

交易结算测试网新版 VPN 客户端及网络配置 操作指引

一、概述

因交易结算测试网VPN环境全面升级，原有的基于浏览器的VPN方式将停止服务，统一更换为客户端方式接入，推荐使用UniVpn（其他VPN客户端请参考以下配置参数，自行调试）。用户需下载安装VPN客户端软件，并按照本指引完成网络配置，以确保各项业务测试工作平稳过渡。

独立测试系统为市场用户进行深市结算、全国股转、易境通、开放式基金等业务测试提供服务（由于VPN特性，暂不支持组播业务流量）。

备注：用户申请VPN账号，请登录深证通统一客户专区办理申请，具体路径：<https://biz.sccc.com> - 业务申请 - 通信服务业务申请 - 独立测试系统VPN接入申请 - 申请。

二、VPN 客户端环境说明

客户端软件：UniVPN Client（远程接入终端方案）

支持操作系统：Windows系统、麒麟OS、统信UOS等

连接协议：SSL VPN

隧道模式：自适应模式

新版VPN网关接入信息如下：

线路	连接名称	远程网关地址	端口
电信线路	SSLVPN 电信	113.108.41.94	3688
联通线路	SSLVPN 联通	58.250.178.124	3688

三、UniVPN 客户端下载与安装

1. 下载 UniVPN 客户端

请通过以下链接下载 UniVPN 客户端软件安装包：

下载地址：<http://www.leagsoft.com/doc/article/103107.html>

请根据操作系统选择对应版本下载（本文仅以 UniVPN 客户端 Windows 版作为案例演示）。如下图所示：

UniVPN Client 远程接入终端方案

 Windows windows国家UKey  Linux  MacOS 信创ARM64 信创AMD64 信创MIPS64 信创 LoongArch64  iOS  Android

软件版本	正式版	版本信息	10781.19.0.1214
软件包MD5	exe:7E8FA623CF962276971829B0B41B3049 msi:FC249743913361F9235D2F5B9B7DB225	支持平台	Win7/Win8.1/Win10/Win11/Win Server 2012/2008 兼容软件 X86架构
软件版本更新说明	2026-4-17正式发布10781.19.0.1214		
下载地址	软件包下载 文档下载		

[查看历史版本](#)

