云安全接入管理系统

用户使用手册

Etaray

杭州奕锐电子有限公司

目　录

一、 系统概述.....3
1.1 访问方式.....4
二、 应用场景说明.....4
三、 准备使用系统.....5
3.1 系统管理员说明.....5
3.2 安全组规则开放.....6
3.3 首次登录系统.....6
四、 系统使用说明.....7
4.1 系统管理员.....7
4.1.1 系统状态.....7
4.1.2 用户管理.....9
4.2 安全管理员.....10
4.2.1 系统状态.....11
4.2.2 系统监控.....11
4.2.3 隧道设置.....13
4.2.4 IPSec 网关.....19
4.2.5 用户管理.....23
4.2.6 网络设置.....23
4.2.7 配置管理.....25
4.2.8 系统设置.....26
4.2.9 软件升级.....28
4.4 审计管理员.....30
4.4.1 日志审计.....30

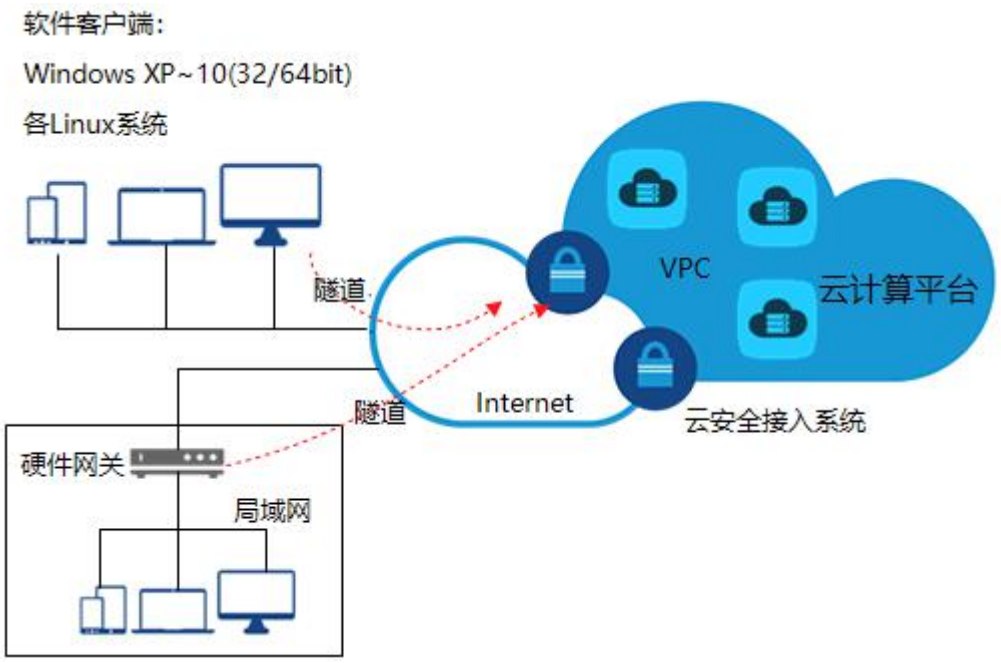
4.4.2 用户管理.....31
4.5 客户端用户.....31
五 客户端软件相关.....34
5.1windows 客户端.....34
5.1.1 软件安装/卸载.....34
5.1.2 客户端配置.....39
5.2 Linux 客户端.....50
5.2.1 检查虚拟网络设备.....50
5.2.2 检查 tun 驱动.....50
5.2.3 无 tun 驱动.....50
5.2.4 导入客户端.....50
5.2.5 执行客户端.....51
5.2.6 查看执行结果.....51
5.2.7 开机自启设置.....51
5.3 客户端配置（MAC OS X）.....52
5.3.1 软件配置.....53
5.4 手机客户端配置.....55
5.4.1 Android 系统.....55
5.4.2 IOS 系统.....56
5.4.3 MAC OSx 系统自带 APP.....57

一、 系统概述

本系统可以理解成虚拟专用网络（Virtual Private Network，以下简称 VPN）的云化产品部署形态，用于在远端用户和云端虚拟私有云（Virtual Private Cloud，以下简称 VPC）之间建立一条安全加密的公网通信隧道。当您作为远端用户需要访问 VPC 的业务资源时，您可以通过 VPN 连通 VPC。

默认情况下，在虚拟私有云(VPC) 中的弹性云服务器无法与您自己的数据中心或私有网络进行通信。如果您需要将 VPC 中的弹性云服务器和您的数据中心或私有网络连通，可以通过本系统的安全互联来实现。本系统的 VPN 连接是通过加密技术，将线下本地网络与云端 VPC 连接，使本地数据节点与虚拟私有云通信，更快速、安全的构建混合云环境。

VPN 组网如下图所示：



1.1 访问方式

本系统的配置是通过 WEB 配置界面完成，推荐使用新版 Chrome 浏览器进行登录配置。

二、 应用场景说明

（1）客户端软件访问 VPC：此场景是最常见的用户场景，解决安装客户端软件的机器或者移动设备安全接入云端 VPC。客户端软件支持 windows 系统、各版本的 linux 系统，手机端（安卓、苹果）可使用自带的 VPN 功能进行接入。

（2）线下局域网访问 VPC：此场景也较为典型，通过在线下某数据中心或者局域网内部署一台硬件网关设备与云端安全接入系统建立隧道，使得局域网与 VPC 连通。硬件网关支持奕锐自研网关产品以及第三方网关产品（如：华为路由器/防火墙、华三路由器/防火墙、深信服 VPN 网关、Sonicwall 防火墙包括其他各种支持标准 VPN 模块的工业路由器等）。

（3）客户端访问客户端：此场景一般用于移动客户端访问线下局域网内的某台应用服务器，这台应用服务器与移动客户端都通过隧道接入后，客户端之间可以用虚拟 IP 地址互访。

（4）客户端软件访问线下局域网：此场景一般是为了解决移动办公客户端接入公司内网的场景。云安全接入系统部署在云端，移动办公的客户端软件与公司内网的硬件网关都与云安全接入系统建立隧道后，客户端软件可通过隧道访问至公司内网。注：此场景中的网关设备仅指奕锐自研硬件网关。

（5）混合云安全互联：此场景一般是为了解决多局域网安全互联的场景。云安全接入系统部署在云端，公司 A 的内网硬件网关与公司 B 的内网硬件网关都与云安全接入系统建立隧道后，公司 A 与公司 B 的内网即可安全互联。注：此场景中的网关设备仅指奕锐自研硬件网关。

三、 准备使用系统

3.1 系统管理员说明

管理员类型	功能说明	账户名、口令
系统管理员	主要负责管理其他权限的管理员（增加、删除、编辑管理员账户）	admin etapublic（缺省）
安全管理员	主要负责 VPN 隧道的相关配置	由系统管理员开户，口令可自行修改
审计管理员	主要负责审计安全日志、系统操作日志等	由系统管理员开户，口令可自行修改
客户端用户	可以查看系统帮助或者下载对应的客户端，同时还允许修改登录口令	“隧道设置”中配置的客户端账户

3.2 安全组规则开放

一般情况下，系统的使用有以下几个相关的协议、端口需要在云控制台的安全组规则中开放：

序号	协议	端口	说明
1	TCP	443	WEB 管理端口
2	UDP	25500	VPN 接入端口
3	UDP	500 4500	移动端的 VPN 接入端口
4	TCP	22	远程终端管理端口：部署、升级、后台维护管理

3.3 首次登录系统

WEB 管理地址：https://x.x.x.x （一般情况下，x.x.x.x 是指系统的外网 IP 地址）。缺省管理员登录信息：系统管理员（用户名：admin 口令：etapublic）。

注意：

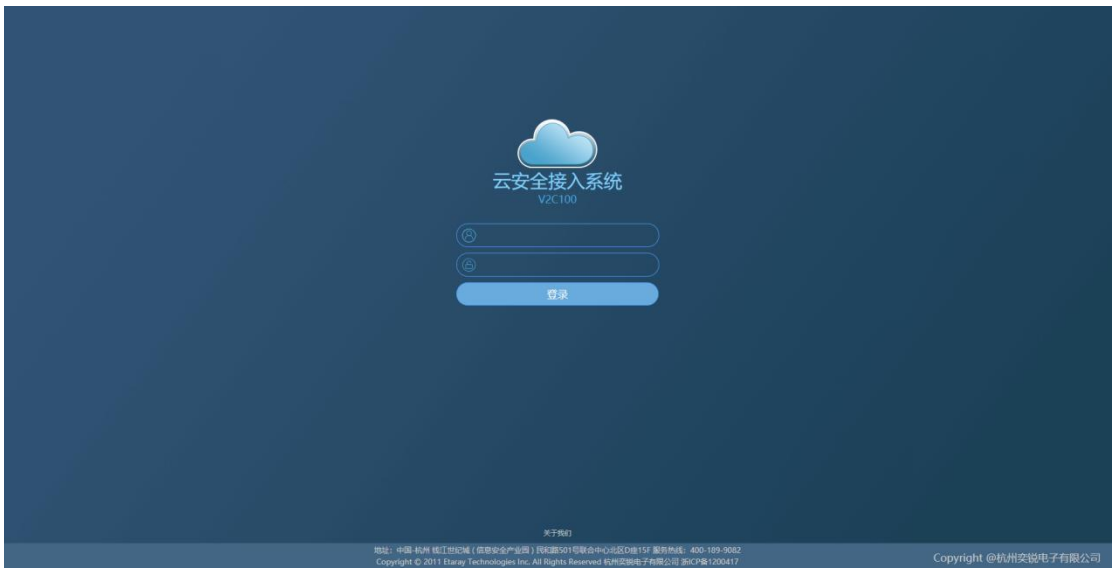
1. VPN 镜像的缺省 web 管理端口为 TCP 443 端口，管理员需要在云端控制台的安全组规则的入方向规则中增加 TCP 443（web 管理端口），否则通过外网无法进行 web 管理；

