通过ASA部署AnyConnect网络安全

目录

简介

本文档介绍为在思科自适应安全设备(ASA)上终止的基于客户端的VPN部署AnyConnect网络安全模块。
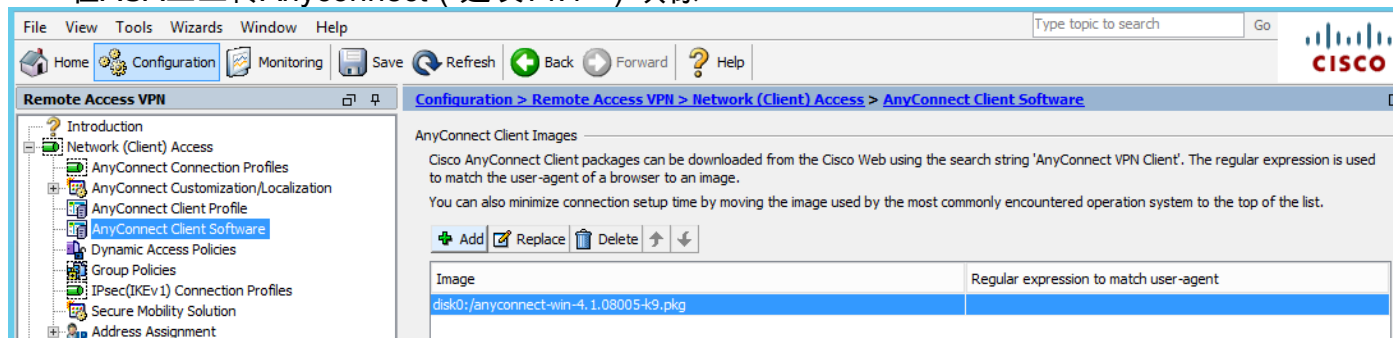
先决条件

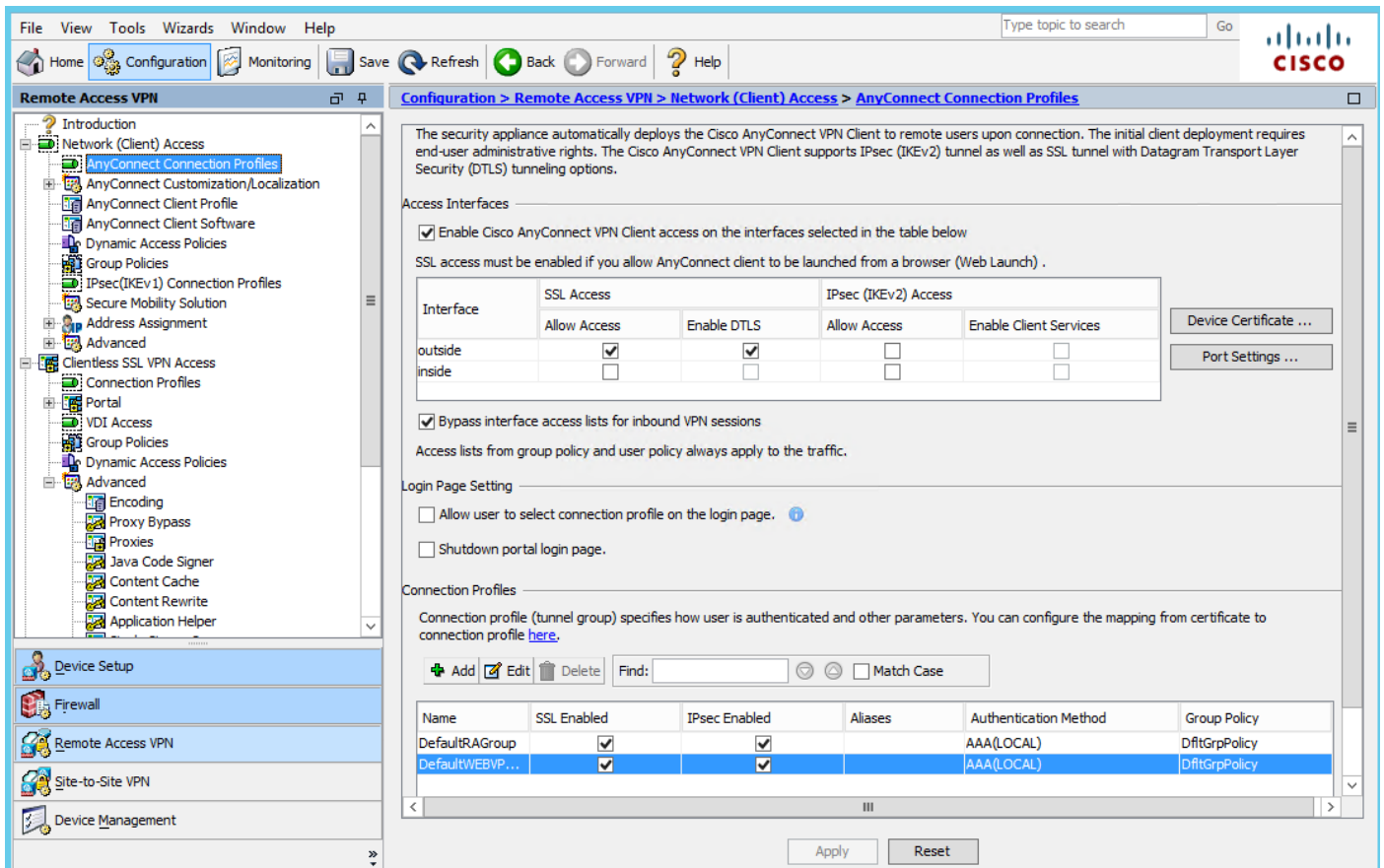### 要求

本文档没有任何特定的要求。

使用的组件

本文档不限于特定的软件和硬件版本。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始（默认）配置。如果您使用的是真实网络，请确保您已经了解所有命令的潜在影响。

