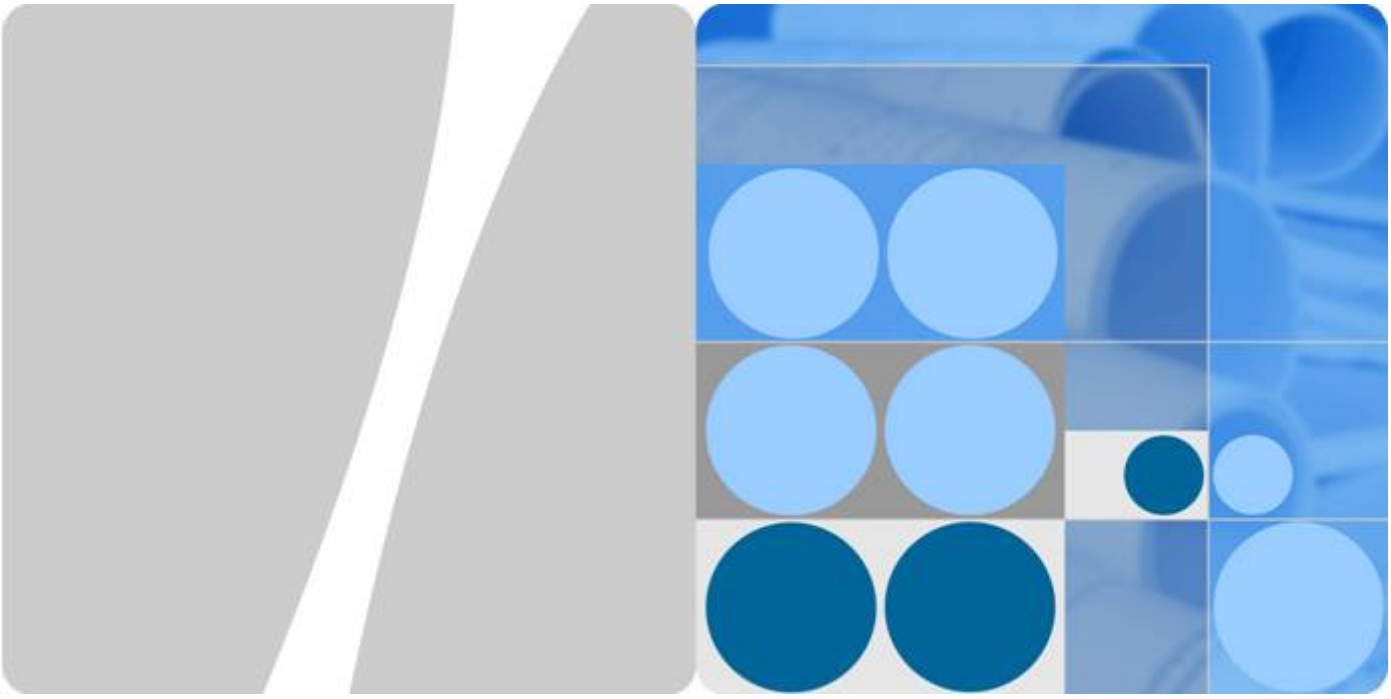


HUAWEI SecoClient 客户端

管理员指南

文档版本 18

发布日期 2020-07-06

华为技术有限公司

HUAWEI

商标声明


和其他华为商标均为华为技术有限公司的商标。
本文档提及的其他所有商标或注册商标，由各自的所有人拥有。

注意

您购买的产品、服务或特性等应受华为公司商业合同和条款的约束，本文档中描述的全部或部分产品、服务或特性可能不在您的购买或使用范围之内。除非合同另有约定，华为公司对本文档内容不做任何明示或默示的声明或保证。

由于产品版本升级或其他原因，本文档内容会不定期进行更新。除非另有约定，本文档仅作为使用指导，本文档中的所有陈述、信息和建议不构成任何明示或暗示的担保。

华为技术有限公司

地址： 深圳市龙岗区坂田华为总部办公楼 邮编：518129

网址： https://www.huawei.com

客户服务邮箱： support@huawei.com

客户服务电话： 4008302118

目 录

1 前言

配套产品及版本

产品名称	产品版本	操作系统
USG6000	V100R001C30SPCa00及以后版本 V500R001C30SPC100及以后版本	• Windows • Mac OS • Linux（V500R005C10SPC300及以后版本配套支持） • iOS（V500R001C60SPC500及以后版本配套支持） • Android（V500R005C00SPC100及以后版本配套支持）
USG6000E	V600R006C00及以后版本	• Windows • Mac OS • Linux（V600R006C00SPC300及以后版本配套支持） • iOS • Android
USG9500	V500R001C30SPC100及以后版本	• Windows • Mac OS • Linux（V500R005C10SPC300及以后版本配套支持） • iOS（V500R001C60SPC500及以后版本配套支持） • Android（V500R005C00SPC100及以后版本配套支持）

产品名称	产品版本	操作系统
Eudemon200E-N	V100R001C30SPCa00及以后版本 V500R002C00SPC100及以后版本	• Windows • Mac OS • Linux（V500R005C10SPC300及以后版本配套支持） • iOS（V500R002C20SPC500及以后版本配套支持） • Android（V500R005C00SPC100及以后版本配套支持）
Eudemon200E-G	V600R006C00及以后版本	• Windows • Mac OS • Linux（V600R006C00SPC300及以后版本配套支持） • iOS • Android
Eudemon1000E-N	V100R001C30SPCa00及以后版本 V500R002C00SPC100及以后版本	• Windows • Mac OS • Linux（V500R005C10SPC300及以后版本配套支持） • iOS（V500R002C20SPC500及以后版本配套支持） • Android（V500R005C00SPC100及以后版本配套支持）
Eudemon1000E-G	V600R006C00及以后版本	• Windows • Mac OS • Linux（V600R006C00SPC300及以后版本配套支持） • iOS • Android
Eudemon8000E-X	V500R002C00SPC100及以后版本	• Windows • Mac OS • Linux（V500R005C10SPC300及以后版本配套支持） • iOS（V500R002C20SPC500及以后版本配套支持） • Android（V500R005C00SPC100及以后版本配套支持）
SVN5600	V200R003C10SPCa00及以后版本	• Windows • Mac OS

产品名称	产品版本	操作系统
SVN5800	V200R003C10SPCa00及以后版本	• Windows • Mac OS
SVN5800-C	V200R003C10SPCa00及以后版本	• Windows • Mac OS
SeMG9811	V500R002C20SPC100及以后版本	• Windows • Mac OS • Linux（V500R005C10SPC300及以后版本配套支持） • iOS（V500R002C20SPC500及以后版本配套支持） • Android（V500R005C00SPC100及以后版本配套支持）
NGFW Module	V100R001C30SPCa00及以后版本 V500R002C00SPC100及以后版本	• Windows • Mac OS • Linux（V500R005C10SPC300及以后版本配套支持） • iOS（V500R002C20SPC500及以后版本配套支持） • Android（V500R005C00SPC100及以后版本配套支持）
USG6000V	V500R003C00SPC100及以后版本	• Windows • Mac OS • Linux（V500R005C10SPC300及以后版本配套支持） • iOS（V500R005C00SPC100及以后版本配套支持） • Android（V500R005C00SPC100及以后版本配套支持）
Eudemon1000E-V	V500R003C00SPC100及以后版本	• Windows • Mac OS • Linux（V500R005C10SPC300及以后版本配套支持） • iOS（V500R005C00SPC100及以后版本配套支持） • Android（V500R005C00SPC100及以后版本配套支持）

说明

- 上表中列出的不同操作系统下的SecoClient客户端与网关之间的版本配套关系已经通过全量测试验证，明确宣称支持。
- 在实际使用时，由于SecoClient客户端是一个独立的VPN接入软件，与网关之间没有强绑定关系，因此上述配套关系以外的网关版本也可能支持与SecoClient客户端进行对接，具体支持情况以实际测试验证结果为准。

读者对象

本文档适用于负责管理SecoClient和FW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SecoClient和FW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
	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。
	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 18 (2020-07-06) 产品版本 7.0.3**
  第十八次正式发布。

新增支持OS X 10.15.x版本的Mac操作系统，不再支持OS X 10.11.x 及以前版本的Mac操作系统。

对Linux版本的SecoClient，不再支持Ubuntu-14.4.04（32位/64位）和Ubuntu-16.4.04（32位），仅支持Ubuntu-16.4.04（64位）。

- **文档版本 17 (2019-05-21) 产品版本 7.0.2**

  第十七次正式发布。

  SecoClient在SSL VPN场景下新增支持国密算法。

  Windows版本的SecoClient在SSL VPN场景下新增支持路由覆盖。

  Linux版本的SecoClient支持终端安全。

- **文档版本 16 (2018-12-28) 产品版本 6.0.3**

  第十六次正式发布。

  SecoClient新增支持Linux操作系统。

- **文档版本 15 (2018-12-10) 产品版本 6.0.2**

  第十五次正式发布。

  SecoClient开始支持与USG6000E、Eudemon200E-G、Eudemon1000E-G建立VPN隧道。

- **文档版本 14 (2018-06-30) 产品版本 5.0.2**

  第十四次正式发布。

  增加**8.1 移动客户端**章节。

  推出基于Android操作系统的移动版客户端。

- **文档版本 13 (2018-03-30) 产品版本 5.0.1**

  第十三次正式发布。

- **文档版本 12 (2018-03-12) 产品版本 3.0.3**

  第十二次正式发布。

- **文档版本 11 (2017-12-31) 产品版本 3.0.2**

  第十一次正式发布。

  新增支持OS X 10.13.x版本的Mac操作系统。

- **文档版本 10 (2017-12-10) 产品版本 3.0.1**

  第十次正式发布。

  推出基于iOS操作系统的移动版客户端。

  SecoClient开始支持与USG6000V、Eudemon1000E-V建立VPN隧道。

- **文档版本 09 (2017-12-07) 产品版本 1.60.5**

  第九次正式发布。

- **文档版本 08 (2017-11-10) 产品版本 1.60.3**

  第八次正式发布。

- **文档版本 07 (2017-08-11) 产品版本 1.60.2**

  第七次正式发布。

- **文档版本 06 (2017-06-15) 产品版本 1.60.1**

  第六次正式发布。

  新增支持10种界面语言。

  新增支持OS X 10.12.x版本的Mac操作系统。

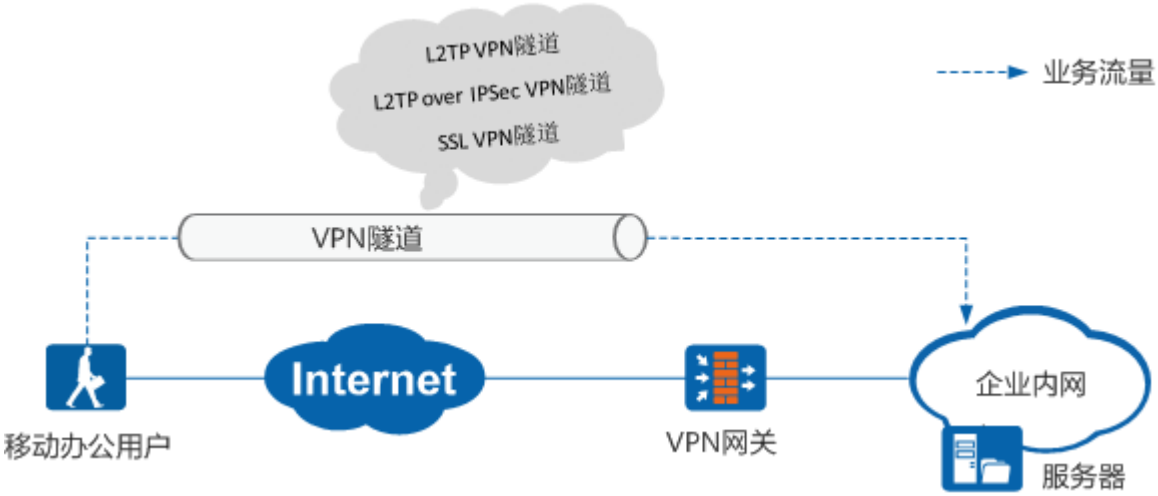
新增支持在MAC操作系统下通过安装/卸载程序手动安装或卸载客户端。
SecoClient开始支持与SeMG9811建立VPN隧道。

- **文档版本 05 (2017-04-20) 产品版本 1.50.3**
  第五次正式发布。
- **文档版本 04 (2017-03-09) 产品版本 1.50.2**
  第四次正式发布。
  细化MAC操作系统的规格。
- **文档版本 03 (2017-01-17) 产品版本 1.50.1**
  第三次正式发布。
  SecoClient开始支持IPSec隧道分离功能。
- **文档版本 02 (2016-09-14) 产品版本 1.30.2**
  第二次正式发布。
- **文档版本 01 (2016-08-12) 产品版本 1.30.1**
  第一次正式发布。

2 简介

SecoClient是华为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1所示。

图 2-1 移动办公用户使用 SecoClient 通过 VPN 隧道访问企业内网



SecoClient具备以下几个特点：

- 强大的接入能力

  SecoClient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SecoClient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。SecoClient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。SecoClient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

SecoClient提供的功能列表如**表1**所示。

表 2-1 SecoClient 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。
	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，SecoClient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。

功能名称		说明
	断线重连	当SSL VPN隧道异常中断时，SecoClient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SecoClient与一台对外提供了多个IP地址的SSL VPN网关建立VPN隧道时，SecoClient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，SecoClient将会进行断线重连，3次重连失败，SecoClient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。
	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。

功能名称		说明
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。 SecoClient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。
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。SecoClient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。 SecoClient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SecoClient随系统启动。
	界面语言切换	目前支持12种界面语言，包括： ● 英语 ● 法语 ● 德语 ● 俄语 ● 日语 ● 韩语 ● 简体中文 ● 繁体中文 ● 阿拉伯语 ● 意大利语 ● 葡萄牙语 ● 西班牙语
	自动登录	首次登录VPN网关后，SecoClient会记住用户名和密码。后续再次登录时，无需输入用户名、密码。
配置文件	导入	SecoClient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SecoClient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。

功能名称	说明
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。
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SecoClient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。

3 安装

介绍SecoClient的安装方法。

网络管理员安装SecoClient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。

3.1 在 Windows 操作系统下手动安装 SecoClient

介绍Windows操作系统下SecoClient的安装和卸载方法。

安装前须知

- SecoClient针对32位Windows操作系统和64位Windows操作系统分别提供了安装包，请您根据当前的操作系统环境选择正确的安装包。
- SecoClient支持的Windows操作系统版本包括：
  - Windows Vista（32位/64位）
  - 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（32位/64位）
  - Windows Server 2012（32位/64位）

- SecoClient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

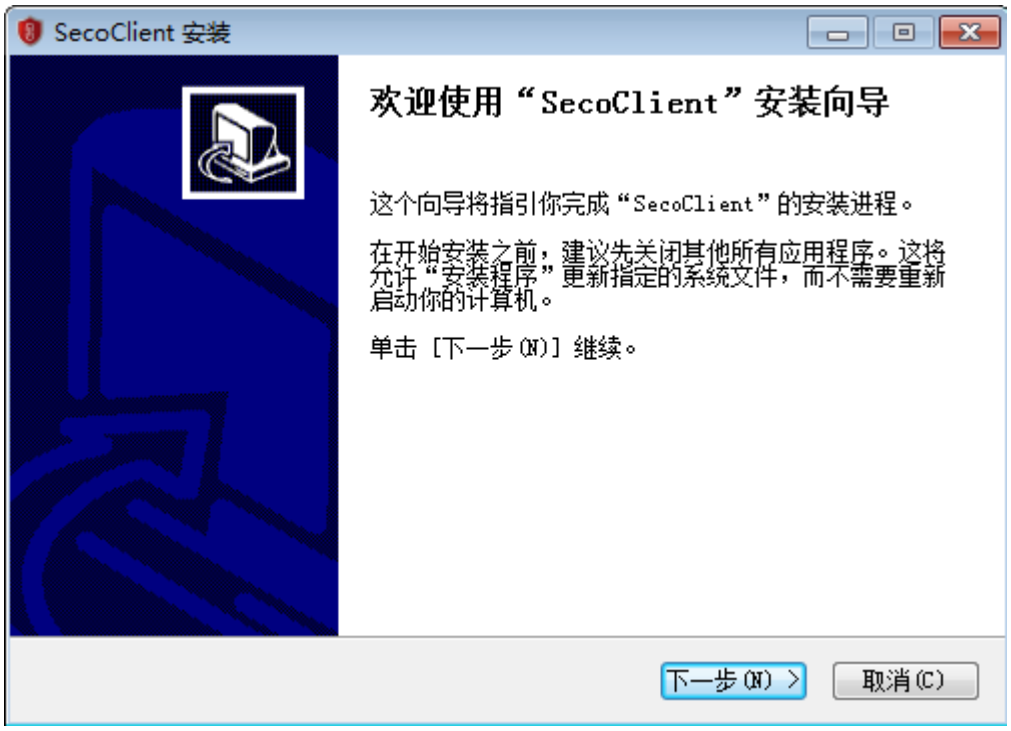
32位操作系统和64位操作系统下SecoClient的安装方法相同，下面以32位操作系统为例进行介绍。

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。

- 对于企业网用户：使用注册帐号登录网站**http://support.huawei.com/enterprise**，进入“企业网络 > 安全 > 防火墙&VPN网关 >（选择款型）”，选择下载对应版本的软件安装包。
- 对于运营商用户：使用注册帐号登录网站**http://support.huawei.com/carrier**，进入“产品软件 > 网络 > 交换机与企业网关 > 交换机与企业网关 >（选择款型）”，选择下载对应版本的软件安装包。