2. 推荐使用谷歌浏览器；

四、 系统使用说明

4.1 系统管理员

在浏览器中输入服务器 IP：https://×.×.×.×默认系统管理员 admin，首次登陆密码：etapublic，首次登陆进去后，要求修改缺省口令。

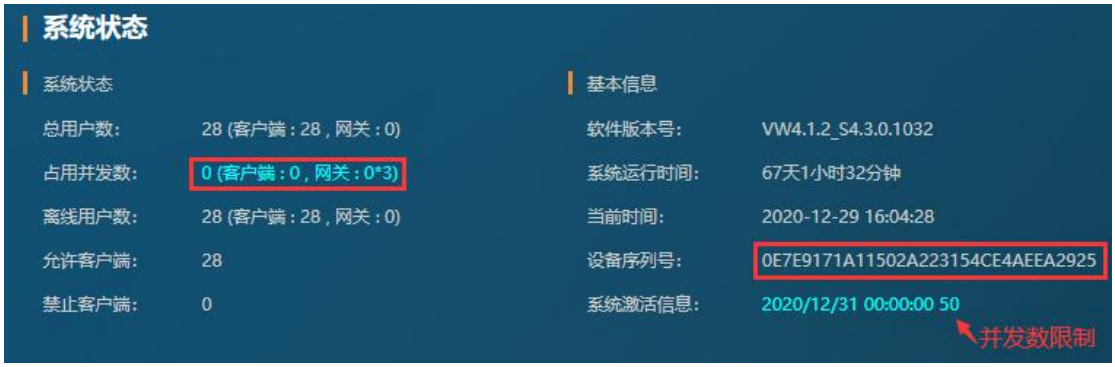


4.1.1 系统状态

系统管理员登录，可查看服务器基本信息和系统状态，可开启/关闭 VPN 服务。

开启、关闭 VPN 服务，点击位置如下图所示：

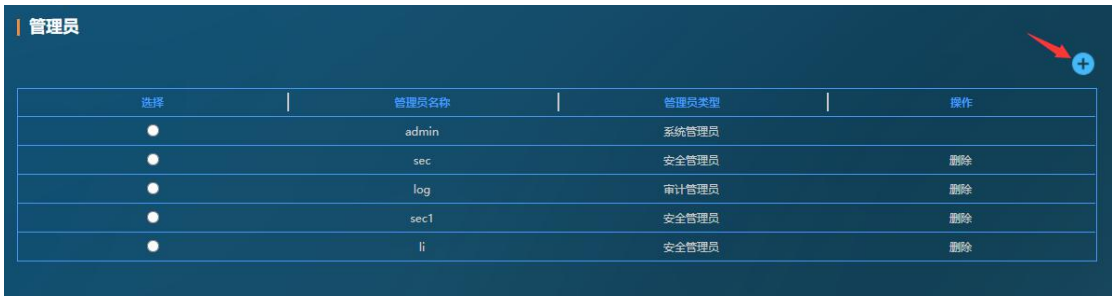
设备序列号是指当前系统主机的硬件特征码，如下图所示。系统激活的时候，需要将该串设备特征码提交给厂商，厂商根据此特征码生成 license 文件。在“系统设置”菜单中提交该文件即可完成激活，参考 4.2.8 节。在本系统中，每个客户端软件在线将占用一个并发数，每个硬件网关在线将占用三个并发数。并发数总数不能超过 license 的并发总数。



4.1.2 用户管理

系统账户下的用户管理模块可以实现对管理员的新增和删除、修改。

点击新增图标，在弹窗内填写账户名和口令，选择用户类型（安全管理员、日志管理员）点击新增即可创建新的管理账户。



选中某个账户，即可在弹出框内对选中的账户进行口令和类型的修改。

点击删除，即可删除选中的账户。

4.2 安全管理员

安全管理员主要负责完成系统的安全功能设置，包括网络相关、隧道相关、升级相关的配置管理。系统管理员 admin 可以对安全管理员进行开户（参考 4.1.2 节），开户完成后就可以通过安全管理员的

账户、口令登录系统进行配置。主要菜单包含：系统状态、隧道设置、IPSec 网关、网络设置、配置管理、软件升级。

4.2.1 系统状态

详见4.1.1 系统状态。

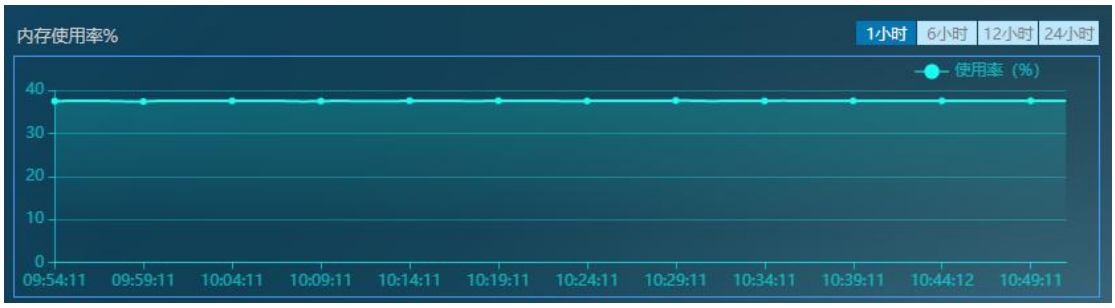
4.2.2 系统监控

系统监控页主要监控“CPU 使用率%”、“内存使用率%”、“物理网卡流量图”、“虚拟网卡流量图”以及“隧道并发月趋势图”。其中前 4 项提供的历史数据为 24 小时。

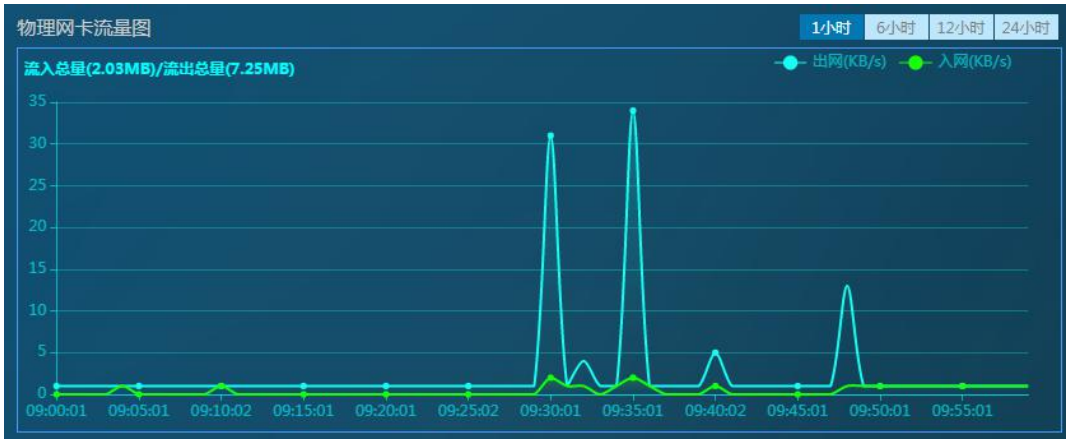
CPU 使用率的实时监控，监控时间参数为 1 小时、6 小时、12 小时和 24 小时。

内存使用率的实时监控，监控时间参数为 1 小时、6 小时、12 小

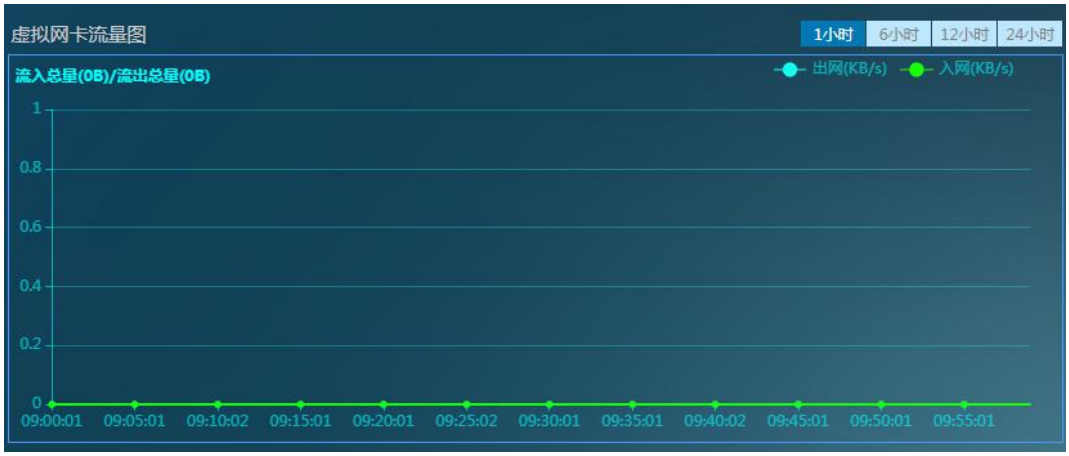
时和 24 小时。



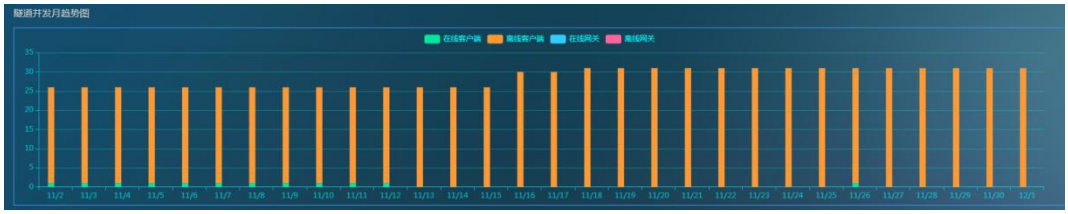
物理网卡流量图的实时监控，监控时间参数为 1 小时、6 小时、12 小时和 24 小时。



虚拟网卡流量（VPN 流量）图的实时监控，监控时间参数为 1 小时、6 小时、12 小时和 24 小时。



隧道并发月趋势图的实时监控。监控参数为最近的一个月。



4.2.3 隧道设置

“隧道设置”菜单共有三个选项卡，分别为：客户端、网关、访问策略。对应的功能如下表所示：

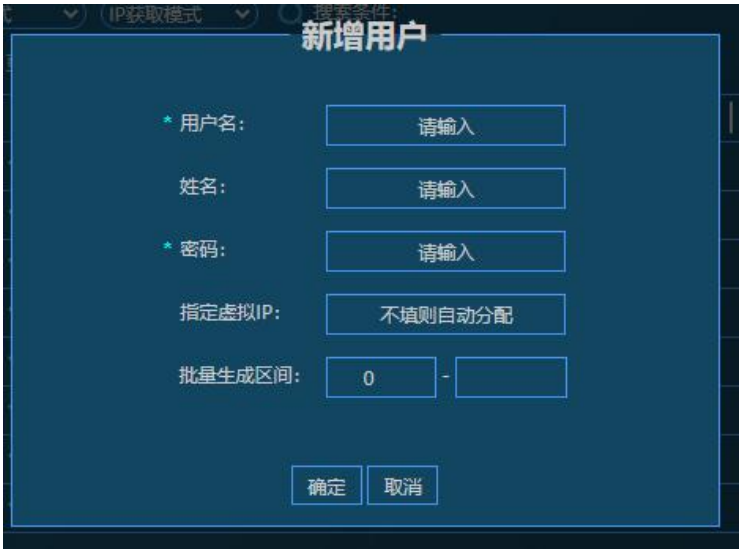
选项卡	功能说明
客户端	创建 VPN 客户端的接入账户（包括 PC 端和移动端）
网关	创建奕锐自研硬件网关接入账户
访问策略	设置客户端或硬件网关的白名单并配置这些白名单通过隧道后允许访问的网络资源