背景信息

- 在ASA上上传Anyconnect（建议v4.1+）映像

- 在ASA上启用VPN配置文件，如图所示

配置

通过ASA部署AnyConnect Web安全

配置中涉及的步骤如下：

- 配置AnyConnect网络安全客户端配置文件
- 编辑Anyconnect VPN组策略
- 为Web安全设置拆分排除并选择下载Web安全客户端模块
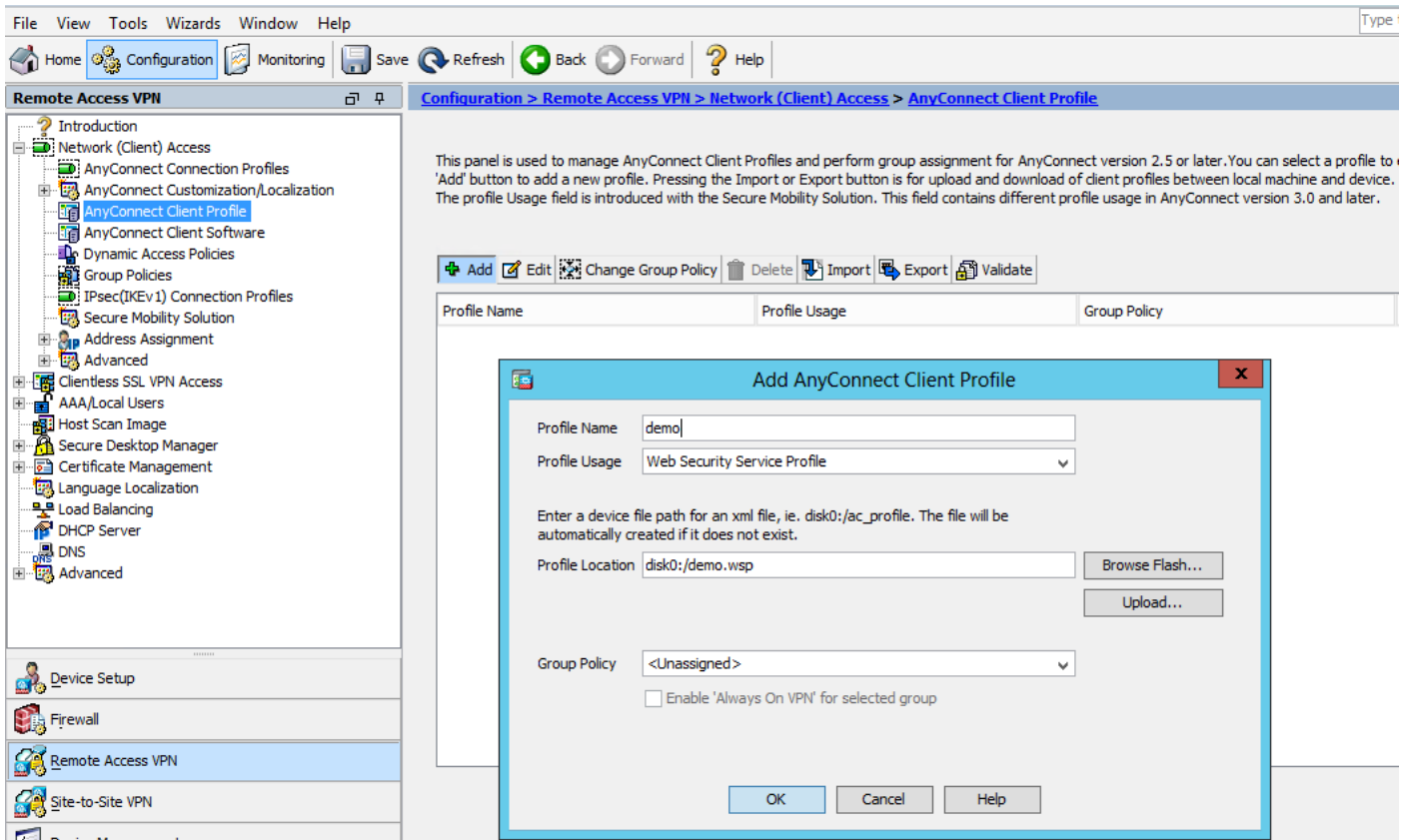- 编辑Anyconnect VPN组策略并选择网络安全客户端配置文件

步骤1.配置AnyConnect Websecurity客户端配置文件

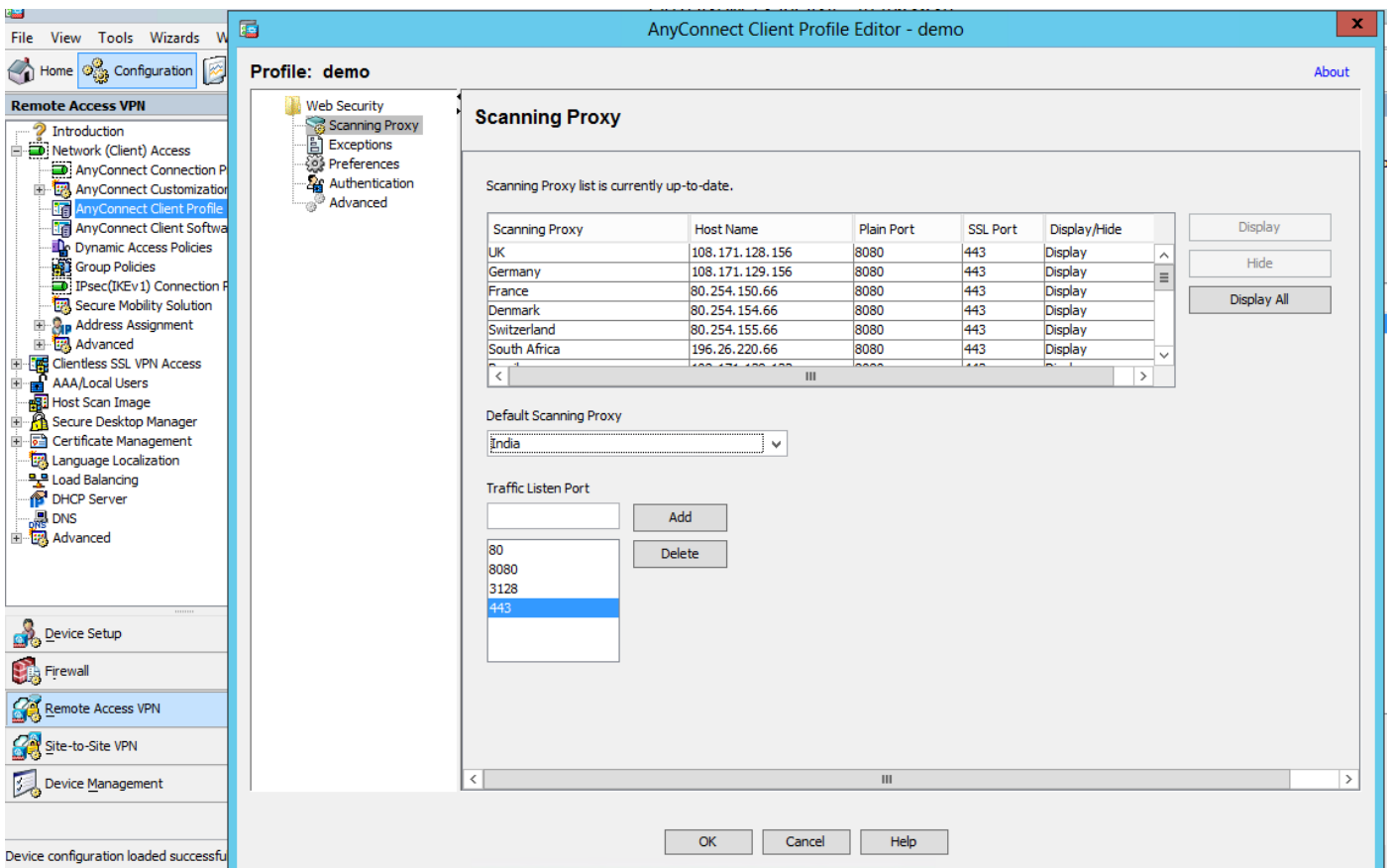导航至**配置>删除接入VPN>网络（客户端）接入>Anyconnect客户端配置文件**，单击