步骤3 双击下载的安装包，进入安装向导界面，单击“下一步”。

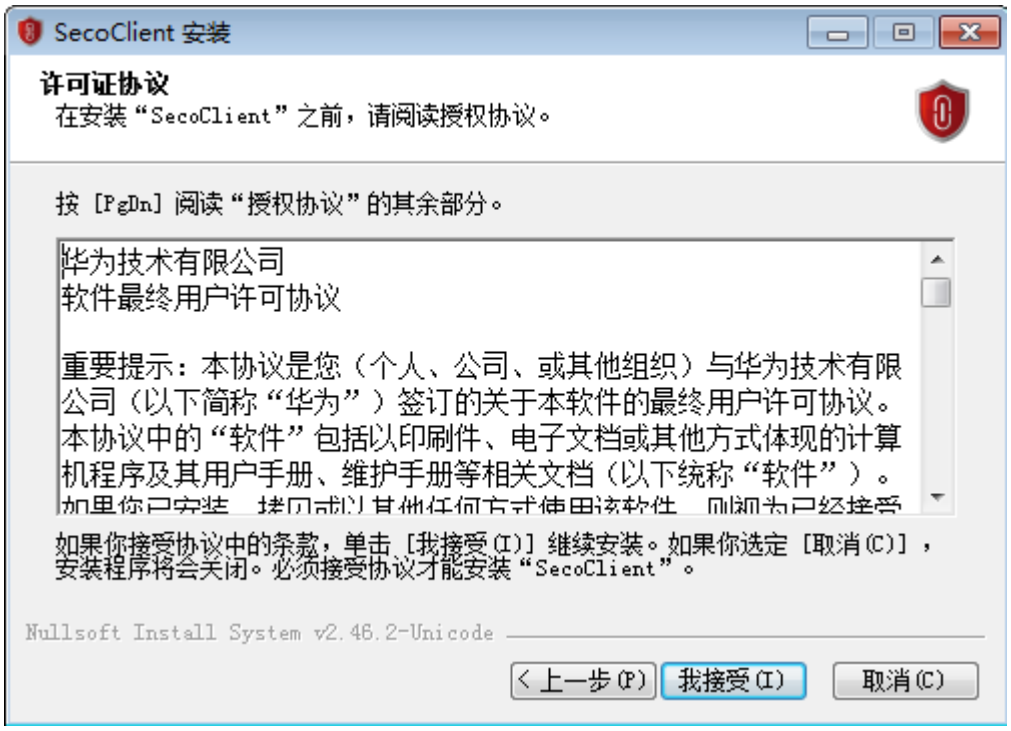


说明

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。

步骤4 进入“许可证协议”界面，仔细阅读软件许可证协议后，单击“我接受”。

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



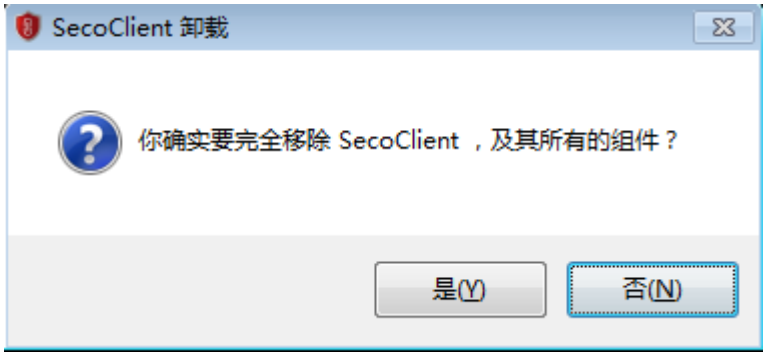
步骤5 单击“完成”。

----结束

卸载方法

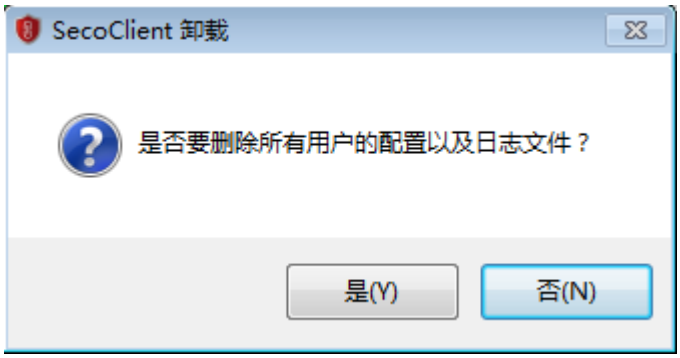
步骤1 选择“开始 > 所有程序 > SecoClient”。

步骤2 单击“Uninstall”，系统弹出卸载提示，单击“是”。

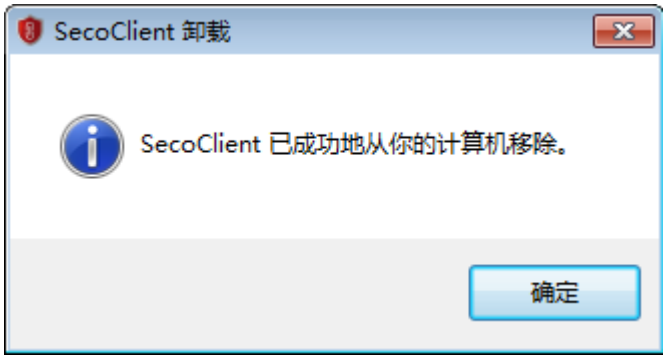


步骤3 在卸载过程中，系统会提示是否删除用户配置及日志文件，请根据需要进行选择。

此处选择“是”，删除用户配置及日志文件。



步骤4 单击“确定”，完成卸载。



----结束

3.2 在 MAC 操作系统下手动安装 SecoClient

介绍MAC操作系统下SecoClient的安装和卸载方法。

安装前须知

- SecoClient只支持64位MAC操作系统。
- SecoClient 7.0.2及以前版本支持的MAC操作系统版本包括：
  - OS X 10.7.x
  - OS X 10.8.x
  - OS X 10.9.x
  - OS X 10.10.x
  - OS X 10.11.x
  - OS X 10.12.x
  - OS X 10.13.x
  - OS X 10.14.x
- SecoClient 7.0.3及以后版本支持的MAC操作系统版本包括：
  - OS X 10.12.x
  - OS X 10.13.x
  - OS X 10.14.x
  - OS X 10.15.x

- SecoClient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

步骤1 登录MAC操作系统。

步骤2 下载对应版本的软件安装包。

- 对于企业网用户：使用注册帐号登录网站**http://support.huawei.com/enterprise**，进入“企业网络 > 安全 > 防火墙&VPN网关 >（选择款型）”，选择下载对应版本的软件安装包。
- 对于运营商用户：使用注册帐号登录网站**http://support.huawei.com/carrier**，进入“产品软件 > 网络 > 交换机与企业网关 > 交换机与企业网关 >（选择款型）”，选择下载对应版本的软件安装包。

步骤3 双击下载好的安装包，系统会自动将安装包解压成文件夹，与安装包放置在同一级目录下。

步骤4 双击打开该文件夹，文件夹中包含“Info.plist”和“SecoClientInstaller.pkg”两个文件。双击“SecoClientInstaller.pkg”文件，运行安装程序。

步骤5 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，软件介绍和许可协议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和许可协议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. 仔细阅读软件许可协议后，单击“继续”。支持在安装程序中手动切换许可协议的语言（简体中文或英文），并可通过安装程序中提供的“打印”和“存储”按钮打印或存储该份协议。
3. 如果同意软件许可协议，单击“同意”进入后续安装步骤。
4. 单击“安装”。软件安装在固定路径下，无法手动更改安装位置。
5. 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。
6. 单击“关闭”。

步骤6 安装完成后，可在应用程序文件夹中找到应用程序和对应的卸载程序。

步骤7 双击“SecoClient.app”，运行应用程序并进行连接参数的配置。

说明

首次运行应用程序时，需要使用系统的“root”权限对客户端进行提权操作，成功后方可运行程序。

----结束

卸载方法

说明

请参考如下步骤，通过卸载程序完成软件的卸载任务。不建议通过将“SecoClient.app”等文件直接拖入回收站（Trash）的方式进行卸载，若系统中存在残留文件未被完全清除，则可能导致下次安装时出现异常。

步骤1 在应用程序文件夹中找到卸载程序“SecoClientUninstaller.app”，双击启动。

步骤2 单击“卸载”，并进行用户权限的鉴定。

说明

此处可能需要对用户的系统权限进行鉴定，鉴定成功后方可完成卸载。仅具有“root”权限的用户可卸载此软件。

步骤3 用户权限鉴定成功后，即可完成卸载。

----结束

3.3 在 Linux 操作系统下手动安装 SecoClient

介绍Linux操作系统下SecoClient的安装和卸载方法。

安装前须知

- SecoClient针对32位Linux操作系统和64位Linux操作系统分别提供了安装包，请您根据当前的操作系统环境选择正确的安装包。
- SecoClient 7.0.2及以前版本支持的Linux操作系统版本包括：Ubuntu-16.4.04（32位/64位）和Ubuntu-14.4.04（32位/64位），同时支持Ubuntu桌面系统和Server系统。
- SecoClient 7.0.3及以后版本的SecoClient，支持的Linux操作系统版本包括：Ubuntu-16.4.04（64位），同时支持Ubuntu桌面系统和Server系统。

- SecoClient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SecoClient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“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。

- 对于企业网用户：使用注册帐号登录网站**http://support.huawei.com/enterprise**，进入“企业网络 > 安全 > 防火墙&VPN网关 >（选择款型）”，选择下载对应版本的软件安装包。
- 对于运营商用户：使用注册帐号登录网站**http://support.huawei.com/carrier**，进入“产品软件 > 网络 > 交换机与企业网关 > 交换机与企业网关 >（选择款型）”，选择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 > sec”）中。

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

```
root@sec-virtual-machine:~# cd ..
root@sec-virtual-machine:/# cd home/sec
root@sec-virtual-machine:/home/sec# ./secoclient-linux-64.xx.x.xx.run
install.sh
uninstall.sh
sysconfig.ini
qt.conf
bak/
component/
config/
driver/
```

步骤5 安装成功，如下所示。

```
Starting SecoclientPromoteService daemon: SecoClientPromoteService.
*****The program has been install in directory SecoClient of your home Directory!*****
*****Enjoy!*****
```

步骤6 单击桌面上生成的SecoClient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/SecoClient”目录下。

```
root@sec-virtual-machine:~# cd ..
root@sec-virtual-machine:/# cd usr/local/SecoClient/
root@sec-virtual-machine:/usr/local/SecoClient#
```

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

```
root@sec-virtual-machine:/usr/local/SecoClient# ./uninstall.sh
Stopping SecoClientPromoteService daemon: SecoClientPromoteService.
 Removing any system startup links for /etc/init.d/SecoClientPromoteService.sh ...
```

----结束

3.4 通过 AD 服务器分发并自动安装 SecoClient

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

AD服务器将SecoClient软件安装包分发到各个终端用户主机，当用户登录主机时，SecoClient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MAC操作系统和Linux操作系统，则不支持这种安装方式。

3.4.1 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**（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。

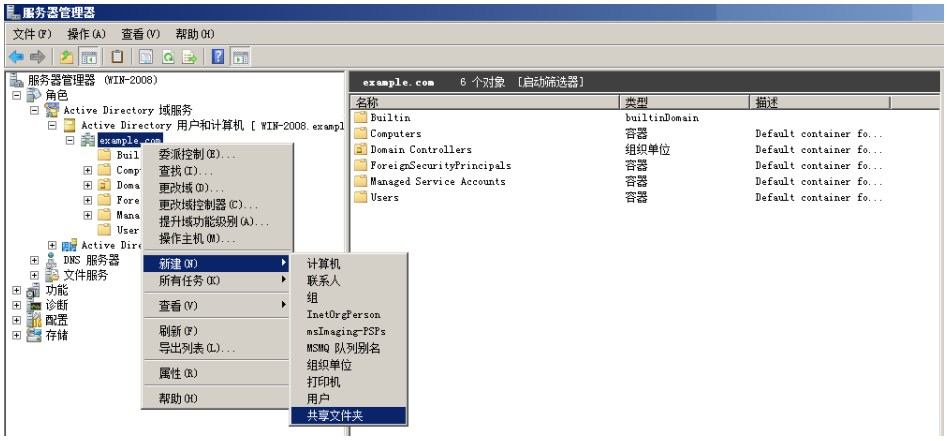
  通过AD服务器分发并自动安装的SecoClient软件安装包必须为msi格式，msi格式的软件安装包可以通过以下途径获取：

