联软科技
LEAGSOFT

Leagsoft UniVPN

Administration Guide

Contents

1 About This Document **1**

2 Overview **3**

3 Limitation and Specifications **8**

4 Installation and Uninstallation **14**

4.1 Installing and Uninstalling the UniVPN in the Windows Operating System 14

4.2 Installing and Uninstalling the UniVPN in the Linux Operating System 17

4.3 Manually Installing the UniVPN on a Mac Operating System 19

4.4 Distributing the UniVPN Installation Package and Automatically Installing the UniVPN Through the AD Server 21

4.4.1 (Optional) Creating an Active Directory Domain and Domain User 21

4.4.2 Converting the Format of an Installation Package from EXE to MSI 31

4.4.3 Creating a Software Installation Policy 40

5 Configuration **49**

5.1 Using the UniVPN to Establish VPN Tunnels 49

5.1.1 Manual Mode 49

5.1.1.1 Establishing an SSL VPN Tunnel 49

5.1.1.2 Establishing an L2TP VPN Tunnel 55

5.1.1.3 Establishing an L2TP over IPSec VPN Tunnel 59

5.1.2 Profile Mode 70

5.2 Common Settings 74

6 Upgrade **80**

7 Troubleshooting **82**

8 FAQ **83**

9 Appendix **85**

9.1 FAQs About the Mobile Client 86

9.1.1 How Do I Import a Chinese Cryptographic Certificate? 88

9.1.2 How Do I Report an iOS Client Problem? 95

9.1.3 How Do I Disable Automatic Login (Android)? 102

9.2 Using Commands to Configure the Client in the Linux System 103

9.2.1 Starting the Client 103

9.2.2 Configuring an SSL VPN Connection 103
9.2.3 Configuring an L2TP VPN Connection 105
9.2.4 Configuring an L2TP over IPSec VPN Connection 107
9.3 Acronyms and Abbreviations 110

1 About This Document

Intended Audience

This document is intended for network administrators who manage the UniVPN and device. The administrators must be familiar with basic Ethernet knowledge and experienced in network management. In addition, the administrators must have general knowledge of the enterprise network, including the UniVPN and device network topology and the provided network services.

Symbol Conventions

The symbols that may be found in this document are defined as follows.

Symbol	Description
NOTICE	Indicates a potentially hazardous situation which, if not avoided, could result in equipment damage, data loss, performance deterioration, or unanticipated results. NOTICE is used to address practices not related to personal injury.
NOTE	Calls attention to important information, best practices and tips. NOTE is used to address information not related to personal injury, equipment damage, and environment deterioration.

GUI Conventions

The GUI conventions that may be found in this document are defined as follows.

Convention	Description
Boldface	Buttons, menus, parameters, tabs, window, and dialog titles are in **boldface**. For example, click **OK**.
>	Multi-level menus are in **boldface** and separated by the ">" signs. For example, choose **File** > **Create** > **Folder**.

Change History

The change history includes all the updates. Therefore, the latest document issue contains all updates made in previous issues.

- **Issue 07 (2023-02-28) of Product Version 10781.11.0**

  The seventh commercial release.

  Internal optimization.
- **Issue 06 (2022-12-30) of Product Version 10781.9.0**

  The sixth commercial release.

  New support system for univpn client: Ubuntu 22.04.
- **Issue 05 (2022-11-30) of Product Version 10781.8.0**

  The fifth commercial release.

  New support system for univpn client: MacOS Ventura 13.
- **Issue 04 (2022-10-31) of Product Version 10781.7.0**

  The fourth commercial release.

  The OS X 10.12.x system is no longer supported by UniVPN clients after version 10781.7.0.
- **Issue 03 (2022-08-30) of Product Version 10781.5.0**

  The thrid commercial release.

  The new interface of univpn client displays: virtual IP and Bytes sent/Received statistics.

  New features of univpn client: VPN fast switching.
- **Issue 02 (2022-07-30) of Product Version 10781.3**

  The second commercial release.

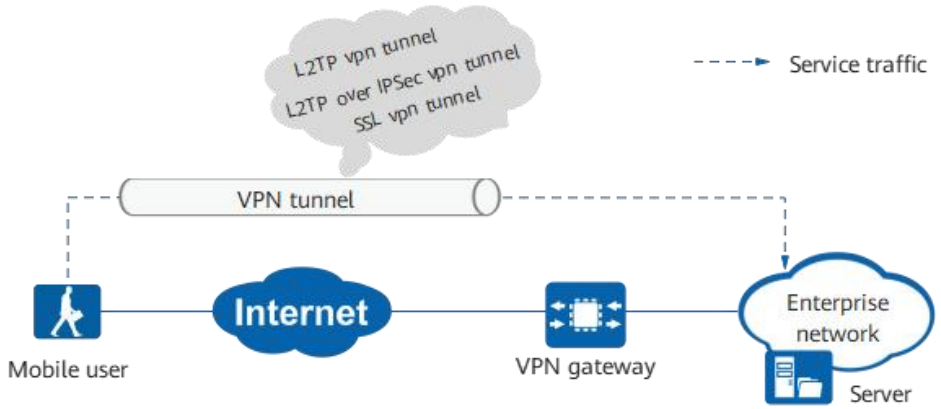
  New support system for univpn client: windows11.
- **Issue 01 (2022-03-18) of Product Version 10781.2**

  The first commercial release.

2 Overview

UniVPN is a VPN client software launched by Shenzhen Leagsoft Technologies inc to provide secure and convenient access services for mobile users to remotely access enterprise network resources. Figure 2-1 shows the typical application scenario.

Figure 2-1 Mobile user uses the UniVPN to access the enterprise network over a VPN tunnel



The UniVPN has the following characteristics:

- **Powerful access ability**

  The UniVPN integrates SSL VPN, L2TP VPN, and L2TP over IPSec VPN access technologies and can meet the VPN access requirements in different scenarios. The enterprise does not need to purchase diversified terminal software for different VPN access scenarios, reducing investment costs.

- **Flexible tunnel splitting**

  The UniVPN enables mobile users to access enterprise network resources and Internet and LAN resources at the same time using different tunnels. The traffic of different services is not mutually affected.

- **Preferential gateway selection**

  A large enterprise usually provides multiple VPN gateways for external users to access. If one of the VPN gateways has a large number of access users, the system resources of the gateway may become exhausted, users' access may be delayed, and excess users may be forced to log out, affecting user experience. If the UniVPN is installed, the VPN gateway with the highest response speed is automatically selected for mobile users.

When the preferential gateway selection function is used, gateways may be selected randomly for mobile users, and the users' access requests are distributed to different VPN gateways, which effectively alleviate the performance bottleneck of a single VPN gateway from massive user access. In addition, this function improves user access speed and success rate.

- **Reliable link backup**

  In SSL VPN access scenarios, one VPN gateway may provide multiple IP addresses (one IP address corresponds to one link) for mobile users to connect to. If an SSL VPN tunnel is disconnected unexpectedly, the UniVPN automatically re-establishes a VPN tunnel with another IP address of the gateway. After the new VPN tunnel is established, service traffic will be continuously transmitted using the new tunnel. This mechanism reduces network fault influence on services and ensures service continuity.

- **Diverse authentication methods**

  In most cases, the VPN gateway provides multiple methods for authenticating mobile users. Therefore, the number of authentication methods supported by the VPN terminal software determines the number of application scenarios of this software. The UniVPN provides various authentication methods, including user name and password authentication, certificate-anonymous authentication, certificate-challenge authentication, and two-factor authentication. Therefore, the UniVPN can be applied to most VPN access scenarios.

Functions

Table 2-1 lists the functions provided by the UniVPN.

Table 2-1 UniVPN functions

Function		Description
SSL VPN	Network extension	Network extension enables mobile users to establish secure SSL VPN tunnels with the SSL VPN gateway so that the mobile users can access all intranet resources. In network extension, an SSL VPN tunnel can be established in either reliable or quick transmission mode.
	Endpoint security	The endpoint security function prevents illegitimate devices from accessing the enterprise network and reduces insecure device threats to the enterprise network. Endpoint security includes: • Host check Checks whether the operating systems, ports, processes, and antivirus software of devices used by mobile users meet security requirements. The devices that do not meet security requirements are not allowed to access the enterprise network. In addition, the host check function provides the anti-nested remote desktop connections and anti-snapshot capabilities to mitigate security risks from user devices. • Cache clearing Clears the access history to enhance information

Function		Description
		security. Note that the endpoint security function is implemented by the VPN gateway. The UniVPN and the devices on which the UniVPN is installed are the objects being verified, and no configuration is required.
	Preferential gateway selection	If an enterprise provides multiple SSL VPN gateways, enabling this function ensures that users can connect to the gateway with the highest response speed. This function improves user access speed and success rate and effectively alleviates the performance bottleneck of a single VPN gateway from massive user access.
	Reconnection	When an SSL VPN tunnel is disconnected unexpectedly, the UniVPN automatically sends a reconnection request to the SSL VPN gateway every five seconds. If the tunnel cannot be reconnected after three reconnection requests, the reconnection ends.
	Link backup	When the UniVPN establishes VPN tunnels with an SSL VPN gateway that provides multiple public IP addresses, the UniVPN automatically records all the IP addresses. If an SSL VPN tunnel fails, the UniVPN reconnects the tunnel. If the tunnel cannot be reconnected after three reconnection requests, the UniVPN automatically re-establishes an SSL VPN tunnel with another IP address of the gateway. The link backup function effectively resolves the tunnel availability problem if the gateway has multiple IP addresses and reduces network fault impact on services.
	Route Overwrite	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 overwrite function is enabled, the route delivered by the peer gateway overwrites the existing route. This prevents network access exceptions caused by local route conflicts.
	Chinese cryptographic algorithm	The client supports to use the Chinese cryptographic algorithm to establish an SSL VPN connection with the peer gateway. The Chinese cryptographic algorithm is a commercial password block standard symmetric algorithm compiled by China's National Password Administration. The block length and key length are both 128 bits. Under high security requirements, using Chinese cryptographic algorithm can meet the requirements.
	Two-factor	The client supports token code+SMS verification

Function		Description
	authentication	code two-factor authentication. This function is triggered when a third-party server is required for user authentication. When you enter your user name and password for login, enter the token code or SMS verification code for two-factor users, enhancing security.
L2TP VPN		L2TP VPN is a Layer-2 tunnel protocol. It supports PPP frame transmission over tunnels and relies on PPP for user access authentication. However, L2TP VPN does not provide the encryption function and lacks security protection. PPP supports both PAP and CHAP authentication.
L2TP over IPSec VPN		L2TP over IPSec is a common extension of IPSec. L2TP over IPSec combines the benefits of both VPN technologies. L2TP authenticates users and assigns IP addresses, and IPSec ensures tunnel security.
NAT traversal		If a NAT device is deployed on the VPN packet forwarding path, the NAT traversal function must be enabled on the devices on both ends of the VPN tunnel to ensure service continuity. SSL VPN, L2TP VPN, and L2TP over IPSec VPN provided by the UniVPN support the NAT traversal function, and this function is enabled by default.
Proxy traversal		Employees of some enterprises may use a proxy server to access the Internet. In this scenario, all packets sent by the employees are forwarded by the proxy server to the remote VPN gateway. When employees use proxy servers, the UniVPN can establish SSL VPN, L2TP VPN, and L2TP over IPSec VPN tunnels with the remote VPN gateway.
Tunnel splitting		Tunnel splitting is an application scenario of VPN. With the tunnel splitting function, users can access enterprise network resources and Internet and LAN resources at the same time using VPN tunnels. SSL VPN, L2TP VPN, and L2TP over IPSec provided by the UniVPN support tunnel splitting.
Basic functions	Automatic startup upon power-on	The UniVPN is started when the system is powered on.
	Language	The UniVPN provides three species of UI language, including: • English • Chinese(Simplified) • Follow system NOTE

Function		Description
		During the installation, the UI language is the same as that of the system by default. For systems whose language is not Chinese or English, the default UI language is English.
	Automatic login	In the first login to the VPN gateway, the UniVPN remembers the user name and password. In subsequent logins, the user does not need to enter the user name or password.
VPN profile	Import	On the UniVPN, a user can save the existing VPN connection into a profile. Then other users can use the VPN connection after importing the profile to the UniVPN.
	Export	Existing VPN connections can be exported as profiles for other users to use.
Configuration using commands		The SSL VPN, L2TP VPN, and L2TP over IPSec VPN connections can be created using commands in the Linux operating system.
Non-administrator user configuration		Non-administrator users can configure and set up VPN connections on the client.
Fault location		Users can view the UniVPN running status and collect logs and error reports to know UniVPN operation, analyze the network condition, and locate problem causes, providing reference for system diagnosis and maintenance.

NOTE

The preceding table lists all the functions of the UniVPN client. Some functions may not be supported when the client is interconnected with devices from different versions.

3 Limitation and Specifications

This section describes the product specifications and usage restrictions of the server and UniVPN client.

Products and Versions

Product Name	Version	Operating System
USG6000	V500R005C20SPC500 and later version	• Windows • Linux • Mac OS
USG9500	V500R005C20SPC500 and later version	• Windows • Linux • Mac OS
USG6000E	V600R007C20SPC300 and later version (except SPC301/SPC302)	• Windows • Linux • Mac OS
Eudemon200E-N	V500R005C20SPC500 and later version	• Windows • Linux • Mac OS
Eudemon200E-G	V600R007C20SPC300 and later version (except SPC301/SPC302)	• Windows • Linux • Mac OS
Eudemon1000E-N	V500R005C20SPC500 and later version	• Windows • Linux • Mac OS
Eudemon1000E-G	V600R007C20SPC300 and later version (except SPC301/SPC302)	• Windows • Linux • Mac OS
Eudemon8000E-	V500R005C20SPC500 and later	• Windows

Product Name	Version	Operating System
X	version	• Linux • Mac OS
SeMG9811	V500R005C20SPC500 and later version	• Windows • Linux • Mac OS
NGFW Module	V500R005C20SPC500 and later version	• Windows • Linux • Mac OS
USG12000	V600R021C10 and later version	• Windows • Linux • Mac OS
USG6000F	V600R021C10 and later version	• Windows • Linux • Mac OS
Eudemon9000E-X	V600R021C10 and later version	• Windows • Linux • Mac OS
Eudemon9000E-F	V600R021C10 and later version	• Windows • Linux • Mac OS
Eudemon1000E-F	V600R021C10 and later version	• Windows • Linux • Mac OS

Operating system version supported by UniVPN client

Client	Operating System
UniVPN-10781.9	• New support system for univpn client: Ubuntu 22.04.
UniVPN-10781.8	• New support system for univpn client: MacOS Ventura 13.
UniVPN-10781.7	• UniVPN clients no longer support OS X 10.12.x version systems since version 10781.7.0.1025.
UniVPN-10781.3	• New support system for univpn client: windows11.
UniVPN-10781.2	• Windows: 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 R2（32-bit/64-bit） Windows Server 2012（64-bit） • Linux: Ubuntu 20.04 • Mac OS: OS X 10.11.x OS X 10.12.x OS X 10.13.x OS X 10.14.x OS X 10.15.x MacOS 11.x.x MacOS 12.x.x

Specifications

Table 3-1 lists the function specifications of the UniVPN.

Table 3-1 Function specifications of the UniVPN

Function		Windows Operating System	Linux Operating System	Mac Operating System
SSL VPN	Network extension	Supported	Supported	Supported
	Endpoint security	Supported	Supported **NOTE** Only host firewall check, host operating system check, host port check, host process check, host files check, anti-nested	Not supported

Function		Windows Operating System	Linux Operating System	Mac Operating System
			remote desktop connection, and anti-printscreen are supported.	
	Preferential gateway selection	Supported	Supported	Supported
	Reconnection	Supported	Supported	Supported
	Link backup	Supported	Supported	Supported
	Route overwrite	Supported	Not supported	Supported
	Chinese cryptographic algorithm	Supported	Supported	Supported
	Certificate authentication	Supported	Supported **NOTE** SSL VPN connections that are configured and established using commands support only user name and password authentication.	Supported
	MAC Address Authenticatio n	Supported	Supported	Supported
	Certificate filtering	Supported	Supported	Supported
	Two-factor authentication	Supported token code+SMS verification code two-factor authentication.	Supported	Supported token code+SMS verification code two-factor authentication.
L2TP VPN		Supported	Supported	Supported
L2TP over IPSec VPN		Supported **NOTE** L2TP over IPSec supports user name and password authentication, and USB key authentication. The prerequisite for L2TP over IPSec to	Supported **NOTE** L2TP over IPSec supports only user name and password authentication but not USB key authentication.	Supported **NOTE** L2TP over IPSec supports only user name and password authentication but not USB key authentication.

Function		Windows Operating System	Linux Operating System	Mac Operating System
		support USB key authentication is that the corresponding USB key can be identified by the OS.		
NAT traversal		Supported In proxy traversal scenarios, IPSec does not support the tunnel mode.	Supported In proxy traversal scenarios, IPSec does not support the tunnel mode.	Supported In proxy traversal scenarios, IPSec does not support the tunnel mode.
Proxy traversal		Supported In proxy traversal scenarios, IPSec does not support the tunnel mode.	Supported In proxy traversal scenarios, IPSec does not support the tunnel mode.	Supported In proxy traversal scenarios, IPSec does not support the tunnel mode.
Tunnel splitting		Supported	Supported	Supported
Basic functions	Automatic startup upon power-on	Supported	Supported	Supported
	Language	Supported	Supported	Supported
	Automatic login	Supported	Supported	Supported
Profile	Import	Supported	Supported	Supported
	Export	Supported	Supported	Supported
Fault location		Supported	Not supported	Supported
Configuration using commands		Not supported	Supported	Not supported
Non-administrator user configuration		Supported	Supported	Supported

Table 3-2 lists the performance specifications of the UniVPN.

Table 3-2 Performance specifications of the UniVPN

Function	Specifications
Number of new VPN connections per second	16
Number of preferential VPN gateways	16

Table 3-3 lists specifications of USB-Key products supported by the UniVPN through validation.

Table 3-3 Specifications of USB-Key products supported by the UniVPN

Vendor	Model
Haitai Fangyuan	HaiKey3000 Series
FEITIAN	ePass3000 Series

Table 3-4 lists the support for USB key certificate authentication in different OSs and VPN types.

Table 3-4 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
L2TP VPN	N	N	N
L2TP over IPSec VPN	Y	N	N

Restrictions

The UniVPN cannot be used on IPv6 networks, including IPv6-and-IPv4 hybrid networks.

4 Installation and Uninstallation

This section describes how to install and uninstall the UniVPN.

You usually have two ways to install the UniVPN.

- When the number of users is small, manually install the UniVPN on the hosts one by one.
- If the number of users is large, use the AD server to deliver software installation packages to user hosts in batches for automatic installation.

4.1 Installing and Uninstalling the UniVPN in the Windows Operating System

This section describes how to install and uninstall the UniVPN in the Windows operating system.

4.2 Installing and Uninstalling the UniVPN in the Linux Operating System

This section describes how to install and uninstall the UniVPN in the Linux operating system.

4.3 Manually Installing the UniVPN on a Mac Operating System

This section describes how to install and uninstall the UniVPN in the Mac operating system.

4.4 Distributing the UniVPN Installation Package and Automatically Installing the UniVPN Through the AD Server

This section describes how to use the AD server to distribute UniVPN installation packages in batches and install the UniVPN for automatic deployment, which improves the enterprise network maintenance efficiency.

4.1 Installing and Uninstalling the UniVPN in the Windows Operating System

This section describes how to install and uninstall the UniVPN in the Windows operating system.

Before You Start

- Different UniVPN software installation packages are available for 32-bit and 64-bit Windows operating systems. Select the correct software installation package based on the operating system.

- The UniVPN supports the following versions of the Windows operating system:
  - Windows 7 (32-bit and 64-bit)
  - Windows 8 (32-bit and 64-bit)
  - Windows 8.1 (32-bit and 64-bit)
  - Windows 10 (32-bit and 64-bit)
  - Windows Server 2008 R2 (32-bit and 64-bit)
  - Windows Server 2012 (64-bit)
  - Windows 11
- The UniVPN does not have special requirements on the software or hardware resources of the operating system, such as on the memory, hard disk, or CPU.

Installation Method

The methods for installing the UniVPN in the 32-bit and 64-bit Windows operating systems are the same. This section uses the 64-bit operating system as an example.

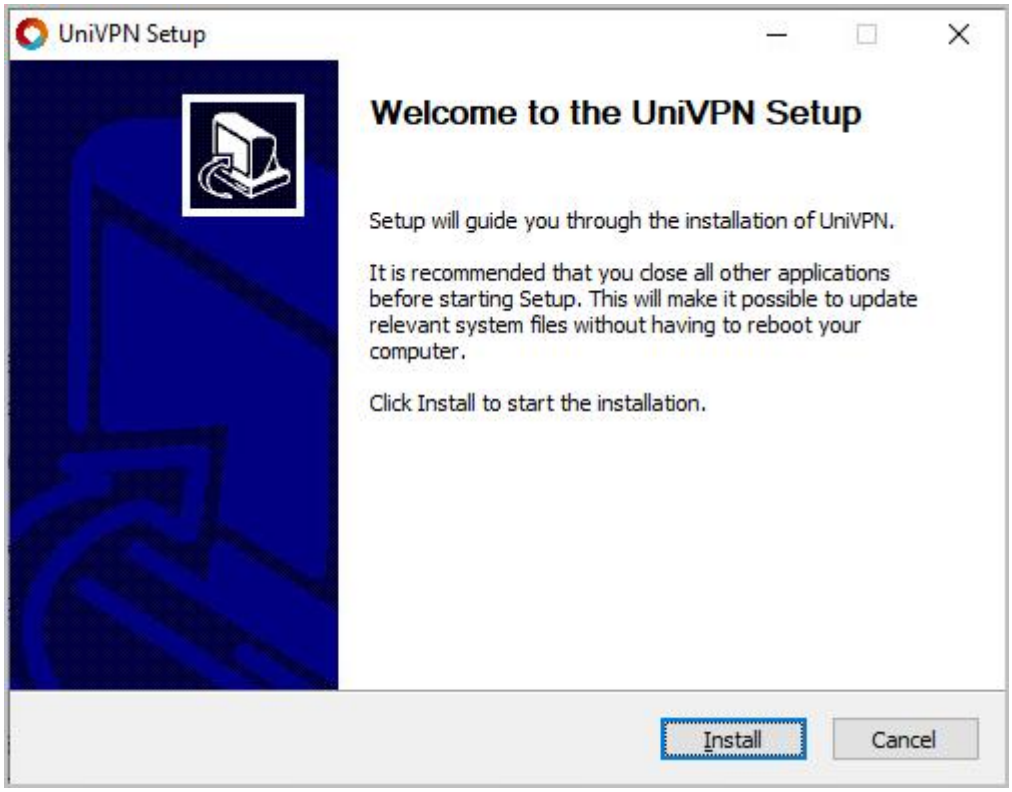
Step 1 Log in to the Windows operating system as the administrator.

Step 2 Download the correct software installation package.

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.

Step 3 Double-click the downloaded installation package. On the installation page that is displayed, click **Install**. The UniVPN client is then automatically installed.

The system automatically installs the UniVPN software. By default, the UniVPN software is installed in the system disk. For example, if the system is installed in drive C, the default UniVPN installation path is **C:\Program Files (x86)\UniVPN.**



NOTE

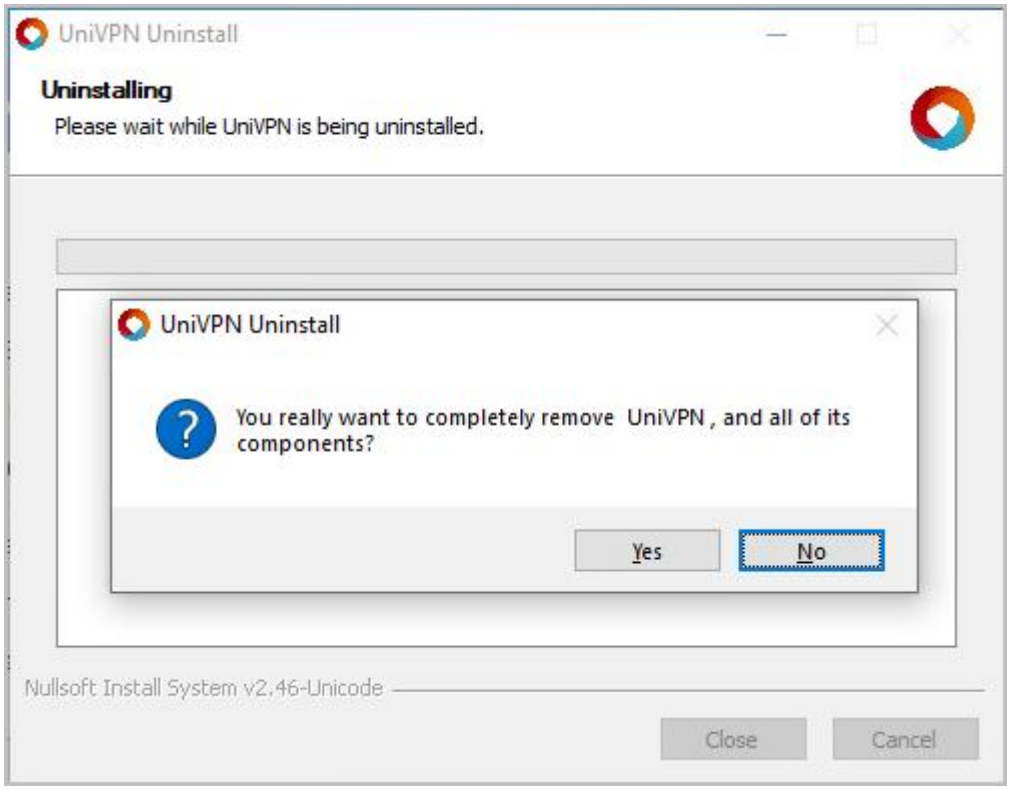
When the operating system language is Chinese (Simplified or Traditional), the installation wizard language is Simplified Chinese by default. Otherwise, the installation wizard language is English by default.

----End

Uninstallation Method

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

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



----End

4.2 Installing and Uninstalling the UniVPN in the Linux Operating System

This section describes how to install and uninstall the UniVPN in the Linux operating system.

Installation Precautions

- The UniVPN supports only 64-bit Linux operating systems.
- The UniVPN supports the following Linux operating system versions:
  - Ubuntu 20.04
  - Ubuntu 22.04
- The UniVPN has no special requirements for software and hardware resources such as memory, hard disk, and CPU resources of the OS.

Installation Method

The following uses Ubuntu 20.04 as an example to describe how to install the UniVPN.

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

Step 2 When the network connection is successful, open the browser and download the software installation package of the required version.

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.

Step 3 Save the downloaded installation package to the main folder (**Computer** > **home** > **UniVPN**).

Step 4 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
/
UniVPNA.sh
install.sh
uninstall.sh
sysconfig.ini
qt.conf
bak/
component/
config/
driver/
image/
language/
help/
lib/
log/
plugins/
plugins/platforms/
serviceclient/
update/
UniVPN
UniVPNUpdate
```

Step 5 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 6 Click the UniVPN icon on the desktop to start the program.

----End

Uninstallation Method

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

Step 2 Start the **Terminal** and access the **/usr/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@zzh-virtual-machine:/usr/local/UniVPN# ./uninstall.sh
Stopping UniVPNPromoteService daemon: ./uninstall.sh: line 19: 222576 killed
sh UniVPNPromoteService.sh stop
```

----End

4.3 Manually Installing the UniVPN on a Mac Operating System

This section describes how to install and uninstall the UniVPN on a Mac operating system.

Before You Start

- The UniVPN supports only 64-bit Mac operating systems.
- The UniVPN supports the following Mac operating system versions:
  - OS X 10.11.x
  - OS X 10.12.x
  - OS X 10.13.x
  - OS X 10.14.x
  - OS X 10.15.x
  - Mac OS 11.x.x
  - Mac OS 12.x.x
  - Mac OS 13.x.x
- The UniVPN has no special requirements on software and hardware resources (such as memory, hard disk, and CPU) of Mac devices.

NOTE

UniVPN clients no longer support OS X 10.12.x version systems since version 10781.7.0.1025.

Installation Method

The following uses Mac OS 11.5 as an example to describe how to install the UniVPN.

Step 1 Log in to the Mac operating system.

Step 2 When the network connection is successful, open a browser and download the software installation package of the required version.

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.

Step 3 Double-click the downloaded installation package to run the installation program.

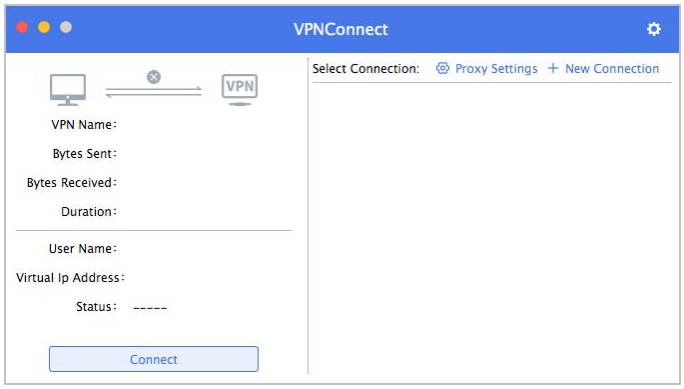
Step 4 Complete the installation as prompted by the installation program.

1. On the **Introduction** page, click **Continue**.

   You can configure the UI language of the installation program on the software introduction page, which can be simplified Chinese or English. By default, the UI language is the same as the system language by default. For systems whose language is not Chinese or English, the default UI language is English.
2. Click **Install**. The software is installed in a fixed path, which cannot be manually changed.
3. Enter the user name **root** and the corresponding password. After authentication is successful, click **Install Software**. Your permission may be authenticated here, and the installation continues only after the authentication succeeds. Only users with the root permission can install this software.
4. Click **Close**.

Step 5 After the installation is complete, you can find the application in the application folder.

Step 6 Double-click **UnIVPN** to start the program.



----End

Uninstallation Method

Step 1 Double-click **UniVPNUninstaller** in the application folder.

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

----End

4.4 Distributing the UniVPN Installation Package and Automatically Installing the UniVPN Through the AD Server

This section describes how to use the AD server to distribute UniVPN installation packages in batches and install the UniVPN for automatic deployment, which improves the enterprise network maintenance efficiency.

The AD server distributes UniVPN software installation packages to terminal user hosts. When a user attempts to log in to a host, the UniVPN starts silent installation. After the user logs in, the user can directly use the UniVPN. In this example, the AD server has Windows Server 2008 installed, and the user host has Windows 7 installed.

NOTE

Batch installation through the AD server is supported only by Windows hosts.

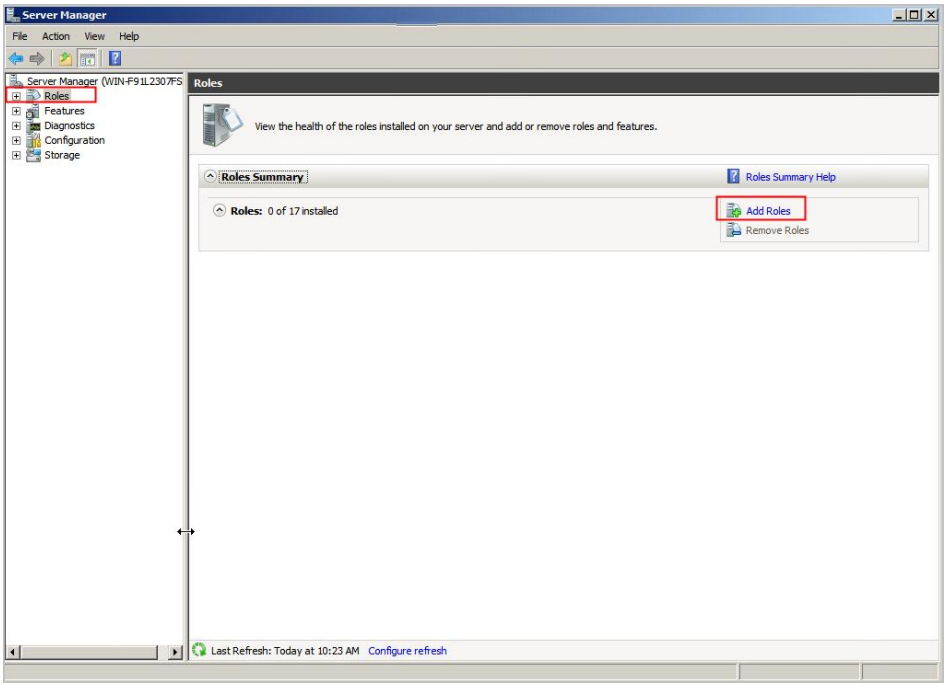
4.4.1 (Optional) Creating an Active Directory Domain and Domain User

This section describes how to distribute Active Directory domain and domain.