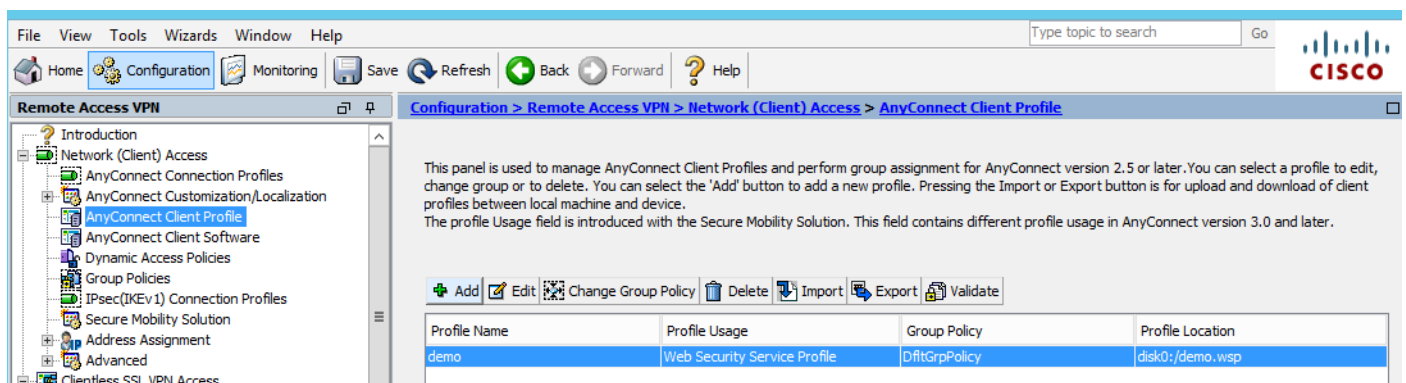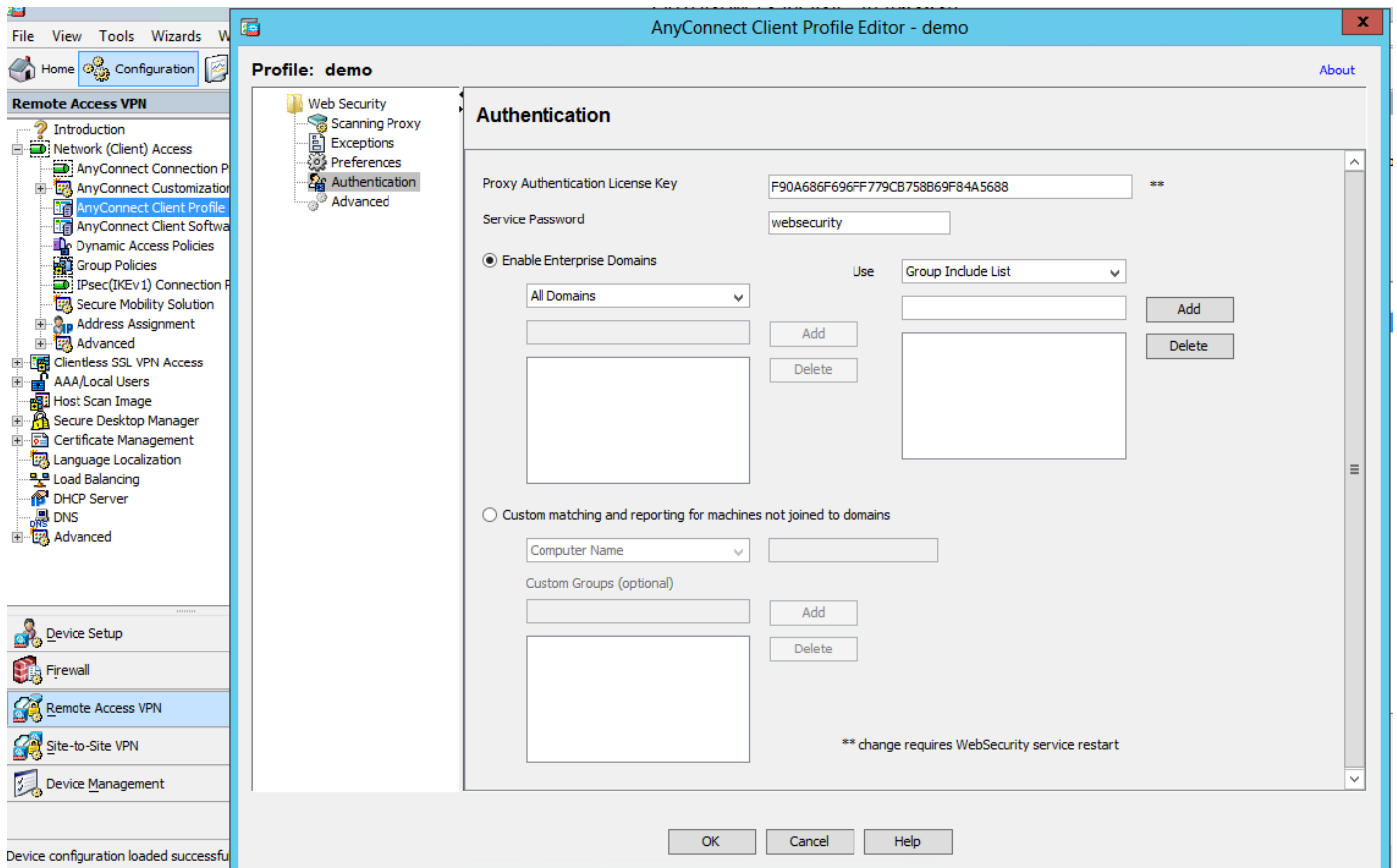**添加并**选择AnyConnect网络安全客户端配置文件。