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

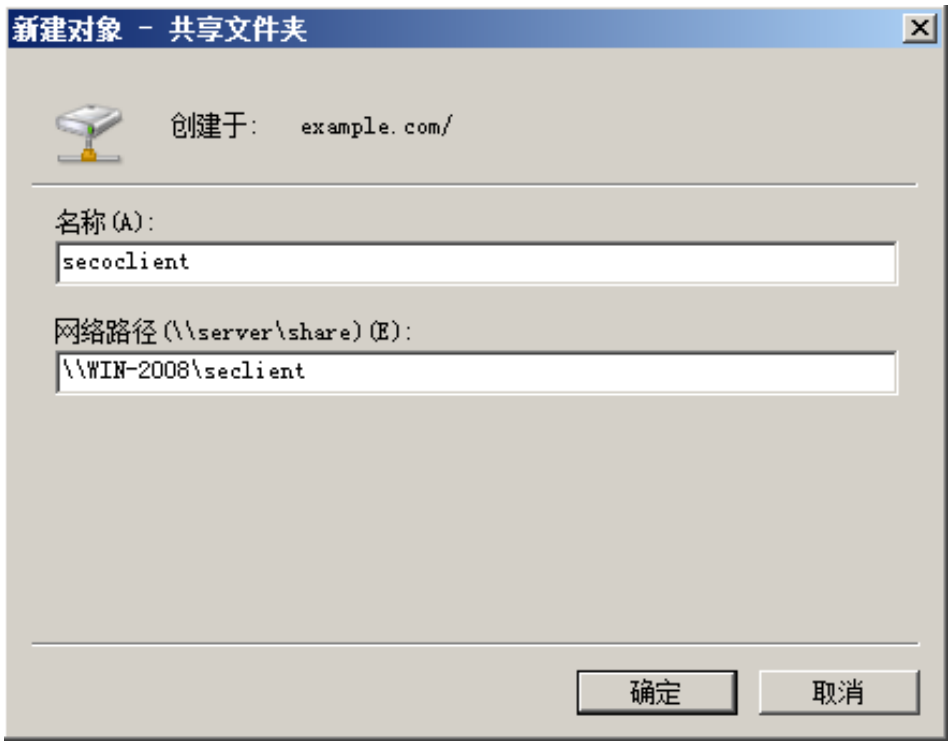
操作步骤

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”。

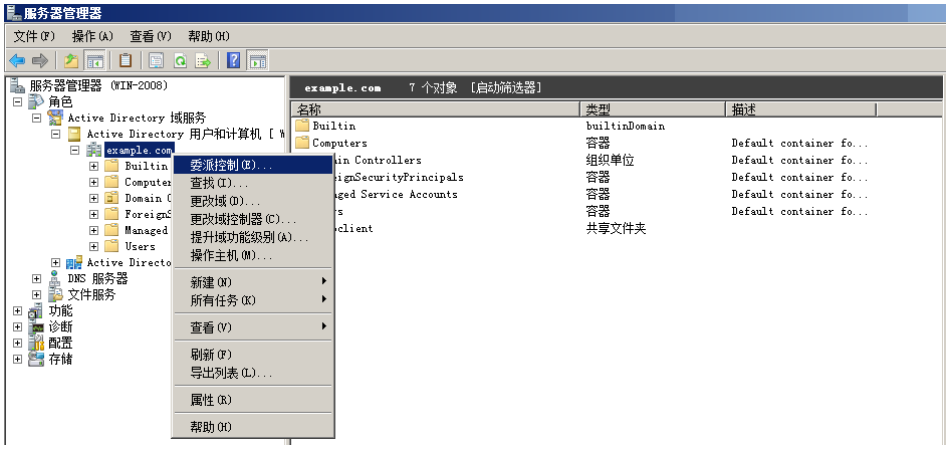


2. 输入之前创建的共享文件夹的名称，以及共享文件夹的网络路径。



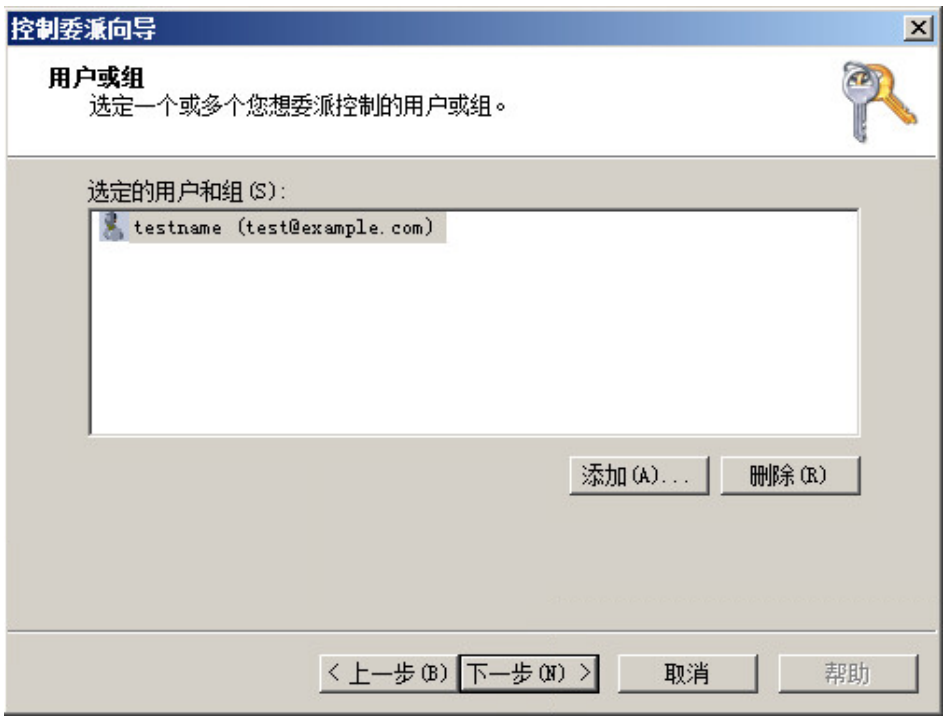
步骤2 设置用户的委派控制。

1. 在example.com域上单击右键，选择“委派控制”。

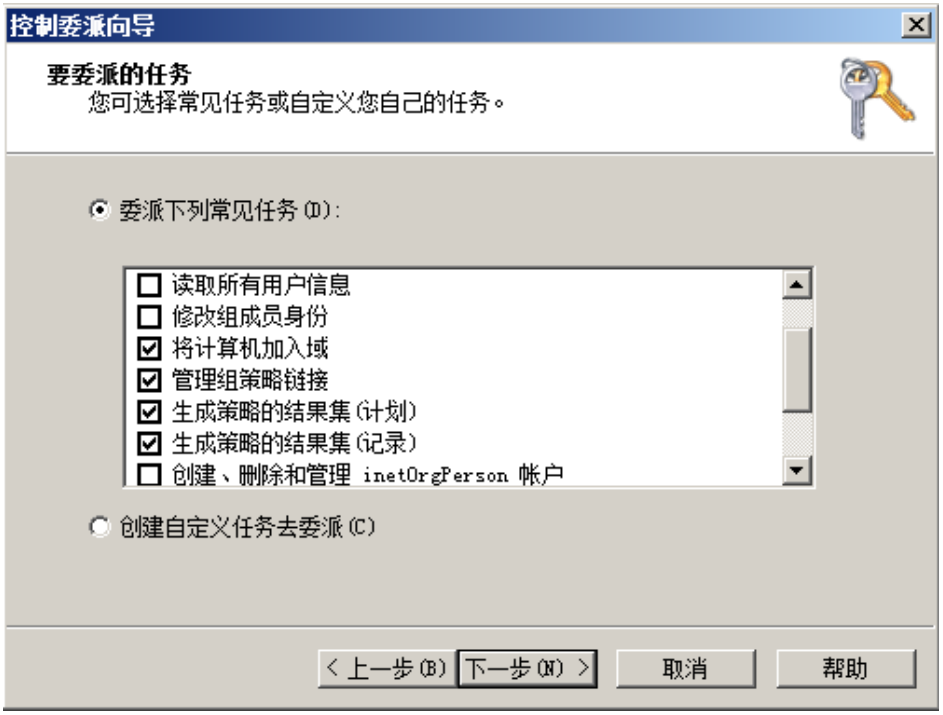


2. 单击下一步。

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”。



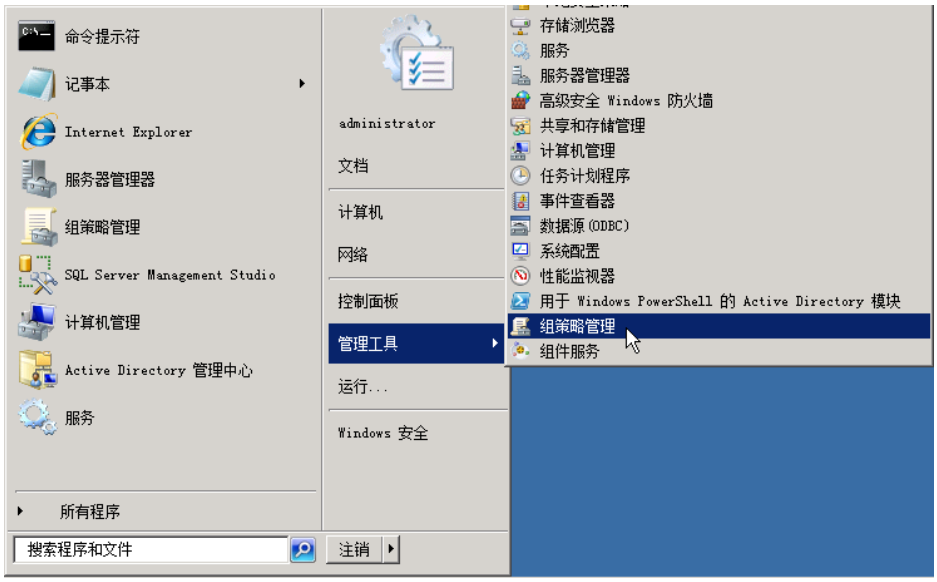
4. 勾选为用户委派的任务，单击“下一步”。



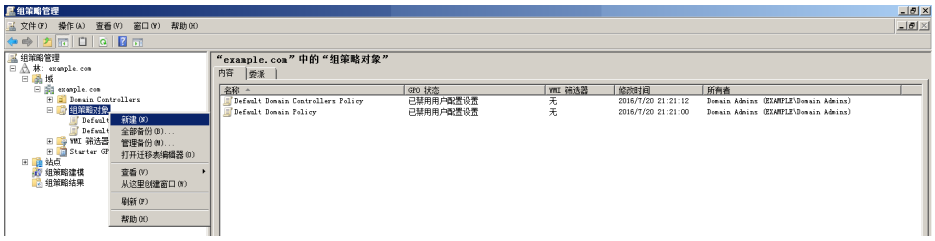
5. 单击“完成”，结束委派控制配置。

步骤3 设置软件安装策略。

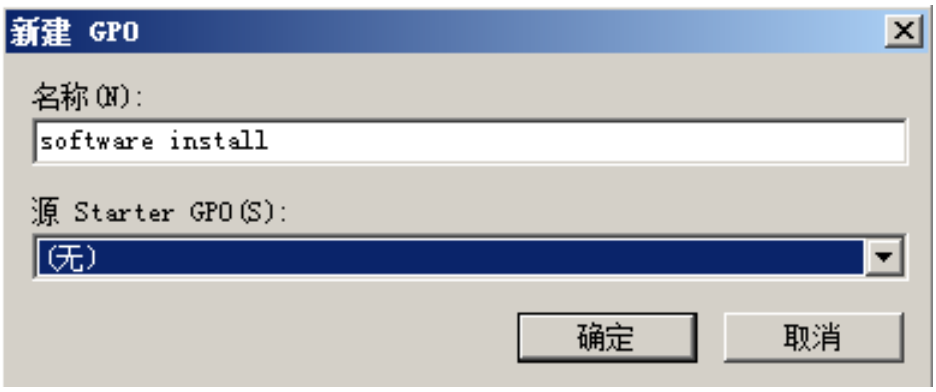
1. 在开始菜单中选择“管理工具 > 组策略管理”。



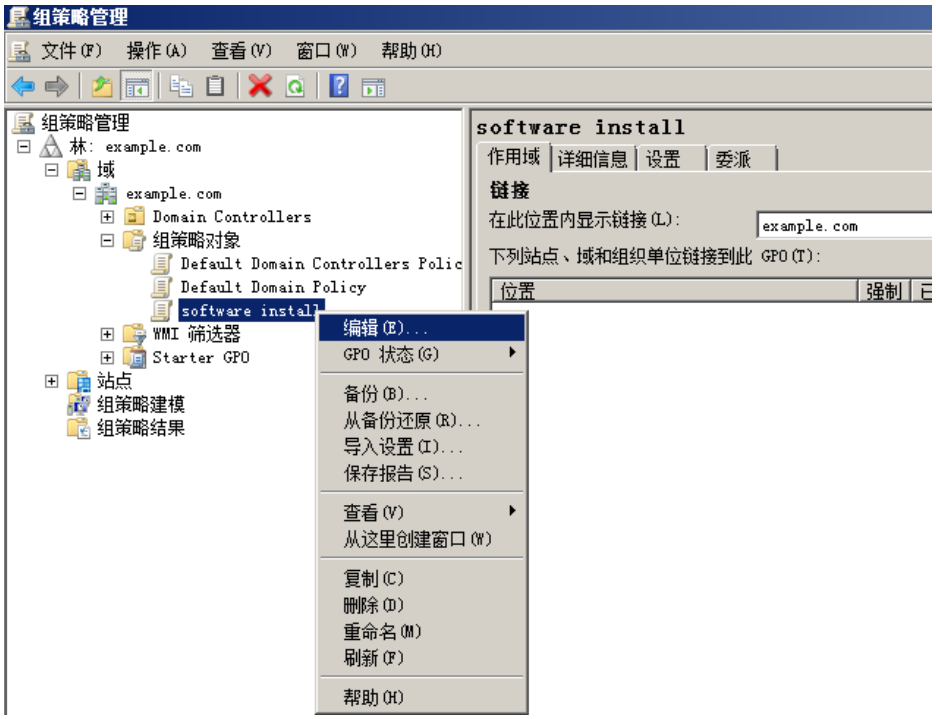
2. 在组策略对象上单击右键，选择“新建”。



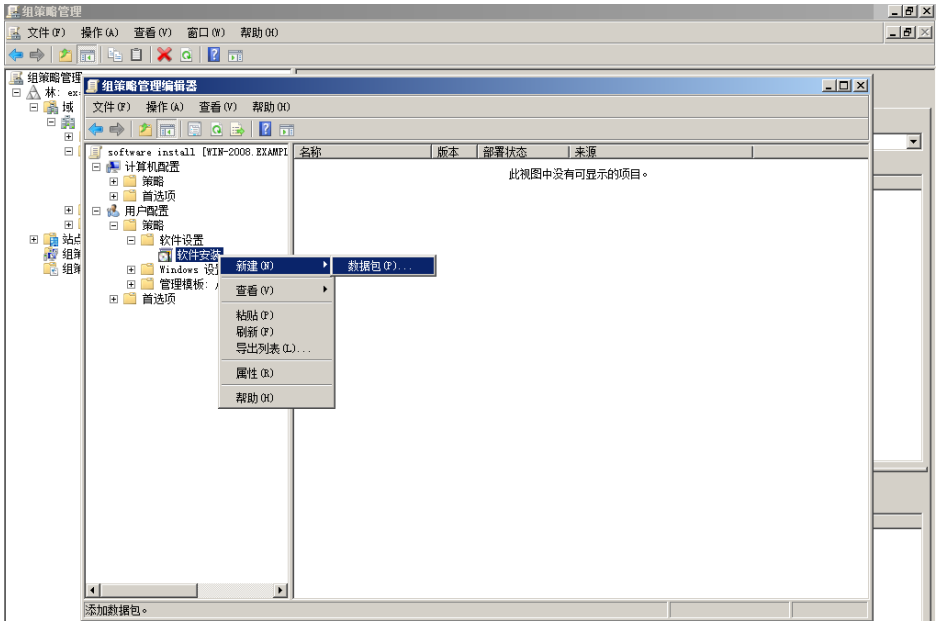
3. 创建一个名称为“software install”的策略对象，单击“确定”。



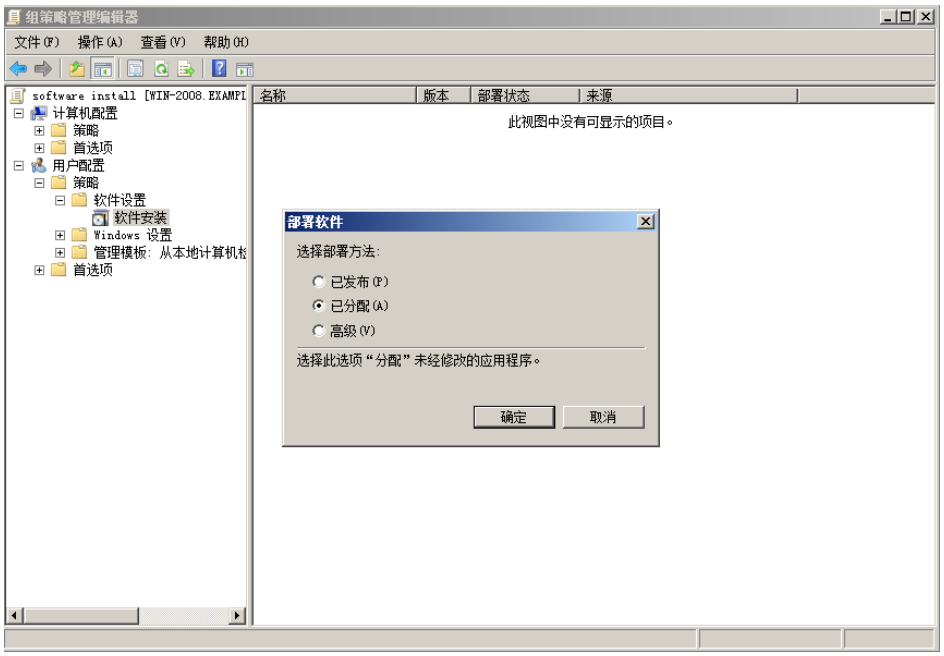
4. 在新建的策略对象“software install”上单击右键，选择“编辑”。



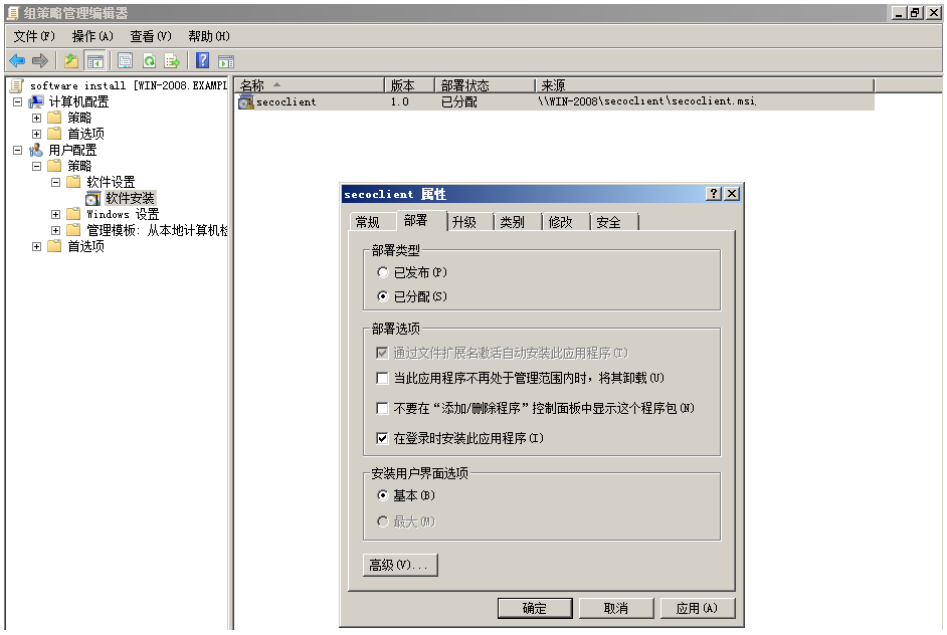
5. 在“软件安装”上单击右键，依次选择“新建 > 数据包”。



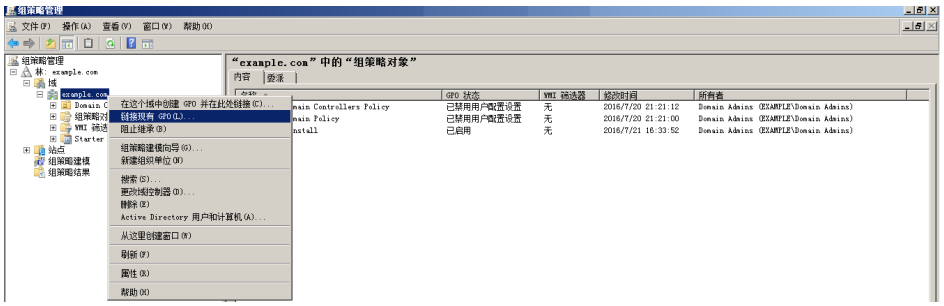
6. 系统会提示用户选择制作好的secoclient.msi文件，选中文件后，系统接着会弹出如下提示，选择“已分配”，单击“确定”。



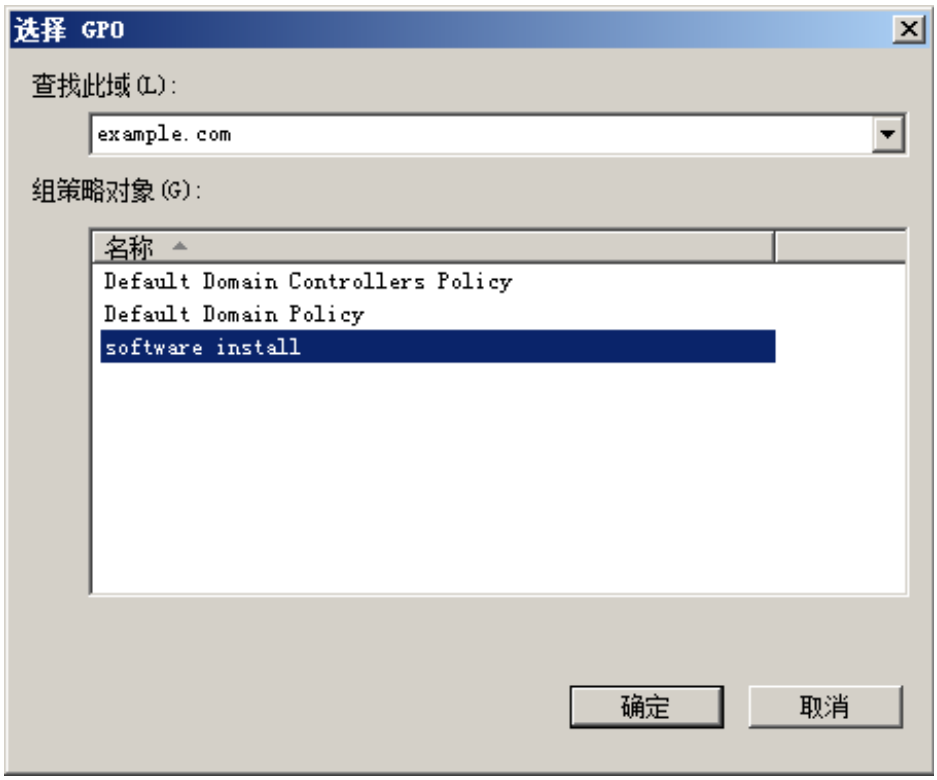
7. 双击右侧窗口新生成的secoclient记录，选择“部署”页签，并按照下图进行设置，然后单击“确定”。