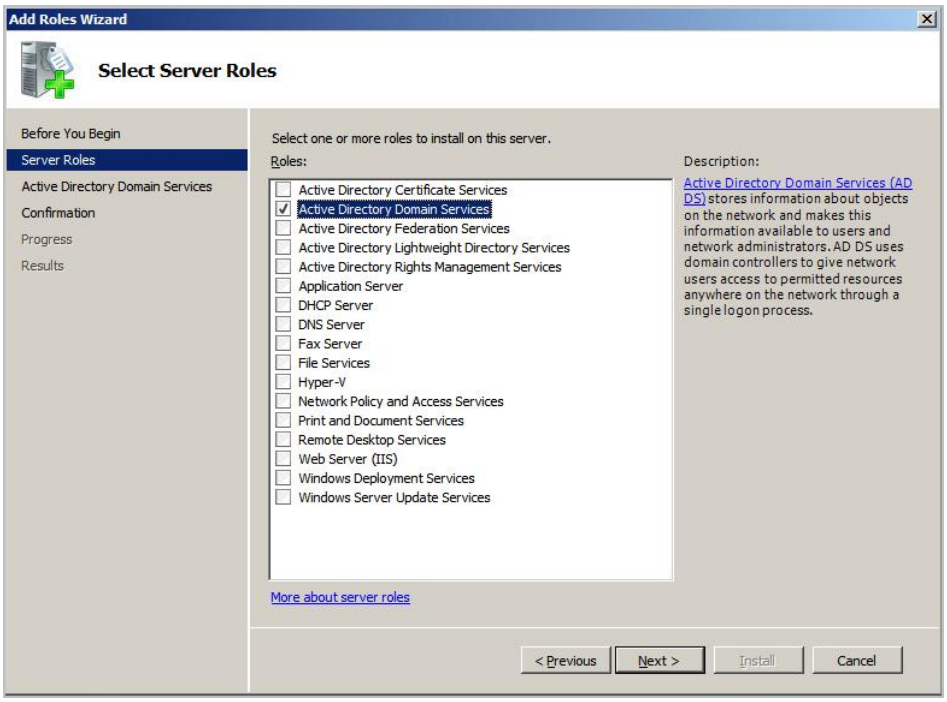
Procedure

Step 1 Create an Active Directory domain server rule.

1. Choose **Administrative Tools > Server Manager** in **Start** menu.
2. In **Server Manager**, select **Add Roles**.

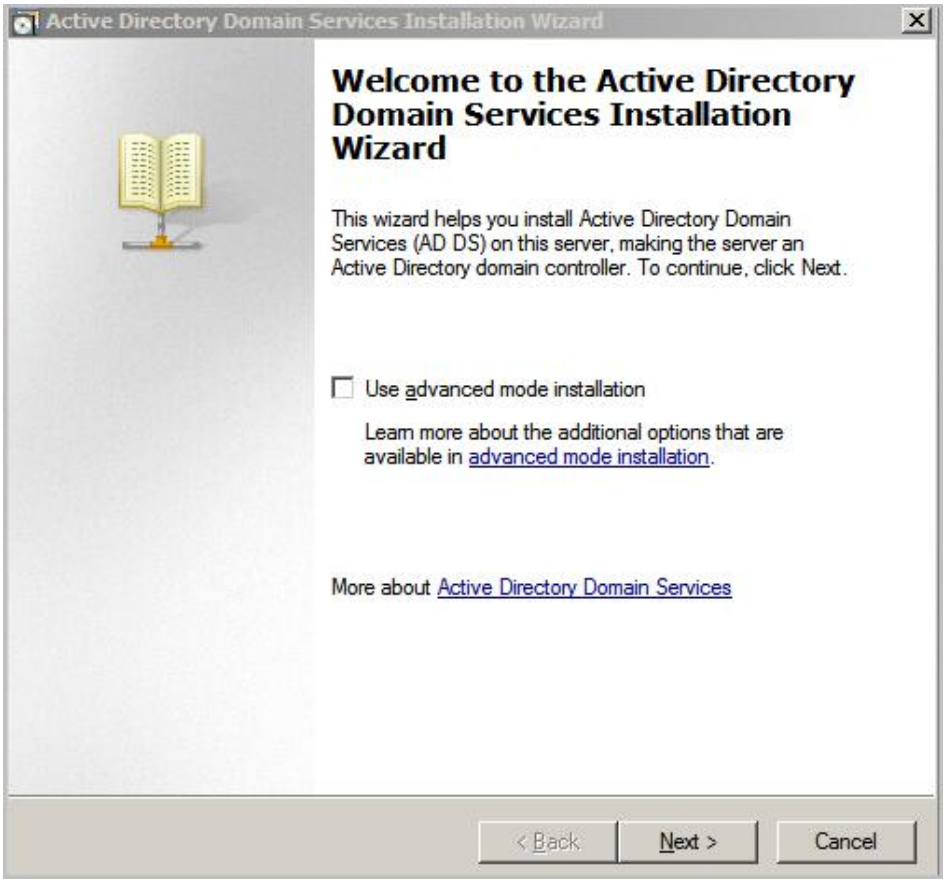


3. Select **Active Directory Domain Services** and click **Next** until the installation is complete.

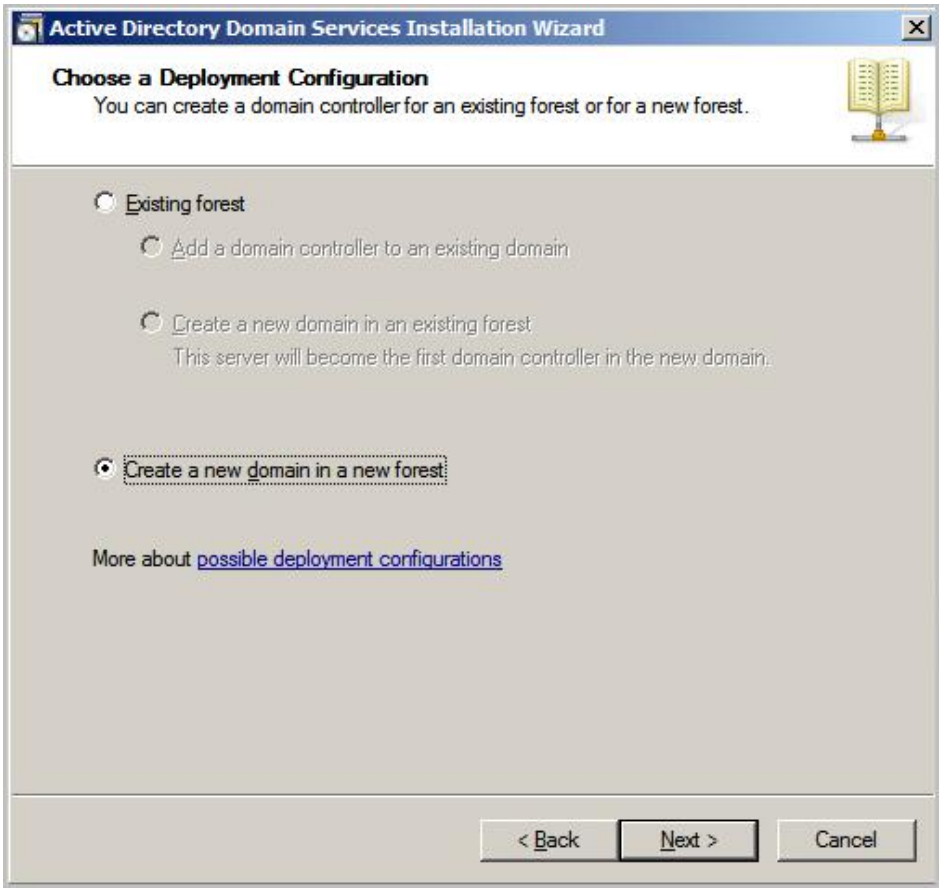


Step 2 Create an Active Directory domain service.

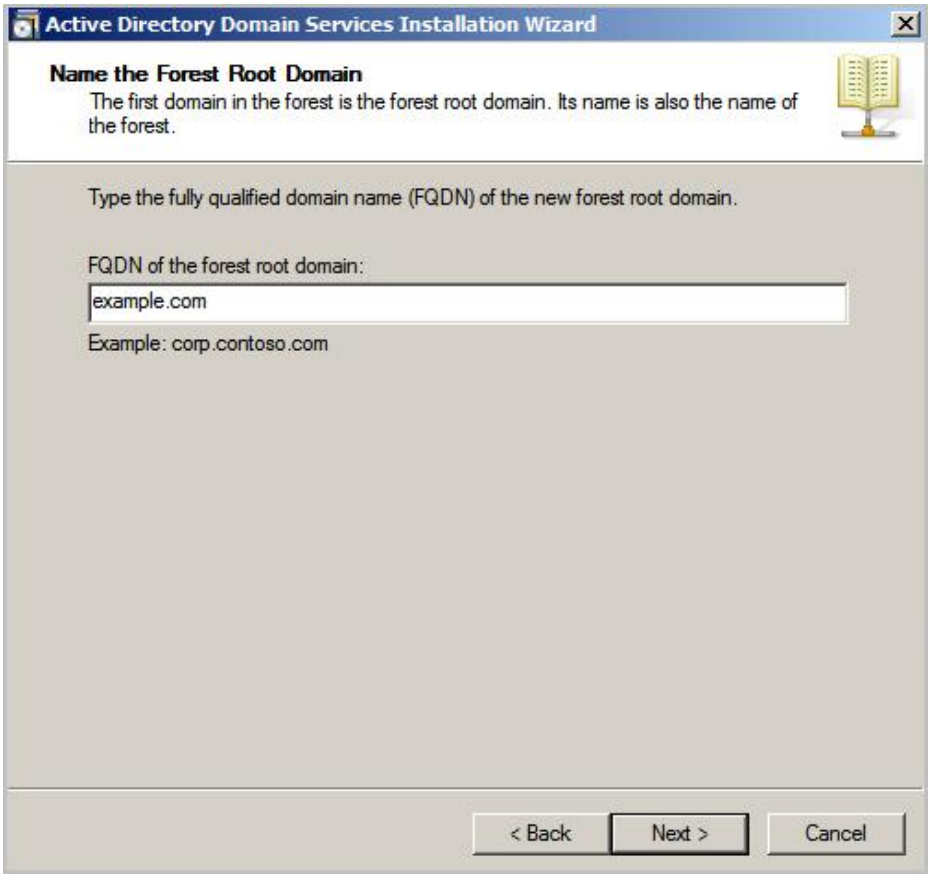
1. Choose **Start > Run**. On the CLI, enter **dcpromo** to display the installation wizard, click **Next**.



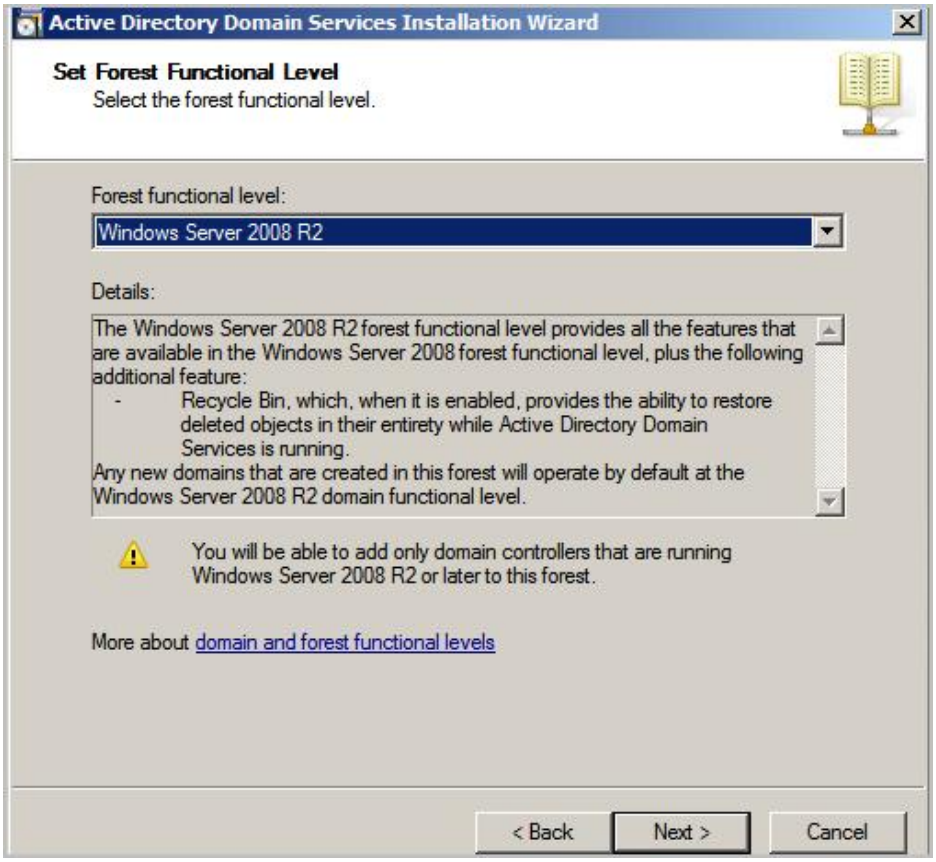
2. Select **Create a new domain in a new forest**, click **Next**.



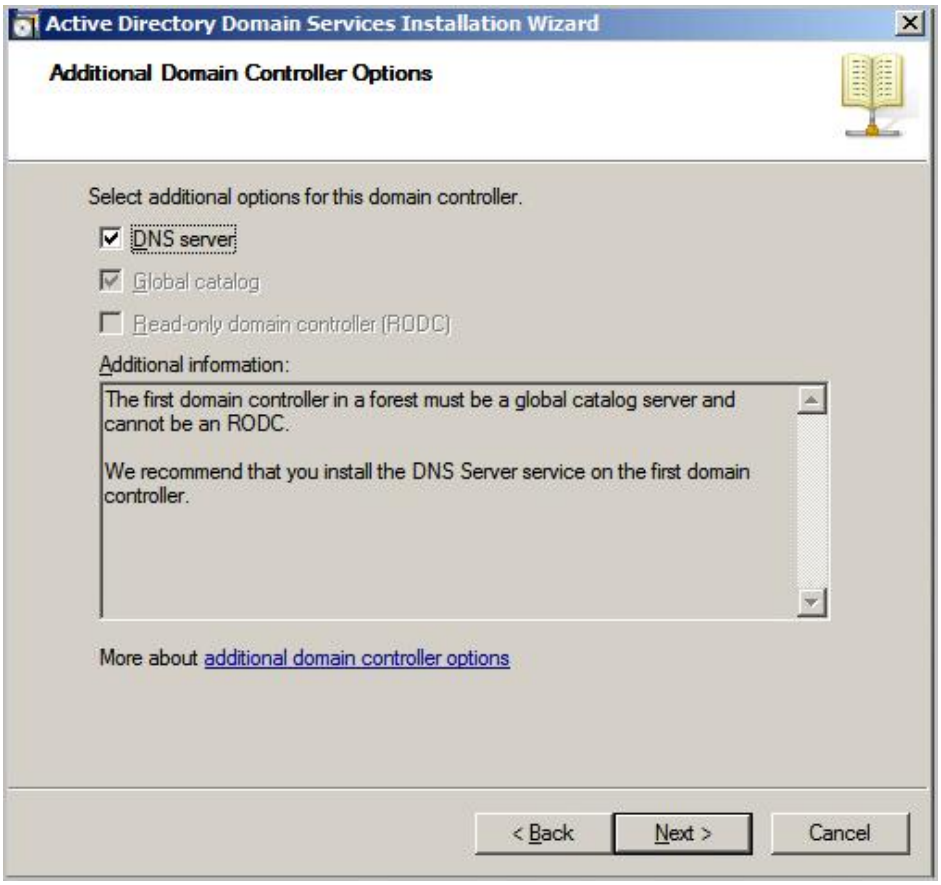
3. Enter the FQDN of the forest root domain, click **Next**.



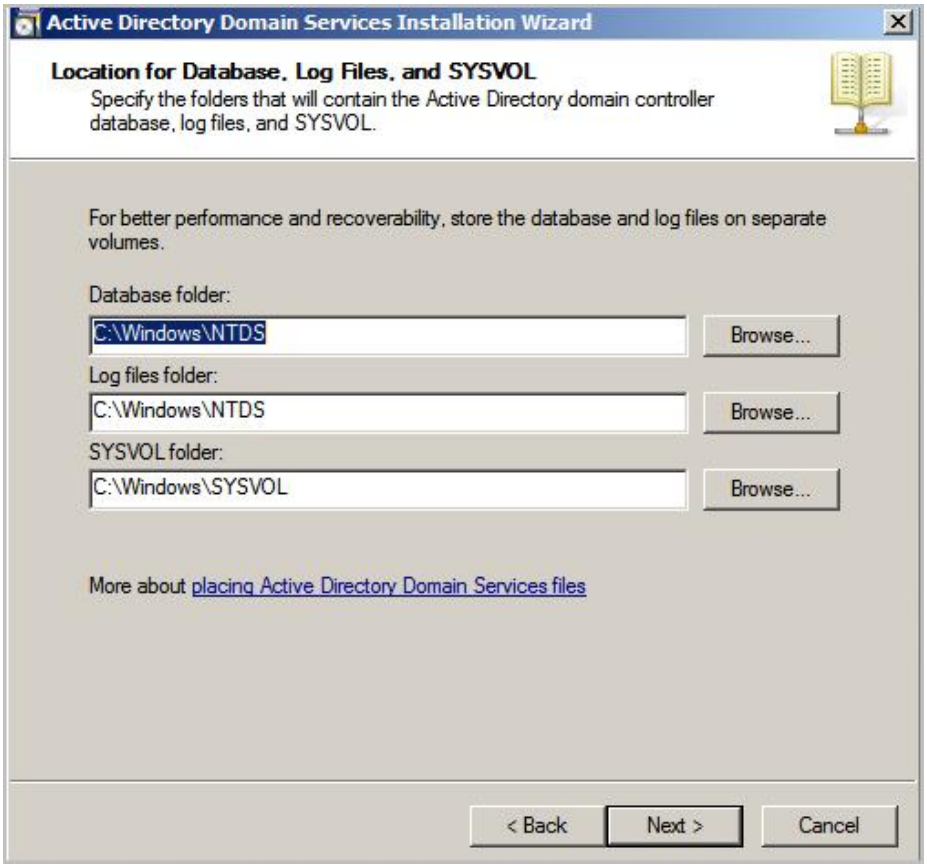
4. Set the forest function level, click **Next**.



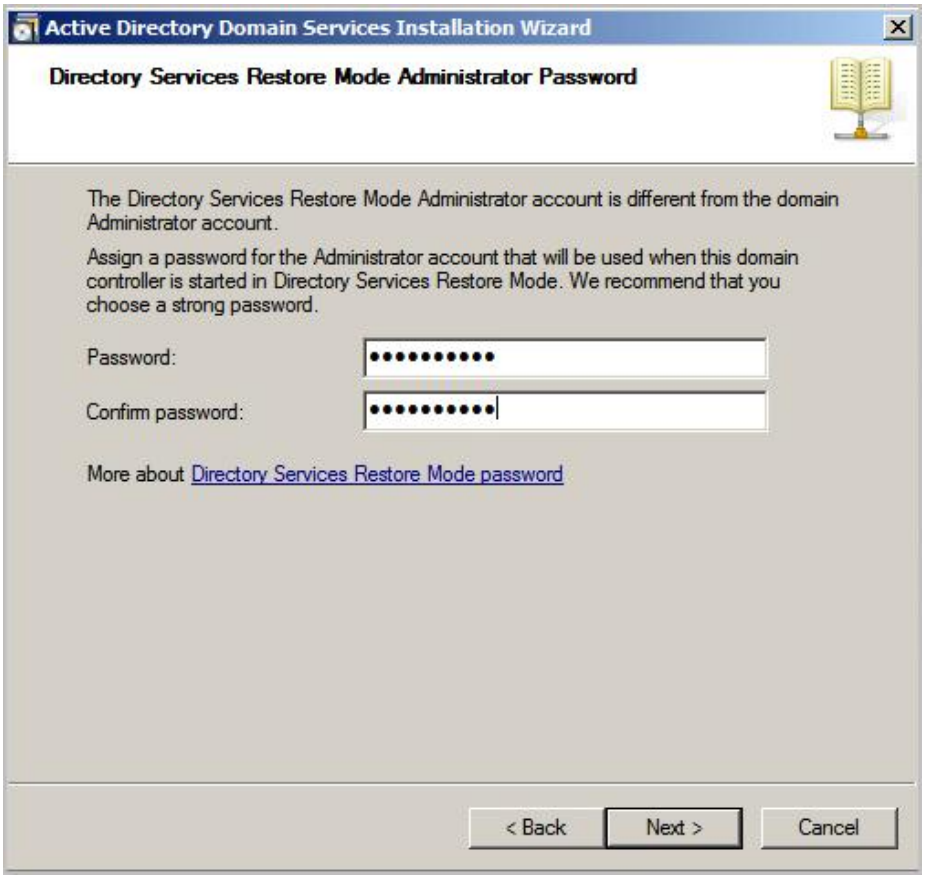
5. If the DNS server function is not installed on the server, install the DNS server to use the AD domain function, click **Next**.



6. Specify paths for storing the database, log file, and SYSVOL, click **Next**.

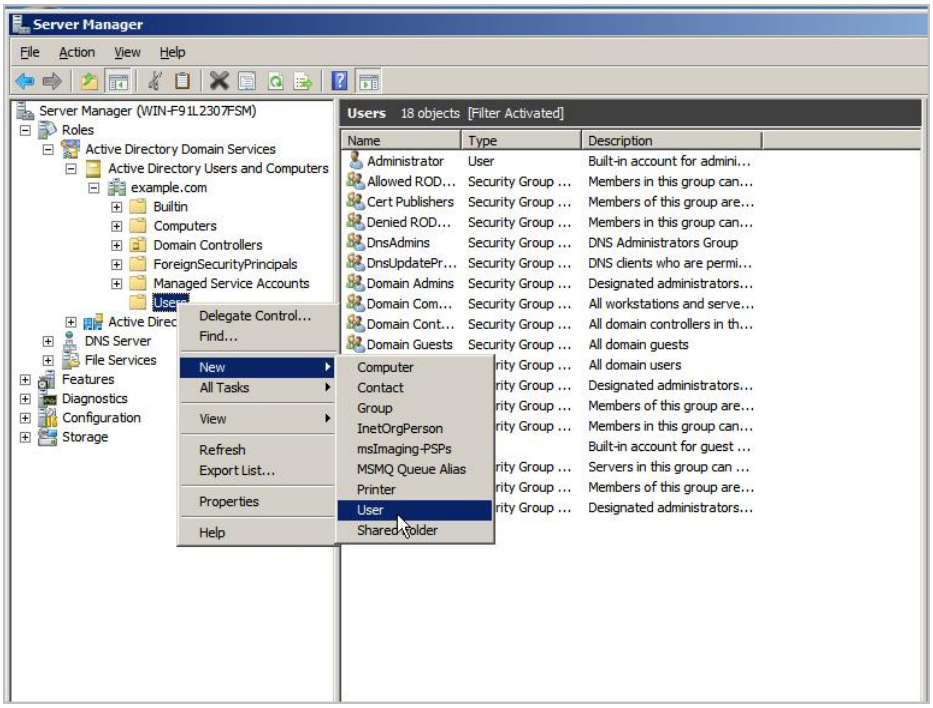


7. Enter the administrator password. Click **Next** until the installation is complete. Restart the operating system.

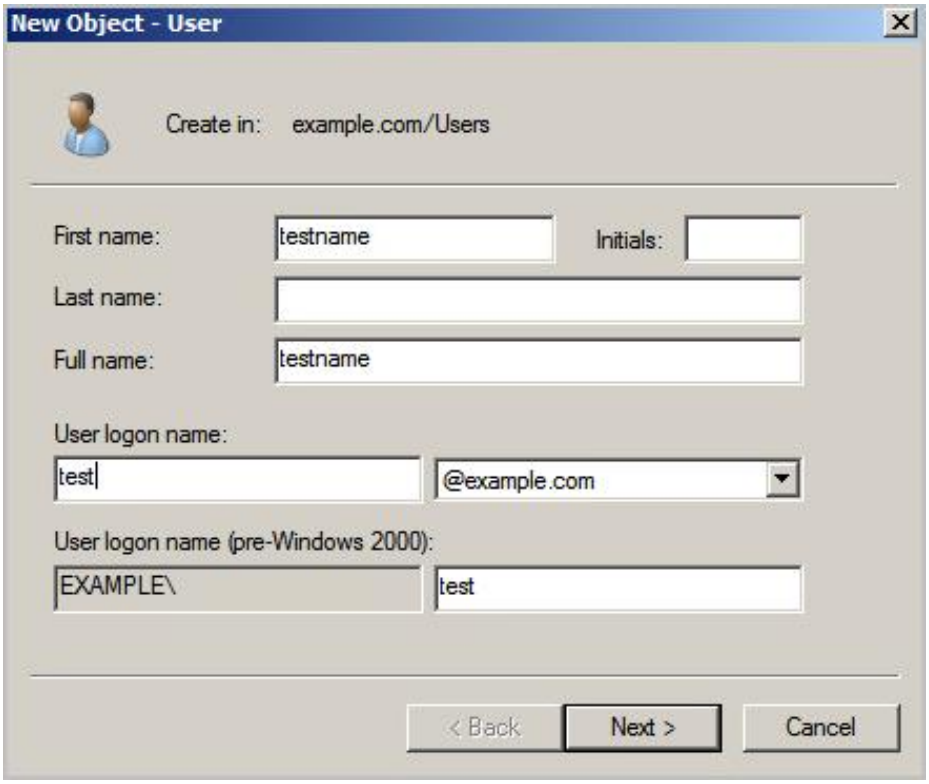


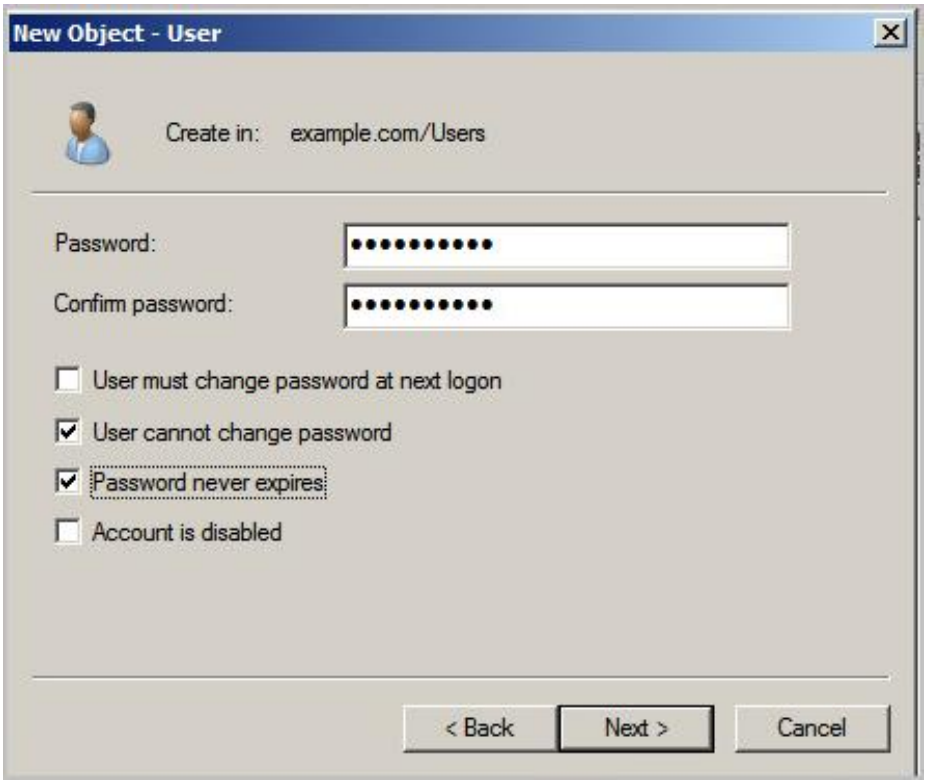
Step 3 Create an Active Directory domain user.

1. In **Server Manager**, choose **Roles > Active Directory Domain Services > Active Directory Users and Computers > example.com**. In **User**, right-click and choose **New > User** from the shortcut menu.

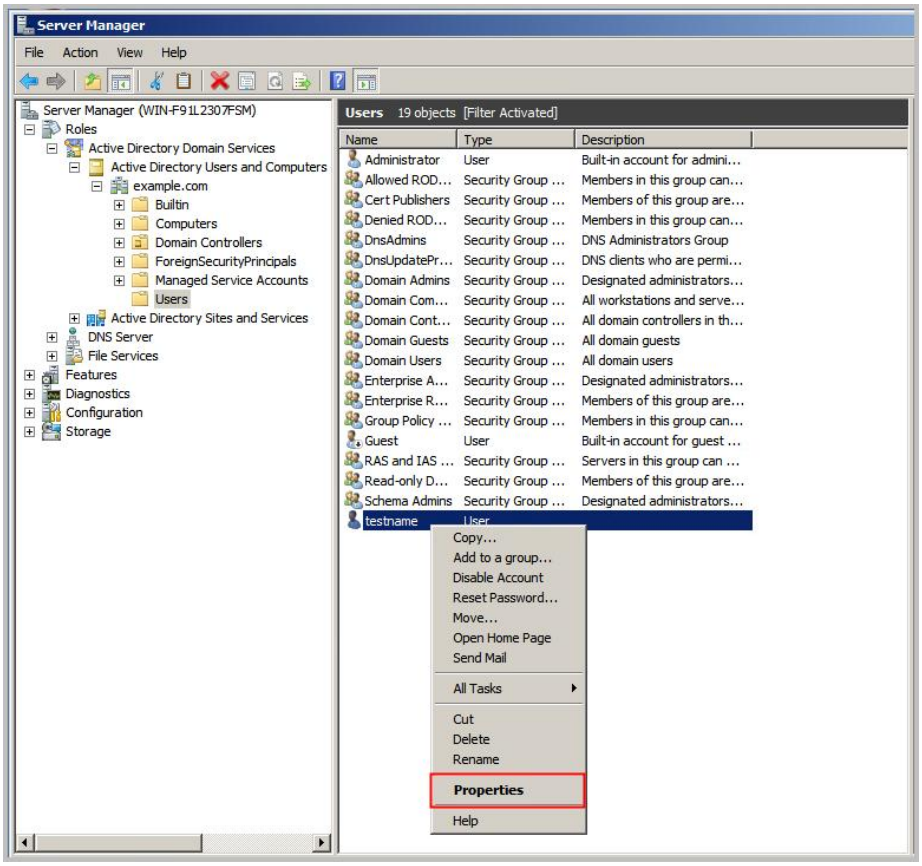


2. Configure the basic user information and login password, click **Next**.

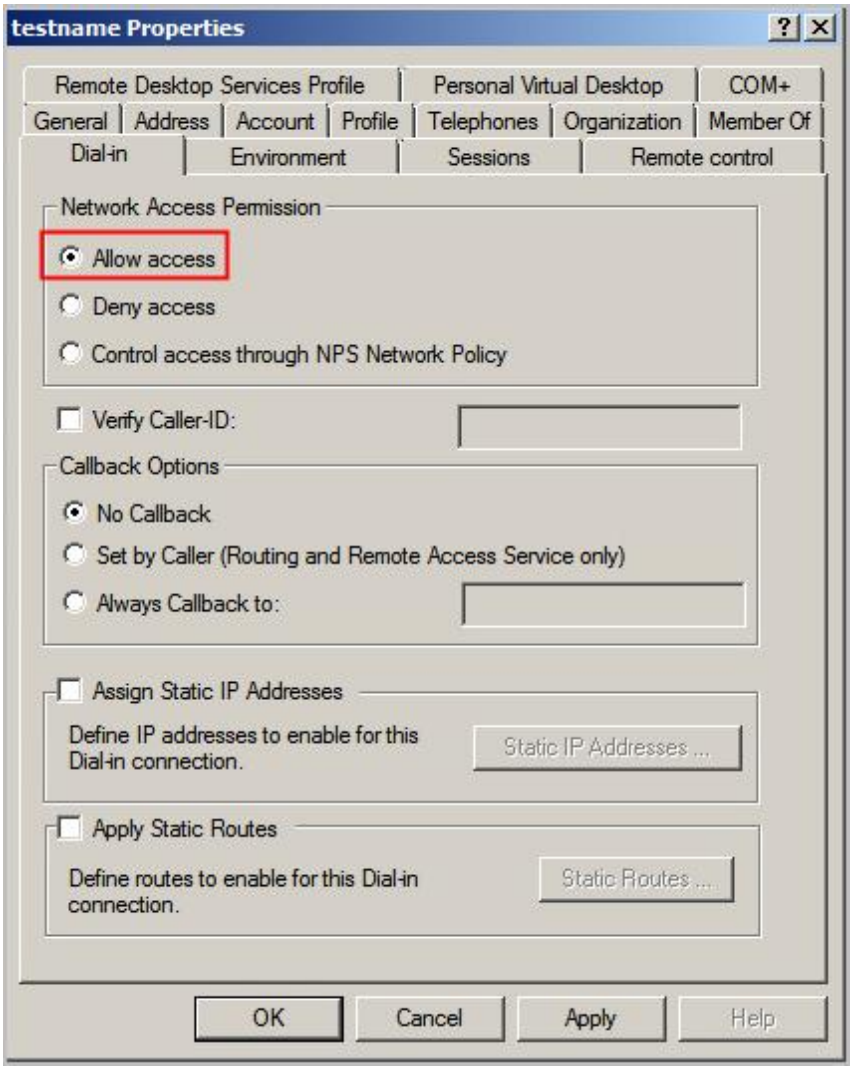




3. Right-click the created user and choose **Property** from the shortcut menu.



4. On the **Dial-in** tab, select **Allow access**, click **OK**.



----End

4.4.2 Converting the Format of an Installation Package from EXE to MSI

This section describes how to use the Advanced Installer to convert the format of a software installation package from EXE to MSI on the AD server.