> **注意**：配置文件名称在客户端上是硬编码的，因此，无论配置了什么名称，ASA始终将Websecurity_serviceprofile.wso推送到客户端。
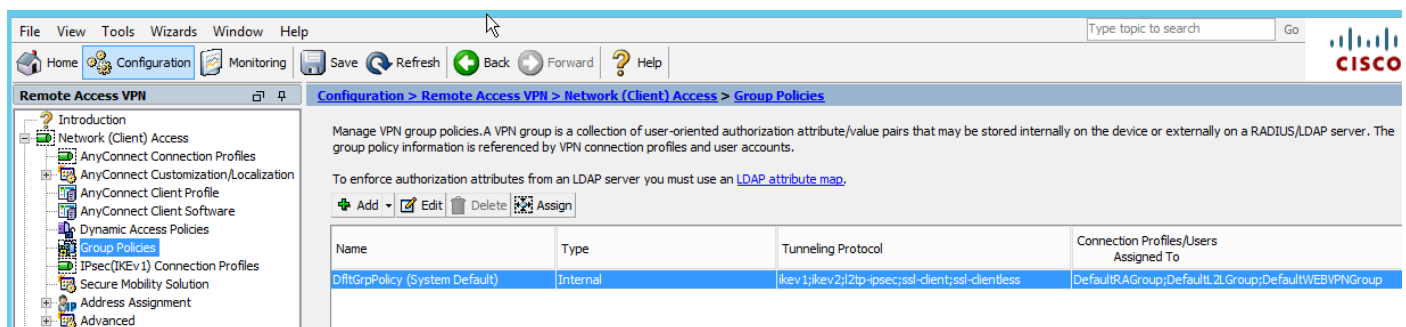
> **注意**：这是没有身份验证许可证密钥的默认配置文件。
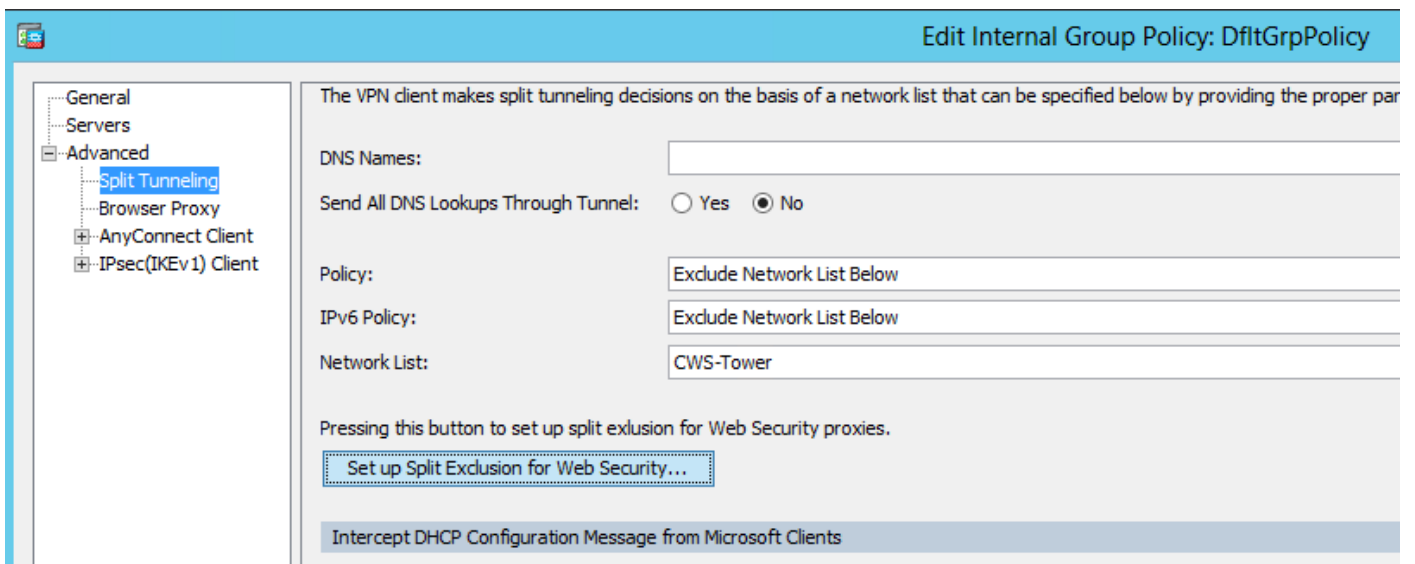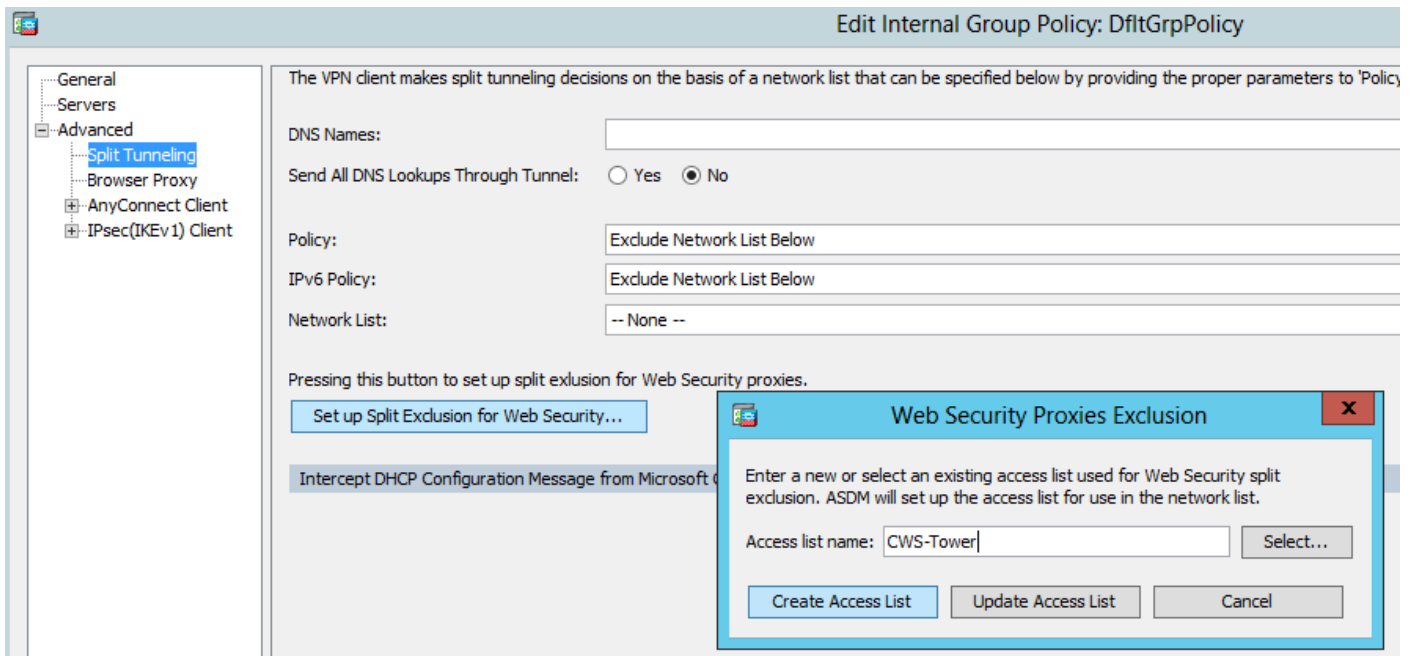
步骤2.编辑新创建的配置文件以添加身份验证许可证密钥并自定义配置。

