iSecSP 客户端定制化帮助文档

iSecSP 客户端定制化有两部分：基础定制化和高级定制化。

1.基础定制化

基础定制化包括：安装文件自定义、公司名称自定义、iSecSP 产品名称自定义、公司网站自定义等，见 1.1 [Startup]。

管理员可以通过修改 OEM.ini 文件来实现上述定制化。当管理员修改 OEM.ini 文件时，只能修改“=”后面的内容。特别注意的是，OEM.ini 必须以 ANSI 编码格式保存，否则中文会出现乱码问题。

OEM.ini 包含以下预定义部分：[Startup], [Settings], [DNSProxy], [DesktopDirect], [OEMUI], [OEMString], [SSL], [GMSKF], [CAPIEngine], [WinTUN], [WG], [GetToken], [sandbox], [LocalAPP], [isecspwm], [browser], [IPSec], [InstallPKG], [UninstallPKG], [KillPKGProcess], [ThirdPartyFile], [ThirdPartyDir], [NetsdkHomeTools], [NetAuth]和[LaunchCmd]。

1.1 [Startup]

CompanyName=Infosec Technologies

ApplicationName=iSecSP

CompanyURL=http://www.infosec.com.cn

注释：

CompanyName: 指定公司名称。公司名称的长度必须少于 128 个字符；否则，VPN 可能会异常工作。

ApplicationName: 指定（VPN 客户端）应用程序名称。应用程序名称的长度最好少于 36 个字符；否则，可能会异常显示 VPN 客户端安装 UI。此外，长度必须小于 128 个字符；否则，VPN 可能会异常工作。

CompanyURL: 指定公司网站的 URL。URL 的长度必须少于 128 个字符。

1.2 [Settings]

CreateShortcut=1

DisableAutoLoginWindows=0

DisableFFTrustSystemRootca=0

SetLocalDNSDropFlag=0

EnableClientSecurityV5=1

H5EdgeDetect=1

DisableClientUpgrade=1

ShowDDResource=0

ShowWebResource=0

RetainCurrentConfig=1

DisplayTabwidget=0

ShowWebPortal=1

LeftClickWebPortal=0

LaunchWebAfterConnected=0

DisableCheckOldPwd=0

BrowserType=ECIF3Q

BrowserPath=default

LaunchURL=

ProxyScriptNoRewrite=0

VirtualNetworkCardType=5

AuthorizePwdDown=0

VPNRealConnected=1

SSTPAdapterPort=55443

InstallTDIonWin7=0

EnableBestWay=1

EnableHttpdCheck=0

ShowUIAfterConnected=0

ShowMenuAfterConnected=1

ClearIECookie=0

ShowIDWithUnameNULL=0

HWIDType=100

HWIDDomainType=0

ProfileBackupType=0

VPNTunnelProtocol=10

ProfileAutoImport=0

MPProfileUrl=

SSTPRouteMonitorOff=0

MachineCertFlag=0

InterfaceMetric=10

PPPoEFlag=0

DisableKillPopMsg=0

PortalUIName=

IESSLSetting=0

AutoRSACertFlag=0

AutoSavePasswordFlag=0

NoZeroTrustFlag=0

AutoConnectAfterInstall=1

AutoHideCertDialog=0

SSTPAdapterName=

CheckAdapterStatus=0

DisableIPv6=0

EnableReconnectToDetectHost=0

VirtualGatewayType=1

DeleteVsiteRoute=0

注释：

CreateShortcut: 控制是否在桌面上创建快捷方式。该值可以是 0（未创建）或 1（已创建）。

DisableAutoLoginWindows: 控制是否禁用自动登录 windows。该值可以是 0（启用）或 1（禁用）。

DisableFFTrustSystemRootca: 控制是否禁用 Firefox 信任系统根证书。该值可以是 0（启用）或 1（禁用）。

SetLocalDNSDropFlag: 指定 DNS 删除的标志。该值可以是 0（将所有本地 DNS 添加到列表中）或 1（不将本地 DNS 添加到此列表中）。

