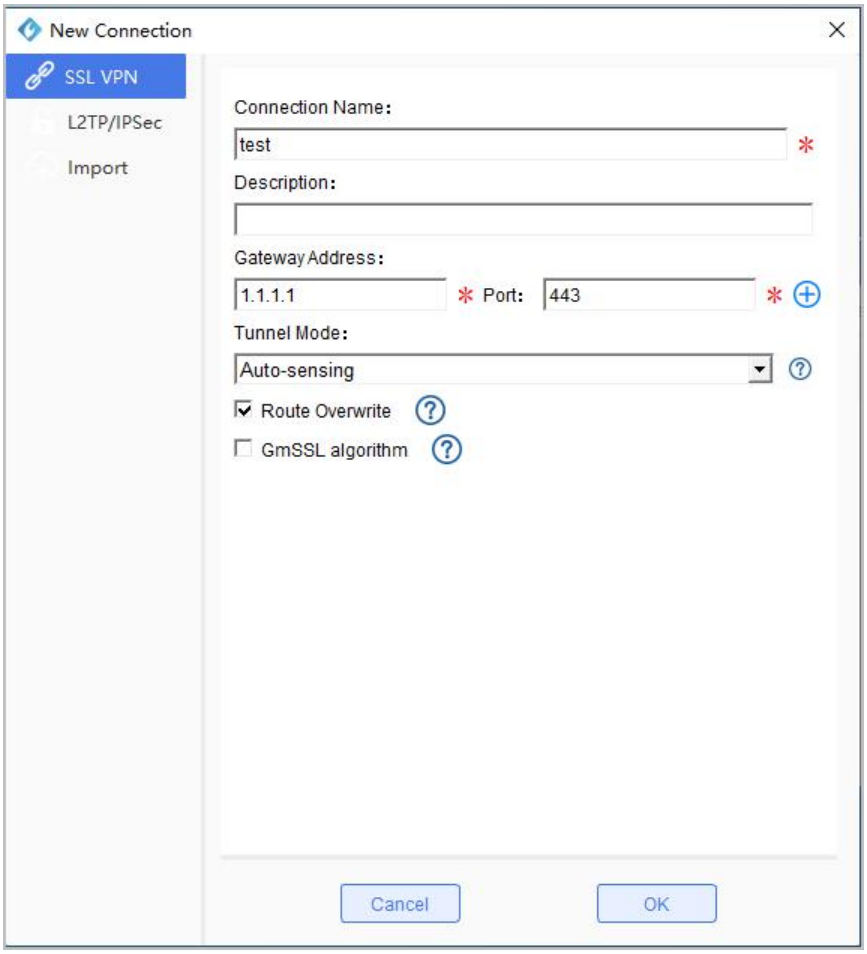
Check Item		Remarks
Port		Specifies the port number used to establish an SSL VPN tunnel. Obtain this value from your enterprise network administrator.
Tunnel mode	Reliable Transmission	• Confirm the mode with your enterprise network administrator. • The reliable transmission mode is recommended when the network environment is unstable. If the network environment is stable, you are advised to use the quick transmission mode to improve data transmission efficiency. If you do not know the network environment condition, select the auto-sensing mode.
	Quick Transmission	
	Auto-sensing	
Route coverage		When the route delivered by the peer gateway is the same as the address prefix and subnet mask of the existing local route, if the route coverage function is enabled, the route delivered by the peer gateway overwrites the existing route. This prevents network access exceptions caused by local route conflicts. By default, route coverage function is enabled.
National Secret Algorithm		The client supports to use the national secret algorithm to establish an SSL VPN connection with the peer gateway. By default, the national secret algorithm function is disabled. After **National Secret Algorithm** is selected, the cipher suite of the peer gateway is automatically switched to ECC-SM4-SM3.
Certificate Authentication **NOTE** This item is displayed only in the Linux operating system.		If you use certificate authentication to establish an SSL VPN connection, select **Certificate Authentication**. After **Certificate Authentication** is selected, you can select a certificate for certificate authentication.
Password **NOTE** This item is displayed only in the Linux operating system.		This parameter specifies the login password corresponding to the user name extracted from the certificate during certificate authentication. This password can be set only when an SSL VPN connection is set up using certificate authentication and **Certificate Authentication** is selected.

Procedure

Step 1 On the main page of the UniVPN client, click **+ New Connection** next to **Select the VPN connection** to create a connection.



Step 2 In the **New connection** dialog box, select **SSL VPN** from the left navigation tree and set connection parameter values.



Step 3 After the configurations are complete, click **OK** to return to the main interface of the UniVPN. You can see that a VPN connection has been created successfully.

----End

Follow-Up Procedure

- After the preceding configurations are complete, you can try **5** Establishing a VPN Connection.
- You can also go back to **2** Getting Started and perform subsequent configurations by referring to the **task map**.

4.2 Configuring an L2TP VPN Connection

If you have confirmed with your enterprise network administrator that the type of the VPN to be connected is L2TP VPN, perform the following steps to configure the VPN connection.

Before You Start

Before the configuration, check the following table to ensure that you have obtained the connection parameters required for setting up the L2TP VPN connection.

NOTE

You can also use the configuration and connection templates in **8** Appendix to check whether the obtained connection parameters are complete.

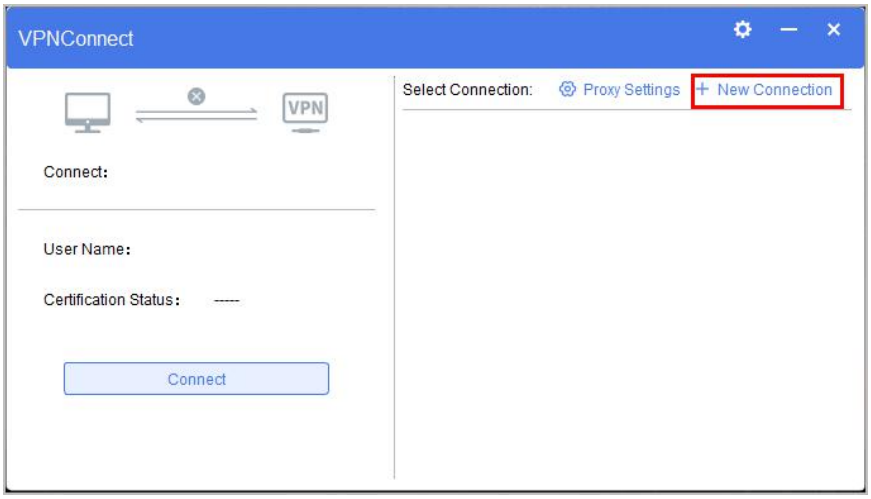
Table 4-2 L2TP VPN connection parameters

Check Item	Remarks
Proxy Settings	
Are Proxy Settings needed?	**NOTE** L2TP VPN tunnels do not support the proxy function.
L2TP Configuration	
Connection name	Identifies an L2TP VPN connection. You can set it as required.
Description	Indicates information about the connection, such as the creator, creation time, and connection purpose. You can set the information as required.
LNS server address	Specifies the IP address of an L2TP VPN gateway. Obtain this value from your enterprise network administrator.
Tunnel Configuration	
Tunnel name	Identifies a device in the tunnel. Obtain this

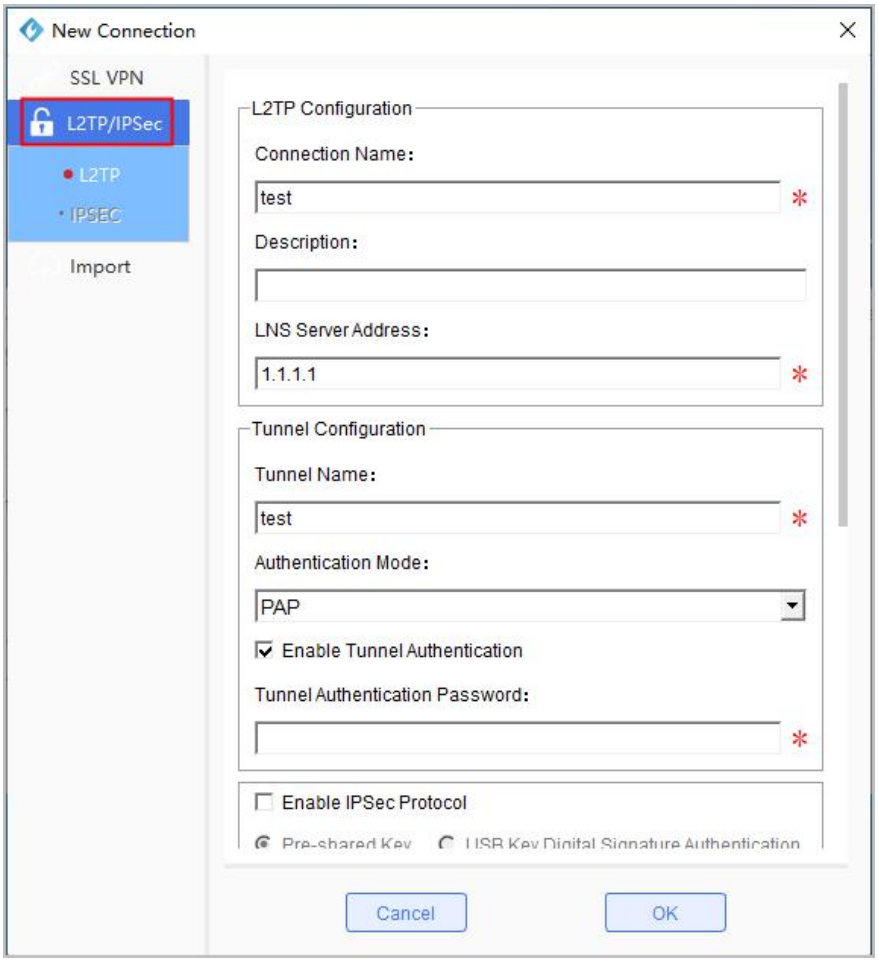
Check Item		Remarks
		value from your enterprise network administrator.
Authentication Mode	CHAP	Confirm the mode with your enterprise network administrator.
	PAP	
Enable tunnel validation	Deselected	• Confirm this option with your enterprise network administrator. • If **Enable tunnel validation** is selected, you need to enter the tunnel authentication password. Obtain the password from your enterprise network administrator.
	Selected	
Route Settings		• Confirm the settings with your enterprise network administrator. • Select **made config** to access all network resources. • There are three configuration options: – Deselect **Allow Internet access after connection**. You can access intranet resources but cannot access the Internet. – Select **Allow Internet access after connection**, but no IP address is added to the IP address list. You can access the intranet resources that are on the same network segment as the intranet address allocated by the peer gateway, the Internet, and LAN. – Select **Allow Internet access after connection** and add IP addresses to the IP address list. You can access the enterprise intranet resources set in the IP address list, intranet resources in the same network segment as the intranet IP address allocated by the peer gateway, the Internet, and LAN. Obtain the IP addresses to be added to the IP address list from your enterprise network administrator.

