



Cisco AnyConnect 安全移动客户端管理员指南，4.1 版

首次发布日期: 2014 年 05 月 04 日

上次修改日期: 2015 年 05 月 22 日

Americas Headquarters

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
USA
<http://www.cisco.com>
Tel: 408 526-4000
800 553-NETS (6387)
Fax: 408 527-0883



目录

部署 AnyConnect 1

AnyConnect 部署概述 1

为 AnyConnect 准备终端 2

结合使用 AnyConnect 和移动宽带卡 2

在 Windows 上将 ASA 添加到 Internet Explorer 的受信任站点列表 3

阻止 Internet Explorer 中的代理更改 3

配置 AnyConnect 如何处理 Windows RDP 会话 4

Windows 上仅使用 DES 的 SSL 加密 6

预部署 AnyConnect 6

用于预部署和网络部署的 AnyConnect 模块可执行文件 7

预部署 AnyConnect 配置文件的位置 8

将 AnyConnect 模块预部署为独立应用 9

在 Windows 上使用 SMS 部署独立模块 9

将网络访问管理器和网络安全部署为独立应用 10

独立模块的用户安装 10

预部署到 Windows 11

使用 ISO 分发 AnyConnect 11

AnyConnect ISO 文件内容 11

使用 SMS 分发 AnyConnect 12

Windows 预部署 MSI 示例 12

Windows 预部署安全选项 14

Windows 上的 AnyConnect 模块安装和删除顺序 14

预部署到 Mac OS X 15

在 Mac OS X 上安装和卸载 AnyConnect 15

在 Mac OS X 上将网络安全模块安装为独立应用 15

限制 Mac OS X 上的应用 16

预部署到 Linux 16

安装用于 Linux 的模块	16
卸载用于 Linux 的模块	17
初始化 Firefox 的服务器证书验证	17
在 Linux 设备上手动安装 DART	17
网络部署 AnyConnect	18
在 ASA 上配置网络部署	19
WebLaunch 的浏览器限制	19
下载 AnyConnect 软件包	19
在 ASA 上加载 AnyConnect 软件包	20
启用其他 AnyConnect 模块	20
在 ASDM 中创建客户端配置文件	21
在 ISE 上配置网络部署	21
准备 AnyConnect 文件进行 ISE 上传	22
配置 ISE 以部署 AnyConnect	23
更新 AnyConnect 软件和配置文件	24
禁用 AnyConnect 自动更新	25
在 WebLaunch 期间提示用户下载 AnyConnect	25
允许用户延期升级	26
在 ASA 上配置延迟更新	26
在 ISE 中配置延期更新	27
延期更新 GUI	27
设置更新策略	28
更新策略概述	28
已授权服务器更新策略行为	28
未授权的服务器更新策略行为	29
更新策略指南	30
更新策略示例	30
AnyConnect 参考信息	31
本地计算机上用户首选项文件的位置	31
AnyConnect 和传统 VPN 客户端使用的端口	32
定制和本地化 AnyConnect 客户端和安装程序	33
修改 AnyConnect 安装行为	33

- 禁用客户体验反馈 33
- 修改安装行为 (Windows) 34
 - 用于定制客户端安装的 Windows 安装程序属性 34
 - AnyConnect 模块的 Windows 安装程序属性 35
 - 将定制安装程序转换导入自适应安全设备 36
 - 定制 AnyConnect 用户界面的转换示例 37
 - 本地化 AnyConnect 安装程序屏幕 38
 - 将本地化的安装程序转换导入自适应安全设备 38
- 修改安装行为 (Mac OSX) 40
 - 使用 ACTransforms.xml 在 Mac OS X 上定制安装程序行为 40
 - 禁用客户体验反馈模块 40
- 修改安装行为 (Linux) 41
 - 使用 ACTransform.xml 在 Linux 上定制安装程序行为 41
- 定制 AnyConnect GUI 文本和消息 41
 - 添加或编辑 AnyConnect 文本和消息 43
 - 将转换表导入自适应安全设备 45
 - 为企业部署创建消息目录 45
 - 将新消息合并到 ASA 上的定制转换表中 46
 - 在客户端上选择 Windows 的默认语言 47
- 为 AnyConnect GUI 创建定制图标和徽标 47
 - 更换 AnyConnect GUI 组件 48
 - Windows 的 AnyConnect 图标和徽标 49
 - Linux 的 AnyConnect 图标和徽标 52
 - Mac OS X 的 AnyConnect 图标和徽标 54
- 创建并上传 AnyConnect 客户端帮助文件 55
- 编写和部署脚本 56
 - 编写、测试和部署脚本 57
 - 为脚本配置 AnyConnect 配置文件 59
 - 脚本故障排除 59
- 使用 AnyConnect API 编写和部署定制应用 60
- 准备 AnyConnect 定制和本地化进行 ISE 部署 61
 - 准备 AnyConnect 本地化捆绑包 61

准备 AnyConnect 定制捆绑包	62
AnyConnect 配置文件编辑器	65
关于配置文件编辑器	65
AnyConnect 配置文件	65
从 ASDM 添加新配置文件	66
独立配置文件编辑器	66
安装独立 AnyConnect 配置文件编辑器	67
使用独立配置文件编辑器编辑客户端配置文件	68
AnyConnect VPN 配置文件	68
AnyConnect 配置文件编辑器, 首选项 (第 1 部分)	69
AnyConnect 配置文件编辑器, 首选项 (第 2 部分)	71
AnyConnect 配置文件编辑器, 备用服务器	75
AnyConnect 配置文件编辑器, 证书匹配	75
AnyConnect 配置文件编辑器, 证书注册	78
AnyConnect 配置文件编辑器, 移动策略	79
AnyConnect 配置文件编辑器, 服务器列表	79
AnyConnect 配置文件编辑器, 添加/编辑服务器列表	80
AnyConnect 本地策略	81
本地策略参数和值	82
手动更改本地策略参数	84
在 MST 文件中启用本地策略参数	85
通过“启用 FIPS”工具启用本地策略参数	86
配置 VPN 接入	87
连接和断开 VPN	87
AnyConnect VPN 连接选项	87
配置 VPN 连接服务器	89
登录前自动启动 Windows VPN 连接	90
关于“登录前启动”	90
“登录前启动”的限制	91
配置“登录前启动”	91
安装 AnyConnect “登录前启动”模块	91
在 AnyConnect 配置文件中启用 SBL	92

“登录前启动”故障排除	93
AnyConnect 启动时自动启动 VPN 连接	93
在 Windows 系统上配置登录前启动 (PLAP)	93
安装 PLAP	94
使用 PLAP 登录至 Windows PC	94
使用 PLAP 从 AnyConnect 断开连接	95
自动重新启动 VPN 连接	95
使用值得信赖的网络检测来连接和断开连接	96
关于值得信赖的网络检测	96
值得信赖的网络检测指南	96
配置值得信赖的网络检测	97
需要使用永远在线的 VPN 连接	98
关于永远在线 VPN	98
永远在线 VPN 的限制	99
永远在线 VPN 指南	99
配置永远在线 VPN	99
在 AnyConnect VPN 客户端配置文件中配置永远在线	100
向服务器列表添加负载均衡备用集群成员	100
豁免来自永远在线 VPN 的用户	101
为永远在线设置连接失败策略	102
关于连接失败策略	102
设置连接失败策略指南	102
配置连接失败策略	103
使用强制网络门户热点检测和补救	103
关于强制网络门户	103
配置强制网络门户补救	104
对强制网络门户检测和补救进行故障排除	104
通过 L2TP 或 PPTP 配置 AnyConnect	105
指示用户覆盖 PPP 排除	105
配置 AnyConnect 代理连接	106
关于 AnyConnect 代理连接	106
AnyConnect 代理连接的要求	107

- 代理连接的限制 107
- 允许本地代理连接 108
- 公共代理 108
 - 配置公共代理连接, Windows 108
 - 配置公共代理连接, Mac 109
 - 配置公共代理连接, Linux 109
- 配置专用代理连接 109
 - 将客户端配置为忽略浏览器代理设置 109
 - 锁定 Internet Explorer 的 Connections 选项卡 110
- 验证代理设置 110
- 选择并排除 VPN 流量 111
 - 将 IPv4 或 IPv6 流量配置为绕过 VPN 111
 - 配置支持本地打印机和关联设备的客户端防火墙 112
 - 配置拆分隧道 112
 - 拆分 DNS 112
 - 拆分 DNS 的要求 112
 - 配置拆分 DNS 112
 - 使用 AnyConnect 日志验证拆分 DNS 113
 - 检查哪些域使用拆分 DNS 113
- 管理 VPN 身份验证 114
 - 重要安全注意事项 114
 - 配置服务器证书处理 114
 - 服务器证书验证 114
 - 无效的服务器证书处理 115
 - 配置仅证书身份验证 117
 - 配置证书注册 118
 - SCEP 代理注册和操作 118
 - 传统 SCEP 注册和操作 119
 - 证书颁发机构要求 120
 - 证书注册指南 120
 - 配置 SCEP 代理证书注册 121
 - 为 SCEP 代理注册配置 VPN 客户端配置文件 121

配置 ASA 以支持 SCEP 代理注册	121
配置传统 SCEP 证书注册	122
为传统 SCEP 注册配置 VPN 客户端配置文件	122
配置 ASA 以支持传统 SCEP 注册	122
为 SCEP 设置 Windows 2008 服务器证书颁发机构	123
在证书颁发机构上禁用 SCEP 密码	123
在证书颁发机构上设置 SCEP 模板	124
配置证书到期通知	125
配置证书选择	126
配置要使用的 Windows 证书存储区	126
提示 Windows 用户选择身份验证证书	127
为 Mac 和 Linux 创建 PEM 证书存储区	128
配置证书匹配	129
配置密钥使用	129
配置扩展密钥使用	129
配置自定义扩展匹配密钥	130
配置证书可分辨名称	130
使用 SDI 令牌 (SoftID) 集成进行 VPN 身份验证	132
SDI 身份验证交换的类别	133
比较本地 SDI 与 RADIUS SDI	134
配置 ASA 以支持 RADIUS/SDI 消息	135
配置网络访问管理器	137
关于网络访问管理器	137
套件 B 和 FIPS	138
单点登录“单一用户”实施	138
配置单点登录单一用户实施	139
网络访问管理器部署	139
网络访问管理器配置文件	140
Client Policy 窗口	140
Authentication Policy 窗口	142
Networks 窗口	143
Networks 窗口的 Media Type 页面	144

Networks 窗口的 Security Level 页面	145
配置身份验证网络	145
802.1X Settings 窗格	145
Security 窗格	146
Port Authentication Exception Policy 窗格	147
关联模式	147
配置开放网络	147
配置共享密钥网络	148
Networks, Network Connection Type 窗格	149
Networks, User or Machine Authentication 页面	149
EAP 概述	150
EAP-GTC	150
EAP-TLS	151
EAP-TTLS	151
配置 EAP-TTLS	152
PEAP 选项	153
配置 PEAP	154
EAP-FAST 设置	154
配置 EAP-FAST	155
LEAP 设置	156
定义网络凭证	156
配置用户凭证	157
配置计算机凭证	159
配置受信任服务器验证规则	160
Network Groups 窗口	161
配置终端安全评估	163
ISE 终端安全评估模块提供的功能	164
终端安全评估检查	164
任何必要的补救措施	164
重新评估终端合规性	165
自动合规性	165
VLAN 监控和转换	166
用于中断 AnyConnect ISE 流的操作	166

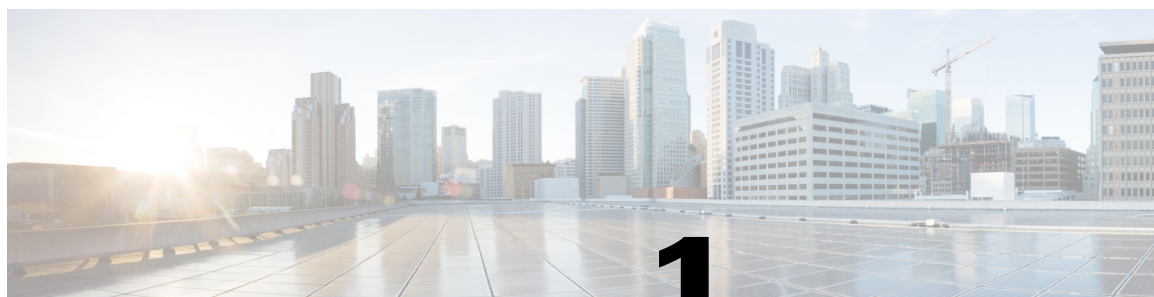
ISE 终端安全评估的状态	167
终端上的并发用户	169
终端安全评估模块的日志记录	169
终端安全评估模块的日志文件和位置	169
OPSWAT 支持图表	170
ASA 终端安全评估模块提供的功能	170
HostScan	170
基本功能	171
终端评估	171
高级终端评估：防病毒、反间谍软件和防火墙补救	171
为 HostScan 配置防病毒应用	172
与动态访问策略集成	172
DAP 中的 BIOS 序列号	172
将 BIOS 指定为 DAP 终端属性	173
如何获取 BIOS 序列号	173
确定在 ASA 上启用的 HostScan 映像	173
ISE 终端安全评估配置文件编辑器	173
高级面板	175
配置网络安全	177
关于网络安全模块	177
典型网络安全配置	178
客户端配置文件中的思科云网络安全扫描代理	178
用户如何选择扫描代理	179
更新扫描代理列表	179
向用户显示或隐藏扫描代理	180
选择默认扫描代理	181
指定 HTTP(S) 流量侦听端口	181
配置 Windows Internet 选项以配置公共代理	182
排除或包含来自网络扫描服务的终端流量	183
排除或包含主机例外	183
排除代理例外	184
排除静态例外	184

- 配置用户控制和计算最快的扫描代理响应时间 185
- 使用安全值得信赖的网络检测 186
 - 不使用安全值得信赖的网络检测 187
- 配置身份验证和将组成员身份发送到思科云网络安全代理 187
- 高级网络安全设置 189
 - 配置 KDF 侦听端口 189
 - 配置端口如何侦听传入连接 190
 - 配置超时/重试的发生时间 190
 - DNS 查找 191
 - 调试设置 191
 - 阻止和允许流量 191
- 其他可定制的网络安全性选项 192
 - 导出选项 192
 - 导出纯文本网络安全客户端配置文件 192
 - 导出 DART 捆绑包的纯文本网络安全客户端配置文件 192
 - 从 ASDM 编辑并导入明文网络安全客户端配置文件 192
 - 导出经过模糊处理的网络安全客户端配置文件 193
 - 为网络安全配置拆分隧道排除 193
 - 使用思科云网络安全托管配置文件 194
 - 关闭和启用 Cisco AnyConnect 网络安全代理 195
 - 使用 Windows 关闭和启用过滤器 195
 - 使用 Mac OS X 关闭和启用过滤器 195
- 网络安全日志记录 196
- 配置 AMP 启用程序 197
 - 关于 AMP 启用程序 197
 - AMP 启用程序部署 197
 - AMP 启用程序配置文件编辑器 198
 - AMP 启用程序的状态 198
- 在本地策略中启用 FIPS 199
 - 关于 FIPS、NGE 和 AnyConnect 199
 - AnyConnect 中的 FIPS 功能 200
 - AnyConnect FIPS 要求 200

AnyConnect FIPS 的限制	201
AnyConnect FIPS 指南	201
为 AnyConnect 核心 VPN 客户端配置 FIPS	202
为 AnyConnect 核心 VPN 启用 FIPS	202
在 Windows 安装期间启用 FIPS	202
为网络访问管理器配置 FIPS	203
为网络访问管理器启用 FIPS	203
为网络访问管理器实施 FIPS 模式	204
Cisco AnyConnect 客户体验反馈模块	205
配置客户体验反馈	205
移动设备上的 AnyConnect	207
移动设备上的 AnyConnect 操作和选项	207
关于 AnyConnect 移动 VPN 连接	207
移动设备上的 AnyConnect VPN 连接条目	208
隧道模式	208
移动设备的安全网关身份验证	209
移动设备上的客户端身份验证	209
在移动设备上本地化	210
移动设备上的 FIPS 和套件 B 加密	211
Apple iOS 设备上的 AnyConnect	212
Apple iOS 的特别注意事项	212
Android 设备上的 AnyConnect	215
Android 特定注意事项	215
在 ASA 安全网关上配置移动设备 VPN 连接	216
安装 Cisco AnyConnect 企业应用选择器工具	217
定义 Per App VPN 策略	218
创建 Per App 定制属性	219
将定制属性分配到 ASA 上的策略	220
在 AnyConnect VPN 配置文件中配置移动设备连接	220
AnyConnect 配置文件编辑器，移动设置	221
使用 URI 处理程序自动执行 AnyConnect 操作	223
生成 VPN 连接条目	224

- 建立 VPN 连接 227
- 断开 VPN 连接 229
- 导入证书 230
- 导入 VPN 客户端配置文件 230
- 对移动设备上的 Anyconnect 进行故障排除 230
- AnyConnect 故障排除 233**
 - 收集用于故障排除的信息 233
 - 查看统计详细信息 233
 - 运行 DART 以收集用于故障排除的数据 234
 - 获取计算机系统信息 235
 - 获取 Systeminfo 文件转储 235
 - 检查注册表文件 235
 - AnyConnect 日志文件的位置 235
 - AnyConnect 连接或断开连接问题 236
 - AnyConnect 无法建立初始连接或未断开连接 236
 - AnyConnect 无法传输流量 237
 - VPN 服务故障 238
 - VPN 服务连接失败 238
 - 确定服务的冲突项 239
 - VPN 客户端驱动程序遇到错误（Microsoft Windows 更新后） 239
 - 修复 VPN 客户端驱动程序错误 240
 - 驱动程序故障 240
 - 修复 VPNVA.sys 中的驱动程序故障 240
 - 修复 vpnagent.exe 中的驱动程序故障 240
 - 网络访问管理器的链路/驱动程序问题 241
 - 其他故障 241
 - AnyConnect 故障 241
 - 如何备份 .log 或 .dmp 文件 241
 - vpndownloader 中的 AnyConnect 故障（分层服务提供商 (LSP) 模块和 NOD32 AV） 242
 - 蓝屏（AT&T 拨号器） 242
 - 安全告警 242

- Microsoft Internet Explorer 安全告警 242
 - “Certified by an Unknown Authority” 告警 242
 - 在客户端上安装受信任根证书 242
- 掉线的连接 243
 - 无线连接在引入有线连接时掉线（Juniper Odyssey 客户端） 243
 - 配置 Odyssey 客户端 243
 - 连接 ASA 失败 (Kaspersky AV Workstation 6.x) 244
 - 没有 UDP DTLS 连接 (McAfee Firewall 5) 244
 - 连接主机设备失败（Microsoft 路由和远程访问服务器） 244
 - 连接失败/缺少凭证（负载均衡器） 244
- 安装故障 244
 - AnyConnect 无法下载 (Wave EMBASSY Trust Suite) 244
- 不兼容问题 245
 - 更新路由表失败（Bonjour 打印服务） 245
 - TUN 的版本不兼容（OpenVPN 客户端） 245
 - Winsock 目录冲突（LSP 症状 2 冲突） 245
 - 数据吞吐慢（LSP 症状 3 冲突） 245
 - 禁用 SSL 协议扫描 245
 - DPD 失败（EVDO 无线网卡和 Venturi 驱动程序） 246
 - DTLS 流量失败（DSL 路由器） 246
 - NETINTERFACE_ERROR（CheckPoint 和其他第三方软件，如 Kaspersky） 246
 - 性能问题（虚拟机网络服务驱动程序） 246
- 已知的第三方应用冲突 247



第 1 章

部署 AnyConnect

- [AnyConnect 部署概述](#)，第 1 页
- [为 AnyConnect 准备终端](#)，第 2 页
- [预部署 AnyConnect](#)，第 6 页
- [网络部署 AnyConnect](#)，第 18 页
- [更新 AnyConnect 软件和配置文件](#)，第 24 页
- [AnyConnect 参考信息](#)，第 31 页

AnyConnect 部署概述

部署 AnyConnect 指安装、配置和升级 AnyConnect 客户端及其相关文件。

Cisco AnyConnect 安全移动客户端可通过以下方法部署到远程用户：

- 预部署 - 新安装和升级可以由最终用户执行，也可以由企业软件管理系统 (SMS) 执行。
- 网络部署 - AnyConnect 软件包在头端（ASA 或 ISE 服务器）加载。当用户连接到 ASA 或 ISE 时，AnyConnect 会部署到客户端。

对于新安装，用户可连接到头端以下载 AnyConnect 客户端。客户端可手动或自动安装（通过网络启动）。

更新由已安装 AnyConnect 的系统上运行的 AnyConnect 完成，或者通过将用户定向至 ASA 无客户端门户完成。

部署 AnyConnect 时，您可以启用额外功能的可选模块以及用于配置 VPN 和可选功能的客户端配置文件。

有关 ASA、IOS、Microsoft Windows、Linux 和 Mac OS X 的系统、管理和终端要求，请参阅版本说明，即 [Cisco AnyConnect 安全移动客户端版本说明](#)，版本 4.1。

决定如何安装 AnyConnect

AnyConnect 可以由 ISE 1.3 和 ASA 头端进行网络部署。

- 从 ASA 进行网络部署 - 用户连接到 ASA 上的 AnyConnect 无客户端门户，然后选择下载 AnyConnect。ASA 下载 AnyConnect 下载程序。AnyConnect 下载程序下载客户端，安装客户端，并启动 VPN 连接。
- 从 ISE 版本 1.3 进行网络部署 - 用户连接到网络访问设备 (NAD)，例如 ASA、无线控制器或交换机。NAD 授权用户，并将用户重定向至 ISE 门户。AnyConnect 下载程序在客户端上安装，以管理软件包提取和安装，但不会启动 VPN 连接。

预部署指通过以下方式部署 AnyConnect:

- 企业软件管理系统 (SMS)，例如 Windows 转换。
- 手动 - 手动分发 AnyConnect 文件存档，附带指导用户如何安装的说明。对于 Windows，文件存档格式是 ISO；对于 Mac OS X，是 DMG；对于 Linux，是 gzip。

有关系统要求和许可依赖性，请参阅《AnyConnect 安全移动客户端功能、许可证和操作系统》：
<http://www.cisco.com/c/en/us/support/security/anyconnect-secure-mobility-client/products-feature-guides-list.html>

确定安装 AnyConnect 所需的资源

部署 AnyConnect 需要多种类型的文件:

- AnyConnect 核心客户端，包含在 AnyConnect 软件包中。
- 支持额外功能的模块，包含在 AnyConnect 软件包中。
- 配置 AnyConnect 和额外功能的客户端配置文件，您可以创建这些配置文件。
- 如果您要定制或本地化部署，还可以使用语言文件、图像、脚本和帮助文件。
- AnyConnect ISE 终端安全评估和合规性模块 (OPSWAT)。

为 AnyConnect 准备终端

结合使用 AnyConnect 和移动宽带卡

某些 3G 卡在使用 AnyConnect 前需要执行配置步骤。例如，VZAccess Manager 有三种设置:

- modem manually connects
- modem auto connect except when roaming
- LAN adapter auto connect

如果选择 **LAN adapter auto connect**，请将首选项设置为 NDIS 模式。NDIS 是“永远在线”的连接，即使在 VZAccess 管理器关闭时，您仍可保持连接状态。当 VZAccess 管理器为 AnyConnect 安

装准备就绪时，它将自动连接局域网适配器显示为设备连接首选项。当检测到 AnyConnect 接口时，3G 管理器将丢弃接口并允许 AnyConnect 连接。

当您进入更高优先级的连接时（有线网络的优先级最高，WiFi 次之，最后是移动宽带），AnyConnect 将在断开旧连接之前建立新连接。

在 Windows 上将 ASA 添加到 Internet Explorer 的受信任站点列表

Active Directory 管理员可以使用组策略将 ASA 添加到 Internet Explorer 中的受信任站点列表。此过程不同于本地用户在 Internet Explorer 中添加受信任站点的方式。

过程

- 步骤 1 在 Windows 域服务器上，以域管理员组成员的身份登录。
- 步骤 2 打开 Active Directory 用户和计算机 MMC 管理单元。
- 步骤 3 右键单击要在其中创建组策略对象的域或组织单元，然后单击 **Properties**。
- 步骤 4 选择 **Group Policy** 选项卡，然后单击 **New**。
- 步骤 5 为新的组策略对象键入名称，并按 **Enter** 键。
- 步骤 6 为阻止这一新策略应用于某些用户或组，请点击 **Properties**。选择 **Security** 选项卡。添加要阻止应用此策略的用户或组，然后在 Allow 列中清除 **Read** 和 **Apply Group Policy** 复选框。单击 **OK**。
- 步骤 7 单击 **Edit** 并选择 **User Configuration > Windows Settings > Internet Explorer Maintenance > Security**。
- 步骤 8 在右侧窗格中，右键单击 **Security Zones and Content Ratings**，然后单击 **Properties**。
- 步骤 9 选择 **Import the current security zones and privacy settings**。出现提示时，单击 **Continue**。
- 步骤 10 单击 **Modify Settings**，选择 **Trusted Sites**，然后单击 **Sites**。
- 步骤 11 键入要添加到受信任站点列表的安全设备的 URL，然后单击 **Add**。该格式可包含主机名 (<https://vpn.mycompany.com>) 或 IP 地址 (<https://192.168.1.100>)。它可以是精确匹配 (<https://vpn.mycompany.com>) 或使用通配符 (https://*.mycompany.com)。
- 步骤 12 单击 **Close**，并连续单击 **OK**，直至所有对话框都关闭。
- 步骤 13 留足时间让策略传播到整个域或林。
- 步骤 14 在 Internet 选项窗口中单击 **OK**。

阻止 Internet Explorer 中的代理更改

某些情况下，AnyConnect 会隐藏（锁定）Internet Explorer 的 **Tools > Internet Options > Connections** 选项卡。显示此选项卡时，可让用户设置代理信息。隐藏此选项卡可防止用户有意或无意绕过隧道。断开连接后，该选项卡的锁定设置会撤消。选项卡锁定可被应用于该选项卡的任何管理员定义的策略覆盖。在以下情况下应用锁定：

- ASA 配置指定 **Connections** 选项卡锁定

- ASA 配置指定专用端代理
- Windows 组策略之前锁定了 Connections 选项卡（覆盖未锁定的 ASA 组策略设置）

过程

-
- 步骤 1** 在 ASDM 中，转到 **Configuration > Remote Access VPN > Network (Client) Access > Group Policies**。
 - 步骤 2** 选择组策略，点击 **Edit** 或 **Add** 可编辑或新增组策略。
 - 步骤 3** 在导航窗格中，转到 **Advanced > Browser Proxy**。系统显示 Proxy Server Policy 窗格。
 - 步骤 4** 点击 **Proxy Lockdown** 以显示更多代理设置。
 - 步骤 5** 取消选中 **Inherit** 并选择以下两个选项之一：
 - **Yes**，将启用代理锁定，并在 AnyConnect 会话期间隐藏 Internet Explorer 的 Connections 选项卡。
 - **No**，将禁用代理锁定，并在 AnyConnect 会话期间显示 Internet Explorer 的 Connections 选项卡。
 - 步骤 6** 点击 **OK** 保存代理服务器策略更改。
 - 步骤 7** 点击 **Apply** 保存组策略更改。
-

配置 AnyConnect 如何处理 Windows RDP 会话

AnyConnect 可配置为允许来自 Windows RDP 会话的 VPN 连接。默认情况下，由 RDP 连接到计算机的用户无法启动使用 Cisco AnyConnect 安全移动客户端的 VPN 连接。下表显示来自 RDP 会话的 VPN 连接的登录和注销选项。这些选项在 VPN 客户端配置文件中配置。

首选项名称	值	在 SBL 模式下是否可用？
Windows Logon Enforcement	<ul style="list-style-type: none"> • Single Local Logon (默认值) - 在整个 VPN 连接期间只允许一个本地用户登录。此外，当一个或多个远程用户登录到客户端 PC 时，本地用户可以建立 VPN 连接。此设置对通过 VPN 连接从企业网络登录的远程用户没有影响。 <p>注释 如果为全有或全无隧道配置了 VPN 连接，则修改 VPN 连接的客户端 PC 路由表会导致远程登录断开连接。如果 VPN 连接进行了分割隧道配置，远程登录可能会也可能不会断开连接，这取决于 VPN 连接的路由配置。</p> <ul style="list-style-type: none"> • Single Logon - 在整个 VPN 连接期间只允许一个用户登录。如果通过本地或远程登录的用户不止一个，当 VPN 连接建立时，该连接不被允许。如果 VPN 连接期间有第二个用户通过本地或远程登录，则 VPN 连接将终止。由于在 VPN 连接期间不允许进行其他登录，所以无法通过 VPN 连接进行远程登录。 	是
Windows VPN Establishment	<ul style="list-style-type: none"> • Local Users Only (默认值) - 阻止远程登录用户建立 VPN 连接。此功能与 AnyConnect 早期版本中的功能相同。 • Allow Remote Users - 允许远程用户建立 VPN 连接。但是，如果所配置的 VPN 连接路由导致远程用户断开连接，则 VPN 连接会终止，以允许远程用户重新获得对客户端 PC 的访问权限。如果远程用户想要断开其远程登录会话而不终止 VPN 连接，则必须在 VPN 建立后等待 90 秒钟。 	否

有关其他 VPN 会话连接选项，请参阅 [AnyConnect VPN 连接选项](#)。

Windows 上仅使用 DES 的 SSL 加密

默认情况下，Windows 不支持 DES SSL 加密。如果在 ASA 上配置仅使用 DES，AnyConnect 连接将失败。由于很难将这些操作系统配置为使用 DES，因此建议不要将 ASA 配置为仅使用 DES 的 SSL 加密。

预部署 AnyConnect

可使用 SMS 预部署 AnyConnect，方法是手动为最终用户分发要安装的文件或向用户提供 AnyConnect 文件存档以供连接。

当创建文件存档以安装 AnyConnect 时，存档的目录结构必须与客户端上安装的文件目录结构一致，如中所述。 [预部署 AnyConnect 配置文件的位置，第 8 页](#)

开始之前

如果手动部署 VPN 配置文件，还必须将配置文件上传到头端。当客户端系统连接时，AnyConnect 会验证客户端上的配置文件是否与头端上的配置文件匹配。如果已禁用配置文件更新，并且头端上的配置文件与客户端上的配置文件不同，则手动部署的配置文件将不起作用。

如果手动部署 AnyConnect ISE 终端安全评估配置文件，您还必须将该文件上传到 ISE。

过程

- 步骤 1** 下载 AnyConnect 预部署软件包。
用于预部署的 AnyConnect 文件在 cisco.com 上提供。

操作系统	AnyConnect 预部署软件包名称
Windows	anyconnect-win-<version>-pre-deploy-k9.iso
Mac OS X	anyconnect-macosx-i386-<version>-k9.dmg
Linux (64位)	anyconnect-predeploy-linux-64-<version>-k9.tar.gz

- 步骤 2** 创建客户端配置文件；某些模块和功能需要客户端配置文件。
以下模块需要客户端配置文件：

- AnyConnect VPN
- Cisco AnyConnect 网络访问管理器
- AnyConnect 网络安全
- AnyConnect ISE 终端安全评估
- AnyConnect AMP 启用程序

以下模块不需要 AnyConnect 客户端配置文件：

- AnyConnect VPN 登录前开始
- AnyConnect 诊断和报告工具
- AnyConnect 终端安全评估
- AnyConnect 客户体验反馈

可在 ASDM 中创建客户端配置文件，并将这些文件复制到您的 PC。或者，您可以使用 Windows PC 上的独立配置文件编辑器。有关 Windows 独立编辑器的详细信息，请参阅[关于配置文件编辑器](#)。

步骤 3 或者，[定制和本地化 AnyConnect 客户端和安装程序](#)。

步骤 4 准备分发的文件。这些文件的目录结构在[预部署 AnyConnect 配置文件的位置](#)中进行了描述。

步骤 5 创建 AnyConnect 安装所需的所有文件后，可将它们分发在一个存档文件中，或将这些文件复制到客户端。确保您计划连接到的头端（ASA 和 ISE）上也有相同的 AnyConnect 文件。

用于预部署和网络部署的 AnyConnect 模块可执行文件

下表列出了将网络访问管理器、AMP 启用程序及网络安全客户端预部署或网络部署到 Windows 计算机时终端计算机上的文件名：

表 1: 网络部署或预部署的模块文件名

模块	网络部署安装程序（已下载）	预部署安装程序
网络访问管理器	AnyConnect NAM WINS <i>x.x.x - k9</i> . <i>msi</i>	AnyConnect NAM WINS <i>x.x.x - k9</i> . <i>msi</i>
网络安全	anyconnect-websecurity-win- <i>x.x.x</i> -web-deploy-k9.exe	anyconnect-websecurity-win- <i>x.x.x</i> -pre-deploy-k9.msi
ISE 终端安全评估	anyconnect-iseposture-win- <i>x.x.x</i> -web-deploy-k9.msi	anyconnect-iseposture-win- <i>x.x.x</i> -pre-deploy-k9.msi
AMP 启用程序	anyconnect-amp-win- <i>x.x.x</i> -web-deploy-k9.exe	anyconnect-amp-win- <i>x.x.x</i> -pre-deploy-k9.msi



注释

如果有 Windows 2008R2 服务器，在尝试安装 AnyConnect 网络访问管理器时，可能会发生安装错误。默认情况下，服务器操作系统上未安装 WLAN 服务，因此，您必须安装并重新启动 PC。

预部署 AnyConnect 配置文件的位置

如果要将文件复制到客户端系统，下表显示您必须将文件放置到的位置。

表 2: *AnyConnect* 核心文件

文件	描述
<i>anyfilename.xml</i>	AnyConnect 配置文件 此文件指定了为特定用户类型配置的功能和属性值。
AnyConnectProfile.xsd	定义 XML 架构格式。 AnyConnect 使用此文件验证配置文件。

表 3: 所有操作系统的配置文件位置

操作系统	模块	位置
Windows 7 和 8.x	使用 VPN 的核心客户端	%ProgramData%\Cisco\Cisco AnyConnect Secure Mobility Client\Profile
	网络访问管理器	%ProgramData%\Cisco\Cisco AnyConnect Secure Mobility Client\NetworkAccessManager\newConfigFiles
	网络安全	%ProgramData%\Cisco\Cisco AnyConnect Secure Mobility Client\Web Security
	客户体验反馈	%ProgramData%\Cisco\Cisco AnyConnect Secure Mobility Client\CustomerExperienceFeedback
	OPSWAT	%PROGRAMFILES%\Cisco\Cisco AnyConnect Secure Mobility Client\opswat
	ISE 终端安全评估	%ProgramData%\Cisco\Cisco AnyConnect Secure Mobility Client\ISE Posture
	AMP 启用程序	%ProgramData%\Cisco\Cisco AnyConnect Secure Mobility Client\AMP Enabler

操作系统	模块	位置
Mac OS X	所有其他模块	/opt/cisco/anyconnect/profile
	客户体验反馈	/opt/cisco/anyconnect/CustomerExperienceFeedback
	二进制文件	/opt/cisco/anyconnect/bin
	OPSWAT	/opt/cisco/anyconnect/lib/opswa
	图书馆	/opt/cisco/anyconnect/lib
	用户界面资源	/Applications/Cisco/Cisco AnyConnect Secure Mobility Client.app/Contents/Resources/
	ISE 终端安全评估	/opt/cisco/anyconnect/iseposture/
	AMP 启用程序	/opt/cisco/anyconnect/ampenabler/
Linux	所有模块	/opt/cisco/anyconnect/profile

将 AnyConnect 模块预部署为独立应用

网络访问管理器和网络安全模块可作为独立应用运行。安装 AnyConnect 核心客户端，但不使用 VPN 和 AnyConnect UI。

在 Windows 上使用 SMS 部署独立模块

过程

- 步骤 1** 通过配置软件管理系统 (SMS) 来设置 MSI 属性 PRE_DEPLOY_DISABLE_VPN=1，从而禁用 VPN 功能。例如：

```
msiexec /package anyconnect-win-ver-pre-deploy-k9.msi /norestart /passive
PRE_DEPLOY_DISABLE_VPN=1 /lvx* <log_file_name>
```

MSI 将其中嵌入的 VPNDisable_ServiceProfile.xml 文件复制到为 VPN 功能的配置文件指定的目录。

- 步骤 2** 安装模块。例如，以下 CLI 命令安装网络安全：

```
msiexec /package anyconnect-websecurity-win-<version>-pre-deploy-k9.msi /norestart /passive
/lvx* c:\test.log
```

步骤 3 (可选) 安装 DART。

```
msiexec /package anyconnect-dart-win-<version>-k9.msi /norestart /passive /lvx* c:\test.log
```

步骤 4 将模糊的网络安全客户端配置文件的副本保存到适当的 Windows 文件夹。

步骤 5 重新启动 Cisco AnyConnect 网络安全代理 Windows 服务。

将网络访问管理器和网络安全部署为独立应用

您可以将 AnyConnect 模块“网络访问管理器”和“网络安全”部署为用户计算机上的独立应用程序。DART 得到这些应用程序的支持。

要求

VPNDisable_ServiceProfile.xml 文件还必须是在 VPN 客户端配置文件目录中的唯一 AnyConnect 配置文件。

独立模块的用户安装

您可以手动拆分各个安装程序并将它们分发给用户。

如果您决定向用户提供 ISO 映像并要求他们安装，请务必向用户说明仅安装独立模块。



注释 如果计算机中此前未安装网络访问管理器，用户必须重启计算机才能完成网络访问管理器安装。此外，如果安装属于需要升级某些系统文件的升级安装，用户也必须重启计算机。

过程

步骤 1 指导用户检查 AnyConnect 网络访问管理器或 AnyConnect 网络安全模块。

步骤 2 指导用户取消选中 **Cisco AnyConnect VPN Module**。

这将禁用核心客户端的 VPN 功能，安装实用程序将网络访问管理器和网络安全安装为不具有 VPN 功能的独立应用。

步骤 3 (可选) 选中 **Lock Down Component Services** 复选框。锁定组件服务将阻止用户关闭或停止 Windows 网络安全服务。

步骤 4 指导用户运行可选模块的安装程序，这些模块可在没有 VPN 服务的情况下使用 AnyConnect GUI。如果用户点击 **Install Selected** 按钮，将发生以下情况：

- a) 弹出一个对话框，要求确认独立网络访问管理器和/或独立网络安全模块的选择。
- b) 如果用户点击 OK，安装实用程序将使用 `PRE_DEPLOY_DISABLE_VPN=1` 设置调用 AnyConnect 核心安装程序。

- c) 安装实用程序将删除所有现有 VPN 配置文件，然后安装 VPNDisable_ServiceProfile.xml。
- d) 安装实用程序将调用网络访问管理器安装程序或网络安全安装程序。
- e) 计算机将启用网络访问管理器或网络安全模块，但不提供 VPN 服务。

预部署到 Windows

使用 ISO 分发 AnyConnect

ISO 软件包文件包含安装实用程序（用于启动单个组件安装程序的选择器菜单程序）以及核心和可选 AnyConnect 模块的 MSI。将 ISO 软件包文件提供给用户后，用户运行安装程序 (setup.exe)。该程序显示安装实用程序菜单，用户从中选择要安装的 AnyConnect 模块。您可能不希望用户选择要加载哪些模块。因此，如果您决定使用 ISO 进行分发，请编辑 ISO 以删除不想使用的模块，然后编辑 HTA 文件。

分发 ISO 的一种方法是使用虚拟 CD 挂载软件，如 SlySoft 或 PowerIS。

预部署 ISO 修改

- 使用您在捆绑文件时创建的配置文件更新 ISO 文件，并删除不希望分发的任何模块安装程序。
- 编辑 HTA 文件可对安装菜单进行个性化设置，并删除到不希望分发的任何模块安装程序的链接。

AnyConnect ISO 文件内容

文件	目的
GUI.ico	AnyConnect 图标图像。
Setup.exe	启动安装实用程序。
anyconnect-dart-win-x.x.x-k9.msi	DART 可选模块的 MSI 安装程序文件。
anyconnect-gina-win-x.x.x-pre-deploy-k9.msi	SBL 可选模块的 SBL 安装程序文件。
anyconnect-ise posture-win-x.x.x-pre-deploy-k9.msi	ISE 终端安全评估模块的 MSI 安装程序。
anyconnect-amp-win-x.x.x-pre-deploy-k9.msi	AMP Enabler 的 MSI 安装程序。
anyconnect-nam-win-x.x.x.msi	网络访问管理器可选模块的 MSI 安装程序文件。
anyconnect-posture-win-x.x.x-pre-deploy-k9.msi	终端安全评估模块的 MSI 安装程序文件。
anyconnect-websecurity-win-x.x.x-pre-deploy-k9.msi	网络安全可选模块的 MSI 安装程序文件。
anyconnect-win-x.x.x-pre-deploy-k9.msi	AnyConnect 核心客户端的 MSI 安装程序文件。

文件	目的
autorun.inf	setup.exe 的信息文件。
eula.html	可接受使用政策。
setup.hta	安装实用程序 HTML 应用 (HTA)，您可以针对自己的站点进行定制。

使用 SMS 分发 AnyConnect

从 ISO 映像提取要部署的模块的安装程序 (*.msi) 后，可以手动分发这些安装程序。

必须按照第 2-24 页上的“使用 SMS 预部署 AnyConnect 模块”一节所述的顺序安装预部署模块。

要求

- 在 Windows 上安装 AnyConnect 时，必须禁用 AlwaysInstallElevated 或 Windows 用户帐户控制 (UAC) 组策略设置。否则，AnyConnect 安装程序可能无法访问安装所需的某些目录。
- Microsoft Internet Explorer (MSIE) 用户应将头端添加到受信任站点列表或安装 Java。添加到受信任站点列表会启用 ActiveX 控件进行安装，此时用户交互最少。

配置文件部署过程

- 如果使用 MSI 安装程序，MSI 将选择已放置在 Profiles 文件夹中的任何配置文件并在安装过程中将其放置在相应的文件夹中。在 CCO 上可用的预部署 MSI 文件中会提供适当的文件夹路径。
- 如果在安装后手动预部署配置文件，请手动复制配置文件或使用 SMS（如 Altiris）将配置文件部署到相应的文件夹。
- 确保放到头端上的客户端配置文件与预部署到客户端的客户端配置文件相同。如果客户端配置文件与头端配置文件不匹配，可能会获得不一致的行为，包括拒绝访问。

Windows 预部署 MSI 示例

已安装的模块	命令和日志文件
没有 VPN 功能的 AnyConnect 核心客户端。 安装独立网络访问管理器或网络安全模块时使用。	<pre>msiexec /package anyconnect-win-x.x.x-pre-deploy-k9.msi /norestart /passive PRE_DEPLOY_DISABLE_VPN=1 /lvx*</pre> <p>anyconnect-win-x.x.x-pre-deploy-k9-install-datetimestamp.log</p>

已安装的模块	命令和日志文件
有 VPN 功能的 AnyConnect 核心客户端。	msiexec /package anyconnect-win-x.x.x-pre-deploy-k9.msi /norestart /passive /lvx* anyconnect-win-x.x.x-pre-deploy-k9-install-datetimestamp.log
客户体验反馈	msiexec /package anyconnect-win-x.x.x-pre-deploy-k9.msi /norestart /passive DISABLE_CUSTOMER_EXPERIENCE_FEEDBACK=1 /lvx* anyconnect-win-x.x.x-pre-deploy-k9-install-datetimestamp.log
诊断和报告工具 (DART)	msiexec /package anyconnect-dart-win-x.x.x-k9.msi /norestart /passive /lvx* anyconnect-dart-x.x.x-pre-deploy-k9-install-datetimestamp.log
SBL	msiexec /package anyconnect-gina-win-x.x.x-k9.msi /norestart /passive /lvx* anyconnect-gina-x.x.x-pre-deploy-k9-install-datetimestamp.log
网络访问管理器	msiexec /package anyconnect-nam-win-x.x.x-k9.msi /norestart /passive /lvx* anyconnect-nam-x.x.x-pre-deploy-k9-install-datetimestamp.log
网络安全	msiexec /package anyconnect-websecurity-win-x.x.x-pre-deploy-k9.msi /norestart/passive /lvx* anyconnect-websecurity-x.x.x-pre-deploy-k9-install-datetimestamp.log
ASA 终端安全评估	msiexec /package anyconnect-posture-win-x.x.x-pre-deploy-k9.msi /norestart/passive /lvx* anyconnect-posture-x.x.x-pre-deploy-k9-install-datetimestamp.log
ISE 终端安全评估	msiexec /package anyconnect-ise posture-win-x.x.x-pre-deploy-k9.msi /norestart/passive /lvx* anyconnect-ise posture-x.x.x-pre-deploy-k9-install-datetimestamp.log
AMP 启用程序	msiexec /package anyconnect-amp-win-x.x.x-pre-deploy-k9.msi /norestart/passive /lvx* AnyConnect amp x.x.x - pre - deploy - k9 - install - datetimestamp.log

AnyConnect 示例 Windows 转换

思科提供示例 Windows 转换以及介绍如何使用转换的文档。以下划线字符 () 开头的转换是一般 Windows 转换。以字母字符开头的转换是 VPN 转换。每个转换都有使用说明文档。转换下载是 sampleTransforms-x.x.x.zip。

Windows 预部署安全选项

思科建议授予最终用户对托管 Cisco AnyConnect 安全移动客户端的设备的有限权限。如果最终用户确保其他权利，则安装程序可提供锁定功能，防止用户和本地管理员关闭或停止终端上建立为锁定的 Windows 服务。在网络安全模块中，您可以使用服务密码将客户端设置为绕过模式。您还可以阻止用户卸载 AnyConnect。

Windows 锁定属性

每个 MSI 安装程序都支持通用属性 (LOCKDOWN)，当该属性设置为非零值时，可防止与安装程序相关的 Windows 服务被终端设备上的用户或本地管理员控制。我们建议您使用安装时提供的示例转换来设置该属性，并将转换应用至您想锁定的每个 MSI 安装程序。锁定选项同样是 ISO 安装实用程序中的一个复选框。

从添加/删除程序列表中隐藏 AnyConnect

您可以隐藏安装的 AnyConnect 模块，这样用户从 Windows 添加/删除程序列表中便看不到该模块。即使您使用 ARPSYSTEMCOMPONENT=1 启动任何安装程序，该模块都不会显示在 Windows 添加/删除程序列表中。

我们建议您使用我们提供的示例转换来设置此属性。将该转换应用于您希望隐藏的每个模块的每个 MSI 安装程序。

Windows 上的 AnyConnect 模块安装和删除顺序

模块安装程序在开始安装之前会确认其版本与核心客户端相同。如果版本不匹配，该模块不会安装，并且安装程序通知用户存在版本不匹配。如果您使用安装实用程序，则会构建软件包中的模块并将其封装在一起，且版本始终匹配。

以下步骤列出必须遵守的 AnyConnect 模块安装顺序。

过程

-
- 步骤 1** 安装 AnyConnect 核心客户端模块，此过程会安装 GUI 和 VPN 功能（SSL 和 IPsec）。
 - 步骤 2** 安装 AnyConnect 诊断和报告工具 (DART) 模块，以提供有关 AnyConnect 核心客户端安装的有用诊断信息。
 - 步骤 3** 按任意顺序安装 AMP 启用程序、SBL、网络访问管理器、网络安全或终端安全评估模块。
 - 步骤 4** 按任意顺序卸载 AMP 启用程序、网络访问管理器、网络安全、终端安全评估或 SBL。
 - 步骤 5** 卸载 AnyConnect 核心客户端。
 - 步骤 6** 最后卸载 DART。如果卸载过程失败，DART 信息会很有用。
-



注释 根据设计，卸载 AnyConnect 后，某些 XML 文件仍然保留。

预部署到 Mac OS X

在 Mac OS X 上安装和卸载 AnyConnect

用于 Mac OS X 的 AnyConnect 以 DMG 文件形式分配，其中包括所有 AnyConnect 模块。当用户打开 DMG 文件，然后运行 AnyConnect.pkg 文件时，系统会启动安装对话框，引导用户完成安装。在 Installation Type 屏幕上，用户可以选择要安装的软件包（模块）。

要从您的分配中删除任何 AnyConnect 模块，可使用 Apple pkgutil 工具，并在修改后签署软件包。也可以使用 ACTransforms.xml 修改安装程序。您可以定制语言和外观，以及更改一些其他安装操作，如 [Cisco AnyConnect 安全移动客户端管理员指南，版本 4.1](#) 的“定制”章节中所述。

在 Mac OS X 上将网络安全模块安装为独立应用

可以只安装网络安全模块而不要 VPN。不使用 VPN 和 AnyConnect UI。

以下过程通过安装独立配置文件编辑器、创建网络安全配置文件和将该网络安全配置文件添加到 DMG 软件包中，来说明如何定制网络安全模块。它还将 AnyConnect 用户界面设置为在启动时自动启动，这使 AnyConnect 可以为网络安全模块提供必要的用户和组信息。

过程

- 步骤 1** 从思科 ScanCenter 支持区域或从 Cisco.com 下载区域下载 Cisco AnyConnect 安全移动客户端 DMG 软件包。
- 步骤 2** 打开文件访问安装程序。请注意，下载的映像是只读文件。
- 步骤 3** 通过运行磁盘实用程序或使用终端应用以使安装程序映像可写入，如下所示：

```
hdiutil convert <source dmg> -format UDRW -o <output dmg>
```
- 步骤 4** 在运行 Windows 操作系统的计算机上安装独立配置文件编辑器。默认情况下，不安装网络安全配置文件编辑器组件。您必须在定制安装或完全安装过程中选择该组件。
- 步骤 5** 启动网络安全配置文件编辑器并创建配置文件。
- 步骤 6** 在安全位置将配置文件另存为 WebSecurity_ServiceProfile.xml。
网络安全配置文件编辑器创建另一个名为 WebSecurity_ServiceProfile.wso 的配置文件的模糊版本，并将其保存在 WebSecurity_ServiceProfile.xml 文件的保存位置。
- 步骤 7** 将 WebSecurity_ServiceProfile.wso 文件从 Windows 计算机复制到 AnyConnect x.x.x/Profiles/websecurityMac OS X 安装程序软件包。或者，使用终端应用，如下所示：

```
cp <path to the wso> \Volumes\"AnyConnect <VERSION>\Profiles\websecurity\
```

- 步骤 8** 在 Mac OS X 安装程序中，转到 AnyConnect x.x.x/Profiles 目录并在 TextEdit 中打开 ACTransforms.xml 文件进行编辑。将 <DisableVPN> 元素设置为 **True** 可确保不安装 VPN 功能：
- ```
<ACTransforms>
<DisableVPN>True</DisableVPN>
</ACTransforms>
```
- 步骤 9** 在 Cisco.com 上用于 Cisco AnyConnect 安全移动客户端 x.x.x 的下载区域中，找到 VPNDisable\_ServiceProfile.xml 文件并将其下载到您要安装 AnyConnect 网络安全的计算机，然后将其保存到 AnyConnect 安装程序的 AnyConnect x.x.x/profiles/vpn 目录。
- 步骤 10** AnyConnect DMG 数据包现在已准备就绪，可分配给您的用户。

## 限制 Mac OS X 上的应用

Mac OS X 10.8 推出了一项称为 Gatekeeper 的新功能，该功能可限制允许在系统上运行的应用。您可选择允许从以下位置下载的应用：

- Mac App Store
- Mac App Store 和已确定的开发商
- 任何地点

默认设置为 Mac App Store and identified developers（已签名的应用）。

AnyConnect 当前版本是使用 Apple 证书的已签名应用。如果（仅）面向 Mac App Store 配置 Gatekeeper，则您必须选择 Anywhere 设置或按住 Ctrl 键点击，以绕过选定的设置，进而通过预部署的安装方式安装和运行 AnyConnect。有关详细信息，请参阅：<http://www.apple.com/macosx/mountain-lion/security.html>。

## 预部署到 Linux

### 安装用于 Linux 的模块

您可以打开用于 Linux 的单个安装程序并手动分配它们。预部署安装包中的各个安装程序均可以单独运行。使用压缩文件实用程序查看和提取 tar.gz 文件中的文件。

#### 过程

- 步骤 1** 安装 AnyConnect 核心客户端模块，此过程会安装 GUI 和 VPN 功能（SSL 和 IPsec）。
- 步骤 2** 安装 DART 模块，该模块提供关于 AnyConnect 核心客户端安装的有用诊断信息。
- 步骤 3** 安装终端安全评估模块。



## 卸载用于 Linux 的模块

用户卸载 AnyConnect 的顺序非常重要。  
如果卸载过程失败，DART 信息将非常有价值。

### 过程

- 
- 步骤 1** 卸载状态模块。
  - 步骤 2** 卸载 AnyConnect 核心客户端。
  - 步骤 3** 卸载 DART。
- 

## 初始化 Firefox 的服务器证书验证

如果要将服务器证书与 AnyConnect 配合使用，必须使 AnyConnect 可访问证书存储区，并将证书验证为受信任。默认情况下，AnyConnect 使用 Firefox 证书存储区。

### 激活 Firefox 证书存储区

在 Linux 设备上安装 AnyConnect 后，请在首次尝试连接 AnyConnect 前打开 Firefox 浏览器。打开 Firefox 后，会创建一个包含证书存储区的配置文件。

### 如果不使用 Firefox 证书存储区

如果选择不使用 Firefox，则必须将本地策略配置为排除 Firefox 证书存储区，并且必须配置 PEM 存储区。

### 多模块要求

如果部署核心客户端以及一个或多个可选模块，则必须对每个安装程序应用锁定属性。以下小节中介绍锁定：[Windows 预部署 MSI 示例，第 12 页](#)

此操作适用于 VPN 安装程序、网络访问管理器安装程序和网络安全安装程序。



---

**注释** 如果选择激活对 VPN 安装程序的锁定，将因此也会锁定 AMP 启用程序。

---

## 在 Linux 设备上手动安装 DART

- 1** 将 anyconnect-dart-linux-(ver)-k9.tar.gz 存储在本地。如果您使用 3.0.3050 版本或更高版本进行安装，则此 DART 组件已包含在 anyconnect-linux-(ver)-k9.pkg 下载中。
- 2** 从终端使用 `tar -zxvf <含文件名的 tar.gz 文件路径命令` 提取 tar.gz 文件。

- 3 从终端导航到提取的文件夹，并使用 `sudo ./dart_install.sh` 命令运行 `dart_install.sh`。
- 4 接受许可协议，并等待安装完成。



注释 您仅可使用 `/opt/cisco/anyconnect/dart/dart_uninstall.sh` 卸载 DART。

## 网络部署 AnyConnect

网络部署是指客户端系统上的 AnyConnect 下载程序从头端获取 AnyConnect 软件或使用头端上的门户安装或更新 AnyConnect。

### 使用 ASA 的网络部署

ASA 上的无客户端门户执行 AnyConnect 网络部署。流程如下：

用户打开浏览器并连接到 ASA 的无客户端门户。ASA 建立与客户端的初始 SSL 连接，并打开登录页。如果用户成功登录并通过身份验证，无客户端门户页面将显示 Start AnyConnect Client 对话框。用户选择 AnyConnect 下载后，ASA 将下载与其计算机的操作系统匹配的客户端。下载完成后，客户端将进行安装和自我配置，并建立与 ASA 的 IPsec (IKEv2) 或 SSL 连接（网络启动）。如果网络启动由于 ActiveX 或 Java 问题而无法运行，则用户可手动下载 AnyConnect。

### ASA 网络部署限制

- 不支持将同一 O/S 的多个 AnyConnect 软件包加载到 ASA。
- 网络部署时，ASA 终端安全评估模块中不含 OPSWAT 定义。您必须手动部署主机扫描模块或将其加载到 ASA 上，以向客户端提供 OPSWAT 定义。
- 如果 ASA 只有默认内部闪存大小，您在 ASA 上存储和加载多个 AnyConnect 客户端软件包时可能会遇到问题。即使您的闪存有足够的空间承载软件包，ASA 也可能在解压缩和加载客户端映像时耗尽缓存内存。有关部署 AnyConnect 以及升级 ASA 内存时 ASA 内存要求的详细信息，请参阅最新的 VPN 设备发行说明。
- 用户可使用 IP 地址或 DNS 连接到 ASA，但不支持链路本地安全网关地址。
- 您必须将支持网络启动的安全设备的 URL 添加到 Internet Explorer 的受信任站点列表中。可使用组策略完成此操作，如在 [Windows 上将 ASA 添加到 Internet Explorer 的受信任站点列表](#) 所述。

### 使用 ISE 的网络部署

ISE 上的策略确定 AnyConnect 客户端的部署时间。用户打开浏览器并连接到 ISE 控制的资源，然后重新定向到 AnyConnect 客户端门户。该 ISE 门户将帮助用户下载和安装 AnyConnect。在 Internet Explorer 中，ActiveX 控件将指导用户进行安装。在其他浏览器中，门户将下载网络设置助理，该工具会帮助用户安装 AnyConnect。

### ISE 部署限制

- 如果 ISE 和 ASA 均执行 AnyConnect 网络部署，则两个头端上的配置必须匹配。
- 如果在 ISE 客户端调配策略中配置了 AnyConnect ISE 终端安全评估代理，则 ISE 服务器只能由该代理发现。ISE 管理员可在 Agent Configuration > Policy > Client Provisioning 下配置 NAC 代理或 AnyConnect ISE 终端安全评估模块。

## 在 ASA 上配置网络部署

### WebLaunch 的浏览器限制

表 4: 操作系统支持的 *Weblaunch* 的 *AnyConnect* 浏览器

操作系统	浏览器
Windows 8.x x86 (32 位) 和 x64 (64 位)	Internet Explorer 10 Firefox 9.0.1 及更高版本 Chrome 23.0.1271.95 m 及更高版本
Windows 7 x86 (32 位) 和 x64 (64 位)	Internet Explorer 8 和 9 Firefox 3 及更高版本 Google Chrome 6 及更高版本
Mac OS X 10.7、10.8 (32 位和 64 位)	Safari 2 及更高版本 Google Chrome 6 及更高版本
Linux64 (仅限 VPN 安装)	Firefox 3 及更高版本

### 下载 AnyConnect 软件包

从 [Cisco AnyConnect 软件下载](#) 网页下载最新的 Cisco AnyConnect 安全移动客户端软件包。

操作系统	AnyConnect 网络部署软件包名称
Windows	anyconnect-win-x.x.x-k9.pkg
Mac OS X	anyconnect-macosx-i386-x.x.x-k9.pkg
Linux (64 位)	anyconnect-linux-64-x.x.x-k9.pkg



---

注释 您不应具有 ASA 上同一操作系统的不同版本。

---

## 在 ASA 上加载 AnyConnect 软件包

### 过程

- 
- 步骤 1** 导航到 **Configuration > Remote Access > VPN > Network (Client) Access > AnyConnect Client Software**。AnyConnect 客户端映像面板会显示当前在 ASA 上加载的 AnyConnect 映像。映像出现的顺序是 ASA 将其下载到远程计算机的顺序。
- 步骤 2** 要添加 AnyConnect 映像，点击 **Add**。
- 点击 **Browse Flash** 可选择已上传到 ASA 的 AnyConnect 映像。
  - 点击 **Upload** 浏览至您存储于本地计算机上的 AnyConnect 图像。
- 步骤 3** 点击 **OK** 或 **Upload**。
- 步骤 4** 点击 **Apply**。
- 

## 启用其他 AnyConnect 模块

要启用其他功能，请在组策略或本地用户配置中指定新模块名称。注意启用附加模块将影响下载时间。启用功能时，AnyConnect 必须将这些模块下载到 VPN 终端。



---

注释 如果您选择 Start Before Logon，还必须在 AnyConnect 客户端配置文件中启用此功能。

---

### 过程

- 
- 步骤 1** 在 ASDM 中，转到 **Configuration > Remote Access VPN > Network (Client) Access > Group Policies**。
- 步骤 2** 选择组策略，点击 **Edit** 或 **Add** 可编辑或新增组策略。
- 步骤 3** 在导航窗格中，选择 **VPN Policy (> AnyConnect Client**。在 **Client Modules to Download** 中，点击 **Add**，然后选择要添加到此组策略的每个模块。可用的模块是您添加或上传到 ASA 的模块。
- 步骤 4** 点击 **Apply** 并保存对组策略的更改。
-

## 在 ASDM 中创建客户端配置文件

必须将 AnyConnect 网络部署软件包添加到 ASA，然后才能在 ASA 上创建客户端配置文件。

### 过程

- 步骤 1 导航到 **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Profile**。
- 步骤 2 选择要与组关联的客户端配置文件，然后点击 **Change Group Policy**。
- 步骤 3 在 **Change Policy for Profile** 策略名称窗口中，从 **Available Group Policies** 字段中选择组策略，然后点击右箭头，将其移到 **Policies** 字段。
- 步骤 4 点击 **OK**。
- 步骤 5 在 **AnyConnect Client Profile** 页面上，点击 **Apply**。
- 步骤 6 点击 **Save**。
- 步骤 7 完成配置时，点击 **OK**。

## 在 ISE 上配置网络部署

ISE 可配置和部署 AnyConnect 核心、ISE 终端安全评估模块和 OPSWAT（合规性模块）以支持 ISE 的终端安全评估。ISE 还可以部署在连接到 ASA 时可使用的所有 AnyConnect 模块和资源。当用户浏览到 ISE 控制的资源时：

- 如果 ISE 在 ASA 之后，则用户连接 ASA，下载 AnyConnect，然后建立 VPN 连接。如果 AnyConnect ISE 终端安全评估并非由 ASA 安装，则用户将重定向到 AnyConnect 客户端门户来安装 ISE 终端安全评估。
- 如果 ISE 不在 ASA 之后，则用户连接到 AnyConnect 客户端门户，该门户会引导用户在 ISE 上安装 AnyConnect 配置中定义的 AnyConnect 资源。如果 ISE 终端安全评估状态未知，常见配置是将浏览器重定向到 AnyConnect 客户端调配门户。
- 当用户在 ISE 中被定向到 AnyConnect 客户端调配门户时：

如果浏览器是 Internet Explorer，则 ISE 将下载 Anyconnect 下载程序，然后该下载程序会加载 AnyConnect。

对于所有其他浏览器，ISE 将打开客户端调配重定向门户，该门户会显示下载网络设置助理 (NSA) 工具的链接。用户运行 NSA，该工具可查找 ISE 服务器并下载 Anyconnect 下载程序。

NSA 在 Windows 上运行完毕后会自行删除。在 Mac OS X 上运行完毕后，必须手动将其删除。

ISE 文档介绍了如何执行以下操作：

- 在 ISE 中创建 AnyConnect 配置文件
- 将 AnyConnect 资源从本地计算机添加到 ISE
- 从远程站点添加 AnyConnect 调配资源
- 部署 AnyConnect 客户端和资源

ISE 可配置和部署以下 AnyConnect 资源：

- AnyConnect 核心和模块，包括 ISE 终端安全评估模块
- 配置文件：AMP Enabler、VPN、网络访问管理器、网络安全、客户反馈和 AnyConnect ISE 终端安全评估
- 定制文件
  - 用户界面资源
  - 二进制文件、连接脚本文件和帮助文件
- 本地化文件
  - 用于消息本地化的 AnyConnect gettext 转换
  - Windows Installer 转换

## 准备 AnyConnect 文件进行 ISE 上传

- 下载适用于操作系统的 AnyConnect 软件包，以及您希望在本机 PC 上部署的其他 AnyConnect 资源。
- 为您计划部署的模块创建配置文件。至少要创建一个 AnyConnect ISE 终端安全评估配置文件。
- 将定制和本地化资源合并成一个 ZIP 存档，该存档在 ISE 中称为捆绑包。捆绑包可包含：

AnyConnect UI 资源

VPN 连接脚本

帮助文件

安装程序转换

AnyConnect 本地化捆绑包可包含：

二进制格式的 AnyConnect Gettext 转换

安装程序转换

按照[准备 AnyConnect 定制和本地化进行 ISE 部署](#)中所述的步骤创建 ISE 捆绑包。

## 配置 ISE 以部署 AnyConnect

必须先将 AnyConnect 软件包上传到 ISE，然后再上传和创建其他 AnyConnect 资源。



注释

在 ISE 中配置 AnyConnect 配置对象时，取消选中 AnyConnect Module Selection 下的 VPN 模块不会禁用已部署/已调配客户端上的 VPN。必须配置 VPNDisable\_ServiceProfile.xml 才能禁用 AnyConnect GUI 上的 VPN 图块。VPNDisable\_ServiceProfile.xml 和其他 AnyConnect 文件都位于 CCO 上。

- 1 在 ISE 中，选择 **Policy > Policy Elements > results**。展开 **Client Provisioning** 显示 **Resources**，然后选择 **Resources**。
- 2 选择 **Add > Agent resources from local disk**，然后上传 AnyConnect 软件包文件。为您计划部署的任何其他 AnyConnect 资源重复添加本地磁盘代理资源。
- 3 选择 **Add > AnyConnect Configuration**。此 AnyConnect 配置用于对模块、配置文件、定制/语言包和 Opswat 软件包进行配置，如下表所述。

可在 ISE、ASA 或 Windows AnyConnect 配置文件编辑器中创建和编辑 AnyConnect ISE 终端安全评估配置文件。下表显示 ISE 中每个 AnyConnect 资源的名称以及资源类型的名称。

表 5: ISE 中的 AnyConnect 资源

提示符	ISE 资源类型和说明
AnyConnect 软件包	AnyConnectDesktopWindows AnyConnectDesktopOSX AnyConnectWebAgentWindows AnyConnectWebAgentOSX
合规性模块	AnyConnectComplianceModuleWindows AnyConnectComplianceModuleOSX
AnyConnect 配置文件	AnyConnectProfile ISE 为上传的 AnyConnect 软件包所提供的每个配置文件显示一个复选框。
定制捆绑包	AnyConnectCustomizationBundle
本地化捆绑包	AnyConnectLocalizationBundle

- 4 创建基于角色或基于操作系统的客户端调配策略。对于客户端调配终端安全评估代理，可选择 AnyConnect 和 ISE 传统 NAC/MAC 代理。每个客户端调配策略只能调配一个代理，要么是

AnyConnect 代理，要么是传统 NAC/MAC 代理。配置 AnyConnect 代理时，请选择一个在步骤 2 创建的 AnyConnect 配置。

## 更新 AnyConnect 软件和配置文件

AnyConnect 可通过多种方式更新。

- AnyConnect 客户端 - 当 AnyConnect 连接 ASA 时，AnyConnect 下载程序将检查 ASA 上是否加载了任何新软件或配置文件。AnyConnect 下载程序可在身份验证和建立 VPN 隧道之前将这些更新下载到客户端。
- ASA 门户 - 指示用户连接到 ASA 的无客户端门户以获取更新。
- ISE - 当用户连接到 ISE 时，ISE 将使用其 AnyConnect 配置判断是否有更新的组件或新的终端安全评估要求。

