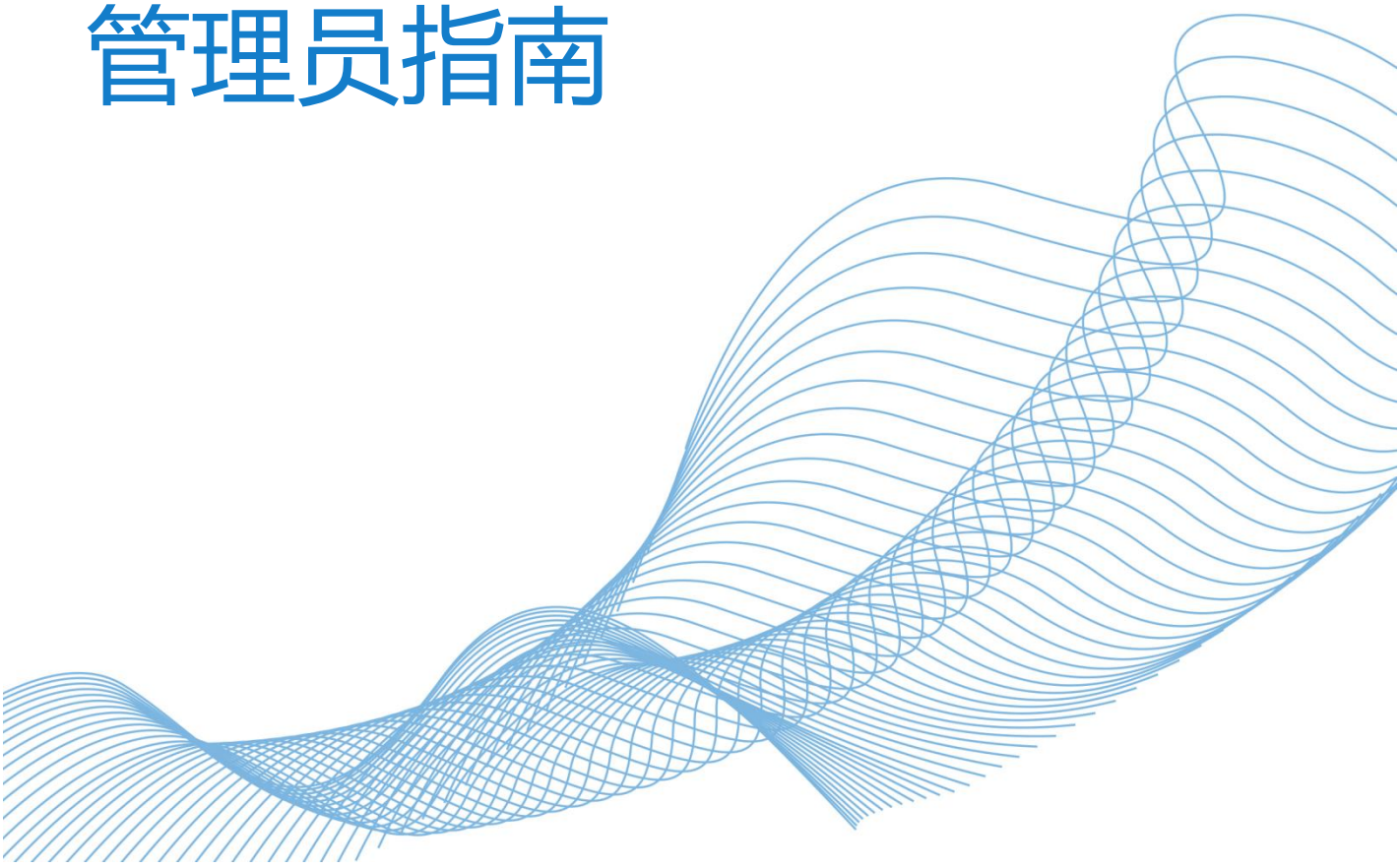
联软科技
LEAGSOFT

LeagSoft UniVPN 客户端

管理员指南



目 录

1 前言

读者对象

本文档适用于负责管理 UniVPN 和设备的网络管理员。您应该熟悉以太网基础知识，且具有丰富的网络管理经验。此外，您应该非常了解您的网络，包括 UniVPN 和设备工作的组网拓扑，以及承载在它们之上的网络业务等。

符号约定

在本文中可能出现下列标志，它们所代表的含义如下。

符号	说明
注意	用于传递设备或环境安全警示信息，若不避免，可能会导致设备损坏、数据丢失、设备性能降低或其它不可预知的结果。 “注意”不涉及人身伤害。
说明	用于突出重要/关键信息、最佳实践和小窍门等。 “说明”不是安全警示信息，不涉及人身、设备及环境伤害信息。

图形界面元素引用约定

在本文中可能出现下列图形界面元素，它们所代表的含义如下。

格式	意义
“”	带双引号“”的格式表示各类界面控件名称和数据表，如单击“确定”。
>	多级菜单用“>”隔开。如选择“文件 > 新建 > 文件夹”，表示选择“文件”菜单下的“新建”子菜单下的“文件夹”菜单项。

修订记录

修改记录累积了每次文档更新的说明。最新版本的文档包含以前所有文档版本的更新内容。

- **文档版本 02 (2022-07-30) 产品版本 10781.3**

  第二次正式发布。

  UniVPN 客户端新增支持系统：Windows11。

  UniVPN 客户端国产化系统安装包变更为**.deb** 格式。

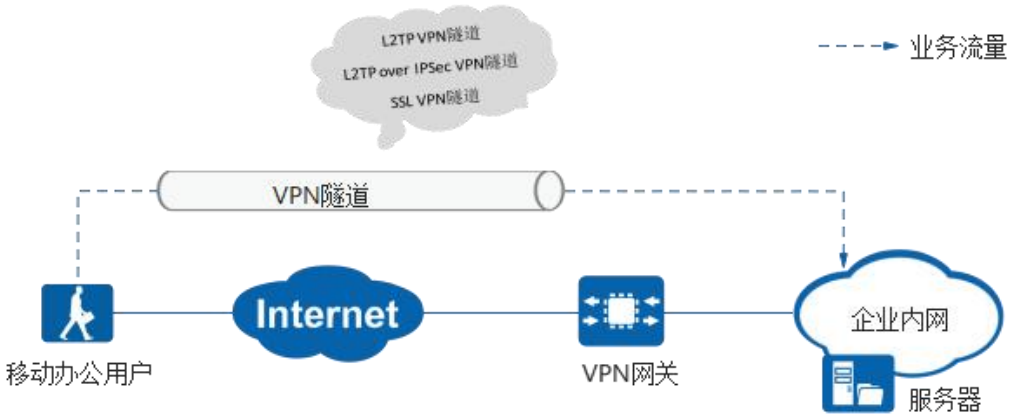
- **文档版本 01 (2022-03-18) 产品版本 10781.2**

  第一次正式发布。

2 简介

UniVPN 是深圳市联软科技股份有限公司推出的一款用于 VPN 远程接入的终端软件，主要为移动办公用户远程访问企业内网资源提供安全、便捷的接入服务。典型的应用场景如图 2-1 所示。

图 2-1 移动办公用户使用 UniVPN 通过 VPN 隧道访问企业内网



UniVPN 具备以下几个特点：

- 强大的接入能力

  UniVPN 集成了 SSL VPN、L2TP VPN 和 L2TP over IPSec VPN 三大主流的 VPN 接入技术，可以满足用户在不同场景下的 VPN 接入需求。用户无需为不同的 VPN 接入场景购置多种终端软件，有效节约了投资成本。

- 灵活的隧道分离技术

  可以支持移动办公用户在访问企业内网资源的同时，还可以访问 Internet 和本地局域网。各种业务流量之间互不影响，避免了业务冲突。

- 智能的网关优选

  大型企业通常对外会提供多个 VPN 网关，用以支撑大量的用户访问。当一台 VPN 网关接入的用户数较多时，往往会出现系统资源不足，接入响应延迟，用户超额被迫下线等现象，影响了用户体验。移动办公用户使用 UniVPN 的网关优选功能，可以支持在多个 VPN 网关中自动选择一个响应速度最快的网关进行接入。使用网关

优选功能，用户对 VPN 网关的选择带有一定的随机性，各个用户的接入请求会被负载到不同的 VPN 网关上，有效缓解了单台 VPN 网关在面对大量用户接入时的性能瓶颈。同时，该功能也提高了用户的接入速度和成功率。

- 可靠的链路备份

  在 SSL VPN 的接入场景中，一台 VPN 网关可能会对外提供多个 IP 地址（一个 IP 地址对应一条链路）供移动办公用户接入使用。UniVPN 可以在当前 SSL VPN 隧道出现异常中断的情况下，自动与该网关的其他 IP 地址重新建立 VPN 隧道。新的 VPN 隧道建立成功后，业务流量通过新建隧道继续传输，减少网络故障对业务带来的冲击，保证了用户业务的接续。

- 丰富的认证方式

  通常情况下，VPN 网关会对移动办公用户的身份认证提供多种不同的认证方式，VPN 终端软件支持认证方式的多少，决定了这款软件所能满足的应用场景的多少。UniVPN 提供了用户名和密码认证、证书匿名认证、证书挑战认证、双因子认证等多种身份认证方式，因此可以覆盖多数的 VPN 接入场景。

功能列表

UniVPN 提供的功能列表如表 2-1 所示。

表 2-1 UniVPN 的功能列表

功能名称		说明
SSL VPN	网络扩展	网络扩展功能可以在移动办公用户与 SSL VPN 网关之间建立安全的 SSL VPN 隧道，实现用户对企业内网资源的全面访问。网络扩展功能支持两种 SSL VPN 隧道建立模式：可靠传输模式和快速传输模式。

功能名称		说明
	终端安全	终端安全功能可以防止非法终端接入，降低不安全终端对企业网络的威胁。终端安全包含了如下两部分内容： • 主机检查 用于检查移动办公用户所使用终端的操作系统、端口、进程以及杀毒软件等是否符合安全要求，不符合要求的终端禁止接入企业内网。同时，主机检查还具备防跳转、防截屏的能力，消除了潜藏在用户终端上的安全隐患。 • 缓存清理 用于清理远程用户访问企业内网过程中在终端上留存的访问痕迹，加固了用户的信息安全。 需要说明的是，终端安全功能是由VPN 网关侧来完成的，UniVPN 及其所在终端作为被检查对象，无需做任何配置。
	网关优选	如果企业对外提供了多个 SSL VPN 网关，启用自动优选功能可以保证用户连接到响应最快的那台虚拟网关。该功能提高了用户的接入速度和成功率，也缓解了单台 VPN 网关在面对大量用户接入时的性能瓶颈。
	断线重连	当 SSL VPN 隧道异常中断时，UniVPN 会自动每隔 5 秒向 SSL VPN 网关发送一次连接请求，3 次连接请求过后，隧道依然无法恢复时，重连功能终止。
	链路备份	当 UniVPN 与一台对外提供了多个 IP 地址的 SSL VPN 网关建立 VPN 隧道时，UniVPN 会自动记录该虚拟网关的所有 IP 地址。如果初始建立的 SSL VPN 隧道出现故障，UniVPN 将会进行断线重连，3 次重连失败，UniVPN 将会与该网关提供的其他 IP 地址建立 SSL VPN 隧道。 链路备份功能有效解决了虚拟网关多 IP 场景下隧道可靠性问题，减少了网络故障给业务造成的影响。

功能名称		说明
	路由覆盖	当对端网关下发的路由和本地已经存在的路由的目的地址和子网掩码完全相同时，如果启用了路由覆盖功能，则对端网关下发的路由会覆盖本地已经存在的路由，避免本地路由冲突造成网络访问异常。
	国密算法	客户端支持使用国密算法与对端网关建立 SSL VPN 连接。 国密算法是由国家密码管理局编制的一种商用密码分组标准对称算法，国密算法的分组长度和密钥长度都为 128bit。在安全级别要求较高的情况下，使用国密算法可以充分满足加密需求。
	双因子认证	客户端支持 Token 序列号和短信验证码两种双因子认证方式。 此功能在第三方认证服务器认证的组网场景下会被触发。当用户输入用户名、密码进行登录时，需要在弹出的输入框中输入 Token 序列号或短信验证码进行双因子认证。
L2TP VPN		L2TP VPN 是一种二层隧道协议，它提供了对 PPP 链路层数据帧的隧道传输支持，并依托 PPP 功能完成了用户接入认证。L2TP VPN 的不足是自身没有加密功能，缺少安全保护。 其中 PPP 协议在身份认证时支持 PAP 和 CHAP 两种认证方式。
L2TP over IPSec VPN		L2TP over IPSec 是 IPSec 应用中一种常见的扩展方式，它可以综合两种 VPN 的优势，通过 L2TP 实现用户验证和地址分配，并利用 IPSec 保障隧道安全。
NAT 穿越		如果 VPN 报文转发路径上存在 NAT 设备，VPN 隧道两端的设备必须要支持并启用 NAT 穿越功能，才能保证业务畅通。 UniVPN 提供的 SSL VPN、L2TP VPN、L2TP over IPSec VPN 都支持 NAT 穿越功能，且该功能默认开启。

功能名称		说明
代理穿越		一些企业下的用户可能会使用代理服务器来访问 Internet，在该场景下用户发出的报文都会交由代理服务器转发出去，并最终到达对端 VPN 网关。UniVPN 可以在用户使用代理服务器的情况下，与对端 VPN 网关建立 SSL VPN、L2TP VPN、L2TP over IPSec VPN 隧道。
隧道分离		隧道分离是 VPN 的一种应用场景，是指用户在使用 VPN 隧道访问远端企业内网的时候，还可以访问 Internet 和本地局域网。 UniVPN 提供的 SSL VPN、L2TP VPN、L2TP over IPSec VPN 都支持隧道分离功能。
基本功能	开机自启动	开机后 UniVPN 随系统启动并显示主界面。
	界面语言切换	目前支持 2 种界面语言，包括： • 英语 • 简体中文 • 跟随系统 **说明** 安装时界面语言默认跟随系统，非中英文以外的系统语言默认界面语言为英文。
	自动登录	首次登录 VPN 网关后，UniVPN 会记住用户名和密码。后续客户端重启时会自动连接上次登录成功且开启自动登录的网关，无需操作。
配置文件	导入	UniVPN 支持将已经创建好的 VPN 连接制作成配置文件。用户只需将配置文件导入到 UniVPN 即可使用，节省了用户创建 VPN 连接的时间。
	导出	导出功能用于将已经创建好的 VPN 连接制作成配置文件，方便其他用户使用。
命令行配置		支持在 Linux 操作系统下通过命令行方式创建 SSL VPN、L2TP VPN、L2TP over IPSec VPN 连接。
非管理员权限用户配置		支持非管理员权限的用户使用客户端完成配置和建立 VPN 连接。

功能名称	说明
故障定位	通过查看运行状态、收集日志和错误报告，用户可以了解 UniVPN 的运行过程、分析网络状况以及定位问题发生的原因，为后续故障诊断和维护提供依据。

说明

- 上表列出的 UniVPN 客户端全部功能，在和不同版本的设备对接时部分功能可能不支持。

3 产品规格和使用限制

介绍服务器设备和 UniVPN 客户端的产品规格和使用限制。

配套产品及版本

产品名称	产品版本	操作系统
USG6000	V500R005C20SPC500 及以后版本	• Windows • Linux • Mac OS • 国产化
USG9500	V500R005C20SPC500 及以后版本	• Windows • Linux • Mac OS • 国产化
USG6000E	V600R007C20SPC300 及以后版本（SPC301/SPC 302 版本除外）	• Windows • Linux • Mac OS • 国产化
Eudemon200E-N	V500R005C20SPC500 及以后版本	• Windows • Linux • Mac OS • 国产化
Eudemon200E-G	V600R007C20SPC300 及以后版本（SPC301/SPC 302 版本除外）	• Windows • Linux • Mac OS • 国产化

产品名称	产品版本	操作系统
Eudemon1000E-N	V500R005C20SPC500 及以后版本	• Windows • Linux • Mac OS • 国产化
Eudemon1000E-G	V600R007C20SPC300 及以后版本（SPC301/SPC 302 版本除外）	• Windows • Linux • Mac OS • 国产化
Eudemon8000E-X	V500R005C20SPC500 及以后版本	• Windows • Linux • Mac OS • 国产化
SeMG9811	V500R005C20SPC500 及以后版本	• Windows • Linux • Mac OS • 国产化
NGFW Module	V500R005C20SPC500 及以后版本	• Windows • Linux • Mac OS • 国产化
USG12000	V600R021C10 及以后版本	• Windows • Linux • Mac OS • 国产化
USG6000F	V600R021C10 及以后版本	• Windows • Linux • Mac OS • 国产化
Eudemon9000E-X	V600R021C10 及以后版本	• Windows • Linux • Mac OS • 国产化
Eudemon9000E-F	V600R021C10 及以后版本	• Windows • Linux • Mac OS • 国产化

产品名称	产品版本	操作系统
Eudemon1000E-F	V600R021C10 及以后版本	• Windows • Linux • Mac OS • 国产化

UniVPN 客户端支持的操作系统版本

客户端版本	操作系统版本
UniVPN-10781.2	• Windows：Windows 7（32 位/64 位） Windows 8（32 位/64 位） Windows 8.1（32 位/64 位） Windows 10（32 位/64 位） Windows Server 2008 R2（32 位/64 位） Windows Server 2012（64 位） Windows 11 • 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 • 国产化：银河麒麟 V10+Loongson-3A3000（mips） 银河麒麟 V10+Loongson-3A4000（mips）

UniVPN 客户端产品规格

UniVPN 的功能规格如表 3-1 所示。

表 3-1 UniVPN 的功能规格

功能名称		Windows 操作系统	Linux 操作系统	MAC 操作系统	国产化
SSL VPN	网络扩展	支持	支持	支持	支持

功能名称		Windows 操作系统	Linux 操作系统	MAC 操作系统	国产化
	终端安全	支持	支持 **说明** 仅支持检查主机防火墙、检查主机操作系统、检查主机端口、检查主机进程、检查主机文件、防主机二次跳转和防截屏功能。	不支持	支持 **说明** 仅支持检查主机防火墙、检查主机操作系统、检查主机端口、检查主机进程、检查主机文件、防主机二次跳转和防截屏功能。
	网关优选	支持	支持	支持	支持
	断线重连	支持	支持	支持	支持
	链路备份	支持	支持	支持	支持
	路由覆盖	支持	支持	支持	支持
	国密算法	支持	支持	支持	支持
	证书认证	支持	支持 **说明** 通过命令行方式配置并建立的 SSL VPN 连接仅支持通过用户名/密码认证方式认证登录。	支持	支持
	MAC 认证	支持	支持	支持	支持
	证书筛选	支持	支持	支持	支持
	双因子认证	支持 Token 序列号和短信验证码两种双因子认证方式。	支持 Token 序列号和短信验证码两种双因子认证方式。	支持 Token 序列号和短信验证码两种双因子认证方式。	支持 Token 序列号和短信验证码两种双因子认证方式。
L2TP VPN		支持	支持	支持	支持

功能名称		Windows 操作系统	Linux 操作系统	MAC 操作系统	国产化
L2TP over IPSec VPN		支持 说明 L2TP over IPSec 的身份认证方式既支持用户名密码认证，也支持 USBKey 认证。支持 USBKey 认证的前提是对应的 USBKey 要能被操作系统识别。	支持 说明 L2TP over IPSec 的身份认证方式只支持用户名密码认证，不支持 USBKey 认证。	支持 说明 L2TP over IPSec 的身份认证方式只支持用户名密码认证，不支持 USBKey 认证。	支持 说明 L2TP over IPSec 的身份认证方式只支持用户名密码认证，不支持 USBKey 认证。
NAT 穿越		支持 代理穿越场景中 IPSec 不支持隧道模式。	支持 代理穿越场景中 IPSec 不支持隧道模式。	支持 代理穿越场景中 IPSec 不支持隧道模式。	支持 代理穿越场景中 IPSec 不支持隧道模式。
代理穿越		支持 代理穿越场景中 IPSec 不支持隧道模式。	支持 代理穿越场景中 IPSec 不支持隧道模式。	支持 代理穿越场景中 IPSec 不支持隧道模式。	支持 代理穿越场景中 IPSec 不支持隧道模式。
隧道分离		支持	支持	支持	支持
基本功能	开机自启动	支持	支持	支持	支持
	界面语言切换	支持	支持	支持	支持
	自动登录	支持	支持	支持	支持
配置文件	导入	支持	支持	支持	支持
	导出	支持	支持	支持	支持
故障定位		支持	支持	支持	支持
命令行配置		不支持	支持	不支持	支持
非管理员权限用户配置		支持	不支持	支持	不支持

UniVPN 的性能规格如表 4-2 所示。

表 3-2 UniVPN 的性能规格

功能名称	规格
VPN 新建连接数	16 个
VPN 优选网关的数量	16 个

通过验证，UniVPN 支持的 USB-Key 产品规格如表 4-3 所示。

表 3-3 UniVPN 支持的 USB-Key 产品规格

厂商名称	产品型号
海泰方圆	HaiKey3000 系列
飞天诚信	ePass3000 系列

USB-Key 证书认证在不同操作系统和 VPN 类型下的支持情况如表 4-4 所示：

表 3-4 USB-Key 证书认证的支持情况

VPN 类型/操作系统	Windows	Linux	Mac OS	国产化
SSL VPN（证书匿名认证）	Y	N	N	N
SSL VPN（证书挑战认证）	Y	N	N	N
L2TP VPN	N	N	N	N
L2TP over IPSec VPN	Y	N	N	N

使用限制

UniVPN 不支持在 IPv6 网络中使用，这里包括纯 IPv6 和 IPv6 混合 IPv4 的网络都不支持。

4 安装和卸载

介绍 UniVPN 的安装和卸载方法。

网络管理员安装 UniVPN 通常有两种方法。

- 终端用户较少，逐个在终端用户的主机上手动安装。
- 终端用户较多，利用 AD 服务器批量下发软件安装包到终端用户主机进行自动安装。

介绍 Windows 操作系统下 UniVPN 的安装和卸载方法。

介绍 Linux 操作系统下 UniVPN 的安装和卸载方法。

介绍 MAC OS 操作系统下 UniVPN 的安装和卸载方法。

介绍国产化操作系统下 UniVPN 的安装和卸载方法。

本节介绍网络管理员使用 AD 服务器批量分发和安装 UniVPN，实现自动化部署，有效提高企业网络维护效率。

4.1 在 Windows 操作系统下手动安装和卸载 UniVPN

介绍 Windows 操作系统下 UniVPN 的安装和卸载方法。

安装前须知

- UniVPN 对 32 位 Windows 操作系统和 64 位 Windows 操作系统提供统一安装包，请您安装前确认 UniVPN 是否支持当前的操作系统。
- UniVPN 支持的 Windows 操作系统版本包括：
  - Windows 7（32 位/64 位）

- Windows 8（32 位/64 位）
- Windows 8.1（32 位/64 位）
- Windows 10（32 位/64 位）
- Windows Server 2008 R2（32 位/64 位）
- Windows Server 2012（64 位）
- Windows 11

- UniVPN 对操作系统的内存、硬盘、CPU 等软硬件资源没有特殊要求。

安装方法

32 位操作系统和 64 位操作系统下 UniVPN 的安装方法相同，下面以 64 位操作系统为例进行介绍。

步骤 1 使用具有“Administrators”权限的操作系统用户登录 Windows 操作系统。

步骤 2 下载对应版本的软件安装包。

登录网站 https://www.leagsoft.com，在首页进入“产品与方案 > 通用方案 > Uni VPN Client 远程接入终端方案”，在 UniVPN 介绍页面最下方单击链接下载对应版本的软件安装包。

步骤 3 双击下载的安装包，进入安装界面，单击“安装”，UniVPN 客户端将自动安装完成。

系统开始自动安装 UniVPN 软件，UniVPN 默认会被安装在系统盘下。例如，系统安装在 C 盘下，则 UniVPN 的默认安装路径为“C:\Windows\LVUAAgentInstBaseRoot”。

说明

当操作系统的语言为中文（简体或繁体）时，安装向导的界面语言默认为简体中文；除此以外，安装向导的界面语言均默认为英文。

----结束

卸载方法

步骤 1 选择“开始 > 所有程序 >UniVPN”。

步骤 2 单击“卸载”，系统弹出卸载提示，单击“是(Y)”，自动完成卸载。

----结束

4.2 在 Linux 操作系统下手动安装和卸载 UniVPN

介绍 Linux 操作系统下 UniVPN 的安装和卸载方法。

安装前须知

- UniVPN 仅对 Ubuntu 20.04 的 64 位 Linux 操作系统提供了安装包，请您安装前确认 UniVPN 是否支持当前的操作系统。
- UniVPN-10781.2 及以后版本的 UniVPN，支持的 Linux 操作系统版本包括：Ubuntu-20.04（64 位）系统。
- UniVPN 对操作系统的内存、硬盘、CPU 等软硬件资源没有特殊要求。

安装方法

下面以 Ubuntu 20.04 操作系统为例进行介绍 UniVPN 的安装方法。

步骤 1 使用具有“root”权限的操作系统用户登录 Linux 操作系统。

步骤 2 在网络连接成功的情况下，打开浏览器下载对应版本的软件安装包。

登录网站 https://www.leagsoft.com，在首页进入“产品与方案 > 通用方案 > Uni VPN Client 远程接入终端方案”，在 UniVPN 介绍页面最下方单击链接下载对应版本的软件安装包。

步骤 3 将下载的客户端安装包放到主文件夹（“计算机 > home > UniVPN”）中。

步骤 4 打开“终端”，在“home/UniVPN”目录下使用 root 身份执行./ 安装包名称.run，安装 UniVPN 客户端。

```
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
```

步骤 5 安装成功，如下所示。

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

步骤 6 单击桌面上生成的 UniVPN 客户端图标，即可启动程序并进行配置。

----结束

卸载方法

步骤 1 使用具有“root”权限的操作系统用户登录 Linux 操作系统。

步骤 2 打开“终端”，进入“ **/usr/local/UniVPN**”目录下。

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

步骤 3 使用 root 身份执行./ uninstall.sh，卸载 UniVPN 客户端。

```
root@zzh-virtual-machine:/usr/local/UniVPN# ./uninstall.sh
Stopping UniVPNPromoteService daemon: ./uninstall.sh: 行 19: 222576 已杀死              sh
UniVPNPromoteService.sh stop
```

----结束

4.3 在 MAC 操作系统下手动安装和卸载 UniVPN

介绍 MAC 操作系统下 UniVPN 的安装和卸载方法

安装前须知

- UniVPN 只支持 64 位 MAC 操作系统。
- UniVPN 支持的 MAC 操作系统版本包括：
  - 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
- UniVPN 对 MAC 操作系统的内存、硬盘、CPU 等软硬件资源没有特殊要求。

安装方法

下面以 MacOS11.5 操作系统为例进行介绍 UniVPN 的安装方法。

步骤 1 登录 MAC 操作系统。

步骤 2 在网络连接成功的情况下，打开浏览器下载对应版本的软件安装包。

登录网站 https://www.leagsoft.com，在首页进入“产品与方案 > 通用方案 > Uni VPN Client 远程接入终端方案”，在 UniVPN 介绍页面最下方单击链接下载对应版本的软件安装包。