4.2.3.1“客户端”设置

新增客户端账户，点击增加按钮，如下图：

如下图所示，输入用户名、姓名（可选）、密码等信息。可指定虚拟 IP 地址（如不填写该项，则系统在客户端建立隧道后会自动为客户端账户分配虚拟 IP 地址）。可批量生成多个账户（用户名后面

直接加序号的方式）。



安全管理员点击重置按钮，即可重置客户端账户的口令为“123456”，如下图所示：

VPN 客户端接入的认证模式支持列表如下：

认证模式	支持用户类型
用户名、口令	Windows 客户端 Linux 客户端 MacOSx 客户端 Android、IOS 移动客户端
机器码	Windows 客户端（详见机器码说明）

口令+机器码	Windows 客户端（详见机器码说明）
口令+OTP	Windows 客户端
U 盾	Windows 客户端

如果选择了“口令+OTP”的认证方式，则会产生一个二维码，通过在手机上安装 OTP 验证器的 APP，即可对这个二维码进行扫描并上产生动态口令码）。

通常身份验证器的 APP 可选用：

（1）“谷歌身份验证器——Google_Authenticator”；

（2）“微软身份验证器——Microsoft Authenticator”；

推荐使用微软的身份验证器，可在手机应用市场中搜索安装并下载使用。具体使用可参考 5.1.2.2 节说明。

如果选择了“机器码”或者“口令+机器码”的认证方式，需要

把安装 windows 客户端的 PC 机的机器码拷贝进去，并点击提交按钮才能生效。如下图所示：

切换 IP 获取模式，不管是由动态 IP 切换到静态 IP，还是由静态 IP 切换到动态 IP，都需要点击“提交”按钮才能生效。

“截止日期”是指允许某个客户端账户在某个时间节点之前允许建立 VPN 隧道，设置生效也需要点击“提交”按钮。

在“动作”一栏中，“禁止”是指不允许该客户端账户建立 VPN 隧道(如果当前账户已经在线，点击禁止并不能立即停止该账户隧道，而是禁止该账户重新建立隧道）。建立账户的缺省策略是“允许”。

“登录次数”可以进行手工重置成 0，点击位置如下图所示：

系统在“客户端”选项卡中提供了针对客户端账户的“操作列表”，具体说明如下表：

操作列表	说明
批量导入	具体请参考“批量导入”小节说明
下载导入结果	批量导入操作完成后，可点击“下载导入结果”查看批量导入的统计结果
批量允许	勾选对应账户，可进行“批量允许”操作
批量禁止	勾选对应账户，可进行“批量禁止”操作
批量删除	勾选对应账户，可进行“批量删除”操作
清空全部用户	清空所有用户
导出用户列表	下载 Excel 格式的所有用户
删除登录次数	勾选对应账户，点击“删除登录次数”即可清零登录次数；

4.2.3.2 客户端账户批量导入

创建 excel 文件，文件内容示例如下：

LoginID	Names	Password	VirtualIP	AuthMode
User1	张三	123456	192.168.88.2	0
User2	李四	123456	192.168.88.3	1

其中，AuthMode 为 0，代表认证模式为口令模式

AuthMode 为 1，代表认证模式为 U 盾模式

AuthMode 为 2，代表认证模式为机器码模式

AuthMode 为 3，代表认证模式为口令+机器码模式

AuthMode 为 4，代表认证模式为口令+OTP 模式

4.2.3.3“网关”设置

新增网关（是指奕锐自研硬件网关系统）操作中，需要填写网关名、密码、网关的保护子网等信息，如下图所示。可指定虚拟 IP 地址，如果不填则系统自动分配。

4.2.3.4“访问策略”设置

访问策略主要设置客户端或硬件网关的白名单并配置这些白名单

通过隧道后允许访问的网络资源。

访问策略类型有四种：客户端访问中心，客户端访问硬件网关，网关访问中心，网关访问网关。（具体应用场合请参考：第二节、应用场景说明）

其中，单一地址可配置成：x.x.x.x/255.255.255.255。

4.2.4 IPSec 网关

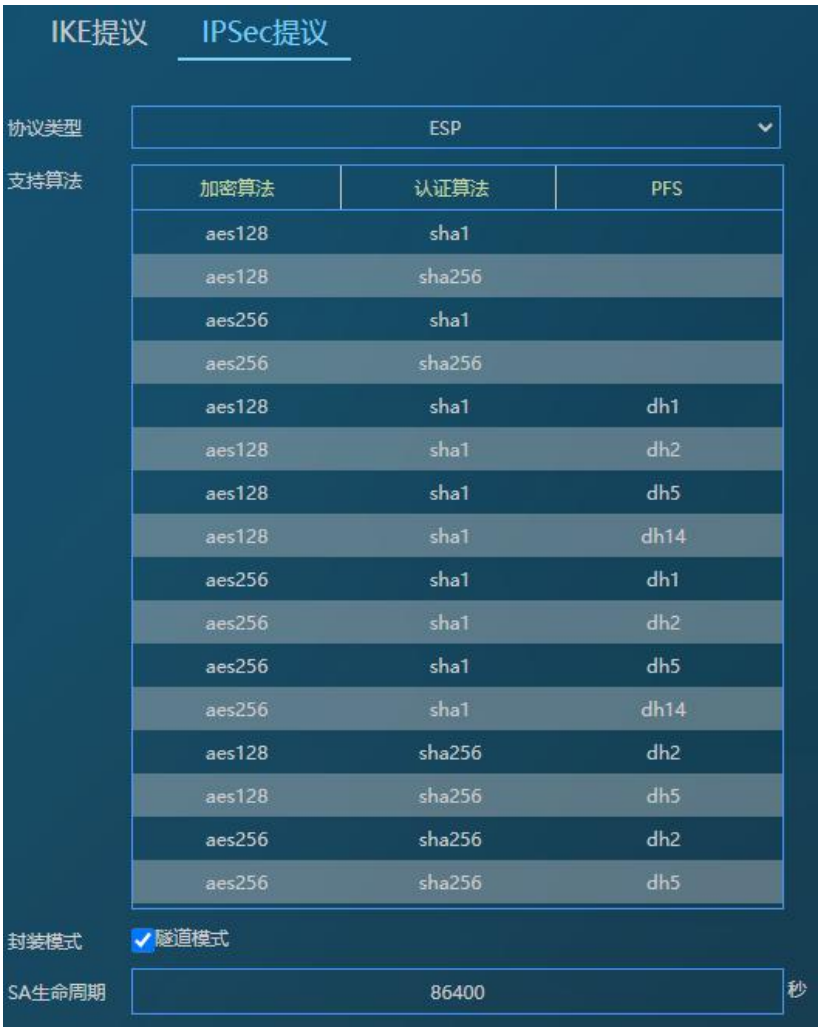
IPSec 网关在本系统中是指支持标准 VPN 模块的第三方网关产品（如：华为路由器/防火墙、华三路由器/防火墙、深信服 VPN 网关、Sonicwall 防火墙包括其他各种支持标准 VPN 模块的工业路由器等）。

新增 IPSec 网关配置如下图所示，设置节点网关的 ID 号、节点保护子网以及中心保护子网。

隧道基本配置中可以对中心 ID 号进行设置，缺省为：vpn.etaray.com。接入地址和预共享密钥在“系统设置”菜单中进行设置（请参考 4.2.8 节）

IKE 提议算法支持列表查看：

IPSec 提议算法支持列表查看：



第三方网关配置参数示例：

- **第一阶段：**

  对端是固定 IP：一般是指云安全接入系统的外网 IP（EIP）

  认证方式：预共享密钥（在“系统设置”菜单中设置）

  ISAKMP 时间:3600 秒

  重试 10 次

  支持模式：野蛮模式

  DH：MODP1024(2)

  本端身份类型：FQDN

  本端 ID：与“IPSec 网关”中配置的“网关 ID”保持一致

  对端身份类型：FQDN

  对端 ID：与“IPSec 网关”中配置的“中心 ID”保持一致

  启用 DPD：检测间隔 30s，超时次数 5

  算法：SHA-1,AES

- **第二阶段：**

  入站策略地址段:与“IPSec 网关”中配置的“中心保护子网”保持一致

  出站策略地址段:与“IPSec 网关”中配置的“节点保护子网”保持一致

  算法：SHA-1,AES

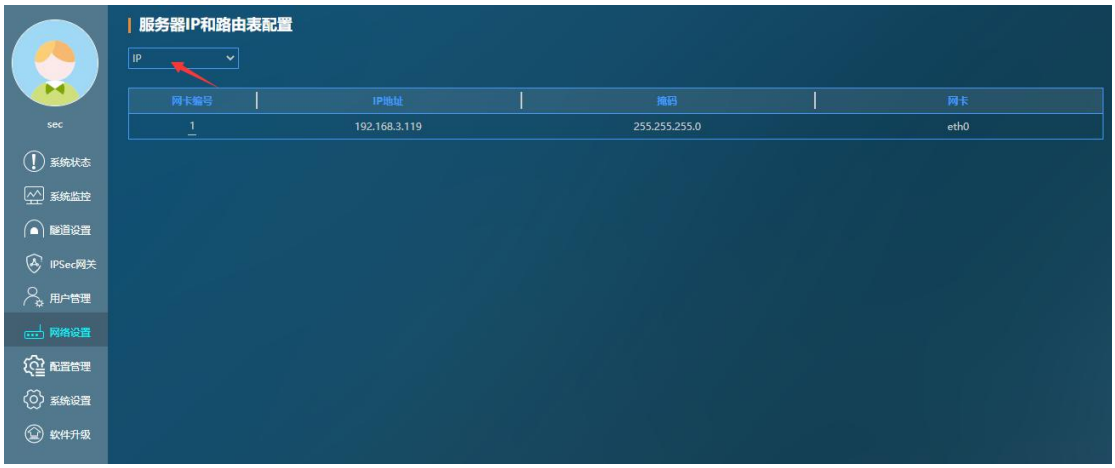
4.2.5 用户管理

选择“用户管理”，原密码验证通过后，可点击“修改”设置安全管理员的新密码。

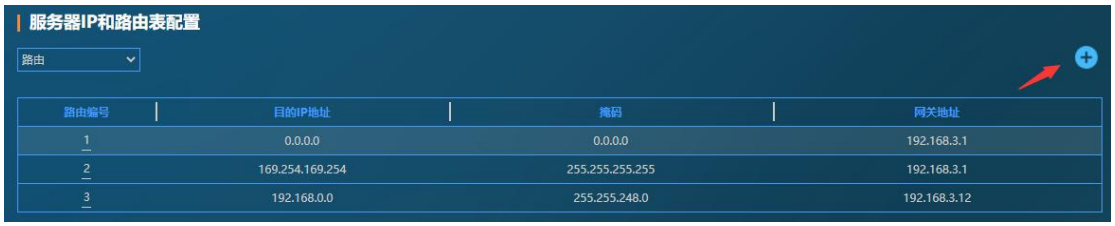
4.2.6 网络设置

网络设置包含服务器 IP 和路由配置.