可以通过多种方法来支持最终用户延迟更新。您还可以阻止客户端更新，即使您已将更新加载到头端也是。

### 升级示例流程

#### 必备条件

以下示例假定：

- 您已在 ISE 中创建动态授权控制列表 (DACL)，且列表已推送到 ASA。该列表使用客户端的终端安全评估状态确定何时将客户端重定向到 ISE 上的 AnyConnect 客户端调配门户。
- ISE 在 ASA 之后。

#### AnyConnect 已安装在客户端上

- 1 用户启动 AnyConnect，提供凭证，并点击 Connect。
- 2 ASA 建立与客户端的 SSL 连接，将身份验证凭证传递到 ISE，ISE 验证凭证。
- 3 AnyConnect 启动 AnyConnect 下载程序，该下载程序执行所有升级操作，并启动 VPN 隧道。

如果 ASA 未安装 ISE 终端安全评估，则

- 1 用户浏览到任何站点时，DACL 将其重定向到 ISE 上的 AnyConnect 客户端调配门户。
- 2 如果使用 Internet Explorer 浏览器，ActiveX 控件将启动 AnyConnect 下载程序。在其他浏览器中，用户下载并执行网络设置助理 (NSA)，该工具会下载并启动 AnyConnect 下载程序。
- 3 AnyConnect 下载程序执行在 ISE 上配置的所有 AnyConnect 升级，其中现在包括 AnyConnect ISE 终端安全评估模块。
- 4 客户端上的 ISE 终端安全评估代理将启动终端安全评估。

#### 未安装 AnyConnect



- 1 用户浏览到站点，启动到 ASA 无客户端门户的连接。
- 2 用户提供身份验证凭证，该凭证将传输到 ISE 并进行验证。
- 3 AnyConnect 下载程序由 Internet Explorer 中的 ActiveX 控件和其他浏览器中的 Java 小应用启动。
- 4 AnyConnect 下载程序执行在 ASA 上配置的升级，然后启动 VPN 隧道。下载程序完成。

如果 ASA 未安装 ISE 终端安全评估，则

- 1 用户再次浏览到站点，然后重定向到 ISE 上的 AnyConnect 客户端调配门户。
- 2 在 Internet Explorer 中，ActiveX 控件启动 AnyConnect 下载程序。在其他浏览器中，用户下载并执行网络设置助理，该工具将下载并启动 AnyConnect 下载程序。
- 3 AnyConnect 下载程序通过现有 VPN 隧道执行 ISE 上配置的所有升级，其中包括添加 AnyConnect ISE 终端安全评估模块。
- 4 ISE 终端安全评估代理启动终端安全评估。

## 禁用 AnyConnect 自动更新

可以通过配置和分发客户端配置文件来禁用或限制 AnyConnect 自动更新。

- 在 VPN 客户端配置文件中：

Auto Update 将禁用自动更新。此配置文件可随附在 AnyConnect 网络部署安装中或添加到现有客户端安装中。您也可以允许用户切换此设置。

- 在 VPN 本地策略配置文件中：

Bypass Downloader 阻止将 ASA 上的所有更新内容下载到客户端。

Update Policy 在连接到不同头端时提供对软件和配置文件更新的精细控制。

## 在 WebLaunch 期间提示用户下载 AnyConnect

您可以将 ASA 配置为提示远程用户启动网络部署，并配置一个时间段，在这个时间段内他们可以选择下载 AnyConnect 或转到无客户端入口页面。

提示用户下载 AnyConnect 在组策略或用户帐户中进行配置。以下步骤显示如何在组策略中启用此功能。

## 过程

- 
- 步骤 1** 在 ASDM 中，转到 **Configuration > Remote Access VPN > Network (Client) Access > Group Policies**。
- 步骤 2** 选择组策略，点击 **Edit** 或 **Add** 可编辑或新增组策略。
- 步骤 3** 在导航窗格中，选择 **Advanced > AnyConnect Client > Login Settings**。如果需要，取消选中 **Inherit** 复选框，然后选择 Post Login 设置。  
如果您选择提示用户，请指定超时时间段并选择在 Default Post Login Selection 区域中该时间段过期后要采取的默认操作。
- 步骤 4** 点击 **OK** 并确保将更改应用到组策略中，然后点击 **Save**。
- 

## 允许用户延期升级

您可以强制用户通过禁用 AutoUpdate 接受 AnyConnect 更新，如[禁用 AnyConnect 自动更新](#)中所述。默认情况下，AutoUpdate 为启用状态。

也可以允许用户延迟客户端更新，直到以后设置 Deferred Update。如果配置了 Deferred Update，则当客户端更新可用时，AnyConnect 会打开一个对话框，询问用户想要更新还是延迟。所有 Windows、Linux 和 OS X 都支持 Deferred Upgrade。

### 在 ASA 上配置延迟更新

在 ASA 上，通过添加定制属性，然后在组策略中引用和配置这些属性，可以启用延迟更新。必须创建并配置所有定制属性来使用延迟更新。

向 ASA 配置添加定制属性的过程取决于所运行的 ASA/ASDM 版本。请根据您部署的 ASA/ASDM 版本，参阅 *Cisco ASA 系列 VPN ASDM 配置指南* 或 *Cisco ASA 系列 VPN CLI 配置指南*，了解定制属性配置过程。

以下属性和值用于在 ASDM 中配置延迟更新：

定制属性 *	有效值	默认值	备注
DeferredUpdateAllowed	true false	False	True 将启用延迟更新。如果延期更新被禁用 (false)，则会忽略以下设置。
DeferredUpdateMinimumVersion	x.x.x	0.0.0	必须安装可以延迟更新的最低 AnyConnect 版本。  此最低版本检查适用于在头端上启用的所有模块。如果任何已启用模块（包括 VPN）未安装或未达到最低版本，则连接不符合延迟更新。  如果该属性未指定，则会显示延期提示（或自动取消），无论终端上安装了何种版本。

定制属性 *	有效值	默认值	备注
DeferredUpdateDismissTimeout	0 - 300 (秒)	150 秒	<p>延期更新提示在被自动取消之前显示的秒数。此属性仅当会显示延期更新提示（首先会评估最低版本属性）时才适用。</p> <p>如果缺少此属性，则自动取消功能被禁用，并显示一个对话框（如果需要），直到用户响应。</p> <p>若将此属性设置为零，则允许根据以下条件进行自动延期或强制更新：</p> <ul style="list-style-type: none"> <li>• DeferredUpdateMinimumVersion 的安装版本和值。</li> <li>• DeferredUpdateDismissResponse 的值。</li> </ul>
DeferredUpdateDismissResponse	延迟更新	更新	DeferredUpdateDismissTimeout 发生时要采取的操作。

\* 定制属性值区分大小写。

## 在 ISE 中配置延期更新

开始之前

过程

- 
- 步骤 1**
- 选择 **Policy > Results**。
  - 展开 **Client Provisioning**。
  - 选择 **Resources**，然后点击 **Add > Agent Resources from Local Disk**。
  - 上传 AnyConnect pkg 文件，然后选择 **Submit**。
- 步骤 2** 上载您创建的任何其他 AnyConnect 资源。
- 步骤 3** 在 **Resources** 上，使用您上传的 AnyConnect 软件包添加 **AnyConnect Configuration**。AnyConnect Configuration 具有用于配置延期更新的字段。
- 

## 延期更新 GUI

下图显示当有更新可用且配置了延迟更新时用户看到的用户界面。图的右边部分显示当配置了 **DeferredUpdateDismissTimeout** 时的用户界面。

## 设置更新策略

### 更新策略概述

如果 AnyConnect 软件和配置文件更新可用且客户端允许更新，则可在连接到头端时进行更新。为 AnyConnect 更新配置头端，以便可以进行更新。VPN 本地策略文件中的更新策略设置决定了是否允许更新。

更新策略有时被称之为软件锁定。如果配置了多个头端，更新策略也称之为多域策略。

默认情况下，更新策略设置允许来自任何头端的软件和配置文件更新。请按如下方式设置更新策略参数以限制此操作：

- 通过在**服务器名称**列表中指定头端，允许或授权特定头端更新所有 AnyConnect 软件和配置文件。  
头端服务器名可以是 FQDN 或 IP 地址。同时也可以是通配符，例如：`*.example.com`。  
有关更新发生方式的完整说明，请参阅以下[已授权服务器更新策略行为](#)。
- 对于所有其他未指定或未授权的头端：
  - 使用 **Allow Software Updates From Any Server** 选项，允许或拒绝 VPN 核心模块和其他可选模块的软件更新。
  - 使用 **Allow VPN Profile Updates From Any Server** 选项，允许或拒绝 VPN 配置文件更新。
  - 使用 **Allow Service Profile Updates From Any Server** 选项，允许或拒绝其他服务模块配置文件更新。
  - 使用 **Allow ISE Posture Profile Updates From Any Server** 选项允许或拒绝 ISE 终端安全评估配置文件更新。
  - 使用 **Allow Compliance Module Updates From Any Server** 选项允许或拒绝合规性模块更新。有关更新发生方式的完整说明，请参阅以下[未授权的服务器更新策略行为](#)。

### 已授权服务器更新策略行为

当连接到**服务器名称**列表中识别的未授权头端时，其他更新策略参数不适用，并将出现以下情况：

- 头端上 AnyConnect 软件包的版本与客户端版本进行比较，以确定软件是否应该更新。
  - 如果 AnyConnect 软件包的版本比客户端上的版本旧，则不进行软件更新。
  - 如果 AnyConnect 软件包的版本与客户端上的版本相同，则只下载和安装在头端上配置以供下载并且在客户端上不存在的软件模块。
  - 如果 AnyConnect 软件包的版本比客户端的版本新，则下载和安装头端上为下载配置的软件模块以及客户端上已安装的软件模块。

- 头端上的 VPN 配置文件、ISE 终端安全评估配置文件和每个服务配置文件都将与客户端上的配置文件进行比较以确定是否应更新：

如果头端的配置文件与客户端的配置文件相同，则不会进行更新。

如果头端的配置文件与客户端的配置文件不同，则会进行下载。

## 未授权的服务器更新策略行为

当连接到未授权头端时，**Allow ... Updates From Any Server** 选项用于确定如何更新 AnyConnect，如下所示：

- **Allow Software Updates From Any Server:**

如果选中此选项，则允许对此未授权的 ASA 进行软件更新。根据对上述授权头端的版本比较进行更新。

如果未选中此选项，则不会进行软件更新。此外，如果基于版本比较发生更新，系统将终止 VPN 连接尝试。

- **Allow VPN Profile Updates From Any Server:**

如果选中此选项，则当头端的 VPN 配置文件与客户端的配置文件不同时，对 VPN 配置文件进行更新。

如果未选中此选项，则不会更新 VPN 配置文件。此外，如果基于差异发生 VPN 配置文件更新，系统将终止 VPN 连接尝试。

- **Allow Service Profile Updates From Any Server:**

如果选中此选项，则当头端的配置文件与客户端的配置文件不同时，对每个服务配置文件进行更新。

如果未选中此选项，则不会更新服务配置文件。

- **Allow ISE Posture Profile Updates From Any Server:**

如果选中此选项，则在头端 ISE 终端安全评估配置文件不同于客户端 ISE 终端安全评估配置文件时更新 ISE 终端安全评估配置文件。

如果未选中此选项，则不会更新 ISE 终端安全评估配置文件。ISE 终端安全评估代理需要具备 ISE 终端安全评估配置文件才能运行。

- **Allow Compliance Module Updates From Any Server:**

如果选中此选项，则在头端合规性模块不同于客户端合规性模块时更新合规性模块。

如果未选中此选项，则不更新合规性模块。ISE 终端安全评估代理需要具备合规性模块才能运行。

## 更新策略指南

- 通过在授权的**服务器名称**列表中列出服务器的 IP 地址，远程用户可以使用该 IP 地址连接到头端。如果用户尝试使用 IP 地址连接，但头端被列为 FQDN，那么该尝试将被视为连接到未授权的域。
- 软件更新包括下载定制、本地化、脚本和转换。在禁止软件更新时，这些项目不会下载。如果某些客户端不允许脚本更新，请不要依赖脚本来实施策略。
- 下载启用 永远在线 的 VPN 配置文件将删除客户端上的所有其他 VPN 配置文件。在决定允许或拒绝从未授权头端或非企业头端更新 VPN 配置文件时，请注意这一点。
- 如果因安装和更新策略而未能将 VPN 配置文件下载到客户端，则以下功能将不可用。

服务禁用	不受信任网络策略
证书存储区覆盖	受信任的 DNS 域
显示预连接消息	受信任 DNS 服务器
本地局域网接入	永远在线
在登录前启动	强制网络门户补救
本地代理连接	脚本编写
PPP 排除	注销时保持 VPN
自动 VPN 策略	需要设备锁定
受信任的网络策略	自动服务器选择

- 下载程序将创建一个单独的文本日志 (UpdateHistory.log) 来记录下载历史信息。此日志包含更新时间、更新客户端的 ASA、更新的模块以及升级前后安装的版本。此日志文件存储于：  
%AllUsers%\Application Data\Cisco\Cisco AnyConnect Secure Mobility Client\Logs 目录。

## 更新策略示例

此示例显示了客户端上的 AnyConnect 版本不同于各 ASA 头端时客户端的更新行为。

假定 VPN 本地策略 XML 文件中的更新策略如下：

```
<?xml version="1.0" encoding="UTF-8"?>
<AnyConnectLocalPolicy acversion="2.4.140"
xmlns=http://schemas.xmlsoap.org/encoding/
xmlns:xsi=http://www.w3.org/2001/XMLSchema-instance
xsi:schemaLocation="http://schemas.xmlsoap.org/encoding/ AnyConnectLocalPolicy.xsd">
<FipsMode>>false</FipsMode>
<BypassDownloader>>false</BypassDownloader><RestrictWebLaunch>>false</RestrictWebLaunch>
<StrictCertificateTrust>>false</StrictCertificateTrust>
<RestrictPreferenceCaching>>false</RestrictPreferenceCaching>
```

```

<RestrictTunnelProtocols>>false</RestrictTunnelProtocols>
<UpdatePolicy>
<AllowSoftwareUpdatesFromAnyServer>>true</AllowSoftwareUpdatesFromAnyServer>
<AllowVPNProfileUpdatesFromAnyServer>>true</AllowVPNProfileUpdatesFromAnyServer>
<AllowServiceProfileUpdatesFromAnyServer>>true</AllowServiceProfileUpdatesFromAnyServer>
<AllowISEProfileUpdatesFromAnyServer>>false</AllowISEProfileUpdatesFromAnyServer>
<AllowComplianceModuleUpdatesFromAnyServer>>true</AllowComplianceModuleUpdatesFromAnyServer>
<AuthorizedServerList>
 <ServerName>seattle.example.com</ServerName>
 <ServerName>newyork.example.com</ServerName>
</AuthorizedServerList>
</UpdatePolicy>
</AnyConnectLocalPolicy>

```

有以下 ASA 头端配置：

ASA 头端	加载的 AnyConnect 软件包	要下载的模块
seattle.example.com	版本 3.1.05182	VPN、网络访问管理器、网络安全
newyork.example.com	版本 3.1.06079	VPN、网络访问管理器
raleigh.example.com	版本 3.1.07021	VPN、终端安全评估

当客户端当前运行 AnyConnect VPN 和网络访问管理器模块时，可能出现以下更新序列：

- 客户端连接到 seattle.example.com，这是一个采用相同版本的 AnyConnect 来配置的授权服务器。下载并安装了网络安全软件模块和网络安全配置文件（如果可用）。如果 VPN 和网络访问管理器配置文件可供下载，且不同于客户端上的 VPN 和配置文件，则也会被下载。
- 客户端随后连接到 newyork.example.com，这是一个采用较新版本的 AnyConnect 来配置的授权 ASA。下载并安装了 VPN、网络访问管理器和网络安全模块。若配置文件可供下载且不同于客户端上的配置文件，则也会被下载。
- 客户端随后连接到 raleigh.example.com，这是一个未授权的 ASA。因为允许软件更新，所以 VPN、网络访问管理器、网络安全和终端安全评估模块均会升级。由于不允许更新 VPN 配置文件和服务配置文件，因此无法下载这些配置文件。如果认为 VPN 配置文件已更新（基于差异），则连接将终止。

## AnyConnect 参考信息

### 本地计算机上用户首选项文件的位置

AnyConnect 将某些配置文件设置存储在用户计算机上的用户首选项文件和全局首选项文件中。AnyConnect 使用本地文件配置客户端 GUI 上 Preferences 选项卡中用户可控制的设置并显示有关最新连接的信息，如用户、组和主机。

AnyConnect 使用全局文件来配置登录之前发生的操作，例如 Start Before Logon 和 AutoConnect On Start。

下表显示客户端计算机上首选项文件的文件名和安装路径：

操作系统	类型	文件和路径
Windows	用户	C:\Users\username\AppData\Local\Cisco\Cisco AnyConnect VPN Client\preferences.xml
	全局	C:\ProgramData\Cisco\Cisco AnyConnect VPN Client\preferences_global.xml
Mac OS X	用户	/Users/username/.anyconnect
	全局	/opt/cisco/anyconnect/.anyconnect_global
Linux	用户	/home/username/.anyconnect
	全局	/opt/cisco/anyconnect/.anyconnect_global

## AnyConnect 和传统 VPN 客户端使用的端口

下表列出了传统 Cisco VPN 客户端使用的端口和每个协议的 Cisco AnyConnect 安全移动客户端。

协议	Cisco AnyConnect 客户端端口
TLS (SSL)	TCP 443
SSL 重定向	TCP 80 (可选)
DTLS	UDP 443 (可选, 但强烈推荐)
IPsec/IKEv2	UDP 500、UDP 4500

协议	Cisco VPN 客户端 (IPsec) 端口
IPsec/NATT	UDP 500、UDP 4500
IPsec/NATT	UDP 500、UDP 4500
IPsec/TCP	TCP (可配置)
IPsec/UDP	UDP 500、UDP X (可配置)





## 第 2 章

# 定制和本地化 AnyConnect 客户端和安装程序

- [修改 AnyConnect 安装行为](#)，第 33 页
- [定制 AnyConnect GUI 文本和消息](#)，第 41 页
- [为 AnyConnect GUI 创建定制图标和徽标](#)，第 47 页
- [创建并上传 AnyConnect 客户端帮助文件](#)，第 55 页
- [编写和部署脚本](#)，第 56 页
- [使用 AnyConnect API 编写和部署定制应用](#)，第 60 页
- [准备 AnyConnect 定制和本地化进行 ISE 部署](#)，第 61 页

## 修改 AnyConnect 安装行为

### 指南

- Web 部署使用 AnyConnect Web 启动，后者是无客户端 SSL 门户的一部分。可以定制无客户端 SSL 门户，但不能定制门户的 AnyConnect 部分。例如，不能定制 Start AnyConnect 按钮。

## 禁用客户体验反馈

默认情况下，已启用客户体验反馈模块。此模块向思科提供有关客户已启用和正在使用的功能和模块的匿名信息。此信息让我们可以深入了解用户体验，以便思科可以持续改进质量、可靠性、性能和用户体验。

可使用以下方法禁用客户体验反馈模块：

- 客户体验反馈模块客户端配置文件 - 取消选中 Enable Customer Experience Feedback Service，并分发此配置文件。
- MST 文件 - 从 sampleTransforms-X.X.xxxxx.zip 中提取 anyconnect-win-disable-customer-experience-feedback.mst 文件。

## 修改安装行为 (Windows)

- 使用 Windows 安装程序属性修改 AnyConnect 安装行为。在以下位置可使用这些属性：
  - 命令行参数 - 一个或多个属性作为参数传递到命令行安装程序 `msiexec`。此方法用于预部署，Web 部署不支持此方法。
  - 安装程序转换 - 可以使用转换修改安装程序属性表。多种工具可用于创建转换；一个常用工具是 Microsoft Orca。Orca 工具是 Microsoft Windows Installer 软件开发套件 (SDK) 的一部分，包含在 Microsoft Windows SDK 内。要获取 Windows SDK，请浏览至 <http://msdn.microsoft.com>，然后搜索与您的 Windows 版本对应的 SDK。  
转换可用于预部署和 Web 部署。转换可作为参数传递到命令行，也可以上传到自适应安全设备 (**Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Customization/Localization > Customized Installer Transforms**) 进行 Web 部署。
- 在 ISO 映像中，安装程序 `setup.hta` 是 HTML 文件，可以对其进行编辑。

### 限制

AnyConnect 卸载提示不可定制。

## 用于定制客户端安装的 Windows 安装程序属性

以下 Windows 安装程序属性可定制 AnyConnect 安装。请注意，您还可以使用 Microsoft 支持的很多其他 Windows 安装程序属性。

- 重置系统 MTU - 当 VPN 安装程序属性 (`RESET_ADAPTER_MTU`) 设置为 1 时，安装程序会将所有 Windows 网络适配器 MTU 设置重置为默认值。必须重新启动系统，更改方可生效。
- 设置 Windows 锁定 - 思科建议为设备上的最终用户授予有限的 Cisco AnyConnect 安全移动客户端权限。如果最终用户拥有额外的权限，安装程序可提供锁定功能，防止用户和本地管理员关闭或停止 AnyConnect 服务。您还可以通过在命令提示符下使用服务密码来停止服务。

适用于 VPN、网络访问管理器和网络安全的 MSI 安装程序支持一个公用属性 (`LOCKDOWN`)。当 `LOCKDOWN` 设置为非零值时，终端设备上的用户或本地管理员无法控制与该安装程序关联的 Windows 服务。我们建议您使用我们提供的示例转换来设置此属性，并将转换应用于您希望锁定的每个 MSI 安装程序。您可以从 Cisco AnyConnect 安全移动客户端软件下载页面下载示例转换。

如果部署核心客户端以及一个或多个可选模块，则必须对每个安装程序应用 `LOCKDOWN` 属性。此操作为单向操作，无法删除，除非您重新安装产品。



注释 AMP 启用程序安装程序与 VPN 安装程序配对使用。

- 开启 ActiveX 控件 - 在默认情况下，早期版本的 AnyConnect 在预部署 VPN 软件包时会安装 VPN WebLaunch ActiveX 控件。从 AnyConnect 3.1 开始，默认情况下将关闭 VPN ActiveX 控件安装。此更改旨在确保默认配置最为安全。

在预部署 AnyConnect 客户端和可选模块时，如果您需要将 VPN ActiveX 控件与 AnyConnect 一同安装，则您必须使用 NOINSTALLACTIVEX=0 选项和 msixec 或转换。

- 将 AnyConnect 从 Add/Remove Program 列表中隐藏 - 可将已安装的 AnyConnect 模块从用户 Windows 控制面板中的 Add/Remove Programs 列表中隐藏。向安装程序传送 ARPSYSTEMCOMPONENT=1 可阻止该模块显示在已安装的程序列表中。

我们建议您使用我们提供的示例转换来设置此属性，从而将转换应用于您希望隐藏的每个模块的每个 MSI 安装程序。您可以从 Cisco AnyConnect 安全移动客户端软件下载页面下载示例转换。

## AnyConnect 模块的 Windows 安装程序属性

下表提供 MSI 安装命令行调用和配置文件部署位置的示例。

已安装的模块	命令和日志文件
没有 VPN 功能的 AnyConnect 核心客户端 (安装独立网络访问管理器或网络安全模块时使用)	msiexec /package anyconnect-win-ver-pre-deploy-k9.msi /norestart /passive PRE_DEPLOY_DISABLE_VPN=1 /lvx* anyconnect-win-<version>-pre-deploy-k9-install-datetimestamp.log
有 VPN 功能的 AnyConnect 核心客户端	msiexec /package anyconnect-win-ver-pre-deploy-k9.msi /norestart /passive /lvx* anyconnect-win-<version>-pre-deploy-k9-install-datetimestamp.log
客户体验反馈	msiexec /package anyconnect-win-ver-pre-deploy-k9.msi /norestart /passive DISABLE_CUSTOMER_EXPERIENCE_FEEDBACK=1 /lvx* anyconnect-win-<version>-pre-deploy-k9-install-datetimestamp.log
诊断和报告工具 (DART)	msiexec /package anyconnect-dart-win-ver-k9.msi /norestart /passive /lvx* anyconnect-dart-<version>-pre-deploy-k9-install-datetimestamp.log
SBL	msiexec /package anyconnect-gina-win-ver-k9.msi /norestart /passive /lvx* anyconnect-gina-<version>-pre-deploy-k9-install-datetimestamp.log
网络访问管理器	msiexec /package anyconnect-nam-win-ver-k9.msi /norestart /passive /lvx* anyconnect-nam-<version>-pre-deploy-k9-install-datetimestamp.log

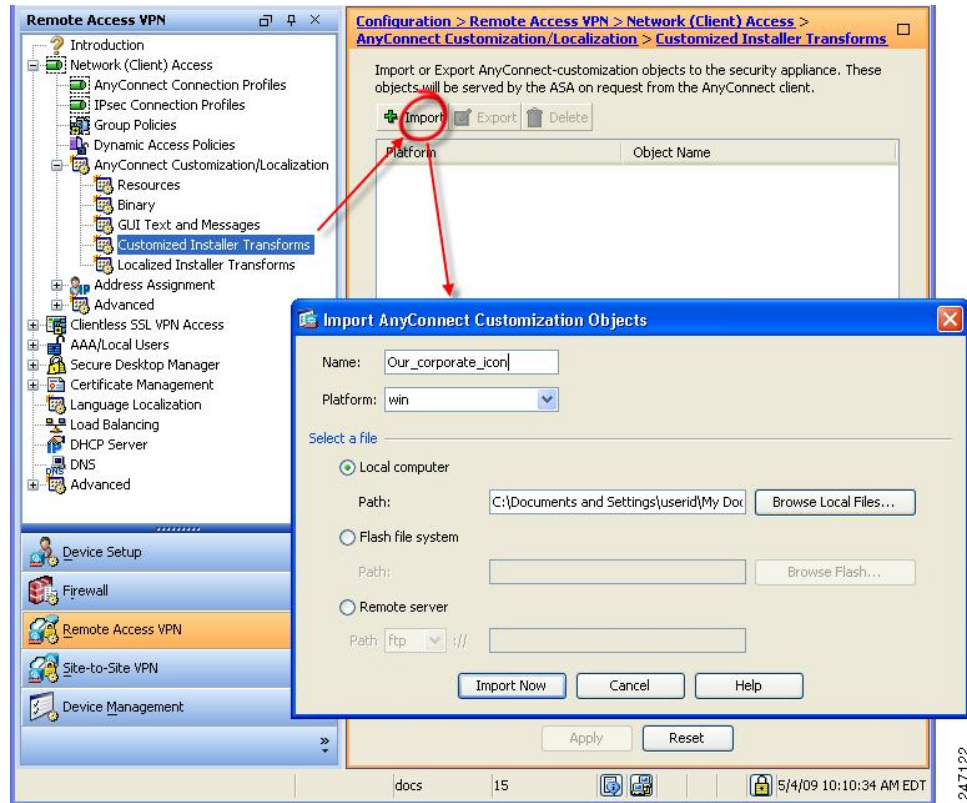
已安装的模块	命令和日志文件
网络安全	<pre>msiexec /package anyconnect-websecurity-win-ver-pre-deploy-k9.msi /norestart/passive /lvx*</pre> <p>anyconnect-websecurity-&lt;version&gt;-pre-deploy-k9-install-datetimestamp.log</p>
终端安全评估	<pre>msiexec /package anyconnect-posture-win-ver-pre-deploy-k9.msi /norestart/passive /lvx*</pre> <p>anyconnect-posture-&lt;version&gt;-pre-deploy-k9-install-datetimestamp.log</p>

## 将定制安装程序转换导入自适应安全设备

将 Windows 转换导入自适应安全设备让您可以将其用于网络部署。

### 过程

- 
- 步骤 1** 在 ASDM 中，转到 **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Customization/Localization > Customized Installer Transforms**。
- 步骤 2** 点击 **Import**。  
系统会显示 Import AnyConnect Customization Objects 窗口：



**步骤 3** 输入要导入的文件名。不同于其他定制对象的名称，该名称对 ASA 而言并不重要，仅为了方便您自己。

**步骤 4** 选择平台，并指定要导入的文件。点击 **Import Now**。此文件会立即显示在安装程序转换表中。

### 定制 AnyConnect 用户界面的转换示例

虽然创建转换的教程超出了本文档范围，但是以下文本是转换中的一些代表性条目。此示例将 `company_logo.bmp` 替换为本地副本，并且安装定制配置文件 `MyProfile.xml`。

```
DATA CHANGE - Component Component ComponentId
+ MyProfile.xml {39057042-16A2-4034-87C0-8330104D8180}
```

```
Directory_Attributes Condition KeyPath
Profile_DIR 0 MyProfile.xml
```

```
DATA CHANGE - FeatureComponents Feature_ Component_
+ MainFeature MyProfile.xml
```

```
DATA CHANGE - File File Component_FileName FileSize Version Language Attributes Sequence
+ MyProfile.xml MyProfile.xml MyProf~1.xml|MyProfile.xml 601 8192 35
<> company_logo.bmp 37302{39430} 8192{0}
```

```
DATA CHANGE - Media DiskId LastSequence DiskPrompt Cabinet VolumeLabel Source
+ 2 35
```

## 本地化 AnyConnect 安装程序屏幕

您可以转换 AnyConnect 安装程序显示的消息。ASA 使用转换功能来转换安装程序显示的消息。该转换会更改安装，但会保持原始安全签名的 MSI 不变。这些转换仅转换安装程序屏幕，而不转换客户端 GUI 屏幕。



注释

AnyConnect 的每个版本都包括本地化转换，管理员可在上传含有新软件的 AnyConnect 软件包时将转换上传到自适应安全设备。如果您使用我们的本地化转换，请确保在上传新的 AnyConnect 软件包时用 [cisco.com](http://cisco.com) 的最新版本更新这些转换。

您可以使用转换编辑器（如 Orca）编辑转换来更改消息字符串，并将转换导入 ASA。当用户下载客户端时，客户端会检测计算机的首选语言（区域设置在安装操作系统时指定）并应用相应转换。

我们目前提供 30 种语言转换。这些转换在 [cisco.com](http://cisco.com) 的 AnyConnect 软件下载页面以下面的 .zip 文件形式提供：

```
anyconnect-win-<VERSION>-web-deploy-k9-lang.zip
```

在此文件中，<VERSION> 是 AnyConnect 的版本（例如 3.1.xxxxx）。

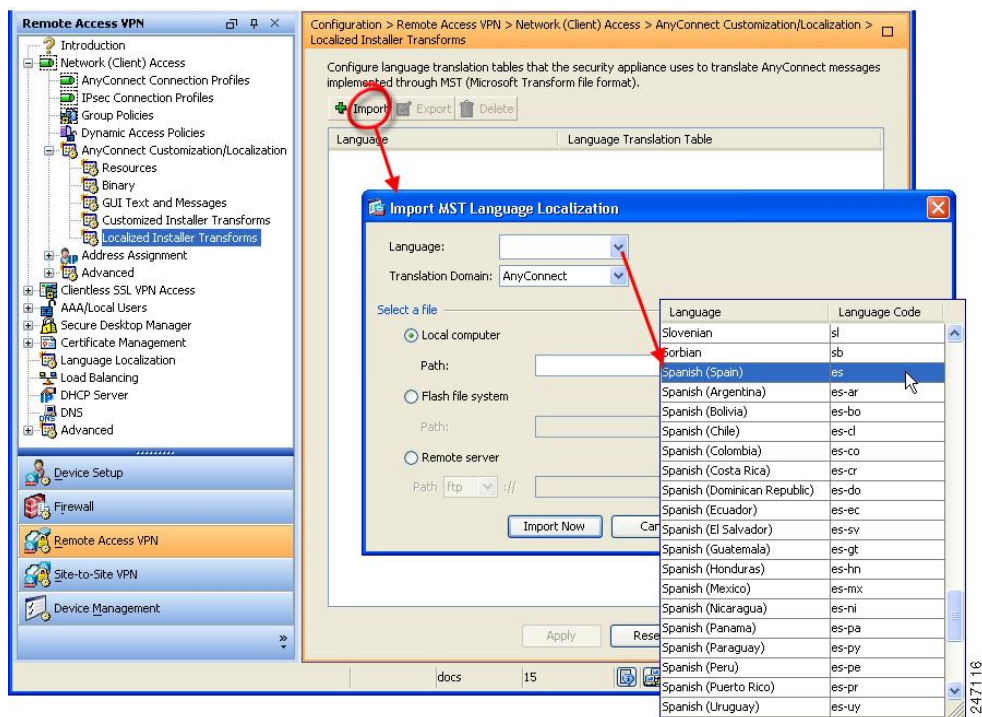
存档包含用于可用转换的转换功能（.mst 文件）。如果需要为远程用户提供的语言不是我们提供的 30 种语言之一，您可以创建您自己的转换并将其作为新语言导入 ASA。使用 Microsoft 的数据库编辑器 Orca，可以修改现有安装以及新文件。Orca 是 Microsoft Windows 安装程序软件开发套件 (SDK) 的一部分，包含在 Microsoft Windows SDK 内。

## 将本地化的安装程序转换导入自适应安全设备

以下过程显示如何使用 ASDM 将转换导入 ASA。

### 过程

- 步骤 1** 在 ASDM 中，转到 **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Customization/Localization > Localized Installer Transforms**。
- 步骤 2** 点击 **Import**。系统将打开 Import MST Language Localization 窗口：



- 步骤 3** 点击 **Language** 下拉列表，选择用于此转换的一种语言（和行业认可的缩写）。如果您手动输入缩写，请确保使用浏览器和操作系统识别的缩写。
- 步骤 4** 点击 **Import Now**。  
将显示已成功导入表格的提示消息。
- 步骤 5** 点击 **Apply** 保存更改。

在此过程中我们将语言指定为西班牙语 (ES)。下图显示在 Languages 列表中的用于 AnyConnect 的西班牙语新转换。



## 修改安装行为 (Mac OSX)

### 限制

AnyConnect 安装程序无法本地化。该安装程序使用的字符串来自 Mac 安装程序应用，而不是 AnyConnect 安装程序。

### 使用 ACTransforms.xml 在 Mac OS X 上定制安装程序行为

对于 Mac OS X 没有提供定制 .pkg 行为的标准方式，因此我们创建了 ACTransforms.xml。使用安装程序定位此 XML 文件时，安装程序读取本文件，然后运行安装。您必须将文件置于与安装程序相关的特定位置。安装程序按以下顺序搜索以查看是否找到修改：

- 1 在与 .pkg 安装程序文件相同的目录内的“Profile”目录中。
- 2 在装载的磁盘映像卷的根目录中的“Profile”目录中。
- 3 在与 .dmg 文件相同的目录内的“Profile”目录中。

XML 文件格式如下：

```
<ACTransforms>
<PropertyName1>Value</PropertyName1>
<PropertyName2>Value</PropertyName2>
</ACTransforms>
```

例如，OS X ACTransforms.xml 属性是 DisableVPN，用于创建网络访问管理器或网络安全的“独立”部署。ACTransforms.xml 在 DMG 文件所在的 Profiles 目录中。

### 禁用客户体验反馈模块

默认情况下，已启用客户体验反馈模块。要在 Mac OS X 上关闭此功能，请执行以下操作：

#### 过程

---

**步骤 1** 使用磁盘实用程序或 hdiutil 将 dmg 软件包从只读转换为读/写。例如：

```
hdiutil convert anyconnect-macosx-i386-ver-k9.dmg -format UDRW -o
anyconnect-macosx-i386-ver-k9-rw.dmg
```

**步骤 2** 编辑 ACTransforms.xml 并设置或添加以下值（如果尚未设置）。

```
<DisableCustomerExperienceFeedback>>false</DisableCustomerExperienceFeedback>
```

---



## 修改安装行为 (Linux)

### 使用 ACTransform.xml 在 Linux 上定制安装程序行为

没有为 Linux 提供定制 .pkg 行为的标准方式，所以我们创建了 ACTransforms.xml。使用安装程序定位此 XML 文件时，安装程序读取本文件，然后运行安装。您必须将文件置于与安装程序相关的特定位置。安装程序按以下顺序搜索以查看是否找到修改：

- 在与 .pkg 安装程序文件相同的目录内的“Profile”目录中
- 在装载的磁盘映像卷的根目录中的“Profile”目录中
- 在与 .dmg 文件相同的目录内的“Profile”目录中

预部署软件包中的 Profiles 目录内的 XML 文件 ACTransforms.xml 的格式如下：

```
<ACTransforms>
<PropertyName1>Value</PropertyName1>
<PropertyName2>Value</PropertyName2>
</ACTransforms>
```

## 定制 AnyConnect GUI 文本和消息

自适应安全设备 (ASA) 使用转换表转换 AnyConnect 显示的用户消息。转换表是具有转换消息文本字符串的文本文件。您可以使用 ASDM 或转换（用于 Windows）编辑现有消息或添加其他语言。

以下 Windows 本地化转换示例在 [www.cisco.com](http://www.cisco.com) 上提供：

- 用于 Windows 平台预部署软件包的语言本地化转换文件
- 用于 Windows 平台网络部署软件包的语言本地化转换文件

Windows 的 AnyConnect 软件包文件包含用于 AnyConnect 消息的默认英语模板。当您在 ASA 中加载 AnyConnect 软件包时，ASA 会自动导入此文件。此模板包含 AnyConnect 软件中消息字符串的最新更改。您可以使用为其他语言创建新的转换表，也可以导入 [www.cisco.com](http://www.cisco.com) 上提供的以下转换表之一（请参阅[将转换表导入自适应安全设备](#)，第 45 页）：

- 中文（简体）
- 中文（繁体）
- 捷克语
- 荷兰语
- 法语
- 法语（加拿大）
- 德语

- 匈牙利语
- 意大利语
- 日语
- 韩语
- 波兰语
- 葡萄牙语（巴西）
- 俄文
- 西班牙文（拉美）

以下各节介绍所需语言不可用或您希望进一步定制导入转换表时转换 GUI 文本和消息的过程。

- [添加或编辑 AnyConnect 文本和消息](#)。您可以按照以下任一方式添加或编辑文件来更改一个或多个消息 ID 的消息文本，从而更改消息文件：

在打开的对话框中键入对文本的更改。

将打开的对话框中的文本复制到文本编辑器，进行更改，然后粘贴回对话框。

- [将转换表导入自适应安全设备，第 45 页](#)。您可以通过点击 Save to File、编辑文件并将其导入回 ASDM 来导出消息文件。

在 ASA 上更新转换表后，直到客户端重新启动并成功建立另一个连接，才会应用更新后的消息。



注释

---

如果没有从 ASA 部署客户端和使用诸如 Altiris 坐席的公司软件部署系统，您可以采用诸如 Gettext 的目录实用程序手动将 AnyConnect 转换表 (anyconnect.po) 转换为 .mo 文件并将 .mo 文件安装到客户端计算机的相应文件夹中。有关详细信息，请参阅[为企业部署创建消息目录](#)。

---

### 指南和限制

AnyConnect 并不完全符合所有国际化要求，但以下内容除外：

- 日期/时间格式并不总是遵循区域设置要求。
- 不支持从右到左的语言。
- 由于硬编码字段的长度要求，有些字符串在 UI 中会截断。
- 一些硬编码英语字符串保持如下：
  - 更新时的状态消息。
  - 不受信任的服务器消息。
  - 延期更新消息。

## 添加或编辑 AnyConnect 文本和消息

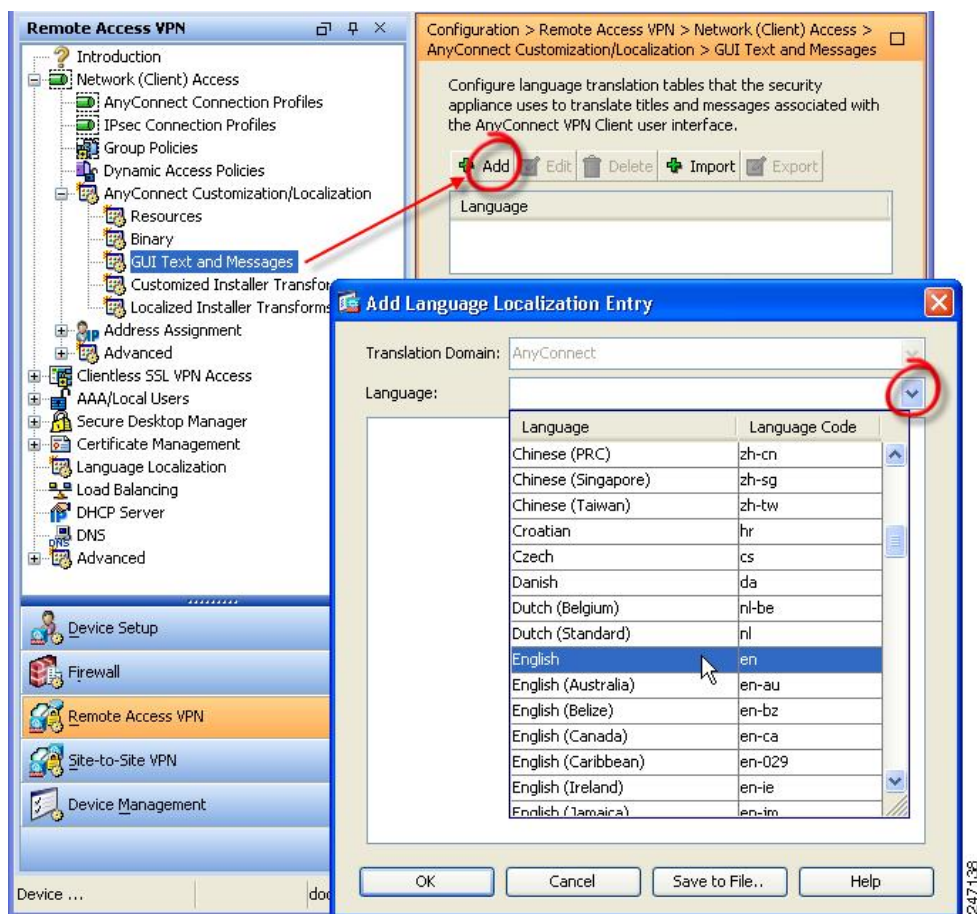
您可以通过添加或编辑英语转换表并且更改一条或多条消息 ID 的消息文本，来更改 AnyConnect GUI 上显示的英文消息。打开消息文件后，您可通过以下方式编辑：

- 在打开的对话框中键入对文本的更改。
- 将打开的对话框中的文本复制到文本编辑器，进行更改，然后粘贴回对话框。
- 点击 Save to File、编辑文件并将其导入到 ASDM，以导出消息文件。

### 过程

**步骤 1** 在 ASDM 中，转到 **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Customization/Localization > GUI Text and Messages**。

**步骤 2** 点击 **Add**。系统将显示 Add Language Localization Entry 窗口。

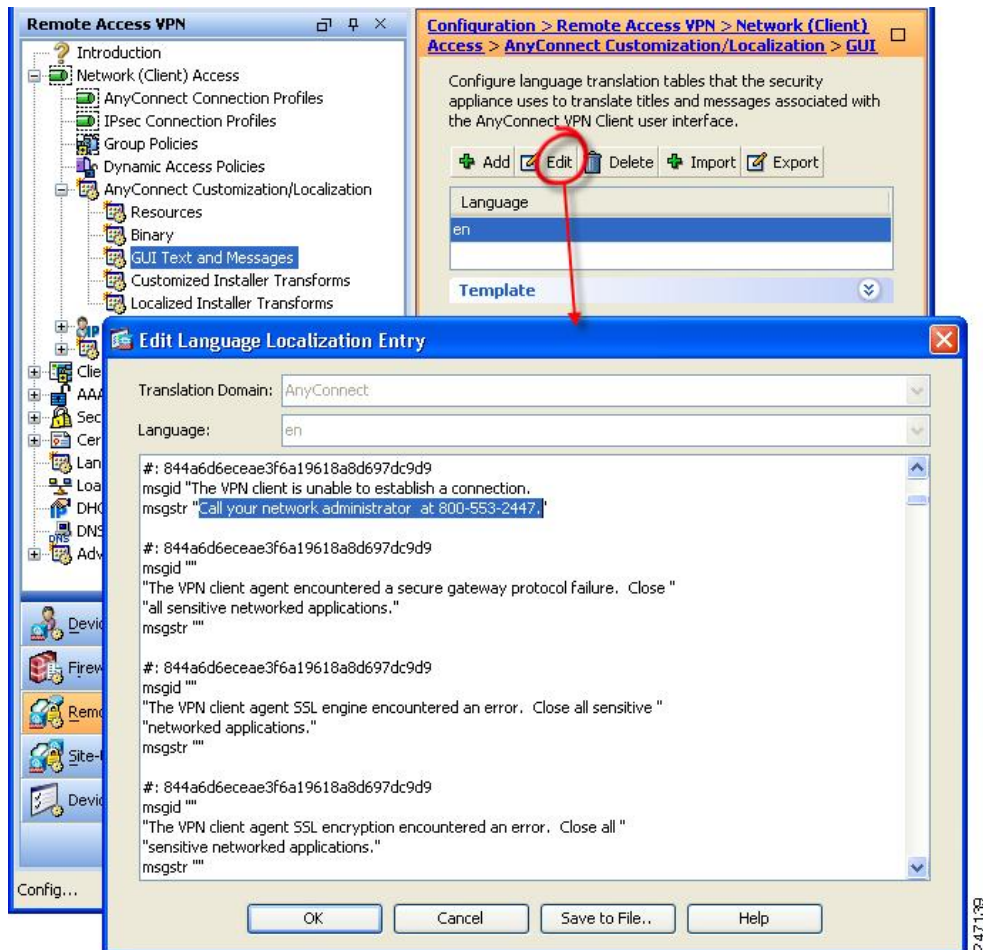


**步骤 3** 点击 Language 下拉列表，然后指定语言为英语 (en)。英语转换表显示在窗格的语言列表中。

**步骤 4** 点击 **Edit** 开始编辑消息。

系统将显示 Edit Language Localization Entry 窗口。msgid 的引号之间的文本是客户端显示的默认英语文本，不能更改。msgstr 字符串包含客户端用于替换 msgid 中默认文本的文本。在 msgstr 的引号之间插入您自己的文本。

在以下示例中，我们插入“Call your network administrator at 800-553-2447”。



**步骤 5** 点击 **OK**，然后点击 **Apply** 以保存更改。

## 将转换表导入自适应安全设备

### 过程

- 步骤 1 从 [www.cisco.com](http://www.cisco.com) 下载所需的转换表。
- 步骤 2 在 ASDM 中，转到 **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Customization/Localization > GUI Text and Messages**。
- 步骤 3 点击 **Import**。系统会显示 Import Language Localization Entry 窗口。
- 步骤 4 从下拉列表中选择适合的语言。
- 步骤 5 指定从何处导入转换表。
- 步骤 6 点击 **Import Now**，即可将此转换表部署至 AnyConnect 客户端，并将其用作首选语言。本地化将在 AnyConnect 重新启动并连接后应用。



#### 注释

对于在非移动设备上运行的 AnyConnect，即使没有使用思科安全桌面，也必须将思科安全桌面转换表导入自适应安全设备，这样主机扫描消息才会进行本地化。

## 为企业部署创建消息目录

如果没有将客户端与 ASA 一起部署，且正在使用企业软件部署系统（例如 Altiris Agent），则可以使用实用程序（例如 Gettext）将 AnyConnect 转换表手动转换为消息目录。将表格从 .po 文件转换为 .mo 文件，之后将文件置于客户端计算机上相应的文件夹内。

Gettext 是来自 GNU 项目的实用程序并在命令窗口中运行。有关详细信息，请参阅 GNU 网站 [gnu.org](http://gnu.org)。还可以使用基于 GUI 的实用程序（该程序使用 Gettext），例如 Poedit。poedit.net 上提供了此软件。此过程使用 Gettext 来创建消息目录：

### AnyConnect 消息模板目录

AnyConnect 消息模板位于以下为每个操作系统列出的文件夹中：



#### 注释

\l10n 目录是如下所列的每个目录路径的一部分。目录名称拼写：小写 l("el")、1、0、小写 n。

- 对于 Windows - <DriveLetter>:\Program Data\Cisco\Cisco AnyConnect Secure Mobility Client\l10n\<LANGUAGE-CODE>\LC\_MESSAGES
- 对于 Mac OS X 和 Linux -  
/opt/cisco/anyconnect/l10n/<LANGUAGE-CODE>/LC\_MESSAGES

## 过程

- 
- 步骤 1** 从 <http://www.gnu.org/software/gettext/> 下载 Gettext 实用程序并将 Gettext 安装在您用于管理的计算机（不是远程用户计算机）上。
- 步骤 2** 在已安装 AnyConnect 的计算机上检索 AnyConnect 消息模板 AnyConnect.po 的副本。
- 步骤 3** 根据需要，编辑 AnyConnect.po 文件（使用 notepad.exe 或任何明文文本编辑器）来更改字符串。
- 步骤 4** 运行 Gettext 消息文件编译器以基于 .po 文件创建 .mo 文件：  
**msgfmt -o AnyConnect.mo AnyConnect.po**
- 步骤 5** 将 .mo 文件副本置于用户计算机上正确的消息模板目录下。
- 

## 将新消息合并到 ASA 上的定制转换表中

新用户消息将添加到 AnyConnect 的某些版本中。为启用这些新消息的转换，新消息字符串会添加到与最新客户端映像一起打包的转换模板中。如果您已基于以前的客户端附带的模板创建了转换表，新消息不会自动向远程用户显示。您必须将最新模板与您的转换表合并以确保转换表包含这些新消息。

可使用免费的第三方工具执行合并。来自 GNU 项目的 Gettext 实用程序可用于 Windows，并可在命令窗口中运行。有关详细信息，请参阅 GNU 网站 [gnu.org](http://gnu.org)。还可以使用基于 GUI 的实用程序（该程序使用 Gettext），例如 Poedit。poedit.net 上提供了此软件。以下过程涵盖了这两种方法。



**注释** 此过程假设您已将最新的 AnyConnect 映像软件包加载到 ASA 中。除非您执行此操作，否则模板无法导出。

---

## 过程

- 
- 步骤 1** 从 **Remote Access VPN > Language Localization > Templates** 导出最新的 AnyConnect 转换模板。导出的模板文件名为 AnyConnect.pot。此文件名确保 msgmerge.exe 程序将此文件识别为消息目录模板。
- 步骤 2** 合并 AnyConnect 模板与转换表。  
如果使用的是适用于 Windows 的 Gettext 实用程序，打开命令提示符窗口并运行以下命令。该命令会合并 AnyConnect 转换表 (.po) 和模板 (.pot)，从而创建新的 AnyConnect\_merged.po 文件：  
**msgmerge -o AnyConnect\_merged.po AnyConnect.po AnyConnect.pot**  
以下示例显示命令的结果：

```
C:\Program Files\GnuWin32\bin> msgmerge -o AnyConnect_merged.po AnyConnect.po
AnyConnect.pot..... done.
```

如果使用 Poedit，则首先打开 AnyConnect.po 文件；转到 **File > Open > <AnyConnect.po>**。然后将其与模板合并；从 POT 文件 <AnyConnect.pot> 转到 **Catalog > Update**。Poedit 将在 Update Summary 窗口显示新字符串和模糊字符串。保存文件，在下一步骤中将导入此文件。

- 步骤 3** 将已合并的转换表导入 **Remote Access VPN > Language Localization**。点击 **Import**，指定语言，然后选择 **AnyConnect** 作为转换域。将要导入的文件指定为 AnyConnect\_merged.po。

## 在客户端上选择 Windows 的默认语言

当远程用户连接到 ASA 并下载客户端时，AnyConnect 会检测计算机的首选语言并通过检测指定系统区域设置应用相应的转换表。

在 Windows 上查看或更改指定的系统区域设置：

### 过程

- 步骤 1** 导航到 **Control Panel > Region and Languages** 对话框。如果按类别查看控制面板，请选择 **Clock, Language, and Region > Change display language**。
- 步骤 2** 指定语言/区域设置，并指定应使用这些设置作为所有用户帐户的默认设置。
- 步骤 3** 如果部署使用的是网络安全，[重新启动网络安全代理](#)可获得新转换。



### 注释

如果未指定位置，AnyConnect 将默认使用该语言。例如，如果未找到“fr-ca”目录，AnyConnect 将检查是否存在“fr”目录。您无需更改显示语言、位置或键盘即可查看转换。

## 为 AnyConnect GUI 创建定制图标和徽标

本节中的各表列出了可针对各操作系统替换的 AnyConnect 文件。表中的图像被 AnyConnect VPN 客户端、网络访问管理器和网络安全模块所使用。

### 限制

- 定制组件的文件名必须匹配 AnyConnect GUI 使用的文件名；文件名因操作系统而有所不同，并且在 Mac 和 Linux 下区分大小写。例如，如果要替换 Windows 客户端的公司徽标，则必须导入名为 company\_logo.png 的公司徽标。如果以其他文件名导入，AnyConnect 安装程序不会更改组件。不过，如果部署您自己的可执行文件来定制 GUI，该可执行文件调用的资源文件可使用任意文件名。
- 如果导入图像作为资源文件（如 company\_logo.bmp），导入的图像将定制 AnyConnect，直至您重新导入另一个使用相同文件名的图像。例如，如果将 company\_logo.bmp 替换为定制图像，



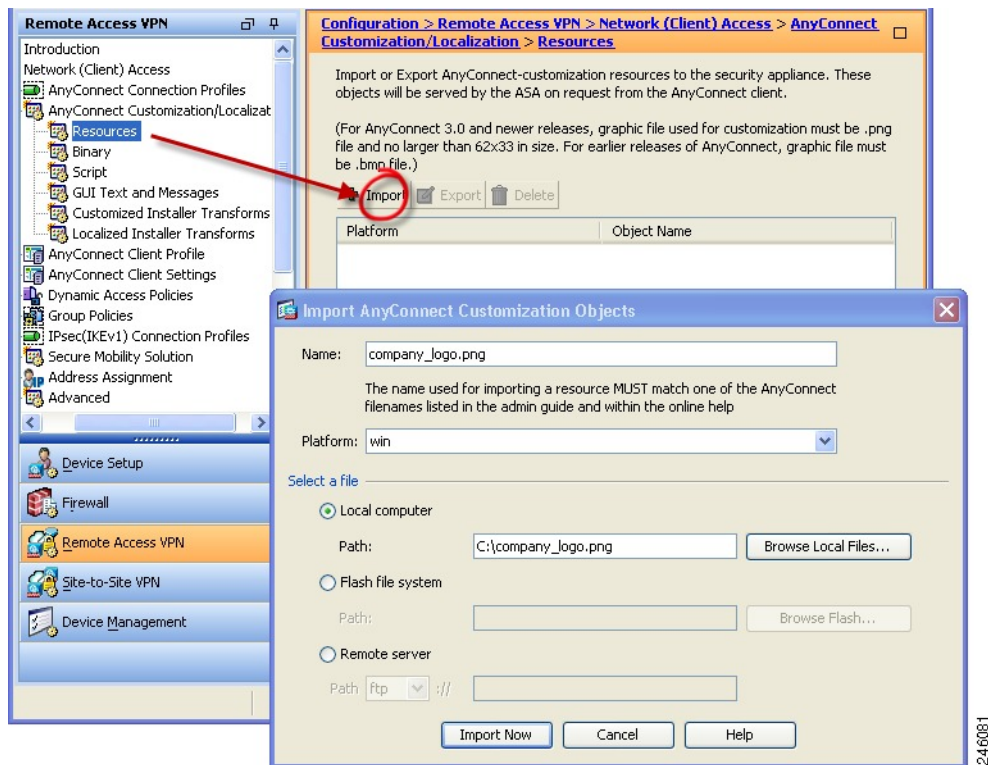
然后删除该图像，客户端会继续显示该图像，直至导入相同文件名的新图像（或原始思科徽标图像）为止。

## 更换 AnyConnect GUI 组件

可通过将您自己的定制文件导入到安全设备来定制 AnyConnect，该安全设备在客户端部署新文件。

### 过程

- 步骤 1** 在 ASDM 中，转到 **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Customization/Localization > Resources**。
- 步骤 2** 点击 **Import**。**Import AnyConnect Customization Objects** 窗口随即显示。



- 步骤 3** 输入要导入的文件名。
- 步骤 4** 选择平台，并指定要导入的文件。点击 **Import Now**。现在，文件显示在对象列表中。



## Windows 的 AnyConnect 图标和徽标

Windows 的所有文件位于：

```
%PROGRAMFILES%\Cisco\Cisco AnyConnect Secure Mobility Client\res\
```





注释

%PROGRAMFILES% 指相同名称的环境变量。在大多数 Windows 安装中，这是 C:\Program Files。

Windows 安装中的文件名和说明。	图像尺寸 (像素, 长 x 高) 和类 型
<p>about.png</p> <p>Advanced 对话框右上角的 About 按钮。</p> <p>大小不可调整。</p> 	<p>24 x 24</p> <p>PNG</p>
<p>about_hover.png</p> <p>Advanced 对话框右上角的 About 按钮。</p> <p>大小不可调整。</p> 	<p>24 x 24</p> <p>PNG</p>
<p>app_logo.png</p> <p>128 x 128 是最大大小。如果自定义文件不是该大小，则在应用中将其调整为 128 x 128。如果比例不同，则会将其拉伸。</p> 	<p>128 x 128</p> <p>PNG</p>

Windows 安装中的文件名和说明。	图像尺寸 (像素, 长 x 高) 和类 型
<p>attention.ico</p> <p>系统托盘图标警告用户需要注意或交互的情况。例如, 有关用户凭证的对话框。</p> <p>大小不可调整。</p> 	<p>16 x 16</p> <p>ICO</p>
<p>company_logo.png</p> <p>托盘浮出控件左上角和 <b>Advanced</b> 对话框中显示的公司徽标。</p> <p>最大大小为 97 x 58。如果自定义文件不是该大小, 则其在应用中会调整为 97 x 58。如果比例不同, 则会将其拉伸。</p> 	<p>97 x 58 (最 大)</p> <p>PNG</p>
<p>company_logo_alt.png</p> <p>About 对话框右下角显示的公司徽标。</p> <p>最大大小为 97 x 58。如果自定义文件不是该大小, 则其在应用中会调整为 97 x 58。如果比例不同, 则会将其拉伸。</p> 	<p>97 x 58</p> <p>PNG</p>
<p>cues_bg.jpg</p> <p>托盘浮出控件、Advanced 窗口和 About 对话框的背景图像。</p> <p>因为图像未进行拉伸, 因此使用过小的替换图像会导致出现黑色区域。</p> 	<p>1260 x 1024</p> <p>JPEG</p>

Windows 安装中的文件名和说明。	图像尺寸 (像素, 长 x 高) 和类 型
<p>error.ico</p> <p>系统托盘图标警告用户有一个或多个组件出现严重错误。</p> <p>大小不可调整。</p> 	<p>16 x 16</p> <p>ICO</p>
<p>neutral.ico</p> <p>表示客户端组件运行正常的系统托盘图标。</p> <p>大小不可调整。</p> 	<p>16 x 16</p> <p>ICO</p>
<p>transition_1.ico</p> <p>系统托盘图标, 它与 transition_2.ico 和 transition_3.ico 一同显示, 表示一个或多个客户端组件在不同状态间过渡 (例如 VPN 连接或网络访问管理器连接时)。3 个图标文件连续显示, 看起来好像单个图标从左至右跳动。</p> <p>大小不可调整。</p> 	<p>16 x 16</p> <p>ICO</p>
<p>transition_2.ico</p> <p>系统托盘图标, 它与 transition_1.ico 和 transition_3.ico 一同显示, 表示一个或多个客户端组件在不同状态间过渡 (例如 VPN 连接或网络访问管理器连接时)。3 个图标文件连续显示, 看起来好像单个图标从左至右跳动。</p> <p>大小不可调整。</p> 	<p>16 x 16</p> <p>ICO</p>


Windows 安装中的文件名和说明。	图像尺寸 (像素, 长 x 高) 和类 型
<p>transition_3.ico</p> <p>系统托盘图标, 它与 transition_1.ico 和 transition_2.ico 一同显示, 表示一个或多个客户端组件在不同状态间过渡 (例如 VPN 连接或网络访问管理器连接时)。3 个图标文件连续显示, 看起来好像单个图标从左至右跳动。</p> <p>大小不可调整。</p> 	<p>16 x 16</p> <p>ICO</p>
<p>vpn_connected.ico</p> <p>表示 VPN 已连接的系统托盘图标。</p> <p>大小不可调整。</p> 	<p>16 x 16</p> <p>ICO</p>

## Linux 的 AnyConnect 图标和徽标

Linux 的所有文件位于:

/opt/cisco/anyconnect/pixmaps/

下表列出了您可替换的文件以及受影响的客户端 GUI 区域。

Linux 安装中的文件名和说明	图像尺寸 (像素, 长 x 高) 和类 型
<p>company-logo.png</p> <p>出现在用户界面各个选项卡上的公司徽标。</p> <p>对于 AnyConnect 3.0 及更高版本, 使用大小不超过 62x33 像素的 PNG 图像。</p> 	<p>142 x 92</p> <p>PNG</p>

Linux 安装中的文件名和说明	图像尺寸 (像素, 长 x 高) 和类 型
CVCabout.png About 选项卡上显示的图标。 	16 x 16 PNG
cvc-connect.png Connect 按钮旁和 Connection 选项卡上显示的图标。 	16 x 16 PNG
CVCdisconnect.png Disconnect 按钮旁显示的图标。 	16 x 16 PNG
CVCinfo.png Statistics 选项卡上显示的图标。 	16 x 16 PNG
systray_connected.png 客户端连接时显示的托盘图标。 	16 x 16 PNG
systray_notconnected.png 客户端未连接时显示的托盘图标。 	16 x 16 PNG

Linux 安装中的文件名和说明	图像尺寸 (像素, 长 x 高) 和类 型
systray_disconnecting.png 客户端断开连接时显示的托盘图标。 	16 x 16 PNG
systray_quarantined.png 客户端隔离时显示的托盘图标。 	16x16 PNG
systray_reconnecting.png 客户端重新连接时显示的托盘图标。 	16 x 16 PNG
vpnui48.png 主程序图标。 	48 x 48 PNG

## Mac OS X 的 AnyConnect 图标和徽标

OS X 的所有文件都位于:

/Cisco AnyConnect Secure Mobility Client/Contents/Resources

下表列出了您可替换的文件以及受影响的客户端 GUI 区域。

Mac OS X 安装中的文件名和说明	图像尺寸（像素，长 x 高）
bubble.png 客户端连接或断开连接时显示的通知气泡。 	142 x 92 PNG
logo.png 主屏幕右上角显示的徽标图标。 	50 x 33 PNG
vpngui.icns 用于所有图标服务（如平台、表单和查找工具）的 Mac OS X 图标文件格式。 	128 x 128 ICNS
Mac OS X 状态图标。 	16 x 16 PNG

## 创建并上传 AnyConnect 客户端帮助文件

要向 AnyConnect 用户提供帮助，请创建有关您站点的附带说明的帮助文件，并将其加载到自适应安全设备上。当用户通过 AnyConnect 连接时，AnyConnect 将下载帮助文件，并在 AnyConnect 用户界面显示帮助图标。当用户点击帮助图标时，浏览器将打开帮助文件。支持 PDF 和 HTML 文件。

## 过程

- 步骤 1 创建名为 `help_AnyConnect.html` 的 HTML 文件。
- 步骤 2 在 ASDM 中，转到 **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Customization/Localization > Binary**。
- 步骤 3 导入 `help_AnyConnect.xxx` 文件。支持的格式如下：PDF、HTML、HTM 和 MHT。
- 步骤 4 在 PC 上，启动 AnyConnect 并连接到自适应安全设备。将帮助文件下载至客户端 PC。您应该看到帮助图标已自动添加至 UI。
- 步骤 5 点击帮助图标可在浏览器中打开帮助文件。  
如果帮助图标未出现，请查看帮助目录以查看 AnyConnect 下载程序是否能检索帮助文件。  
下载程序将删除文件名的“help\_”部分，因此您应该在以下目录之一看到 AnyConnect.html（具体因操作系统而异）：

- Windows—`C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client\Help`
- Mac OS X—`/opt/cisco/anyconnect/help`

## 编写和部署脚本

发生以下事件时，您可以通过 AnyConnect 下载和运行脚本：

- 与安全设备建立新的客户端 VPN 会话。我们将此事件触发的脚本称为 *OnConnect* 脚本，因为该脚本需要此文件名前缀。
- 用安全设备终止客户端 VPN 会话时。我们将此事件触发的脚本称为 *OnDisconnect* 脚本，因为该脚本需要此文件名前缀。

值得信赖的网络检测发起的建立新客户端 VPN 会话将触发 *OnConnect* 脚本（假设满足运行脚本的要求），但网络中断后重新连接永久性 VPN 会话不会触发 *OnConnect* 脚本。

介绍此功能使用方法的某些示例包括：

- VPN 连接后刷新组策略。
- VPN 连接后映射网络驱动器，断开连接后取消映射。
- VPN 连接后登录到服务，断开连接后注销服务。

AnyConnect 支持在网络启动和独立启动期间启动脚本。

这些说明假定您了解如何编写脚本，并了解如何从目标终端的命令行运行脚本以进行脚本测试。



**注释**

AnyConnect 软件下载站点提供了某些示例脚本；查看时，请注意这些只是示例脚本。它们可能无法满足本地计算机运行这些脚本的要求，也可能在未针对网络 and 用户需求进行定制之前无法使用。思科不支持示例脚本或客户编写的脚本。

**脚本要求和限制**

请注意脚本有以下要求和限制：

- 支持的脚本数量 - AnyConnect 仅运行一个 OnConnect 脚本和一个 OnDisconnect 脚本；但这些脚本可启动其他脚本。
- 文件格式 - AnyConnect 通过文件名识别 OnConnect 脚本和 onDisconnect 脚本。它查找名称以 OnConnect 或 OnDisconnect 开头的文件，并忽略文件扩展名。AnyConnect 将执行找到的第一个前缀匹配的脚本。AnyConnect 可识别解释型脚本（例如 VBS、Perl 或 Bash）或可执行文件。
- 脚本语言 - 客户端不要求脚本以特定语言编写，但要求在客户端计算机上安装可运行脚本的应用。因此，为了保证客户端可以启动脚本，脚本必须能够从命令行运行。
- Windows 安全环境对脚本的限制 - 在 Microsoft Windows 中，AnyConnect 仅在用户登录 Windows 并建立 VPN 会话后方可启动脚本。因此，用户的安全环境施加的限制适用于这些脚本；脚本只能执行用户有权调用的功能。AnyConnect 将在 Windows 执行脚本期间隐藏 cmd 窗口，因此用户无法出于测试目的在 .bat 文件中执行显示消息的脚本。
- 启用脚本 - 默认情况下，客户端不会启动脚本。应使用 AnyConnect 配置文件 EnableScripting 参数来启用脚本。执行该操作时，客户端不要求提供脚本。
- 客户端 GUI 终止 - 客户端 GUI 终止不一定会终止 VPN 会话；OnDisconnect 脚本在会话终止后运行。
- 在 64 位 Windows 中运行脚本 - AnyConnect 客户端是 32 位应用。在 64 位 Windows 版本中运行时，AnyConnect 将使用 cmd.exe 的 32 位版本。