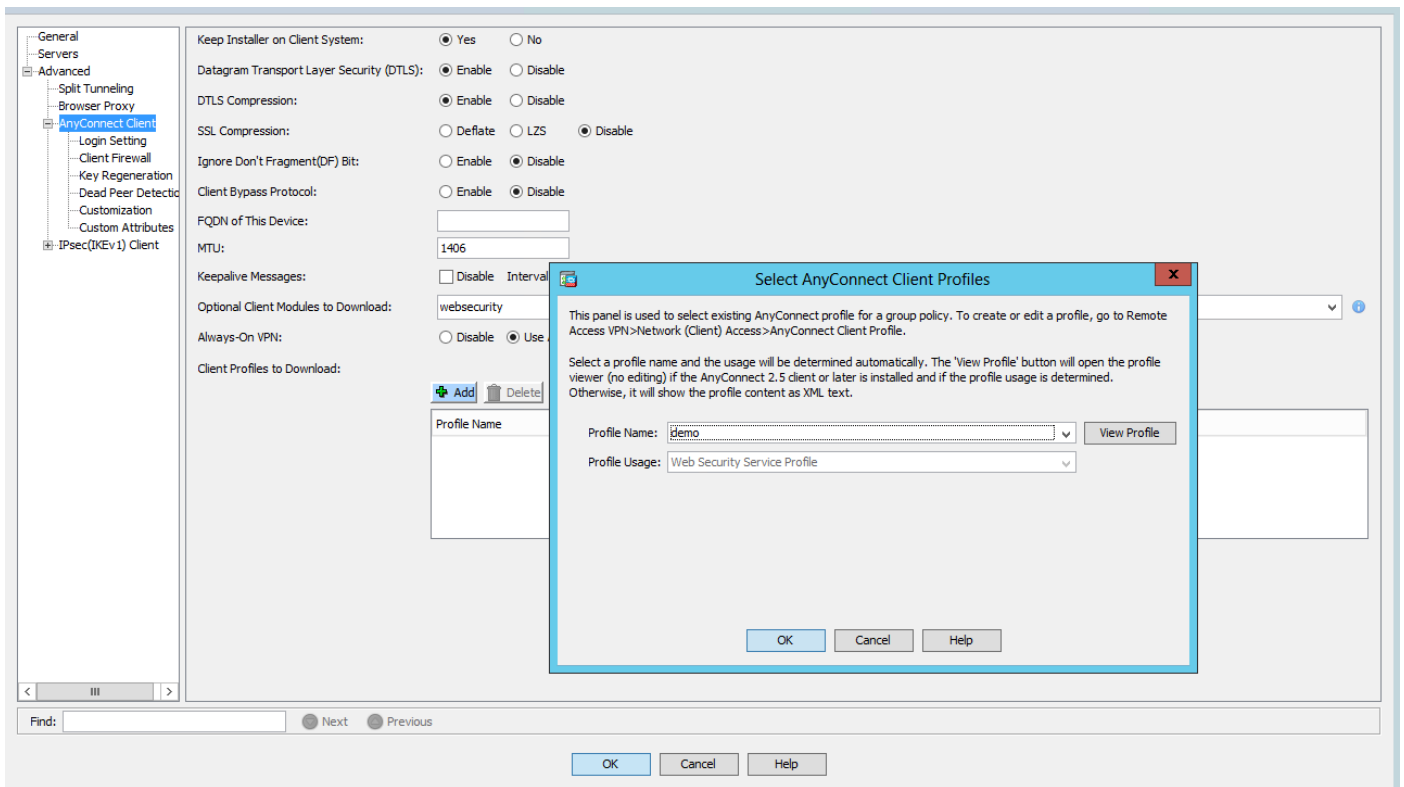## 步骤3.为Web安全设置拆分排除并选择下载Web安全客户端模块

编辑Anyconnect VPN组策略，如图所示。

如图所示，为Web安全设置拆分排除。

选择下载网络安全客户端模块，如图所示。
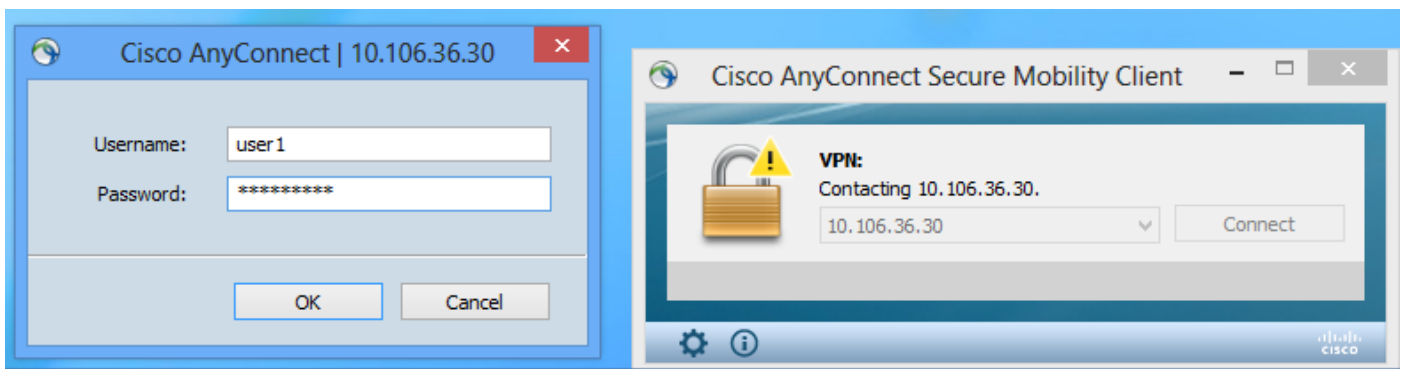