步骤 3 双击下载好的安装包，运行安装程序。

步骤 4 安装程序会引导用户完成安装任务，具体步骤如下。

1. 在“介绍”页面单击“继续”。

   安装程序的界面语言默认与系统语言保持一致，软件介绍仅支持简体中文和英文两种语言。在简体中文操作系统下启动安装程序时软件介绍默认显示为简体中文，在除简体中文外的其他语言的操作系统下则默认显示为英文。
2. 单击“安装”。软件安装在固定路径下，无法手动更改安装位置。
3. 输入 root 用户名和密码，验证身份后，单击“安装软件”。此处可能需要对用户的系统权限进行鉴定，鉴定成功后方可继续安装。仅具有“root”权限的用户可安装此软件。
4. 单击“关闭”。

步骤 5 安装完成后，可在应用程序文件夹中找到应用程序。

步骤 6 双击“UnIVPN”，即可启动程序并进行配置。

----结束

卸载方法

步骤 1 在应用程序文件夹中双击“UniVPNUninstaller”启动卸载程序。

步骤 2 单击“卸载”，卸载 UniVPN 客户端。

----结束

4.4 在国产化操作系统下手动安装和卸载 UniVPN

介绍国产化操作系统下 UniVPN 的安装和卸载方法。

安装前须知

- UniVPN 仅对银河麒麟桌面操作系统 V10 提供了安装包，请您安装前确认 UniVPN 是否支持当前的操作系统。

- UniVPN-10781.2 及以后版本的 UniVPN，支持的国产化操作系统版本包括：银河麒麟桌面操作系统 V10+Loongson-3A3000、银河麒麟桌面操作系统 V10+Loongson-3A4000。
- UniVPN 对操作系统的内存、硬盘、CPU 等软硬件资源没有特殊要求。

安装方法

下面以 linux4.4.131（3A3000）操作系统为例进行介绍 UniVPN 的安装方法。

方法一：

步骤 1 使用具有“root”权限的操作系统用户登录国产化操作系统。

步骤 2 在网络连接成功的情况下，打开浏览器下载对应版本的软件安装包。

登录网站 https://www.leagsoft.com，在首页进入“产品与方案 > 通用方案 > Uni VPN Client 远程接入终端方案”，在 UniVPN 介绍页面最下方单击链接下载对应版本的软件安装包。

步骤 3 将下载的客户端安装包放到主文件夹（“计算机 > home > UniVPN”）中。

步骤 4 打开“终端”，在“home/UniVPN”目录下使用 root 身份执行./ 安装包名称.deb，安装 UniVPN 客户端。

```
root@UniVPN-virtual-machine:~# cd /home/UniVPN/
root@UniVPN-virtual-machine:/home/UniVPN# dpkg UniVPN-xxxxx.xx.xxx.xxxx.deb
/
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
```

步骤 5 安装成功，如下所示。

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

步骤 6 单击桌面上生成的 UniVPN 客户端图标，即可启动程序并进行配置。

----结束

方法二：

步骤 1 使用具有“root”权限的操作系统用户登录国产化操作系统。

步骤 2 在网络连接成功的情况下，打开浏览器下载对应版本的软件安装包。

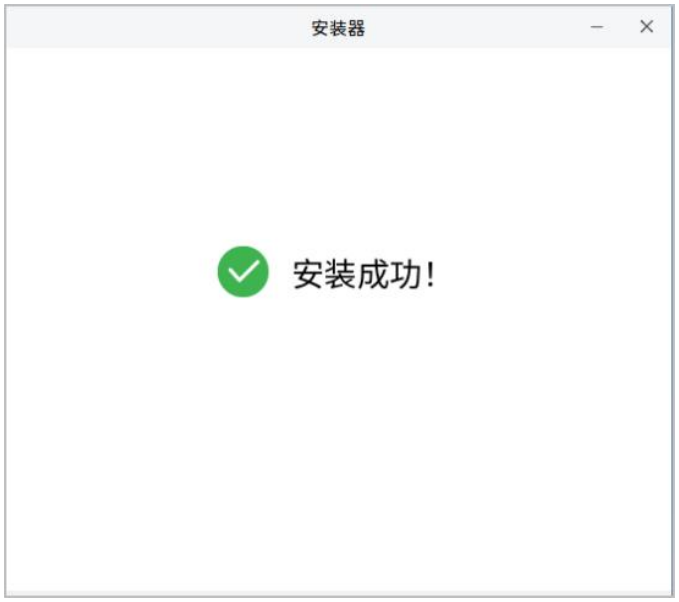
登录网站 https://www.leagsoft.com，在首页进入“产品与方案 > 通用方案 > Uni VPN Client 远程接入终端方案”，在 UniVPN 介绍页面最下方单击链接下载对应版本的软件安装包。

步骤 3 双击下载的安装包，进入安装界面，左键单击“一键安装”。

UniVPN 默认会被安装在系统盘下。例如，系统安装在/盘下，则 UniVPN 的默认安装路径为“/home/用户名/UniVPN”。

步骤 4 在授权界面输入正确的密码，单击“授权”，安装器自动完成安装。

步骤 5 安装成功，如下所示。



----结束

卸载方法

方法一：

步骤 1 使用具有“root”权限的操作系统用户登录 linux4.4.131（3A3000）操作系统。

步骤 2 打开“终端”，进入“/usr/local/UniVPN”目录下。

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

步骤 3 使用 root 身份执行 dpkg --purge --force-all univon，卸载 UniVPN 客户端。

```
root@zzh-virtual-machine:/usr/local/UniVPN# dpkg --purge --force-all univpn
Stopping UniVPNPromoteService daemon: /var/lib/dpkg/info/univpn.prerm: 行 38: 12855
 已杀死                sh UniVPNPromoteService.sh stop
```

----结束

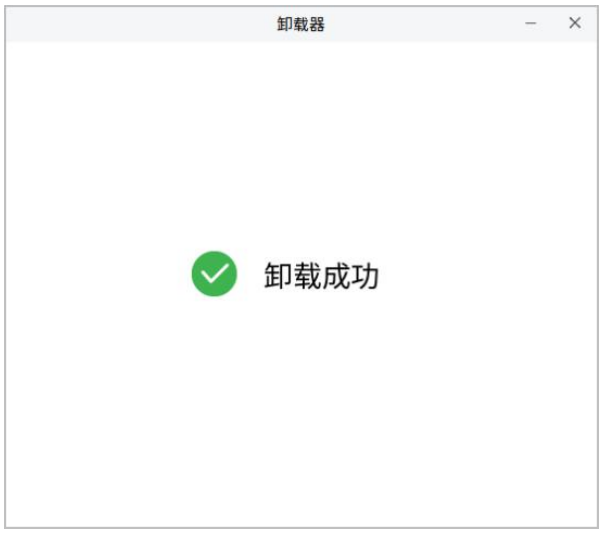
方法二：

步骤 1 打开“开始”菜单栏，选择“所有程序”，选择 UniVPN 单击右键。

步骤 2 选择“卸载”。

步骤 3 在授权页面，输入用户密码后左键单击“授权”。

步骤 4 卸载成功，如下所示。



----结束

4.5 通过 AD 服务器分发并自动安装 UniVPN

本节介绍网络管理员使用 AD 服务器批量分发和安装 UniVPN，实现自动化部署，有效提高企业网络维护效率。

AD 服务器将 UniVPN 软件安装包分发到各个终端用户主机，当用户登录主机时，UniVPN 就会进行静默安装，用户登录成功后就可以直接使用了。以下将以 Windows Server 2008（AD 服务器）和 Windows 7（终端用户）为例进行介绍。

说明

只有终端用户的操作系统是 Windows 情况下才能使用 AD 服务器批量安装方法。如果终端用户使用的是其他操作系统，则不支持这种安装方式。

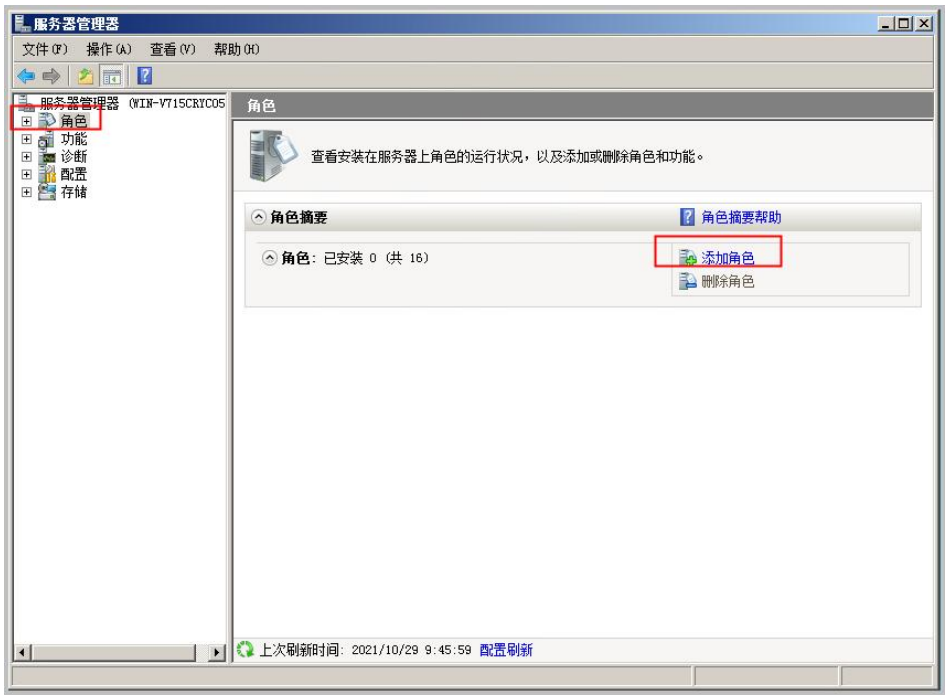
4.5.1（可选）创建 AD 域和域用户

本节介绍如何在 AD 服务器上创建 AD 域和域用户。

操作步骤

步骤 1 创建 Active Directory 域服务器角色。

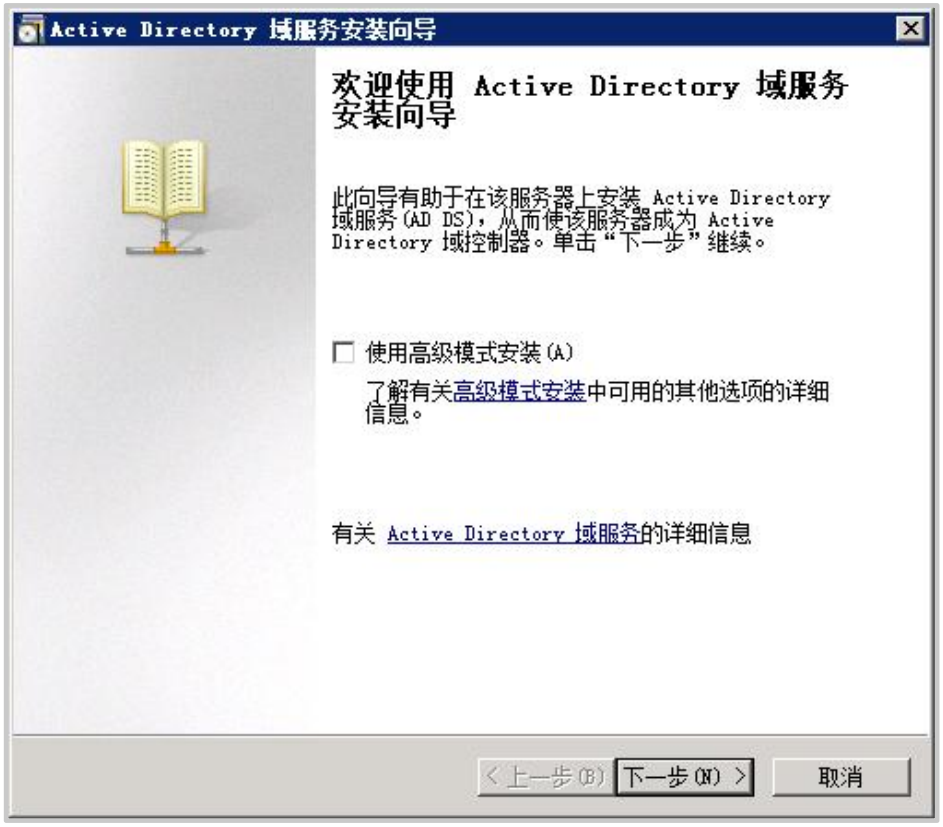
1. 在开始菜单中选择“管理工具 > 服务器管理器”。
2. 在“服务器管理器”界面，选择“添加角色”。



3. 勾选“Active Directory 域服务”，单击“下一步”直至完成安装。

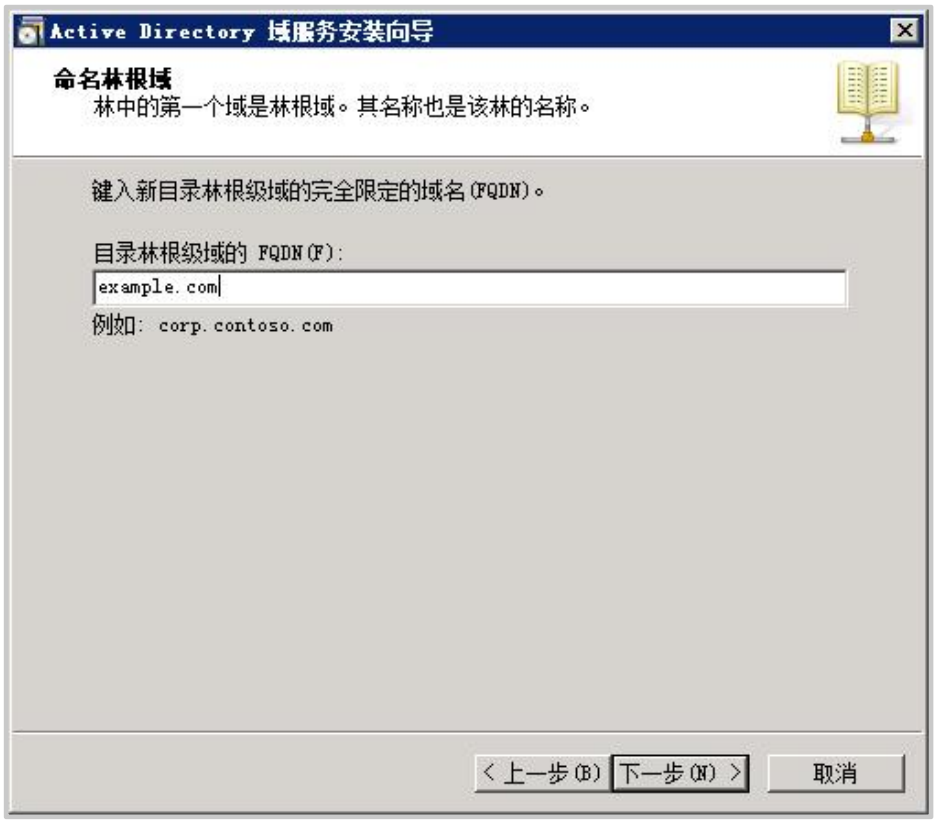
步骤 2 创建 Active Directory 域服务。

1. 在“开始 > 运行”中输入 **dcpromo**，进入安装向导。



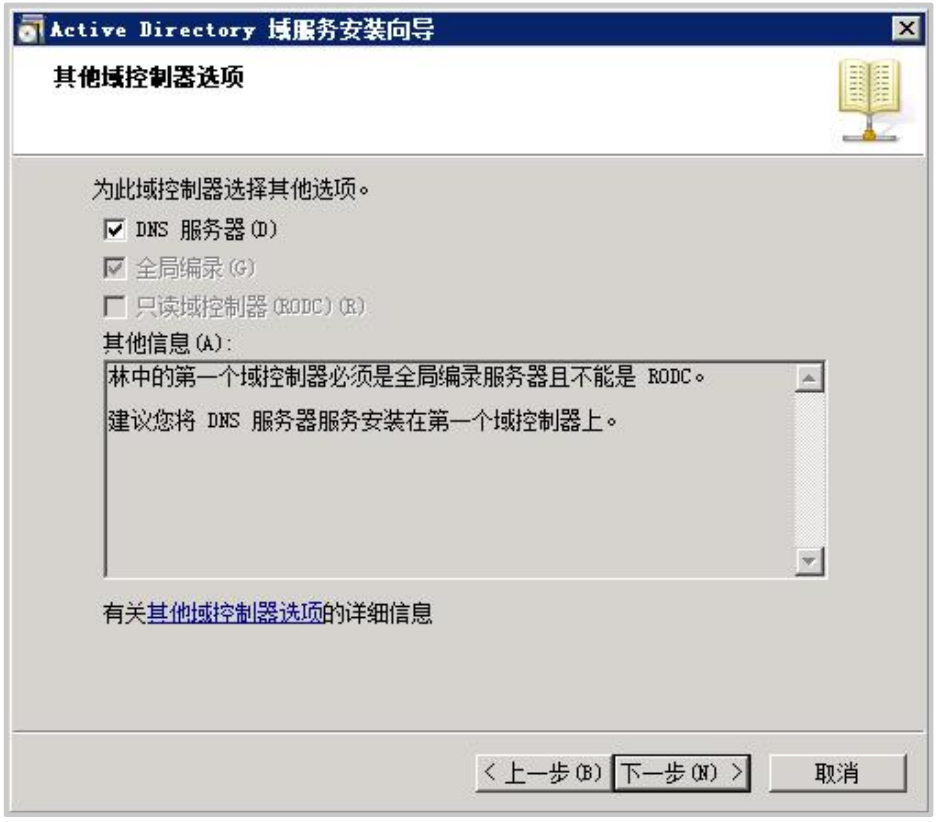
2. 选择“在新林中新建域”。

3. 输入林根域名称。

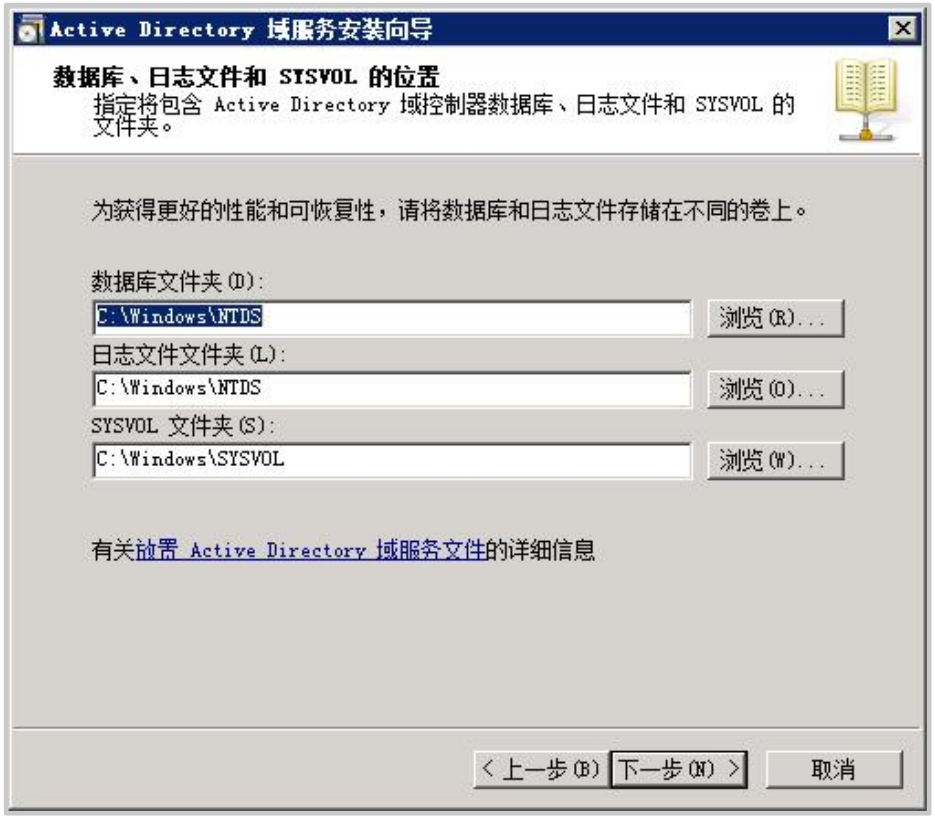


4. 选择林功能级别。

5. 在未安装 DNS 服务的服务器上，需要安装 DNS 服务器后才能使用 AD 域功能。



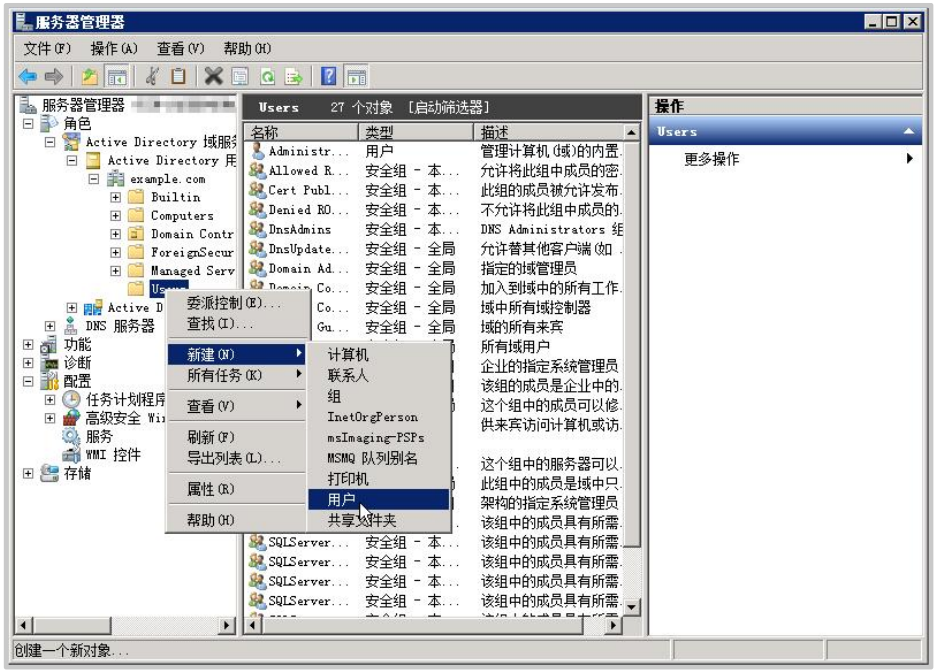
6. 指定数据库、日志文件、SYSVOL 存放路径。



7. 输入管理员密码。单击“下一步”，直至完成安装，并重启操作系统以生效。

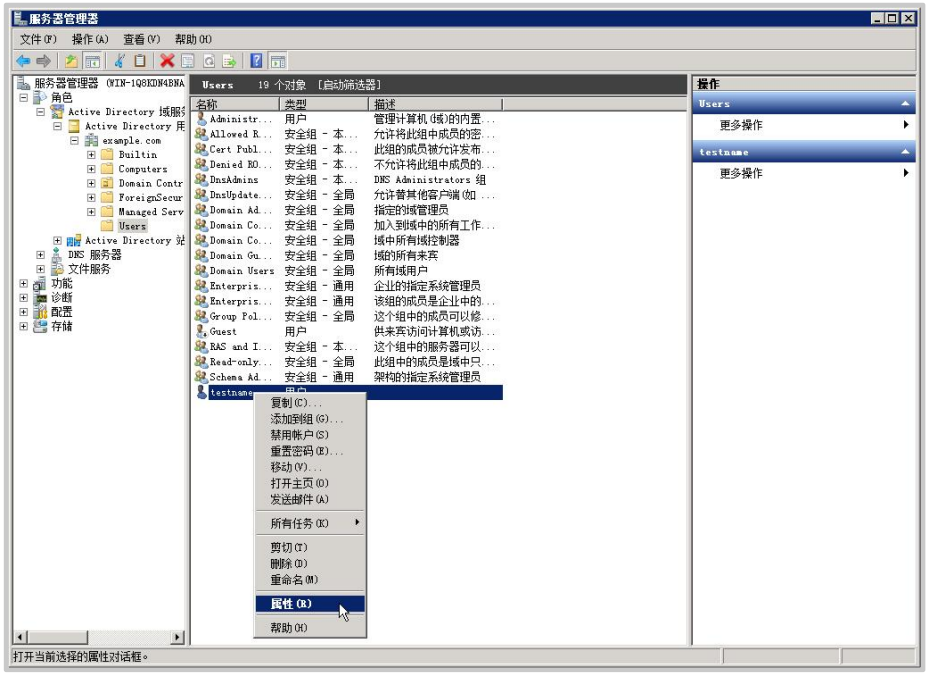
步骤 3 创建 Active Directory 域用户。

1. 在“服务器管理器”界面，展开“角色 > Active Directory 域服务 > Active Directory 用户和计算机 > example.com”，在“User”上右键选择新建用户。

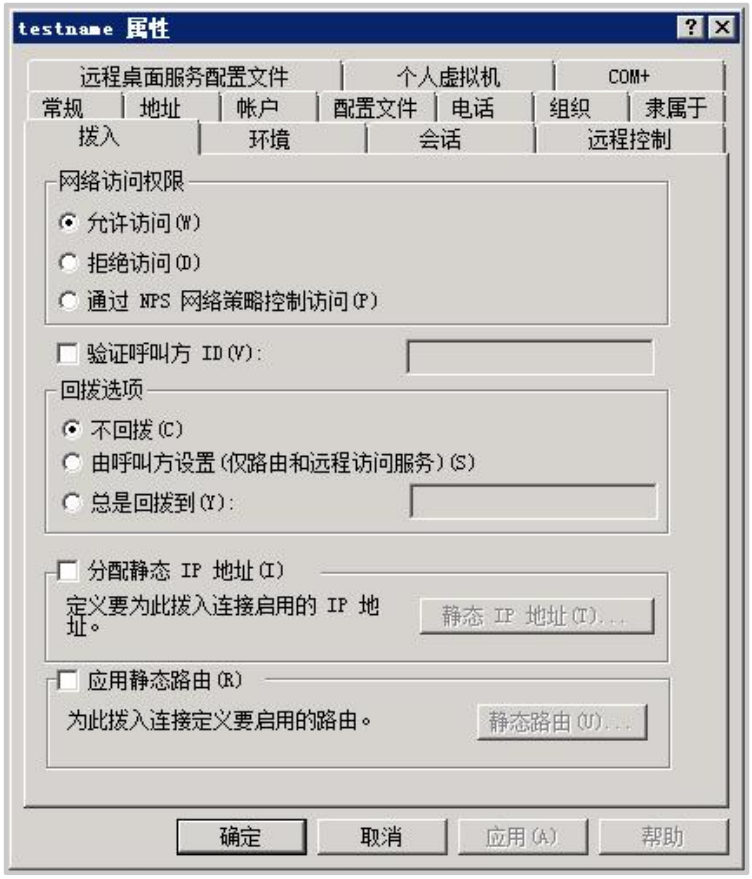


2. 配置用户基本信息和登录密码。

3. 在已创建的用户上右键选择属性。



4. 进入“拨入”页签，选择允许访问，单击“确定”。



----结束

4.5.2 将 exe 格式的安装包转换为 msi 格式

本节介绍如何在 AD 服务器上使用 Advanced Installer 将 exe 格式的软件安装包转换为 msi 格式。

操作步骤

步骤 1 下载 UniVPN 软件安装包至 AD 服务器本地。

登录网站 https://www.leagsoft.com，在首页进入“产品与方案 > 通用方案 > Uni VPN Client 远程接入终端方案”，在 UniVPN 介绍页面最下方单击链接下载对应版本的软件安装包。