由于 32 位 cmd.exe 缺乏某些 64 位 cmd.exe 支持的命令，因此某些脚本可能会在尝试运行不支持的命令时停止执行，或部分运行后停止。例如，32 位版本的 Windows 7 可能无法理解 64 位 cmd.exe 支持的 msg 命令（位于 %WINDIR%\SysWOW64 中）。

因此，在创建脚本时，请使用 32 位 cmd.exe 支持的命令。

## 编写、测试和部署脚本

在目标操作系统上编写和测试您的脚本。如果脚本无法从本地操作系统的命令行正常运行，则 AnyConnect 也无法正常运行该脚本。

## 过程

**步骤 1** 编写和测试您的脚本。

**步骤 2** 选择部署脚本的方式：

- 使用 ASDM 将脚本作为二进制文件导入 ASA。

转到 **Network (Client) Access > AnyConnect Customization/Localization > Script**。

如果您使用 ASDM 6.3 版或更高版本，ASA 会在您的文件名中添加前缀 `scripts_` 和前缀 `OnConnect` 或 `OnDisconnect`，以将该文件识别为脚本。当客户端连接时，安全设备会将脚本下载到远程计算机的相应目标目录中，删除 `scripts_` 前缀，并保留 `OnConnect` 或 `OnDisconnect` 前缀。例如，如果您导入脚本 `myscript.bat`，则脚本将在安全设备中显示为 `scripts_OnConnect_myscript.bat`。在远程计算机上，脚本显示为 `OnConnect_myscript.bat`。

如果您使用的 ASDM 版本低于 6.3，则您必须导入具有以下前缀的脚本：

`scripts_OnConnect`

`scripts_OnDisconnect`

为确保脚本能够稳定运行，请将所有 ASA 配置为部署相同的脚本。如果您要修改或替换脚本，请使用与早期版本相同的名称，并将替换脚本分配到用户可能连接的所有 ASA。当用户连接时，新脚本将覆盖同名脚本。

- 使用企业软件部署系统手动将脚本部署到 VPN 终端。

如果您使用此方法，请使用以下脚本文件名前缀：

`OnConnect`

`OnDisconnect`

在以下目录中安装脚本：

**表 6:** 规定的脚本位置

操作系统	目录
Microsoft Windows	%ALLUSERSPROFILE%\Cisco\Cisco AnyConnect Secure Mobility Client\Script
Linux (在 Linux 中，为用户、组和其他类型的文件分配执行权限。)	/opt/cisco/anyconnect
Mac OS X	/opt/cisco/anyconnect/script

## 为脚本配置 AnyConnect 配置文件

### 过程

- 步骤 1** 打开 VPN 配置文件编辑器，从导航窗格中选择 **Preferences (Part 2)**。
- 步骤 2** 选中 **Enable Scripting**。客户端在连接或断开 VPN 连接时启动脚本。
- 步骤 3** 选中 **User Controllable** 使用户可以启用或禁用 On Connect 和 OnDisconnect 脚本的运行。
- 步骤 4** 选中 **Terminate Script On Next Event**，可在过渡到另一个可编写脚本的事件时使客户端可以终止运行脚本流程。例如，在 AnyConnect 启动新 VPN 会话时，如果 VPN 会话结束并终止运行 OnDisconnect 脚本，则客户端会终止运行 On Connect 脚本。在 Microsoft Windows 上，客户端也会终止 On Connect 或 OnDisconnect 脚本启动的所有脚本及其所有脚本派生项。在 Mac OS 和 Linux 上，客户端仅终止 On Connect 或 OnDisconnect 脚本，而不会终止子脚本。
- 步骤 5** 选中 **Enable Post SBL On Connect Script**（默认情况下启用）可在 SBL 建立 VPN 会话时使客户端启动 On Connect 脚本（如果有）。



**注释** 请务必将客户端配置文件添加到 ASA 组策略，以将其下载到 VPN 终端。

## 脚本故障排除

如果脚本无法运行，按如下所述尝试解决问题：

### 过程

- 步骤 1** 确保脚本有 OnConnect 或 OnDisconnect 前缀名称。 [编写、测试和部署脚本](#) 显示每个操作系统所需的脚本目录。
- 步骤 2** 尝试从命令行运行脚本。如果无法从命令行运行脚本，客户端便无法运行脚本。如果脚本在命令行运行失败，请确保已安装运行脚本的应用，并尝试在操作系统上重写脚本。
- 步骤 3** 验证 VPN 终端上的脚本目录中仅有一个 OnConnect 脚本和一个 OnDisconnect 脚本。如果客户端从 ASA 下载 OnConnect 脚本，然后下载与另一个 ASA 的文件名后缀不同的另一个 OnConnect 脚本，则客户端可能不会运行您打算运行的脚本。如果脚本路径包含多个 OnConnect 或 OnDisconnect 脚本，而且您正在使用 ASA 部署脚本，则删除脚本目录的内容并重新建立 VPN 会话。如果脚本路径

包含多个 OnConnect 或 OnDisconnect 脚本，而且您采用手动部署方法，则删除不需要的脚本并重新建立 VPN 会话。

**步骤 4** 如果操作系统是 Linux，请确保脚本文件的权限已设置为执行。

**步骤 5** 确保客户端配置文件已启用脚本功能。

## 使用 AnyConnect API 编写和部署定制应用

对于 Windows、Linux 和 Mac 计算机，您可以使用 AnyConnect API 开发自己的可执行用户界面 (UI)。通过替换 AnyConnect 二进制文件部署您的 UI。

下表列出了不同操作系统的客户端可执行文件的文件名。

客户端操作系统	客户端 GUI 文件	客户端 CLI 文件
Windows	vpnui.exe	vpncli.exe
Linux	vpnui	vpn
Mac	ASA 部署不支持。但是，您可以为使用其他方法（例如 Altiris 代理）替换客户端 GUI 的 Mac 部署可执行文件。	vpn

可执行文件能够调用您导入 ASA 的任何资源文件，例如徽标图像。部署自己的可执行文件时，您可以对资源文件使用任意文件名。

### 限制

- 无法从自适应安全设备部署更新的 AnyConnect 软件。如果您在自适应安全设备上放置了更新版本的 AnyConnect 软件包，AnyConnect 客户端将下载更新，可替换定制 UI。您必须处理定制客户端以及相关 AnyConnect 软件的分发问题。尽管 ASDM 允许您上传二进制文件以替换 AnyConnect 客户端，但在使用定制应用时不支持此部署功能。
- 如果您部署网络安全或网络访问管理器，请使用 Cisco AnyConnect 安全移动客户端 GUI。
- 不支持登录前启动功能。

# 准备 AnyConnect 定制和本地化进行 ISE 部署

## 准备 AnyConnect 本地化捆绑包

AnyConnect 本地化捆绑包是包含用于本地化 AnyConnect 的转换表文件和安装程序转换文件的压缩文件。此压缩文件是 ISE AnyConnect 资源的一部分，该资源用于从 ISE 向用户部署 AnyConnect。此压缩文件的内容由 AnyConnect 部署中您支持的语言进行定义，如此过程中所述。

### 开始之前

ISE 要求在其 AnyConnect 本地化捆绑包中有经过编译的二进制转换表。在 Gettext 中有两种文件格式：用于进行编辑的文本 .po 格式和在运行时使用的已编译二进制 .mo 格式。可使用 Gettext 工具 msgfmt 完成编译。从 <http://www.gnu.org/software/gettext/> 下载 Gettext 实用程序并在您用于管理的本地计算机（不是远程用户计算机）上安装 Gettext。

### 过程

**步骤 1** 获取并准备 AnyConnect 部署使用的转换表文件。

- a) 从 [www.cisco.com](http://www.cisco.com) 上的 Cisco AnyConnect 安全移动客户端 Software Download 页下载并打开 AnyConnect-Localization-(release).zip 文件。  
此压缩文件包含思科提供的所有语言转换的 \*.po 文件。
- b) （可选）查找您已为自己的环境定制或创建的任何其他转换表文件 (\*.po 文件)。
- c) 运行 Gettext 消息文件编译器以从您正使用的各个 \*.po 文件创建 \*.mo 文件：  
msgfmt -o AnyConnect.mo AnyConnect.po

**步骤 2** 汇编 AnyConnect 部署使用的转换表文件。

- a) 在本地计算机的工作区中创建名为 l10n 的目录。
- b) 为要包含的各个语言在 l10n 下创建目录，以语言代码命名。  
例如，fr-ch 代表法语（加拿大）。
- c) 将要包含的各个编译转换表放入适当命名的目录中。

目录结构与以下类似，其中包括法语（加拿大）、希伯来语和日语的转换表：

```
l10n\fr-ch\AnyConnect.mo
 \he\AnyConnect.mo
 \ja\AnyConnect.mo
```

**步骤 3** （仅适用于 Windows）获取并准备 AnyConnect 部署所使用的语言本地化转换文件。

- a) 在 [www.cisco.com](http://www.cisco.com) 上的 Cisco AnyConnect 安全移动客户端 的软件下载页，下载和打开包含适用于您的部署的语言本地化转换文件的压缩文件。  
压缩文件名为 anyconnect-win-(release)-web-deploy-k9-lang.zip 或 anyconnect-gina-win-(release)-web-deploy-k9-lang.zip。  
**注释** 语言本地化文件的版本必须与您的环境中使用的 AnyConnect 版本一致。当升级到 AnyConnect 的新版本时，还必须将本地化捆绑包中使用的语言本地化文件升级到同一版本。

b) 找到您为自己的环境定制或创建的所有语言本地化转换文件。

**步骤 4** (仅适用于 Windows) 汇编 AnyConnect 部署使用的语言本地化文件。

- a) 在本地计算机的同一工作区中创建名为 `mst` 的目录。
- b) 为要包含的各个语言在 `mst` 下创建目录，以语言代码命名。  
例如，`fr-ch` 代表法语（加拿大）。
- c) 将要包含的各个语言本地化文件放入适当命名的目录中。

现在，您的目录结构与以下结构类似：

```
110n\fr-ch\AnyConnect.mo
 \he\AnyConnect.mo
 \ja\AnyConnect.mo
mst\fr-ch\AnyConnect_fr-ca.mst
 \he\AnyConnect_he.mst
 \ja\AnyConnect_ja.mst
```

**步骤 5** 使用标准压缩实用程序将此目录结构压缩到适当命名的文件中，例如

`AnyConnect-Localization-Bundle-(版本).zip`，以创建 AnyConnect 本地化捆绑包。

### 接下来的操作

将 AnyConnect 本地化捆绑包作为 ISE AnyConnect 资源（用于向用户部署 AnyConnect）的一部分上传到 ISE。

## 准备 AnyConnect 定制捆绑包

AnyConnect 定制捆绑包是包含定制 AnyConnect GUI 资源、定制帮助文件、VPN 脚本和安装程序转换的压缩文件。此压缩文件是 ISE AnyConnect 资源的一部分，该资源用于从 ISE 向用户部署 AnyConnect。它的目录结构如下：

```
win\resource\
 \binary
 \transform
mac-intel\resource
 \binary
 \transform
```

定制的 AnyConnect 组件包含在 Windows 和 Mac OSX 平台的 `resource`、`binary` 和 `transform` 子目录中，具体如下所示：

- 每个 `resource` 子目录都包含该平台的所有定制 AnyConnect GUI 组件。  
要创建这些资源，请参阅 [AnyConnect GUI 创建定制图标和徽标](#)，第 47 页。
- 每个 `binary` 子目录都包含该平台的定制帮助文件和 VPN 脚本。
  - 要创建 AnyConnect 帮助文件，请参阅 [创建并上传 AnyConnect 客户端帮助文件](#)，第 55 页。
  - 要创建 VPN 脚本，请参阅 [编写和部署脚本](#)，第 56 页。
- 每个 `transform` 子目录都包含该平台的安装程序转换。

要创建 Windows 定制安装程序转换，请参阅 [修改安装行为 \(Windows\)](#)，第 34 页

要创建 Max OSX 安装程序转换，请参阅 [使用 ACTransforms.xml 在 Mac OS X 上定制安装程序行为](#)，第 40 页

## 开始之前

准备 AnyConnect 定制捆绑包之前，先创建所有必要的定制组件。

## 过程

- 
- 步骤 1** 在本地计算机的工作区创建所述目录结构。
  - 步骤 2** 在 resources 目录下存放各个平台的定制 AnyConnect GUI 文件。确认文件均适当命名，且图标和徽标的大小合适。
  - 步骤 3** 在 binary 目录下存放定制 help\_AnyConnect.html 文件。
  - 步骤 4** 在 binary 目录下存放 VPN OnConnect 和 OnDisconnect 脚本及其调用的任何其他脚本。
  - 步骤 5** 在 transform 目录下存放特定于平台的安装程序转换。
  - 步骤 6** 使用标准压缩实用程序将此目录结构压缩到适当命名的文件中，例如 AnyConnect-Customization-Bundle.zip，以创建 AnyConnect 定制捆绑包。
- 

## 接下来的操作

将 AnyConnect 定制捆绑包作为 ISE AnyConnect 资源（用于向用户部署 AnyConnect）的一部分上传到 ISE。







## 第 3 章

# AnyConnect 配置文件编辑器

- [关于配置文件编辑器，第 65 页](#)
- [独立配置文件编辑器，第 66 页](#)
- [AnyConnect VPN 配置文件，第 68 页](#)
- [AnyConnect 本地策略，第 81 页](#)

## 关于配置文件编辑器

Cisco AnyConnect 安全移动客户端软件包包含适用于所有操作系统的配置文件编辑器。在 ASA 上加载 AnyConnect 客户端映像时，ASDM 会激活配置文件编辑器。您可从本地或闪存上传客户端配置文件。

如果加载多个 AnyConnect 软件包，ASDM 会激活来自最新的 AnyConnect 软件包的客户端配置文件编辑器。此方法可确保编辑器显示所加载的最新 AnyConnect 以及早期版本客户端的功能。

还有在 Windows 上运行的独立配置文件编辑器。

## AnyConnect 配置文件

- [AnyConnect VPN 配置文件，第 68 页](#)
- [AnyConnect 本地策略，第 81 页](#)
- [网络访问管理器配置文件，第 140 页](#)
- [ISE 终端安全评估配置文件编辑器，第 173 页](#)
- [典型网络安全配置，第 178 页](#)
- [配置客户体验反馈，第 205 页](#)

## 从 ASDM 添加新配置文件



**注释** 在创建客户端配置文件之前，必须先上传客户端映像。

配置文件按照管理员定义的最终用户要求和终端上的身份验证策略部署为 AnyConnect 的一部分，使预配置的网络配置文件可供最终用户使用。使用配置文件编辑器创建并配置一个或多个配置文件。AnyConnect 将配置文件编辑器作为 ASDM 的一部分，并且作为独立的 Windows 程序。

要从 ASDM 向 ASA 添加新的客户端配置文件，请执行以下操作：

### 过程

- 步骤 1** 打开 ASDM，选择 **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Profile**。
- 步骤 2** 点击 **Add**。
- 步骤 3** 输入配置文件名称。
- 步骤 4** 从 **Profile Usage** 下拉列表中选择要为其创建配置文件的模块。
- 步骤 5** （可选）在 **Profile Location** 字段中，点击 **Browse Flash**，并选择 ASA 上 XML 文件的设备文件路径。
- 步骤 6** （可选）如果使用独立编辑器创建了配置文件，请点击 **Upload** 以使用该配置文件定义。
- 步骤 7** （可选）从下拉列表中选择 AnyConnect 组策略。
- 步骤 8** 点击 **OK**。

## 独立配置文件编辑器

除了 ASDM 中的配置文件编辑器外，您还可以使用 Windows 配置文件编辑器的独立版本。预部署客户端时，您可以使用独立配置文件编辑器为 VPN 服务及使用软件管理系统部署到计算机的其他模块创建配置文件。

您可以通过使用 **Add or Remove Programs** 修改独立 Cisco AnyConnect 配置文件编辑器安装，或卸载 VPN、网络访问管理器、网络安全、客户体验反馈或 ISE 终端安全评估配置文件编辑器。

### 要求

- Java - JRE 1.6 是配置文件编辑器的最低必备要求，但管理员必须自行部署。



**注释** 卸载独立配置文件编辑器时，JRE 1.6 不会自动卸载。您必须单独卸载。

- 支持的操作系统 - 此应用已在 Windows 7 上测试。MSI 仅在 Windows 上运行。
- 支持的浏览器 - Firefox 和 Internet Explorer 支持此应用中的帮助文件。这些帮助文件尚未在其他浏览器中测试。
- 所需的硬盘驱动器空间 - Cisco AnyConnect 配置文件编辑器应用所需的硬盘空间不超过 5 MB。JRE 1.6 所需的硬盘空间不超过 100 MB。
- 必须将 ASA 添加到 VPN 配置文件的服务器列表中，以便客户端 GUI 在第一次连接时显示所有用户可控的设置。如果您不将 ASA 地址或 FQDN 添加为配置文件中的主机条目，则不会向会话应用过滤器。例如，如果您创建了一个证书匹配，且证书与条件正确匹配，但您未将 ASA 添加为该配置文件中的主机条目，那么证书匹配将被忽略。

## 安装独立 AnyConnect 配置文件编辑器

独立 AnyConnect 配置文件编辑器是与 AnyConnect ISO 和 .pkg 文件分开来以 Windows 可执行文件 (.exe) 的形式分配的，并具有以下文件命名约定：

anyconnect-profileeditor-win-<version>-k9.exe。

### 过程

- 步骤 1** 从 Cisco.com 下载 anyconnect-profileeditor-win-<version>-k9.exe。
- 步骤 2** 双击 anyconnect-profileeditor-win-<version>-k9.exe 以启动安装向导。
- 步骤 3** 在 Welcome 屏幕上，点击 **Next**。
- 步骤 4** 在 Choose Setup Type 窗口，点击以下其中一个按钮并点击 **Next**:
  - **Typical** - 仅自动安装网络访问管理器配置文件编辑器。
  - **Custom** - 允许选择安装以下任何配置文件编辑器：AMP 启用程序配置文件编辑器、ISE 状态配置文件编辑器、网络访问管理器配置文件编辑器、网络安全配置文件编辑器、客户体验反馈配置文件编辑器和 VPN 配置文件编辑器。
  - **Complete** - 自动安装 AMP 启用程序配置文件编辑器、ISE 终端安全评估配置文件编辑器、网络访问管理器配置文件编辑器、网络安全配置文件编辑器、客户体验反馈配置文件编辑器和 VPN 配置文件编辑器。
- 步骤 5** 如果在上一步点击 **Typical** 或 **Complete**，可跳到下一步。如果在上一步点击 **Custom**，可点击要安装的独立配置文件编辑器的图标并选择 **Will be installed on local hard drive**，或者点击 **Entire Feature will be unavailable** 以防止安装独立配置文件编辑器。点击 **Next**。
- 步骤 6** 在 Ready to Install 屏幕，点击 **Install**。
- 步骤 7** 点击 **Finish**.
  - 独立 AnyConnect 配置文件编辑器即安装在 C:\Program Files\Cisco\Cisco AnyConnect Profile Editor 目录中。

- 您可以通过选择 **Start > All Programs > Cisco > Cisco AnyConnect Profile Editor**，然后单击子菜单中所需的独立配置文件编辑器，或者通过点击桌面上安装的相应配置文件编辑器快捷方式图标，启动 AMP 启用程序、VPN、网络访问管理器、ISE 终端安全评估和网络安全配置文件编辑器。

---

## 使用独立配置文件编辑器编辑客户端配置文件

为了安全起见，您不能在独立配置文件编辑器外手动编辑客户端配置文件 XML 文件。ASA 不接受在独立配置文件编辑器外编辑的任何配置文件 XML 文件。

### 过程

---

**步骤 1** 通过双击桌面上的快捷方式图标或导航至 **Start > All Programs > Cisco > Cisco AnyConnect Profile Editor** 并从子菜单中选择所需的配置文件编辑器，启动需要的配置文件编辑器。

**步骤 2** 选择 **File > Open**，然后导航到要编辑的客户端配置文件 XML 文件。

如果您使用另一功能（例如 VPN）的配置文件编辑器错误地尝试打开某种功能（例如网络安全）的客户端配置文件，您会收到 **Schema Validation failed** 消息而无法编辑配置文件。

如果无意中尝试在同一种配置文件编辑器的两个实例中编辑同一客户端配置文件，将保存对客户端配置文件进行的最后编辑。

**步骤 3** 对配置文件进行更改，然后选择 **File > Save** 可保存更改。

---

## AnyConnect VPN 配置文件

AnyConnect 配置文件中启用了 Cisco AnyConnect 安全移动客户端功能。这些配置文件包含核心客户端 VPN 功能和可选客户端模块网络访问管理器、ISE 终端安全评估、客户体验反馈和网络安全的配置设置。在 AnyConnect 安装和更新过程中，ASA 将部署配置文件。用户无法管理或修改配置文件。

您可以配置 ASA 或 ISE，以向所有 AnyConnect 用户全局部署配置文件，或基于用户的组策略向用户部署。通常情况下，对于安装的每个 AnyConnect 模块，用户都有一个配置文件。在某些情况下，您可能希望为用户提供多个 VPN 配置文件。在多个位置工作的某些用户可能需要多个 VPN 配置文件。

某些配置文件设置本地存储在用户计算机的用户首选项文件或全局首选项文件中。用户文件包含 AnyConnect 客户端在客户端 GUI 的 Preferences 选项卡中显示用户可控设置所需的信息，以及有关上一次连接的信息，例如用户、组和主机。

全局文件包含有关用户可控设置的信息，因此您可以在登录之前应用这些设置（因为此时无用户）。例如，客户端需要了解登录前是否已启用“登录前启动”和/或“启动时自动连接”功能。

## AnyConnect 配置文件编辑器，首选项（第 1 部分）

- **Use Start Before Logon** -（仅限 Windows）通过在 Windows 登录对话框出现之前启动 AnyConnect，强制用户在登录到 Windows 之前通过 VPN 连接而连接到企业基础设施。进行身份验证之后，登录对话框将会显示，用户可以像平常一样登录。
- **Show Pre-connect Message** - 支持管理员在用户首次尝试连接之前显示一条一次性消息。例如，此消息可以提醒用户将智能卡插入读卡器。此消息出现在 AnyConnect 消息目录中并已本地化。
- **Certificate Store** - 控制 AnyConnect 使用哪个证书存储库来存储和读取证书。默认设置 (All) 适用于大多数情况。请勿更改此设置，除非有特定原因或场景要求这样做。
  - All（默认值）- 指示 AnyConnect 客户端使用所有证书存储库来定位证书。
  - Machine - 指示 AnyConnect 客户端仅在 Windows 本地计算机证书存储库中查找证书。
  - User - 指示 AnyConnect 客户端仅在本地用户证书存储库中查找证书。
- **Certificate Store Override** - 允许管理员指示 AnyConnect 在用户对其设备没有管理员权限时在 Windows 计算机证书存储库中搜索证书。



注释

为了使用计算机证书与 Windows 连接，您必须具有预部署的配置文件并且启用了此选项。如果在连接之前 Windows 设备上不存在此配置文件，则在计算机存储库中无法访问证书，因而连接失败。

- **Auto Connect on Start** - 启动时，AnyConnect 自动与 AnyConnect 配置文件指定的安全网关建立 VPN 连接，或者连接到客户端连接到的最后一个网关。
- **Minimize On Connect** - 建立 VPN 连接后，AnyConnect GUI 最小化。
- **Local LAN Access** - 允许用户在与 ASA 的 VPN 会话期间完成对连接到远程计算机的本地 LAN 的访问。



注释

若启用本地 LAN 访问，则用户计算机进入企业网络可能导致来自公共网络的安全漏洞。或者，您可以配置安全设备（版本 8.4(1) 或更高版本）来部署一个 SSL 客户端防火墙，该防火墙使用默认组策略中包含的 AnyConnect 客户端本地打印防火墙规则。要启用此防火墙规则，还必须在此编辑器中启用“自动 VPN 策略”，永远在线，和“允许 VPN 断开连接”，首选项（第 2 部分）。

- **Auto Reconnect** - 连接丢失时，AnyConnect 尝试重新建立 VPN 连接（默认为启用）。如果禁用 Auto Reconnect，则无论连接出于何种原因断开连接，都不会尝试重新连接。

### 自动重新连接行为

- **DisconnectOnSuspend**（默认值）- AnyConnect 在系统暂停时释放分配给 VPN 会话的资源，并且在系统恢复之后不尝试重新连接。
- **ReconnectAfterResume** - 连接丢失时，AnyConnect 尝试重新建立 VPN 连接。
- **Auto Update** - 选中此选项时，将启用客户端的自动更新。如果选中 **User Controllable**，则用户可以在客户端覆盖此设置。
- **RSA Secure ID Integration**（仅限 Windows）- 控制用户如何与 RSA 交互。默认情况下，AnyConnect 确定 RSA 交互的正确方法（自动设置：软件或硬件令牌均接受）。
- **Windows Logon Enforcement** - 允许从远程桌面协议 (RDP) 会话建立 VPN 会话。必须在组策略中配置拆分隧道。当建立 VPN 连接的用户退出时，AnyConnect 会断开 VPN 连接。如果连接由远程用户建立，则该远程用户退出时 VPN 连接会终止。

**Single Local Logon**（默认值）- 在整个 VPN 连接期间只允许一个本地用户登录。此外，当一个或多个远程用户登录到客户端 PC 时，本地用户可以建立 VPN 连接。此设置对通过 VPN 连接从企业网络登录的远程用户没有影响。



**注释** 如果为全有或全无隧道配置了 VPN 连接，则修改 VPN 连接的客户端 PC 路由会导致远程登录断开连接。如果 VPN 连接进行了分割隧道配置，远程登录可能会也可能不会断开连接，这取决于 VPN 连接的路由配置。

**Single Logon** - 在整个 VPN 连接期间只允许一个用户登录。如果通过本地或远程登录的用户不止一个，当 VPN 连接建立时，该连接不被允许。如果 VPN 连接期间有第二个用户通过本地或远程登录，则 VPN 连接将终止。由于在 VPN 连接期间不允许进行其他登录，所以无法通过 VPN 连接进行远程登录。

- **Windows VPN Establishment** - 确定当远程登录到客户端 PC 的用户建立 VPN 连接时 AnyConnect 的行为。可能的值包括：

**Local Users Only**（默认值）- 阻止远程登录用户建立 VPN 连接。此功能与 AnyConnect 早期版本中的功能相同。

**Allow Remote Users** - 允许远程用户建立 VPN 连接。但是，如果所配置的 VPN 连接路由导致远程用户断开连接，则 VPN 连接会终止，以允许远程用户重新获得对客户端 PC 的访问权限。如果远程用户想要断开其远程登录会话而不终止 VPN 连接，则必须在 VPN 建立后等待 90 秒钟。

- **Clear SmartCard PIN**
- **IP Protocol Supported** - 若同时具有 IPv4 和 IPv6 地址的客户端尝试使用 AnyConnect 连接到 ASA，AnyConnect 需要决定使用哪种 IP 协议发起连接。默认情况下，AnyConnect 先使用 IPv4 尝试连接。如果这样不成功，AnyConnect 将尝试使用 IPv6 发起连接。

此字段配置初始 IP 协议和回退顺序。

IPv4 - 仅可建立到 ASA 的 IPv4 连接。

IPv6 - 仅可建立到 ASA 的 IPv6 连接。

IPv4, IPv6 - 先尝试建立到 ASA 的 IPv4 连接。如果客户端无法使用 IPv4 建立连接，则尝试建立 IPv6 连接。

IPv6, IPv4 - 先尝试建立到 ASA 的 IPv6 连接。如果客户端无法使用 IPv6 进行连接，则尝试进行 IPv4 连接。



**注释** IPv4 与 IPv6 协议之间的故障切换也可能发生在 VPN 会话期间。如果主 IP 协议丢失，在可能的情况下将通过副 IP 协议重新建立 VPN 会话。

## AnyConnect 配置文件编辑器，首选项（第 2 部分）

- **Disable Automatic Certificate Selection**（仅限 Windows）— 禁止客户端自动选择证书并提示用户选择身份验证证书。

相关主题：[配置证书选择](#)

- **Proxy Settings** - 在 AnyConnect 配置文件中指定一个策略来控制客户端对代理服务器的访问。当代理配置阻止用户从企业网络外部建立隧道时，使用此设置。在隧道建立后，您可以在组策略中配置以下代理设置。

**Native** - 让客户端既使用以前由 AnyConnect 配置的代理设置，也使用在浏览器中配置的代理设置。在全局用户首选项中配置的代理设置优先于浏览器代理设置。

**IgnoreProxy** - 忽略用户计算机上的浏览器代理设置。不影响可以访问 ASA 的代理。

**Override** - 手动配置公共代理服务器的地址。公共代理是唯一一种对 Linux 支持的代理类型。Windows 也支持公共代理。您可以将公共代理地址配置为用户可控制。

- **Allow Local Proxy Connections** - 默认情况下，AnyConnect 让 Windows 用户通过本地 PC 上的透明或不透明代理服务建立 VPN 会话。如果要禁用对本地代理连接的支持，请取消选中此参数。例如，某些无线数据卡提供的加速软件和某些防病毒软件上的网络组件都可提供透明代理服务
- **Enable Optimal Gateway Selection (OGS)**，（仅限 IPv4 客户端）- AnyConnect 根据往返时间 (RTT) 确定并选择哪个安全网关对于连接或断开连接是最佳选择，从而尽可能缩短互联网流量延迟，而且无需用户干预。OGS 不是安全功能，它不会在安全网关集群之间或集群内执行负载均衡。您控制 OGS 的激活和取消激活，并指定最终用户是否可以自己控制此功能。Automatic Selection 显示在客户端 GUI 的 Connection 选项卡中的 Connect To 下拉列表中。

**注释**

如果配置了自动代理检测，则无法执行 OGS。在配置了代理自动配置 (PAC) 文件后或启用了 Always On 时也无法执行 OGS。

如果使用 AAA，则在过渡到另外一个安全网关时，用户可能必须重新输入凭证。使用证书可消除此问题。

**Suspension Time Threshold** (小时) - 输入在调用新网关选择计算之前 VPN 必须已暂停的最短时间（以小时为单位）。通过优化此值以及下一个可配置的性能改进阈值 Performance Improvement Threshold，您可以在选择最佳网关和减少强制重新输入凭证次数之间找到适当的平衡。

**Performance Improvement Threshold (%)** - 在系统恢复后触发客户端重新连接到另一个安全网关的性能改进百分比。为特定网络调整这些值，可在选择最佳网关与减少次数之间找到合适的平衡，从而强制重新输入凭证。默认值为 20%。

- **Automatic VPN Policy** (仅限 Windows 和 Mac) - 启用 Trusted Network Detection allowing AnyConnect 可根据 Trusted Network Policy 和 Untrusted Network Policy 自动管理何时启动或停止 VPN 连接。如果禁用，则 VPN 连接只能手动启动和停止。设置 Automatic VPN Policy 不会阻止用户手动控制 VPN 连接。

**Trusted Network Policy** - 当用户处于企业网络（受信任网络）中时，AnyConnect 对 VPN 连接自动采取的操作。

Disconnect (默认值) - 检测到受信任网络时断开 VPN 连接。

Connect - 检测到受信任网络时发起 VPN 连接。

Do Nothing - 在受信任网络中不执行任何操作。将 Trusted Network Policy 和 Untrusted Network Policy 都设置为 Do Nothing 会禁用 Trusted Network Detection。

Pause - 如果用户在受信任网络外建立 VPN 会话之后进入被配置为受信任的网络，则 AnyConnect 会暂停此 VPN 会话而不是将其断开连接。当用户再次离开受信任网络时，AnyConnect 会恢复该会话。此功能是为了给用户方便，因为有了它，在用户离开受信任网络后不需要建立新的 VPN 会话。

**Untrusted Network Policy** - 当用户处于企业网络外（不受信任的网络）时，AnyConnect 启动 VPN 连接。此功能可以在用户处于受信任网络外时发起 VPN 连接，从而提高安全意识。

Connect (默认值) - 在检测到不受信任网络时发起 VPN 连接。

Do Nothing - 在受信任网络中不执行任何操作。此选项禁用永远在线 VPN。将 Trusted Network Policy 和 Untrusted Network Policy 都设置为 Do Nothing 会禁用 Trusted Network Detection。

**Trusted DNS Domains** - 客户端处于受信任网络中时，网络接口可能具有的 DNS 后缀（逗号分隔的字符串）。例如：\*.cisco.com。通配符 (\*) 可用于 DNS 后缀。



**Trusted DNS Servers** - 客户端处于受信任网络中时, 网络接口可能具有的 DNS 服务器地址 (逗号分隔的字符串)。 例如: 192.168.1.2, 2001:DB8::1。 DNS 服务器地址支持通配符 (\*)。

- **Always On** - 确定当用户登录到运行受支持的 Windows 或 Mac OS X 操作系统的计算机时 AnyConnect 是否自动连接到 VPN。 您可以实施企业策略, 以便在计算机不在受信任网络中时阻止计算机访问互联网资源, 从而保护它免遭安全威胁。 根据分配策略所用的匹配条件, 您可以指定异常情况, 从而在组策略和动态访问策略中设置 永远在线 VPN 参数来覆盖此设置。 如果 AnyConnect 策略启用 永远在线, 而动态访问策略或组策略禁用它, 只要其条件匹配关于建立每个新会话的动态访问策略或组策略, 客户端就为当前和将来的 VPN 会话保留此禁用设置。 在启用后, 您就可以配置其他参数。

相关主题: [需要使用 永远在线 的 VPN 连接](#)

**Allow VPN Disconnect** - 确定 AnyConnect 是否为 永远在线 VPN 会话显示 Disconnect 按钮。 由于当前 VPN 会话存在性能问题或 VPN 会话中断后重新连接出现问题, 永远在线 VPN 会话的用户可能想要点击 Disconnect 以选择其他安全网关。

Disconnect 会锁定所有接口, 以防止数据泄漏并防止计算机在建立 VPN 会话外还以其他方式访问互联网。 出于上述原因, 禁用 Disconnect 按钮有时可能会阻碍或防止 VPN 接入。

**Connect Failure Policy** - 确定在 AnyConnect 无法建立 VPN 会话 (例如, 无法访问 ASA) 时计算机是否可访问互联网。 此参数只在启用了 永远在线 和 Allow VPN Disconnect 时才适用。 如果选择 永远在线, 则 fail-open 策略允许网络连接, fail-close 策略禁用网络连接。

**Closed** - 当无法访问 VPN 时限制网络访问。 此设置的目的是, 当负责保护终端的专用网络中的资源不可用时, 帮助保护企业资产免遭网络威胁。

**Open** - 当无法访问 VPN 时允许网络访问。



注意

如果 AnyConnect 未能建立 VPN 会话, 连接故障关闭策略会阻止网络访问。 它主要用在网络访问的安全持久性比始终可用性更重要的企业中, 以特别保证企业的安全。 除本地资源 (例如, 分隔隧道允许和 ACL 限制的打印机和系留设备等) 外, 它会阻止所有网络访问。 如果用户在安全网关不可用时需要 VPN 以外的互联网接入, 它可能停止运行。 AnyConnect 检测大多数强制网络门户。 如果它不能检测到强制网络门户, 连接故障关闭策略会阻止所有网络连接。

如果您部署关闭连接策略, 我们强烈建议您采用分阶段方法。 例如, 首先利用连接失败打开策略部署 永远在线 VPN, 并调查用户 AnyConnect 无法无缝连接的频率。 然后, 在早期采用者用户中部署连接失败关闭策略的一个小型试点部署, 并征求他们的反馈。 逐步扩展试点计划, 同时继续征求反馈, 再考虑全面部署。 部署连接失败关闭策略时, 请确保向 VPN 用户告知网络访问限制以及连接失败关闭策略的优点。

相关主题: [关于强制网络门户](#)

如果 Connect Failure Policy 为 Closed, 则您可以配置以下设置:

**Allow Captive Portal Remediation** - 当客户端检测到强制网络门户（热点）时，让 AnyConnect 解除关闭连接失败策略所施加的网络访问限制。酒店和机场通常使用强制网络门户，它们要求用户打开浏览器并满足允许互联网访问所需的条件。默认情况下，此参数处于未选中状态可提供最高安全性；但是，如果您想要客户端连接到 VPN 而强制网络门户却阻止它这样做，则您必须启用此参数。

**Remediation Timeout** - AnyConnect 解除网络访问限制的分钟数。此参数只在 Allow Captive Portal Remediation 参数被选中且客户端检测到强制网络门户时适用。指定满足一般强制网络门户要求所需的足够时间（例如，5 分钟）。

**Apply Last VPN Local Resource Rules** - 如果 VPN 无法访问，则客户端应用其从 ASA 收到的最后一个客户端防火墙，此 ASA 可能包含允许访问本地 LAN 资源的 ACL。

相关主题：[配置连接失败策略](#)

- **PPP Exclusion** - 对于通过 PPP 连接的 VPN 隧道，指定是否以及如何确定排除路由。客户端可以将去往此安全网关的流量从去往安全网关外目标的隧道流量中排除。排除路由在 AnyConnect GUI 的 Route Details 中显示为非安全路由。如果将此功能设置为用户可控制，则用户能够读取和更改 PPP 排除设置。

**Automatic** - 启用 PPP 排除。AnyConnect 自动使用 PPP 服务器的 IP 地址。指示用户仅在自动检测无法获取 IP 地址时更改值。

**Disabled** - 不应用 PPP 排除。

**Override** - 也会启用 PPP 排除。当自动检测无法获取 PPP 服务器的 IP 地址且您将 PPP 排除配置为用户可控制时，选择此选项。

如果启用了 PPP Exclusion，则还要设置：

**PPP Exclusion Server IP** - 用于 PPP 排除的安全网关 IP 地址。

相关主题：[指示用户覆盖 PPP 排除](#)

- **Enable Scripting** - 如果 OnConnect 和 OnDisconnect 脚本在安全设备闪存上，请启动它们。

**Terminate Script On Next Event** - 发生向另一个可编写脚本事件的过渡时终止正在运行的脚本进程。例如，如果 VPN 会话结束，则 AnyConnect 终止正在运行的 OnConnect 脚本；如果客户端启动新的 VPN 会话，则终止正在运行的 OnDisconnect 脚本。在 Microsoft Windows 上，客户端还会终止 OnConnect 或 OnDisconnect 脚本启动的任何脚本以及它们所有的脚本子代。在 Mac OS 和 Linux 上，客户端只会终止 OnConnect 或 OnDisconnect 脚本；它不会终止子脚本。

**Enable Post SBL On Connect Script** - 启动 OnConnect 脚本（如果存在），然后 SBL 建立 VPN 会话。（仅当 VPN 终端运行 Microsoft Windows 时才受支持。）

- **注销时保留 VPN** - 确定是否在用户注销 Windows 操作系统时保持 VPN 会话。

**User Enforcement** - 指定当其他用户登录时是否结束 VPN 会话。此参数仅在 Retain VPN On Logoff 被选中且原始用户在 VPN 会话进行中注销 Windows 时适用。

- **Authentication Timeout Values** - 默认情况下，AnyConnect 在终止连接尝试前，要等待长达 12 秒才能从安全网关获得身份验证。然后，AnyConnect 显示一条消息，指示身份验证已超时。输入介于 0 - 20 之间的秒数。

## AnyConnect 配置文件编辑器，备用服务器

您可以配置一个备用服务器列表，以便客户端在用户选择的服务器发生故障时使用。如果用户选择的服务器发生故障，客户端会尝试连接到在列表顶端的最佳服务器备用。如果该尝试失败了，客户端会按其选择结果依次尝试最佳网关选择列表中剩余的每个服务器。

**Host Address** - 指定一个 IP 地址或完全限定域名 (FQDN) 以包含在备用服务器列表中。

- **Add** - 将主机地址添加到备用服务器列表。
- **Move Up** - 将选定的备用服务器在列表中向上移动。如果用户选择的服务器发生故障，则客户端首先尝试连接到此列表顶端的备用服务器，必要时再沿着列表从上到下逐个尝试。
- **Move Down** - 将选定的备用服务器在列表中向下移动。
- **Delete** - 从服务器列表中删除备用服务器。

## AnyConnect 配置文件编辑器，证书匹配

启用可用于优化此窗格中自动客户端证书选择的各属性的定义。

如果未指定证书匹配条件，则 AnyConnect 应用以下证书匹配规则：

- **Key Usage: Digital\_Signature**
- **Extended Key Usage: Client Auth**

如果配置文件中指定了任何条件匹配规范，则不应用这些匹配规则，除非配置文件中具体列出了这些规则。

- **Key Usage** - 在选择可接受的客户端证书时，使用以下证书密钥属性：

Decipher\_Only - 解密数据，且未设置其他位（Key\_Agreement 除外）。

Encipher\_Only - 加密数据，且未设置其他位（Key\_Agreement 除外）。

CRL\_Sign - 验证 CRL 上的 CA 签名。

Key\_Cert\_Sign - 验证证书上的 CA 签名。

Key\_Agreement - 密钥协议。

Data\_Encipherment - 加密除 Key\_Encipherment 以外的数据。

Key\_Encipherment - 加密密钥。

Non\_Repudiation - 验证数字签名保护，以免错误拒绝某些操作（Key\_Cert\_sign 或 CRL\_Sign 除外）。

Digital\_Signature - 验证数字签名（Non\_Repudiation、Key\_Cert\_Sign 或 CRL\_Sign 除外）。

- **Extended Key Usage** - 使用以下 Extended Key Usage 设置。OID 括在括号内：

ServerAuth (1.3.6.1.5.5.7.3.1)

ClientAuth (1.3.6.1.5.5.7.3.2)

CodeSign (1.3.6.1.5.5.7.3.3)

EmailProtect (1.3.6.1.5.5.7.3.4)

IPSecEndSystem (1.3.6.1.5.5.7.3.5)

IPSecTunnel (1.3.6.1.5.5.7.3.6)

IPSecUser (1.3.6.1.5.5.7.3.7)

TimeStamp (1.3.6.1.5.5.7.3.8)

OCSPSign (1.3.6.1.5.5.7.3.9)

DVCS (1.3.6.1.5.5.7.3.10)

IKE Intermediate

- **Custom Extended Match Key**（最多 10 个）- 指定定制扩展匹配密钥（如果有，最多 10 个）。证书必须与您输入的所有指定密钥匹配。以 OID 格式（例如 1.3.6.1.5.5.7.3.11）输入密钥。
- **Distinguished Name**（最多 10 个）- 指定在选择可接受的客户端证书时用于完全匹配条件的可分辨名称 (DN)。

**Name** - 用于匹配的可分辨名称 (DN):

CN - 主题通用名

C - 主题国家/地区

DC - 域组件

DNQ - 主题 DN 限定符

EA - 主题邮件地址

GENQ - 主题代际限定符

GN - 主题给定名称

I - 主题首字母缩写

L - 主题城市

N - 主题未定义的名称

O - 主题公司

OU - 主题部门

SN - 主题姓氏

SP - 主题省/自治区  
ST - 主题州  
T - 主题称谓  
ISSUER-CN - 颁发者通用名  
ISSUER-DC - 颁发者组件  
ISSUER-SN - 颁发者姓氏  
ISSUER-GN - 颁发者给定名称  
ISSUER-N - 颁发者未定义的名称  
ISSUER-I - 颁发者首字母缩写  
ISSUER-GENQ - 颁发者代际限定符  
ISSUER-DNQ - 颁发者 DN 限定符  
ISSUER-C - 颁发者国家/地区  
ISSUER-L - 颁发者城市  
ISSUER-SP - 颁发者所在省/自治区  
ISSUER-ST - 颁发者所在州  
ISSUER-O - 颁发者所在公司  
ISSUER-OU - 颁发者所在部门  
ISSUER-T - 颁发者称谓  
ISSUER-EA - 颁发者邮件地址

**Pattern** - 指定要匹配的字符串。要匹配的模式应仅包括要匹配的字符串部分。不需要包括模式匹配或正则表达式语法。如果输入了语法，此语法将被视为待搜索字符串的一部分。

例如，如果示例字符串是 `abc.cisco.com`，且为了与 `cisco.com` 匹配，则输入的模式应该是 `cisco.com`。

**Operator** - 为此 DN 执行匹配时使用的运算符。

Equal - 与 `==` 等效

Not Equal - 与 `!=` 等效

**Wildcard** - 启用后将包含通配符模式匹配。在通配符启用的情况下，该模式可以位于字符串的任何位置。

**Match Case** - 选中可启用区分大小写的模式匹配。

## 相关主题

[配置证书匹配，第 129 页](#)

# AnyConnect 配置文件编辑器，证书注册

证书注册使 AnyConnect 能够使用简单证书注册协议 (SCEP) 调配和续订用于客户端身份验证的证书。

- **Certificate Expiration Threshold** - 在证书过期日前，AnyConnect 提醒用户其证书即将过期的天数（RADIUS 密码管理不支持该功能）。默认值为零（不显示警告）。值范围为 0 到 180 天。
- **Certificate Import Store** - 选择保存注册证书的 Windows 证书存储区。
- **Automatic SCEP Host** - 对于旧式 SCEP，指定已配置 SCEP 证书检索的 ASA 的主机名和连接配置文件（隧道组）。输入 ASA 的完全限定域名 (FQDN) 或连接配置文件名称。例如，主机名 `asa.cisco.com` 和连接配置文件名称 `scep_eng`。
- **CA URL** - 对于旧式 SCEP，识别 SCEP CA 服务器。输入 CA 服务器的 FQDN 或 IP 地址。例如，`http://ca01.cisco.com`。

**Prompt For Challenge PW** - 启用此项可让用户手动发出证书请求。当用户点击 **Get Certificate** 时，客户端将提示用户输入用户名和一次性密码。

**Thumbprint** - CA 的证书拇指指纹。使用 SHA1 或 MD5 哈希值。



### 注释

CA 服务器管理员可提供 CA URL 和拇指指纹，并应从服务器（而非签发的服务器证书的“fingerprint”或“thumbprint”属性字段）直接检索拇指指纹。

- **Certificate Contents** - 指定要包含在 SCEP 注册请求中的证书内容：

名称 (CN) - 证书中的通用名。

部门 (OU) - 证书中指定的部门名称。

公司 (O) - 证书中指定的公司名称。

州 (ST) - 证书中指定的州标识符。

州 (SP) - 另一个州标识符。

国家/地区 (C) - 证书中指定的国家/地区标识符。

邮件 (EA) - 邮件地址。以下示例中，邮件地址 (EA) 为 `%USER%@cisco.com`。 `%USER%` 对应用户的 ASA 用户名登录凭证。

域 (DC) - 域组件。在以下示例中，域 (DC) 设置为 `cisco.com`。

姓氏 (SN) - 家族名或姓。

给定名称 (GN) - 通常为名。

UnstructName (N) - 未定义的名称。

首字母缩写 (I) - 用户的首字母缩写。

限定符 (GEN) - 用户的代限定符。例如，“Jr.”或“III.”

限定符 (DN) - 整个 DN 的限定符。

城市 (L) - 城市标识符。

称谓 (T) - 人员的称谓。例如，女士、夫人、先生

CA 域 - 用于 SCEP 注册，一般为 CA 域。

密钥大小 - 为待注册证书所生成的 RSA 密钥的大小。

- **Display Get Certificate Button** - 启用 AnyConnect GUI 可在下列条件下显示 Get Certificate 按钮：

证书设置为在证书过期阈值定义的时间段后过期（RADIUS 不支持）。

证书已过期。

证书不存在。

证书无法匹配。

#### 相关主题

[配置证书注册，第 118 页](#)

## AnyConnect 配置文件编辑器，移动策略

AnyConnect 3.0 版及更高版本不支持 Windows Mobile 设备。请参阅 *Cisco AnyConnect 安全移动客户端管理员指南*，版本 2.5，了解 Windows Mobile 设备的相关信息。

## AnyConnect 配置文件编辑器，服务器列表

您可以配置在客户端 GUI 中显示的服务器列表。用户可以在该列表中选择服务器以建立 VPN 连接。

服务器列表表列：

- 主机名 - 用于指代主机、IP 地址或完全限定域名 (FQDN) 的别名。
- 主机地址 - 服务器的 IP 地址或 FQDN。
- 用户组 - 用于与主机地址一同组成基于组的 URL。
- 自动 SCEP 主机 - 为调配和续订进行客户端身份验证的证书而指定的简单证书注册协议。
- CA URL - 此服务器用于连接到证书颁发机构 (CA) 的 URL。

**Add/Edit** - 启动 Server List Entry 对话框，您可在此指定上述服务器参数。

**Delete** - 从服务器列表中删除服务器。

**Details** - 显示有关备用服务器或服务器 CA URL 的更多详细信息。

相关主题

[配置 VPN 连接服务器，第 89 页](#)

## AnyConnect 配置文件编辑器，添加/编辑服务器列表

- **Host Display Name** - 输入用于指代主机的别名、IP 地址或完全限定域名 (FQDN)。
- **FQDN or IP Address** - 指定服务器的 IP 地址或 FQDN。
  - 如果在 Host Address 字段中指定了 IP 地址或 FQDN，则 Host Name 字段中的条目会变成 AnyConnect 客户端弹出式托盘的连接下拉列表中的服务器标签。
  - 如果仅在 Hostname 字段中指定了 FQDN，而未在 Host Address 字段中指定 IP 地址，则 Hostname 字段中的 FQDN 将由 DNS 服务器进行解析。
  - 如果输入 IP 地址，请使用安全网关的公共 IPv4 地址或全局 IPv6 地址。不支持使用链路本地安全网关地址。
- **User Group** - 指定一个用户组。

用户组用于与主机地址一起形成一个基于组的 URL。如果指定 Primary Protocol 为 IPsec，则 User Group 必须是连接配置文件（隧道组）的确切名称。对于 SSL，用户组是连接配置文件的组 URL 或组别名。
- **Additional mobile-only settings** - 选择此项可配置 Apple iOS 和 Android 移动设备。
- **Backup Server List**

您可以配置一个备用服务器列表，以便客户端在用户选择的服务器发生故障时使用。如果服务器发生故障，则客户端首先尝试连接到此列表顶端的服务器，必要时再沿着列表从上到下逐个尝试。

  - Host Address** - 指定一个 IP 地址或 FQDN 以包含在备用服务器列表中。如果客户端无法连接到主机，则它尝试连接到备用服务器。
  - Add** - 将主机地址添加到备用服务器列表。
  - Move Up** - 将选定的备用服务器在列表中向上移动。如果用户选择的服务器发生故障，则客户端首先尝试连接到此列表顶端的备用服务器，必要时再沿着列表从上到下逐个尝试。
  - Move Down** - 将选定的备用服务器在列表中向下移动。
  - Delete** - 从服务器列表中删除备用服务器。
- **Load Balancing Server List**

如果此服务器列表条目的主机是安全设备的负载均衡集群，且启用了 永远在线 功能，则在此列表中指定集群的备用设备。否则，永远在线 会阻止对负载均衡集群中备用设备的访问。

  - Host Address** - 指定负载均衡集群中备用设备的 IP 地址或 FQDN。



**Add** - 将地址添加到负载均衡备用服务器列表中。

**Delete** - 从列表中删除负载均衡备用服务器。

- **Primary Protocol** - 指定连接到此服务器所用的协议，即 SSL 或 IPsec（与 IKEv2 结合使用）。默认协议是 SSL。

**Standard Authentication Only (IOS Gateways)**- 当选择 IPsec 作为协议时，您可以选择此选项，将连接的身份验证方法限制为 IOS 服务器。



**注释** 如果此服务器是 ASA，则将身份验证方法从专有的 AnyConnect EAP 更改为基于标准的方法会禁用 ASA 的以下功能：配置会话超时、空闲超时、断开连接超时、拆分隧道、拆分 DNS、MSIE 代理配置及其他功能。

**Auth Method During IKE Negotiation** - 选择一种基于标准的身份验证方法。

**IKE Identity** - 如果选择基于标准的 EAP 身份验证方法，您可以在此字段中输入一个组或域作为客户端标识。客户端将字符串以 ID\_GROUP 型 IDi 负载形式发送。默认情况下，此字符串是 \*\$AnyConnectClient\$\*。

- **Automatic SCEP Host** - 此主机用于传统 SCEP。
- **CA URL** - 指定 SCEP CA 服务器的 URL。输入 FQDN 或 IP 地址。例如，<http://ca01.cisco.com>。
- **Prompt For Challenge PW** - 启用此项可让用户手动发出证书请求。当用户点击 Get Certificate 时，客户端将提示用户输入用户名和一次性密码。
- **CA Thumbprint** - CA 的证书拇指指纹。使用 SHA1 或 MD5 哈希值。



**注释** CA 服务器管理员可以提供 CA URL 和拇指指纹。拇指指纹应直接从服务器获取，而不是从它发布的证书的“fingerprint”或“thumbprint”属性字段中获取。

相关主题

[配置 VPN 连接服务器，第 89 页](#)

## AnyConnect 本地策略

AnyConnectLocalPolicy.xml 是包含安全设置的客户端上的 XML 文件。ASA 不部署该文件。您必须使用企业软件部署系统手动安装该文件或将其部署到用户计算机中。如果您对用户系统中的现有本地策略文件进行了更改，则系统将重启。

## 本地策略参数和值

以下参数是 VPN 本地策略编辑器中和 AnyConnectLocalPolicy.xml 文件中的元素。XML 元素显示在尖括号中。



**注释** 如果您手动编辑此文件并忽略策略参数，则该功能采取默认行为。

- **<acversion>**

指定能够解释该文件中所有参数的最低版本的 AnyConnect 客户端。如果客户端运行比此版本更早的 AnyConnect，则它读取文件时会发出事件日志警告。

格式是 acversion="<version number>"。

- **FIPS Mode <FipsMode>**

为客户端启用 FIPS 模式。此设置强制客户端仅使用 FIPS 标准批准的算法和协议。

- **Bypass Downloader <BypassDownloader>**

选择后，禁用 VPNDownloader.exe 模块启动，该模块负责检测本地版本动态内容的存在和更新。客户端不检查 ASA 上的动态内容，包括转换、定制、可选模块和核心软件更新。

选中 Bypass Downloader 时，在客户端连接到 ASA 时将发生两种情况之一：

如果 ASA 上的 VPN 客户端配置文件不同于客户端上的 VPN 客户端配置文件，则客户端将中止连接尝试。

如果 ASA 上没有 VPN 客户端配置文件，则客户端会建立 VPN 连接，但它使用其硬编码的 VPN 客户端配置文件设置。



**注释** 如果您在 ASA 上配置 VPN 客户端配置文件，则这些文件必须在客户端连接到 ASA 之前安装在客户端上（BypassDownloader 设置为 true）。因为配置文件可以包含管理员定义的策略，所以只在您不依赖于 ASA 来集中管理客户端配置文件时，才建议将 BypassDownloader 设置为 true。

- **Enable CRL Check<EnableCRLCheck>**

仅对 Windows 桌面实现此功能。对于 SSL 和 IPsec VPN 连接，可以选择执行证书吊销列表 (CRL) 检查。启用此设置后，AnyConnect 检索链中所有证书的已更新 CRL。然后，AnyConnect 验证有关证书是否包含在不应再信任的这些已吊销证书中；如果发现该证书已被证书颁发机构 (CA) 吊销，则不进行连接。

默认情况下会禁用 CRL 检查。仅当选中（或启用）Enable CRL Check 时，AnyConnect 才会执行 CRL 检查，因此，最终用户可能会观察到以下情况：

- 如果通过 CRL 吊销证书，即使在 AnyConnect 本地策略文件中禁用 Strict Certificate Trust，与安全网关的连接也会无条件失败。

- 如果无法检索 CRL（例如由于无法访问 CRL 分发点），并且在 AnyConnect 本地策略文件中启用 Strict Certificate Trust，与安全网关的连接也会无条件失败。否则，如果禁用 Strict Certificate Trust，则系统可能会提示该用户绕过此错误。



**注释** 启用 Always On 时，AnyConnect 无法执行 CRL 检查。此外，如果 CRL 分发点不是公开可访问，则 AnyConnect 可能会遇到服务中断。

- **Restrict Web Launch** <RestrictWebLaunch>

阻止用户使用不符合 FIPS 的浏览器来发起 WebLaunch。其实现途径是阻止客户端获取用于发起 AnyConnect 隧道的安全 Cookie。客户端向用户显示一条信息性消息。

- **Strict Certificate Trust** <StrictCertificateTrust>

如果选中此项，则在远程安全网关进行身份验证时，AnyConnect 不允许它无法验证的任何证书。客户端并不提示用户接受这些证书，而是无法使用自签证书连接到安全网关并显示 Local policy prohibits the acceptance of untrusted server certificates. A connection will not be established.。如果未选中，客户端将提示用户接受证书。这是默认行为。

我们强烈建议您为 AnyConnect 客户端启用 Strict Certificate Trust，原因如下：

- 随着有针对性攻击的日益增多，在本地策略中启用 Strict Certificate Trust 有助于在用户从不受信任网络（例如公共访问网络）连接时，防止受到“中间人”攻击。
- 即使您使用完全可验证且受信任的证书，默认情况下 AnyConnect 客户端也允许最终用户接受不可验证的证书。如果最终用户受到中间人攻击，他们可能会被提示接受恶意证书。要从最终用户删除此决定，请启用 Strict Certificate Trust。

- **限制首选项缓存** <RestrictPreferenceCaching>

根据设计，AnyConnect 不将敏感信息缓存到磁盘。启用此参数会将本策略扩展到在 AnyConnect 首选项中存储的任何类型的用户信息。

Credentials - 不缓存用户名和辅助用户名。

Thumbprints - 不缓存客户端和服务器的证书拇指指纹。

CredentialsAndThumbprints - 不缓存证书拇指指纹和用户名。

All - 不缓存任何自动首选项。

false - 所有首选项都写入磁盘（默认值）。

- **Exclude Pem File Cert Store (Linux and Mac)** <ExcludePemFileCertStore>

防止客户端使用 PEM 文件证书存储区来验证服务器证书和搜索客户端证书。

存储库使用支持 FIPS 的 OpenSSL，并具有关于在哪里可以获取客户端证书身份验证所需证书的信息。允许 PEM 文件证书存储区可确保远程用户使用符合 FIPS 的证书存储区。

- **Exclude Mac Native Cert Store (Mac only)** <ExcludeMacNativeCertStore>

防止客户端使用 Mac 本地 (keychain) 证书存储区验证服务器证书和搜索客户端证书。

- **Exclude Firefox NSS Cert Store** (Linux and Mac) <ExcludeFirefoxNSSCertStore>

防止客户端使用 Firefox NSS 证书存储区来验证服务器证书和搜索客户端证书。  
存储区有关于在何处为客户端证书身份验证取得证书的信息。

- **Update Policy** <UpdatePolicy>

控制客户端可以从哪些头端获取软件或配置文件更新。

- **Allow Software Updates From AnyServer** <AllowSoftwareUpdatesFromAnyServer>

允许或不允许 VPN 核心模块和其他可选模块的来自未授权服务器（未列在服务器名称列表中）的软件更新。

- **Allow VPN Profile Updates From AnyServer** <AllowVPNProfileUpdatesFromAnyServer>

允许或不允许来自未授权服务器（未列在服务器名称列表中）的 VPN 配置文件更新。

- **Allow Service Profile Updates From AnyServer** <AllowServiceProfileUpdatesFromAnyServer>

允许或不允许来自未授权服务器（未列在服务器名称列表中）的其他服务模块配置文件更新。

- **Allow ISE Posture Profile Updates From Any Server** <AllowISEProfileUpdatesFromAnyServer>

允许或不允许来自未授权服务器（未列在服务器名称列表中）的 ISE 终端安全评估配置文件更新。

- **Allow Compliance Module Updates From Any Server** <AllowComplianceModuleUpdatesFromAnyServer>

允许或不允许来自未授权服务器（未列在服务器名称列表中）的合规性模块更新。

- **Server Name** <ServerName>

在此列表中指定已授权服务器。允许这些头端在建立 VPN 连接后进行所有 AnyConnect 软件和配置文件的完全更新。服务器名称可以是 FQDN、IP 地址、域名或通配符加域名。

相关主题：[设置更新策略](#)

## 手动更改本地策略参数

### 过程

**步骤 1** 从客户端安装检索 AnyConnect 本地策略文件 (AnyConnectLocalPolicy.xml) 的副本。

表 7: 操作系统和 **AnyConnect** 本地策略文件安装路径

操作系统	安装路径
Windows	C:\ProgramData\Cisco\Cisco AnyConnect Secure Mobility Client

操作系统	安装路径
Linux	/opt/cisco/anyconnect
Mac OS X	/opt/cisco/anyconnect

- 步骤 2** 编辑参数设置。您可以手动编辑 AnyConnectLocalPolicy 文件，或使用随 AnyConnect 配置文件编辑器安装程序分发的 VPN 本地策略编辑器。
- 步骤 3** 将该文件另存为 AnyConnectLocalPolicy.xml，并使用公司软件部署系统将文件部署到远程计算机。
- 步骤 4** 重启远程计算机，以便使对本地策略文件的更改生效。

## 在 MST 文件中启用本地策略参数

有关说明和可以设置的值，请参阅[本地策略参数和值](#)。

创建 MST 文件以更改本地策略参数。MST 参数名称对应于 AnyConnect 本地策略文件 (AnyConnectLocalPolicy.xml) 中的参数：

- LOCAL\_POLICY\_BYPASS\_DOWNLOADER
- LOCAL\_POLICY\_FIPS\_MODE
- LOCAL\_POLICY\_RESTRICT\_PREFERENCE\_CACHING
- LOCAL\_POLICY\_RESTRICT\_TUNNEL\_PROTOCOLS
- LOCAL\_POLICY\_RESTRICT\_WEB\_LAUNCH
- LOCAL\_POLICY\_STRICT\_CERTIFICATE\_TRUST



**注释** AnyConnect 安装不会自动覆盖用户计算机上的现有本地策略文件。必须先删除用户计算机上的现有策略文件，以便客户端安装程序可以创建新的策略文件。



**注释** 对本地策略文件的任何更改都需要重新启动系统。

## 通过“启用 FIPS”工具启用本地策略参数

对于所有操作系统，都可以使用思科的“启用 FIPS”工具创建启用了 FIPS 的 AnyConnect 本地策略文件。“启用 FIPS”工具是一个命令行工具，在 Windows 上使用管理员权限运行，或在 Linux 和 Mac 上以 root 用户身份运行。

有关在何处下载“启用 FIPS”工具的信息，请参阅收到的 FIPS 客户端许可信息。

在计算机的命令行中输入命令 `EnableFIPS<参数>` 运行“启用 FIPS”工具。以下使用说明适用于“启用 FIPS”工具：

- 如果未提供任何参数，该工具将启用 FIPS 并重新启动 `vpnagent` 服务 (Windows) 或 `vpnagent` 后台守护程序 (Mac 和 Linux)。
- 使用空格分隔多个参数。

以下示例显示在 Windows 计算机上运行的“启用 FIPS”工具命令：

```
EnableFIPS rwl=false sct=true bd=true fm=false
```

下一个示例显示在 Linux 或 Mac 计算机上运行的命令：

```
./EnableFIPS rwl=false sct=true bd=true fm=false
```

下表显示可使用“启用 FIPS”工具配置的策略设置。参数与 AnyConnect 本地策略文件中的参数相匹配。

策略设置	参数和语法
FIPS 模式	<code>fm=[true   false]</code>
旁路下载程序	<code>bd=[true   false]</code>
限制 Web 启动	<code>rwl=[true   false]</code>
严格证书信任	<code>sct=[true   false]</code>
限制首选项缓存	<code>rpc=[Credentials   Thumbprints   CredentialsAndThumbprints   All   false]</code>
排除 Firefox NSS 证书存储区 (Linux 和 Mac)	<code>efn=[true   false]</code>
排除 PEM 文件证书存储区 (Linux 和 Mac)	<code>epf=[true   false]</code>
排除 Mac 本地证书存储区 (仅 Mac)	<code>emn=[true   false]</code>



# 第 4 章

## 配置 VPN 接入

---

- [连接和断开 VPN](#)，第 87 页
- [选择并排除 VPN 流量](#)，第 111 页
- [管理 VPN 身份验证](#)，第 114 页

## 连接和断开 VPN

### AnyConnect VPN 连接选项

AnyConnect 客户端为自动连接、自动重新连接或自动断开 VPN 会话提供多种选项。这些选项方便用户连接您的 VPN，它们还支持您的网络安全要求。

#### 启动和重新启动 AnyConnect 连接

[配置 VPN 连接服务器](#)，以为您的用户所要手动连接的安全网关提供名称和地址。

选择以下 AnyConnect 功能，以提供方便的自动 VPN 连接：

- [登录前自动启动 Windows VPN 连接](#)
- [AnyConnect 启动时自动启动 VPN 连接](#)
- [自动重新启动 VPN 连接](#)

此外，还应考虑使用以下自动 VPN 策略选项实施增强的网络安全或将网络访问仅限于 VPN：

- [关于值得信赖的网络检测](#)
- [需要使用永远在线的 VPN 连接](#)
- [使用强制网络门户热点检测和补救](#)

## 重新协商和维护 AnyConnect 连接

您可以限制 ASA 对用户保持 AnyConnect VPN 连接的时间长度（即便没有活动）。如果 VPN 会话进入空闲状态，您可以终止连接或重新协商连接。

- **Keepalive** - ASA 定期发送保持连接消息。这些消息会被 ASA 忽略，但对于维持客户端与 ASA 之间设备的连接很有用。

有关使用 ASDM 配置 Keepalive 的说明，请参阅使用 ASDM 的 *Cisco ASA 5500* 系列配置指南中的。

有关使用 CLI 配置 Keepalive 的说明，请参阅使用 CLI 的 *Cisco ASA 5500* 系列配置指南中的[启用保持连接](#)。

- **Dead Peer Detection** - ASA 和 AnyConnect 客户端发送“R-U-There”消息。这些消息的发送频率低于 IPsec 的保持连接消息。

如果客户端未响应 ASA 的 DPD 消息，ASA 将再重试三次才将会话置于“等待恢复”模式。此模式可使用户漫游网络，或进入睡眠模式，然后恢复连接。如果用户在默认空闲超时之前没有重新连接，ASA 将终止隧道。建议的网关 DPD 间隔是 300 秒。