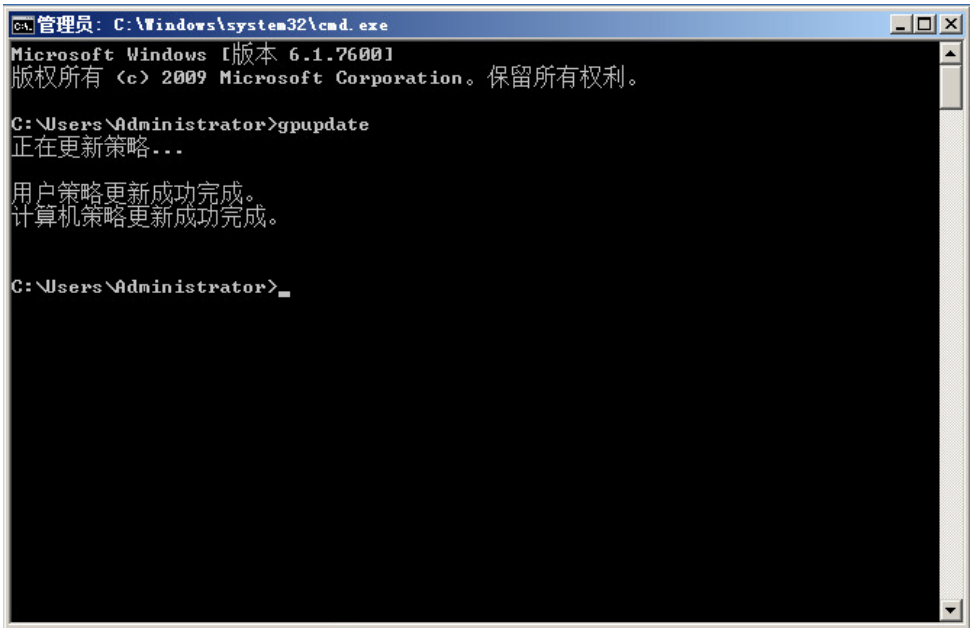
8. 在example.com上单击右键，选择“链接现有GPO”。



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SecoClient安装完成，桌面已经生成快捷方式。

SecoClient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。

3.4.2 （可选）创建 AD 域和域用户

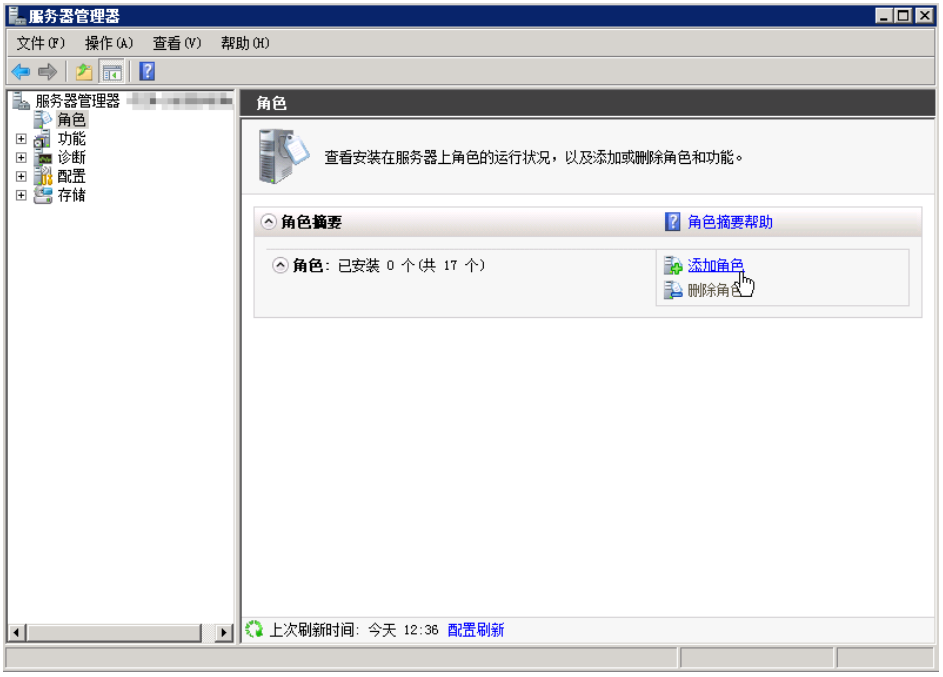
本节介绍如何在AD服务器上创建AD域和域用户。

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”。

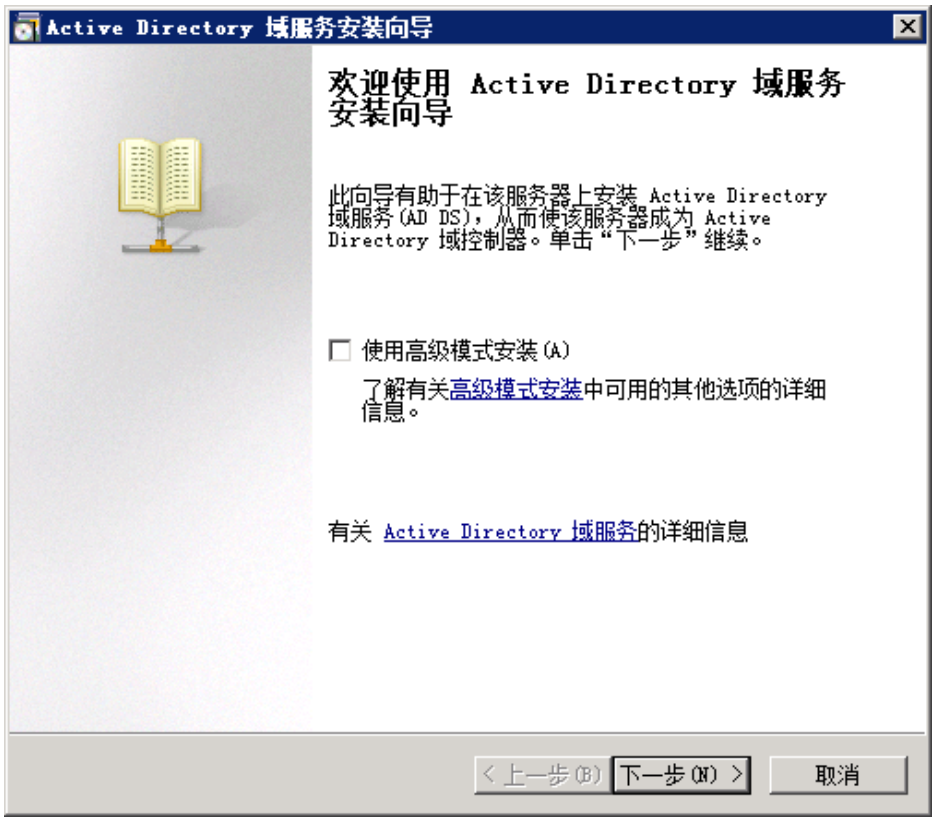
2. 在“服务器管理器”界面，选择“添加角色”。



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

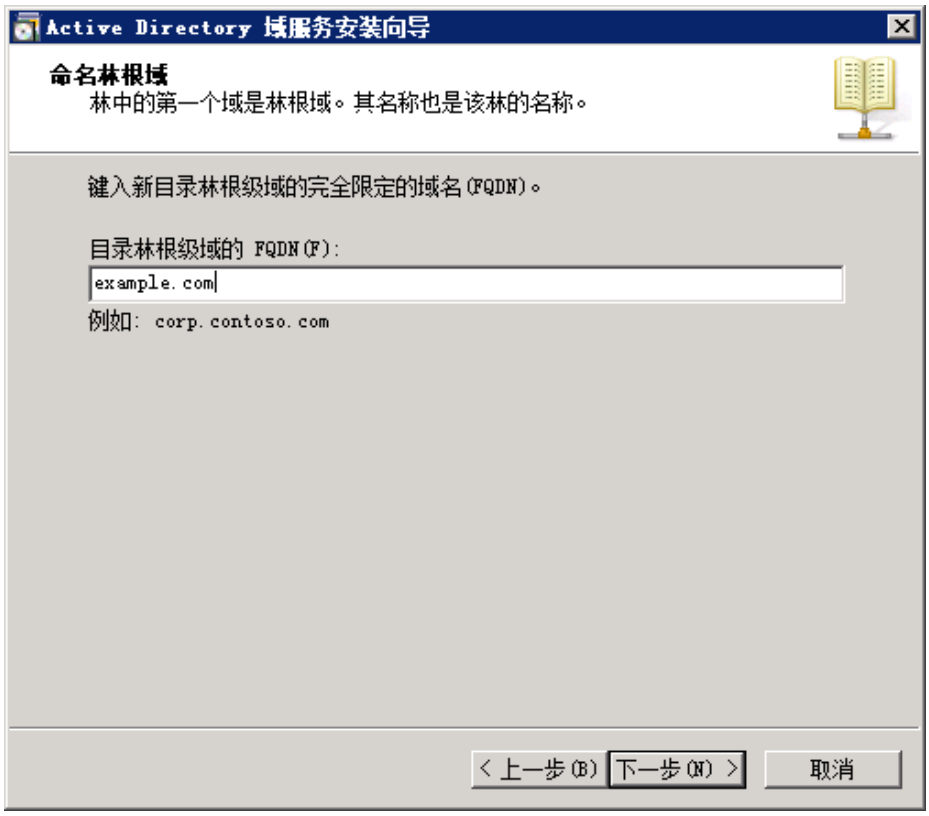
步骤2 创建Active Directory域服务。

1. 在“开始 > 运行”中输入**dcpromo**，进入安装向导。

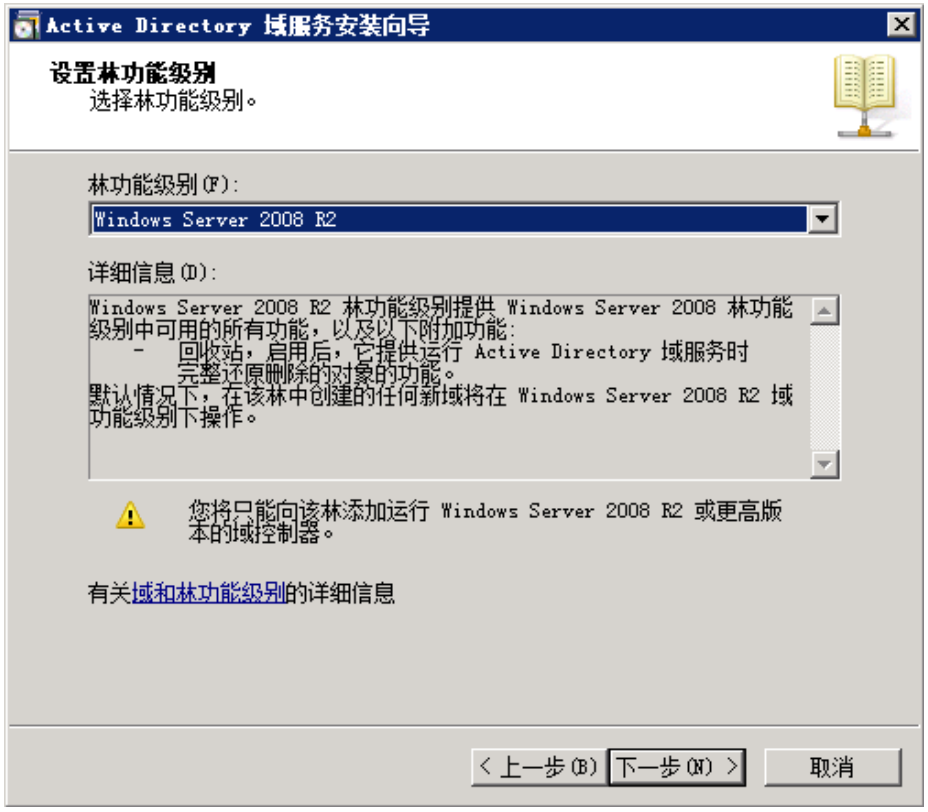


2. 选择“在新林中新建域”。

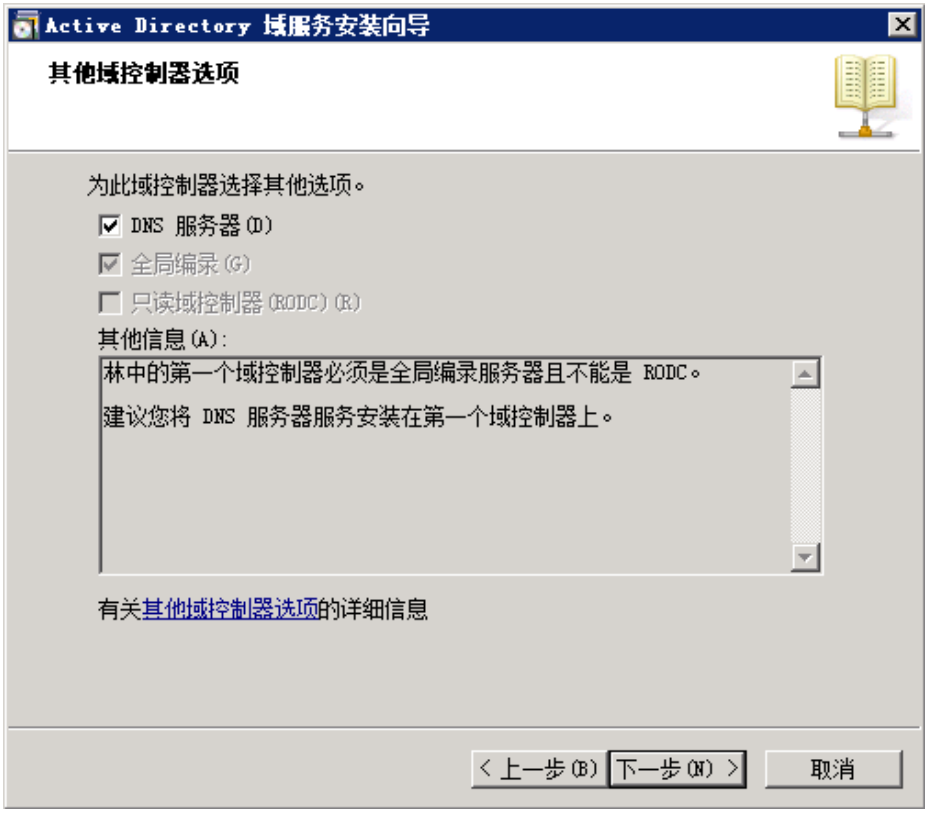
3. 输入林根域名称。



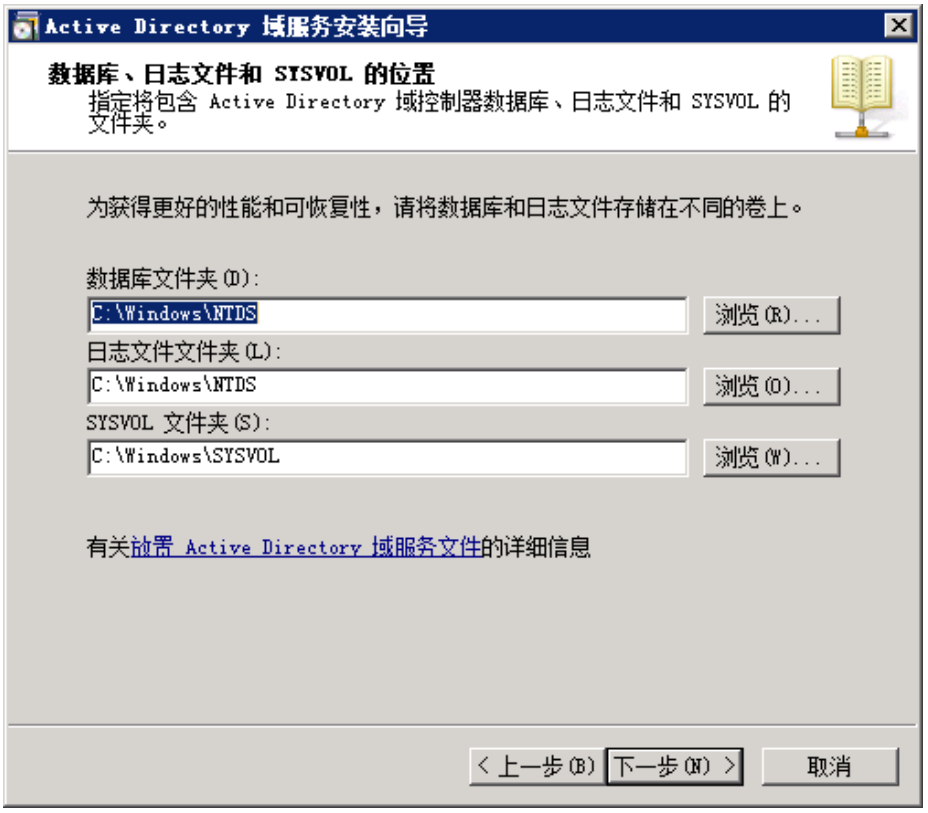
4. 选择林功能级别。



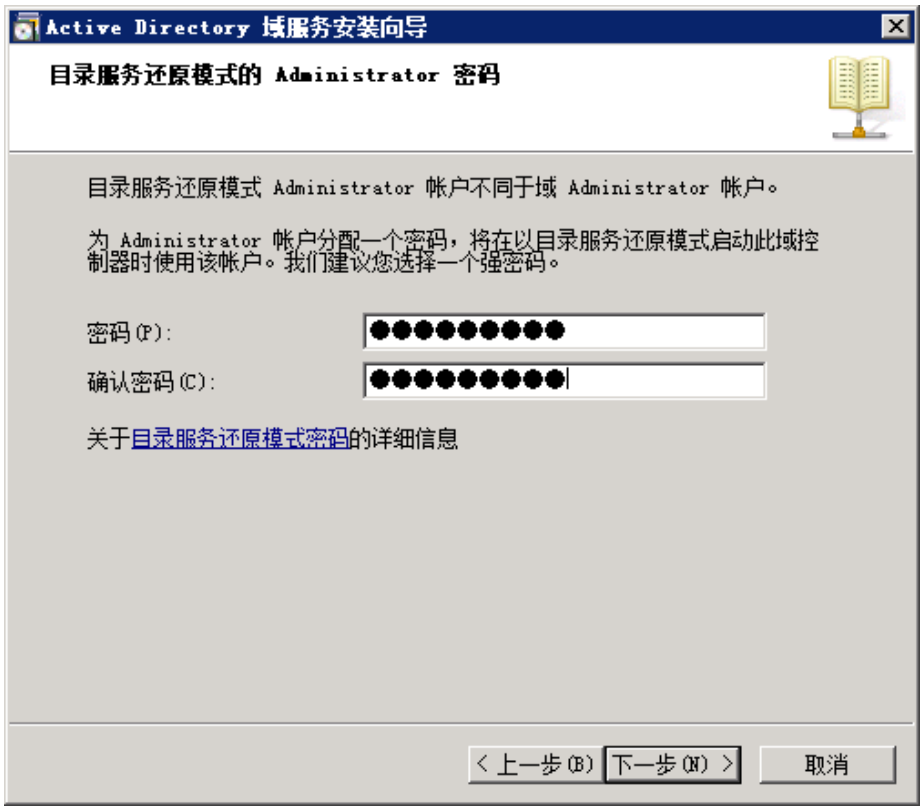
5. 在未安装DNS服务的服务器上，需要安装DNS服务器后才能使用AD域功能。



6. 指定数据库、日志文件、SYSVOL存放路径。

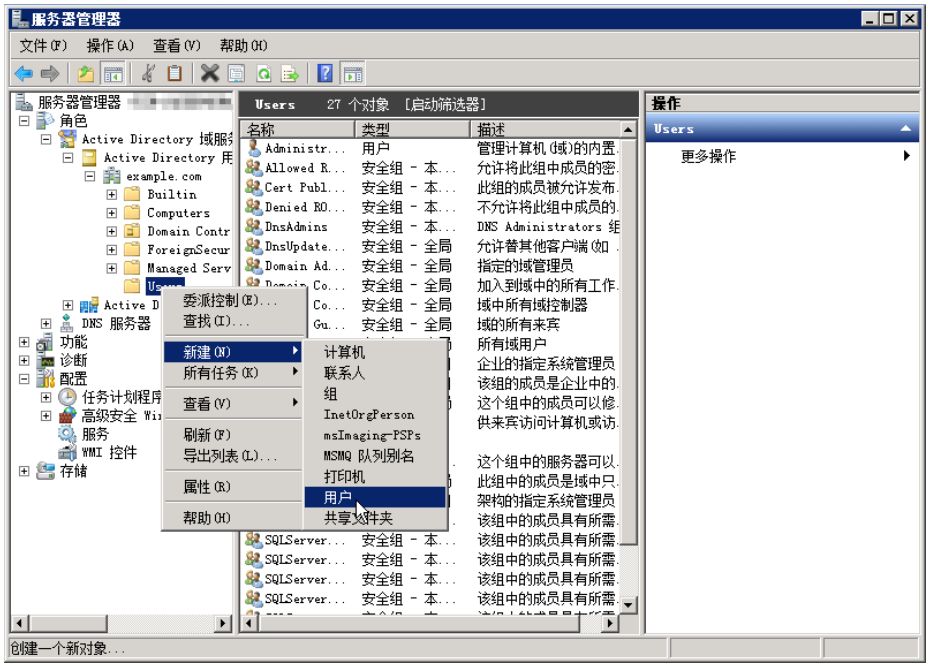


7. 输入管理员密码。单击“下一步”，直至完成安装，并重启操作系统以生效。

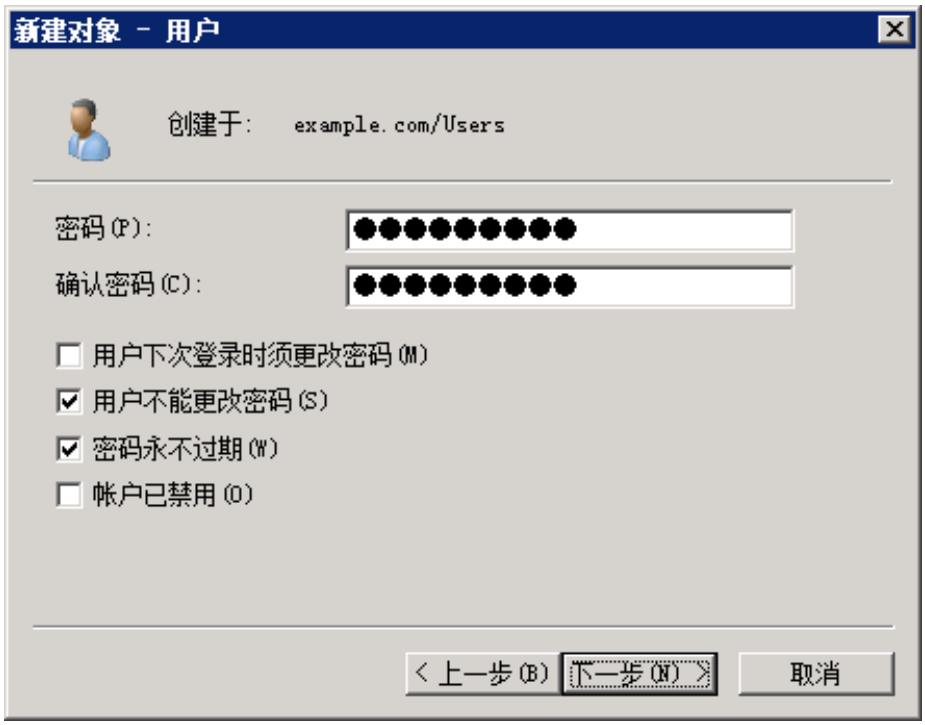


步骤3 创建Active Directory域用户。

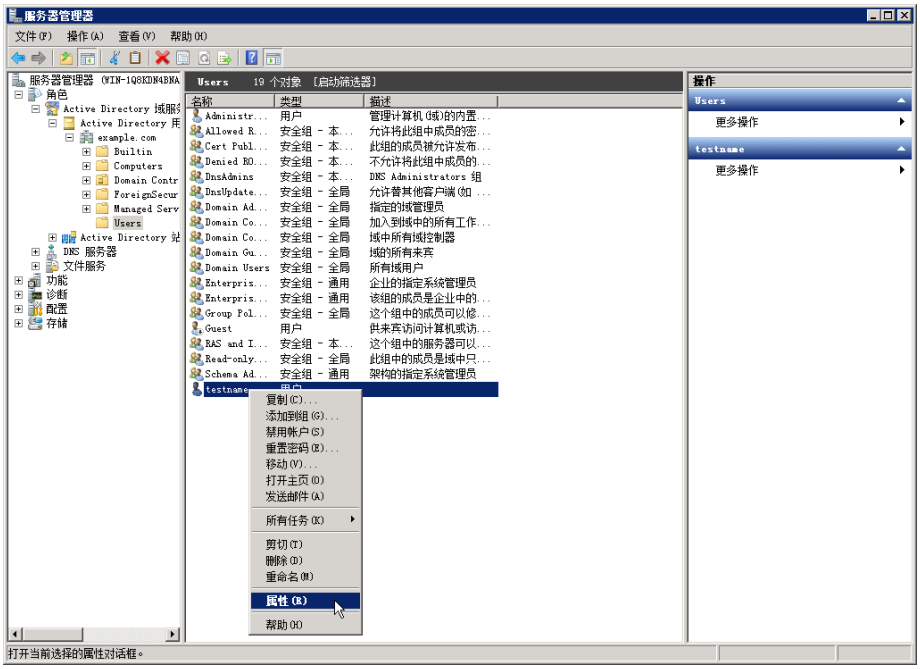
1. 在“服务器管理器”界面，展开“角色 > Active Directory域服务 > Active Directory用户和计算机 > example.com”，在“User”上右键选择新建用户。



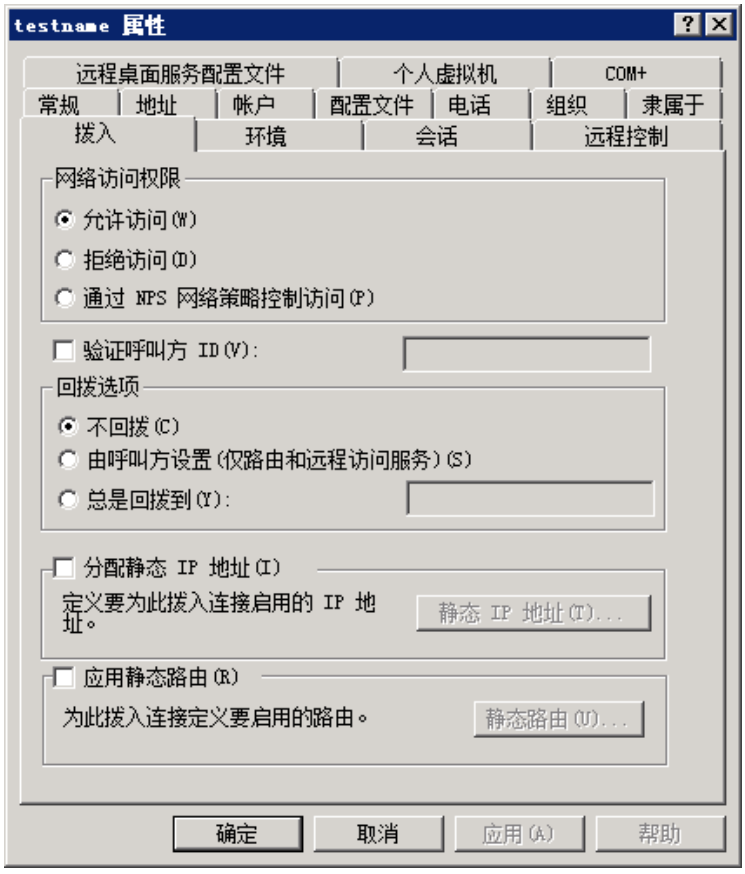
2. 配置用户基本信息和登录密码。



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。



----结束

3.4.3 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SecoClient软件安装包至AD服务器本地。

