使用SDM在Cisco IOS上配置CSD

目錄

簡介

雖然安全套接字層(SSL)VPN（思科WebVPN）會話是安全的，但會話完成後，客戶端可能仍保留有cookie、瀏覽器檔案和電子郵件附件。Cisco Secure Desktop(CSD)通過將會話資料以加密格式寫入客戶端磁碟的特殊*vault*區域，擴展了SSL VPN會話的固有安全性。此外，此資料將在SSL VPN會話結束時從磁碟中刪除。本文檔提供在Cisco IOS® 路由器上配置CSD的示例。

以下思科裝置平台支援CSD:

- Cisco IOS路由器版本12.4(6)T及更高版本
- 思科870、1811、1841、2801、2811、2821、2851、3725、3745、3825、3845、7200和7301路由器
- Cisco VPN 3000系列集中器版本4.7及更高版本
- Cisco ASA 5500系列安全裝置版本7.1及更高版本
- 適用於Cisco Catalyst和Cisco 7600系列版本1.2及更高版本的Cisco WebVPN服務模組

必要條件

需求

嘗試此組態之前，請確保符合以下要求：

Cisco IOS路由器的要求

- 採用高級映像12.4(6T)或更高版本的Cisco IOS路由器
- Cisco Router Secure Device Manager(SDM)2.3或更高版本
- 管理工作站上的CSD for IOS軟體包的副本
- 路由器自簽名數位證書或證書頒發機構(CA)的身份驗證**注意：**任何時候使用數位證書時，請確保正確設定路由器的主機名、域名和日期/時間/時區。
- 路由器上的使能加密口令
- 您的路由器上啟用了DNS。有幾個WebVPN服務需要DNS才能正常工作。

客戶端電腦的要求

- 遠端客戶端應具有本地管理許可權；這不是必需的，但強烈建議這樣做。
- 遠端客戶端必須具有Java Runtime Environment(JRE)1.4版或更高版本。
- 遠端客戶端瀏覽器：Internet Explorer 6.0、Netscape 7.1、Mozilla 1.7、Safari 1.2.2或Firefox 1.0
- 在遠端客戶端上啟用Cookie和允許彈出視窗

採用元件

本文中的資訊係根據以下軟體和硬體版本：

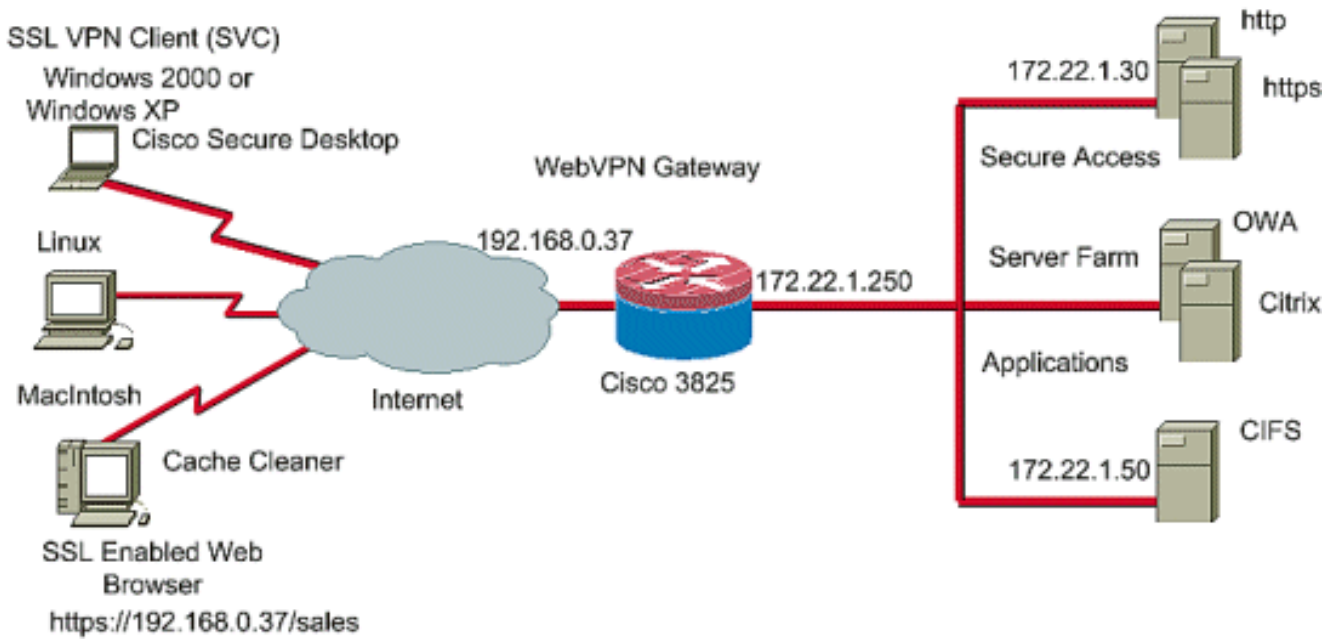
- 採用12.9(T)版的Cisco IOS路由器3825
- SDM 2.3.1版