步骤 2 下载 Advanced Installer 软件至 AD 服务器本地，并安装运行。

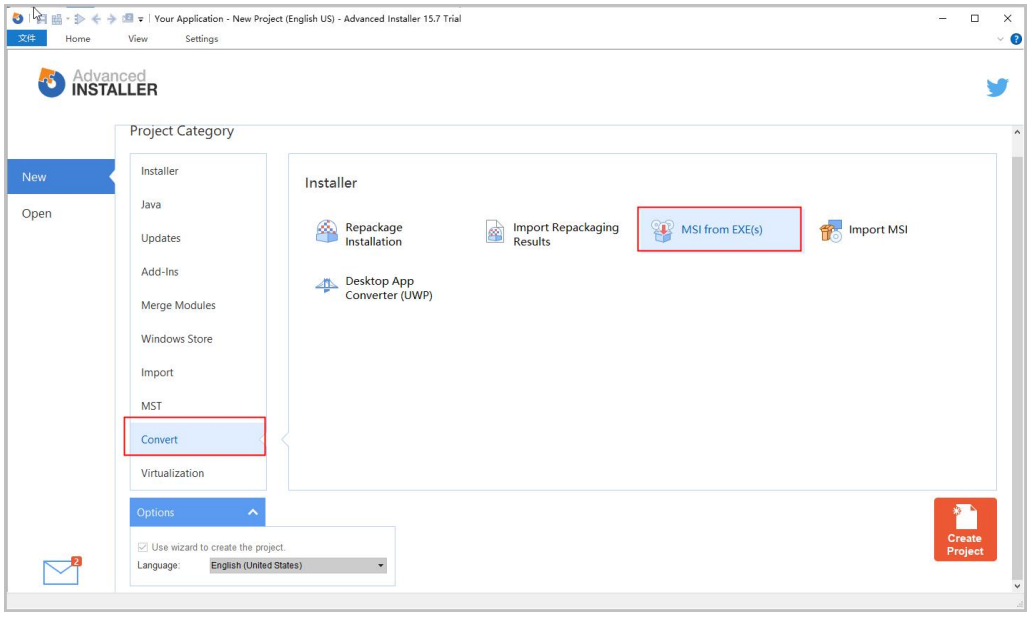
AD 服务器在批量分发 UniVPN 软件安装包到终端用户主机的时候，使用的安装包格式是 msi 格式。使用 Advanced Installer 软件是为了将 UniVPN 原有的 exe 格式安装包转换成 msi 格式。

说明

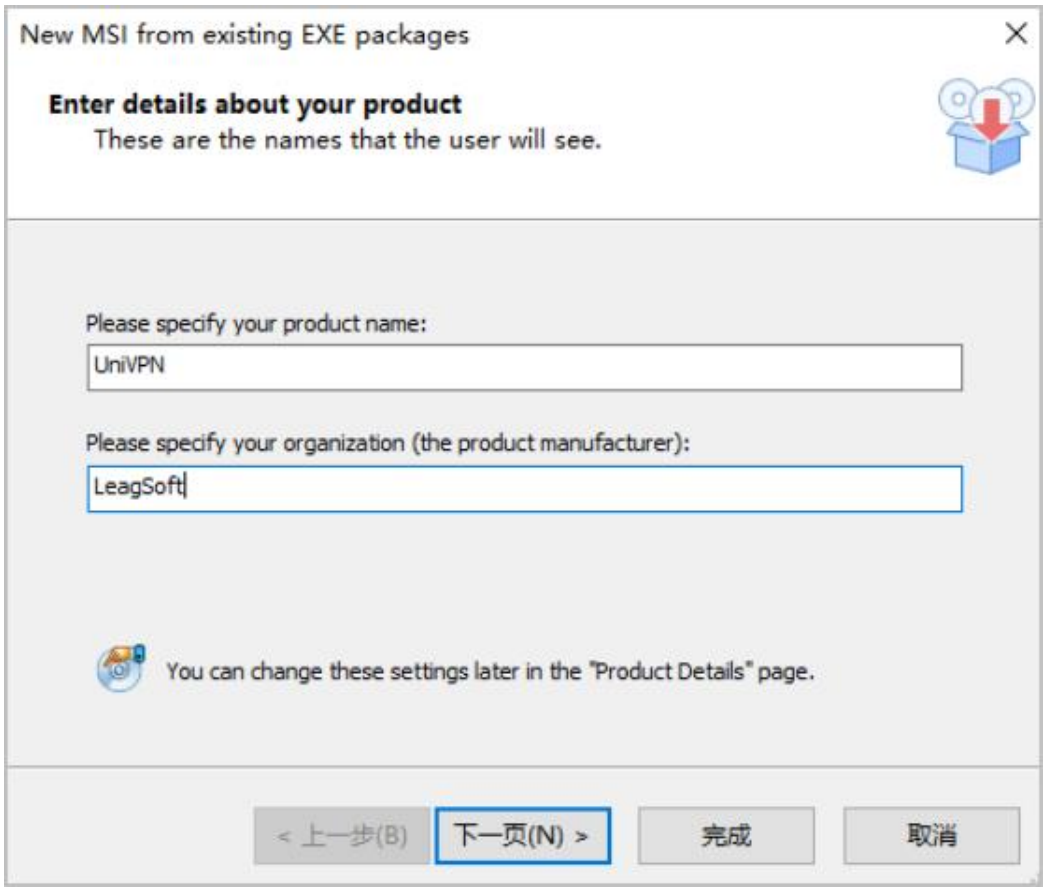
有很多种工具都可以把 exe 格式的软件安装包转换成 msi 格式，此处仅以 Advanced Installer 工具为例进行介绍，不表示只能通过 Advanced Installer 进行转换。

步骤 3 在 Advanced Installer 上创建一个工程。

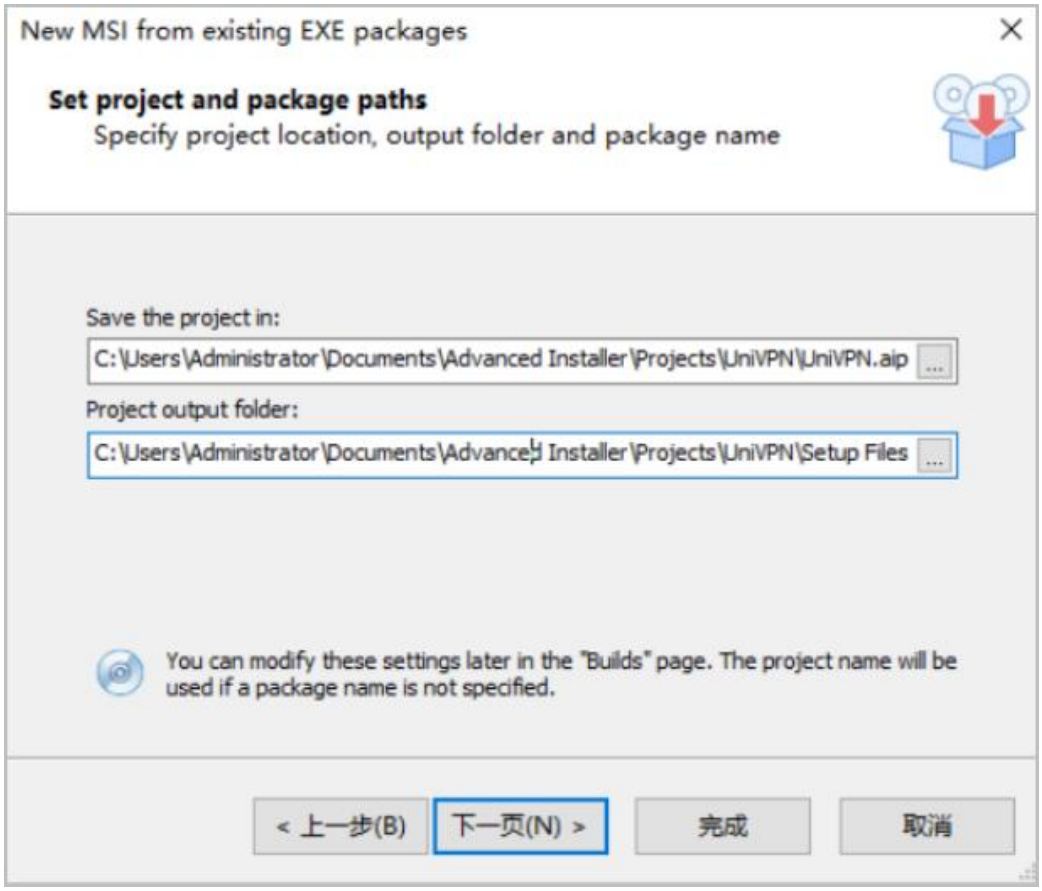
打开 Advanced Installer 软件，选择“Convert > MSI from EXE”，单击“Create Project”。



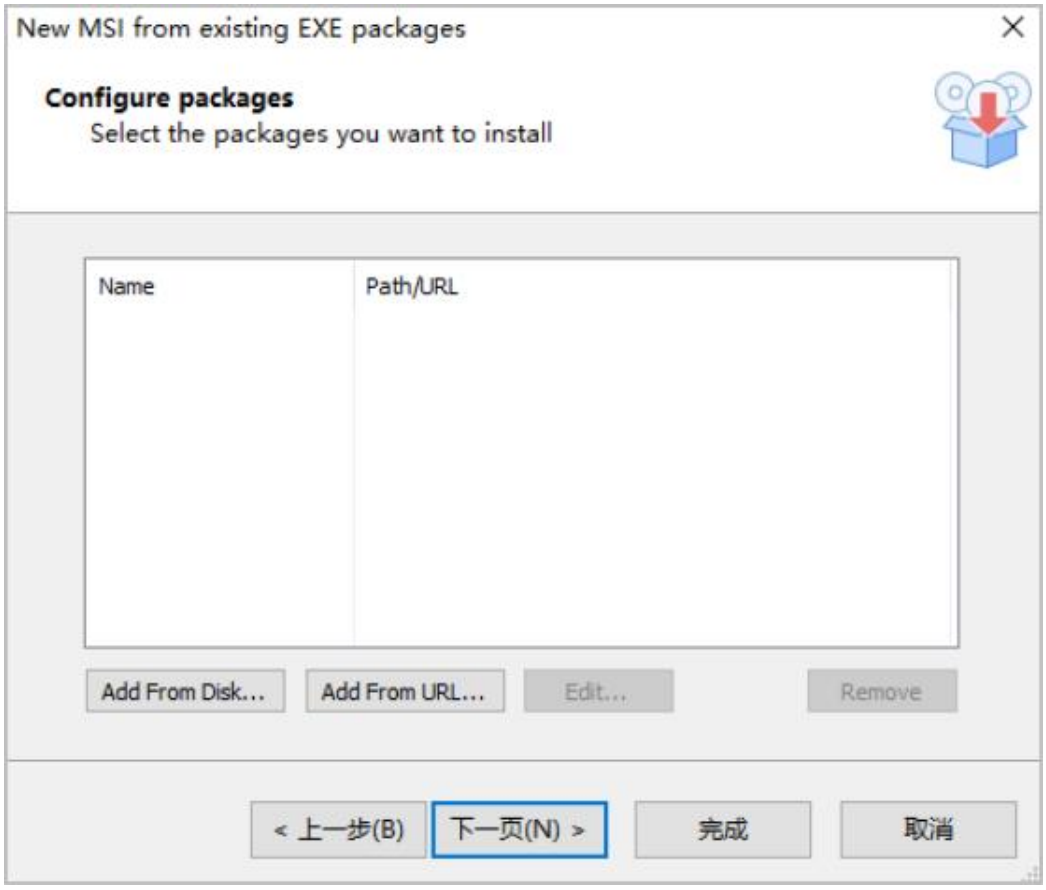
步骤 4 在弹出的对话框中输入产品名称和企业名称，单击“下一页”。



步骤 5 依次输入工程名、工程的输出路径和安装包名称，单击“下一页”。



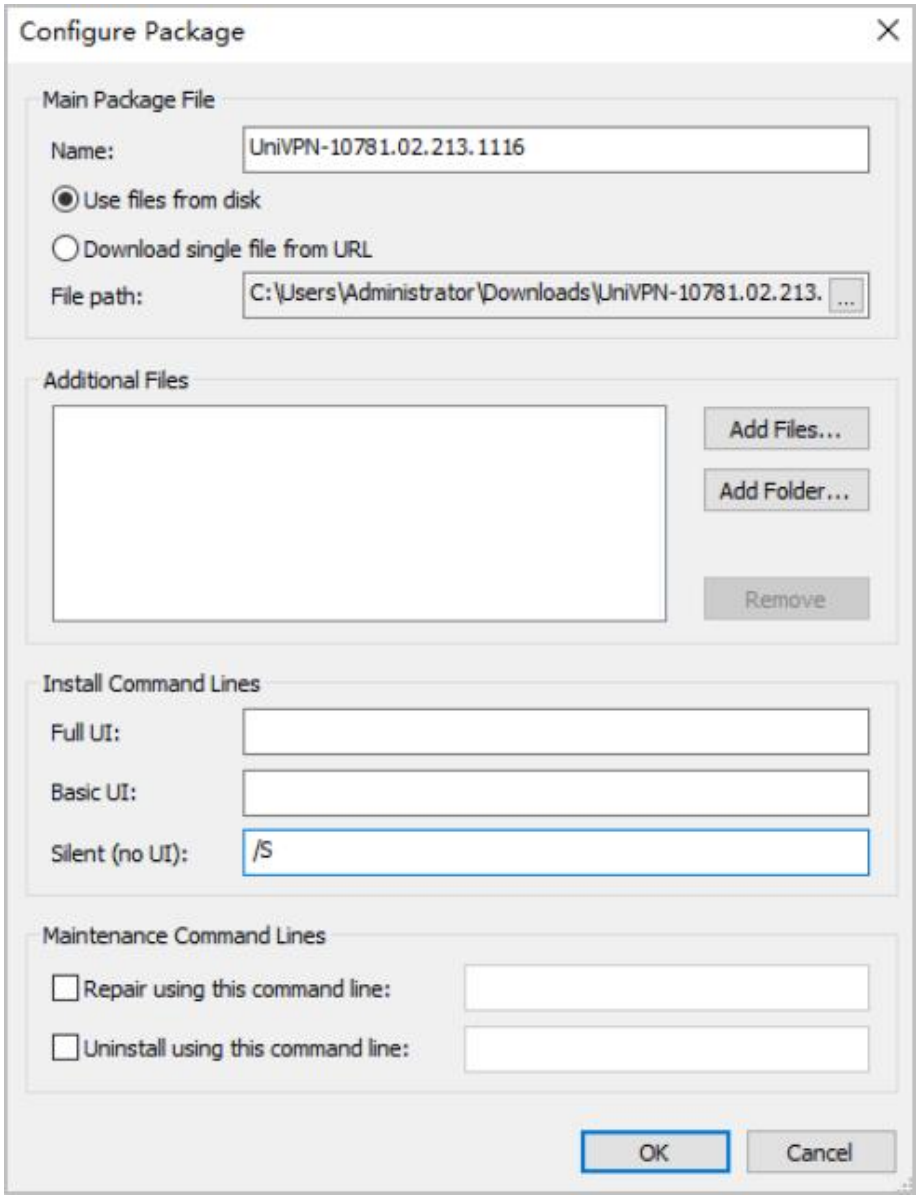
步骤 6 单击“Add From Disk”，系统会弹出窗口提示您选择要转换格式的软件安装包。



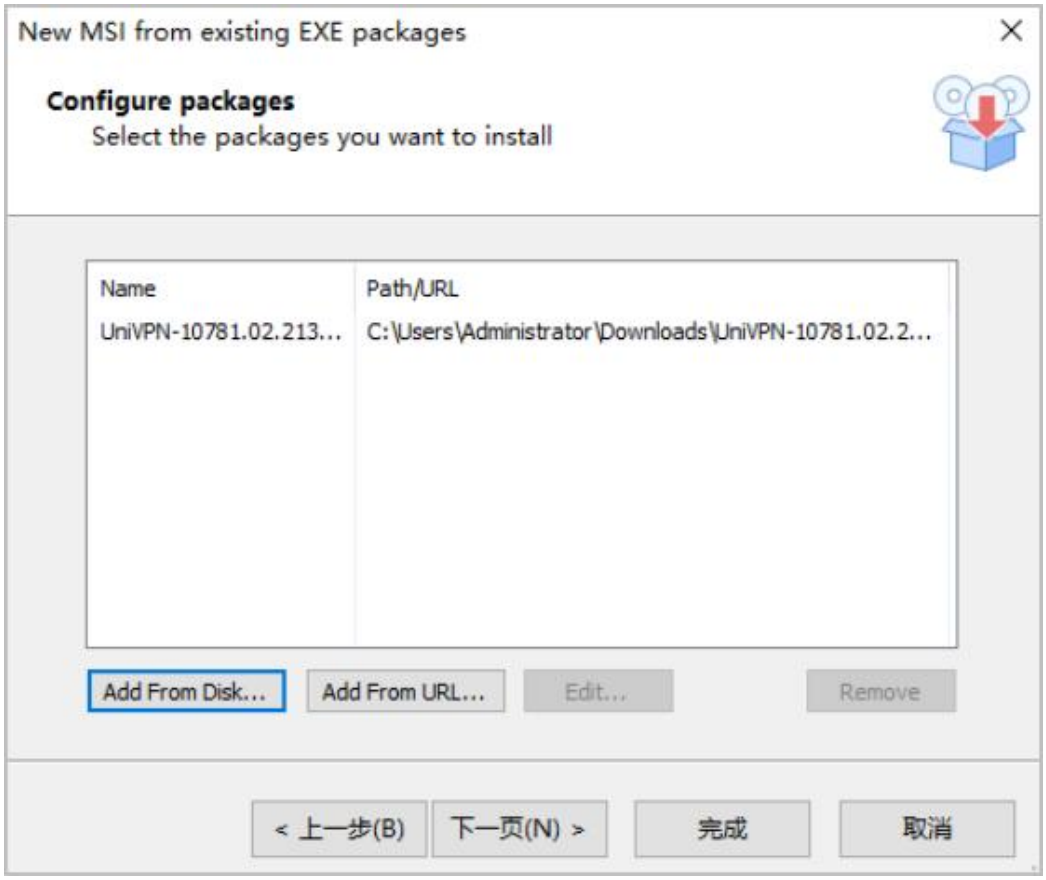
步骤 7 完成如下界面设置，单击“OK”。

须知

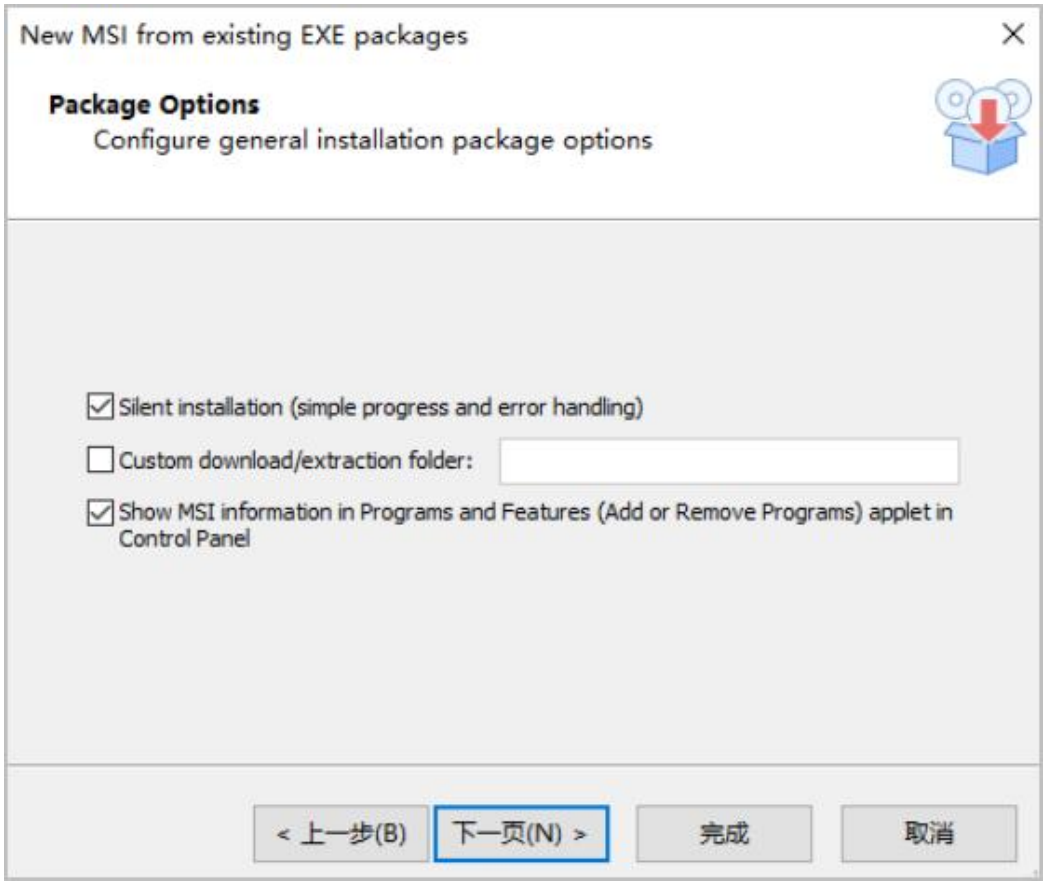
下图“Silent（no UI）”中“/S”的 S 要求用大写。


Configure Package
Main Package File
Name:
UniVPN-10781.02.213.1116
Use files from disk
Download single file from URL
File path:
C:\Users\Administrator\Downloads\UniVPN-10781.02.213.
Additional Files
Add Files...
Add Folder...
Remove
Install Command Lines
Full UI:
Basic UI:
Silent (no UI):
/S
Maintenance Command Lines
Repair using this command line:
Uninstall using this command line:
OK
Cancel

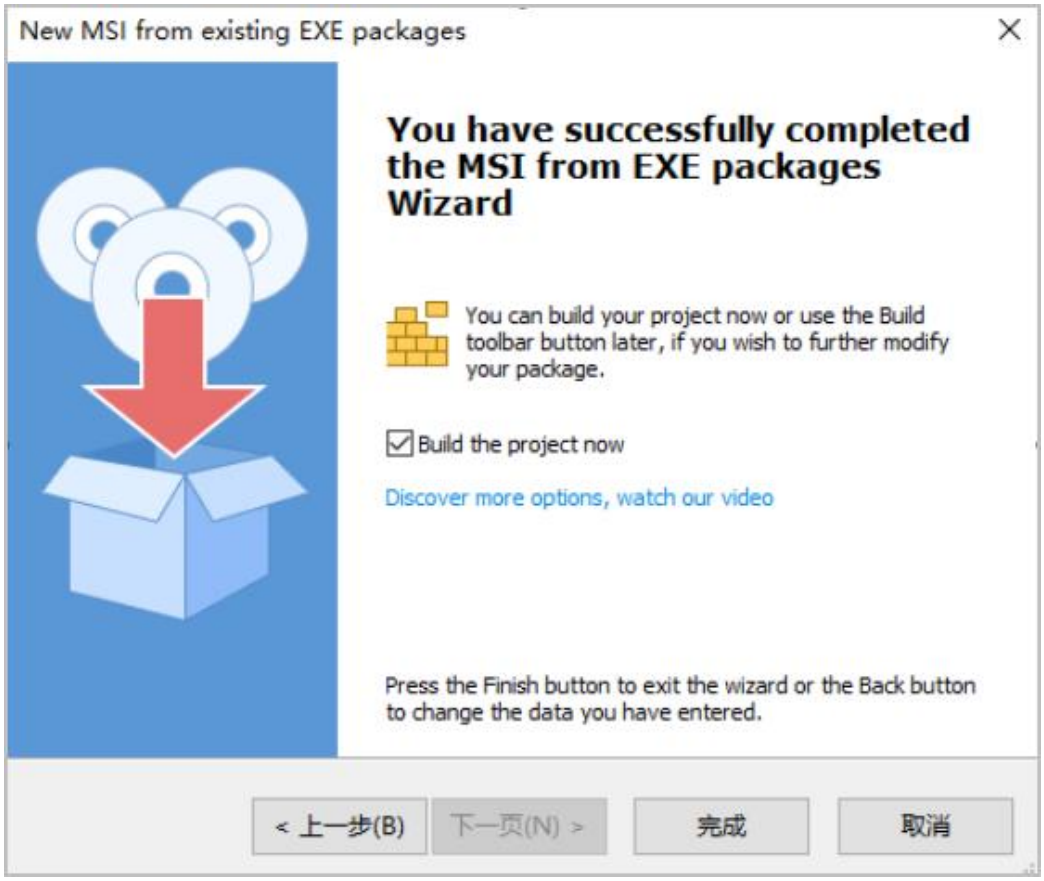
步骤 8 单击“下一页”。



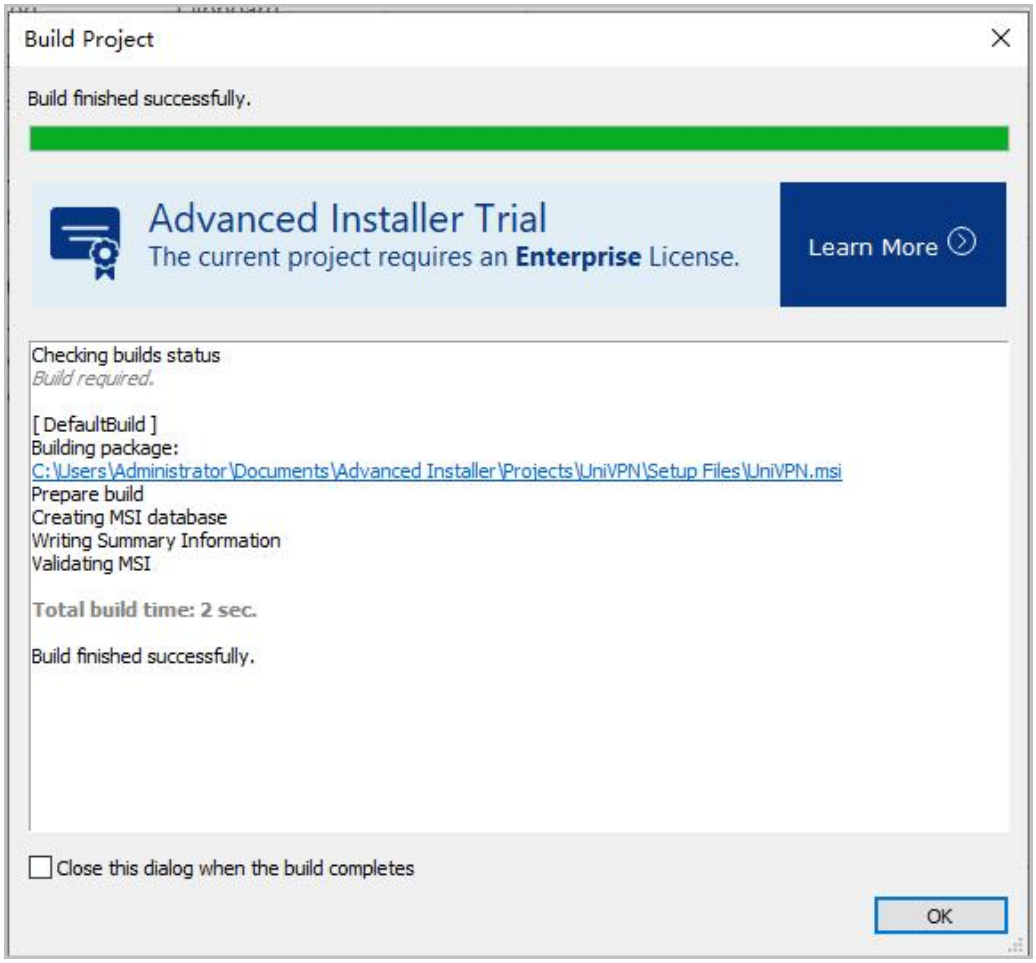
步骤 9 勾选“Silent installation”选项，单击“下一页”。


New MSI from existing EXE packages
Package Options
Configure general installation package options
Silent installation (simple progress and error handling)
Custom download/extraction folder:
Show MSI information in Programs and Features (Add or Remove Programs) applet in Control Panel
< 上一步(B)
下一页(N) >
完成
取消