2. 安装 UniVPN 客户端

下载完成后，双击安装包进行安装，按照安装向导提示完成安装即可。安装完成后，桌面将出现 UniVPN 快捷方式图标：



四、VPN 连接配置（Windows 客户端）

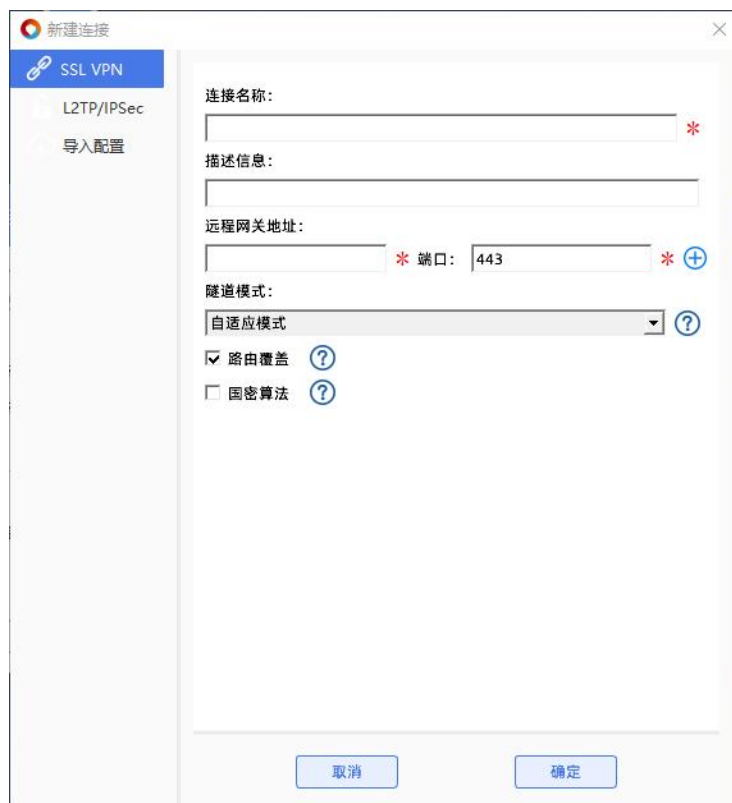
1. 打开 UniVPN 客户端

双击桌面 UniVPN 图标，打开客户端，界面如下：



2. 新建 VPN 连接

点击客户端右上角"+ 新建连接"按钮，进入新建连接配置界面。选择"SSL VPN"类型，按如下信息填写：



(1) 配置电信线路连接

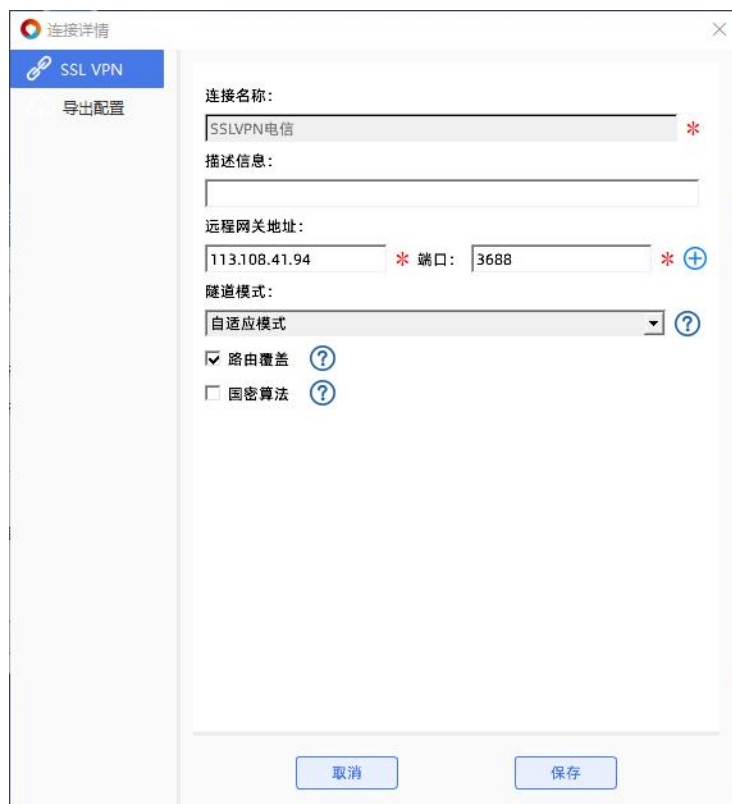
连接名称：SSLVPN 电信

远程网关地址：113.108.41.94

端口：3688

隧道模式：自适应模式

勾选"路由覆盖"，不勾选"国密算法"。填写完成后点击"确定"保存。



The screenshot shows a configuration window titled "连接详情" (Connection Details) for an "SSL VPN" connection. The window has a sidebar with "SSL VPN" and "导出配置" (Export Configuration) options. The main area contains the following fields and controls:

- 连接名称:** A text box containing "SSLVPN电信" with a red asterisk indicating it is required.
- 描述信息:** An empty text box.
- 远程网关地址:** A text box containing "113.108.41.94" with a red asterisk.
- 端口:** A text box containing "3688" with a red asterisk and a blue plus icon.
- 隧道模式:** A dropdown menu set to "自适应模式" with a blue question mark icon.
- 路由覆盖:** A checked checkbox with a blue question mark icon.
- 国密算法:** An unchecked checkbox with a blue question mark icon.

At the bottom of the window are two buttons: "取消" (Cancel) and "保存" (Save).

(2) 配置联通线路连接

连接名称：SSLVPN 联通

远程网关地址：58.250.178.124

端口：3688

隧道模式：自适应模式

勾选"路由覆盖"，不勾选"国密算法"。填写完成后点击"确定"保存。

连接详情

SSL VPN

导出配置

连接名称:
SSLVPN联通 *

描述信息:

远程网关地址:
58.250.178.124 * 端口: 3688 * +

隧道模式:
自适应模式 ?