步骤4.下载Web安全客户端配置文件

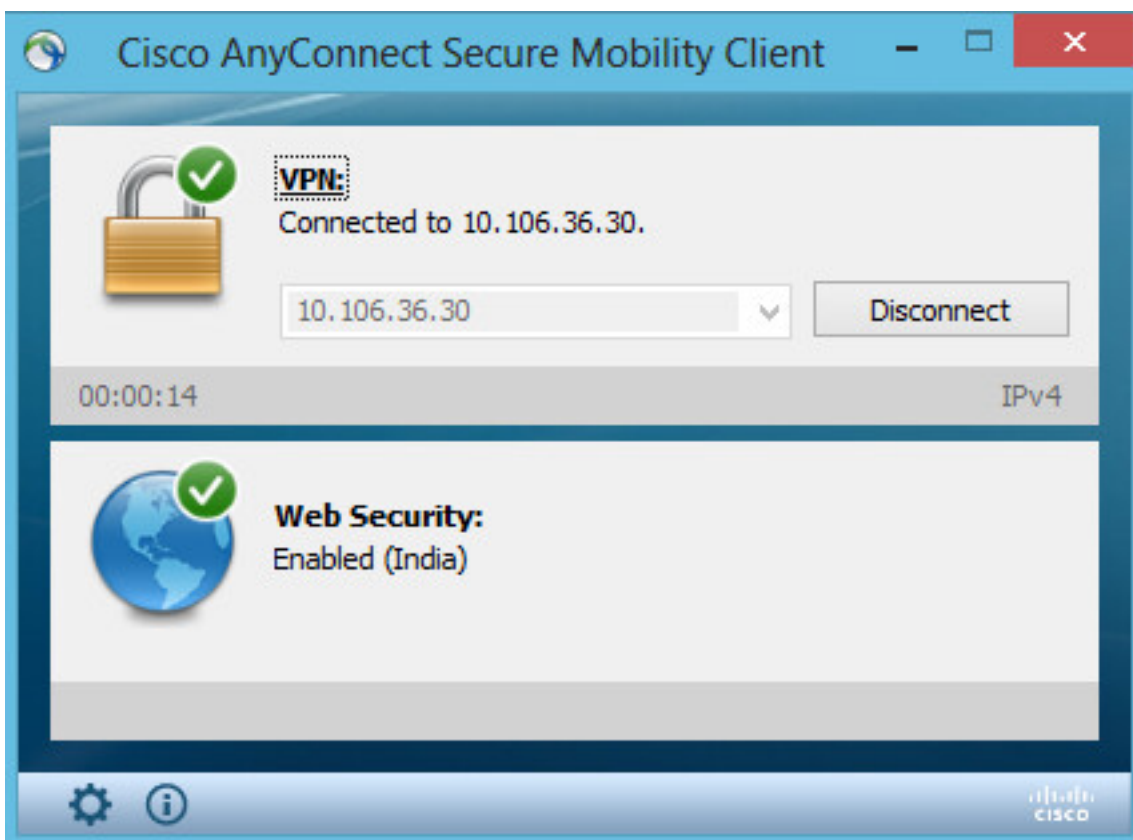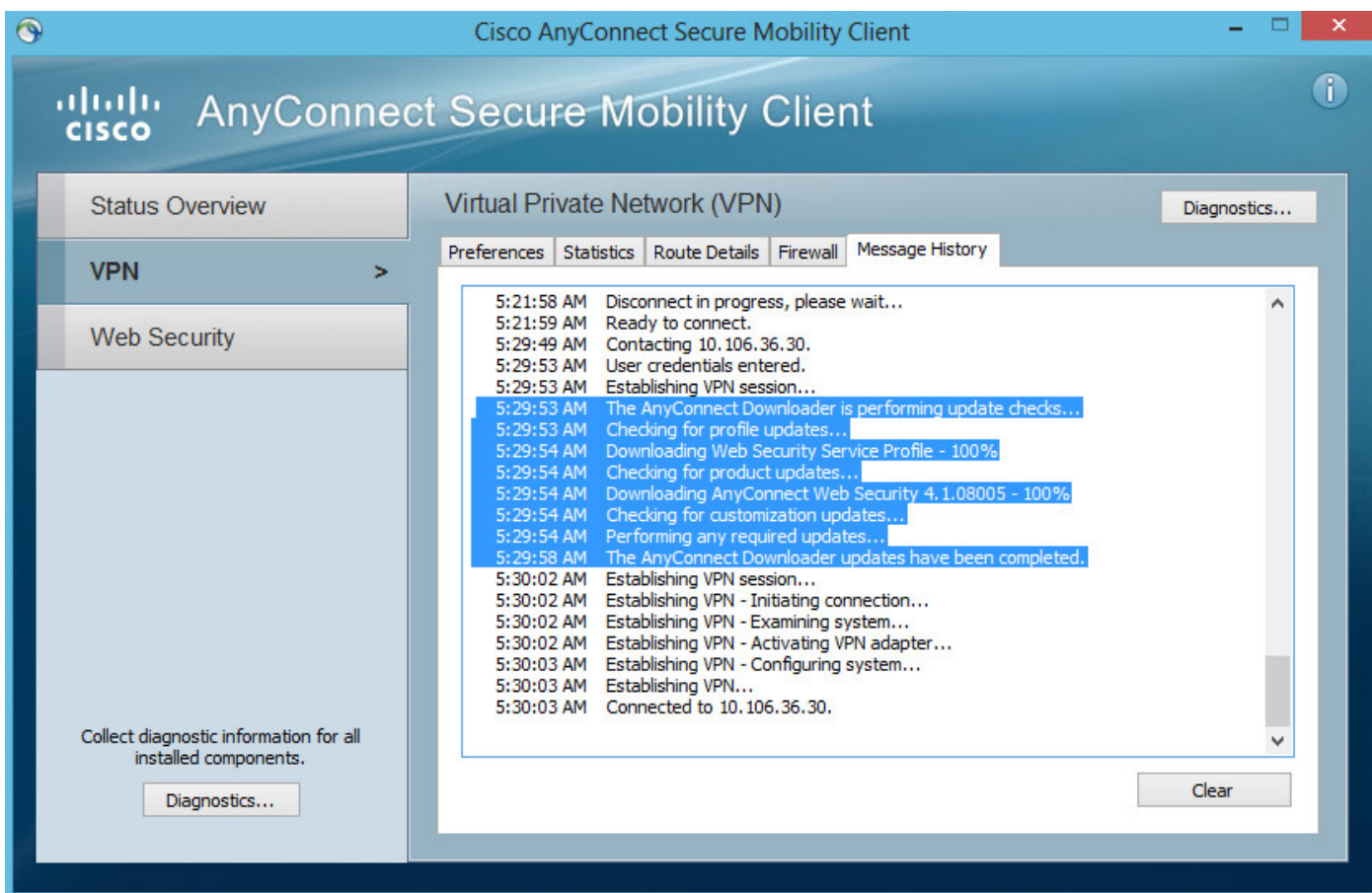编辑Anyconnect VPN组策略>要下载的客户端配置文件>添加，现在选择创建的配置文件（如步骤1中所示）