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態開始。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。

網路圖表

本檔案會使用以下網路設定：

本示例使用Cisco 3825系列路由器來允許對公司內部網的安全訪問。Cisco 3825系列路由器通過可配置的CSD功能和特性增強SSL VPN連線的安全。客戶端可以通過以下三種SSL VPN方法之一連線到啟用CSD的路由器：無客戶端SSL VPN(WebVPN)、瘦客戶端SSL VPN（埠轉發）或SSL VPN客戶端（全通道SVC）。



相關產品

此配置還可以用於以下硬體和軟體版本：

- 思科路由器平台870、1811、1841、2801、2811、2821、2851、3725、3745.3825、3845、7200和7301
- Cisco IOS進階安全映像版本12.4(6)T及更新版本

慣例

請參閱思科技術提示慣例以瞭解更多有關檔案慣例的資訊。

設定

WebVPN網關允許使用者通過其中一個SSL VPN技術連線到路由器。裝置上每個IP地址只允許有一個WebVPN網關，但可以將WebVPN網關連線多個WebVPN上下文。每個上下文都由唯一的名稱標識。組策略標識可用於特定WebVPN上下文的配置資源。

IOS路由器上的CSD配置分兩個階段完成：

階段I:使用SDM為CSD配置準備路由器

1. **配置WebVPN網關、WebVPN上下文和組策略。注意：**此步驟是可選步驟，本文檔沒有詳細介紹。如果您已為路由器配置了其中一個SSL VPN技術，請忽略此步驟。
2. **在WebVPN上下文中啟用CSD。**

第二階段：使用Web瀏覽器配置CSD。

1. 定義*Windows位置。*
2. **確定位置條件。**
3. **配置Windows位置模組和功能。**
4. **配置Windows CE、Macintosh和Linux功能。**

階段I:使用SDM為CSD配置準備路由器。

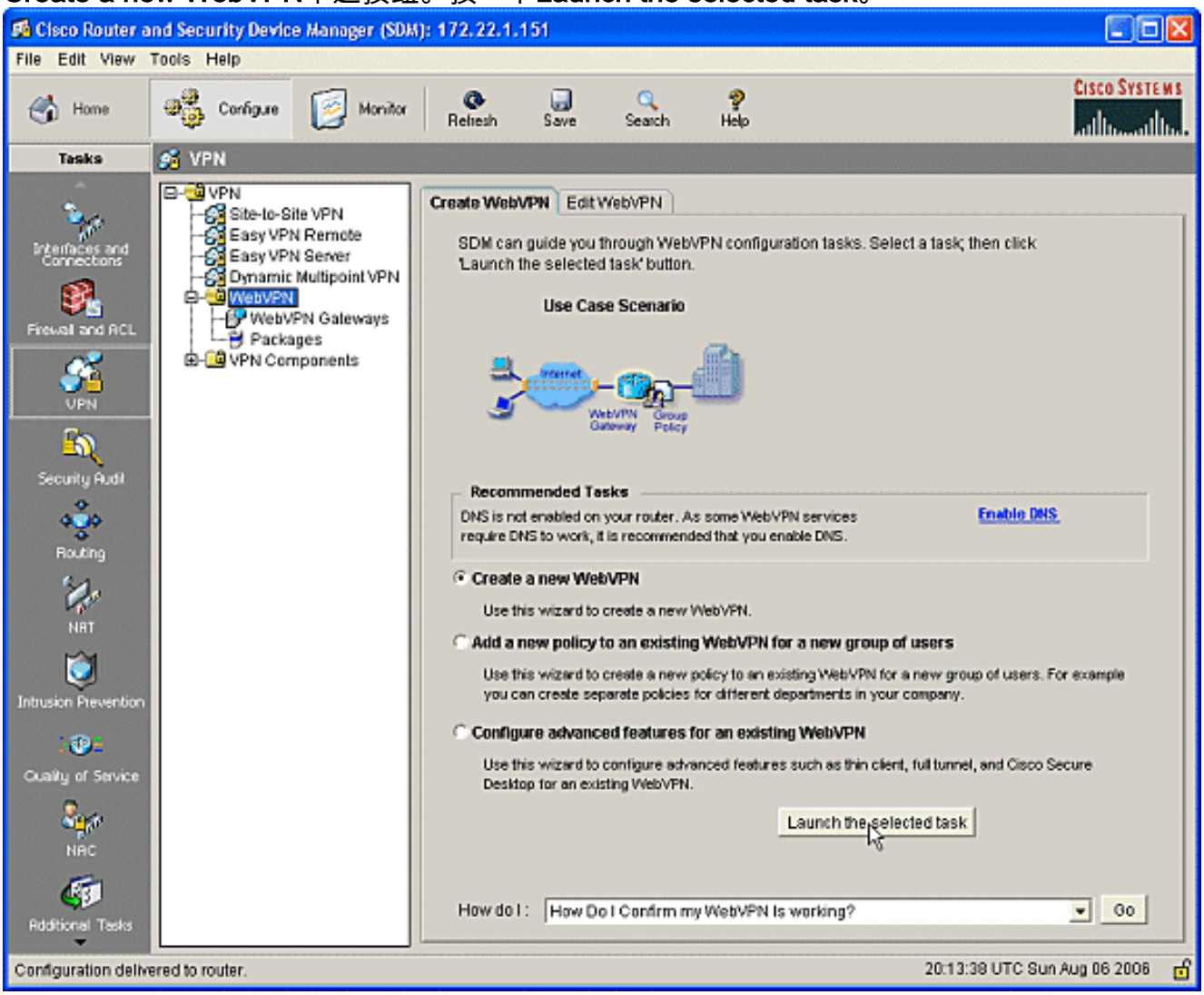
可以使用SDM或通過命令列介面(CLI)配置CSD。 此配置使用SDM和Web瀏覽器。