☒ 路由覆盖 ?

☐ 国密算法 ?

取消 保存

说明：电信和联通线路二选一即可，用户可根据自身网络环境选择合适的线路。建议同时配置两条线路，当一条线路出现故障时，可尝试切换另一个 VPN 链路。

五、信创系统 VPN 连接配置

信创系统（如麒麟 OS、统信 UOS 等）用户同样可以使用 UniVPN 客户端接入测试网 VPN。信创版客户端的操作流程与 Windows 版基本一致，以下为信创系统下的配置说明。

1. 打开 UniVPN 客户端

双击桌面 UniVPN 图标，打开客户端，界面如下：



2. 新建 VPN 连接

打开 UniVPN 客户端后，点击"+ 新建连接"按钮，选择"SSL VPN"类型，按照以下信息填写连接配置。

(1) 配置电信线路连接

连接名称：SSLVPN 电信

远程网关地址：113.108.41.94

端口：3688

隧道模式：自适应模式

勾选"路由覆盖"，不勾选"国密算法"。填写完成后点击"保存"。



连接名称: SSLVPN电信

描述信息:

远程网关地址: 113.108.41.94 端口: 3688

隧道模式: 自适应模式

☒ 路由覆盖

☐ 国密算法

☐ 证书认证

密码:

取消 保存

(2) 配置联通线路连接

连接名称: SSLVPN 联通

远程网关地址: 58.250.178.124

端口: 3688

隧道模式: 自适应模式

勾选"路由覆盖", 不勾选"国密算法"。填写完成后点击"保存"。

连接详情

SSLVPN

导出配置

连接名称：
SSLVPN联通 *

描述信息：

远程网关地址：
58.250.178.124 * 端口： 3688 *

隧道模式：
自适应模式 ?

☒ 路由覆盖 ?

☐ 国密算法 ?

☐ 证书认证

密码

取消 保存

说明：电信和联通线路二选一即可，用户可根据自身网络环境选择合适的线路。建议同时配置两条线路，当一条线路出现故障时可快速切换。

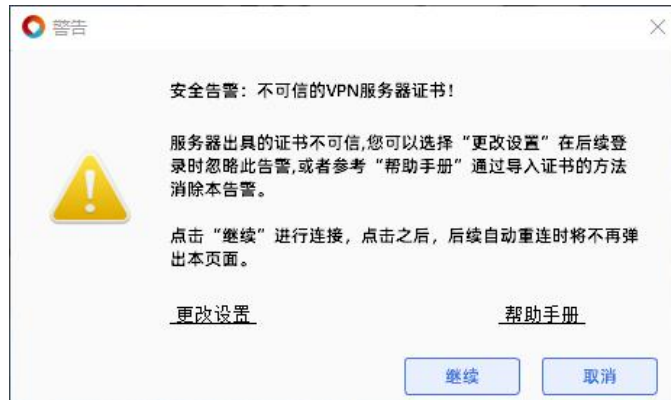
六、VPN 登录

1. 选择 VPN 连接并登录

在客户端右侧"选择 VPN 连接"列表中，点击选择要连接的 VPN 线路（如"SSLVPN 联通"或"SSLVPN 电信"），然后点击左下方"连接"按钮。

2. 处理安全告警

首次连接时，可能会弹出"安全告警：不可信的 VPN 服务器证书！"的提示框。点击"继续"按钮进行连接，后续自动重连时将不再弹出本页面。



3. 输入用户名和密码

在弹出的登录窗口中输入 VPN 账号和密码，点击登录。

4. 接收并输入手机动态验证码

输入用户名和密码后，系统将向您绑定的手机号发送动态验证码短信。在弹出的"动态验证码"窗口中，输入收到的验证码，点击"确定"完成登录认证。验证通过后将提示"登录成功！"。



5. 确认 VPN 连接成功

VPN 连接成功后，客户端界面将显示连接状态信息，包括：VPN 名称、上行/下行数据总量、连接时长、用户名、虚拟 IP 地址（172.18.x.x 开头）、认证状态（登录成功！）等。如下图所示：

