使用SDM在Cisco IOS上配置CSD

目录

简介

虽然安全套接字层 (SSL) VPN (Cisco WebVPN) 会话是安全的，但客户端仍可能在会话完成后留下 Cookie、浏览器文件和电子邮件附件。Cisco Secure Desktop (CSD) 扩展了 SSL VPN 会话的固有安全性，它将会话数据以加密格式写入客户端磁盘的专用*保管库 区域*。此外，此数据还会在 SSL VPN 会话结束后从磁盘上删除。本文档提供Cisco IOS®路由器上CSD的示例配置。

以下 Cisco 设备平台支持 CSD：

- Cisco IOS 路由器版本 12.4(6)T 及更高版本
- Cisco 870、1811、1841、2801、2811、2821、2851、3725、3745、3825、3845、7200 和 7301 路由器
- Cisco VPN 3000 系列集中器 4.7 版及更高版本
- Cisco ASA 5500 系列安全设备版本 7.1 及更高版本
- Cisco Catalyst 与 Cisco 7600 系列 Cisco WebVPN 服务模块版本 1.2 及更高版本

先决条件

要求

尝试进行此配置之前，请确保满足以下要求：

Cisco IOS 路由器要求

- 带高级映像 12.4(6T) 或更高版本的 Cisco IOS 路由器
- Cisco 路由器安全设备管理器 (SDM) 2.3 或更高版本
- 管理站上的 IOS 软件包的 CSD 副本
- 路由器自签名数字证书或证书颁发机构 (CA) 的身份验证**注意：**任何时候使用数字证书，请确保正确设置路由器的主机名、域名和日期/时间/时区。
- 路由器上的启用加密口令
- 在路由器上启用 DNS。若干 WebVPN 服务要求使用 DNS 以便正常工作。

客户端计算机要求

- 远程客户端应当具有本地管理特权；这不是必需的，但强烈建议进行此设置。
- 远程客户端必须安装有 Java Runtime Environment (JRE) 1.4 或更高版本。
- 远程客户端浏览器：Internet Explorer 6.0、Netscape 7.1、Mozilla 1.7、Safari 1.2.2 或 Firefox 1.0
- 已在远程客户端上启用 Cookie，并允许弹出窗口

使用的组件

本文档中的信息基于以下软件和硬件版本：

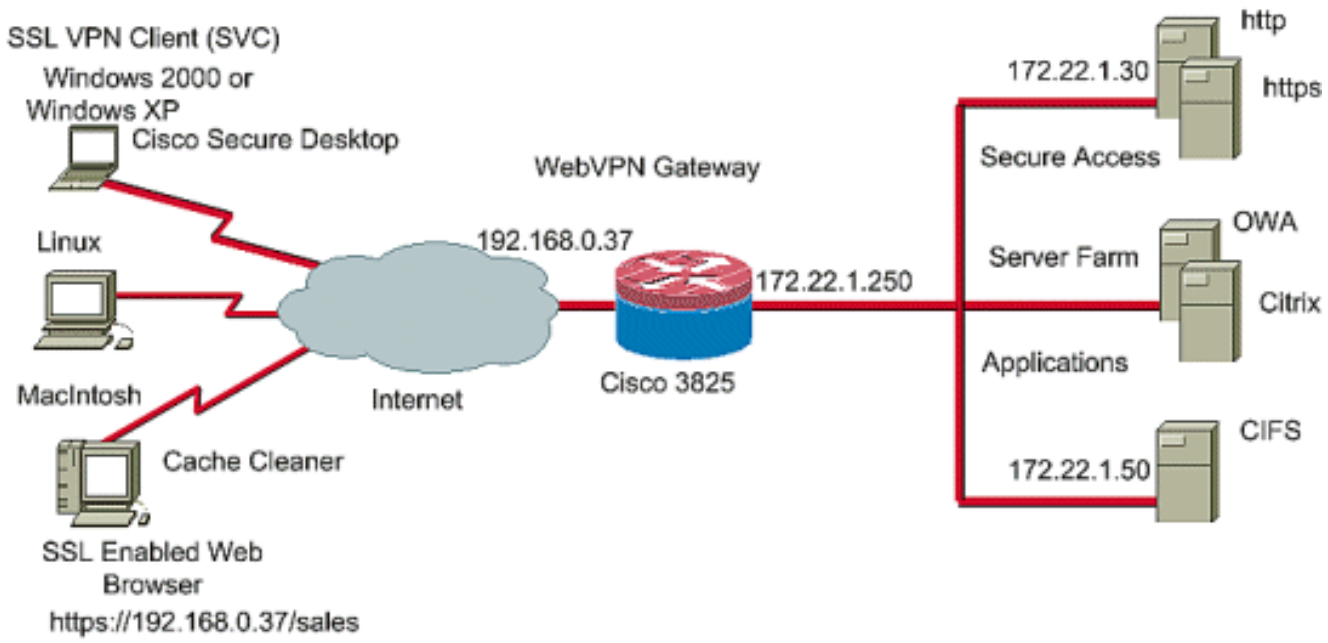
- Cisco IOS 路由器 3825 版本 12.9(T)
- SDM 版本 2.3.1

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。

网络图

本文档使用以下网络设置：

本示例使用 Cisco 3825 系列路由器以允许安全访问公司 Intranet。Cisco 3825 系列路由器具有可配置的 CSD 功能和特性，由此增强了 SSL VPN 连接的安全性。客户端可以通过以下三种 SSL VPN 方法之一连接到启用了 CSD 的路由器：无客户端 SSL VPN (WebVPN)、瘦客户端 SSL VPN（端口转发）或 SSL VPN 客户端（全隧道 SVC）。



相关产品

此配置也可用于以下硬件和软件版本：

- Cisco 路由器平台 870、1811、1841、2801、2811、2821、2851、3725、3745、3825、3845、7200 和 7301
- Cisco IOS 高级安全映像版本 12.4(6)T 及更高版本

规则

有关文档规则的详细信息，请参阅 Cisco 技术提示规则。

配置

WebVPN 网关允许用户通过其中一种 SSL VPN 技术连接到路由器。在设备上，每个 IP 地址只允许有一个 WebVPN 网关，但一个 WebVPN 网关可以连接多个 WebVPN 上下文。每个上下文都由一个唯一名称标识。组策略标识了特定 WebVPN 上下文所配置的可用资源。

IOS 路由器上的 CSD 配置分两个阶段完成：

阶段 I：使用 SDM 配置 CSD 的路由器准备工作

1. **配置 WebVPN 网关、WebVPN 上下文和组策略**。**注意：**此步骤为可选步骤，本文档未详细介绍。如果您的路由器已经配置了其中一种 SSL VPN 技术，请忽略此步骤。
2. **在 WebVPN 上下文中启用 CSD**。

阶段 II：使用 Web 浏览器配置 CSD。

1. **定义 *Windows 位置*。**
2. **标识位置条件**。
3. **配置 Windows 位置模块和功能**。
4. **配置 Windows CE、Macintosh 和 Linux 功能**。

阶段 I：使用 SDM 配置 CSD 的路由器准备工作。

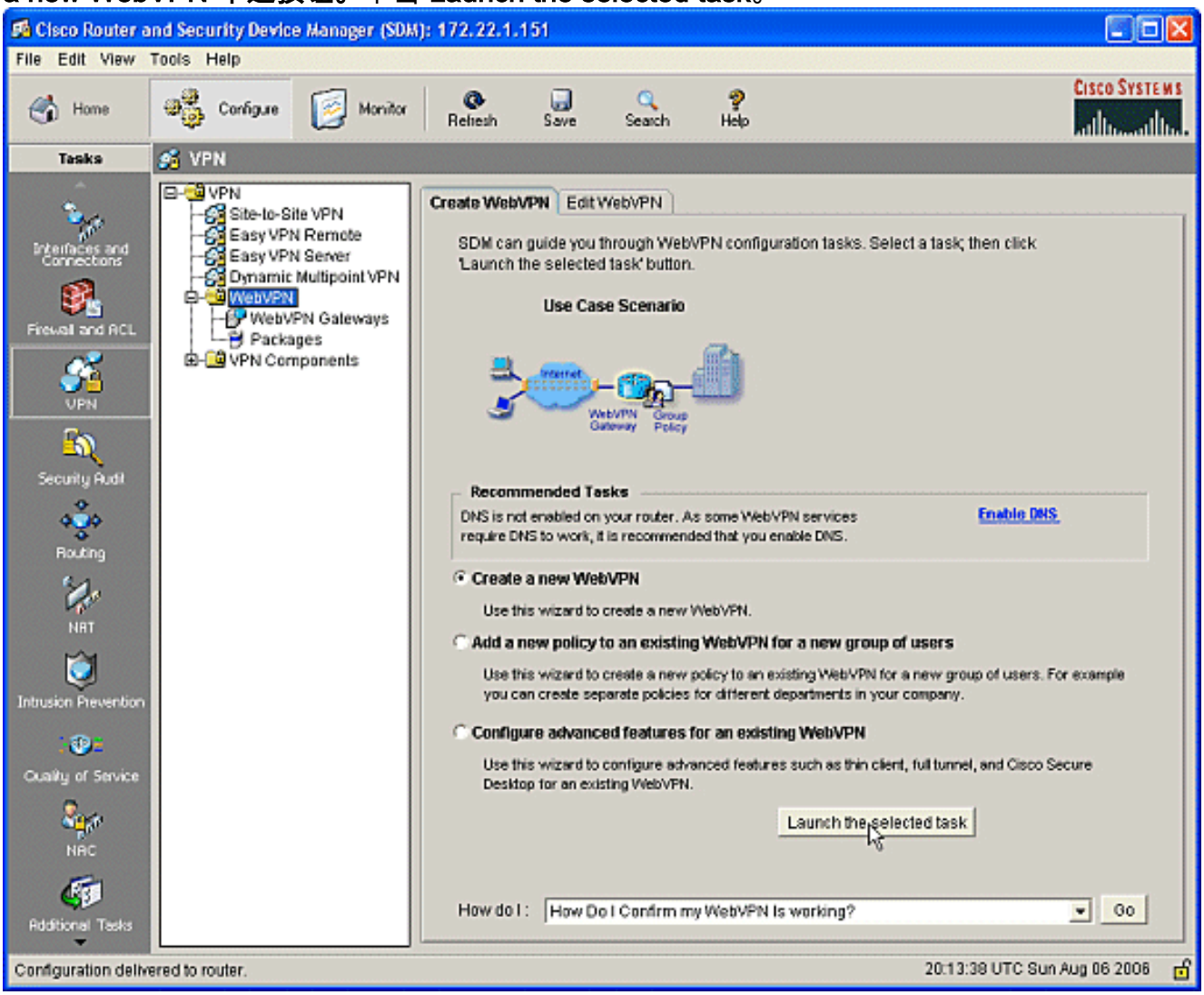
可以使用 SDM 或从命令行界面 (CLI) 配置 CSD。 此配置使用 SDM 和 Web 浏览器。

使用以下步骤在您的 IOS 路由器上完成 CSD 配置。

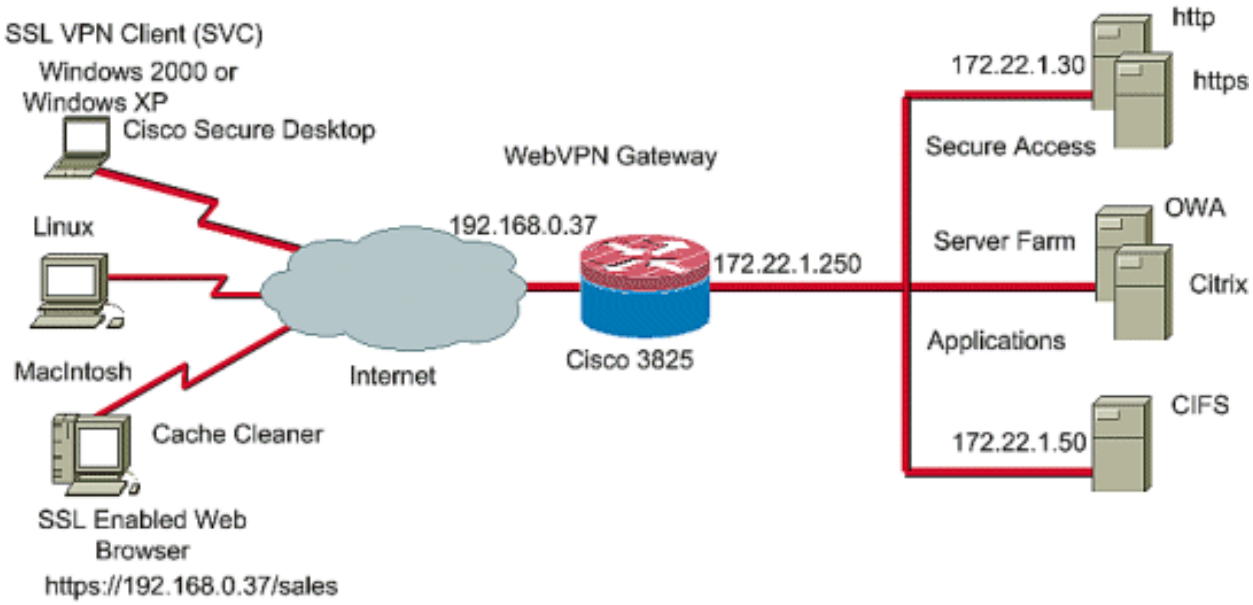
阶段 I：步骤 1：配置 WebVPN 网关、WebVPN 上下文和组策略。

您可以使用 WebVPN Wizard 完成此任务。

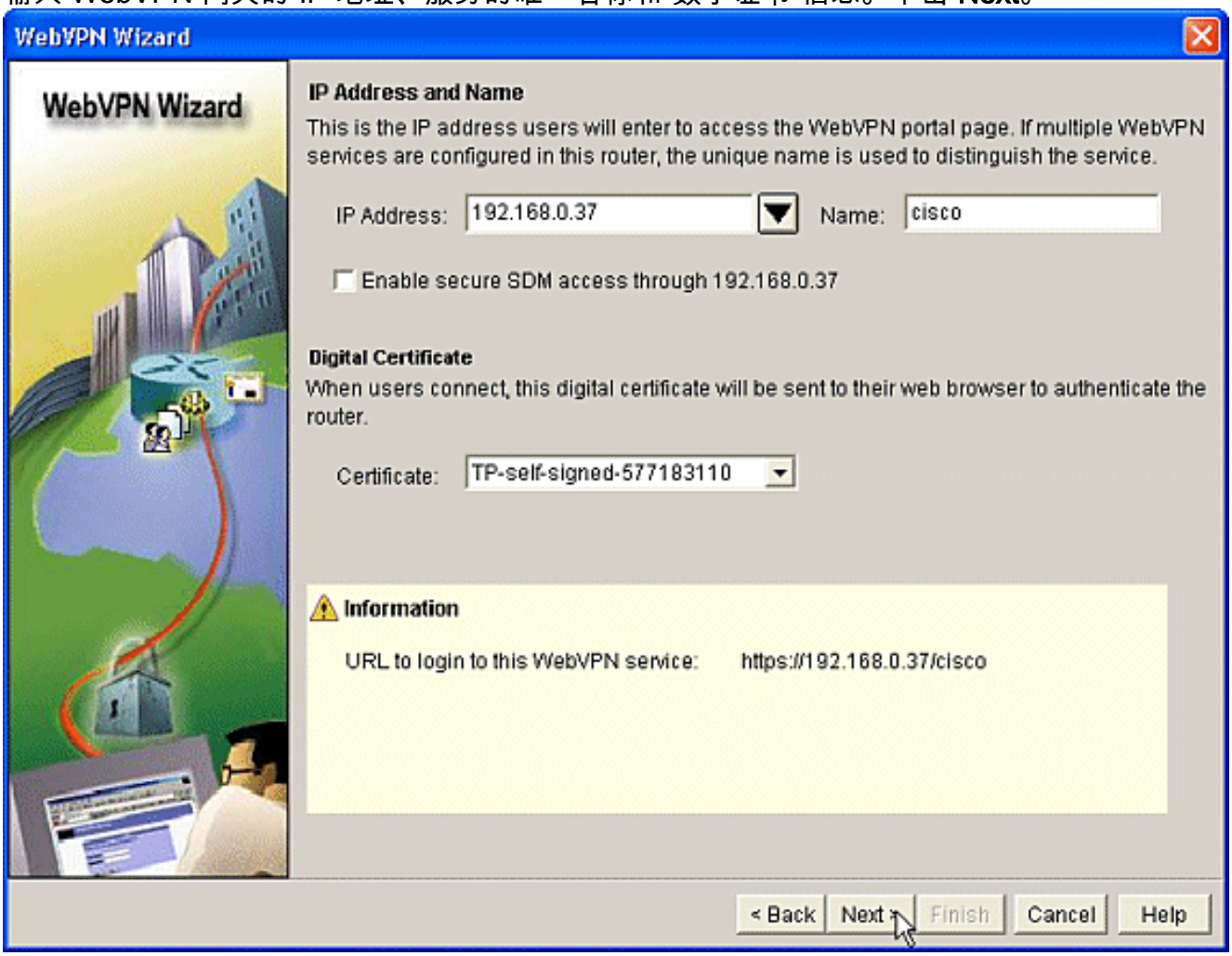
1. 打开 SDM 并转到 **Configure > VPN > WebVPN**。单击 **Create WebVPN 选项卡并选中“Create a new WebVPN”单选按钮。**单击 **Launch the selected task**。



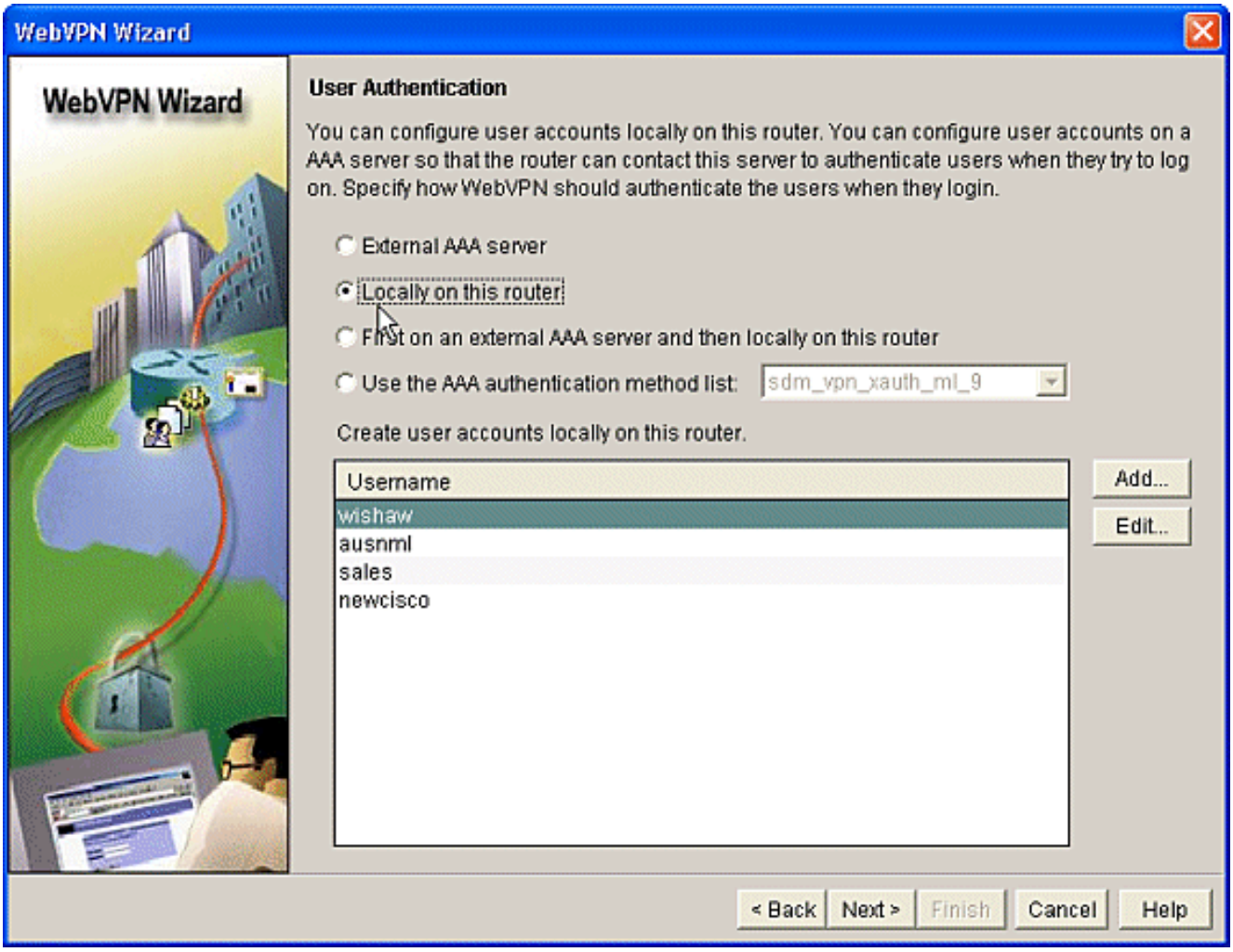
2. WebVPN Wizard 屏幕列出了您可以配置的参数。单击 **Next**。