EnableClientSecurityV5: 控制是否启用客户端安全 V5。该值可以是 0（禁用）或 1（启用）。

H5EdgeDetect: 控制是否启用 H5 边缘检测。该值可以是 0（禁用）或 1（启用）。

DisableClientUpgrade: 控制是否禁用 VPN 客户端升级。该值可以是 0（启用）或 1（禁用）。

ShowDDResource: 控制 VPN 连接后是否在 UI 页面上显示 DD 资源。该值可以是 0（不显示）或 1（显示）。

ShowWebResource: 控制 VPN 连接后是否在 UI 页面上显示 web 资源。该值可以是 0（不显示）或 1（显示）。

RetainCurrentConfig: 控制卸载 VPN 客户端时是否保留当前配置。该值可以是 0（不保留）或 1（保留）。

DisplayTabwidget: 控制选项卡控件是否显示在 VPN 客户端的 UI 页面上。该值可以是 0（不显示）或 1（显示）。

ShowWebPortal: 控制 VPN 连接后是否显示 web 门户。该值可以是 0（不显示）或 1（显示）。

LeftClickWebPortal: 控制是否可以左键单击 web 门户按钮。该值可以是 0（禁用）或 1（启用）。

LaunchWebAfterConnected: 控制是否在 VPN 连接后启动 web。该值可以是 0（不启动）或 1（启动）。

DisableCheckOldPwd: 控制更改密码时是否禁用检查旧密码。该值可以是 0（启用）或 1（禁用）。

BrowserType: 按类型指定启动浏览器的优先级。默认值为“ECIF3Q”。E：Edge，C：Chrome，I：IE，F：FireFox，3：60 浏览器，Q：QQ 浏览器。

BrowserPath: 指定浏览器的路径。

LaunchURL: 指定显示 web 门户时的启动 url。

ProxyScriptNoRewrite: 控制是否禁用代理脚本重写。该值可以是 0（启用）或 1（禁用）。

VirtualNetworkCardType: 指定虚拟网卡的类型。该值可以是 1（SSTP），2（VNIC），3（VTAP），4（VNIC-GM），5（VTAP-GM），6（WinTUN）或 11（SSTP，无需切换到 VNIC）。

AuthorizePwdDown: 指定多因素身份验证的密码输入框的顺序。值可以为 0 （顺序: 密码 -> 一次性口令 -> 第二密码 -> 第三密码）或 1（顺序: 密码 -> 第二密码 -> 第三密码 -> 一次性口令）。

VPNRealConnected: 控制是否启用 VPN 真实连接。该值可以是 0（禁用）或 1（启用）。

SSTPAdapterPort: 指定 SSTP 适配器的端口。

InstallTDIonWin7: 控制 TDI 是否安装在 win7 上。该值可以是 0（未安装）或 1（已安装）。

EnableBestWay: 控制是否启用最佳网关连接。该值可以是 0（禁用）或 1（启用）。

EnableHttpdCheck: 控制是否启用 Httpd 检查。该值可以是 0（禁用）或 1（启用）。

ShowUIAfterConnected: 控制 VPN 连接后是否显示 UI。该值可以是 0（不显示）或 1（显示）。

ShowMenuAfterConnected: 控制 VPN 连接后是否显示菜单。该值可以是 0（不显示）或 1（显示）。

ClearIECookie: 控制是否清除 IE cookie。该值可以是 0（不清除）或 1（清除）。

ShowIDWithUnameNULL: 控制是否显示用户名为空的 ID。该值可以是 0（不显示）或 1（显示）。

HWIDType: 指定 HWID 的类型。该值可以为 0（硬件 ID），1（操作系统 ID), 2（iSecSP 设备标识符），3（ART 设备标识符），或 4（CPU ID）。

HWIDDomainType: 指定 HWID 域的类型。该值可以是 0，1 或 2。

ProfileBackupType: 指定查找配置文件备份的优先级。值可以为 0（顺序：默认配置文件目录 -> 当前用户目录 -> VPN 客户端安装目录），1（默认配置文件目录 -> VPN 客户端安装目录 -> 当前用户目录）或 2 （VPN 客户端安装目录 -> 当前用户目录 -> 默认配置文件目录）。

VPNTunnelProtocol: 指定 VPN 隧道的协议。该值可以是 0（TCP 协议）、1（UDP 协议）或 10（默认隧道协议）。

ProfileAutoImport: 控制是否可以自动导入配置文件。该值可以是 0（禁用）或 1（启用）。

MPProfileUrl: 指定 VPN 客户端配置文件的 url。

SSTPRouteMonitorOff: 控制是否关闭 SSTP 路由监视器。该值可以是 0（打开）或 1（关闭）。

MachineCertFlag: 指定计算机证书的标志。该值可以是 0（当前用户），1（本地计算机）或 2（当前用户和本地计算机）。

InterfaceMetric: 指定接口值。该值范围为 0 到 9999。

PPPoEFlag: 控制 fulltunnel 时是否启用 PPPoE，当启用时，可以解决 fulltunnel 场景数据通过物理网卡发不出去进而导致网关端断开 TCP 连接问题。该值可以是 0（禁用）或 1（启用）。