Procedure

Step 1 Download the UniVPN software installation package to the local AD server.

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.

Step 2 Download the Advanced Installer software to the local AD server, and install and operate it.

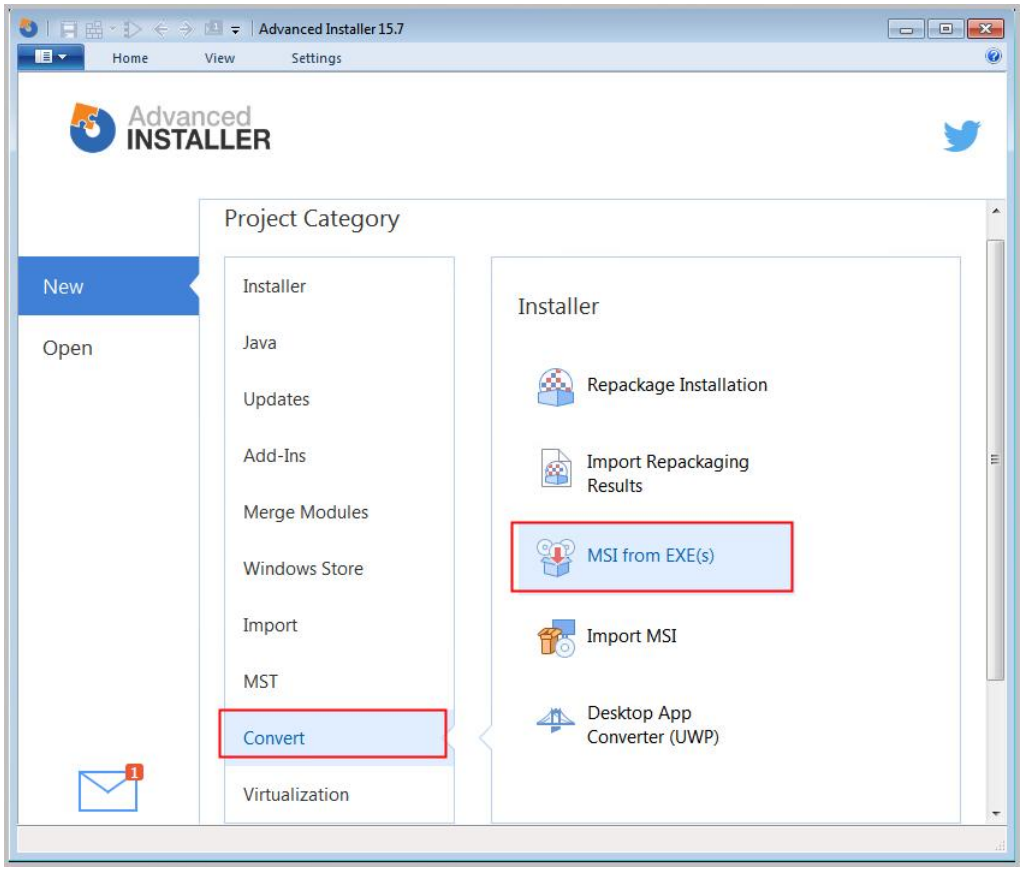
UniVPN software installation packages delivered by the AD server to user hosts in batches are in MSI format. You can use the Advanced Installer software to convert the format of the installation packages from EXE to MSI.

NOTE

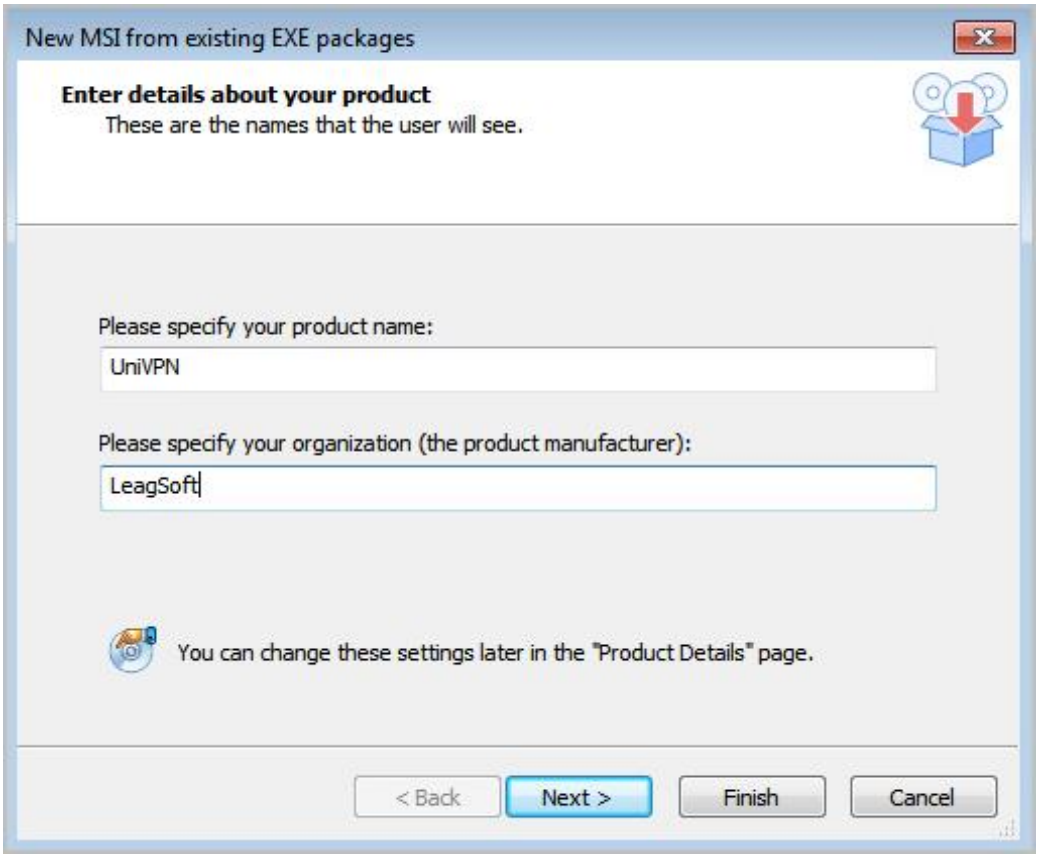
Multiple tools can deliver this function, and the Advanced Installer is described as an example.

Step 3 Create a project on the Advanced Installer.

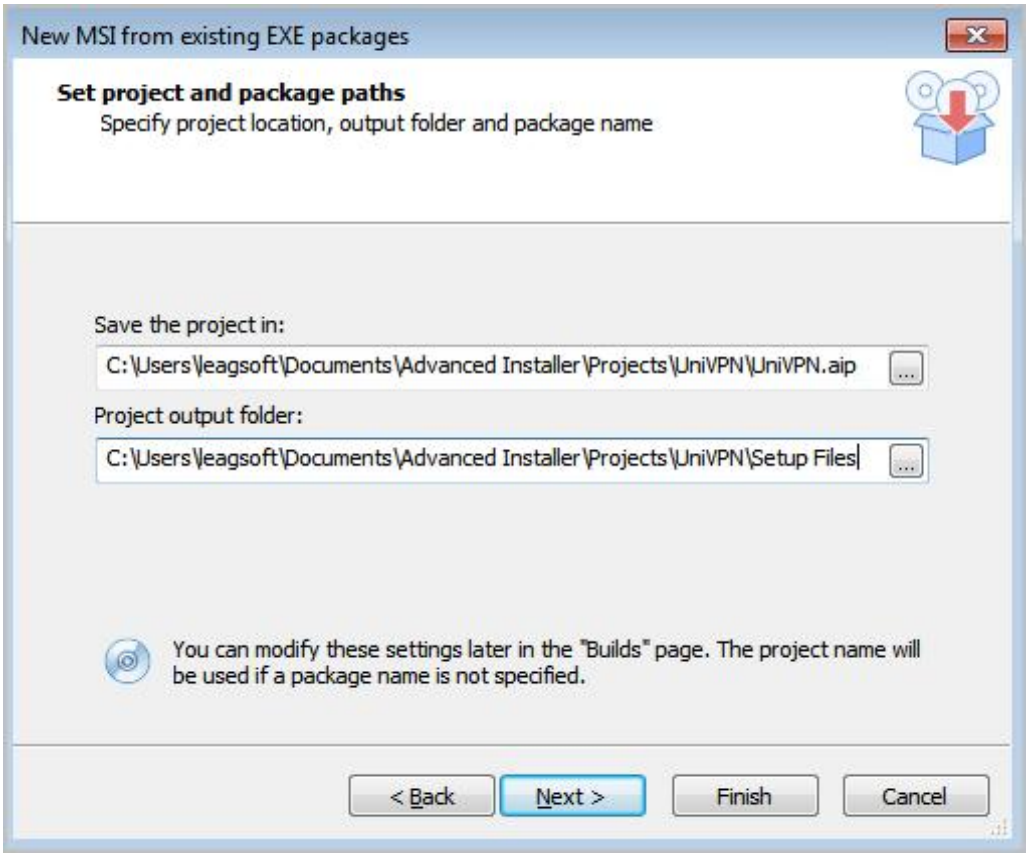
Open the Advanced Installer software, choose **Convert > MSI from EXE**, and click **Create Project**.



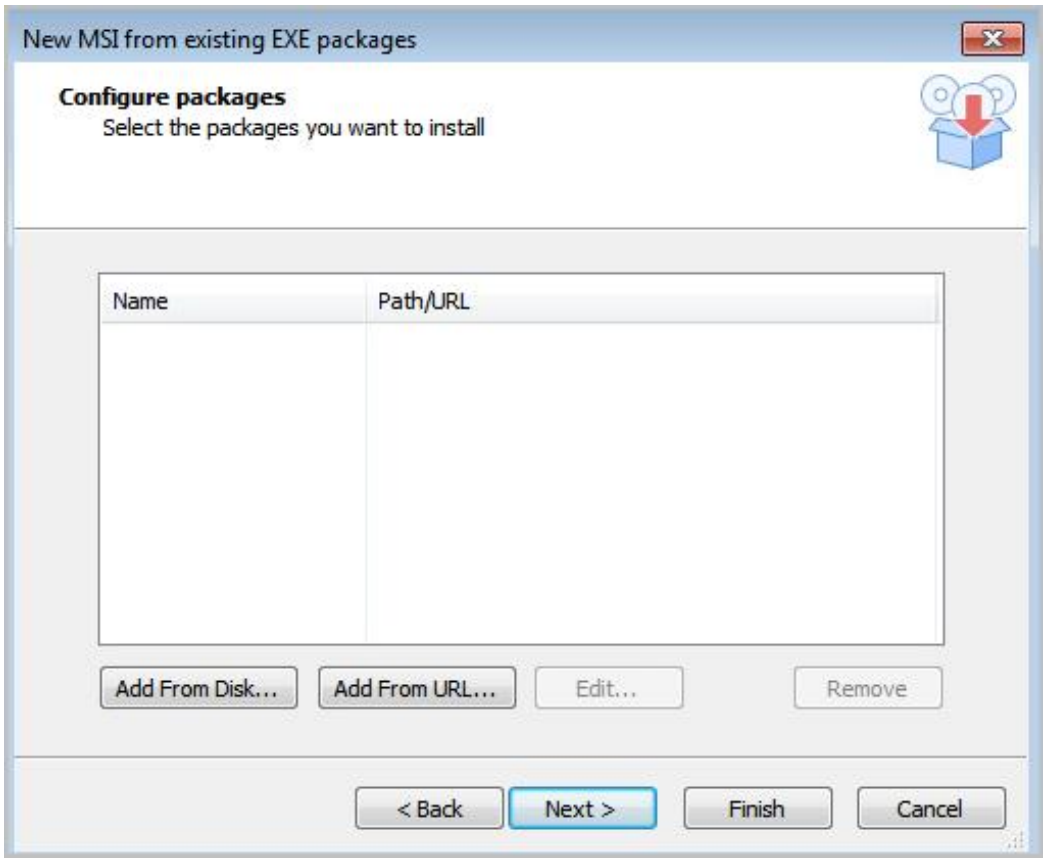
Step 4 Enter the product name and enterprise name in the dialog box displayed and click **Next**.



Step 5 Enter the project name, output path, and installation package name, and click **Next**.



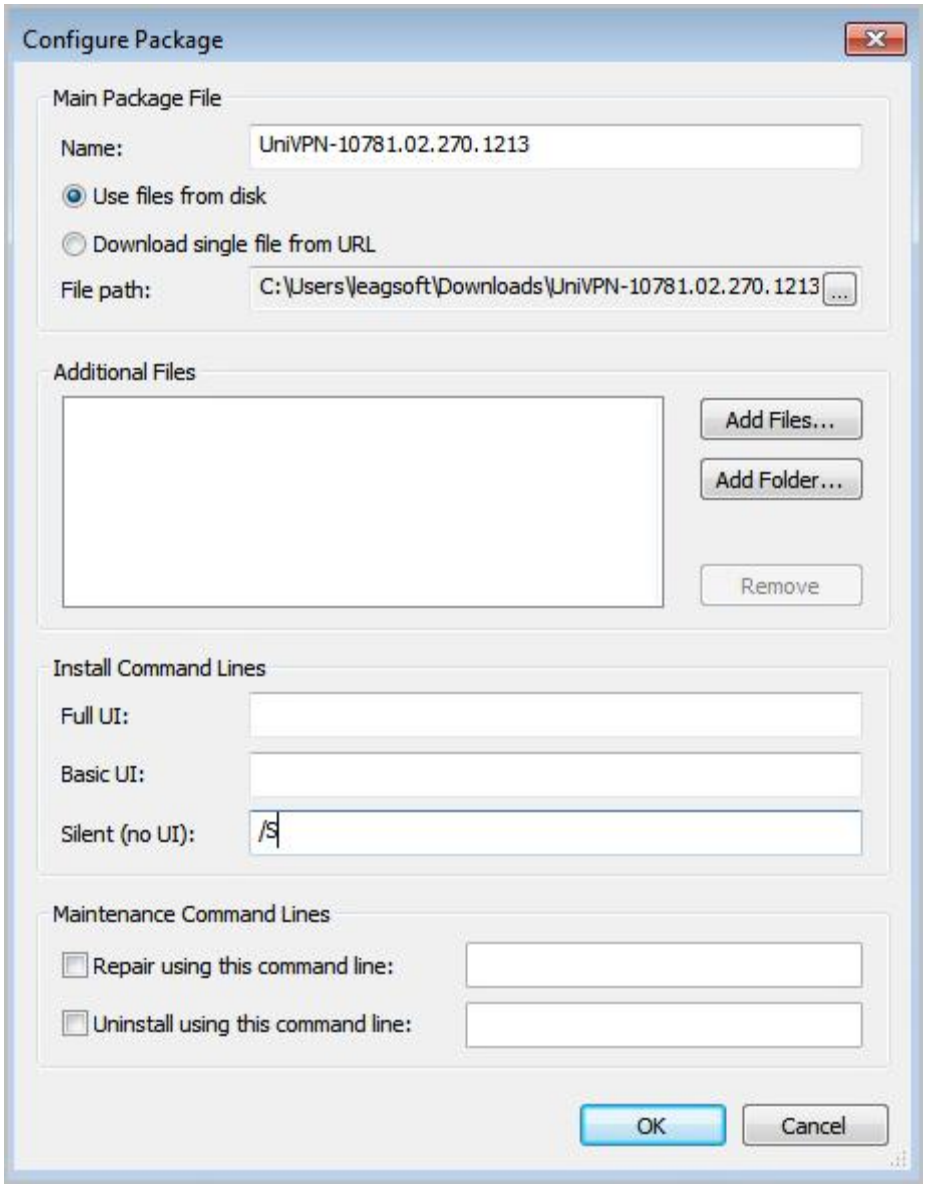
Step 6 Click **Add From Disk**. The system prompts you to select the software installation package for which the format is to be converted.



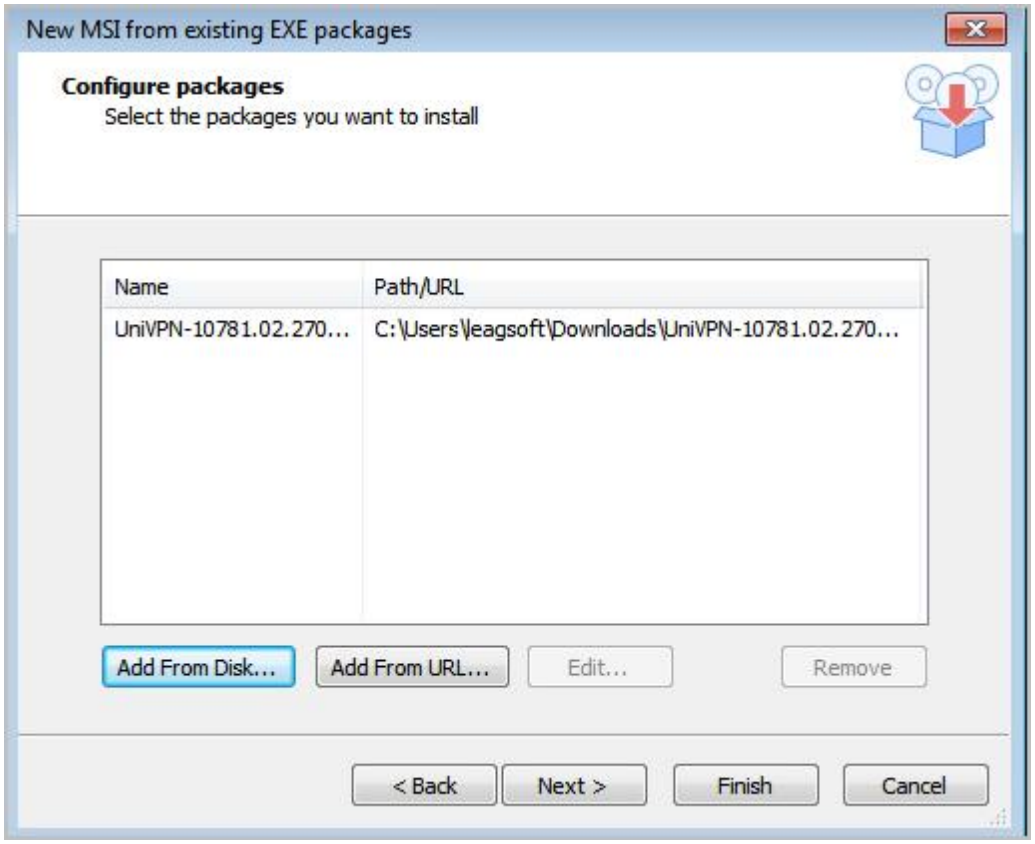
Step 7 Complete settings as follows and click **OK**.

NOTICE

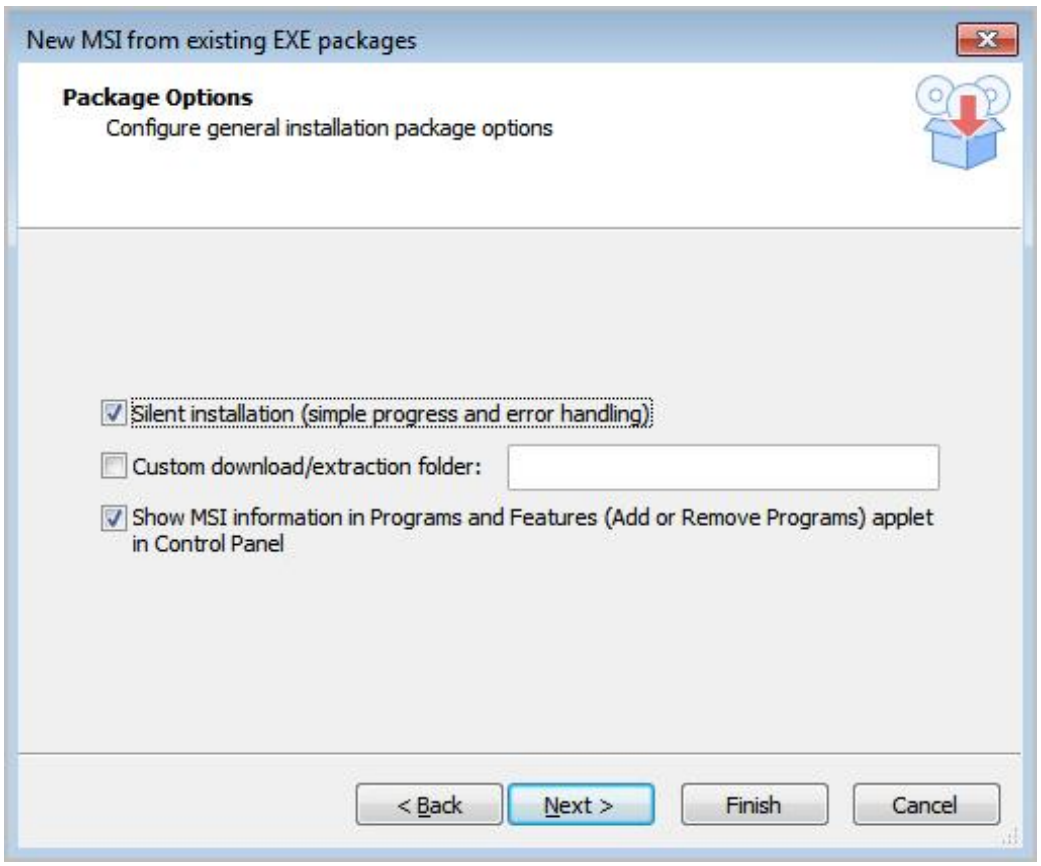
The **S** in **/S** of **Silent (no UI)** must be in upper-case format.



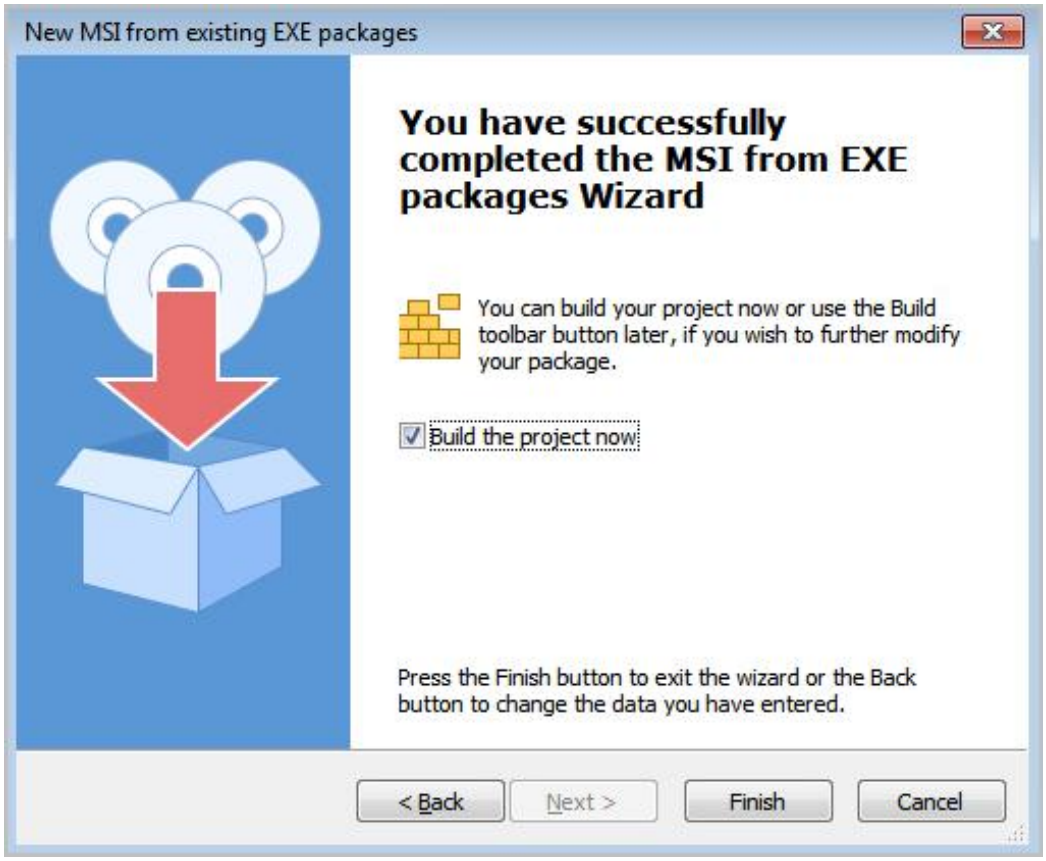
Step 8 Click **Next**.



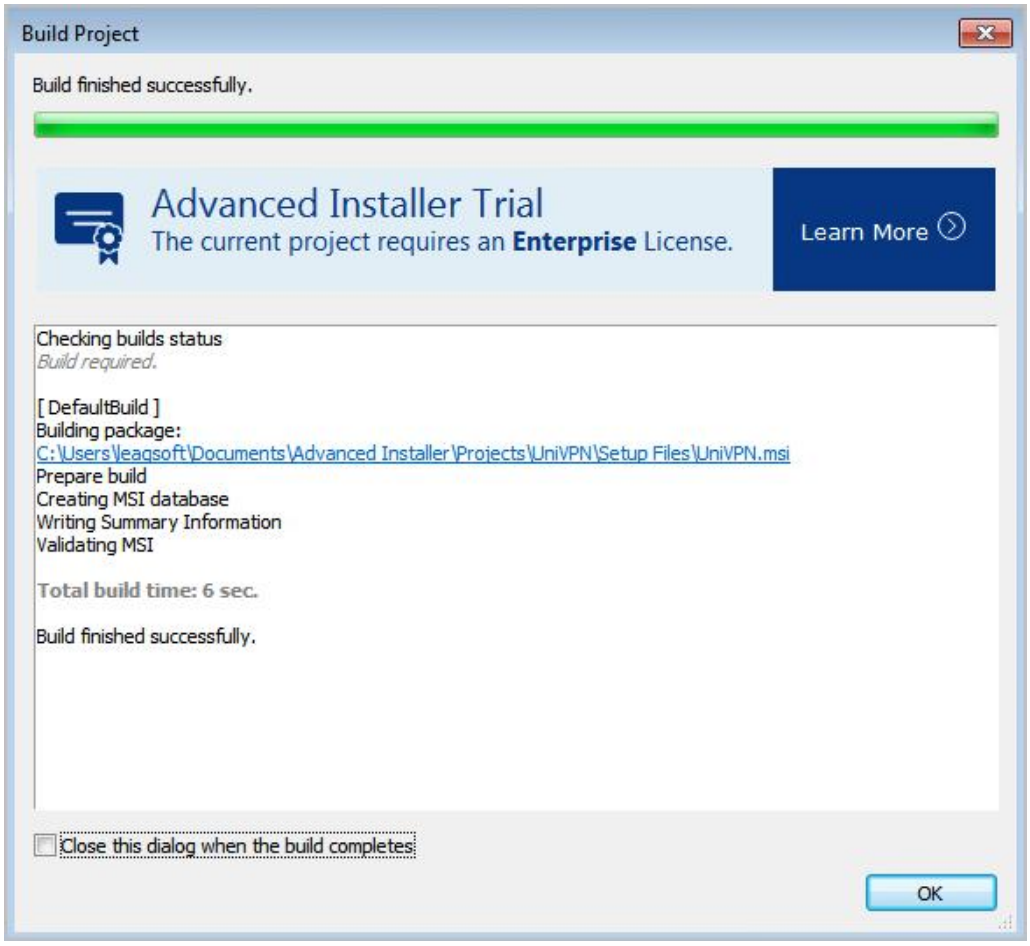
Step 9 Select **Silent installation** and click **Next**.



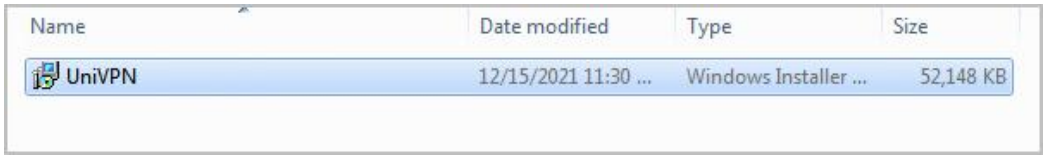
Step 10 Click **Finish**.



Step 11 After the previous step is complete, you need to wait for at least 10 seconds for the system to undergo a compilation process. When the system displays the following information, click **OK**.

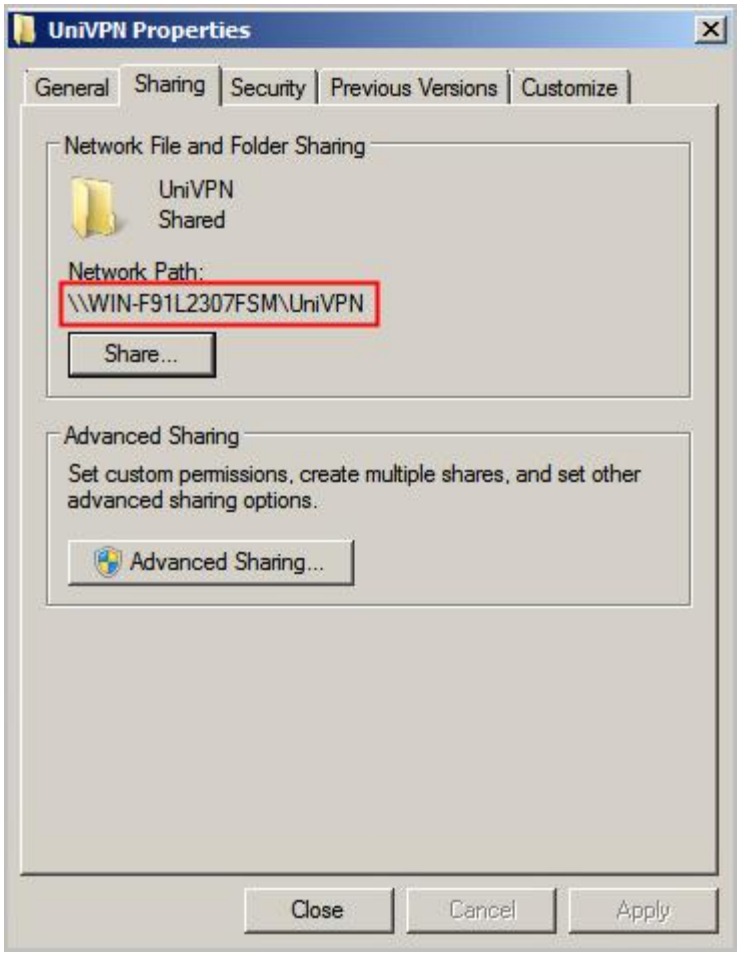


Step 12 Check whether the UniVPN.msi file is generated under the specified project path.