步骤 10 单击“完成”。


New MSI from existing EXE packages
You have successfully completed the MSI from EXE packages Wizard
You can build your project now or use the Build toolbar button later, if you wish to further modify your package.
Build the project now
Discover more options, watch our video
Press the Finish button to exit the wizard or the Back button to change the data you have entered.
< 上一步(B)
下一页(N) >
完成
取消

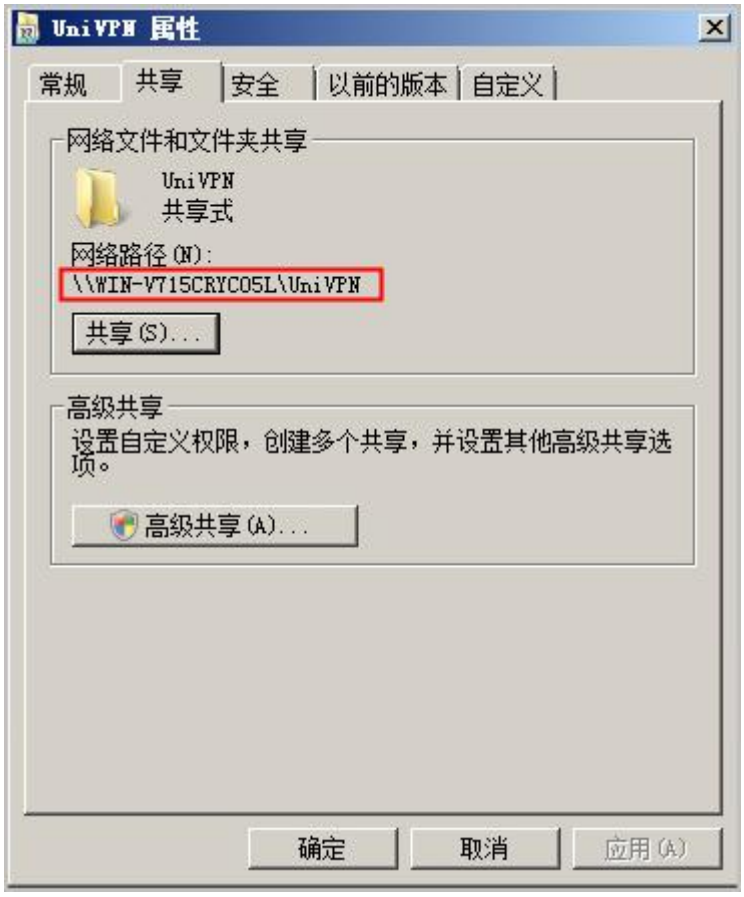
步骤 11 上一步完成后，系统会有一个编译过程，这里需等待约 10 多秒。当出现如下提示时，单击“OK”。



步骤 12 检查指定工程路径下是否生成了 UniVPN.msi 文件。

步骤 13 在 AD 服务器本地创建一个共享文件夹，共享的范围和权限要能保证所有域用户都能访问，然后将制作好的 UniVPN.msi 文件放入到这个文件夹中。

本例中共享文件夹的名称为 UniVPN。在共享文件夹上单击右键，选择“属性”，记住该文件夹的网络路径，在后续操作中会使用到。


UniVPN 属性
常规
共享
安全
以前的版本
自定义
网络文件和文件夹共享
UniVPN
共享式
网络路径(N):
\\WIN-V715CRYCO5L\UniVPN
共享(S)...
高级共享
设置自定义权限，创建多个共享，并设置其他高级共享选项。
高级共享(A)...
确定
取消
应用(A)

----结束

4.5.3 创建软件安装策略

本节介绍如何在 AD 服务器上创建软件安装策略，域下的用户将会根据该策略自动执行软件安装操作。

前置任务

- 创建 AD 域、AD 域用户。

  如果当前网络中已经部署了 AD 域系统，此步骤可直接跳过。

  如果当前网络中未部署 AD 域系统，可参考 4 3.3.1 （可选）创建 AD 域和域用户完成部署。

- 获取 msi 格式的软件安装包。

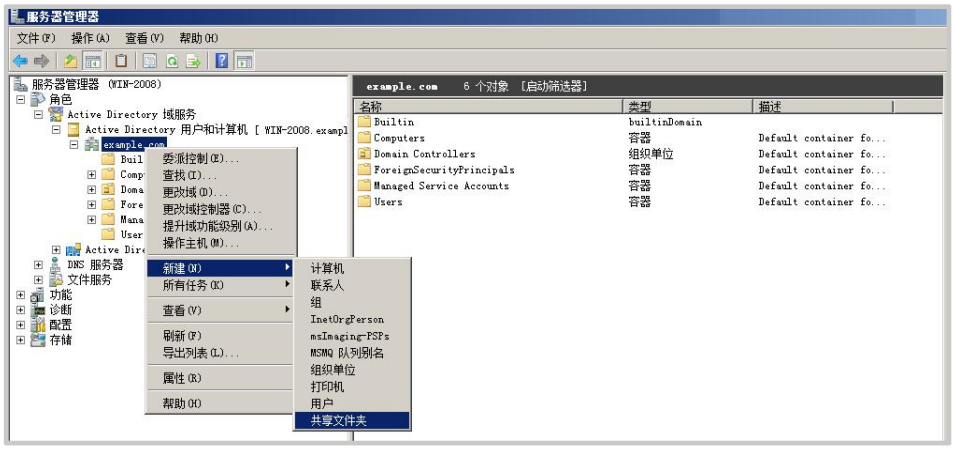
  通过 AD 服务器分发并自动安装的 UniVPN 软件安装包必须为 msi 格式，msi 格式的软件安装包可以通过以下途径获取：

  在 AD 服务器上使用转换工具将已有的 exe 格式的 UniVPN 软件安装包转换为 msi 格式，具体方法可参考 3.3.2 将 exe 格式的安装包转换为 msi 格式。

操作步骤

步骤 1 在 example.com 域下引用之前创建的共享文件夹。

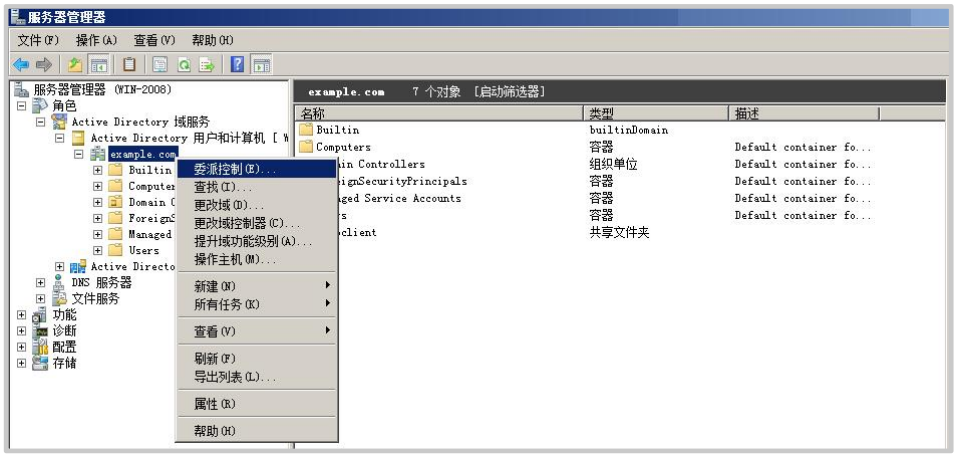
1. 在 example.com 域上单击右键，选择“新建 > 共享文件夹”。



2. 输入之前创建的共享文件夹的名称，以及共享文件夹的网络路径。

步骤 2 设置用户的委派控制。

1. 在 example.com 域上单击右键，选择“委派控制”。



2. 单击“下一步”。

3. 在弹出的对话框中，单击“添加”，将已经创建的域用户加入委派控制组中，单击“下一步”。

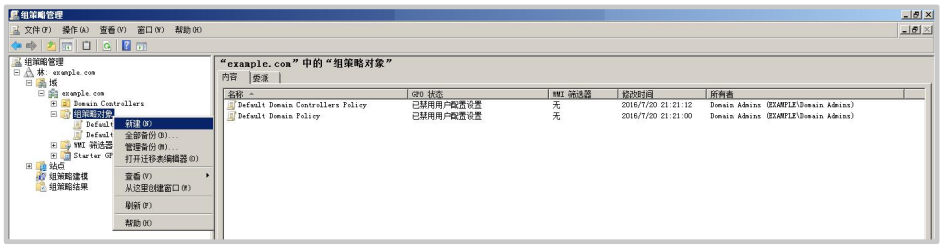
4. 勾选为用户委派的任务，单击“下一步”。

5. 单击“完成”，结束委派控制配置。

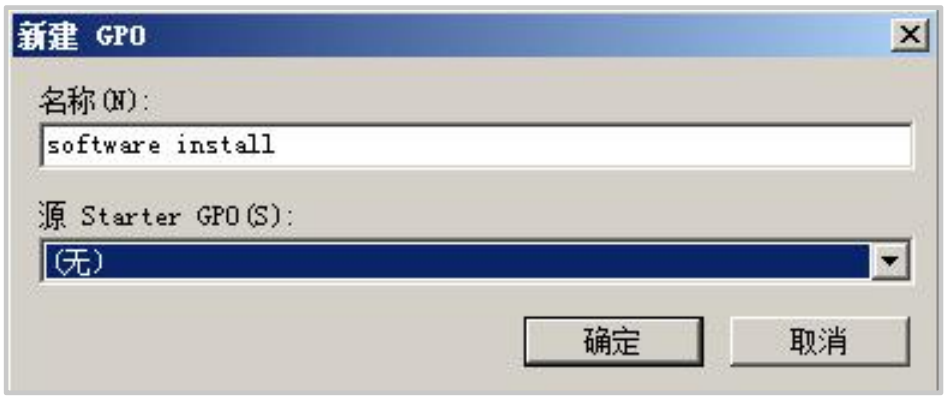
步骤 3 设置软件安装策略。

1. 在开始菜单中选择“管理工具 > 组策略管理”。

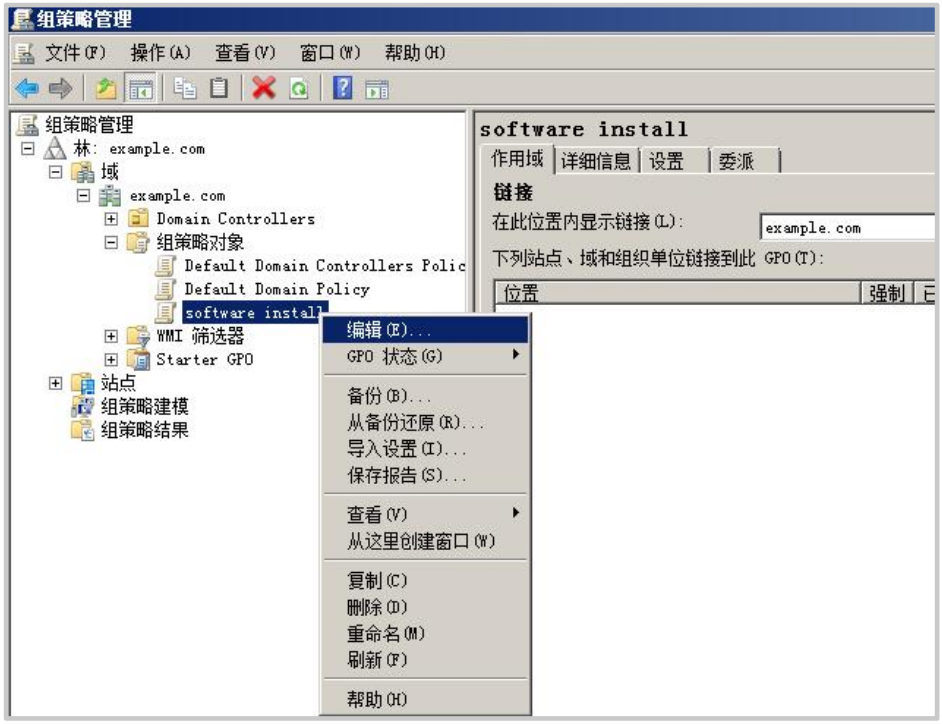
2. 在组策略对象上单击右键，选择“新建”。



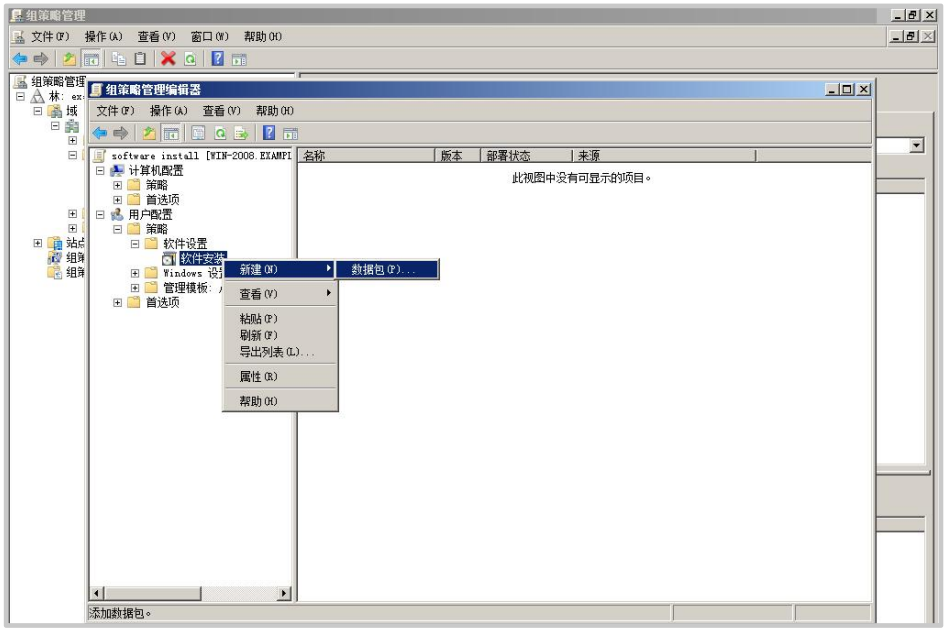
3. 创建一个名称为“software install”的策略对象，单击“确定”。



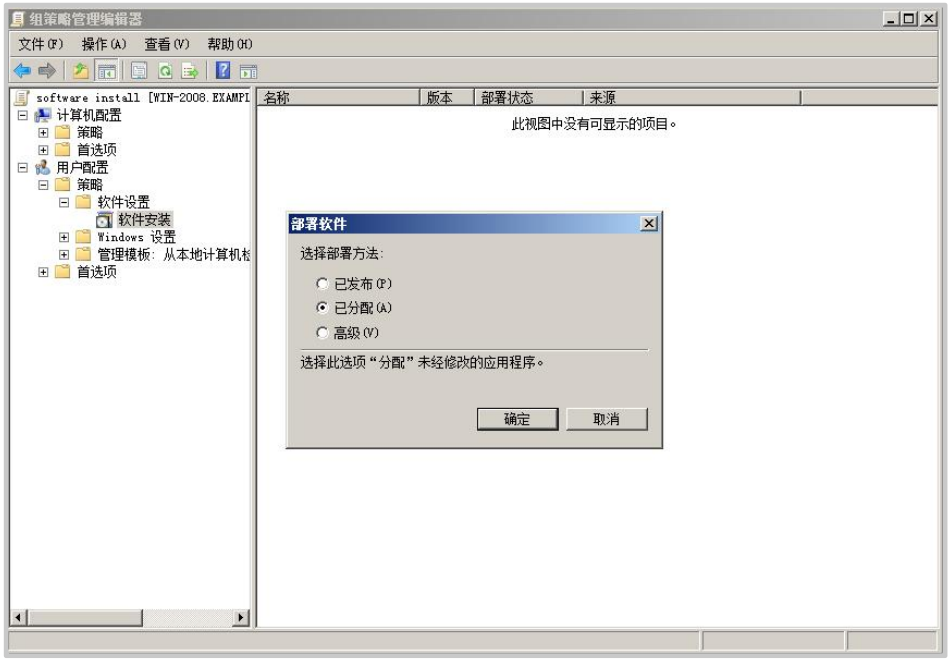
4. 在新建的策略对象“software install”上单击右键，选择“编辑”。



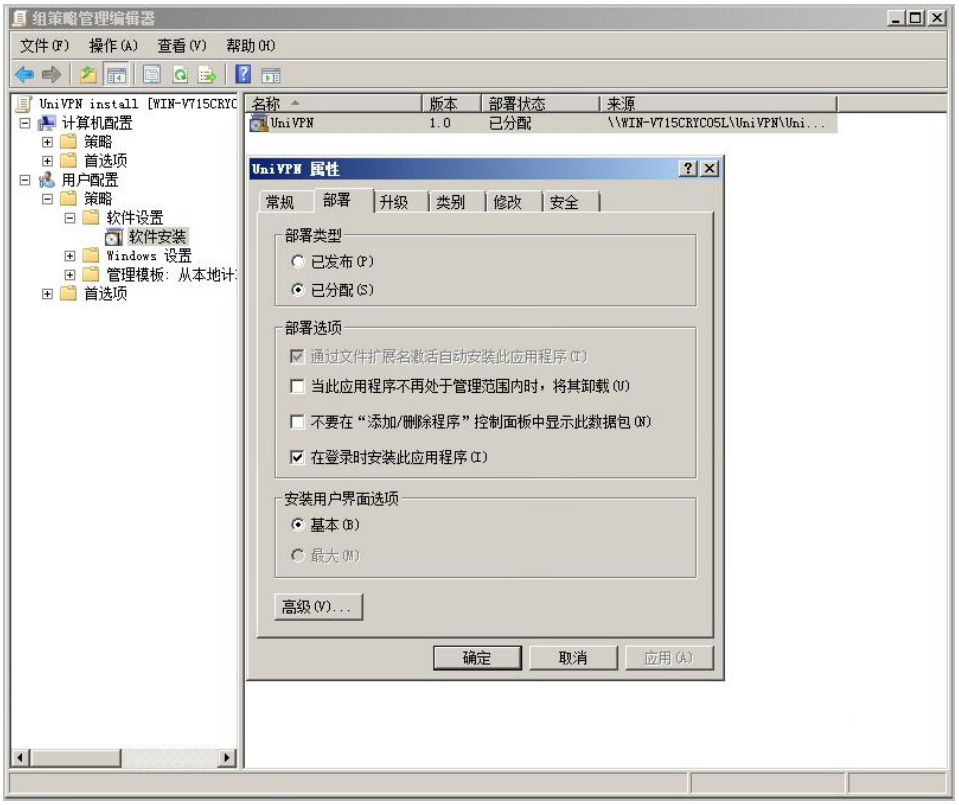
5. 在“软件安装”上单击右键，依次选择“新建 > 数据包”。



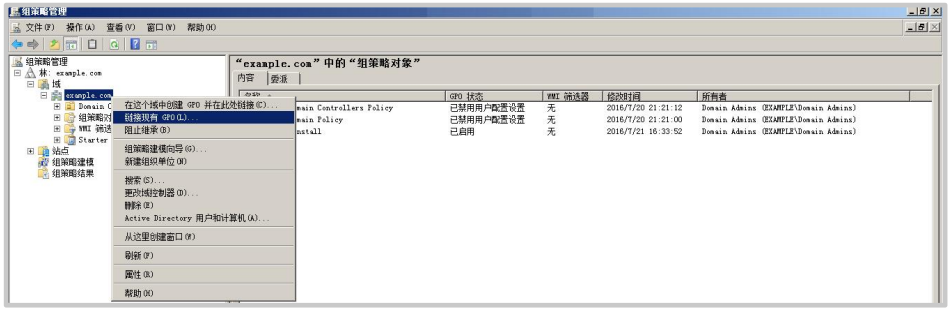
6. 系统会提示用户选择制作好的 UniVPN.msi 文件，选中文件后，系统接着会弹出如下提示，选择“已分配”，单击“确定”。



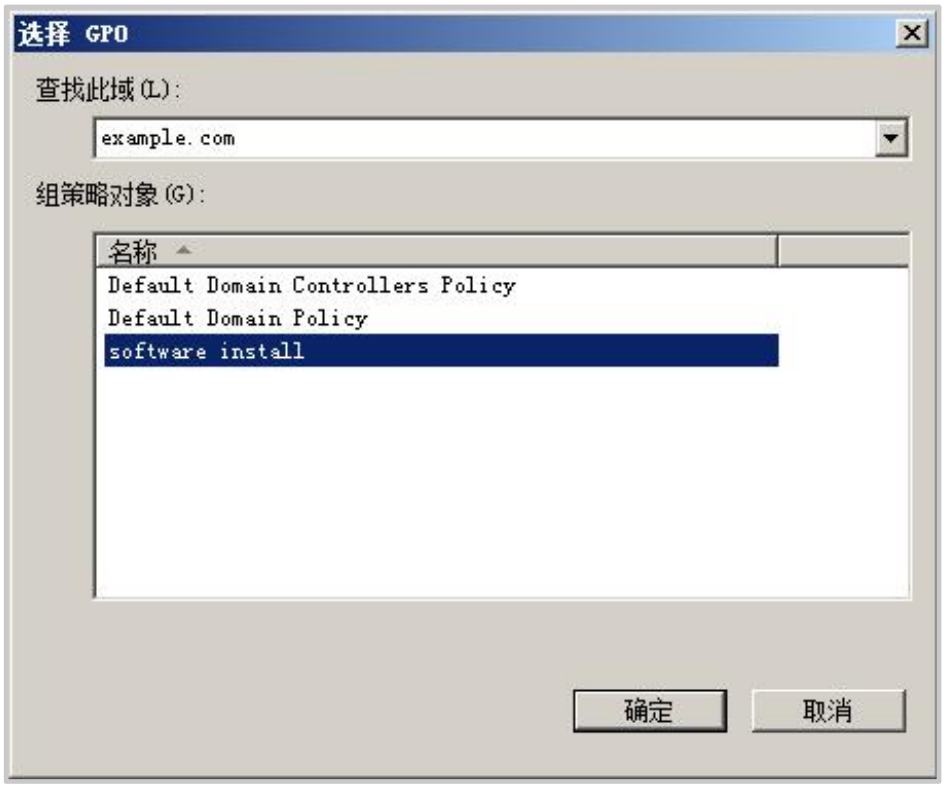
7. 双击右侧窗口新生成的 UniVPN 记录，选择“部署”页签，并按照下图进行设置，然后单击“确定”。



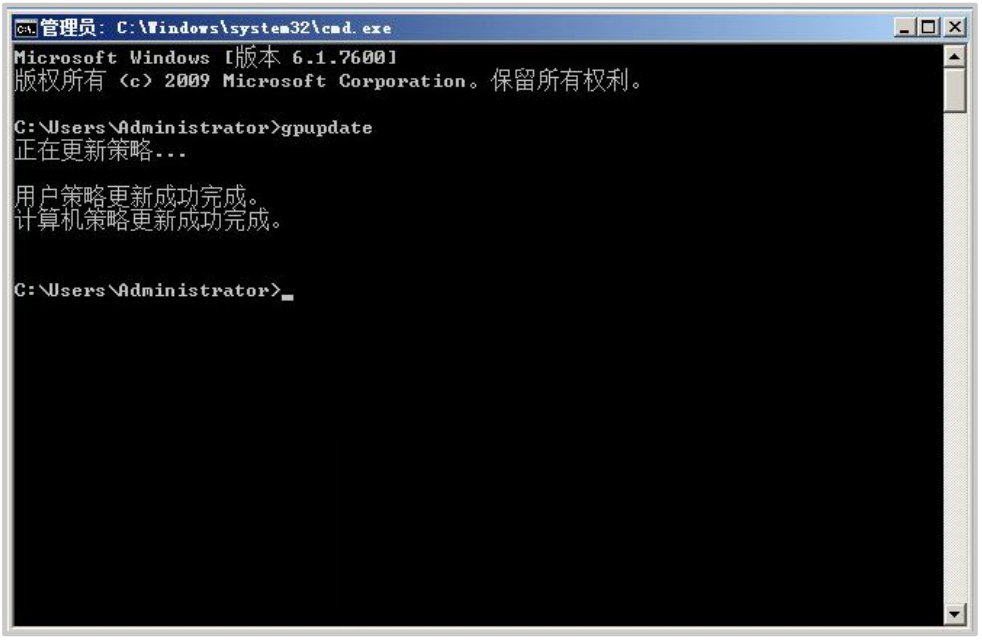
8. 在 example.com 上单击右键，选择“链接现有 GPO”。



9. 选择“software install”，然后单击“确定”。



步骤 4 打开 cmd 命令行，执行 gpupdate 命令，更新新建的组策略。



----结束

结果验证

在终端用户侧，域用户成功登录主机后，发现 UniVPN 安装完成。

UniVPN 的软件安装是在域用户登录系统过程中完成的，整个安装过程无需用户参与。

5 配置

Windows 操作系统、Linux 操作系统、MAC OS 操作系统和国产化操作系统下使用 UniVPN 建立 VPN 隧道、进行常用设置的配置方法基本相同，下面以 Windows 操作系统为例进行介绍。

5.1 使用 UniVPN 建立 VPN 隧道

UniVPN 建立 VPN 隧道的方式有两种，一种是手工方式，另一种是配置文件方式。

5.1.1 通过手工方式建立 VPN 隧道

手工方式是指 UniVPN 使用者自己手动创建 VPN 连接，配置相关参数，建立 VPN 隧道的一种方式。

UniVPN 可以创建 SSL VPN、L2TP VPN 和 L2TP over IPSec VPN 这三种类型的 VPN 隧道。具体选用哪一种 VPN 隧道访问企业内网，这取决于实际的网络部署，请您根据真实需要选择创建对应类型的 VPN 隧道。