连接联通线路成功示例：



连接电信线路成功示例：



信创系统连接电信线路成功示例：



信创系统连接联通线路成功示例：



6. 断开 VPN 连接

测试完成后，点击客户端左下方的"断开连接"按钮即可断开 VPN。使用过程中请保持客户端运行，不要关闭客户端窗口。

七、验证 VPN 连通性测试

VPN 连接成功后，请按以下步骤验证网络连通性：

1. 检查 VPN 虚拟网卡和路由

打开"CMD"命令行窗口，执行 `ipconfig` 命令查看网卡信息，`route print` 命令查看路由信息确认已获取到以 172.18. 开头的 VPN 虚拟 IP 地址。如下图所示：

```
C:\WINDOWS\system32\cmd.exe
(c) Microsoft Corporation。保留所有权利。
C:\Users\pc>ipconfig

Windows IP 配置

未知适配器 本地连接:

    连接特定的 DNS 后缀 . . . . . :
    本地连接 IPv6 地址. . . . . : fe80::5559:3c03:183:2ff4%68
    IPv4 地址 . . . . . : 172.18.3.96
    子网掩码 . . . . . : 255.255.255.255
    默认网关. . . . . :

C:\Users\pc>route print | findstr 172.
    172.18.0.112 255.255.255.255          在链路上
    172.70.0.0   255.255.0.0             在链路上
    172.70.255.255 255.255.255.255        在链路上
    172.200.0.0  255.255.0.0             在链路上
    172.200.255.255 255.255.255.255       在链路上
    224.0.0.0    240.0.0.0              在链路上
    255.255.255.255 255.255.255.255       在链路上
```

信创系统用户可在终端中通过 `ifconfig` 命令查看网卡信息，`ip route` 命令查看路由信息，确认 VPN 隧道路由已正确配置。如下图所示：

```
c:~$ ifconfig
cnem_vnic: flags=4305<UP,POINTOPOINT,RUNNING,NOARP,MULTICAST> mtu 1300
    inet 172.18.0.200 netmask 255.255.255.255 destination 172.18.0.200
    inet6 fe80::6bec:7018:d94:5b42 prefixlen 64 scopeid 0x20<link>
    unspec 00-00-00-00-00-00-00-00-00-00-00-00-00-00-00-00 txqueuelen 500 (未指定)
    RX packets 0 bytes 0 (0.0 B)
    RX errors 0 dropped 0 overruns 0 frame 0
    TX packets 59 bytes 3504 (3.5 KB)
    TX errors 0 dropped 0 overruns 0 carrier 0 collisions 0

c:~$ ip route
default via 172.20.0.2 dev ens32 proto dhcp src 172.20.0.170 metric 100
113.108.41.94 via 172.20.0.2 dev ens32
169.254.0.0/16 dev ens32 scope link metric 1000
172.18.0.200 via 127.0.0.1 dev lo
172.20.0.0/24 dev ens32 proto kernel scope link src 172.20.0.170 metric 100
172.20.0.2 dev ens32 scope link
172.70.0.0/16 via 172.18.0.200 dev cnem_vnic
172.200.0.0/16 via 172.18.0.200 dev cnem_vnic
```

2. Ping 测试

在 CMD 窗口中，对测试环境服务器进行 ping 测试，确认网络连通：

ping 172.200.1.92 (D-COM 服务器)

ping 172.200.1.173 (开放式基金服务器)

ping 172.70.1.170 (易境通交易服务器)

Windows 系统 ping 测试成功示例：

```
正在 Ping 172.200.1.92 具有 32 字节的数据:
来自 172.200.1.92 的回复: 字节=32 时间=10ms TTL=60
来自 172.200.1.92 的回复: 字节=32 时间=8ms TTL=60
来自 172.200.1.92 的回复: 字节=32 时间=8ms TTL=60
来自 172.200.1.92 的回复: 字节=32 时间=7ms TTL=60

172.200.1.92 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 7ms, 最长 = 10ms, 平均 = 8ms
```

```
正在 Ping 172.70.1.170 具有 32 字节的数据:
来自 172.70.1.170 的回复: 字节=32 时间=47ms TTL=58
来自 172.70.1.170 的回复: 字节=32 时间=45ms TTL=58
来自 172.70.1.170 的回复: 字节=32 时间=46ms TTL=58
来自 172.70.1.170 的回复: 字节=32 时间=47ms TTL=58

172.70.1.170 的 Ping 统计信息:
    数据包: 已发送 = 4, 已接收 = 4, 丢失 = 0 (0% 丢失),
往返行程的估计时间(以毫秒为单位):
    最短 = 45ms, 最长 = 47ms, 平均 = 46ms
```