DisableKillPopMsg: 控制是否禁用终止弹出窗口的进程。该值可以是 0（启用）或 1（禁用）。

PortalUIName: 指定 UI 上显示的 web 门户的名称。

IESSLSetting: 指定 IE 浏览器的 SSL 设置。该值可以是 32（SSL 3.0），128（TLS1.0），512（TLS1.1），2048（TLS1.2）或 8192（TLS1.3）。如果要同时设置两个或多个，请将它们的值相加。（例如 SSL 3.0 和 TLS1.0：160）

AutoRSACertFlag: 指定证书认证的证书类型。该值可以是 0（CryptAPI），1（openssl）。

AutoSavePasswordFlag: 控制是否自动保存登录密码。该值可以是 0（不保存）或 1（保存）。

NoZeroTrustFlag: 控制是否是零信任站点。该值可以是 0（是）或 1（不是）。

AutoConnectAfterInstall: 控制安装后首次运行客户端时是否自动连接。该值可以是 0（不自动连接）或 1（自动连接）。

AutoHideCertDialog：控制是否隐藏证书选择对话框。该值可以是 0（显示）或 1（隐藏）。

SSTPAdapterName：指定 SSTP 网卡名称。

CheckAdapterStatus：控制是否检查网卡状态。该值可以是 0（不检查）或 1（检查）。默认不检查。

DisableIPv6：控制是否禁用 IPv6 路由。该值可以是 0（不禁用）或 1（禁用）。若 禁用 IPv6，则在连接之后且在 fulltunnel 场景下，删除 ::/0 路由。

EnableReconnectToDetectHost：由于网络问题重连失败时，控制是否启用探路优选并重连，以满足某链路故障时可无缝切换其他链路的场景。该值可以是 0（禁用）或 1（启用）。此外，还需在接入点的“高级配置 -> 网络设置”中勾选“会话失 效时自动重连”。

VirtualGatewayType：指定获取虚拟网关地址的算法。该值可以是 1：虚拟网关地址= (虚拟 IP & 掩码) + 1，2：虚拟网关地址= (虚拟 IP & 255.255.255.0) + 1，3：虚拟网关地址=虚拟 IP。

DeleteVsiteRoute：控制连接 VPN 后是否删除接入点路由。该值可以是 0（不删除）或 1（删除）。若删除该路由，可解决用户系统与网关端同网段时，连接 VPN 后反复重连问题。

例如：接入点 10.6.0.2 的路由：

10.6.0.2　255.255.255.255　<用户系统网关地址>　<用户系统 IP 地址>　<跃点数>

1.3 [DNSProxy]

DNSProxyType=4

DNSProxyEnableHosts=0

DNSProxyEnableRedirect=0

注释：

DNSProxyType: 指定 DNS 代理的类型。该值可以是 0（DNS 代理启用编辑）、1（DNS 代理禁用编辑）、2（启用 DNS 代理）、3（禁用 DNS 代理）或 4（DNS 代理服务器）。

DNSProxyEnableHosts: 控制是否在选项对话框中启用高级域名映射。该值可以是 0（禁用）或 1（启用）。

DNSProxyEnableRedirect: 控制是否在选项对话框中启用高级重定向。该值可以是 0（禁用）或 1（启用）。

1.4 [DesktopDirect]

DDMaxDescriptionLenW=0

DDMaxDescriptionLenH=0

注释：

DDMaxDescriptionLenW: 指定远程桌面图标的最大宽度。值范围为 128 到 1024，默认值为 160。

DDMaxDescriptionLenH: 指定远程桌面图标的最大高度。值范围为 64 到 512，默认值为 80。

1.5 [OEMUI]