点击OK并应用更改。

验证

当您连接到Anyconnect VPN时，ASA将通过VPN推送Anyconnect网络安全模块，如图所示。
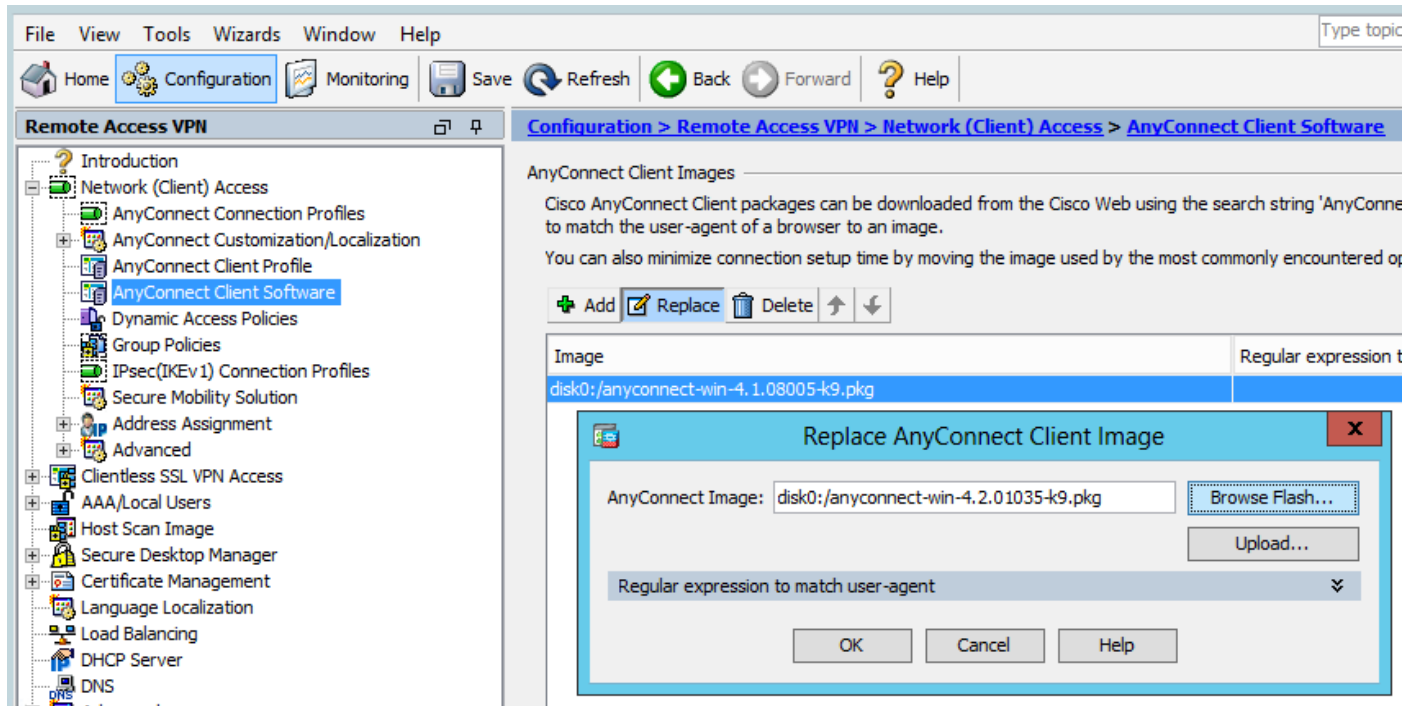
如果已登录，则建议注销，然后重新登录以启用功能。