- 对于企业网用户：使用注册帐号登录网站**http://support.huawei.com/enterprise**，进入“企业网络 > 安全 > 防火墙&VPN网关 >（选择款型）”，选择下载对应版本的软件安装包。
- 对于运营商用户：使用注册帐号登录网站**http://support.huawei.com/carrier**，进入“产品软件 > 网络 > 交换机与企业网关 > 交换机与企业网关 >（选择款型）”，选择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。

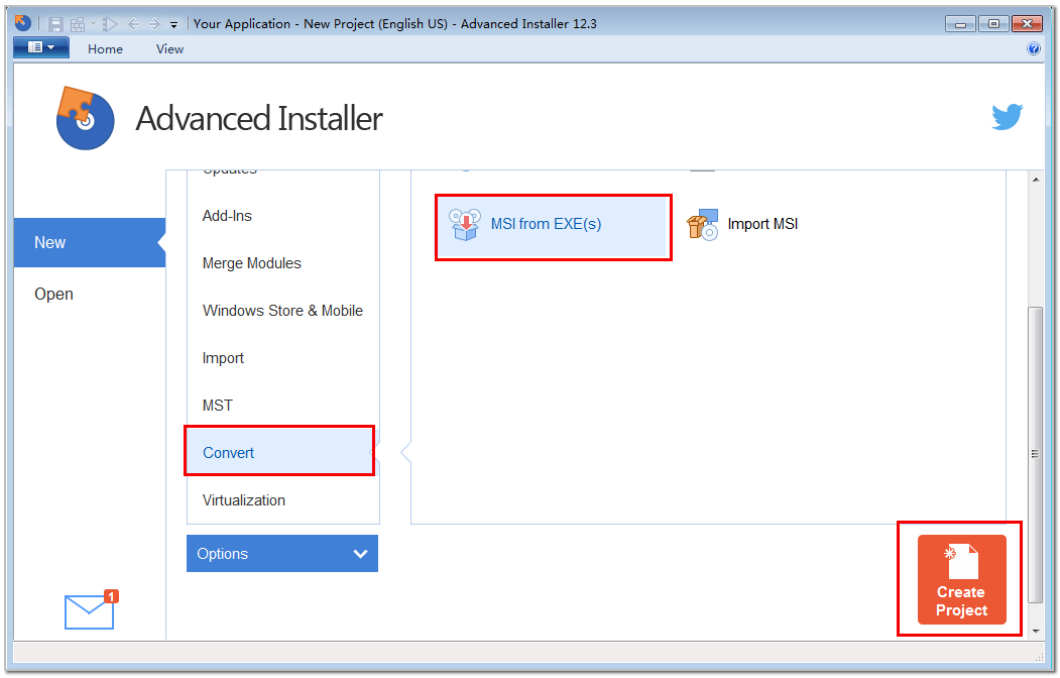
AD服务器在批量分发SecoClient软件安装包到终端用户主机的时候，使用的安装包格式是msi格式。使用Advanced Installer软件是为了将SecoClient原有的exe格式安装包转换成msi格式。

说明

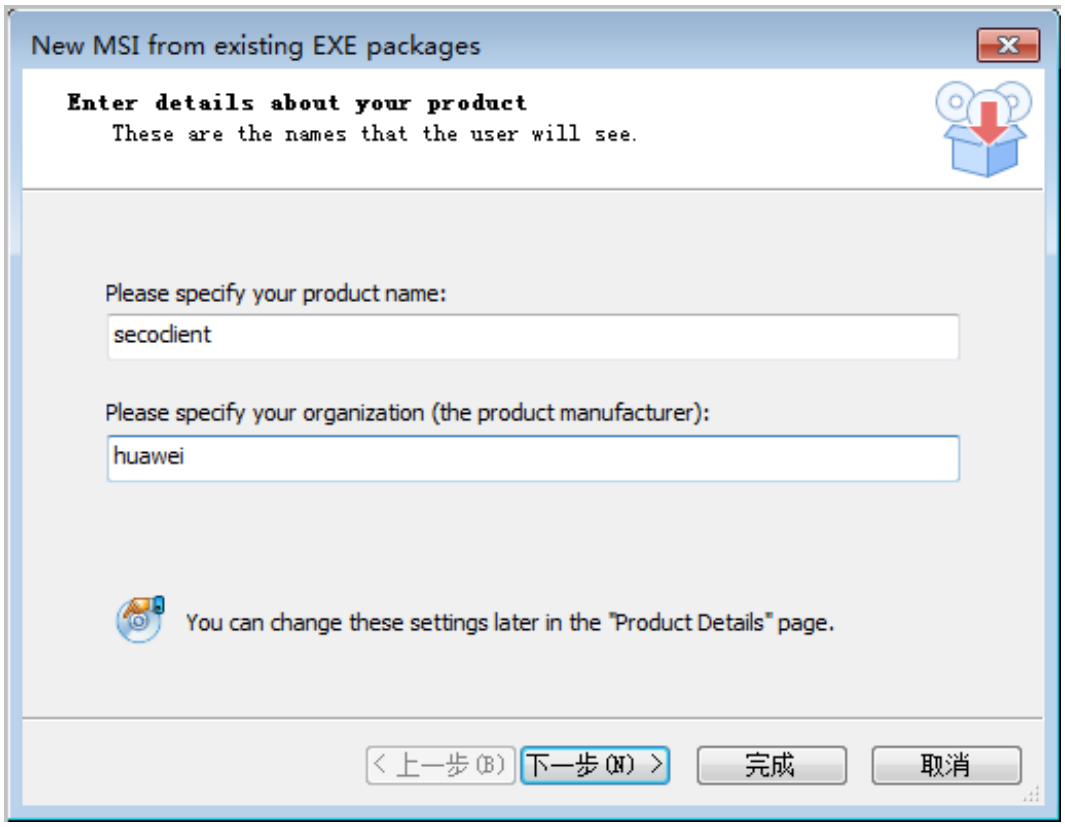
有很多种工具都可以把exe格式的软件安装包转换成msi格式，此处仅以Advanced Installer工具为例进行介绍，不表示只能通过Advanced Installer进行转换。

步骤3 在Advanced Installer上创建一个工程。

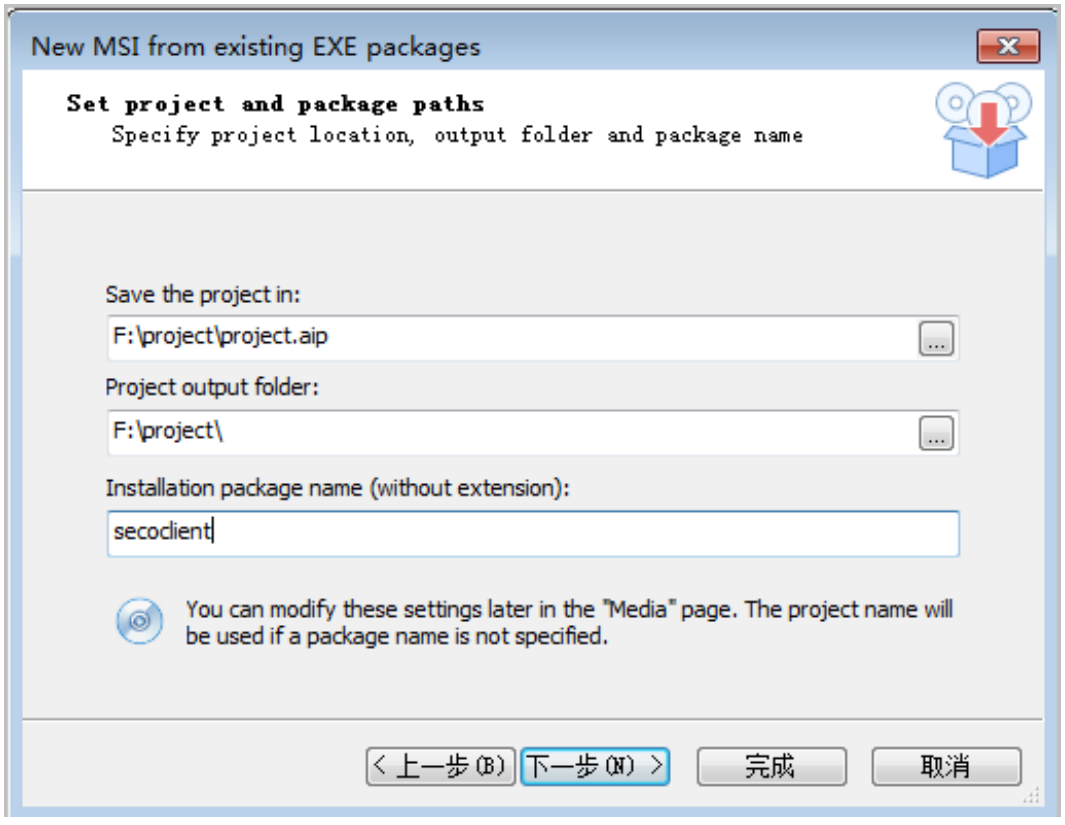
打开Advanced Installer软件，选择“Convert > MSI from EXE”，单击“Create Project”。



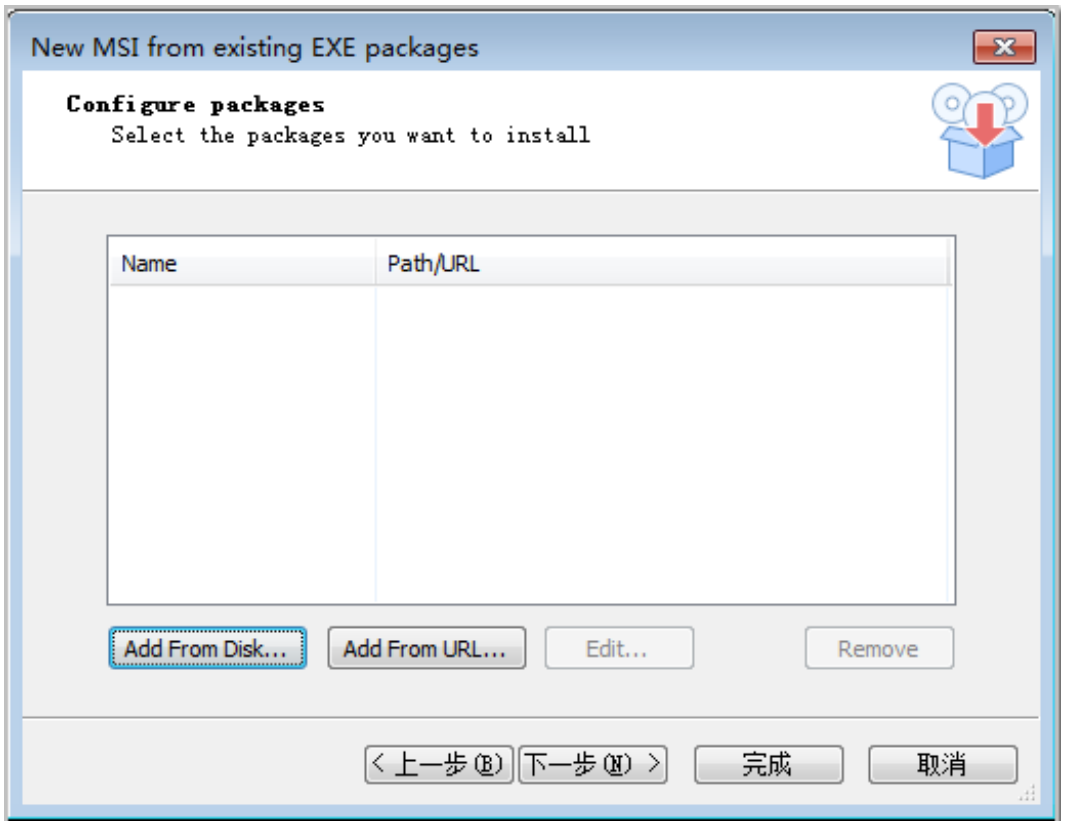
步骤4 在弹出的对话框中输入产品名称和企业名称，单击“下一步”。



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“下一步”。



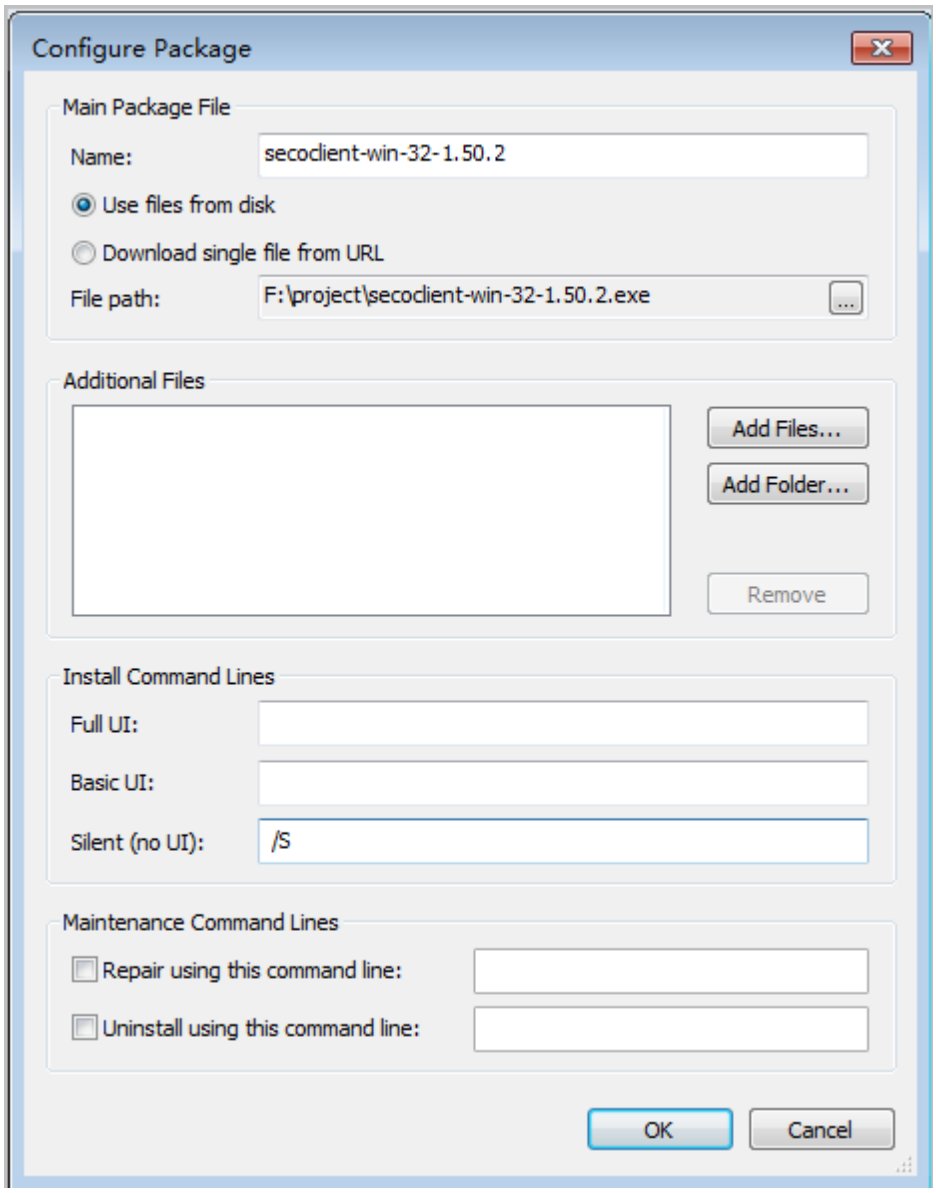
步骤6 单击“Add From Disk”，系统会弹出窗口提示您选择要转换格式的软件安装包。