Step 13 Create a shared folder that can be accessed by users in all domains on the AD server and place the UniVPN.msi file in this folder.

In this example, the shared folder is named UniVPN. Right-click the shared folder, select **Properties**, and remember the path of this folder for subsequent operations.


UniVPN Properties
General
Sharing
Security
Previous Versions
Customize
Network File and Folder Sharing
UniVPN
Shared
Network Path:
\\WIN-F91L2307FSM\UniVPN
Share...
Advanced Sharing
Set custom permissions, create multiple shares, and set other advanced sharing options.
Advanced Sharing...
Close
Cancel
Apply

----End

4.4.3 Creating a Software Installation Policy

This section describes how to create a software installation policy on the AD server based on which automatic software installation is performed for users under the domain.

Prerequisite

- Create an Active Directory domain and domain user.

  If the AD domain system has been deployed on the existing network, skip this operation.

  If not, refer to 4.4.1 (Optional) Creating an Active Directory Domain and Domain User to complete the deployment.
- Obtaining the software package in MSI format.

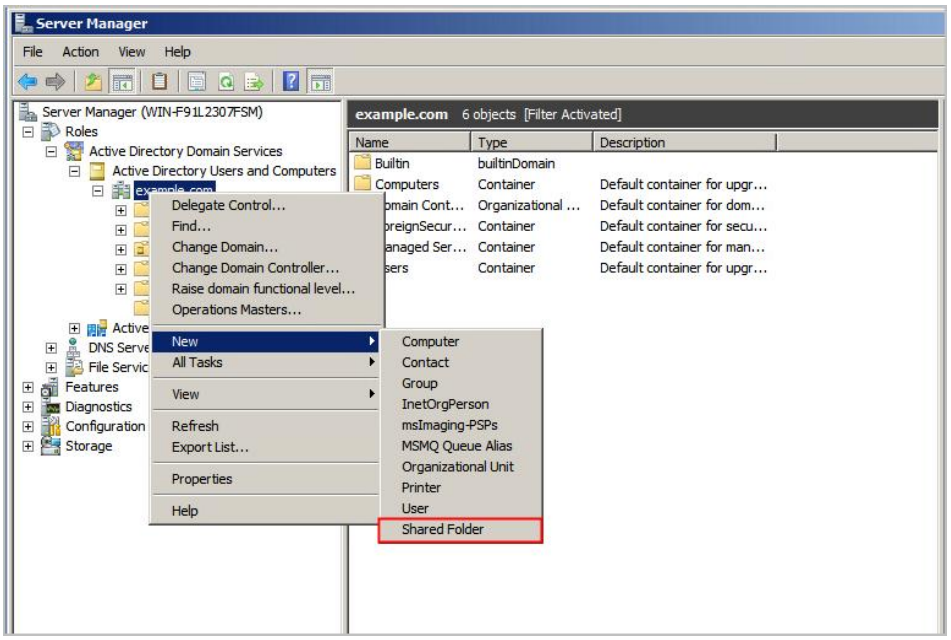
  The UniVPN software package delivered and automatically installed through the AD server must be in MSI format. You can obtain the software package in MSI format in following ways.

  Use a conversion tool to convert the existing UniVPN software package in EXE format to the MSI format. For details, see 4.4.2 Converting the Format of an Installation Package from EXE to MSI.

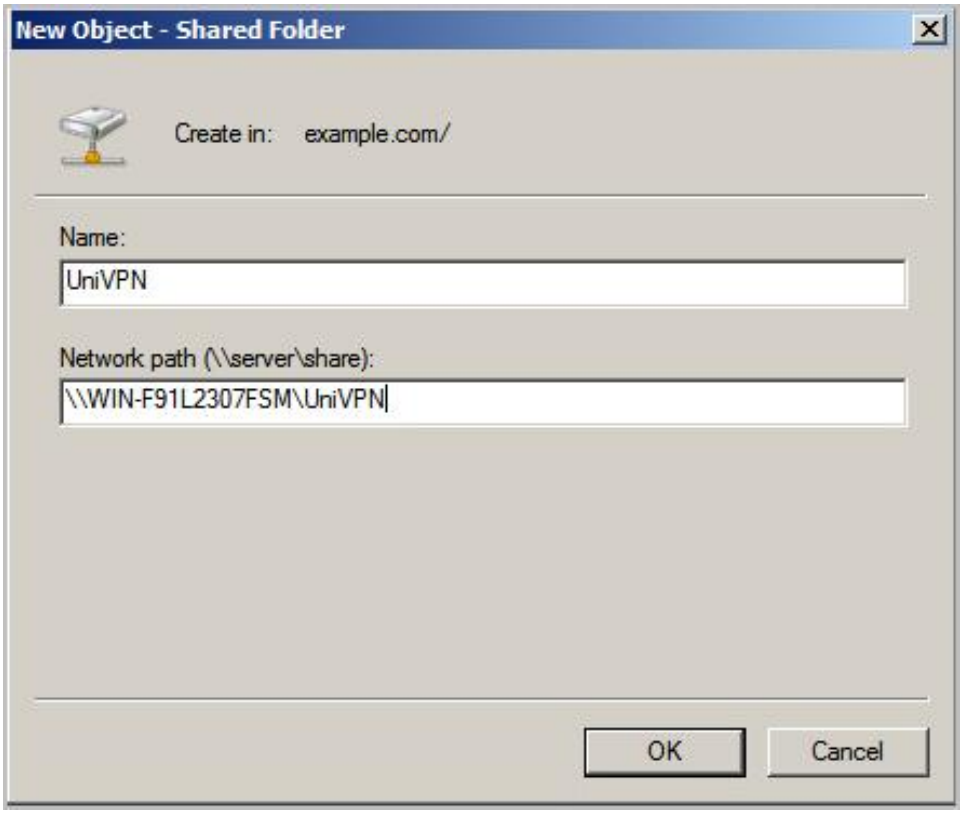
Procedure

Step 1 Reference the previously created shared folder under the example.com domain.

1. Right-click the example.com domain and choose **New > Shared Folder**.

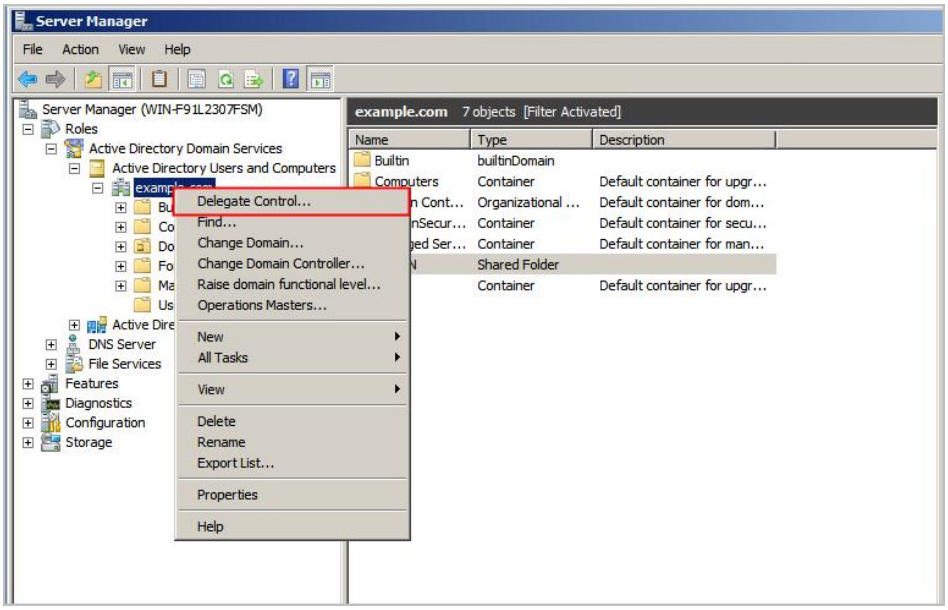


2. Enter the name and path of the previously created shared folder.



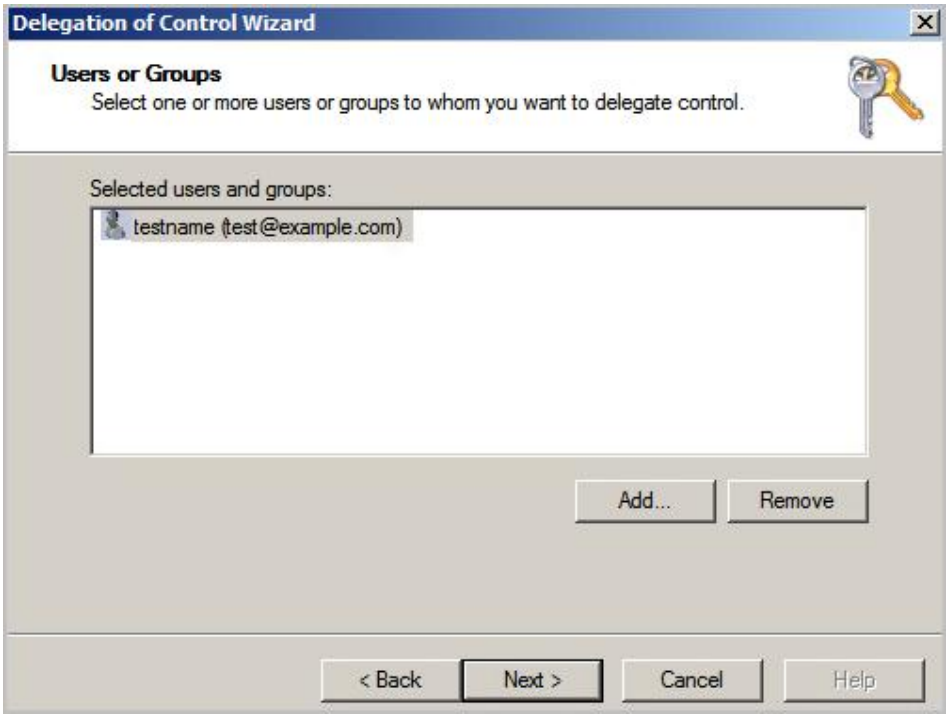
Step 2 Configure delegate control for users.

1. Right-click the example.com domain and choose **Delegate Control**.

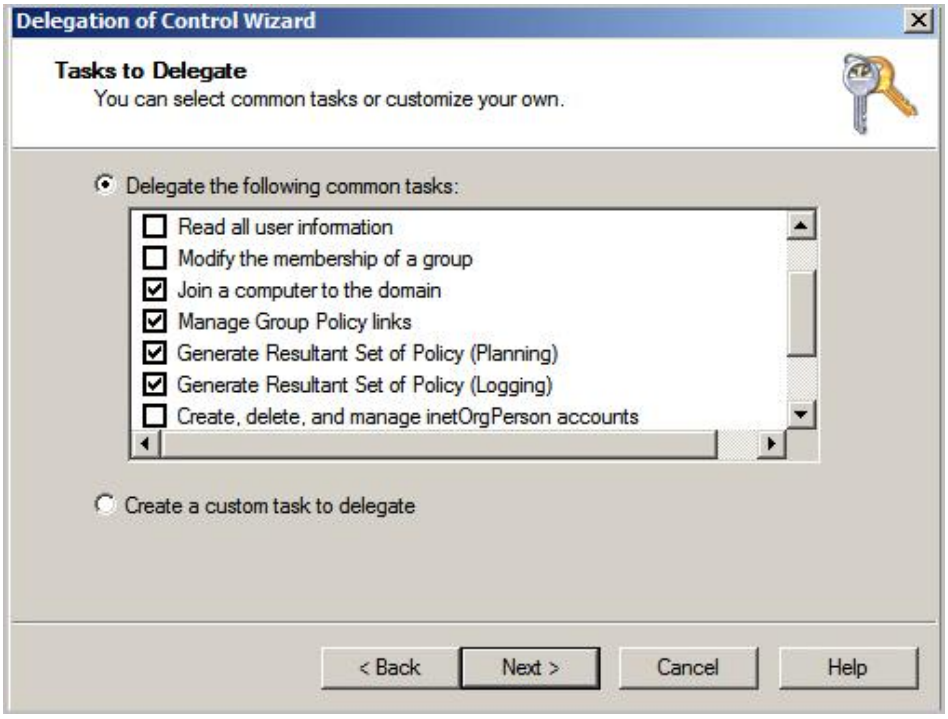


2. Click **Next**.

3. In the dialog box displayed, click **Add** to add existing domain users to the delegate control group and click **Next**.



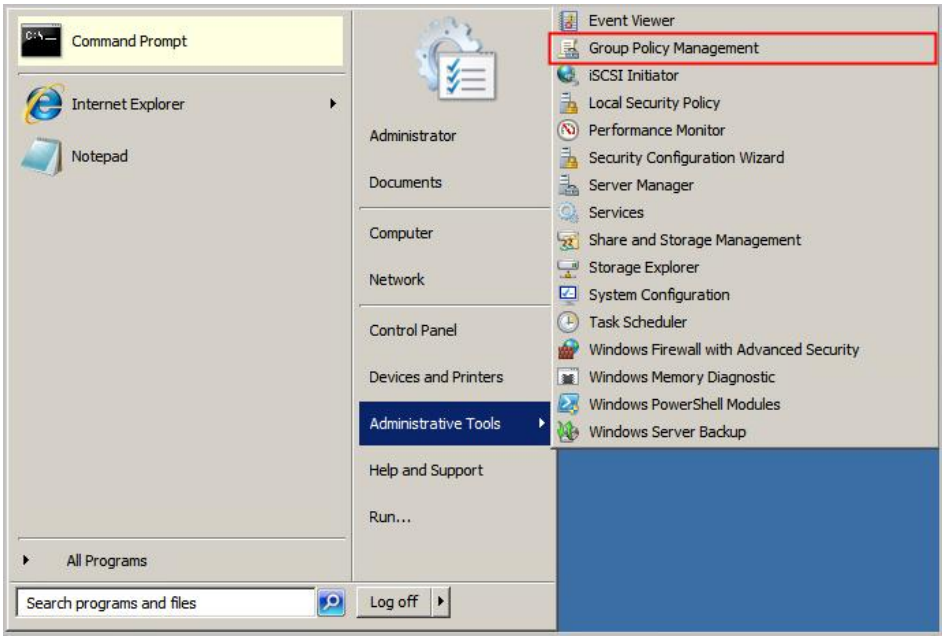
4. Select tasks delegated to users and click **Next**.



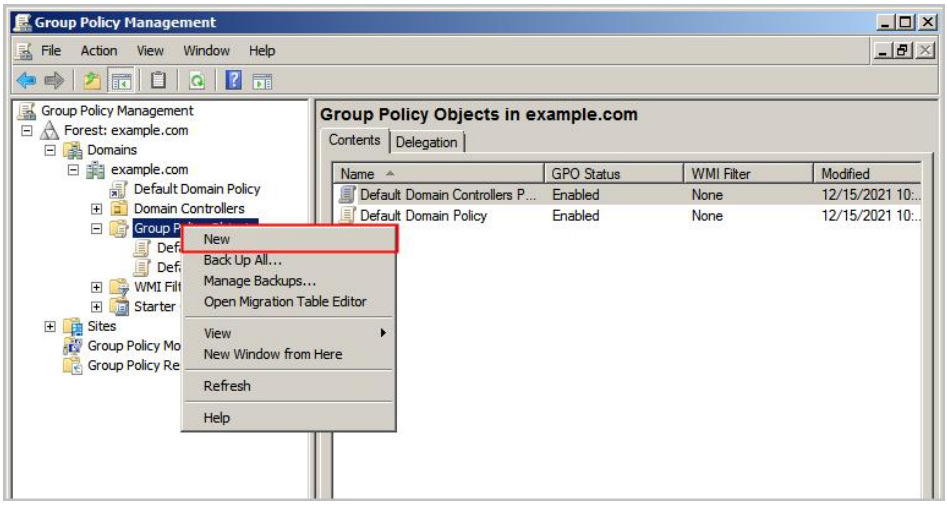
5. Click **Finish** to complete the delegate control configuration.

Step 3 Create a software installation policy.

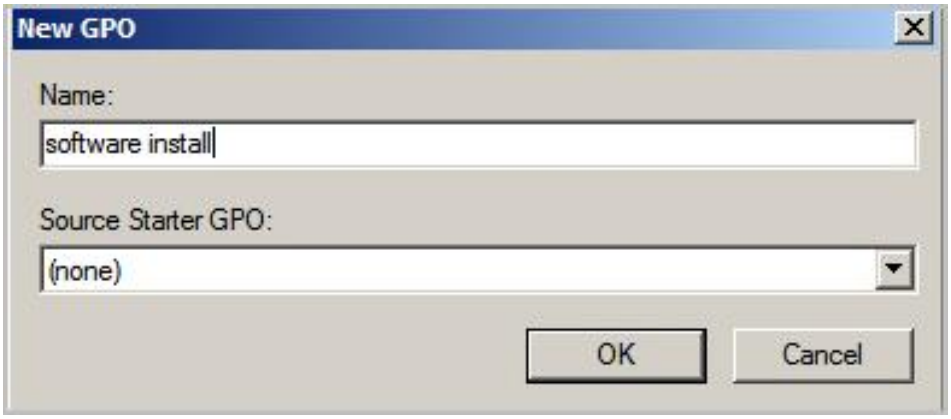
1. Choose **Administrative Tools > Group Policy Management** in the start menu.



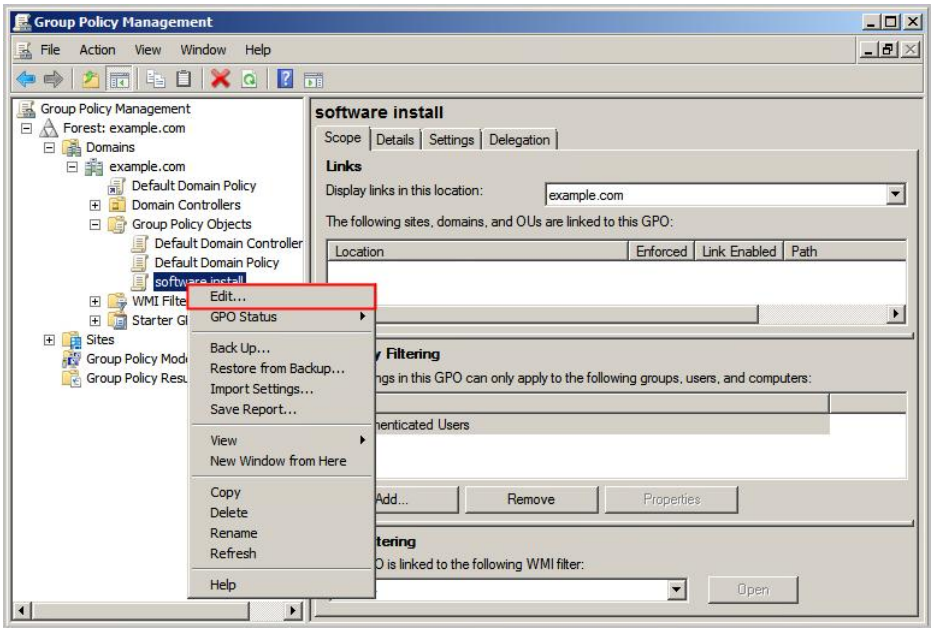
2. Right-click a group policy object and select **new**.



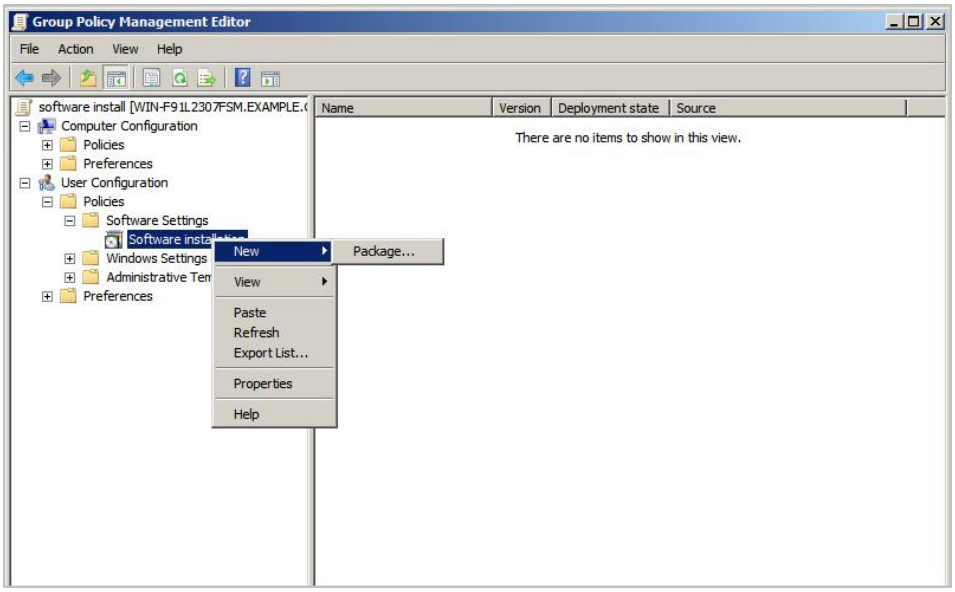
3. Create a policy object named **software install** and click **OK**.



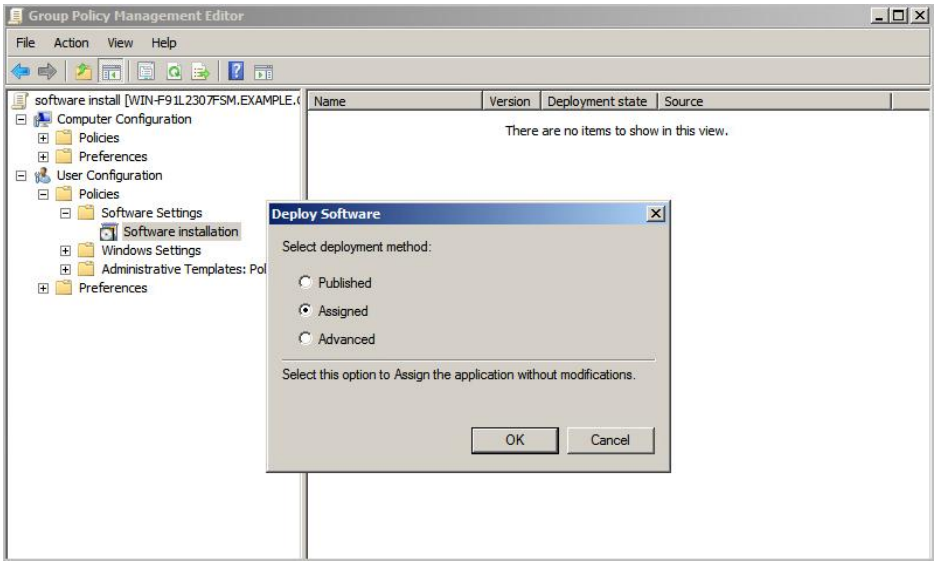
4. Right-click the newly created policy object **software install** and select **Edit**.



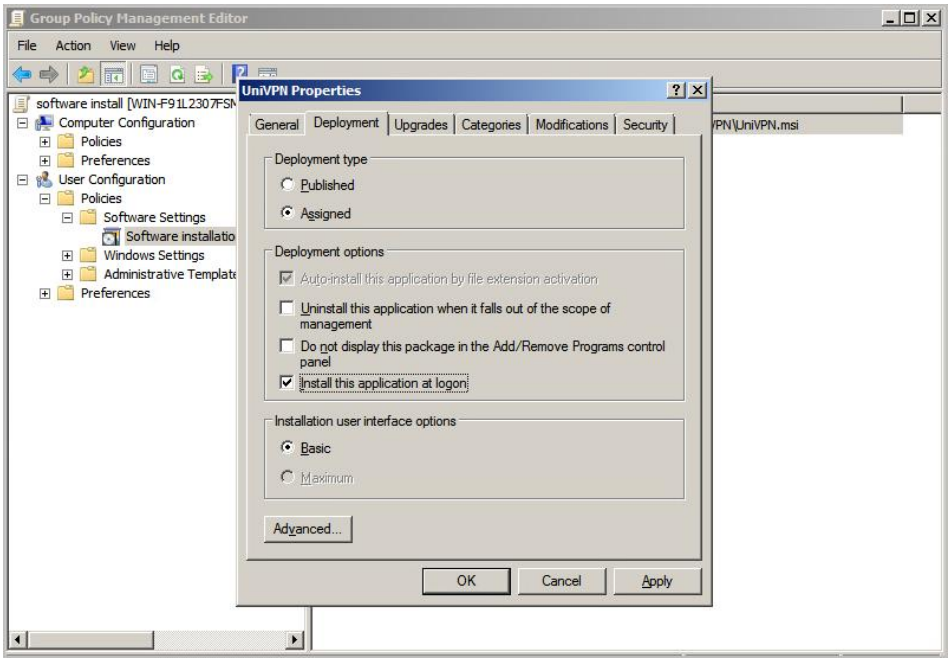
5. Right-click **Software Installation** and choose **New > Package**.



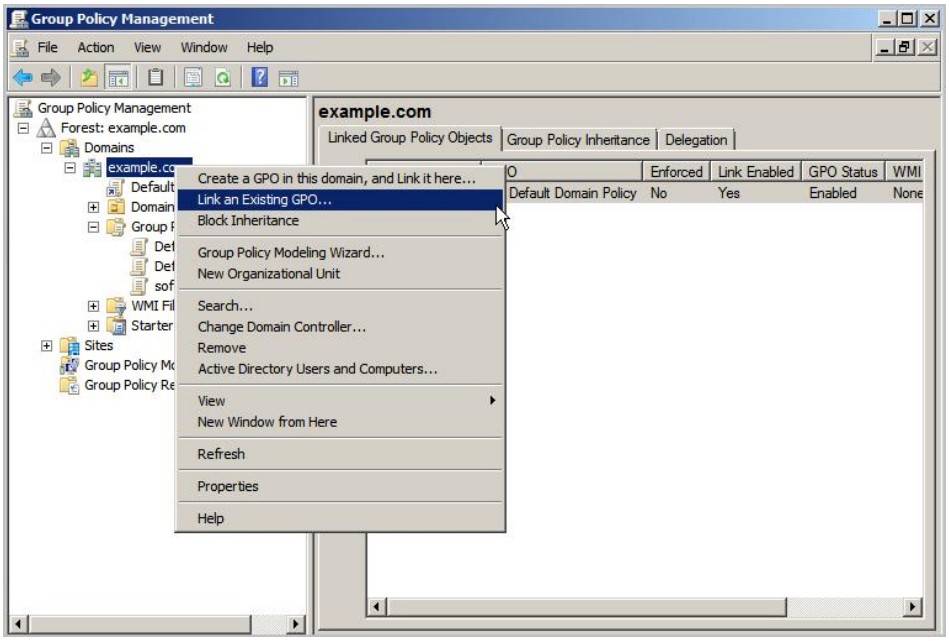
6. The system prompts you to select a UniVPN.msi file. After that, the system displays the following information. In this case, select **Assigned** and click **OK**.



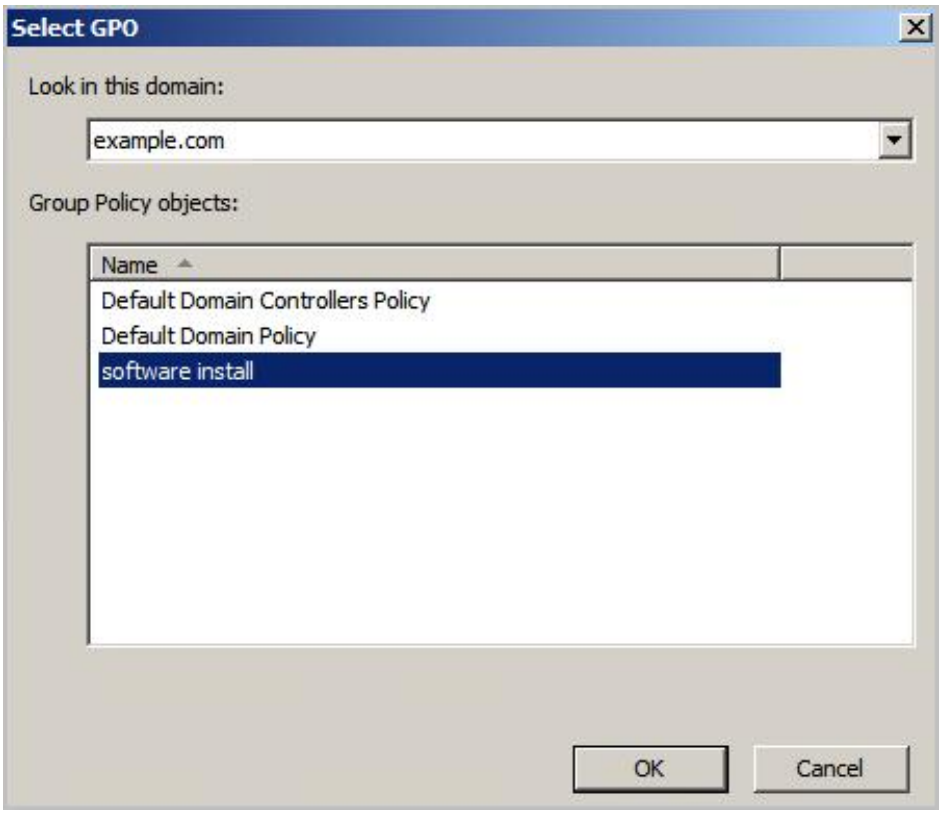
7. Right-click the UniVPN record generated in the window on the right, click the **Deployment** tab, and perform settings as shown in the following figure. Then click **OK**.



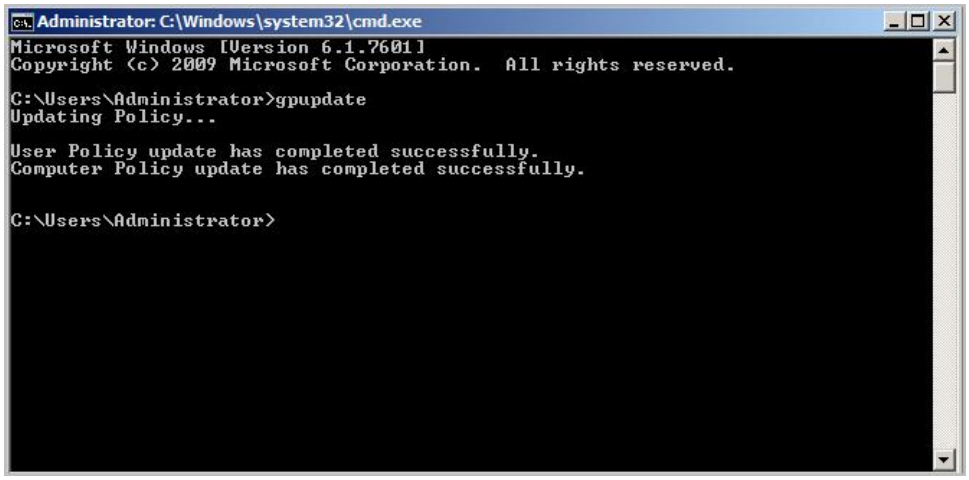
8. Right-click example.com and select **Link an existing GPO**.



9. Select **software install** and click **OK**.



Step 4 Run the **gpupdate** command in the CLI to update the group policy.



----End

Verification

After a domain user successfully logs in to the host, the system has installed the UniVPN.

The UniVPN software installation completes during the user's login to the system and requires no manual intervention.