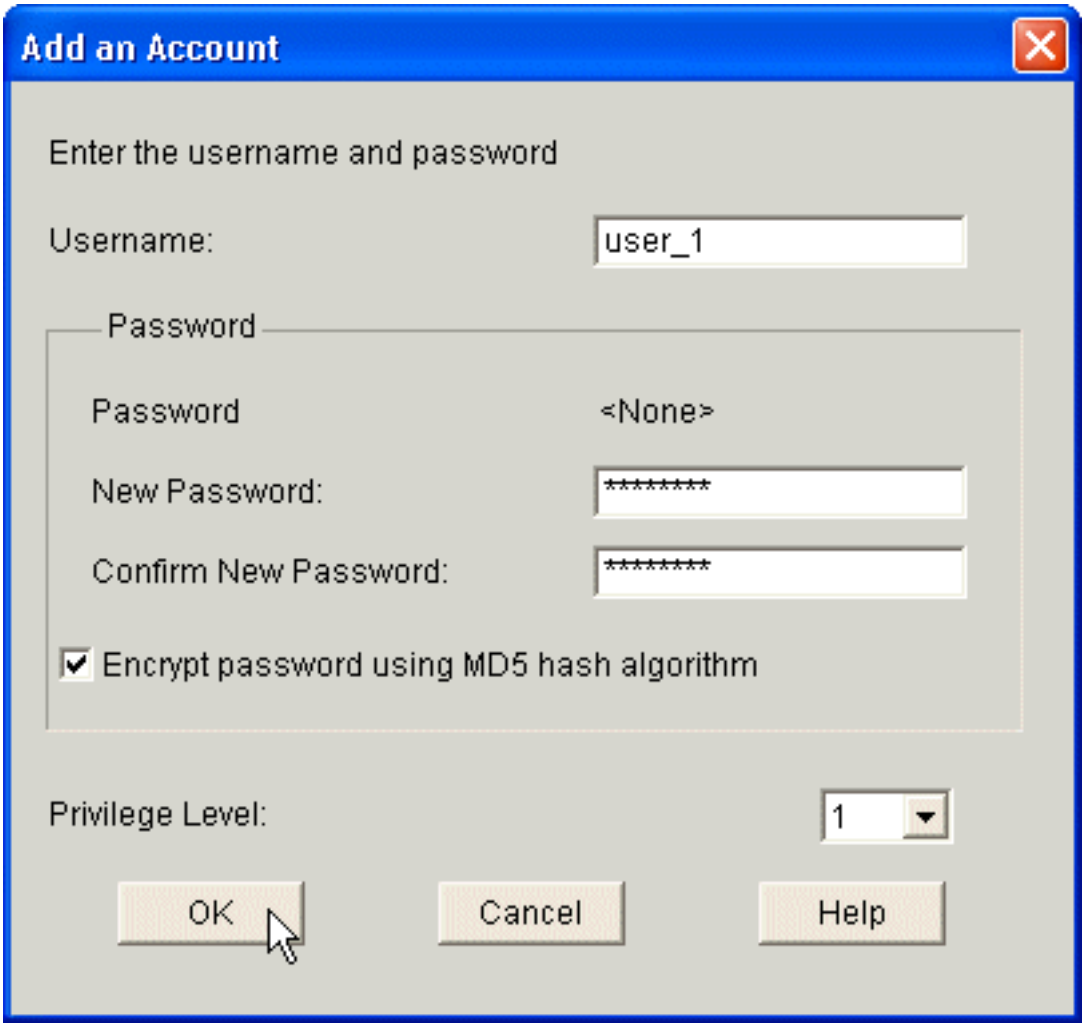
3. 输入 WebVPN 网关的 IP 地址、服务的唯一名称和“数字证书”信息。单击 **Next**。



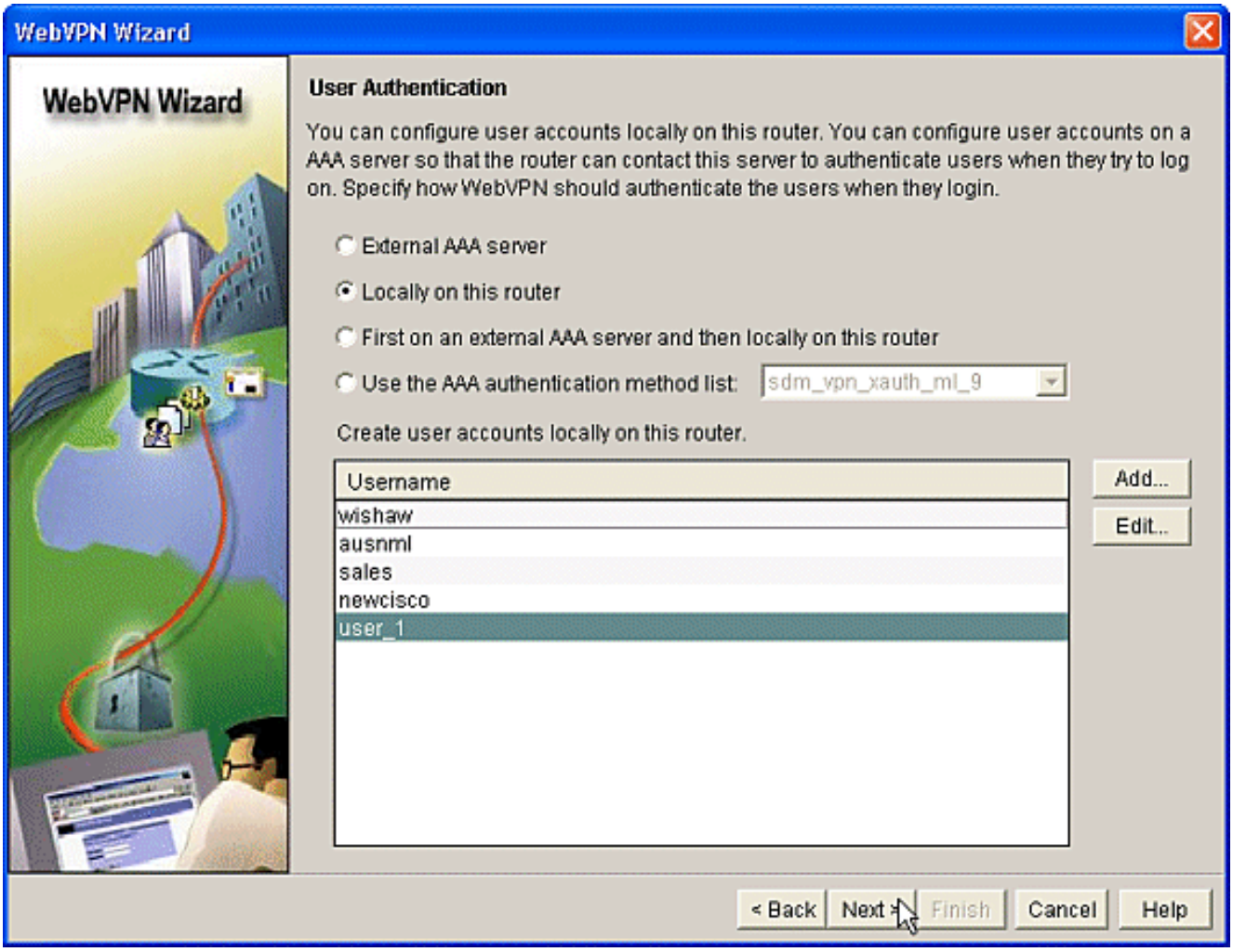
4. 可以为此 WebVPN 网关的身份验证创建用户帐户。可以使用本地帐户或在外部身份验证、授权和记账 (AAA) 服务器上创建的帐户。本示例使用路由器上的本地帐户。选中单选按钮 **Locally on this router** 并单击“Add”。



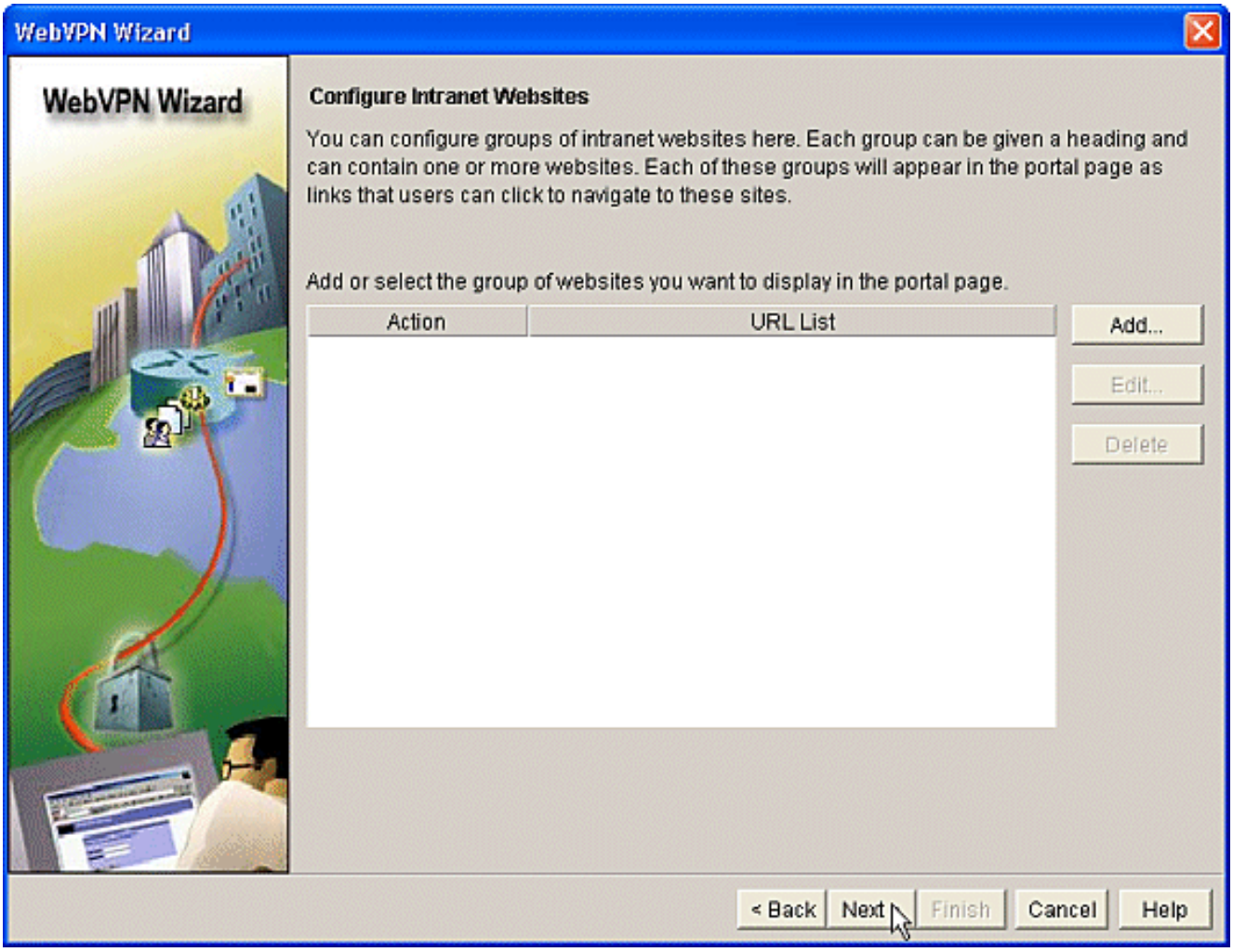
5. 在“Add an Account”屏幕上输入新用户的帐户信息并单击 **OK**。



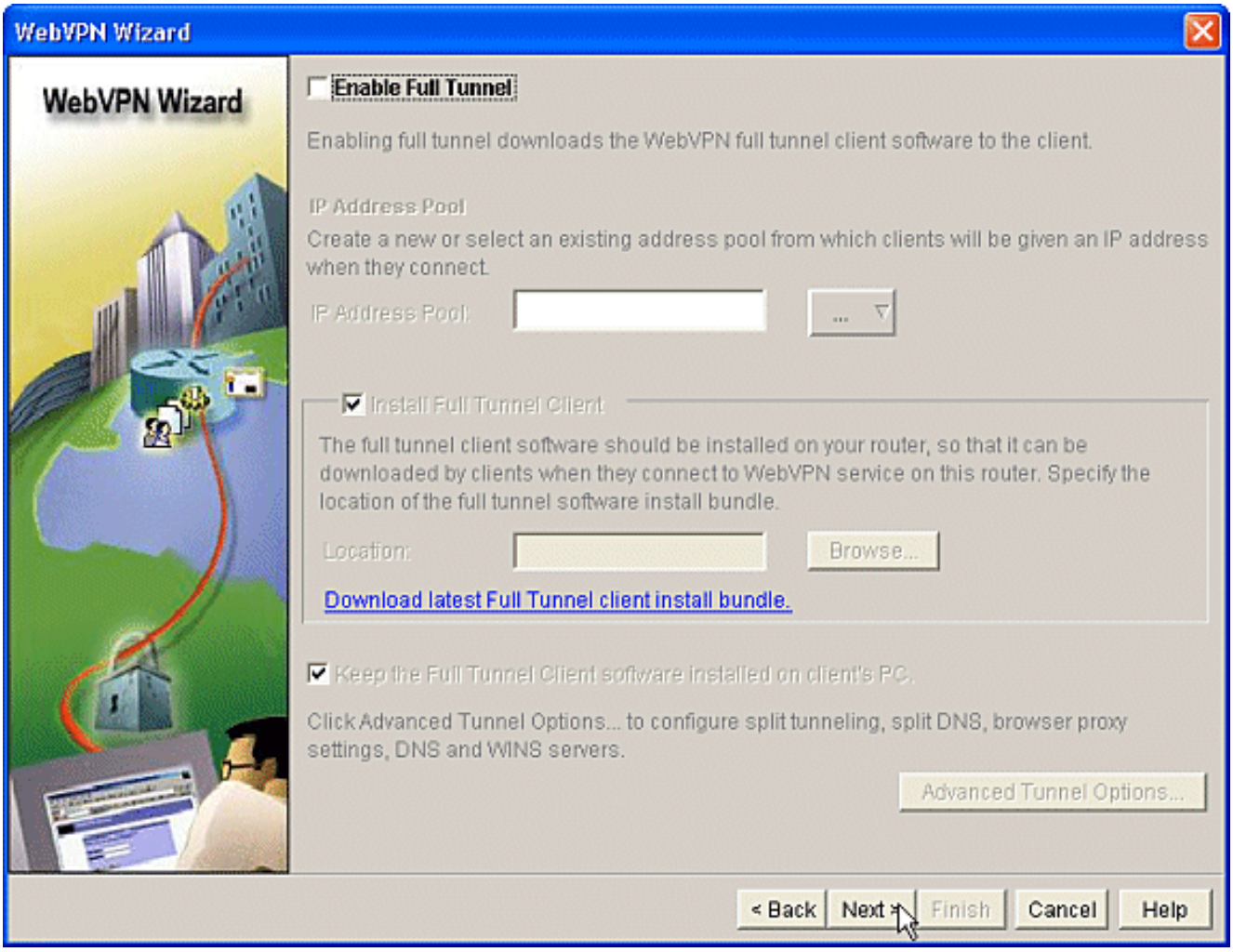
6. 创建用户后，在“User Authentication”页面上单击 **Next。**



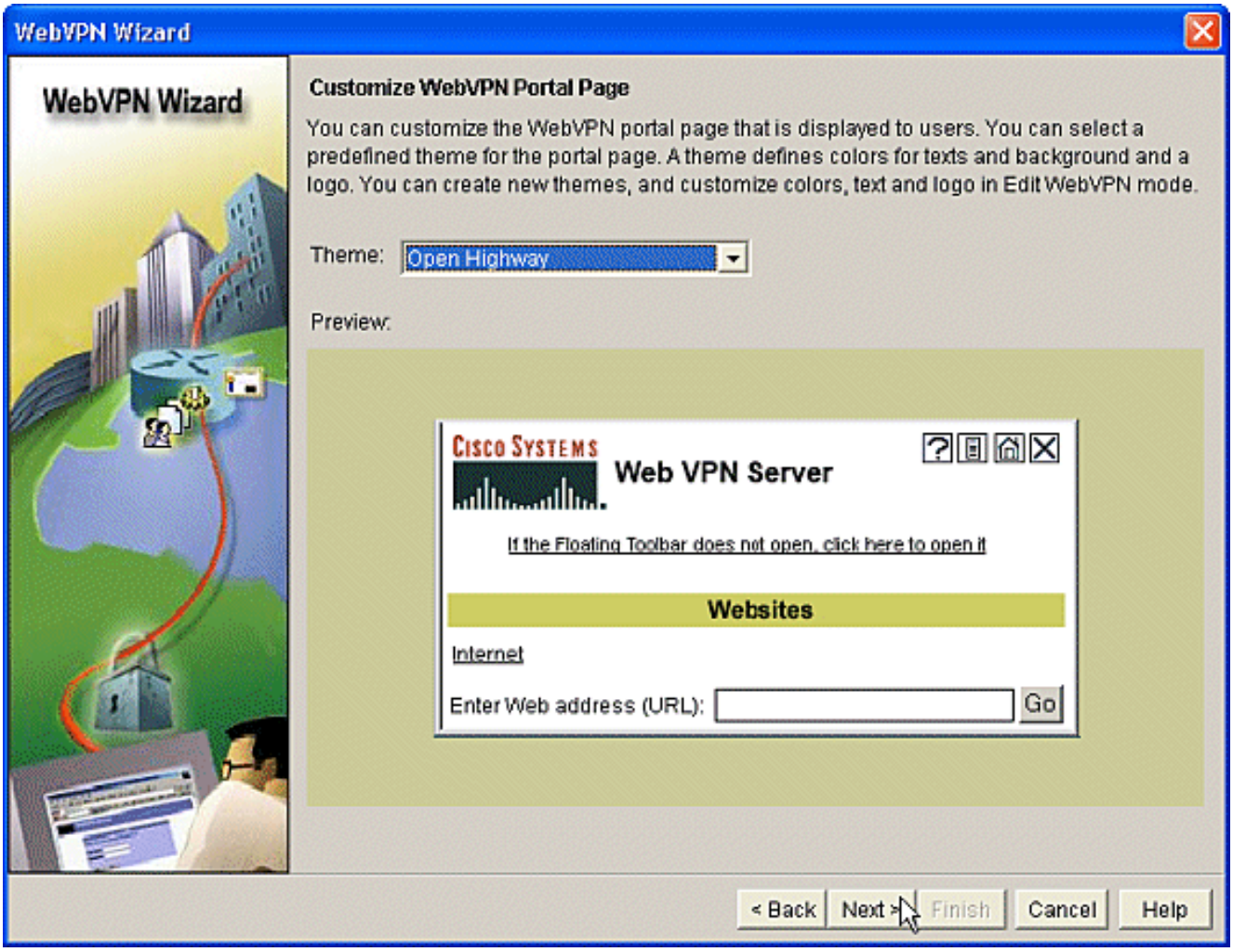
7. “Configure Intranet Websites”屏幕允许您配置 WebVPN 网关用户的可用网站。本文档主要关注 CSD 的配置，因此略过此页。单击 **Next**。



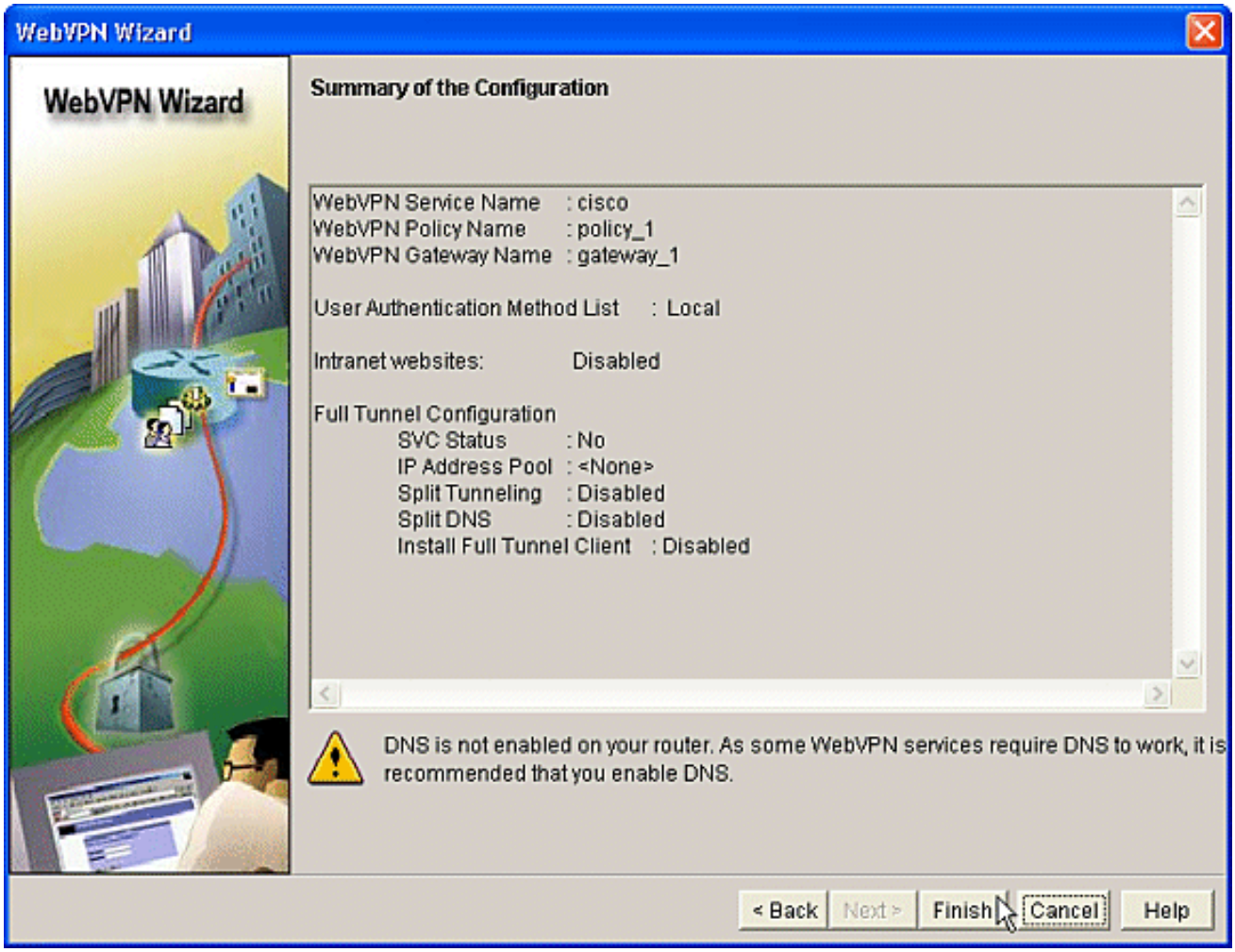
8. 虽然在下一个 WebVPN Wizard 屏幕上可以选择启用全隧道 SSL VPN 客户端，但本文档关注的是如何启用 CSD。取消选中 **Enable Full Tunnel 并单击“Next”。**