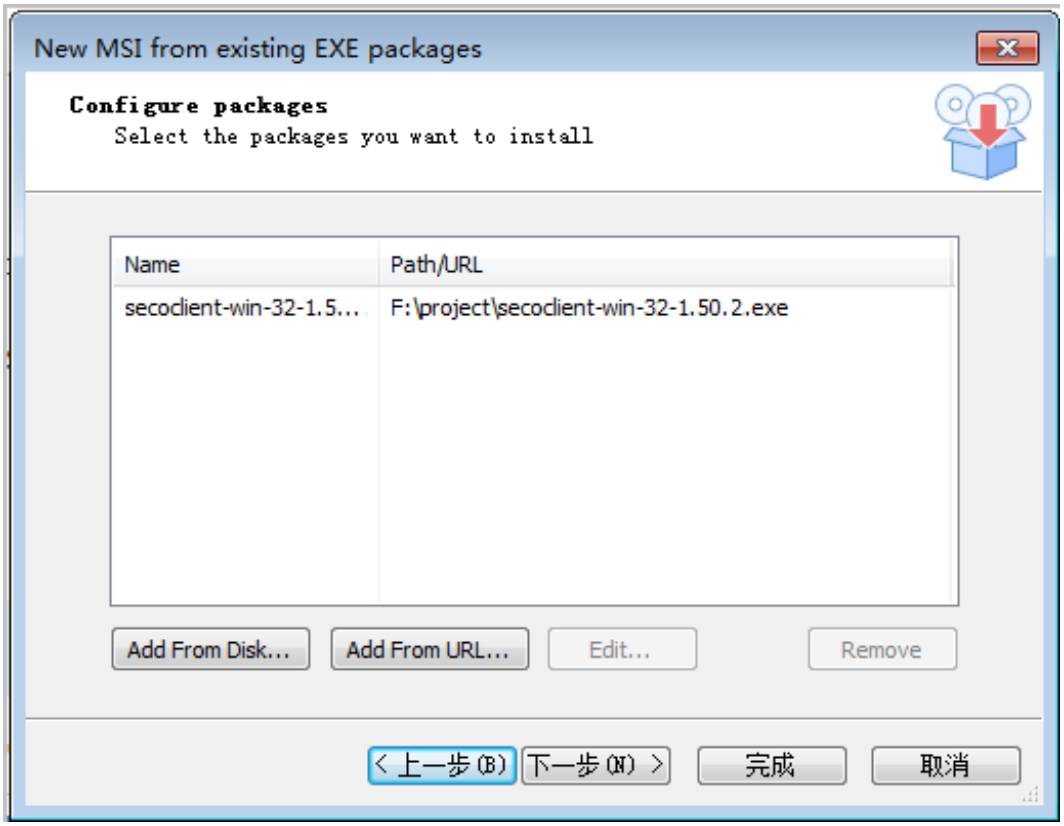
步骤7 完成如下界面设置，单击“OK”。

须知

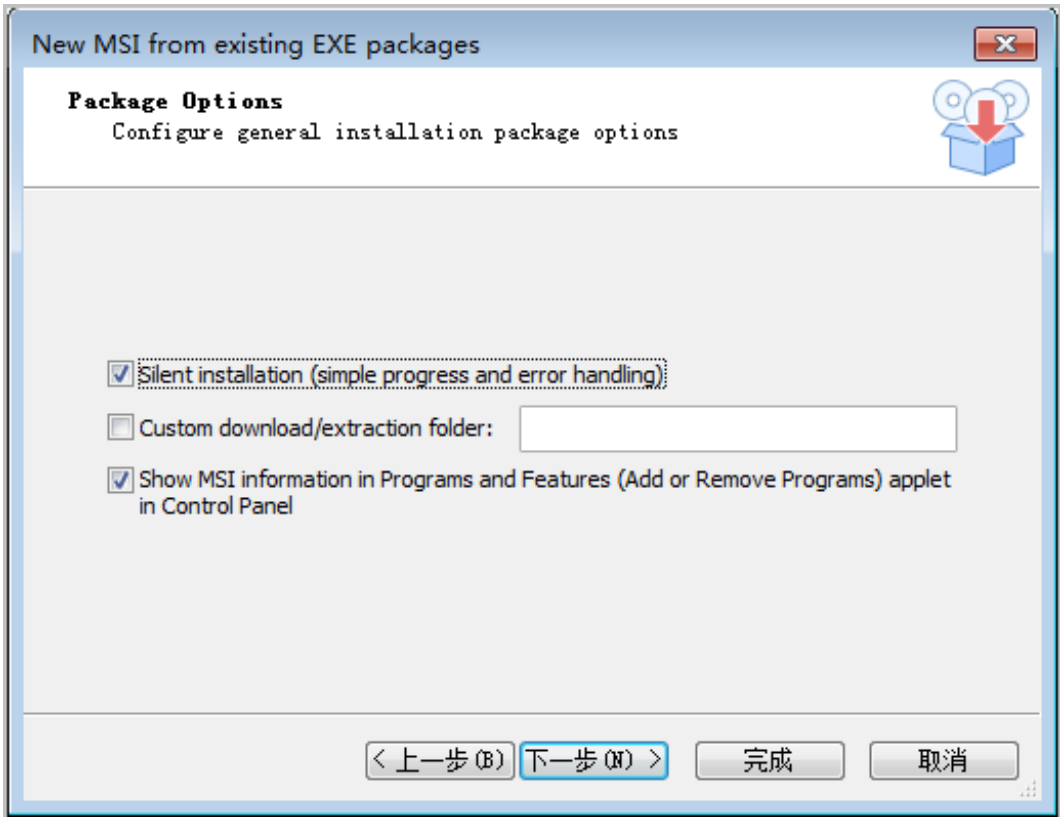
下图“Silent（no UI）”中“/S”的S要求用大写。



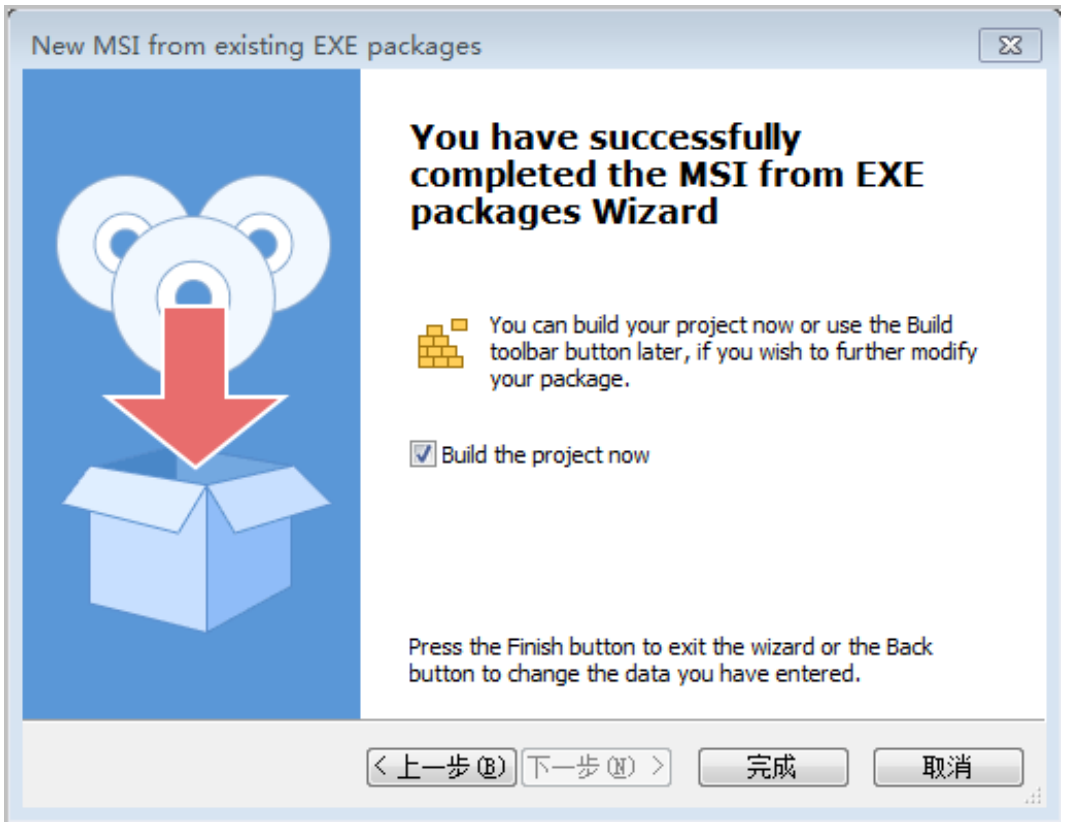
步骤8 单击“下一步”。



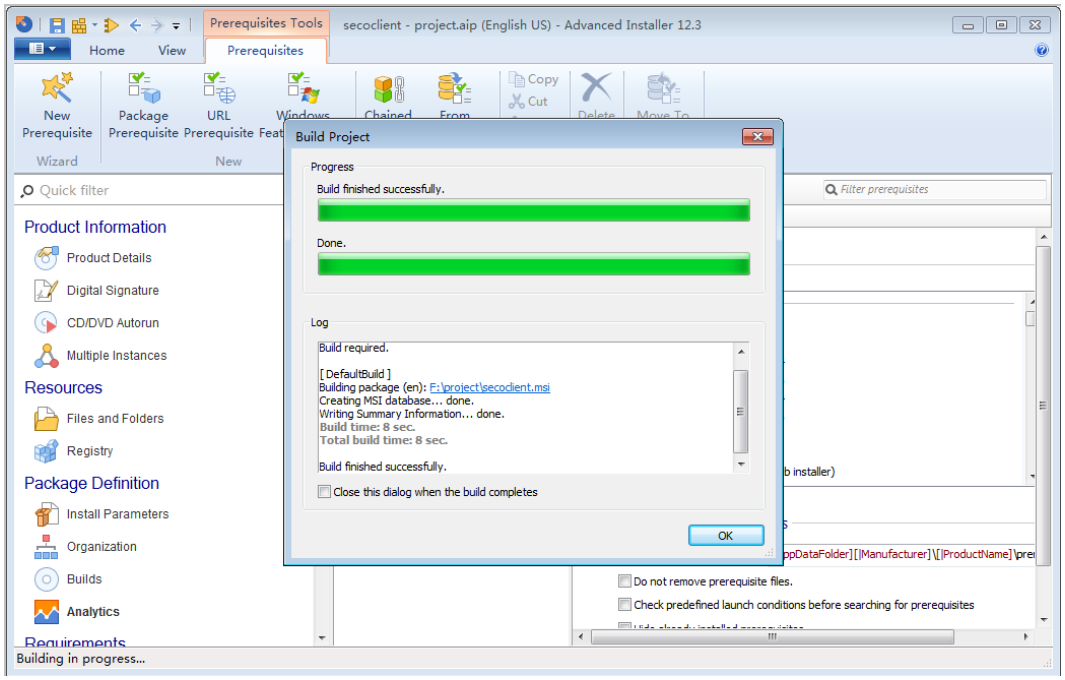
步骤9 勾选“Silent installation”选项，单击“下一步”。



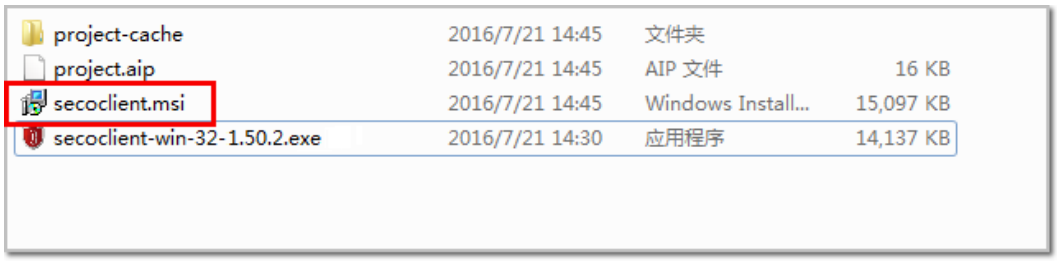
步骤10 单击“完成”。



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”。

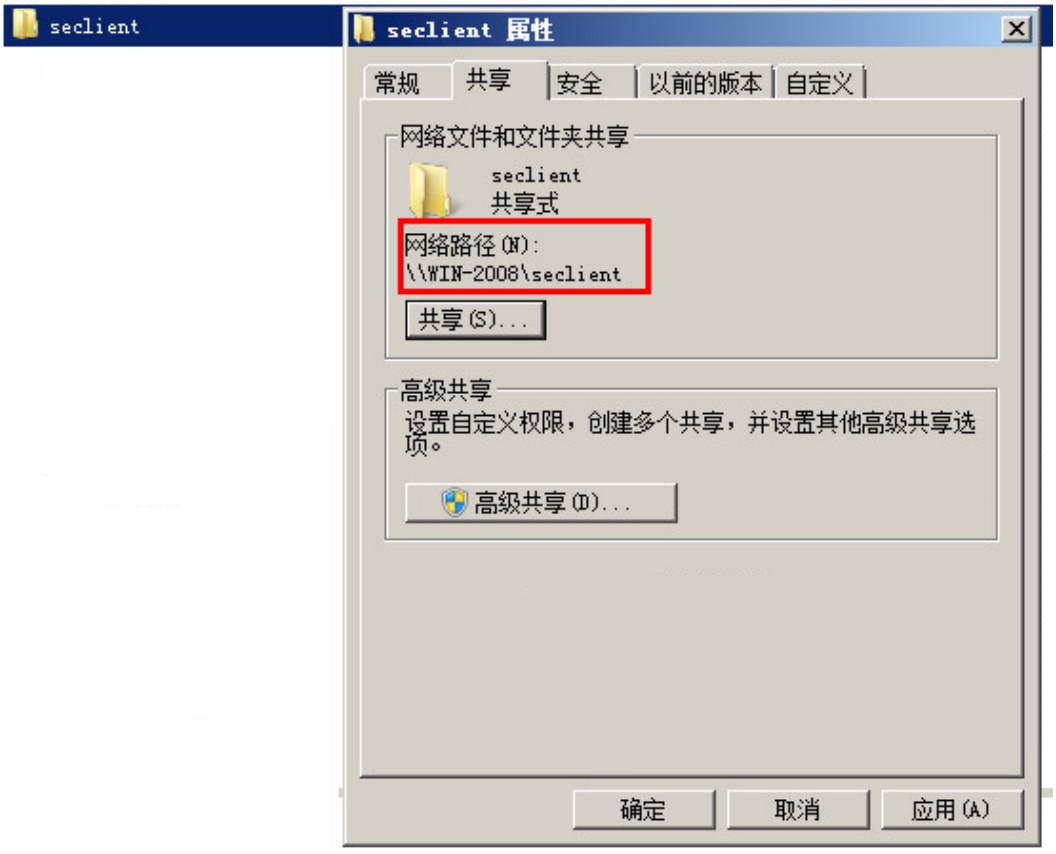


步骤12 检查指定工程路径下是否生成了secoclient.msi文件。



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secoclient.msi文件放入到这个文件夹中。

本例中共享文件夹的名称为secoclient。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。



----结束

4 产品规格和使用限制

介绍SecoClient的产品规格和使用限制。

产品规格

SecoClient的功能规格如表1所示。

表 4-1 SecoClient 的功能规格

功能名称		Windows操作系统	MAC操作系统	Linux操作系统
SSL VPN	网络扩展	支持	支持	支持
	终端安全	支持	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
	断线重连	支持	支持	支持
	链路备份	支持	支持	支持
	路由覆盖	支持	不支持	不支持
	国密算法	支持	支持	支持

功能名称		Windows操作系统	MAC操作系统	Linux操作系统
	证书认证	支持	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。
	MAC认证	支持	支持	支持
	证书筛选	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。	不支持
L2TP VPN		支持	支持	支持
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。
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。
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。
隧道分离		支持	支持	支持
基本功能	开机自启动	支持	支持	支持
	界面语言切换	支持	支持	支持
	自动登录	支持	支持	支持
配置文件	导入	支持	支持	支持
	导出	支持	支持	支持
故障定位		支持	支持	不支持

功能名称	Windows操作系统	MAC操作系统	Linux操作系统
命令行配置	不支持	不支持	支持
非管理员权限用户配置	支持	支持	支持

SecoClient的性能规格如表2所示。

表 4-2 SecoClient 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，SecoClient支持的USB-Key产品规格如表3所示。

表 4-3 SecoClient 支持的 USB-Key 产品规格

厂商名称	产品型号
大明五洲	eSafe C系列 eSafe E系列
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 4-4 USB-Key 证书认证的支持情况

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

使用限制

SecoClient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。

5 配置

Windows操作系统、MAC操作系统和Linux操作系统下使用SecoClient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 SecoClient 建立 VPN 隧道

SecoClient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 手工方式

手工方式是指SecoClient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。

SecoClient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SecoClient，进入主界面。
   在“连接”对应的下拉列表框中，选择“新建连接”。

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中“SSL VPN”，并配置相关的连接参数。

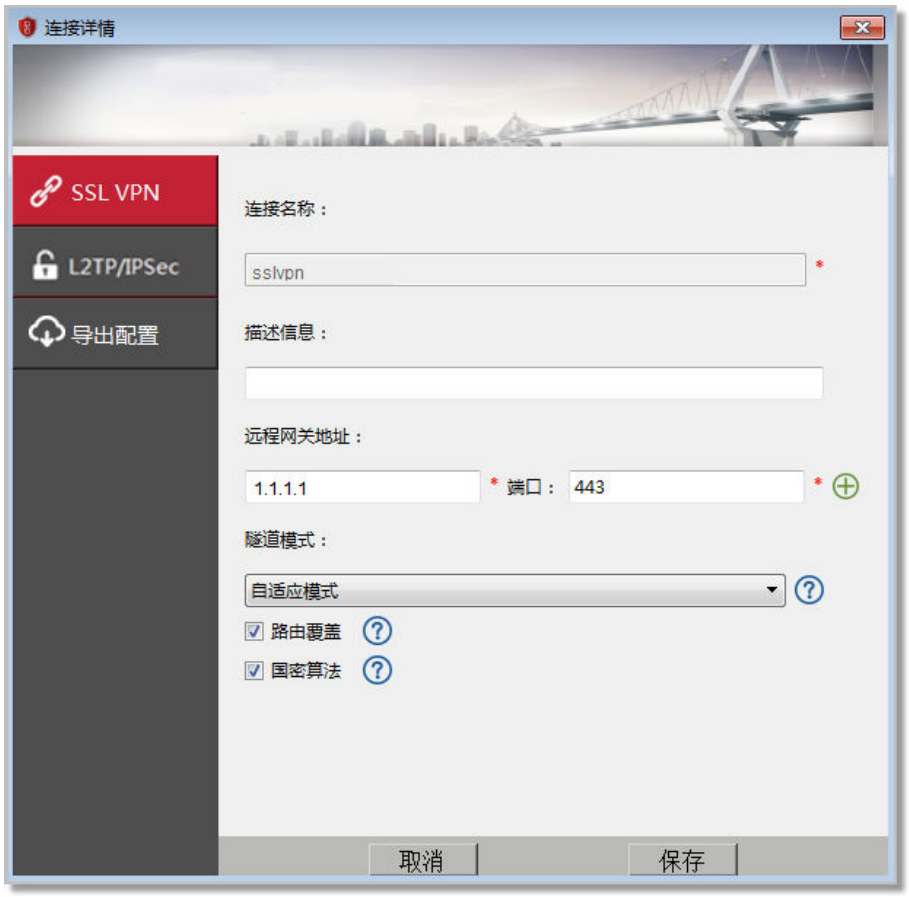


表 5-2 SSL VPN 配置参数说明

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，默认端口号是443。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。 单击端口后的，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15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“启用自动优选”，SecoClient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“启用自动优选”时，则要在虚拟网关列表中先选中一个地址，然后单击“设置默认网关”按钮，表示SecoClient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隧道的模式有两种：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，SecoClient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。

参数	说明
路由覆盖 **说明** 仅在Windows操作系统下会显示此项。	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。
证书认证 **说明** 仅在Linux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。
密码 **说明** 仅在Linux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“确定”，返回主界面。

步骤2 登录SSL VPN虚拟网关。

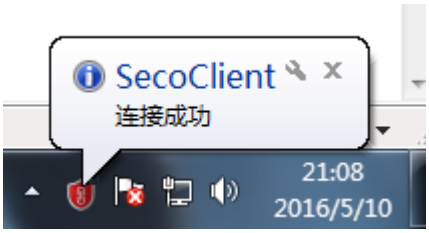
1. 在“连接”下拉列表框中选择已经创建的SSL VPN连接，单击“连接”。

2. 在登录界面输入用户名、密码。
   勾选“自动”，表示存在多个虚拟网关时，系统会自动选择响应速度最快的虚拟网关建立SSL VPN隧道。只有一个网关的情况下，无需勾选“自动”单选框。单击“登录”，发起VPN连接。

若在Windows或MAC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SecoClient，进入主界面。
   在“连接”对应的下拉列表框中，选择“新建连接”。

表 5-3 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。 **说明** L2TP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 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。

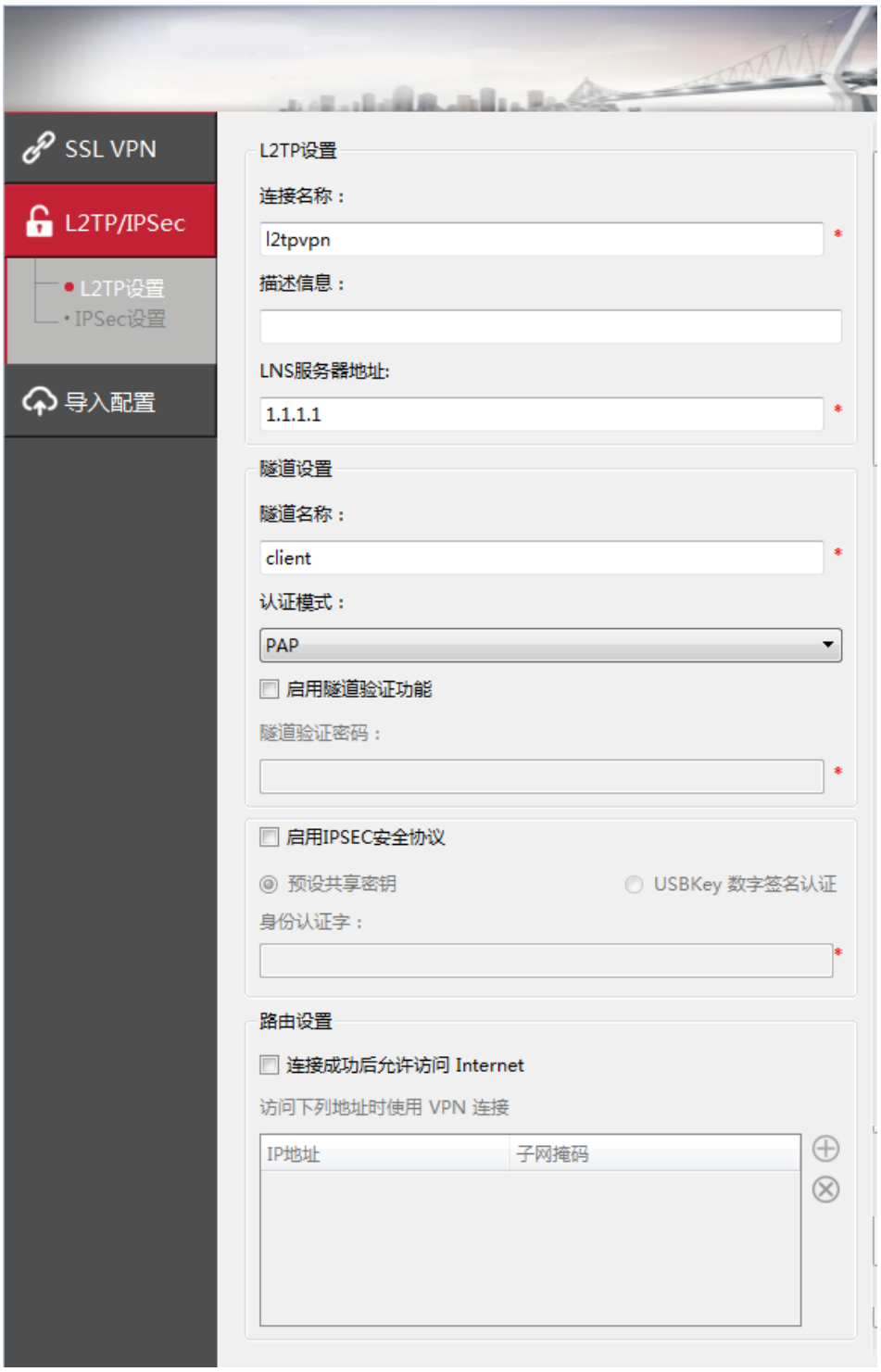


表 5-4 L2TP 配置参数说明

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。

参数	说明
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。
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SecoClient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。