如果 ASA 不响应客户端的 DPD 消息，客户端将再尝试三次才终止隧道。建议的客户端 DPD 间隔是 30 秒。

您可以同时启用 ASA（网关）和客户端来发送 DPD 消息，并配置超时间隔。有关使用 ASDM 配置 DPD 的说明，请参阅 *Cisco ASA* 系列 *VPN ASDM* 配置指南中的。有关使用 CLI 配置 DPD 的说明，请参阅 *Cisco ASA* 系列 *VPN CLI* 配置指南中的[启用和调整失效对等项检测](#)。

- **最佳实践：**

将客户端 DPD 设置为 30 秒 (Group Policy > Advanced > AnyConnect Client > Dead Peer Detection)。

将服务器 DPD 设置为 300 秒 (Group Policy > Advanced > AnyConnect Client > Dead Peer Detection)。

将 SSL 和 IPsec 的密钥重新生成均设置为 1 小时 (Group Policy > Advanced > AnyConnect Client > Key Regeneration)。

## 终止 AnyConnect 连接

终止 AnyConnect 连接要求用户在安全网关上对其终端设备重新进行身份验证，并创建新的 VPN 连接。

以下配置参数基于简单的超时终止 VPN 会话：

- **Default Idle Timeout** - 当会话处于非活动状态达到指定的时间时，终止任何用户会话。默认值为 30 分钟。

您只能使用 CLI 在 webvpn 配置模式下修改 default-idle-timeout。默认值为 1800 秒。



- **VPN Idle Timeout** - 当会话处于非活动状态达到指定的时间时，终止任何用户会话。仅限 SSL VPN，如果未配置 `vpn-idle-timeout`，则使用 `default-idle-timeout`。

有关使用 ASDM 配置 VPN 空闲超时的说明，请参阅使用 ASDM 的 *Cisco ASA 5500* 系列配置指南中的。

有关使用 CLI 配置 VPN 空闲超时的说明，请参阅使用 CLI 的 *Cisco ASA 5500* 系列配置指南中的。

## 配置 VPN 连接服务器

AnyConnect VPN 服务器列表包含主机名和主机地址对，它们标识 VPN 用户将连接到的安全网关。主机名可以是别名、FQDN 或 IP 地址。

添加到服务器列表的主机显示在 AnyConnect GUI 的 **Connect to** 下拉列表中。然后，用户可以从下拉列表中进行选择以发起 VPN 连接。列表顶部的主机是默认服务器，在 GUI 下拉列表中首先出现。如果用户从列表中选择备用服务器，则所选服务器成为新的默认服务器。

一旦您将服务器添加到服务器列表，就可以查看其详细信息以及编辑或删除服务器条目。要将服务器添加到服务器列表，请遵循此过程。

### 过程

- 步骤 1** 打开 VPN 配置文件编辑器，从导航窗格中选择 **Server List**。
- 步骤 2** 点击 **Add**。
- 步骤 3** 配置服务器的主机名和地址：
  - 输入 **Host Display Name**、用于指代主机的别名、FQDN 或 IP 地址。请勿在名称中使用 “&” 或 “<” 字符。如果您输入 FQDN 或 IP 地址，则无需在下一步骤中输入 **FQDN** 或 **IP Address**。如果输入 IP 地址，请使用安全网关的公共 IPv4 地址或全局 IPv6 地址。不支持使用链路本地安全网关地址。
  - （可选）输入主机的 **FQDN** 或 **IP Address**（如果在 Host Display Name 中没有输入）。
  - （可选）指定 **User Group**。  
AnyConnect 使用 FQDN 或 IP 地址以及用户组来构成组 URL。
- 步骤 4** （可选）将备用服务器添加到 **Backup Server List**。请勿在名称中使用 “&” 或 “<” 字符。如果您配置的服务器不可用，则客户端尝试连接到此备用服务器列表中的服务器，然后才尝试使用全局备用服务器列表。
- 步骤 5** （可选）将负载均衡服务器添加到 **Load Balancing Server List**。请勿在名称中使用 “&” 或 “<” 字符。如果此服务器列表条目的主机指定安全设备的负载均衡集群，且启用了永远在线功能，请将集群中的负载均衡设备添加到此列表中。否则，永远在线将阻止访问负载均衡集群中的设备。
- 步骤 6** 为客户端指定 **Primary Protocol** 以用于此 ASA：
  - 选择 SSL（默认值）或 IPsec。

如果您指定 IPsec，则用户组必须是连接配置文件（隧道组）的准确名称。对于 SSL，用户组是连接配置文件的组 URL 或组别名。

- b) 如果您指定 IPsec，请选择 **Standard Authentication Only** 以禁用默认身份验证方法（专有 AnyConnect EAP），然后从下拉列表中选择一种方法。

**注释** 将身份验证方法从专有的 AnyConnect EAP 更改为基于标准的方法会禁用 ASA 配置会话超时、空闲超时、连接断开超时、分割隧道、分离 DNS、MSIE 代理配置及其他功能的能力。

**步骤 7** （可选）为此服务器配置 SCEP：

- a) 指定 SCEP CA 服务器的 URL。输入 FQDN 或 IP 地址。例如，<http://ca01.cisco.com>。
- b) 选中 **Prompt For Challenge PW** 以让用户手动发出证书请求。当用户点击 **Get Certificate** 时，客户端将提示用户输入用户名和一次性密码。
- c) 输入 CA 的证书拇指指纹。使用 SHA1 或 MD5 哈希值。您的 CA 服务器管理员可以提供 CA URL 和拇指指纹，且应该直接从服务器（而不是发布证书的“fingerprint”或“thumbprint”属性字段）检索拇指指纹。

**步骤 8** 点击 **OK**。

#### 相关主题

[AnyConnect 配置文件编辑器，服务器列表，第 79 页](#)

[AnyConnect 配置文件编辑器，添加/编辑服务器列表，第 80 页](#)

## 登录前自动启动 Windows VPN 连接

### 关于“登录前启动”

“登录前启动”（SBL）这一功能允许用户在登录 Windows 之前建立与企业基础设施的 VPN 连接。

SBL 安装并启用时，AnyConnect 在 Windows 登录对话框出现之前启动，确保用户在登录前连接到其公司基础设施。在 VPN 身份验证后，会显示 Windows 登录对话框，且用户可正常登录。

SBL 还包括网络访问管理器图块，允许使用用户配置的家庭网络配置文件进行连接。SBL 模式中允许的网络配置文件包括使用非 802-1X 身份验证模式的所有媒体类型。

SBL 仅在 Windows 系统中可用，并使用取决于 Windows 版本的不同机制来实施：

- 在 Windows 中，登录前访问提供商 (PLAP) 用于实施 AnyConnect SBL。

使用 PLAP 时，按 Ctrl+Alt+Del 组合键后打开一个窗口，在这个窗口中用户可以选择登录到系统或使用窗口右下角的 Network Connect 按钮激活“网络连接”（PLAP 组件）。

PLAP 支持 Windows 的 32 位和 64 位版本。

您应该考虑为用户启用 SBL 的原因包括：

- 用户的计算机加入 Active Directory 基础设施。

- 用户拥有要求使用 Microsoft Active Directory 基础设施进行身份验证的网络映射驱动器。
- 用户无法在计算机上缓存凭证（组策略禁止缓存凭证）。在这种情况下，用户必须能够与公司网络中的域控制器通信，以便在获得计算机访问权限之前对其凭证进行验证。
- 用户必须运行从网络资源执行的登录脚本或需要访问网络资源。SBL 处于启用状态时，用户可访问本地基础设施和用户办公室时通常会运行的登录脚本。这包括域登录脚本、组策略对象和用户登录其系统时通常发生的其他 Active Directory 功能。
- 存在可能需要连接到基础设施的网络组件（例如 MS NAP/CS NAC）。

## “登录前启动”的限制

- AnyConnect 不与快速用户切换兼容。
- AnyConnect 无法由第三方登录前启动应用启动。

## 配置“登录前启动”

### 过程

- 步骤 1** 安装 AnyConnect “登录前启动”模块。
- 步骤 2** 在 AnyConnect 配置文件中启用 SBL。

## 安装 AnyConnect “登录前启动”模块

AnyConnect 安装程序会检测基础操作系统，并将来自 AnyConnect SBL 模块的适当 AnyConnect DLL 置于系统目录中。在 Windows 7 或 Windows 2008 服务器上，安装程序会确定正在使用的是 32 位还是 64 位版本的操作系统，并安装适当的 PLAP 组件，即 vpnplap.dll 或 vpnplap64.dll。



### 注释

如果在保留已安装的 VPNGINA 或 PLAP 组件的情况下卸载 AnyConnect，VPNGINA 或 PLAP 组件会禁用且远程用户看不见它们。

您可以预部署 SBL 模块或配置 ASA 以下载 SBL 模块。预部署 AnyConnect 时，“登录前启动”模块要求先安装核心客户端软件。如果使用 MSI 文件预部署 AnyConnect 核心和“登录前启动”组件，则必须按照正确的顺序进行操作。

## 过程

---

- 步骤 1 在 ASDM 中，转到 **Configuration > Remote Access VPN > Network (Client) Access > Group Policies**。
  - 步骤 2 选择组策略，点击 **Edit** 或 **Add** 可编辑或新增组策略。
  - 步骤 3 在左侧导航窗格中选择 **Advanced > AnyConnect Client**。
  - 步骤 4 对 **Optional Client Module for Download** 设置取消选中 **Inherit**。
  - 步骤 5 在下拉列表中选择 **AnyConnect SBL** 模块。
- 

## 在 AnyConnect 配置文件中启用 SBL

### 开始之前

- 在调用 SBL 时需要存在网络连接。但在有些情况下，网络连接可能无法实现，因为无线连接可能依靠用户凭证才能连接到无线基础设施。由于 SBL 模式先于登录的凭证阶段存在，因此此情况下连接不可用。此时，无线连接需要配置为在登录过程中缓存凭证，或者需要配置其他无线身份验证，SBL 才可正常运行。
- 如果安装了网络访问管理器，必须部署计算机连接才能确保适当的连接可用。

## 过程

---

- 步骤 1 打开 VPN 配置文件编辑器，从导航窗格中选择 **Preferences (Part 1)**。
  - 步骤 2 选择 **Use Start Before Logon**。
  - 步骤 3 （可选）要允许远程用户控制 SBL，请选择 **User Controllable**。
- 注释 在 SBL 生效之前，用户必须重新启动远程计算机。
-

## “登录前启动”故障排除

### 过程

- 步骤 1 确保 AnyConnect 配置文件已加载到 ASA 上，随时可部署。
- 步骤 2 删除之前的配置文件（在硬盘驱动器上搜索这些文件以找到位置，\*.xml）。
- 步骤 3 使用 Windows Add/Remove Programs 卸载 SBL 组件。重新启动计算机并重新测试。
- 步骤 4 在事件查看器中清除用户的 AnyConnect 日志并重新测试。
- 步骤 5 浏览回安全设备以再次安装 AnyConnect。
- 步骤 6 重新启动一次。下次重新启动时，您应看到 Start Before Logon 提示。
- 步骤 7 收集 DART 捆绑包并将其发送给 AnyConnect 管理员。
- 步骤 8 如果看到以下错误，请删除用户的 AnyConnect 配置文件：

```
Description: Unable to parse the profile C:\Documents and Settings\All Users\Application Data
\Cisco\Cisco AnyConnect Secure Mobility Client\Profile\VABaseProfile.xml. Host data not
available.
```

- 步骤 9 返回 .tmp1 文件，将副本另存为 .xml 文件，并将该 XML 文件用作默认配置文件。

## AnyConnect 启动时自动启动 VPN 连接

此功能称为 Auto Connect On Start，它在 AnyConnect 启动时自动与 VPN 客户端配置文件指定的安全网关建立 VPN 连接。

Auto Connect On Start 默认禁用，需要用户指定或选择安全网关。

### 过程

- 步骤 1 打开 VPN 配置文件编辑器，从导航窗格中选择 **Preferences (Part 1)**。
- 步骤 2 选择 **Auto Connect On Start**。
- 步骤 3 （可选）要让用户控制 Auto Connect On Start，请选择 **User Controllable**。

## 在 Windows 系统上配置登录前启动 (PLAP)

登录前启动 (SBL) 功能在用户登录到 Windows 之前启动一个 VPN 连接。这将确保用户在登录到计算机之前连接其公司基础设施。

SBL AnyConnect 功能称为登录前接入提供商 (PLAP)，它是一个可连接的凭证提供商。此功能可让编程网络管理员在登录前执行特定的任务，如收集凭证或连接到网络资源。PLAP 在所有受支持的 Windows 操作系统上提供 SBL 功能。PLAP 分别以 vpnplap.dll 和 vpnplap64.dll 支持 32 位和 64 位版本的操作系统。PLAP 功能支持 x86 和 x64。

## 安装 PLAP

vpnplap.dll 和 vpnplap64.dll 组件是现有安装的一部分，因此您可以在安全设备上加载一个附加 SBL 软件包，然后，该软件包将为目标平台安装适当的组件。PLAP 是一项可选功能。安装程序软件检测底层操作系统，并将适当的 DLL 放入系统目录中。在 Windows 7 或更高版本或者 Windows 2008 服务器中，安装程序会确定 32 位或 64 位版操作系统是否在使用中，以及是否安装了适当的 PLAP 组件。



**注释** 如果在保留已安装的 PLAP 组件的情况下卸载 AnyConnect，PLAP 组件会禁用且远程用户看不见该组件。

安装后，在您修改用户配置文件 <profile.xml> 以激活 SBL 之前，PLAP 处于不活动状态。请参阅在 [AnyConnect 配置文件中启用 SBL](#)，第 92 页。激活后，用户通过点击 Switch User 调用网络连接组件，然后，屏幕右下部分会显示 Network Connect 图标。



**注释** 如果用户误将用户界面最小化，用户可以通过按下 **Alt+Tab** 组合键还原界面。

## 使用 PLAP 登录至 Windows PC

### 过程

- 步骤 1** 用户在 Windows 启动窗口按下 **Ctrl+Alt+Del** 组合键。系统显示登录窗口，其中包含 Switch User 按钮。
- 步骤 2** 用户点击 **Switch User**。系统显示 Network Connect 窗口。如果用户已通过 AnyConnect 连接建立其连接并点击了 **Switch User**，该 VPN 连接将保持。如果用户点击 **Network Connect**，原来的 VPN 连接将终止。如果用户点击 **Cancel**，VPN 连接将终止。
- 步骤 3** 用户点击窗口右下角的 **Network Connect** 按钮可启动 AnyConnect。系统打开 AnyConnect 登录窗口。
- 步骤 4** 用户可以使用此 GUI 照常登录。  
此示例假设 AnyConnect 是唯一安装的连接提供商。如果安装了多个提供商，用户必须从此窗口中显示的项目中选择一个供应商进行使用。
- 步骤 5** 当用户连接时，用户将看到一个类似于 Network Connect 窗口的屏幕，但该屏幕的右下角有一个 Microsoft Disconnect 按钮。连接成功只能由该按钮表示。
- 步骤 6** 用户点击与其登录相关的图标。

建立连接后，即有几分钟时间可以进行登录。在经过大约两分钟的空闲超时后，用户登录会话将会超时，并向 AnyConnect PLAP 组件发出表明断开连接的消息，使 VPN 隧道断开连接。

## 使用 PLAP 从 AnyConnect 断开连接

成功建立 VPN 会话后，PLAP 组件会返回原窗口，此时窗口的右下角会显示一个 Disconnect 按钮。当用户点击 **Disconnect** 时，VPN 隧道将断开连接。

除了在响应 **Disconnect** 按钮时显式断开连接外，隧道还在以下情况下断开连接：

- 当用户使用 PLAP 登录 PC 但接着按下 **Cancel** 时。
- 当 PC 在用户登录到系统之前关机时。
- 当 Windows 上的用户登录会话超时，系统返回到“Press CTRL + ALT + DEL to log on”屏幕时。

此行为是 Windows PLAP 架构的功能，而不是 AnyConnect 的功能。

## 自动重新启动 VPN 连接

启用 Auto Reconnect（默认值）时，AnyConnect 将从 VPN 会话中断中恢复并重新建立会话，而不管初始连接使用哪种介质。例如，它可以重新建立有线、无线或 3G 会话。启用 Auto Reconnect 后，您还可以指定系统暂停或系统恢复后的重新连接行为。系统暂停是低功耗待机状态，如 Windows 的“休眠”或者 Mac OS 或 Linux 的“睡眠”。系统恢复是系统暂停后的恢复。

如果禁用 Auto Reconnect，无论连接出于何种原因断开，客户端都不会尝试重新连接。思科强烈建议对此功能使用默认设置（启用）。禁用此设置可能导致连接不稳定时 VPN 连接中断。

### 过程

**步骤 1** 打开 VPN 配置文件编辑器，从导航窗格中选择 **Preferences (Part 1)**。

**步骤 2** 选择 **Auto Reconnect**。

**步骤 3** 选择 Auto Reconnect Behavior:

- **Disconnect On Suspend** -（默认值）AnyConnect 在系统暂停时释放分配给 VPN 会话的资源，并且在系统恢复后不尝试重新连接。
- **Reconnect After Resume** - 客户端在系统暂停期间保留分配给 VPN 会话的资源，并且在系统恢复后尝试重新连接。

## 使用值得信赖的网络检测来连接和断开连接

### 关于值得信赖的网络检测

值得信赖的网络检测 (TND) 可让您在用户处于公司网络（值得信赖的网络）内时让 AnyConnect 自动断开 VPN 连接，并在用户处于公司网络（不值得信赖的网络）之外时启动 VPN 连接。

TND 不会影响用户手动建立 VPN 连接的能力。它不会断开用户在值得信赖的网络中手动启动的 VPN 连接。如果用户先在不值得信赖的网络中，然后进入值得信赖的网络，TND 只断开 VPN 会话的连接。举例来说，如果用户在家建立 VPN 连接，然后移动到公司办公室，则 TND 会断开 VPN 会话的连接。



注释

有关网络安全模块的同等功能，请参阅配置网络安全一章中的[使用安全值得信赖的网络检测](#)。

您可以在 AnyConnect VPN 客户端配置文件中配置 TND。不需要更改 ASA 配置。您需要指定 AnyConnect 识别出正在值得信赖的网络和不值得信赖的网络之间过渡时应采取的措施或策略，并确定值得信赖的网络和服务器。

### 值得信赖的网络检测指南

- 因为 TND 功能控制 AnyConnect GUI 并自动启动连接，所以 GUI 应该始终运行。如果用户退出 GUI，则 TND 不会自动启动 VPN 连接。
- 如果 AnyConnect 也在运行“登录前启动”，且用户进入受信任网络，则计算机上显示的 SBL 窗口将自动关闭。
- 无论是否配置了永远在线，在通过 IPv4 和 IPv6 网络到 ASA 的 IPv6 和 IPv4 VPN 连接上都支持值得信赖的网络检测。
- 如果 TND 配置不同，在用户计算机上的多个配置文件可能会出现冲突。

如果用户收到过已启用 TND 的配置文件，则系统重新启动时，AnyConnect 会尝试连接它最后一次连接到的安全设备，而这可能不是您希望的行为。要连接到其他安全设备，用户必须手动断开连接并重新连接到该头端。以下解决方法将帮助您避免发生此问题：

在已加载到您企业网络中所有 ASA 上的客户端配置文件中启用 TND。

创建一个配置文件（在其主机条目中列出所有 ASA），并将该配置文件加载到所有 ASA 上。

如果用户不需要多个不同的配置文件，请为所有 ASA 上的配置文件使用相同的配置文件名称。每个 ASA 都会覆盖现有配置文件。



## 配置值得信赖的网络检测

### 过程

**步骤 1** 打开 VPN 配置文件编辑器，从导航窗格中选择 **Preferences (Part 1)**。

**步骤 2** 选择 **Automatic VPN Policy**。

**步骤 3** 在 **Trusted Network Policy** 中选择一个受信任网络策略。  
这是用户处于公司网络（受信任网络）中时客户端执行的操作。选项有：

- **Disconnect** - （默认值）客户端终止受信任网络中的 VPN 连接。
- **Connect** - 客户端启动受信任网络中的 VPN 连接。
- **Do Nothing** - 客户端不在受信任网络中执行任何操作。将 **Trusted Network Policy** 和 **Untrusted Network Policy** 都设置为 **Do Nothing**，会禁用 **Trusted Network Detection (TND)**。
- **Pause** - 如果用户在受信任网络外建立 VPN 会话之后进入被配置为受信任的网络，则 **AnyConnect** 会暂停此 VPN 会话而不是将其断开连接。当用户再次离开受信任网络时，**AnyConnect** 会恢复该会话。此功能是为了给用户方便，因为有了它，在用户离开受信任网络后不需要建立新的 VPN 会话。

**步骤 4** 在 **Untrusted Network Policy** 中选择一个不受信任的网络策略。

这是用户在公司网络之外时客户端执行的操作。选项有：

- **Connect** - 客户端在检测到不受信任网络后启动 VPN 连接。
- **Do Nothing** - 客户端在检测到不受信任网络后不执行任何操作。此选项禁用 **永远在线 VPN**。将 **Trusted Network Policy** 和 **Untrusted Network Policy** 都设置为 **Do Nothing** 会禁用 **Trusted Network Detection**。

**步骤 5** 指定 **Trusted DNS Domains**。

指定客户端在信任网络中时网络接口可能具有的 DNS 后缀（逗号分隔的字符串）。如果您将多个 DNS 后缀添加到 **split-dns** 列表并在 ASA 上指定一个默认域，则可以分配多个 DNS 后缀。

**AnyConnect** 客户端按以下顺序构建 DNS 后缀列表：

- 头端传输的域。
- 头端传输的拆分 DNS 后缀列表。
- 公共接口的 DNS 后缀（如果已配置）。否则，是主后缀和连接特定后缀，以及主 DNS 后缀的父后缀（如果在 **Advanced TCP/IP Settings** 中选中了相应的复选框）。

要匹配此 DNS 后缀，请执行以下操作：	将此值用于 <b>TrustedDNSDomains</b> ：
example.com（仅限）	*example.com

要匹配此 DNS 后缀，请执行以下操作：	将此值用于 TrustedDNSDomains：
example.com AND anyconnect.cisco.com	*.example.com OR example.com, anyconnect.example.com
asa.example.com AND example.cisco.com	*.example.com OR asa.example.com, anyconnect.example.com

通配符 (\*) 可用于 DNS 后缀。

#### 步骤 6 在 Trusted DNS Servers 中指定受信任的 DNS 服务器。

客户端在受信任网络中时网络接口可能具有的所有 DNS 服务器地址（逗号分隔的字符串）。例如：203.0.113.1,2001:DB8::1。通配符 (\*) 不可用于 DNS 服务器地址。

您必须具有通过 DNS 可解析的头端服务器的 DNS 条目。如果按 IP 地址连接，则需要可以解析 mus.cisco.com 的 DNS 服务器。如果通过 DNS 无法解析 mus.cisco.com，则强制网络门户检测不会按预期工作。

**注释** 您可以配置 TrustedDNSDomains 和/或 TrustedDNSServers。如果配置 TrustedDNSServers，请确保输入所有 DNS 服务器，这样您的站点会成为受信任网络的一部分。

如果某个活动接口匹配 VPN 配置文件中的所有规则，则将其视为在受信任网络中。

## 需要使用 永远在线 的 VPN 连接

### 关于 永远在线 VPN

除非 VPN 会话处于活动状态，否则计算机不在受信任网络中时，永远在线 操作将阻止对互联网资源的访问。在此情况下，始终将 VPN 设置为开启可保护计算机免受安全威胁。

启用了 永远在线 时，它在用户登录并检测到不受信任网络后自动建立 VPN 会话。VPN 会话保持打开状态，直到用户从计算机中注销，或者会话计时器或空闲会话计时器（在 ASA 组策略中指定）到期为止。AnyConnect 连续尝试重新建立连接以重新激活会话（如果它仍然打开）；否则，它连续尝试建立新 VPN 会话。

在 VPN 配置文件中启用了 永远在线 时，AnyConnect 可通过删除其他所有下载的 AnyConnect 配置文件并忽略配置为连接到 ASA 的所有公共代理来保护终端。

启用 永远在线 时，还需要考虑以下 AnyConnect 选项：

- 允许用户将 永远在线 VPN 会话断开连接：AnyConnect 使用户可以将 永远在线 VPN 会话断开连接。如果启用 **Allow VPN Disconnect**，则 AnyConnect 在建立 VPN 会话时会显示 Disconnect 按钮。默认情况下，启用了 永远在线 VPN 时，配置文件编辑器启用 Disconnect 按钮。

按 **Disconnect** 按钮将锁定所有接口以防止数据泄漏以及保护计算机免受互联网访问（除非为了建立 VPN 会话）。永远在线 VPN 会话的用户可能希望点击 **Disconnect**，这样，在当前 VPN 会话出现性能问题或 VPN 会话中断后的重新连接问题时，他们可以选择备用安全网关。

- 设置连接失败策略：如果永远在线 VPN 已启用且 AnyConnect 无法建立 VPN 会话，则连接失败策略确定计算机是否可以访问互联网。请参阅[设置连接失败策略](#)。
- 处理强制网络门户热点：请参阅[使用强制网络门户热点检测和补救](#)。

## 永远在线 VPN 的限制

- 如果启用了永远在线，但用户没有登录，则 AnyConnect 不建立 VPN 连接。AnyConnect 仅在登录后启动 VPN 连接。
- 永远在线 VPN 不支持通过代理进行连接。

## 永远在线 VPN 指南

为增强威胁防范，如果您配置了永远在线 VPN，我们建议采取以下额外保护措施：

- 我们强烈建议从证书颁发机构(CA)购买数字证书并在安全网关上注册。ASDM 在 **Configuration > Remote Access VPN > Certificate Management > Identity Certificates** 面板上提供一个 **Enroll ASA SSL VPN with Entrust** 按钮，以方便公共证书注册。
- 向终端预部署一个配置有永远在线的配置文件，以限制只能连接到预定义的 ASA。预部署可以防止与欺诈服务器联系。
- 限制管理员权限，以使用户无法终止进程。具有管理权限的 PC 用户可以通过停止代理而忽略永远在线策略。如果想要确保永远在线绝对安全，您必须拒绝给用户分配本地管理权限。
- 限制对 Windows 计算机上思科子文件夹的访问，通常是 C:\ProgramData。
- 具有有限或标准权限的用户有时可能对其程序数据文件夹具有写访问权限。他们可以利用这种访问权限删除 AnyConnect 配置文件，从而避开永远在线功能。
- 为 Windows 用户预部署一个组策略对象(GPO)，以防止具有有限权限的用户终止 GUI。为 Mac OS 用户预部署相应的措施。

## 配置 永远在线 VPN

### 过程

- 
- 步骤 1** 在 [AnyConnect VPN 客户端配置文件中配置永远在线](#)。
  - 步骤 2** （可选）向服务器列表添加负载均衡备用集群成员。
  - 步骤 3** （可选）豁免来自永远在线 VPN 的用户。
-

## 在 AnyConnect VPN 客户端配置文件中配置永远在线

### 开始之前

永远在线 VPN 要求在 ASA 上配置有效、受信任的服务器证书；否则它将失败，并记录表示证书无效的事件。此外，确保服务器证书能通过严格的证书信任模式，可防止永远在线 VPN 配置文件的下载锁定与欺诈服务器的 VPN 连接。

### 过程

- 
- 步骤 1** 打开 VPN 配置文件编辑器，从导航窗格中选择 **Preferences (Part 2)**。
  - 步骤 2** 选择 **Automatic VPN Policy**。
  - 步骤 3** [配置值得信赖的网络检测](#)。
  - 步骤 4** 选择 **Always On**。
  - 步骤 5** （可选）选择或取消选择 **Allow VPN Disconnect**。
  - 步骤 6** （可选）[配置连接失败策略](#)。
  - 步骤 7** （可选）[配置强制网络门户补救](#)。
- 

## 向服务器列表添加负载均衡备用集群成员

永远在线 VPN 会影响 AnyConnect VPN 会话的负载均衡。在永远在线 VPN 禁用后，当客户端连接到负载均衡集群中的主设备时，客户端遵守从主设备到任何备用集群成员的重定向。在永远在线启用后，除非在客户端配置文件的服务器列表中指定备用集群成员的地址，否则客户端不遵守从主设备重定向。因此，请确保向服务器列表中添加任何备份集群成员。

要在客户端配置文件中指定备用集群成员的地址，请按以下步骤使用 ASDM 添加负载均衡备用服务器列表：

### 过程

- 
- 步骤 1** 打开 VPN 配置文件编辑器，从导航窗格中选择 **Server List**。
  - 步骤 2** 选择作为负载均衡集群主设备的服务器，然后点击 **Edit**。
  - 步骤 3** 输入任何负载均衡集群成员的 FQDN 或 IP 地址。
-

## 豁免来自 永远在线 VPN 的用户

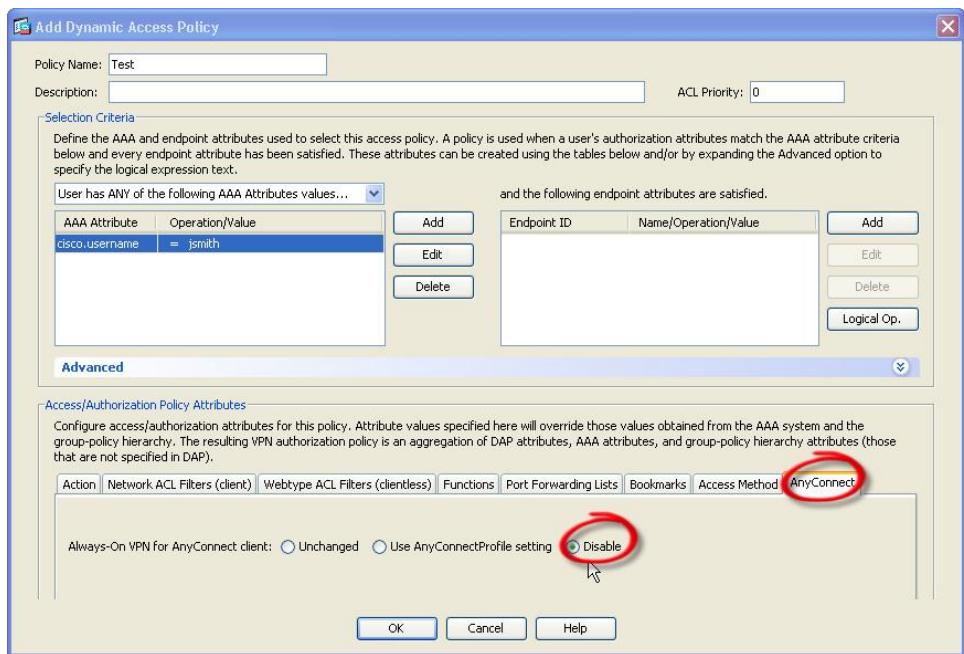
可以配置豁免以覆盖 永远在线 策略。例如，您可能要让某些个人建立与其他公司的 VPN 会话，或者豁免用于非公司资产的 永远在线 策略。

在 ASA 的组策略和动态访问策略中设置的豁免可覆盖 永远在线 策略。根据用于分配策略的匹配条件指定例外情况。如果 AnyConnect 策略启用 永远在线，而动态访问策略或组策略禁用它，则只要客户端的条件与建立每个新会话时的动态访问策略或组策略相符，客户端就会对当前和将来的 VPN 会话保留禁用设置。

此过程配置使用 AAA 终端条件的动态访问策略以将会话匹配至非公司资产。

### 过程

- 步骤 1 选择 **Configuration > Remote Access VPN > Network (Client) Access > Dynamic Access Policies > Add** 或 **Edit**。
- 步骤 2 配置条件以豁免来自 永远在线 VPN 的用户。例如，使用 Selection Criteria 区域指定匹配用户登录 ID 的 AAA 属性。
- 步骤 3 点击 Add or Edit Dynamic Access Policy 窗口下半部分的 **AnyConnect** 选项卡。



- 步骤 4 点击“永远在线 VPN for AnyConnect client”旁边的 **Disable**。

## 为永远在线设置连接失败策略

### 关于连接失败策略

如果 永远在线 VPN 已启用且 AnyConnect 无法建立 VPN 会话，连接失败策略会确定计算机是否可以访问互联网。当安全网关无法访问，或者 AnyConnect 无法检测到强制网络门户热点的存在时，就会出现这种情况。

开放策略允许完全网络访问，从而使用户可在需要访问互联网或其他本地网络资源时继续执行任务。

封闭策略在 VPN 会话建立前禁用所有网络连接。为此，AnyConnect 启用阻止来自终端（对于允许计算机连接的安全网关不受限制）的所有流量的数据包过滤器。

尽管采用了连接失败策略，AnyConnect 仍会继续尝试建立 VPN 连接。

### 设置连接失败策略指南

使用允许完全网络访问的开放策略时，请考虑以下内容：

- 直到建立 VPN 会话之后，安全和保护才可用；因此，终端设备可能会受到基于 Web 的恶意软件感染或者泄漏敏感数据。
- 如果启用了 Disconnect 按钮且用户点击 **Disconnect**，则打开连接失败策略不适用。

使用在建立 VPN 会话之前一直禁用所有网络连接的关闭策略时，请考虑以下内容：

- 如果用户需要 VPN 之外的互联网访问，则关闭策略会停止工作。
- 关闭策略旨在当保护终端的专用网络中的资源不可用时帮助保护企业资产免受网络威胁。终端始终受到保护以免遭基于 Web 的恶意软件攻击和防止敏感数据泄漏，因为除拆分隧道允许的本地资源（如打印机和外围设备）之外，所有网络访问都被阻止。
- 此选项主要用在网络访问的安全持久性比始终可用性更重要的企业中。
- 关闭策略会阻止强制网络门户补救，除非您专门启用它。
- 如果客户端配置文件中启用了 **Apply Last VPN Local Resources**，则您可以允许应用最新 VPN 会话实施的本地资源规则。例如，这些规则可以确定对活动同步和本地打印的访问权限。
- 若不顾关闭策略而启用了 永远在线，则在 AnyConnect 软件升级期间，网络是畅通且开放的。
- 如果您部署关闭连接策略，我们强烈建议您采用分阶段方法。例如，首先利用连接失败打开策略部署 永远在线，并向用户调查 AnyConnect 不能无缝连接的频率。然后，在早期采用者用户中部署连接失败关闭策略的一个小型试点部署，并征求他们的反馈。逐步扩展试点计划，同时继续征求反馈，再考虑全面部署。部署连接失败关闭策略时，请确保向 VPN 用户告知网络访问限制以及连接失败关闭策略的优点。



注意

如果 AnyConnect 未能建立 VPN 会话，连接故障关闭策略会阻止网络访问。实施连接故障关闭策略时要极度小心谨慎。

### 配置连接失败策略

仅在 永远在线 功能启用时才配置连接失败策略。默认情况下，连接失败策略是关闭的，以防止在无法访问 VPN 时访问互联网。要允许在此情况下访问互联网，必须将连接失败策略设置为开放。

### 过程

**步骤 1** 打开 VPN 配置文件编辑器，从导航窗格中选择 **Preferences (Part 2)**。

**步骤 2** 将 **Connect Failure Policy** 参数设置为以下设置之一：

- **Closed-**（默认值）当无法连接到安全网关时限制网络访问。
- **Open** - 当客户端无法连接到安全网关时，允许通过浏览器和其他应用访问网络。

**步骤 3** 如果您指定了关闭策略，请执行以下操作：

- a) [配置强制网络门户补救](#)。
- b) 如果要在禁用网络访问时保留最后一个 VPN 会话的本地设备规则，请选择 **Apply Last VPN Local Resources**。

## 使用强制网络门户热点检测和补救

### 关于强制网络门户

许多设施（例如，机场、咖啡店和酒店）提供 Wi-Fi 和有线访问，但可能要求用户在获得访问权之前先付款和/或同意遵守可接受的使用政策。这些设施使用称为强制网络门户的技术来防止应用连接，直到用户打开浏览器并接受访问条件为止。强制网络门户检测用于识别此限制，而强制网络门户补救是满足强制网络门户热点的要求以获取网络访问权限的过程。

在启动无需额外配置的 VPN 连接时，由 AnyConnect 自动检测强制网络门户。此外，AnyConnect 在强制网络门户检测期间不会修改任何浏览器配置设置，且不会自动补救强制网络门户。它依靠最终用户来执行补救。AnyConnect 根据当前配置对强制网络门户检测进行响应：

- 如果 永远在线 已禁用，或者 永远在线 已启用且连接失败策略处于打开状态，则在每个连接尝试时显示以下消息：

The service provider in your current location is restricting access to the Internet. You need to log on with the service provider before you can establish a VPN session. You can try this by visiting any website with your browser.

最终用户必须通过满足热点提供商的要求来执行强制网络门户补救。这些要求可以是付费接入网络、签署可接受使用策略、此两者或提供商规定的一些其他要求。

- 如果永远在线已启用并且连接失败策略关闭，需要明确启用强制网络门户补救。如果已启用，最终用户可以如上文所述执行补救。如果已禁用，则会在每次尝试连接时显示以下消息，且 VPN 无法连接。

```
The service provider in your current location is restricting access to the Internet.
The AnyConnect protection settings must be lowered for you to log on with the service
provider. Your current enterprise security policy does not allow this.
```

## 配置强制网络门户补救

仅在永远在线功能启用且连接失败策略设置为关闭时，才配置强制网络门户补救。在这种情况下，可通过配置强制网络门户补救，在强制网络门户阻止 AnyConnect 连接到 VPN 时允许它连接到 VPN。

如果连接失败策略设置为打开或永远在线未启用，则用户对网络的访问不会受到限制，而且用户无需在 AnyConnect VPN 客户端配置文件中进行任何特定配置，即可补救强制网络门户。

强制网络门户补救默认为禁用以提供最高安全性。

### 过程

---

**步骤 1** 打开 VPN 配置文件编辑器，从导航窗格中选择 **Preferences (Part 1)**。

**步骤 2** 选择 **Allow Captive Portal Remediation**。

此设置可提升连接失败策略关闭导致的网络访问限制。

**步骤 3** 指定补救超时。

输入 AnyConnect 提升网络访问限制的分钟数。要满足强制网络门户要求，用户需要足够的时间。

---

## 对强制网络门户检测和补救进行故障排除

AnyConnect 在以下情况下会错误地假设自己处于强制网络门户中。

- 如果 AnyConnect 尝试与包含不正确的服务器名称 (CN) 的证书的 ASA 通信，则 AnyConnect 客户端会认为它处于“强制网络门户”环境中。

要避免此情况，请确保正确配置了 ASA 证书。证书中的 CN 值必须匹配 VPN 客户端配置文件中 ASA 服务器的名称。

- 如果在 ASA 之前，网络中有另一台设备，且该设备通过阻止对 ASA 的 HTTPS 访问来对客户端尝试联系 ASA 做出响应，则 AnyConnect 客户端会认为它处于“强制网络门户”环境中。当用户位于内部网络且通过防火墙连接 ASA 时，可能发生此情况。

如果您需要从公司内部限制对 ASA 的访问，请配置防火墙以使至 ASA 地址的 HTTP 和 HTTPS 流量不会返回 HTTP 状态。应允许和完全阻止（也称为黑洞）对 ASA 的 HTTP/HTTPS 访问，从而确保发送至 ASA 的 HTTP/HTTPS 请求不会返回意外响应。

如果用户无法访问强制网络门户补救页面，请要求用户尝试以下操作：



- 终止任何使用 HTTP 的应用，如即时消息程序、邮件客户端、IP 电话客户端和除了一个执行补救的浏览器之外的一切应用。

强制网络门户可能会通过忽略重复的连接尝试使它们在客户端超时，从而积极地抑制 DoS 攻击。若很多应用都尝试进行 HTTP 连接，会加剧此问题。

- 禁用并重新启用网络接口。此操作会触发强制网络门户检测重试。
- 重启计算机。

## 通过 L2TP 或 PPTP 配置 AnyConnect

某些国家/地区的 ISP 要求支持第 2 层隧道协议 (L2TP) 和点对点隧道协议 (PPTP)。

要通过点对点协议 (PPP) 连接将流量发送到安全网关，AnyConnect 使用外部隧道生成的点对点适配器。通过 PPP 连接建立 VPN 隧道时，客户端必须从要发送到 ASA 以外目标的隧道流量排除发送目标为 ASA 的流量。要指定是否排除路由及如何确定排除路由，请使用 AnyConnect 配置文件中的 PPP 排除设置。排除路由在 AnyConnect GUI 的 Route Details 中显示为非安全路由。

### 过程

---

**步骤 1** 打开 VPN 配置文件编辑器，从导航窗格中选择 **Preferences (Part 2)**。

**步骤 2** 选择一种 **PPP Exclusion** 方法。此外，为此字段选中 **User Controllable**，让用户查看和更改此设置：

- **Automatic** - 启用 PPP 排除。AnyConnect 自动使用 PPP 服务器的 IP 地址。指示用户仅在自动检测无法获取 IP 地址时更改值。
- **Override** - 也会启用 PPP 排除。如果自动检测无法获取 PPP 服务器的 IP 地址，并且 PPP Exclusion UserControllable 值为 true，则指示用户按照下一节的说明使用此设置。
- **Disabled** - 不应用 PPP 排除。

**步骤 3** 在 **PPP Exclusion Server IP** 字段中，输入连接所用的 PPP 服务器的 IP 地址。为此字段选中 **User Controllable**，可让用户通过 preferences.xml 文件更改 PPP 服务器的此 IP 地址。

---

### 接下来的操作

有关更改 preferences.xml 文件的信息，请参阅“指示用户覆盖 PPP 排除”一节。

## 指示用户覆盖 PPP 排除

如果自动检测不起作用，并且您已将 PPP Exclusion 字段配置为用户可控制，则用户可以在本地计算机上通过编辑 AnyConnect 首选文件来覆盖设置。

## 过程

**步骤 1** 使用编辑器（如记事本）打开首选 XML 文件。

此文件位于用户计算机上的以下路径之一：

- Windows: %LOCAL\_APPDATA%\Cisco\Cisco AnyConnect Secure Mobility Client\preferences.xml。  
例如，
- Mac OS X: /Users/username/.anyconnect
- Linux: /home/username/.anyconnect

**步骤 2** 在 <ControllablePreferences> 下插入 PPPExclusion 详细信息，同时指定 Override 值和 PPP 服务器的 IP 地址。地址必须是格式正确的 IPv4 地址。例如：

```
<AnyConnectPreferences>
<ControllablePreferences>
<PPPExclusion>Override
<PPPExclusionServerIP>192.168.22.44</PPPExclusionServerIP></PPPExclusion>
</ControllablePreferences>
</AnyConnectPreferences>
```

**步骤 3** 保存文件。

**步骤 4** 退出并重新启动 AnyConnect。

## 配置 AnyConnect 代理连接

### 关于 AnyConnect 代理连接

AnyConnect 通过本地、公共和私有代理来支持 VPN 会话：

- 本地代理连接：

本地代理与 AnyConnect 在同一台计算机上运行，且有时用作透明代理。例如，一些无线数据卡提供的加速软件或一些防病毒软件（例如，Kaspersky）上的网络组件就是透明代理服务。

本地代理的使用在 AnyConnect VPN 客户端配置文件中启用或禁用，请参阅[允许本地代理连接](#)。

- 公共代理连接：

公共代理通常用于将网络流量匿名化。当 Windows 配置为使用公共代理时，AnyConnect 使用该连接。在 Mac 和 Linux 上支持使用公共代理用于本地和覆盖目的。

[配置公共代理连接](#)，[Windows](#)中描述了如何配置公共代理。

- 私有代理连接：

在企业网络上使用私有代理服务器来基于企业使用政策防止企业用户访问特定网站，例如色情、赌博或游戏站点。

将组策略配置为在隧道建立后将私有代理设置下载到浏览器。在 VPN 会话结束后，设置恢复到其初始状态。请参阅[配置专用代理连接](#)。



**注释** 通过代理服务器的 AnyConnect SBL 连接取决于 Windows 操作系统版本和系统（机器）配置或其他第三方代理软件功能；因此，请参阅 Microsoft 或您使用的任何第三方代理应用提供的系统范围代理设置。

### 使用 VPN 客户端配置文件控制客户端代理

VPN 客户端配置文件可以阻止或重定向客户端系统的代理连接。对于 Windows 和 Linux，您可以配置（也可以允许用户配置）公共代理服务器的地址。

有关在 VPN 客户端配置文件中配置代理设置的详细信息，请参阅 [AnyConnect 配置文件编辑器，首选项（第 2 部分）](#)

### 生成代理自动配置文件以提供无客户端支持

某些版本的 ASA 需要 AnyConnect 配置才能支持在建立 AnyConnect 会话后通过代理服务器进行无客户端门户访问。为使此情况发生，AnyConnect 使用代理自动配置 (PAC) 文件修改客户端代理设置。仅在 ASA 没有指定私有端代理设置时，AnyConnect 才生成此文件。

## AnyConnect 代理连接的要求

代理连接支持的操作系统视情况而定，如下所示：

代理连接类型	Windows	Mac OS X	Linux
本地代理	是	否	否
私有代理	是（在 Internet Explorer 上）	是（在 Safari 上）	否
公共代理	是（IE 和覆盖）	是（覆盖和本地）	是（覆盖和本地）

## 代理连接的限制

- IPv6 代理不支持进行任何类型的代理连接。
- 当已启用 永远在线 功能时，不支持通过代理进行连接。
- 要允许访问本地代理，需要一个 VPN 客户端配置文件。

## 允许本地代理连接

### 过程

---

- 步骤 1** 打开 VPN 配置文件编辑器，从导航窗格中选择 **Preferences (Part 2)**。
  - 步骤 2** 选择（默认值）或取消选择 **Allow Local Proxy Connections**。
- 

## 公共代理

公共代理在 Windows 和 Linux 平台上受支持。系统根据在客户端配置文件中设置的首选项选择代理服务器。在代理覆盖的情况下，AnyConnect 从配置文件抽取代理服务器。通过版本 4.1，我们在 Mac 上添加了代理支持，同时还在 Linux 和 Mac 上添加了本地代理配置。

在 Linux 上，在 AnyConnect 运行之前会导出本地代理设置。如果更改设置，则必须重新启动。

向代理服务器进行身份验证需要用户名和密码。当代理服务器配置为需要身份验证时，AnyConnect 支持基本和 NTLM 身份验证。AnyConnect 对话管理身份验证过程。成功向代理服务器进行身份验证后，AnyConnect 会提示输入 ASA 用户名和密码。

### 配置公共代理连接，Windows

请按照以下步骤在 Windows 上配置公共代理连接。

### 过程

---

- 步骤 1** 从 Internet Explorer 或控制面板打开 **Internet Options**。
  - 步骤 2** 选择 **Connections** 选项卡，然后点击 **LAN Settings** 按钮。
  - 步骤 3** 配置局域网以使用代理服务器，并输入代理服务器的 IP 地址。
-

## 配置公共代理连接，Mac

### 过程

- 
- 步骤 1** 请转至系统首选项，然后选择您连接的相应接口。
  - 步骤 2** 点击 **Advanced**。
  - 步骤 3** 从新窗口中选择 **Proxies** 选项卡。
  - 步骤 4** 启用 HTTPS 代理
  - 步骤 5** 在右侧面板的 Secure Proxy Server 字段中输入代理服务器地址。
- 

## 配置公共代理连接，Linux

要在 Linux 中配置公共代理连接，您必须设置环境变量。

## 配置专用代理连接

### 过程

- 
- 步骤 1** 在 ASA 组策略中配置私有代理信息。请参阅 *Cisco ASA* 系列 *VPN ASDM* 配置指南中的[为内部组策略配置浏览器代理](#)。  
**注释** 在 Mac 环境中，在打开终端并发出 `scutil --proxy` 之前，在浏览器中看不到从 ASA（在 VPN 连接时）向下推送的代理信息。
  - 步骤 2** （可选）[将客户端配置为忽略浏览器代理设置](#)。
  - 步骤 3** （可选）[锁定 Internet Explorer 的 Connections 选项卡](#)。
- 

## 将客户端配置为忽略浏览器代理设置

您可以在 AnyConnect 配置文件中指定策略以绕过用户 PC 上的 Microsoft Internet Explorer 或 Safari 代理配置设置。这可防止用户在公司网络之外建立隧道，并防止 AnyConnect 通过不需要或非法的代理服务器进行连接。

## 过程

- 
- 步骤 1** 打开 VPN 配置文件编辑器，从导航窗格中选择 **Preferences (Part 2)**。
- 步骤 2** 在 Proxy Settings 下拉列表中，选择 **IgnoreProxy**。Ignore Proxy 会使客户端忽略所有的代理设置。不会针对从 ASA 下载的代理执行任何操作。
- 

## 锁定 Internet Explorer 的 Connections 选项卡

在某些情况下，AnyConnect 会隐藏 Internet Explorer Tools > Internet Options > Connections 选项卡。显示此选项卡时，可让用户设置代理信息。隐藏此选项卡可防止用户有意或无意绕过隧道。在连接断开时会撤销选项卡锁定，并且被应用于该选项卡的所有管理员定义的策略所取代。此锁定发生的情况如下：

- ASA 配置指定 Connections 选项卡锁定。
- ASA 配置指定私有端代理。
- Windows 组策略之前锁定了 Connections 选项卡（覆盖未锁定 ASA 组策略设置）。

您可在组策略中将 ASA 配置为允许或不允许代理锁定。要使用 ASDM 执行此操作，请执行以下操作步骤：

## 过程

- 
- 步骤 1** 在 ASDM 中，转到 **Configuration > Remote Access VPN > Network (Client) Access > Group Policies**。
- 步骤 2** 选择组策略，点击 **Edit** 或 **Add** 可编辑或新增组策略。
- 步骤 3** 在导航窗格中，转到 **Advanced > Browser Proxy**。系统显示 Proxy Server Policy 窗格。
- 步骤 4** 点击 **Proxy Lockdown** 以显示更多代理设置。
- 步骤 5** 取消选中 **Inherit** 并选择 **Yes**，可启用代理锁定并在 AnyConnect 会话期间隐藏 Internet Explorer Connections 选项卡；或者，选择 **No** 可禁用代理锁定并在 AnyConnect 会话期间显示 Internet Explorer Connections 选项卡。
- 步骤 6** 点击 **OK** 保存代理服务器策略更改。
- 步骤 7** 点击 **Apply** 保存组策略更改。
- 

## 验证代理设置

- 对于 Windows：在注册表中的以下位置找到代理设置：

```
HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Internet Settings
```

- 对于 Mac OS X: 打开终端窗口, 并键入:

```
scutil --proxy
```

## 选择并排除 VPN 流量

### 将 IPv4 或 IPv6 流量配置为绕过 VPN

使用 Client Bypass Protocol 设置, 您可以配置 AnyConnect 客户端在 ASA 只需要 IPv6 流量时如何管理 IPv4 流量, 或者在 ASA 只需要 IPv4 流量时如何管理 IPv6 流量。

当 AnyConnect 客户端建立与 ASA 的 VPN 连接时, ASA 可以为客户端分配 IPv4 和/或 IPv6 地址。

如果为 IP 协议启用 Client Bypass Protocol, 但未对该协议配置地址池 (即, 未通过 ASA 向客户端分配用于该协议的 IP 地址), 则使用该协议的任何 IP 流量都不会通过 VPN 隧道发送, 而会在隧道外部发送。

如果禁用 Client Bypass Protocol, 且未对该协议配置地址池, 则客户端将在 VPN 隧道建立后丢弃该 IP 协议的所有流量。

例如, 假设 ASA 只将一个 IPv4 地址分配到 AnyConnect 连接, 且终端为双协议栈。当终端尝试连接 IPv6 地址时, 如果 Client Bypass Protocol 已禁用, IPv6 流量将被丢弃。如果 Client Bypass Protocol 已启用, IPv6 流量将以明文形式从客户端发送。

请在 ASA 的组策略中配置 Client Bypass Protocol。

#### 过程

- 
- 步骤 1** 在 ASDM 中, 转到 **Configuration > Remote Access VPN > Network (Client) Access > Group Policies**。
  - 步骤 2** 选择组策略, 点击 **Edit** 或 **Add** 可编辑或新增组策略。
  - 步骤 3** 选择 **Advanced > AnyConnect**。
  - 步骤 4** 如果该组策略不是默认组策略, 请取消选中 **Client Bypass Protocol** 旁边的 **Inherit**。
  - 步骤 5** 选择以下选项之一:
    - 点击 **Disable** 以丢弃 ASA 未向其分配地址的 IP 流量。
    - 点击 **Enable** 以明文形式发送该 IP 流量。
  - 步骤 6** 点击 **OK**。
  - 步骤 7** 点击 **Apply**。
-

## 配置支持本地打印机和关联设备的客户端防火墙

请参阅 *Cisco ASA* 系列 *VPN ASDM* 配置指南中的[支持本地打印机和关联设备的客户端防火墙](#)。

## 配置拆分隧道

分割隧道在网络（客户端）访问组策略中配置。请参阅 *Cisco ASA* 系列 *VPN ASDM* 配置指南中的[为 AnyConnect 流量配置分割隧道](#)。

在 ASDM 中更改组策略后，在 **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles > Add/Edit > Group Policy** 中确保组策略与连接配置文件关联。

## 拆分 DNS

在网络（客户端）访问策略中配置拆分 DNS 时，AnyConnect 将通过隧道向特定 DNS 服务器传送指定 DNS 查询（同时也在组策略内配置）。所有其他 DNS 查询将以明文形式进入客户端操作系统中的 DNS 解析程序来进行 DNS 解析。如果未配置拆分 DNS，AnyConnect 将通过隧道传送所有 DNS 查询。

### 拆分 DNS 的要求

拆分 DNS 支持标准和更新查询（包括 A、AAAA、NS、TXT、MX、SOA、ANY、SRV、PTR 和 CNAME）。与任意隧道网络匹配的 PTR 查询均获准通过隧道。

Windows 和 Mac OS X 平台均支持 AnyConnect 拆分 DNS。

对 Mac OS X，只有在符合以下条件之一时，AnyConnect 才能对特定 IP 协议使用真正的拆分 DNS：

- 为一种 IP 协议（例如 IPv4）配置拆分 DNS，为组策略中的另一种 IP 协议（例如 IPv6）配置客户端旁路协议（没有为后一种 IP 协议配置地址池）。
- 为两个 IP 协议都配置分离 DNS。

### 配置拆分 DNS

要在组策略中配置拆分 DNS，请执行以下操作：

#### 过程

#### 步骤 1 配置至少一个 DNS 服务器。

请参阅 *Cisco ASA* 系列 *VPN ASDM* 配置指南中的[为内部组策略配置服务器属性](#)。

确保指定的专用 DNS 服务器与客户端平台配置的 DNS 服务器不重叠。如果重叠，域名解析不会正常运转，且查询可能会终止。



**步骤 2** 配置拆分-包含隧道:

在 **Configuration > Remote Access VPN > Network (Client) Access > Group Policies > Advanced > Split Tunneling** 窗格中, 选择 **Tunnel Network List Below** 策略, 然后指定要隧道化的地址的 **Network List**。

拆分 DNS 不支持 Exclude Network List Below 拆分隧道策略。您必须使用 Tunnel Network List Below 拆分隧道策略来配置拆分 DNS。

**步骤 3** 配置拆分 DNS:

在 **Configuration > Remote Access VPN > Network (Client) Access > Group Policies > Advanced > Split Tunneling** 窗格中, 取消选中 **Send All DNS lookups through tunnel**, 然后在 **DNS Names** 中指定其查询要隧道化的域的名称。

---

**接下来的操作**

在 ASDM 中更改组策略后, 在 **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles > Add/Edit > Group Policy** 中确保组策略与连接配置文件关联。

## 使用 AnyConnect 日志验证拆分 DNS

要验证是否启用了拆分 DNS, 请搜索 AnyConnect 日志中包含 “Received VPN Session Configuration Settings” 的条目。该条目指示已启用拆分 DNS。IPv4 拆分 DNS 和 IPv6 拆分 DNS 有各自的日志条目。

## 检查哪些域使用拆分 DNS

您可以使用依赖于操作系统 DNS 解析程序的任何工具或应用来解析域名。例如, 您可以使用 ping 或网络浏览器来测试拆分 DNS 解析。其他工具 (如 nslookup 或 dig) 会规避操作系统 DNS 解析程序。

要使用客户端检查哪些域用于拆分 DNS, 请按照以下步骤操作:

**过程**

---

**步骤 1** 运行 **ipconfig/all** 并记录 DNS 后缀搜索列表旁边列出的域。**步骤 2** 建立 VPN 连接, 并再次检查 DNS 后缀搜索列表旁边列出的域。  
在建立隧道后添加的这些额外域是用于拆分 DNS 的域。

**注释** 此过程假定从 ASA 推送的域不会与已在客户端主机上配置的域重叠。

---

# 管理 VPN 身份验证

## 重要安全注意事项

- 我们不建议在安全网关上使用自签证书，因为用户有可能无意中将浏览器配置为信任欺诈服务器上的证书，并且用户在连接到安全网关时必须响应安全警告，这会带来不便。
- 我们强烈建议您为 AnyConnect 客户端启用 Strict Certificate Trust，原因如下：
  - 随着有针对性攻击的日益增多，在本地策略中启用 Strict Certificate Trust 有助于在用户从不受信任网络（例如公共访问网络）连接时，防止受到“中间人”攻击。
  - 即使您使用完全可验证且受信任的证书，默认情况下 AnyConnect 客户端也允许最终用户接受不可验证的证书。如果最终用户受到中间人攻击，他们可能会被提示接受恶意证书。要从最终用户删除此决定，请启用 Strict Certificate Trust。

要配置 **Strict Certificate Trust**，请参阅 [Cisco AnyConnect 安全移动客户端管理员指南，版本 4.1](#) 中的本地策略参数和值一节。

## 配置服务器证书处理

### 服务器证书验证

- AnyConnect 客户端不支持使用证书吊销列表 (CRL) 进行证书验证。

很多站点将它们所使用的认证授权机构用于在公司网络内验证服务器证书。这意味着客户端无法在尝试连接到头端时验证 CRL，因为客户端无法在公共网络中访问 CRL。客户端操作系统可配置为在 Windows 和 Mac OS X 中验证 CRL，但我们忽略该设置。
- 当用户连接到使用服务器证书配置的 ASA 时，系统仍将显示表示信任并导入该证书的复选框，即便信任链（根证书、中间证书等）存在问题也是如此。如果存在其他证书问题，则不显示该复选框。
- 如果使用 FQDN 的初始验证失败，则通过 FQDN 执行的 SSL 连接不会进行第二次服务器证书验证（包括使用 FQDN 的解析 IP 地址进行名称验证）。
- 如果服务器证书包含“密钥使用”，则 IPsec 和 SSL 连接将要求属性必须不仅包含 DigitalSignature，还包含 KeyAgreement 或 KeyEncipherment。如果服务器证书包含 EKU，则属性必须包含 serverAuth（用于 SSL 和 IPsec）或 ikeIntermediate（仅用于 IPsec）。请注意，接受 KU 或 EKU 不需要服务器证书。
- IPsec 连接将对服务器证书执行名称验证。出于 IPsec 名称验证的目的而应用以下规则：

如果存在具有相关属性的主题备选名称扩展，则仅对主题备选名称执行名称验证。相关属性包括针对所有证书的 DNS 名称属性，此外，如果针对某一 IP 地址执行连接，则还包括 IP 地址属性。

如果不存在主题备选名称扩展，或存在主题备选名称扩展但不包含相关属性，则对证书主题中找到的任何公用名称属性执行名称验证。

如果证书出于名称验证目的而使用了通配符，则通配符只能位于第一个（最左）子域，且必须是子域中的最后一个（最右）字符。出于名称验证的目的而将忽略任何不合规的通配符条目。

- 对于 OS X，过期的证书仅在密钥链访问配置为“Show Expired Certificates”时显示。默认情况下，过期的证书将隐藏，这可能会给用户造成困扰。

## 无效的服务器证书处理

为了应对不断增加的针对不受信任网络上移动用户的定向攻击，我们改进了客户端的安全保护，以帮助阻止严重的安全漏洞。默认的客户行为已更改，以提供一层额外防御来阻挡中间人攻击。

### 用户交互

当用户尝试连接到安全网关，并且存在证书错误（由于过期、日期无效、密钥使用错误或 CN 不匹配）时，用户会看到一个红色对话框，其中含有 **Change Settings** 和 **Keep Me Safe** 按钮。

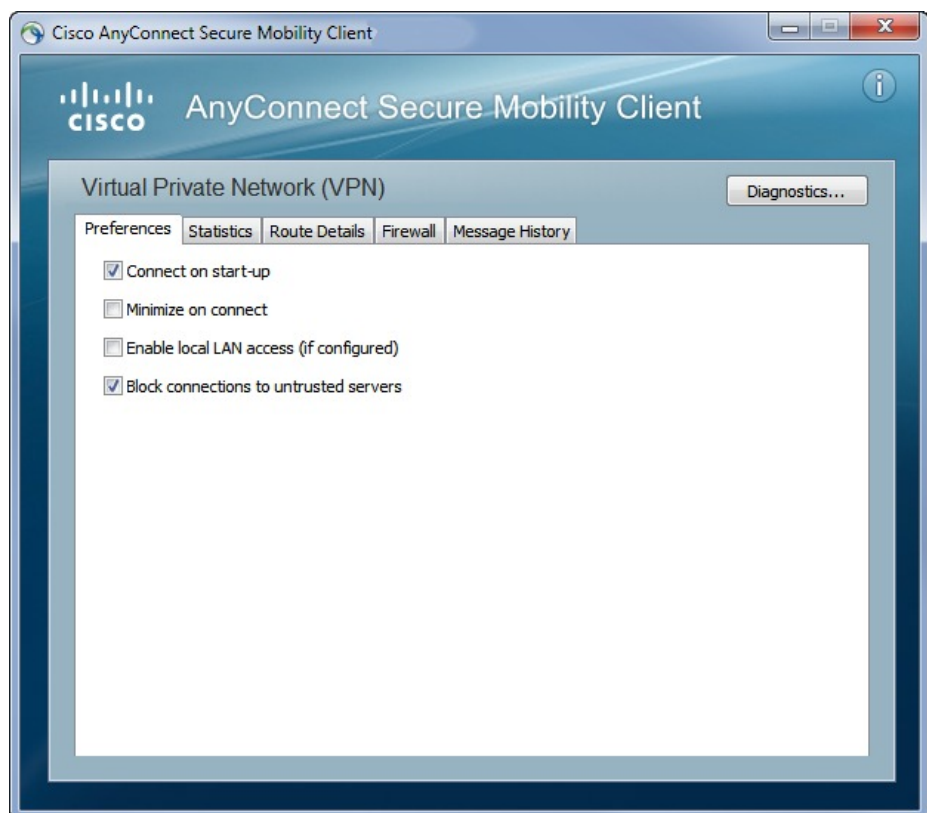


注释

Linux 下的对话框可能看起来与本文档所示的对话框不同。



- 点击 **Keep Me Safe** 将取消连接。
- 点击 **Change Settings** 将打开 AnyConnect 的 Advance > VPN > Preferences 对话框，用户可在其中启用与不受信任服务器的连接。当前连接尝试将被取消。



如果用户取消选中 **Block connections to untrusted servers**，并且唯一的证书问题是 CA 不受信任，则用户下次尝试连接到此安全网关时，将看不到 Certificate Blocked Error Dialog 对话框；他们只会看到以下对话框：



如果用户选中 **Always trust this VPN server and import the certificate** 选项，则未来与此安全网关的连接不会提示用户继续。



注释

如果用户在 **AnyConnect** 的 **Advanced > VPN > Preferences** 中选中 **Block connections to untrusted servers**，或者用户的配置满足准则和限制部分下描述的模式列表中的条件之一，则 **AnyConnect** 将拒绝无效服务器证书。

### 改进的安全行为

当客户端接受无效的服务器证书时，该证书保存在客户端的证书存储区中。以前，仅保存证书的拇指指纹验证。请注意，仅当用户选择始终信任并导入无效服务器证书时，才保存无效证书。

不会出现管理权限改写而自动导致最终用户安全性降低的情况。要完全删除最终用户先前的安全决策，请在用户的本地策略文件中启用 **Strict Certificate Trust**。启用 **Strict Certificate Trust** 后，用户将看到一条错误消息，并且连接失败；没有用户提示。

有关在本地策略文件中启用 **Strict Certificate Trust** 的信息，请参阅 [Cisco AnyConnect 安全移动客户端管理员指南，版本 4.1](#) 中的 *AnyConnect* 本地策略参数和值一节。

### 指南和限制

在以下情况下将拒绝无效服务器证书：

- **AnyConnect** VPN 客户端配置文件启用了 **Always On**，并且应用的组策略或 **DAP** 未将其关闭。
- 客户端的本地策略启用了 **Strict Certificate Trust**。
- **AnyConnect** 配置为在登录前启动。
- 使用机器证书存储区中的客户端证书进行身份验证。

## 配置仅证书身份验证

您可以指定想要用户使用 **AAA** 通过用户名和密码进行身份验证，还是使用数字证书验证（或同时使用两种方式）。配置仅证书身份验证时，用户可以使用数字证书进行连接，不需要提供用户 **ID** 和密码。

为了在使用多个组的环境中支持仅通过证书身份验证，您可以配置多个组 **URL**。每个组 **URL** 包含一个不同的客户端配置文件，其中包含一些定制数据，以允许创建特定于组的证书映射。例如，可在 **ASA** 上调配工程部的 **Department\_OU** 值，以便在此过程中的证书显示给 **ASA** 时将用户放入此组。



注释

用于向安全网关验证客户端身份的证书必须有效且受信任（由 **CA** 签署）。不接受自签客户端证书。

## 过程

- 步骤 1** 转至 **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles**。选择一个连接配置文件，然后单击 **Edit**。系统将打开 **Edit AnyConnect Connection Profile** 窗口。
- 步骤 2** 单击窗口左侧窗格中导航树的 **Basic** 节点（如果尚未单击）。在窗口右窗格的 **Authentication** 区域中，启用 **Certificate** 方法。
- 步骤 3** 单击 **OK** 应用更改。

## 配置证书注册

Cisco AnyConnect 安全移动客户端使用简单证书注册协议 (SCEP) 在客户端身份验证过程中调配和续约证书。采用以下方式通过 AnyConnect IPsec 和 SSL VPN 连接到 ASA 来支持使用 SCEP 的证书注册：

- **SCEP 代理：**ASA 作为客户端与证书颁发机构 (CA) 之间 SCEP 请求和响应的代理。
  - CA 必须能够接入 ASA，而不是 AnyConnect 客户端，因为客户端不会直接访问 CA。
  - 注册始终会由客户端自动发起。无需用户参与。
- **传统 SCEP：**AnyConnect 客户端与 CA 直接通信以注册和获取证书。
  - CA 必须能够访问 AnyConnect 客户端，而不是 ASA，通过建立的 VPN 隧道或直接在客户端所在的同一网络打开。
  - 注册由客户端自动发起，并且可由用户手动发起（如果需要配置）。