5.1.1.1 建立 SSL VPN 隧道

介绍 SSL VPN 隧道的配置方法。

配置步骤

步骤 1 新建一条 SSL VPN 连接。

1. 打开 UniVPN，进入主界面。
   在“选择 VPN 连接”最右侧单击“+新建连接”。

如您需要使用代理设置，可以单击“选择 VPN 连接”右侧的 代理设置 。

表 5-1 代理设置

参数	说明
代理设置	按照您访问 Internet 时是否使用代理服务器，这里有两种选择。 • 不使用代理 如果您当前访问 Internet 时没有使用代理服务器，此处选择该类型。 • 使用代理服务器 使用代理服务器的场景中细分了 3 种情况： – 使用系统代理：表示使用浏览器中设置的代理服务器信息。 – 使用 HTTP/HTTPS 代理：表示使用 HTTP 或 HTTPS 代理服务器。 – 使用 Sockets5 代理：表示使用 Sockets5 代理服务器 请根据网络实际情况选择代理类型。另外，在选择代理服务器的时候，会要求输入地址、端口、账号、密码信息，该信息请向代理服务器管理员获取。 缺省情况下，代理类型为“不使用代理”。

2. 配置 SSL VPN 连接参数。

   在“新建连接”窗口左侧导航栏中选择“SSL VPN”，并配置相关的连接参数。

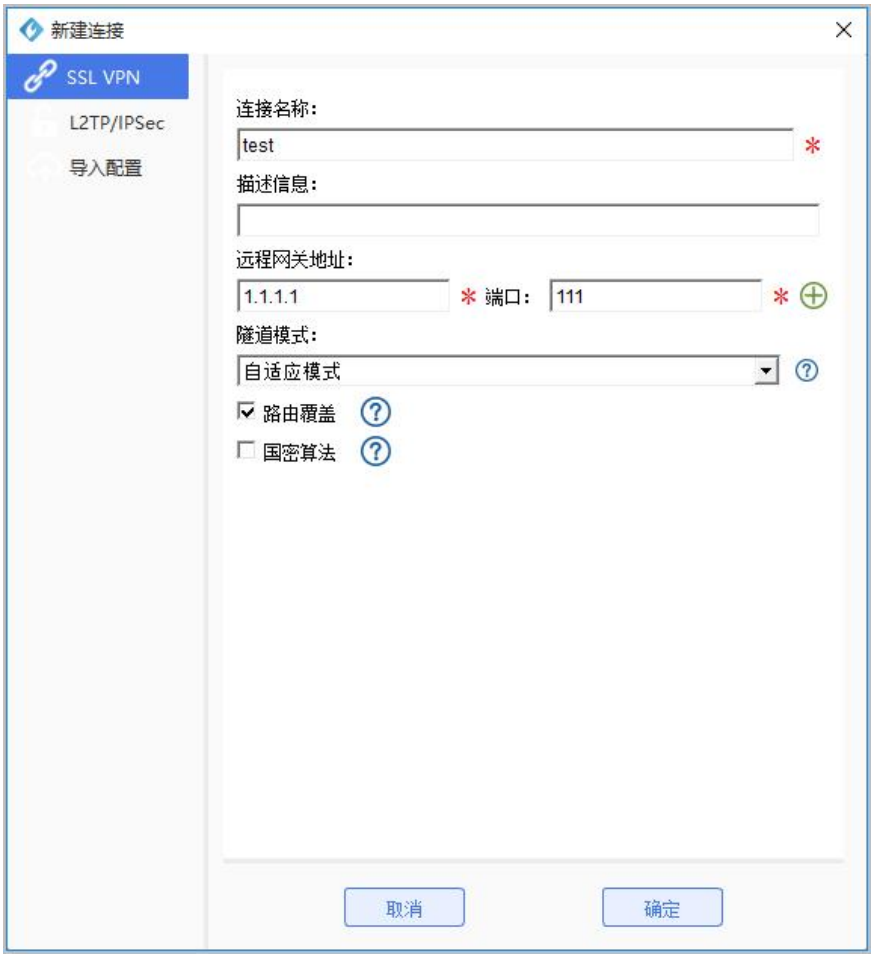


表 5-2 SSL VPN 配置参数说明

参数	说明
连接名称	用于标识一条 SSL VPN 连接。连接名称具有唯一性，不允许重复。
描述信息	用于补充说明该条连接的相关信息。例如，可以在此处添加该条连接的创建者、创建时间以及连接用途等信息。
远程网关地址	SSL VPN 虚拟网关地址。该地址必须与 SSL VPN 虚拟网关地址保持一致。地址填写错误，会导致 SSL VPN 隧道建立失败。

参数	说明
端口	表示建立 SSL VPN 隧道的端口号。该端口号必须与 SSL VPN 虚拟网关提供的端口号保持一致。端口号填写错误，会导致 SSL VPN 隧道建立失败。 单击“远程网关：”后的  ，会将当前虚拟网关地址加入到虚拟网关列表。可以持续向虚拟网关列表中添加多个地址，最多能添加 16 个地址。选中虚拟网关列表中的某条记录，单击端口后的  ，可以删除该记录。 在网关优选场景中将会用到虚拟网关列表，勾选“启动自动优选”，UniVPN 将探测虚拟网关列表中所有网关的响应速度，然后从中选择响应速度最快的那台虚拟网关建立 SSL VPN 隧道。 如果虚拟网关列表中存在多个网关地址，而用户又没有勾选“启动自动优选”时，则要在虚拟网关列表中先选中一个地址，然后勾选“设为默认”，表示 UniVPN 将与被选中的虚拟网关建立 SSL VPN 隧道。
隧道模式	网络扩展功能建立 SSL VPN 隧道的模式有三种：自适应模式、可靠传输模式和快速传输模式。 可靠传输模式中，SSL VPN 采用 SSL 协议封装报文，并以 TCP 协议作为传输协议；快速传输模式中，SSL VPN 采用 QUIC（Quick UDP Internet Connections）协议封装报文，并以 UDP 协议作为传输协议。QUIC 也是基于 TLS/SSL 协议实现的数据加密协议，它的作用和 SSL 一样，只是经 QUIC 封装的报文要基于 UDP 协议来传输。 自适应模式下，UniVPN 会优先使用快速模式与虚拟网关建立隧道，当快速模式建立隧道失败时，再选择使用可靠模式与虚拟网关建立隧道。 在网络环境不稳定的情况下推荐使用可靠传输模式；而网络环境比较稳定的情况下，推荐使用快速传输模式，这样数据传输的效率更高。在不了解当前网络环境的情况下可以选择自适应模式。
路由覆盖	当对端网关下发的路由和本地已经存在的路由的目的地址和子网掩码完全相同时，如果启用了路由覆盖功能，则对端网关下发的路由会覆盖本地已经存在的路由，避免本地路由冲突造成网络访问异常。 缺省情况下，路由覆盖功能开启。
国密算法	客户端支持使用国密算法与对端网关建立 SSL VPN 连接。 缺省情况下，国密算法功能关闭。勾选“国密算法”后，对端网关的加密套件会自动切换为 ECC-SM4-SM3。
证书认证 **说明** 仅在 Linux 和国产化操作系统下会显示此项。	如果使用证书认证的方式建立 SSL VPN 连接，则需要勾选“证书认证”。 勾选“证书认证”后，可以选择用于进行证书认证的证书。

参数	说明
密码 **说明** 仅在 Linux 和国产化操作系统下会显示此项。	用于设置证书认证时证书中提取的用户名对应的登录密码。 仅当使用证书认证的方式建立 SSL VPN 连接，且勾选了“证书认证”时可以设置此密码。

3. 设置完成后，单击“保存”，返回主界面。

步骤 2 登录 SSL VPN 虚拟网关。

1. 在“新建 VPN 连接”栏下方选择已经创建的 SSL VPN 连接，双击建立连接或单击左下角“连接”按钮建立连接。

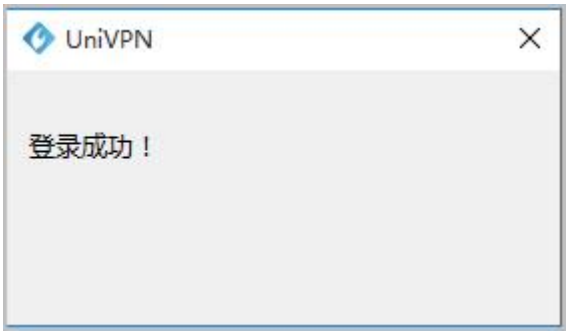
2. 在登录界面输入用户名、密码。

   单击“登录”，发起 VPN 连接。

   若在 Windows 操作系统下采用证书认证，则需要选择证书、输入证书中提取的用户名对应的登录密码，完成登录。在 Windows 证书认证场景下，证书都是导入到 IE 浏览器中的；在 MAC 证书认证场景下，证书需要导入到“凭证”中；在 Linux 和国产化系统证书认证场景下，证书需要放入主目录下的 Certificate 文件夹。导入成功后即可在证书选择列表中选择对应证书。

3. 若组网中存在第三方认证服务器且第三方认证服务器上配置了 Token 序列号认证或短信认证，客户端会弹出输入框，要求用户输入动态令牌码进行双因子认证。客户端支持 Token 序列号和短信验证码两种双因子认证方式，输入获取到的 Token 序列号或短信验证码，单击“确定”完成认证。

4. VPN 接入成功时，系统会在界面右下角进行提示。



连接成功后移动办公用户就可以和企业内网用户一样访问内网资源了。

----结束

5.1.1.2 建立 L2TP VPN 隧道

介绍 L2TP VPN 隧道的配置方法。

配置步骤

步骤 1 新建一条 L2TP VPN 连接。

1. 打开 UniVPN，进入主界面。
   在“选择 VPN 连接”最右侧单击“+新建连接”。

说明

L2TP VPN 不支持使用代理。

2. 配置 L2TP VPN 连接参数。
   在“新建连接”窗口左侧导航栏中选择“L2TP/IPSec”，并配置相关参数。

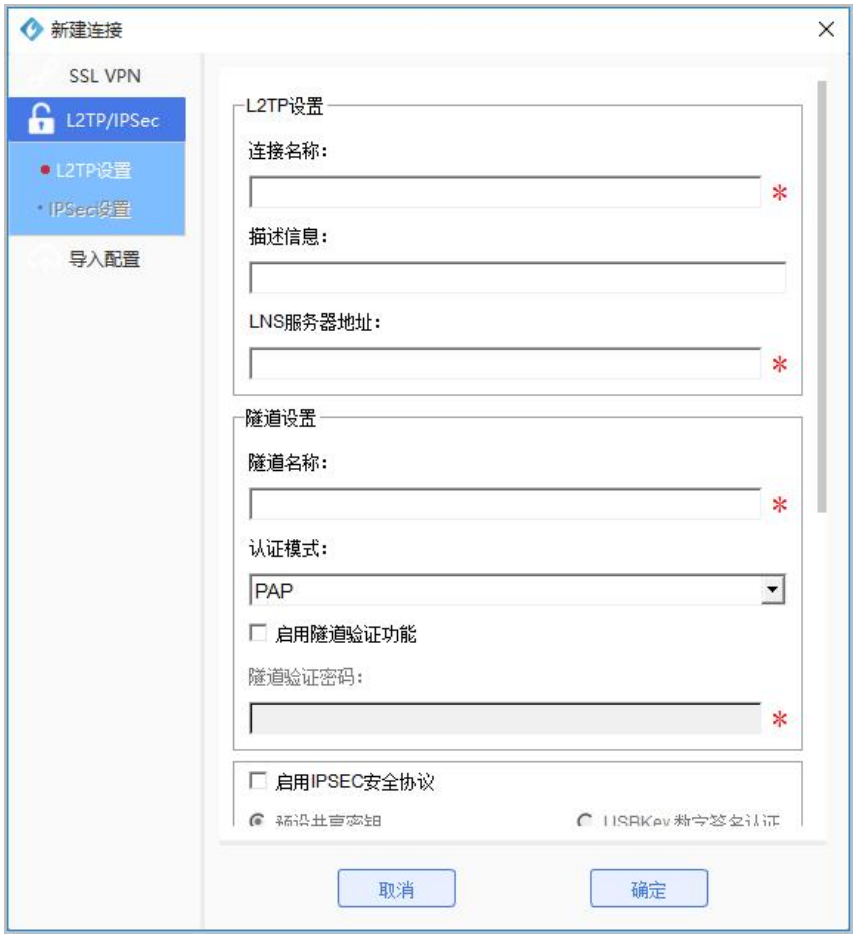


表 5-3 L2TP 配置参数说明

参数	说明
连接名称	用于标识一条 L2TP VPN 连接。连接名称具有唯一性，不允许重名。
描述信息	用于补充说明该条连接的相关信息。例如，可以在此处添加该条连接的创建者、创建时间以及连接用途等信息。
LNS 服务器地址	L2TP VPN 网关地址。该地址必须与 L2TP VPN 网关地址保持一致。地址填写错误，会导致 L2TP VPN 隧道建立失败。
隧道名称	用于在隧道中标识设备本身。隧道名称必须与 LNS 侧配置的名称保持一致，隧道名称填写错误，会导致 L2TP VPN 隧道建立失败。

参数	说明
认证模式	• CHAP 认证：CHAP（Challenge Handshake Authentication Protocol）是一种三次握手验证协议，只在网络上传输用户名，而不传输密码。 • PAP 认证：PAP（Password Authentication Protocol）是一种两次握手验证协议，在网络上传输用户名和密码，密码为明文。 **说明** PAP 不是安全协议，建议使用 CHAP 协议。
启用隧道验证功能	为安全起见，L2TP VPN 在隧道协商时会有隧道验证环节。只有远程接入用户使用的隧道验证密码与 L2TP VPN 网关侧设置的隧道验证密码一致时，隧道才可建立。隧道验证在 L2TP VPN 隧道建立过程中不是必须的，这取决于 L2TP VPN 网关侧的配置。如果网关侧启用了隧道验证功能，则 UniVPN 侧也必须启用此功能。
隧道验证密码	启用隧道验证功能以后，需要设置隧道验证密码，该密码需要向 L2TP VPN 网关管理员获取。
启用 IPSec 安全协议	该参数在 L2TP over IPSec 场景使用，单纯的 L2TP 远程接入场景中无需配置。
路由设置	在设置“连接成功后允许访问 Internet”参数时有如下三种选择，请根据实际需要进行设置。 • 不勾选 移动办公用户拨号成功后，其个人 PC 的默认路由下一跳会被修改为虚拟网卡的 IP 地址。此时，所有流量都会经过虚拟网卡发送到隧道对端，这意味着该用户只能访问企业内网资源，不能访问 Internet。 • 勾选但不在 IP 地址列表框中添加 IP 地址 移动办公用户拨号成功后，其个人 PC 会生成一条目的网段为虚拟网卡对应的 IP 地址段，下一跳为虚拟网卡的 IP 地址的路由。此时，该用户只能访问与虚拟网卡 IP 地址同网段的企业内网资源。由于用户原有路由没有受到影响，所以还可以访问 Internet 和本地局域网。 • 勾选并在 IP 地址列表框中添加 IP 地址 移动办公用户拨号成功后，其个人 PC 会根据 IP 地址列表框中添加的 IP 地址段作为目的网段，生成明细路由，路由下一跳为虚拟网卡。此时，该用户就可以访问 IP 地址列表框中设置的那些企业内网资源了。由于用户原有路由没有受到影响，所以还可以访问 Internet 和本地局域网。

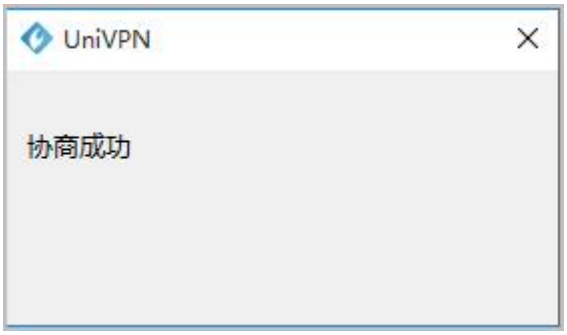
步骤 2 登录 L2TP VPN 网关。

1. 在“选择 VPN 连接”栏下方选择已经创建的 L2TP VPN 连接，双击建立连接或单击左下角“连接”。

2. 在登录界面输入用户名、密码。

3. 单击“登录”，发起 VPN 连接。

VPN 接入成功时，系统会在界面右下角进行提示。



连接成功后移动办公用户就可以和企业内网用户一样访问内网资源了。

----结束

5.1.1.3 建立 L2TP over IPSec VPN 隧道

介绍 L2TP over IPSec VPN 隧道的配置方法。

配置步骤

步骤 1 新建一条 L2TP over IPSec VPN 连接。

1. 打开 UniVPN，进入主界面。
   在“选择 VPN 连接”最右侧单击“+新建连接”。

如您需要使用代理设置，可以单击“选择 VPN 连接”右侧的 Proxy Settings 。

表 5-4 代理设置

参数	说明

参数	说明
代理设置	按照您访问 Internet 时是否使用代理服务器，这里有两种选择。 • 不使用代理 如果您当前访问 Internet 时没有使用代理服务器，此处选择该类型。 • 使用代理服务器 使用代理服务器的场景中细分了 3 种情况 – 使用系统代理：表示使用浏览器中设置的代理服务器信息。 – 使用 HTTP/HTTPS 代理：表示使用 HTTP 或 HTTPS 代理服务器。 – 使用 Sockets5 代理：表示使用 Sockets5 代理服务器 请根据网络实际情况选择代理类型。另外，在选择代理服务器的时候，会要求输入地址、端口、账号、密码信息，该信息请向代理服务器管理员获取。 **说明** L2TP over IPSec 隧道只支持 Sockets5 代理。 缺省情况下，代理类型为“不使用代理”。

2. 配置 L2TP over IPSec VPN 连接参数。

   在“新建连接”窗口左侧导航栏中选中“L2TP/IPSec”，并配置相关参数。

   a. 配置 L2TP 参数。

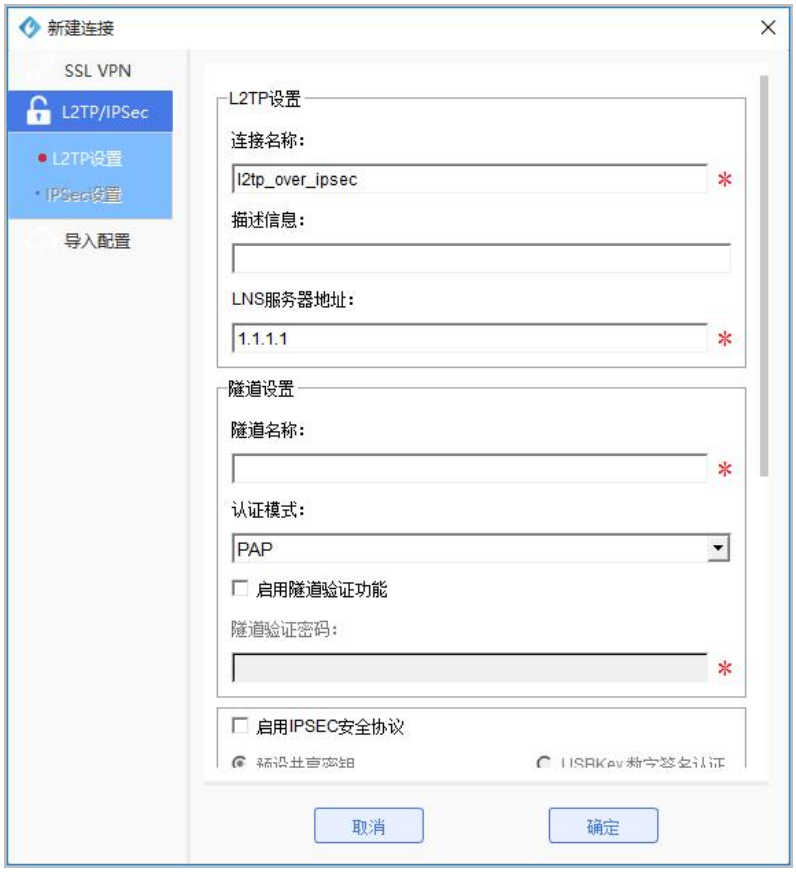


表 5-5 L2TP 配置参数说明

参数	说明
连接名称	用于标识一条 L2TP VPN 连接。连接名称具有唯一性，不允许重名。
描述信息	用于补充说明该条连接的相关信息。例如，可以在此处添加该条连接的创建者、创建时间以及连接用途等信息。
LNS 服务器地址	L2TP VPN 网关地址。该地址必须与 L2TP VPN 网关地址保持一致。地址填写错误，会导致 L2TP VPN 隧道建立失败。
隧道名称	用于在隧道中标识设备本身。隧道名称必须与 LNS 侧配置的名称保持一致，隧道名称填写错误，会导致 L2TP VPN 隧道建立失败。

参数	说明
认证模式	• CHAP 认证：CHAP（Challenge Handshake Authentication Protocol）是一种三次握手验证协议，只在网络上传输用户名，而不传输密码。 • PAP 认证：PAP（Password Authentication Protocol）是一种两次握手验证协议，在网络上传输用户名和密码，密码为明文。 **说明** PAP 不是安全协议，建议使用 CHAP 协议。
启用隧道验证功能	为安全起见，L2TP VPN 在隧道协商时会有隧道验证环节。只有远程接入用户使用的隧道验证密码与 L2TP VPN 网关侧设置的隧道验证密码一致时，隧道才可建立。隧道验证在 L2TP VPN 隧道建立过程中不是必须的，这取决于 L2TP VPN 网关侧的配置。如果网关侧启用了隧道验证功能，则 UniVPN 侧也必须启用此功能。
隧道验证密码	启用隧道验证功能以后，需要设置隧道验证密码，该密码需要向 L2TP VPN 网关管理员获取。

b. 配置 IPSec 参数。


新建连接
SSL VPN
L2TP/IPSec
L2TP设置
IPSec设置
导入配置
L2TP设置
连接名称:
l2tp_over_ipsec
描述信息:
LNS服务器地址:
1.1.1.1
隧道设置
隧道名称:
认证模式:
PAP
启用隧道验证功能
隧道验证密码:
启用IPSEC安全协议
预设共享密钥
USBKey 数字签名认证
身份认证字:
路由设置
连接成功后允许访问 Internet
访问下列地址时使用 VPN 连接
IP地址
子网掩码
取消
确定

表 5-6 IPSec 配置参数说明

参数	说明
启用 IPSec 安全协议	在 L2TP over IPSec 场景中需要勾选此选项。 IPSec 的身份认证分为了预共享密钥认证和 USBKey 数字签名认证两种。 预共享密钥方式下需要输入身份认证字，身份认证字请向 IPSec VPN 网关管理员获取。 USBKey 数字签名认证需要输入 USB Pin 码，USB Pin 码是 USBKey 的持有人为了保护 USBKey 的安全性而设置的加密密码，该密码需要从 USBKey 的持有人处获取。 说明 Linux、国产化和 MAC OS 操作系统下不支持 USBKey 数字签名认证。
IPSec 设置	
IPSec 服务器地址	IPSec VPN 网关的地址。该地址必须与 IPSec VPN 网关地址保持一致。地址填写错误，会导致 VPN 隧道建立失败。
使用 LNS 服务器地址	当 L2TP VPN 网关和 IPSec VPN 网关是同一台网关时，勾选此选项。
封装模式	IPSec 封装是指将 AH（Authentication Header）协议或 ESP（Encapsulating Security Payload）协议相关的字段插入到原始 IP 报文中，以实现对报文的认证和加密，封装模式有传输模式和隧道模式两种。 • 隧道模式：只保护报文载荷部分，常用于 VPN 网关与网关之间建立隧道。 • 传输模式：保护整个报文，常用于移动终端与 VPN 网关建立隧道。 缺省情况下使用传输模式。
ESP 协议验证算法	ESP 协议验证算法用于对原始报文进行完整性校验，可以防止报文在传输过程中被篡改。ESP 协议验证算法包括 MD5、SHA1 和 SHA2-256 三种，考虑到 SHA2-256 的安全性较高，推荐使用 SHA2-256 算法。
ESP 协议加密算法	ESP 协议加密算法用于对原始报文进行加密保护，可以防止报文在传输过程中被窃取。ESP 协议加密算法包括 DES、3DES 和 AES-128/192/256 三种，AES 算法安全性比 DES 和 3DES 算法安全性要高。 AES 算法根据密钥长度不同分为了 AES128、AES192 和 AES256 三种。密钥长度越长，其算法安全性越高，但是相应的报文加解密所消耗的时间也会越长。综合考虑算法安全性以及加解密的效率，此处推荐使用 AES256 算法。
IKE 设置	

参数	说明
协商模式	IPSec 隧道双方在 IKE 协商的时候有两种协商模式。 • 主模式 • 野蛮模式 缺省情况下使用主模式进行隧道协商。如果隧道发起方对于隧道响应方的策略有全面的了解，采用野蛮模式能够更快地创建 IKE SA。
ID 类型	表示身份类型。 身份认证是 IKE 协商的一种保护机制，它通过确认通信双方的身份来确保安全性。 IKE 对等体的身份可采用不同类型，包括 IP 类型和名字类型两种。协商模式选择为主模式时，默认使用 IP 类型，表示以本端的 IP 地址作为本端身份标识；协商模式选择为野蛮模式时，ID 类型转为可选状态，ID 类型就可以选择是使用 IP 或是名字。
本端名字	当身份类型选择为“名字”时，需要设置此参数。 本端名字作为本端的身份标识，要提供给 IPSec VPN 网关进行身份认证。身份认证通过，IPSec VPN 网关才允许 UniVPN 与其建立 IPSec 隧道。“本端名字”要和 IPSec VPN 网关上的对端名称保持一致，名称不一致隧道将建立失败。该参数需要向 IPSec VPN 网关管理员获取。
安全网关名字	当身份类型选择为“名字”时，需要设置此参数。“安全网关名字”要和 IPSec VPN 网关上的本端名称保持一致，名称不一致隧道将建立失败。该参数需要向 IPSec VPN 网关管理员获取。 安全网关名字是 IPSec VPN 网关的身份标识。身份认证是相互的，UniVPN 在与 IPSec VPN 网关建立隧道时，也要校验网关的身份，确保要访问的 IPSec VPN 网关的真实性。IPSec VPN 网关要将自身的身份标识提交给 UniVPN 认证，身份认证通过，UniVPN 才会与 IPSec VPN 网关建立 IPSec 隧道。
验证算法	IKE 协商时，验证算法用于保护报文的完整性。验证算法有 MD5、SHA-1 和 SHA2-256 三种，考虑到 SHA2-256 安全性较高，推荐使用 SHA2-256 算法。
加密算法	IKE 协商时，加密算法用于保护报文的私密性，防止报文在传输过程中被窃取。加密算法有 DES-CBC、3DES-CBC 和 AES-128/192/256 这几种，考虑到 AES-256 安全性较高，推荐使用 AES-256 算法。
DH 组标识	IKE 协商时，DH 组用于实现隧道双方进行密钥材料交换。DH 组按照密钥长度的不同分为了 group1（768 bit）、group2（1024 bit）和 group5（1536 bit）三种。group1 存在安全隐患，推荐使用 Group2 或 Group5。