选择“IP/路由设置”下拉栏选择“IP”，点击网卡编号，修改 IP 地址。



可增加路由，如下图所示：



点击“路由编号”可对路由进行编辑或者删除。

4.2.7 配置管理

备份数据库文件，可将系统配置备份到本地或服务器。

数据恢复方式，可以从服务器恢复数据库，也可以从本地导入数据库文件恢复到系统。

注意：1.本功能在恢复备份数据的同时，将全部覆盖原有数据，请确定是否需要恢复。

2.数据恢复功能只能恢复由本系统导出的数据文件，其他软件导出格式无法识

别。

3.从本地恢复数据需要服务器支持文件上传并保证数据尺寸小于允许上传的上限。

4.2.8 系统设置

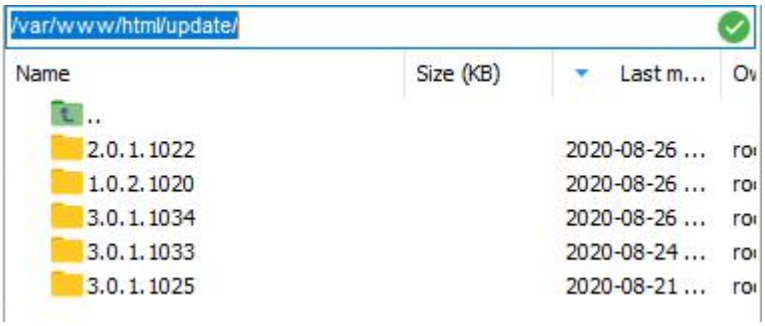
配置参数	说明
服务端外网 IP 地址	是指 VPN 服务器的外部 IP 地址
接入端口	默认为 25500，参考 3.2 节
客户端虚拟 IP 池	缺省为： 192.168.88.1/255.255.255.0 虚拟 IP 池是指 VPN 客户端接入隧道后，系统会自动从虚拟 IP 池中获取空闲 IP 地址下发给客户端
客户端 DNS 地址	配置此项可下发内网 DNS 服务器，配合客户端软件的桥接模式使用
安全 WEB 服务端口	WEB 管理端口： https://x.x.x.x:port 缺省为 443 端口，如果修改需要重启服务器才能生效
WEB 代理服务	开启该项服务后，允许 Windows 系统通过代理模式浏览网页。 举例： （1）在“系统设置”页中开启“WEB 代理服务”；

	（2）为某客户端账户配置0.0.0.0/0.0.0.0的访问策略，参考4.2.3.4节说明； （3）Windows客户端启动隧道； （4）Windows浏览器会自动设置代理地址，此时浏览器所有流量都通过VPN服务器；
外部日志服务器地址	缺省无需填写此项配置。如果需要日志重定向功能，可配置外部syslog服务器地址
预共享密钥	即第三方IPSec VPN网关或者手机移动端VPN模块接入系统需要设置的预共享密钥
系统激活文件	激活文件获取方式： （1）在云市场搜索奕锐云安全接入VPN系统购买激活码； （2）在安全管理员登陆后，“系统设置”菜单中，点击“获取测试激活文件按钮”，可填写手机、邮箱获取测试激活文件；

4.2.9 软件升级

“软件升级”是系统针对 windows 客户端的远程升级功能。可通过 SSH 软件将需要升级的文件上传到系统/var/www/html/update/目

录下，以版本号命名子目录并将升级文件上传至对应的升级目录中，如下图所示：

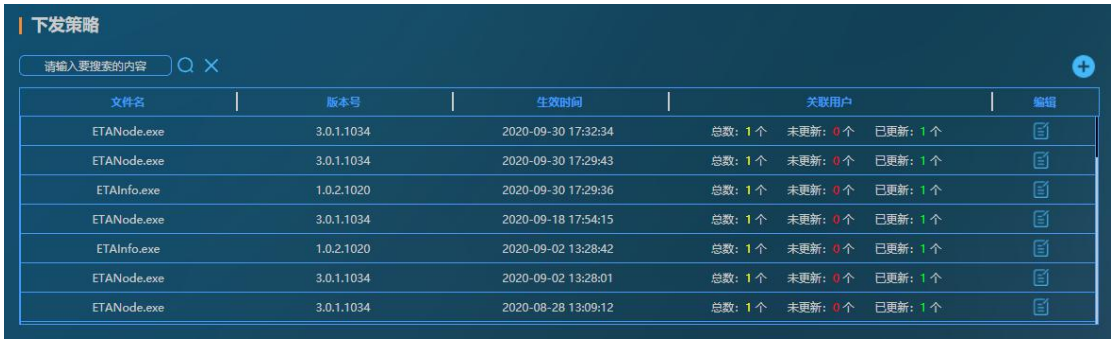


新增升级策略，如下图：

选择版本号后自动列出升级文件，点击新增。

下发升级策略，首先选择升级策略，输入生效时间以及哪些客户端账户需要升级，如下图所示：

策略下发并到达生效时间后，客户端后续上线都会自动完成软件更新。



4.4 审计管理员

审计管理员主要负责查看系统操作日志和安全日志以及日志的备份。

4.4.1 日志审计

审计管理员可根据条件筛选出后台日志或者操作日志信息进行审计查看。

系统支持下载日志，如下图所示，首先选择日志类型，然后点击“日志备份”即可导出 excel 类型的日志文件。

4.4.2 用户管理

选择“用户管理”可修改审计管理员密码。可参考 4.2.5 节。

4.5 客户端用户

在安全管理员创建客户端账户后（请参考 4.2.3.1 节），客户端账户也可登录 WEB 管理界面，可下载对应版本的客户端软件以及在线阅读帮助文档，同时还能修改用户口令。