5 Configuration

In the Windows, Linux, and Mac operating systems, the methods for setting up VPN tunnels using the UniVPN are similar. The following uses the Windows operating system as an example.

5.1 Using the UniVPN to Establish VPN Tunnels

The UniVPN can establish VPN tunnels in two modes: manual and using a profile.

5.2 Common Settings

This section describes common functional settings of the UniVPN.

5.1 Using the UniVPN to Establish VPN Tunnels

The UniVPN can establish VPN tunnels in two modes: manual and using a profile.

5.1.1 Manual Mode

In manual mode, a UniVPN user manually creates a VPN connection and sets relevant parameters to create a VPN tunnel.

The UniVPN supports the creation of SSL VPN, L2TP VPN, and L2TP over IPSec VPN tunnels. Select a VPN tunnel type for intranet access based on the actual network deployment.

5.1.1.1 Establishing an SSL VPN Tunnel

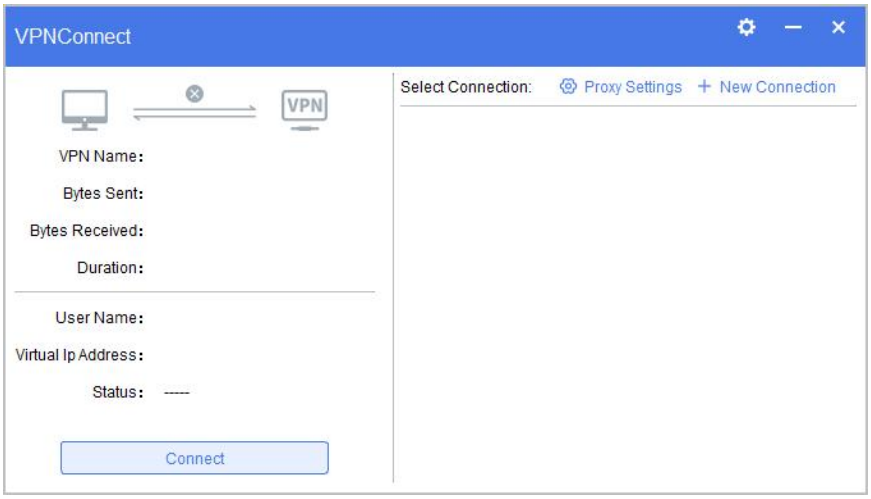
This section describes how to establish an SSL VPN tunnel.

Procedure

Step 1 Create an SSL VPN connection.

1. Open the UniVPN.

   Click + **New Connection** on the right of **Select the VPN connection**.



To configure the proxy function, click Proxy Settings on the right of **Select the VPN connection**.

Table 5-1 Proxy Settings

Parameter	Description
Agent setting	Two options are available depending on whether you use a proxy server to access the Internet. • No proxy server Select this type if you do not use the proxy server to access the Internet. • Proxy server involved The scenario where a proxy server is used is further divided into three sub-scenarios: – Use the system proxy: indicates that the proxy server information set in the browser is used. – Use Http/Https proxy: indicates that an HTTP or HTTPS proxy server is used. – Use the Socks5 proxy: indicates that a Sockets5 proxy server is used. Select a proxy type based on the actual network situation. In the selection of a proxy server, you need to enter the address, port, account, and password. Obtain these information from the proxy server administrator. The default proxy type is **NO proxy is used**.

2. Set SSL VPN connection parameter values.

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

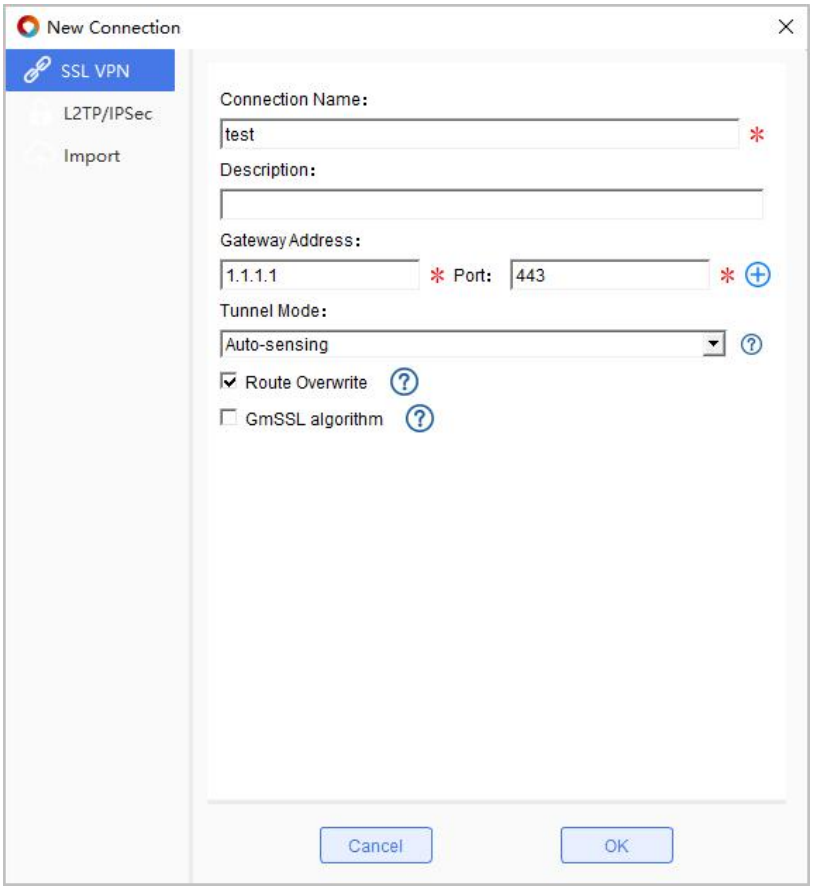


Table 5-2 SSL VPN parameter description

Parameter	Description
Connection Name	Enter the name of an SSL VPN connection. Each connection name must be unique.
Description	Configure a description for the connection. For example, you can add the creator, creation time, and connection use.
Remote gateway	Enter the SSL VPN virtual gateway address. The value must be the same as the IP address of the SSL VPN virtual gateway. Otherwise, the SSL VPN tunnel cannot be established.
Port	Enter the port number used to establish the SSL VPN tunnel. The value must be the same as the port number of the SSL VPN virtual gateway. Otherwise, the SSL VPN tunnel cannot be established. Click ⊕ under **Remote gateway** to add the current virtual gateway address to the virtual gateway list. A maximum of 16 addresses can be added to the virtual gateway

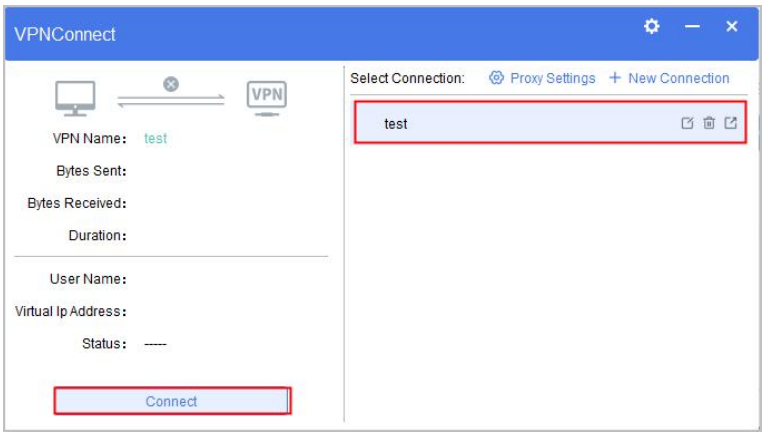
Parameter	Description
	list. To delete a record from the virtual gateway list, click in the line of the record. The virtual gateway list will be used in the gateway selection scenario. Specifically, when **Start automatic optimization** is selected, the UniVPN detects the response speed of all gateways in the virtual gateway list and establishes an SSL VPN tunnel with the gateway responding fastest. If there are multiple gateway addresses in the virtual gateway list and **Start automatic optimization** is not selected, you need to select an address in the virtual gateway list and select **Set as default,** so that the UniVPN establishes an SSL VPN tunnel with the selected virtual gateway.
Tunnel Mode	An SSL VPN tunnel can be established using the network extension function in three modes: **Auto-sensing, Reliable Transmission**, and **Quick Transmission**. In reliable transmission mode, SSL VPN uses SSL to encapsulate packets and TCP to transmit packets. In quick transmission mode, SSL VPN uses Quick UDP Internet Connections (QUIC) to encapsulate packets and UDP to transmit packets. QUIC encrypts data based on TLS/SSL. QUIC functions the same as SSL, except that packets encapsulated by QUIC are transmitted using UDP. In auto-sensing mode, the UniVPN preferentially uses the quick transmission mode to establish a tunnel with the virtual gateway. If tunnel establishment fails, the UniVPN tries the reliable transmission mode. In the network is unstable, the **Reliable Transmission** mode is recommended. If the network is stable, the **Quick Transmission** mode is preferred for its higher data transmission efficiency. If the network condition is unknown, select the **Auto-sensing** mode.
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 overwrite function is enabled, the route delivered by the peer gateway overwrites the existing route. This prevents network access

Parameter	Description
	exceptions caused by local route conflicts. By default, route overwrite 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.

3. Click **Save**. The home page is displayed.

Step 2 Log in to the SSL VPN virtual gateway.

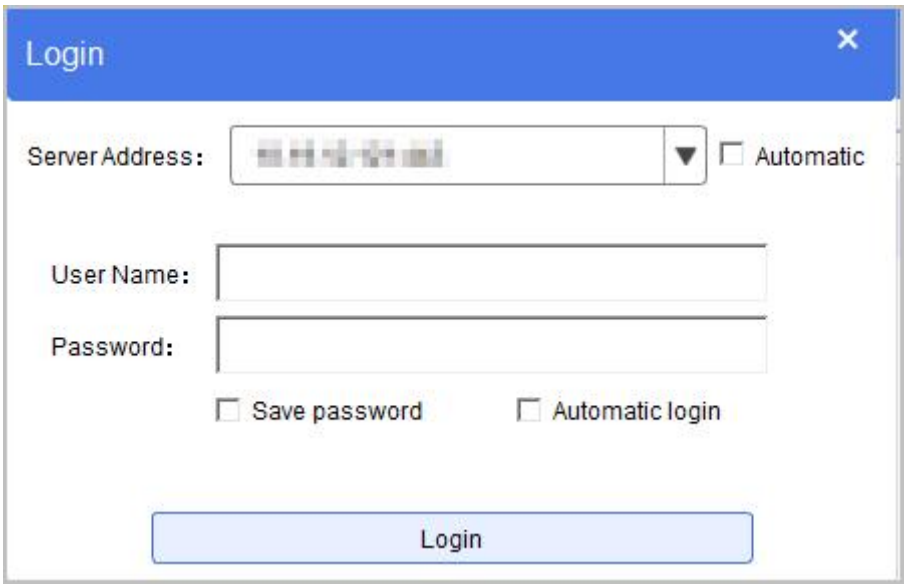
1. In the **Select the VPN connection** area, select a created SSL VPN connection, and then double-click it or click **connection** in the upper right corner to establish the connection.



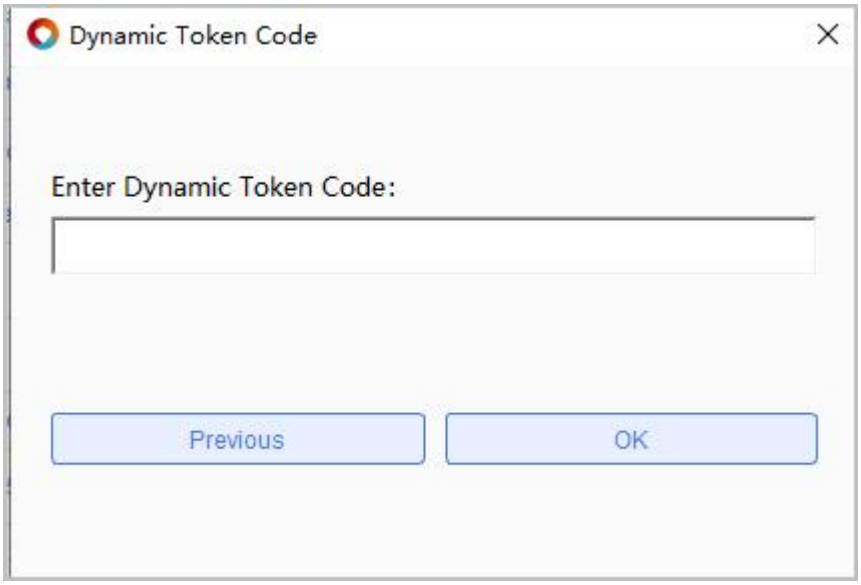
1. On the login page, enter the user name and password.

Click **Log in** to initiate a VPN connection.

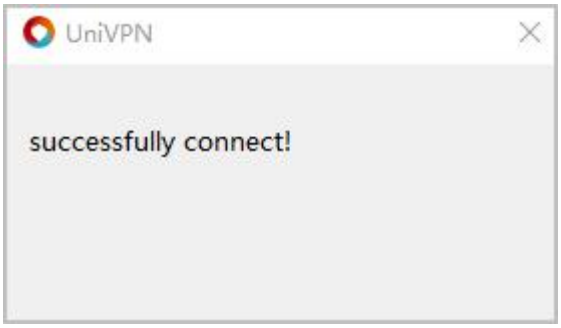
If certificate authentication is used in the Windows operating system, you need to select the certificate and enter the login password corresponding to the user name extracted from the certificate. In the Windows certificate authentication scenario, all certificates are imported to the Internet Explorer. In the Linux certificate authentication scenario, the certificate must be stored in the **Certificate** folder in the home directory. After the certificate is imported successfully, you can select the corresponding certificate from the certificate list.



2. If token code authentication or SMS authentication is configured on the third-party server in the networking, a dialog box is displayed to ask users to enter **Dynamic Token Code** for two-factor authentication. In the dialog box that is displayed, set for two-factor authentication. The client supports token code+SMS verification code two-factor authentication. Enter the obtained token code or SMS verification code and click **OK**.



3. When the VPN access succeeds, a prompt is displayed at the lower right corner of the screen.



Using the connection, the mobile user can access intranet resources as users in the enterprise intranet.

----End

5.1.1.2 Establishing an L2TP VPN Tunnel

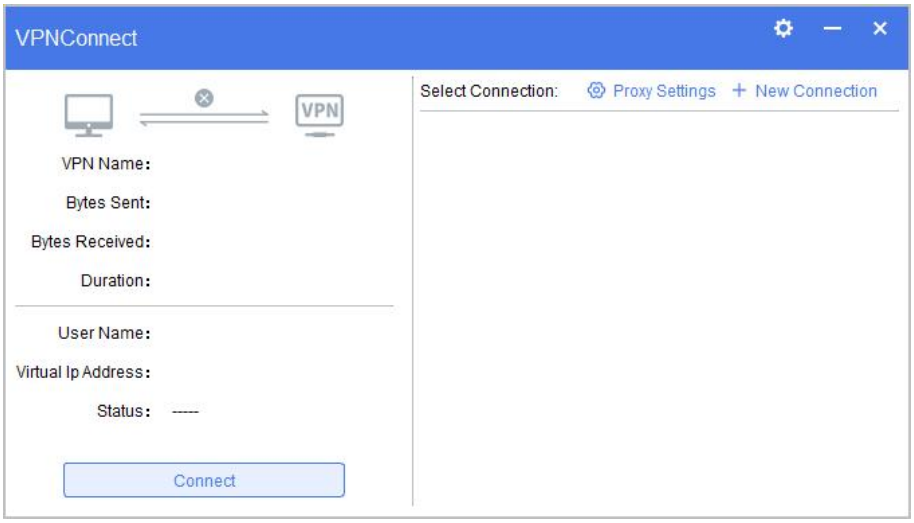
This section describes how to establish an L2TP VPN tunnel.

Procedure

Step 1 Create an L2TP VPN connection.

1. Open the UniVPN.

   Click + **New Connection** on the right of **Select the VPN connection**.



NOTE

L2TP VPN does not support the proxy function.

2. Set L2TP VPN connection parameter values.

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

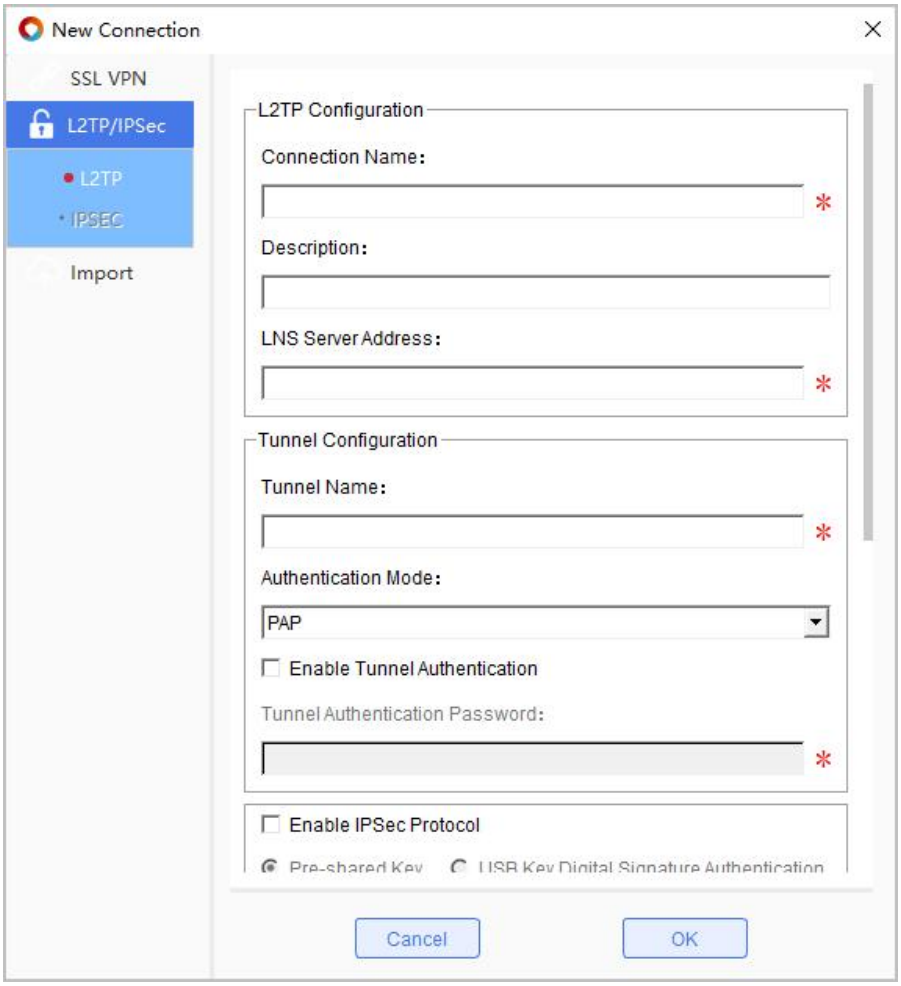


Table 5-3 L2TP parameter description

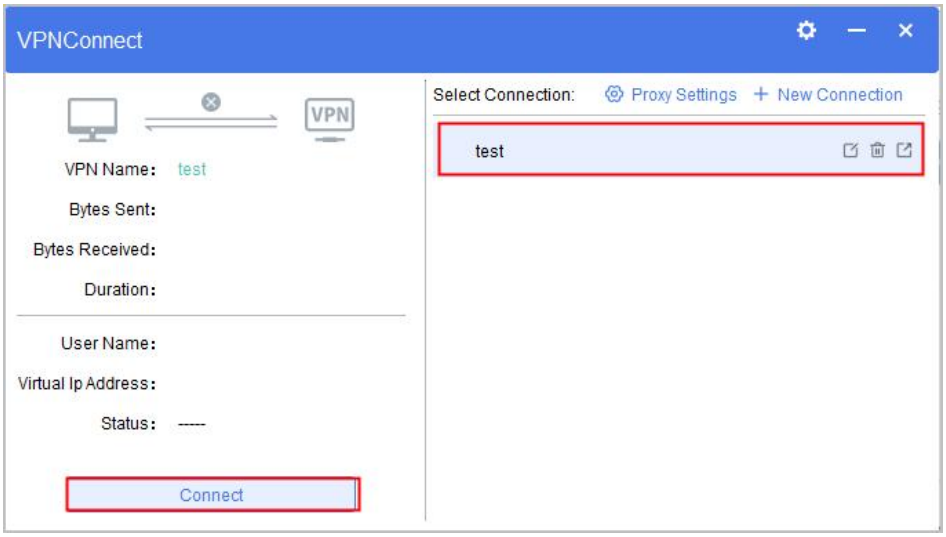
Parameter	Description
Connection Name	Enter the name of an L2TP VPN connection. Each connection name must be unique.
Description	Configure a description for the connection. For example, you can add the creator, creation time, and connection use.
LNS server address	Enter the L2TP VPN gateway address. The value must be the same as the IP address of the L2TP VPN virtual gateway. Otherwise, the L2TP VPN tunnel cannot be established.
Tunnel Name	Enter a tunnel name. The tunnel name must be the same as that configured on the LNS. Otherwise, the L2TP VPN tunnel cannot be established.
Authentication Mode	• CHAP authentication: CHAP is a three-way handshake authentication protocol. Using this protocol, only user names, not passwords, are transmitted on the network. • PAP authentication: PAP is a two-way handshake

Parameter	Description
	authentication protocol. Using this protocol, user names and passwords are transmitted on the network in plaintext. **NOTE** PAP is not a secure protocol, and CHAP is recommended.
Enable tunnel validation	For security, the tunnel is authenticated during L2TP VPN tunnel negotiation. The tunnel can be established only when the tunnel authentication password used by the remote access user is the same as that configured on the L2TP VPN gateway. Tunnel authentication is not mandatory during L2TP VPN tunnel establishment. Whether to enable this function depends on the L2TP VPN gateway configuration. If tunnel authentication is enabled on the gateway, it must be enabled on the UniVPN.
tunnel verification password	If tunnel authentication is enabled, you must set a tunnel authentication password. Obtain the password from the L2TP VPN administrator.
Enable IPsec security protocol	This parameter is used in the L2TP over IPSec scenario and does not need to be configured in the common L2TP remote access scenario.
Route Settings	There are three options for setting up the **Allow Internet access after connection**, Please set according to actual needs. • No select After the mobile office user dials successfully, its individual PC's default route next hop will be modified to the IP address of the virtual network card. All traffic will be sent to the end of the tunnel through the virtual network card, which means that the user can access the enterprise network resources but cannot access the Internet. • If this mode is selected, but no IP addresses are added to the IP address list: After a mobile user successfully dials in, the user PC generates a route destined to the IP address segment corresponding to the virtual network adapter, with the next hop being the IP address of the virtual network adapter. In this case, the user can access only enterprise intranet resources of the same network segment as the IP address of the virtual network adapter. In this process, original routes of the user are not affected, and the user can still access the Internet and LAN when accessing resources on the enterprise intranet. • If this mode is selected, and IP addresses are added to the IP address list: After a mobile user successfully dials in, the user PC uses the IP address segments added in the IP address list as the destination network segments and generates specific

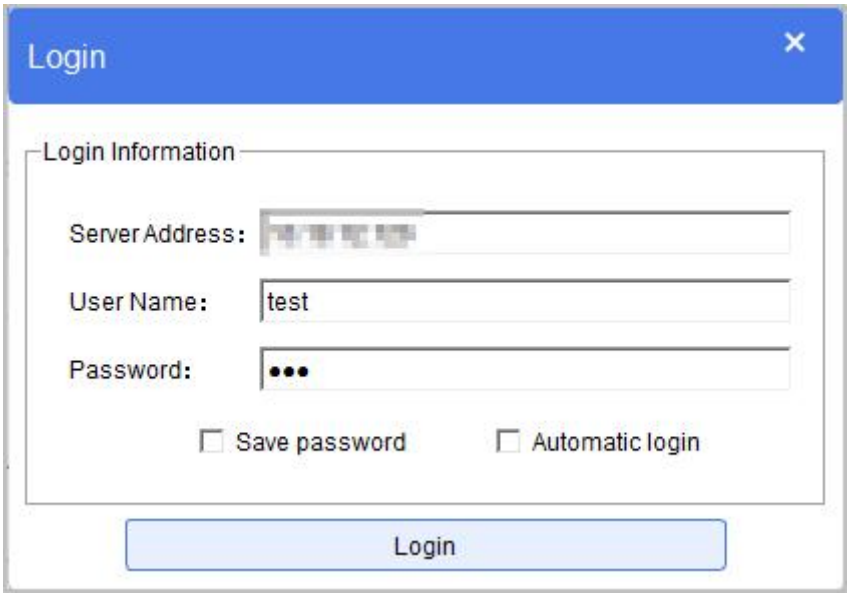
Parameter	Description
	routes with the next hop being the IP address of the virtual network adapter. In this case, the user can access enterprise intranet resources configured in the IP address list. In this process, original routes of the user are not affected, and the user can still access the Internet and LAN when accessing resources on the enterprise intranet.

Step 2 Log in to the L2TP VPN gateway.

1. In the **Select the VPN connection** area, select a created L2TP VPN connection, and then double-click it or click **connection** in the upper right corner to establish the connection.

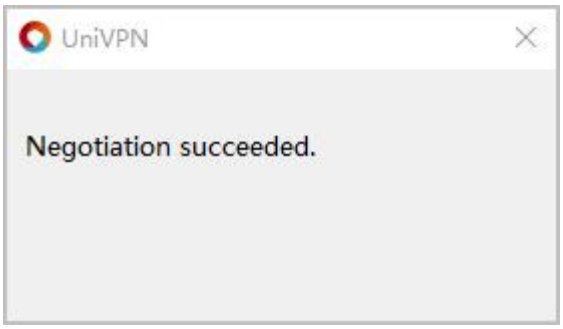


2. On the login page, enter the user name and password.



3. Click **Login** to initiate a VPN connection.

When the VPN access succeeds, a prompt is displayed at the lower right corner of the screen.



Using the connection, the mobile user can access intranet resources as users in the enterprise intranet.

----End

5.1.1.3 Establishing an L2TP over IPSec VPN Tunnel

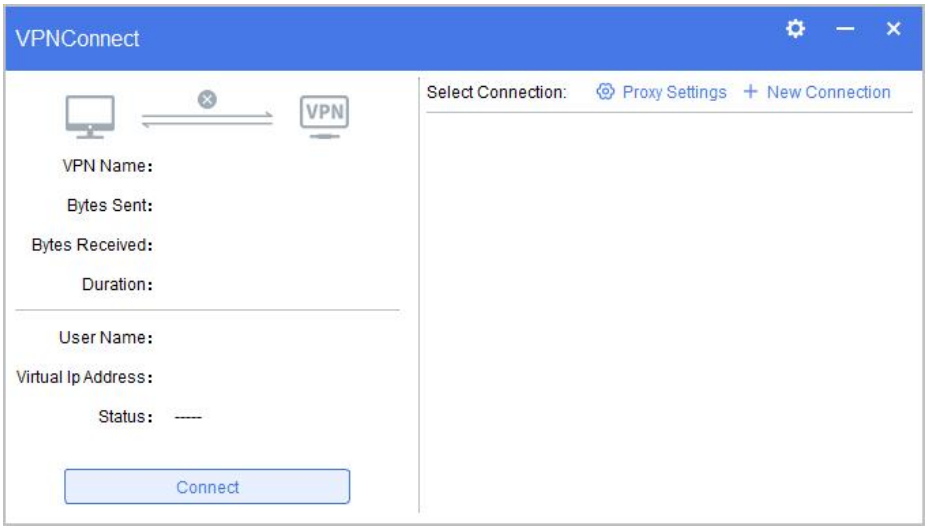
This section describes how to establish an L2TP over IPSec VPN tunnel.

Procedure

Step 1 Create an L2TP over IPSec VPN connection.

1. Open the UniVPN.

   Click + on the right of **Select the VPN connection**.



   To configure the proxy function, click

on the right of **Select the VPN connection**.

Table 5-4 Proxy Settings

Parameter	Description

Parameter	Description
Agent setting	Two options are available depending on whether you use a proxy server to access the Internet. • No proxy server Select this type if you do not use the proxy server to access the Internet. • Proxy server involved The scenario where a proxy server is used is further divided into three sub-scenarios: – Use the system proxy: indicates that the proxy server information set in the browser is used. – Use Http/Https proxy: indicates that an HTTP or HTTPS proxy server is used. – Use the Socks5 proxy: indicates that a Sockets5 proxy server is used. Select a proxy type based on the actual network situation. In the selection of a proxy server, you need to enter the address, port, account, and password. Obtain these information from the proxy server administrator. **NOTE** The L2TP over IPSec tunnels support only the sockets5 proxy server. The default proxy type is **NO proxy is used**.

2. Set L2TP over IPSec VPN connection parameter values.

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

   a. Set L2TP parameters.

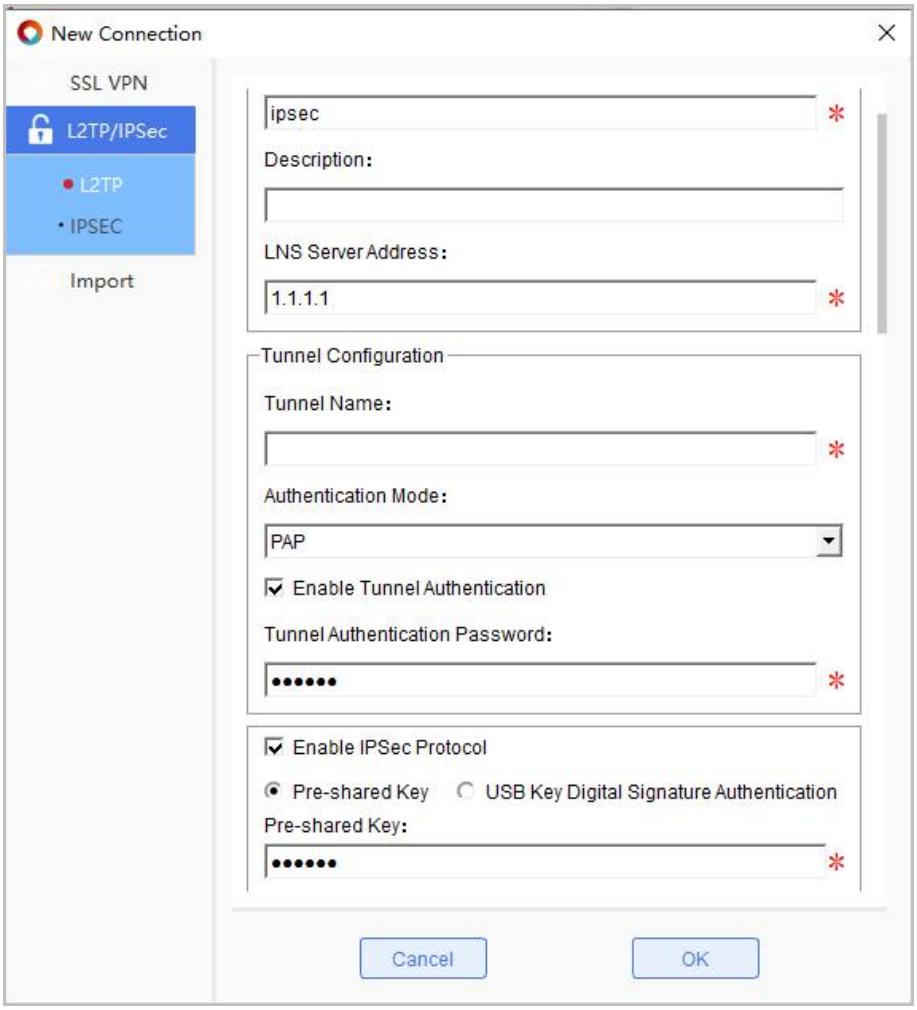


Table 5-5 L2TP parameter description

Parameter	Description
Connection Name	Enter the name of an L2TP VPN connection. Each connection name must be unique.
Description	Configure a description for the connection. For example, you can add the creator, creation time, and connection use.
LNS server address	Enter the L2TP VPN gateway address. The value must be the same as the IP address of the L2TP VPN virtual gateway. Otherwise, the L2TP VPN tunnel cannot be established.
Tunnel name	Enter a tunnel name. The tunnel name must be the same as that configured on the LNS. Otherwise, the L2TP VPN tunnel cannot be established.
Authentication mode	• CHAP authentication: CHAP is a three-way handshake authentication protocol. Using this protocol, only user names, not passwords, are

Parameter	Description
	transmitted on the network. • PAP authentication: PAP is a two-way handshake authentication protocol. Using this protocol, user names and passwords are transmitted on the network in plaintext. **NOTE** PAP is not a secure protocol, and CHAP is recommended.
Enable tunnel validation	For security, the tunnel is authenticated during L2TP VPN tunnel negotiation. The tunnel can be established only when the tunnel authentication password used by the remote access user is the same as that configured on the L2TP VPN gateway. Tunnel authentication is not mandatory during L2TP VPN tunnel establishment. Whether to enable this function depends on the L2TP VPN gateway configuration. If tunnel authentication is enabled on the gateway, it must be enabled on the UniVPN.
tunnel verification password	If tunnel authentication is enabled, you must set a tunnel authentication password. Obtain the password from the L2TP VPN administrator.

b. Set IPSec parameters.