Procedure

Step 1 On the main page of the UniVPN client, click **+ New Connection** next to **Select the VPN connection** to create a connection.



Step 2 In the **New connection** dialog box, select **L2TP/IPSec** from the left navigation tree and set connection parameter values.



Step 3 After the settings are complete, click **OK** to return to the main interface of the UniVPN. You can see that a VPN connection has been created successfully.

----End

Follow-Up Procedure

- After the preceding configurations are complete, you can try **5** Establishing a VPN Connection.
- You can also go back to **2** Getting Started and perform subsequent configurations by referring to the **task map**.

4.3 Configuring an L2TP over IPSec VPN Connection

If you have confirmed with your enterprise network administrator that the type of the VPN to be connected is L2TP over IPSec VPN, perform the following steps to configure the VPN connection.

Before You Start

Before the configuration, check the following table to ensure that you have obtained the connection parameters required for setting up the L2TP over IPSec VPN connection.

NOTE

You can also use the configuration and connection templates in **8** Appendix to check whether the obtained connection parameters are complete.

Table 4-3 L2TP over IPSec VPN connection parameters

Check Item		Remarks
Proxy Settings		
Are Proxy Settings needed?	No	If you do not use any proxy server when accessing the Internet, Proxy Settings are unnecessary.
	Yes (Use the Socks5 proxy) **NOTE** L2TP over IPSec VPN tunnels support only the Socks5 proxy.	After selecting the **Use the Socks5 proxy**, enter the address, port number, account, and password. You can obtain this information from your enterprise network administrator.
L2TP Configuration		
Connection name		Identifies an L2TP over IPSec VPN connection. You can set it as required.
Description		Indicates information about the connection, such as the creator, creation time, and connection purpose. You can set the information as required.

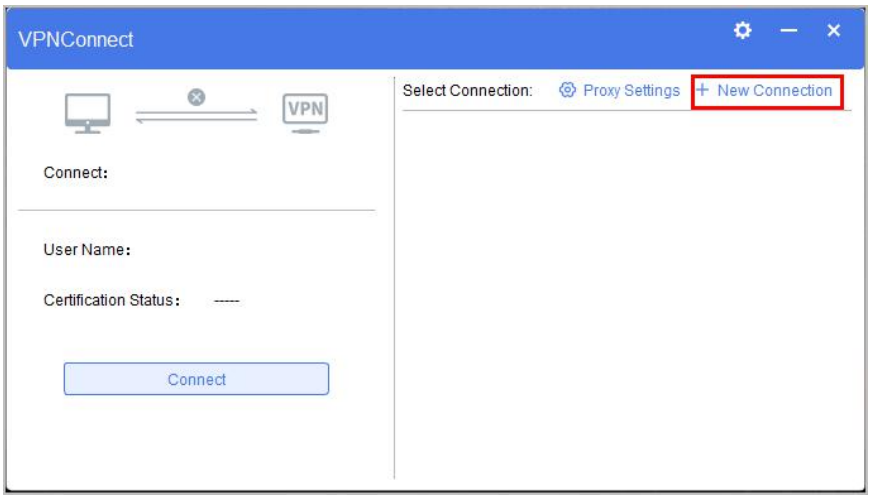
Check Item		Remarks
LNS server address		Specifies the IP address of an L2TP VPN gateway. Obtain this value from your enterprise network administrator.
Tunnel Configuration		
Tunnel name		Identifies a device in the tunnel. Obtain this value from your enterprise network administrator.
Authentication Mode	CHAP	Confirm the mode with your enterprise network administrator.
	PAP	
Enable tunnel validation	Deselected	• Confirm the settings with your enterprise network administrator. • If **Enable tunnel validation** is selected, you need to enter the tunnel authentication password. Obtain the password from your enterprise network administrator.
	Selected	
Enable tunnel validation		This option is mandatory for L2TP over IPSec VPN connections.
IPSec Identity Authentication Mode	Preset shared key	If you select this mode, the pre-shared key is required. Obtain this value from your enterprise network administrator.
	USB key digital signature authentication **NOTE** This option is supported only in the Windows OS.	If you select this mode, the USB PIN code is required. Obtain this value from your enterprise network administrator.
IPSec Configuration		
IPSec server address		• Specifies the IP address of an IPSec VPN gateway. Obtain this value from your enterprise network administrator. • If the L2TP VPN gateway and IPSec VPN gateway are the same, select **Using LNS server**.
Encapsulation Mode	Tunnel mode	Confirm the mode with your enterprise network administrator.
	Transmission mode	
ESP protocol verification algorithm		The value can be MD5, SHA1, or SHA2-256. Confirm the algorithm with your enterprise network administrator.
ESP protocol encryption algorithm		The value can be DES, 3DES, AES-128, AES-192, or AES-256. Confirm the

Check Item		Remarks
		algorithm with your enterprise network administrator.
IKE Basic Configuration		
Negotiation Mode	Main mode	Confirm the mode with your enterprise network administrator.
	Aggressive mode	
ID Type		• Indicates the identity authentication type for IKE negotiation. The ID can be an IP address or name. • Confirm the type with your enterprise network administrator.
Local name		• This parameter is mandatory when **ID Type** is set to **Name**. • Confirm the names with your enterprise network administrator.
Security gateway Name		
Validation algorithm		The value can be MD5, SHA1, or SHA2-256. Confirm the algorithm with your enterprise network administrator.
Encryption algorithm		The value can be DES-CBC, 3DES-CBC, or AES-128/192/256. Confirm the algorithm with your enterprise network administrator.
DH group mark		The value can be Group1, Group2, or Group5. Confirm the algorithm with your enterprise network administrator.
IKE Advanced Configuration		
Enable PFS feature		• Indicates that the Perfect Forward Secrecy (PFS) function is used during IKE negotiation. • After this function is enabled, you need to set security parameters, including Group1, Group2, and Group5. • Confirm the configuration with your enterprise network administrator.
Security alliance life cycle		• Specifies an interval at which the IKE SA is updated, which reduces the risk of IKE SA cracking and improves security. • Confirm the value with your enterprise network administrator.
IPSec Advanced Configuration		
Security alliance life cycle		• Specifies an interval at which the IPSec SA is updated, which reduces the risk

Check Item		Remarks
		of IPSec SA cracking and improves security. • Confirm the value with your enterprise network administrator.
Route Settings	Mode Config	After the **Mode Config** parameter is set, the actual effect depends on whether the peer gateway supports **Mode Config** (also called the tunnel separation mode). • If the peer gateway supports and is configured with the **Mode Config** mode: You can access intranet resources, the Internet, and LAN. • If the peer gateway does not support the **Mode Config** mode or the **Mode Config** mode is not configured: You can access intranet resources but cannot access the Internet or LAN. Confirm the configuration with your enterprise network administrator.
	Allow Internet access after connection	You can use either of the following methods to set the parameters for accessing the Internet after the connection is set up: • Select **Allow Internet access after connection**, but no IP address is added to the IP address list: You can access the intranet resources that are on the same network segment as the intranet address allocated by the peer gateway, the Internet, and LAN. • Select **Allow Internet access after connection** and add IP addresses to the IP address list: You can access the enterprise intranet resources set in the IP address list, intranet resources in the same network segment as the intranet IP address allocated by the peer gateway, the Internet, and LAN. Obtain the IP addresses to be added to the IP address list from your enterprise network administrator. Confirm the configuration with your enterprise network administrator.

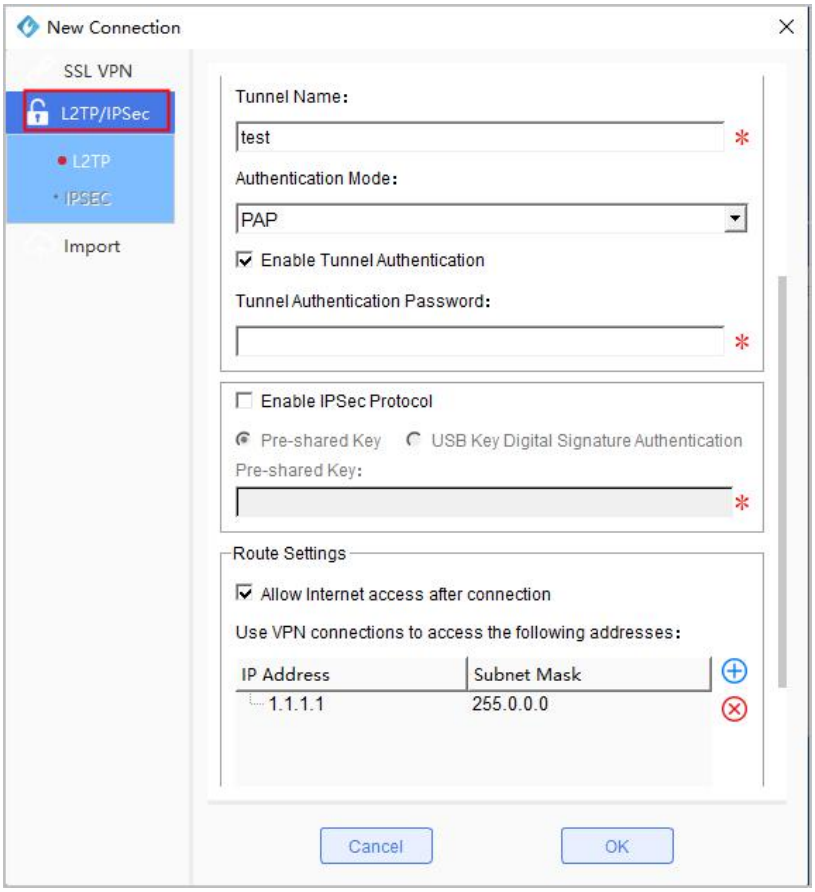
Procedure

Step 1 On the main page of the UniVPN client, click + **New Connection** next to **Select the VPN connection** to create a connection.

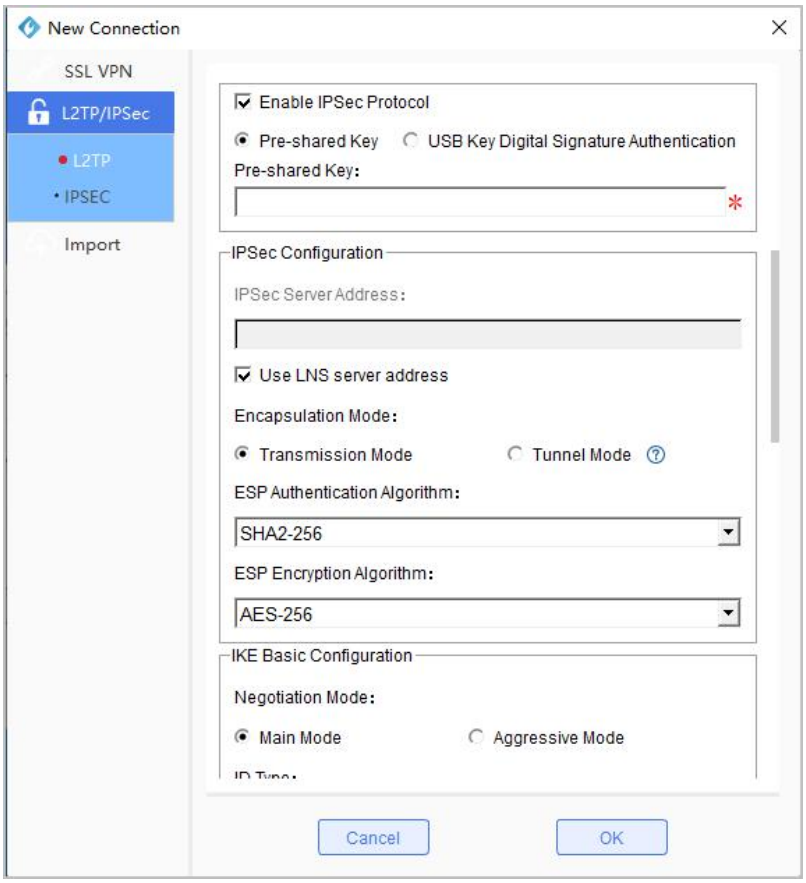


Step 2 In the **New connection** dialog box, select **L2TP/IPSec** from the left navigation tree and set connection parameter values.