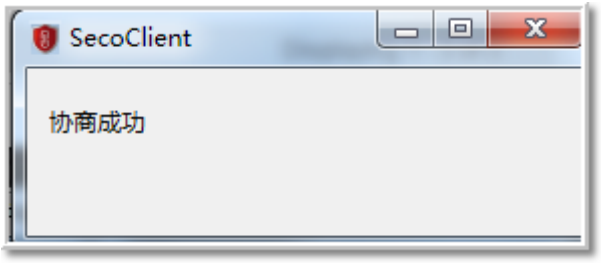
参数	说明
路由设置	在设置“连接成功后允许访问Internet”参数时有如下三种选择，请根据实际需要进行设置。 – 不勾选 移动办公用户拨号成功后，其个人PC的默认路由下一跳会被修改为虚拟网卡的IP地址。此时，所有流量都会经过虚拟网卡发送到隧道对端，这意味着该用户只能访问企业内网资源，不能访问Internet。 – 勾选但不在IP地址列表框中添加IP地址 移动办公用户拨号成功后，其个人PC会生成一条目的网段为虚拟网卡对应的IP地址段，下一跳为虚拟网卡的IP地址的路由。此时，该用户只能访问与虚拟网卡IP地址同网段的企业内网资源。由于用户原有路由没有受到影响，所以还可以访问Internet和本地局域网。 – 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“连接”下拉列表框中选择已经创建的L2TP VPN连接，单击“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SecoClient，进入主界面。
   在“连接”对应的下拉列表框中，选择“新建连接”。

表 5-5 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。 **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 5-6 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SecoClient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。

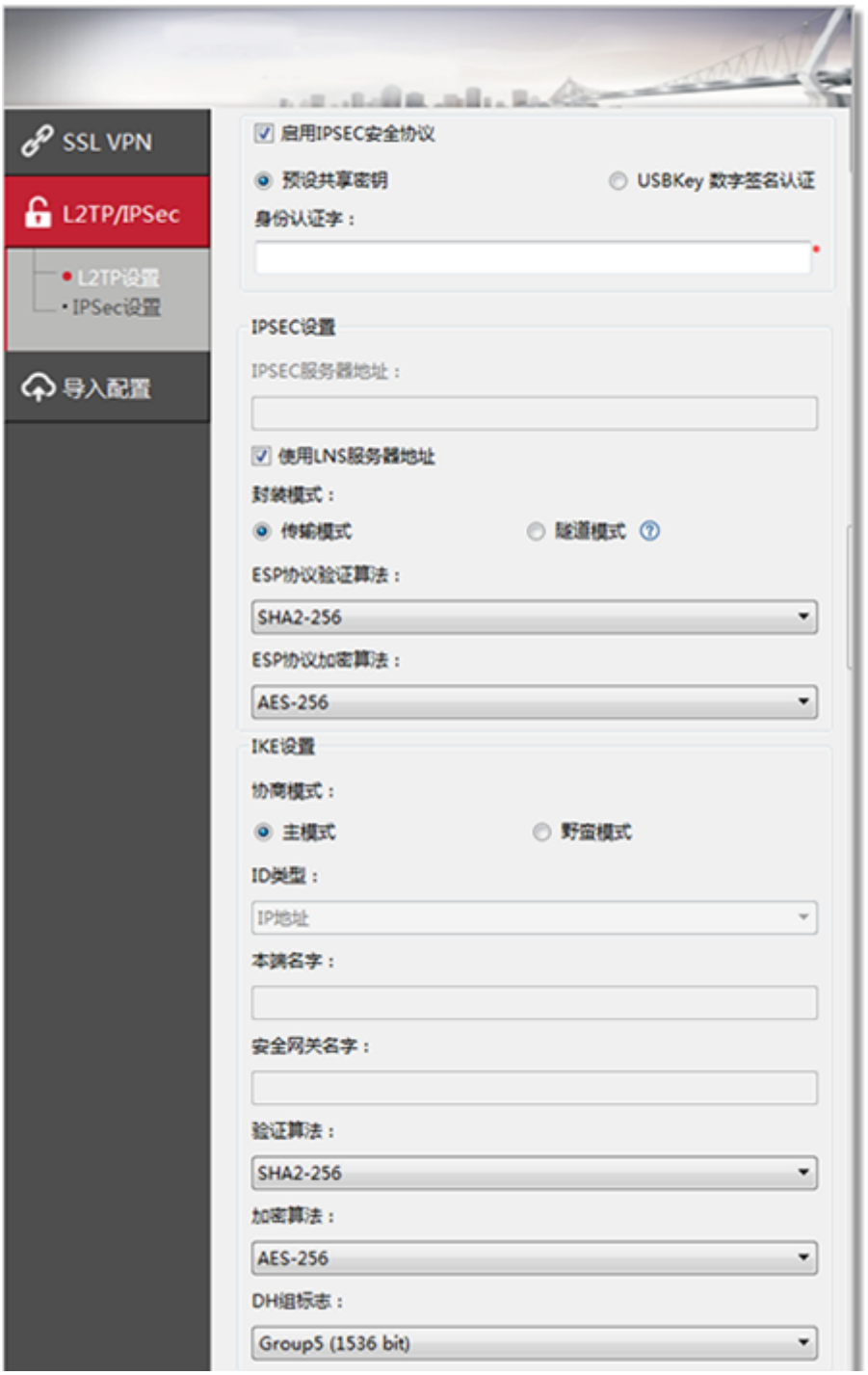


表 5-7 IPSec 配置参数说明

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** MAC和Linux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。

参数	说明
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	
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。

参数	说明
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SecoClient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，SecoClient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SecoClient认证，身份认证通过，SecoClient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、SHA1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。
IKE高级设置	

参数	说明
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、group2和group5。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SecoClient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。

参数	说明
	○ 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“确定”，返回主界面。

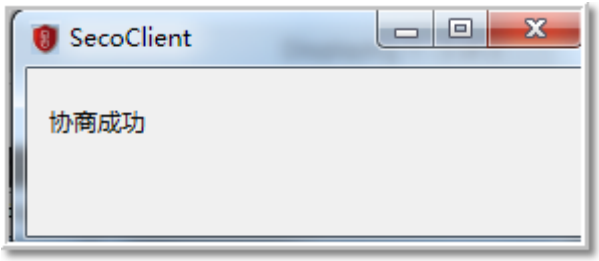
步骤2 登录L2TP over IPSec VPN网关。

1. 在“连接”下拉列表框中选择已经创建的L2TP over IPSec VPN连接，单击“连接”。

2. 在登录界面输入用户名、密码。

   若在Windows或MAC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 配置文件方式

配置文件方式是指SecoClient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SecoClient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

步骤1 选中一个已存在的VPN连接，单击连接右侧的编辑  。

步骤2 在“连接详情”窗口中，单击导航栏左侧的“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。

----结束

导入配置文件

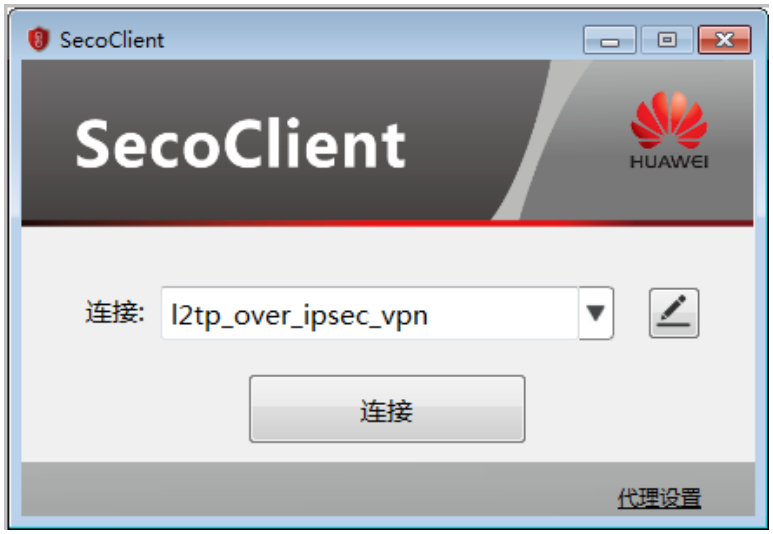
步骤1 在SecoClient主界面的“连接”下拉列表框中，选择“新建连接”。

步骤2 在“新建连接”窗口中，单击导航栏左侧的“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SecoClient主界面。

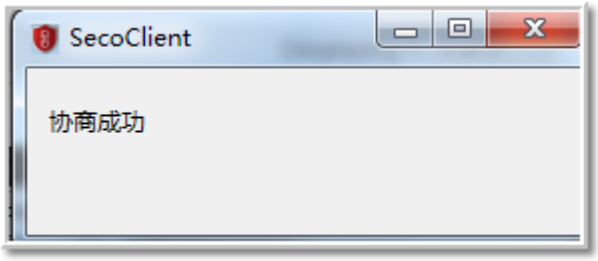
可以看到l2tp_over_ipsec_vpn这条VPN连接已经生成，单击“连接”。



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SecoClient的一些常用功能设置。

显示主界面

步骤1 右键单击SecoClient的托盘图标。

步骤2 在菜单中选择“显示主界面”，回到SecoClient主界面。

----结束

连接/断开连接

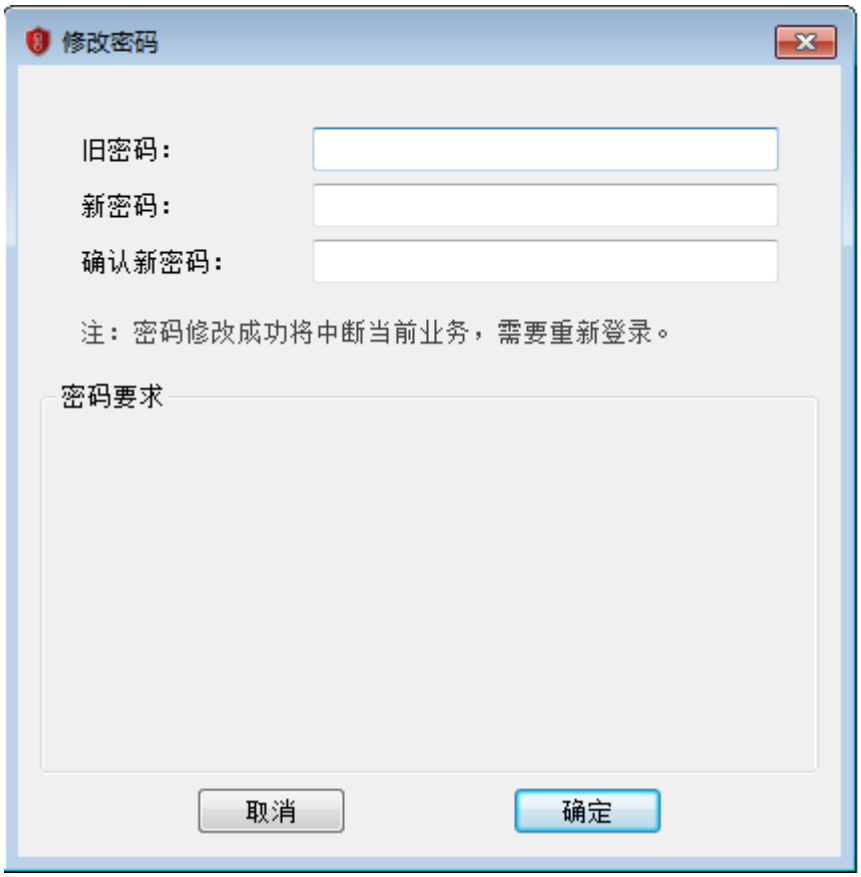
右键单击SecoClient的托盘图标，在菜单中选择“连接”可以直接向VPN网关发起隧道连接请求；在菜单中选择“断开连接”，将会拆除当前的VPN隧道。

修改密码

右键单击SecoClient的托盘图标，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SecoClient与FW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”菜单项是灰色显示无法选择。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SecoClient出现无法排除的故障时，请向华为工程师获取帮助。为了便于华为工程师快速的定位问题，请您在获取帮助之前预先收集SecoClient的错误报告。

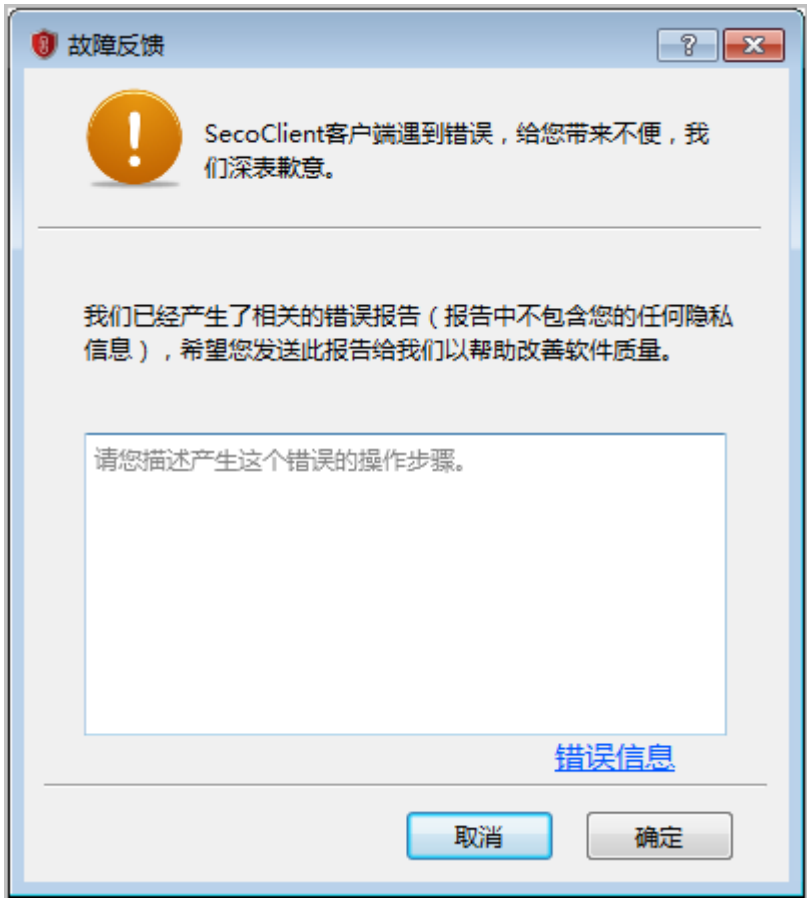
说明

SecoClient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。

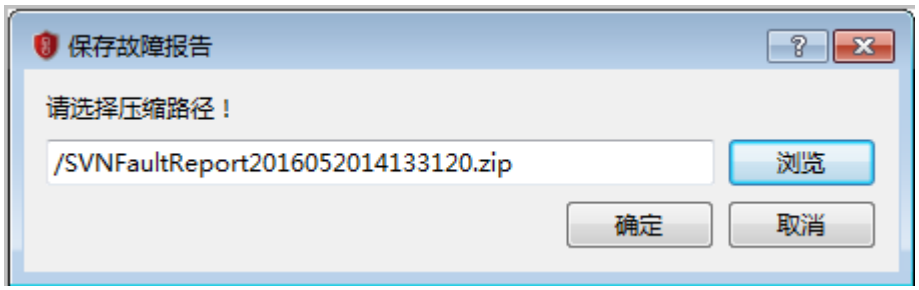
- **error_detail.txt**：记录用户手动输入的对产生该错误的操作步骤的描述，以及所用客户端的版本号信息。
- **netcard_info.txt**：记录SecoClient所在PC的网卡信息。
- **operate_system_info.txt**：记录SecoClient所在PC的操作系统信息。
- **proxy_info.txt**：记录SecoClient所在PC的代理服务器信息。
- **route_info.txt**：记录SecoClient所在PC的路由信息。
- **SecoClient_SecoClientCS_0.log**：记录SecoClient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。
- **SecoClient_SecoClientUI_0.log**：记录SecoClient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。
- **SecoClient_SecoClientPromoteService_0.log**：SecoClient的服务进程，用于确保SecoClient正常运行。
- **崩溃文件**：当SecoClient在出现异常关闭的情况下将生成崩溃文件，不同原因造成的SecoClient异常关闭所生成的崩溃文件名称不一样。在Windows操作系统下崩溃文件的后缀是*.dmp，在MAC和Linux操作系统下生成的崩溃文件后缀为*.core。

步骤1 右键单击SecoClient的托盘图标。

步骤2 选择“错误报告”。



步骤3 单击“确定”，选择错误报告的存放路径。



说明

在Linux操作系统下保存错误报告的压缩包时，选择的保存路径中不能含有~ < > | ; ? ' , & #等特殊字符。

步骤4 单击“确定”。

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华为工程师，由华为工程师协助您解决问题。

----结束

取消自动登录

右键单击SecoClient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。

选项

步骤1 右键单击SecoClient的托盘图标，在弹出的菜单中选择“选项”，设置如下参数。

表 5-8 高级页签参数说明

功能项	说明
开机自启动	勾选此项，SecoClient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。
阻塞连接到不信任的服务器	SecoClient与FW建立SSL VPN隧道时，SecoClient会校验FW发送过来的设备证书。 ● 勾选此选项 SecoClient校验FW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。
检测新版本	勾选后，系统会检查待连接的FW网关上是否存在新的SecoClient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12种界面语言，包括： ● 英语 ● 法语 ● 德语 ● 俄语 ● 日语 ● 韩语 ● 简体中文 ● 繁体中文 ● 阿拉伯语 ● 意大利语 ● 葡萄牙语 ● 西班牙语 **说明** 首次运行客户端时，若操作系统的语言在支持的12种界面语言范围内，则客户端界面语言与操作系统的语言一致；若操作系统的语言不在支持的12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“高级 > 网络”页签，单击“连接”下的“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。

帮助

右键单击SecoClient的托盘图标，在菜单中选择“帮助”。

“关于”子选项中记录了SecoClient的版本和版权信息；“帮助”子选项包含了SecoClient软件的使用指导，可以帮助用户更好的熟悉和使用SecoClient，以及解决您在使用SecoClient过程中遇到的问题。

退出

右键单击SecoClient的托盘图标，在菜单中选择“退出”，关闭SecoClient软件。

5.3 升级

本节介绍SecoClient的升级方法。

背景信息

SecoClient升级的基本过程是，网络管理员先把新的SecoClient软件上传至FW，用户通过SecoClient与FW建立VPN隧道时，SecoClient客户端会自动检查FW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。

说明

SecoClient在与V100R001C30SPC800版本的网关对接时不支持升级功能。

操作步骤

步骤1 网络管理员上传SecoClient软件安装包至FW。

1. 用户使用注册帐号登录网站**http://support.huawei.com/enterprise**，进入“企业网络 > 安全 > 防火墙&VPN网关 > Secospace USG6600 > 软件”，选择下载对应版本的软件安装包。
2. 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SecoClient软件安装包。

   SecoClient针对Windows操作系统（32位/64位）、MAC操作系统（64位）和Linux操作系统（32位/64位）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SecoClient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FW侧软件安装包升级。

步骤2 用户侧升级SecoClient版本。

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

----结束

6 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，请登录**华为技术支持网站**获取防火墙产品的产品文档；如果您需要了解客户端常见故障的定位及处理方法，请登录**华为技术支持网站**获取防火墙产品的维护宝典。

7 FAQ

介绍您在使用SecoClient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。

SecoClient 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 SecoClient 客户端?

这是因为之前已经安装了SecoClient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SecoClient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 SecoClient 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 SecoClient 软件更新会提示失败?