HideAppResource=0

HideNetworkResource=0

HideEnvirDetect=0

HideNetDiag=0

HideCleanCache=0

ShowResourceWelcome=0

ContactInfo=

UnameTop=0

uiWidth=0

uiHeight=0

QRCodeWidth=160

QRCodeHeight=160

menuIconWidth=18

menuIconHeight=18

注释：

HideAppResource：控制连接 VPN 后是否隐藏应用资源。该值可以是 0（不隐藏）或 1（隐藏）。

HideNetworkResource：控制连接 VPN 后是否隐藏网络资源。该值可以是 0（不隐藏）或 1（隐藏）。

HideEnvirDetect：控制连接 VPN 后是否隐藏环境检测。该值可以是 0（不隐藏）或 1（隐藏）。

HideNetDiag：控制连接 VPN 后是否隐藏网络诊断。该值可以是 0（不隐藏）或 1（隐藏）。

HideCleanCache：控制连接 VPN 后是否隐藏清理缓存。该值可以是 0（不隐藏）或 1（隐藏）。

ShowResourceWelcome：控制连接 VPN 后应用资源界面是否显示欢迎卡片。该值可以是 0（不显示）或 1（显示）。

ContactInfo：控制连接 VPN 前是否在最底部显示联系方式。该值如果为空，则不显示联系方式；该值如果不为空，则在最底部显示所指定的联系方式。

UnameTop：控制是否将登录后的用户名显示在左上角（程序图标改为左下角显示）。该值可以为 1（改为左上角显示用户名）或 0（保持原样）。

uiWidth：定制主界面宽度，单位为像素，或者为 0（保持默认宽度）。

uiHeight：定制主界面高度，单位为像素，或者为 0（保持默认高度）。宽度与高度均须大于最小限定值（850x550），否则此处的自定义尺寸不会生效。

QRCodeWidth: 指定二维码图片的宽度。

QRCodeHeight: 指定二维码图片的高度。

menuIconWidth: 指定右上角设置、最大化、最小化、关闭按钮的宽度。

menuIconHeight: 指定右上角设置、最大化、最小化、关闭按钮的高度。

1.6 [OEMString]

labwelcome=

labsecuretunnel=

labconnected=

btnaddprofile=

labLogin=

labMethod=

labUsername=

labUsernameHint=

labPwd=

labPwdHint=

labPwd2=

labPwd2Hint=

labPwd3=

labPwd3Hint=

labPwdSMS=

labPwdSMSHint=

注释：

labwelcome: 指定 VPN 客户端主 UI 页面上的欢迎消息。

labsecuretunnel: 在 VPN 客户端的主 UI 页面上指定连接后的隧道提示。

labconnected: 在 VPN 客户端的主 UI 页面上指定成功连接的提示。

btnaddprofile: 指定 VPN 客户端主 UI 页面上添加配置文件按钮的提示。

labLogin: 指定身份验证对话框的标题。

labMethod: 指定身份验证对话框中登录方法标签的提示。

labUsername: 指定身份验证对话框中用户名标签的提示。

labUsernameHint: 指定验证对话框中用户名输入框的提示。

labPwd: 指定身份验证对话框中密码标签的提示。

labPwdHint: 指定身份验证对话框中密码输入框的提示。

labPwd2: 指定身份验证对话框中第二个密码标签的提示。

labPwd2Hint: 指定身份验证对话框中第二个密码输入框的提示。

labPwd3: 指定身份验证对话框中第三个密码标签的提示。

labPwd3Hint: 指定身份验证对话框中第三个密码输入框的提示。

labPwdSMS: 指定短信验证码标签的提示。

labPwdSMSHint: 指定短信验证码输入框的提示。

1.7 [SSL]

DisableTLS1.3=0

注释：

DisableTLS1.3: 控制是否禁用 TLS1.3 协议。值可以为 0 (不禁用)，1 (禁用)。特别注意，若开启重协商，不支持 TLS1.3 协议，则需禁用 TLS1.3。

1.8 [GMSKF]

sslproto=6

skfdriverlist=

skfshowtype=2

monitor=1

注释：

sslproto: 指定 ssl 协议。值可以为 0 (INIT), 1 (TLS10), 2 (TLS12), 3 (SSLV3), 4 (TLS11), 5 (TLS13) 或 6 (SM2)。

skfdriverlist: 指定 SKF 证书驱动程序的名称。用户需要将 SKF 证书驱动程序放入 VPN 客户端的安装包中。通过这种方式，可以调整不同版本的 UKey 证书。可以同时设置多个驱动程序，名称以“;”分隔。

skfshowtype: 指定 GM SKF 证书规则。值可以是 0（显示有效证书）、1（显示所有证书）或 2（显示最新颁发的证书）。

monitor: 指定 SKF 插拔动作引发的行为规则。值可以是 0（拔掉 UKey 时不断开隧道）、1（以 SKF 协议相关接口监测 UKey 动作，拔掉 UKey 时断开隧道）或 2（以 USB 模式监测 UKey 动作，拔掉 UKey 时断开隧道）。

1.9 [CAPIEngine]

enable=1

dlg_title=iSecSP 身份认证

dlg_prompt=请选择证书:

store_name=

csp_name=

注释：

enable: 控制在 OpenSSL 初始化过程中是否允许加载 CAPI Engine。该值可以是 0（禁止）或 1（允许）。

dlg_title: 指定弹出证书选择框时显示的标题。

dlg_prompt: 指定弹出证书选择框时显示的提示信息。

store_name: 指定显示哪个证书库里头的证书，默认为空，即显示 “MY”。

csp_name: 指定使用谁家的 csp， 一般用谁家的 csp，也会指定谁家的证书 store。

1.10 [WinTUN]

adapterName="iSecSP-WinTUN"

adapterType="iSecSP"