1. Set L2TP parameters.



2. Set IPSec parameters.



Step 3 After the settings are complete, click **OK** to return to the main interface of the UniVPN. You can see that a VPN connection has been created successfully.

----End

Follow-Up Procedure

- After the preceding configurations are complete, you can try **5** Establishing a VPN Connection.
- You can also go back to **2** Getting Started and perform subsequent configurations by referring to the **task map**.

4.4 Configuring a VPN Connection by Importing a Configuration File

The configuration file is an .ini file generated by your enterprise network administrator using the configuration file export function of the UniVPN. The file contains all parameters required for creating a specific VPN connection. After obtaining the configuration file, you

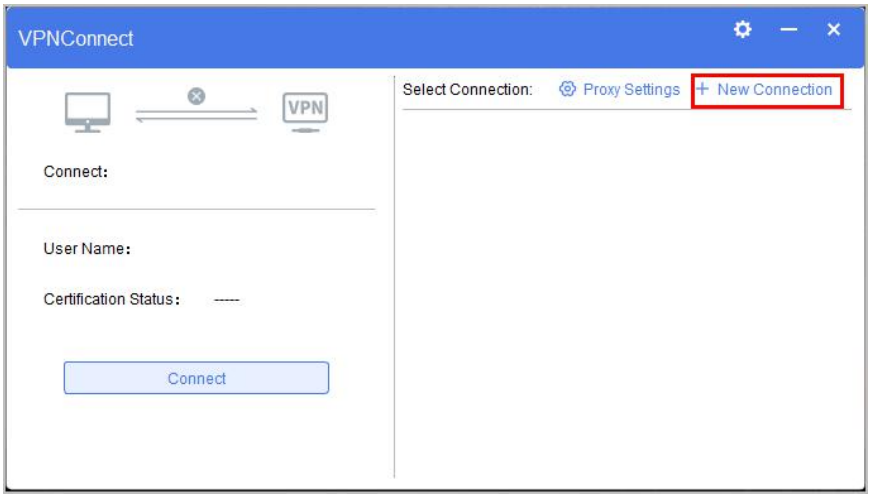
can import the configuration file to the UniVPN client to generate the configured VPN connection. This simplifies your configuration.

Before You Start

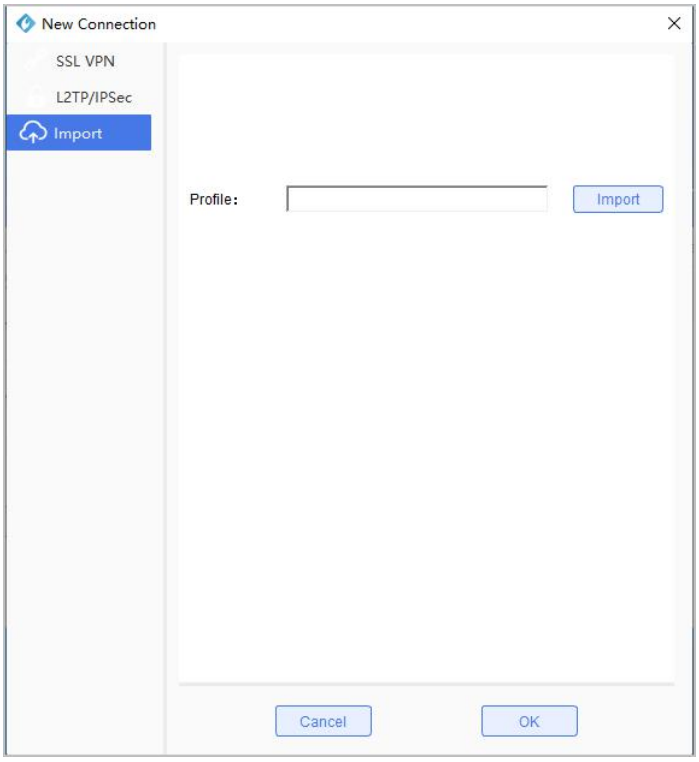
Confirm with your enterprise network administrator about the integrity and accuracy of the configuration file. If some content in the configuration file is missing or incorrect, the VPN connection cannot be set up.

Procedure

Step 1 On the main page of the UniVPN client, click + **New Connection** next to **Select the VPN connection** to create a connection.



Step 2 In the **New connection** dialog box, select **Load Config** from the left navigation tree.



Step 3 Click **Import** in the right pane, select the prepared configuration file, and click **Open**.

Step 4 Click **OK** to return to the main interface of the UniVPN. You can see that a VPN connection has been created successfully.

----End

Follow-Up Procedure

- After the preceding configurations are complete, you can try **5** Establishing a VPN Connection.
- You can also go back to **2** Getting Started and perform subsequent configurations by referring to the **task map**.

5 Establishing a VPN Connection

After a VPN connection is configured, the connection name is displayed in the **Connection** drop-down list on the main page of the UniVPN.

1. You can select the connection name and try **5.1** Initiating a VPN Connection.
2. After a VPN tunnel is established, the peer gateway needs to authenticate your identity. For details, see **5.2** User Identity Authentication. After authentication succeeds, your mobile device will obtain an intranet address. Then, you can securely access intranet resources through the device.

   Currently, the UniVPN supports the following user identity authentication modes. The authentication mode that you can use depends on the configuration on the peer gateway.

   - **5.2.1** User Name/Password Authentication
   - **5.2.2** Authentication by Importing the PKI Digital Certificate
   - **5.2.3** USB Key Authentication
   - **5.2.4** Two-Factor Authentication

   Before establishing a VPN connection, confirm the identity authentication mode with your enterprise network administrator and obtain necessary authentication information such as the user name, password, and certificate from the administrator.

The methods for establishing VPN connections using the UniVPN on the Windows and Linux operating systems are basically the same. The following uses the Windows operating system as an example.

5.1 Initiating a VPN Connection

After the VPN connection is configured, you can initiate a VPN connection and establish a VPN tunnel.

5.2 User Identity Authentication

After you initiate a VPN connection request through the UniVPN, the peer gateway returns a user identity authentication request. After authentication succeeds, your mobile device will obtain an intranet address. Then, you can securely access intranet resources through the device.

5.1 Initiating a VPN Connection

After the VPN connection is configured, you can initiate a VPN connection and establish a VPN tunnel.

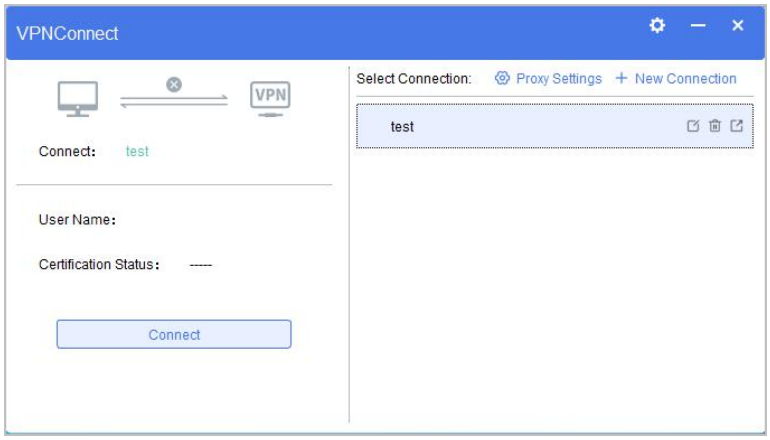
Before You Start

- Before initiating a VPN connection, ensure that the parameter settings in the VPN connection configuration are complete and correct.
- If you configure a VPN connection by importing a configuration file, access the configuration modification page and check that every mandatory item has been set.

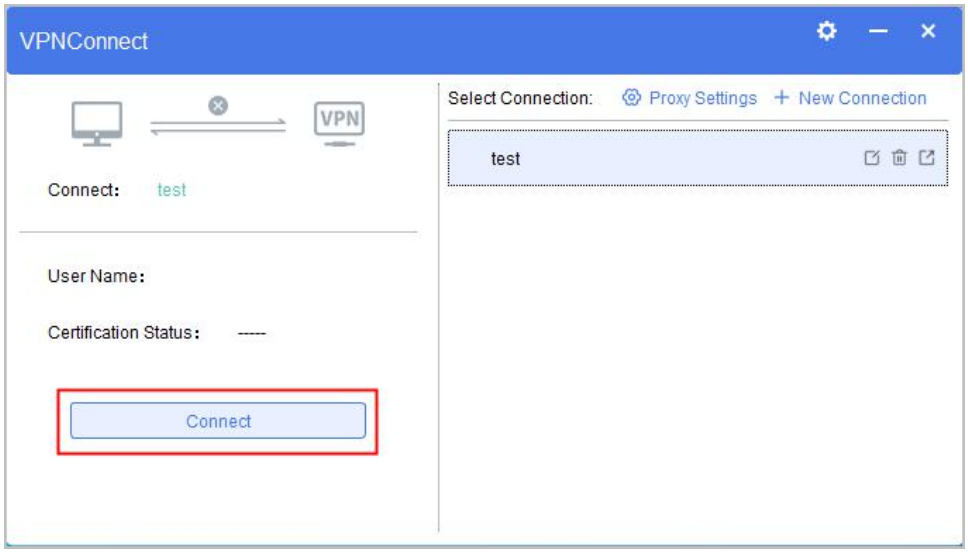
Procedure

Step 1 On the main page of the UniVPN client, select the configured VPN connection under **Select the VPN connection**.

Step 2 Double-click the connection to initiate a VPN connection request.



Alternatively, select the VPN connection and click **connect** in the upper right corner of the page.



----End

Follow-Up Procedure

- After a VPN tunnel is established, the peer gateway needs to authenticate your identity. For details, see **5.2** User Identity Authentication. After authentication succeeds, your mobile device will obtain an intranet address. Then, you can securely access intranet resources through the device.
- If an error occurs during the connection, rectify the fault by referring to **7.3** Connection Faults.
- You can also go back to **2** Getting Started and perform subsequent configurations by referring to the **task map**.