### 相关主题

[AnyConnect 配置文件编辑器，证书注册，第 78 页](#)

## SCEP 代理注册和操作

以下步骤说明如何获取证书，以及在为 SCEP 代理配置 AnyConnect 和 ASA 时如何建立基于证书的连接。

- 1** 用户使用为证书和 AAA 身份验证配置的连接配置文件连接到 ASA 头端。ASA 向客户端请求证书和 AAA 凭证进行身份验证。
- 2** 用户输入其 AAA 凭证，但有效证书不可用。此情形将在使用输入的 AAA 凭证建立隧道之后触发客户端发送一个自动 SCEP 注册请求。
- 3** ASA 将注册请求转发到 CA，并将 CA 的响应返回客户端。

- 4 如果 SCEP 注册成功，则客户端向用户显示一条（可配置的）消息，并断开当前会话连接。现在，用户即可使用证书身份验证连接到 ASA 隧道组。

如果 SCEP 注册失败，客户端会向用户显示一条（可配置）消息并断开当前会话连接。用户应与其管理员联系。

其他 SCEP 代理操作注意事项：

- 如果进行了相应的配置，则客户端将在证书过期之前自动续订，无需用户干预。
- SCEP 代理注册使用 SSL 进行 SSL 和 IPsec 隧道证书身份验证。

## 传统 SCEP 注册和操作

以下步骤说明当 AnyConnect 配置为传统 SCEP 时如何获取证书以及如何建立基于证书的连接。

- 1 当用户使用为证书身份验证配置的隧道组发起与 ASA 头端的连接时，ASA 向客户端请求证书进行身份验证。
- 2 客户端未提供有效证书。无法建立连接。证书失败表明需要进行 SCEP 注册。
- 3 用户必须使用为 AAA 身份验证配置的隧道组（其地址必须与客户端配置文件中配置的自动 SCEP 主机相匹配）发起与 ASA 头端的连接。ASA 向客户端请求 AAA 凭证。
- 4 客户端显示一个对话框供用户输入 AAA 凭证。

如果客户端配置为手动注册而且客户端知道其需要发起 SCEP 注册（请参阅步骤 2），在凭证对话框中将显示 **Get Certificate** 按钮。如果客户端可直接访问用户网络上的 CA，用户在此时将能够通过点击此按钮来手动获取证书。



注释

如果对 CA 的访问依赖于要建立的 VPN 隧道，则此时手动注册无法完成，因为当前未建立 VPN 隧道（AAA 凭证尚未输入）。

- 5 用户输入 AAA 凭证并建立 VPN 连接。
- 6 客户端知道其需要发起 SCEP 注册（请参阅步骤 2）。它通过已建立的 VPN 隧道向 CA 发起注册请求，并从 CA 接收响应。
- 7 如果 SCEP 注册成功，则客户端向用户显示一条（可配置的）消息，并断开当前会话连接。现在，用户即可使用证书身份验证连接到 ASA 隧道组。

如果 SCEP 注册失败，客户端会向用户显示一条（可配置）消息并断开当前会话连接。用户应与其管理员联系。

其他传统 SCEP 操作注意事项：

- 如果客户端配置为手动注册并且满足 **Certificate Expiration Threshold** 值，**Get Certificate** 按钮会显示在出现的隧道组选择对话框中。用户可以通过点击此按钮来手动续订证书。
- 如果证书过期且客户端不再有有效证书，客户端将重复传统 SCEP 注册过程。

## 证书颁发机构要求

- 支持所有符合 SCEP 的 CA，包括 IOS CS、Windows Server 2003 CA 和 Windows Server 2008 CA。
- CA 必须处于自动授予模式；不支持证书轮询。
- 您可以将某些 CA 配置为将注册密码用邮件发送给用户，以增加一层安全保护。CA 密码是发送到证书颁发机构来识别用户的质询密码或令牌。然后，密码被配置在 AnyConnect 客户端配置文件中，此配置文件成为授予证书之前 CA 验证的 SCEP 请求的一部分。如果使用手动传统 SCEP 注册，我们建议您在客户端配置文件中启用 CA 密码。

## 证书注册指南

- 对 ASA 的无客户端（基于浏览器的）VPN 访问不支持 SCEP 代理，但 WebLaunch（无客户端发起的 AnyConnect）支持 SCEP 代理。
- ASA 负载均衡支持通过 SCEP 注册。
- ASA 并不指出注册失败的原因，尽管它记录从客户端收到的请求。必须在 CA 或客户端上调试连接问题。
- ASA 上的仅通过证书身份验证和证书映射：

为了在使用多个组的环境中支持仅通过证书身份验证，您可以配置多个组 URL。每个组 URL 包含一个不同的客户端配置文件，其中包含一些定制数据，以允许创建特定于组的证书映射。例如，会在 ASA 上配置 Engineering 的 Department\_OU 值，以便当来自此进程的证书呈现给 ASA 时将用户放入此隧道组中。

- 识别注册连接应用策略。

在 ASA 上，`aaa.cisco.sceprequired` 属性可用于捕获注册连接和在选择的 DAP 记录中应用适当的策略。

- Windows 证书警告：

Windows 客户端在首次尝试从证书颁发机构获得证书时可能收到一条警告。出现提示时，用户必须点击 Yes。这会允许他们导入根证书。它不影响他们使用客户端证书进行连接。



## 配置 SCEP 代理证书注册

### 为 SCEP 代理注册配置 VPN 客户端配置文件

#### 过程

- 
- 步骤 1** 打开 VPN 配置文件编辑器，从导航窗格中选择 **Certificate Enrollment**。
- 步骤 2** 选择 **Certificate Enrollment**。
- 步骤 3** 配置在注册证书中要请求的 **Certificate Contents**。有关证书字段的定义，请参阅 [AnyConnect 配置文件编辑器，证书注册](#)。
- 注释
- 如果您使用 %machineid%，则必须为桌面客户端加载 HostScan/Posture。
  - 对于移动客户端，必须指定至少一个证书字段。
- 

### 配置 ASA 以支持 SCEP 代理注册

对于 SCEP 代理，一个 ASA 连接配置文件支持证书注册和证书的授权 VPN 连接。

#### 过程

- 
- 步骤 1** 创建组策略，例如，cert\_group。设置以下字段：
- 在 General 中的 **SCEP Forwarding URL** 内输入 CA 的 URL。
  - 在 Advanced > AnyConnect Client 窗格中，取消选中 **Inherit for Client Profiles to Download** 并指定针对 SCEP 代理配置的客户端配置文件。例如，指定 ac\_vpn\_scep\_proxy 客户端配置文件。
- 步骤 2** 为证书注册和证书授权连接创建连接配置文件，例如 cert\_tunnel。
- 身份验证：两者（AAA 和证书）。
  - 默认组策略：cert\_group。
  - 在 Advanced > General 中，选中 **Enable SCEP Enrollment for this Connction Profile**。
  - 在 Advanced > GroupAlias/Group URL 中，创建包含此连接配置文件的组 (cert\_group) 的组 URL。
-

## 配置传统 SCEP 证书注册

### 为传统 SCEP 注册配置 VPN 客户端配置文件

#### 过程

- 
- 步骤 1** 打开 VPN 配置文件编辑器，从导航窗格中选择 **Certificate Enrollment**。
- 步骤 2** 选择 **Certificate Enrollment**。
- 步骤 3** 指定 **Automatic SCEP Host** 以指示客户端检索证书。  
输入 FQDN 或 IP 地址，以及为 SCEP 证书检索配置的连接配置文件（隧道组）的别名。例如，如果 asa.cisco.com 是 ASA 的主机名，scep\_eng 是连接配置文件的别名，则输入 asa.cisco.com/scep-eng。  
当用户启动连接时，选择或指定的地址必须与此值完全匹配，传统 SCEP 注册才会成功。例如，如果此字段设置为 FQDN，但用户指定 IP 地址，SCEP 注册会失败。
- 步骤 4** 配置证书颁发机构属性：  
**注释** CA 服务器管理员可以提供 CA URL 和拇指指纹。直接从服务器检索拇指指纹，而不是从颁发的证书中的“fingerprint”或“thumbprint”属性字段检索。
- 指定 CA URL 以识别 SCEP CA 服务器。输入 FQDN 或 IP 地址。例如：  
http://ca01.cisco.com/certsrv/mscep/mscep.dll。
  - （可选）选中 **Prompt For Challenge PW**，提示用户输入其用户名和一次性密码。
  - （可选）输入 CA 证书的指纹验证。使用 SHA1 或 MD5 哈希值。例如：  
8475B661202E3414D4BB223A464E6AAB8CA123AB。
- 步骤 5** 配置在注册证书中要请求的 **Certificate Contents**。有关证书字段的定义，请参阅 [AnyConnect 配置文件编辑器，证书注册](#)。  
**注释** 如果您使用 %machineid%，在客户端上加载 HostScan/Posture。
- 步骤 6** （可选）选中 **Display Get Certificate Button** 允许用户手动请求调配或续订身份验证证书。如果证书身份验证失败，该按钮对用户可见。
- 步骤 7** （可选）为服务器列表中的特定主机启用 SCEP。这样会覆盖上述 Certificate Enrollment 窗格中的 SCEP 设置。
- 从导航窗格中选择 **Server List**。
  - Add** 或 **Edit** 服务器列表条目。
  - 如上面的步骤 5 和 6 所述，指定 Automatic SCEP Host 和 Certificate Authority 属性。
- 

### 配置 ASA 以支持传统 SCEP 注册

对于 ASA 上的传统 SCEP，必须创建连接配置文件和组策略以进行证书注册，然后创建另一个连接配置文件和组策略以进行证书颁发机构的 VPN 连接。

## 过程

- 步骤 1** 创建用于注册的组策略，例如 `cert_enroll_group`。设置以下字段：  
在 **Advanced > AnyConnect Client** 窗格中，取消选中 **Inherit for Client Profiles to Download** 并指定为传统 SCEP 配置的客户端配置文件。例如，指定 `ac_vpn_legacy_scep` 客户端配置文件。
- 步骤 2** 创建另一个用于授权的组策略，例如 `cert_auth_group`。
- 步骤 3** 创建用于注册的连接配置文件，例如 `cert_enroll_tunnel`。设置以下字段：
- 在 **Basic** 窗格中，将 **Authentication Method** 设置为 **AAA**。
  - 在 **Basic** 窗格中，将 **Default Group Policy** 设置为 `cert_enroll_group`。
  - 在 **Advanced > GroupAlias/Group URL** 中，创建一个组 URL，其中包含用于此连接配置文件的注册组 (`cert_enroll_group`)。
  - 请勿在 ASA 上启用连接配置文件。没有必要为了使用户具有对组的访问权，而将该组公开给用户。
- 步骤 4** 创建用于授权的连接配置文件，例如 `cert_auth_tunnel`。设置以下字段。
- 在 **Basic** 窗格中，将 **Authentication Method** 设置为 **Certificate**。
  - 在 **Basic** 窗格中，将 **Default Group Policy** 设置为 `cert_auth_group`。
  - 请勿在 ASA 上启用此连接配置文件。没有必要为了使用户具有对组的访问权，而将该组公开给用户。
- 步骤 5** （可选）在每个组策略的 **General** 窗格中，将 **Connection Profile (Tunnel Group) Lock** 设置为相应的 SCEP 连接配置文件，以限制到 SCEP 所配置的连接配置文件的流量。

## 为 SCEP 设置 Windows 2008 服务器证书颁发机构

如果证书颁发机构软件在 Windows 2008 服务器上运行，您可能需要对服务器做出以下配置更改之一，以支持 SCEP 与 AnyConnect 一起使用。

### 在证书颁发机构上禁用 SCEP 密码

以下步骤说明如何禁用 SCEP 质询密码，以便客户端无需在 SCEP 注册之前提供带外密码。

## 过程

- 步骤 1 在认证中心服务器上，启动注册编辑器。您可以通过选择 **Start > Run**，键入 **regedit** 然后点击 **OK** 来执行此操作。
- 步骤 2 导航到 **HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Cryptography\MSCEP\EnforcePassword**。如果 **EnforcePassword** 密钥不存在，请将其创建为新密钥。
- 步骤 3 编辑 **EnforcePassword**，并将其设置为“0”。如果不存在，请将其创建为 **REG-DWORD**。
- 步骤 4 退出 **regedit**，然后重新引导证书颁发机构服务器。

## 在证书颁发机构上设置 SCEP 模板

以下步骤说明如何创建证书模板，并将其指定为默认 SCEP 模板。

## 过程

- 步骤 1 启动 **Server Manager**。可通过选择 **Start > Admin Tools > Server Manager** 执行此操作。
- 步骤 2 展开 **Roles > Certificate Services**（或 **AD Certificate Services**）。
- 步骤 3 导航到 **CA Name > Certificate Templates**。
- 步骤 4 右键单击 **Certificate Templates > Manage**。
- 步骤 5 从 **Cert Templates Console** 中，右键单击用户模板并选择 **Duplicate**。
- 步骤 6 为新模板选择 **Windows Server 2008 version**，然后点击 **OK**。
- 步骤 7 将模板显示名更改为描述性名称，如 **NDES-IPSec-SSL**。
- 步骤 8 调整站点的有效期。大多数站点选择三年或更长有效期以避免证书过期。
- 步骤 9 在 **Cryptography** 选项卡中，为部署设置最小密钥长度。
- 步骤 10 在 **Subject Name** 选项卡中，选择 **Supply in Request**。
- 步骤 11 在 **Extensions** 选项卡中，将 **Application Policies** 设置为至少包括：

- 客户端身份验证
- IP 安全端系统
- IP 安全 IKE intermediate
- IP 安全隧道终止
- IP 安全用户

这些值对于 **SSL** 或 **IPsec** 有效。

- 步骤 12** 点击 **Apply**，然后点击 **OK** 保存新模板。
- 步骤 13** 从 Server manager > Certificate Services-CA Name，右键点击 Certificate Templates。选择 New > Certificate Template to Issue，然后选择您创建的新模板（在本示例中为 NDES-IPSec-SSL）并点击 **OK**。
- 步骤 14** 编辑注册表。您可以通过选择 Start > Run、regedit 并点击 **OK** 执行此操作。
- 步骤 15** 导航到 HKEY\_LOCAL\_MACHINE\SOFTWARE\Microsoft\Cryptography\MSCEP。
- 步骤 16** 将以下三个关键字的值设置为 **NDES-IPSec-SSL**。
- EncryptionTemplate
  - GeneralPurposeTemplate
  - SignatureTemplate
- 步骤 17** 点击 **Save**，并重新启动证书颁发机构服务器。
- 

## 配置证书到期通知

配置 AnyConnect 以提醒用户其身份验证证书即将到期。 **Certificate Expiration Threshold** 设置指定 AnyConnect 在证书到期之前多少天提醒用户其证书即将到期。 AnyConnect 在每次连接时都会提醒用户，直到证书实际到期或已获取新证书。



**注释** 证书到期阈值功能不能与 RADIUS 一起使用。

---

### 过程

---

- 步骤 1** 打开 VPN 配置文件编辑器，从导航窗格中选择 **Certificate Enrollment**。
- 步骤 2** 选择 **Certificate Enrollment**。
- 步骤 3** 指定 **Certificate Expiration Threshold**。  
这是 AnyConnect 在证书到期前提醒用户其证书即将到期的天数。  
默认值为 0（不显示警告）。范围为 0 至 180 天。
- 步骤 4** 点击 **OK**。
-

## 配置证书选择

以下步骤显示 AnyConnect 配置文件中可以配置证书搜索方式的所有位置，以及在客户端系统中选择证书的方式。这些都不是必须执行的步骤，如果您未指定任何条件，AnyConnect 将使用默认密钥匹配。

AnyConnect 读取 Windows 上的浏览器证书存储区。对于 Mac 和 Unix，必须创建 Privacy Enhanced Mail (PEM) 格式的文件存储。

### 过程

- 
- 步骤 1** 仅限 Windows: [配置要使用的 Windows 证书存储区，第 126 页](#)  
在 VPN 客户端配置文件中指定 AnyConnect 使用的证书存储区。
  - 步骤 2** 仅限 Windows: [提示 Windows 用户选择身份验证证书，第 127 页](#)  
配置 AnyConnect，为用户显示有效的证书列表，让他们选择证书以对会话进行身份验证。
  - 步骤 3** 对于 Mac 和 Linux 环境: [为 Mac 和 Linux 创建 PEM 证书存储区，第 128 页](#)
  - 步骤 4** 对于 Mac 和 Linux 环境: 在 VPN 本地策略配置文件中选择要排除的证书存储区。
  - 步骤 5** [配置证书匹配，第 129 页](#)  
配置 AnyConnect 在存储区中搜索证书时尝试匹配的密钥。您可以指定密钥、扩展密钥，并添加定制扩展密钥。还可以使用可分辨名称指定 AnyConnect 匹配的运算符值模式。
- 

## 配置要使用的 Windows 证书存储区

Windows 为本地计算机和当前用户提供单独的证书存储区。在 VPN 客户端配置文件中指定 AnyConnect 使用的证书存储区。默认情况下，它同时搜索两者，但是您可以将 AnyConnect 配置为只使用一个存储。

拥有计算机管理权限的用户有权访问两个证书存储区。没有管理权限的用户只能访问用户证书存储区。通常，Windows 用户不具备管理权限。选择 **Certificate Store Override** 将允许 AnyConnect 访问计算机存储区，即使在用户没有管理权限时也是如此。



### 注释

---

计算机存储区的访问控制会因 Windows 版本和安全设置而异。因此，即使用户具备管理权限，也可能无法使用计算机存储区中的证书。在此情况下，选择 **Certificate Store Override** 可允许访问计算机存储区。

---

下表描述 AnyConnect 如何基于搜索何种 **Certificate Store** 以及是否选中 **Certificate Store Override** 从而在 Windows 客户端中搜索证书。

Certificate Store 设置	Certificate Store Override 设置	AnyConnect 搜索策略
全部	已清除	AnyConnect 搜索所有的证书存储区。当用户不具备管理权限时，不允许 AnyConnect 访问计算机存储区。 该设置为默认设置。此设置适合大多数情况。请勿更改此设置，除非有特定原因或场景要求这样做。
全部	已选中	AnyConnect 搜索所有的证书存储区。当用户不具备管理权限时，允许 AnyConnect 访问计算机存储区。
Machine	已选中	AnyConnect 搜索计算机证书存储区。当用户不具备管理权限时，允许 AnyConnect 搜索计算机存储区。
Machine	已清除	AnyConnect 搜索计算机证书存储区。当用户不具备管理权限时，不允许 AnyConnect 搜索计算机存储区。 注释 仅当允许有限的一组用户使用证书进行身份验证时，才可以使用此配置。
用户	不适用	AnyConnect 只在用户证书存储区中进行搜索。证书存储区覆盖不适用，原因是没有管理权限的用户可以访问此证书存储区。

## 过程

### 步骤 1 设置 Certificate Store。

控制 AnyConnect 使用哪个证书存储库来存储和读取证书。默认设置 (All) 适用于大多数情况。请勿更改此设置，除非有特定原因或场景要求这样做。

- All (默认值) - 指示 AnyConnect 客户端使用所有证书存储库来定位证书。
- Machine - 指示 AnyConnect 客户端仅在 Windows 本地计算机证书存储库中查找证书。
- User - 指示 AnyConnect 客户端仅在本地用户证书存储库中查找证书。

### 步骤 2 如果要在用户不具备管理权限时允许 AnyConnect 搜索计算机证书存储区，请选择 Certificate Store Override。

## 提示 Windows 用户选择身份验证证书

您可以将 AnyConnect 配置为向用户显示有效证书列表并让他们选择证书以对会话进行身份验证。此配置仅对 Windows 可用。默认情况下，用户证书选择被禁用。

## 过程

- 
- 步骤 1** 打开 VPN 配置文件编辑器，从导航窗格中选择 **Preferences (Part 2)**。
- 步骤 2** 要启用证书选择，请取消选中 **Disable Certificate Selection**。
- 步骤 3** 取消选中 **User Controllable**，除非您要用户能够在 **Advanced > VPN > Preferences** 窗格中打开和关闭自动证书选择。
- 

## 为 Mac 和 Linux 创建 PEM 证书存储区

AnyConnect 支持从隐私增强型邮件 (PEM) 格式化文件存储区中检索证书。AnyConnect 从远程计算机上的文件系统读取 PEM 格式化的证书文件，对其进行验证和签署。

### 开始之前

为了使客户端在任何情况下都能获得适当的证书，请确保您的文件满足以下要求：

- 所有证书文件必须以扩展名 `.pem` 结尾。
- 所有的私钥文件都必须以扩展名 `.key` 结尾。
- 客户端证书及其对应的私有密钥必须具有相同的文件名。 例如：`client.pem` 和 `client.key`。



**提示** 可以使用指向 PEM 文件的软链接，而不是保留 PEM 文件的副本。

要创建 PEM 文件证书存储区，请创建如下列出的路径和文件夹。将相应的证书置于这些文件夹中：

PEM 文件证书存储区文件夹	所存储证书的类型
~/.cisco/certificates/ca(1) ~ 注释 这是主目录。	受信任 CA 和根证书
~/.cisco/certificates/client	客户端证书
~/.cisco/certificates/client/private	私有密钥

计算机证书与 PEM 文件证书相同（除了根目录）。对于计算机证书，用 `/opt/.cisco` 替代 `~/.cisco`。否则，将应用列出的证书的路径、文件夹和类型。



## 配置证书匹配

AnyConnect 可将其证书搜索限于匹配一组特定密钥的证书。证书匹配是在 AnyConnect VPN 客户端配置文件的 **Certificate Matching** 窗格中设置的全局条件。条件包括：

- 密钥使用
- 扩展密钥使用
- 可分辨名称

### 相关主题

[AnyConnect 配置文件编辑器，证书匹配，第 75 页](#)

## 配置密钥使用

选择 **Key Usage** 密钥会将 AnyConnect 可用的证书限于至少有一个所选密钥的证书。支持的密钥列在 VPN 客户端配置文件的 **Key Usage** 列表中，其中包括：

- DECIPHER\_ONLY
- ENCIPHER\_ONLY
- CRL\_SIGN
- KEY\_CERT\_SIGN
- KEY\_AGREEMENT
- DATA\_ENCIPHERMENT
- KEY\_ENCIPHERMENT
- NON\_REPUDIATION
- DIGITAL\_SIGNATURE

如果指定一个或多个条件，证书必须匹配至少一个条件才被视为匹配的证书。

## 配置扩展密钥使用

选择 **Extended Key Usage** 密钥会将 AnyConnect 可用的证书限于具有这些密钥的证书。下表列出一组已知的限制条件及其对应的对象标识符 (OID)。

限制条件	OID
serverAuth	1.3.6.1.5.5.7.3.1
ClientAuth	1.3.6.1.5.5.7.3.2
CodeSign	1.3.6.1.5.5.7.3.3
EmailProtect	1.3.6.1.5.5.7.3.4

限制条件	OID
IPSecEndSystem	1.3.6.1.5.5.7.3.5
IPSecTunnel	1.3.6.1.5.5.7.3.6
IPSecUser	1.3.6.1.5.5.7.3.7
TimeStamp	1.3.6.1.5.5.7.3.8
OCSPSign	1.3.6.1.5.5.7.3.9
DVCS	1.3.6.1.5.5.7.3.10
IKE Intermediate	1.3.6.1.5.5.8.2.2

### 配置自定义扩展匹配密钥

所有其他 OID（例如本文档的一些示例中所使用的 1.3.6.1.5.5.7.3.11）被视为“自定义”。作为管理员，如果您所需的 OID 未包含在众所周知的集合中，则可以添加自己的 OID。

### 配置证书可分辨名称

**Distinguished Name** 表包含证书标识符，用于将客户端可以使用的证书限于符合指定条件的证书。点击 **Add** 按钮以在列表中添加条件，并且设置值或通配符以与添加了条件的内容匹配。

标识符	描述
CN	SubjectCommonName
SN	SubjectSurName
GN	SubjectGivenName
N	SubjectUnstructName
I	SubjectInitials
GENQ	SubjectGenQualifier
DNQ	SubjectDnQualifier
C	SubjectCountry
L	SubjectCity
SP	SubjectState

标识符	描述
ST	SubjectState
O	SubjectCompany
OU	SubjectDept
T	SubjectTitle
EA	SubjectEmailAddr
DC	DomainComponent
ISSUER-CN	IssuerCommonName
ISSUER-SN	IssuerSurName
ISSUER-GN	IssuerGivenName
ISSUER-N	IssuerUnstructName
ISSUER-I	IssuerInitials
ISSUER-GENQ	IssuerGenQualifier
ISSUER-DNQ	IssuerDnQualifier
ISSUER-C	IssuerCountry
ISSUER-L	IssuerCity
ISSUER-SP	IssuerState
ISSUER-ST	IssuerState
ISSUER-O	IssuerCompany
ISSUER-OU	IssuerDept
ISSUER-T	IssuerTitle
ISSUER-EA	IssuerEmailAddr
ISSUER-DC	IssuerDomainComponent

**Distinguished Name** 可以包含零个或多个匹配条件。证书必须匹配所有指定的条件才被视为匹配的证书。**Distinguished Name** 匹配指定证书必须或不能具有指定的字符串，并且指定是否允许对字符串使用通配符。

## 使用 SDI 令牌 (SoftID) 集成进行 VPN 身份验证

AnyConnect 支持在 Windows 7 x86 (32 位) 和 x64 (64 位) 上运行 RSA SecurID 客户端软件 1.1 版和更高版本。

RSA SecurID 软件验证器可减少用户为确保企业资产访问安全而需要管理的项目数量。远程设备上的 RSA SecurID 软件令牌将生成一个随机的一次性验证码，该验证码每 60 秒变更一次。术语 SDI 的全称是 Security Dynamics, Inc. 技术，指代这一项使用硬件和软件令牌的一次性密码生成技术。

通常情况下，用户通过点击工具托盘中的 AnyConnect 图标、选择希望连接的连接配置文件，然后在身份验证对话框中输入适当的凭证来建立 AnyConnect 连接。登录（质询）对话框将匹配为用户所属的隧道组配置的身份验证类型。登录对话框中的输入字段可明确表明身份验证需要哪类输入。

对于 SDI 身份验证，远程用户需要在 AnyConnect 软件界面中输入 PIN（个人识别码）并接收 RSA SecurID 验证码。用户在安全应用中输入验证码后，RSA 身份验证管理器将验证该验证码并准许用户获得访问权限。

使用 RSA SecurID 硬件或软件令牌的用户将看到输入字段，这些字段指示用户应输入验证码或 PIN，PIN 或验证码以及对话框底部的状态行可提供更多要求信息。用户直接向 AnyConnect 用户界面输入软件令牌 PIN 或密码。

初始登录对话框的外观取决于安全网关设置：用户可通过主登录页面、主索引 URL、隧道组登录页面或隧道组 URL（URL/隧道组）访问安全网关。要通过主登录页面访问安全网关，则必须在 Network (Client) Access AnyConnect Connection Profiles 页面上选中 Allow user to select connection 复选框。在任何一种情况中，安全网关都会向客户端发送登录页面。主登录页面具有可供用户选择隧道组的下拉列表；由于在 URL 中指定隧道组，隧道组登录页面不含下拉列表。

在主登录页面（具有连接配置文件或隧道组的下拉列表）上，默认隧道组的身份验证类型将确定密码输入字段标签的初始设置。例如，如果默认隧道组使用 SDI 身份验证，则字段标签为“Passcode”，但如果默认隧道组使用 NTLM 身份验证，字段标签为“Password”。在 2.1 版及更高版本中，字段标签不会因用户选择不同的隧道组而动态更新。对于隧道组登录页面，字段标签将与隧道组要求匹配。

客户端支持在密码输入字段中输入 RSA SecurID 软件令牌 PIN。如果安装 RSA SecurID 软件令牌软件，并且隧道组身份验证类型为 SDI，则字段标签为“Passcode”，并且状态栏会声明“Enter a username and passcode or software token PIN”。如果使用 PIN，则针对同一隧道组和用户名的后续连续登录都将包含“PIN”字段标签。客户端使用输入的 PIN 从 RSA SecurID 软件令牌 DLL 检索验证码。每次身份验证成功后，客户端均会保存隧道组、用户名以及身份验证类型，保存的隧道组将成为新的默认隧道组。

AnyConnect 接受针对任意 SDI 身份验证的验证码。即使密码输入标签为“PIN”，用户仍可按照状态栏的指示输入验证码。客户端将按照原样向安全网关发送验证码。如果使用验证码，则针对同一隧道组和用户名的后续连续登录都将包含“Passcode”字段标签。

RSASecureIDIntegration 配置文件设置有三个可能的值：

- Automatic - 客户端首先尝试一种方法，如果失败，则尝试另一种方法。默认将用户输入视为令牌验证码 (HardwareToken)，如果失败，则将其视为软件令牌 PIN (SoftwareToken)。如果身份验证成功，该成功方法将设置为新 SDI 令牌类型，并缓存在用户首选项文件中。对于下一次身份验证尝试，SDI 令牌类型将定义首先尝试的方法。通常，用于当前身份验证尝试的令牌与上

次成功身份验证尝试中使用的令牌相同。然而，当用户名或组选择更改时，它将恢复为首先尝试默认方法，如输入字段标签所示。



**注释** SDI 令牌类型仅在自动设置中有意义。当身份验证模式不是自动模式时，可以忽略 SKI 令牌类型的日志。HardwareToken 作为默认选项可避免触发下一个令牌模式。

- SoftwareToken - 客户端始终将用户输入视为软件令牌 PIN，输入字段标签为“PIN:”。
- HardwareToken - 客户端始终将用户输入视为令牌验证码，输入字段标签为“Passcode:”。



**注释** AnyConnect 不支持将多个令牌的令牌选择导入 RSA 软件令牌客户端软件。相反，客户端使用通过 RSA SecurID 软件令牌 GUI 选择的默认选项。

## SDI 身份验证交换的类别

所有 SDI 身份验证交换均属于以下类别之一：

- 普通 SDI 身份验证登录
- 新用户模式
- 新 PIN 模式
- 清除 PIN 模式
- 下一个令牌码模式

### 普通 SDI 身份验证登录

普通登录质询始终用作第一个质询。SDI 身份验证用户必须分别在用户名和验证码或 PIN 字段中提供用户名和令牌验证码（或者在使用软件令牌时提供 PIN）。客户端将信息返回到安全网关（中心站点设备），然后安全网关使用身份验证服务器（SDI 或通过 RADIUS 代理的 SDI）对身份验证进行验证。

如果身份验证服务器接受身份验证请求，则安全网关会将成功页面发送回客户端，身份验证交换完成。

如果验证码不被接受，则身份验证失败，安全网关会发送一个新的登录质询页面以及一条错误消息。如果达到 SDI 服务器上的验证码失败次数阈值，则 SDI 服务器会将令牌放入下一个令牌码模式中。

### 新用户模式、清除 PIN 模式和新 PIN 模式

PIN 只能在 SDI 服务器上由网络管理员清除。

在新用户模式、清除 PIN 模式和新 PIN 模式中，AnyConnect 缓存用户创建的 PIN 或系统分配的 PIN，供以后在“下一个验证码”登录质询中使用。

从远程用户的角度来看，清除 PIN 模式和新用户模式是相同的，而且安全网关对两者同等对待。在这两种情况下，远程用户要么必须输入新 PIN，要么由 SDI 服务器分配一个新 PIN。唯一的区别在于对初始质询的用户响应。

对于新 PIN 模式，现有 PIN 用于生成验证码，就像在任何普通质询中一样。对于清除 PIN 模式，硬件令牌根本不会使用 PIN，用户只需输入令牌码。连续八个零 (00000000) 的 PIN 用于为 RSA 软件令牌生成验证码。无论哪种情况，SDI 服务器管理员都必须通知用户使用什么 PIN 值（如果有的话）。

将新用户添加到 SDI 服务器与清除现有用户的 PIN 这两种操作会得到相同的结果。在这两种情况下，用户必须提供新 PIN 或者由 SDI 服务器分配一个新 PIN。在这些模式中，对于硬件令牌，用户只需从 RSA 设备输入一个令牌码。无论哪种情况，SDI 服务器管理员都必须通知用户使用什么 PIN 值（如果有的话）。

### 创建新 PIN

如果没有当前 PIN，则 SDI 服务器要求满足以下条件之一（具体取决于系统的配置）：

- 系统必须给用户分配一个新 PIN（默认值）
- 用户必须创建一个新 PIN
- 用户可以选择创建 PIN 或由系统分配 PIN

如果 SDI 服务器配置为允许远程用户选择是创建 PIN 还是由系统分配 PIN，则登录屏幕会显示一个包含这些选项的下拉列表。状态行提供提示消息。

对于系统分配的 PIN，如果 SDI 服务器接受用户在登录页面上输入的验证码，则安全网关会向客户端发送系统分配的 PIN。客户端向安全网关发送回响应，表示用户看到了新 PIN，系统继续“下一个验证码”质询。

如果用户选择创建新 PIN，则 AnyConnect 会显示一个对话框以便输入该 PIN。PIN 必须是一个 4 到 8 位的数字。由于 PIN 是一种类型的密码，用户在这些输入字段中输入的任何内容都显示为星号。

使用 RADIUS 代理时，PIN 确认是继原始对话框之后的一个单独质询。客户端将新 PIN 发送到安全网关，安全网关继续“下一个验证码”质询。

#### “下一个验证码”和“下一个令牌代码”质询

对于“下一个验证码”质询，客户端使用在创建或分配新 PIN 过程中缓存的 PIN 值从 RSA SecurID 软件令牌 DLL 检索下一个验证码并将其返回给安全网关，而不会提示用户。同样，对于软件令牌的“下一个令牌代码”质询，客户端从 RSA SecurID 软件令牌 DLL 检索下一个令牌代码。

## 比较本地 SDI 与 RADIUS SDI

网络管理员可以配置安全网关，以允许通过以下模式之一进行 SDI 身份验证：

- 本地 SDI 指安全网关中与 SDI 服务器直接通信以便处理 SDI 身份验证的本地能力。
- RADIUS SDI 指安全网关使用 RADIUS SDI 代理（与 SDI 服务器通信）执行 SDI 身份验证的过程。

对于远程用户而言，本地 SDI 和 RADIUS SDI 看起来是相同的。由于 SDI 消息在 SDI 服务器上可配置，ASA 上的消息文本必须与 SDI 服务器上的消息文本匹配。否则，向远程客户端用户显示的提示可能不适合身份验证过程中所需的操作。AnyConnect 可能无法响应，并且身份验证可能失败。

RADIUS SDI 质询基本上反映本地 SDI 交换，仅有极少例外情况。因为两者最终都与 SDI 服务器进行通信，需从客户端获取的信息和索取信息的顺序相同。

在身份验证过程中，RADIUS 服务器向 ASA 显示访问质询消息。这些质询消息中有包含来自 SDI 服务器的文本的应答消息。ASA 直接与某 SDI 服务器通信时的消息文本与通过 RADIUS 代理通信时的消息文本不同。因此，为了向 AnyConnect 显示为本地 SDI 服务器，ASA 必须解析来自 RADIUS 服务器的消息。

此外，由于 SDI 消息在 SDI 服务器上可配置，ASA 的消息文本必须与 SDI 服务器的消息文本（全部或部分）匹配。否则，向远程客户端用户显示的提示可能不适合身份验证过程中所需的操作。AnyConnect 可能无法响应，并且身份验证可能失败。

## 配置 ASA 以支持 RADIUS/SDI 消息

要配置 ASA 以解释特定于 SDI 的 RADIUS 回复消息并提示 AnyConnect 用户执行相应的操作，您必须配置连接配置文件（隧道组），以模拟与 SDI 服务器直接通信的方式转发 RADIUS 回复消息。用户对 SDI 服务器进行身份验证时，必须通过此连接配置文件进行连接。

### 过程

- 步骤 1 转至 **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles**。
- 步骤 2 选择要配置来解释特定于 SDI 的 RADIUS 回复消息的连接配置文件，然后点击 **Edit**。
- 步骤 3 在 **Edit AnyConnect Connection Profile** 窗口中，展开左侧导航窗格中的 **Advanced** 节点，然后选择 **Group Alias / Group URL**。
- 步骤 4 选中 **Enable the display of SecurID messages on the login screen**。
- 步骤 5 点击 **OK**。
- 步骤 6 选择 **Configuration > Remote Access VPN > AAA/Local Users > AAA Server Groups**。
- 步骤 7 点击 **Add** 以添加 AAA 服务器组。
- 步骤 8 在 **Edit AAA Server Group** 对话框中配置 AAA 服务器组，然后点击 **OK**。
- 步骤 9 在 **AAA Server Groups** 区域，选择您刚刚创建的 AAA 服务器组，然后点击 **Servers in the Selected Group** 区域中的 **Add**。
- 步骤 10 在 SDI 消息区域中，展开 **Message Table** 区域。双击消息文本字段以编辑消息。在 ASA 上配置 RADIUS 回复消息文本以匹配（全部或部分）RADIUS 服务器发送的消息文本。  
下表显示消息代码、默认 RADIUS 回复消息文本和每个消息的功能：

**注释** ASA 使用的默认消息文本是思科安全访问控制服务器 (ACS) 使用的默认消息文本。如果您使用思科安全 ACS，且它使用默认消息文本，则您无需在 ASA 上配置消息文本。

由于安全设备按字符串在表中显示的顺序搜索字符串，因此您必须确保用于消息文本的字符串不是另一字符串的子集。例如，“new PIN”是 new-pin-sup 和 next-ccode-and-reauth 的默认消息文本的子集。如果您将 new-pin-sup 配置为“new PIN”，则当安全设备从 RADIUS 服务器收到“new PIN with the next card code”时，它将此文本与 new-pin-sup 代码（而不是 next-ccode-and-reauth 代码）匹配。

消息代码	默认的 RADIUS 回复消息文本	功能
next-code	Enter Next PASSCODE	表示用户必须输入下一个令牌代码，无需 PIN。
new-pin-sup	请牢记您的新 PIN	指示已提供新系统 PIN 并显示用户的此 PIN。
new-pin-meth	您是否要输入自己的 PIN	来自于用户要使用哪个新 PIN 方法创建新 PIN 的请求
new-pin-req	输入新的思科 Alpha-Numerical PIN。	表示用户生成的 PIN 和要求用户输入 PIN。
new-pin-reenter	重新输入 PIN:	在内部由 ASA 用于确认用户提供的 PIN。客户端确认 PIN 而不提示用户。
new-pin-sys-ok	接受新 PIN	表示已接受用户提供的 PIN。
next-ccode-and-reauth	具有下一个卡代码的新 PIN	遵循 PIN 操作，表示用户必须等待下一个令牌代码并输入新 PIN 和下一个令牌代码才能进行身份验证。
ready - for - sys - PIN	接受系统生成的 PIN	在内部由 ASA 用于表示用户已为系统生成的 PIN 做好准备。

**步骤 11** 点击 **OK**，然后点击 **Apply**，再点击 **Save**。





## 第 5 章

# 配置网络访问管理器

本章提供网络访问管理器的配置概述以及添加和配置用户策略和网络配置文件的说明。

- [关于网络访问管理器，第 137 页](#)
- [网络访问管理器部署，第 139 页](#)
- [网络访问管理器配置文件，第 140 页](#)

## 关于网络访问管理器

网络访问管理器是依据其策略提供安全第 2 层网络的客户端软件。可检测并选择最佳第 2 层接入网络并对有线和无线网络的访问执行设备身份验证。网络访问管理器对安全访问所需的用户及设备身份和网络访问协议进行管理。智能化地工作可防止最终用户进行违反管理员定义的策略的连接。



注释

网络访问管理器在 Mac OS X 或 Linux 上不支持。可使用 AnyConnect ISE 终端安全评估来支持它，且必须在 AnyConnect ISE 终端安全评估启动之前进行安装。

Cisco AnyConnect 安全移动客户端的网络访问管理器组件支持以下主要功能：

- 有线 (IEEE 802.3) 和无线 (IEEE 802.11) 网络适配器。
- 搭配 Windows 7 的多种移动宽带 (3G) 网络适配器。（需要支持 Microsoft 移动宽带 API 的 WAN 适配器。）
- 使用 Windows 机器凭证的登录前身份验证。
- 使用 Windows 登录凭证的单点登录用户身份验证。
- 简化的 IEEE 802.1X 配置。
- IEEE MACsec 有线加密和企业策略控制。
- EAP 方法：

EAP-FAST、PEAP、EAP-TTLS、EAP-TLS 和 LEAP（EAP-MD5、EAP-GTC 和仅用于 IEEE 802.3 有线的 EAP-MSCHAPv2）。

- 内部 EAP 方法：

PEAP - EAP-GTC、EAP-MSCHAPv2 和 EAP-TLS。

EAP-TTLS - EAP-MD5 和 EAP-MSCHAPv2 和传统方法（PAP、CHAP、MSCHAP 和 MSCHAPv2）。

EAP-FAST - GTC、EAP-MSCHAPv2 和 EAP-TLS。

- 加密模式 - 静态 WEP（打开或共享）、动态 WEP、TKIP 和 AES。
- 密钥建立协议 - WPA、WPA2/802.11i。
- AnyConnect 在以下环境中支持提供智能卡的凭证：
  - Windows 中的 Microsoft CAPI 1.0 和 CAPI 2.0 (CNG)。
  - Windows 登录不支持 ECDSA 证书；因此，网络访问管理器单点登录 (SSO) 不支持 ECDSA 客户端证书。

## 套件 B 和 FIPS

以下功能经过 FIPS 认证，并且列出了所有例外：

- ACS 和 ISE 不支持 Suite B，但具有 OpenSSL 1.x 的 FreeRADIUS 2.x 支持 Suite B。Microsoft NPS 2008 部分支持 Suite B（NPS 证书仍必须是 RSA）。
- 802.1X/EAP 只支持过渡性 Suite B 配置文件（如 RFC 5430 中定义）。不支持 TLS 1.2。
- MACsec 在 Windows 7 上与 FIPS 兼容。
- 在 Windows 7 上支持 Elliptic Curve Diffie-Hellman (ECDH) 密钥交换。
- 在 Windows 7 上支持 ECDSA 客户端证书。
- 在 Windows 7 上支持操作系统存储区中的 ECDSA CA 证书。
- 在 Windows 7 上支持网络配置文件中的 ECDSA CA 证书（PEM 编码）。
- 在 Windows 7 上支持服务器的 ECDSA 证书链验证。

## 单点登录“单一用户”实施

Microsoft Windows 允许多名用户同时登录，但 Cisco AnyConnect 网络访问管理器将网络身份验证仅限于对单一用户执行。无论有多少用户登录，AnyConnect 网络访问管理器都在每个桌面或每台服务器上为一位用户保持活动状态。单用户登录实施意味着只有一位用户可以随时登录到系统，并且管理员无法强制当前登录的用户注销。

如果网络访问管理器客户端模块安装在 Windows 桌面上，系统的默认行为是实施单一用户登录。如果该模块安装在服务器上，默认行为是解除单一用户登录实施。但无论是哪种情况，您都可修改或添加注册表来更改默认行为。

#### 限制

- Windows 管理员无法强制注销当前登录的用户。
- 对于同一用户，支持与所连接工作站的 RDP 会话。
- 凭证格式相同才会被视为同一用户。例如，user/example 与 user@example.com 就不相同。
- 智能卡用户也必须确保 PIN 相同才会被视为同一用户。

## 配置单点登录单一用户实施

要更改 Windows 工作站或服务器处理多位用户的方式，请更改注册表中 **EnforceSingleLogon** 的值。

在 Windows 中，该注册表项是 **EnforceSingleLogon** 且与 **OverlayIcon** 项在同一注册表位置：

```
HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Authentication\Credential Providers\{B12744B8-5BB7-463a-B85E-BB7627E73002}
```

要配置一位或多位用户登录，请添加名为 **EnforceSingleLogon** 的 DWORD，并为其赋值 1 或 0。

对于 Windows：

- 1 表示仅限一个用户登录。
- 0 允许多位用户进行登录。

## 网络访问管理器部署

网络访问管理器作为 AnyConnect 的一部分进行部署。有关如何安装 AnyConnect 以及网络访问管理器和其他模块的信息，请参阅 [AnyConnect 部署概述](#)。

#### 指南

- Windows 网络状态任务托盘图标引起的困扰 - 网络访问管理器将覆盖 Windows 网络管理。因此，在安装网络访问管理器后，无法使用网络状态图标连接到网络。  
建议操作：通过在 Windows 组策略中设置 **删除网络图标** 来删除任务托盘中的 Windows 网络图标。此设置仅影响托盘图标。用户仍可以使用控制面板创建本地无线网络。
- Windows 7 的隐藏网络和网络选择 - 网络访问管理器尝试只连接在网络访问管理器网络扫描列表中配置的网络。

在 Windows 7 中，网络访问管理器会探测隐藏的 SSID。当发现第一个隐藏的 SSID 后，即停止查找。当配置了多个隐藏网络时，网络访问管理器按如下方式选择 SSID：

第一个管理员定义的隐藏公司网络。工作站的默认配置为 1；服务器的默认配置为 0。

管理员定义的隐藏网络。

第一个用户定义的隐藏网络。由于网络访问管理器一次只能探测一个非广播 SSID，因此思科建议在您的站点只使用一个隐藏的公司网络。

- 网络连接短暂丢失或更长的连接时间 - 如果在安装网络访问管理器之前在 Windows 中定义了网络，Windows 连接管理器可能偶尔尝试与该网络建立连接。

建议操作：当网络在范围内时，对所有 Windows 定义的网络关闭 **Connect Automatically** 或删除所有 Windows 定义的网络。

- 当网络访问管理器模块首次安装到客户端系统时，该模块可以配置为将一些现有 Windows 7 或更高版本无线配置文件转换为网络访问管理器配置文件格式。可以转换匹配以下条件的基础设施网络：

- 开放
- 静态 WEP
- WPA/WPA2 个人
- 只转换非 GPO 本地 Wi-Fi 用户网络配置文件。
- 在配置文件转换期间，系统上必须运行 WLAN 服务。
- 如果网络访问管理器 XML 配置文件已存在 (userConfiguration.xml)，则不会进行转换。

要启用网络配置文件转换，请创建一个 MSI 转换将 PROFILE\_CONVERSION 属性值设置为 1，然后将其应用到 MSI 包。或者在命令行中将 PROFILE\_CONVERSION 属性更改为 1，然后安装 MSI 包。例如，`msiexec /i anyconnect-nam-win-3.1.xxxxx-k9.msi PROFILE_CONVERSION=1`。

- 必须先安装网络访问管理器，再启动 ISE 终端安全评估。ISE 终端安全评估使用网络访问管理器插件检测网络更改事件和 802.1x WiFi。

## 网络访问管理器配置文件

网络访问管理器配置文件在网络访问管理器配置文件编辑器中进行配置，后者在 ASDM 中提供，也可以作为独立的 Windows 应用。

### Client Policy 窗口

Client Policy 窗口可用于配置客户端策略选项。包括以下部分：

#### Connection Settings

可用于定义是在用户登录之前还是之后尝试建立网络连接。

- **Default Connection Timeout** - 用作用户创建的网络的连接超时秒数。默认值是 40 秒。

- **Before User Logon** - 在用户登录之前连接网络。支持的用户登录类型包括用户帐户 (Kerberos) 身份验证, 加载用户 GPO 和执行基于 GPO 的登录脚本。如果选择了 Before User Logon, 您还可以设置 *Time to Wait Before Allowing a User to Logon*。
- **Time to wait before allowing user to Logon** - 指定等待网络访问管理器建立完整网络连接的最大秒数 (最坏情况)。如果无法在此时间内建立网络连接, 则 Windows 登录进程继续进行用户登录。默认值为 5 秒。



**注释** 如果网络访问管理器配置为管理无线连接, 则必须将 **Time to wait before allowing user to logon** 设置为 30 秒或更长时间, 因为可能还要额外花时间来建立无线连接。您还应该考虑到通过 DHCP 获取 IP 地址所需的时间。如果配置了两个或更多网络配置文件, 您应该增大此值以涵盖两次或更多次连接尝试。

- **After User Logon** - 在用户登录到 Windows 之后连接网络。

## Media

指定哪些类型的媒体由网络访问管理器客户端控制。

- **Manage Wi-Fi (wireless) Media** - 启用 Wi-Fi 媒体的管理和 WPA/WPA2 握手的验证 (可选)。IEEE 802.11i 无线网络标准指定请求方 (在本例中是网络访问管理器) 必须验证接入点的 RSN IE (即稳健的安全网络信息交换)。IE 是在密钥派生期间放在 IEEE 801.X 协议数据包的 EAPOL 密钥数据中发送的, 它应该与信标/探针响应帧中接入点的 RSN IE 匹配。
- **Enable validation of WPA/WPA2 handshake** - 验证 WPA/WPA2 握手。如果未选中, 则跳过此可选验证步骤。



**注释** 某些适配器并不一直提供接入点的 RSN IE, 因此身份验证尝试失败, 客户端将无法连接。

- **Default Association Timeout** (秒) - 如果启用 WPA/WPA2 握手, 则必须指定默认关联超时。
- **Manage Wired (IEEE 802.3) Media** - 启用有线连接的管理。
- **Manage Mobile Broadband (3G) Media** - 启用 Windows 7 移动宽带适配器的管理。此功能默认为已禁用。



**注释** 此功能处于试用版本状态。思科 TAC 对试用版本不提供支持。

- **Enable Data Roaming** - 确定是否允许数据漫游。

## End-user Control

可以为用户配置以下控制:

- **Disable Client** - 允许用户禁用和启用使用 AnyConnect UI 进行网络访问管理器的有线和无线媒体管理。
- **Display user groups** - 让用户创建的组（从 CSSC 5.x 创建）可见且能够连接，即使它们并不是管理员定义的组也是如此。
- **Specify a script or application to run when connected** - 允许用户指定网络连接时运行的脚本或应用。



## 注释

脚本设置特定于一个用户配置的网络，并允许用户指定当该网络处于连接状态时运行的本地文件（.exe、.bat 或 .cmd）。为避免冲突，此脚本功能允许用户只为用户定义的网络（而不为管理员定义的网络）配置脚本或应用。此功能不允许用户就脚本运行而更改管理员网络；因此，管理员网络界面对用户不可用。此外，如果不允许用户配置正在运行的脚本，则此功能不会出现在网络访问管理器 GUI 中。

- **Auto-connect** - 自动连接到一个网络，无需用户选择它。默认值为自动连接。

### Administrative Status

- **Service Operation** - 如果关闭服务，则使用此配置文件的客户端将无法连接以建立第二层连接。
- **FIPS Mode** - 如果启用 FIPS 模式，则网络访问管理器以符合政府要求的方式执行密码操作。

联邦信息处理标准（FIPS 140-2 级别 1）是指定加密模块的安全要求的美国政府标准。根据软件和硬件的类型，FIPS 由面向 MACsec 或 Wi-Fi 的网络访问管理器支持。

表 8: 网络访问管理器的 FIPS 支持

媒体/操作系统	Windows 7
MACsec 有线网络	当使用支持 MACsec 的英特尔硬件 NIC 或任何非硬件 MACsec 时，都符合 FIPS。
Wi-Fi	不兼容的 FIPS

## Authentication Policy 窗口

Authentication Policy 窗口可用于创建关联和身份验证网络过滤器，这些过滤器适用于所有网络连接。如果未选中任何关联或身份验证模式，则用户无法连接到身份验证 Wi-Fi 网络。如果选择了模式的子集，则用户仅能连接到这些类型的网络。选择每个所需的关联或身份验证模式，或者选择 **Select All**。

内部方法也可以仅限于特定的身份验证协议。内部方法缩进显示在 Allowed Authentication Modes 窗格中外部方法（隧道）的下面。

选择身份验证协议的机制与当前客户端身份验证数据库集成在一起。安全无线局域网部署不要求为用户创建新的身份验证系统。

对内部隧道可用的 EAP 方法取决于内部方法凭证类型和外部隧道方法。在以下列表中，每个外部隧道方法都列出了针对每种凭证类型受支持的内部方法类型。

- PEAP

- 密码凭证：EAP-MSCHAPv2 或 EAP-GTC

- 令牌凭证：EAP-GTC

- 证书凭证：EAP-TLS

- EAP-FAST

- 密码凭证：EAP-MSCHAPv2 或 EAP-GTC

- 令牌凭证：EAP-GTC

- 证书凭证：EAP-TLS

- EAP-TTLS

- 密码凭证：EAP-MSCHAPv2、EAP-MD5、PAP（传统）、CHAP（传统）、MSCHAP（传统）、MSCHAP-v2（传统）

- 令牌凭证：PAP（传统）。网络访问管理器支持的默认令牌选项是 PAP，因为质询/响应方法并不是很适合基于令牌的身份验证。

- 证书凭证：不适用

## Networks 窗口

Networks 窗口可用于为企业用户配置预定义的网络。您可以配置对所有组可用的网络，或创建具有特定网络的组。Networks 窗口显示向导，可将窗格添加到现有窗口中，并且可让您通过点击 **Next** 访问更多配置选项。

从根本上说，组是一套配置的连接（网络）。每个已配置的连接必须属于某个组，或者是所有组的成员。



### 注释

为向后兼容，使用思科安全服务客户端部署的由管理员创建的网络被视为隐藏的网络，不广播 SSID。但是，用户网络被视为广播 SSID 的网络。

只有管理员可以创建新组。如果配置中未定义组，配置文件编辑器会创建一个自动生成的组。自动生成的组中包含未分配到任何管理员定义的组的网络。客户端尝试使用在活动组中定义的连接创建

网络连接。根据 Network Groups 窗口中 **Create Networks** 选项的设置，最终用户可以将用户网络添加到活动组，或者从活动组删除用户网络。

定义的网络可用于列表顶部的所有组。因为您控制哪些网络位于全球网络中，所以您可以指定最终用户能够连接的网络，即使存在用户定义的网络也一样。最终用户无法修改或删除管理员配置的网络。



注释

最终用户可以将网络添加到组，但全球网络部分的网络除外，因为这些网络存在于所有组中，只能使用配置文件编辑器创建。

企业网络的典型最终用户不需要了解组即可使用此客户端。活动组是配置中的第一个组，但如果只有一个组可用，客户端不会知道活动组，也不会显示活动组。但是，如果存在多个组，用户界面会显示组的列表，并且指示活动组已选中。然后，用户可以从活动组中选择，重启后该设置也保持不变。根据 Network Groups 窗口中 **Create Networks** 选项的设置，最终用户无需使用组即可添加或删除自己的网络。



注释

组选择在重启和网络修复（右键点击托盘图标并选择 **Network Repair** 来完成）后保持不变。网络访问管理器在修复或重新启动时，会开始使用以前的活动组。

## Networks 窗口的 Media Type 页面

您可以在 Networks 窗口的 Media Type 页面中创建或编辑有线或无线网络。设置随您的具体选择而不同。

第一个对话框中包括以下部分：

- Name - 输入将为该网络显示的名称。
- Group Membership - 选择此配置文件应该对哪些网络组或组可用。
- Network Media - 选择有线或 Wi-Fi（无线）。如果选择 Wi-Fi，您还可以配置以下参数：

SSID - 输入您的无线网络的 SSID（服务集标识符）。

Hidden Network - 允许连接到网络，即使它不广播其 SSID。

Corporate Network - 如果附近有企业网络，强制将网络连接首先配置为 Corporate。当企业网络使用非广播（隐藏）SSID 并且配置为隐藏时，网络访问管理器会主动寻找隐藏的 SSID，并且当有企业 SSID 在范围内时建立连接。

Association Timeout - 输入网络访问管理器在重新评估可用网络之前等待与特定无线网络相关联的时长。默认的关联超时为 5 秒。

- 常用设置

Script or application - 输入将在本地系统中运行的文件的路径和文件名，或者浏览文件夹并选择一个文件。以下规则适用于脚本和应用：



接受扩展名为 .exe、.bat 或 .cmd 的文件。

用户不得更改管理员创建的网络中定义脚本或应用。

您可以使用配置文件编辑器仅指定路径和脚本或应用的文件名。如果脚本或应用不存在于用户的机器上，将会显示一条错误消息。用户获通知，脚本或应用不存在于其机器上，并且需要联系系统管理员。

您必须指定要运行的应用的完整路径，除非应用存在于用户的路径中。如果应用存在于用户的路径中，您可以仅指定应用或脚本的名称。

Connection Timeout - 输入网络访问管理器尝试连接到其他网络（当连接模式为自动时）或者使用另一个适配器之前等待建立网络连接的秒数。



注释

某些智能卡身份验证系统需要近 60 秒才能完成身份验证。使用智能卡时，您应增加 Connection Timeout 值，尤其是当智能卡可能必须尝试几个网络才能连接成功时。

## Networks 窗口的 Security Level 页面

在 Networks 向导的 Security Level 页面中，选择 Open Network、Authentication Network 或（仅为无线网络介质显示的）Shared Key Network。每种网络类型的配置流程都不同，在以下各节进行说明。

- [配置身份验证网络](#) - 建议用于安全企业。
- [配置开放网络](#) - 不推荐，但是可用于通过强制网络门户环境提供访客接入。
- [配置共享密钥网络](#) - 建议用于小型办公室或家庭办公室等无线网络。

### 配置身份验证网络

如果您在 Security Level 部分选择 Authenticating Network，将显示额外的窗格，如下所述。在这些窗格中完成配置后，请点击 **Next** 按钮，或选择 **Connection Type** 选项卡打开 Network Connection Type 对话框。

#### 802.1X Settings 窗格

根据网络配置调整 IEEE 802.1X 设置：



注释

当 AnyConnect ISE 终端安全评估安装了网络访问管理器时，ISE 终端安全评估使用网络访问管理器插件检测到网络更改事件和 802.1X WiFi。

- **authPeriod** (秒) - 身份验证开始时，此设置将确定在身份验证消息超时之前请求方等待的时长，该时间过后需要验证方重新发起身份验证。
- **heldPeriod** (秒) - 身份验证失败时，此设置定义请求方等待多长时间后才能发出另一次身份验证尝试。
- **startPeriod** (秒) - 没有从验证方收到对 EAPOL-Start 消息的任何响应时，再次传输 EAPOL-Start 消息之间的时间间隔 (秒)。
- **maxStart** - 请求方通过发送 IEEE 801.X 协议数据包、EAPOL 密钥数据或 EAPoL-Start，向验证方发起身份验证的次数，达到此次数后，请求方会假定没有验证方。此时，请求方允许数据流量。



## 提示

您可以仔细设置 **startPeriod** 和 **maxStart**，使发起身份验证所花的总时间小于网络连接计时器时间 ( $\text{startPeriod} \times \text{maxStart} < \text{网络连接计时器时间}$ )，配置单一身份验证有线连接以同时支持开放网络和身份验证网络。

请注意，在这种情况下，您应将网络连接计时器时间增加 ( $\text{startPeriod} \times \text{maxStart}$ ) 秒，让客户端有足够的时间获取 DHCP 地址和完成网络连接。

相反，若要仅在身份验证成功后才允许数据流量，您应该设置 **startPeriod** 和 **maxStart**，确保发起身份验证所花的总时间大于网络连接计时器时间 ( $\text{startPeriod} \times \text{maxStart} > \text{网络连接计时器时间}$ )。

## Security 窗格

仅为有线网络显示。

在 Security 窗格中，选择以下参数的值：

- **Key Management** - 确定哪个密钥管理协议用于启用 MACsec 的有线网络。
  - None - 没有使用密钥管理协议，并且不执行有线加密。
  - MKA - 请求方尝试协商 MACsec 密钥管理协议策略和加密密钥。MACsec 是 MAC 层安全，在有线网络上提供 MAC 层加密。MACsec 协议采用加密手段来保护 MAC 层帧，依靠 MACsec 密钥协议 (MKA) 实体进行协商并分发加密密钥。
- **加密**
  - None - 对数据流量执行完整性检查，但不加密。
  - MACsec: AES-GCM-128 - 仅当选择 MKA 进行密钥管理时，此选项才可用。它会使用 AES-GCM-128 对数据流量进行加密。

有关详细信息，请参阅[基于身份的网络服务：MAC 安全](#)。

## Port Authentication Exception Policy 窗格

此窗格仅为有线网络显示。

Port Authentication Exception Policy 窗格可让您在身份验证过程中定制 IEEE 802.1X 请求方的行为。如果端口异常未启用，请求方会继续其现有行为并仅在成功完成完整配置后（或如此部分之前所述，发起身份验证的 maxStarts 数量而没有验证器响应之后）才会打开端口。选择以下其中一个选项：

- 在身份验证前允许数据流量通过 - 在身份验证尝试之前允许数据流量通过。
- 在身份验证之后允许数据流量通过，即使：

EAP 失败 - 选择后，请求方尝试身份验证。如果身份验证失败，请求方在身份验证失败的情况下依然允许数据流量通过。

EAP 成功，但密钥管理失败 - 选择后，请求方尝试与密钥服务器就密钥进行协商，但在密钥协商因任何原因失败的情况下依然允许数据流量通过。此设置仅在已配置密钥管理的情况下有效。如果密钥管理设置为无，则复选框以灰色显示。



### 限制

MACsec 需要 ACS 版本 5.1 及更高版本和支持 MACsec 的交换机。请参阅《Catalyst 3750-X 和 3560-X 交换机软件配置指南》以了解 ACS 或交换机配置。

## 关联模式

该窗格仅对无线网络显示。

选择关联模式：

- WEP
- WAP Enterprise (TKIP)
- WPA Enterprise (AES)
- WPA 2 Enterprise (TKIP)
- WPA 2 Enterprise (AES)
- CCKM (TKIP) - (需要思科 CB21AG 无线网卡)
- CCKM (AES) - (需要思科 CB21AG 无线网卡)

## 配置开放网络

开放网络不使用身份验证或加密。如果要创建开放（非安全）网络，请执行以下步骤。

## 过程

- 步骤 1 从 Security Level 页面选择 **Open Network**。此选择提供的网络安全性最低，建议用于访客接入无线网络。
- 步骤 2 点击 **Next**。
- 步骤 3 确定连接类型。

## 配置共享密钥网络

Wi-Fi 网络可使用共享密钥获得加密密钥，用于在终端之间和网络接入点之间对数据加密。配合 WPA 或 WPA2 Personal 使用共享密钥，可提供中等级别的安全性，适合于小型或家庭办公室。



注释 不建议对企业无线网络使用共享密钥安全性。

如果要将共享密钥网络作为您的安全级别，请执行以下步骤。

## 过程

- 步骤 1 选择 **Shared Key Network**。
- 步骤 2 在 Security Level 窗口中点击 **Next**。
- 步骤 3 指定 **User Connection** 或 **Machine Connection**。
- 步骤 4 点击 **Next**。
- 步骤 5 **Shared Key Type** - 指定共享密钥关联模式，用于确定共享密钥类型。选项如下所示：
  - WEP - 与静态 WEP 加密关联传统 IEEE 802.11 开放系统。
  - Shared - 与静态 WEP 加密关联传统 IEEE 802.11 共享密钥。
  - WPA/WPA2-Personal - 一种 Wi-Fi 安全协议，用于从密码预共享密钥 (PSK) 获得加密密钥。
- 步骤 6 如果选择了传统 IEEE 802.11 WEP 或共享密钥，请选择 40 位、64 位、104 位或 128 位。40 位或 64 位 WEP 密钥必须是 5 个 ASCII 字符或 10 个十六进制数字。104 位或 128 位 WEP 密钥必须是 13 个 ASCII 字符或 26 个十六进制数字。
- 步骤 7 如果选择了 WPA 或 WPA2 Personal，请选择要使用的加密类型 (TKIP/AES)，然后输入共享密钥。输入的密钥必须为 8 到 63 个 ASCII 字符或正好 64 个十六进制数字。如果共享密钥由 ASCII 字符组成，请选择 **ASCII**。如果共享密钥包含 64 个十六进制数字，请选择 **Hexadecimal**。
- 步骤 8 点击 **Done**。然后点击 **OK**。

## Networks, Network Connection Type 窗格

本节介绍 Networks 窗口的网络连接类型窗格，该窗格遵循网络访问管理器配置文件编辑器中的安全级别。选择以下连接类型之一：

- **Machine Connection** - 存储在 Windows Active Directory 中的设备名称用来进行授权。计算机连接通常用于无需用户凭证进行连接的情况。即使用户已注销且用户凭证不可用，如果终端站应登录到网络，也请选择此选项。此选项通常用于在用户获得访问权限之前连接域并从网络获得 GPO 和其他更新。



**注释** 如果没有可用的已知网络，VPN 登录前启动 (SBL) 会失败。如果为 Before User Logon 和计算机连接授权配置网络访问管理器，网络访问管理器将要求用户提供网络信息，并且 VPN SBL 成功启动。

- **User Connection** - 用户凭证用于进行授权。

如果在 Client Policy 窗格中选择了 Before User Logon，则用户在 Windows 开始屏幕中输入登录凭证后，网络访问管理器会收集用户的凭证。在 Windows 启动用户的 Windows 会话时，网络访问管理器会建立网络连接。

如果在 Client Policy 窗格中选择了 After User Logon，则用户登录到 Windows 后，网络访问管理器才启动连接。

用户注销后，当前用户网络连接即终止。如果计算机网络配置文件可用，NAM 会重新连接到计算机网络。

- **Machine and User Connection** - 仅在配置网络身份验证时可用，如在 Security Level 窗格中所选。计算机 ID 和用户凭证均使用，但仅当用户未登录到设备时，计算机部分才有效。这两部分的配置是相同的，但是，计算机连接的身份验证类型和凭证可能与用户连接的身份验证类型和凭证不同。

当用户未登录时，选择此选项可始终通过计算机连接将 PC 连接到网络；当用户已登录时，选择此选项可始终通过用户连接将 PC 连接到网络。

在 EAP-FAST 配置为 EAP 方法（在下一个窗格中）时，支持 EAP 链接。这意味着网络访问管理器会确认计算机和用户为已知实体并且由公司管理。

当您选择网络连接类型时，Networks 对话框中会显示其他选项卡。使用这些选项卡，可为所选网络连接类型设置 EAP 方法和凭证。

## Networks, User or Machine Authentication 页面

在选择网络连接类型后，选择这些连接类型的身份验证方法。在选择身份验证方法后，显示屏幕会更新为选择的方法，并要求您提供其他信息。



注释

如果您已启用 MACsec，请确保选择支持 MSK 密钥派生的 EAP 方法，例如 PEAP、EAP-TLS 或 EAP-FAST。此外，即使没有启用 MACsec，使用网络访问管理器也可将 MTU 从 1500 降低至 1468 以支持 MACsec。

## EAP 概述

EAP 是一种 IETF RFC，可满足身份验证协议与承载它的传输协议进行分离的要求。此分离允许传输协议（如 IEEE 802.1X、UDP 或 RADIUS）承载 EAP 协议，而无需更改身份验证协议。