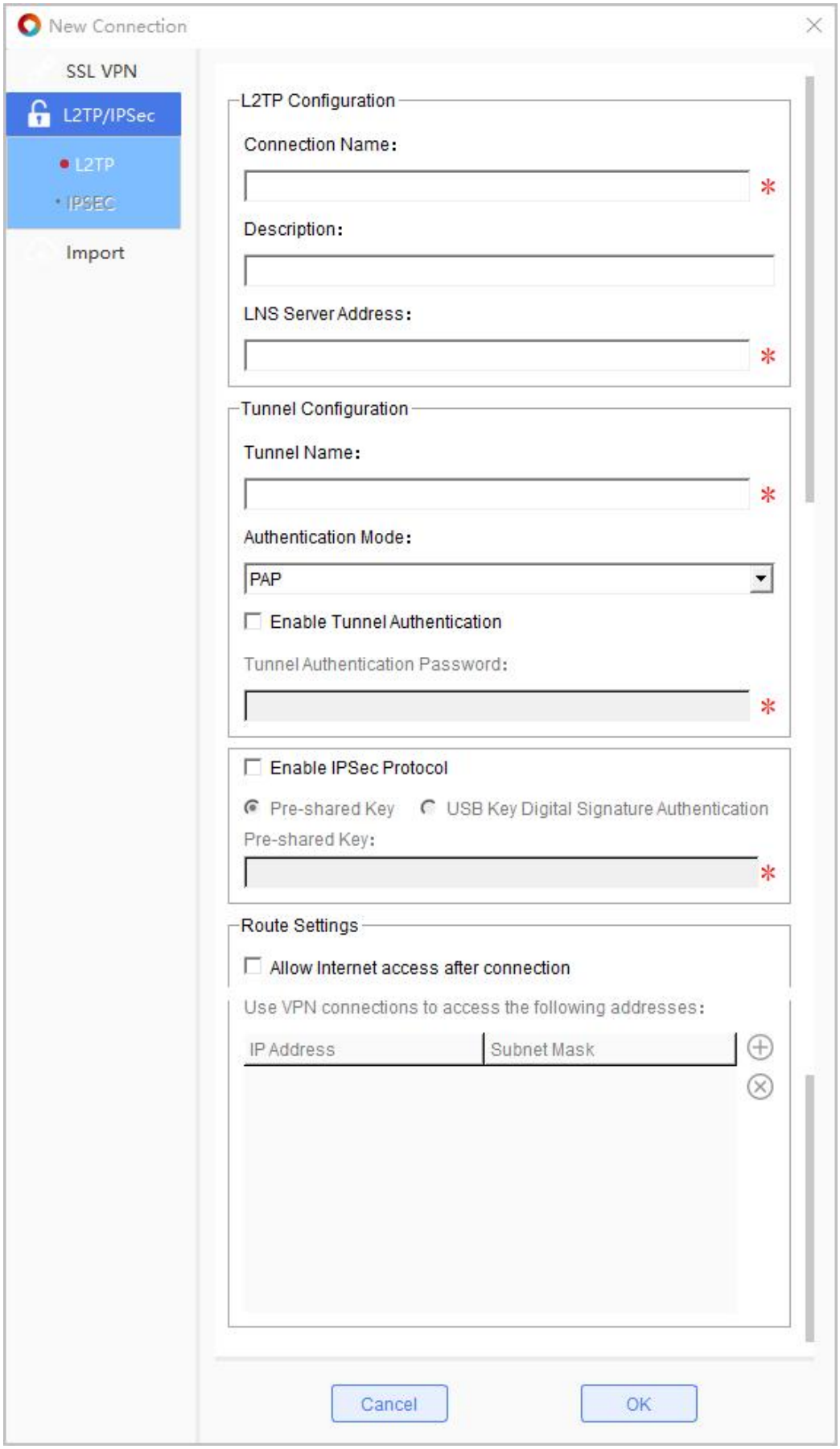

New Connection
SSL VPN
L2TP/IPSec
L2TP
IPSEC
Import
L2TP Configuration
Connection Name:
Description:
LNS Server Address:
Tunnel Configuration
Tunnel Name:
Authentication Mode:
PAP
Enable Tunnel Authentication
Tunnel Authentication Password:
Enable IPSec Protocol
Pre-shared Key
USB Key Digital Signature Authentication
Pre-shared Key:
Route Settings
Allow Internet access after connection
Use VPN connections to access the following addresses:
IP Address
Subnet Mask
Cancel
OK

Table 5-6 IPSec parameter description

Parameter	Description
Enable IPsec security protocol	You shall select this item in L2TP over IPSec scenarios. IPSec authentication falls into pre-shared key authentication and USB key digital signature authentication. • In pre-shared key authentication mode, you need to obtain the pre-shared key from the IPSec VPN gateway administrator and enter it. • In USB key digital signature authentication, you shall enter the USB PIN code, which is an encrypted password set by the USB key owner to secure the USB key. Obtain this password from the USB key owner. **NOTE** USB key digital signature authentication is not supported on the Mac or Linux operating system.
IPSec Configuration	
IPSec Server Address	Address of the IPSec VPN gateway. The value must be the same as the actual IP address of the IPSec VPN gateway. Otherwise, the VPN tunnel cannot be established.
Using LNS server	When the L2TP VPN gateway and the IPSec VPN gateway are the same, select this item.
Encapsulation mode	In IPSec encapsulation, Authentication Header (AH) or Encapsulating Security Payload (ESP) related fields are inserted to original IP packets for packet authentication and encryption. The encapsulation mode can be tunnel or transport mode. • Tunnel: The tunnel mode protects only the packet payload and is used to establish tunnels between VPN gateways. • Transport: The transport mode protects the entire packet and is used to establish tunnels between mobile terminals and VPN gateways. By default, the transport mode is used.

Parameter	Description
ESP protocol Verification algorithm	The ESP authentication algorithm verifies the integrity of original packets, preventing them from being tampered with in transport. The ESP authentication algorithm consists of MD5, SHA1, and SHA2-256. The more secure SHA2-256 is recommended.
ESP protocol Encryption algorithm	The ESP encryption algorithm encrypts original packets, preventing them from being intercepted in transport. The ESP encryption algorithm consists of DES, 3DES, and AES-128/192/256. The AES algorithm has a higher security than the DES and 3DES algorithms. The AES algorithm falls into AES128, AES192, and AES256 according to the key length. A longer key indicates a higher security and a longer time taken to encrypt and decrypt packets. The AES256 algorithm is recommended, taking both the security and encryption and decryption efficiency into consideration.
IKE Basic Configuration	
Negotiation mode	Two IKE negotiation modes are available for IPSec tunnels. • Main mode • Aggressive mode • By default, the **Main mode** is used for negotiation. If the tunnel initiator has a full understanding of the policies of the tunnel responder, using the **Aggressive mode** enables you to create an IKE SA more rapidly.
ID type	ID type. Authentication is a protection mechanism in IKE negotiation. It authenticates the identity of the communication parties to ensure the security. • ID types of IKE peers can be different. The ID falls into IP address and name types. When the negotiation is in **Main mode**, the IP address type is used by default, indicating that the local IP address is used as the local ID. When the negotiation is in **Aggressive mode**, the ID type is optional. That is, the ID can be of the IP address or name

Parameter	Description
	type.
Local name	You shall set this item when you set the ID type to **Name**. The local name serves as the local ID to be authenticated by the IPSec VPN gateway. An IPSec tunnel can be established between the IPSec VPN gateway and UniVPN only when the authentication succeeds. Ensure that the **Local Name** is consistent with the peer name on the IPSec VPN gateway. Otherwise, the tunnel cannot be established. Obtain the local name from the IPSec VPN gateway administrator.
Security gateway Name	You shall set this item when you set the ID type to **Name**. Ensure that **Security Gateway Name** is consistent with the local name on the IPSec VPN gateway. Otherwise, the tunnel cannot be established. Obtain the security gateway name from the IPSec VPN gateway administrator. The name of the IPSec VPN gateway is its ID. The authentication is mutual. When the UniVPN establishes a tunnel with the IPSec VPN gateway, it also authenticates the gateway. The IPSec VPN gateway submits its ID to the UniVPN for authentication. The UniVPN establishes an IPSec tunnel with the IPSec VPN gateway only after the authentication succeeds.
Validation algorithm	In IKE negotiation, the authentication algorithm protects the integrity of packets. The authentication algorithm consists of MD5, SHA1, and SHA2-256. The more secure SHA2-256 is recommended.
Encryption algorithm	In IKE negotiation, the encryption algorithm protects the secrecy of packets to prevent them from being intercepted. The encryption algorithm consists of DES-CBC, 3DES-CBC, and AES-128/192/256. The AES-256 algorithm is recommended, considering that it is more secure.
DH group mark	In IKE negotiation, the DH group is used by the tunnel initiator and responder to exchange keys. According to the key length, the DH group falls into group1 (768 bit), group2 (1024 bit), and group5 (1536 bit). group1 is insecure, and group2 or group5 is recommended.

Parameter	Description
IKE Advanced Configuration	
Enable PFS feature	Enables the Perfect Forward Secrecy (PFS) function in IKE negotiation. In a negotiation initiated by the local end, an additional key exchange (through the DH group) is performed in IKEv1 phase 2 or child SA creation in IKEv2 to ensure the security of the IPSec SA key and communication. To enable this function, you need to set the related security parameter, whose value can be group1, group2, and group5. group1 is insecure, and group2 or group5 is recommended.
Security alliance life cycle	The IKE SA lifecycle is used to periodically update the IKE SA, which reduces the risk of IKE SA cracking and improves security. Before the specified lifecycle is due, a new IKE SA is negotiated for the IKE peer. After the new IKE SA is negotiated, the peer immediately employs the new IKE SA, and the previous IKE SA is automatically deleted after the lifecycle is due. Renegotiating does not interrupt the existing tunnel.
IPSec Advanced Configuration	
Security alliance life cycle	For a dynamic SA, the IPSec tunnel will be renegotiated when the renegotiation interval reaches the threshold for security. Renegotiating does not interrupt the existing tunnel.
Route Settings	Route setting controls the range of resources accessible to mobile users after their remote access. Route setting supports two modes, namely, **Mode Config** and **Allow Internet access after connection**. Their difference lies in that the range of resources accessible to users is subject to the configurations at the gateway side in **Mode Config** mode and to the configurations in the IP address list at the UniVPN side in **Allow Internet access after connection** mode. • **Mode Config** – In a scenario where the peer VPN gateway supports the Mode Config negotiation mode, after a mobile user successfully accesses, the VPN gateway pushes the enterprise

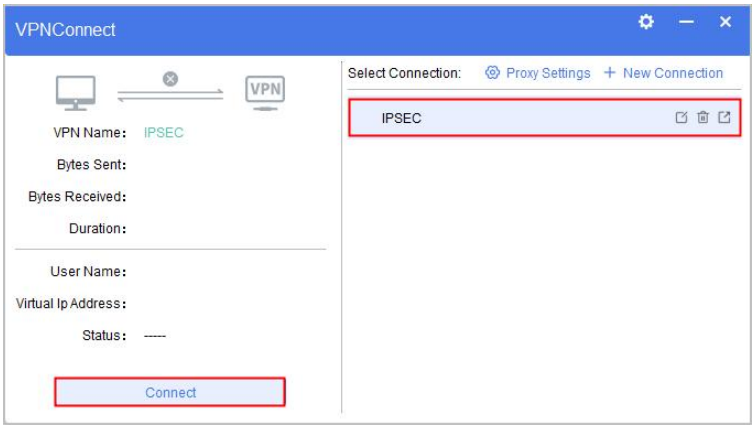
Parameter	Description
	intranet address segments configured at the gateway side, and the user PC generates specific routes to these address segments so that the user can access the resources on the enterprise intranet. In this process, original routes of the user are not affected, and the user can still access the Internet and LAN when accessing resources on the enterprise intranet. – In a scenario where the peer VPN gateway does not support the Mode Config negotiation mode, after a mobile user successfully accesses, the next hop of the default route of the user PC is changed to the IP address of the virtual network adapter. In this case, all traffic is sent to the peer end of the tunnel through the virtual network adapter. This means that the user can access only enterprise intranet resources but not the Internet. • **Allow Internet access after connection** – If this mode is selected, but no IP addresses are added to the IP address list: After a mobile user successfully dials in, the user PC generates a route destined to the IP address segment corresponding to the virtual network adapter, with the next hop being the IP address of the virtual network adapter. In this case, the user can access only enterprise intranet resources of the same network segment as the IP address of the virtual network adapter. In this process, original routes of the user are not affected, and the user can still access the Internet and LAN when accessing resources on the enterprise intranet. – If this mode is selected, and IP addresses are added to the IP address list: After a mobile user successfully dials in, the user PC uses the IP address segments added in the IP address list as the destination network segments

Parameter	Description
	and generates specific routes with the next hop being the IP address of the virtual network adapter. In this case, the user can access enterprise intranet resources configured in the IP address list. In this process, original routes of the user are not affected, and the user can still access the Internet and LAN when accessing resources on the enterprise intranet.

c. After the parameters are set, click **Save** to return to the main page.

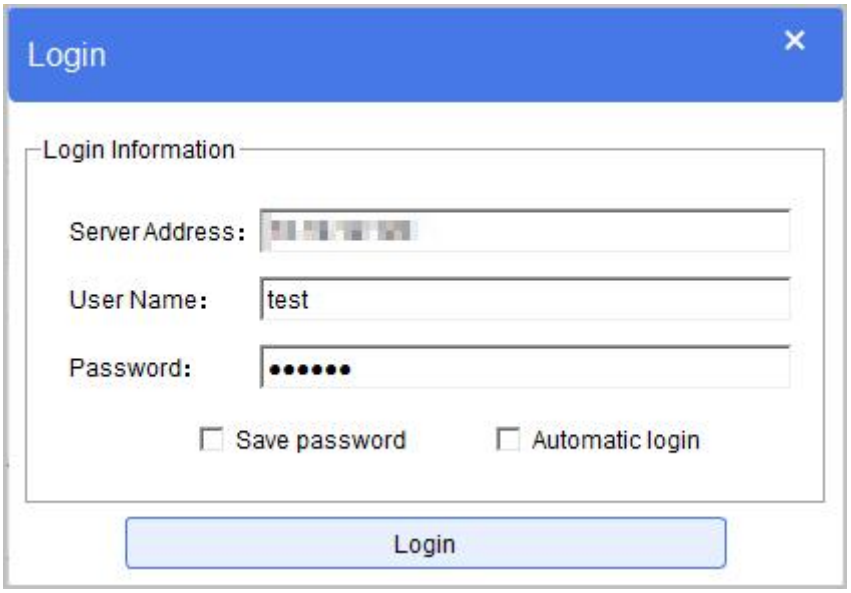
Step 2 Log in to the L2TP over IPSec VPN gateway.

1. In the **Select the VPN connection** area, select a created L2TP over IPSec VPN connection, and then double-click it or click **connection** in the upper right corner to establish the connection.



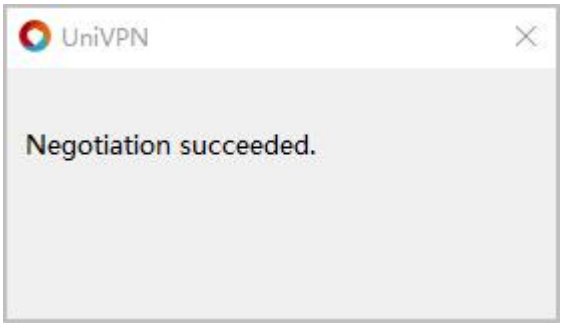
2. On the login page, enter the user name and password.

   If certificate authentication is used in the Windows operating system, you need to select the certificate and enter the login password corresponding to the user name extracted from the certificate. In the Windows certificate authentication scenario, all certificates are imported to the Internet Explorer. In the Linux certificate authentication scenario, the certificate must be stored in the **Certificate** folder in the home directory. After the certificate is imported successfully, you can select the corresponding certificate from the certificate list.



3. Click **Login** to initiate a VPN connection.

   When the VPN access succeeds, a prompt is displayed at the lower right corner of the screen.



   Using the connection, the mobile user can access intranet resources as users in the enterprise intranet.

----End

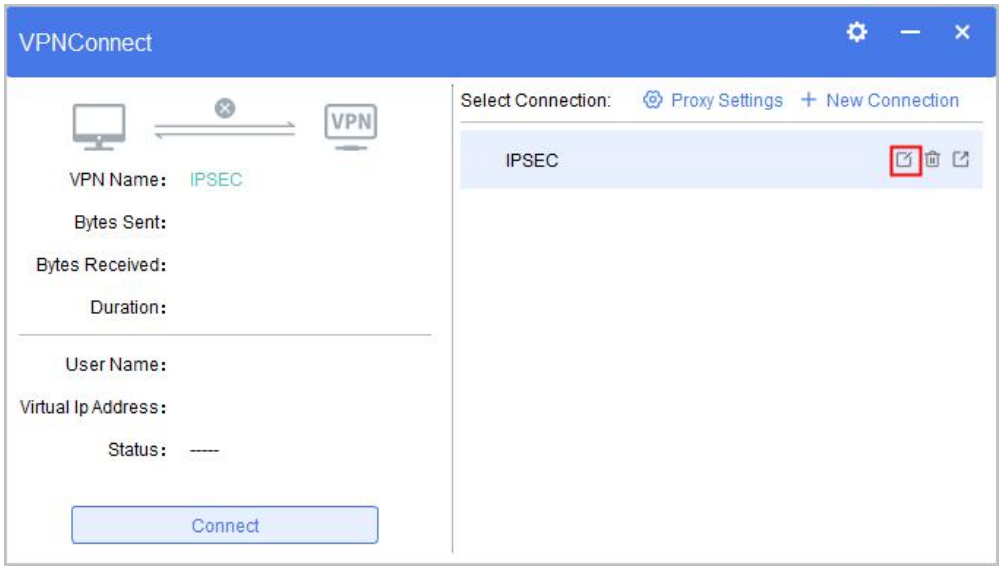
5.1.2 Profile Mode

The profile mode refers to a mode in which the UniVPN user obtains an .ini profile from other personnel (such as the network administrator) and imports the profile to the UniVPN to establish a VPN tunnel. Using the profile to create a VPN connection reduces your configuration workload.

Exporting a Profile

Method 1:

Step 1 Select an existing VPN connection and click the edit icon on the right of the connection.



Step 2 In the **Edit connection** window, click **Export config** in the navigation tree and select a directory for saving the profile.

By default, the profile is saved to an .ini file.

Step 3 Click **Save** to export the profile.

Method 2:

Step 1 Select an existing VPN connection and click the export icon on the right of the connection.

Step 2 Select a directory for saving the profile.

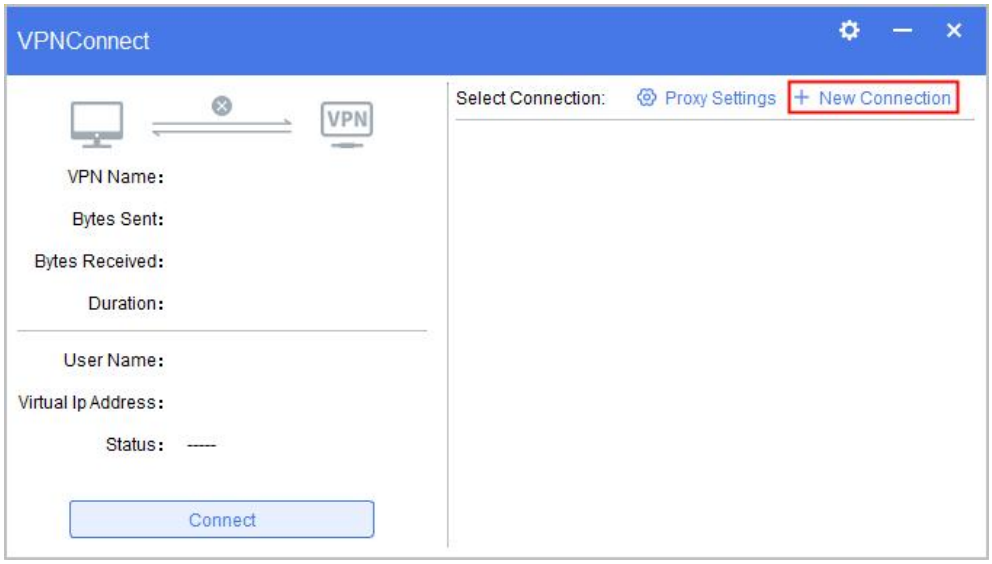
By default, the profile is saved to an .ini file.

Step 3 Click **Save** to export the profile.

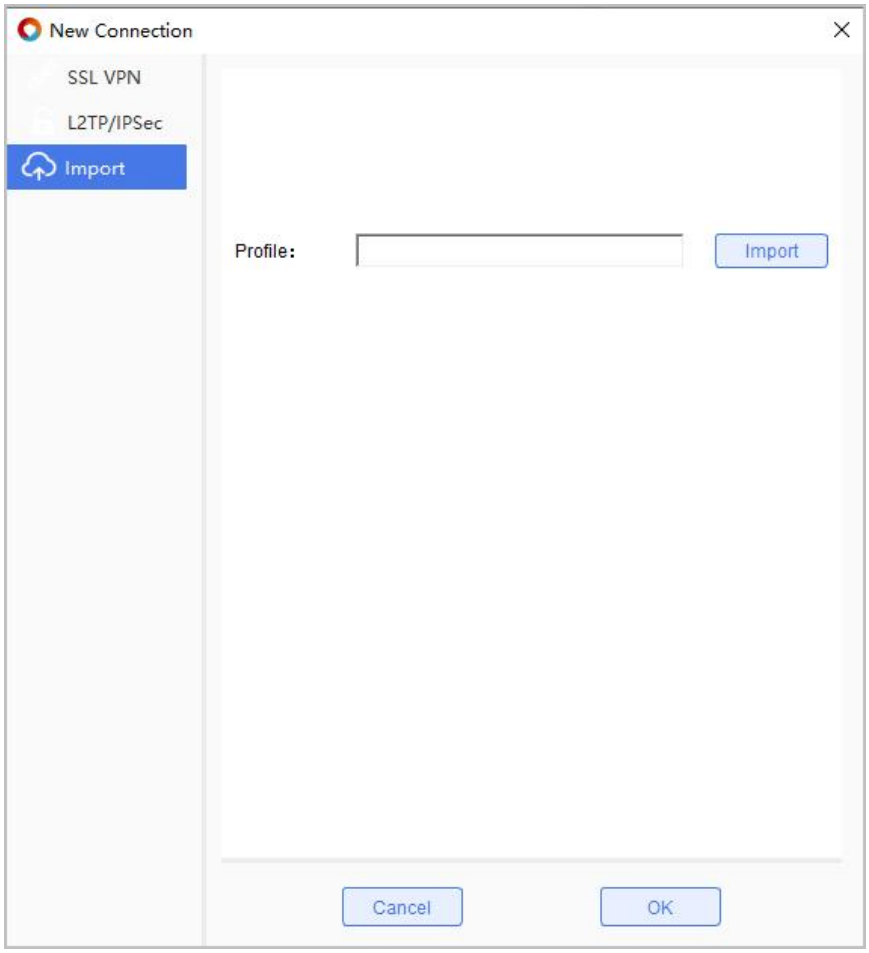
----End

Importing a Profile

Step 1 On the UniVPN main page, click + on the right of **Select the VPN connection**.



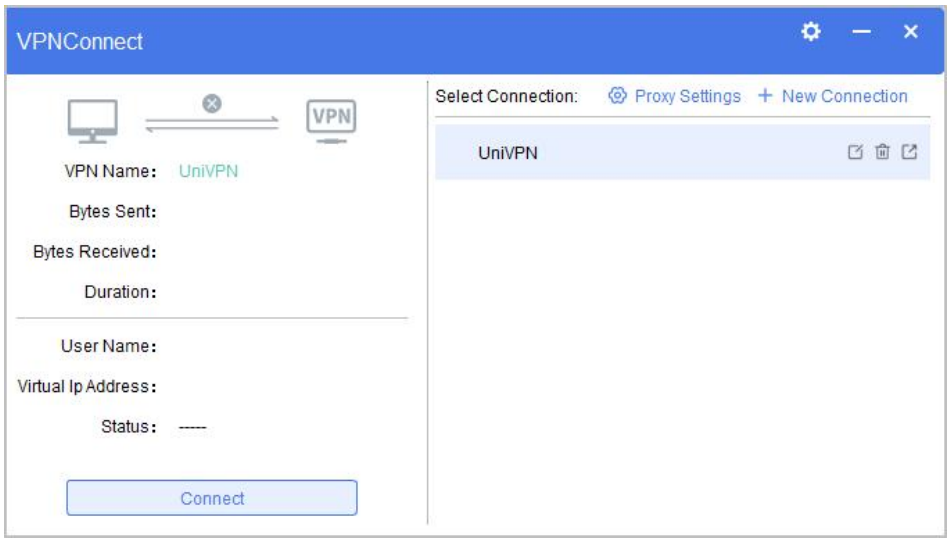
Step 2 In the **New connection** dialog box, select **Load Config** from the left navigation tree.



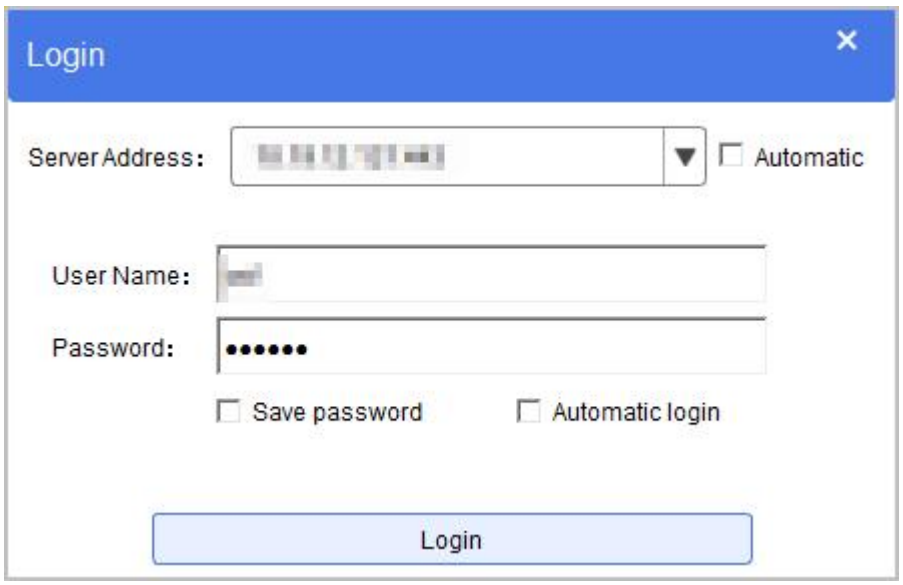
Step 3 Click **Import**, select the prepared profile, and click **Open**.

Step 4 Click **OK** to return to the UniVPN main page.

You can see that the UniVPN VPN connection has been generated. Click **connection** in the upper right corner or double-click the VPN connection to establish the connection.

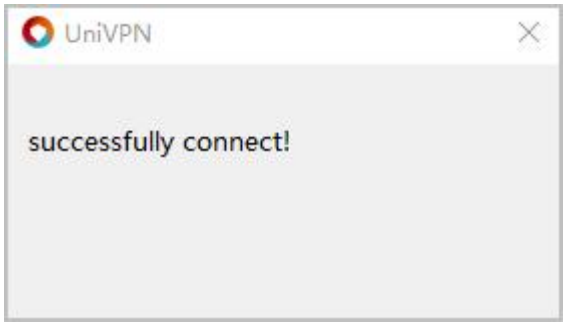


Step 5 On the login page, enter the user name and password.



Step 6 Click **Login** to initiate a VPN connection.

When the VPN access succeeds, a prompt is displayed at the lower right corner of the screen.



Using the connection, the mobile user can access intranet resources as users in the enterprise intranet.

----End

5.2 Common Settings

This section describes common functional settings of the UniVPN.

Connect/Disconnect

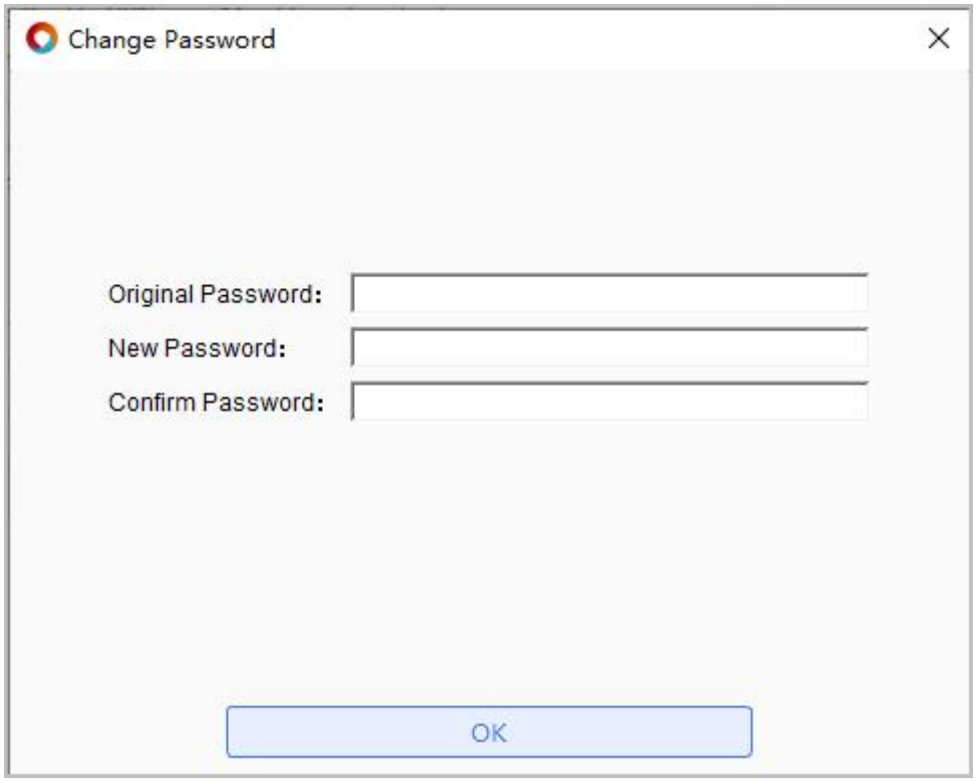
On the main page of the UniVPN client, click **connection** in the upper right corner to directly initiate a tunnel establishment request to the VPN gateway. You can click **Disconnect** in the upper right corner of the page to disconnect the current VPN tunnel.

Change Password

On the main page of the UniVPN client, click in the upper right corner and choose **Change Password** from the menu to change the login password of the current user.

NOTE

- You can change the password only when a VPN tunnel is established between the UniVPN and device. If there is no VPN tunnel in between, the **Change Password** menu is unavailable. In addition, changing the password interrupts the existing service and requires re-login. Exercise this operation with caution.
- The password change function is supported only in SSL VPN scenarios.



Error Report

When you encounter a fault that you cannot rectify, contact technical support personnel. To help technical support personnel with fault location, collect error reports of the UniVPN in advance.