5.2 User Identity Authentication

After you initiate a VPN connection request through the UniVPN, the peer gateway returns a user identity authentication request. After authentication succeeds, your mobile device will obtain an intranet address. Then, you can securely access intranet resources through the device.

Currently, the UniVPN supports four user identity authentication modes. The authentication modes require different authentication information. You need to confirm the identity authentication mode with your enterprise network administrator and obtain necessary authentication information such as the user name, password, and certificate from the administrator.

If you have specified the identity authentication mode to be used and obtained the corresponding authentication information, perform the following operations to authenticate the user identity:

- **5.2.1** User Name/Password Authentication
- **5.2.2** Authentication by Importing the PKI Digital Certificate
- **5.2.3** USB Key Authentication
- **5.2.4** Two-Factor Authentication

5.2.1 User Name/Password Authentication

User name/password authentication is the most commonly used authentication mode.

Before You Start

Obtain the following information required for user name/password authentication from your enterprise network administrator:

1. Valid user name
2. Password corresponding to the user name

NOTE

You can also use the configuration and connection templates in **8** Appendix to check whether the obtained authentication information is complete.

The following table lists the support for user name/password authentication in different OSs and VPN types.

Table 5-1 Support for user name/password authentication

VPN Type/OS	Windows	Linux	Mac OS
SSL VPN	Y	Y	Y
L2TP VPN	Y	Y	Y
L2TP over IPSec VPN	Y	Y	Y

Procedure

Step 1 Initiate a VPN connection request. The user name/password authentication page is displayed.

Step 2 Enter the user name and password, and click **Login**.

Step 3 If the authentication succeeds, the device successfully connects to the intranet. The message "**Connect successful**" is displayed.

----End

Follow-Up Procedure

- If you need to perform two-factor authentication, see **5.2.4** Two-Factor Authentication.
- If the authentication or VPN connection fails, rectify the fault by referring to **7.3** Connection Faults.
- If your device successfully connects to the intranet, you can try to access resources in the intranet. If the resources cannot be accessed, rectify the fault by referring to **7.4** Service Faults.
- Alternatively, you can return to **2** Getting Started to view other content on the **task map**.

5.2.2 Authentication by Importing the PKI Digital Certificate

You can install the PKI digital certificate provided by your enterprise network administrator to your mobile device and log in to the VPN gateway through certificate authentication. In SSL VPN scenarios, PKI digital certificate-anonymous authentication and PKI digital certificate-challenge authentication are supported.

Before You Start

Obtain the following information required for PKI digital certificate authentication from your enterprise network administrator:

1. Valid PKI digital certificate
2. Login password corresponding to the user name extracted from the certificate (required only in PKI digital certificate-challenge authentication mode)
3. Login user name and password (required only in the L2TP over IPSec VPN scenario)

NOTE

You can also use the configuration and connection templates in **8** Appendix to check whether the obtained authentication information is complete.

The following table lists the support for PKI digital certificate authentication in different OSs and VPN types.

Table 5-2 Support for PKI digital certificate authentication

VPN Type/OS	Windows	Linux	Mac OS
SSL VPN (certificate-anonymous authentication)	Y	Y	Y
SSL VPN (certificate-challenge authentication)	Y	Y	Y
L2TP VPN	N	N	N
L2TP over IPSec VPN	Y	N	N

Procedure

Step 1 Import the PKI digital certificate to your mobile device.

- In the Windows certificate authentication scenario, import the certificate to the Internet Explorer.
- In the Linux certificate authentication scenario, save the certificate in the **Certificate** folder in the main directory.
- In MAC certificate authentication scenarios, certificates need to be imported into credentials.

Step 2 Double-click the certificate to install it as prompted.

Step 3 Initiate a VPN connection request. The certificate authentication page is displayed.

Step 4 In the **Please select a certificate** list, select the imported PKI digital certificate. If the SSL VPN certificate-challenge authentication mode is used, enter the login password corresponding to the user name extracted from the certificate. For an L2TP over IPSec VPN connection, you need to enter the user name and password. Then, click **Login**.

Step 5 If the authentication succeeds, the device successfully connects to the intranet. The message "**Connection-successful**" is displayed.

----End

Follow-Up Procedure

- If you need to perform two-factor authentication, see **5.2.4** Two-Factor Authentication.
- If the authentication or VPN connection fails, rectify the fault by referring to **7.3** Connection Faults.
- After your device successfully connects to the intranet, you can try to access resources in the intranet. If the resources cannot be accessed, rectify the fault by referring to **7.4** Service Faults.
- Alternatively, you can return to **2** Getting Started to view other content on the **task map**.

5.2.3 USB Key Authentication

You can insert the USB key device provided by your enterprise network administrator into the USB port of your mobile device and use the certificate in the USB key for identity authentication. USB key certificate-anonymous authentication and USB key certificate-challenge authentication are supported in SSL VPN scenarios. In the L2TP over IPSec VPN scenario, if IPSec identity authentication mode is set to **USB key digital signature authentication**, USB key certificate authentication is used.

Before You Start

Obtain the following information required for USB key certificate authentication from your enterprise network administrator:

1. USB key device, driver, and PIN
2. Login password corresponding to the user name extracted from the certificate (This password is required only in USB key certificate-challenge authentication mode.)
3. Login user name and password (required only in the L2TP over IPSec VPN scenario)

NOTE

You can also use the configuration and connection templates in **8** Appendix to check whether the obtained authentication information is complete.

The following table lists the support for USB key certificate authentication in different OSs and VPN types.

Table 5-3 Support for USB key certificate authentication

VPN Type/OS	Windows	Linux	Mac OS
SSL VPN (certificate-anonymous authentication)	Y	N	N
SSL VPN (certificate-challenge authentication)	Y	N	N

VPN Type/OS	Windows	Linux	Mac OS
L2TP VPN	N	N	N
L2TP over IPSec VPN	Y	N	N

Procedure

Step 1 Insert the USB key into the USB port of your mobile device and install the USB key driver.

Step 2 Initiate a VPN connection request. The certificate authentication page is displayed.

Step 3 In the **Certificate** list, select the identified USB key certificate. If the SSL VPN certificate-challenge authentication mode is used, enter the login password corresponding to the user name extracted from the certificate. For an L2TP over IPSec VPN connection, you need to enter the user name and password. Then, click **Login**.

Step 4 In the displayed dialog box, enter the PIN of the USB key device and click **OK**.

Step 5 If the authentication succeeds, the device successfully connects to the intranet. The message "**Connection-successful**" is displayed.

----End

Follow-Up Procedure

- If you need to perform two-factor authentication, see **5.2.4** Two-Factor Authentication.
- If the authentication or VPN connection fails, rectify the fault by referring to **7.3** Connection Faults.
- After your device successfully connects to the intranet, if you can access the resources in the intranet but cannot access the Internet, rectify the fault by referring to **7.4** Service Faults.
- Alternatively, you can return to **2** Getting Started to view other content on the **task map**.

5.2.4 Two-Factor Authentication

In SSL VPN scenarios, the client supports two-factor authentication. That is, the client uses a dynamic token or SMS verification code to perform secondary authentication based on user name/password authentication or certificate authentication.

Before You Start

Contact your enterprise network administrator to prepare the device for receiving the dynamic token or SMS verification code. The device is used to obtain the verification information required for two-factor authentication.

Before performing two-factor authentication, you need to perform initial authentication. Confirm with your enterprise network administrator about the authentication mode and complete the authentication by referring to one of the following sections:

- **5.2.1** User Name/Password Authentication
- **5.2.2** Authentication by Importing the PKI Digital Certificate
- **5.2.3** USB Key Authentication

NOTE

You can also use the configuration and connection templates in **8** Appendix to check whether the obtained authentication information is complete.

Procedure

Step 1 After the initial authentication succeeds, a dialog box is displayed, asking you to enter the dynamic token or SMS verification code for two-factor authentication.

Step 2 Obtain the dynamic token or SMS verification code on the receiving device, enter it in the text box, and click **OK**.

Step 3 After two-factor authentication succeeds, your device successfully connects to the intranet. The message "**Connection-successful**" is displayed.

----End

Follow-Up Procedure

- If the authentication or VPN connection fails, rectify the fault by referring to **7.3** Connection Faults.
- After your device successfully connects to the intranet, you can try to access resources in the intranet. If the resources cannot be accessed, rectify the fault by referring to **7.4** Service Faults.
- Alternatively, you can return to **2** Getting Started to view other content on the **task map**.

6 Optional Configurations

This section describes the optional configurations of the UniVPN client, including:.

- Uninstalling the software
- Performing an update
- Changing the login password
- Configuring the server to be trusted
- Configuring automatic startup
- Disabling automatic login
- Changing the UI language

6.1 Uninstalling the UniVPN

The UniVPN client supports the Windows, Linux, and Mac operating systems. To uninstall the UniVPN client in these operating systems, you need to start the uninstallation program.

Uninstalling the UniVPN in the Windows System

Step 1 Choose **Start** > **All Programs** > **UniVPN**.

Step 2 Click **Uninstall**. In the displayed dialog box, click **Yes**.

----End

Uninstalling the UniVPN in the Linux System

Step 1 Log in to the Linux system using an account that has the root permission.

Step 2 Start the **Terminal** and access the **/usl/local/UniVPN** directory.

```
root@rtw-virtual-machine:~# cd /usr/local/UniVPN
root@rtw-virtual-machine:/usr/local/UniVPN#
```

Step 3 Run the **./ uninstall.sh** command as the root user to uninstall the UniVPN.

```
root@rtw-virtual-machine:/usr/local/UniVPN# ./uninstall.sh
Stopping UniVPNPromoteService daemon: ./uninstall.sh: line 19: 28692 killed
sh UniVPNPromoteService.sh stop
Uninstall successfully...
```

----End

Uninstalling the Software in the Mac OS System

Step 1 Double-click **UniVPNUninstaller** in the application program folder to start the uninstallation program.

Step 2 Click **Uninstall** to uninstall the UniVPN client.

----End

6.2 Version Detection and Upgrade

The UniVPN supports version detection and upgrade.

Before You Start

- The UniVPN can detect software versions and perform upgrades only after establishing a VPN connection with the peer gateway.
- The basic upgrade procedure is as follows:
  a. The enterprise network administrator uploads the latest UniVPN software package to the enterprise gateway.
  b. When you establish a VPN tunnel with the gateway through the UniVPN, the UniVPN automatically detects and compares the current version with the version of the software installation package on the gateway.
  c. If the software installation package on the gateway is determined as a new version, the system prompts you to perform the upgrade.

Procedure

Step 1 Click in the upper right corner of the client page and choose **Setting** from the menu. Select the **Detect a new version** option. The client will periodically check whether the software installation package of a new version is available on the gateway.

Step 2 If a new version is detected, a prompt is displayed, asking you to upgrade the software. Click **Yes** to download and install the new version.

NOTE

When multiple users log in to the Linux operating system at the same time, automatic upgrade is not supported.