9. 您可以自定义呈现给用户的 WebVPN 门户页面的外观。在本例中，我们选择接受默认外观。单击 **Next**。



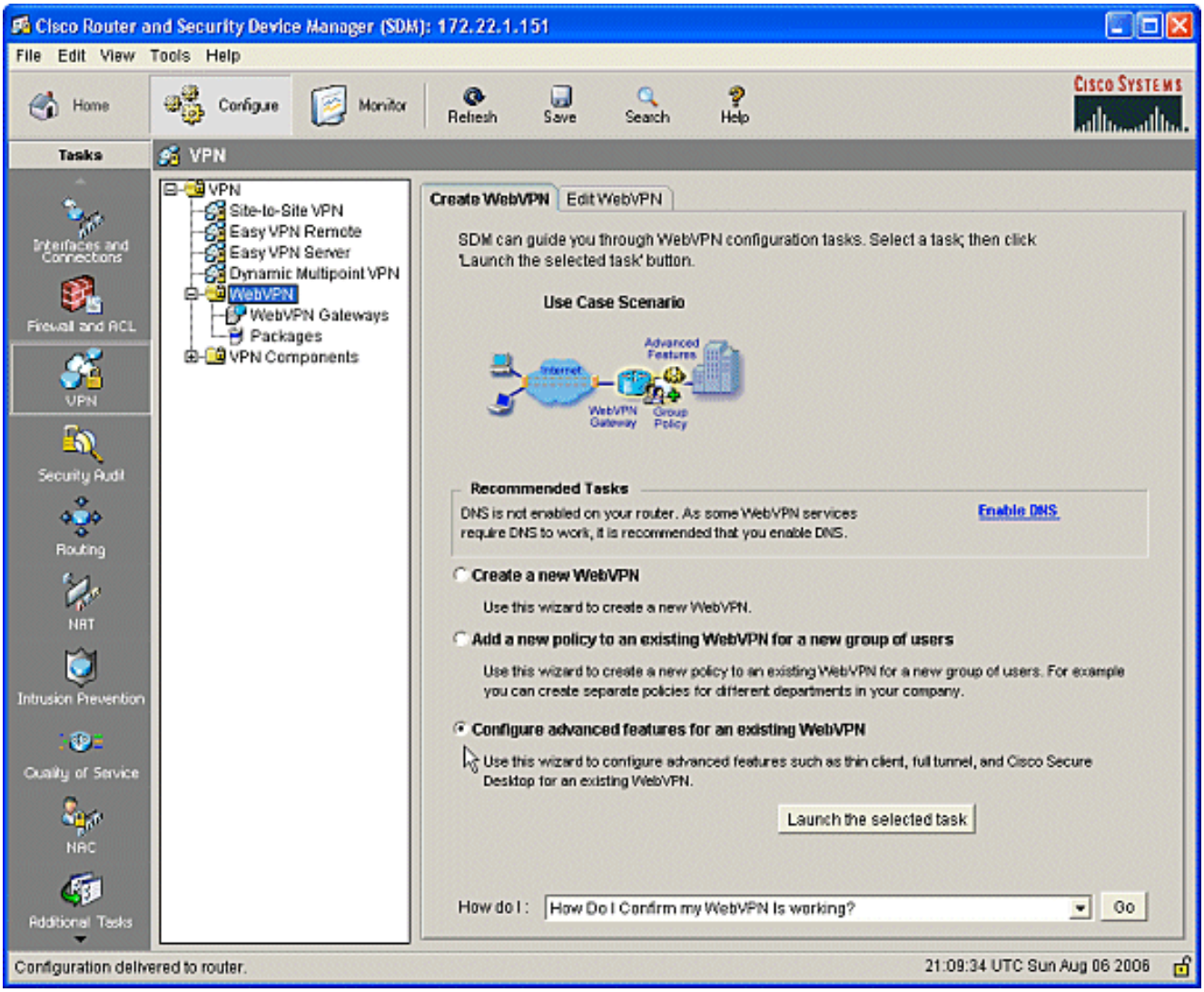
10. 向导显示此屏幕系列中的最后一个屏幕。其中显示了 WebVPN 网关的配置摘要。单击 **Finish** **并在出现提示时单击“OK”。**



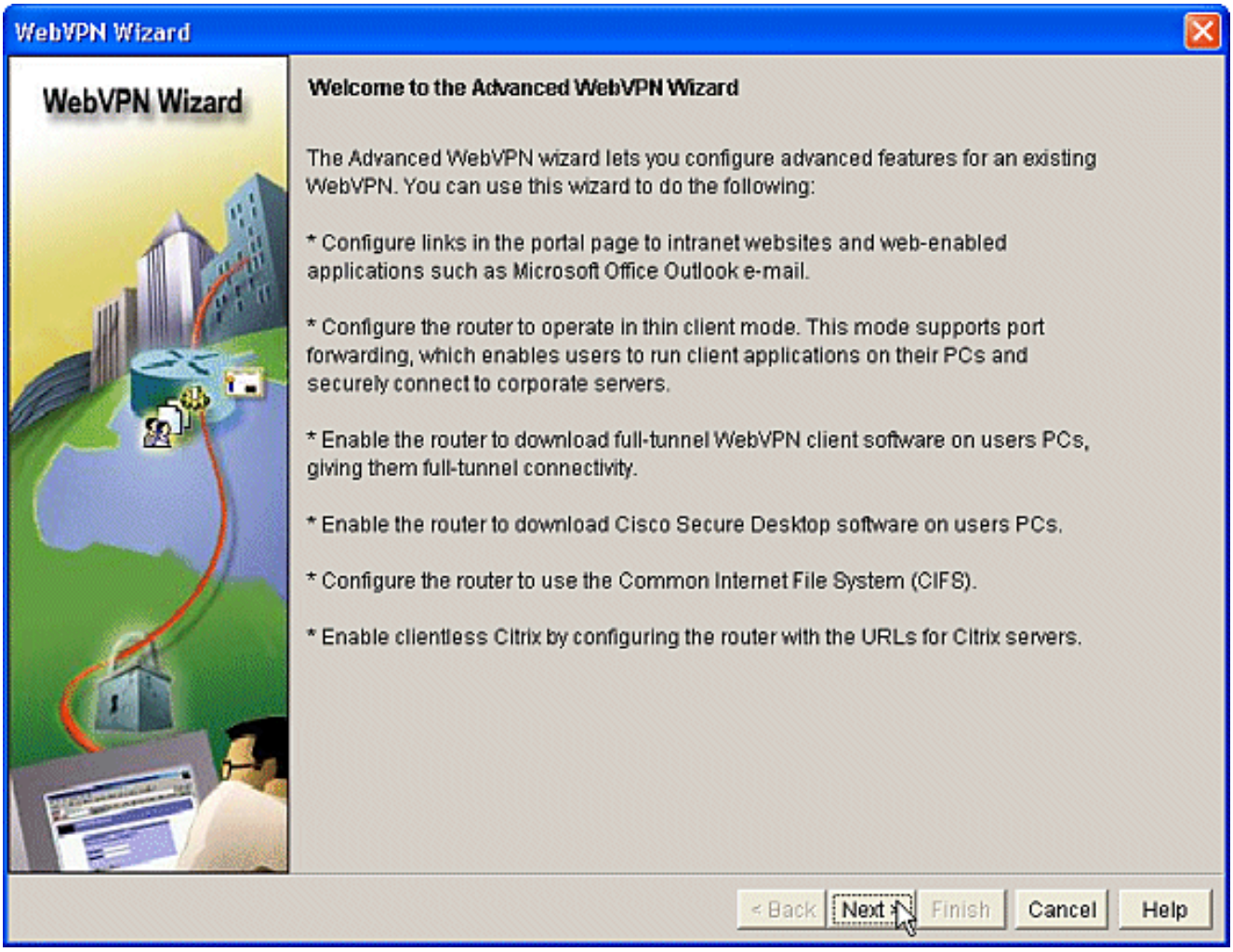
阶段 I：步骤 2：在 WebVPN 上下文中启用 CSD。

使用 WebVPN Wizard 在 WebVPN 上下文中启用 CSD。

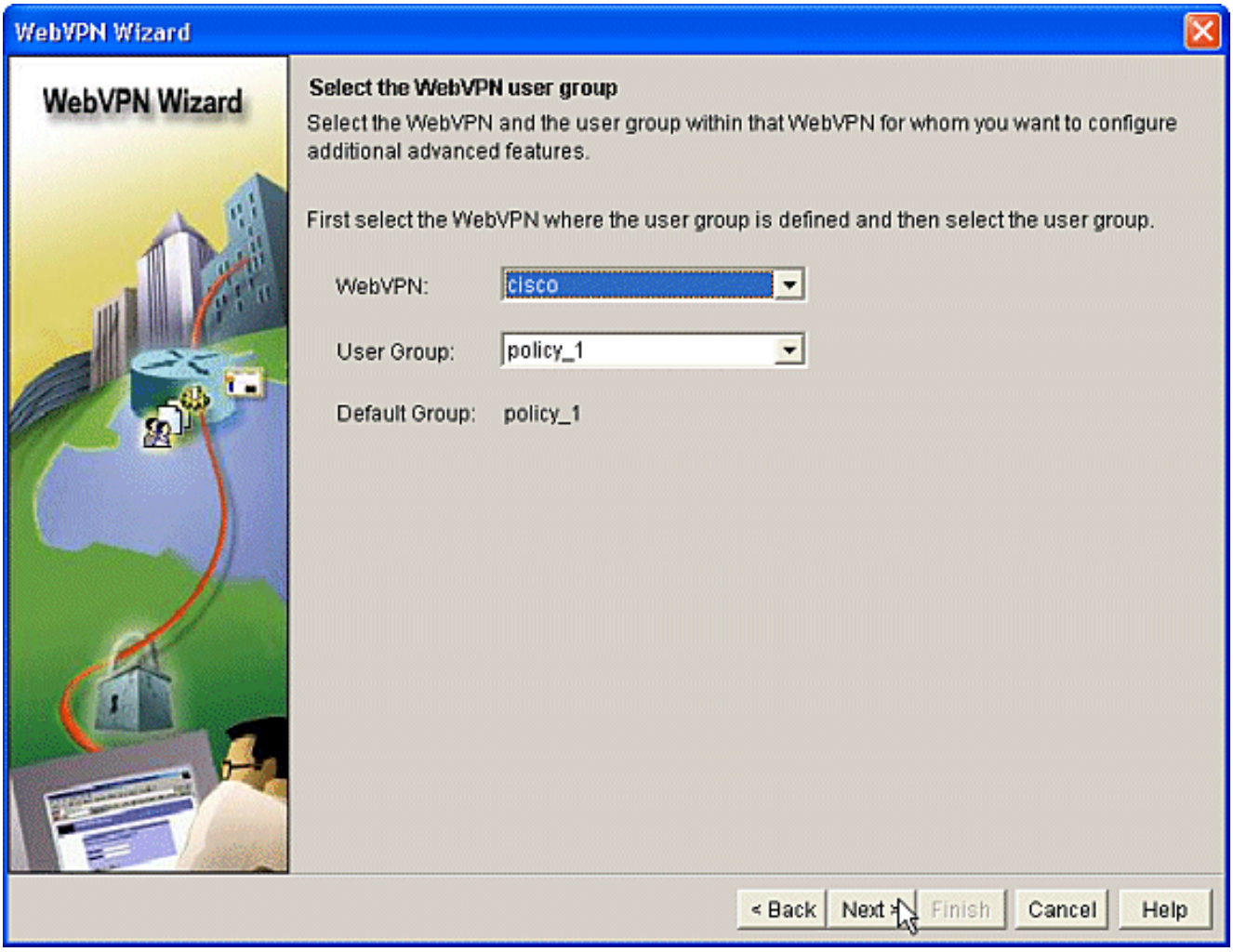
1. 使用 WebVPN Wizard 的高级功能为新创建的上下文启用 CSD。如果尚未安装 CSD 软件包，则该向导允许您进行安装。在 SDM 中，单击 **Configure 选项卡。**在导航窗格中，单击 **VPN > WebVPN。**单击 **Create WebVPN 选项卡。**选中 **Configure advance features for an existing WebVPN 单选按钮。**单击 **Launch the selected task 按钮。**



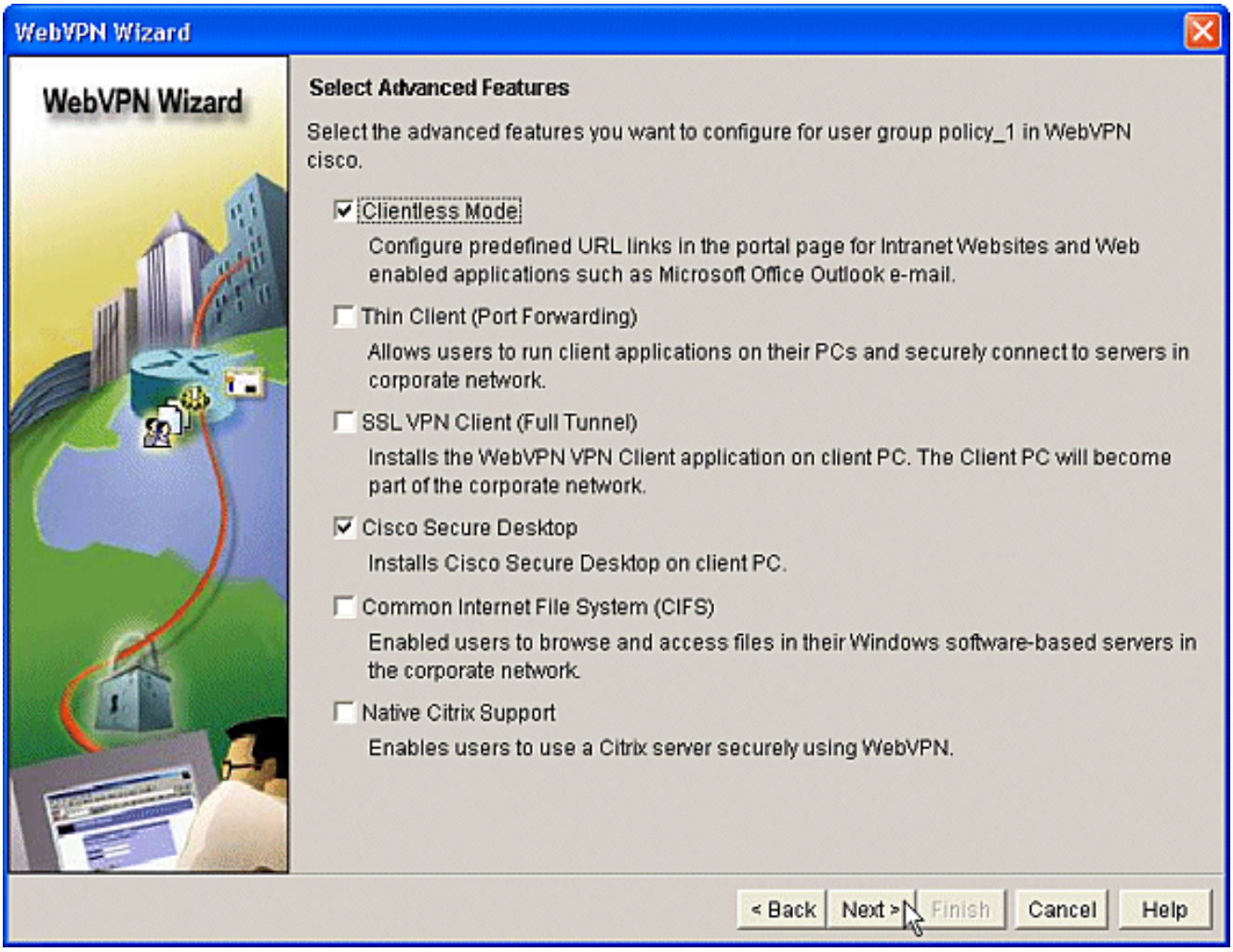
2. 这时将显示 Advanced WebVPN Wizard 的欢迎页面。单击 **Next**。



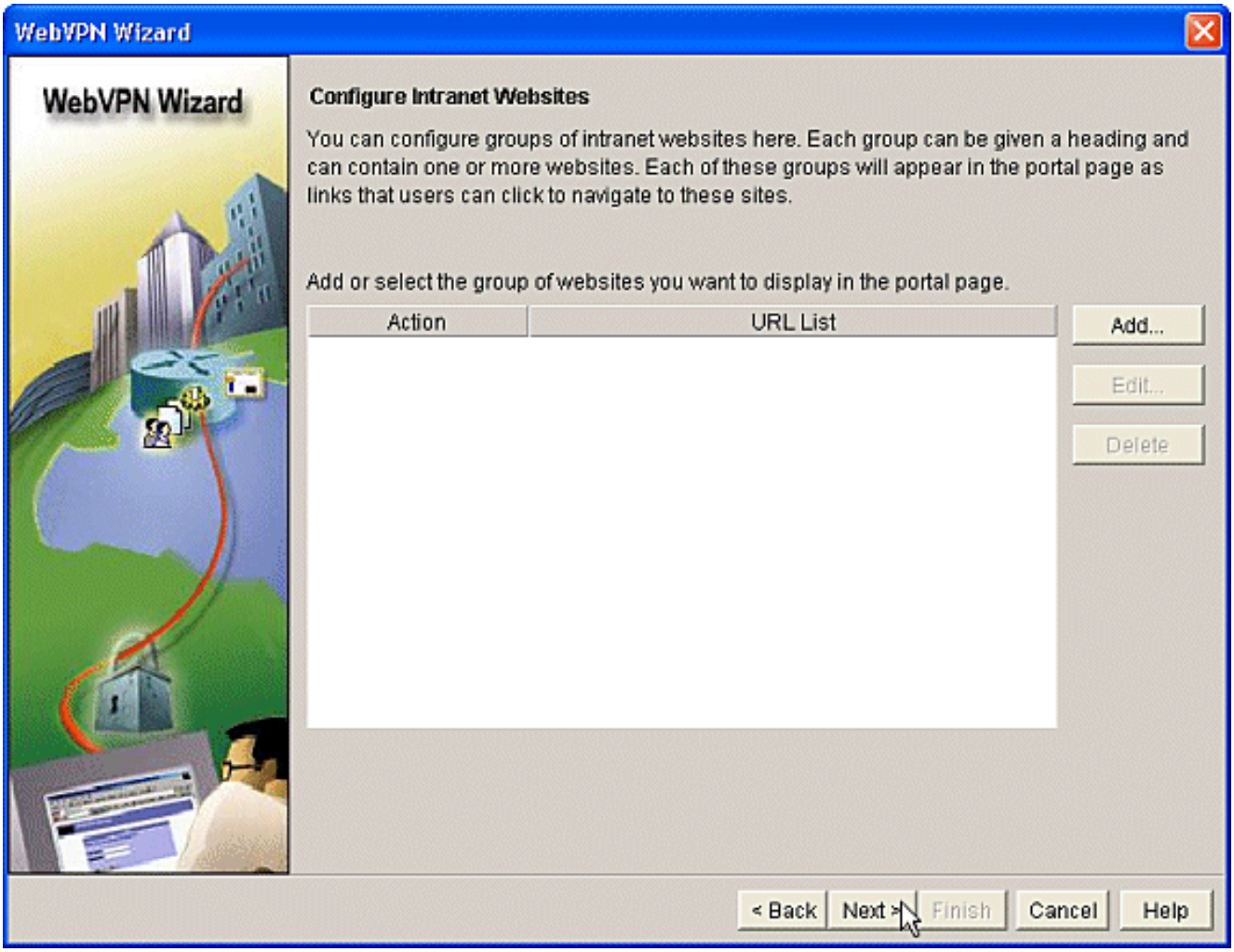
3. 从字段的下拉框中选择 WebVPN 和用户组。Advanced WebVPN Wizard 功能将应用于您的选择。单击 **Next**。



4. “Select Advanced Features”屏幕允许您从所列的技术中进行选择。选中 **Cisco Secure Desktop**。本例选择了 **Clientless Mode**。如果选择所列的任何其他技术，将打开其他窗口，从中可以输入相关信息。单击 **Next 按钮**。