参数	说明
IKE 高级设置	
启用 PFS 特性	表示在 IKE 协商时使用完美的前向安全 PFS（Perfect Forward Secrecy）功能。 该功能用于本端发起协商时，在 IKEv1 阶段 2 或 IKEv2 创建子 SA 交换的协商中进行一次附加的 DH 交换，保证 IPSec SA 密钥的安全，以提高通信的安全性。 启用本功能，需要配置相应的安全参数，这里安全参数支持 group1（768 bit）、group2（1024 bit）和 group5（1536 bit）。group1 存在安全隐患，推荐使用 Group2 或 Group5。
安全联盟生存周期	IKE SA 的生存周期用于 IKE SA 的定时更新，降低 IKE SA 被破解的风险，有利于安全性。 在设定的生存周期超时前，IKE 将为对等体协商新的 IKE SA。在新的 IKE SA 协商好之后，对等体立即采用新的 IKE SA，而旧的 IKE SA 在生存周期到期后被自动清除。重协商不会导致当前隧道中断。
IPSec 高级设置	
安全联盟生存周期	当以 IKE 动态协商方式建立 IPSec SA 时，IPSec 隧道将在建立时间大小达到阈值时重新协商 IPSec SA，以保证隧道安全性。 重协商不会导致当前隧道中断。

参数	说明
路由设置	路由设置用于控制移动办公用户远程接入成功后所能访问的资源范围。路由设置有两种模式，一种是“Mode Config”模式，另一种是“连接成功后允许访问 Internet”模式。两者的区别在于，“Mode Config”模式下，用户访问资源的范围取决于网关侧的配置。“连接成功后允许访问 Internet”模式下，用户访问资源的范围取决于 UniVPN 侧 IP 地址列表框中的配置。 • Mode Config – 如果对端 VPN 网关支持 Mode Config 协商模式，移动办公用户接入成功后，VPN 网关会将网关侧配置的企业内网地址段推送过来，该用户 PC 就会生成到这些地址段的明细路由，用户就可以访问企业内网中的这些资源。在此过程中，该用户 PC 原有的路由未受影响，用户在访问企业内网资源时，还可以访问 Internet 和本地局域网。 – 如果对端 VPN 网关不支持 Mode Config 协商模式，移动办公用户接入成功后，其个人 PC 的默认路由下一跳会被修改为虚拟网卡的 IP 地址。此时，所有流量都会经过虚拟网卡发送到隧道对端，这意味着该用户只能访问企业内网资源，不能访问 Internet。 • 连接成功后允许访问 Internet – 勾选但不在 IP 地址列表框中添加 IP 地址 移动办公用户拨号成功后，其个人 PC 会生成一条目的网段为虚拟网卡对应的 IP 地址段，下一跳为虚拟网卡的 IP 地址的路由。此时，该用户只能访问与虚拟网卡 IP 地址同网段的企业内网资源。在此过程中，该用户 PC 原有路由没有受到影响，所以在访问企业内网资源的时候，还可以访问 Internet 和本地局域网。 – 勾选并在 IP 地址列表框中添加 IP 地址 移动办公用户拨号成功后，其个人 PC 会以 IP 地址列表框中添加的 IP 地址段作为目的网段，生成明细路由，路由下一跳为虚拟网卡。此时，该用户就可以访问 IP 地址列表框中设置的那些企业内网资源了。在此过程中，该用户 PC 原有路由没有受到影响，所以在访问企业内网资源的时候，还可以访问 Internet 和本地局域网。

3. 设置完成后，单击“保存”，返回主界面。

步骤 2 登录 L2TP over IPSec VPN 网关。

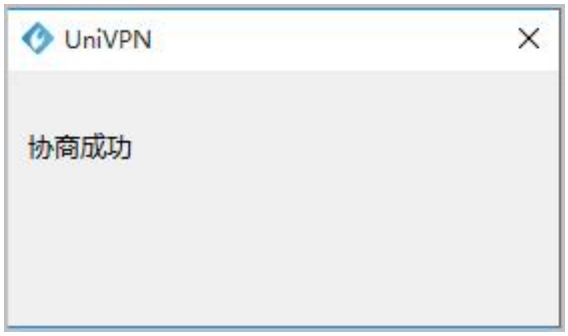
1. 在“连接”下拉列表框中选择已经创建的 L2TP over IPSec VPN 连接，双击建立连接或单击右上角“连接”建立连接。

2. 在登录界面输入用户名、密码。

   若在 Windows 操作系统下采用证书认证，则需要选择证书、输入证书中提取的用户名对应的登录密码，完成登录。在 Windows 证书认证场景下，证书都是导入到 IE 浏览器中的；在 MAC 证书认证场景下，证书需要导入到“凭证”中；在 Linux 和国产化系统证书认证场景下，证书需要放入主目录下的 Certificate 文件夹。导入成功后即可在证书选择列表中选择对应证书。

3. 单击“登录”，发起 VPN 连接。

   VPN 接入成功时，系统会在界面右下角进行提示。



连接成功后移动办公用户就可以和企业内网用户一样访问内网资源了。

----结束

5.1.2 通过配置文件方式建立 VPN 隧道

配置文件方式是指 UniVPN 使用者从其他人员（比如网络管理员）那里拿到一份后缀为.ini 的配置文件，然后将配置文件导入到 UniVPN 就可以建立 VPN 隧道的方式。采用配置文件方式建立 VPN 连接，可以免去您大量的配置工作。

导出配置文件

方法一：

步骤 1 选中一个已存在的 VPN 连接条目，单击连接条目右侧的编辑。

步骤 2 在“编辑连接”窗口中，单击导航栏侧的“导出配置”，并选择配置文件的保存位置。

配置文件默认会被保存为.ini 格式。

步骤 3 单击“保存”，完成导出。

方法二：

步骤 1 选中一个已存在的 VPN 连接条目，单击连接条目右侧的导出。

步骤 2 选择配置文件的保存位置，配置文件默认会保存为.ini 格式。

步骤 3 单击“保存”，完成导出。

----结束

导入配置文件

步骤 1 在 UniVPN 主界面的“选择 VPN 连接”栏右侧，单击“+新建连接”。

步骤 2 在“新建连接”窗口中，选择导航栏左侧的“导入配置”。

步骤 3 单击窗口右侧的“导入配置”，选择预先准备好的配置文件，然后单击“打开”。

步骤 4 单击“确定”，返回 UniVPN 主界面。

可以看到 UniVPN 这条 VPN 连接已经生成，单击左下角“连接”或双击这条 VPN 条目建立连接。

步骤 5 在登录界面输入用户名、密码。

步骤 6 单击“登录”，发起 VPN 连接。

VPN 接入成功时，系统会在界面右下角进行提示。

连接成功后移动办公用户就可以和企业内网用户一样访问内网资源了。

----结束

5.2 常用设置

介绍 UniVPN 的一些常用功能设置。

连接/断开连接

单击 UniVPN 客户端主界面左下角的“连接”图标，可以直接向 VPN 网关发起隧道连接请求；在页面左下角中选择“断开连接”，将会拆除当前的 VPN 隧道。

修改密码

单击 UniVPN 页面右上角的  图标，在菜单中选择“修改密码”，可以修改当前用户的登录密码。

说明

- 只有当 UniVPN 与设备建立了 VPN 隧道的时候才能修改密码，未建立 VPN 隧道时“修改密码”菜单项是无法使用。另外，修改密码将中断当前业务，需要重新登录，请慎重操作。
- 仅 SSL VPN 场景下支持修改密码。

错误报告

在您遇到 UniVPN 出现无法排除的故障时，请向联软工程师获取帮助。为了便于联软工程师快速的定位问题，请您在获取帮助之前预先收集 UniVPN 的错误报告。

说明

UniVPN 生成错误报告时会收集客户端软件的使用信息，请采取足够的措施以确保以下信息受到严格保护。

- **netcard_info.txt：**记录设备的网卡信息,可以在 UniVPN 文件夹中查看。
- **operate_system_info.txt：**记录设备的操作系统信息，可以在 UniVPN 文件夹中查看。
- **route_info.txt：**记录设备的路由信息，可以在 UniVPN 文件夹中查看。
- **UniVPN_UniVPNCS_0.log：**记录 UniVPN 客户端业务配置产生的日志信息，例如用户登录成功或失败、VPN 隧道建立正常或异常等信息，可以在 UniVPN/log 文件夹中查看。
- **UAA_0：**记录连接网关正常或异常的日志信息，可以在 log 文件夹中查看。
- **UniVPNTray_0:** 记录托盘产生的日志信息，可以在 log 文件夹中查看。
- **UniVPN_UniVPNUI_0.log:** 记录客户端配置界面产生的日志信息，例如 VPN 连接配置和中英文界面切换所产生的日志信息，可以在 log 文件夹中查看。
- **UniVPN_UniVPNPromoteService_0.log：**记录 UniVPN 客户端的服务进程信息，服务进程用于确保客户端正常运行，可以在 log 文件夹中查看。
- **崩溃文件：**当 UniVPN 客户端出现异常关闭时会生成崩溃文件，造成异常关闭的原因不同，生成的崩溃文件名称也不同。在 Windows 操作系统下崩溃文件的后缀是“*.dmp”，可以在 log 文件夹中查看，在 MAC、Linux 和国产化操作系统下生成的崩溃文件后缀为*.core。

步骤 1 右键单击 UniVPN 的托盘图标。

步骤 2 选择“错误报告”。

步骤 3 单击“确定”。

可以在错误报告里反馈遇到的问题

单击“确定”会自动生成错误报告，错误报告生成后，您可以将此报告通过邮件、U 盘或是其他方式发送给联软工程师，由联软工程师协助您解决问题。

----结束

取消自动登录

右键单击 UniVPN 的托盘图标，在菜单中选择“取消自动登录”可以取消之前的自动登录设置。

设置

步骤 1 单击 UniVPN 主页面右上角  按钮，在菜单栏里选择“设置”或者右键单击 UniVPN 托盘图标，在菜单栏里选择“设置”，设置参数如下。

表 5-7 高级页签参数说明

功能项	说明
开机自启动	勾选此项，UniVPN 在用户启动主机时会自动启动。 缺省情况下，此选项为去勾选状态。
VPN 验证服务器可信	UniVPN 与设备建立 SSL VPN 隧道时，UniVPN 会校验设备发送过来的设备证书。 • 勾选此选项 UniVPN 校验设备证书失败时，系统会给出“安全告警：不可信的 VPN 服务器证书！”的告警，在确知当前网络安全的情况下，可以选择“是”，继续建立 SSL VPN 隧道。如果对当前网络安全情况不了解，可以选择“否”，中止隧道建立过程。 • 不勾选此选项 则证书校验失败时，系统不会给出告警提示，直接完成隧道建立。 缺省情况下，此选项为勾选状态。
VPN 检测新版本	勾选后，系统会检查待连接的设备网关上是否存在新的 UniVPN 版本。 缺省情况下，此选项为勾选状态。
界面语言	支持手动切换界面语言。 目前客户端支持 2 种界面语言，包括： • 英语 • 中文 • 跟随系统 **说明** 首次运行客户端时，若操作系统的语言在支持的 2 种界面语言范围内，则客户端界面安装语言默认为“跟随系统”与操作系统的语言一致；若操作系统的语言不在支持的 2 种界面语言范围内，则客户端界面语言默认为英语。

步骤 2 单击“确定”。

----结束

代理屏蔽

- 在 Windows 操作系统下：

  Windows 操作系统使用的是 IE 浏览器的代理信息，因此需要修改 IE 浏览器的代理信息设置。

  a. 打开 IE 浏览器，单击“工具”按钮，打开“Internet 选项”。

  b. 选择“连接”页签，单击“局域网设置”按钮。

c. 在“代理服务器”设置界面设置代理屏蔽信息。

d. 单击“确定”，保存设置。

- 在 Linux 操作系统下：

  Linux 操作系统缺省使用火狐浏览器自带的代理信息设置模块。

  a. 打开火狐浏览器，在地址栏中输入“about:preferences”。

  b. 选择“常规 > 网络设置”页签，单击“设置”按钮。

  c. 设置代理屏蔽信息。

  d. 单击“确定”，保存设置。

- 在 MAC 操作系统下：

  MAC 操作系统缺省使用火狐浏览器自带的代理信息设置模块。

  a. 打开火狐浏览器，在地址栏中输入“about:preferences”。

  b. 选择“常规 > 网络设置”页签，单击“设置”按钮。

  c. 设置代理屏蔽信息。

  d. 单击“确定”，保存设置。

- 在国产化操作系统下：

  国产化操作系统缺省使用火狐浏览器自带的代理信息设置模块。

  a. 打开火狐浏览器，在地址栏中输入“about:preferences”。

  b. 选择“常规 > 网络设置”页签，单击“设置”按钮。

  c. 设置代理屏蔽信息。

  d. 单击“确定”，保存设置。

当在“局域网设置”界面配置代理服务器并登录客户端成功后，会自动生成 PAC 文件。在“局域网设置”界面勾选“使用自动配置脚本”后，将会自动填充 PAC 文件地址，并在客户端登录期间使用该 PAC 文件进行代理屏蔽。在客户端退出后，浏览器会自动恢复登录前的代理设置。

PAC 文件中的设置可以引导流量正确访问网关和内网资源，从而防止浏览器中设置的代理服务器引起的内网资源无法正确访问的问题。PAC 文件中对原有代理信息不会做任何修改，不会影响原有的代理功能。

登录客户端期间，如果删除该 PAC 文件，在采用代理的情况下可能出现无法通过 IE 浏览器访问网关或内网资源的情况。

关于

右键单击 UniVPN 托盘图标，在菜单中选择“帮助 > 关于”。

“关于”选项中记录了 UniVPN 的版本和版权信息

帮助

右键单击 UniVPN 托盘图标，在菜单选择“帮助 > 帮助”。

“帮助”选项包含了 UniVPN 软件的使用指导，可以帮助用户更好的熟悉和使用 UniVPN，以及解决您在使用 UniVPN 过程中遇到的问题。

退出

右键单击 UniVPN 客户端托盘图标，选择“退出”按钮，关闭 UniVPN 软件。

6 升级

本节介绍 UniVPN 的升级方法。

背景信息

UniVPN 升级的基本过程是，网络管理员先把新的 UniVPN 软件上传至设备，用户通过 UniVPN 与设备建立 VPN 隧道时，UniVPN 客户端会自动检查设备上是否存在新的版本，如果存在新版本则会提示用户做版本升级。

操作步骤

步骤 1 网络管理员上传 UniVPN 软件安装包至设备。

1. 登录网站 https://www.leagsoft.com，在首页进入“产品与方案 > 通用方案 > Uni VPN Client 远程接入终端方案”，在 UniVPN 介绍页面最下方单击链接下载对应版本的软件安装包。
2. 登录设备管理页面，选择“系统 > VPN 客户端升级”。
3. 单击对应客户端软件后的“本地升级”，单击“浏览”，选择待上传的 UniVPN 软件安装包。

   UniVPN 针对 Windows 操作系统、Linux 操作系统、MAC 操作系统和国产化操作系统分别提供了对应的软件安装包。因此网络管理员要根据用户实际使用的操作系统类型上传对应软件安装包。软件安装包和操作系统类型不匹配，系统会提示升级失败。新上传的软件安装包将覆盖之前旧的软件安装包。

说明

USG6101/6305/6305-W/6310S/6310S-W/6310S-WL/6510/6510-WLUSG6305/6305-W/6310S/6310S-W/6310S-WL-OVS/6510/6510-WL 机型没有提供本地升级功能。网络管理员需要将 UniVPN 软件放置在一台文件服务器上，然后在此处的“客户端软件下载地址”中填写上对应文件服务器的 URL 地址。

4.单击“升级”，完成设备侧软件安装包升级。

步骤 2 用户侧升级 UniVPN 版本。

当用户与设备建立 VPN 隧道时，用户侧会自动检测当前设备上是否存在新的 UniVPN 版本。如果存在，则用户根据系统提示下载并安装即可。

说明

Linux 和 MAC 系统多用户同时登录时，不支持自动升级；国产化不支持自动升级。

7 故障处理

本文档仅介绍客户端的基础配置，如您需要获取场景化的配置案例，或者您在使用过程中遇到任何问题，请联系对应的销售人员进行反馈，我们将尽快为您解决。

8 FAQ

介绍您在使用 UniVPN 过程中常问的问题，并给出解答。

修改系统时间后，VPN 连接断开，如何解决？

启用 IPSec 安全协议后，如果将 IPSec 的安全联盟生存周期时间设置较短，修改系统时间可能会使安全联盟老化，从而导致连接断开。

建议启用 IPSec 安全协议后，不要修改系统时间。

UniVPN 是否可以和其他 VPN 拨号软件一起使用？

建议不要在同一台计算机上同时安装或使用多个 VPN 拨号软件，否则会出现不可预知的错误。

为什么运行安装程序后，安装程序提示卸载 UniVPN 客户端？

这是因为之前已经安装了 UniVPN 客户端，安装程序首先会删除之前安装的版本。在删除完成后，需要再次运行安装程序才可以将 UniVPN 安装到硬盘上。

为什么首次建立 VPN 连接会出现连接失败的现象？

这是因为操作系统自带的防火墙可能会阻断你的 VPN 连接操作，将操作系统自带防火墙的访问规则设置为允许就可以解决这个问题了。

为什么安装 UniVPN 会失败？

请检查您的登录帐户是否拥有管理员权限，只有具备管理员权限的用户才可以安装。

为什么 UniVPN 软件更新会提示失败？

终端用户在更新 UniVPN 软件时系统会提示失败，这有可能是：

- 网络管理员在 VPN 网关中上传了错误的 UniVPN 软件安装包，此时需要联系网络管理员确认软件安装包格式是否正确。
- UniVPN 与 SSL VPN 虚拟网关之间部署了 NAT Server 设备，由于 NAT Server 无法对 UniVPN 的更新消息进行处理，造成 UniVPN 更新失败。

9 附录

9.1 移动客户端

除了 PC 版的 **UniConnect** 客户端外，联软公司还推出了基于 iOS 及 Android 操作系统的移动版客户端。

获取

- **获取 iOS 操作系统版本的移动版客户端**

  方式一：打开“**APP Store**”APP，搜索“**UniConnect**”字段，即可下载最新版本的 UniConnect iOS 版本客户端。

- **获取 Android 操作系统版本的移动版客户端**

  方式一：下载并打开“**应用市场类** APP，搜索“**UniConnect**”字段，即可下载最新版本的 UniConnect Android 版本客户端。

规格

移动版 UniConnect 客户端目前仅支持建立 SSL VPN 连接，具体支持的机型及操作系统版本如下：

表 9-1 移动版 UniConnect 客户端支持的机型及操作系统版本

操作系统	iOS	Android

操作系统	iOS	Android
支持的操作系统版本	支持 iOS 10.0 及以上版本。	支持 Android 5.0 及以上版本。
支持的设备型号	• 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	-
支持的设备屏幕分辨率	-	• 720*1280 • 1080*1920 • 1440*2560 • 2160*4096

移动版 UniConnect 客户端的功能规格如下：

表 9-2 移动版 UniConnect 客户端的功能规格

功能名称		iOS	Android
SSL VPN	网络扩展	支持	支持
	终端安全 **说明** 网关侧开启终端安全功能时，移动版 UniConnect 客户端可以拨号成功。	支持	支持

功能名称		iOS	Android
	网关优选	支持	支持
	断线重连	支持	支持
	链路备份 **说明** 网关侧开启链路备份功能时，移动版 UniConnect 客户端可以拨号成功。	支持	支持
	证书认证	支持	支持
	MAC 认证	不支持	不支持
	证书筛选	支持	支持
	双因子认证	支持	支持 可通过短信验证码进行双因子认证
L2TP VPN		不支持	不支持
L2TP over IPSec VPN		不支持	不支持
NAT 穿越		不支持	不支持
代理穿越		不支持	不支持
隧道分离		支持	支持
基本功能	开机自启动	不支持	不支持
	界面语言切换 **说明** 仅支持中英文切换。	支持	支持
	自动登录	支持	支持
配置文件	导入	不支持	不支持
	导出	不支持	不支持
故障定位		支持	支持

功能名称	iOS	Android
命令行配置	不支持	不支持
非管理员权限用户配置	支持	支持

移动版 UniConnect 客户端的性能规格如下：

表 9-3 移动版 UniConnect 客户端的性能规格

功能名称	规格
VPN 新建连接数	16 个

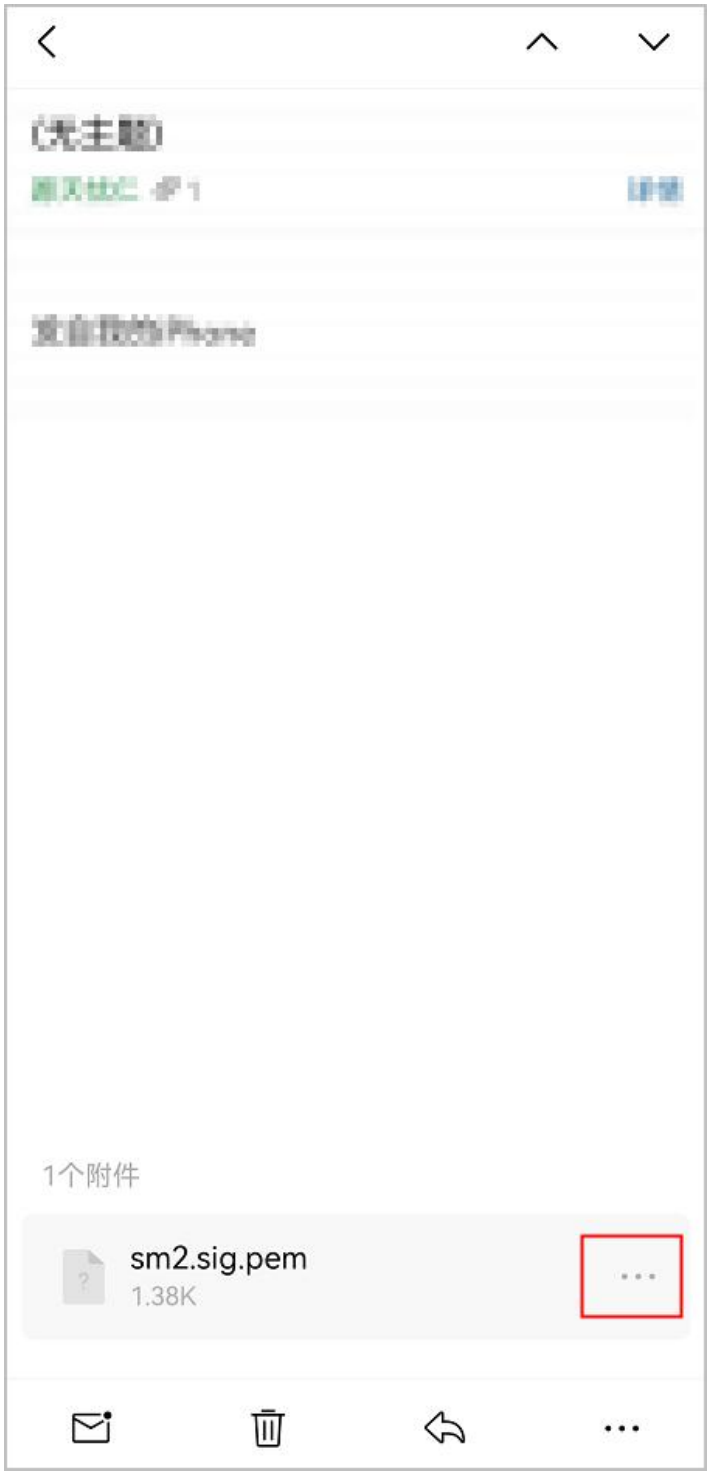
操作

移动版 UniConnect 客户端的具体操作，请参见 APP 内“  > 帮助”节点下的联机帮助。

9.1.1 证书认证场景

国密证书和非国密证书导入客户端方法一致，下面以国密证书导入 UniConnect 为例，介绍 UniConnect 导入并使用证书认证。

步骤 1 打开邮箱找到此文件，点击右下角的  。



步骤 2 单击此文件（没有下载就会请求下载）选择**“分享文件”**。

步骤 3 选择 UniConnect。

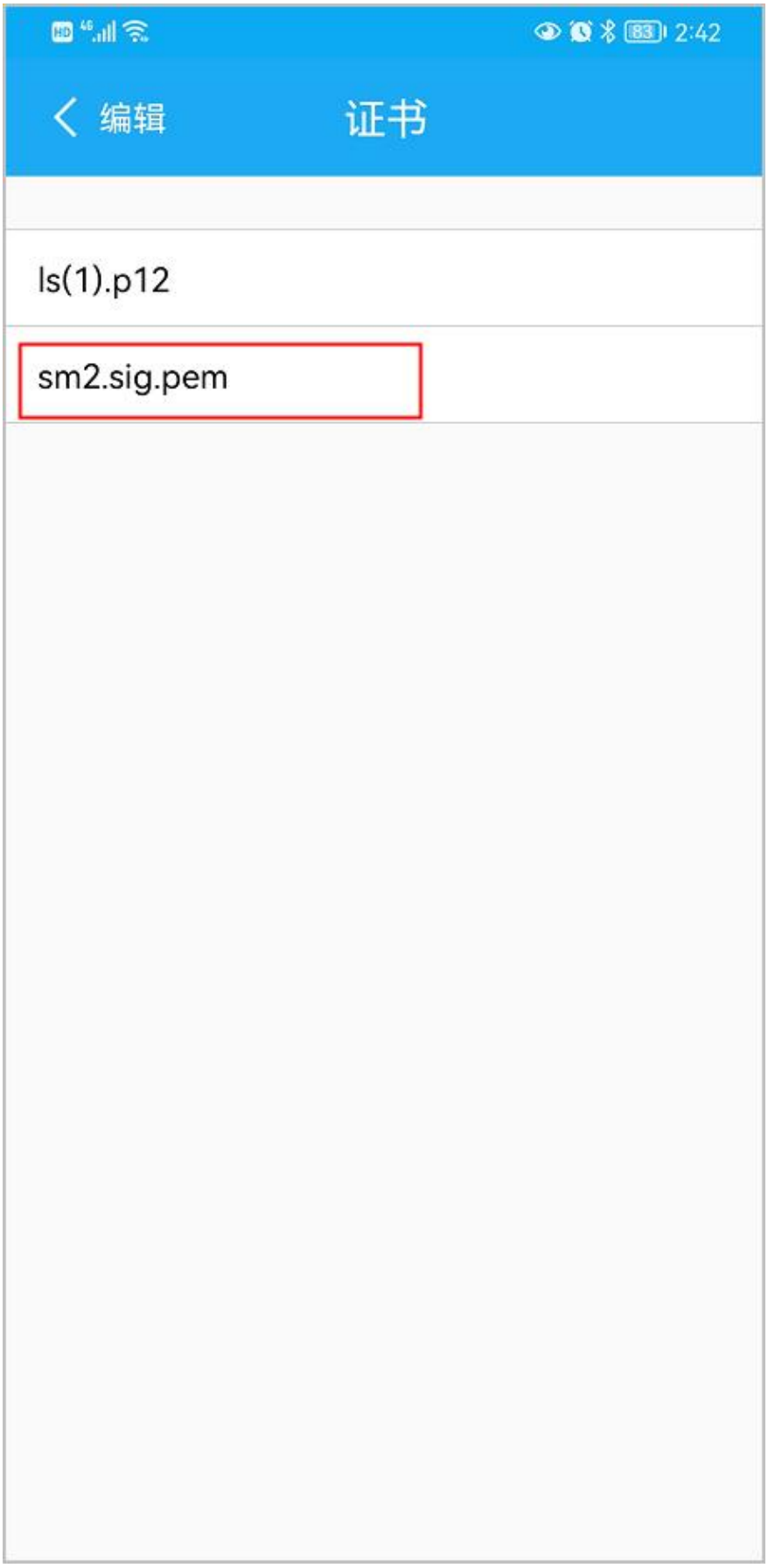

2:42
(无主题)
愿天忧仁 1
详情
请勿轻信邮件中的密保，汇款，中奖信息
分享文件
转为演示
转为PDF
AI 隐私保护
B612咔叽
EasyConnect
Fleet
Telegram
UniConnect
WLAN 直连
取消