----End

6.3 Changing the Login Password

The UniVPN allows users to change their login passwords.

Before You Start

The password can be changed only when a VPN connection is set up between the UniVPN and the peer gateway.

NOTE

The password change function is supported only in SSL VPN scenarios.

Procedure

Step 1 Click in the upper right corner of the client page and choose **Change Password** from the menu. Alternatively, right-click the tray icon of the client and choose **Change Password** from the shortcut menu.

Step 2 In the **VPN password modification** window that is displayed, change the login password.

----End

Follow-Up Procedure

After the password is changed, the current VPN connection is interrupted. You must enter the new password to re-log in.

6.4 Other Configurations

This section describes other optional configurations of the UniVPN.

Blocking Connections to Untrusted Servers

When the UniVPN establishes an SSL VPN tunnel with the peer gateway, it checks the device certificate sent by the gateway.

Click in the upper right corner of the client page and choose **Setting** from the menu. The **Verify trusted servers** option is available.

- If this option is selected:

  When the UniVPN fails to verify the gateway device certificate, the system displays the alarm "**Gateway certificate verification: Untrusted VPN server certificate!**" If you

have confirmed that the peer gateway is secure, click **Continue** to continue establishing the SSL VPN tunnel. If you cannot confirm the security of the peer gateway, click **Cancel** to stop the tunnel establishment.

- If this option is deselected:

  When the UniVPN fails to verify the gateway device certificate, the system does not generate any alarm and directly establishes the tunnel.

Setting Automatic Startup upon Power-On

The UniVPN supports automatic startup upon power-on.

Click in the upper right corner of the client page and choose **Setting** from the menu. The **Auto Start** option is available. When this option is selected, the client automatically starts after the device is powered on.

Canceling Automatic Login

Right-click the tray icon of the UniVPN and choose **Cancel Automatic Login** from the shortcut menu. Then, the UniVPN will not automatically start after the device starts.

Changing the UI Language

The UniVPN client supports two UI languages: Chinese and English.

Click in the upper right corner of the client page and choose **Setting** from the menu. You can set **Interface language** to manually switch the UI language.

Window Skin

On the main page of the UniVPN client, click in the upper right corner and choose **Window Skin** from the menu to set the UI color of the UniVPN client.

NOTE

The personalized skin function is supported only by the Windows operating system.

Error Report

Right-click the tray icon of the UniVPN client in the lower right corner, choose **Error Report** from the shortcut menu, enter fault information, and click **OK**.

Proxy Shielding

- In the Windows system:

  The Windows system uses the proxy information of the Internet Explorer. Therefore, you need to modify the proxy information of the Internet Explorer.

a. Open the Internet Explorer and click **Tools**. The **Internet Options** dialog box is displayed.

b. Click the **Connections** tab and click **LAN Settings**.

c. Set the proxy shielding information on the **Proxy server** setting page.

d. Click **OK** to save the settings.

- In the Linux system:

  By default, the Linux system uses the proxy information setting module of the Firefox browser.

  a. Open the Firefox browser, enter **about:preferences** in the address box, and press **Enter**.

  b. Choose **General** > **Network Settings** and click **Settings**.

  c. Set the proxy shielding information.

  d. Click **OK** to save the settings.

- In the Mac operating system:

  By default, the Mac operating system uses the proxy information setting module of the Firefox browser.

  a. Open the Firefox browser, enter **about:preferences** in the address box, and press **Enter**.

  b. Choose **General** > **Network Settings** and click **Settings**.

  c. Set the proxy shielding information.

  d. Click **OK** to save the settings.

After you configure the proxy server on the **LAN Settings** page and log in to the client, a PAC file is automatically generated. After you select **Use automatic configuration script** on the **LAN Settings** page, the PAC file address is automatically specified and the PAC file is used for proxy shielding during client login. After you log out of the client, the browser automatically restores the proxy settings used before login.

The settings in the PAC file instruct the traffic to correctly access the gateway and intranet resources, preventing intranet resource access failures caused by the proxy server configured in the browser. The PAC file keeps the original proxy information unchanged and therefore does not affect the original proxy function.

If you delete the PAC file while you are logged in to the client, you may fail to access the gateway or intranet resources using Internet Explorer when the proxy is used.

7 Troubleshooting

This section describes the common faults that may occur during the installation and use of the UniVPN and the troubleshooting methods.

Faults can be classified into the following types based on task scenarios:

- 7.2 Installation and Upgrade Faults
- 7.3 Connection Faults
- 7.4 Service Faults

If a fault persists after you try the following troubleshooting methods, collect information required for troubleshooting by referring to 7.1 Collecting Information for Troubleshooting, and send the information to the enterprise network administrator for technical support.

7.1 Collecting Information for Troubleshooting

If you encounter a fault that you cannot rectify when installing or using the client, collect the information required for fault locating on the terminal device, and then contact the enterprise network administrator for technical support.

- The client supports the error report collection function. With this function, you can generate error reports in .zip format by just one click. For details, see 7.1.1 "Collecting Error Reports."
- You also export a configuration file. For details, see 7.1.2 "Exporting a Configuration File."

7.1.1 Collecting Error Reports

You can use the error report collection function to generate error reports in .zip format for fault locating by just one click.

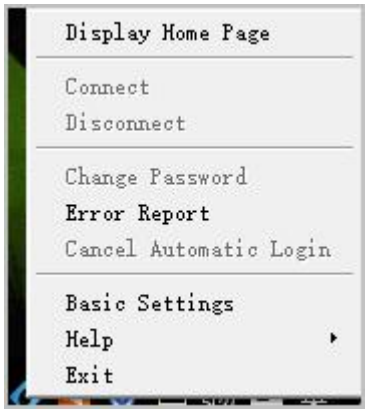
Before You Start

When generating an error report, the UniVPN collects the following client use information and system information, which must be properly protected:

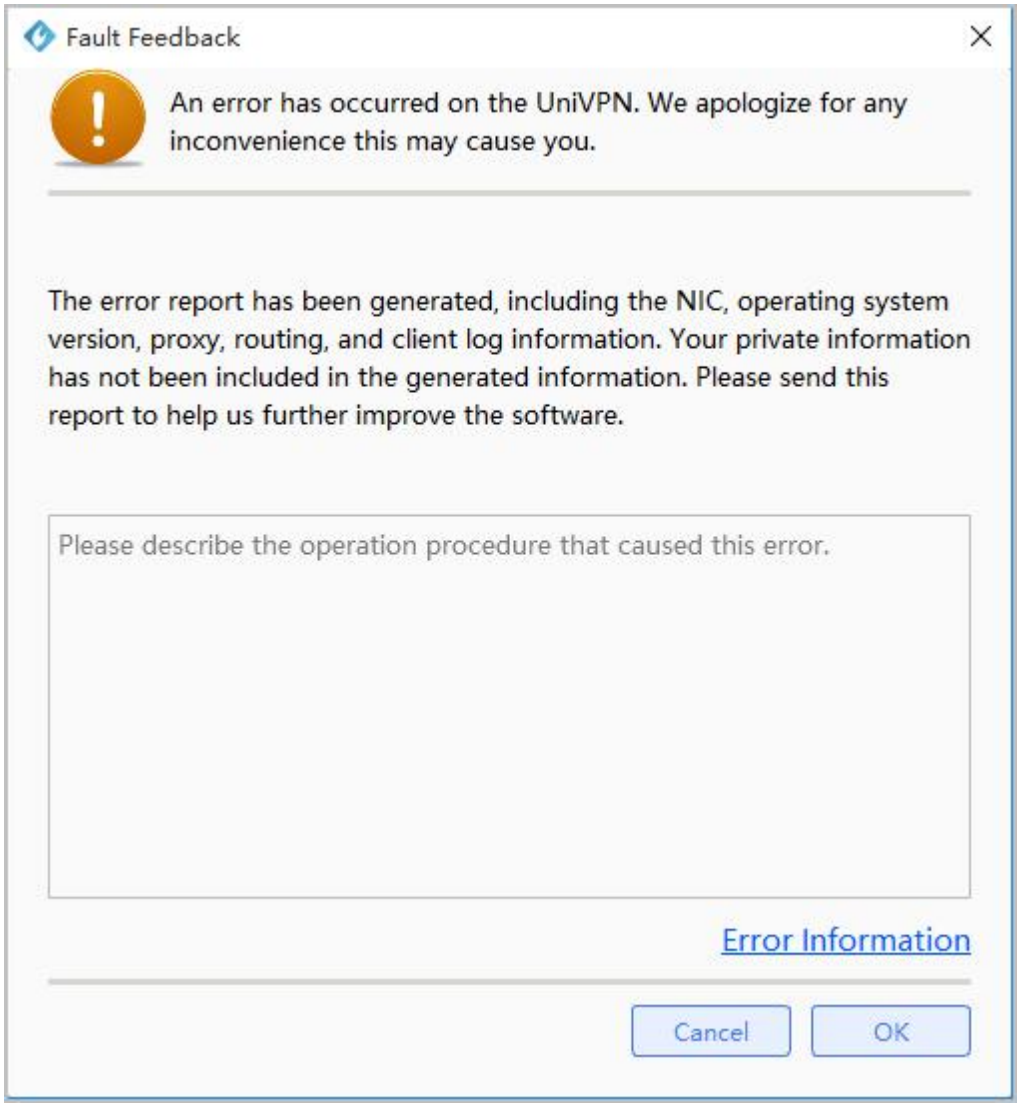
- **error_detail.txt**: contains the manually entered description of the operation steps where a fault occurs and the client version information.
- **netcard_info.txt**: contains the network adapter information of the device.
- **operate_system_info.txt**: contains the operating system information of the device.
- **proxy_info.txt**: records proxy server information.
- **route_info.txt**: contains route information of the device.
- **UniVPN_UniVPN_0.log**: records the logs generated during service configuration on the UniVPN client, such as user login success or failure logs and VPN tunnel establishment success or exception logs.
- **UniVPN_UniVPN_0.log**: records the logs generated for the operations performed on the client configuration page, such as VPN connection configuration and language switching between Chinese and English.
- **UniVPN_UniVPNPromoteService_0.log**: records the service process information of the UniVPN client. The service process is used to ensure normal running of the client.
- Crash file: When the UniVPN client is shut down abnormally, a crash file is generated. The name of the generated crash file varies according to the cause of the abnormal shutdown. In the Windows operating system, the crash file name extension is .dmp. In the Mac and Linux operating systems, the crash file name extension is .core.

Procedure

Step 1 Right-click the UniVPN icon in the tray.



Step 2 Choose **Error report** from the short-cut menu. In the **Fault Feedback** dialog box, enter the configuration procedure or operation that causes the fault, and click **OK**.



Step 3 Click **Browse** and select a directory for storing the error report.

NOTE

When saving the compressed package of an error report in the Linux operating system, ensure that the selected directory does not contain the following special characters: ~ < > | ; ? ' , & #

Step 4 Click **OK** to save the error report to the selected directory.