终端用户在更新SecoClient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SecoClient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。
- SecoClient与SSL VPN虚拟网关之间部署了NAT Server设备，由于NAT Server无法对SecoClient的更新消息进行处理，造成SecoClient更新失败。

8 附录

8.1 移动客户端

除了PC版的SecoClient客户端外，华为公司还推出了基于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“**SecoClient**”字段，即可下载最新版本的SecoClient iOS版本客户端。

  方式二：在华为技术支持网站下载对应版本的软件安装包。

  - 对于企业网用户：使用注册帐号登录网站**http://support.huawei.com/enterprise**，进入“企业网络 > 安全 > 防火墙&VPN网关 > Secospace USG6600 > 软件”，选择下载对应版本的软件安装包。
  - 对于运营商用户：使用注册帐号登录网站**http://support.huawei.com/carrier**，进入“产品软件 > 网络 > 交换机与企业网关 > 交换机与企业网关 > Eudemon1000E-N 系列 > Eudemon1000E-N”，选择下载对应版本的软件安装包。

- **Android操作系统版本的移动版客户端**

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

  方式二：在华为技术支持网站下载对应版本的软件安装包。

  - 对于企业网用户：使用注册帐号登录网站**http://support.huawei.com/enterprise**，进入“企业网络 > 安全 > 防火墙&VPN网关 > Secospace USG6600 > 软件”，选择下载对应版本的软件安装包。

- 对于运营商用户：使用注册帐号登录网站**http://support.huawei.com/carrier**，进入“产品软件 > 网络 > 交换机与企业网关 > 交换机与企业网关 > Eudemon1000E-N 系列 > Eudemon1000E-N”，选择下载对应版本的软件安装包。

规格

移动版SecoClient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 8-1 移动版 SecoClient 客户端支持的机型及操作系统版本

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SecoClient客户端的功能规格如下：

表 8-2 移动版 SecoClient 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SecoClient客户端可以拨号成功。	不支持	不支持

功能名称		iOS	Android
	网关优选	不支持	不支持
	断线重连	不支持	不支持
	链路备份 **说明** 网关侧开启链路备份功能时，移动版SecoClient客户端可以拨号成功。	支持	支持
	证书认证	不支持	不支持
	MAC认证	不支持	不支持
	证书筛选	不支持	不支持
	双因子认证	不支持	不支持
L2TP VPN		不支持	不支持
L2TP over IPSec VPN		不支持	不支持
NAT穿越		支持	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
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SecoClient客户端的性能规格如下：

表 8-3 移动版 SecoClient 客户端的性能规格

功能名称	规格
VPN新建连接数	16个

操作

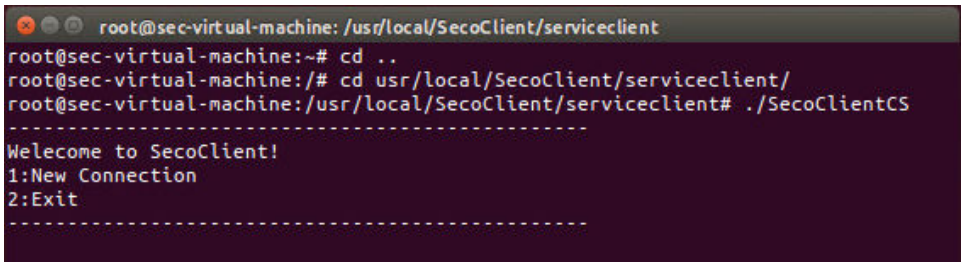
移动版SecoClient客户端的具体操作，请参见APP内“设置 > 帮助”节点下的联机帮助。

8.2 在 Linux 操作系统下通过命令行方式配置客户端

8.2.1 启动客户端

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

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



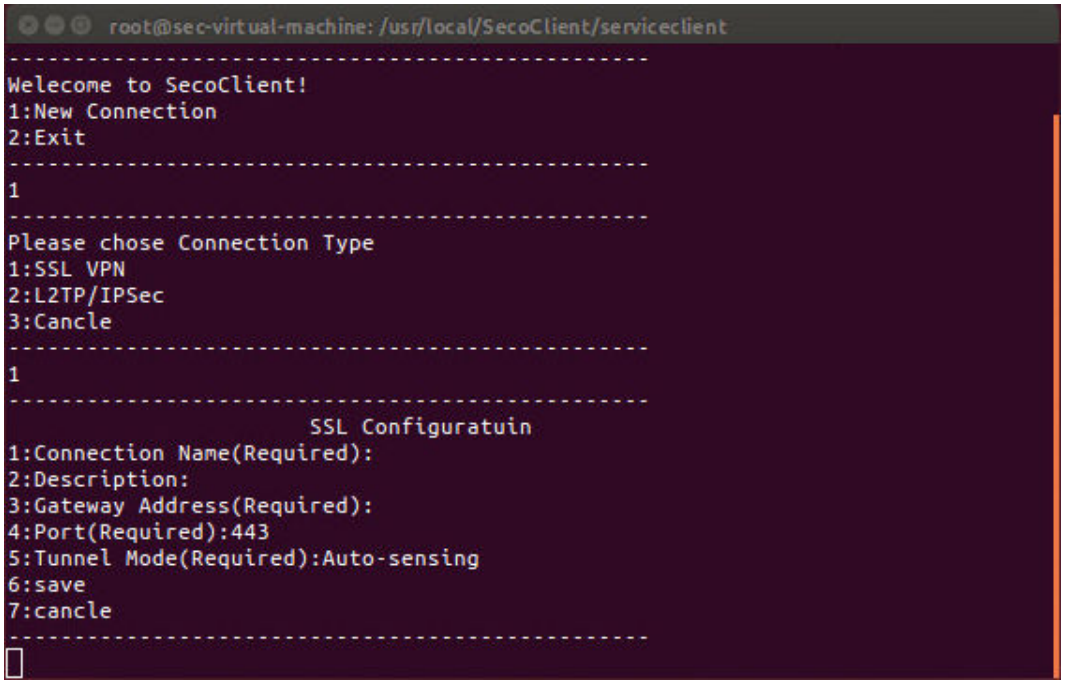
说明

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

8.2.2 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。

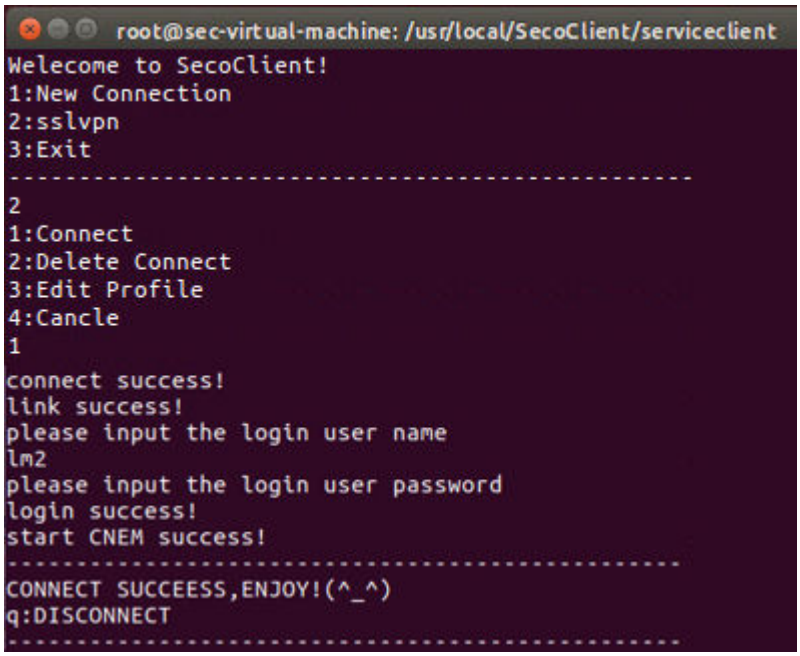
步骤3 输入对应序号，完成参数**1~5**的配置。

- 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**6**，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

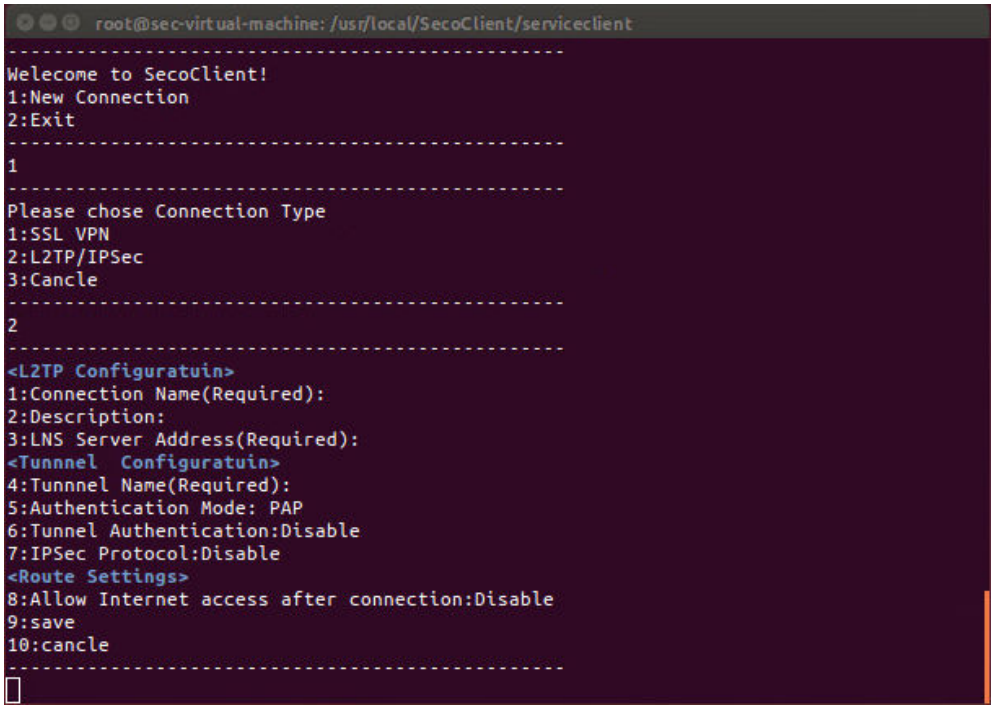
- 在Linux操作系统下通过命令行方式配置并建立的SSL VPN连接仅支持通过用户名/密码认证方式认证登录。
- 连接成功后，不能关闭该终端窗口，否则连接会断开。

断开 SSL VPN 连接

输入**q**，即可断开连接。

8.2.3 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。

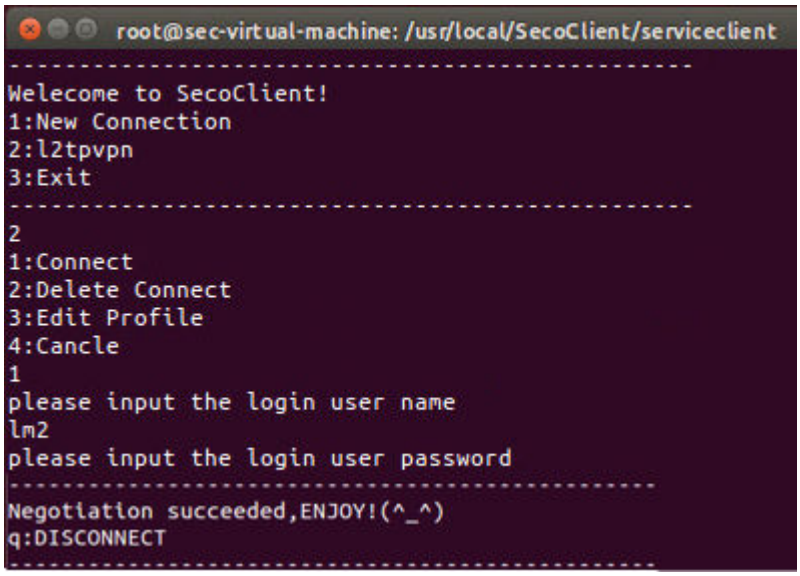
步骤3 输入对应序号，完成参数**1~8**的配置。

- 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

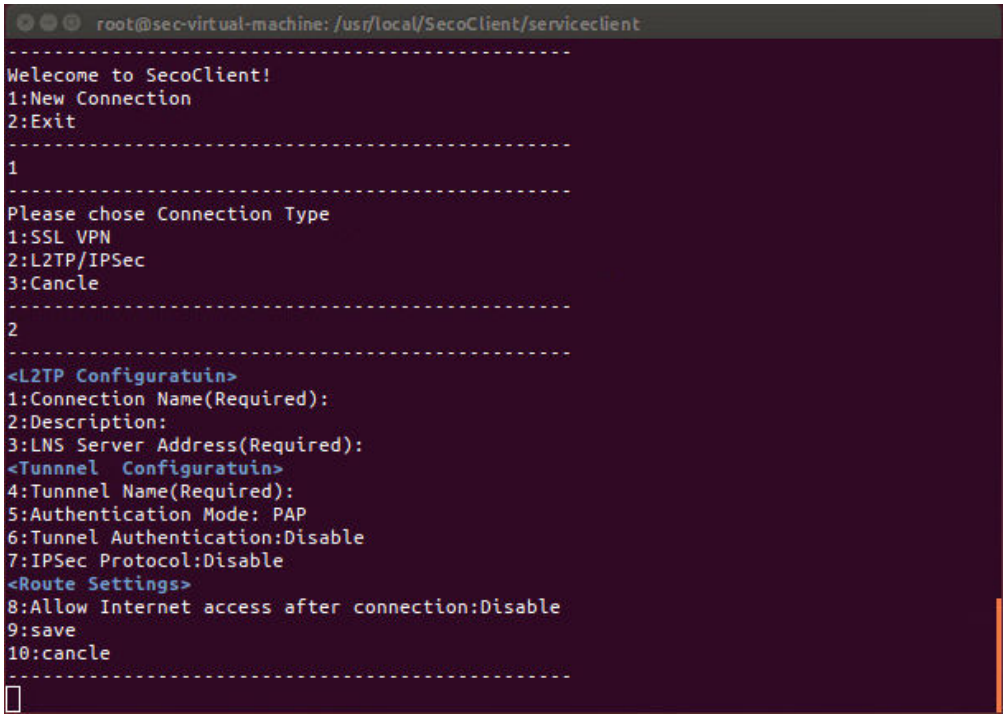
连接成功后，不能关闭该终端窗口，否则连接会断开。

断开 L2TP VPN 连接

输入**q**，即可断开连接。

8.2.4 配置 L2TP over IPSec VPN 连接

配置 L2TP 参数



步骤1 输入**1**，创建新连接。

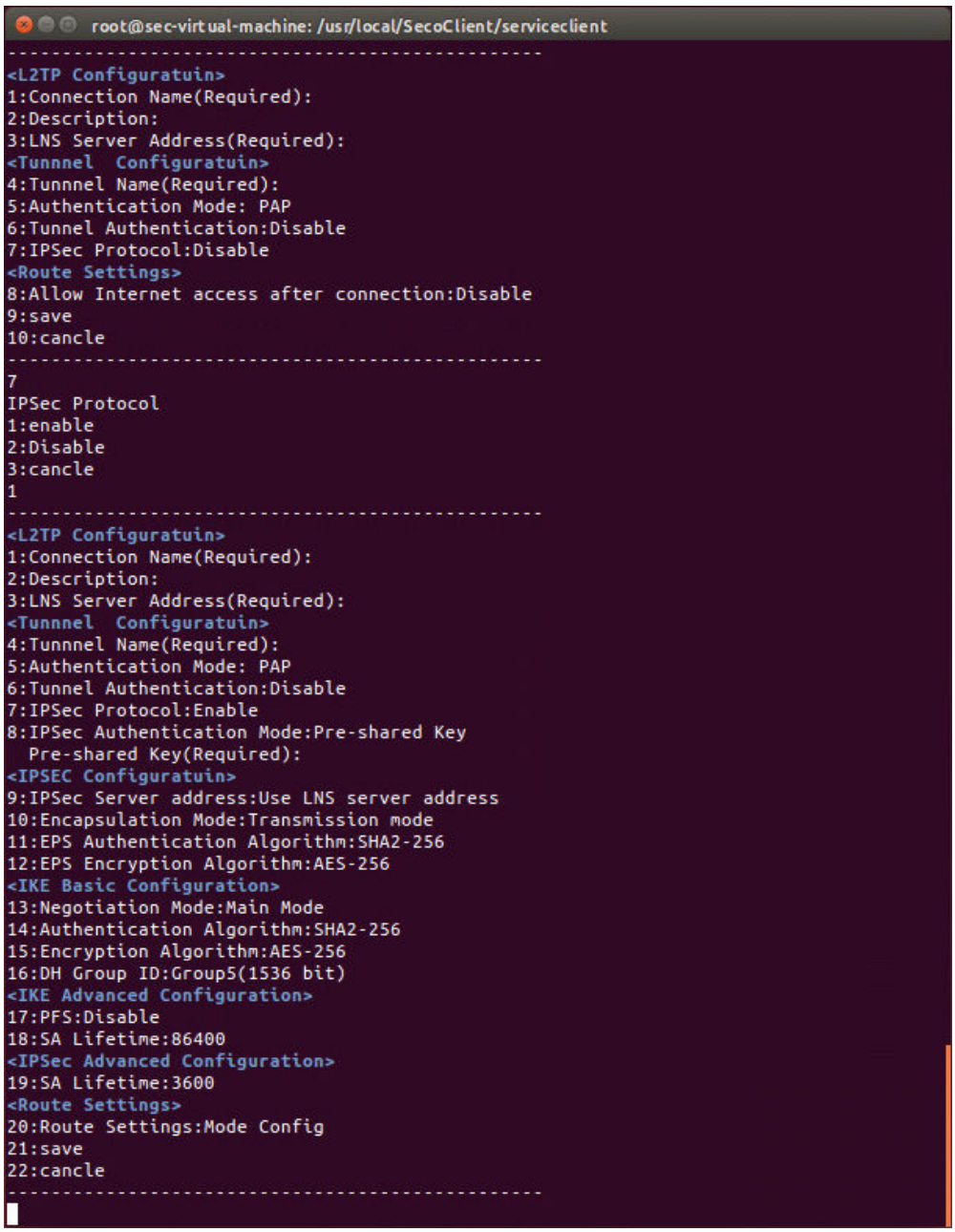
步骤2 输入**2**，选择创建的VPN类型为L2TP/IPSec。

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。

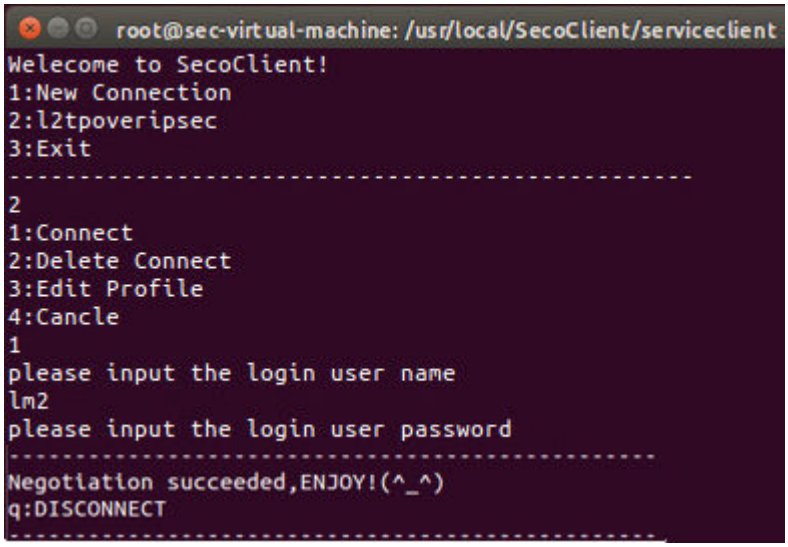
- 8. IPSec Authentication Mode：Linux操作系统下IPSec的身份认证方式目前仅支持预共享密钥认证，预共享密钥方式下需要输入身份认证字（Pre-shared key）；
- 9. IPSec Server address：IPSec服务器地址，缺省设置为使用LNS服务器地址（Use LNS server address）；
- 10. Encapsulation Mode：IPSec封装模式，包括传输模式（Transmission mode）和隧道模式（Tunnel mode）两种；
- 11. ESP Authentication Algorithm：ESP协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

- 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。

8.3 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

缩略语		
NAT	Network Address Translation	网络地址转换
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