信创系统 ping 测试成功示例：

```
PING 172.200.1.92 (172.200.1.92) 56(84) bytes of data.
64 bytes from 172.200.1.92: icmp_seq=1 ttl=60 time=10.9 ms
64 bytes from 172.200.1.92: icmp_seq=2 ttl=60 time=11.1 ms
64 bytes from 172.200.1.92: icmp_seq=3 ttl=60 time=13.1 ms
64 bytes from 172.200.1.92: icmp_seq=4 ttl=60 time=11.2 ms
64 bytes from 172.200.1.92: icmp_seq=5 ttl=60 time=14.0 ms
64 bytes from 172.200.1.92: icmp_seq=6 ttl=60 time=12.3 ms
```

```
PING 172.70.1.170 (172.70.1.170) 56(84) bytes of data.
64 bytes from 172.70.1.170: icmp_seq=1 ttl=58 time=54.0 ms
64 bytes from 172.70.1.170: icmp_seq=2 ttl=58 time=59.3 ms
64 bytes from 172.70.1.170: icmp_seq=3 ttl=58 time=49.4 ms
64 bytes from 172.70.1.170: icmp_seq=4 ttl=58 time=48.1 ms
64 bytes from 172.70.1.170: icmp_seq=5 ttl=58 time=47.7 ms
64 bytes from 172.70.1.170: icmp_seq=6 ttl=58 time=54.0 ms
```

如能正常收到回复（Reply），则表示 VPN 网络已连通，可以正常进行测试工作。

八、测试环境服务器列表

(1) 新一代联网测试环境

服务名称	主机 IP	端口
D-COM	172.200.1.92	7031/7035

(2) 期权测试环境

服务名称	主机 IP	端口
D-COM	172.200.1.91	7031/7035

(3) 股转仿真测试环境

服务名称	主机 IP	端口
股转结算	172.200.1.98	7043
股转 TCP 接口	172.200.1.97	7044
股转文件	172.200.1.182	7015/7016
股转 CCNET 结算	172.200.1.89	7013/7015

(4) 开放式基金测试环境

服务名称	主机 IP	端口
开放式基金	172.200.1.173	7011

开放式基金	172.200.1.174	7011
开放式基金	172.200.1.72	7011
开放式基金	172.200.1.75	7011
开放式基金	172.200.1.76	7011
开放式基金	172.200.1.77	7011

(5) 易境通交易

服务名称	主机 IP	端口
境内券商	172.70.1.170	7002
境外券商	172.70.1.180	7002

九、常见问题

Q1：连接时弹出"不可信的VPN服务器证书"告警怎么办？

A：这是正常现象，由于测试环境原因暂不验证证书的合法性。直接点击"继续"按钮即可正常连接。后续自动重连时将不再弹出此页面。

Q2：电信和联通线路应该选哪个？

A：请根据您所在网络的运营商选择对应线路，电信用户选择"SSLVPN电信"，联通用户选择"SSLVPN联通"。如不确定，可两条线路都尝试，选择连接速度较快，运行流畅稳定的。

Q3：连接后无法 ping 通测试服务器怎么办？

A：请先确认VPN已连接成功（客户端显示"登录成功！"状态），并通过ipconfig命令确认已获取到172.18.x.x的虚拟IP地址。如仍无法连通，请联系技术服务热线：0755-88666462。

十、技术支持

如在安装配置过程中遇到任何问题，请及时与我司联系：

技术服务热线：0755-88666462

深圳证券通信有限公司

2026 年 7 月 3 日