----End

Follow-up Procedure

After the error report is generated, you need to export a configuration file and send the error report and configuration file to the enterprise network administrator by email, USB flash drive, or other methods.

7.1.2 Exporting a Configuration File

You can export the client configuration file in .ini format. The configuration file is an important reference for troubleshooting as it contains all parameters required for creating a specific VPN connection.

Procedure

Method 1:

Step 1 On the main page of the UniVPN client, select the configured VPN connection and click on the right.

Step 2 In the **Connection Details** window, click **Export** on the left of the navigation tree and select a directory for storing the configuration file. By default, the configuration file is saved in .ini format.

Step 3 Click **Save** to save the configuration file to the selected directory.

----End

Method 2

Step 1 On the main page of the UniVPN client, select the configured VPN connection and click on the right.

Step 2 Select a directory for storing the configuration file. By default, the configuration file is saved in .ini format.

Step 3 Click **Save** to save the configuration file to the selected directory.

----End

Follow-up Procedure

After the configuration file is exported, you can send the exported configuration file and the collected error report to the enterprise network administrator by email, USB flash drive, or other methods.

7.2 Installation and Upgrade Faults

Software Installation Failure

Read the precautions in **Installation Precautions** to check whether your login account has the administrator permission. Only the users who have the administrator permission can install the UniVPN.

Before installing the software, ensure that the OS environment and version of your mobile device comply with the system configuration requirements described in **Installation Precautions**.

Software Upgrade Failure

The possible cause is that the software installation package on the gateway is incorrect. Contact your enterprise network administrator for confirmation.

7.3 Connection Faults

Fail to Establish a VPN Connection for the First Time

The possible cause is that the firewall of the OS blocks the VPN connection of the UniVPN. In **Start > Control Panel > System and Security > Windows Firewall**, set the access rule of the built-in firewall of the OS to **Permit** (the Windows 7 system is used as an example).

The Mobile Device Cannot Identify the Certificate in the USB Key

The possible cause is that the USB key is in poor contact with the USB port of the mobile device or the USB key driver is faulty. Remove the USB key from the USB port and insert it again. If the system still cannot identify the USB key, you need to re-install the USB key driver.

The Message "Tunnel keepalive timed out or negotiation timed out" Is Displayed When a VPN Tunnel Is Established in L2TP Mode

The possible cause is that the encryption and decryption negotiation parameters on the UniVPN and gateway are inconsistent or the UniVPN and gateway are unreachable. In this case, contact your enterprise network administrator to confirm the configuration.

The Message "Failure to Obtain the System Proxy" Is Displayed When System Proxy Is Selected

If you set **Agent type** to **Use the system proxy**, the UniVPN uses the proxy configuration in the browser. The message "**Failure to Obtain the System Proxy**" indicates that no proxy is set for the browser.

In this case, set the proxy server by referring to the following procedure:

Step 1 Open the Internet Explorer and choose **Tools > Internet options** on the upper right corner. In the displayed dialog box, click the **Connections** tab.

Step 2 Click **LAN settings** and set the proxy server. Obtain the proxy server information from your enterprise network administrator. After the configuration is complete, click **OK**.

Step 3 Open the UniVPN, set **Agent type** to **Use the system proxy**. Then, you can find that the proxy server information set in the browser is automatically added to the **Agent Settings** of the UniVPN.

----End

7.4 Service Faults

The User Cannot Access the Internet After a VPN Tunnel Is Established

Symptom

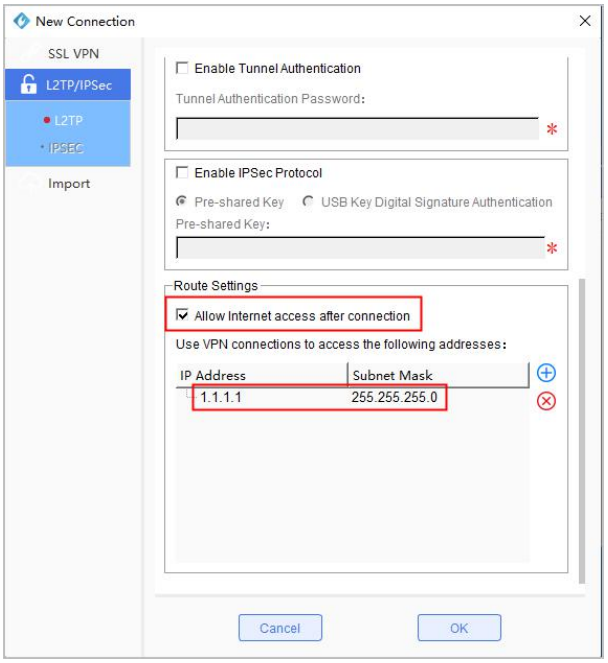
After a VPN tunnel is established, the message "**The Connection is successful**" or "**negotiation succeeded**" is displayed. In this case, the user can access resources on the enterprise network, but cannot access the Internet.

Analysis and handling

The possible cause is that tunnel separation is not configured. As a result, all traffic enters the VPN tunnel.

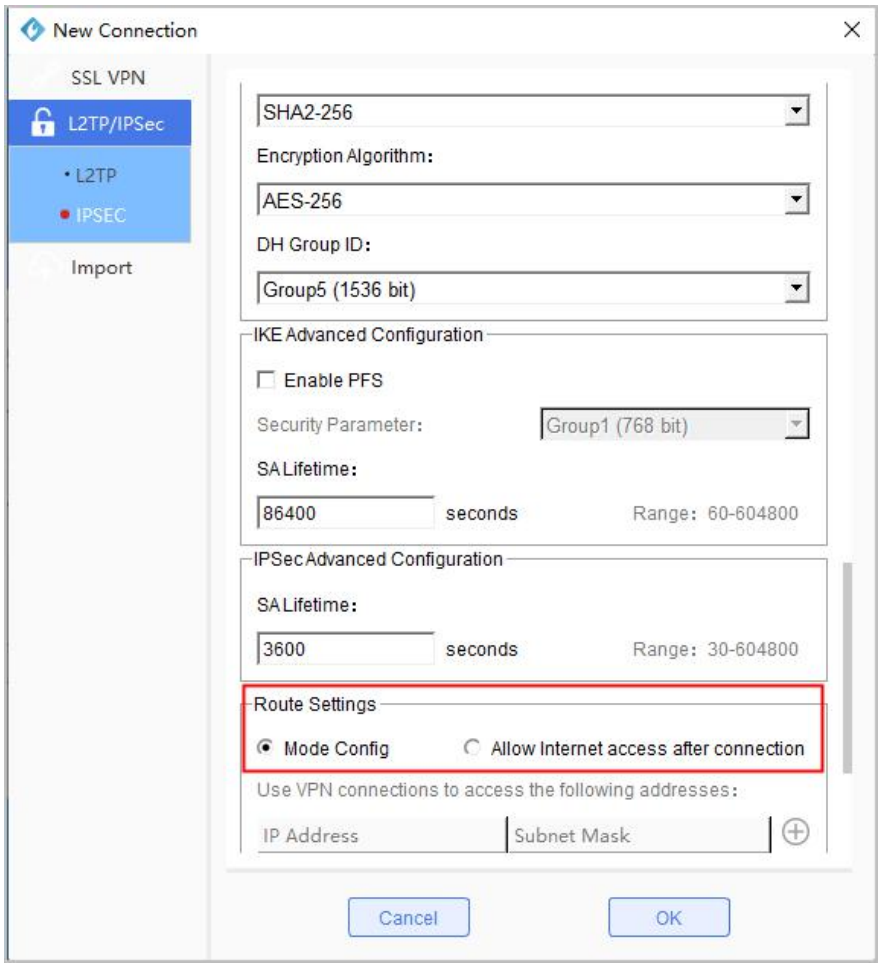
SSL VPN, L2TP VPN, and L2TP over IPSec VPN support tunnel separation.

- SSL VPN tunnel separation involves configuration on the gateway. Therefore, if you cannot access the Internet in an SSL VPN connection, contact your enterprise network administrator to modify the configuration on the gateway.
- L2TP VPN tunnel separation involves configuration on the UniVPN. Check whether **Allow Internet access after connection** is selected and whether the network segment for VPN access is set. If the configuration on the UniVPN is correct, contact your enterprise network administrator.



- L2TP over IPSec VPN tunnel separation can be configured in two modes. Which mode is used depends on the route configuration for the VPN connection:

- If **Mode Config** is selected in the route configuration on the UniVPN, tunnel separation must be configured on the gateway, and the corresponding route must be delivered. In this case, contact your enterprise network administrator to modify the configuration on the gateway.
- If **Allow Internet access after connection** is selected in the route configuration on the UniVPN, check whether the network segment for VPN access is configured. If the configuration on the UniVPN is correct, contact your enterprise network administrator.



8 Appendix

This section describes how to configure the client in the Linux operating system using the CLI. This section also provides SSL VPN, L2TP VPN, and L2TP over IPSec VPN configurations and connection templates, which contain all connection parameters required for configuring and establishing VPN connections, as well as authentication information check items. End users can refer to the templates to check whether the obtained information is complete. The enterprise network administrator can also refer to these templates to provide necessary connection parameters and authentication information for end users.

8.1 Using Commands to Configure the Client in the Linux System

8.2 VPN Configuration and Connection Templates

8.1 Using Commands to Configure the Client in the Linux System

8.1.1 Starting the Client

Step 1 Access the **/usr/local/UnIVPN/serviceclient** directory.

Step 2 Run the **./UniVPNCS** command to start the client. This command can be executed by both common and root users.

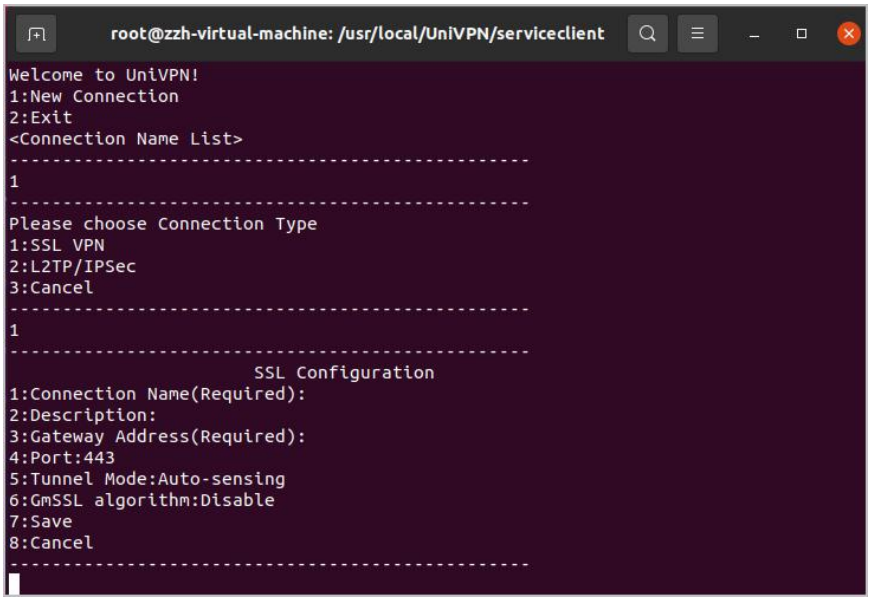
NOTE

Before starting the client using the command, ensure that the client started through the UI desktop has been shut down.