升级/降级AnyConnect版本

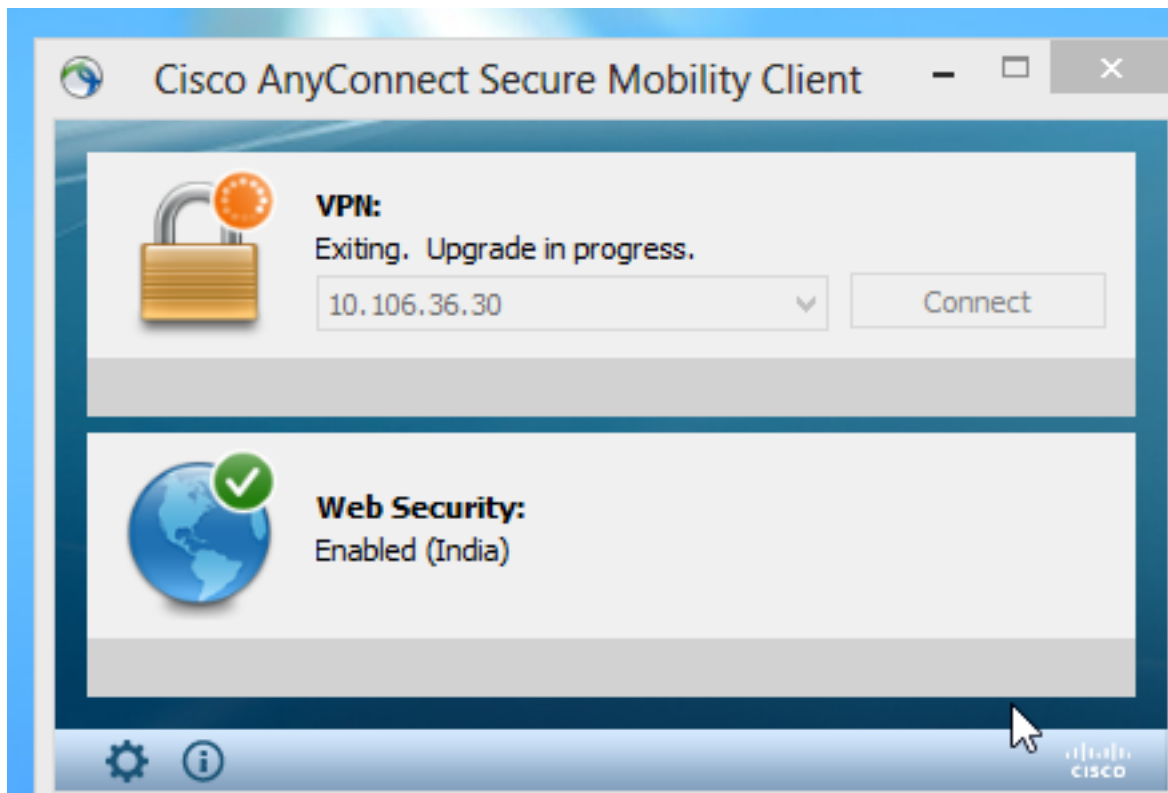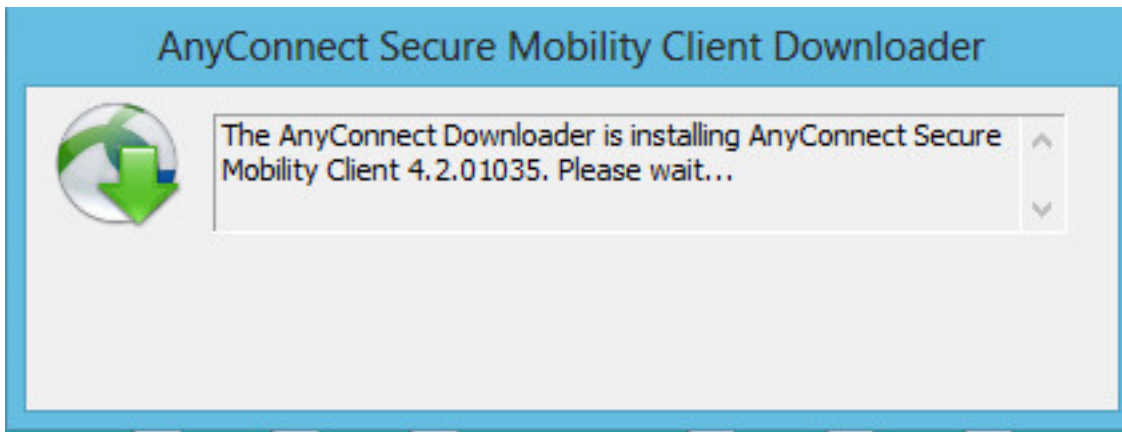升级版本后，部署功能将保持不变。但是，无法降级。因此，使用当前4.1.x示例，可将其升级到

4.2版

涉及的步骤如下：

步骤1.将最新的Anyconnect软件包4.2上传到闪存，并用最新文件替换4.1。

在"**AnyConnect客户端软件**">"**替换**"下，然后选择最近的映像文件。

第二步： 当您重新连接到Anyconnect VPN时，ASA将通过VPN推送最新的Anyconnect模块，而不会更改网络安全配置文件。

注意：不支持降级。

故障排除

本部分提供了可用于对配置进行故障排除的信息。

使用DART收集故障排除信息：

DART是AnyConnect诊断和报告工具，您可以使用它收集数据，以排除AnyConnect安装和连接故障。DART支持Windows 7、Windows Vista、Windows XP、Mac版本10.5和10.6以及Linux Redhat。DART向导在运行AnyConnect的计算机上运行。它为思科技术支持中心(TAC)分析整理日志、状态和诊断信息，不需要管理员权限。

虽然DART不依赖于AnyConnect软件的任何组件来运行，但您可以从AnyConnect启动它，但它将收集AnyConnect日志文件（如果可用）。目前，DART可作为独立安装使用，或者管理员可以将此应用作为AnyConnect动态下载基础设施的一部分推送到客户端PC。安装后，最终用户可以从Cisco文件夹通过"开始"按钮启动向导。