基本 EAP 协议包括四种数据包类型：

- EAP 请求 - 身份验证器向请求方发送请求数据包。每个请求都有一个类型字段，用于指示请求内容，如请求方身份和要使用的 EAP 类型。顺序号允许身份验证器和对等项将 EAP 响应与各个 EAP 请求进行匹配。
- EAP 响应 - 请求方向身份验证器发送响应数据包并使用顺序号与启动的 EAP 请求进行匹配。EAP 响应的类型通常匹配 EAP 请求，除非响应为负 (NAK)。
- EAP 成功 - 身份验证成功后，身份验证器向请求方发送成功数据包。
- EAP 失败 - 如果身份验证失败，身份验证器向请求方发送失败数据包。

在 IEEE 802.11X 系统中使用 EAP 时，接入点在 EAP 穿透模式下工作。在此模式下，接入点检查代码、标识符和长度字段，然后将从请求方收到的 EAP 数据包转发至 AAA 服务器。从 AAA 服务器身份验证器接收的数据包将转发到请求方。

## EAP-GTC

EAP-GTC 是基于简单用户名和密码身份验证的 EAP 身份验证方法。不使用质询响应方法，用户名和密码均以明文传递。建议在隧道 EAP 方法内部（请参阅下面的隧道 EAP 方法）或针对一次性密码 (OTP) 使用此方法。

EAP-GTC 不提供相互身份验证。它只对客户端进行身份验证，因此欺诈服务器可能会获取用户的凭证。如果需要相互身份验证，则在隧道 EAP 方法内部使用 EAP-GTC，这样可提供服务器身份验证。

EAP-GTC 未提供密钥材料；因此，不能对 MACsec 使用此方法。如果进一步的流量加密需要密钥材料，则在隧道 EAP 方法内使用 EAP-GTC，这样可提供密钥材料（如有必要，还提供内部和外部 EAP 方法加密绑定）。

有两个密码源选项：

- 使用密码进行身份验证 - 只适用于有良好保护的有线环境
- 使用令牌进行身份验证 - 更安全，因为令牌代码或 OTP 的生命期较短（通常约为 10 秒）



注释

网络访问管理器、身份验证器和 EAP-GTC 协议均无法区分密码和令牌代码。这些选项只影响网络访问管理器中凭证的生命期。虽然可在注销前或更长时间内记住密码，但不能记住令牌代码（因为每次身份验证时都提示用户输入令牌代码）。

如果使用密码进行身份验证，可以使用此协议对照包含哈希值密码的数据库进行身份验证，因为密码以明文传递到身份验证器。如果存在数据库泄露的可能，建议使用此方法。

## EAP-TLS

EAP 传输层安全 (EAP-TLS) 是基于 TLS 协议 (RFC 2246) 的 IEEE 802.1X EAP 身份验证算法。TLS 使用基于 X.509 数字证书的相互身份验证。EAP-TLS 消息交换提供相互身份验证、加密套件协商、密钥交换、客户端与身份验证服务器之间的身份验证以及可用于流量加密的密钥材料。

下面的列表提供了 EAP-TLS 客户端证书可为有线和无线连接提供强身份验证的主要原因：

- 身份验证自动进行，通常无需用户干预。
- 不存在对用户密码的依赖性。
- 数字证书提供强身份验证保护。
- 使用公共密钥加密保护消息交换。
- 证书不易受字典攻击。
- 身份验证过程会为数据加密和签名生成相互确定的密钥。

EAP-TLS 包含两个选项：

- **Validate Server Certificate** - 启用服务器证书验证。
- **Enable Fast Reconnect** - 启用 TLS 会话恢复，只要 TLS 会话数据同时保存在客户端和服务器上，就允许使用简短的 TLS 握手进行快得多的重新身份验证。



注释

对于计算机连接身份验证，**Disable When Using a Smart Card** 选项不可用。

## EAP-TTLS

EAP 隧道传输层安全 (EAP-TTLS) 是扩展 EAP-TLS 功能的两阶段协议。第 1 阶段执行完整 TLS 会话，并生成用于在第 2 阶段安全地在服务器与客户端之间隧道化属性的会话密钥。您可以使用在第 2 阶段隧道化的属性通过多种不同机制执行其他身份验证。

网络访问管理器不支持在 EAP-TTLS 身份验证期间使用的内部和外部方法加密绑定。如果需要加密绑定，则必须使用 EAP-FAST。加密绑定可防御特殊类别的中间人攻击，在这类攻击中，攻击者无需知道凭证就可以劫持用户的连接。

可以在第 2 阶段使用的身份验证机制包括以下协议：

- PAP（密码验证协议）- 使用双向握手为对等项提供证明其身份的简单方法。对等项向身份验证器重复发送 ID/密码对，直至身份验证确认或失败。如果需要相互身份验证，必须将 EAP-TTLS 配置为在第 1 阶段验证服务器证书。

由于密码传递到身份验证器，您可以使用此协议对照包含哈希值密码的数据库进行身份验证。如果存在数据库泄露的可能，建议使用此方法。



**注释** 可以使用 EAP-TTLS PAP 进行基于令牌和基于 OTP 的身份验证。

- CHAP（质询握手身份验证协议）- 使用三次握手验证对等项的身份。如果需要相互身份验证，应将 EAP-TTLS 配置为在第 1 阶段验证服务器证书。使用此质询响应方法，需要在身份验证器的数据库中存储明文密码。
- MS-CHAP (Microsoft CHAP) - 使用三次握手验证对等项的身份。如果需要相互身份验证，应将 EAP-TTLS 配置为在第 1 阶段验证服务器证书。使用这个基于密码的 NT 哈希值的质询响应方法，需要在身份验证器的数据库中存储明文密码或至少存储密码的 NT 哈希值。
- MS-CHAPv2 - 通过在响应数据包中包含对等项质询以及在成功数据包中包含身份验证器响应来提供对等项之间的相互身份验证。先对客户端、再对服务器进行身份验证。如果服务器需要先于客户端进行身份验证（以防御字典攻击），应该将 EAP-TTLS 配置为在第 1 阶段验证服务器证书。使用这个基于密码的 NT 哈希值的质询响应方法，需要在身份验证器的数据库中存储明文密码或至少存储密码的 NT 哈希值。

## 配置 EAP-TTLS

- EAP - 允许使用以下 EAP 方法之一：

EAP-MD5 (EAP Message Digest 5) - 使用三向握手来验证对等体的身份（类似于 CHAP）。使用这种质询-响应方法，需要在验证方的数据库中存储明文密码。

EAP-MSCHAPv2 - 使用三次握手验证对等体的身份。先对客户端、再对服务器进行身份验证。如果对服务器的身份验证需要先于客户端（例如为防止字典攻击），则应配置 EAP-TTLS 以在第 1 阶段验证服务器的证书。对 NT 哈希值形式的密码使用这种质询-响应方法时，需要在验证方的数据库中存储明文密码或至少 NT 哈希值形式的密码。

- EAP-TTLS 设置

Validate Server Identity - 启用服务器证书验证。





**注释** 如果启用此选项，请确保在 RADIUS 服务器上安装的服务器证书中包含服务器身份验证的扩展密钥用法 (EKU)。当 RADIUS 服务器在身份验证期间将其配置的证书发送到客户端时，必须对网络访问和身份验证使用此服务器身份验证设置。

**Enable Fast Reconnect** - 只启用外部 TLS 会话恢复，而不管内部身份验证是跳过还是由验证方控制。



**注释** **Disable When Using a Smart Card** 不适用于机器连接身份验证。

- **Inner Methods** - 指定在 TLS 隧道创建后使用的内部方法。仅适用于 Wi-Fi 媒体类型。

## PEAP 选项

受保护的 EAP (PEAP) 是基于隧道 TLS 的 EAP 方法。它在客户端身份验证之前使用 TLS 进行服务器身份验证，以加密内部身份验证方法。内部身份验证在受信任加密保护的隧道内进行，支持多种不同的内部身份验证方法，包括证书、令牌和密码。网络访问管理器不支持在 PEAP 身份验证期间使用的内部和外部方法加密绑定。如果需要加密绑定，则必须使用 EAP-FAST。加密绑定可防御特殊类别的中间人攻击，在这类攻击中，攻击者无需知道凭证就可以劫持用户的连接。

PEAP 通过提供以下服务保护 EAP 方法：

- 为 EAP 数据包创建 TLS 隧道
- 消息身份验证
- 消息加密
- 服务器到客户端的身份验证

可以使用以下身份验证方法：

- 使用密码进行身份验证

**EAP-MSCHAPv2** - 使用三次握手验证对等体的身份。先对客户端、再对服务器进行身份验证。如果服务器需要先于客户端进行身份验证（如为了防御字典攻击），则必须配置 PEAP 以验证服务器的证书。使用基于密码的 NT 哈希值的质询响应方法，需要在身份验证器数据库中存储明文密码或至少存储密码的 NT 哈希值。

**EAP-GTC (EAP 通用令牌卡)** - 定义 EAP 信封以承载用户名和密码。如果需要相互身份验证，则必须配置 PEAP 以验证服务器的证书。由于密码以明文传递到身份验证器，可以使用此协议对照包含哈希值密码的数据库进行身份验证。如果存在数据库泄露的可能，建议使用此方法。

- **EAP-TLS**，使用证书

EAP-TLS- 定义 EAP 信封以承载用户证书。为避免中间人攻击（劫持有效用户的连接），建议不要将 PEAP (EAP-TLS) 和 EAP-TLS 配置文件混合在一起向同一身份验证器进行身份验证。应相应地配置身份验证器（不同时启用普通和隧道 EAP-TLS）。

## 配置 PEAP

### • PEAP-EAP 设置

Validate Server Identity - 启用服务器证书验证。



**注释** 如果启用此选项，请确保在 RADIUS 服务器上安装的服务器证书中包含服务器身份验证的扩展密钥用法 (EKU)。当 RADIUS 服务器在身份验证期间将其配置的证书发送到客户端时，必须对网络访问和身份验证使用此服务器身份验证设置。

Enable Fast Reconnect - 仅启用外部 TLS 会话恢复。验证器控制是否跳过内部身份验证。

Disable when using a smart card - 在使用智能卡进行身份验证时，请勿使用“快速重新连接”。智能卡仅适用于用户连接。

Authenticate using a token and EAP GTC - 对计算机身份验证不可用。

### • 基于凭证源的内部方法

使用 EAP-MSCHAPv2 和/或 EAP-GTC 的密码进行身份验证。

EAP-TLS，使用证书进行身份验证。

使用令牌和 EAP-GTC 进行身份验证 - 对计算机身份验证不可用。



**注释** 在用户登录之前，智能卡支持在 Windows 上不可用。

## EAP-FAST 设置

EAP-FAST 是 IEEE 802.1X 身份验证类型，可提供简单灵活的部署和管理。它支持多种用户和密码数据库类型、服务器发起的密码过期和更改以及数字证书（可选）。

EAP-FAST 针对想要部署 IEEE 802.1X EAP 类型的客户而开发，该类型不使用证书但可防御字典攻击。

自 AnyConnect 3.1 起，配置计算机和用户连接时均支持 EAP 链。这意味着网络访问管理器将验证计算机和用户是否为已知实体且由公司管理，这对于控制用户拥有的连接到公司网络的资产来说非常有用。有关 EAP 链的详细信息，请参阅 RFC 3748。

EAP-FAST 将 TLS 消息封装在 EAP 内，包括三个协议阶段：

- 1 调配阶段 - 使用经过身份验证的 Diffie-Hellman 协议 (ADHP) 调配具有名为保护访问凭证 (PAC) 的共享加密凭证的客户端。
- 2 隧道建立阶段 - 使用 PAC 建立隧道。
- 3 身份验证阶段 - 身份验证服务器对用户凭证（令牌、用户名/密码或数字证书）进行身份验证。

与其他隧道 EAP 方法不同，EAP-FAST 提供内部和外部方法之间的加密绑定，可防御特殊类别的中间人攻击，在这类攻击中，攻击者可劫持有效用户的连接。

## 配置 EAP-FAST

### • EAP-FAST 设置

**Validate Server Identity** - 启用服务器证书验证。启用此选项会在管理实用程序中引入两个额外的对话框，并且在网络访问管理器配置文件编辑器任务列表中添加额外的证书窗格。



注释

如果启用此选项，请确保在 RADIUS 服务器上安装的服务器证书中包含服务器身份验证的扩展密钥用法 (EKU)。当 RADIUS 服务器在身份验证期间将其配置的证书发送到客户端时，必须对网络访问和身份验证使用此服务器身份验证设置。

**Enable Fast Reconnect** - 启用会话恢复。用来在 EAP-FAST 中恢复身份验证会话的两种机制是用户授权 PAC（用于代替内部身份验证）和 TLS 会话恢复（用于允许简化的外部 TLS 握手）。此 **Enable Fast Reconnect** 参数可启用或禁用这两种机制。验证方决定具体使用哪一种机制。



注释

计算机 PAC 提供简化的 TLS 握手，无需内部身份验证。此控制通过启用/禁用 PAC 参数来处理。



注释

**Disable When Using a Smart Card** 选项仅适用于用户连接授权。

### • Inner methods based on Credentials Source - 可让您使用密码或证书进行身份验证。

使用 EAP-MSCHAPv2 或 EAP-GTC 的密码进行身份验证。EAP-MSCHAPv2 提供相互身份验证，但它先对客户端、再对服务器进行身份验证。如果要在相互身份验证中先对服务器进行身份验证，请配置 EAP-FAST 只用于经过身份验证的调配，并且验证服务器的证书。EAP-MSCHAPv2 使用基于密码的 NT 哈希值的质询-响应方法，它要求您在验证方的数据库中存储明文密码或至少 NT 哈希值形式的密码。由于密码在 EAP-GTC 中以明文形式传递给验证方，因此您可以使用此协议根据数据库进行身份验证。

如果使用基于密码的内部方法，可使用一个额外的选项来允许未经身份验证的 PAC 调配。

**Authenticate using a certificate** - 决定使用证书进行身份验证的以下条件：收到请求时，以明文形式发送客户端证书，仅在隧道内发送客户端证书，或者使用 EAP-TLS 在隧道中发送客户端证书。

使用令牌和 EAP-GTC 进行身份验证。

- **Use PACs** - 可以指定使用 PAC 进行 EAP-FAST 身份验证。PAC 是分发给客户端以优化网络身份验证的凭证。



注释

通常使用 PAC 选项，因为大多数身份验证服务器对 EAP-FAST 使用 PAC。在删除此选项之前，请验证身份验证服务器不对 EAP-FAST 使用 PAC；否则，客户端的身份验证尝试不会成功。如果身份验证服务器支持经过身份验证的 PAC 调配，思科建议您禁用未经身份验证的调配。未经身份验证的调配不验证服务器的证书，可能允许入侵者发动基于字典的攻击。

您可以选择 PAC Files 窗格并点击 **Add**，手动提供一个或多个特定的 PAC 文件进行分发和身份验证。您还可以突出显示 PAC 文件，然后点击 **Remove** 从列表中删除该 PAC 文件。

**Password protected** - 如果 PAC 已经以受密码保护的形式导出，请选中 **Password Protected** 复选框并提供与 PAC 加密密码匹配的密码。

## LEAP 设置

LEAP（轻量级 EAP）支持无线网络。它基于可扩展身份验证协议 (EAP) 框架，由思科开发，旨在创建比 WEP 更安全的协议。



注释

LEAP 容易受到字典攻击，除非实施强密码并定期使密码过期。思科建议使用 EAP-FAST、PEAP 或 EAP-TLS，它们的身份验证方法不易受字典攻击。

只能用于用户身份验证的 LEAP 设置：

- **注销后延长用户连接** - 用户注销后保持连接打开状态。如果同一用户再次登录，网络连接仍处于活动状态。

请参阅对 [Cisco LEAP 漏洞的字典攻击](#) 以了解详细信息。

## 定义网络凭证

在 Networks > Credentials 窗格中，指定是否使用用户和/或机器凭证，并且配置受信任服务器验证规则。

## 配置用户凭证

EAP 对话可能涉及多种 EAP 身份验证方法，其中每种身份验证要求的身份可能不同（例如先是计算机身份验证，然后是用户身份验证）。例如，对等项最初可能声称身份为 `nouser@cisco.com` 以将身份验证请求发送到 `cisco.com` EAP 服务器。但是，一旦已协商 TLS 会话，对等项可能声称身份为 `johndoe@cisco.com`。因此，即使通过用户的身份提供保护，目标领域也不一定匹配，除非对话在本地身份验证服务器上终止。

对于用户连接，当使用了 `[username]` 和 `[domain]` 占位符模式时，适用以下条件：

- 如果客户端证书用于身份验证 - 从各 X509 证书属性获取 `[username]` 和 `[password]` 的占位符值。根据首次匹配按下述顺序分析属性。例如，如果对于用户身份验证，身份是 `userA@example.com`（其中 `username=userA` 且 `domain=example.com`），对于计算机身份验证，身份是 `hostA.example.com`（其中 `username=hostA` 且 `domain=example.com`），将分析以下属性：

- 如果是基于用户证书的身份验证：

SubjectAlternativeName: UPN = userA@example.com

Subject = .../CN=userA@example.com/...

Subject = userA@example.com

Subject = .../CN=userA/DC=example/DC=com/...

Subject = userA (no domain)

- 如果是基于计算机证书的身份验证：

SubjectAlternativeName: DNS = hostA.example.com

Subject = .../DC=hostA.example.com/...

Subject = .../CN=hostA.example.com/...

Subject = hostA.example.com

- 如果凭证源是最终用户 - 从用户输入的信息获取占位符的值。
- 如果从操作系统获取证书 - 从登录信息获取占位符的值。
- 如果凭证是静态的 - 没有使用占位符。

在 Credentials 窗格中，您可以指定用于对关联网络进行身份验证所需的凭证。

## 过程

**步骤 1** 定义受保护身份模式的用户身份。网络访问管理器支持以下身份占位符模式：

- `[username]` - 指定用户名。如果用户输入 `username@domain` 或 `domain\username`，则域部分会被剥离。
- `[raw]` - 完全按照用户的输入指定用户名。

- [domain] - 指定用户设备的域。

## 步骤 2 指定典型的未受保护的身份模式。

尚未协商的会话遇到身份请求，并以明文响应，而无需完整性保护或身份验证。这些会话可能遭到监听和数据包修改。

- anonymous@[domain] - 常常用在隧道方法中，用于在以明文发送值时隐藏用户身份。在内部方法中，将真实用户身份提供为受保护的名称。
- [username]@[domain] - 用于非隧道化方法。

**注释** 以明文发送未受保护的名称信息。如果初始明文名称请求或响应被篡改，服务器可能会发现一旦建立了 TLS 会话就无法验证名称。例如，用户 ID 可能无效或不在 EAP 服务器处理的领域内。

## 步骤 3 指定保护身份模式。

为防止用户 ID 被监听，明文名称只能提供足以让名称验证请求路由到正确领域的信息。

- [username]@[domain]
- 用作用户名称的实际字符串（无占位符）

## 步骤 4 提供更多用户凭证信息：

- Use Single Sign On Credentials - 从操作系统的登录信息中获取凭证。如果登录凭证失败，网络访问管理器暂时（直到下次登录）开启并提示用户通过 GUI 提供凭证。
- Use Static Credentials - 从该配置文件编辑器提供的网络配置文件获取用户凭证。如果静态凭证失败，网络访问管理器在加载新配置之后才会再次使用凭证。
- Prompt for Credentials - 通过 AnyConnect GUI 获取来自最终用户的凭证，正如下文所指定：
  - Remember Forever - 永久记住凭证。如果记住的凭证失败，则再次提示用户输入凭证。凭证保留在文件中并使用本地计算机密码进行加密。
  - Remember While User Is Logged On - 记住凭证，直到用户注销为止。如果记住的凭证失败，则再次提示用户输入凭证。
  - Never Remember - 从不记住凭证。网络访问管理器每次需要凭证信息以进行身份验证时都会提示用户。

## 步骤 5 在需要证书时确定哪个证书源用于进行身份验证：

- 智能卡或操作系统证书 - 网络访问管理器使用在操作系统证书存储区或智能卡中找到的证书。
- 仅限智能卡证书 - 网络访问管理器仅使用智能卡中找到的证书。

## 步骤 6 在 Remember Smart Card Pin 参数中，确定网络访问管理器记住用于从智能卡检索证书的 PIN 的时间长度。请参阅步骤 2 以了解可用的选项。

**注释** PIN 保留时间绝不能超过证书本身的保留时间。

某些智能卡连接所需时间可能比其他智能卡更长，这取决于智能卡芯片和驱动程序（也称为加密服务提供程序 (CSP) 和密钥存储提供程序 (KSP)）。增加连接超时可能给网络足够时间来执行基于智能卡的身份验证。

## 配置计算机凭证

EAP 对话可能涉及多种 EAP 身份验证方法，其中每种身份验证要求的身份可能不同（例如先是计算机身份验证，然后是用户身份验证）。例如，对等成员最初可能要求 `nouser@example.com` 的身份来将身份验证请求路由到 `cisco.com` EAP 服务器。但是，一旦 TLS 会话经过协商，对等成员就可能要求 `johndoe@example.com` 的身份。因此，即使通过用户的身份提供保护，目标领域也不一定匹配，除非对话在本地身份验证服务器上终止。

对于计算机连接，只要使用 `[username]` 和 `[domain]` 占位符，以下条件即适用：

- 如果客户端证书用于身份验证 - 从各 X509 证书属性获取 `[username]` 和 `[password]` 的占位符值。根据首次匹配按下述顺序分析属性。例如，如果对于用户身份验证来说身份是 `userA@cisco.com`（其中 `username=userA`，`domain=cisco.com`），对于计算机身份验证来说是 `hostA.cisco.com`（其中 `username=hostA`，`domain=cisco.com`），则分析以下属性：

- 如果是基于用户证书的身份验证：

SubjectAlternativeName: UPN = userA@example.com

Subject = .../CN=userA@example.com/...

Subject = userA@example.com

Subject = .../CN=userA/DC=example.com/...

Subject = userA (no domain)

- 如果是基于计算机证书的身份验证：

SubjectAlternativeName: DNS = hostA.example.com

Subject = .../DC=hostA.example.com/...

Subject = .../CN=hostA.example.com/...

Subject = hostA.example.com

- 如果客户端证书不用于身份验证 - 从操作系统获取凭证，`[username]` 占位符代表分配的计算机名称。

使用凭证面板，可以指定所需的计算机凭证。

## 过程

---

**步骤 1** 为受保护的服务器模式定义计算机身份。网络访问管理器支持以下身份占位符模式：

- [username] - 指定用户名。如果用户输入 `username@domain` 或 `domain\username`，则会删除域部分。
- [raw] - 完全按照用户的输入指定用户名。
- [domain] - 指定用户 PC 的域。

**步骤 2** 定义典型的未受保护的计算机身份模式。

尚未协商的会话遇到身份请求，并以明文响应，而无需完整性保护或身份验证。这些会话可能遭到监听和数据包修改。

- `host/anonymous@[domain]`
- 作为计算机身份发送的实际字符串（无占位符）

**步骤 3** 定义受保护的计算机身份模式。

为防止用户 ID 被监听，明文身份只能提供足以让身份验证请求路由到正确领域的信息。典型的受保护的计算机身份模式如下所示：

- `host/[username]@[domain]`
- 作为计算机身份使用的实际字符串（无占位符）

**步骤 4** 提供更多计算机凭证信息。

- 使用机器凭证 - 从操作系统获取凭证。
  - 使用静态凭证 - 指定要在部署文件中发送的实际静态密码。静态凭证不适用于基于证书的身份验证。
- 

## 配置受信任服务器验证规则

为 EAP 方法配置了 `Validate Server Identity` 选项时，`Certificate` 面板允许您配置证书服务器或授权的验证规则。验证的结果将确定证书服务器或授权是否得到信任。

要定义证书服务器验证规则，请执行以下步骤：



## 过程

**步骤 1** 显示 **Certificate Field** 和 **Match** 列的可选设置时，点击下拉箭头并选择所需的设置。

**步骤 2** 在 Value 字段中输入值。

**步骤 3** 在 Rule 下，点击 **Add**。

**步骤 4** 在 Certificate Trusted Authority 窗格中，选择以下选项之一：

- **Trust Any Root Certificate Authority (CA) Installed on the OS (CA)** - 如果选择此选项，仅将本地计算机或证书存储区视为服务器的证书链验证。
- **包括根证书颁发机构 (CA) 证书。**

**注释** 如果选择 **Include Root Certificate Authority (CA) Certificates**，则必须点击 **Add** 将 CA 证书导入到配置。如果使用的证书正在从 Windows 证书库中导出，请使用“**Base 64 encoded X.509 (.cer)**”选项。

## Network Groups 窗口

在 Network Groups 窗口中，可向特定的组分配网络连接。对连接分组提供多项优势：

- 当用户尝试连接时，可改善用户体验。当配置了多个隐藏网络时，客户端可以按照定义的顺序遍历隐藏网络列表，直到成功建立连接。在这些情况下，分组可大幅减少建立连接所需的时间。
- 简化所配置连接的管理。使您可以根据需要将管理员网络与用户网络分隔，并允许公司的多角色用户（或经常访问同一区域的用户）在组中定制网络，以提高可选网络列表的可管理性。

作为分发包的一部分而定义的网络将锁定，从而防止用户编辑配置设置或删除网络配置文件。

您可以将网络定义为全局网络。执行此操作时，网络将显示在全局网络部分中。该部分划分为有线和无线网络类型。在这种类型的网络中只能执行排序编辑。

所有非全局网络必须存在于一个组中。默认情况下，会创建一个组，如果所有网络都是全局网络，用户可以删除该组。

## 过程

**步骤 1** 从下拉列表选择一个组。

**步骤 2** 选择 **Create networks** 可允许最终用户在该组中创建网络。部署后，如果您取消选中此项，网络访问管理器会从该组中删除用户创建的任何网络，这会强制用户在另一个组中重新输入网络配置。

**步骤 3** 选择 **See scan list**，以在使用 AnyConnect GUI 将该组选择为活动组时允许最终用户查看扫描列表。或者，清除复选框以限制用户查看扫描列表。例如，如果您要阻止用户意外连接到相邻设备，应限制扫描列表访问。

**注释** 这些设置应用基于组。

**步骤 4** 使用右箭头和左箭头从在 **Group** 下拉列表中选择的一组中插入和删除网络。如果某网络已移出当前组，则它会放置到默认组中。当默认组正在编辑时，您无法从其中移动网络（使用 > 按钮）。

**注释** 在给定网络中，每个网络的显示名称必须唯一；因此，任何一组不能包含两个或更多具有相同显示名称的网络。

**步骤 5** 使用上箭头和下箭头更改组中网络的优先级顺序。

---



## 第 6 章

# 配置终端安全评估

AnyConnect 安全移动客户端提供 ASA 终端安全评估模块和 ISE 终端安全评估模块。这两个模块都为 Cisco AnyConnect 安全移动客户端提供了评估终端在以下方面是否合规的功能，例如主机上所安装的防病毒、反间谍软件以及防火墙软件。您可以限制网络访问权限直至终端合规，或者提高本地用户的权限，使其可以制定补救措施。

ASA 终端安全评估与 `hostscan_version.pkg` 捆绑在一起，后者是一款收集主机上安装了哪些操作系统、防病毒、反间谍软件和软件信息的应用。AnyConnect 4.0 提供 ISE 终端安全评估，因此您可以在访问 ISE 控制的网络时部署一个客户端，而不必部署 AnyConnect 和 NAC 代理。ISE 终端安全评估是一个模块，可选作额外的安全组件安装到 AnyConnect 产品中（就像网络安全、网络访问管理器）。HostScan 过去包含在 AnyConnect 捆绑包 4.0 版之前的版本中，但现在用户需要单独安装。

ISE 终端安全评估可执行客户端评估。客户端从头端获得终端安全评估要求策略、执行终端安全评估数据收集、将结果与策略进行比较，并将评估结果发送回头端。尽管 ISE 实际确定终端是否合规，但它依赖终端自己的策略评估结果。

相反，HostScan 将执行服务器端评估，其中 ASA 仅请求终端属性（例如操作系统、IP 地址、注册表项、本地证书和文件名）的列表，而且这些属性由 HostScan 返回。根据策略评估的结果，您可以控制哪些主机可获准与安全设备建立远程访问连接。



注  
释

建议不要将 HostScan 与 ESS 终端安全评估代理混合使用，因为两种不同的终端安全评估代理运行时会造成出乎意料的结果。

以下是 HostScan 支持而 ISE 终端安全评估不支持的终端安全评估检查：

- 主机名
- IP 地址
- MAC 地址
- 端口号
- OPSWAT 版本
- BIOS 序列号

- 个人防火墙
- 包含校验和验证的文件检查
- 证书字段属性
  
- [ISE 终端安全评估模块提供的功能](#)，第 164 页
- [用于中断 AnyConnect ISE 流的操作](#)，第 166 页
- [ISE 终端安全评估的状态](#)，第 167 页
- [终端上的并发用户](#)，第 169 页
- [终端安全评估模块的日志记录](#)，第 169 页
- [终端安全评估模块的日志文件和位置](#)，第 169 页
- [OPSWAT 支持图表](#)，第 170 页
- [ASA 终端安全评估模块提供的功能](#)，第 170 页
- [ISE 终端安全评估配置文件编辑器](#)，第 173 页
- [高级面板](#)，第 175 页

## ISE 终端安全评估模块提供的功能

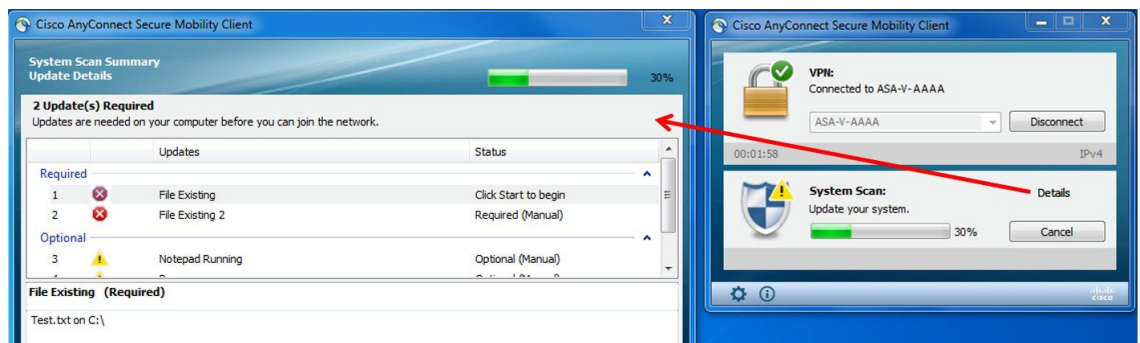
### 终端安全评估检查

ISE 终端安全评估模块使用 OPSWAT v3 库执行终端安全评估检查。对于初始终端安全评估检查，任何未能满足所有强制性要求的终端都被视为不合规。其他终端授权状态为终端安全评估未知或合规（满足强制性要求）。

如果在终端安全评估检查阶段出错并且 AnyConnect 能够继续，用户将收到通知，但如果可能，终端安全评估检查将继续。如果在强制终端安全评估检查期间出错，检查将标记为失败。如果满足所有强制性要求，将授予网络访问权限。否则，用户可以重新启动终端安全评估进程。

### 任何必要的补救措施

补救窗口在后台运行，以保证网络活动更新不会弹出，引起干扰或中断。您可以在 AnyConnect UI 的 ISE 终端安全评估图块部分点击 **Details**，查看检测到的内容和您加入网络前所需的更新。如果必须进行手动补救，补救窗口会打开，显示需要操作的项目。此 System Scan Summary: Update Details 窗口显示更新的进度、所分配更新时间的剩余时间、任何要求的状态以及系统合规性状态。



373454

管理员可以配置在 ISE 终端安全评估过程结束时显示的网络使用策略。访问该策略时，您会看到在授予接入 VLAN 的访问权限前用户必须接受的所有必需条款和条件。

当只剩下可选更新时，才可选择 **Skip** 跳到下一步操作，或选择 **Skip All** 以忽略所有剩余补救项。您可以出于时间考虑跳过可选补救项或仍然保持网络访问。

在补救后（或在无需补救时执行要求检查后），您可能收到可接受使用政策的通知。它要求您接受该政策才能进行网络访问，若拒绝则限制访问。在此部分补救过程中，AnyConnect UI 的终端安全评估图块部分会显示“System Scan: Network Acceptable Use Policy”。

当补救完成后，作为所需更新列出的所有检查都显示 Done 状态和绿色复选框。补救后，代理会向 ISE 发送终端安全评估结果。

## 重新评估终端合规性

当终端被视为合规并授予网络访问权限后，可选择基于管理员配置的控制对终端定期进行重新评估。被动重新评估终端安全评估检查与初始终端安全评估检查不同。如果管理员配置了相应的设置，那么当发生任何不符合要求的情形时，用户都可选择修复选项。配置设置用于控制用户是否维持受信任的网络访问（即使用户未达到一项或多项强制要求）。在初始终端安全评估过程中，如果终端未满足所有强制要求，将被视为不合规。管理员可将结果设置为 Continue、Logoff 或 Remediate，并可配置诸如“强制执行”和“正常时间”等其他选项。

默认情况下，ISE UI 禁用此功能；如果为某一用户角色启用该功能，则每 1 到 24 小时执行一次状态重新终端安全评估。

## 自动合规性

凭借终端安全评估租约，ISE 服务器可以完全跳过终端安全评估检查，直接将系统置于合规状态。通过此功能，如果最近检查过系统终端安全评估，用户不必再经历网络间切换的延迟。ISE 终端安全评估代理仅需在发现 ISE 服务器后立即向 UI 发送状态消息，指示系统是否合规。在 ISE UI (Settings > Posture > General Settings) 中，您可以指定初始合规性检查后多长时间即认为终端安全评估合规。即使用户从一个通信接口切换到另一个，也应保持合规状态。



注释

使用终端安全评估租约时，如果 ISE 上的会话有效，终端会从未知状态变为合规状态。

## VLAN 监控和转换

某些站点使用不同的 VLAN 或子网划分其集团公司和访问级别的网络。来自 ISE 的授权更改 (CoA) 指定 VLAN 更改。管理员操作（例如会话终止）也可能导致发生更改。为支持 VPN 连接期间的 VLAN 更改，请在 ISE 终端安全评估配置文件中配置以下设置：

- **VLAN Detection Interval** - 确定代理检测 VLAN 转换的频率以及监控是否禁用。当此时间间隔设置为非 0 值时，会启用 VLAN 监控。对于 Mac OS X，将此值至少设置为 5。

VLAN 监控在 Windows 和 Mac OS X 上都可实施，但在 Mac 上仅当检测意外 VLAN 更改时才需要实施。如果 VPN 已连接或者 acise（主要 AnyConnect ISE 进程）未运行，它会自动禁用。有效范围为 0 到 900 秒。

- **Enable Agent IP Refresh** - 未选中时，ISE 会向代理发送 Network Transition Delay 值。选中后，ISE 将向代理发送 DHCP 释放和续订值，然后代理更新 IP 以检索最新的 IP 地址。
- **DHCP Release Delay and DHCP Renew Delay** - 用于关联 IP 刷新和 Enable Agent IP Refresh 设置。选中 Enable Agent IP Refresh 复选框且此值不是 0 时，代理会等待一定秒数的释放延迟，更新 IP 地址，然后等待一定秒数的续订延迟。如果 VPN 已连接，将自动禁用 IP 刷新。
- **Network Transition Delay** - 当 VLAN 监控被代理禁用或启用（在 Enable Agent IP Refresh 复选框中）时使用。此延迟在未使用 VLAN 时会增加缓冲，给代理适当的时间等待来自服务器的准确状态。ISE 将此值发送给代理。如果您还在 ISE 用户界面的全局设置中设置了 Network Transition Delay 值，ISE 终端安全评估配置文件编辑器中的值将覆盖它。



注释

ASA 不支持 VLAN 更改，因此这些设置在客户端通过 ASA 连接到 ISE 时不适用。

### 故障排除

如果终端设备在终端安全评估完成后无法访问网络，请检查以下内容：

- 在 ISE 用户界面上是否配置了 VLAN 更改？
  - 如已配置，是否在配置文件中设置了 DHCP 释放延迟和续订延迟？
  - 如果这两项设置都为 0，是否在配置文件中设置了 Network Transition Delay？

## 用于中断 AnyConnect ISE 流的操作

由于各种原因，在初始终端安全评估重新评估或被动重新评估过程中，AnyConnect ISE 终端安全评估流可能中断。

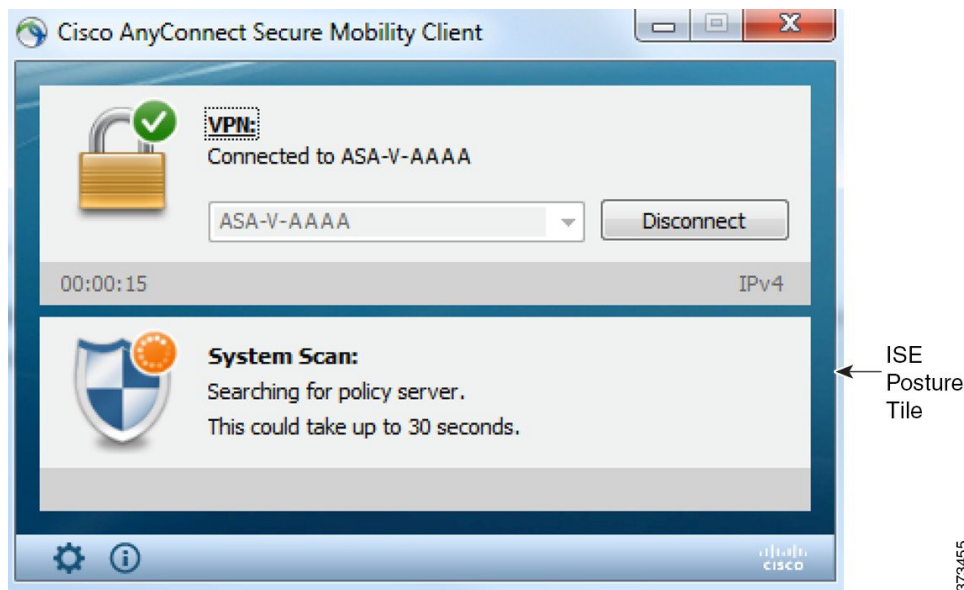
- 用户取消 AnyConnect ISE - 在终端安全评估检查和补救期间，用户可以取消 AnyConnect ISE。UI 会立即通知用户正在进行取消，但只在避免将终端置于出问题状态的时期才会出现这种情

况。如果使用了第三方软件，一些取消操作可能需要重新启动。取消后，AnyConnect UI 的终端安全评估图块部分显示合规状态。

- 修复计时器超时 - 满足终端安全评估要求的管理员控制时间已到期。一份评估报告被发送到终端。在被动重新评估期间，用户保留网络访问权限；而对于终端安全评估，满足所有强制性要求后将授予网络访问权限。
- 终端安全评估检查过程中出错 - 如果在终端安全评估检查阶段出错并且 AnyConnect 能够继续，用户将收到通知，但如果可能，终端安全评估检查将继续。如果在强制终端安全评估检查期间出错，检查将标记为失败。如果满足所有强制性要求，将授予网络访问权限。否则，用户可以重新启动终端安全评估进程。
- 补救过程中出错 - 如果在补救阶段出错并且 AnyConnect ISE 终端安全评估可以继续，用户会收到通知。如果失败的补救步骤与某个强制性终端安全评估要求相关，AnyConnect ISE 终端安全评估将停止补救进程。如果失败的补救步骤与某个可选终端安全评估要求相关，则会尝试继续下一步并完成 ISE 终端安全评估操作。如果满足所有强制性要求，将授予网络访问权限。否则，用户可以重新启动终端安全评估进程。
- 默认网关更改 - 用户可能由于默认网关更改而失去受信任网络访问，导致 ISE 终端安全评估尝试重新发现 ISE。当 ISE 终端安全评估进入重新发现模式时，AnyConnect UI 的 ISE 终端安全评估图块部分会显示 ISE 终端安全评估的状态。
- AnyConnect 和 ISE 之间的连接丢失 - 终端被认为合规并被授予网络访问权限后，可能发生各种网络状况：终端可能遇到网络连接完全丢失的情况，ISE 可能性能下降，ISE 终端安全评估可能出现故障（由于会话超时、手动重启等）或 ASA 后面的 ISE 可能丢失 VPN 隧道。

## ISE 终端安全评估的状态

当 AnyConnect ISE 终端安全评估按预期正常运行和阻止网络访问时，AnyConnect 用户界面的 ISE 终端安全评估图块中显示“System Scan: Searching for policy server”。在 Windows 任务管理器或 Mac OS X 系统日志中，您可以看到该进程正在运行。如果该服务未运行，AnyConnect 用户界面的 ISE 终端安全评估图块中显示“System Scan: Service is unavailable”。



网络变化启动发现阶段。使用 AnyConnect ISE 终端安全评估时，如果主要接口的默认路由发生改变，会使代理回到发现过程。例如，当 WiFi 和主要 LAN 连接时，代理会重新启动发现。同样，如果 WiFi 和主要 LAN 建立连接，然后 WiFi 断开连接，则代理不会重新启动发现。

在 AnyConnect 用户界面的 ISE 终端安全评估图块中的“System Scan”之后，还可能出现以下状态消息：

- Limited or no connectivity - 未进行发现，因为您没有连接。AnyConnect ISE 终端安全评估代理可能正在网络中的错误终端上执行发现。
- System scan not required on current WiFi - 未进行发现，因为检测到不安全的 WiFi。AnyConnect ISE 终端安全评估代理仅在 LAN、无线网络（如果使用 802.1X 身份验证）以及 VPN 上启动发现。WiFi 可能不安全，或者您通过在代理配置文件中将 OperateOnNonDot1XWireless 设置为 1 禁用了该功能。
- Unauthorized policy server - 主机与 ISE 网络的服务器名称规则不匹配，因此网络访问受限或不允许访问。
- The AnyConnect Downloader is performing update... - 下载程序已调用，将比较软件包版本、下载 AnyConnect 配置，并执行必要的升级。
- Scanning System... - 扫描防病毒和反间谍软件安全产品是否已启动。如果在此过程中网络发生改变，代理将循环生成日志文件的过程，并且状态返回到“No policy server detected”。
- Bypassing AnyConnect scan - 网络配置为使用 Cisco NAC 代理。
- Untrusted Policy Server Cancelled by the user - 在 AnyConnect 用户界面中使用 System Scan Preferences 选项卡取消阻止连接到不受信任的服务器时，弹出窗口中会出现 AnyConnect 下载程序的安全警告。在此警告页面上点击 **Cancel Connection** 时，ISE 终端安全评估图块会更改为此状态。
- Network Acceptable Use Policy - 访问网络时，您必须查看并接受“可接受的使用策略”。拒绝该政策可能会导致网络访问受限。



- Updating Network Settings - 在 ISE 用户界面的 Settings > Posture > General Settings 中，您可以指定网络转换之间应发生的延迟秒数。
- Not Compliant. Update time expired - 为补救设置的时间已过期。
- Compliant. Network access allowed. - 补救完成。System Scan > Scan Summary 也显示状态为完成。
- No policy server detected - 找不到 ISE 网络。30 秒钟后，代理会减慢探测。默认网络访问权限生效。

## 终端上的并发用户

当多名用户同时登录到终端而共享网络连接时，AnyConnect ISE 不支持单独的终端安全评估。当运行 AnyConnect ISE 的第一位用户的状态被成功捕获时，终端将被授予受信任的网络访问权限，该终端上的所有其他用户都将继承网络访问权限。为防止发生此情况，管理员可在终端上禁用允许并发用户的功能。

## 终端安全评估模块的日志记录

对于 ISE 终端安全评估，事件将写入本地操作系统的事件日志（Windows 事件日志查看器或 Mac OS X 系统日志）。

对于 ASA 终端安全评估，任何错误和警告都将写入系统日志（非 Windows）和事件查看器 (Windows)。所有可用的消息都将写入日志文件。

ASA 终端安全评估模块组件最多输出到三个日志，具体取决于您的操作系统、权限级别和启动机制（Web 启动或 AnyConnect）：

- cstub.log - 使用 AnyConnect Web 启动时捕获日志记录。
- libcsd.log - 由使用 ASA 终端安全评估 API 的 AnyConnect 线程创建。调试条目根据日志记录级别配置写入此日志。
- cscan.log - 通过扫描可执行文件 (cscan.exe) 而创建，是 ASA 终端安全评估的主要日志。调试条目根据日志记录级别配置写入此日志。

## 终端安全评估模块的日志文件和位置

对于 ISE 终端安全评估，事件包含在安装的 AnyConnect 版本的事件子文件夹中，因此易于与其余 AnyConnect 事件隔开。每个查看器均可搜索关键字和过滤。Web 代理事件写入标准应用日志。

为便于故障排除，会将 ISE 终端安全评估要求策略和评估报告记录到终端上经过模糊处理的单独文件中，而不会是事件日志中。这些日志文件保留五个最新日志。某些日志文件的大小（例如 aciseposture），可由管理员在配置文件中配置；但 UI 日志大小是预定义的。

每当进程异常终止时，都会生成一个小型转储文件，就像其他 AnyConnect 模块提供的一样。

对于 ASA 终端安全评估，文件位于用户主文件夹中的以下目录中：

- （非 Windows） - .cisco/hostscan/log
- (Windows) - Win7/Win8  
C:\Users\

## OPSWAT 支持图表

OPSWAT 支持图表包含您使用的防病毒、反间谍软件和防火墙应用的产品名称及版本信息。HostScan 支持 OPSWAT API 版本 2，而 ISE 终端安全评估合规性模块支持 OPSWAT API 版本 3。这两个版本在组织方面的最大区别是版本 2 按供应商组织库文件，而版本 3 按产品类别组织它们。

库（zip 文件）中的各个文件由 OPSWAT 公司进行数字签名，而库本身被打包为单个自解压的可执行文件，由思科证书进行代码签名。您可以使用 Microsoft Excel、Microsoft Excel Viewer 或 OpenOffice 查看图表。

当头端（ISE 或 ASA）和终端之间版本号存在不匹配时，OPSWAT 就会升级或降级。这些升级/降级是强制性的，并会自动进行，无需最终用户干预，只要建立了到头端的连接即可。

在 AnyConnect 版本 4.0 之前，OPSWAT 二进制文件是 HostScan 软件包的一部分，并利用 HostScan 安装程序进行安装。您可以从 [cisco.com](http://cisco.com) 下载 HostScan 支持图表，此处是 [防病毒、反间谍软件和防火墙应用列表](#)。

对于 AnyConnect 版本 4.0，OPSWAT 二进制文件是作为一个不同的软件包发布的，具有自己的安装程序，独立于使用它的软件包安装程序和模块。

仅 OPSWAT 版本 3 的库可以上传到 ISE，您可以从本地文件系统或直接通过 ISE 更新源 URL 手动加载到 ISE。

## ASA 终端安全评估模块提供的功能

### HostScan

HostScan 是在用户连接到 ASA 后但在登录前安装到远程设备上的软件包。HostScan 由基本模块、终端评估模块和高级终端评估模块任意组合而成。



注释

---

在 AnyConnect 版本 4.0 之前，此软件包捆绑在 `hostscan_version.pkg` 文件中，必须在 ASA 中的 HostScan 映像下更新并启用该文件才能获得 HostScan 功能。此软件包当前单独安装。

---

## 基本功能

HostScan 自动在建立思科无客户端 SSL VPN 或 AnyConnect 客户端会话的任何远程设备上识别操作系统和服务包。

您还可以配置 HostScan 以检查终端的特定流程、文件、注册表项、数字证书和 IP 地址。它在全隧道建立之前执行上述所有检查项，然后向 ASA 发送此信息以区分公司拥有的计算机、个人计算机和公共计算机。该信息也可用于评估。

HostScan 也会自动返回以下其他值，用于根据已配置的 DAP 终端条件进行评估：

- Microsoft Windows、Mac OS 和 Linux 版本
- 在运行 Microsoft Windows 的连接主机上处于活动状态的侦听端口
- Microsoft 知识库编号 (KB)
- 证书信息



注释

HostScan 会收集有关 Windows 客户端系统上 Microsoft 软件更新的服务版本 (GDR) 信息。服务版本包含多个修补程序。服务版本终端属性用在 DAP 规则（而非修补程序）中。

## 终端评估

终端评估是一项 HostScan 扩展功能，用于检查远程计算机上是否存在大量防病毒和反间谍软件应用、相关定义更新以及防火墙。在 ASA 向会话分配特定动态访问策略 (DAP) 之前，可以使用此功能组合终端条件来满足您的要求。

有关详细信息，请参阅 *Cisco ASA 系列 VPN ASDM 配置指南* 中的 [动态访问策略](#)。

## 高级终端评估：防病毒、反间谍软件和防火墙补救

在 Windows、Mac OS X 和 Linux 桌面中，如果软件允许单独的应用启动补救，高级终端评估可以尝试发起防病毒、反间谍软件和个人防火墙保护的各方面的补救。

**防病毒** - 补救防病毒软件的这些组件：

- 强制文件系统保护 - 启用已禁用的防病毒软件。
- 强制病毒定义更新 - 如果防病毒定义在高级终端评估配置定义的天数内未更新，则发起病毒定义更新。

**反间谍软件** - 如果反间谍软件定义在高级终端评估配置定义的天数内未更新，则发起反间谍软件定义更新。

**个人防火墙** - 重新配置不符合高级终端评估配置中定义的要求的防火墙设置和规则。例如，

- 启用或禁用防火墙。

- 阻止或允许应用运行。
- 阻止或打开端口。



注释 并非所有个人防火墙都支持此功能。

如果最终用户在成功建立 VPN 连接后禁用防病毒或个人防火墙，我们的高级终端评估功能会在大约 60 秒内尝试重新启用该应用。

## 为 HostScan 配置防病毒应用

在安装 ASA 终端安全评估模块或 HostScan 之前，将防病毒软件配置到“白名单”中或者将以下这些应用归为安全例项。防病毒应用可能会将这些应用的行为误判为恶意行为。

- cscan.exe
- ciscod.exe
- cstub.exe

## 与动态访问策略集成

ASA 将 HostScan 功能集成到动态访问策略 (DAP) 中。根据配置，ASA 将一个或多个终端属性值与可选 AAA 属性值组合作为分配 DAP 的条件。DAP 的终端属性支持的 HostScan 功能包括操作系统检测、策略、基本结果和终端评估。

可以指定单个属性或组合多个属性来构成将 DAP 分配到会话所需的条件。DAP 提供适用于终端 AAA 属性值级别的网络访问。当满足所有已配置的终端条件后，ASA 应用 DAP。

请参阅 *Cisco ASA 系列 VPN ASDM 配置指南* 中的配置动态访问策略。

## DAP 中的 BIOS 序列号

ASA 终端安全评估可以检索主机的 BIOS 序列号。您可以使用动态访问策略 (DAP) 允许或阻止基于该 BIOS 序列号建立到 ASA 的 VPN 连接。

## 将 BIOS 指定为 DAP 终端属性

### 过程

- 步骤 1 登录到 ASDM。
- 步骤 2 选择 **Configuration > Remote Access VPN > Network (Client) Access** 或 **Clientless SSL VPN Access > Dynamic Access Policies**。
- 步骤 3 在 Configure Dynamic Access Policies 面板中，点击 **Add** 或 **Edit** 将 BIOS 配置为 DAP 终端属性。
- 步骤 4 在 Endpoint ID 表的右侧，点击 **Add**。
- 步骤 5 在 Endpoint Attribute Type 字段中，选择 **Device**。
- 步骤 6 选中 **BIOS Serial Number** 复选框，选择 **=**（等于）或 **!=**（不等于），并且在 BIOS Serial Number 字段中输入 BIOS 编号。点击 **OK** 保存在 Endpoint Attribute 对话框中的更改。
- 步骤 7 点击 **OK** 保存对 Edit Dynamic Access Policy 的更改。
- 步骤 8 点击 **Apply** 保存对动态访问策略的更改。
- 步骤 9 点击 **Save**。

## 如何获取 BIOS 序列号

- Windows - <http://support.microsoft.com/kb/558124>
- Mac OS X - <http://support.apple.com/kb/ht1529>
- Linux - 使用此命令：

```
/usr/bin/hal-get-property --udi /org/freedesktop/Hal/devices/computer --key system.hardware.serial
```

## 确定在 ASA 上启用的 HostScan 映像

打开 ASDM 并选择 **Configuration > Remote Access VPN > HostScan Image**。

## ISE 终端安全评估配置文件编辑器

管理员可以选择使用独立编辑器创建终端安全评估配置文件，然后将其上载至 ISE。否则，嵌入式终端安全评估配置文件编辑器配置在 ISE 用户界面中的 Policy Elements 下。AnyConnect 配置编辑器在 ISE 中启动后，它会创建 AnyConnect 配置以及 AnyConnect 软件及其关联的模块、配置文件、OPSWAT 和任何定制。ASA 中 ISE 终端安全评估的独立配置文件编辑器包含以下参数：

- 代理的行为

**Enable signature check** - 如果选中，则在代理运行可执行文件之前，会启用这些文件的签名检查。

**Log file size** - 代理日志文件的最大大小。有效值为 5 Mb 到 200 Mb。

**Remediation Timer** - 用户必须在此时间内完成补救，否则将被标记为不合规。有效值为 1 - 300 分钟。

**Enable agent log trace** - 在代理上启用调试日志。

**Operate on non-802.1X wireless networks** - 如果选中，会启用代理在非 802.1X 无线网络上工作。

#### • IP 地址更改

为了获得最佳用户体验，请将以下值设置为我们推荐的值。

**VLAN detection interval** - 代理在刷新客户端 IP 地址之前尝试检测 VLAN 更改的时间间隔。有效范围为 0 到 900 秒，推荐值为 5 秒。

**Ping or ARP** - 检测 IP 地址更改的方法。推荐的设置为 ARP。

**Maximum timeout for ping** - 从 1 到 10 秒的 ping 超时时间。

**Enable agent IP refresh** - 选中可启用 VLAN 更改检测。

**DHCP renew delay** - 代理在 IP 刷新之后等待的秒数。启用了 Enable Agent IP Refresh 时，请配置此值。如果该值不是 0，则代理将在此预期的过渡期间进行一次 IP 刷新。如果在刷新时检测到 VPN，则刷新将被禁用。有效值为 0 到 60 秒，推荐值为 5 秒。

**DHCP release delay** - 代理延迟进行 IP 刷新的秒数。启用了 Enable Agent IP Refresh 时，请配置此值。如果该值不是 0，则代理将在此预期的过渡期间进行一次 IP 刷新。如果在刷新时检测到 VPN，则刷新将被禁用。有效值为 0 到 60 秒，推荐值为 5 秒。

**Network transition delay** - 代理暂停网络监控以便等待计划好的 IP 更改的时间范围（以秒为单位）。推荐值为 5 秒。

#### • 终端安全评估协议

**Discovery host** - 代理可以连接的服务器。对于独立配置文件编辑器，仅输入单个主机。

**Server name rules** - 由通配符、逗号分隔名称组成的列表，用于定义代理可以连接到的服务器（如 .cisco.com）。

**PRA retransmission time** - 当发生被动重新评估通信失败时，就会指定此代理重试时间范围。有效范围为 60 到 3600 秒。

## 高级面板

AnyConnect 安全移动客户端 UI 的高级面板是每个组件显示统计信息、用户首选项和特定于组件的任何其他信息的区域。如果点击 AnyConnect 系统托盘上的 **Advanced Window for all components** 图标，新的 System Scan 部分将包含以下选项卡：



注释

这些统计信息、用户首选项、消息历史记录等此类选项卡显示在 Mac OS X 上的 Statistics 窗口下。首选项位于 Preferences 窗口中，而不是如同在 Windows 上一样位于选项卡方向中。

- **Preferences** - 允许您阻止与不受信任的服务器的连接，以便在下载程序过程中，对于任何具有不受信任的认证且未经验证的服务器，您都会收到“Untrusted Server Blocked”消息。如果禁用阻止，AnyConnect 不会阻止与潜在恶意网络设备的连接。
- **Statistics** - 提供当前 ISE 终端安全评估状态（合规或不合规）、OPSWAT 版本信息、“可接受使用策略”的状态、终端安全评估的最新运行时间戳、所有缺少的要求以及对故障排除来说重要而要显示的任何其他统计信息。
- **Security Products** - 访问系统中安装的防病毒和反间谍软件产品的列表。
- **Scan Summary** - 允许用户查看管理员为其配置以供查看的任何终端安全评估项。例如，配置时，他们可以查看查看显示终端安全评估的所有项或者只查看终端安全评估检查和要求的补救失败的项。
- **Message History** - 为组件提供向系统托盘发送的每条状态消息的历史记录。该历史记录对于故障排除非常有用。







## 第 7 章

# 配置网络安全

- [关于网络安全模块，第 177 页](#)
- [典型网络安全配置，第 178 页](#)
- [网络安全日志记录，第 196 页](#)

## 关于网络安全模块

思科云网络安全解构网页的元素，以便同时分析各个元素。例如，如果特定网页包含 HTTP、闪存和 Java 元素，则单独的“scanlets”会并行分析这些元素中的每一个。然后，思科云网络安全基于 Cisco ScanCenter 管理门户中定义的安全策略接受良好或可接受的内容并阻止恶意或不可接受的内容。这样，当整个网页因少数内容不可接受而被限制时，可防止“过度阻止”；当整个网页获准但其中仍有一些不可接受或可能有害的内容正通过网页传递时，可防止“阻止不力”。当用户进入或离开公司网络时，思科云网络安全都会保护用户。

全球有很多思科云网络安全扫描代理，用户可以利用 AnyConnect 网络安全将其流量路由至思科云网络安全扫描代理，该代理将以最快的速度响应，从而最小化延迟。

您可以配置“安全值得信赖的网络检测”功能以识别处于企业局域网中的终端。如果启用此功能，来自企业局域网的任何网络流量会绕过思科云网络安全扫描代理。流量安全是通过企业局域网中的其他方法和设备进行管理的，而不是通过思科云网络安全。

AnyConnect 网络安全功能是使用 AnyConnect 网络安全客户端配置文件配置的，您可以使用 AnyConnect 配置文件编辑器对其进行编辑。

Cisco ScanCenter 是思科云网络安全的管理门户。使用 Cisco ScanCenter 创建或配置的某些组件也会纳入 AnyConnect 网络安全客户端配置文件。



注释

ISE 服务器必须始终列在静态例外列表中，该列表在网络安全客户端配置文件的 Exceptions 窗格中配置。

# 典型网络安全配置

## 过程

- 步骤 1 配置客户端配置文件中的思科云网络安全扫描代理。
- 步骤 2 （可选）如果在配置文件编辑器内将现有思科云网络安全扫描代理列表与从 <http://www.scansafe.cisco.com/> 网站下载的扫描代理列表进行比较，会显示出差异，则更新扫描代理列表。
- 步骤 3 （可选）向用户显示或隐藏扫描代理。
- 步骤 4 选择默认扫描代理。
- 步骤 5 （可选）指定 HTTP(S) 流量侦听端口以过滤 HTTPS 网络流量。
- 步骤 6 配置排除或包含来自网络扫描服务的终端流量的主机、代理或静态例外。此配置会限制对来自指定 IP 地址的网络流量的评估。
- 步骤 7 配置用户控制和计算最快的扫描代理响应时间。此配置用于选择您希望用户连接的思科云网络安全扫描代理。
- 步骤 8 如果要使源自公司局域网的网络流量绕过思科云网络安全扫描代理，请使用安全值得信赖的网络检测。
- 步骤 9 配置身份验证和将组成员身份发送到思科云网络安全代理。此配置根据用户的企业域或 Active Directory 组的 Cisco ScanCenter 对用户进行身份验证。

## 客户端配置文件中的思科云网络安全扫描代理

思科云网络安全分析网络内容，允许根据安全策略向浏览器传输无害内容并且阻止恶意内容。扫描代理是思科云网络安全在其上分析网络内容的思科云网络安全代理服务器。AnyConnect 网络安全配置文件编辑器中的扫描代理面板定义 AnyConnect 网络安全模块向哪些思科云网络安全扫描代理发送网络流量。

### IPv6 网络流量指南

除非指定了 IPv6 地址、域名、地址范围或通配符的异常情况，否则会向扫描代理发送 IPv6 网络流量。扫描代理执行 DNS 查找可查看是否存在用户尝试访问的 URL 的 IPv4 地址。如果扫描代理找到了 IPv4 地址，它会使用该地址进行连接。如果找不到 IPv4 地址，将放弃连接。

要让所有 IPv6 流量绕过扫描代理，请为所有 IPv6 流量添加 ::/0 静态异常。此异常使所有 IPv6 流量绕过所有扫描代理；因此，IPv6 流量不会受到网络安全保护。



## 注释

在运行 Windows 的计算机上，如果 AnyConnect 无法确定用户 ID，则会将内部 IP 地址用作用户 ID。例如，如果未指定 enterprise\_domains 配置文件条目，则使用内部 IP 地址在 Cisco ScanCenter 中生成报告。

在运行 Mac OS X 的计算机上，如果 Mac 绑定到某个域，网络安全模块可以报告计算机所登录的域。如果 Mac 未绑定到域，网络安全模块可以报告 Mac 的 IP 地址或当前登录的用户名。

## 用户如何选择扫描代理

根据配置文件的配置方式，用户可选择扫描代理，或者通过 AnyConnect 网络安全模块连接到具有最快响应时间的扫描代理。

- 如果客户端配置文件允许用户控制，用户可以从 Cisco AnyConnect 安全移动客户端网络安全托盘的 **Settings** 选项卡中选择扫描代理。
- 如果客户端配置文件启用了 **Automatic Scanning Proxy Selection** 首选项，AnyConnect 网络安全将以最快到最慢的顺序对扫描代理排序，并将用户连接到具有最快响应时间的扫描代理。
- 如果客户端配置文件不允许用户控制，但启用了 **Automatic Scanning Proxy Selection**，AnyConnect 网络安全会将用户从默认扫描代理切换至具有最快响应时间的扫描代理，前提是响应时间明显快于用户最初连接到的默认扫描代理。
- 如果用户开始从当前扫描代理漫游，并且在客户端配置文件中配置了 **Automatic Scanning Proxy Selection**，AnyConnect 网络安全会将用户切换到新扫描代理，前提是其响应时间明显快于当前扫描代理。

用户清楚他们连接到的扫描代理，因为 AnyConnect 网络安全在 Windows 的展开的 AnyConnect 托盘图标中、Advanced Settings 选项卡和 AnyConnect GUI 的 Advanced Statistics 选项卡上显示了启用的扫描代理名称。

## 更新扫描代理列表

网络安全配置文件编辑器的扫描代理列表不可编辑，您无法在网络安全配置文件编辑器的表中添加或删除思科云网络安全扫描代理。

网络安全配置文件编辑器启动后，会通过访问思科云网络安全网站（该网站维护扫描代理的当前列表）来自动更新扫描代理列表。

添加或编辑 AnyConnect 网络安全客户端配置文件时，配置文件编辑器将现有思科云网络安全扫描代理列表与从 <http://www.scansafe.cisco.com> 下载的扫描代理列表进行比较。如果列表过时，会显示 **Scanning Proxy list is out of date** 消息以及标有 **Update List** 的命令按钮。点击 **Update List** 可使用最新的思科云网络安全扫描代理列表更新扫描代理列表。

点击 **Update List** 时，配置文件编辑器会尽可能保持现有配置。配置文件编辑器会保留现有思科云网络安全扫描代理的默认扫描代理设置和显示/隐藏设置。

## 向用户显示或隐藏扫描代理

在用户建立了到 ASA 的 VPN 连接后，ASA 会将客户端配置文件下载到终端设备。AnyConnect 网络安全客户端配置文件确定向用户显示哪些思科云网络安全扫描代理。

为了使漫游用户获得最大利益，我们建议您向所有用户显示所有思科云网络安全扫描代理。

用户采用以下方式，与 AnyConnect 网络安全客户端配置文件扫描代理列表中标示为 Display 的扫描代理进行交互：

- 在其 Cisco AnyConnect 安全移动客户端界面的网络安全面板的 Advanced 设置中，向用户显示思科云网络安全扫描代理。
- 按响应时间对扫描代理进行排序时，AnyConnect 网络安全模块会测试标示为“Display”的思科云网络安全扫描代理。
- 如果其配置文件允许用户控制，用户可以选择所连接的思科云网络安全扫描代理。
- 按响应时间对扫描代理进行排序时，AnyConnect 网络安全客户端配置文件扫描代理表格中标示为“Hide”的思科云网络安全扫描代理不会向用户显示，也不会进行评估。用户无法连接至标示为“Hide”的扫描代理。

### 开始之前

创建一个 AnyConnect 网络安全客户端配置文件。

### 过程

---

**步骤 1** 使用以下方法之一启动网络安全配置文件编辑器：

- 打开 ASDM 并选择 **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Profile**。
- 在 Windows 单机模式下，选择 **Start > All Programs > Cisco > Cisco AnyConnect Profile Editor > Web Security Profile Editor**。

**步骤 2** 打开要编辑的网络安全客户端配置文件。

**步骤 3** 要隐藏或显示思科云网络安全扫描代理，请执行以下操作：

- 选择要隐藏的扫描代理并点击 Hide。
- 选择要显示的扫描代理名称，然后点击 Display。建议配置为显示所有思科云网络安全扫描代理。

**步骤 4** 保存 AnyConnect 网络安全客户端配置文件。

---

## 选择默认扫描代理

当用户首次连接网络时，用户会被路由到其默认扫描代理。默认情况下，您创建的配置文件具有以下思科云网络安全扫描代理属性：

- 扫描代理列表填入的是用户有权访问的所有思科云网络安全扫描代理，并且它们都标记为“Display”。
- 已预先选择一个默认的思科云网络安全扫描代理。
- 在侦听 HTTP 流量的 AnyConnect 网络安全模块的端口列表中调配若干端口。

### 过程

---

**步骤 1** 使用以下方法之一启动网络安全配置文件编辑器：

- 打开 ASDM 并选择 **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Profile**。
- 在 Windows 单机模式下，选择 **Start > All Programs > Cisco > Cisco AnyConnect Profile Editor > Web Security Profile Editor**。

**步骤 2** 打开要编辑的网络安全客户端配置文件。

**步骤 3** 从 **Default Scanning Proxy** 字段选择默认扫描代理。

**步骤 4** 保存 AnyConnect 网络安全客户端配置文件。

---

## 指定 HTTP(S) 流量侦听端口

默认情况下，扫描安全网络扫描服务会分析 HTTP 网络流量，因此，您可以通过配置过滤 HTTPS 网络流量。在网络安全客户端配置文件中，指定面对这些网络流量类型，要让网络安全“侦听”哪些端口。