----End

8.1.2 Configuring an SSL VPN Connection

Configuring SSL VPN



Step 1 Enter **1** to create a connection.

Step 2 Enter **1** to set the VPN type to SSL VPN.

Step 3 Enter the corresponding sequence number to complete the configuration of parameters 1 to 5.

- 1. Connection Name(Required)
- 2. Description
- 3. Gateway Address
- 4. Port(Required)
- 5. Tunnel Mode(Required): The options are **Reliable Transmission**, **Quick Transmission**, and **Auto-sensing**.

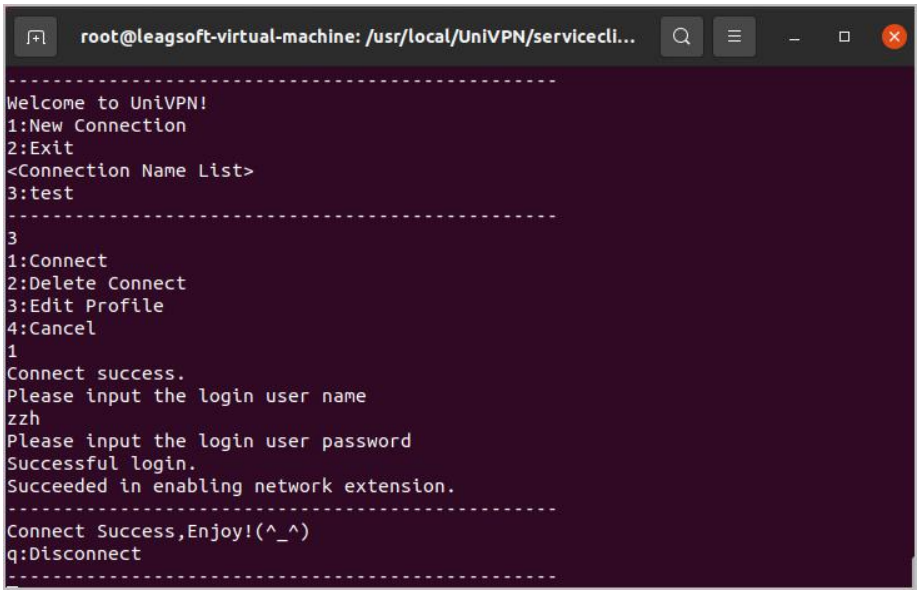
NOTE

For details about the parameters, see Establishing an SSL VPN Tunnel.

Step 4 Enter **7** to save the configuration.

----End

Establishing an SSL VPN Connection



Step 1 Enter the corresponding number to establish an SSL VPN connection.

Step 2 Enter **1** to set up an SSL VPN connection.

Step 3 A message is displayed, indicating that the connection is set up successfully. Enter the user name and password to log in.

----End

NOTE

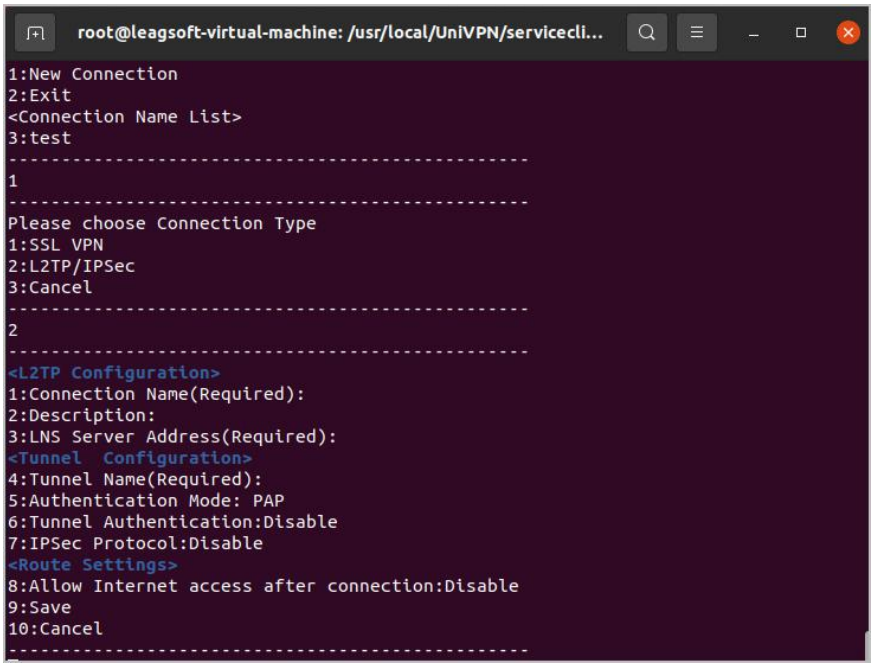
- In the Linux system, the SSL VPN connection configured and established using commands supports only user name/password authentication.
- After the connection is successful, do not close the terminal window. Otherwise, the connection will be disconnected.

SSL VPN Disconnection

Enter **q** to cut off the connection.

8.1.3 Configuring an L2TP VPN Connection

Configuring L2TP VPN



Step 1 Enter **1** to create a connection.

Step 2 Enter **2** and set the VPN type to L2TP/IPSec.

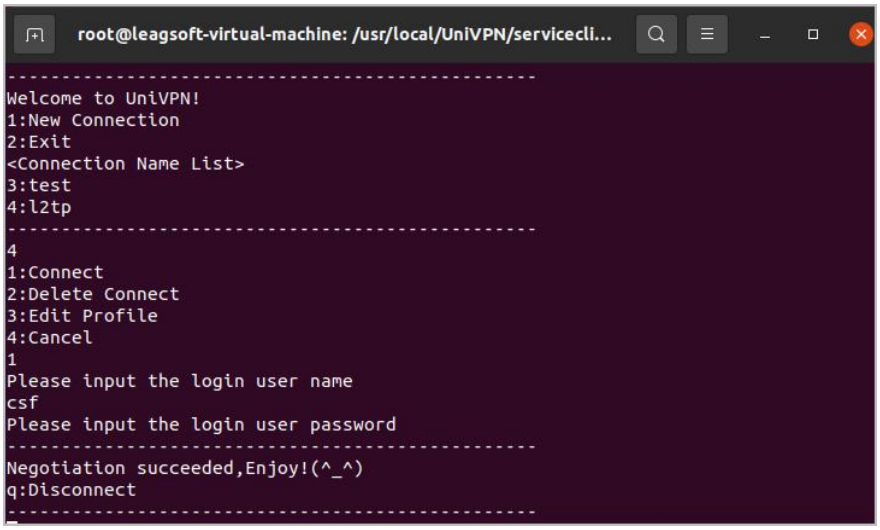
Step 3 Enter the corresponding sequence number to complete the configuration of parameters 1 to 8.

- 1. Connection Name(Required)
- 2. Description
- 3. LNS Server Address(Required)
- 4. Tunnel Name(Required)
- 5. Authentication Mode
- 6. Tunnel Authentication: Enable the tunnel authentication function. After the tunnel authentication function is enabled, you need to enter the tunnel authentication password.
- 7. IPSec Protocol: Enable the IPSec protocol. Do not enable this function.
- 8. Allow Internet access after connection: Set routes. After this option is enabled, you can set the traffic to be encrypted in the VPN tunnel by adding an IP address segment.

Step 4 Enter **9** to save the configuration.

----End

Establishing an L2TP VPN Connection



Step 1 Enter the corresponding number to establish an L2TP VPN connection.

Step 2 Enter **1** to set up an L2TP VPN connection.

Step 3 Enter the user name and password to log in.

----End

NOTE

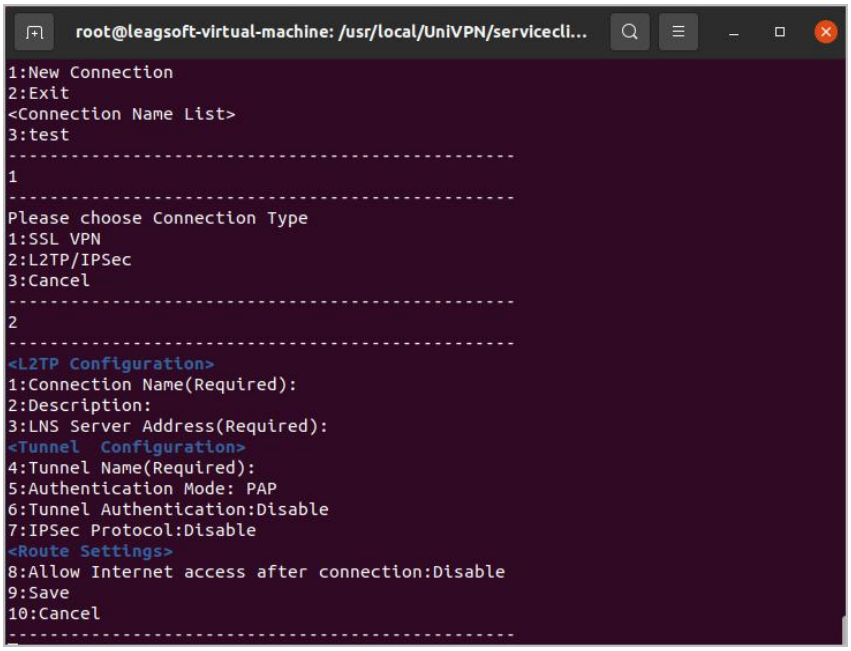
After the connection is successful, do not close the terminal window. Otherwise, the connection will be disconnected.

L2TP VPN Disconnection

Enter **q** to cut off the connection.

8.1.4 Configuring an L2TP over IPSec VPN Connection

Setting L2TP Parameters



Step 1 Enter **1** to create a connection.

Step 2 Enter **2** and set the VPN type to L2TP/IPSec.

Step 3 Enter the corresponding sequence number to complete the configuration of parameters 1 to 6.

- 1. Connection Name(Required)
- 2. Description
- 3. LNS Server Address(Required)
- 4. Tunnel Name(Required)
- 5. Authentication Mode
- 6. Tunnel Authentication: Enable the tunnel authentication function. After the tunnel authentication function is enabled, you need to enter the tunnel authentication password.