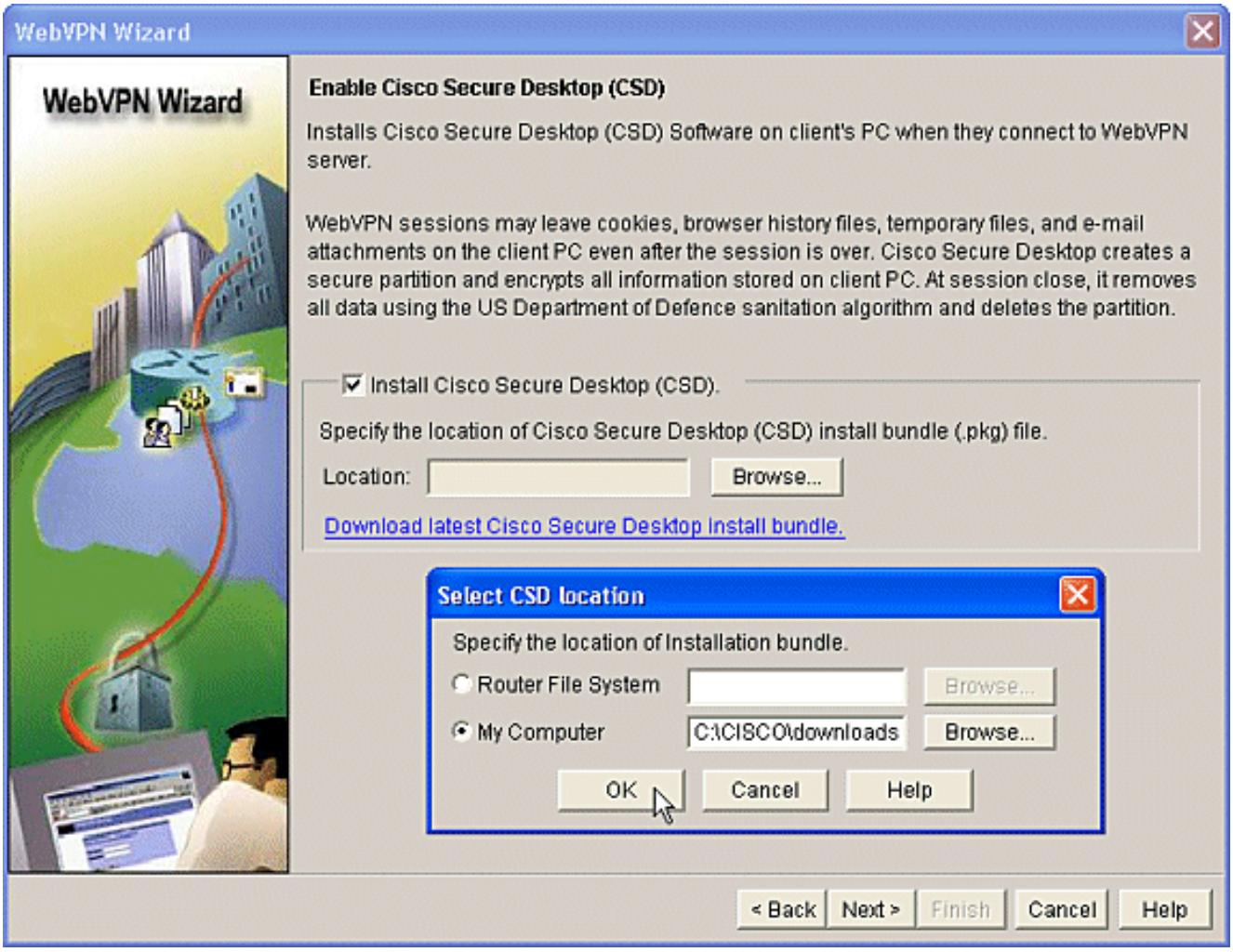


5. “Configure Intranet Websites”屏幕允许您配置希望提供给用户的网站资源。您可以添加公司的内部网站，例如 Outlook Web Access (OWA)。



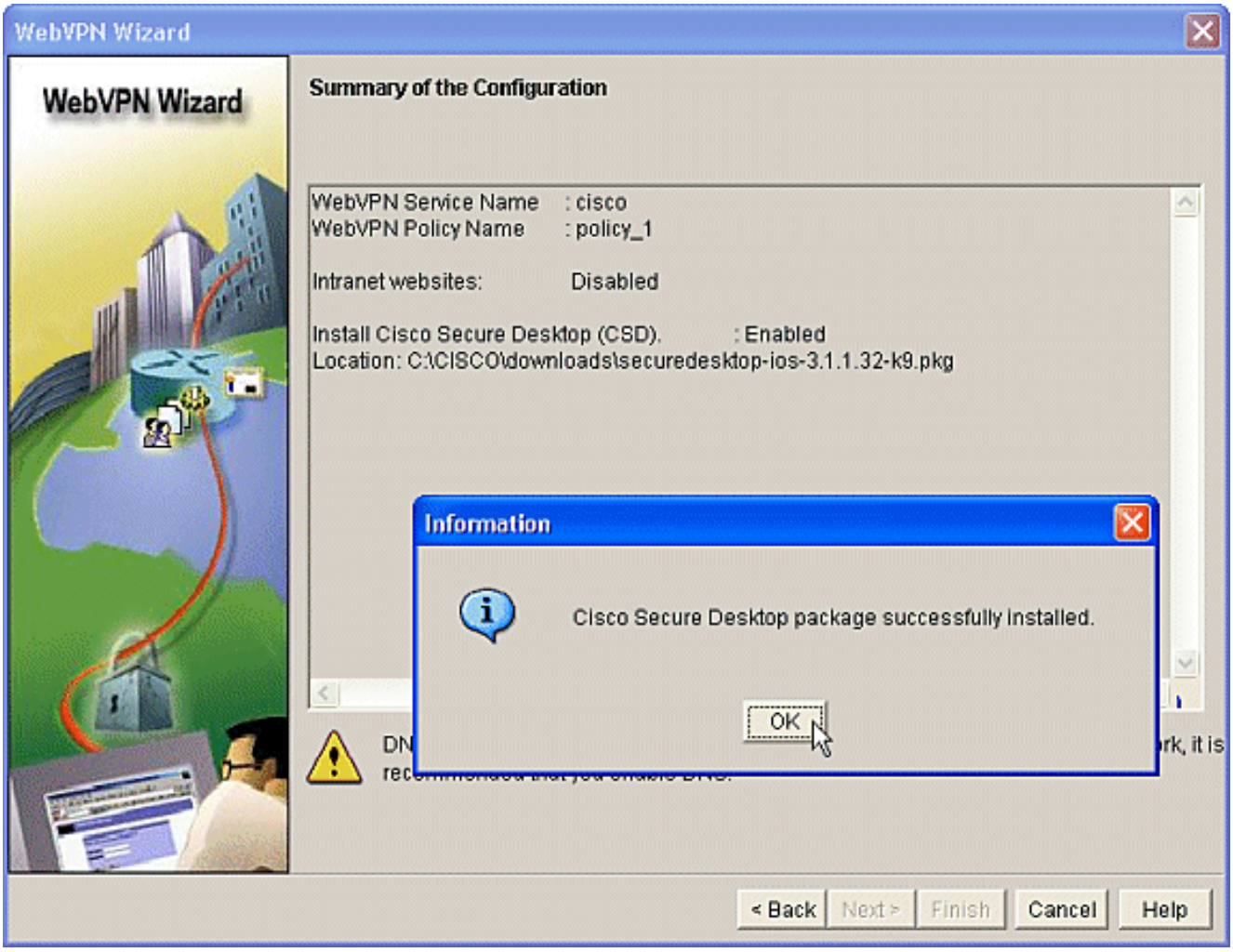
6. 在“Enable Cisco Secure Desktop (CSD)”屏幕中，可以选择为此上下文启用 CSD。选中 **Install Cisco Secure Desktop (CSD)** 旁边的框并单击“Browse”。

7. 在“Select CSD Location”区域中，选中 **My Computer**。单击 **Browse 按钮**。选择您的管理工作站上的 CSD IOS 软件包文件。单击 **OK 按钮**。单击 **Next 按钮**。



8. 这时将显示“Summary of the Configuration”屏幕。此时请单击完成按钮。

9. 当看到成功安装了 CSD 软件包文件后，单击 **OK**。



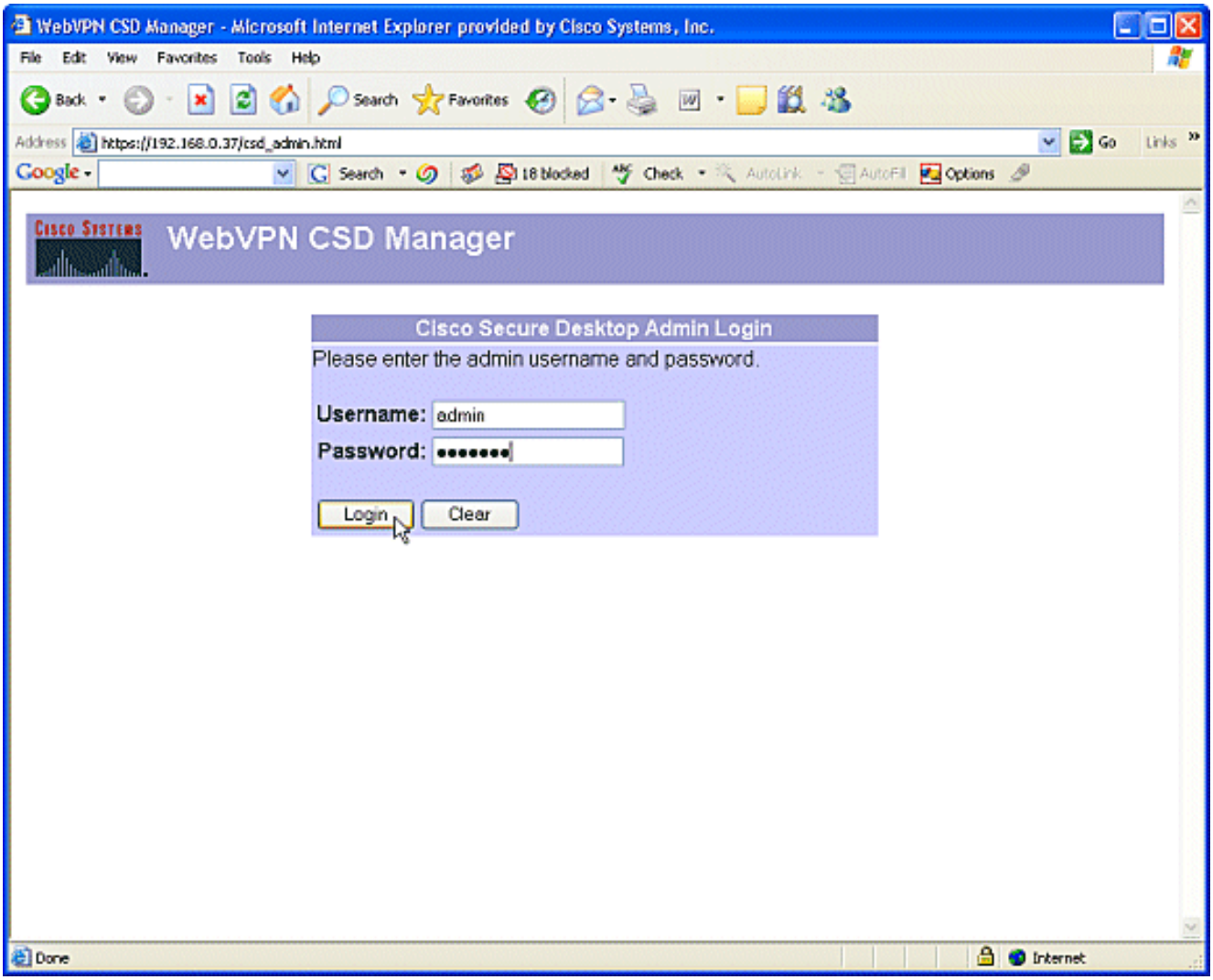
阶段 II：使用 Web 浏览器配置 CSD。

使用以下步骤在您的 Web 浏览器上完成 CSD 配置。

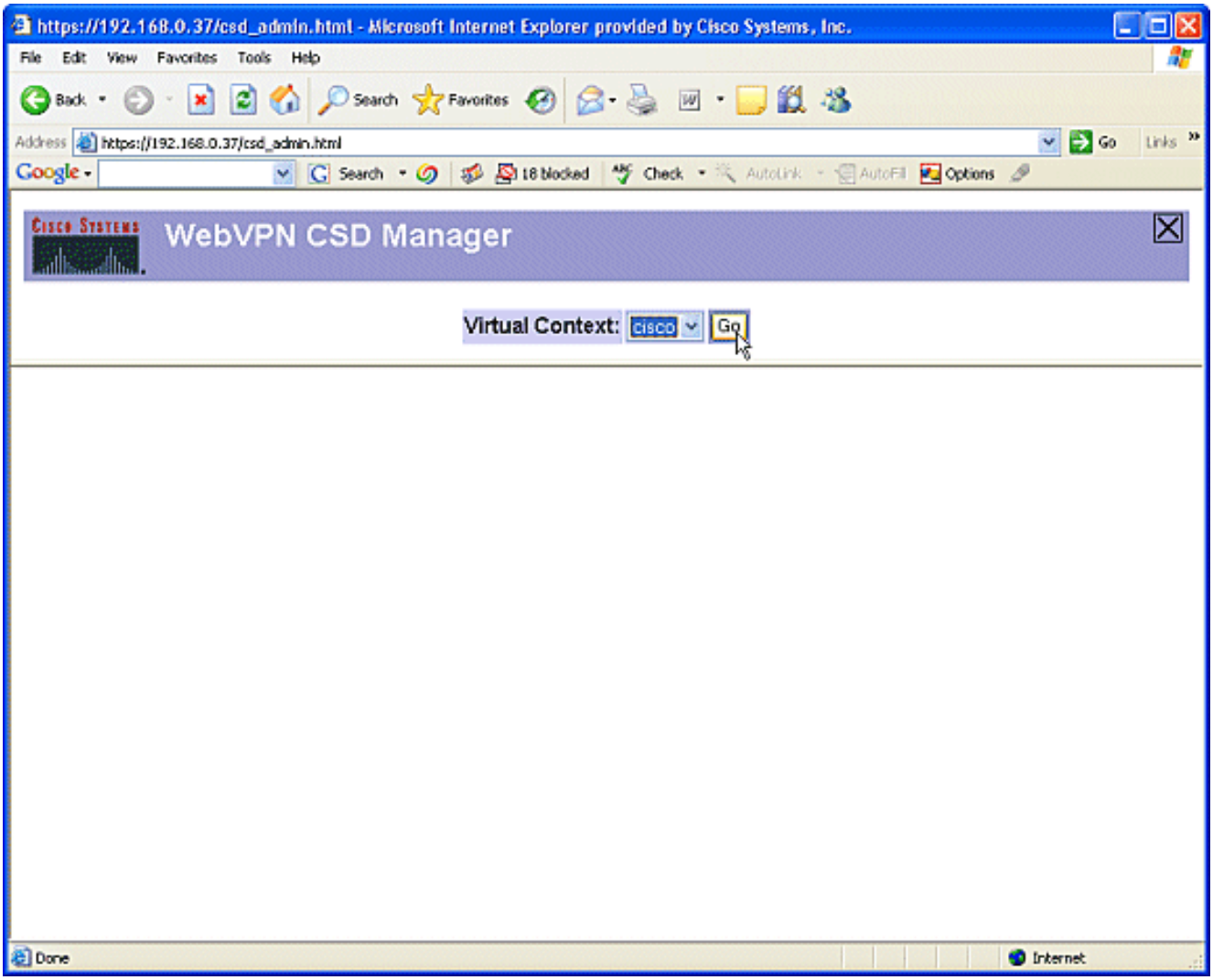
阶段 II：步骤 1：定义 Windows 位置。

定义 Windows 位置。

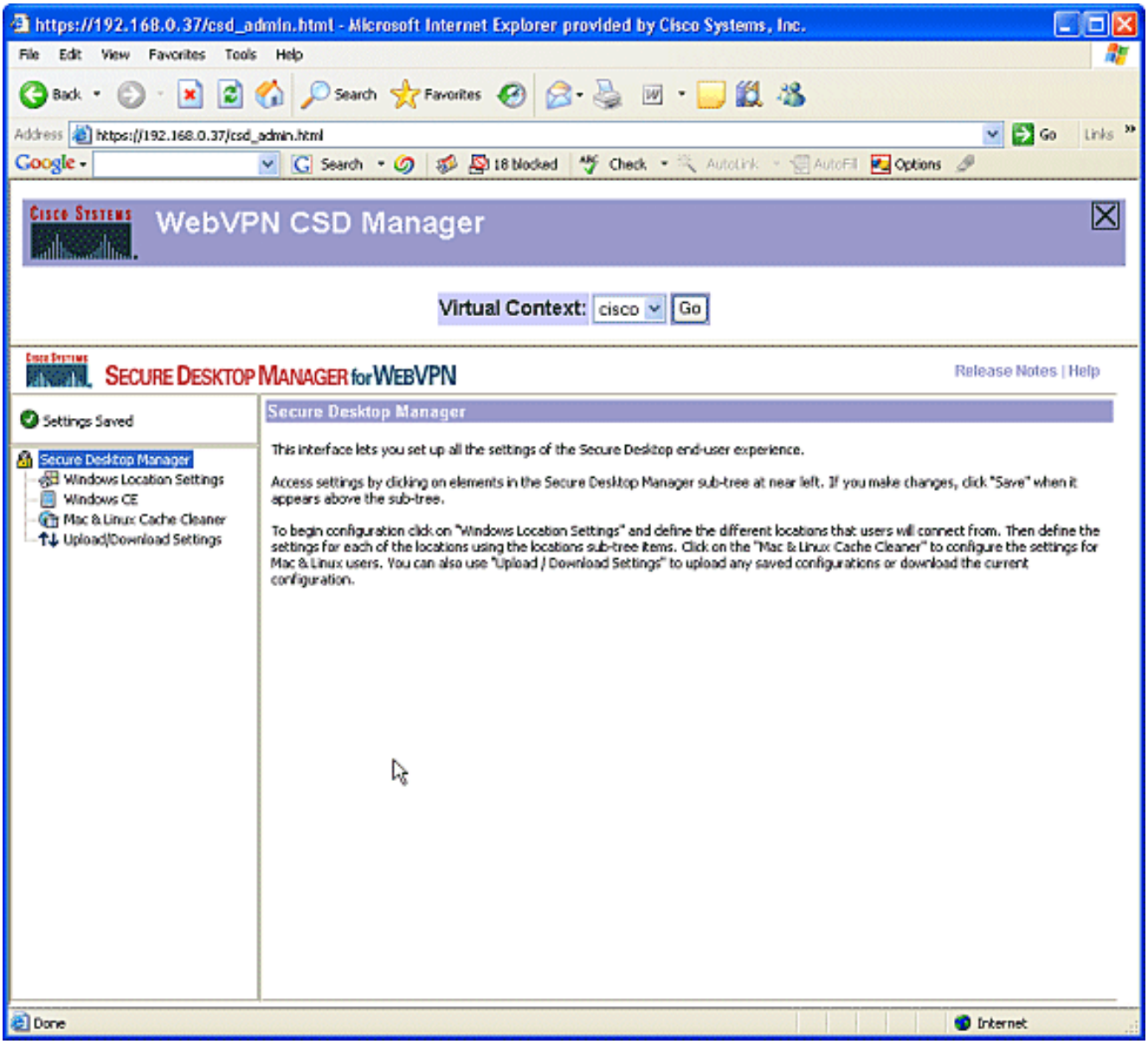
1. 在您的 Web 浏览器中打开 **https://WebVPNgateway_IP Address/csd_admin.html**，例如 https:/192.168.0.37/csd_admin.html。
2. 输入用户名 **admin**。输入口令，这是路由器的启用加密口令。单击 **Login**。