注释：

adapterName: 指定 WinTUN 网卡名称。

adapterType: 指定 WinTUN 网卡类型。

1.11 [WG]

EnableShowAll=0

注释：

EnableShowAll: 控制在 WireGuard 列表界面是否显示“全部”选项。该值可以是 0（不显示）或 1（显示）。如果用户选择“全部”选项，则同时连接所有的 WireGuard server，并实现隧道分流功能。

1.12 [GetToken]

showInMethodName=

uiName=

url=

注释：

showInMethodName: 指定显示“获取动态码”按钮的认证方法名称。

uiName: 指定“获取动态码”按钮显示的名称。

url: 指定“获取动态码”按钮所链接的 URL。

1.13 [sandbox]

SandBoxInstall=0

SandBoxEnable=0

SandBoxVersion=2

SandBoxBurnafterReading=1

SandBoxPrinterRedirection=0

SandBoxClipboadRedirection=0

SandBoxScreenRecording=0

SandBoxScreenShots=0

SandBoxSafeSubscript=1

SandBoxRightInfo ="在 iSecSP 沙箱中运行"

注释：

SandBoxInstall：控制是否安装沙箱。0：不安装，1：仅安装沙箱 V1，2：仅安装沙箱 V2，3：沙箱 V1，V2 均安装。默认不安装。

SandBoxEnable：指定是否启动沙箱。0：禁止启动沙箱，1：允许启动沙箱。默认禁止。

SandBoxVersion：指定沙箱版本。1：V1 版本，2：V2 版本。默认 V2 版本。

SandBoxBurnafterReading：指定是否允许阅后即焚。0：禁止，1：允许。默认允许。若开启阅后即焚功能，则在 iSecSP 断开后，立即销毁沙箱空间。

SandBoxPrinterRedirection：指定是否允许打印机重定向。0：禁止，1：允许。默认禁止。若开启打印机重定向功能，则在沙箱内可以使用打印机，否则不可以。

SandBoxClipboadRedirection：指定是否允许剪切板重定向。0：禁止，1：允许。默认禁止。若开启剪切板重定向功能，则在沙箱内可以进行剪切，否则不可以。

SandBoxScreenRecording：指定是否开启防录屏功能。0：关闭，1：开启。默认关闭。若开启防录屏功能，个人空间的录屏工具/Windows 的 PrtSc 均无法录取到安全空间内的画面。

SandBoxScreenShots：指定是否开启防截屏功能。0：关闭，1：开启。默认关闭。若开启防截屏功能，个人空间的截屏工具/Windows 的 PrtSc 均无法截取到安全空间内的画面。

SandBoxSafeSubscript：指定沙箱资源是否显示安全角标。0：不显示，1：显示。默认显示。

SandBoxRightInfo：指定右键菜单显示信息。默认为"在 iSecSP 沙箱中运行"。

1.14 [LocalAPP]

number=0

name1=

path1=

iconpath1=

permission1=

注释：

number: 指定沙箱内置应用的数量。如果 number>=1，则开始依次查找内置应用的名称等信息（name1，name2，...，name[number]）。VPN 连接成功后，在安全沙箱界面显示内置应用名称与图标，点击则会在沙箱内打开该内置应用。

name1: 指定沙箱内置应用的名称。

path1: 指定沙箱内置应用的路径。

iconpath1: 指定沙箱内置应用的图标路径。

permission1: 指定沙箱内置应用的访问权限。0：表示沙盒内不显示该应用；1：表示沙盒内显示该应用，该应用仅允许在沙盒内运行；2：表示沙盒内显示该应用，该应用在沙盒内外都可以运行。

1.15 [isecspwm]