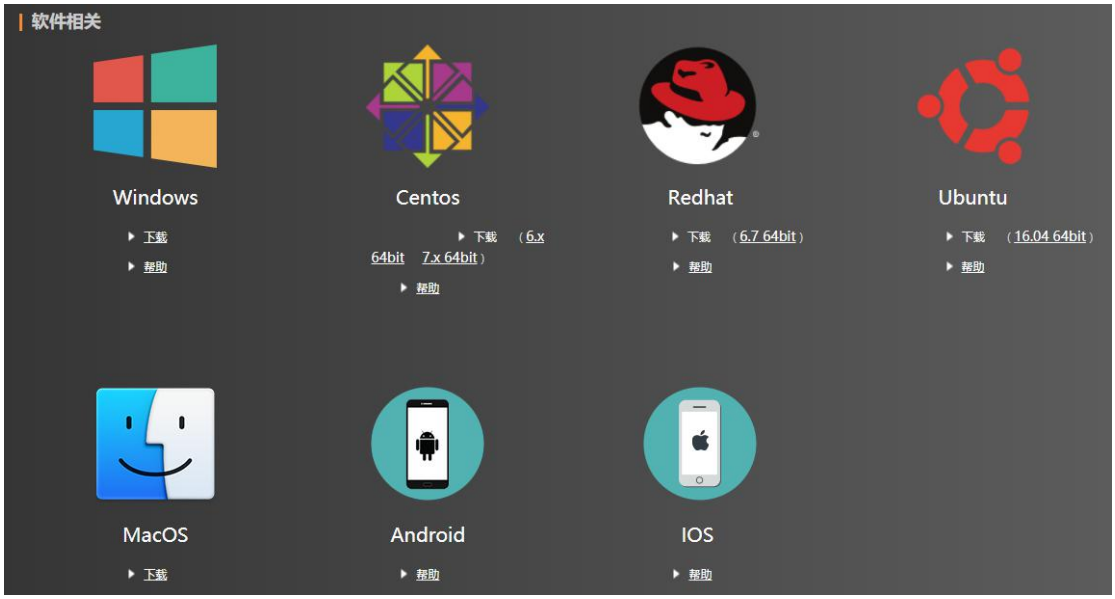
登录界面切换，在首页右上角处点击，如下图所示：

切换成功后，界面如下图所示：

登录成功后，界面如下图所示：

在”用户管理“中，可以修改自己的口令。

“软件相关”菜单中，支持下载 Windows、Linux（Centos、Redhat、Ubuntu）以及 MacOS 等各版本的客户端软件以及相关帮助文档。



五 客户端软件相关

5.1windows 客户端

5.1.1 软件安装/卸载

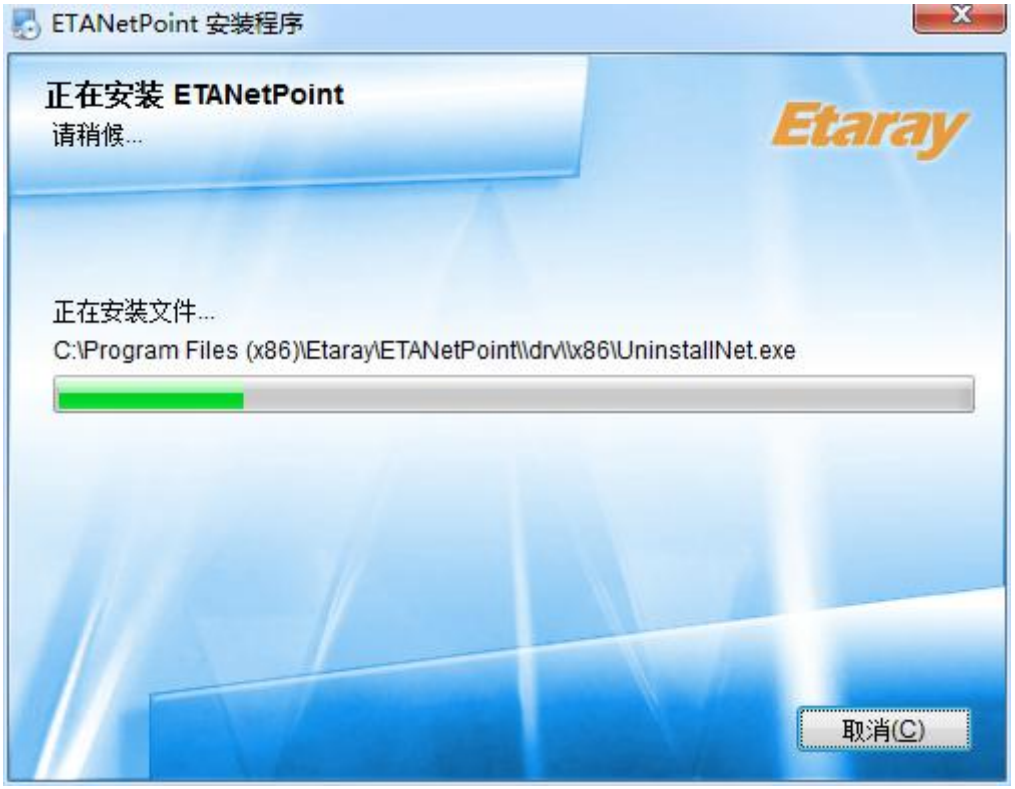
双击 

图标开始安装 Windows 客户端，根据引导完成安装。


ETANetPoint 安装程序
Etaray
欢迎
欢迎使用 ETANetPoint 3.2.0 安装程序。
强烈建议您在继续该安装之前，退出所有 Windows 程序。
如果您有任何其他程序正在运行，请单击"取消"，关闭程序，然后再次运行该安装程序。
否则，请单击"下一步"继续。
杭州奕锐电子有限公司
www.etaray.com
< 返回(B)
下一步(N) >
取消(C)


ETANetPoint 安装程序
许可协议
请仔细阅读以下许可协议。
Etaray
软件许可协议
重要须知：杭州奕锐电子有限公司在此特别提醒用户认真阅读本《软件许可协议》—用户应认真阅读本《软件许可协议》(下称《协议》)中各条款，包括免除或者限制云安全接入客户端软件责任的免责条款及对用户的权利限制。请您审阅并接受或不接受本《协议》（未成年人应在法定监护人陪同下审阅）。除非您接受本《协议》条款，否则您无权下载、安装或使用本"软件"及其相关服务。您的安装使用行为将视为对本《协议》的接受，并同意接受本《协议》各项条款的约束。
我同意该许可协议的条款
我不同意该许可协议的条款
< 返回(B)
下一步(N) >
取消(C)

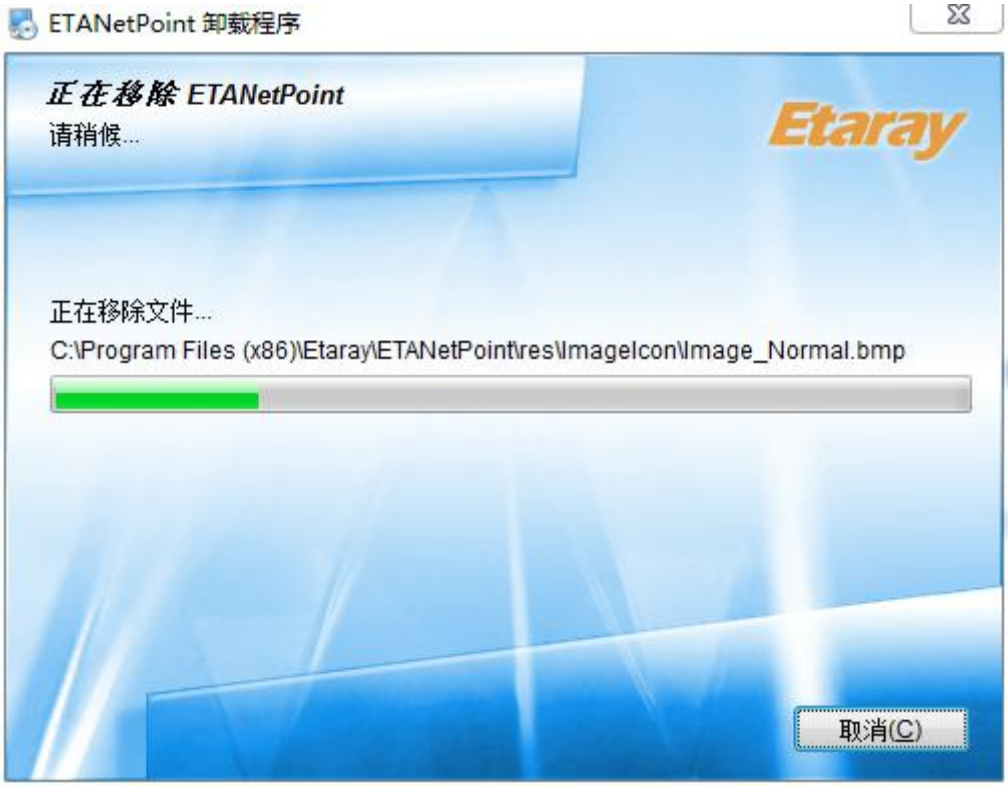

ETANetPoint 安装程序
安装文件夹
您想将 ETANetPoint 安装到何处?
Etaray
软件将被安装到以下列出的文件夹中。要选择不同的位置，键入新的路径，或单击"更改"浏览现有的文件夹。
将 ETANetPoint 安装到:
C:\Program Files (x86)\Etaray\ETANetPoint
更改(H)...
所需空间: 7.52 MB
选定驱动器的可用空间: 57.17 GB
< 返回(B)
下一步(N) >
取消(C)


ETANetPoint 安装程序
正在安装 ETANetPoint
请稍候...
Etaray
正在安装文件...
C:\Program Files (x86)\Etaray\ETANetPoint\\drv\\x86\UninstallNet.exe
取消(C)

卸载软件

在开始菜单选择“卸载云安全接入客户端”，根据引导完成卸载。

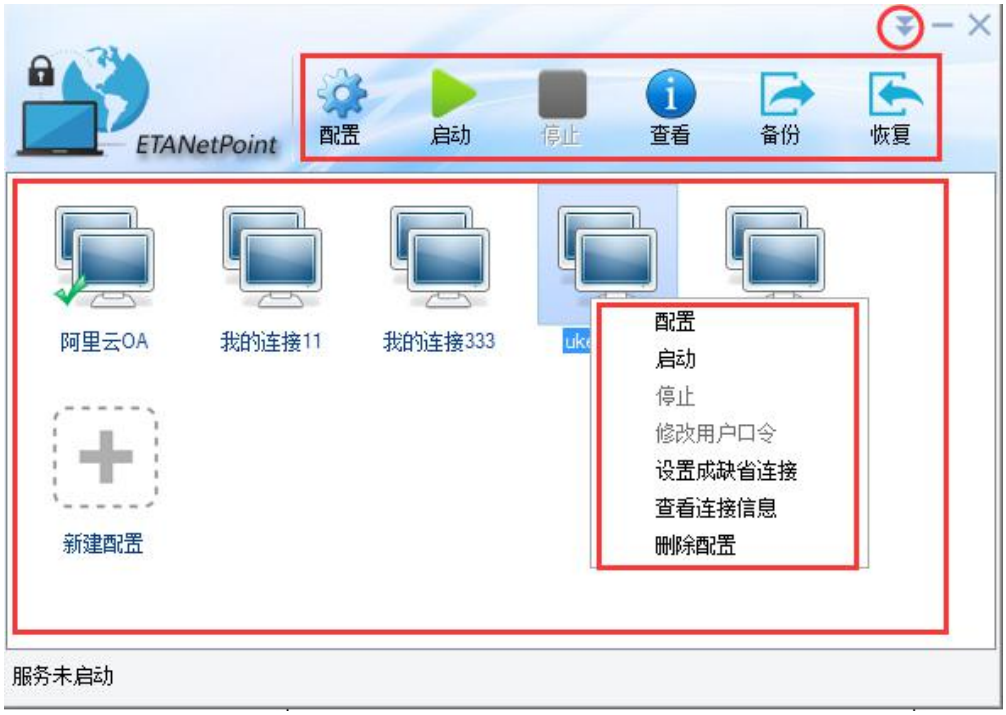

ETANetPoint 卸载程序
Etaray
卸载 ETANetPoint
该程序将卸载 ETANetPoint 3.2.0。
如果 ETANetPoint 当前正在运行，继续卸载之前请将其关闭。
否则，请单击"下一步"继续。
杭州奕锐电子有限公司
www.etaray.com
< 返回(B)
下一步(N) >
取消(C)


ETANetPoint 卸载程序
正在移除 ETANetPoint
请稍候...
Etaray
正在移除文件...
C:\Program Files (x86)\Etaray\ETANetPoint\res\ImageIcon\Image_Normal.bmp
取消(C)