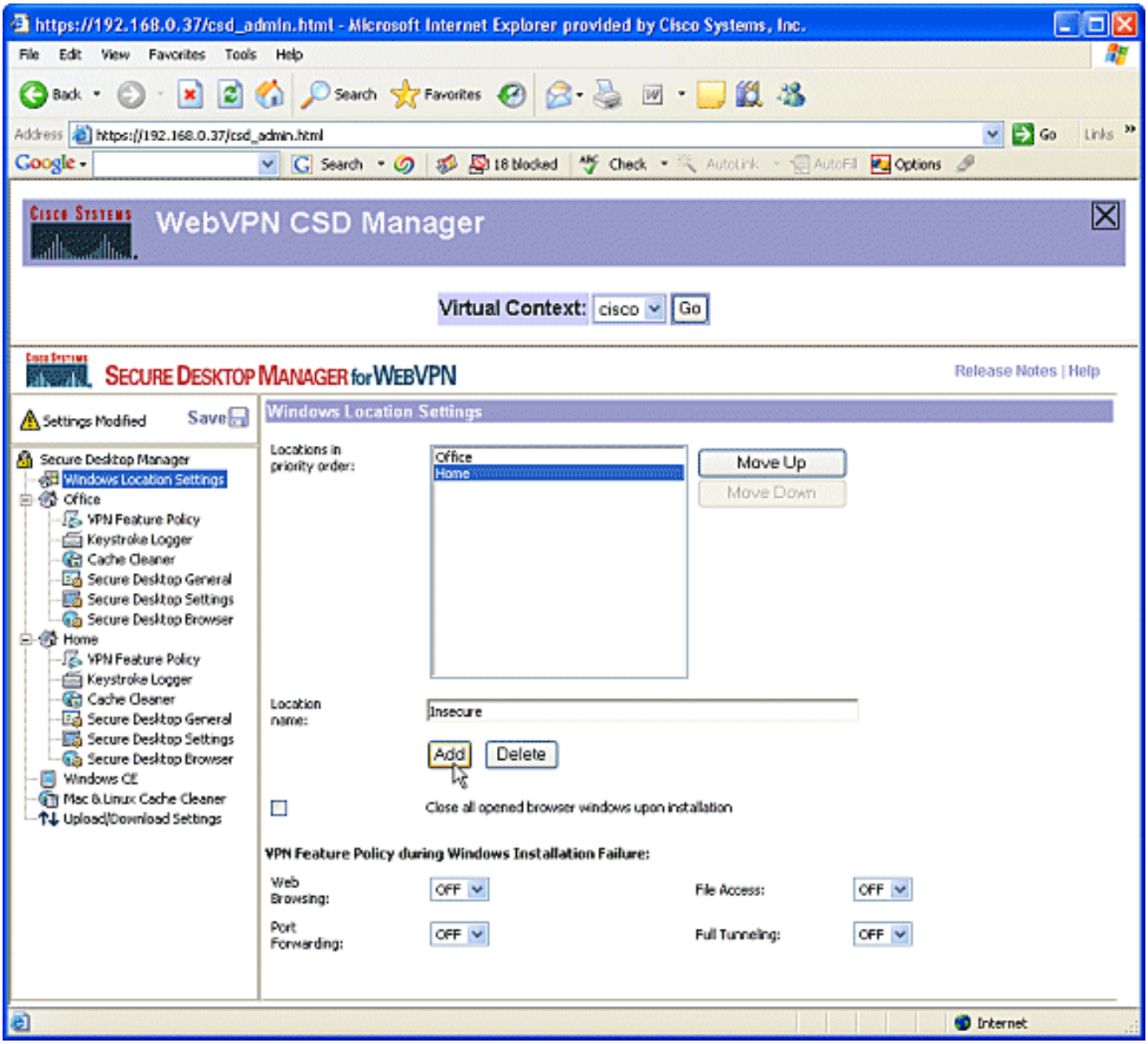
3. 接受路由器提供的证书，从下拉框中选择上下文并单击 **Go**。



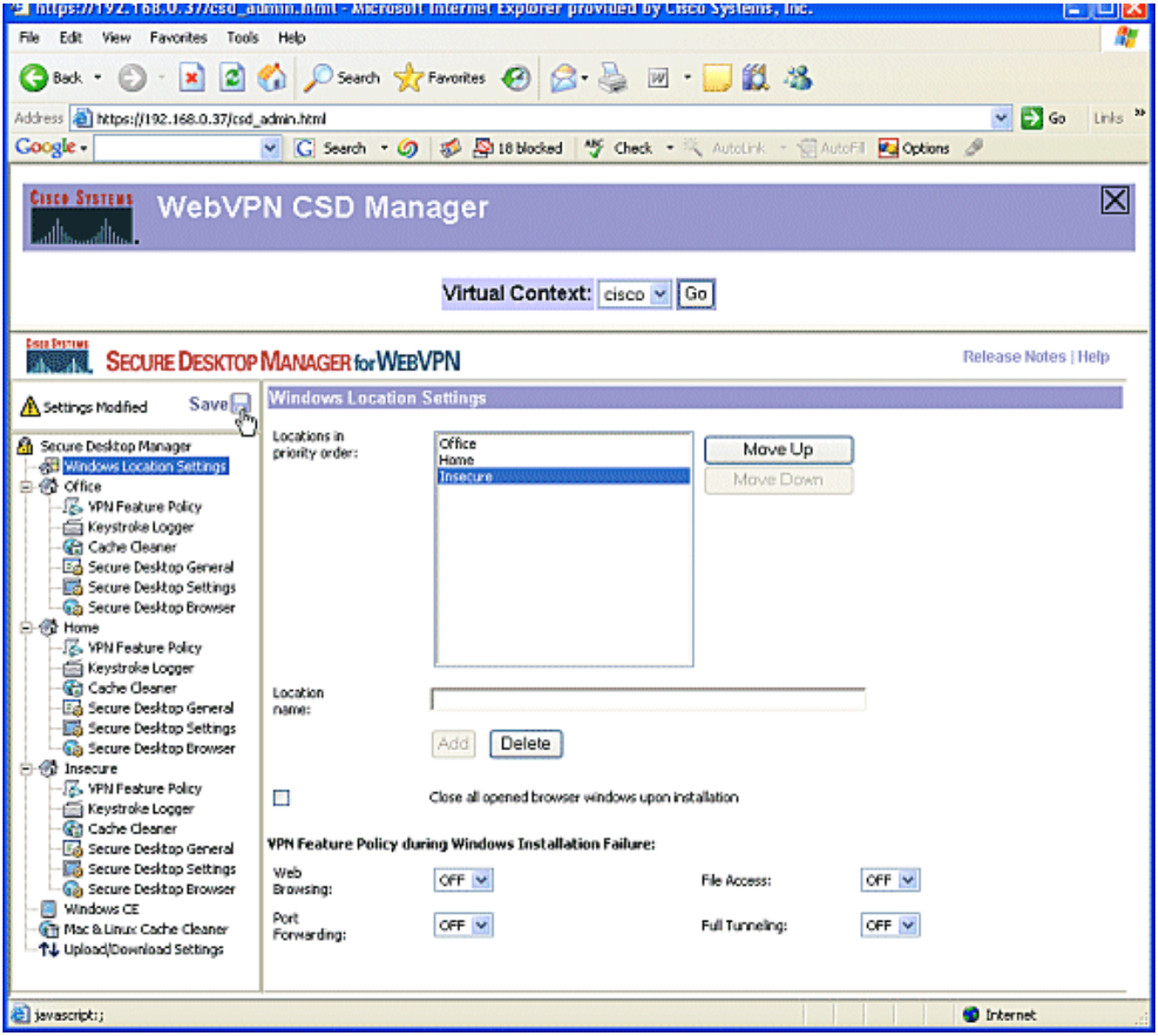
4. 这将打开 Secure Desktop Manager for WebVPN。



5. 在左侧窗格中，选择 **Windows Location Settings**。将光标放在“Location name”旁边的框中并输入位置名称。单击 **Add**。本示例显示了三个位置名称：“Office”、“Home”和“Insecure”。每次添加新位置时，左侧导航窗格将随该位置的可配置参数扩展。



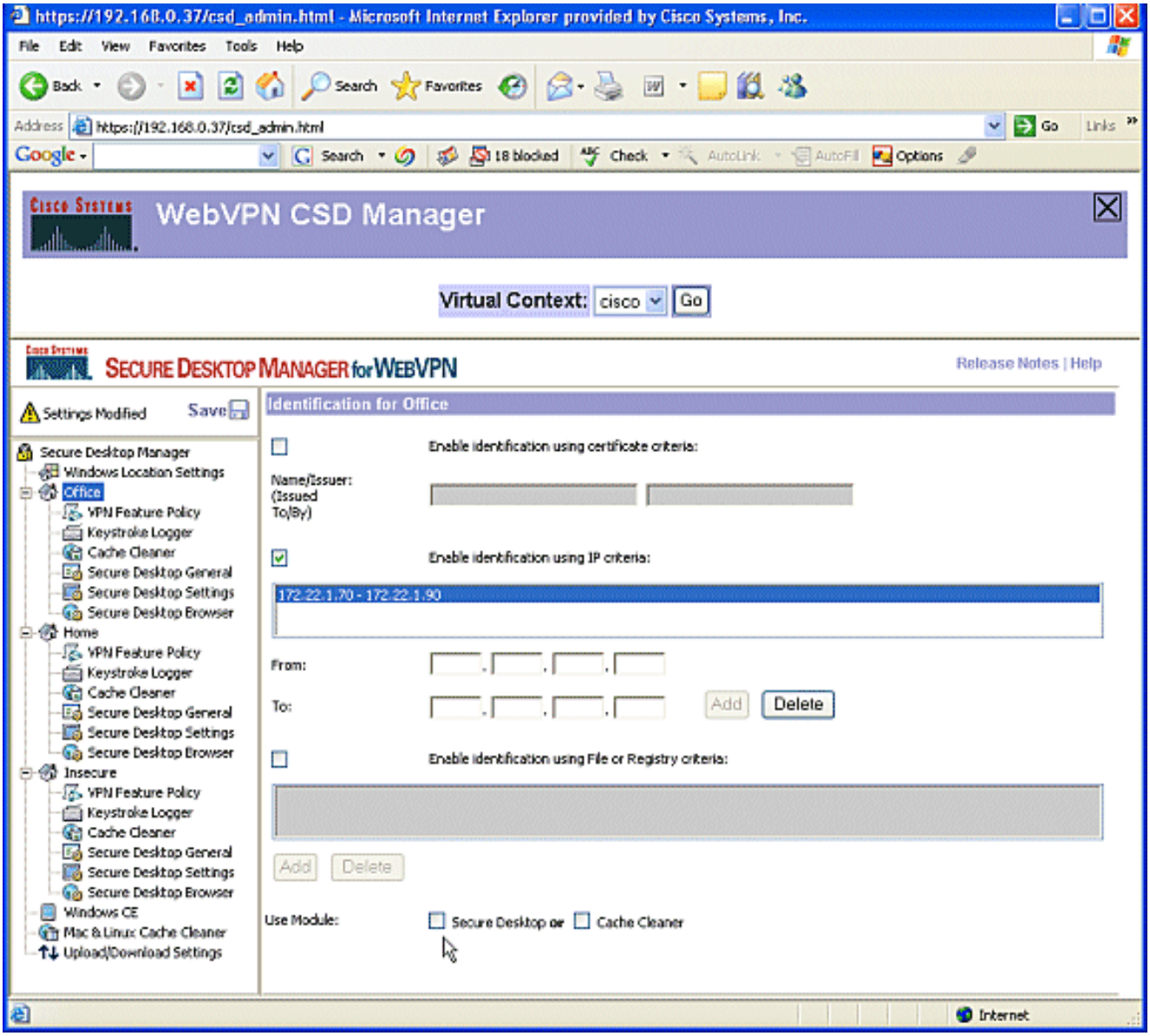
6. 创建 Windows 位置后，单击左侧窗格顶部的 **Save。注意：** 请经常保存您的配置，因为一旦断开与 Web 浏览器的连接，设置就将丢失。



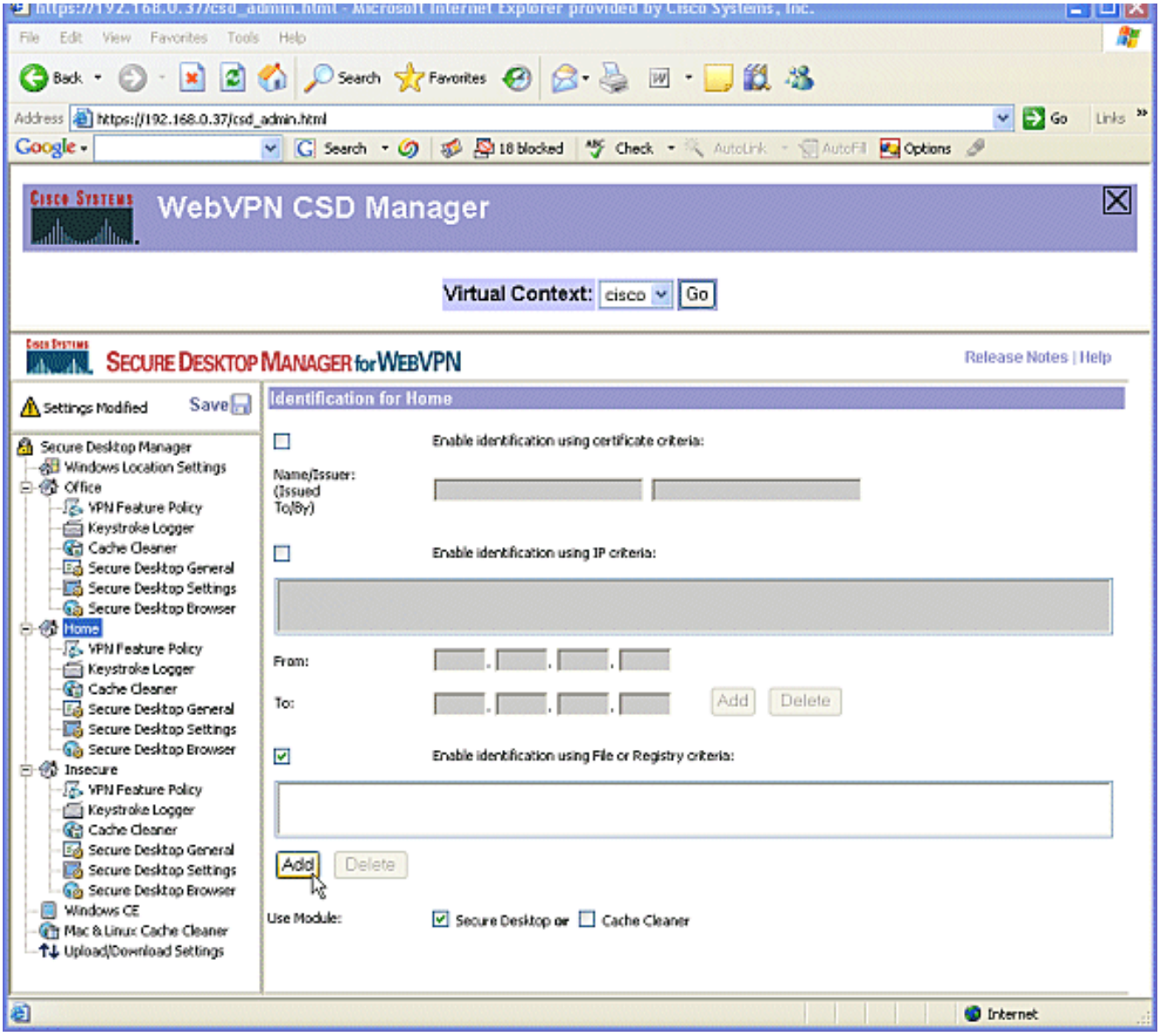
阶段 II：步骤 2：标识位置条件

为彼此区分各个 Windows 位置，需要为每个位置分配特定条件。这使得 CSD 能够确定要为特定 Windows 位置应用哪些功能。

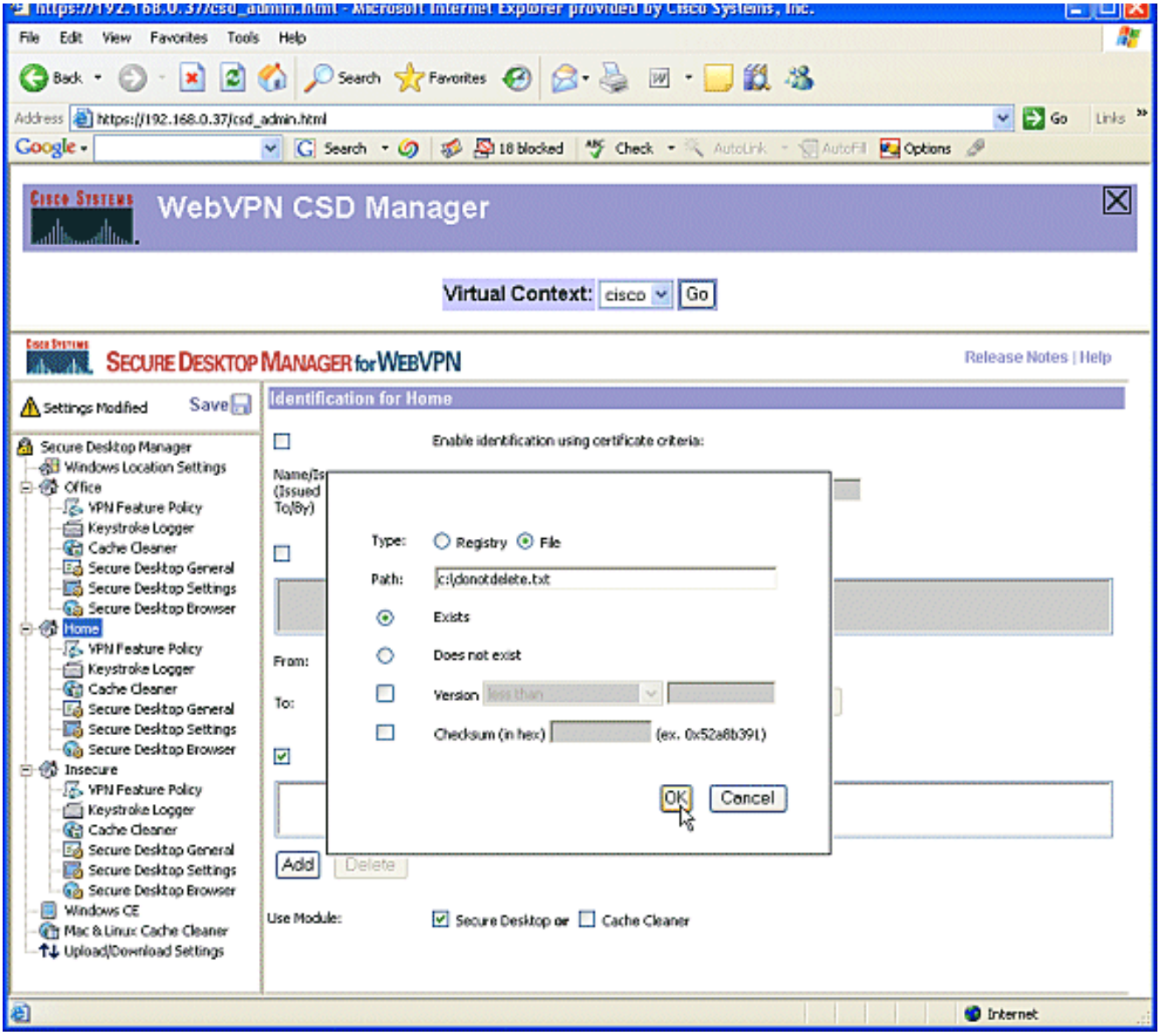
1. 在左侧窗格中，单击 **Office**。您可以使用证书条件、IP 条件、文件或注册表条件标识 Windows 位置。还可以为这些客户端选择 Secure Desktop 或 Cache Cleaner。由于这些用户是内部办公室员工，因此使用 IP 条件标识他们。在 **From 和“To”框中输入 IP 地址范围。**单击 **Add**。取消选中 **Use Module:Secure Desktop**。出现提示后，单击 **Save**，再单击“OK”。



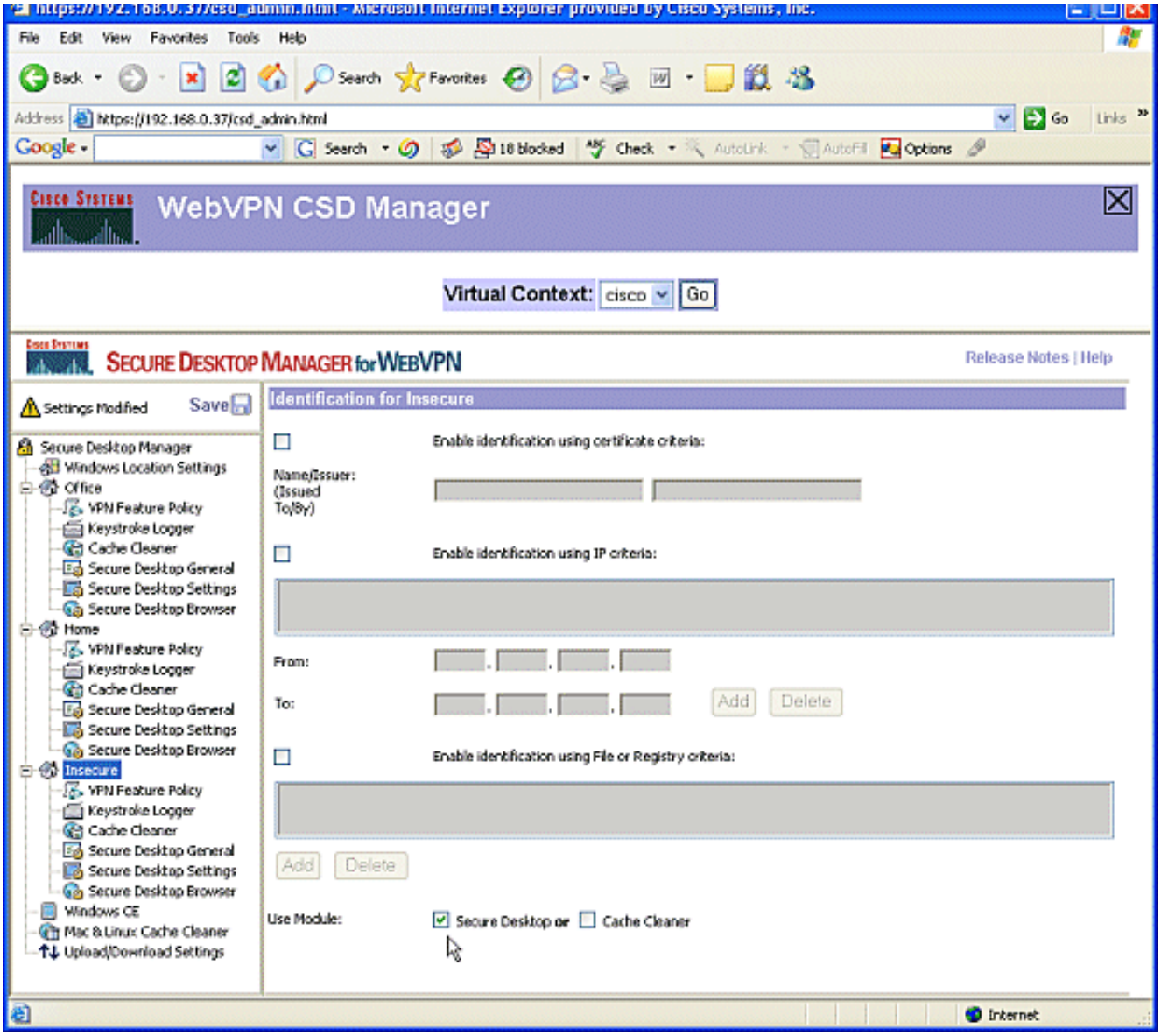
2. 在左侧窗格中，单击第二个“Windows Location Setting”**Home**。确保选中 **Use Module:Secure Desktop**。这将发布一个标识这些客户端的文件。您可以选择为这些用户分发证书和/或注册表条件。选中 **Enable identification using File or Registry criteria**。单击 **Add**。