### 过程

---

**步骤 1** 使用以下方法之一启动网络安全配置文件编辑器：

- 打开 ASDM 并选择 **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Profile**。

- 在 Windows 单机模式下，选择 **Start > All Programs > Cisco > Cisco AnyConnect Profile Editor > Web Security Profile Editor**。

**步骤 2** 打开要编辑的网络安全客户端配置文件。

**步骤 3** 在 **Traffic Listen Port** 字段中，输入面向 HTTP 流量和/或 HTTPS 流量，要让网络安全模块“侦听”的逻辑端口号。

**步骤 4** 保存网络安全客户端配置文件。

## 配置 Windows Internet 选项以配置公共代理

公共代理通常用于将网络流量匿名化。公共代理服务器称为身份验证代理服务器，并且可能需要用户名和密码。AnyConnect 网络安全支持两种类型的身份验证：基本和 NTLM。当代理服务器配置为需要身份验证时，AnyConnect 网络安全会在运行时检测代理并管理身份验证过程。成功对代理服务器进行身份验证后，AnyConnect 网络安全通过公共代理将网络流量路由到思科云网络安全扫描代理：AnyConnect 网络安全加密代理凭证，将其安全缓存在内存中，并且不再需要凭证，即使用户从代理访问非代理网络并返回到同一网络也如此。无需重新启动服务即可与公共代理结合使用。当用户移至非代理网络时，AnyConnect 网络安全在运行时自动对其进行检测，并开始将网络流量直接发送到思科云网络安全扫描代理。

当 Windows Internet 选项被配置为在客户端上使用公共代理时，AnyConnect 将使用该连接。



**注释** 在 Windows 上支持基本和 NTLM 公共代理。在 Mac 上仅支持基本公共代理。

- 1 从 Internet Explorer 或控制面板打开 Internet Options。
- 2 选择 Connections 选项卡，然后点击 **LAN settings**。
- 3 将 LAN 配置为使用代理服务器。
- 4 输入代理服务器的 IP 地址或主机名。如果为 FTP/HTTP/HTTPS 配置了单独的代理，则仅考虑 HTTPS 代理。

限制

- 不支持基于 IPv6 和 TND 的公共代理。
- 在 AnyConnect 网络安全异常列表中不应包含代理 IP；否则，不会将流量定向到 AnyConnect 网络安全。
- 如果代理端口与默认 Web 端口不同，则需要在 AnyConnect 网络安全配置文件的 kdf 侦听端口列表中添加代理端口。

## 排除或包含来自网络扫描服务的终端流量

要排除或包含来自思科云网络安全扫描的特定网络流量，请使用网络安全配置文件编辑器来配置流量的异常。可配置以下几种类别的异常：

- **Host Exceptions 或 Host Inclusions** - 在已配置 Host Exceptions 的情况下，会绕过所输入的 IP 地址（公共或专用，主机名或子网）。在已配置 Host Inclusions 的情况下，所输入的 IP 地址（公共或专用，主机名或子网）会转发到网络安全代理，而所有剩余流量会被绕过。



**注释** AnyConnect 仍然可以拦截 Host Exceptions 中列出的流量。

- **Proxy Exceptions** - 在扫描中会排除此处列出的内部代理服务器。
- **Static Exceptions** - 在扫描和 AnyConnect 中会排除此处列出的 IP 地址。

### ISE 服务器要求

ISE 服务器必须始终列在静态例外列表中，该列表在网络安全客户端配置文件的 Exceptions 窗格中配置。此外，网络安全模块必须绕过 ISE 终端安全评估探测，以便 ISE 终端安全评估客户端可访问 ISE 服务器。ISE 终端安全评估配置文件发送网络探头以查找 ISE 服务器，顺序如下：

- 1 默认网关
- 2 发现主机
- 3 enroll.cisco.com
- 4 以前连接过的 ISE 服务器

## 排除或包含主机例外

### 开始之前

- 请勿在顶级域的两端使用通配符（如 \*.cisco.\*），因为这可能包括网络钓鱼网站。
- 请勿删除或更改任何默认主机例外条目。

### 过程

- 步骤 1** 选择 Host Exceptions 或 Host Inclusions。
- 步骤 2** 根据在步骤 1 中的选择，添加要绕过或转发的 IP 地址（公共或专用，主机名或子网）。
- 步骤 3** 使用以下语法输入子网和 IP 地址：

语法	示例

单独 IPv4 和 IPv6 地址	10.255.255.255 2001:0000:0234:C1AB:0000:00A0:AABC:003F
无类域间路由 (CIDR) 表示法	10.0.0.0/8 2001:DB8::/48
完全限定域名	windowsupdate.microsoft.com ipv6.google.com 注释 不支持部分域；例如，不支持 example.com。
完全限定域名或 IP 地址中的通配符	127.0.0.* *.cisco.com

## 排除代理例外

在 Proxy Exceptions 区域中，输入授权内部代理的 IP 地址（如 172.31.255.255）。

您可在字段中指定 IPv4 和 IPv6 地址，但是您无法为其指定端口号。使用 CIDR 标记，您无法指定 IP 地址。

指定 IP 地址将禁止思科云网络安全拦截流向这些服务器的网络数据，并禁止使用 SSL 使数据以隧道方式通过这些服务器。随后代理服务器即可无中断地运行。如果不在此处添加代理服务器，则会将思科云网络安全流量视为 SSL 隧道。

对于列表中未列出的代理，网络安全将尝试使用 SSL 以隧道方式通过它们。因此，如果您的用户位于不同的公司站点，且该站点需要一个网外代理以访问互联网，则思科云网络安全可为其提供相同级别的支持，就像他们拥有开放互联网连接一样。

## 排除静态例外

确定应绕过思科云网络安全的流量，并添加使用无类域间路由 (CIDR) 表示法的单独 IP 地址或 IP 地址范围列表。在列表中，请包括 VPN 网关的入口 IP 地址。

默认情况下，所述的私有 IP 地址包括在静态例外列表中。



注释

如果存在一个代理服务器，并且它的 IP 地址在静态例外列表的其中一个范围内，则将该例外移到主机例外列表中。例如，10.0.0.0/8 出现在静态例外列表中。如果存在一个位于 10.1.2.3 的代理，则将 10.0.0.0/8 移动到主机例外列表；否则，发送到此代理的流量会绕过云网络安全。



可以指定使用 CIDR 表示法的 IPv4 和 IPv6 地址或地址范围。您无法指定完全限定域名或在 IP 地址中使用通配符。正确的语法示例如下所示：

```
10.10.10.5
192.0.2.0/24
```



**注释** 将 SSL VPN 集中器 IP 地址添加到静态例外列表。

## 配置用户控制和计算最快的扫描代理响应时间

为了允许用户选择要连接到哪个思科云网络安全扫描代理，请执行以下操作：

### 过程

**步骤 1** 使用以下方法之一启动网络安全配置文件编辑器：

- 打开 ASDM 并选择 **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Profile**。
- 在 Windows 单机模式下，选择 **Start > All Programs > Cisco > Cisco AnyConnect Profile Editor > Web Security Profile Editor**。

**步骤 2** 打开要编辑的网络安全客户端配置文件。

**步骤 3** 点击 **Preferences**。

**步骤 4** 选择 **User Controllable**。（这是默认设置。）User Controllable 确定用户是否可以更改 AnyConnect 界面中的 Automatic Tower Selection 和 Order Scanning Proxies by Response Time 设置。

**步骤 5** 选择 **Enable Cloud-Hosted Configuration** 来启用通过 Cisco ScanCenter 更新配置文件。

**步骤 6** 为了让网络安全自动选择扫描代理，请选择 **Automatic Scanning Proxy Selection**。如果您执行此操作，将自动选择 **Order Scanning Proxies by Response Time**。

- 如果您选择 **Automatic Scanning Proxy Selection**，网络安全将确定哪个扫描代理的响应时间最快并自动将用户连接到该扫描代理。
- 如果没有选择 **Automatic Scanning Proxy Selection**，且仍然选择了 **Order Scanning Proxies by Response Time**，则将向用户呈现可以连接的扫描代理列表（按最快到最慢的响应时间排序）。
- 如果没有选择 **Automatic Scanning Proxy Selection**，用户仍然可以从 AnyConnect 用户界面启用此功能，但是一旦启用，则无法将其再次关闭。

**注释** 您启用 Automatic Scanning Proxy Selection 后，瞬时通信中断和故障会导致当前选择的扫描代理自动更改。有时更改扫描代理可能产生不利影响，导致发生意外行为，例如，从使用其他语言的不同国家/地区中的扫描代理返回搜索结果。

**步骤 7** 如果您选择 **Order Scanning Proxies by Response Time**，请配置以下设置来计算哪个扫描代理的响应时间最短。

- **Test Interval:** 运行各个性能测试之间的时间（以分钟为单位，默认为 2 分钟）。清除 Enable Test Interval 复选框可关闭测试间隔，从而阻止测试运行。
- **Test Inactivity Timeout:** 以分钟为单位的时间，若用户处于非活动状态的时间超过此值，网络安全将暂停响应时间测试。只要扫描代理遇到连接尝试，网络安全就立即恢复测试。不应该更改此设置，除非客户端支持人员指导您这么做。

**注释** **Ordering Scanning Proxies by Response Time** 测试将根据 Test Interval 时间连续运行，以下情况除外：

- 安全值得信赖的网络检测已启用并检测到计算机在企业 LAN 中。
- 网络安全许可证密钥丢失或无效。
- 用户处于非活动状态的时间达到所配置的时间，因此满足了“测试非活动超时”阈值。

**步骤 8** 保存网络安全客户端配置文件。

### 接下来的操作

请参阅 *ScanCenter* 管理员指南，版本 5.2 以获取更多信息。

## 使用安全值得信赖的网络检测

当终端通过物理方式或 VPN 连接方式接入企业局域网时，安全受信网络检测功能将进行检测。如果启用安全受信网络检测功能，所有来自企业局域网的网络流量都会绕过思科云网络安全扫描代理。这类流量的安全将通过其他方法和位于企业局域网中的设备（而非思科云网络安全）进行管理。

安全受信网络检测将使用已知 URL（地址、IP 或 FQDN）的服务器上 SSL 证书的 SHA-256 哈希值（拇指指纹）验证客户端是否连接到企业网络。证书使用的加密算法无关紧要，但仅可使用 SHA-256 哈希。

如果您选择不使用安全受信网络检测，且网络中存在代理（例如思科云网络安全连接器），则必须在配置文件编辑器中，将每个代理添加到例外面板的代理例外列表中。

**多个服务器：**如果您定义多台服务器，则客户端在连续两次尝试后仍无法连接到第一台服务器时将尝试连接到第二台服务器。尝试连接列表中的所有服务器之后，客户端将等待五分钟，然后再次尝试连接第一台服务器。



**注释**

当安全受信网络检测在内部网络以外运行时，它将发出 DNS 请求，并尝试与您调配的 HTTPS 服务器通信。思科强烈建议使用别名，以确保在内部网络以外使用的机器不会通过这些请求泄露您组织的名称和内部结构。

### 开始之前

- [排除代理例外](#)

- 对数据丢失防护 (DLP) 设备等某些要求流量不受网络安全影响的第三方解决方案而言，您必须配置安全受信网络检测功能。
- 编辑配置文件时，请确保您与托管 SSL 证书的服务器建立了直接连接。

## 过程

---

**步骤 1** 使用以下方法之一启动网络安全配置文件编辑器：

- 打开 ASDM 并选择 **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Profile**。
- 在 Windows 单机模式下，选择 **Start > All Programs > Cisco > Cisco AnyConnect Profile Editor > Web Security Profile Editor**。

**步骤 2** 打开要编辑的网络安全客户端配置文件。

**步骤 3** 点击网络安全树状窗格中的 **Preferences**。

**步骤 4** 选择 **Enable Trusted Network Detection**。

**步骤 5** 在 **https** 字段中，输入每个受信任服务器的 URL，然后点击 **Add**。URL 可包括端口地址。配置文件编辑器此时将尝试连接受信任服务器。如果无法连接，而您知道服务器证书的 SHA-256 哈希值，请在 **Certificate hash** 框中输入该值并点击 **Set**。

注释 代理后的受信任服务器不受支持。

**步骤 6** 保存网络安全客户端配置文件。

---

## 不使用安全值得信赖的网络检测

如果选择不使用安全值得信赖的网络检测，并且在网络中有代理（例如，思科云网络安全连接器），则您必须将每个代理添加到配置文件编辑器的 **Exceptions** 面板中的代理例外列表。

# 配置身份验证和将组成员身份发送到思科云网络安全代理

开始之前

使用 [Windows 关闭和启用过滤器](#)

## 过程

---

**步骤 1** 使用以下方法之一启动网络安全配置文件编辑器：

- 打开 ASDM 并选择 **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Profile**。

- 在 Windows 单机模式下，选择 **Start > All Programs > Cisco > Cisco AnyConnect Profile Editor > Web Security Profile Editor**。

**步骤 2** 打开要编辑的网络安全客户端配置文件。

**步骤 3** 点击 **Authentication**。

**步骤 4** 在 **Proxy Authentication License Key** 字段中，输入与在 Cisco ScanCenter 中创建的公司密钥、组密钥或用户密钥对应的许可证密钥。要根据用户的企业域对用户进行身份验证，请输入您创建的公司密钥。要根据用户的 Cisco ScanCenter 或 Active Directory 组对用户进行身份验证，请输入您创建的组密钥。该标记默认为空。如果将其留空，网络安全以直通模式运行。

**步骤 5** 输入 **Service Password**。网络安全的默认密码是 websecurity。请在定制配置文件时更改此密码。密码只能包含字母数字字符（a-z、A-Z、0-9）和以下特殊字符，因为其他字符可能被 Windows 命令外壳误认为控制字符或在 XML 中有特殊意义。

~ @ # \$ % \* - \_ + = { } [ ] : , . ? /

使用此密码时，具有管理员权限的用户可以停止网络安全服务。无论是否具有管理员权限，用户都可以在不提供此密码的情况下启动网络安全服务。

**步骤 6** 随每个 HTTP 请求发送扫描代理服务器企业域信息和思科云网络安全或 Active Directory 组信息。扫描代理根据其了解应用流量过滤规则。

**注释** 要将用户的定制用户名和定制组信息发送到扫描服务器代理，请跳过此步骤并转到步骤 7。如果企业不使用 Active Directory，也请跳到步骤 7。

- 点击 **Enable Enterprise Domains**。在列表中，点击 **All Domains**。当选择 All Domains 选项并且计算机在域中时，则将匹配用户所属的域，并且将用户名和组成员身份信息发送到思科云网络安全扫描代理。此选项适用于具有多个域的公司。
- 或者，点击 **Specify Individual Domains**。  
以 NetBIOS 格式输入每个域名，然后点击 Add。例如，example.cisco.com 的 NetBIOS 格式是 cisco。使用 DNS 格式，请不要输入域：abc.def.com。

如果在 Enterprise Domain name 字段中指定域名，思科云网络安全会识别当前登录的 Active Directory 用户、枚举该用户的 Active Directory 组，并将该信息随每个请求发送到扫描代理。

- 在 Use 列表中，点击 **Group Include List** 或 **Group Exclude List**，以在发送到思科云网络安全扫描代理的 HTTP 请求中包含或排除组信息。值可以是要匹配的字符串的任何子字符串。

**Group Include List**。选择 **Group Include List** 之后，将思科云网络安全或 Active Directory 组名称添加到 Group Include List 中。这些组名称将随 HTTP 请求发送到思科云网络安全扫描代理服务器。如果请求来自指定企业域中的用户，将根据用户的组成员身份对 HTTP 请求进行过滤。如果用户没有组成员身份，将使用一组默认的规则对 HTTP 请求进行过滤。

**Group Exclude List**。将思科云网络安全或 Active Directory 组名称添加到 **Group Exclude List**。这些组名不发送到 HTTP 请求的思科云网络安全扫描代理服务器。如果用户属于 Group Exclude List 中的一个组，该组名称不会发送到扫描代理服务器，并将根据其他组成员身份或至少根据一组默认过滤规则对用户的 HTTP 请求进行过滤，该组规则为没有 Active Directory 或思科云网络安全组附属关系的用户进行定义。

**步骤 7** 点击 **Custom matching and reporting for machines not joined to domains** 可发送扫描代理服务器定制名称。

a) 在列表中，点击 **Computer Name** 可使用该计算机的名称。或者，点击 **Local User** 可使用本地用户名。或者，点击 **Custom Name**，然后输入定制用户名。它可由任何字符串定义。如果不输入字符串，则会将计算机的 IP 地址发送到扫描代理服务器。此用户名或 IP 地址用于任何 Cisco ScanCenter 报告中，以识别来自定制用户的 HTTP 流量。

b) 在 **Authentication Group** 字段中，输入最多 256 个字母数字字符的定制组名称，然后点击 **Add**。当 HTTP 请求发送到扫描代理服务器时，如果定制组名称已发送，并且扫描代理服务器上有对应的组名，则根据与定制组名称关联的规则对 HTTP 流量进行过滤。如果在扫描代理服务器上未定义对应的定制组，将根据默认规则对 HTTP 请求进行过滤。

如果仅配置定制用户名而未配置定制组，将根据扫描代理服务器默认规则对 HTTP 请求进行过滤。

**步骤 8** 保存网络安全客户端配置文件。

## 高级网络安全设置

网络安全客户端配置文件的 **Advanced** 面板显示多项设置，它们可帮助思科客户端支持工程师进行故障排除。您不应更改此面板的设置，除非客户端支持人员明确要求您更改它们。

在配置文件编辑器的 **Advanced** 面板中，执行以下任务：

- [配置 KDF 侦听端口](#)
- [配置端口如何侦听传入连接](#)
- [配置超时/重试的发生时间](#)
- [DNS 查找](#)
- [调试设置](#)
- [阻止和允许流量](#)

### 配置 KDF 侦听端口

内核驱动程序框架 (KDF) 拦截将某个流量侦听端口用作其目标端口的所有连接并将流量转发到 KDF 侦听端口。网络扫描服务分析转发到 KDF 侦听端口的所有流量。

#### 开始之前

不应该更改此设置，除非客户端支持人员指导您这么做。

#### 过程

**步骤 1** 使用以下方法之一启动网络安全配置文件编辑器：

- 打开 ASDM 并选择 **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Profile**。

- 在 Windows 单机模式下，选择 **Start > All Programs > Cisco > Cisco AnyConnect Profile Editor > Web Security Profile Editor**。

- 步骤 2** 打开要编辑的网络安全客户端配置文件。
- 步骤 3** 在 Web Security 树窗格中点击 **Advanced**。
- 步骤 4** 在 **KDF Listen Port** 字段中指定 KDF 侦听端口。
- 步骤 5** 保存网络安全客户端配置文件。
- 

## 配置端口如何侦听传入连接

服务通信端口是网络扫描服务侦听从 AnyConnect GUI 组件及某些其他实用程序组件传入的连接的端口。

### 开始之前

不应该更改此设置，除非客户端支持人员指导您这么做。

### 过程

---

- 步骤 1** 使用以下方法之一启动网络安全配置文件编辑器：
- 打开 ASDM 并选择 **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Profile**。
  - 在 Windows 单机模式下，选择 **Start > All Programs > Cisco > Cisco AnyConnect Profile Editor > Web Security Profile Editor**。
- 步骤 2** 选择要编辑的网络安全客户端配置文件，然后点击 **Edit**。在 **Web Security** 树窗格中点击 **Advanced**。
- 步骤 3** 编辑 **Service Communication Port** 字段。
- 步骤 4** 保存网络安全客户端配置文件。
- 注释** 如果更改端口的默认值 5300，必须重新启动网络安全服务和 AnyConnect GUI 组件。
- 

## 配置超时/重试的发生时间

连接超时设置使您可以设置网络安全尝试访问互联网之前的超时值（不使用扫描代理）。如果保留为空，则使用的默认值为 4 秒。此设置使用户可以更快地访问已付费的网络服务，而不必等待发生超时再重试。

## 过程

**步骤 1** 使用以下方法之一启动网络安全配置文件编辑器：

- 打开 ASDM 并选择 **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Profile**。
- 在 Windows 单机模式下，选择 **Start > All Programs > Cisco > Cisco AnyConnect Profile Editor > Web Security Profile Editor**。

**步骤 2** 打开要编辑的网络安全客户端配置文件。

**步骤 3** 在 Web Security 树窗格中点击 **Advanced**。

**步骤 4** 更改 **Connection Timeout** 字段。

**步骤 5** 保存网络安全客户端配置文件。

## DNS 查找

配置文件编辑器的 **Advanced** 面板包含几个用于管理域名服务器查询的字段。这些设置已经为 DNS 查找配置了最佳值。

### 指南

不应该更改此设置，除非客户端支持人员指导您这么做。

## 调试设置

**Debug Level** 是一个可配置字段。

### 指南

不应该更改此设置，除非客户端支持人员指导您这么做。

## 阻止和允许流量

在连接故障策略列表中，选择 **Fail Close** 以在无法与思科云网络安全代理服务器建立连接时阻止流量。或者，选择 **Fail Open** 以允许流量。

在 **When a captive portal is detected** 列表中，选择 **Fail Open** 以在无法与思科云网络安全代理服务器建立连接但检测到强制网络门户（如 Wi-Fi 热点）时允许流量。或者，选择 **Fail Close** 以阻止流量。



注释

如果主机、代理或静态例外配置为包括强制网络门户地址，则 **Fail Close** 不会阻止流量。

## 其他可定制的网络安全选项

### 导出选项

#### 导出纯文本网络安全客户端配置文件

从 ASA 导出模糊的网络安全客户端配置文件并将其分配到终端设备。

#### 过程

- 
- 步骤 1** 打开 ASDM，选择 **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Profile**。
  - 步骤 2** 选择要编辑的网络安全客户端配置文件，然后点击 **Export**。
  - 步骤 3** 浏览到本地文件夹以保存文件。编辑 Local Path 字段中的文件名，以使用此新文件名来保存网络安全客户端配置文件。
  - 步骤 4** 点击 **Export**。  
ASDM 即导出网络安全客户端配置文件的明文版本 filename.wsp。
- 

#### 导出 DART 捆绑包的纯文本网络安全客户端配置文件

如果需要将诊断 AnyConnect 报告工具 (DART) 捆绑包发送到思科客户服务，请连同 DART 捆绑包一起发送网络安全客户端配置文件 (filename.wsp 或 filename.xml) 的明文版本。思科客户服务无法读取模糊的版本。

配置文件编辑器的独立版本可创建两个版本的网络安全配置文件：一个为模糊处理版本，文件名为 filename.wso, ; 另一个为纯文本版本，文件名为 filename.xml。

向思科客户服务发送 DART 捆绑包前，将纯文本版本的网络安全客户端配置文件添加到 DART 捆绑包中。

#### 从 ASDM 编辑并导入明文网络安全客户端配置文件

导出明文网络安全客户端配置文件后，可使用任何明文或 XML 编辑器在本地计算机上编辑此文件，该编辑器允许编辑 AnyConnect 网络安全配置文件编辑器不支持的文件。除非客户端支持人员有明确指示，否则您不应更改网络安全客户端配置文件的明文版本。使用此过程来导入编辑器。

#### 开始之前

导入该文件将覆盖所选的网络安全客户端配置文件的内容。



## 过程

- 步骤 1** 打开 ASDM，选择 **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Client Profile**。
- 步骤 2** 选择要编辑的网络安全客户端配置文件，然后点击 **Export**。
- 步骤 3** 在更改 `filename.wsp` 后，返回到 AnyConnect Client Profile 页面，然后选择您编辑的文件的配置文件名称。
- 步骤 4** 点击 **Import**。
- 步骤 5** 浏览到网络安全客户端配置文件的已编辑版本，然后点击 **Import**。

## 导出经过模糊处理的网络安全客户端配置文件

### 过程

- 步骤 1** 打开 ASDM 并选择 **Tools > File Management**。
- 步骤 2** 在 File Management 屏幕中选择 **File Transfer > Between Local PC and Flash**，并使用 File Transfer 对话框将模糊的 `filename.wso` 客户端配置文件传输到您的本地计算机中。

## 为网络安全配置拆分隧道排除

当用户建立 VPN 会话后，所有网络流量均通过 VPN 隧道发送。但是，当 AnyConnect 用户使用网络安全时，在终端产生的 HTTP 流量需要从隧道排除，并直接发送到云网络安全扫描代理。

要为用于云网络安全扫描代理的流量设置拆分隧道排除，请使用组策略中的 **Set up split exclusion for Web Security** 按钮。

### 开始之前

- 配置用于 AnyConnect 客户端的网络安全。
- 创建一个组策略，然后为其分配使用网络安全配置的 AnyConnect 客户端的一个连接配置文件。

如果使用安全值得信赖的网络检测功能，并且想确保网络安全和 VPN 同时处于活动状态，请配置网络，以便 HTTPS 服务器不可通过 VPN 隧道连接。这样，仅当用户在企业局域网中时，网络安全功能才进入旁路模式。

## 过程

- 步骤 1 在 ASDM 中，转到 **Configuration > Remote Access VPN > Network (Client) Access > Group Policies**。
- 步骤 2 选择组策略，点击 **Edit** 或 **Add** 可编辑或新增组策略。
- 步骤 3 选择 **Advanced > Split Tunneling**。
- 步骤 4 点击 **Set up split exclusion for Web Security**。
- 步骤 5 输入新的或选择现有的用于网络安全分隔排除的接入列表。ASDM 设置要用于网络列表的访问列表。
- 步骤 6 对新列表点击 **Create Access List**，或者对现有列表点击 **Update Access List**。
- 步骤 7 点击 **OK**。

## 接下来的操作

添加其他扫描代理时，请使用新信息更新您在此过程中创建的统一访问列表。

## 使用思科云网络安全托管配置文件

从 AnyConnect 版本 3.0.4 开始，通过网络安全托管客户端配置文件的 Cisco ScanCenter 托管配置可以为网络安全客户端提供新配置。带网络安全功能的设备可以从云端（位于 Cisco ScanCenter 服务器上的托管配置文件）下载新的网络安全托管客户端配置文件。使用网络安全配置文件编辑器创建客户端配置文件，然后将明文 XML 文件上传到 Cisco ScanCenter 服务器。该 XML 文件必须包含来自思科云网络安全的有效许可证密钥。新配置文件应用于托管配置服务器后，客户端最多可在 8 小时内将其取回。

在从托管配置 (Cisco ScanCenter) 服务器取回新客户配置文件时，托管配置功能使用该许可证密钥。如果现有网络安全客户端配置文件中的许可证与托管服务器上客户端配置文件关联的许可证相同，则一旦服务器上出现新客户配置文件，带网络安全的设备就会自动轮询服务器并下载新客户配置文件。下载新客户配置文件后，在您使新客户配置文件可用之前，网络安全不会再次下载同一文件。

有关许可证密钥的详细信息，请参阅 *Cisco ScanCenter* 管理指南，版本 5.2。

## 开始之前

- 使用包含思科云网络安全许可证密钥的有效客户端配置文件安装网络安全客户端设备。
- 重启网络安全代理服务选项仅供拥有重启服务所需权限的用户使用。

## 过程

- 步骤 1** 使用网络安全配置文件编辑器，为网络安全设备创建新的客户端配置文件。该客户端配置文件必须包含思科云网络安全许可证密钥。
- 步骤 2** 将该客户端配置文件另存为明文 XML 文件。将此文件上传到 Cisco ScanCenter 服务器。文件上传后，使新的客户端配置文件可用于网络安全客户端。
- 步骤 3** 如果为公司启用了托管配置功能，则通过 Cisco ScanCenter 为公司上传新的客户端配置文件并应用该配置文件。托管客户端配置文件与某个许可证关联。如果正在使用不同的许可证（例如，不同的组许可证密钥），每个许可证都可以有各自关联的客户端配置文件。然后您可以向不同的用户推送不同的客户端配置文件，具体取决于为用户配置的许可证。您可以为每个许可证存储多个配置，并设置供客户端下载的默认客户端配置文件。用户随后可以切换到存储在 Cisco ScanCenter 的托管配置区域中的其他配置修订版之一，方法是选择该客户端配置文件作为默认客户端配置文件。一个许可证只与一个客户端配置文件关联；因此，当有多个修订版与许可证关联时，只能有一个默认客户端配置文件。

## 关闭和启用 Cisco AnyConnect 网络安全代理

您可通过执行以下步骤关闭和启用 Cisco AnyConnect 网络安全代理拦截网络流量的功能。

### 使用 Windows 关闭和启用过滤器

#### 过程

- 步骤 1** 打开命令提示符窗口。
- 步骤 2** 转到 `%PROGRAMFILES%\Cisco\Cisco AnyConnect Secure Mobility Client` 文件夹。
- 步骤 3** 打开或关闭过滤：
  - 要启用过滤，请输入 `acwebsecagent.exe -enablesvc`
  - 要禁用过滤，请输入 `acwebsecagent.exe -disablesvc -servicepassword`

### 使用 Mac OS X 关闭和启用过滤器

服务密码在网络安全配置文件编辑器的 Authentication 面板中配置。

## 过程

---

**步骤 1** 启动 Terminal 应用。

**步骤 2** 转到 `/opt/cisco/anyconnect/bin` 文件夹。

**步骤 3** 启用或关闭过滤：

- 要启用过滤，请输入 `./acwebsecagent -enablesvc`。
  - 要禁用过滤，请输入 `./acwebsecagent -disablesvc -servicepassword`。
- 

# 网络安全日志记录

## Windows

所有网络安全消息都记录在 Event Viewer (Local)\Cisco AnyConnect Web Security Module 文件夹的 Windows 事件查看器中。该事件查看器中的事件网络安全记录由思科技术支持中心的工程师进行分析。

## Mac OS X

查看来自系统日志或控制台的网络安全消息。



## 第 8 章

# 配置 AMP 启用程序

- [关于 AMP 启用程序，第 197 页](#)
- [AMP 启用程序部署，第 197 页](#)
- [AMP 启用程序配置文件编辑器，第 198 页](#)
- [AMP 启用程序的状态，第 198 页](#)

## 关于 AMP 启用程序

AnyConnect AMP 启用程序用作终端部署高级恶意软件防护 (AMP) 的介质。它将面向终端的 AMP 软件从企业中本地托管的服务器推送到一个终端设备子集，并将 AMP 服务安装到现有用户群中。此方法为 AnyConnect 用户群管理员提供了额外的安全代理，可以检测网络中可能发生的潜在恶意软件威胁、删除这些威胁并保护企业免受危害。它能节省带宽和下载时间，不需要在门户端进行任何更改，而且无需向终端发送身份验证凭证即可完成操作。

## AMP 启用程序部署

为了恰当地分发面向终端的 AMP 软件，必须完成以下工作流程。

- 1 登录面向终端的 AMP 门户。
- 2 在面向终端的 AMP 门户上配置适当的策略。根据您的策略，将创建相应的面向终端的 AMP 软件包。该软件包是适用于 Windows 的 .exe 文件或适用于 Mac 的 .pkg 文件。对于 Windows，您可以选择可再分发的 .exe 文件。
- 3 将生成的套件（Windows 或 Mac）下载到本地服务器中。
- 4 登录 ASA 或 ESS 头端创建并保存 AMP 启用程序配置文件。
- 5 在 ASA 或 ESS 头端上，从可选模块列表中选择 AMP 启用程序模块并指定 AMP 启用程序配置文件。

您创建的配置文件将用于 AnyConnect AMP 启用程序。AMP 启用程序连同此配置文件一起从 ASA 或 ESS 头端被推送到终端。

## AMP 启用程序配置文件编辑器

管理员可以选择使用独立编辑器创建 AMP 启用程序配置文件，然后将此配置文件上传到 ASA。否则，会在 Policy Elements 下的 ISE UI 中或在 ASDM 中配置嵌入式 AMP 启用程序配置文件编辑器。为使本地 Web 服务器与 AMP 配置文件编辑器结合使用，必须使用 keytool 命令将根 CA 证书导入到 Java 证书库中：

```
对于 Windows - keytool -import -keystore [JAVA-HOME]/lib/security/cacerts -storepass changeit -trustcacerts -alias root -file [PATH_TO_THE_CERTIFICATE]/certnew.cer
```

```
对于 Mac - sudo keytool -import -keystore [JAVA-HOME]/lib/security/cacerts -storepass changeit -trustcacerts -alias root -file [PATH_TO_THE_CERTIFICATE]/certnew.cer
```

- 名称
- 描述
- Install AMP for Endpoints - 选择是否要将此配置文件配置为安装适用于终端的 AMP。
- Uninstall AMP for Endpoints- 选择是否要将此配置文件配置为卸载适用于终端的 AMP。如果选择卸载，则在其他字段中不应有任何输入。
- Windows Installer - 输入 .exe 文件所在的本地托管服务器地址或 URL。
- Mac Installer - 输入 .pkg 文件所在的本地托管服务器地址或 URL。
- Check - 点击运行对 URL 的检查以确保其有效。有效 URL 是可访问并包含受信任证书的 URL。如果服务器可访问，并且在此 URL 建立了连接，则可以保存配置文件。
- Add to Start Menu - 创建“开始”菜单快捷方式。
- Add to Desktop - 创建桌面图标。
- Add to Context Menu - 如果选择此选项，则可以从任何文件或文件夹右键点击，然后选择 Scan Now 激活扫描。

## AMP 启用程序的状态

任何与实际下载和安装 AMP 相关的消息都显示为 AnyConnect 用户界面的 AMP Enabler 磁贴中的部分磁贴。安装后，所有与 AMP 相关的消息都位于 AMP 中，可在终端用户界面中显示。例如，当防恶意软件保护安装或卸载时，如果收到任何出现故障或需要重新启动的指示，用户就会看到消息。



## 第 9 章

# 在本地策略中启用 FIPS

- [关于 FIPS、NGE 和 AnyConnect](#)，第 199 页
- [为 AnyConnect 核心 VPN 客户端配置 FIPS](#)，第 202 页
- [为网络访问管理器配置 FIPS](#)，第 203 页

## 关于 FIPS、NGE 和 AnyConnect

AnyConnect 集成了思科通用加密模块 (C3M)。此思科 SSL 实施在其下一代加密 (NGE) 算法中，包含了符合联邦信息处理标准 (FIPS) 140-2 标准的加密模块和美国国家安全局 (NSA) 套件 B 加密。

NGE 引入新加密、身份验证、数字签名和密钥交换算法，以升级安全和性能需求。RFC 6279 定义设备为符合美国 FIPS 140-2 标准而必须支持的套件 B 加密算法。

AnyConnect 组件根据头端、ASA 或 IOS 路由器的配置协商并使用 FIPS 标准加密。以下 AnyConnect 客户端模块支持 FIPS:

- **AnyConnect 核心 VPN** - 通过在用户计算机上的本地策略文件中使用 FIPS 模式参数，启用符合 FIPS 标准的 VPN 客户端。套件 B 加密仅适用于 IKEv2/IPsec VPN 连接。有关详细信息和过程，请参阅 [为 AnyConnect 核心 VPN 客户端配置 FIPS](#)。

除 FIPS 模式以外，AnyConnect 本地策略文件 AnyConnectLocalPolicy.xml 还包含适用于本地客户端的其他安全设置。此文件并未通过 ASA 进行部署，且必须手动安装，或使用企业软件部署系统进行部署。有关使用此配置文件的详细信息，请参阅 [AnyConnect 本地策略](#)。

- **AnyConnect 网络访问管理器** - 通过在 AnyConnectLocalPolicy.xml 文件中使用 FIPS 模式参数和在网络访问管理器配置文件中使用的 FIPS 模式参数，启用符合 FIPS 标准的网络访问管理器。Windows 中支持用于网络访问管理器的 FIPS。有关详细信息和步骤，请参阅 [为网络访问管理器配置 FIPS](#)。

## AnyConnect 中的 FIPS 功能

功能	核心 VPN 模块	网络访问管理器模块
对称加密和完整性的 AES-GCM 支持。	用于 IKEv2 负载加密和身份验证的 128 位、192 位和 256 位密钥。 ESP 数据包加密和身份验证。	软件中有线流量加密的 802.1AE (MACsec) 的 128 位密钥 (Windows)。
哈希值算法的 SHA-2 支持，采用 256/384/512 位的 SHA。	IKEv2 负载身份验证和 ESP 数据包身份验证。(Windows 7 或更高版本和 Mac OS X 10.7 或更高版本。)	能够在基于 TLS 的 EAP 方法中使用 SHA-2 证书。
密钥交换的 ECDH 支持。	组 19、20 和 21 IKEv2 密钥交换及 IKEv2 PFS。	能够在基于 TLS 的 EAP 方法中使用 ECDH (Windows)。
ECDSA 支持数字签名、非对称加密和身份验证，以及 256 位、384 位和 521 位椭圆曲线。 <sup>1</sup>	IKEv2 用户身份验证和服务器证书验证。	能够在基于 TLS 的 EAP 方法中使用 ECDSA 证书。
其他支持	IPsecV3 所需的所有加密算法预期为空加密。 <sup>2</sup> IKEv2 的 Diffie-Hellman 组 14 和 24。 DTLS 和 IKEv2 的 4096 位密钥 RSA 证书。	不适用

<sup>1</sup> 在 Linux 上，ECDSA 仅支持 AnyConnect 文件库。要向文件存储库添加证书，请参阅[为 Mac 和 Linux 创建 PEM 证书存储库](#)。

<sup>2</sup> IPsecV3 还指定必须支持扩展序列号 (ESN)，但是 AnyConnect 不支持 ESN。

## AnyConnect FIPS 要求

- 套件 B 加密仅适用于 IKEv2/IPsec VPN 连接。
- 安全网关中需要 FIPS 和/或套件 B 支持。思科在 ASA 9.0 版及更高版本中提供套件 B 功能，在 ASA 8.4.1 版及更高版本中提供 FIPS 功能。
- ECDSA 证书要求：
  - 摘要强度必须大于或等于曲线强度。例如，EC-384 密钥必须使用 SHA2-384 或更高版本。



- 在以下操作系统上受支持：Windows 7 或更高版本、Mac OS X 10.7 或更高版本、Red Hat Enterprise Linux 6.x 或 6.4（64 位），以及 Ubuntu 12.4 和 12.10（64 位）。ECDSA 智能卡仅在 Windows 7 中受支持。

## AnyConnect FIPS 的限制

- AnyConnect 不支持 TLS/DTLS、SRTP 和 SSH 套件 B。
- 在验证使用 SHA-2 签署的证书时，除了在基于 TLS 的 EAP 中，没有 EAP 方法支持 SHA-2。
- 不支持 TLS v1.2 握手。
- 不支持 TLS v1.2 证书身份验证。

## AnyConnect FIPS 指南

- AnyConnect 客户端的 Statistics 面板（在 Transport Information 标题下）显示正在使用的密码名称。
- 由于 AES-GCM 是计算密集型的算法，因此使用这些算法时您可能会体验到整体数据速率降低。部分新 Intel 处理器包含专门引进以提升 AES-GCM 性能的特别说明。AnyConnect 会自动检测正在运行的处理器是否支持这些新指令。若支持，AnyConnect 将使用新指令，从而相对于那些没有特殊指令的处理器来说，可以显著提高 VPN 数据速率。请参阅 <http://ark.intel.com/search/advanced/?s=t&AESTech=true>，了解支持新指令的处理器列表。有关详细信息，请参阅 <http://software.intel.com/en-us/articles/intel-carry-less-multiplication-instruction-and-its-usage-for-computing-the-gcm-mode/>。
- 组合模式加密算法（它在一次操作中同时执行加密和完整性验证）仅在具有硬件加密加速的 SMP ASA 网关（例如 5585 和 5515-X）上受支持。AES-GCM 是思科支持的组合模式加密算法。



### 注释

IKEv2 策略既可以包含普通模式加密算法，也可以包含组合模式加密算法，但不能同时包含这两种类型。当组合模式算法配置在 IKEv2 策略中时，所有普通模式算法都被禁用，因此唯一有效的完整性算法为 NULL。

IKEv2 IPsec 提议使用其他模型，可以在同一提议中同时指定普通模式和组合模式加密算法。对于这种用法，您需要为这两种算法都配置完整性算法，给 AES-GCM 加密算法配置的是非 NULL 完整性算法。

- 当 ASA 配置为对 SSL 和 IPsec 使用不同的服务器证书时，请使用受信任证书。如果使用具有不同 IPsec 和 SSL 证书的套件 B (ECDSA) 不受信任证书，则状态评估、WebLaunch 或下载程序可能发生故障。

### 避免因 AnyConnect FIPS 注册表更改导致的终端问题

为核心 AnyConnect 客户端启用 FIPS 会更改终端上的 Windows 注册表设置。终端的其他组件可能会检测到 AnyConnect 已启用 FIPS 并开始使用加密。例如，Microsoft 终端服务客户端远程桌面协议 (RDP) 将不工作，因为 RDP 要求服务器使用符合 FIPS 的加密。

为避免这些问题，您可以通过将参数 Use FIPS compliant algorithms for encryption, hashing, and signing 更改为 Disabled，在 Windows Local System Cryptography 设置中临时禁用 FIPS 加密。请注意重启终端设备将此设置改回已启用。

下表显示您应了解的 AnyConnect 执行的 Windows 注册表更改：

注册表项	更改
HKLM\System\CurrentControlSet\Control\Lsa	FIPSAlgorithmPolicy 从 0 更改为 1。
HKCU\Software\Microsoft\Windows\CurrentVersion\Internet Settings	通过使用原始设置对 0x080 执行按位 OR 运算，SecureProtocols 设置更改为 TLSV1。
HKLM\Software\Policies\Microsoft\Windows\CurrentVersion\Internet	通过使用原始设置对 0x080 执行按位 OR 运算，SecureProtocols 设置更改为 TLSV1。 这会为组策略设置 TLSv1。

## 为 AnyConnect 核心 VPN 客户端配置 FIPS

### 为 AnyConnect 核心 VPN 启用 FIPS

#### 过程

**步骤 1** 在 AnyConnect 配置文件编辑器中打开或创建一个 VPN 本地策略配置文件。

**步骤 2** 选择 **FIPS Mode**。

**步骤 3** 保存此 VPN 本地策略配置文件。

我们建议您对此配置文件进行命名来表示已启用 FIPS。

### 在 Windows 安装期间启用 FIPS

对于 Windows 安装，您可以将 Cisco MST 文件应用于标准 MSI 安装文件，以便在 AnyConnect 本地策略中启用 FIPS。有关此 MST 文件的下载位置的信息，请参阅您收到的 FIPS 的许可信息。安装期间将生成已启用 FIPS 的 AnyConnect 本地策略文件。在运行此实用程序后，更新用户系统。



注释

此 MST 只启用 FIPS。它不会更改其他参数。要在 Windows 安装期间更改其他本地策略设置，请参阅[在 MST 文件中启用本地策略参数](#)。

## 为网络访问管理器配置 FIPS

网络访问管理器可配置为同时连接到 FIPS 和非 FIPS 网络，或者只连接到 FIPS 网络。

### 过程

#### 步骤 1 为网络访问管理器启用 FIPS。

启用 FIPS 可允许网络访问管理器同时连接到 FIPS 和非 FIPS 网络。

#### 步骤 2 如果需要，请参阅[为网络访问管理器实施 FIPS 模式](#)。

实施 FIPS 模式会将网络访问管理器连接仅限于 FIPS 网络。

## 为网络访问管理器启用 FIPS

### 过程

#### 步骤 1 在 AnyConnect 本地策略中启用 FIPS 模式：

- a) 在 AnyConnect 配置文件编辑器中打开或创建一个 VPN 本地策略配置文件。
- b) 选择 **FIPS Mode**。
- c) 保存此 VPN 本地策略配置文件。  
我们建议您对此配置文件进行命名来表示已启用 FIPS。

#### 步骤 2 在 AnyConnect 网络访问管理器客户端配置文件中启用 FIPS 模式：

- a) 在 AnyConnect 配置文件编辑器中打开或创建一个网络访问管理器配置文件。
- b) 选择 **Client Policy** 配置窗口。
- c) 在 **Administrative Status** 部分下，为 **FIPS Mode** 选择 Enable。
- d) 保存网络访问管理器配置文件。  
我们建议您对此配置文件进行命名来表示已启用 FIPS。

## 为网络访问管理器实施 FIPS 模式

通过在网络访问管理器配置文件中限制允许的关联和加密模式以及身份验证方法，强制企业员工只连接到符合 FIPS 的网络。

必须首先[为网络访问管理器启用 FIPS](#) 以强制实施 FIPS 模式。

### 过程

- 
- 步骤 1** 在 AnyConnect 配置文件编辑器中打开网络访问管理器配置文件。
  - 步骤 2** 网络访问管理器 FIPS 合规性要求 FIPS 批准的 AES 加密模式，包括 WPA2 个人模式 (WPA2-PSK) 和 WPA2 企业模式 (802.1X)。
  - 步骤 3** 网络访问管理器 FIPS 支持 EAP 方法，包括 EAP-TLS、EAP-TTLS、PEAP、EAP-FAST 和 LEAP。
  - 步骤 4** 保存网络访问管理器配置文件。

我们建议您将配置文件命名为指出只能进行 FIPS 连接。

---



# 第 10 章

## Cisco AnyConnect 客户体验反馈模块



注  
释

默认情况下，思科将收集您的私人和企业数据。

客户体验反馈 (CEF) 模块为我们提供有关客户使用和启用的功能和模块的信息。此信息将让我们了解用户体验，从而让思科继续改善 AnyConnect 的质量、可靠性、性能和用户体验。

有关信息收集和使用的详细信息，请参阅[思科在线隐私声明要点](#)页面，其中提供了 [AnyConnect 安全移动客户端补充信息](#)。所有数据都以匿名方式收集，且不包含个人可识别数据。数据发送也将安全进行。

思科收集以下类型的数据：

- 使用情况数据 - 有关详细信息，请参阅隐私政策。此数据每月收集和发送一次。
- 网络威胁数据 - 发生威胁报告时即发送。
- 故障报告 - 每 24 小时检查一次 AnyConnect 生成的故障转储文件，收集并发送至客户体验反馈服务器。

客户体验反馈模块的主要组件如下：

- 反馈模块 - 用于收集信息并定期发送到服务器的 AnyConnect 软件组件。
- 思科反馈服务器 - 思科自有的云基础设施，用于收集客户体验反馈数据，并以原始格式存储在临时存储区中。
- [配置客户体验反馈](#)，第 205 页

## 配置客户体验反馈

AnyConnect 客户体验反馈模块随 AnyConnect 部署，默认启用。您可以通过创建客户体验反馈配置文件来修改发送的反馈，包括完全退出体验反馈。此方法是禁用反馈模块的首选方法，但您也可以在任何 AnyConnect 部署过程中删除它。

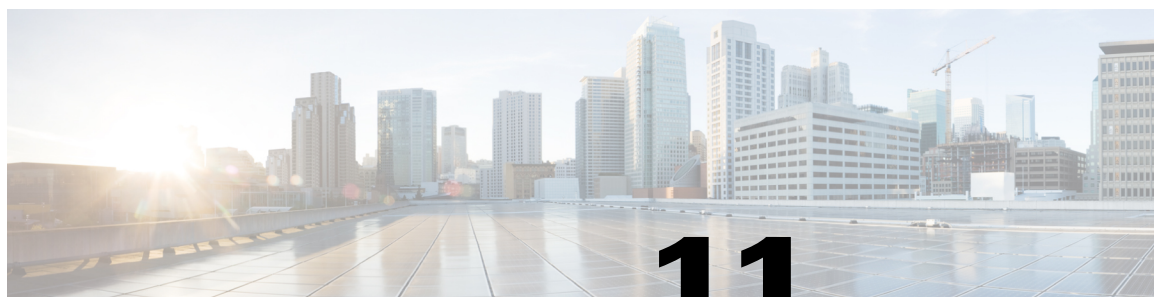
## 开始之前

客户体验反馈模块自动启用。

## 过程

---

- 步骤 1** 单独打开客户体验反馈配置文件编辑器或在 ASDM 中打开。导航到 **Configuration > Remote Access VPN (> Network (Client) Access > AnyConnect Client Profile**。
  - 步骤 2** 创建 AnyConnect 客户端配置文件，并且提供**反馈服务配置文件的配置文件使用情况**。
  - 步骤 3** 如果您不想提供反馈，请取消选中 **Enable customer Experience Feedback Service**。  
安装后可随时禁用反馈。
  - 步骤 4** 如果不想发送 AnyConnect 生成的故障报告，请取消选中 **Include Crash Report**。  
默认包括故障报告。
  - 步骤 5** 输入您选择的客户密钥或 ID。  
此 ID 可让思科识别您的组织的信息。
-



# 第 11 章

## 移动设备上的 AnyConnect

移动设备上的 AnyConnect 类似于 Windows、Mac 和 Linux 平台上的 AnyConnect。本章介绍设备信息、配置信息、支持信息，以及适用于移动设备的 AnyConnect 特定的其他管理任务。

- [移动设备上的 AnyConnect 操作和选项](#)，第 207 页
- [Apple iOS 设备上的 AnyConnect](#)，第 212 页
- [Android 设备上的 AnyConnect](#)，第 215 页
- [在 ASA 安全网关上配置移动设备 VPN 连接](#)，第 216 页
- [在 AnyConnect VPN 配置文件中配置移动设备连接](#)，第 220 页
- [使用 URI 处理程序自动执行 AnyConnect 操作](#)，第 223 页
- [对移动设备上的 Anyconnect 进行故障排除](#)，第 230 页

## 移动设备上的 AnyConnect 操作和选项

### 关于 AnyConnect 移动 VPN 连接

AnyConnect 安全移动客户端可用于 Apple iOS 和 Android 移动设备。各个受支持平台的应用商店中都提供 Cisco AnyConnect。它并未在 [www.cisco.com](http://www.cisco.com) 上提供，也不通过安全网关分发。

AnyConnect 移动应用仅包含核心 VPN 客户端，不包括其他 AnyConnect 模块，例如网络访问管理器、终端安全评估或网络安全；但是，VPN 正在连接时，将向使用 AnyConnect Identify Extensions (ACIDex) 的头端提供终端安全评估信息（称为 Mobile Posture）。

AnyConnect VPN 连接通过以下方法之一建立：

- 由用户在 AnyConnect UI 中选择连接条目时手动建立。
- 由用户在点击管理员提供的自动连接操作时手动建立。请参阅[使用 URI 处理程序自动执行 AnyConnect 操作](#)，第 223 页。

- 通过“按需连接”功能自动建立。（仅适用于 Apple iOS）。

## 移动设备上的 AnyConnect VPN 连接条目

连接条目通过安全网关的完全限定域名或 IP 地址（如有需要，包括隧道组 URL）识别安全网关地址，并包括许多其他连接属性。

AnyConnect 支持在一个移动设备上拥有多个连接条目，以便寻址不同安全网关和/或 VPN 隧道组。如果配置了多个连接条目，则用户应了解使用哪个条目来发起 VPN 连接。通过以下方法之一来配置连接条目：

- 用户手动配置。  
有关在移动设备上配置连接条目的过程，请参阅相应的用户指南。
- 连接条目将在用户点击管理员提供的用于配置连接条目的链接后添加。  
请参阅[生成 VPN 连接条目](#)，第 224 页可向用户提供此类连接条目配置。
- 由 Anyconnect VPN 客户端配置文件定义。

AnyConnect VPN 客户端配置文件指定客户端行为并定义 VPN 连接条目。有关详细信息，请参阅在[AnyConnect VPN 配置文件中配置移动设备连接](#)，第 220 页。

## 隧道模式

AnyConnect 可以在托管或未托管的自带设备 (BYOD) 环境中运行。这些环境中的 VPN 隧道只在以下一种模式中运行：

- 系统隧道模式 - VPN 连接用于传送所有数据（全隧道），或仅传送流入/流出特定域或地址的数据（拆分隧道）。
- Per App VPN 模式 - VPN 连接用于移动设备上的特定应用集。

AnyConnect 允许的应用集由头端上的管理员使用 ASA 定制属性机制进行定义。此列表将发送给 AnyConnect 客户端，并在设备上实施。对于所有其他应用，在隧道之外或以明文形式发送数据。

在 Apple iOS 上，要求托管环境在此模式下运行。在 Android 上，托管和未托管环境均受支持。在这两个平台上的托管环境中，移动设备管理器还必须将设备配置为传送与 AnyConnect 配置传送相同的应用列表。

AnyConnect 基于从 ASA 头端接收的配置信息确定它将在哪种模式下运行。具体而言，当正建立会话时，与连接相关的组策略或动态访问策略 (DAP) 中存在或缺少 Per App VPN 列表。如果 Per App VPN 列表存在，AnyConnect 将在 Per App VPN 模式下运行；如果它不存在，AnyConnect 将在系统隧道模式下运行。



## 移动设备的安全网关身份验证

建立 VPN 连接时，AnyConnect 将使用从安全网关接收的数字证书来验证服务器的身份。如果服务器证书无效（因过期或日期无效、密钥使用错误或名称不匹配导致证书错误），或证书不受信任（证书无法由证书颁发机构验证），抑或同时出现上述两种情况，则连接将被阻止。此时将显示一条阻止消息，用户必须选择如何处理。

**Block Untrusted Servers** 应用设置确定 AnyConnect 在无法识别安全网关时的响应方式。默认情况下开启此保护；用户可关闭此保护，但不建议这样做。

当 **Block Untrusted Servers** 开启后，将向用户显示一条 **Untrusted VPN Server** 阻止通知，告知此安全威胁。用户可选择：

- **Keep Me Safe** 以终止此连接，保持安全。
- **Change Settings** 以关闭 Block Untrusted Servers 应用首选项，但不建议这样做。用户禁用此安全保护功能后，必须重新初始化 VPN 连接。

当 **Block Untrusted Servers** 关闭后，将向用户显示一条 **Untrusted VPN Server** 取消阻止通知，告知此安全威胁。用户可选择：

- **Cancel** 以取消连接并保持安全。
- **Continue** 以继续连接，但不建议这样做。
- **View Details** 以查看证书详细信息，更直观地判断证书的可接受性。

如果用户正在查看的证书有效但不受信任，则用户可以：

选择 **Import and Continue** 将服务器证书导入 AnyConnect 证书存储区供以后使用，并继续连接。

当此证书导入 AnyConnect 存储区后，使用此数字证书与服务器建立的后续连接将被自动接受。

返回上一屏幕并选择 **Cancel** 或 **Continue**。

如果证书因任何原因无效，用户只能返回上一屏幕并选择 **Cancel** 或 **Continue**。

最安全的网络 VPN 连接配置是：将 Block Untrusted Servers 设置为 ON，在安全网关上配置有效、受信任的服务器证书，并指示移动用户始终选择 Keep Me Safe。

## 移动设备上的客户端身份验证

要完成 VPN 连接，用户必须提供用户名和密码、数字证书或这两种形式的凭证进行身份验证。管理员可以定义隧道组上的身份验证方法。为了保证在移动设备上提供最佳用户体验，思科建议根据身份验证配置情况使用多个 AnyConnect 连接配置文件。您必须确定平衡用户体验和安全的最佳方法。我们的建议如下：

- 对于移动设备的基于 AAA 的身份验证隧道组，组策略应有很长的空闲超时（例如 24 小时），以让客户端在无需用户重新进行身份验证的情况下即可保持重新连接状态。
- 要实现最透明的最终用户体验，请仅使用证书进行身份验证。使用数字证书时，无需用户交互即可建立 VPN 连接。

为了使用证书对连接安全网关的移动设备进行身份验证，最终用户必须在其设备上导入证书。之后，此证书可用于自动证书选择，也可以手动将其与特定连接条目关联。可使用以下方法导入证书：

- 由用户手动导入。  
有关向移动设备导入证书的过程，请参阅相关的用户指南。
- 使用 SCEP。  
有关详细信息，请参阅 [配置证书注册](#)，第 118 页。
- 在用户点击管理员提供的链接以导入证书之后，便会添加。  
请参阅 [导入证书](#)，第 230 页为您的用户提供这种证书部署。

## 在移动设备上本地化

适用于 Android 和 Apple iOS 的 AnyConnect 安全移动客户端支持本地化，可根据用户的区域设置调整 AnyConnect 用户界面和消息。

### 预先打包的本地化

AnyConnect 和 Apple iOS 应用包括以下语言翻译：

- 加拿大法语 (fr-ca)
- 中文（台湾地区）(zh-tw)
- 捷克语 (cs-cz)
- 荷兰语 (nl-nl)
- 法语 (fr-fr)
- 德语 (de-de)
- 匈牙利语 (hu-hu)
- 意大利语 (it-it)
- 日语 (ja-jp)
- 韩语 (ko-kr)
- 拉丁美洲西班牙语 (es-co)
- 波兰语 (pl-pl)

- 葡萄牙语（巴西）(pt-br)
- 俄语 (ru-ru)
- 简体中文 (zh-cn)
- 西班牙语 (es-es)

安装 AnyConnect 时，这些语言的本地化数据会安装到移动设备上。显示的语言取决于在移动设备上指定的区域设置。AnyConnect 会依次使用语言规范和地区规范来确定最佳匹配设置。例如，安装完成后，在法语-瑞士(fr-ch)区域设置下，最终的显示为法语-加拿大(fr-ca)。AnyConnect 启动后，AnyConnect 用户界面和消息会立即翻译为本地语言。

### 下载的本地化

对于不在 AnyConnect 软件包中的语言，管理员向 ASA 添加要通过 AnyConnect VPN 连接下载到设备的本地化数据。

思科在 Cisco.com 的产品下载中心提供 anyconnect.po 文件，其中包括所有可本地化的 AnyConnect 字符串。AnyConnect 管理员可下载 anyconnect.po 文件，提供可用字符串的翻译，然后将文件上传到 ASA。已在 ASA 上安装 anyconnect.po 文件的 AnyConnect 管理员应下载此更新版本。

最初，AnyConnect 用户界面和消息以安装语言向用户显示。当最终用户首次连接到 ASA 时，AnyConnect 将设备的首选语言与 ASA 上可用的本地化语言进行比较。如果 AnyConnect 找到匹配的本地化文件，则下载该本地化文件。下载完成后，AnyConnect 将使用已添加到 anyconnect.po 文件的翻译字符串显示用户界面和用户消息。如果字符串未翻译，AnyConnect 将显示默认的英语字符串。

有关在 ASA 上配置本地化的说明，请参阅[将转换表导入自适应安全设备](#)，第 45 页。如果 ASA 不包含设备区域设置的本地化数据，将继续使用 AnyConnect 应用软件包中预装的本地化数据。

### 提供移动设备本地化的其他方法

[本地化 AnyConnect 用户界面和消息](#) 通过为用户提供 URI 链接。

要求移动设备用户在自己的设备上管理本地化数据。请参阅相应的用户指南来了解执行以下本地化活动的步骤：

- 从指定服务器导入本地化数据。用户选择导入本地化数据并指定安全网关的地址和区域设置。根据 ISO 639-1 指定区域设置，如适用，可添加国家代码（例如，en-US、fr-CA、ar-IQ 等等）。此本地化数据用来替代预先打包的已安装本地化数据。
- 恢复默认的本地化数据。此操作将恢复使用 AnyConnect 软件包中预装的本地化数据并删除所有已导入的本地化数据。

## 移动设备上的 FIPS 和套件 B 加密

用于移动设备的 AnyConnect 包含思科通用加密模块 (C3M)，该 Cisco SSL 实现包括 FIPS 140-2 兼容的加密模块和 NSA 套件 B 加密，是下一代加密 (NGE) 算法的一部分。套件 B 加密仅适用于 IPsec VPN；FIPS 兼容加密同时适用于 IPsec 和 SSL VPN。

连接时与头端协商加密算法的使用。协商取决于 VPN 连接两端的端功能。因此，安全网关还必须支持 FIPS 兼容加密和套件 B 加密。

用户可将 AnyConnect 配置为仅在协商期间接受 NGE 算法，方法是在 AnyConnect 应用设置中启用 **FIPS Mode**。当 FIPS Mode 处于禁用状态时，AnyConnect 也接受 VPN 连接使用非 FIPS 加密算法。

请参阅[关于 FIPS、NGE 和 AnyConnect](#)，第 199 页了解常规支持信息。

#### 其他移动准则和限制

- 套件 B 加密要求 Apple iOS 5.0 或更高版本；这是支持套件 B 中使用的 ECDSA 证书的 Apple iOS 最低版本。
- 套件 B 加密要求 Android 4.0 (Ice Cream Sandwich) 或更高版本；这是支持套件 B 中使用的 ECDSA 证书的 Android 最低版本。
- 在 FIPS 模式下运行的设备与按代理方法或传统方法使用 SCEP 为移动用户提供数字证书的方式不兼容。请相应计划您的部署。

## Apple iOS 设备上的 AnyConnect

有关此版本支持的功能和设备，请参阅[Cisco AnyConnect 安全移动客户端版本说明](#)，版本 4.0.x (Apple iOS)。

有关如何安装、升级或使用 AnyConnect 应用，请参阅[Cisco AnyConnect 安全移动客户端用户指南](#)，版本 4.0.x (Apple iOS)。

## Apple iOS 的特别注意事项

在 Apple iOS 设备上为 AnyConnect 提供支持时，请考虑以下注意事项：

- 本文档中的 SCEP 参考信息仅适用于 AnyConnect SCEP，不适用于 Apple iOS SCEP。
- 由于 Apple iOS 的限制，无法通过 VPN 推送邮件通知。但是，当隧道策略从会话中排除外部可访问的 ActiveSync 连接时，AnyConnect 可以与这些连接并行工作。

#### Apple iPhone 配置实用程序

Windows 或 Mac OS X 版本的 iPhone 配置实用程序 (IPCU) 用于对 Apple iOS 设备执行配置创建和部署过程，此程序可从 Apple 公司获取。此操作可代替在安全网关上配置 AnyConnect 客户端配置文件。

现有的 IPCU GUI 由苹果公司控制，不支持 AnyConnect IPsec 功能。通过在 Server 字段中使用以下 URI 语法（如 RFC 2996 中所定义），在 IPCU 中的现有 AnyConnect GUI 内配置 IPsec VPN 连接：（此 Server 字段语法与已记录的用于配置 SSL VPN 连接的用法向后兼容。）

```
[ipsec://][<AUTHENTICATION>[":" <IKE-IDENTITY> "@"]]
<HOST>[":" <PORT>["/" <GROUP-URL>]
```

参数	描述
ipsec	: 表示这是 IPsec 连接。如果省略, 则假设是 SSL。
AUTHENTICATION	指定 IPsec 连接的身份验证方法。如果省略, 则假设是 EAP-AnyConnect。有效值为: <ul style="list-style-type: none"> <li>• EAP-AnyConnect</li> <li>• EAP-GTC</li> <li>• EAP-MD5</li> <li>• EAP-MSCHAPv2</li> <li>• IKE-RSA</li> </ul>
IKE-IDENTITY	当 AUTHENTICATION 设置为 EAP-GTC、EAP-MD5 或 EAP-MSCHAPv2 时, 指定 IKE 标识。用于其他身份验证设置时, 此参数无效。
HOST	指定服务器地址。要使用的主机名或 IP 地址。
PORT	当前忽略, 包括用于与 HTTP URI 方案保持一致。
GROUP=URL	附加到服务器名称的隧道组名称。

示例:

```
ipsec://EAP-AnyConnect@asa-gateway.example.com
ipsec://asa-gateway.example.com
```

要仅连接到符合标准的 Cisco IOS 路由器, 请使用以下资源:

```
ipsec://eap-md5:<identity>@ios-gateway.example.com
```

### Connect on Demand 使用指南

Apple iOS Connect On Demand 功能支持其他应用 (例如 Safari) 发起 VPN 连接。Apple iOS 根据为设备的活动连接条目配置的规则评估应用所请求的域。仅在符合以下所有条件时, Apple iOS 才代表应用建立 VPN 连接:

- VPN 连接尚未建立。
- 与 Apple iOS Connect On Demand 框架兼容的应用请求一个域。
- 连接条目被配置为使用有效证书。
- 已在连接条目中启用 Connect On Demand。
- Apple iOS 无法将 Never Connect 列表中的字符串与域请求匹配。

- 出现以下两种情况之一：Apple iOS 将 Always Connect 列表中的字符串与域请求匹配（仅限在 Apple iOS 6 上），或者 DNS 查找失败，则 Apple iOS 将 Connect if Needed 列表中的字符串与域请求匹配。

使用 Connect On Demand 功能时，请牢记以下注意事项：

- 在通过 iOS 的按需连接发起 VPN 连接后，如果隧道在特定时间间隔内不活动（没有流量通过隧道），则 iOS 断开隧道连接。请参阅苹果公司的 VPN On Demand 文档了解详细信息。
- 如果您配置规则，我们建议使用 Connect if Needed 选项。如果内部主机上的 DNS 查找失败，Connect if Needed 规则将发起 VPN 连接。它需要正确的 DNS 配置，以便企业中的主机名仅使用内部 DNS 服务器进行解析。
- 对于配置了 Connect On Demand 的移动设备，基于证书的身份验证隧道组应该有一个短暂的（60 秒）空闲超时时间 (vpn-idle-timeout)。如果 VPN 会话对于应用并不重要且不需要始终连接，则设置短暂的空闲超时时间。苹果设备在不再需要 VPN 连接时（例如，设备进入休眠模式）会将其关闭。隧道组的默认空闲超时时间为 60 分钟。
- 始终连接的行为与版本有关：

在 Apple iOS 6 中，iOS 始终在此列表中的规则匹配时尝试发起 VPN 连接。

iOS 7.x 上不支持 Always Connect，当此列表中的规则匹配时，其行为与 Connect If Needed 规则相同。

更高版本中不使用 Always Connect，配置的规则将跳转到 Connect if Needed 列表，并按照该规则操作。

- 苹果公司已经向 Connect On Demand 功能引入了值得信赖的网络检测 (TND) 增强功能。此增强功能：

通过确定用户是否在受信任网络中扩展了 Connect On Demand 功能。

仅适用于 Wi-Fi 连接。使用其他类型的网络连接时，Connect On Demand 不使用 TND 来确定是否应连接 VPN。

不是单独的功能，无法在 Connect On Demand 功能之外配置或使用。

请联系苹果公司，了解有关 iOS 6 中 Connect On Demand 值得信赖的网络检测的详细信息。

- 集成的 Apple iOS IPsec 客户端和 AnyConnect 使用相同的 Apple iOS VPN on Demand 框架。

### 利用拆分隧道拆分 DNS 解析行为

ASA 拆分隧道功能允许您指定哪种流量通过 VPN 隧道，哪种流量畅通无阻。一个称为拆分 DNS 的相关功能允许您指定哪种 DNS 流量适合通过 VPN 隧道进行 DNS 解析，哪种 DNS 流量由终端 DNS 解析器处理（畅通无阻）。拆分 DNS 在 Apple iOS 设备上与在其他设备（如果也配置了拆分隧道）上的工作方式不同。Apple iOS 版本的 AnyConnect 对此命令的响应如下：