步骤 4 单击**“确定”**。


2:42
返回
保存
提示
确认保存?
取消
确定

步骤 5 导入成功后开启“证书认证”开关。

步骤 6 单击“证书选择”选择国密证书。


2:42
编辑
证书
ls(1).p12
sm2.sig.pem

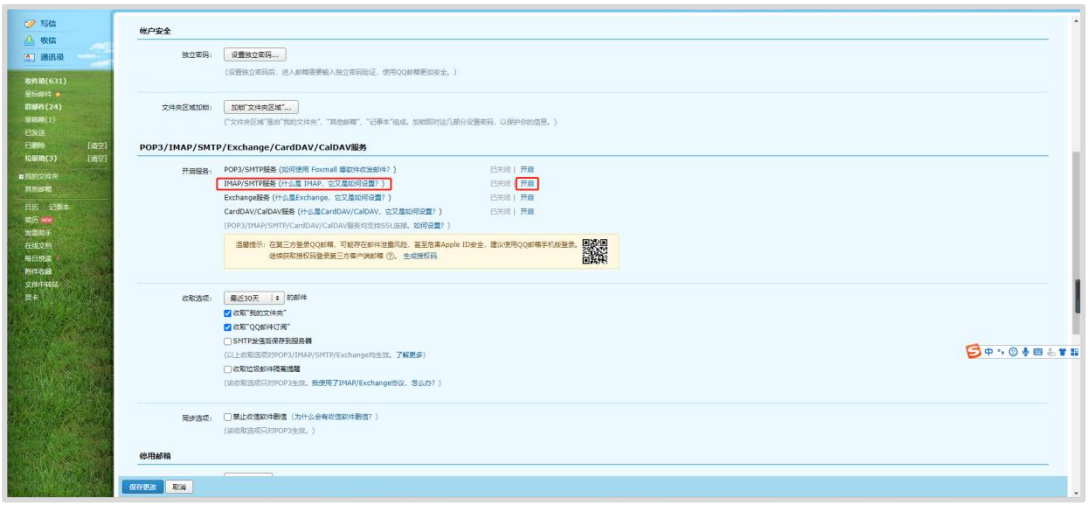
----结束

9.1.2 IOS 问题反馈

配置邮箱

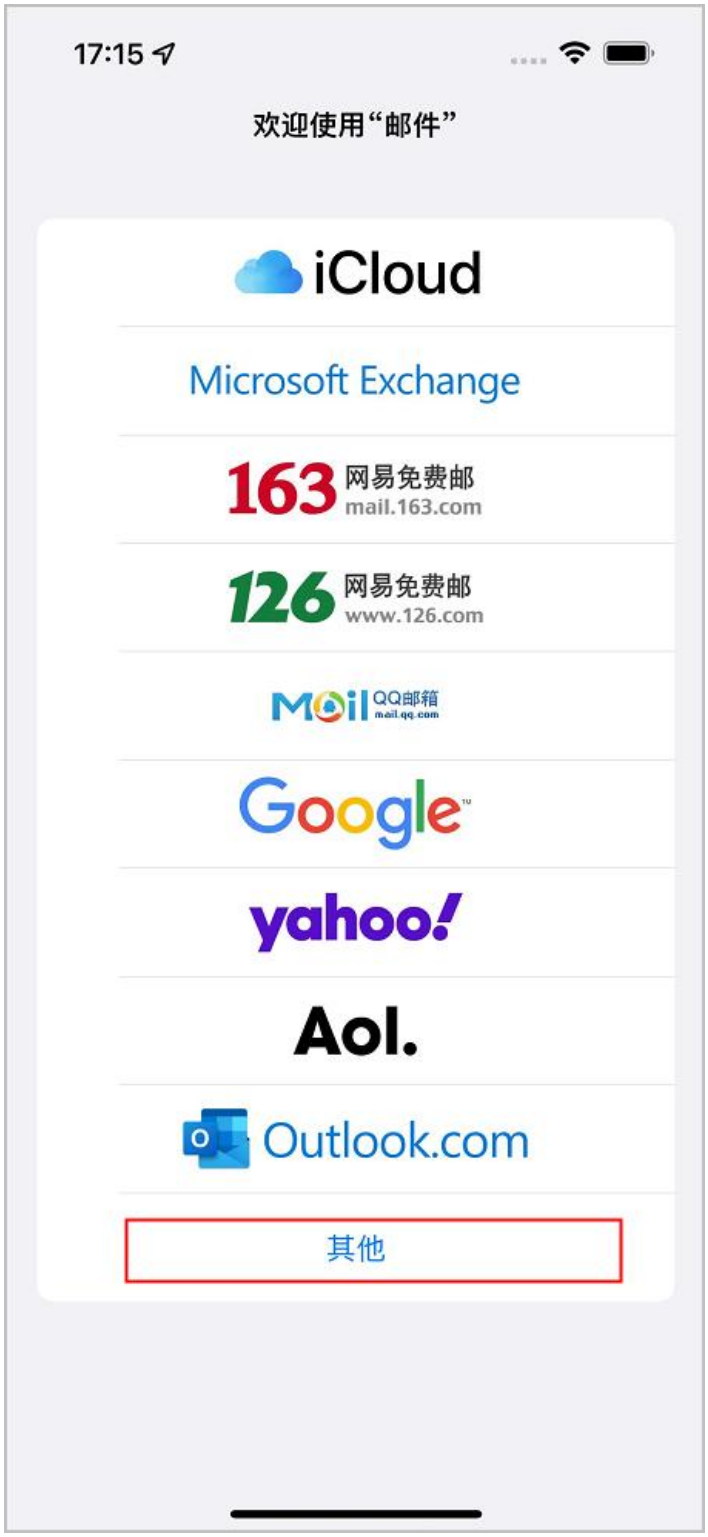
步骤 1 进入 QQ 邮箱，单击左上角“设置”，选择“账户”。

步骤 2 在 “账户”页中，单击 IMAP/SMTP 后的“开启”开启 IMAP 服务。



步骤 3 单击开启后发送短信，获得授权码。

步骤 4 打开手机桌面中的邮箱，选择“其他”QQ 邮箱。



步骤 5 将电脑页面显示的授权码填入此密码框。

步骤 6 单击右上角的 “下一步”。

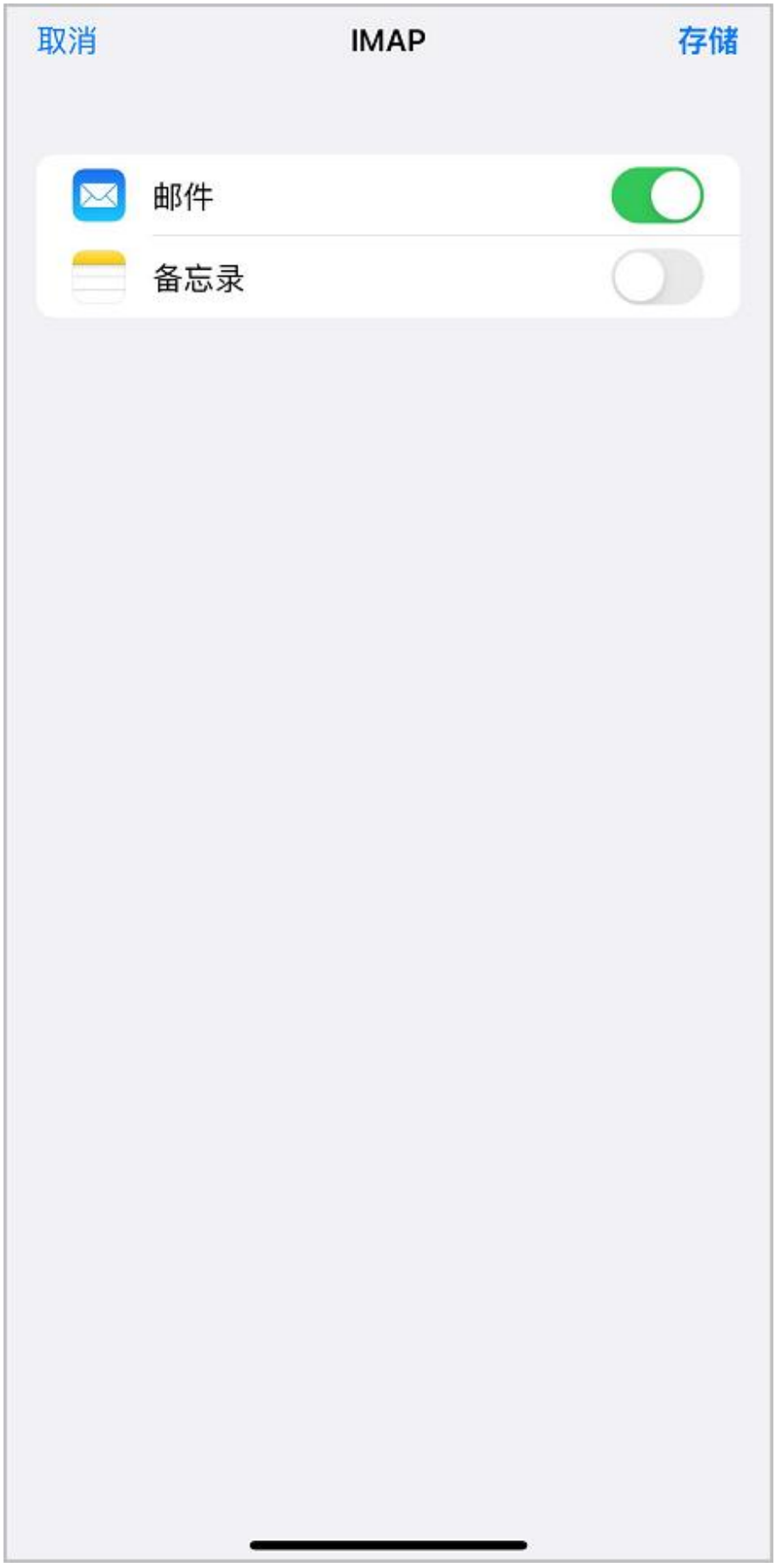
步骤 7 填写 QQ 账户信息：全名，电子邮箱，描述；

收件服务器： 主机名（imap.qq.com），用户名(为电子邮箱），密码（填写 step3 中获取的授权码）；

发件服务器所填写信息与收件服务器相同,（Host name 为 smtp.qq.com,密码填写授权码）


取消
帐户
完成
QQ帐户信息
全名
电子邮件
描述
收件服务器
主机名
imap.qq.com
用户名
密码
发件服务器
SMTP
smtp.qq.com
高级

步骤 8 单击“存储”。


取消
IMAP
存储
邮件
备忘录

步骤 9 配置成功后，在登录页面选择“ >反馈”开启反馈日志后进行操作。

----结束

9.1.3 取消自动登录（安卓）

步骤 1 步骤 1 在登录时用户密码时开启自动登录，然后连接成功。

步骤 2 步骤 2 断开连接后，编辑任一连接将自动登录按钮关闭，单击“保存”即取消自动登录已。

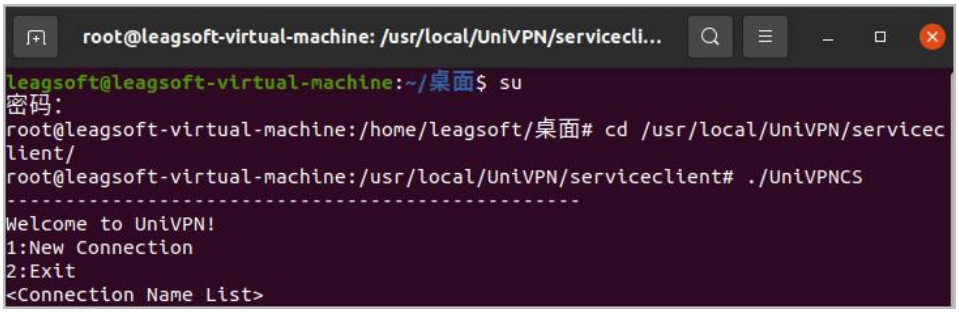
----结束

9.2 在 Linux 操作系统下通过命令行方式配置客户端

9.2.1 启动客户端

步骤 1 进入/usr/local/UniVPN/serviceclient 目录。

步骤 2 执行：./UniVPNCS，启动客户端。该命令普通用户和 root 用户均可执行。



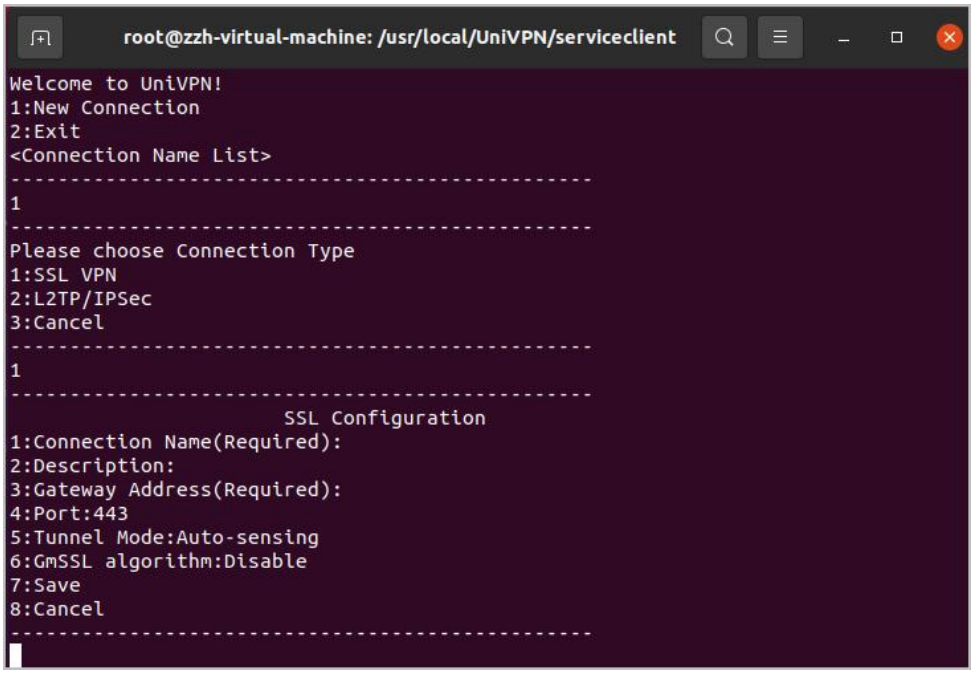
说明

通过命令行方式启动客户端前，请确保通过 UI 桌面启动的客户端已经关闭，二者无法同时运行。

----结束

9.2.2 配置 SSL VPN 连接

配置 SSL VPN



步骤 1 输入 **1**，创建新连接。

步骤 2 输入 **1**，选择创建的 VPN 类型为 SSL VPN。

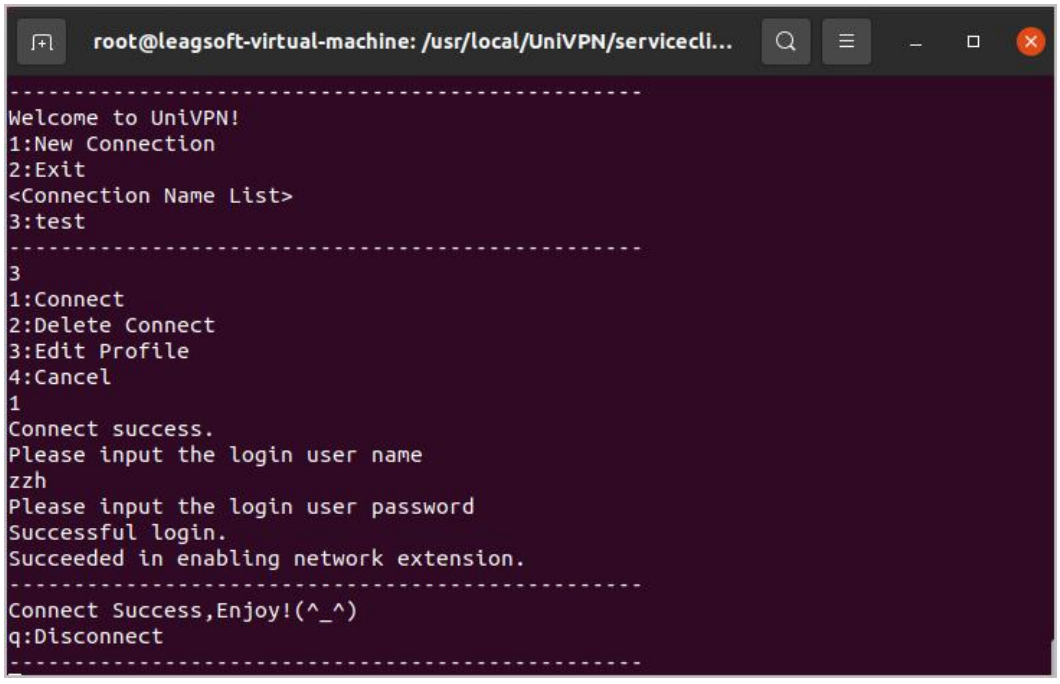
步骤 3 输入对应序号，完成参数 1~5 的配置。

- 1. Connection Name(Required)：连接名称；
- 2. Description：描述信息；
- 3. Gateway Address：远程网关地址；
- 4. Port(Required)：端口；
- 5. Tunnel Mode(Required)：隧道模式，可选模式有 Reliable Transmission（可靠传输模式）、Quick Transmission（快速传输模式）、Auto-sensing（自适应模式）。

步骤 4 输入 **7**，保存配置。

----结束

建立 SSL VPN 连接



步骤 1 输入对应序号，选择创建的 SSL VPN 连接。

步骤 2 输入 **1**，开始建立 SSL VPN 连接。

步骤 3 界面显示连接建立成功，输入用户名和密码进行登录。

----结束

说明

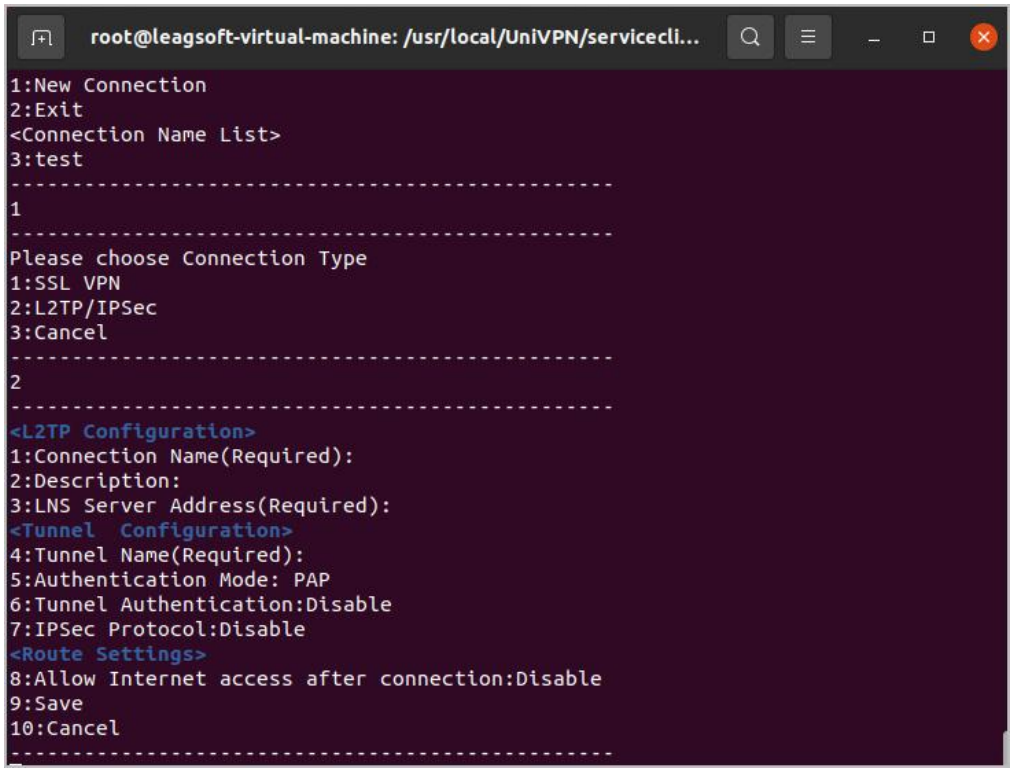
- 在 Linux 操作系统下通过命令行方式配置并建立的 SSL VPN 连接仅支持通过用户名/密码认证方式认证登录。
- 连接成功后，不能关闭该终端窗口，否则连接会断开。

断开 SSL VPN 连接

输入 **q**，即可断开连接。

9.2.3 配置 L2TP VPN 连接

配置 L2TP VPN



步骤 1 输入 **1**，创建新连接。

步骤 2 输入 **2**，选择创建的 VPN 类型为 L2TP/IPSec。

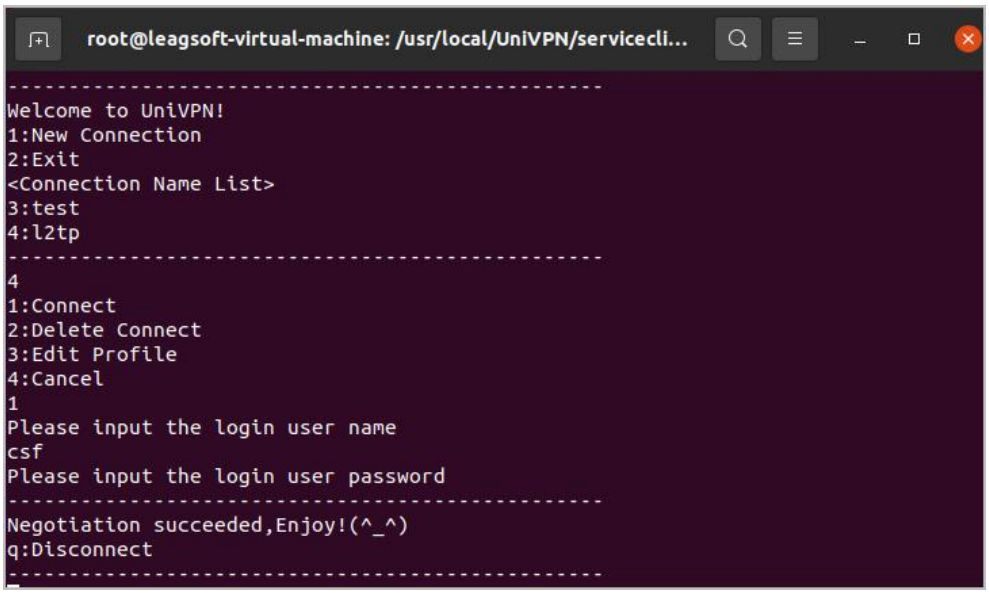
步骤 3 输入对应序号，完成参数 1~8 的配置。

- 1. Connection Name(Required)：连接名称；
- 2. Description：描述信息；
- 3. LNS Server Address(Required)：LNS 服务器地址；
- 4. Tunnel Name(Required)：隧道名称；
- 5. Authentication Mode：认证模式；
- 6. Tunnel Authentication：启用隧道验证功能，启用后，需要输入隧道验证密码（Tunnel Authentication Password）；
- 7. IPSec Protocol：启用 IPSec 安全协议，此功能请勿启用；
- 8. Allow Internet access after connection：路由设置，启用后，可以通过添加 IP 地址网段设置需要进入 VPN 隧道的待加密流量。