3. 在该对话框中，选择 **File** 并输入文件的路径。该文件必须分发给所有“home”客户端。选中单选按钮 **Exists**。出现提示后，单击 **OK**，再单击“Save”。



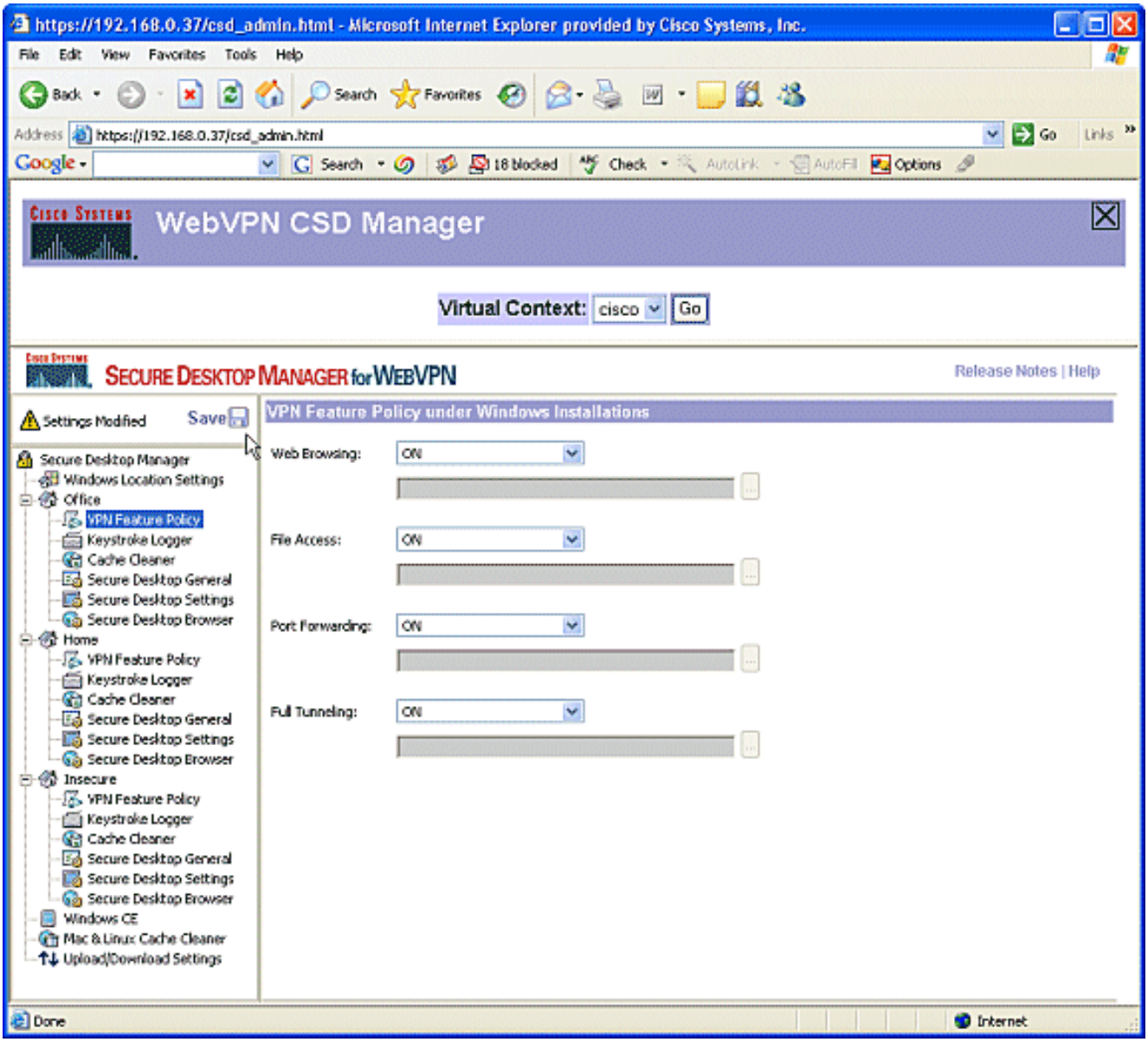
4. 要配置 Insecure 位置的标识，只需不应用任何识别条件。在左侧窗格中，单击 Insecure。取消选中所有条件。选中 Use Module:Secure Desktop。出现提示后，单击 Save，再单击“OK”。



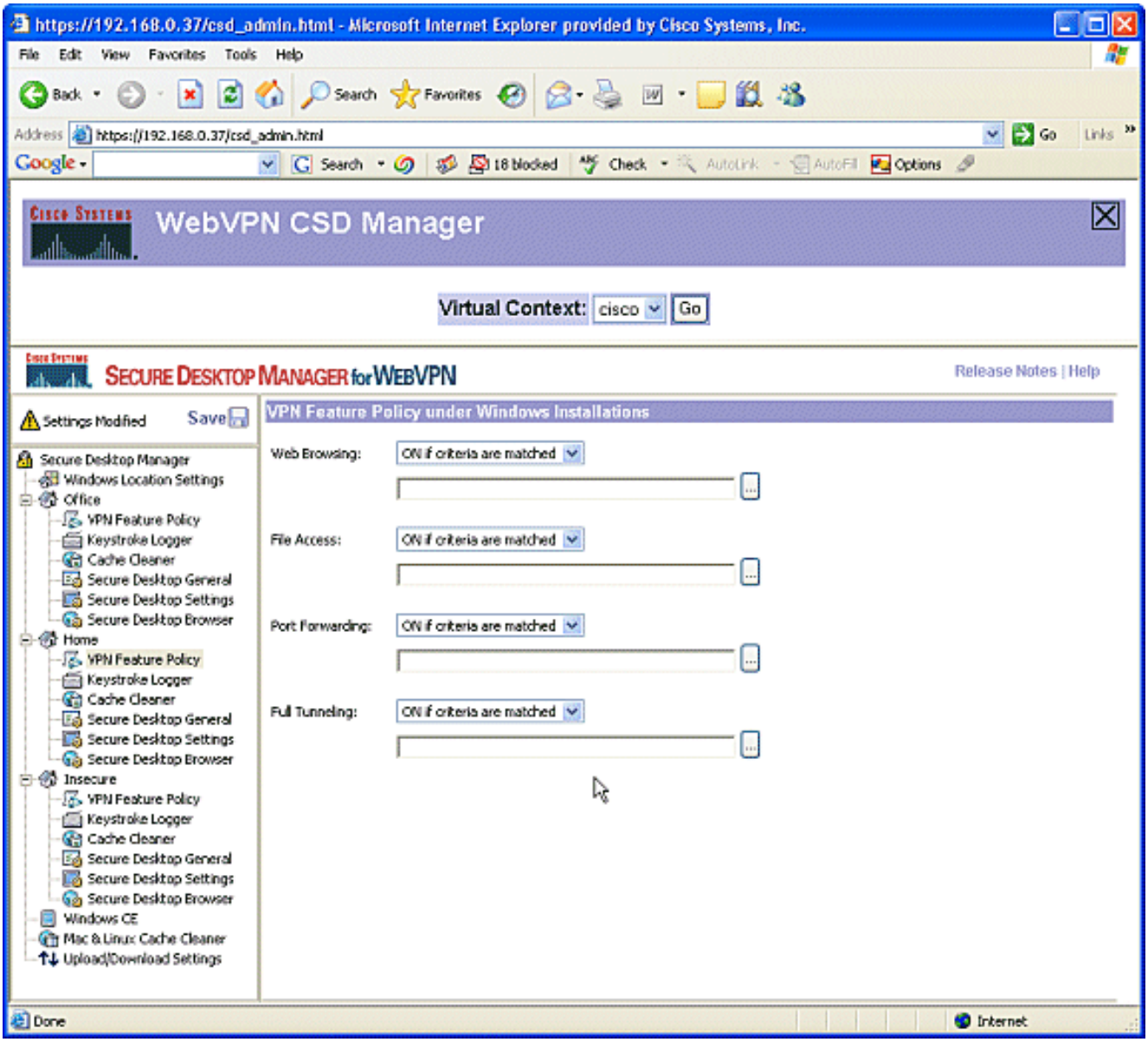
阶段 II：步骤 3：配置 Windows 位置模块和功能。

为每个 Windows 位置配置 CSD 功能。

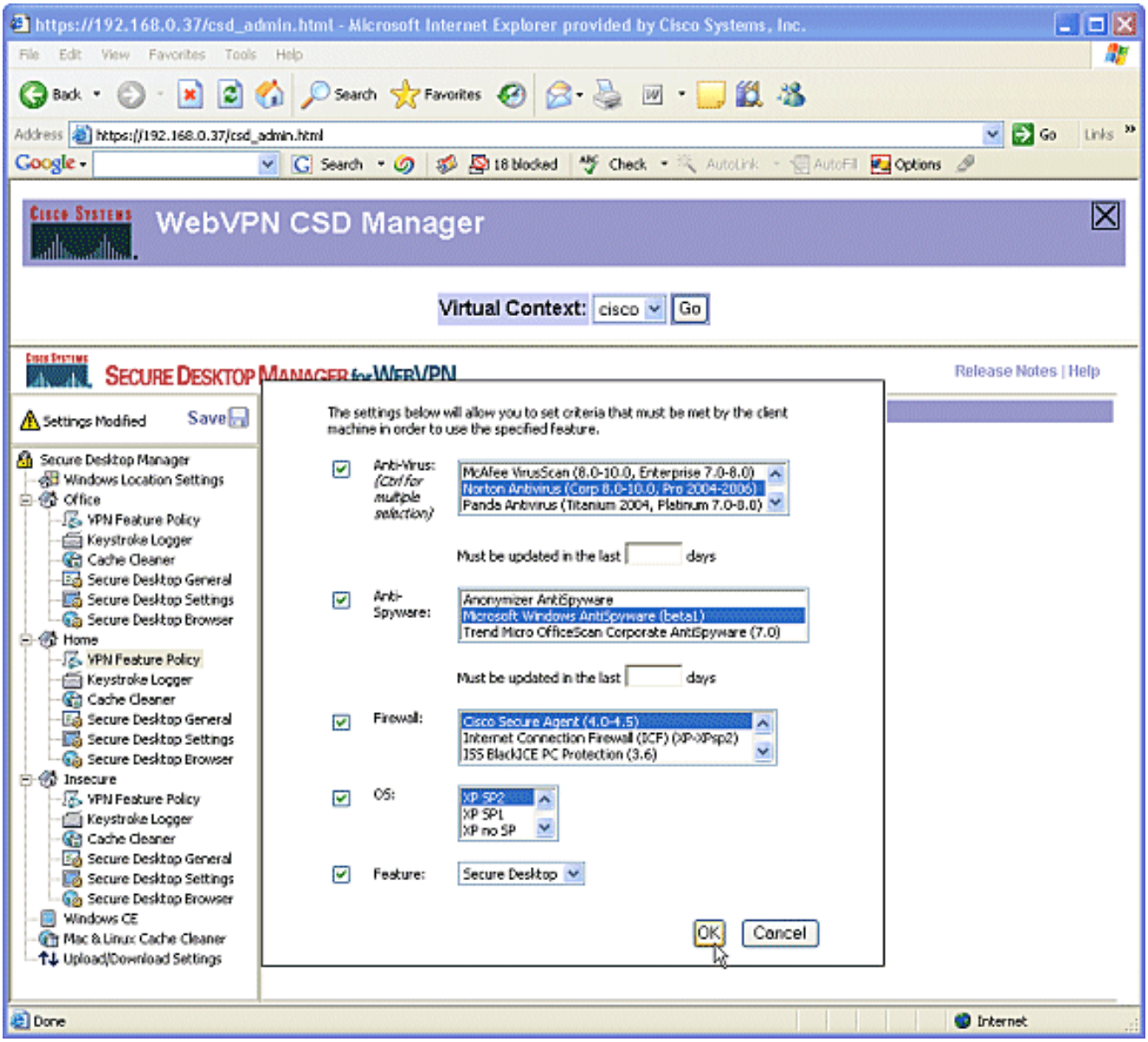
1. 在 **Office** 下，单击“VPN Feature Policy”。由于这些是受信任的内部客户端，因此既未启用 CSD，也未启用 Cache Cleaner。其他参数均不可用。



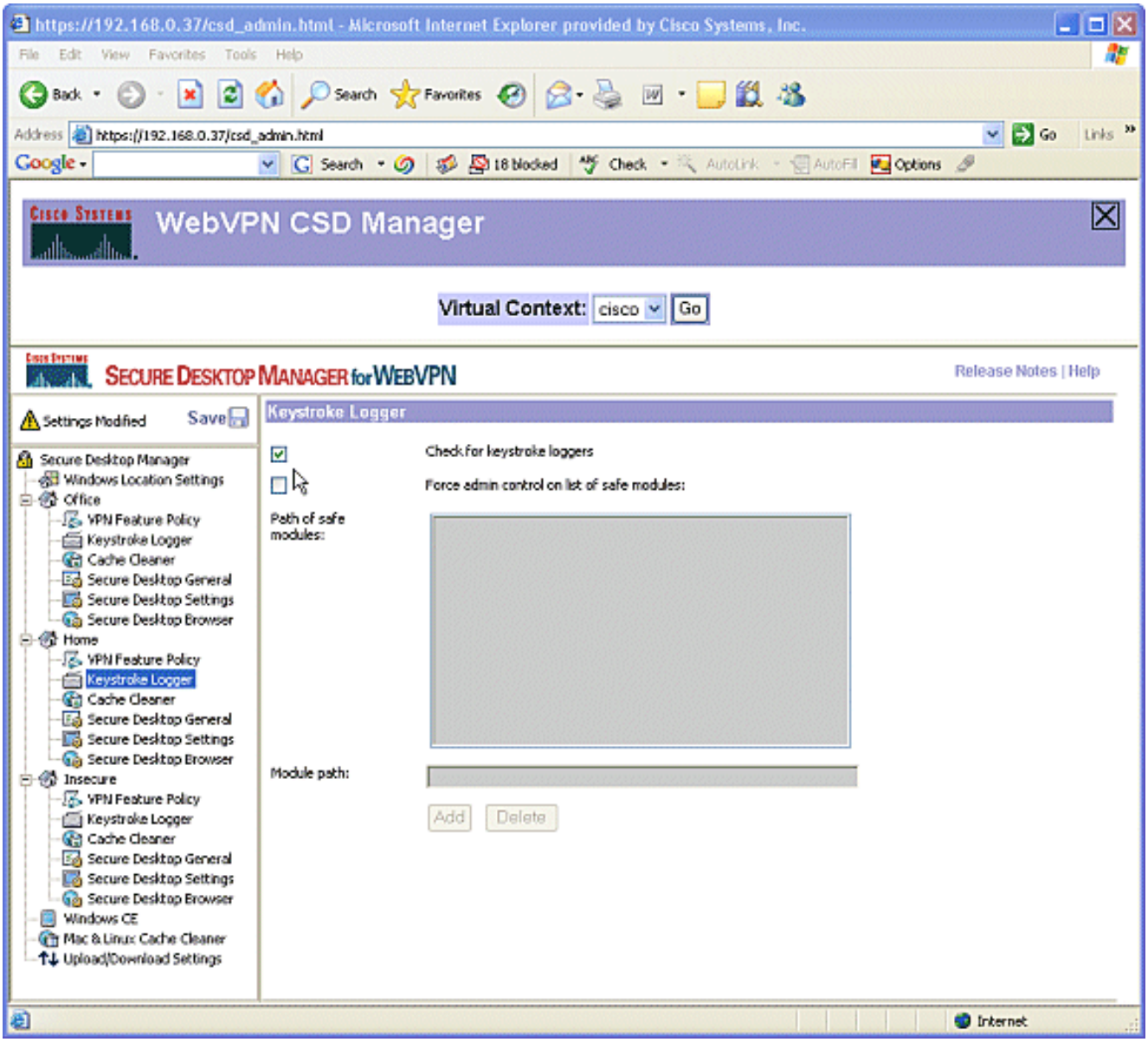
2. 如下所示启用相应功能。在左侧窗格中，在“Home”下选择 **VPN Feature Policy**。如果客户端满足特定条件，则允许“Home”用户访问公司 LAN。在每种访问方法之下，选择 **ON if criteria are matched**。



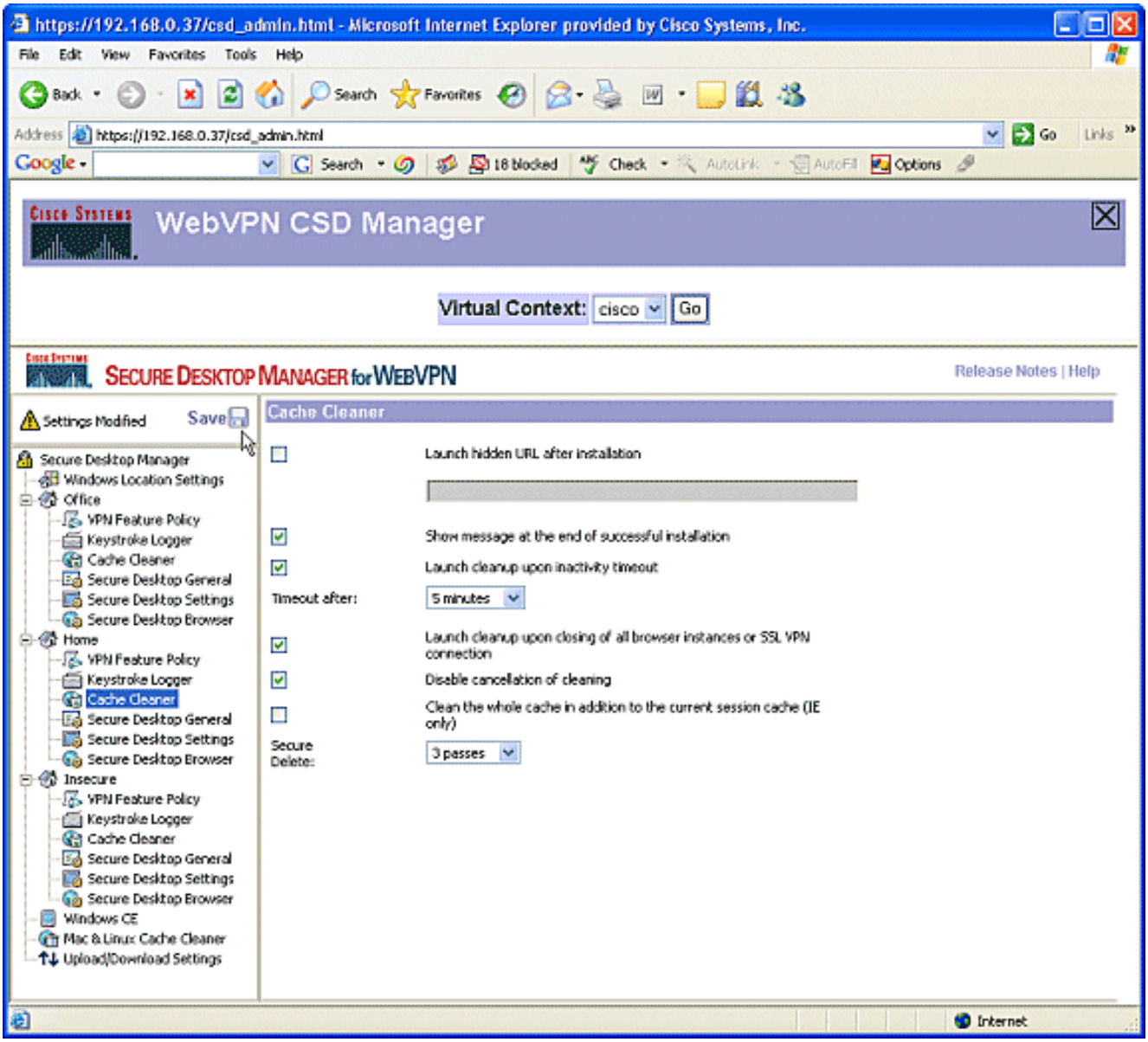
3. 对于“Web Browsing”，单击省略号按钮并选择必须匹配的条件。在对话框中单击 **OK**。