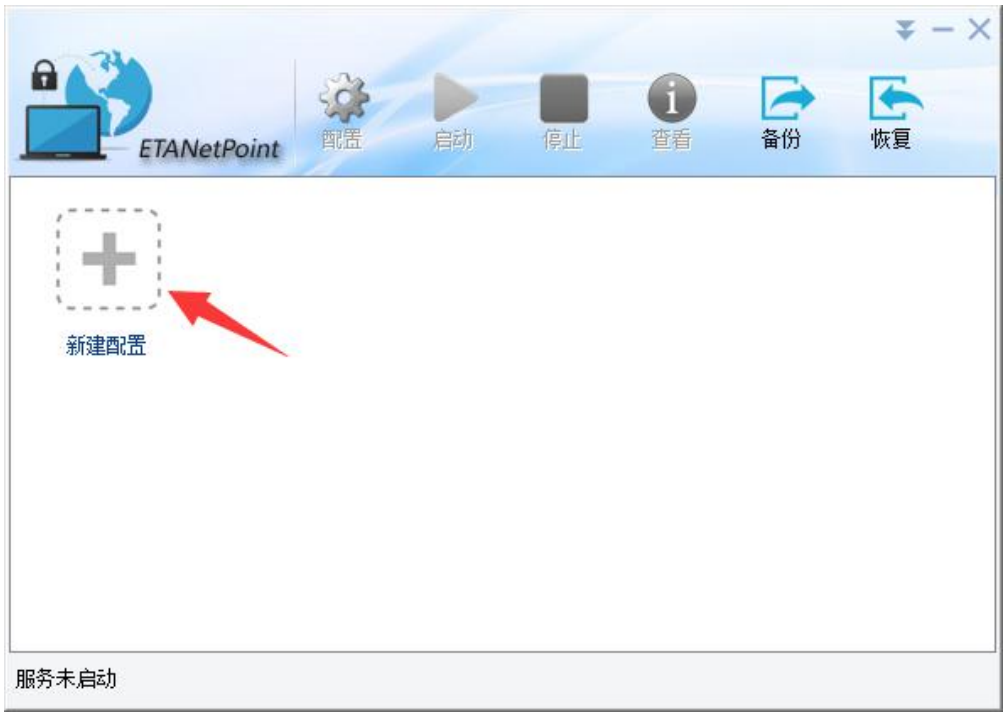
5.1.2 客户端配置

双击打开云安全接入管理系统 Windows 客户端。

客户端配置界面功能区大致分成：常用菜单、主窗口、右键菜单、系统菜单四个部分，如下图所示：


ETANetPoint
配置
启动
停止
查看
备份
恢复
阿里云OA
我的连接11
我的连接333
新建配置
配置
启动
停止
修改用户口令
设置成缺省连接
查看连接信息
删除配置
服务未启动

新增配置

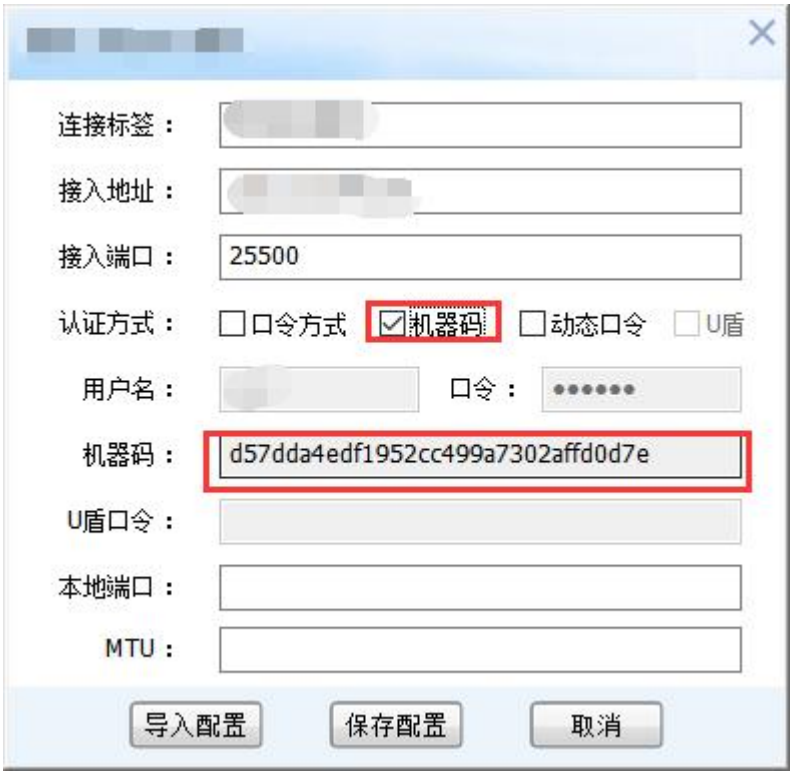

ETANetPoint
配置
启动
停止
查看
备份
恢复
新建配置
服务未启动

连接标签	自定义名称
接入地址	VPN 服务器的地址
接入端口	VPN 服务器的接入端口
用户名	VPN 服务器上配置的账户
认证方式	口令方式（缺省方式） 机器码（可单独勾选，也可与口令方式一同勾选） 动态口令（需配合口令方式一起勾选） U 盾认证方式
口令	账户密码
U 盾口令	如果使用 U 盾认证，需要输入 U 盾口令（U 盾认证和口令认证只能选择其中一种）
本地端口	可选设置，本地数据端口