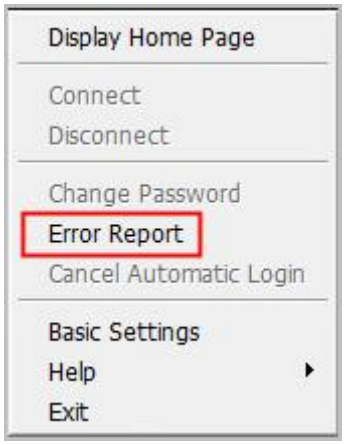
NOTE

In the generation of error reports, the UniVPN collects usage information of the client software. Take proper measures to ensure that the following information is strictly protected.

- **netcard_info.txt**: contains the network adapter information of the device. You can view this file in the **UniVPN** folder.
- **operate_system_info.txt**: contains the operating system information of the device. You can view this file in the **UniVPN** folder.
- **route_info.txt**: contains route information of the device. You can view this file in the UniVPN folder.
- **UniVPN_UniVPNCS_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. You can view this file in the **UniVPN/log** folder.
- **UAA_0**: records the gateway connection success or exception logs. You can view this file in the **log** folder.
- **UniVPNTray_0**: records the logs generated for the operations performed on the tray. You can view this file in the **log** folder.
- **UniVPN_UniVPNUI_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. You can view this file in the **log** folder.
- **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. You can view this file in the **log** folder.

- 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. You can view crash files in the **log** folder.

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



Step 2 Select **Error Report**.

Step 3 Click **OK**.

After the error report is generated, you can send the report to technical support personnel through email, USB disk, or other means for them to rectify the fault.

----End

Cancel Auto Login

Right-click the tray icon of the UniVPN and choose **Cancel Automatic Login** from the menu to cancel the automatic login setting.

Setting

Step 1 Click in the upper right corner of the UniVPN home page and choose **Setting** from the menu. Alternatively, right-click the tray icon of the UniVPN and choose **Setting** from the shortcut menu. Then, set parameters.

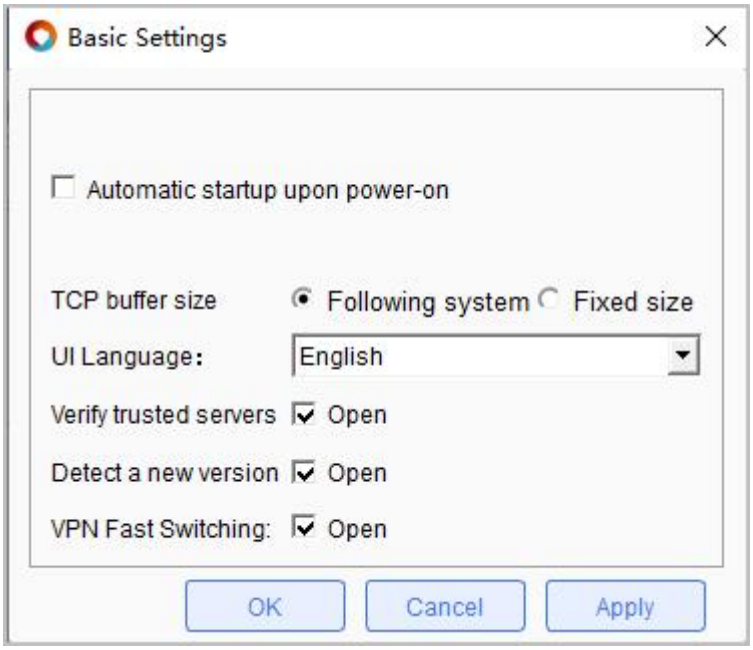


Table 5-7 Parameter description

Parameter	Description
Auto Start	After you select this item, the UniVPN automatically starts when you start the PC. By default, this item is not selected.
Verify trusted servers	When the UniVPN establishes an SSL VPN tunnel with the device, the UniVPN verifies the device certificate sent from the device. • Item selected When the device certificate of the device fails to be verified by the UniVPN, the system displays **Gateway certificate verification: Untrusted VPN server certificate!** for your confirmation. If you are sure about the network security, select **Continue** to continue the SSL VPN tunnel establishment. If you are unsure about the network security, select **Cancel** to terminate tunnel establishment. • Item not selected When the certificate fails to be verified, the system does not prompt an alarm, and the tunnel is established. By default, this item is selected.
Detect a new version	After this option is selected, the system checks whether the gateway to be connected has a new UniVPN version. By default, this item is selected.
Interface language	The Interface language can be manually switched. The UniVPN provides two species of language, including: • English

Parameter	Description
	• Chinese • Follow system **NOTE** When the client runs for the first time, if the operating system language is one of the supported two types of Interface languages, the client Interface language is the same as the operating system language. If the operating system language is beyond the supported language scope, the client Interface language is English by default.
VPN Fast Switching	The UniVPN client supports fast switching between VPN connections through the tray menu and floating window. • Select this option. After the UniVPN client is started, you can switch between different VPN connections through the floating window on the desktop or by choosing Tray Menu > Switch Network. • Deselect this option. The client does not have a floating window and the tray menu does not have the network switch option. By default, this option is not selected.

Step 2 Click **OK**.

----End

VPN Fast Switching

The UniVPN client supports fast switching between VPN connections through the tray menu and floating window.

Click in the upper right corner of the client and choose Settings from the menu that is displayed. The VPN fast switchover option is provided. Select this option to switch between different VPN connections through the floating window and tray menu.

Proxy Shielding

- In the Windows system:

  The Windows operating 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 OS 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.

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.

About

Right-click the tray icon of the UniVPN and choose **About** from the menu.

The **About** item records the UniVPN version and proprietary information.

Help

Right-click the tray icon of the UniVPN and choose **Help** from the menu.

The **Help** item includes the UniVPN usage guide that helps users to familiarize themselves with the UniVPN and rectify faults they encounter.

Exit

Right-click the tray icon of the UniVPN and choose **Exit** from the menu to close the software.

6 Upgrade

This section describes how to upgrade the UniVPN.

Context

The basic process for upgrading the UniVPN is as follows: The network administrator uploads the new UniVPN software to the device. When the user establishes a VPN tunnel with the device through the UniVPN, the UniVPN automatically checks whether a new version exists on the device. If yes, the system prompts the user to perform version upgrade.

Procedure

Step 1 Upload the UniVPN software installation package to the device.

1. 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.
2. Access the device management page, and choose **System** > **VPNClient Upgrade**.
3. Click **Locally Upgrade** next to the corresponding client software, click **Browse**, and select the UniVPN software installation package to be uploaded.

   Different UniVPN software installation packages are provided for the Windows, Linux and Mac operating systems. Therefore, the network administrator needs to upload the software installation package based on the operating system in use. If the software installation package does not match the operating system type, the system displays a message indicating an upgrade failure. The newly uploaded software installation package overwrites the previous software installation package.

   NOTE

   The USG6101/6305/6305-W/6310S/6310S-W/6310S-WL/6510/6510-WLUSG6305/6305-W/6310S/6310S-W/6310S-WL-OVS/6510/6510-WL does not provide the local upgrade function. The administrator needs to place the UniVPN software on a file server and then enters the URL address of the file server in network extension client address.

4. Click Upgrade to upgrade the software installation package on the device.

Step 2 Upgrade the UniVPN at the user side.

When the user establishes a VPN tunnel with the device, the user side automatically checks whether a new UniVPN version exists on the device. If yes, the user shall download and install the new version as prompted.

NOTE

When multiple users log in to the Linux or Mac operating system simultaneously, automatic upgrade is not supported.

7 Troubleshooting

This document describes only the basic configuration of the client. If you need to obtain scenario-specific configuration cases or encounter any problems during the use of the client, contact the corresponding sales personnel. We will resolve the problem as soon as possible.

8 FAQ

This section answers frequently asked questions in the usage of the UniVPN.

What If a VPN Disconnection Occurs After the System Time Is Changed?

In a scenario where the IPSec protocol is enabled, if you set the IPSec SA lifetime to a small value, modifying the system time may cause the SA to age and the VPN to be disconnected.

You are advised not to change the system time after enabling the IPSec protocol.

Can the UniVPN Be Used Together with Other VPN Dial-up Software Programs?

You are advised not to install or use multiple VPN dial-up software programs on a PC. Otherwise, an unexpected error may occur.

Why Does the UniVPN Installation Program Prompt Me to Uninstall the UniVPN in Its Operation?

This is because the UniVPN has already been installed earlier. The installation program needs to delete the previously installed version. After the deletion, you need to run the installation program again to install the UniVPN on the hard disk.

Why Do I Fail to Establish a VPN Connection for the First Time?

This is because the firewall of the operating system blocks your operation of establishing a VPN connection. Modify the access rule setting of the firewall to allow the operation.

Why Do I Fail to Install the UniVPN?

Check whether your account has the administrator permission. Only a user with the administrator permission can install the UniVPN.

Why Does the System Prompt a UniVPN Software Update Failure?

The system prompts a failure when a user updates the UniVPN software. The possible cause is that:

- The network administrator uploaded an incorrect UniVPN software package to the VPN gateway. Contact the administrator to check whether the software package format is correct.

- A NAT Server is deployed between the UniVPN and SSL VPN virtual gateway, the NAT Server cannot process UniVPN update messages, causing UniVPN update to fail.

9 Safety reinforcement

Introduce the security reinforcement measures adopted by VPN clients.

9.1 UniVPN Client Security Reinforcement

Use digital signature reinforcement. After reinforcement, it has security features such as anti decompilation, anti cracking, anti secondary packaging, and anti data leakage.

9.1.1 Anti tampering

Digitally sign the client application package and executable file, and extract the complete features of the file. If the client application package is tampered with or bundled with other content and republished, the digital signature will become invalid; If the digital signature of the installation package obtained is not from Shenzhen Lianruan Technology Co., Ltd., please do not install and use it.

9.2 Uniconnect Client Security Reinforcement

Use 360 for security reinforcement. After reinforcement, it has security features such as anti debugging, anti tampering, and anti decompilation.

9.2.1 Anti tampering

Generate file fingerprints for the code files, main configuration files, and resource files within the application package, extract the complete features of the files, and verify the file fingerprints and integrity during program operation. If a file is tampered with or does not match the original signature, the application will stop running, ensuring the security of the application operation.

10 Appendix

9.1 Using Commands to Configure the Client in the Linux System

9.2 Acronyms and Abbreviations

This lists the acronyms and abbreviations used in this documentation.

10.1 FAQs About the Mobile Client

In addition to the PC-based UniConnect client, Leagsoft 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 **Huawei AppGallery, Xiaomi AppGallery, oppo AppGallery,** and **vivo AppGallery** apps and search for **UniConnect** to download the latest version.

Specifications

Currently, the UniConnect mobile client supports only the 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
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
	Endpoint 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
	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

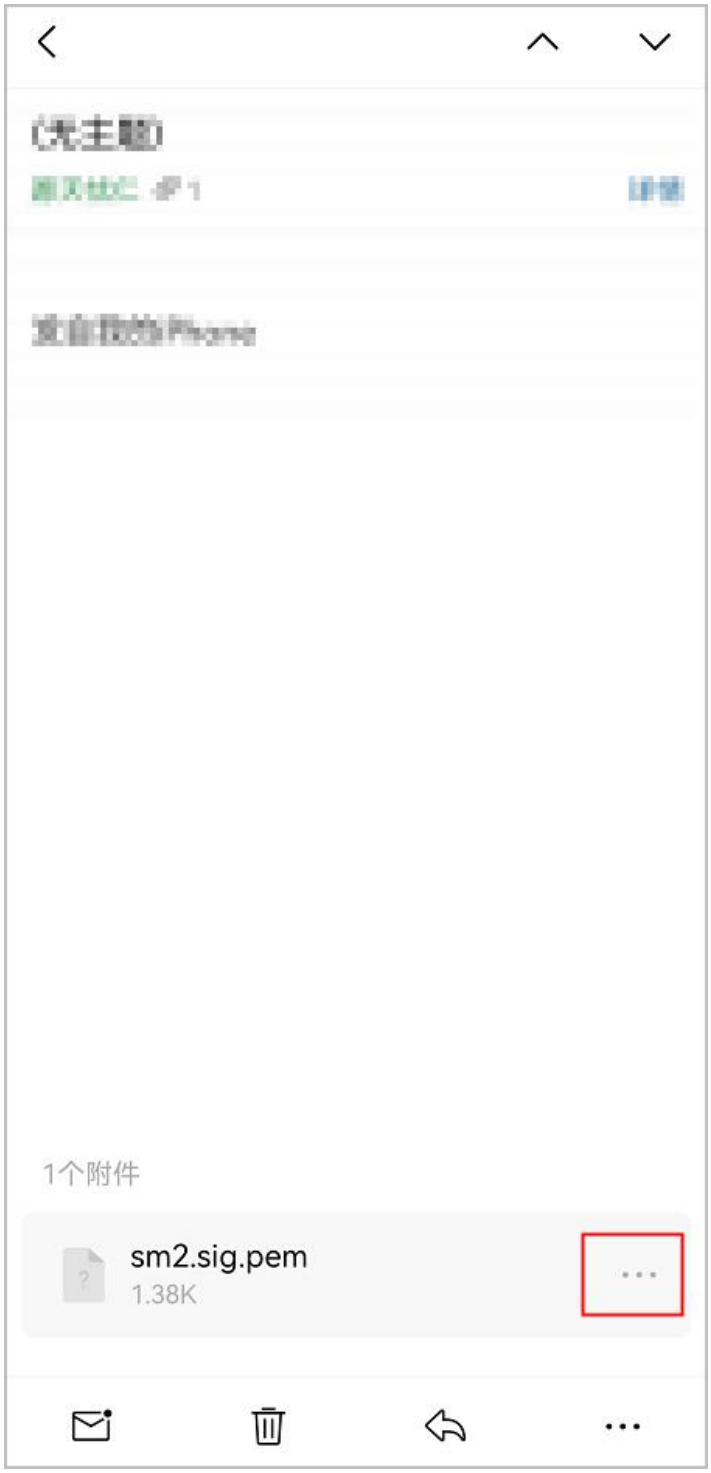
Operations

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

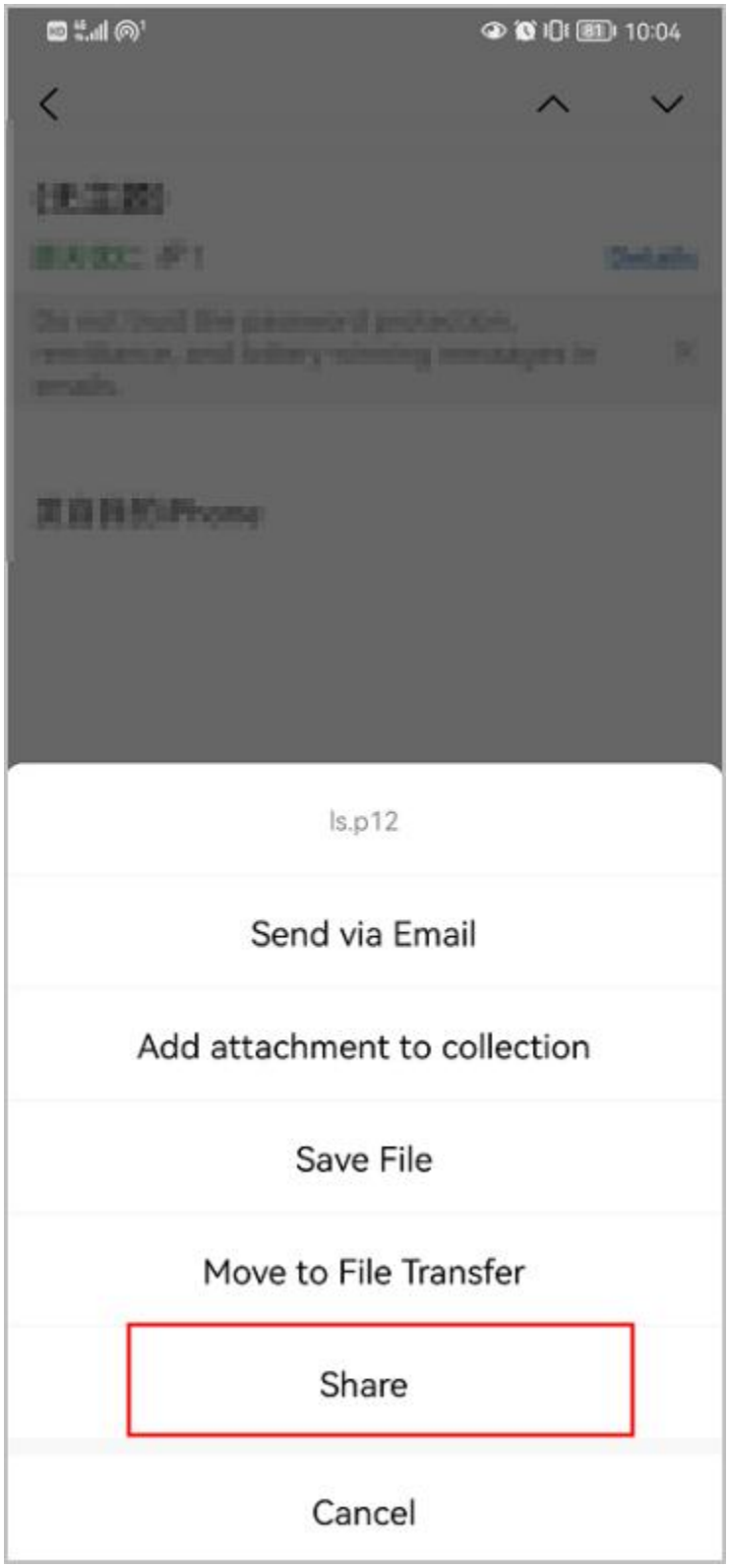
10.1.1 How Do I Import a Chinese Cryptographic Certificate?

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.

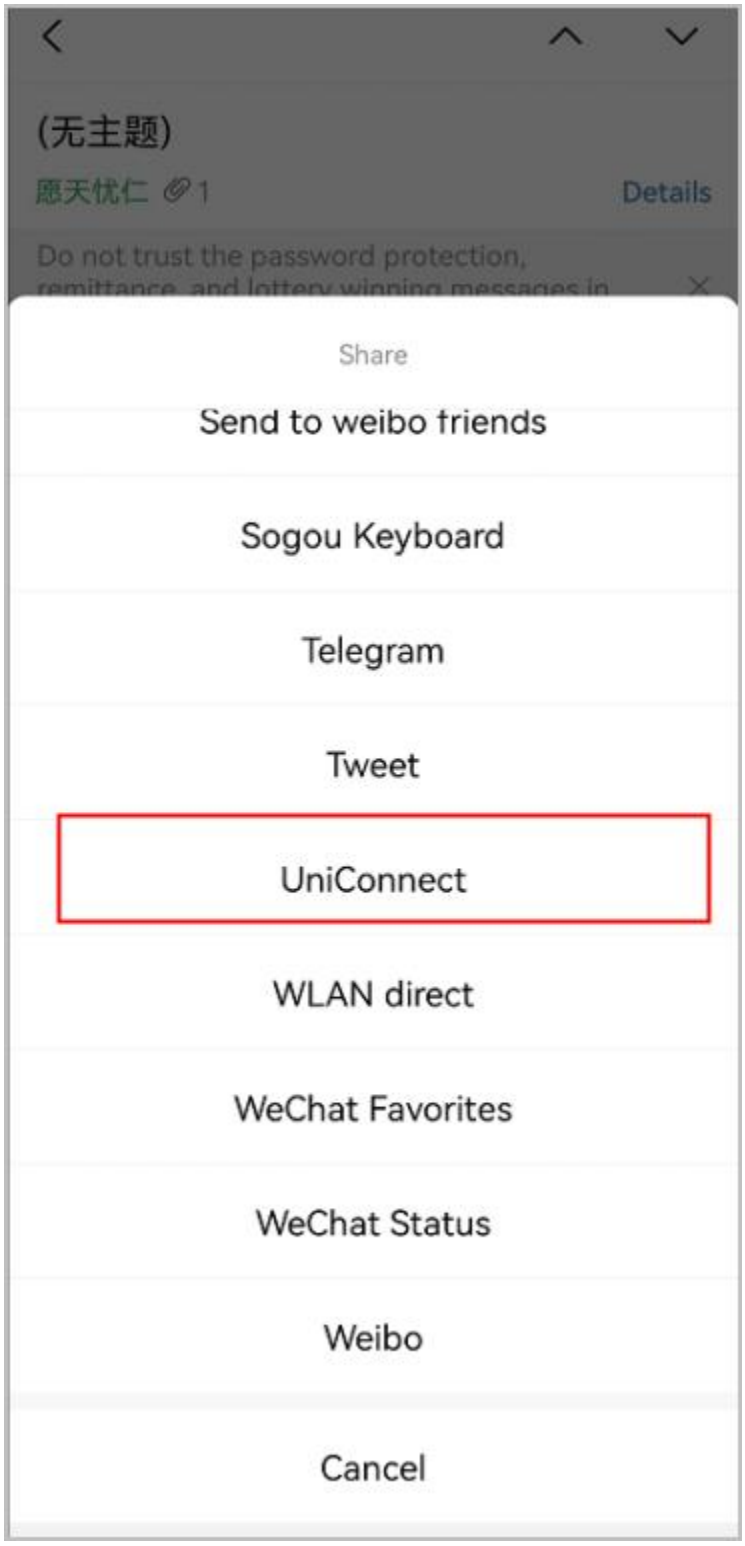
Step 1 Open your mailbox, find the certificate file, and click ··· in the lower right corner.



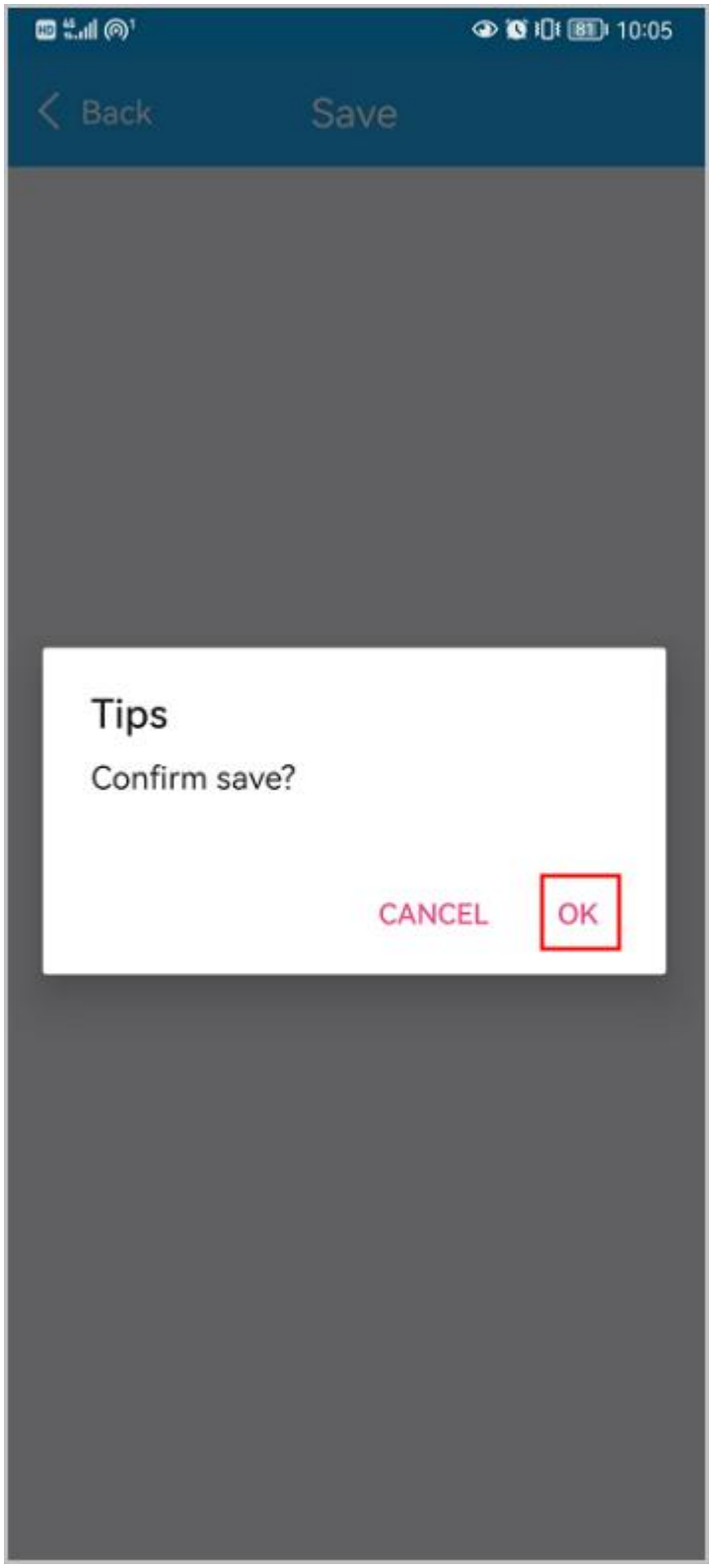
Step 2 Click the file (The download starts when the file is not downloaded) and click **Share**.



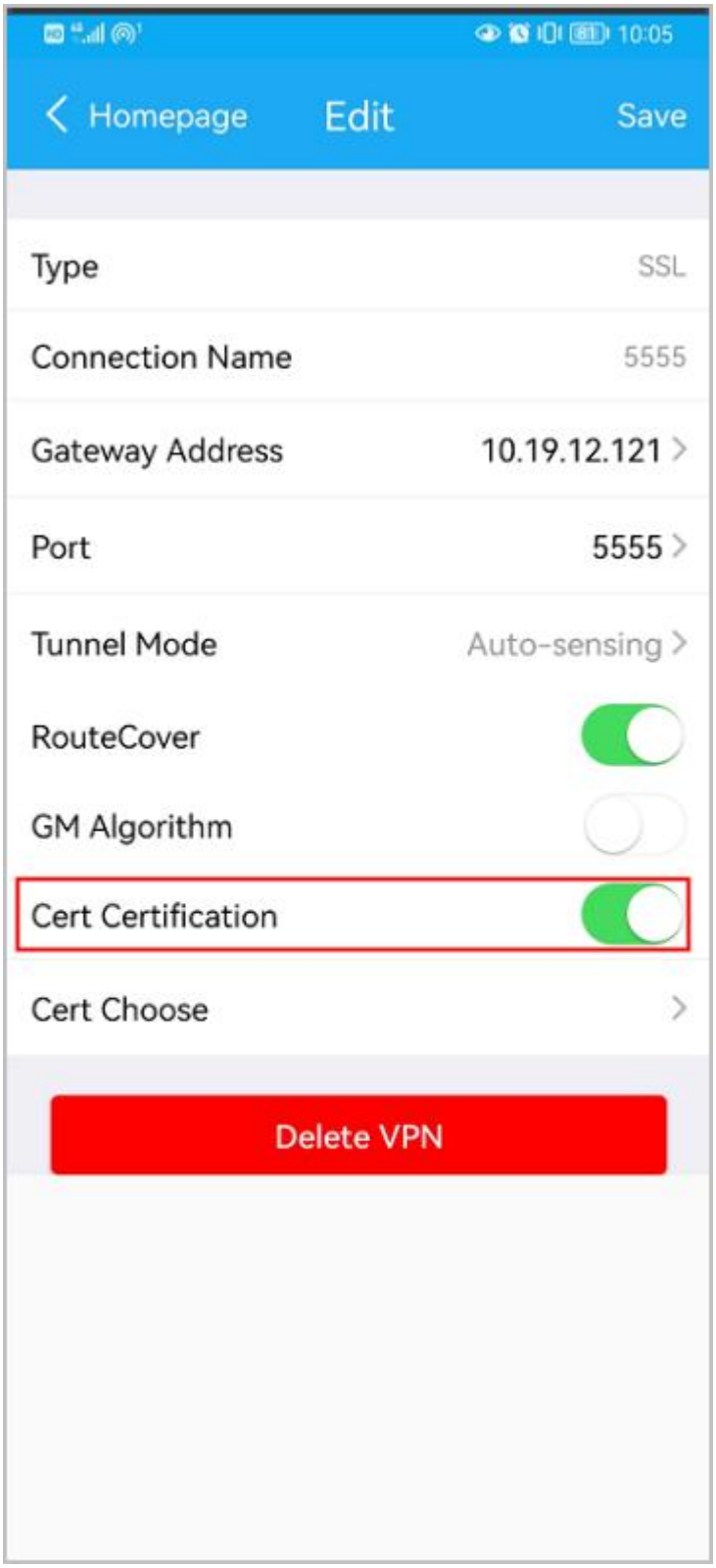
Step 3 Click **UniConnect**.



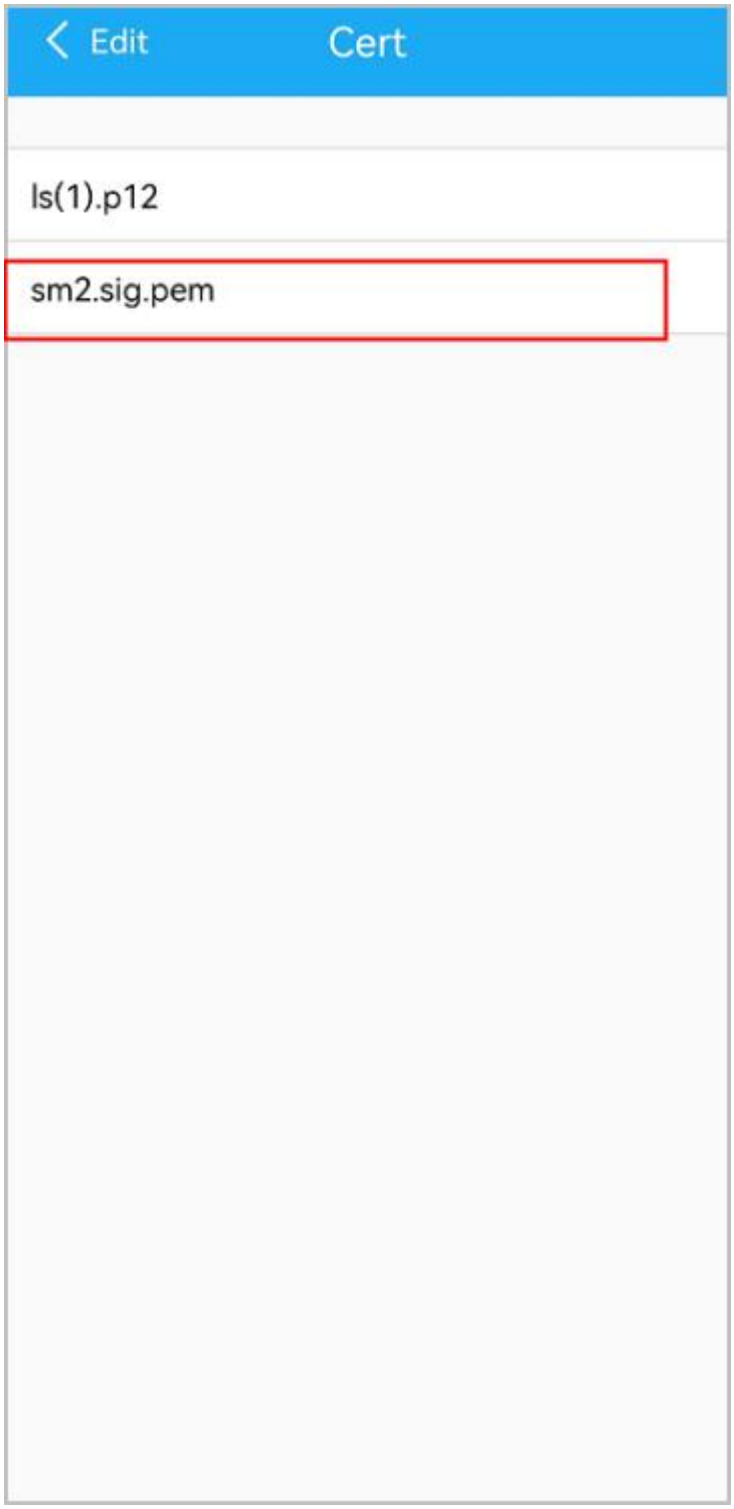
Step 4 Click **OK**.