start=0

DisplayAffinity=0

wmShowHostname=1

wmShowIP=1

wmShowMac=1

wmShowPhone=1

wmShowUname=1

wmShowTime=1

wmMsg=

wmFont=SimSun

wmFontSize=20

wmTransparency=200

wmColorR=255

wmColorG=0

wmColorB=0

wmAngle=315

wmSpacing=200

注释：

start: 控制 VPN 连接后是否启用屏幕水印。该值可以是 0（禁用）或 1（启用）。

DisplayAffinity: 控制是否启用防截屏功能。该值可以是 0（禁用）或 1（启用）。

wmShowHostname: 控制水印是否显示主机名称。该值可以是 0（不显示）或 1（显示）。

wmShowIP: 控制水印是否显示 IP 地址。该值可以是 0（不显示）或 1（显示）。

wmShowMac: 控制水印是否显示 mac 地址。该值可以是 0（不显示）或 1（显示）。

wmShowPhone: 控制水印是否显示电话号码后 4 位。该值可以是 0（不显示）或 1（显示）。

wmShowUname: 控制水印是否显示用户名。该值可以是 0（不显示）或 1（显示）。

wmShowTime: =1 控制水印是否显示当前时间。该值可以是 0（不显示）或 1（显示）。

wmMsg: 指定水印的内容。

wmFont: 指定水印的字体系列。

wmFontSize: 指定水印的字体大小。

wmTransparency: 指定水印的透明度。取值范围为 0 到 255。

wmColorR: 指定水印的颜色（R）。取值范围为 0 到 255。

wmColorG: 指定水印的颜色（G）。取值范围为 0 到 255。

wmColorB: 指定水印的颜色（B）。取值范围为 0 到 255。例如：（wmColorR、wmColorG、wmColorB）：rgb（255,0,0）表示“红色”。

wmAngle: 指定水印的角度。取值范围为 0 到 360。

wmSpacing: 指定水印的间距。单位为像素。

1.16 [browser]

version=

EnableAccessWebPortal=1

EnablePrint=0

EnableScreenShots=0

EnableDebug=0

EnableSourceCode=0

注释：

version: 指定待安装的安全浏览器组件 libcef.dll 的版本号。覆盖安装时，如果此版本号高于已安装 libcef.dll 的版本号，才进行覆盖安装 libcef.dll。

EnableAccessWebPortal: 控制是否启用安全浏览器访问 Web 资源。该值可以是 0（禁用）或 1（启用）。

EnablePrint: 控制在安全浏览器内是否可以打印。该值可以是 0（禁用）或 1（启用）。

EnableScreenShots: 控制在安全浏览器内是否可以截屏录屏。该值可以是 0（禁用）或 1（启用）。

EnableDebug: 控制在安全浏览器内是否可以进行 Debug。该值可以是 0（禁用）或 1（启用）。

EnableSourceCode: 控制在安全浏览器内是否可以查看源代码。该值可以是 0（禁用）或 1（启用）。

1.17 [IPSec]

enable=0

注释：

enable：控制是否安装 IPSec。0：不安装，1：安装。

1.18 [InstallPKG]

CNGInstall=0

CNGVersion=

number=0

pkg1=

注释：

CNGInstall: 控制是否安装 NetAuthSSOCNG.exe。0：不安装，1：安装。若需安装 NetAuthSSOCNG.exe，需满足三个条件：（1）CNGInstall=1，（2）pkg=NetAuthSSOCNG.exe /silent，（3）NetAuthSSOCNG.exe 放在 VPN 客户端的安装文件夹中。

CNGVersion: 指定 NetAuthSSOCNG.exe 的版本号。覆盖安装时，如果版本号高于已安装版本号，才进行覆盖安装 NetAuthSSOCNG.exe。

特别注意：若不安装 NetAuthSSOCNG.exe，有以下两种方法：

（1）修改 OEM.ini：设置 number=0；

（2）删除文件夹：删除 iSecSPSetup 安装包中的 CNG 文件夹。

number: 指定需要安装的插件的数量。如果 number>=1，请开始查找插件安装程序的名称（pkg1，pkg2，...，pkg[number]），然后依次安装它们。

pkg1: 指定插件安装程序的名称及安装参数。此安装程序应放在 VPN 客户端的安装文件夹中。

1.19 [UninstallPKG]

number=0

path1=

注释：

number: 指定需要卸载的插件的数量。如果 number>=1，则开始查找插件卸载程序的路径（path1，path2，...，path[number]），然后依次卸载它们。

path1: 指定插件卸载程序的路径。

1.20 [KillPKGProcess]

number=0

process1=

注释：

number: 指定需要终止的插件进程的数量。如果 number>=1，则开始查找插件的进程路径（process1，process2，...，process[number]），并依次终止它们。

process1: 指定插件进程的路径。

注:

[InstallPKG]，[UninstallPKG] 和 [KillPKGProcess]同时定制，实现插件和 VPN 客户端的联合安装和卸载。如下例所示：

[InstallPKG]

number=1

pkg1=NetAuthSSOCNG.exe /silent

[UninstallPKG]

number=4

path1=C:\Program Files (x86)\Infosec NetAuthSSOCNG\unins000.exe

path2=C:\Program Files (x86)\Infosec NetAuthSSOCNG\unins001.exe

path3=C:\Program Files\Infosec NetAuthSSOCNG\unins000.exe

path4=C:\Program Files\Infosec NetAuthSSOCNG\unins001.exe

[KillPKGProcess]

number=2

process1=InfosecNetAuthSSOCNGService.exe

process2=InfosecNetAuthSSOCNG.exe

1.21 [ThirdPartyFile]