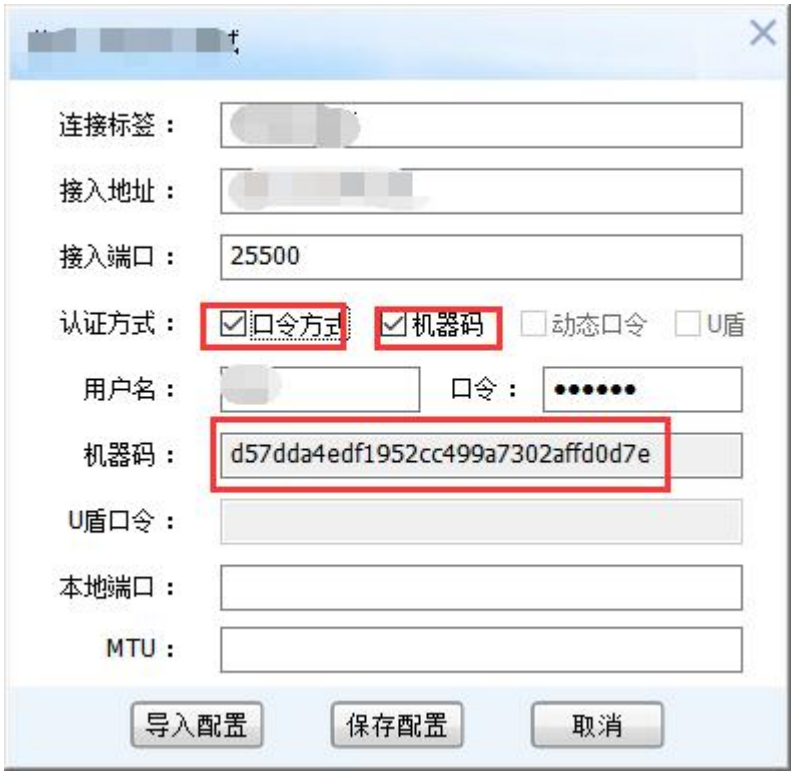
MTU	可选设置虚拟网卡 MTU 设置

5.1.2.1 机器码说明

（1）如果选择“机器码”认证模式，要求软件使用者在配置窗口拷贝出机器码，并将该机器码告知后台管理员进行配置。

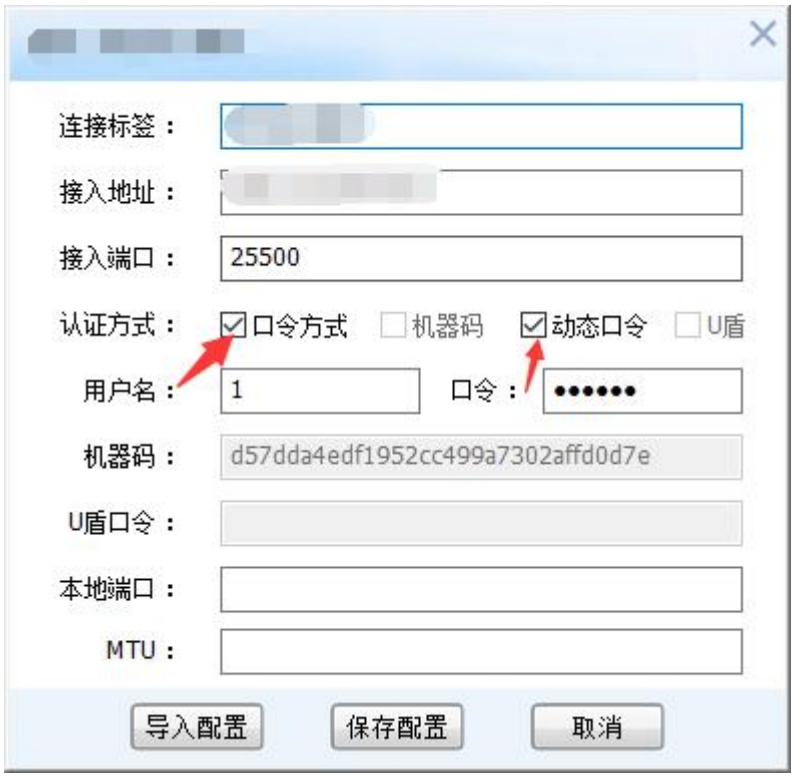


（2）如果选择“口令+机器码”模式，则客户端软件在首次建立隧道的时候会自动提交机器码至后台系统。



5.1.2.2 动态口令说明

在客户端设置页里面选择口令+动态口令模式。



点击“启动”后，提示需要输入动态口令。

打开 OTP 的手机 APP，获取到对应账户的动态口令码填入，即可完成隧道建立。OTP APP 添加账户的过程如下：

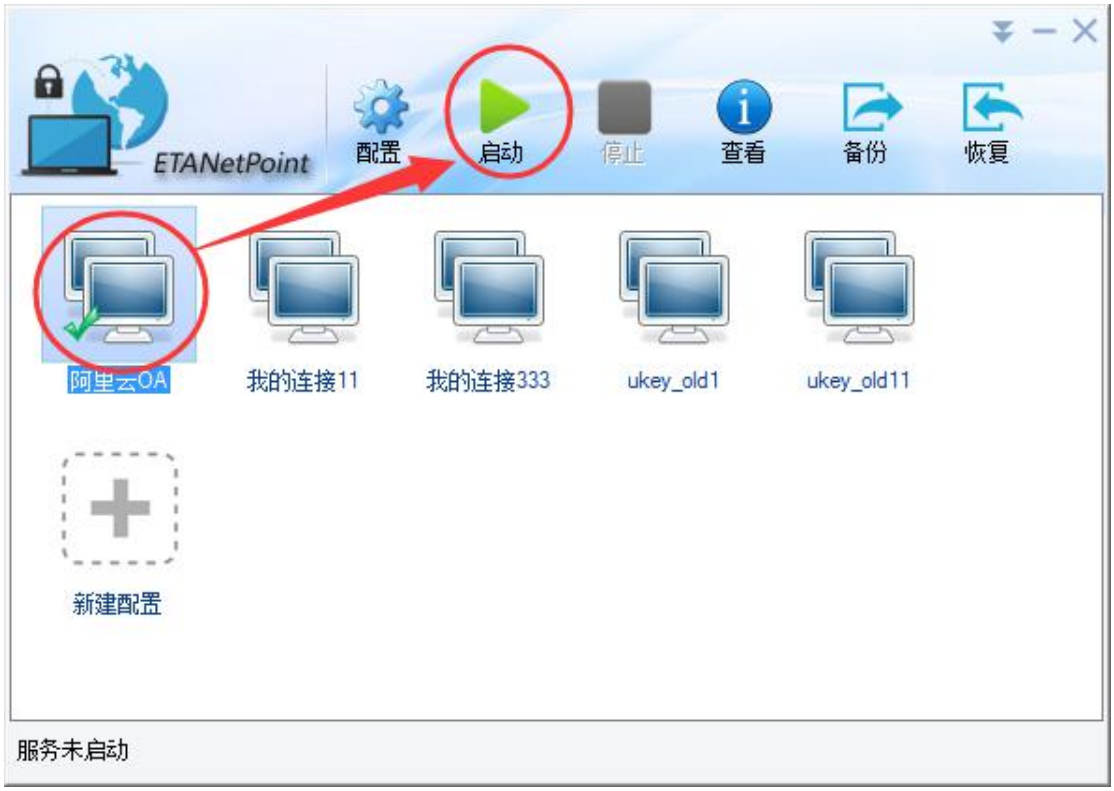
（1）VPN 后台配置成“口令+OTP”模式从而生成二维码；

（2）通过 APP 扫描后即可添加该账户（以下截图以 Microsoft Authenticator 为例）。

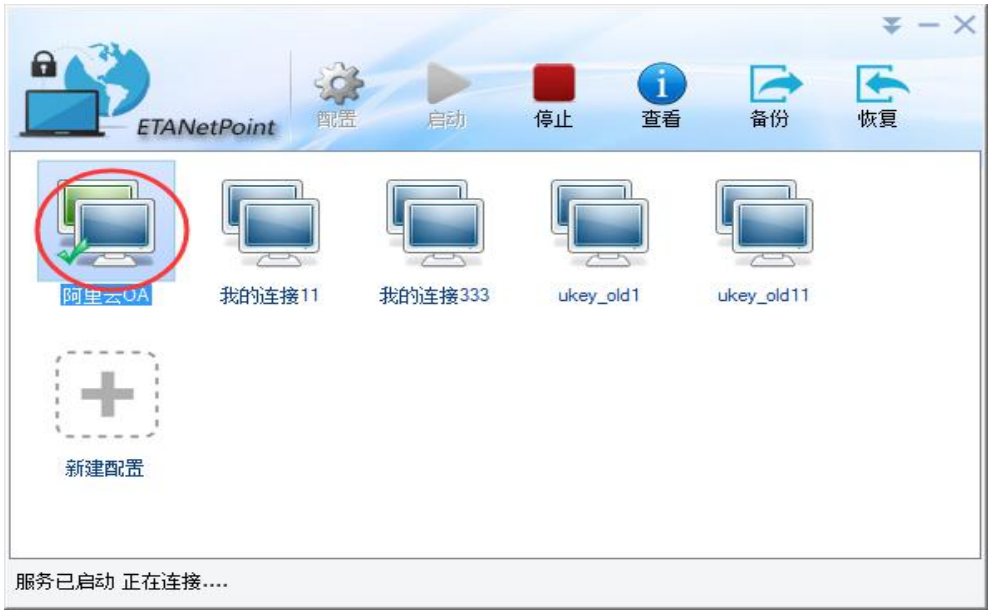
（3）点击账户，即可在 APP 上显示动态口令码。

5.1.2.3 启动隧道

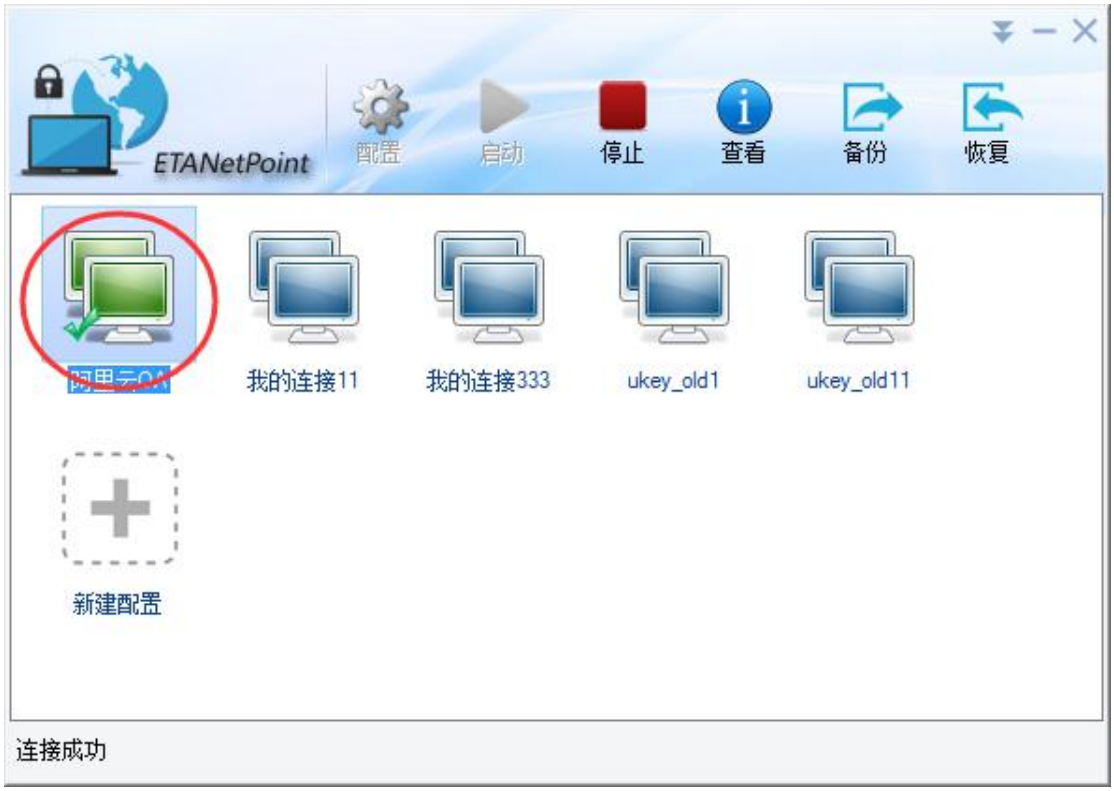
选中某个连接，点击常用菜单中的“启动”按钮。



连接过程中，图标处于闪动状态，如下图所示：



连接成功后，图标变成常绿状态，如下图所示：



5.1.2.4 查看连接信息

连接建立成功后，可以通过常用菜单中的“查看”来查询具体的连接地址信息，如下图所示：

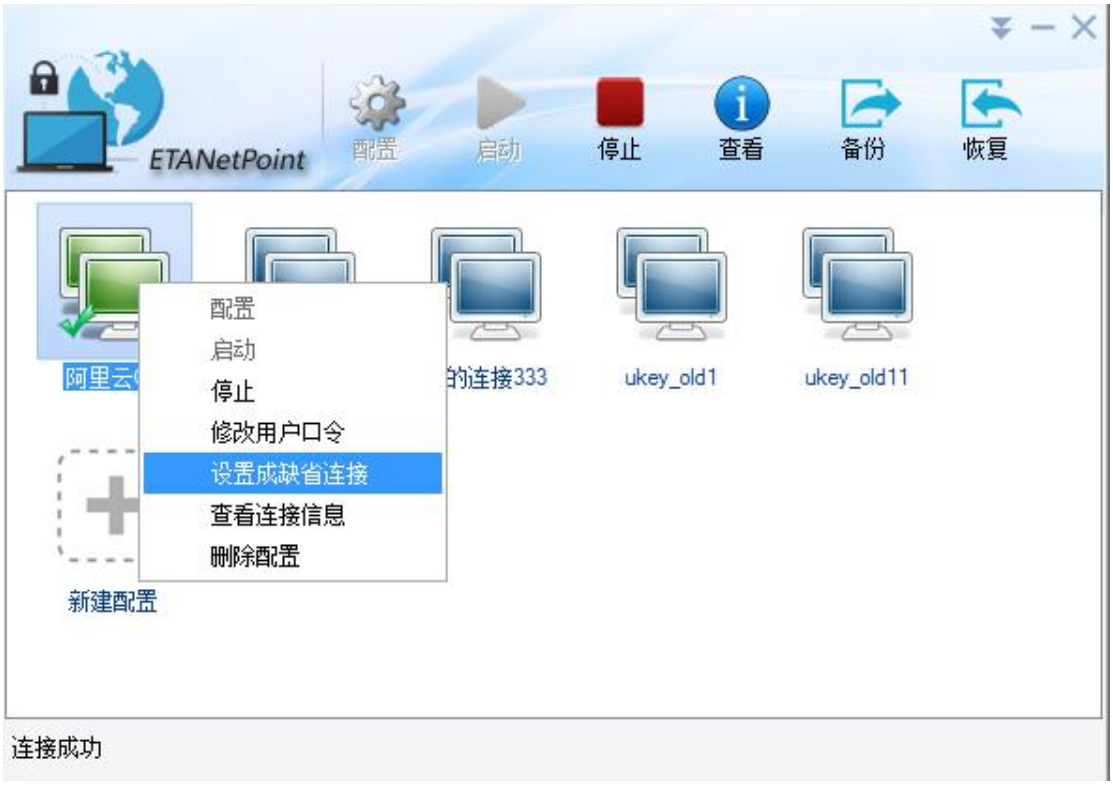
5.1.2.5 备份恢复功能

客户端支持对当前的配置做备份，并能够按需恢复备份。

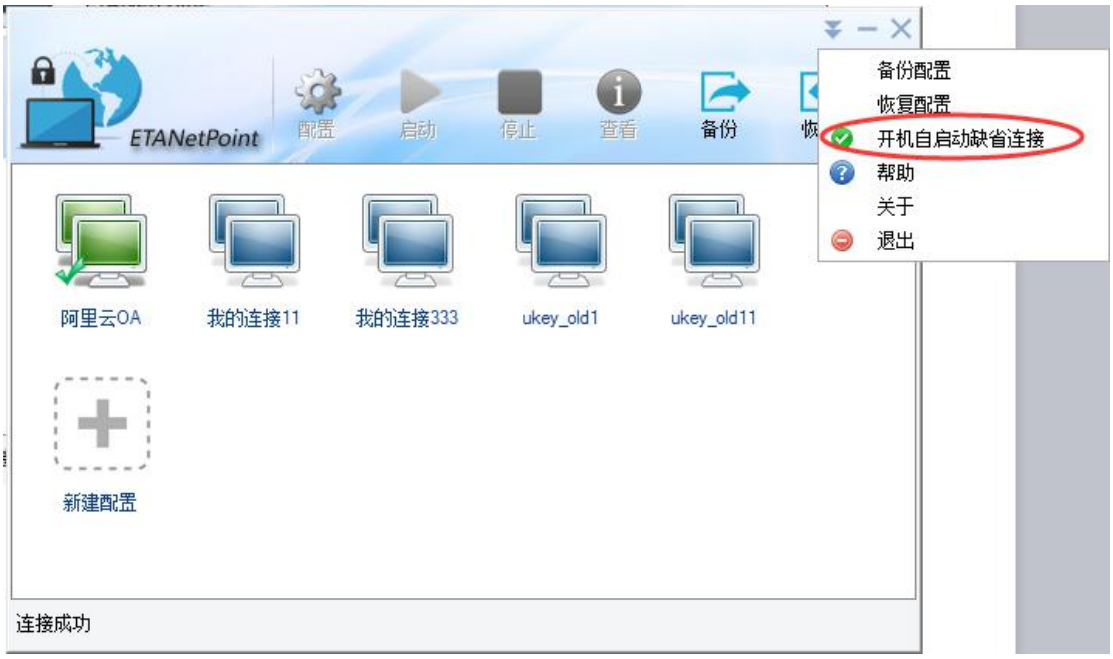
5.1.2.6 设置开机自启动

客户端支持选择某个 VPN 连接作为缺省连接，并可以设置成开机自启动。

鼠标右键点击某个连接，点击菜单“设置成缺省连接”，设置成功后，该连接的图标变成缺省连接图标。



然后点击系统菜单中的“开机自启动缺省连接”。



5.2 Linux 客户端

5.2.1 检查虚拟网络设备

查看是否内核支持虚拟网络设备：

ll /dev/net/tun ，查看结果如下图所示：

```
[root@localhost ~]# ll /dev/net/tun
crw-rw-rw-. 1 root root 10, 200 12?28 08:57 /dev/net/tun
```

✓ 如果有 tun 设备，说明该系统内核支持虚拟网络设备（跳至 2.1 节）

✓ 如果没有 tun 设备，请查收是否有 tun 驱动（跳至 1.2 节）

5.2.2 检查 tun 驱动

执行 modprobe tun，执行完成后，再执行 lsmod |grep tun

```
[root@localhost ~]# lsmod |grep tun
tun                    16934  2 vhost_net
```

如果看到 tun 驱动已经加载成功，可跳至 2.1 节。

5.2.3 无 tun 驱动

如果以上两步均执行失败，则需要客户联系奕锐电子技术人员并提供 linux 系统对应的内核源码来编译出 tun.ko，或者进入定制内核环节。