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



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

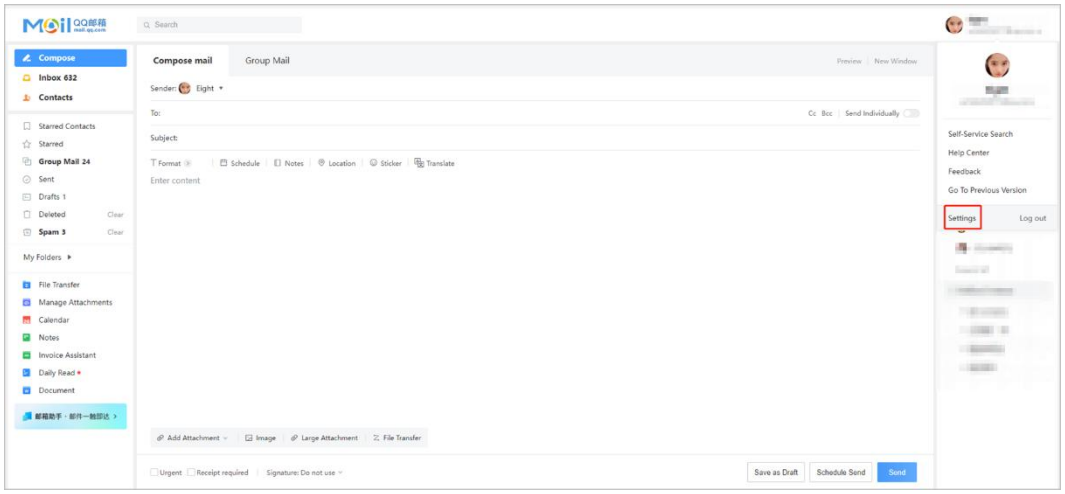


----End

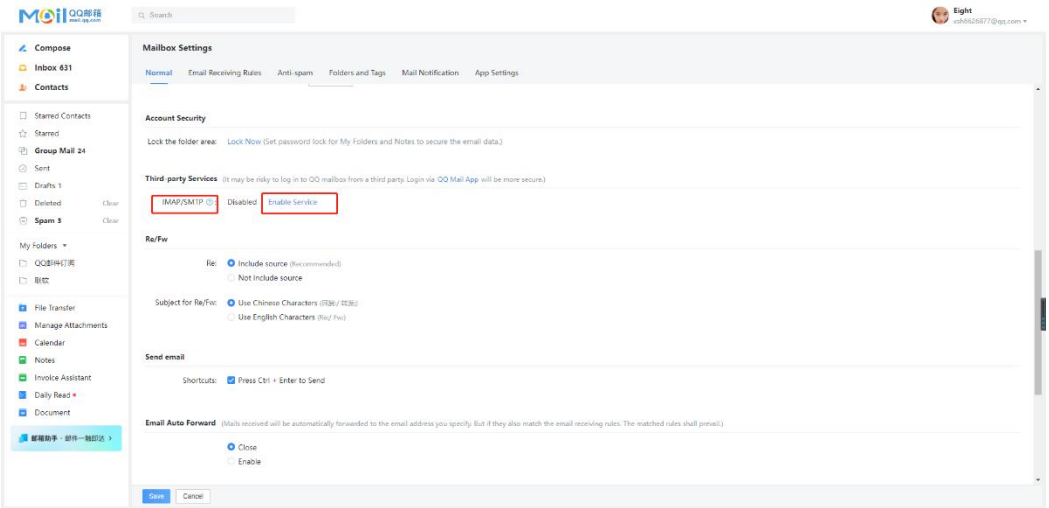
10.1.2 How Do I Report an iOS Client Problem?

Configuring the Mailbox

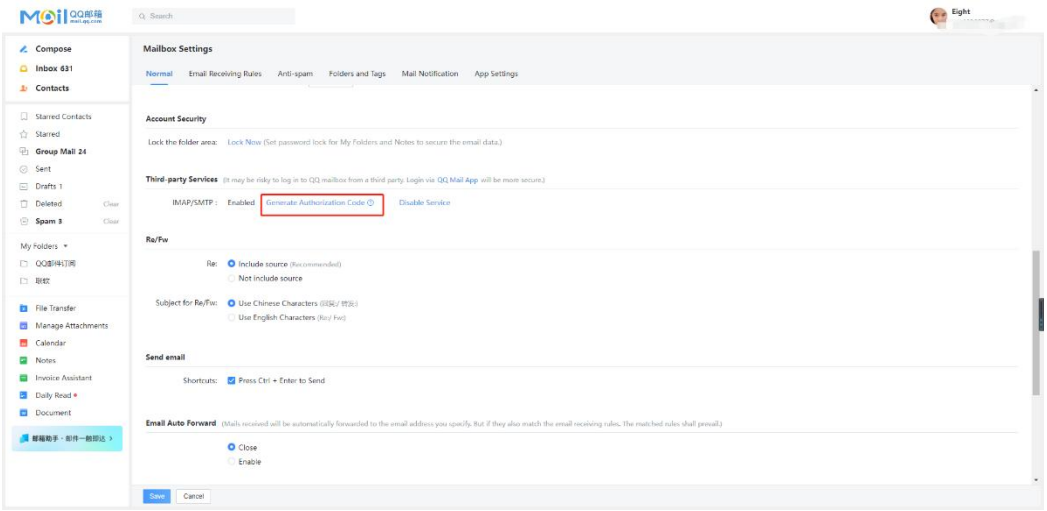
Step 1 Go to QQMail, click the user name in the upper right corner, and click **Settings**.

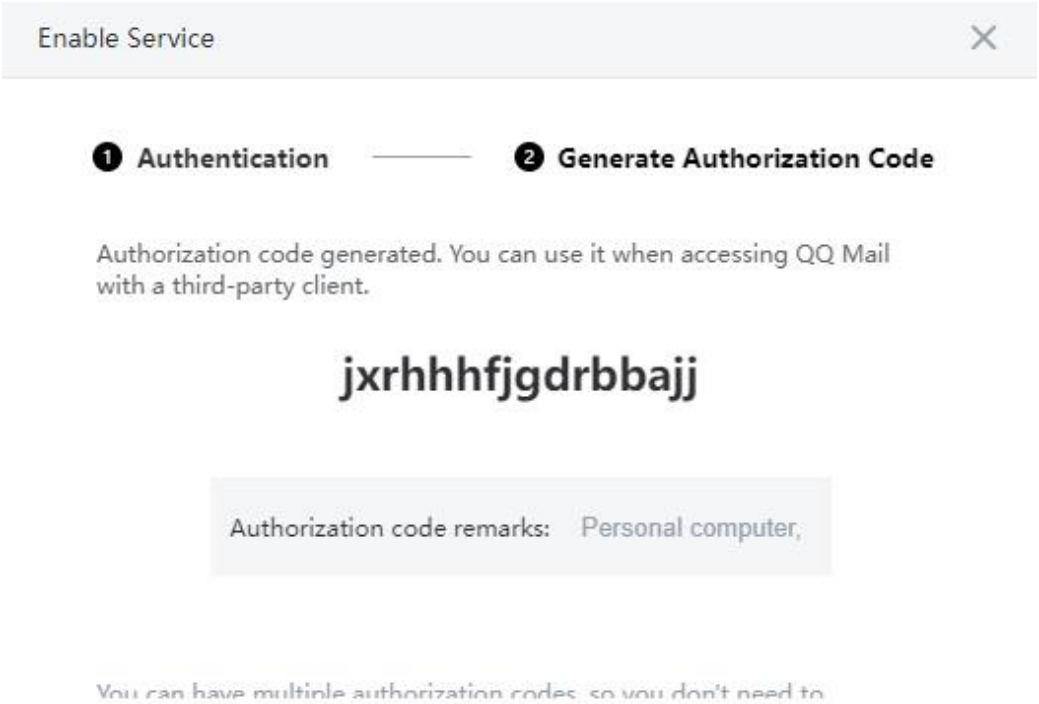


Step 2 On the **Normal** tab page, click **Enable Service** behind **IMAP/SMTP** to enable the IMAP service.



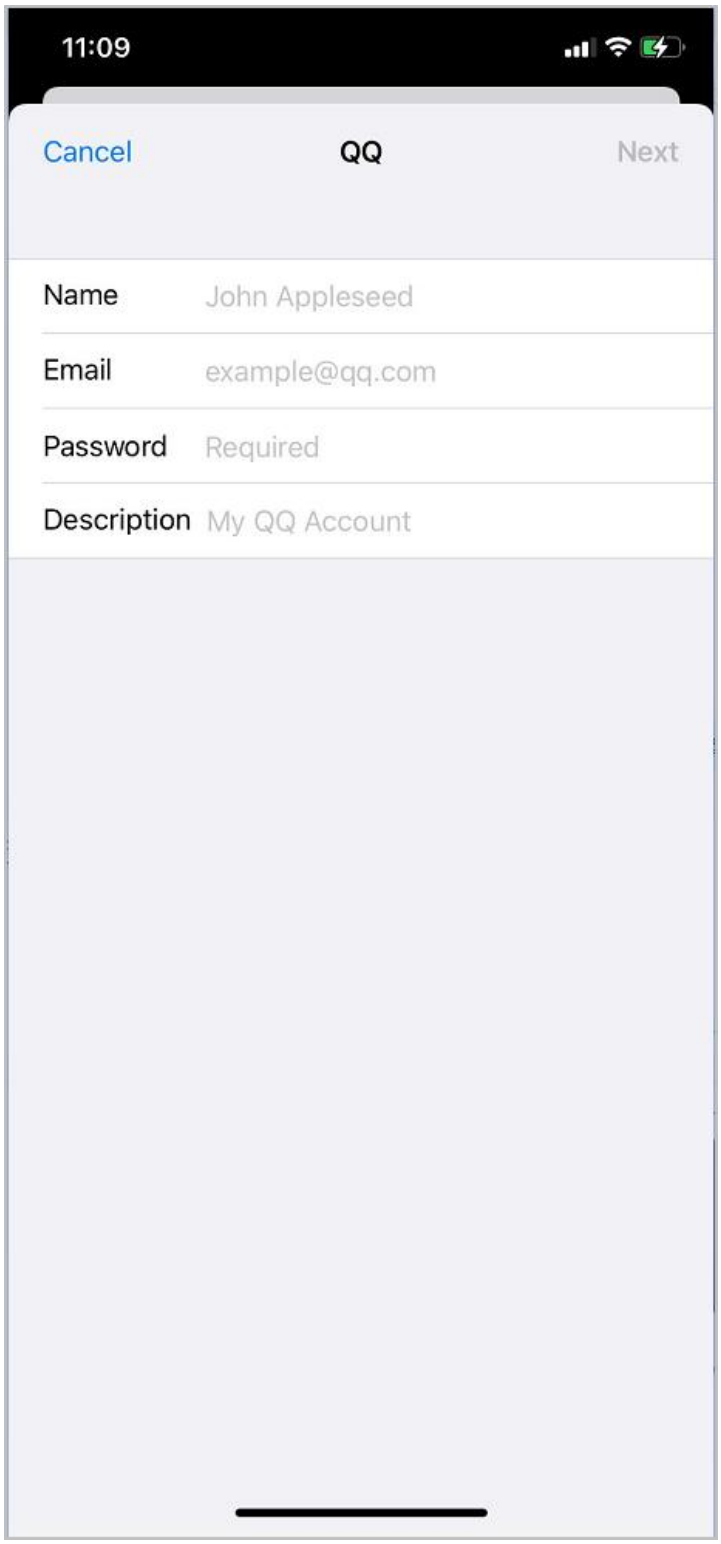
Step 3 Click **Generate Authorization Code** to obtain an authorization code.





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).



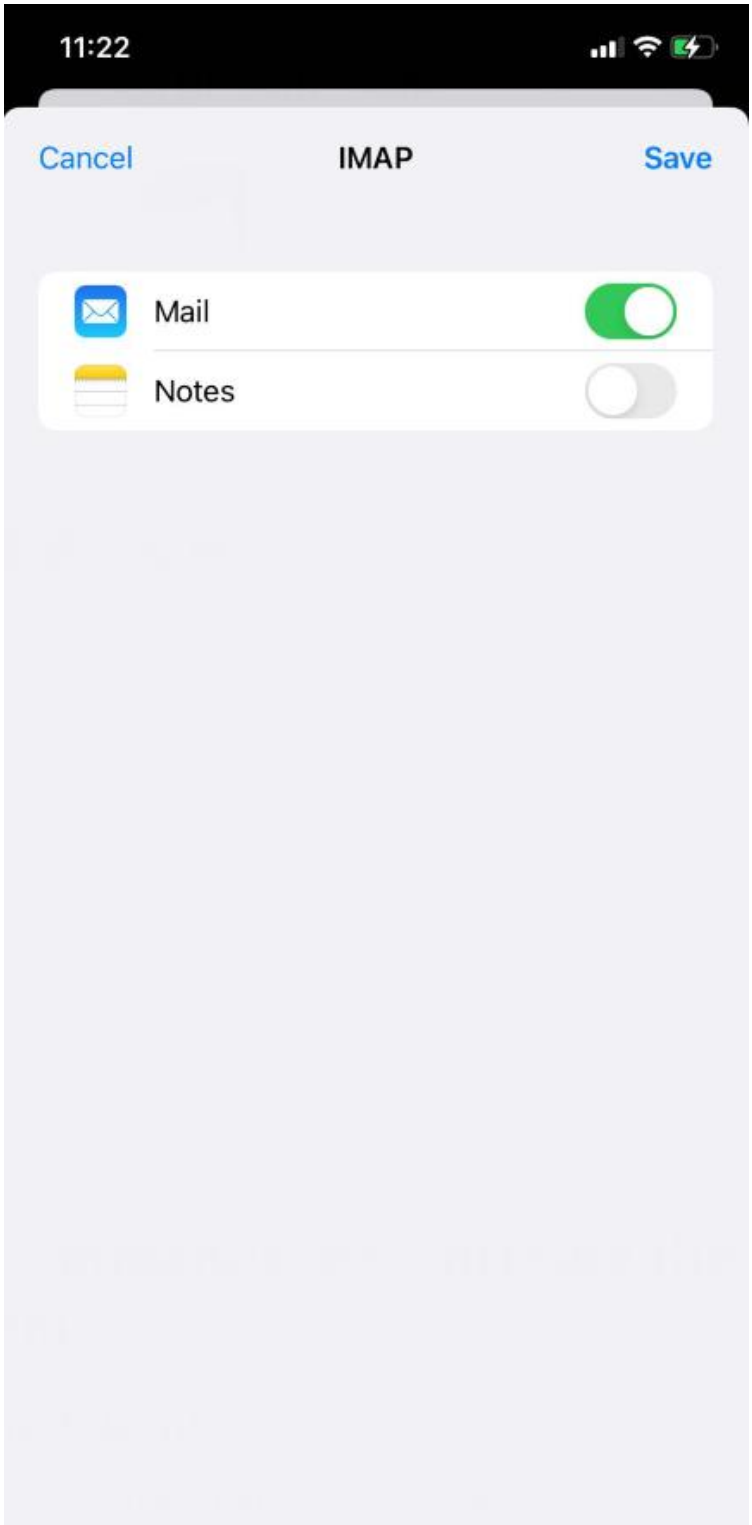
Step 6 Click **Next** in the upper right corner.

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**.



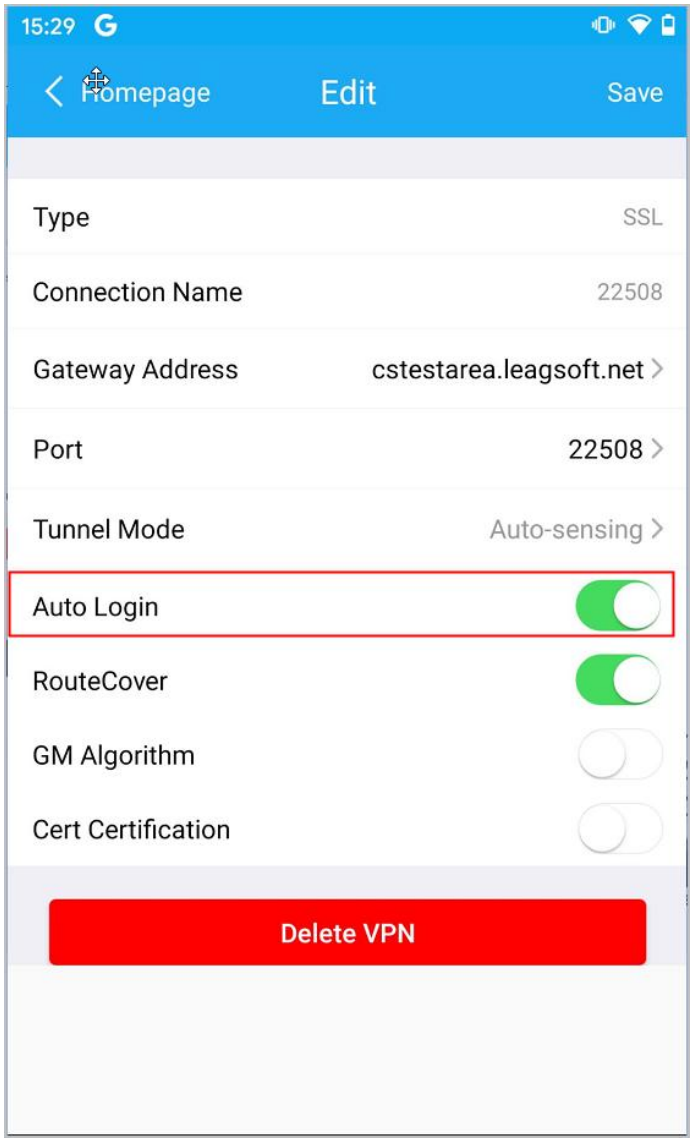
Step 1 After the configuration is successful, choose > **Feedback** on the login page of the UniVPN client to enable the feedback log function.

----End

10.1.3 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.



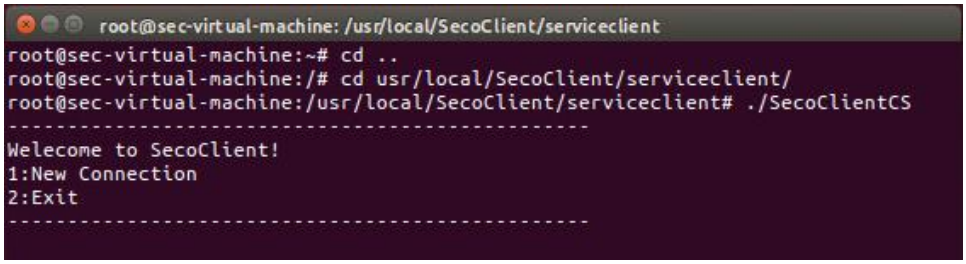
----End

10.2 Using Commands to Configure the Client in the Linux System

10.2.1 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.



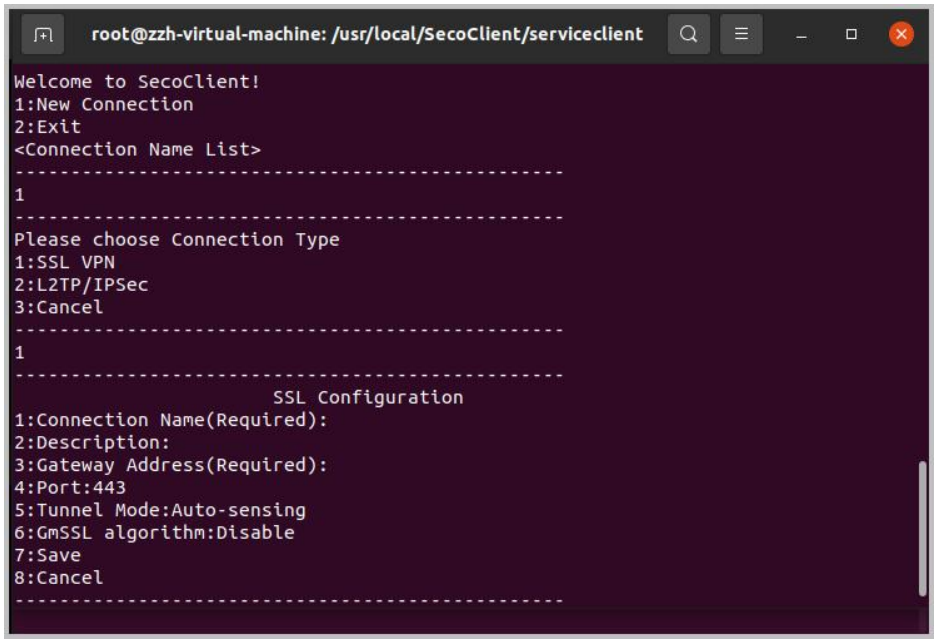
NOTE

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

----End

10.2.2 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.

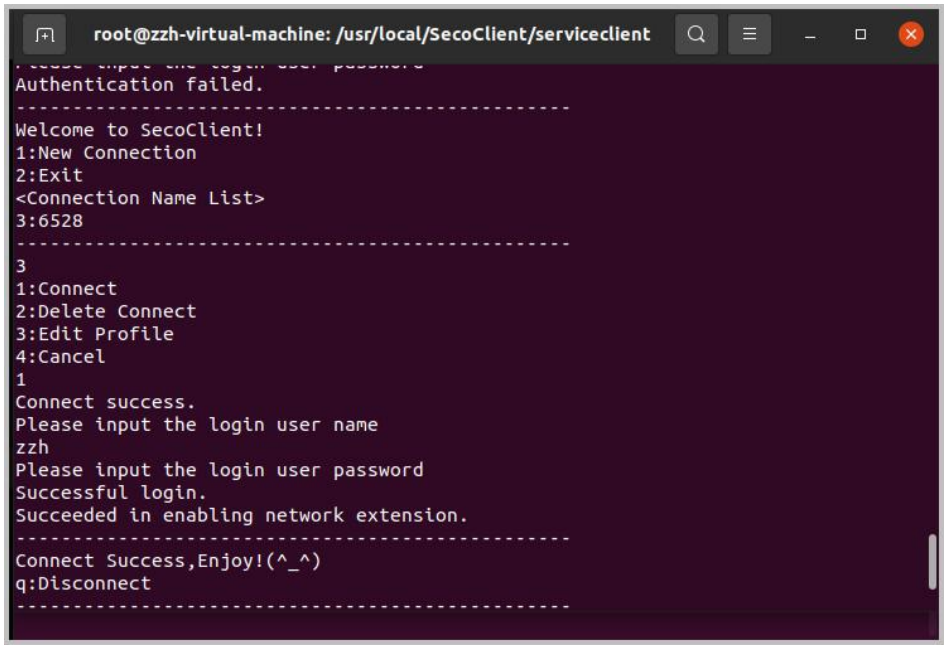
Step 3 Enter the corresponding sequence number to complete the configuration of parameters 1 to 5.

- 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**.

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

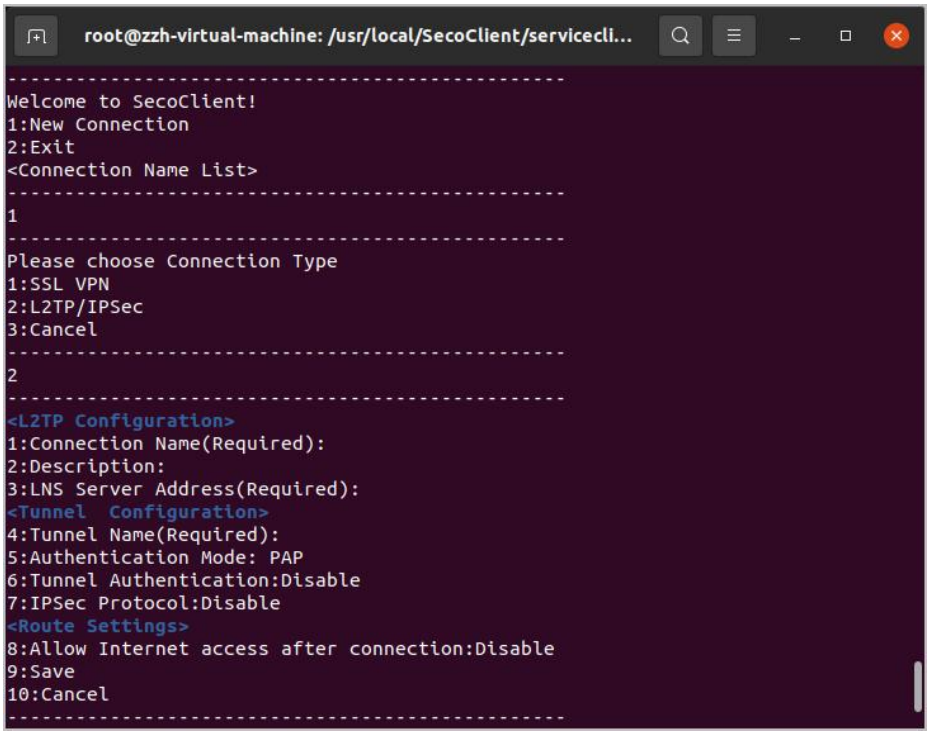
- In the Linux system, the SSL VPN connection configured and established using commands supports only user name/password authentication.
- After the connection is successful, do not close the terminal window. Otherwise, the connection will be disconnected.

SSL VPN Disconnection

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

10.2.3 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.

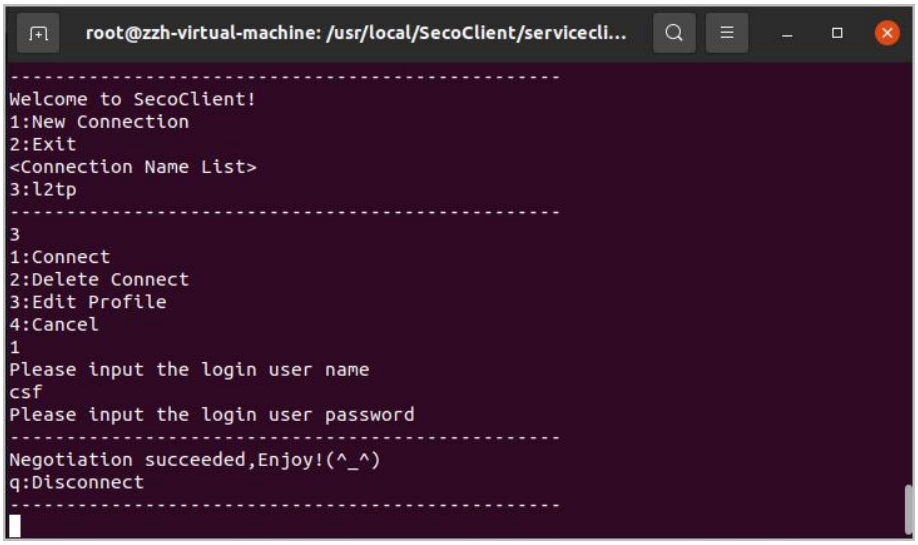
NOTE

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

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

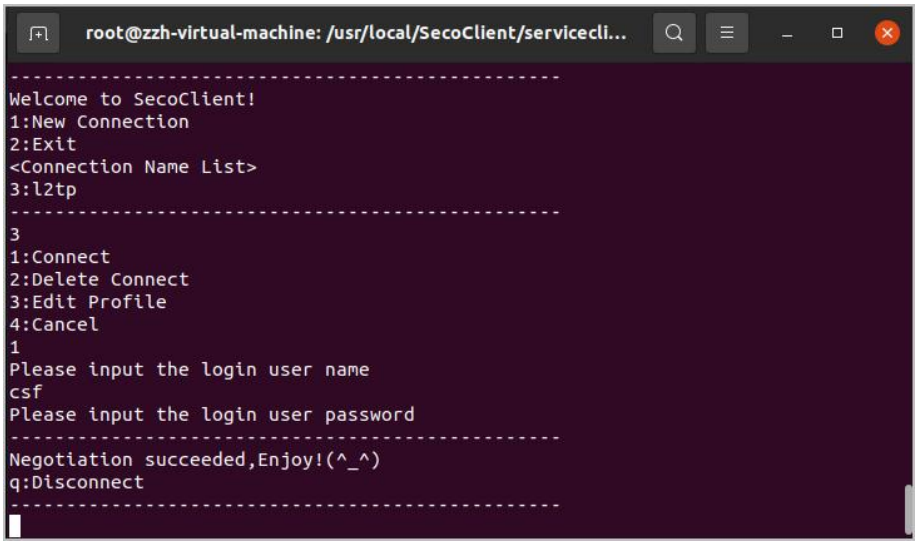
After the connection is successful, do not close the terminal window. Otherwise, the connection will be disconnected.

L2TP VPN Disconnection

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

10.2.4 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@zzh-virtual-machine: /usr/local/SecoClient/serviceclient
-----------------------------------------------
<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>
13:Negotiation Mode:Main Mode
14:Authentication Algorithm:SHA2-256
15:Encryption Algorithm:AES-256
16:DH Group ID:Group5(1536 bit)
<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.

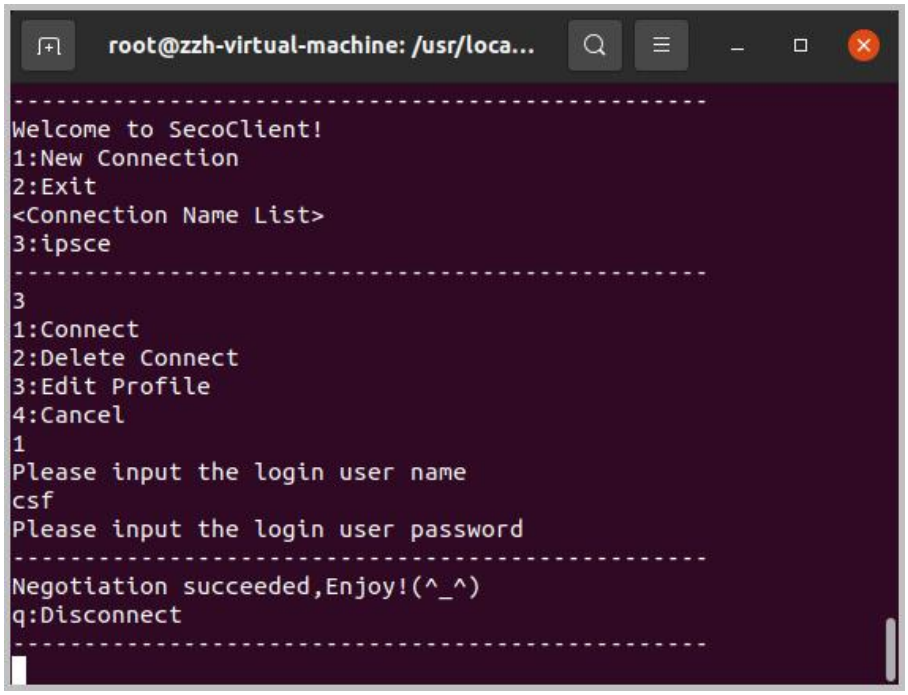
- 8. IPSec Authentication Mode: In the Linux system, IPSec supports only pre-shared key authentication. In pre-shared key authentication mode, the pre-shared key is required.
- 9. IPSec Server address: IP address of the IPSec server. By default, the IP address of the LNS server is used (Use LNS server 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.

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.

10.3 Acronyms and Abbreviations

This lists the acronyms and abbreviations used in this documentation.

Acronyms and Abbreviations	
A - E	
AES	Advanced Encryption Standard
AH	Authentication Header
CBC	Cipher Block Chaining
CHAP	Challenge Handshake Authentication Protocol
DES	Data Encryption Standard
DES-CBC	DES-Cipher Block Chaining
DH	Diffie-Hellman algorithm
DNS	Domain Name System
ESP	Encapsulating Security Payload
F - J	
ID	Identification/Identity
IKE	Internet Key Exchange
IP	Internet Protocol
IPSec	IP Security Protocol
K - O	
L2TP	Layer 2 Tunneling Protocol
LAC	L2TP Access Concentrator
LNS	L2TP Network Server
MD5	Message-Digest Algorithm 5
NAT	Network Address Translation
P - T	
PAP	Password Authentication Protocol

Acronyms and Abbreviations	
PC	Personal Computer
PFS	Perfect Forward Secrecy
PPP	Point-to-Point Protocol
SA	Security Association
SHA	Secure Hash Algorithm
U - Z	
VPN	Virtual Private Network