----End

Setting IPSec Parameters

```
root@leagsoft-virtual-machine: /usr/local/UniVPN/servicecli...
-----------------------------------------------
<L2TP Configuration>
1:Connection Name(Required):
2:Description:
3:LNS Server Address(Required):
<Tunnel  Configuration>
4:Tunnel Name(Required):
5:Authentication Mode: PAP
6:Tunnel Authentication:Disable
7:IPSec Protocol:Disable
<Route Settings>
8:Allow Internet access after connection:Disable
9:Save
10:Cancel
-----------------------------------------------
7
IPSec Protocol
1:enable
2:Disable
3:Cancel
1
-----------------------------------------------
<L2TP Configuration>
1:Connection Name(Required):
2:Description:
3:LNS Server Address(Required):
<Tunnel  Configuration>
4:Tunnel Name(Required):
5:Authentication Mode: PAP
6:Tunnel Authentication:Disable
7:IPSec Protocol:Enable
8:IPSec Authentication Mode:Pre-shared Key
  Pre-shared Key(Required):
<IPSEC Configuration>
9:IPSec Server address:Use LNS server address
10:Encapsulation Mode:Transmission mode
11:EPS Authentication Algorithm:SHA2-256
12:EPS Encryption Algorithm:AES-256
<IKE Basic Configuration>
```

```
<IKE Advanced Configuration>
17:PFS:Disable
18:SA Lifetime:86400
<IPSec Advanced Configuration>
19:SA Lifetime:3600
<Route Settings>
20:Route Settings:Mode Config
21:Save
22:Cancel
-----------------------------------------------
```

Step 1 Enter **7** to enable the IPSec protocol.

Step 2 Enter the corresponding sequence number to complete the configuration of parameters 8 to 20.

- 8. IPSec Authentication Mode: In the Linux system, IPSec supports only pre-shared key authentication. In pre-shared key authentication mode, the pre-shared key is required.
- 9. IPSec Server address: IP address of the IPSec server. By default, the IP address of the LNS server is used (Use LNS server address).
- 10. Encapsulation Mode: IPSec encapsulation mode, which can be **Transmission mode** or **Tunnel mode**.
- 11. ESP Authentication Algorithm
- 12. ESP Encryption Algorithm

- 13. Negotiation Mode: IKE negotiation mode, which can be **Main Mode** or **Aggressive Mode**.
- 14. Authentication Algorithm: authentication algorithm used for IKE negotiation
- 15. Encryption Algorithm: encryption algorithm used for IKE negotiation
- 16. DH Group ID: DH group ID used for IKE negotiation
- 17. PFS: After the PFS function is enabled, the corresponding security parameter (Security Parameter) must be configured.
- 18. SA Lifetime(IKE Advanced Configuration): IKE SA lifetime
- 19. SA Lifetime(IPSec Advanced Configuration): IPSec SA lifetime
- 20. Route Settings: The mode can be **Mode Config** or **Allow Internet access after connection**. After this parameter is set to **Allow Internet access after connection**, you can set the traffic to be encrypted in the VPN tunnel by adding an IP address segment.

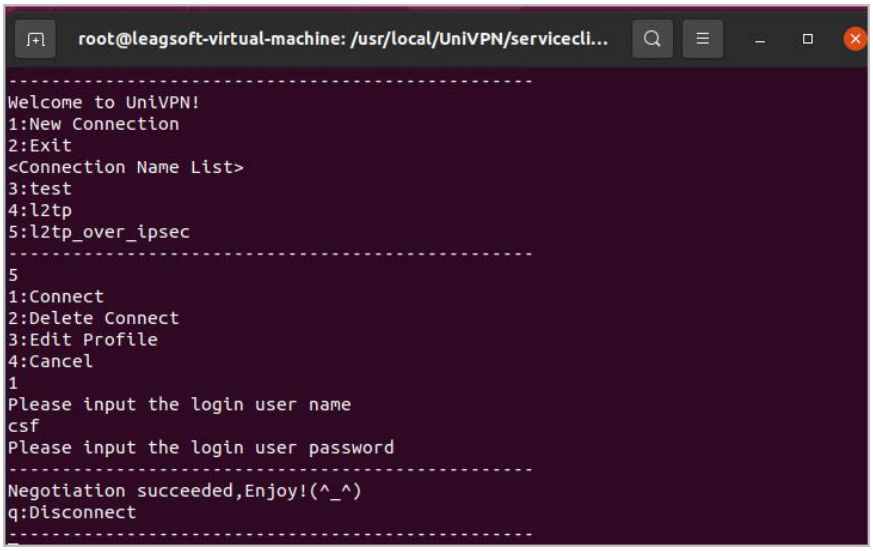
NOTE

For details about the parameters, see Establishing an L2TP over IPSec VPN Tunnel.

Step 3 Enter **21** to save the configuration.

----End

Establishing an L2TP over IPSec VPN Connection



Step 1 Enter the corresponding number to establish an L2TP over IPSec VPN connection.

Step 2 Enter **1** to set up the L2TP over IPSec VPN connection.

Step 3 Enter the user name and password to log in.

----End

NOTE

- In the Linux system, the L2TP over IPSec VPN connection configured and established using commands supports only user name/password authentication.

- After the connection is successful, do not close the terminal window. Otherwise, the connection will be disconnected.

L2TP over IPSec VPN Disconnection

Enter **q** to cut off the connection.

8.2 VPN Configuration and Connection Templates

8.2.1 SSL VPN Configuration and Connection Template

Table 8-1 SSL VPN Configuration and Connection Template

<table>
<tr><th colspan="7">SSL VPN Configuration Template</th></tr>
<tr><th>No.</th><th colspan="5">Item</th><th>Parameter</th></tr>
<tr><td rowspan="4">1</td><td rowspan="4">Are Proxy Settings needed?</td><td colspan="4">No</td><td>-</td></tr>
<tr><td rowspan="3">Yes</td><td rowspan="3">Which proxy mode is used?</td><td>Use proxy is used</td><td rowspan="3">Address, Port Account, and Password</td><td></td></tr>
<tr><td>Use Http/Https proxy</td><td></td></tr>
<tr><td>Use the Socks5 proxy</td><td></td></tr>
<tr><td>2</td><td colspan="5">Connection name</td><td></td></tr>
<tr><td>3</td><td colspan="5">Description</td><td></td></tr>
<tr><td>4</td><td colspan="5">Remote gateway</td><td></td></tr>
<tr><td>5</td><td colspan="5">Port</td><td></td></tr>
<tr><td rowspan="3">6</td><td rowspan="3">Which tunnel mode is used?</td><td colspan="4">Reliable Transmission</td><td>-</td></tr>
<tr><td colspan="4">Quick Transmission</td><td>-</td></tr>
<tr><td colspan="4">Auto-sensing</td><td>-</td></tr>
<tr><td>7</td><td colspan="5">Are you sure you want to enable the route coverage function?</td><td>-</td></tr>
<tr><td>8</td><td colspan="5">Are you sure you want to enable the national secret algorithm function?</td><td>-</td></tr>
<tr><th colspan="7">SSL VPN Connection Template</th></tr>
<tr><th>No.</th><th>User Identity</th><th colspan="5">Required Information</th></tr>
</table>

	Authentication			
1	User name/password authentication	Name		
		Password		
2	PKI digital certificate authentication	Certificate-anonymous authentication	Valid PKI digital certificate	
		Certificate-challenge authentication	Valid PKI digital certificate	
			Login password corresponding to the user name extracted from the certificate	
3	USB key certificate authentication	Certificate-anonymous authentication	USB key device, driver, and PIN	
		Certificate-challenge authentication	USB key device, driver, and PIN	
			Login password corresponding to the user name extracted from the certificate	
4	Two-factor authentication	Initial authentication	User name/password authentication (referring to the above)	
			PKI digital certificate authentication (referring to the above)	
			USB key certificate authentication (referring to the above)	
		Two-factor authentication	Dynamic token code authentication	Obtain the value from the dynamic token code receiving device.
			SMS verification code authentication	Obtain the value from the SMS verification code receiving device.

8.2.2 L2TP VPN Configuration and Connection Template

Table 8-2 L2TP VPN Configuration and Connection Template

L2TP VPN Configuration Template

No.	Item			Parameter
Proxy Settings				
1	Are Proxy Settings needed?	No		-
		Yes (Socks5 proxy is used.)	Address	
			Port	
			Account	
			Password	
L2TP Configuration				
2	Connection name			
3	Description			
4	LNS server address			
Tunnel Configuration				
5	Tunnel name			
6	Which authentication mode is used?	CHAP		-
		PAP		-
7	Is tunnel authentication enabled?	No		-
		Yes	tunnel verification password	
Route Settings				
8	Deselect **Allow Internet access after connection**.			-
	Select **Allow Internet access after connection**. No IP address is added to the IP address list.			-
	Select **Allow Internet access after connection**. Add IP addresses to the IP address list.		IP addresses to be added	
L2TP VPN Connection Template				
No.	**User Identity Authentication**	**Required Information**		
1	User name/password authentication	User Name		
		Password		

8.2.3 L2TP over IPSec VPN Configuration and Connection Template

Table 8-3 L2TP over IPSec VPN Configuration and Connection Template

L2TP over IPSec VPN Configuration Template				
No.	**Item**			**Parameter**
Proxy Settings				
1	Are Proxy Settings needed?	No		-
		Yes (Use the Socks5 proxy)	Address	
			Port	
			Account	
			Password	
L2TP Configuration				
2	Connection name			
3	Description			
4	LNS server address			
Tunnel Configuration				
5	Tunnel name			
6	Which authentication mode is used?	CHAP		-
		PAP		-
7	Is tunnel authentication enabled?	No		-
		Yes	tunnel verification password	
Enable IPSec Protocol				
8	Which IPSec identity authentication mode is used?	Preset shared key	Identity authentication word	
		USB key digital signature authentication	USB pin	
IPSec Settings				
9	IPsec server address	Are L2TP VPN	No	-

		and IPSec VPN gateways are the same?	Yes		Select **Using LNS server**.
10	Which encapsulation mode is used?	Tunnel mode			-
		Transmission mode			-
11	Which ESP authentication algorithm is used?	MD5			-
		SHA1			-
		SHA2-256			-
12	Which ESP encryption algorithm is used?	DES			-
		3DES			-
		AES			-
IKE Settings					
13	Which negotiation mode is used?	Main Mode			-
		Aggressive Mode			-
14	Which type of ID is used?	IP address			-
		Name			-
15	Local name (this parameter is required if the ID type is set to **Name**.)				
16	Security gateway name (this parameter is required if the ID type is set to **Name**.)				
17	Authentication algorithm	MD5			-
		SHA1			-
		SHA2-256			-
18	Encryption algorithm	DES-CBC			-
		3DES-CBC			-
		AES-128			
		AES-192			-
		AES-256			-
19	DH Group ID	Group1			-
		Group2			-
		Group5			-
IKE Advanced Settings					
20	Is PFS enabled?	No			-
		Yes	Securi	Group1	-

			ty Param eter	Group2	-
				Group5	-
21	Security alliance life cycle				
IPsec Advanced Settings					
22	Security alliance life cycle				
Route Settings					
23	Select **Mode Config**.				-
	Select **Allow Internet access after connection**. No IP address is added to the IP address list.				-
	Select **Allow Internet access after connection**. Add IP addresses to the IP address list.		IP addresses to be added		
L2TP over IPSec VPN Connection Template					
No.	**User Identity Authentication**	**Required Information**			
1	User name/password authentication	User name			
		Password			
2	PKI digital certificate authentication	Valid PKI digital certificate			
		User name			
		Password			
3	USB key certificate authentication	USB key device, driver, and PIN			
		User name			
		Password			