number=0

file1=

注释：

number: 指定需要复制到安装目录下的第三方文件数量。如果 number>0，则开始查找文件的目标路径（file1，file 2，...，file [number]），并依次复制它们到指定路径下。

file1: 指定需要复制的第三方文件的目标路径。且需将文件内置到安装包的“iSecSPSetup\ThirdPartyFile”文件夹中。

如：

[ThirdPartyFile]

number=1

file1=C:\Program Files\Infosec Technologies\iSecSP Client\ msvcp140.dll

注：msvcp140.dll 需放置到安装包“iSecSPSetup\ThirdPartyFile”中。

1.22 [ThirdPartyDir]

number=0

dir1=

注释：

number: 指定需要复制到安装目录下的文件夹数量。如果 number>0，则开始查找文件夹的目标路径（dir1，dir 2，...，dir [number]），并依次复制它们到指定路径下。

dir1: 指定需要复制的文件夹的目标路径。且需将文件夹内置到安装包“iSecSPSetup”中。

如：

[ThirdPartyDir]

number=1

dir1=C:\Program Files\Infosec Technologies\iSecSP Client\help

注：help 文件夹需放置到安装包“iSecSPSetup”中。

1.23 [NetsdkHomeTools]

number=0

file1=

注释：

number: 指定 Net sdk home tools（如摄像机等）的数量。如果 number>=1，则开始查找文件（file1，file2，...，file[number]）。

file1: 指定文件名称。如果该文件在安装包内，安装客户端时，将会将其复制到客户端安装目录下。

1.24 [NetAuth]

Address=

GetSPAPwdSuccess=

注释：

Address: 指定 NetAuth 地址。

GetSPAPwdSuccess: 指定成功获取 SPA 密码的提示信息。

1.25 [LaunchCmd]

path=

para=

注释：

path: 指定连接 VPN 后想要运行 APP 的路径。

para: 指定连接 VPN 后想要运行 APP 的参数。

2. 高级定制化

高级定制化包括：徽标、图标和背景图片自定义以及 UI 显示信息和样式自定义。要进行自定义，请替换安装包中的相应文件。

2.1 Logo（徽标）

application.ico：VPN 连接建立后，UI 页面上显示的公司标志。

2.2 Icon（图标）

connected.ico, disconnected.ico or reconnecting.ico

- connected.ico: VPN 连接后应用程序的托盘图标。
- disconnected.ico: 成功 VPN 连接前应用程序的托盘图标。
- reconnecting.ico: VPN 重新连接期间应用程序的托盘图标。

2.3 背景图片

about_background.png：右上角菜单“关于”界面的背景图片。

2.4 UI 显示信息

ui.ini：应用程序 UI 页面上所显示的文字信息。若需使用英文版客户端，只需将安装包中的 ui.ini 文件内容置空即可（ui.ini 文件必须存在，否则客户端仍是中文版）。

2.5 UI 样式

ui.qss：应用程序 UI 样式文件。

•

如何自定义 isecsp.ini 文件？

您可能希望向所有用户提供 VPN 设置配置文件。当用户安装软件包时，配置文件中的设置将自动导入。您可以编辑 isecsp.ini 文件，或复制 isecsp.ini 文件以替换旧文件。默认情况下，isecsp.ini 文件不存在。特别注意的是，isecsp.ini 必须以 UTF-8 编码格式保存。

此外，我们在安装包中提供了一个名为 isecsp_tcomplete.ini 的模板。您可以使用此模板自定义自己的 isecsp.ini 文件。请注意，iSecSP 客户端只能识别名为“isecsp.ini”的文件。因此，请保持文件名正确。此外，密码设置无法自定义。

参数描述

isecsp.ini 中参数的含义如下：

[global]

参数	含义
autoconnect	启动独立客户端时是否自动连接 VPN。其值可以为 true 或 false。
autologinwindows	是否使用以下自动登录用户名和密码自动登录 Windows 操作系统。其值可以为 true 或 false。
lockscreen	登录成功时是否锁定 Windows 操作系统的屏幕。其值可以为 true 或 false。
windows_username	用于自动登录 Windows 操作系统的用户名。
windows_password	用于自动登录 Windows 操作系统的用户名的密码。
autorun	Windows 操作系统启动时是否自动启动独立客户端。其值可以为 true 或 false。
autorun_only_outside	Windows 操作系统启动时自动启动独立客户端的运行方式是否是只在外网。其值可以为 true 或 false。
intranet_ip	开机后只在外网自动运行的内网 IP 地址。
intranet_port	开机后只在外网自动运行的内网端口号。
default_profile	默认配置文件。可以将任何配置文件设置为默认配置文件。
DDUseTerminalSize	远程桌面是否使用自定义尺寸。其值可以为 true 或 false。
DDSize_H	远程桌面自定义高度。
DDSize_W	远程桌面自定义宽度。

enable_dnsproxy	是否启用 DNS 代理。其值可以为 true 或 false。
TunnelType	隧道类型。其值可以为 0:TCP, 1:UDP, 10:Default。