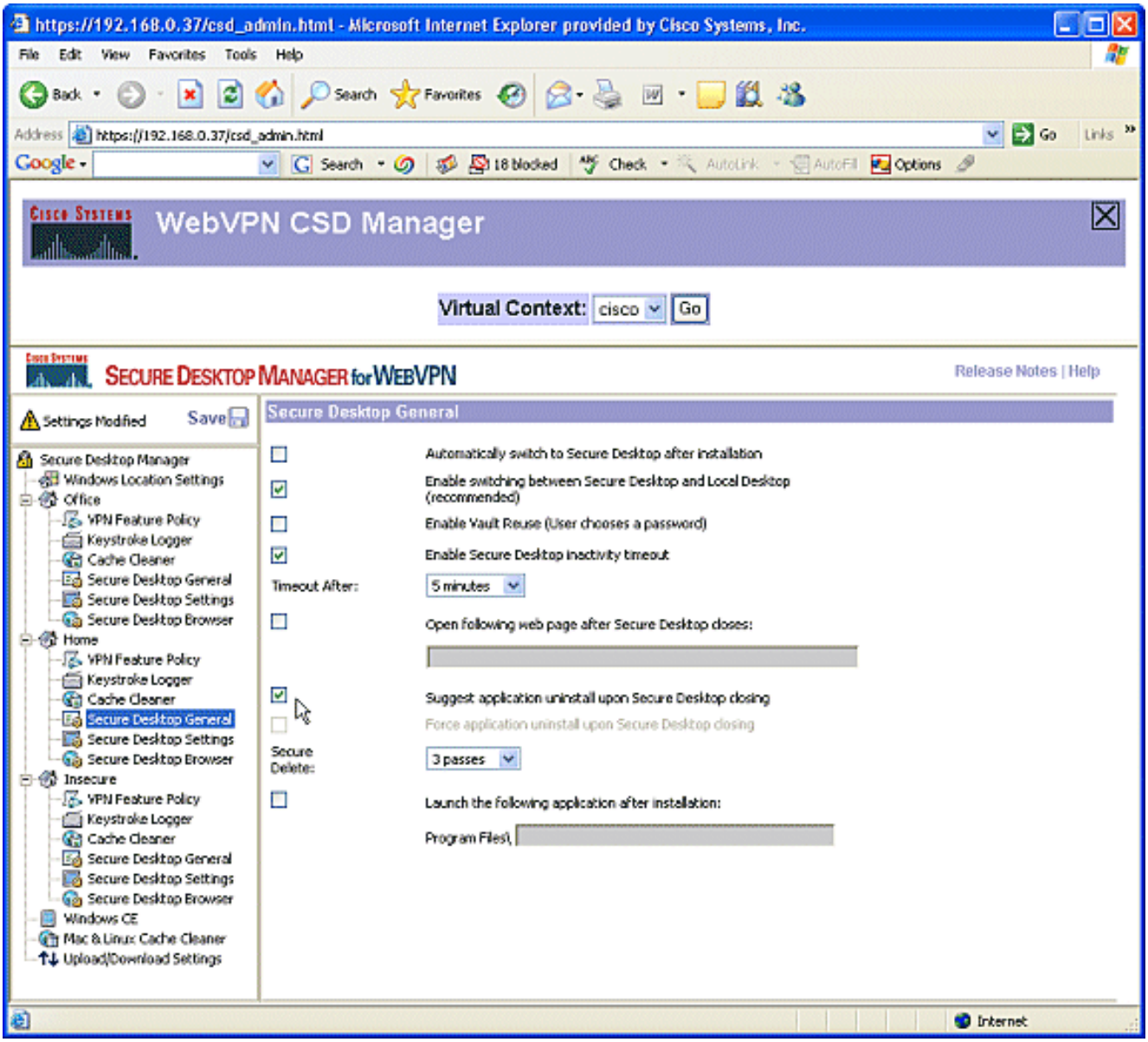
4. 您可以通过类似方式配置其他访问方法。在 **Home** 下，选择“Keystroke Logger”。选中 **Check for keystroke loggers** 旁边的复选框。出现提示后，单击 **Save**，再单击“OK”。



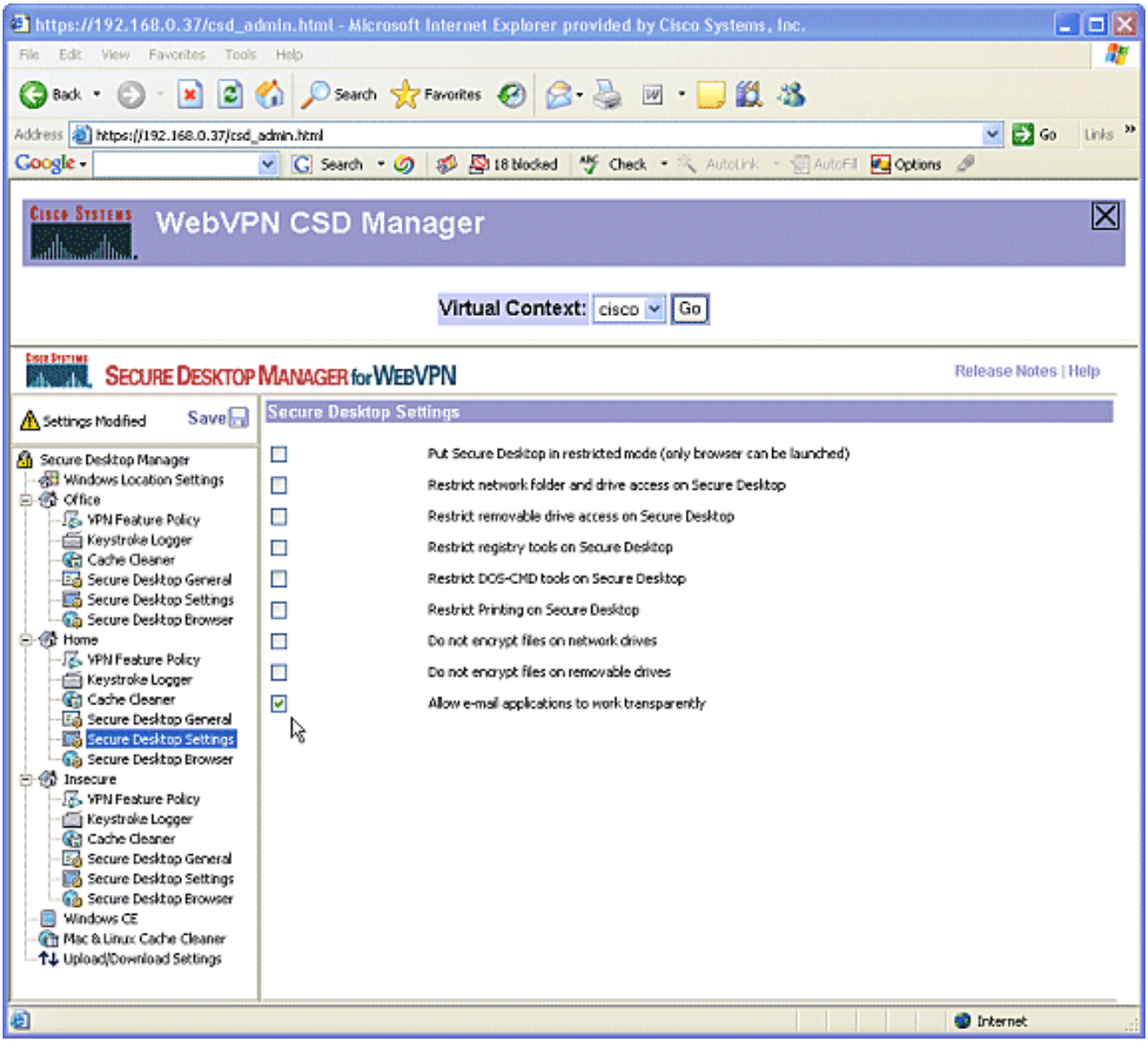
5. 在“Home”Windows 位置下，选择 **Cache Cleaner**。保留默认设置，如屏幕快照中所示。



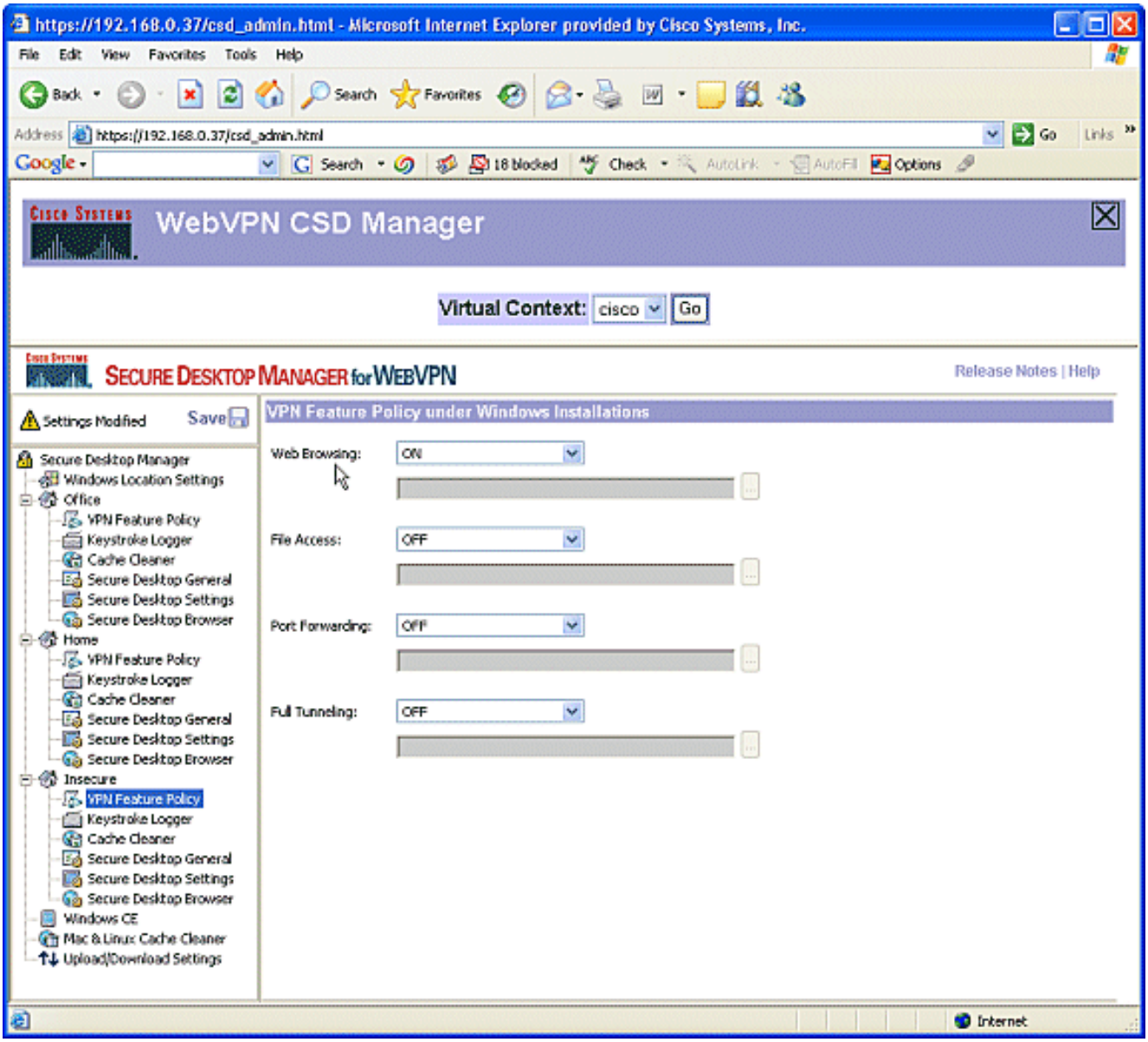
6. 在“Home”下，选择 **Secure Desktop General**。选中 **Suggest application uninstall upon Secure Desktop closing**。保留所有其他参数的默认设置，如屏幕快照中所示。



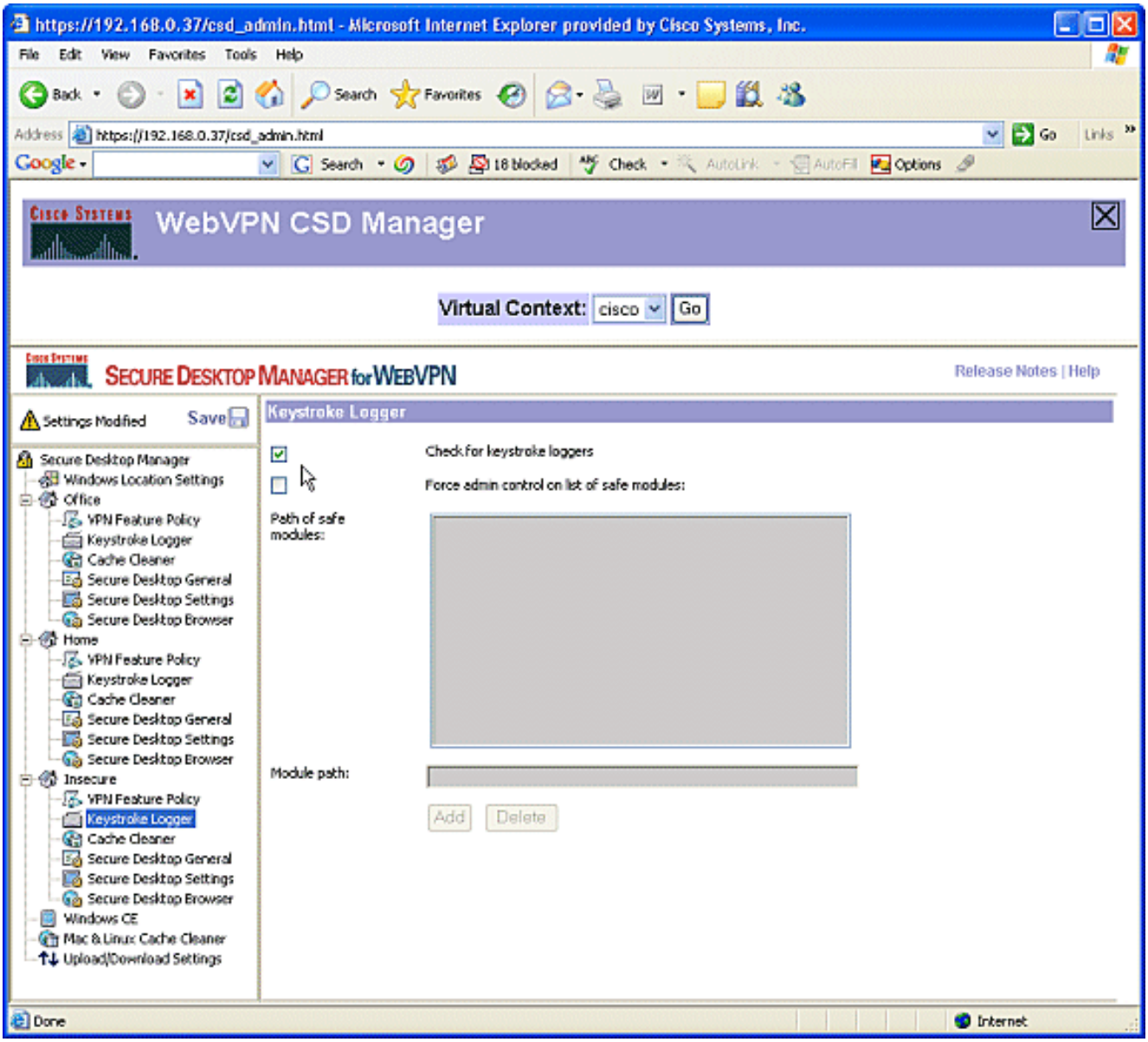
7. 对于“Home”下的“Secure Desktop Settings”，选择 **Allow e-mail applications to work transparently**。出现提示后，单击 **Save**，再单击“OK”。



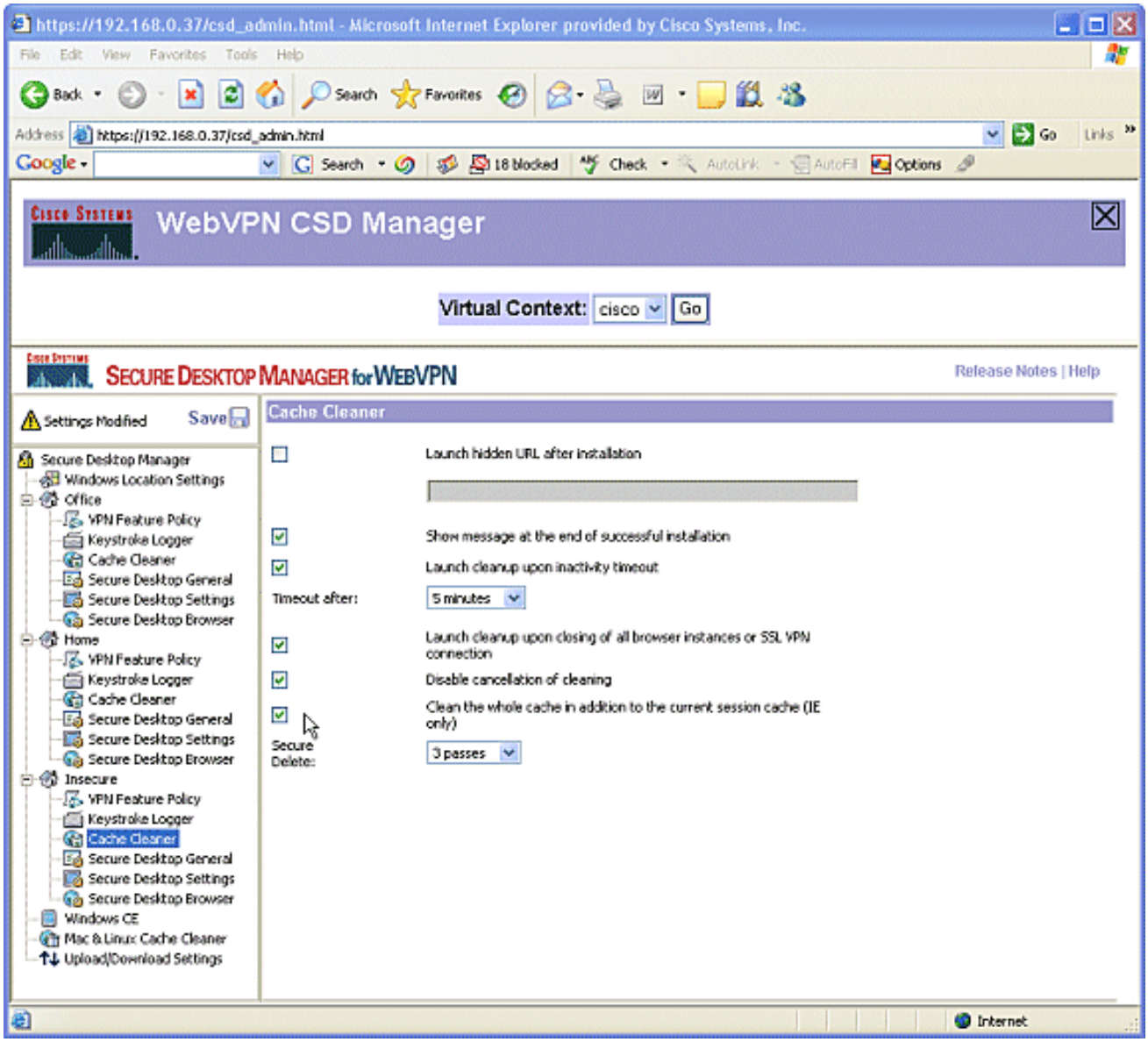
8. **Secure Desktop Browser** 的配置取决于您是否希望这些用户访问具有预配置的收藏夹的公司网站。在“Insecure”下，选择 **VPN Feature Policy**。由于这些不是受信任的用户，因此只允许进行 Web 浏览。从“Web Browsing”的下拉菜单中选择 **ON**。所有其他访问均设置为 **OFF**。



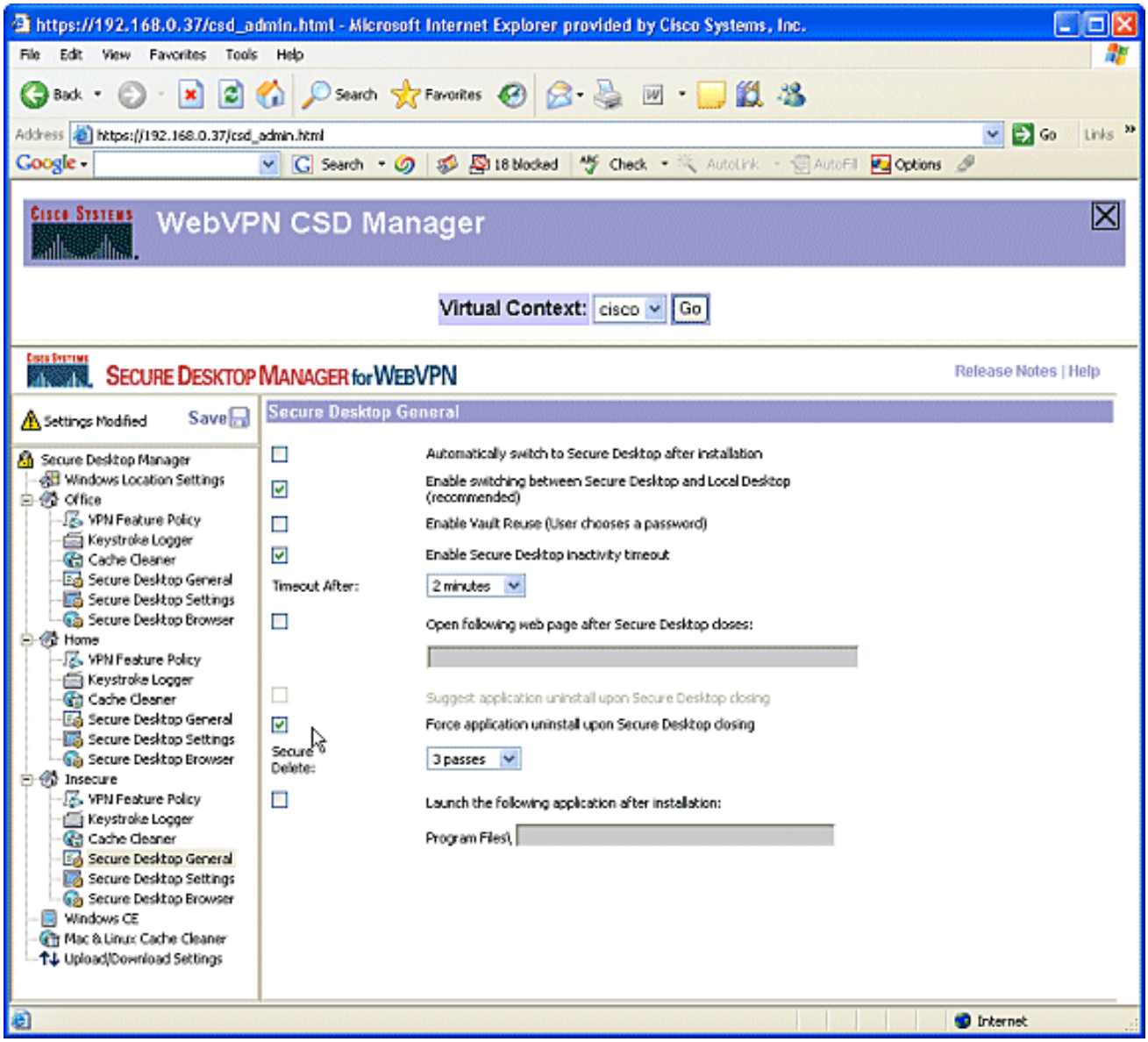
9. 选中 **Check for keystroke loggers 复选框。**