步骤 4 输入 **9**，保存配置。

----结束

建立 L2TP VPN 连接



步骤 1 输入对应序号，选择创建的 L2TP VPN 连接。

步骤 2 输入 **1**，开始建立 L2TP VPN 连接。

步骤 3 输入用户名和密码进行登录。

----结束

说明

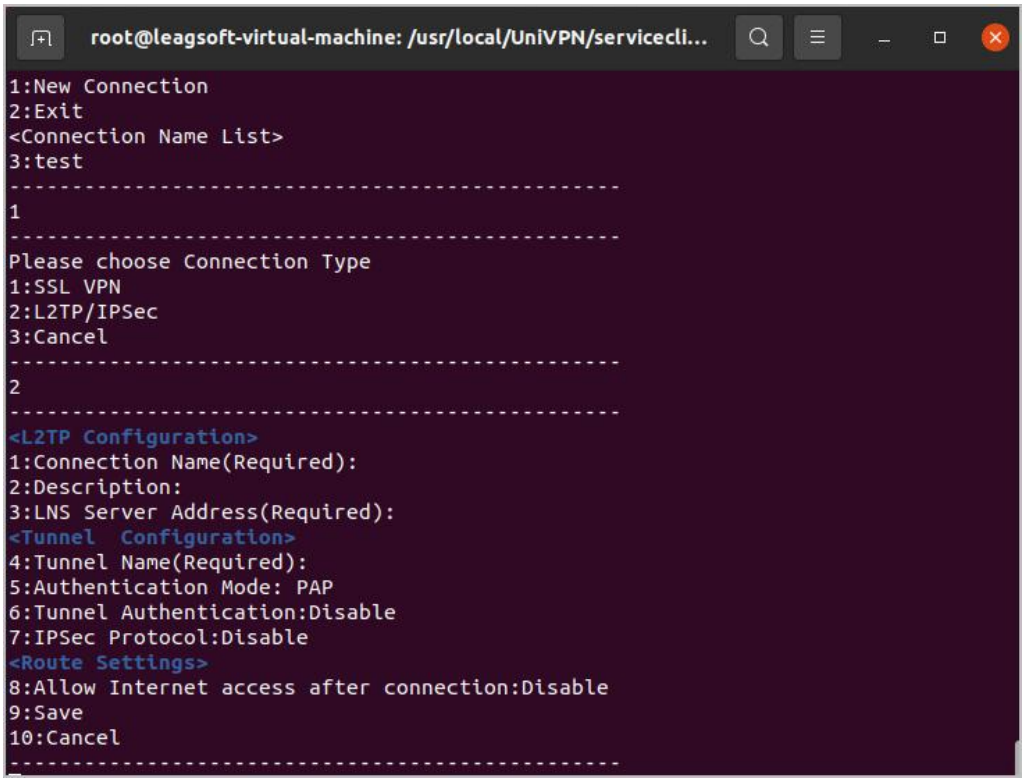
连接成功后，不能关闭该终端窗口，否则连接会断开。

断开 L2TP VPN 连接

输入 **q**，即可断开连接。

9.2.4 配置 L2TP over IPSec VPN 连接

配置 L2TP 参数



步骤 1 输入 **1**，创建新连接。

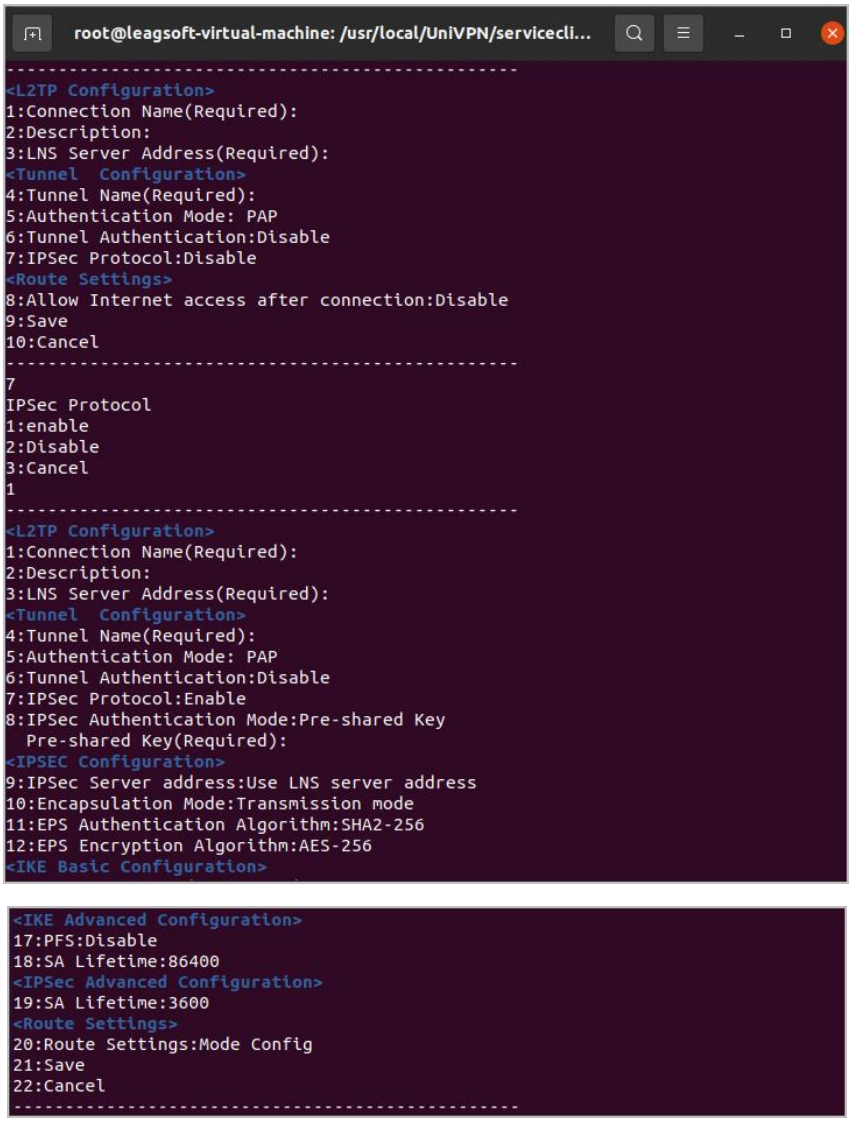
步骤 2 输入 **2**，选择创建的 VPN 类型为 L2TP/IPSec。

步骤 3 输入对应序号，完成参数 1~6 的配置。

- 1. Connection Name(Required)：连接名称；
- 2. Description：描述信息；
- 3. LNS Server Address(Required)：LNS 服务器地址；
- 4. Tunnel Name(Required)：隧道名称；
- 5. Authentication Mode：认证模式；
- 6. Tunnel Authentication：启用隧道验证功能，启用后，需要输入隧道验证密码（Tunnel Authentication Password）；

----结束

配置 IPSec 参数



步骤 1 输入 **7**，启用 IPSec 安全协议。

步骤 2 输入对应序号，完成参数 8~20 的配置。

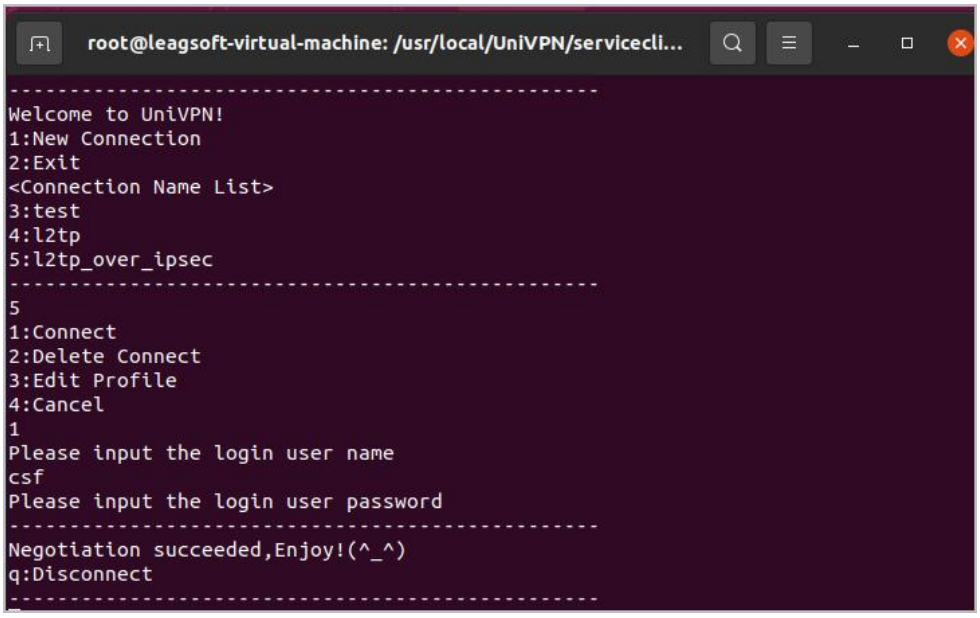
- 8. IPSec Authentication Mode：Linux 操作系统下 IPSec 的身份认证方式目前仅支持预共享密钥认证，预共享密钥方式下需要输入身份认证字（Pre-shared key）；
- 9. IPSec Server address：IPSec 服务器地址，缺省设置为使用 LNS 服务器地址（Use LNS server address）；
- 10. Encapsulation Mode：IPSec 封装模式，包括传输模式（Transmission mode）和隧道模式（Tunnel mode）两种；
- 11. ESP Authentication Algorithm：ESP 协议验证算法；
- 12. ESP Encryption Algorithm：ESP 协议加密算法；
- 13. Negotiation Mode：IKE 协商模式，包括主模式（Main Mode）和野蛮模式（Aggressive Mode）两种；
- 14. Authentication Algorithm：IKE 协商验证算法；
- 15. Encryption Algorithm：IKE 协商加密算法；

- 16. DH Group ID：IKE 协商 DH 组标识；
- 17. PFS：启用 PFS 特性，启用后，需要配置相应的安全参数（Security Parameter）；
- 18. SA Lifetime(IKE Advanced Configuration)：IKE 安全联盟生存周期；
- 19. SA Lifetime(IPSec Advanced Configuration)：IPSec 安全联盟生存周期；
- 20. Route Settings：路由设置，包括“Mode Config”模式和“Allow Internet access after connection”模式，设置为“Allow Internet access after connection”模式后，可以通过添加 IP 地址网段设置需要进入 VPN 隧道的待加密流量。

步骤 3 输入 21，保存配置。

----结束

建立 L2TP over IPSec VPN 连接



步骤 1 输入对应序号，选择创建的 L2TP over IPSec VPN 连接。

步骤 2 输入 **1**，开始建立 L2TP over IPSec VPN 连接。

步骤 3 输入用户名和密码进行登录。

----结束

说明

- 在 Linux 操作系统下通过命令行方式配置并建立的 L2TP over IPSec VPN 连接仅支持通过用户名/密码认证方式认证登录。
- 连接成功后，不能关闭该终端窗口，否则连接会断开。

断开 L2TP over IPSec VPN 连接

输入 **q**，即可断开连接。

9.3 在国产化操作系统下通过命令行方式配置客户端

9.3.1 启动客户端

步骤 1 进入/usr/local/UniVPN/serviceclient 目录。

步骤 2 执行：./UniVPNCS，启动客户端。该命令普通用户和 root 用户均可执行。

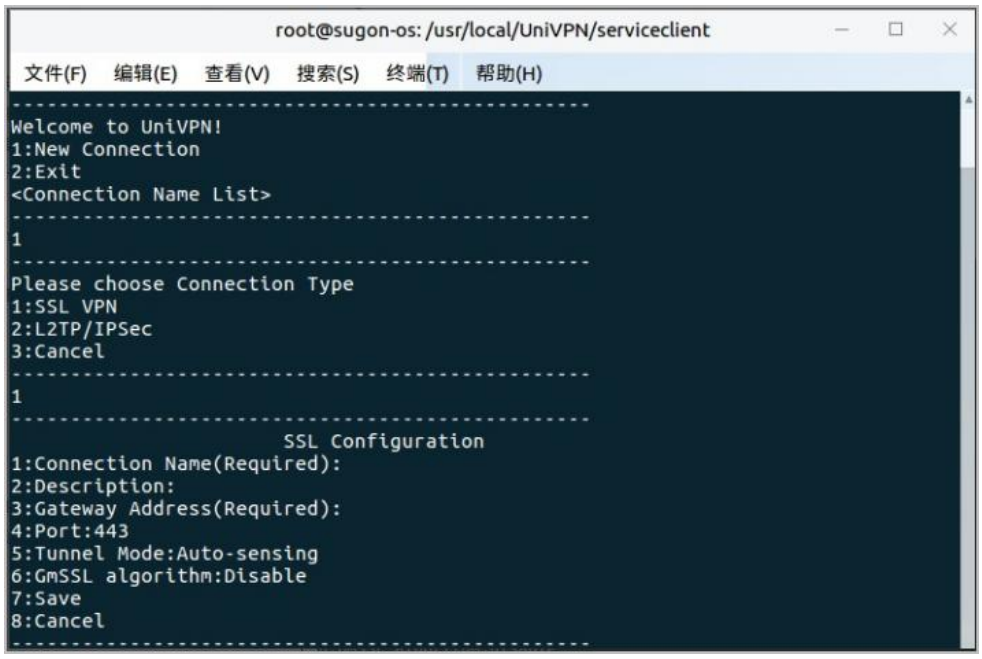
说明

通过命令行方式启动客户端前，请确保通过 UI 桌面启动的客户端已经关闭，二者无法同时运行。

----结束

9.3.2 配置 SSL VPN 连接

配置 SSL VPN



步骤 1 输入 **1**，创建新连接。

步骤 2 输入 **1**，选择创建的 VPN 类型为 SSL VPN。

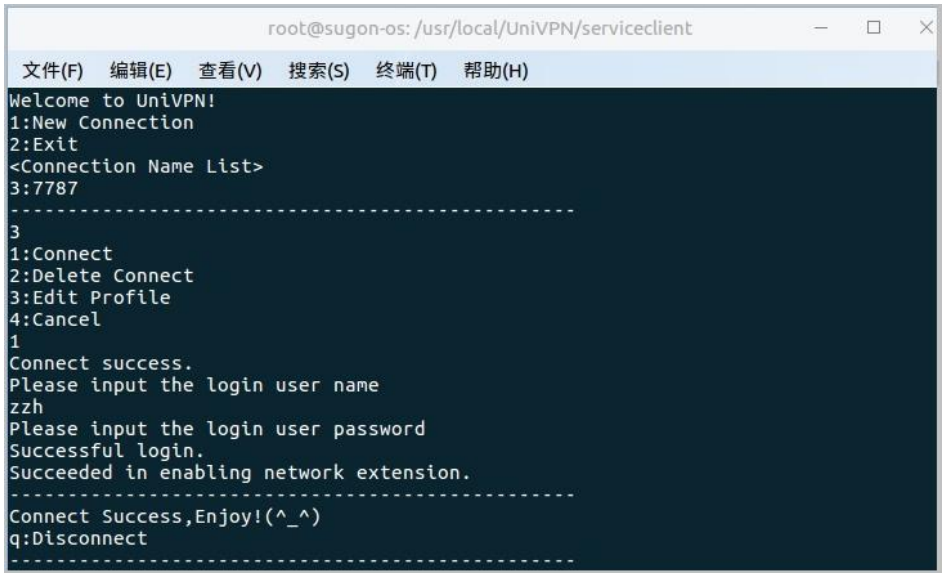
步骤 3 输入对应序号，完成参数 1~5 的配置。

- 1. Connection Name(Required)：连接名称；
- 2. Description：描述信息；
- 3. Gateway Address：远程网关地址；
- 4. Port(Required)：端口；
- 5. Tunnel Mode(Required)：隧道模式，可选模式有 Reliable Transmission（可靠传输模式）、Quick Transmission（快速传输模式）、Auto-sensing（自适应模式）。

步骤 4 输入 **7**，保存配置。

----结束

建立 SSL VPN 连接



步骤 1 输入对应序号，选择创建的 SSL VPN 连接。

步骤 2 输入 **1**，开始建立 SSL VPN 连接。

步骤 3 界面显示连接建立成功，输入用户名和密码进行登录。

----结束

说明

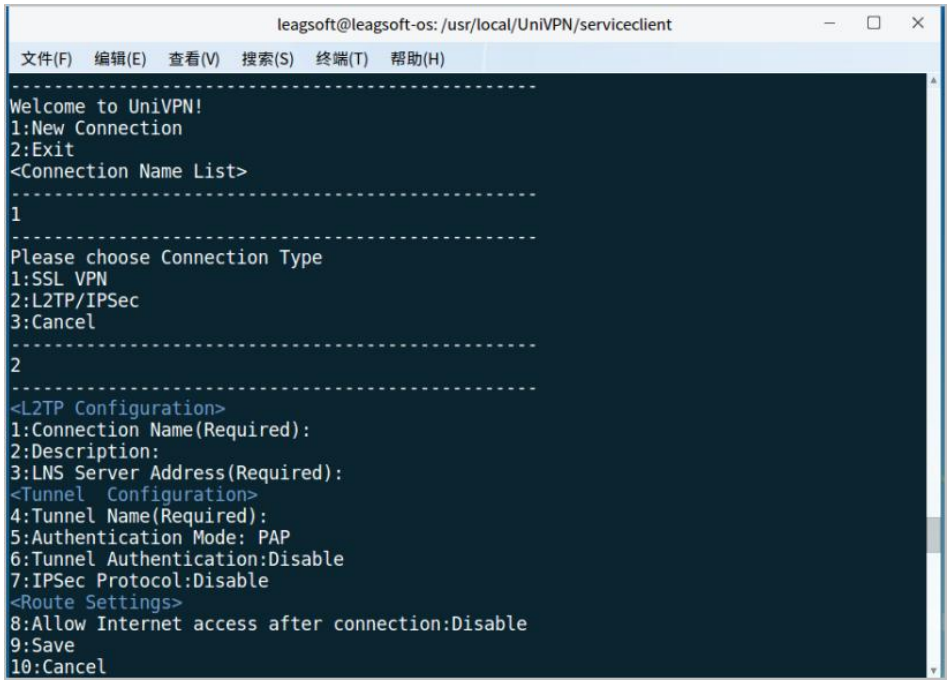
- 在国产化操作系统下通过命令行方式配置并建立的 SSL VPN 连接仅支持通过用户名/密码认证方式认证登录。
- 连接成功后，不能关闭该终端窗口，否则连接会断开。

断开 SSL VPN 连接

输入 **q**，即可断开连接。

9.3.3 配置 L2TP VPN 连接

配置 L2TP VPN



步骤 1 输入 **1**，创建新连接。

步骤 2 输入 **2**，选择创建的 VPN 类型为 L2TP/IPSec。

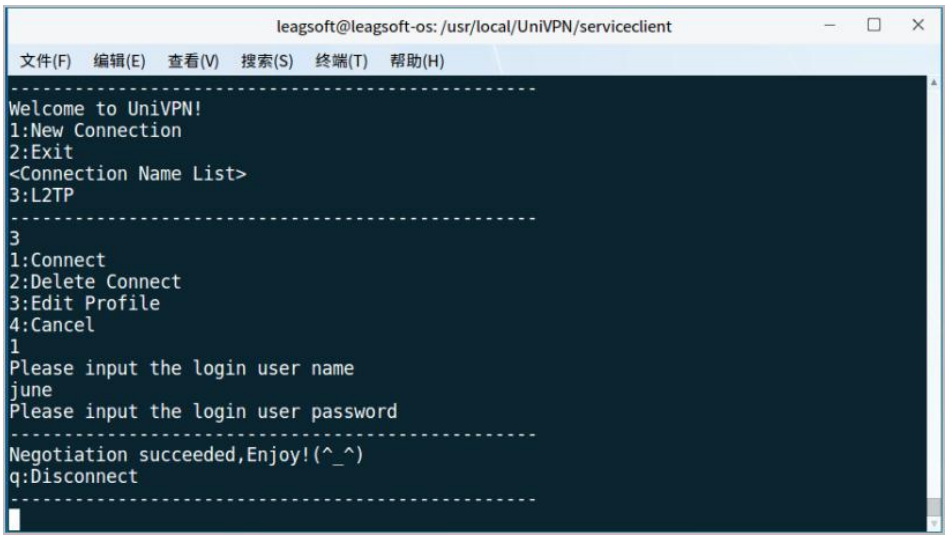
步骤 3 输入对应序号，完成参数 1~8 的配置。

- 1. Connection Name(Required)：连接名称；
- 2. Description：描述信息；
- 3. LNS Server Address(Required)：LNS 服务器地址；
- 4. Tunnel Name(Required)：隧道名称；
- 5. Authentication Mode：认证模式；
- 6. Tunnel Authentication：启用隧道验证功能，启用后，需要输入隧道验证密码（Tunnel Authentication Password）；
- 7. IPSec Protocol：启用 IPSec 安全协议，此功能请勿启用；
- 8. Allow Internet access after connection：路由设置，启用后，可以通过添加 IP 地址网段设置需要进入 VPN 隧道的待加密流量。

步骤 4 输入 **9**，保存配置。

----结束

建立 L2TP VPN 连接



步骤 1 输入对应序号，选择创建的 L2TP VPN 连接。

步骤 2 输入 **1**，开始建立 L2TP VPN 连接。

步骤 3 输入用户名和密码进行登录。

----结束

说明

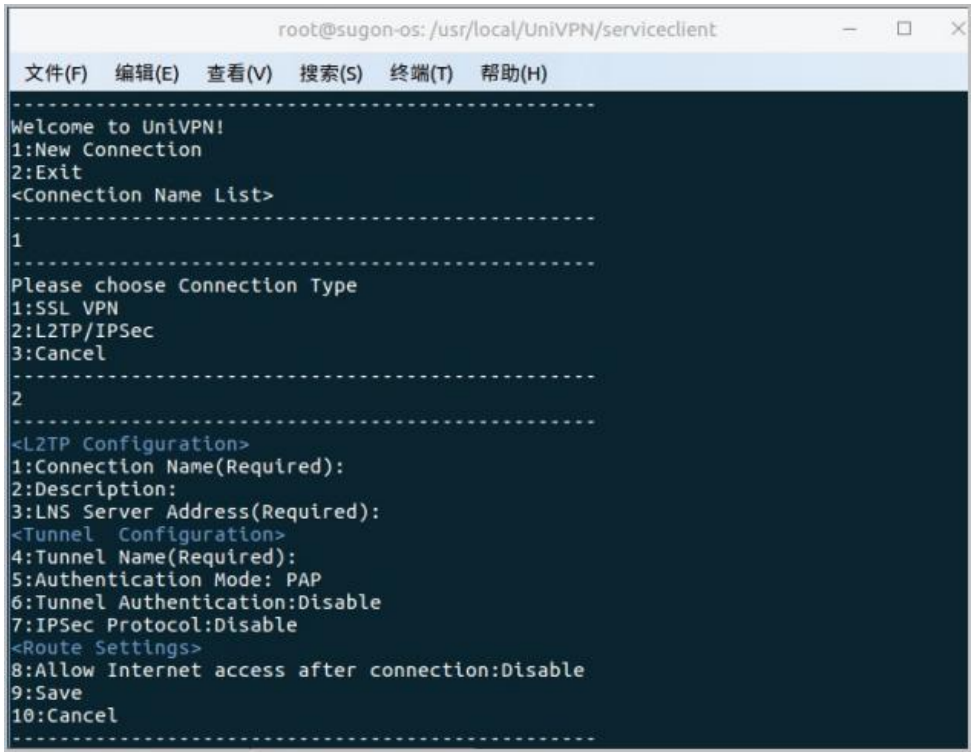
连接成功后，不能关闭该终端窗口，否则连接会断开。

断开 L2TP VPN 连接

输入 **q**，即可断开连接。

9.3.4 配置 L2TP over IPSec VPN 连接

配置 L2TP 参数



步骤 1 输入 **1**，创建新连接。

步骤 2 输入 **2**，选择创建的 VPN 类型为 L2TP/IPSec。

步骤 3 输入对应序号，完成参数 1~6 的配置。

- 1. Connection Name(Required)：连接名称；
- 2. Description：描述信息；
- 3. LNS Server Address(Required)：LNS 服务器地址；
- 4. Tunnel Name(Required)：隧道名称；
- 5. Authentication Mode：认证模式；
- 6. Tunnel Authentication：启用隧道验证功能，启用后，需要输入隧道验证密码（Tunnel Authentication Password）；

----结束

配置 IPSec 参数

步骤 1 输入 **7**，启用 IPSec 安全协议。

步骤 2 输入对应序号，完成参数 8~20 的配置。

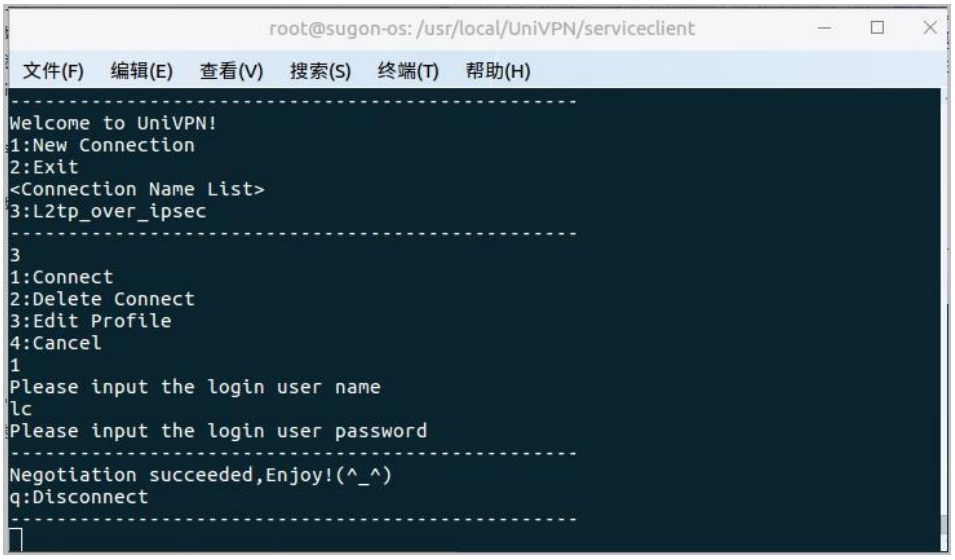
- 8. IPSec Authentication Mode：Linux 操作系统下 IPSec 的身份认证方式目前仅支持预共享密钥认证，预共享密钥方式下需要输入身份认证字（Pre-shared key）；
- 9. IPSec Server address：IPSec 服务器地址，缺省设置为使用 LNS 服务器地址（Use LNS server address）；
- 10. Encapsulation Mode：IPSec 封装模式，包括传输模式（Transmission mode）和隧道模式（Tunnel mode）两种；
- 11. ESP Authentication Algorithm：ESP 协议验证算法；
- 12. ESP Encryption Algorithm：ESP 协议加密算法；
- 13. Negotiation Mode：IKE 协商模式，包括主模式（Main Mode）和野蛮模式（Aggressive Mode）两种；

- 14. Authentication Algorithm：IKE 协商验证算法；
- 15. Encryption Algorithm：IKE 协商加密算法；
- 16. DH Group ID：IKE 协商 DH 组标识；
- 17. PFS：启用 PFS 特性，启用后，需要配置相应的安全参数（Security Parameter）；
- 18. SA Lifetime(IKE Advanced Configuration)：IKE 安全联盟生存周期；
- 19. SA Lifetime(IPSec Advanced Configuration)：IPSec 安全联盟生存周期；
- 20. Route Settings：路由设置，包括“Mode Config”模式和“Allow Internet access after connection”模式，设置为“Allow Internet access after connection”模式后，可以通过添加 IP 地址网段设置需要进入 VPN 隧道的待加密流量。

步骤 3 输入 21，保存配置。

----结束

建立 L2TP over IPSec VPN 连接



步骤 1 输入对应序号，选择创建的 L2TP over IPSec VPN 连接。

步骤 2 输入 **1**，开始建立 L2TP over IPSec VPN 连接。

步骤 3 输入用户名和密码进行登录。

----结束

说明

- **说明** 在 Linux 操作系统下通过命令行方式配置并建立的 L2TP over IPSec VPN 连接仅支持通过用户名/密码认证方式认证登录。
- 连接成功后，不能关闭该终端窗口，否则连接会断开。

断开 L2TP over IPSec VPN 连接

输入 **q**，即可断开连接。

9.4 缩略语

介绍本文档中出现过的缩略语。

缩略语		
A - E		
AES	Advanced Encryption Standard	高级加密标准
AH	Authentication Header	报文认证头
CBC	Cipher Block Chaining	密码分组链接
CHAP	Challenge Handshake Authentication Protocol	质询握手验证协议
DES	Data Encryption Standard	数据加密标准
DES-CBC	DES-Cipher Block Chaining	DES 密钥块链接
DH	Diffie-Hellman algorithm	Diffie-Hellman 算法
DNS	Domain Name System	域名系统
ESP	Encapsulating Security Payload	封装安全载荷
F - J		
ID	IDentification/IDentity	身份标识
IKE	Internet Key Exchange	Internet 密钥交换协议
IP	Internet Protocol	互联网协议
IPSec	IP Security Protocol	IP 网络安全协议
K - O		
L2TP	Layer 2 Tunneling Protocol	二层隧道协议
LAC	L2TP Access Concentrator	二层隧道协议接入集中器
LNS	L2TP Network Server	L2TP 网络服务器
MD5	Message-Digest Algorithm 5	信息-摘要算法 5
NAT	Network Address Translation	网络地址转换

缩略语		
P - T		
PAP	Password Authentication Protocol	密码验证协议
PC	Personal Computer	个人计算机
PFS	Perfect Forward Secrecy	完善的前向安全性
PPP	Point-to-Point Protocol	点到点协议
SA	Security Association	安全联盟
SHA	Secure Hash Algorithm	安全散列算法
U - Z		
VPN	Virtual Private Network	虚拟专用网