[profiles]

参数	含义
data\size	接入点的个数
data\1\name	登录接入点的用户名。
data\1\host	接入点的最优链路的主机名或 IP 地址。
data\1\bestip	接入点的最优链路的 IP 地址
data\1\allhost	接入点的主机名或 IP 地址（包括端口号）
data\1\alias	接入点的别称
data\1\port	接入点的端口。
data\1\authmethod	登录接入点的认证方法
data\1\username	登录接入点的用户名称
data\1\password	登录接入点的密码
data\1\password2	登录接入点的第二个密码
data\1\password3	登录接入点的第三个密码
data\1\cert	证书认证中手动导入方式的证书路径。 1. 证书类型为：国密 SSL 证书时，格式如下： （1）加密证书路径|签名证书路径 （2）加密证书路径| （3）|签名证书路径 例如： （1） D:\cert\yangzm\sm2agclientenc.pfx|D:\cert\yangzm\sm2agclientsign.pfx （2）D:\cert\yangzm\sm2agclientenc.pfx| （3）|D:\cert\yangzm\sm2agclientsign.pfx 2. 证书类型为：RSA SSL 证书时，代表：签名证书路径。 例如：D:\cert\yangzm\sm2agclientsign.pfx
data\1\certpassword	证书认证中手动导入方式的证书密码。 1. 证书类型为：国密 SSL 证书时，格式如下： （1）加密证书密码|!@#|签名证书密码 （2）加密证书密码|!@#| （3）|!@#|签名证书密码 例如： （1）click1|!@#|click1

	（2）click1|!@#| （3）|!@#|click1 2. 证书类型为：RSA SSL 证书时，代表：签名证书密码。例如：click1
data\1\capath	证书认证中服务端根证的路径
data\1\cert_detect_text	证书认证的认证方式。该值可以为："自动检测"，"手动导入"，"协同证书"。默认值为："协同证书"。
data\1\server_ca_id	证书认证中导入服务端根证的方式。该值可以为：0（证书路径），1（证书 URL）。
data\1\custom_dns	自定义的 DNS 列表。L3VPN 连接之后，点击"网络资源"，可在 DNS 列表项中显示。
data\1\tunnel_type	VPN 策略。该值可以为：-1（InitValue），0（Auto），1（L3VPN），2（Proxy），3（Both）。
data\1\auth_type	认证类型。该值可以为：0（常规认证），1（手动导入证书认证），2（安全浏览器认证），3（SMS 认证），4（SMX 认证），5（Syferlock 认证），7（系统浏览器认证），8（微软 SAML 认证），100（RSA 自动检测证书认证），101（协同证书认证）。
data\1\prx_enable_id	代理认证方式。该值可以为：0（禁用代理），1（自动代理），2（启动代理）。
data\1\prx_host	启动代理认证方式中的代理地址。
data\1\prx_port	启动代理认证方式中的代理端口号。
data\1\prx_username	启动代理认证方式中的代理用户名称。
data\1\prx_password	启动代理认证方式中的代理密码。
data\1\prx_domain	启动代理认证方式中的代理域名地址。
data\1\reconn_count	重连次数。
data\1\reconn_time	重连时间。单位：秒。
data\1\reconn_sess_invalid	会话失效时是否自动重连。该值可以为：0（重连），1（不重连）。
data\1\auto_open_system_browser	系统浏览器认证获取到 session 后，是否自动关闭系统浏览器。该值可以为：0（关闭），1（不关闭）。注：若选择关闭，则会关闭浏览器所有标签页。
data\1\enable_spa	是否开启 SPA。其值可以为 true 或 false。
data\1\spa_address	SPA 地址，与接入点地址一致。
data\1\spa_port	SPA 端口号。
data\1\spa_username	SPA 用户名。
data\1\spa_password	SPA 密码。
data\1\spa_share_password	SPA 共享密钥。

data\1\spa_time	SPA 超时时间，单位：秒。
data\1\spa_count	SPA 尝试次数。
data\1\ssl_protocol	指定 ssl 协议。值可以为 0 (INIT), 1 (TLS10), 2 (TLS12), 3 (SSLV3), 4 (TLS11), 5 (TLS13) 或 6 (SM2)。
data\1\myRDPHost	“我的远程桌面”的主机地址。
data\1\mauthUsername	协同证书认证用户名。
data\1\phone	SMS 认证默认手机号。
data\1\intranet_address	内网探测地址。