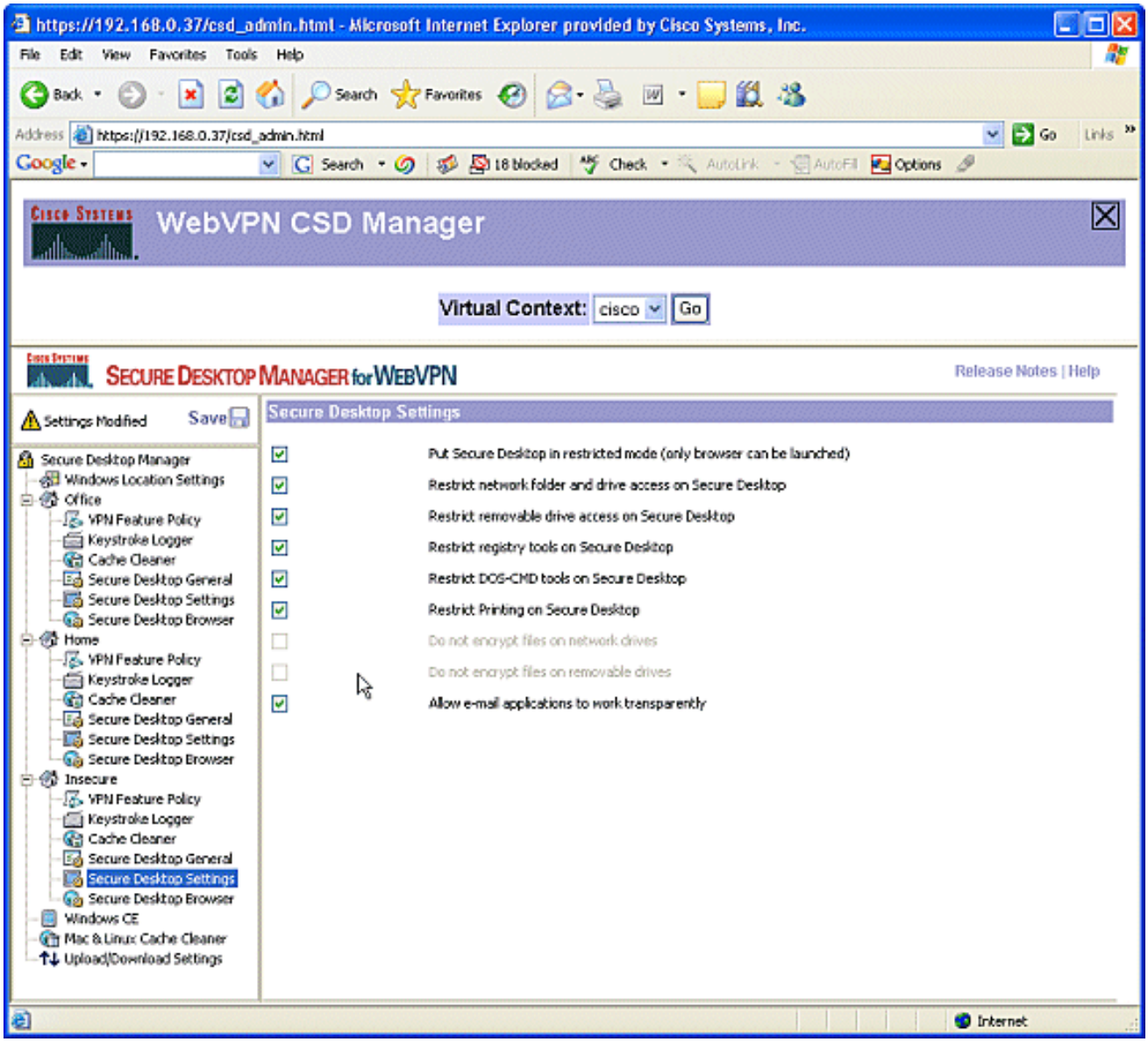
10. 为 Insecure 配置 Cache Cleaner。选中 **Clean the whole cache in addition to the current session cache (IE only) 复选框。**其他设置均保留默认值。



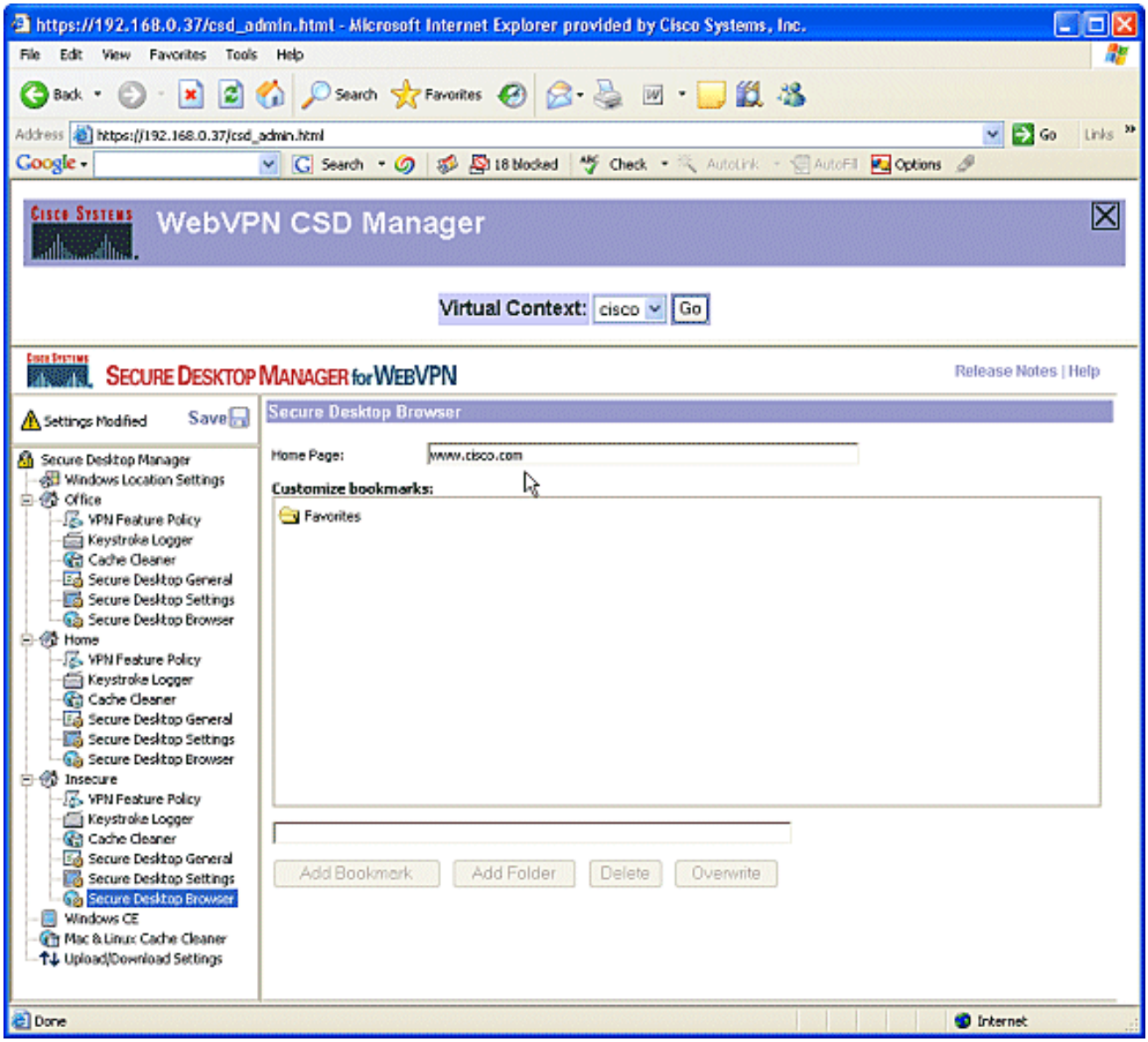
11. 在“Insecure”下，选择 **Secure Desktop General**。将处于非活动状态的超时值减少为 2 分钟。选中 **Force application uninstall upon Secure Desktop closing 复选框。**



12. 在“Insecure”下选择 **Secure Desktop Settings 并配置非常具有限制性的设置，如下所示。**



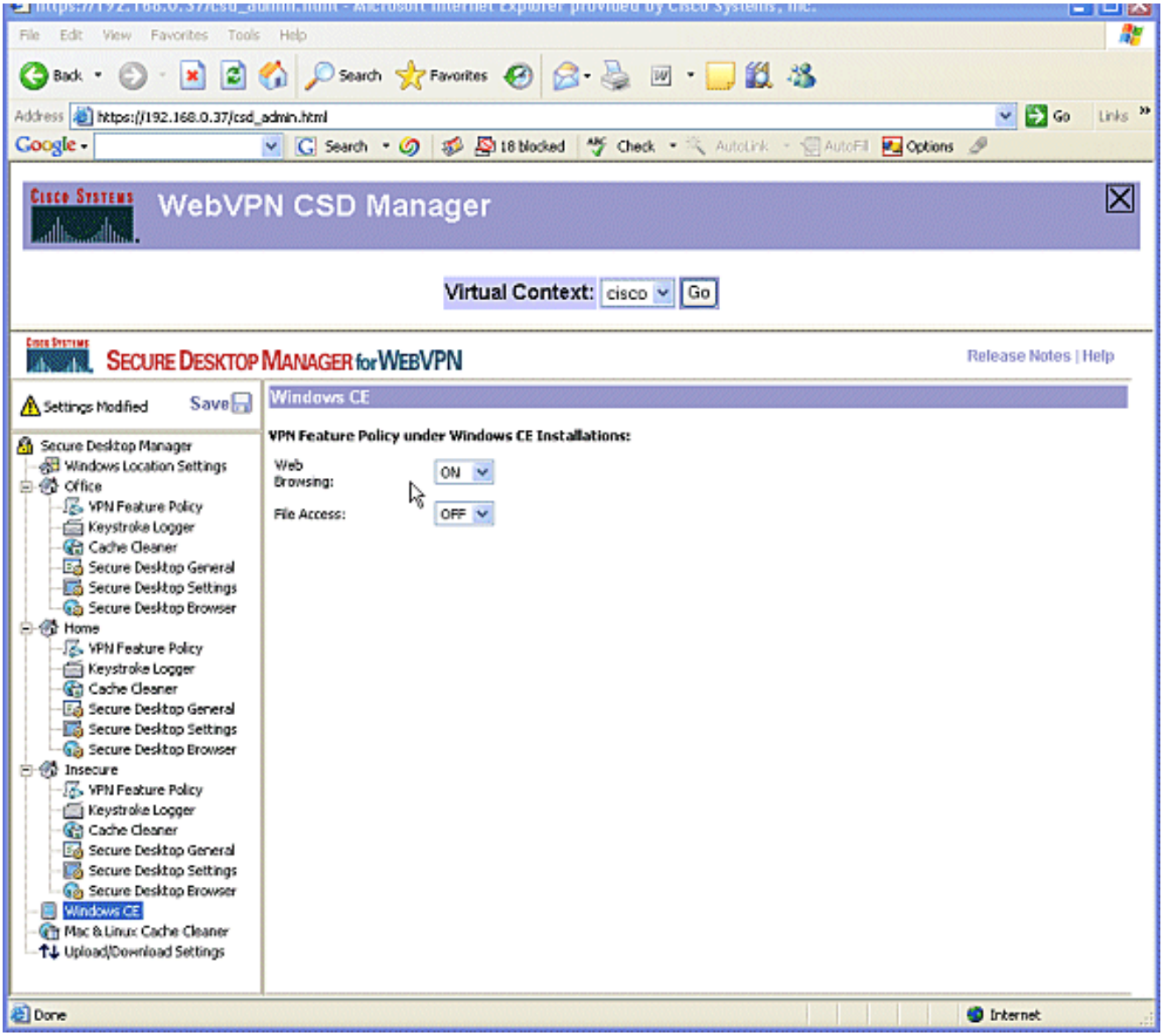
13. 选择 **Secure Desktop Browser**。在“Home Page”字段中，输入要将这些客户端导向的主页网站。



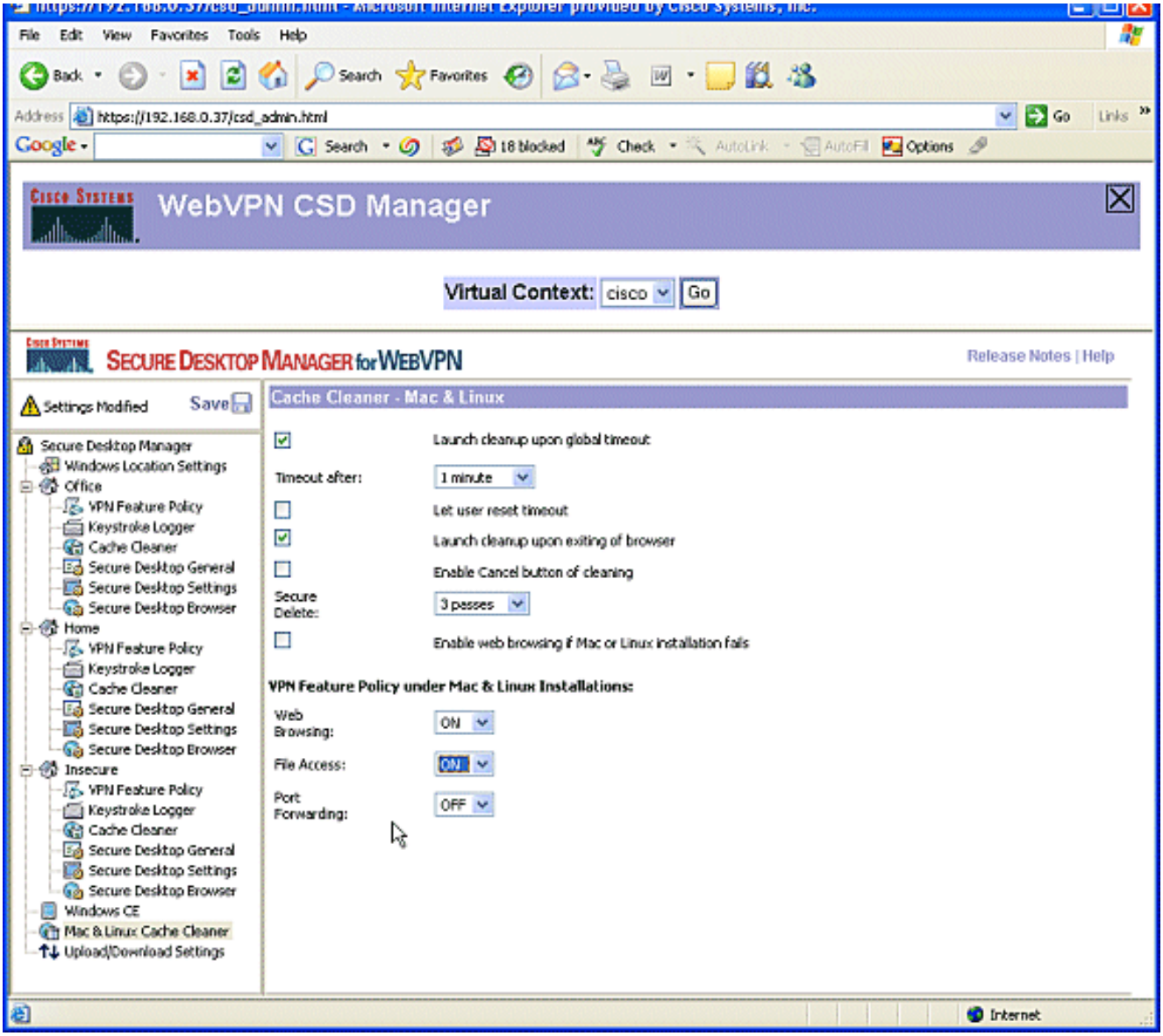
阶段 II：步骤 4：配置 Windows CE、Macintosh 和 Linux 功能。

为 Windows CE、Macintosh 和 Linux 配置 CSD 功能。

1. 在 Secure Desktop Manager 下选择 **Windows CE**。Windows CE 具有有限的 VPN 功能。将 **Web Browsing** 设置为“ON”。



2. 选择 **Mac & Linux Cache Cleaner**。Macintosh 和 Linux 操作系统只能访问 CSD 的 Cache Cleaner 功能。如图所示对其进行配置。出现提示后，单击 **Save**，再单击“OK”。

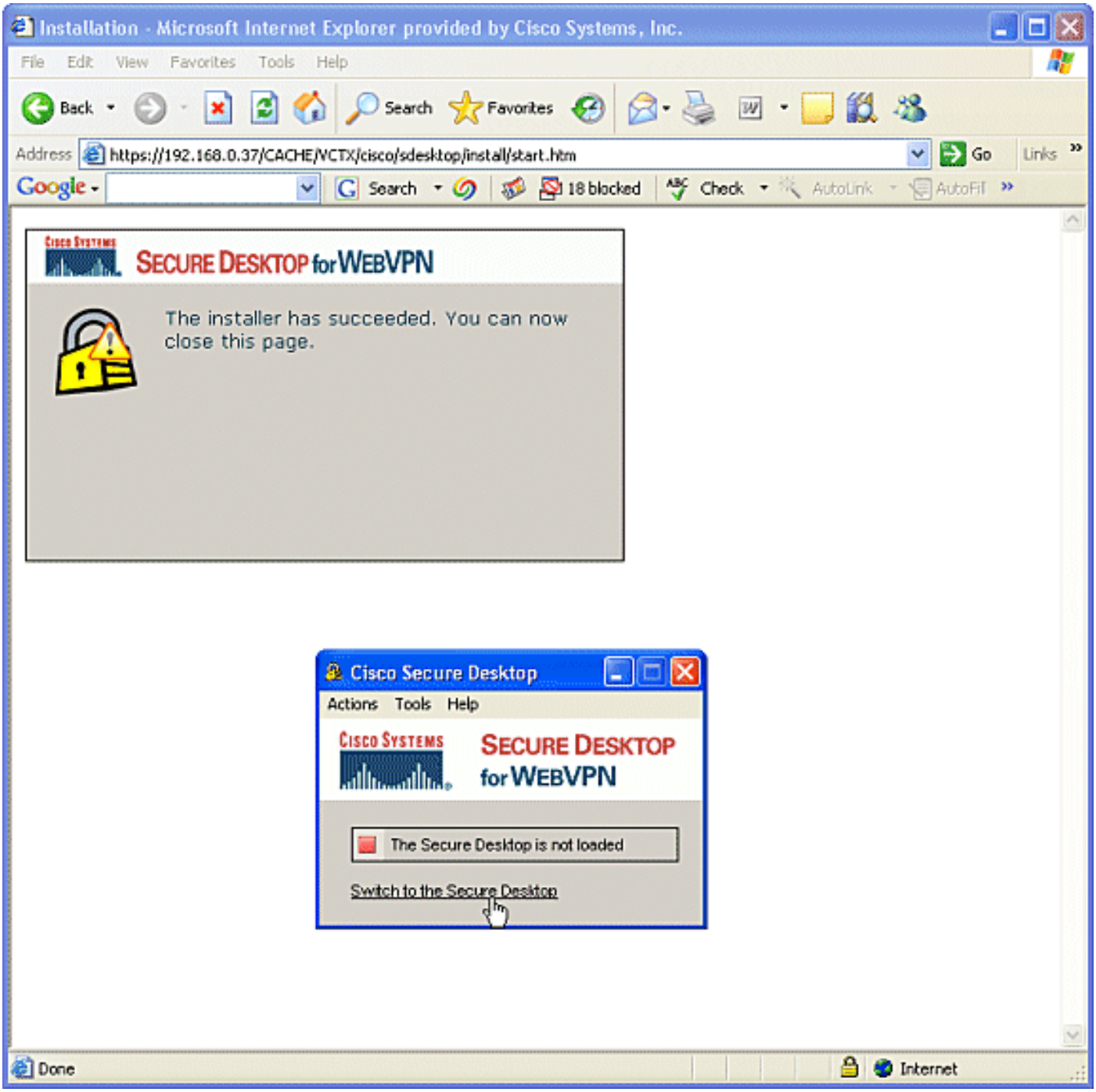


验证

测试 CSD 的运行情况

通过使用启用了 SSL 的浏览器在 **https://WebVPN_Gateway_IP Address** 连接到 WebVPN 网关来测试 CSD 的运行情况。

注意：如果创建了不同的WebVPN上下文，请记住使用该上下文的唯一**名称**。



命令

有若干 **show 命令与 WebVPN 关联。**可以在命令行界面 (CLI) 上执行这些命令以显示统计信息和其他信息。有关 **show 命令的详细信息，请参阅**验证 WebVPN 配置。

注意：CLI Analyzer(仅限注册客户)支持某些**show**命令。使用CLI Analyzer查看对show命令输**出的**分析。

故障排除

命令

有若干 **debug 命令与 WebVPN 关联。**有关这些命令的详细信息，请参阅使用 WebVPN Debug 命令。

注意：使用debug命令可能会对Cisco设备造成负面影响。使用 debug 命令之前，请参阅**有关 Debug 命令的重要信息**。

有关 **clear 命令的详细信息，请参阅**使用 WebVPN Clear 命令。

相关信息

- **WebVPN 和 DMVPN 融合部署指南**
- **SSL VPN - WebVPN**
- **Cisco IOS SSLVPN**
- **技术支持和文档 - Cisco Systems**