- 仅加密 split-dns 列表中所列域的 DNS 查询。

AnyConnect 仅通过隧道传输此命令中指定的域的 DNS 查询，而将所有其他 DNS 查询畅通无阻地发送到本地 DNS 解析器进行解析。例如，响应以下命令时，AnyConnect 仅通过隧道传输对 `example1.com` 和 `example2.com` 的 DNS 查询：

```
hostname(config-group-policy)# split-dns value example1.com example2.com
```

- 仅加密 `default-domain` 命令中域的 DNS 查询。

如果 `split-dns none` 命令存在，且 `default-domain` 命令指定了一个域，则 AnyConnect 仅通过隧道传输该域的 DNS 查询，而将所有其他 DNS 查询畅通无阻地发送到本地 DNS 解析器进行解析。例如，响应以下命令时，AnyConnect 仅通过隧道传输 `example1.com` 的 DNS 查询：

```
hostname(config-group-policy)# split-dns none
hostname(config-group-policy)# default-domain value example1.com
```

- 畅通无阻地发送所有 DNS 查询。如果 `split-dns none` 和 `default-domain none` 命令存在于组策略中，或者虽然这些命令不存在于组策略中，但存在于默认组策略中，则 AnyConnect 将所有 DNS 查询畅通无阻地发送到本地 DNS 解析器进行解析。



注释

如果未指定 `split-dns`，则组策略继承存在于默认组策略中的拆分隧道域列表。要防止继承拆分隧道域列表，请使用 `split-dns none` 命令。

## Android 设备上的 AnyConnect

有关此版本支持的功能和设备，请参阅 [Cisco AnyConnect 安全移动客户端版本说明，版本 4.0.x \(Android\)](#)。

有关如何安装、升级或使用 AnyConnect 应用，请参阅 [Cisco AnyConnect 安全移动客户端用户指南，版本 4.0 \(Android\)](#)。

## Android 特定注意事项

### Android 移动终端安全评估设备 ID 生成

AnyConnect 在安装时生成唯一的 40 字节的设备 ID。用户可在初始 AnyConnect 应用启动后查看生成的设备 ID（从 AnyConnect **Diagnostics > Logging and System Information > System > Device Identifiers** 屏幕），也可在 `device_identifiers.txt` 文件中的 AnyConnect 日志内进行查看。

生成的设备 ID 基于 Android ID 和以下值中的一个或两个值（如果这些值在安装时可用）：

- MEID/IMEI（移动设备标识符/国际移动设备标识）
- MAC-ADDRESS（MAC 地址）完全按照设备上 **Settings > About > Status** 中的显示使用。该值区分大小写，且如果设备中显示了“:”字符，则必须使用这些字符。

可用值	生成算法
如果在安装时两个值都可检索:	<code>device-ID = bytesToHexString(SHA1(Android-ID + MEID/IMEI + MAC-ADDRESS))</code>
如果在安装时只有 MEID/IMEI 可检索:	<code>device-ID = bytesToHexString(SHA1(Android-ID + MEID/IMEI))</code>
如果在安装时只有 MAC-ADDRESS 可检索:	<code>device-ID = bytesToHexString(SHA1(Android-ID + MAC-ADDRESS))</code>
如果在安装时 MEID/IMEI 和 MAC-ADDRESS 均不可检索:	使用随机数字和 Android-ID 一同生成设备 ID。

其中 Android-ID 和 bytesToHexString 的定义如下:

```
Android-ID = Secure.getString(context.getContentResolver(), Secure.ANDROID_ID)
```

```
String bytesToHexString(byte[] shalrawbytes){
 String hashHex = null;
 if (shalrawbytes != null){
 StringBuffer sb = new StringBuffer(shalrawbytes.length * 2);
 for (int i = 0; i < shalrawbytes.length; i++){
 String s = Integer.toHexString(0xFF & shalrawbytes[i]).toUpperCase();
 if (s.length() < 2) { sb.append("0");}
 sb.append(s);
 }
 hashHex = sb.toString();
 }
 return hashHex;
}
```

## 在 ASA 安全网关上配置移动设备 VPN 连接

### 过程

- 步骤 1** 请参阅 [Cisco ASA 系列 VPN ASDM 配置指南](#)，了解桌面和移动终端的通用配置过程，考虑以下注意事项：

属性	ASDM 位置	例外
主页 URL	<b>Configuration &gt; Remote Access VPN &gt; Network (Client) Access &gt; Group Policies &gt; Add / Edit &gt; Advanced &gt; AnyConnect Client &gt; Customization</b>	AnyConnect Mobile 忽略主页 URL 设置，您无法在身份验证成功后重定向移动客户端。



属性	ASDM 位置	例外
AnyConnect 连接配置文件名称和别名	<b>Configuration &gt; Remote Access VPN &gt; Network (Client) Access &gt; AnyConnect Connection Profiles &gt; Add / Edit</b>	请勿在用于 AnyConnect 移动客户端连接的隧道组（连接配置文件）的 Name 或 Aliases 字段中使用特殊字符。使用特殊字符可能导致 AnyConnect 客户端显示错误消息： <code>Connect attempt has failed after logging that it is Unable to process response from Gateway.</code>
Dead Peer Detection	<b>Configuration &gt; Remote Access VPN &gt; Network (Client) Access &gt; Group Policies &gt; Add / Edit &gt; Advanced &gt; AnyConnect Client</b>	因为服务器端失效对等项检测可阻止设备休眠，所以应该将其关闭。但是，客户端的失效对等项检测应保持开启，因为它使客户端可以确定隧道何时由于缺少网络连接而终止。
Keepalive 消息	<b>Configuration &gt; Remote Access VPN &gt; Network (Client) Access &gt; Group Policies &gt; Add / Edit &gt; Advanced &gt; AnyConnect Client</b>	我们建议禁用 keepalive 消息以保护移动设备的电池寿命，尤其是在启用了客户端失效对等项检测功能时。

**步骤 2** 根据需要，将移动终端安全评估配置为接受、拒绝或限制移动连接。  
请参阅 [Cisco ASA 系列 VPN ASDM 配置指南](#) 中的配置 DAP 中使用的终端属性过程。

**步骤 3** （可选）配置 Per App VPN 模式。  
如果未配置 Per App VPN 模式，则 AnyConnect 以系统隧道模式运行。AnyConnect Per App VPN 隧道需要：

- ASA 9.3.1 或更高版本以配置 Per App VPN 隧道。
  - AnyConnect v4.0 Plus 或 Apex 许可证。
  - 在非受管环境中运行 Android 5.0 (Lollipop) 或更高版本的设备。
- a) 安装 [Cisco AnyConnect 企业应用选择器工具](#)，第 217 页。
  - b) 定义 Per App VPN 策略，第 218 页使用 Application Selector 工具。
  - c) 创建 Per App 定制属性，第 219 页在 ASA 上。
  - d) 将定制属性分配到 ASA 上的策略，第 220 页。

## 安装 Cisco AnyConnect 企业应用选择器工具

应用选择器工具是一个独立应用，支持为 Android 和 Apple iOS 设备生成策略。

## 开始之前

Cisco AnyConnect 企业应用选择器需要 Java 7 或更高版本。

## 过程

- 
- 步骤 1** 从 [Cisco.com AnyConnect 安全移动客户端 v4.x 软件中心](#) 下载 Cisco AnyConnect 企业应用选择器工具。
- 步骤 2** 如果您在策略中使用 Google Play 商店中不提供的 Android 应用，则必须在系统中安装 Android SDK 和 Android SDK 构建工具。如果没有安装，请安装 Android SDK：
- 为您运行应用选择器工具所在的平台安装最新版本的 [Android SDK 工具](#)。  
使用默认路径和设置（包括：Install for All Users），为平台安装推荐的 **SDK Tools Only** 软件包，从而可按如下所述访问软件包实体。
  - 使用 Android SDK 管理器，安装最新版本的 **Android SDK Build-tools**。
  - 如果在应用选择器工具中收到提示，请通过指定其安装位置来配置对 Android 资产打包工具 **aapt** 的访问权限。
- 

# 定义 Per App VPN 策略

Per App VPN 策略包括一组规则，其中每条规则识别其数据流经隧道的一个应用。指定规则选项以在移动设备环境中更严格地标识允许的应用及其使用。Application Selector 工具使用来自应用的软件包文件 \*.apk 的信息可设置规则选项。请参阅 <http://developer.android.com/guide/topics/manifest/manifest-element.html> 以了解详细的软件包清单信息。

## 开始之前

Cisco AnyConnect 企业应用选择器需要 Java 7 或更高版本。

## 过程

- 
- 步骤 1** 启动 Application Selector 并选择您为其定义策略的移动设备平台：**Android** 或 **Apple iOS**。
- 步骤 2** 获取特定规则的应用数据包信息。或者，您还可以直接输入此信息。  
选择 **Import from Disk** - 选择位于本地系统上的应用。  
如果在应用选择器工具中收到提示，请通过指定其安装位置来配置对 Android 资产打包工具 **aapt** 的访问权限。
- 步骤 3** （可选）如果需要，请选择列出的一个应用，然后配置其他参数。  
对于 Android：
- Minimum Version - 软件包的清单属性 *android:versionCode* 中指定的所选应用的最低版本。
  - Match Certificate ID - 应用签名证书的摘要

- Allow Shared UID - 默认值为 true。如果设置为 false，则软件包清单中指定了 *android:sharedUserId* 属性的应用将不匹配此规则并被阻止访问隧道。

对于 Apple iOS:

- Match Thumbprint - 允许的应用必须匹配可执行文件的拇指指纹（哈希值）。这旨在匹配特定的应用版本。
- DNS Domains - 分号分隔的域列表，旨在由系统本地浏览器进行隧道化。例如：  
cisco.com;foo.com;bar.com。

注释 可能并非所有平台都支持此选项。

**步骤 4** 点击 **File > Save** 保存此 Per App VPN 策略。

**步骤 5** 选择 **Policy > View Policy** 查看已定义策略的表示。  
复制此字符串，这是将成为 ASA 上 *perapp* 定制属性值的字符串。

## 创建 Per App 定制属性

### 过程

- 步骤 1** 在 ASDM 中，导航到 **Configuration > Remote Access VPN > Network (Client) Access > Advanced > AnyConnect Custom Attributes** 以配置定制属性类型。
- 步骤 2** 选择 **Add** 或 **Edit** 并在 **Create / Edit Custom Attribute Type** 窗格中设置以下项：
- a) 将 *perapp* 输入为类型。  
类型必须是 *perapp*，它是 Per App VPN 的 AnyConnect 客户端了解的唯一属性类型。
  - b) 输入您选择的描述。
- 步骤 3** 点击 **OK** 关闭此窗格。
- 步骤 4** 导航到 **Configuration > Remote Access VPN > Network (Client) Access > Advanced > AnyConnect Custom Attribute Names** 以配置定制属性。
- 步骤 5** 选择 **Add** 或 **Edit** 并在 **Create / Edit Custom Attribute Name** 窗格中设置以下项：
- a) 选择 *perapp* 属性 **Type**。
  - b) 输入 **Name**。此名称用于将此属性分配到策略。
  - c) 选择 **Add**，可通过从策略工具复制 BASE64 格式并将其粘贴在此处来一个或多个值。  
每个值不得超过 420 个字符。如果值超出此长度，请为额外值内容添加多个值。配置的值将被合并，然后发送到 AnyConnect 客户端。
- 步骤 6** 点击 **OK** 关闭打开的配置窗格。

## 将定制属性分配到 ASA 上的策略

perapp 定制属性可以分配到组策略或动态访问策略。

### 过程

---

**步骤 1** 打开 ASA 上的策略：

- 对于组策略，导航到 **Configuration > Remote Access VPN > Network (Client) Access > Group Policies > Add / Edit > Advanced > AnyConnect Client > Custom Attributes**。
- 对于动态访问策略，导航到 **Configuration > Remote Access VPN > Network (Client) Access > Dynamic Access Policies Add / Edit**。在 **Access/Authorization Policy Attributes** 部分中，选择 **AnyConnect Custom Attributes** 选项卡。

**步骤 2** 点击 **Add** 或 **Edit** 添加或编辑现有属性，从而打开 **Create / Edit Custom Attribute** 窗格。

**步骤 3** 从下拉列表中选择预定义的 *perapp* 属性类型。

**步骤 4** 选择 **Select Value**，然后从下拉列表中选择预定义的值。

**步骤 5** 点击 **OK** 关闭打开的配置窗格。

---

## 在 AnyConnect VPN 配置文件中配置移动设备连接

AnyConnect VPN 客户端配置文件是指定客户端行为并定义 VPN 连接条目的 XML 文件。每个连接条目指定终端设备可访问的一个安全网关以及其他连接属性、策略和限制。使用 AnyConnect 配置文件编辑器来创建 VPN 客户端配置文件，其中包括移动设备的主机连接条目。

用户无法修改或删除从 ASA 传输到移动设备的 VPN 配置文件中定义的连接条目。用户只能修改和删除其手动创建的连接条目。

在任一时刻，AnyConnect 在移动设备上只保留一个当前 VPN 客户端配置文件。在启动自动或手动 VPN 连接后，新的 VPN 配置文件完全取代当前配置文件。如果用户手动删除当前配置文件，则会删除此配置文件，同时删除此配置文件中定义的所有连接条目。

### 过程

---

**步骤 1** 配置基本 VPN 访问。

请参阅 [配置 VPN 接入](#)，第 87 页以了解桌面和移动终端的常见过程，考虑以下例外情况：

配置文件属性	例外
Auto Reconnect	无论 Auto Reconnect 设置如何，AnyConnect Mobile 始终尝试执行 ReconnectAfterResume。

**步骤 2** 配置移动特定属性：

- a) 在 VPN 客户端配置文件中，选择导航窗格中的 **Server List**。
- b) 选择 **Add** 将新服务器条目添加至列表，或从列表中选择服务器条目并按 **Edit** 打开 Server List Entry 对话框。
- c) 配置移动特定参数（如 [AnyConnect 配置文件编辑器，移动设置](#)，第 221 页中所述）。
- d) 点击 **OK**

**步骤 3** 使用以下方式之一来分发 VPN 客户端配置文件：

- 配置 ASA 以在建立 VPN 连接后将客户端配置文件上传到移动设备。  
请参阅 [AnyConnect 配置文件编辑器](#)，第 65 页章节，了解关于如何将 VPN 客户端配置文件导入 ASA 并将其与组策略相关联的说明。
- 向用户提供 AnyConnect URI 链接以导入客户端配置文件。  
请参阅 [导入 VPN 客户端配置文件](#)，第 230 页，向您的用户提供这种部署过程。
- 让用户使用移动设备上的 **Profile Management** 来导入 AnyConnect 配置文件。  
请参阅相应的移动设备用户指南，了解特定于设备的过程。

## AnyConnect 配置文件编辑器，移动设置

相关主题 [在 AnyConnect VPN 配置文件中配置移动设备连接](#)，第 220 页

### Apple iOS/Android 设置

- **Certificate Authentication** - 与连接条目关联的证书身份验证策略属性为此连接指定证书的处理方式。有效值为：

**Automatic** - AnyConnect 自动选择连接时进行身份验证所使用的客户端证书。在这种情况下，AnyConnect 将查看所有已安装的证书、忽略那些过期证书、应用 VPN 客户端配置文件中定义的证书匹配条件，然后使用与条件匹配的证书进行身份验证。每当用户尝试建立 VPN 连接时，就会发生这种情况。

**Manual** - AnyConnect 将在下载配置文件并执行以下任一操作时，从 Android 设备上的 AnyConnect 证书存储区中搜索证书：

如果 AnyConnect 基于 VPN 客户端配置文件中定义的证书匹配条件找到一个证书，则它将该证书分配给连接条目并在建立连接时使用该证书。

如果无法找到匹配的证书，则证书身份验证策略将设置为 **Automatic**。

如果分配的证书因任何原因从 AnyConnect 证书存储区删除，则 AnyConnect 将证书身份验证策略重置为 **Automatic**。

**Disabled** - 客户端证书不用于身份验证。

- **Make this Server List Entry active when profile is imported** - 当 VPN 配置文件下载到设备时，将服务器列表条目定义为默认连接。只有一个服务器列表条目可以具有此名称。默认值为禁用。

### 仅适用于 Apple iOS 的设置

- **Reconnect when roaming between 3G/Wifi networks** - 该设置启用时（默认值），AnyConnect 在丢失连接、设备唤醒或连接类型发生更改（例如 EDGE(2G)、1xRTT(2G)、3G 或 Wi-Fi）后不限制用于尝试重新连接的时间。此功能提供了实现跨网络的持续安全连接的无缝移动性。此功能对于需要与企业连接的应用非常有用，但也会消耗更多的电池电量。

如果网络漫游被禁用，且 AnyConnect 丢失连接，它在必要时尝试重新建立连接的时间最长可达 20 秒。如果无法建立连接，用户或应用必须启动新的 VPN 连接（如果必须建立）。



注释 网络漫游不影响数据漫游或使用多个移动服务提供商。

- **Connect on Demand（需要证书颁发机构）** - 此字段可让您配置由 Apple iOS 提供的按需连接功能。您可创建一些规则列表，每当其他应用发起使用域名系统 (DNS) 解析的网络连接时即检查这些规则。

按需连接仅可在 Certificate Authentication 字段设置为 **Manual** 或 **Automatic** 时使用。如果 Certificate Authentication 字段设置为 **Disabled**，则此复选框将灰显。由 **Match Domain or Host** 和 **On Demand Action** 字段定义的按需连接规则在复选框灰显时仍可配置和保存。

相关主题 [Apple iOS 的特别注意事项](#)，第 212 页

- **Match Domain or Host** - 输入您希望为其创建按需连接规则的主机名 (host.example.com)、域名 (.example.com) 或部分域 (.internal.example.com)。请勿在此字段中输入 IP 地址 (10.125.84.1)。
- **On Demand Action** - 当用户尝试连接到上一步骤中定义的域或主机时，指定以下任一操作：

**Never connect** - 当此列表中的规则匹配时，iOS 不尝试发起 VPN 连接。此列表中的规则优先于所有其他列表。



**注释** 当 Connect on Demand 启用时，应用会将服务器地址自动添加到此列表中。这将防止您在尝试使用网络浏览器访问服务器的无客户端门户时自动建立 VPN 连接。如果您不希望发生此行为，请删除此规则。

**Connect if Needed** - 只有在系统无法使用 DNS 解析地址时，iOS 才会在此列表中的规则匹配时尝试发起 VPN 连接。

**Always Connect** - 始终连接行为与版本有关：

在 Apple iOS 6 中，iOS 始终在此列表中的规则匹配时尝试发起 VPN 连接。

iOS 7.x 上不支持 Always Connect，当此列表中的规则匹配时，其行为与 Connect If Needed 规则相同。

更高版本中不使用 Always Connect，配置的规则将跳转到 Connect if Needed 列表，并按照该规则操作。

- **Add/Delete** - 将 Match Domain or Host 和 On Demand Action 字段中指定的规则添加到规则表，或从规则表中删除选定的规则。

## 使用 URI 处理程序自动执行 AnyConnect 操作

AnyConnect 中的 URI 处理程序可让其他应用以通用资源标识符 (URI) 的形式向 AnyConnect 传递操作请求。为简化 AnyConnect 用户设置过程，请将 URI 嵌入网页或电邮消息上的链接，并且向用户提供访问说明。

### 开始之前

- AnyConnect 应用中的 URI 处理默认禁用。移动设备用户通过将 **External Control** 应用设置为 Enable 或 Prompt 来允许此功能。外部控制在启用后允许所有 URI 命令，而无需用户交互。设置提示后，用户会收到 URI 活动的通知，然后可在请求时选择允许或不允许该活动。如果您使用提示，则应该告知用户如何响应与 URI 处理相关的提示。
- 输入 URI 处理程序参数值时，必须使用 **URL 编码**。使用工具（例如此链接中的工具）对操作请求编码。此外，请参阅下面提供的示例。
- 在 URI 中，%20 代表空格、%3A 代表冒号 (:)、%2F 代表正斜线 (/)、%40 代表 @ 符号。
- URI 中的斜线是可选的。

### 过程

向用户提供以下任何操作的说明：

- [生成 VPN 连接条目](#)，第 224 页

- [建立 VPN 连接，第 227 页](#)
- [断开 VPN 连接，第 229 页](#)
- [导入证书，第 230 页](#)
- [导入 VPN 客户端配置文件，第 230 页](#)
- [本地化 AnyConnect 用户界面和消息](#)

要将 URI 添加到 HTML 页面，您需要使其成为超链接的一部分。以下示例显示如何在 HTML 超链接中使用 URI。示例中的粗体部分是 URI。

- HTTP 示例：

```
<p> <a href="anyconnect:import?type=pkcs12
&uri=http%3A%2F%2Fexample.com%2FCertName.p12">
click here to import certificate using http </p>
```

- FTP 示例：

```
<p> <ahref="anyconnect://import?type=pkcs12
&uri=ftp%3A%2F%2FAdministrator%3Apassword%40192.168.10.20%2Fcerts%2FCertName.pfx">
click here to import certificate using ftp </p>
```

- 安全数字卡示例：

```
<p> <a href="anyconnect://import?type=pkcs12
&uri=file%3A%2F%2Fsdcard%2CCertName.pfx">
click here to import certificate from sdcard on mobile device </p>
```



注释

Android 用户无法在 Web 浏览器的地址栏中输入这些 URI。用户需要从远程 Web 服务器访问这些 URI，或者可以点击邮件中的链接（取决于其邮件客户端）。

#### 相关主题

- [生成 VPN 连接条目，第 224 页](#)
- [建立 VPN 连接，第 227 页](#)

## 生成 VPN 连接条目

使用此 AnyConnect URI 处理程序可简化用户生成 AnyConnect 连接条目。

**anyconnect:[/]/create[/]?name=Description&host=ServerAddress[&Parameter1=Value&Parameter2=Value...]**

#### 指南

- *host* 参数是必要参数，其他所有参数都是可选参数。在设备上执行操作时，AnyConnect 会保存您输入到与 *name* 和 *host* 相关联的连接条目的所有参数值。
- 对要添加到设备的每个连接条目使用单独的链接。不支持在单个链路中指定多个创建连接条目操作。



## 参数

- **name**- AnyConnect 主屏幕的连接列表和 AnyConnect 连接条目的 Description 字段中显示的连接条目的唯一名称。AnyConnect 仅在名称唯一时才响应。建议名称不超过 24 个字符，以确保能正常显示在连接列表中。在字段中输入文本时，使用设备上显示的键盘上的字母、数字或符号。字母区分大小写。

- **host**- 输入要连接的 ASA 的域名、IP 地址或组 URL。AnyConnect 会将此参数的值插入 AnyConnect 连接条目的 Server Address 字段中。

```
anyconnect://create/?name=SimpleExample&host=vpn.example.com
anyconnect:create?name=SimpleExample&host=vpn.example.com
```

- **protocol** protocol（可选，如果未指定，则默认为 SSL）- 用于此连接的 VPN 协议。有效值为：

SSL

IPSec

```
anyconnect:create?name=ExampleIPsec&host=vpn.company.com&protocol=IPsec
```

- **authentication**（可选，仅当协议指定为 IPsec 时适用，默认为 EAP-AnyConnect）- 用于 IPsec VPN 连接的身份验证方法。有效值为：

EAP-AnyConnect

EAP-GTC

EAP-MD5

EAP-MSCHAPv2

IKE-RSA

- **ike-identity**（身份验证设置为 EAP-GTC、EAP-MD5 或 EAP-MSCHAPv2 时需要）- 在 AUTHENTICATION 设置为 EAP-GTC、EAP-MD5 或 EAP-MSCHAPv2 时的 IKE 身份。用于其他身份验证设置时，此参数无效。

```
anyconnect:create?name=Description&host=vpn.company.com&protocol=IPsec
&authentication=eap-md5&ike-identity=012A4F8B29A9BCD
```

- **netroam**（可选，仅适用于 Apple iOS）- 确定是否限制在设备唤醒后或连接类型（例如 EDGE、3G 或 Wi-Fi）更改后重新连接所需的时间。此参数不影响数据漫游或使用多个移动服务运营商。有效值为：

**true** -（默认值）此选项可优化 VPN 访问。AnyConnect 在 AnyConnect 连接条目的 Network Roaming 字段中插入值 ON。如果 AnyConnect 失去连接，它将尝试建立新连接，直到成功为止。此设置让应用依赖于与 VPN 的持续连接。AnyConnect 不限制重新连接所需的时间。

**false** - 此选项可延长电池寿命。AnyConnect 将此值与 AnyConnect 连接条目的 Network Roaming 字段中的 OFF 值关联。如果 AnyConnect 失去连接，它在 20 秒内会一直尝试建立新连接，之后停止尝试。如有必要，用户或应用必须启动新的 VPN 连接。

```
anyconnect:create?name=Example%201&host=vpn.example.com&netroam=true
```

- **usecert**（可选）- 确定在建立与主机的 VPN 连接时是否使用设备上安装的数字证书。有效值为：

**true**（默认设置）- 允许建立与主机的 VPN 连接时自动选择证书。将 **usecert** 改为 **true** 而不指定 **certcommonname** 值，会将 **Certificates** 字段设为 **Automatic**，导致在连接时从 AnyConnect 证书存储区中选择证书。

**false** - 禁用自动选择证书。

```
anyconnect:create?name=Example%201&host=vpn.example.com&usecert=true
```

- **certcommonname**（可选，但需要 **usecert** 参数）- 与设备上预装的有效证书的公用名称匹配。AnyConnect 将该值插入 AnyConnect 连接条目的 **Certificate** 字段中。

要查看设备上安装的此证书，请点击 **Diagnostics > Certificates**。您可能需要滚动才能看到主机需要的证书。点击详细信息披露按钮可查看从证书读取的 **Common Name** 参数及其他值。

- **useondemand**（可选，仅适用于 Apple iOS，并且要求 **usecert**、**certcommonname** 参数和以下域规范）- 确定应用（如 Safari）是否可以启动 VPN 连接。有效值为：

**false**（默认值）- 阻止应用启动 VPN 连接。使用此选项是阻止发出 DNS 请求的应用潜在触发 VPN 连接的唯一方式。AnyConnect 将此选项与 AnyConnect 连接条目的 **Connect on Demand** 字段中的 **OFF** 值相关联。

**true** - 允许应用使用 Apple iOS 启动 VPN 连接。如果将 **useondemand** 参数设置为 **true**，AnyConnect 将在 AnyConnect 连接条目的 **Connect on Demand** 字段中插入 **ON** 值。（如果 **useondemand = true**，则需要 **domainlistalways** 或 **domainlistifneeded** 参数）

```
anyconnect:create?name=Example%20with%20certificate&host=vpn.example.com
&netroam=true&usecert=true&certcommonname=example-ID&useondemand=true
&domainlistalways=email.example.com,pay.examplecloud.com
&domainlistnever=www.example.com&domainlistifneeded=intranet.example.com
```

- **domainlistnever**（可选，要求 **useondemand = true**）- 列出域以评估是否符合取消使用 **Connect on Demand** 功能的条件。此列表是 AnyConnect 用于评估域请求是否匹配的列表。如果域请求匹配，AnyConnect 将忽略该域请求。AnyConnect 将此列表插入 AnyConnect 连接条目的 **Never Connect** 字段中。此列表可让您排除特定资源。例如，您可能不想通过面向公众的 Web 服务器自动进行 VPN 连接。示例值为 `www.example.com`。
- **domainlistalways**（如果 **useondemand=true**，则需要 **domainlistalways** 或 **domainlistifneeded** 参数）- 列出域以评估是否匹配 **Connect on Demand** 功能。此列表是 AnyConnect 用于评估域请求是否匹配的列表。如果应用请求访问此参数指定的域之一，并且尚未进行 VPN 连接，则 Apple iOS 会尝试建立 VPN 连接。AnyConnect 会将此列表插入 AnyConnect 连接条目的 **Always Connect** 字段中。示例值列表是 `email.example.com,pay.examplecloud.com`。
- **domainlistifneeded**（如果 **useondemand=true**，则需要 **domainlistalways** 或 **domainlistifneeded** 参数）- 如果发生 DNS 错误，AnyConnect 将根据此列表评估域请求是否匹配。如果此列表中有字符串和域匹配，Apple iOS 会尝试建立 VPN 连接。AnyConnect 会将此列表插入 AnyConnect 连接条目的 **Connect If Needed** 字段中。此列表最常用于对通过企业局域网无法访问的内部资源获取短时间访问权限。示例值为 `intranet.example.com`。

使用以逗号分隔的列表指定多个域。按需连接规则仅支持域名，而不支持 IP 地址。但 AnyConnect 灵活支持每个列表条目的域名格式，如下所示：

匹配	说明	示例条目	示例匹配	示例匹配失败
仅限准确的前缀和域名。	输入前缀、点和域名。	email.example.com	email.example.com	www.example.com email.l.example.com email.example1.com email.example.org
任何具有准确域名的前缀。前导点可阻止连接到以 * example.com（例如 notexample.com）结尾的主机。	输入一个点，后面紧跟要匹配的域名。	.example.org	anytext.example.org	anytext.example.com anytext.l.example.org anytext.example1.org
以您指定的文本结尾的任何域名。	输入要匹配的域名的末尾部分。	example.net anytext.	anytext-example.net anytext.example.net	anytext.example1.net anytext.example.com

## 建立 VPN 连接

使用此 AnyConnect URI 处理程序可连接到 VPN，以使用户轻松建立 VPN 连接。您还可以在 URI 中嵌入附加信息以执行以下任务：

- 预填用户名和密码
- 预填用于双重身份验证的用户名和密码
- 预填用户名和密码，并指定连接配置文件别名

此操作需要 name 或 host 参数，但允许同时使用以下语法之一：

```
anyconnect://connect[/?][name=Description|host=ServerAddress]
[&Parameter1=Value&Parameter2=Value..]
```

或

```
anyconnect://connect[/?]name=Description&host=ServerAddress
[&Parameter1=Value&Parameter2=Value..]
```

### 指南

- 如果语句中的所有参数值与设备上 AnyConnect 连接条目中的参数值都匹配，则 AnyConnect 将使用其余参数建立连接。

- 如果 AnyConnect 无法使语句中的所有参数与连接条目中的参数匹配，并且 name 参数是唯一的参数，则它会生成一个新连接条目，然后尝试 VPN 连接。
- 仅在使用一次性密码 (OTP) 基础设施时，才应该在使用 URI 建立 VPN 连接时指定密码。

## 参数

- **name**- 连接条目的名称与在 AnyConnect 主窗口的连接列表中显示的名称相同。AnyConnect 根据 AnyConnect 连接条目的 Description 字段评估此值，如果使用前述说明在设备上创建了连接条目，则也曾调用 name。此值区分大小写。
- **host**- 输入域名、IP 地址或 ASA 的组 URL 以匹配 AnyConnect 连接条目的 Server Address 字段，如果使用前述说明在设备上生成了连接条目，则也曾调用 host。

在 ASDM 中配置组 URL 的方法是选择 **Access > AnyConnect Connection Profiles > Advanced > Group Alias/Group URL > Group-URL**。

- **onsuccess**- 在连接成功时执行此操作。平台特定的行为：

对于 Apple iOS 设备，指定在此连接转换到已连接状态时要打开的 URL，或使用 anyconnect:close 命令关闭 AnyConnect GUI。

对于 Android 设备，指定在此连接转换为已连接状态或已处于已连接状态时要打开的 URL。可指定多个 onsuccess 操作。AnyConnect 始终在 Android 设备上连接成功后关闭 GUI。

- **onerror**- 连接失败时执行此操作。平台特定的行为：

对于 Apple iOS 设备，指定在此连接失败时要打开的 URL，或使用 anyconnect:close 命令关闭 AnyConnect GUI。

对于 Android 设备，指定在此连接失败时要打开的 URL。可指定多个 onerror 操作。AnyConnect 始终在 Android 设备上连接失败后关闭 GUI。

- **prefill\_username**- 提供连接 URI 中的用户名并将其预填到连接提示中。
- **prefill\_password**- 提供连接 URI 中的密码并且将其预填到连接提示中。此字段应仅用于为一次性密码配置的连接配置文件。
- **prefill\_secondary\_username**- 在配置为需要双重身份验证的环境中，此参数提供连接 URI 中的辅助用户名，并且将其预填到连接提示中。
- **prefill\_secondary\_password**- 在配置为需要双重身份验证的环境中，此参数提供连接 URI 中辅助用户名的密码，并且将其预填到连接提示中。
- **prefill\_group\_list**- 选择 **Configuration > Remote Access VPN > Network (Client) Access > AnyConnect Connection Profiles > Advanced > Group Alias/Group URL > Connection Aliases** 可在 ASDM 中定义连接别名。

## 示例

- 在组 URI 中提供连接名称和主机名或组 URL:

```
anyconnect://connect/?name=Example
anyconnect:connect?host=hr.example.com
anyconnect:connect?name=Example&host=hr.example.com
anyconnect://connect/?name=Example&host=hr.example.com/group-url
&prefill_username=user1&prefill_password=password1
```

- 提供针对成功或失败的操作

使用 `onsuccess` 或 `onerror` 参数可根据连接操作的结果开始打开指定的 URL:

```
anyconnect://connect?host=vpn.company.com
&onsuccess=http%3A%2F%2Fwww.cisco.com
anyconnect://connect?host=vpn.company.com
&onerror=http%3A%2F%2Fwww.cisco.com%2Ffailure.html
&onsuccess=http%3A%2F%2Fwww.cisco.com
```

在 Android 上可以指定多个 `onsuccess` 操作:

```
anyconnect://connect?host=vpn.company.com
&onerror=http%3A%2F%2Fwww.cisco.com%2Ffailure.html
&onsuccess=http%3A%2F%2Fwww.cisco.com
&onsuccess=tel:9781111111
```

在 Apple iOS 设备上, `anyconnect://close` 命令可在 `onsuccess` 或 `onerror` 参数中用来关闭 AnyConnect GUI:

```
anyconnect://connect?host=vpn.company.com
&onsuccess=anyconnect%3A%2F%2Fclose
```

- 提供连接信息并在 URI 中预填用户名和密码:

```
anyconnect://connect/?name=Example&host=hr.example.com
&prefill_username=user1&prefill_password=password1
anyconnect:connect?name=Example&host=hr.example.com/group-url
&prefill_username=user1&prefill_password=password1
```

- 为双重身份验证提供连接信息并预填用户名和密码:

```
anyconnect://connect/?name=Example&host=hr.example.com
&prefill_username=user1&prefill_password=password1
&prefill_secondary_username=user2&prefill_secondary_password=password2
```

- 提供连接信息、预填用户名和密码, 并指定连接配置文件别名:

```
anyconnect://connect/?name=Example&host=hr.example.com
&prefill_username=user1&prefill_password=password1
&prefill_group_list=10.%20Single%20Authentication
```

## 断开 VPN 连接

使用此 AnyConnect URI 处理程序可将用户从 VPN 断开。

**anyconnect:[/]disconnect[/]&onsuccess=URL**

### 参数

`onsuccess` 参数仅适用于 Android 设备。指定 URL 在此连接断开或已处于断开状态时打开。

### 示例

```
anyconnect:disconnect
```

## 导入证书

使用此 URI 处理程序命令可将 PKCS12 编码的证书捆绑包导入到终端。AnyConnect 客户端使用终端上已安装的 PKCS12 编码的证书向 ASA 验证自身。仅支持 pkcs12 证书类型。

```
anyconnect:[//]import[/?type=pkcs12&uri=http%3A%2F%2Fexample.com%2Fcertificatename.p12
```

### 参数

- **类型**- 仅支持 pkcs12 证书类型。
- **uri**- 在其中找到证书的 URL 编码的标识符。

### 示例

```
anyconnect:import?type=pkcs12&uri=http%3A%2F%2Fexample.com%2FCertName.p12
```

## 导入 VPN 客户端配置文件

使用此 URI 处理程序方法将客户端配置文件分发到 AnyConnect 客户端。

```
anyconnect:[//]import[/?type=profile&uri=filename.xml
```

### 示例

```
anyconnect:import?type=profile&uri=file%3A%2F%2Fsdcard%2Fprofile.xml
```

## 对移动设备上的 Anyconnect 进行故障排除

### 开始之前

在移动设备中启用日志记录并遵循相应用户指南中的故障排除说明：

- [Cisco AnyConnect 安全移动客户端用户指南，版本 4.0 \(Android\)](#)
- [Cisco AnyConnect 安全移动客户端用户指南，版本 4.0.x \(Apple iOS\)](#)

如果遵循这些说明未能解决问题，请尝试以下操作：

### 过程

- 
- 步骤 1** 确定在桌面客户端或其他移动操作系统上是否发生相同的问题。
  - 步骤 2** 确保在 ASA 中已安装适当的许可证。
  - 步骤 3** 如果证书身份验证失败，请检查以下项：
    - a) 确保选择了正确的证书。
    - b) 确保设备中的客户端证书将客户端身份验证作为扩展密钥使用。

- c) 确保 AnyConnect 配置文件中的证书匹配规则不会过滤掉用户选择的证书。  
即使用户选择了该证书，如果它与配置文件中的过滤规则不匹配，也不会将其用于身份验证。
- d) 如果身份验证机制使用与 ASA 关联的任何记账策略，请验证用户是否能够成功进行身份验证。
- e) 如果您在期望使用仅证书身份验证时看到身份验证屏幕，请配置该连接以使用组 URL 并确保没有为隧道组配置辅助身份验证。

**步骤 4** 在 Apple iOS 设备上，检查以下项：

- a) 如果在设备唤醒后 VPN 连接未恢复，请确保网络漫游已启用。
- b) 如果使用按需连接，请验证已配置仅证书身份验证和组 URL。

---

### 接下来的操作

如果问题仍然存在，请在客户端上启用日志记录并在 ASA 中启用调试日志记录。有关详细信息，请参阅合适版本的 ASA 配置指南。







# 第 12 章

## AnyConnect 故障排除

---

- [收集用于故障排除的信息，第 233 页](#)
- [AnyConnect 连接或断开连接问题，第 236 页](#)
- [VPN 服务故障，第 238 页](#)
- [驱动程序故障，第 240 页](#)
- [其他故障，第 241 页](#)
- [安全告警，第 242 页](#)
- [掉线的连接，第 243 页](#)
- [安装故障，第 244 页](#)
- [不兼容问题，第 245 页](#)
- [已知的第三方应用冲突，第 247 页](#)

### 收集用于故障排除的信息

#### 查看统计详细信息

管理员或最终用户可查看当前 AnyConnect 会话的统计信息。

#### 过程

- 
- 步骤 1** 在 Windows 上，导航到 **Advanced Window > Statistics > VPN drawer**。在 Linux 上，点击用户 GUI 中的 **Details** 按钮。
  - 步骤 2** 根据客户端计算机上加载的软件包，从以下选项中进行选择。
    - **Export Stats** - 将连接统计信息保存为一个文本文件，供以后分析和调试。

- **Reset** - 将连接信息重置为零。AnyConnect 将立即开始收集新数据。
- **Diagnostics** - 启动 AnyConnect 诊断和报告工具 (DART) 向导，该向导将捆绑指定日志文件和诊断信息，供客户端连接的分析 and 调试。

## 运行 DART 以收集用于故障排除的数据

DART 是 AnyConnect 诊断和报告工具，用来收集数据以对 AnyConnect 安装和连接问题进行故障排除。DART 收集日志、状态和诊断信息，以供思科技术支持中心 (TAC) 分析。

DART 向导在运行 AnyConnect 的设备上运行。DART 不需要管理员权限。您可以从 AnyConnect 启动 DART 或不使用 AnyConnect 自行启动它。

支持以下操作系统：

- Windows
- Mac OS X
- Linux

### 过程

#### 步骤 1 启动 DART：

- 对于 Windows 设备，请启动 Cisco AnyConnect 安全移动客户端。
- 对于 Linux 设备，请选择 **Applications > Internet > Cisco DART** 或 `/opt/cisco/anyconnect/dart/dartui`。
- 对于 Mac 设备，请选择 **Applications > Cisco > Cisco DART**。

#### 步骤 2 点击 **Statistics** 选项卡，然后点击 **Details**。

#### 步骤 3 选择 **Default** 值或 **Custom** 捆绑创建。

- **Default** - 默认包括典型日志文件和诊断信息，例如 AnyConnect 日志文件、有关计算机的常规信息以及 DART 执行和不执行的功能的摘要。捆绑包的默认名称为 `DARTBundle.zip`，它会保存到本地桌面。
- **Custom** - 可指定要在捆绑中包含什么文件（或默认文件）和存储捆绑的位置。

**注释** **Default** 是 Mac OS X 的唯一选项。无法定制要在捆绑包中包含哪些文件。

**注释** 如果您选择 **Custom**，则可以配置要在捆绑中包含哪些文件，并且为文件指定不同的存储位置。

- 步骤 4** 如果 DART 似乎要花很长时间来收集默认文件列表，请点击 **Cancel**，重新运行 DART，并选择 **Custom** 以选择较少的文件。
- 步骤 5** 如果您选择 **Default**，DART 将开始创建捆绑包。如果您选择 **Custom**，请继续按照向导提示指定日志、首选项文件、诊断信息和任何其他定制项。

## 获取计算机系统信息

对于 Windows，键入 `msinfo32 /nfo c:\msinfo.nfo`。

## 获取 Systeminfo 文件转储

对于 Windows，在 `sysinfo` 命令提示符中键入 `c:\sysinfo.txt`。

## 检查注册表文件

SetupAPI 日志文件中如下所示的条目表示找不到文件：

```
E122 Device install failed. Error 2: The system cannot find the file specified.
E154 Class installer failed. Error 2: The system cannot find the file specified.
```

确保 `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\RunOnce` 注册表项存在。若没有此注册表项，将禁止所有 `inf` 安装包。

## AnyConnect 日志文件的位置

日志保留在以下文件中：

Windows—\Windows\Inf\setupapi.app.log or \Windows\Inf\setupapi.dev.log

- Windows—\Windows\Inf\setupapi.app.log or \Windows\Inf\setupapi.dev.log



**注释** 在 Windows 中，您必须使隐藏的文件可见。

如果是初次网络部署安装，则日志文件位于每位用户的临时目录下：

```
%TEMP%\anyconnect-win-4.X.xxxxx-k9-install-yyyyyyyyyyyyyyyy.log。
```

如果升级来自于最佳网关推送，则日志文件位于以下位置：

```
%WINDIR%\TEMP\anyconnect-win-3.X.xxxxx-k9-install-yyyyyyyyyyyyyyyy.log。
```

获取适用于您要安装的客户端版本的最新文件。xxx 因版本而异，yyyyyyyyyyyyyyyy 指定安装的日期和时间。

# AnyConnect 连接或断开连接问题

## AnyConnect 无法建立初始连接或未断开连接

问题：AnyConnect 不会建立初始连接，或者当您点击 Cisco AnyConnect Secure Mobility Client 窗口上的 Disconnect 时出现意外结果。

解决方案：进行以下检查

- 如果使用 Citrix 高级网关客户端版本 2.2.1，请删除 Citrix 高级网关客户端，直到 Citrix 解决 CtxLsp.dll 问题。
- 如果您使用具有 AT&T Sierra 无线 875 网卡的 AT&T 通信管理器 6.2 版或 6.7 版，请执行以下步骤解决此问题：

- 1 禁用 Aircard 加速。
- 2 启动 **AT&T Communication Manager > Tools > Settings > Acceleration > Startup**。
- 3 键入 **manual**。
- 4 点击 **Stop**。

- 从 ASA 获取配置文件，查找连接失败的标志：

从 ASA 控制台键入 **write net x.x.x.x:ASA-Config.txt**，其中 *x.x.x.x* 是 TFTP 服务器在网络中的 IP 地址。

从 ASA 的控制台，键入 **show running-config**。剪切并粘贴配置文件到文本编辑器并保存。

- 查看 ASA 事件日志：

- 1 在 ASA 控制台上，添加以下命令行以查看 ssl、webvpn、anyconnect 和 auth 事件：

```
config terminal
logging enable
logging timestamp
logging class auth console debugging
logging class webvpn console debugging
logging class ssl console debugging
logging class anyconnect console debugging
```

- 2 尝试连接 AnyConnect 客户端，发生连接错误时，则将日志信息从控制台上剪切并粘贴至文本编辑器并保存。
- 3 键入 **no logging enable** 禁用日志记录。

- 使用 Windows 事件查看器从客户端计算机获取 Cisco AnyConnect VPN 客户端日志。

- 1 选择 **Start > Run** 并键入 **eventvwr.msc /s**。
- 2 在（Windows 7 的）应用和服务日志中找到 **Cisco AnyConnect VPN Client**，并选择 **Save Log File As...**。
- 3 指定文件名，例如，**AnyConnectClientLog.evt**。您必须使用 **.evt** 文件格式。

- 修改 Windows 诊断调试实用程序。

- 1 如 WinDbg 文档所示，附加 `vpnagent.exe` 进程。
- 2 确定 IPv6/IPv4 IP 地址分配是否存在冲突。在事件日志中查找是否有已识别的冲突。
- 3 如果发现冲突，则向要使用的客户端计算机注册表添加额外的路由调试。这些冲突在 AnyConnect 事件日志中可能会如下所示：

```
Function: CRouteMgr:modifyRoutingTable Return code: 0xFE06000E File: .\VpnMgr.cpp
Line:1122
Description: ROUTEMGR_ERROR_ROUTE_TABLE_VERIFICATION_FAILED.
Termination reason code 27: Unable to successfully verify all routing table
modifications are correct.
```

```
Function: CChangeRouteTable::VerifyRouteTable Return code: 0xFE070007
File: .\RouteMgr.cpp Line: 615 Description: ROUTETABLE_ERROR_NOT_INITIALIZED
gr.cpp Line: 615 Description: ROUTETABLE_ERROR_NOT_INITIALIZED
```

- 4 通过添加特定的注册表项 (Windows) 或文件 (Linux 和 Mac OS X) 启用一次性基础的路由调试连接。

- 在 32 位 Windows 中，DWORD 注册表值必须是 `HKEY_LOCAL_MACHINE \ SOFTWARE \ Cisco \ Cisco AnyConnect Secure Mobility Client \ DebugRoutesEnabled`
- 在 64 位 Windows 中，DWORD 注册表值必须是 `HKEY_LOCAL_MACHINE \ SOFTWARE \ WOW6432node \ Cisco \ Cisco AnyConnect Secure Mobility Client \ DebugRoutesEnabled`
- 在 Linux 或 Mac OS X 中，使用 `sudo touch` 命令在以下路径中创建文件：`/opt/cisco/anyconnect/debugroutes`



**注释** 密钥或文件将在启动隧道连接时删除。文件的密钥或内容的值不是重要的密钥时或文件足以启用调试。

启动 VPN 连接。找到此密钥或文件时，系统临时目录（在 Windows 中通常是 `C:\Windows\Temp`，在 Mac 或 Linux 中通常是 `/tmp`）中将创建两个路由调试文本文件。如果已经存在这两个文件（`debug_routechangesv4.txt4` 和 `debug_routechangesv6.txt`），它们将会被覆盖。

## AnyConnect 无法传输流量

问题：AnyConnect 客户端在连接后无法将数据发送到专用网络。

解决方案：进行以下检查

- 如果您使用具有 AT&T Sierra 无线 875 网卡的 AT&T 通信管理器 6.2 版或 6.7 版，请执行以下步骤解决此问题：
  - 1 禁用 Aircard 加速。
  - 2 启动 AT&T communication manager > Tools > Settings > Acceleration > Startup。

3 键入 **manual**。

4 点击 **Stop**。

- 获取 `show vpn-sessiondb detail anyconnect filter name <username>` 命令的输出。如果输出指定 `Filter Name: XXXXX`，则还要获取 `show access-list XXXXX` 命令的输出。验证 ACL 未阻止需要的流量。
- 从 AnyConnect VPN Client > Statistics > Details > Export 获取 DART 文件或输出 (AnyConnect-ExportedStats.txt)。观察统计、界面和路由表。
- 检查 ASA 配置文件中的 NAT 语句。如果已启用 NAT，则您必须排除从网络地址转换返回到客户端的数据。例如，要使 NAT 从 AnyConnect 池中排除 IP 地址，需要使用以下代码：

```
access-list in_nat0_out extended permit ip any 10.136.246.0 255.255.255.0
ip local pool IPPool1 10.136.246.1-10.136.246.254 mask 255.252.0.0
nat (inside) 0 access-list in_nat0_out
```

- 验证是否为设置启用了隧道化默认网关。传统默认网关是最不适合非解密流量的网关。

```
route outside 0.0.209.165.200.225
route inside 0 0 10.0.4.2 tunneled
```

如果 VPN 客户端需要访问 VPN 网关路由表中未列出的资源，数据包将由标准默认网关传送。VPN 网关不需要完整的内部路由表。如果您使用隧道化关键字，则路由将处理来自 IPsec/SSL VPN 连接的解密流量。标准流量通常不会路由到 209.165.200.225，而来自 VPN 的流量将路由到 10.0.4.2 且已进行解密。

- 在使用 AnyConnect 建立隧道前后，收集 `ipconfig /all` 的文本转储和路由打印输出。
- 在客户端上执行网络数据包捕获，或在 ASA 上启用捕获。



#### 注释

如果某些应用（例如 Microsoft Outlook）无法使用隧道，则在具有 ping 扩展集的网络中 ping 已知设备，可查看接受的大小（例如，`ping -l 500`，`ping -l 1000`，`ping -l 1500`，以及 `ping -l 2000`）。从 ping 结果中可对网络中的分段问题略知一二。然后，您可以为存在分段问题的用户配置一个特殊组，并将该组的 `anyconnect mtu` 设置为 1200。您也可从旧 IPsec 客户端复制 `Set MTU.exe` 实用程序，并强制将物理适配器 MTU 设置为 1300。重启后，查看是否有区别。

## VPN 服务故障

### VPN 服务连接失败

问题：您收到“Unable to Proceed, Cannot Connect to the VPN Service”消息。AnyConnect 的 VPN 服务未运行。

解决方案：确定是否有另一个应用与该服务冲突。请参阅[确定服务的冲突项](#)。

## 确定服务的冲突项

以下过程确定冲突是在启动时针对服务器的初始化还是针对其他运行的服务，例如，因为服务启动失败。

### 过程

- 步骤 1** 查看 Windows 管理工具下的服务，以确保 Cisco AnyConnect VPN 代理未运行。如果它正在运行并且仍然显示错误消息，则可能需要禁用甚至卸载工作站上的另一个 VPN 应用。在执行该操作后，重新启动，然后重复此步骤。
- 步骤 2** 尝试启动 Cisco AnyConnect VPN 代理。
- 步骤 3** 在事件查看器中检查 AnyConnect 日志以查找是否存在指出服务无法启动的消息。请注意步骤 2 的手动重新启动的时间戳以及工作站启动时的时间戳。
- 步骤 4** 在事件查看器中检查系统和应用日志以查找任何冲突消息的相同通用时间戳。
- 步骤 5** 如果日志指示启动服务失败，请查找在大致相同时间戳的其他信息性消息，这些消息指示以下情况之一：
  - 文件缺失 - 从独立 MSI 安装重新安装 AnyConnect 客户端以排除缺失的文件。
  - 另一相关服务中的延迟 - 禁止启动活动以缩短工作站的启动时间。
  - 与另一应用或服务的冲突 - 确定是否另一项服务在侦听 `vpnagent` 使用的同一端口，或者是否某些 HIDS 软件阻止我们的软件侦听某个端口。
- 步骤 6** 如果日志没有直接指向某个原因，请使用试错法来识别冲突。识别了最可能的候选项后，请从服务面板禁用这些服务（例如 VPN 产品、HIDS 软件、Spybot 清除程序、嗅探器、防病毒软件等）。
- 步骤 7** 重新启动。如果 VPN 代理服务仍无法启动，请开始关闭操作系统的默认安装未安装的服务。

## VPN 客户端驱动程序遇到错误 (Microsoft Windows 更新后)

问题：如果您最近更新了 Microsoft `certclass.inf` 文件，在尝试建立 VPN 连接时会出现以下消息：

```
The VPN client driver has encountered an error.
```

如果检查 `C:\WINDOWS\setupapi.log`，会看到以下错误：

```
#W239 The driver signing class list "C:\WINDOWS\INF\certclass.inf" was missing or invalid.
Error 0xffffbf8: Unknown Error. Assuming all device classes are subject to driver signing
policy.
```

解决方案：在命令提示符下输入 `C:\>systeminfo` 或查看 `C:\WINDOWS\WindowsUpdate.log`，可查看最近安装了哪些更新。按照说明修复 VPN 驱动程序。

## 修复 VPN 客户端驱动程序错误

尽管执行的上述步骤可能表明目录未损坏，但密钥文件仍可能被未签名的文件覆盖。如果此故障仍然存在，请通过向 Microsoft 提交案例来确定驱动程序签名数据库为什么损坏。

### 过程

---

- 步骤 1** 以管理员身份打开命令提示符。
  - 步骤 2** 输入 `net stop CryptSvc`。
  - 步骤 3** 分析数据库，通过输入 `esentutl /g %systemroot%\System32\catroot2\{F750E6C3-38EE-11D1-85E5-00C04FC295EE}\catdb` 验证其有效性或将目录 `%WINDIR%\system32\catroot2` 重命名为 `catroot2_old`。
  - 步骤 4** 出现提示时，选择 **OK** 尝试修复。退出命令提示符并重新启动。
- 

## 驱动程序故障

### 修复 VPNVA.sys 中的驱动程序故障

问题：VPNVA.sys 驱动程序故障。

解决方案：找到被绑定到 Cisco AnyConnect 虚拟适配器的中间驱动程序，并取消选择它们。

### 修复 vpnagent.exe 中的驱动程序故障

#### 过程

---

- 步骤 1** 创建名为 `c:\vpnagent` 的目录。
  - 步骤 2** 查看任务管理器中的 Process 选项卡，确定 `vpnagent.exe` 中的进程 PID。
  - 步骤 3** 打开命令提示符并更改安装了调试工具的目录。默认情况下，Windows 的调试工具位于 `C:\Program Files\Debugging Tools`。
  - 步骤 4** 键入 `cscript vpnagent4.vbs -crash -p PID -o c:\vpnagent -nodumponfirst`，其中 `PID` 是 `vpnagent.exe` 的 PID。
  - 步骤 5** 使打开的窗口以最小化状态运行。监控时不可注销系统。
  - 步骤 6** 当发生故障时，将 `c:\vpnagent` 的内容压缩为 zip 文件。
  - 步骤 7** 使用 `!analyze -v` 进一步诊断 `crashdmp` 文件。
-



## 网络访问管理器的链路/驱动程序问题

如果网络访问管理器无法识别有线适配器，请尝试将网线拔出并重新插入。如果这无法解决问题，则链路可能有问题。网络访问管理器可能无法确定适配器的正确链路状态。请检查 NIC 驱动程序的连接属性。您可能在高级面板中看到 Wait for Link 选项。设置为 On 时，有线 NIC 驱动程序初始化代码等待自动协商完成，再确定连接是否有效。

## 其他故障

### AnyConnect 故障

问题：在系统重启后，您收到 the system has recovered from a serious error 消息。

解决方案：从 %temp% 目录（例如 C:\DOCUME~1\jsmith\LOCALS~1\Temp）中收集生成的 .log 和 .dmp 文件。复制文件或备份文件。请参阅[如何备份 .log 或 .dmp 文件](#)。

### 如何备份 .log 或 .dmp 文件

#### 过程

---

**步骤 1** 从 Start > Run 菜单运行名为 Dr. Watson (Drwtsn32.exe) 的 Microsoft 实用程序。

**步骤 2** 进行以下配置并点击 **OK**：

```
Number of Instructions : 25
Number of Errors to Save : 25
Crash Dump Type : Mini
Dump Symbol Table : Checked
Dump All Thread Contexts : Checked
Append to Existing Log File : Checked
Visual Notification : Checked
Create Crash Dump File : Checked
```

**步骤 3** 在客户端计算机上的 Start > Run 菜单中输入 **eventvwr.msc /s**，以从 Windows 事件查看器中获取 Cisco AnyConnect VPN 客户端日志。

**步骤 4** 在（Windows 7 的）应用和服务日志中找到 **Cisco AnyConnect VPN Client**，并选择 **Save Log File As...**。以 .evt 文件格式分配文件名，例如 AnyConnectClientLog.evt。

---

## vpndownloader 中的 AnyConnect 故障（分层服务提供商 (LSP) 模块和 NOD32 AV）

问题：AnyConnect 在尝试建立连接时成功进行身份验证并建立了 SSL 会话，但随后在使用 LSP 或 NOD32 AV 时，AnyConnect 客户端在 vpndownloader 中发生故障。

解决方案：删除 2.7 版中的 Internet Monitor 组件，并升级到 ESET NOD32 AV 3.0 版。

## 蓝屏（AT&T 拨号器）

问题：如果您使用 AT&T 拨号器，则客户端操作系统有时会出现蓝屏，导致创建微型转储文件。

解决方案：升级到最新的 7.6.2 AT&T 全球网络客户端。

## 安全告警

### Microsoft Internet Explorer 安全告警

问题：Microsoft Internet Explorer 中出现安全告警窗口，其中包含以下文字：

```
Information you exchange with this site cannot be viewed or changed by others. However, there is a problem with the site's security certificate. The security certificate was issued by a company you have not chosen to trust. View the certificate to determine whether you want to trust the certifying authority.
```

解决方案：连接到未识别为受信任网站的 ASA 时可能出现此告警。为防止出现此告警，请在客户端上安装一个受信任根证书。请参阅[在客户端上安装受信任根证书](#)。

### “Certified by an Unknown Authority” 告警

问题：在浏览器中可能出现 Web Site Certified by an Unknown Authority 告警窗口。Security Alert 窗口的上半部分显示以下文本：

```
Unable to verify the identity of <Hostname_or_IP_address> as a trusted site.
```

解决方案：在连接到不被识别为受信任站点的 ASA 时可能出现此安全告警。为防止出现此告警，请在客户端上安装一个受信任根证书。请参阅[在客户端上安装受信任根证书](#)。

### 在客户端上安装受信任根证书

开始之前

生成或获取将用作受信任根证书的证书。

**注释**

您可以通过将自签名证书安装为客户端上的受信任根证书，在短期内避免出现安全证书警告。但是我们不建议这样做，因为用户可能会无意中将浏览器配置为信任欺诈服务器上的证书，并且在连接到安全网关时可能不得不响应安全警告而给用户带来不便。

**过程**

- 步骤 1** 点击 Security Alert 窗口中的 **View Certificate**。
- 步骤 2** 点击 **Install Certificate**。
- 步骤 3** 点击 **Next**。
- 步骤 4** 选择 **Place all certificates in the following store**。
- 步骤 5** 点击 **Browse**。
- 步骤 6** 在下拉列表中，选择 **Trusted Root Certification Authorities**。
- 步骤 7** 遵循证书导入向导提示继续操作。

## 掉线的连接

### 无线连接在引入有线连接时掉线（Juniper Odyssey 客户端）

问题：在 Odyssey 客户端上启用无线抑制后，如果引入有线连接，那么无线连接就会掉线。禁用无线抑制后，无线连接如预期的那样运行正常。

解决方案：[配置 Odyssey 客户端](#)。

### 配置 Odyssey 客户端

**过程**

- 步骤 1** 在 Network Connections 中，复制适配器的名称（与在其连接属性中显示的一样）。如果您编辑注册表，请先进行备份，然后再进行任何更改。一定要谨慎，因为如果修改错误，可能导致严重问题。
- 步骤 2** 打开注册表并转到 HKEY\_LOCAL\_MACHINE\SOFTWARE\Funk Software, Inc.\odyssey\client\configuration\options\adapterType\virtual。
- 步骤 3** 在 virtual 下创建新的字符串值。将适配器的名称从 Network 属性复制到注册表部分。额外的注册表设置一旦保存，就会在创建客户端 MSI 并下推到其他客户端时通过端口传递。

## 连接 ASA 失败 (Kaspersky AV Workstation 6.x)

问题：安装 Kaspersky 6.0.3 后（即使已禁用），到 ASA 的 AnyConnect 连接会在 CSTP state = CONNECTED 之后立即失败。系统会显示以下消息：

```
SVC message: t/s=3/16: Failed to fully establish a connection to the secure gateway (proxy authentication, handshake, bad cert, etc.).
```

解决方案：卸载 Kaspersky 并访问其论坛获得其他更新。

## 没有 UDP DTLS 连接 (McAfee Firewall 5)

问题：使用 McAfee Firewall 5 时，UDP DTLS 连接无法建立。

解决方案：在 McAfee Firewall 中央控制台中，选择 **Advanced Tasks > Advanced options and Logging**，然后取消选中 McAfee Firewall 中的 **Block incoming fragments automatically** 复选框。

## 连接主机设备失败（Microsoft 路由和远程访问服务器）

问题：如果使用 RRAS，则当 AnyConnect 尝试建立到主机设备的连接时，事件日志中会记录以下终止错误：

```
Termination reason code 29 [Routing and Remote Access service is running]
The Windows service "Routing and Remote Access" is incompatible with the Cisco AnyConnect VPN Client.
```

解决方案：禁用 RRAS 服务。

## 连接失败/缺少凭证（负载均衡器）

问题：由于缺少凭证而连接失败。

解决方案：第三方负载均衡器无法洞悉 ASA 设备上的负载。因为 ASA 中的负载均衡功能足够智能，能够在设备之间均衡地分配 VPN 负载，所以我们建议使用内部 ASA 负载均衡。

## 安装故障

### AnyConnect 无法下载 (Wave EMBASSY Trust Suite)

问题：AnyConnect 客户端无法下载，并出现以下错误消息：

```
"Cisco AnyConnect VPN Client Downloader has encountered a problem and needs to close."
```

解决方案：将补丁更新上传到 1.2.1.38 版以解决所有 dll 问题。

## 不兼容问题

### 更新路由表失败（Bonjour 打印服务）

问题：如果您使用的是 Bonjour 打印服务，AnyConnect 事件日志会指出识别 IP 转发表失败。

解决方案：通过在命令提示符下键入 **net stop "bonjour service"** 禁用 Bonjour 打印服务。Apple 公司已经推出了新版 mDNSResponder (1.0.5.11)。要解决此问题，请将新版 Bonjour 捆绑至 iTunes，且作为单独程序从 Apple 网站下载。

### TUN 的版本不兼容（OpenVPN 客户端）

问题：错误表示此系统上已安装 TUN 版本，但该版本与 AnyConnect 客户端不兼容。

解决方案：卸载 Viscosity OpenVPN 客户端。

### Winsock 目录冲突（LSP 症状 2 冲突）

问题：如果客户端上有 LSP 模块，可能会发生 Winsock 目录冲突。

解决方案：卸载 LSP 模块。

### 数据吞吐慢（LSP 症状 3 冲突）

问题：在 Windows 7 系统中使用 NOD32 Antivirus V4.0.468 x64 时可能出现数据吞吐慢。

解决方案：禁用 SSL 协议扫描。请参阅[禁用 SSL 协议扫描](#)。

### 禁用 SSL 协议扫描

#### 过程

- 
- 步骤 1** 转至 Advanced Setup 中的 **Protocol Filtering** > **SSL** 并启用 SSL 协议扫描。
  - 步骤 2** 转到 **Web access protection** > **HTTP、HTTPS**，并选中 **Do not use HTTPS protocol checking**。
  - 步骤 3** 返回到 **Protocol Filtering** > **SSL** 并禁用 **SSL protocol scanning**。
-

## DPD 失败 (EVDO 无线网卡和 Venturi 驱动程序)

问题：如果客户端断开连接时您使用的是 EVDO 无线网卡和 Venturi 驱动程序，则事件日志会报告如下内容：

```
%ASA-5-722037: Group <Group-Name> User <User-Name> IP <IP-Address> SVC closing connection:
DPD failure.
```

解决方案

- 检查应用、系统和 AnyConnect 事件日志中的相关断开连接事件，同时确定是否应用了 NIC 卡重置。
- 确保 Venturi 驱动程序为最新版本。在 6.7 版本的 AT&T 通信管理器中禁用 **Use Rules Engine**。

## DTLS 流量失败 (DSL 路由器)

问题：如果您与 DSL 路由器连接，则即使成功协商，DTLS 流量也可能会失败。

解决方案：连接到采用出厂设置的 Linksys 路由器。此设置支持稳定的 DTLS 会话且 ping 过程中无中断。添加规则以允许 DTLS 返回流量。

## NETINTERFACE\_ERROR (CheckPoint 和其他第三方软件，如 Kaspersky)

问题：尝试在用于建立 SSL 连接的计算机网络上检索操作系统信息时，AnyConnect 日志可能指示未能完全建立到安全网关的连接。

解决方案

- 如果是卸载完整性代理，然后安装 AnyConnect，请启用 TCP/IP。
- 确保如果在完整性代理安装上禁用 SmartDefense，则选中 TCP/IP。
- 如果在检索网络接口信息时第三方软件拦截或以其他方式阻止操作系统 API 调用，请检查是否有可疑的 AV、FW、AS 等。
- 确认设备管理器中只出现一个 AnyConnect 适配器实例。如果只有一个实例，则使用 AnyConnect 进行身份验证，并在 5 秒后手动从设备管理器启用适配器。
- 如果在 AnyConnect 适配器中启用了任何可疑的驱动程序，在 Cisco AnyConnect VPN Client Connection 窗口中取消选中它们予以禁用。

## 性能问题 (虚拟机网络服务驱动程序)

问题：在某些虚拟机网络服务设备上使用 AnyConnect 时，会导致性能问题。

解决方案：取消选中 AnyConnect 虚拟适配器中所有即时消息设备的绑定。应用 dsagent.exe 驻留在 C:\Windows\System\dsagent 中。虽然其未出现在进程列表中，您可以用 TCPview (sysinternals) 打开套接字进行查看。当您终止此进程时，AnyConnect 将恢复正常运行。

## 已知的第三方应用冲突

我们已经知道，以下第三方应用获取 Cisco AnyConnect 安全移动客户端存在困难：

- Adobe 和苹果公司 - Bonjour 打印服务

Adobe Creative Suite 3

BonJour 打印服务

iTunes

- AT&T 通信管理器版本 6.2 和 6.7

AT&T Sierra 无线 875 卡

- AT&T 全球拨号器

- Citrix 高级网关客户端版本 2.2.1

- 防火墙冲突

第三方防火墙可能会干扰 ASA 组策略中配置的防火墙功能。

- Juniper Odyssey 客户端

- Kaspersky AV 工作站 6.x

- McAfee 防火墙 5

- Microsoft Internet Explorer 8

- Microsoft 路由和远程接入服务器

- Microsoft Windows Update

- OpenVPN 客户端

- 负载均衡

- Wave EMBASSY Trust Suite

- 分层服务提供商 (LSP) 模块和 NOD32 AV

- EVDO 无线网卡和 Venturi 驱动程序

- DSL 路由器

- CheckPoint 和其他第三方软件（如卡巴斯基）

- 虚拟机网络服务驱动程序