5.2.4 导入客户端

可以通过 SSH 软件（如：winscp）把文件放入 linux 系统，用户

可自行决定放在哪个目录下（如：/usr/local/bin）。

登录 root 终端，切换到客户端所在的目录（如： cd /usr/local/bin），执行：chmod +x ETANet_Client，赋予程序可执行权限。

5.2.5 执行客户端

确认执行该命令的时候，必须有 root 权限（1. root 账户可直接执行；2.或者加 sudo 可以执行）

命令:sudo ./ETANet_Client -l VPN 外网 IP 地址:VPN 端口 -U VPN 账户名 -P 账户密码

如：sudo ./ETANet_Client -l 122.112.234.170:25500 -U test -P 123456

注：一个 VPN 账号不能同时在多台 PC 上使用。

5.2.6 查看执行结果

ifconfig 查看是否有 ETANetTAP 网卡，并获得了 VPN 网的虚拟 IP 地址。

5.2.7 开机自启设置

以 centos 7.x 系统为例，执行：

```
chmod +x /etc/rc.d/rc.local
systemctl enable rc-local
```

然后编辑 rc.local 文件，写入 ETANet_Client 的启动脚本（参考

3.1）即可实现开机自启。

5.3 客户端配置（MAC OS X）

苹果电脑的系统客户端是一个压缩包：

解压后，提示有两个安装步骤，如下图所示：

首先安装 tuntap.pkg（虚拟网卡驱动），然后再安装 ETANet_Client_GUI（拖动.app 至 Applications 文件夹）,安装完成后，在 dock 栏出现 VPN 客户端图标：

5.3.1 软件配置

客户端默认允许最多配置两个 VPN 连接，但只允许其中一个 VPN 在线。软件主界面如下：

选择其中任何一个 VPN 图标，可以对其进行参数编辑：

连接 VPN，需要点击连接图标，提示输入管理员口令确认：

连接成功，如下图：

关闭 VPN 连接，也需要输入管理员口令：

5.4 手机客户端配置

5.4.1 Android 系统

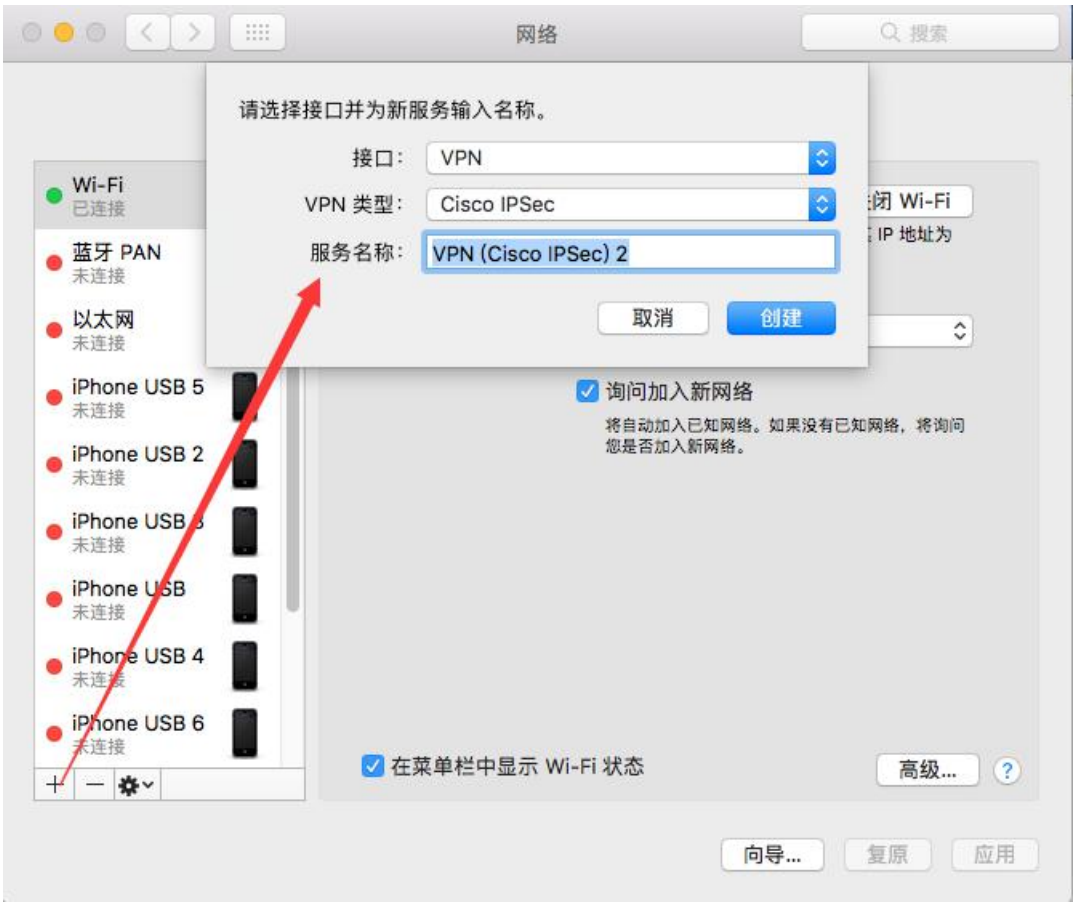
打开设置，选择“网络和连接”中的“其他连接方式”->“VPN”->“添加 VPN”->“IPSec Xauth PSK”，填写名称、服务器 IP、预共享密钥（当前系统已设置为“etaray123”），保存设置，然后输入用户名、密码即可连接到 VPN 服务器。

5.4.2 IOS 系统

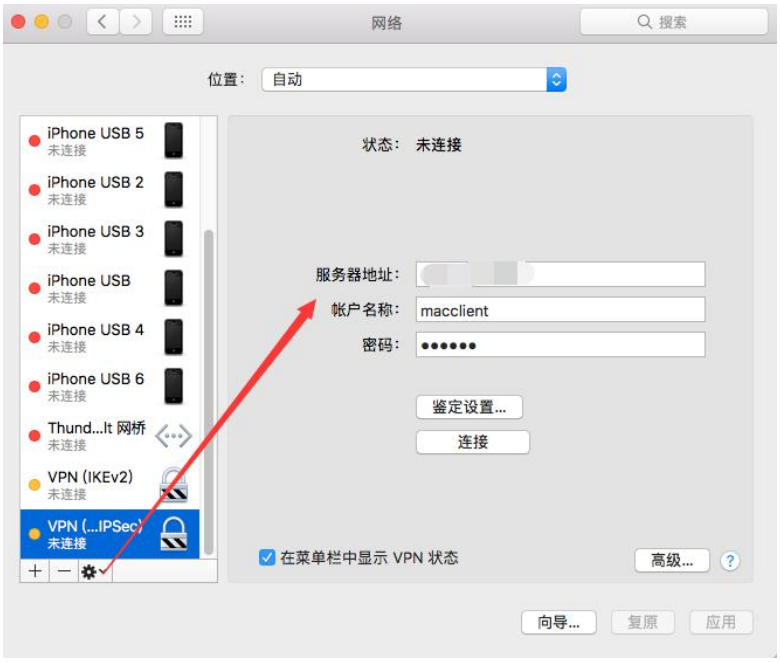
打开设置->通用->VPN->添加 VPN 配置->选择 IPSec 类型并填写描述、服务器、账户、密码、密钥（预共享密钥），完成后打开 VPN 状态，设备连接。

5.4.3 MAC OSx 系统自带 APP

“打开网络偏好设置 -> 点击”+”号，添加新的网络连接 -> 接口选择 VPN -> VPN 类型选择 Cisco IPSec。



建立好连接之后，点击该连接的“设置”：



输入“服务器地址”、“账户名称”、“密码”，同时在“鉴定设置”中设置“预共享密钥”：

最后点击“连接”即可建立隧道。