這些步驟用於在IOS路由器上完成CSD的配置。

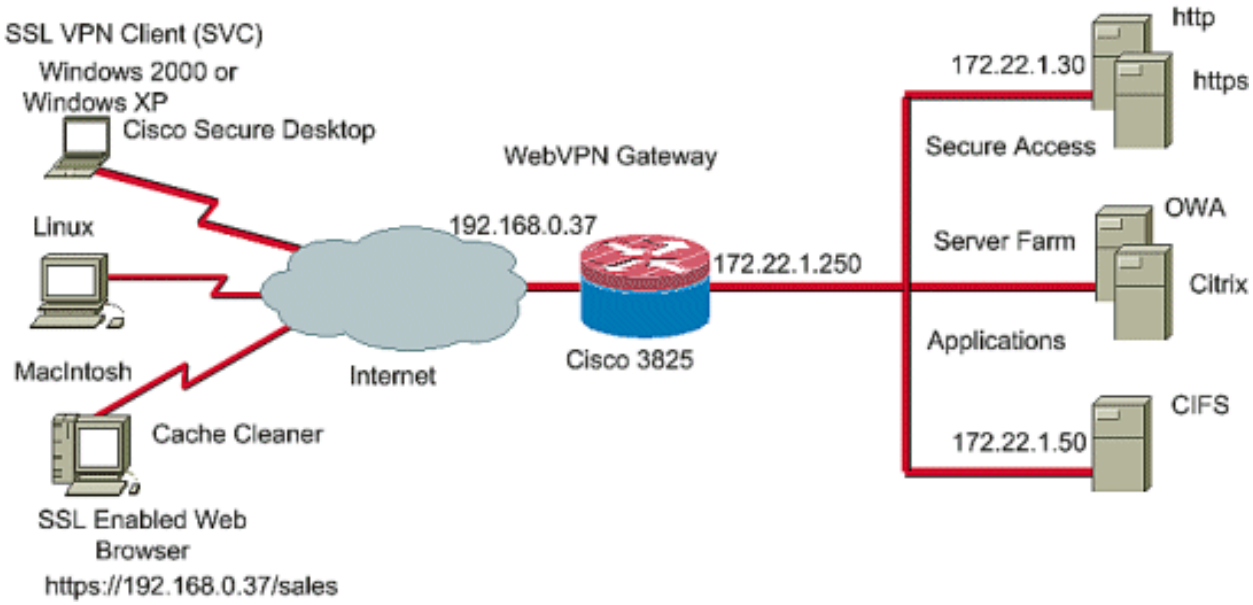
階段I:第1步：配置WebVPN網關、WebVPN上下文和組策略。

您可以使用WebVPN嚮導完成此任務。

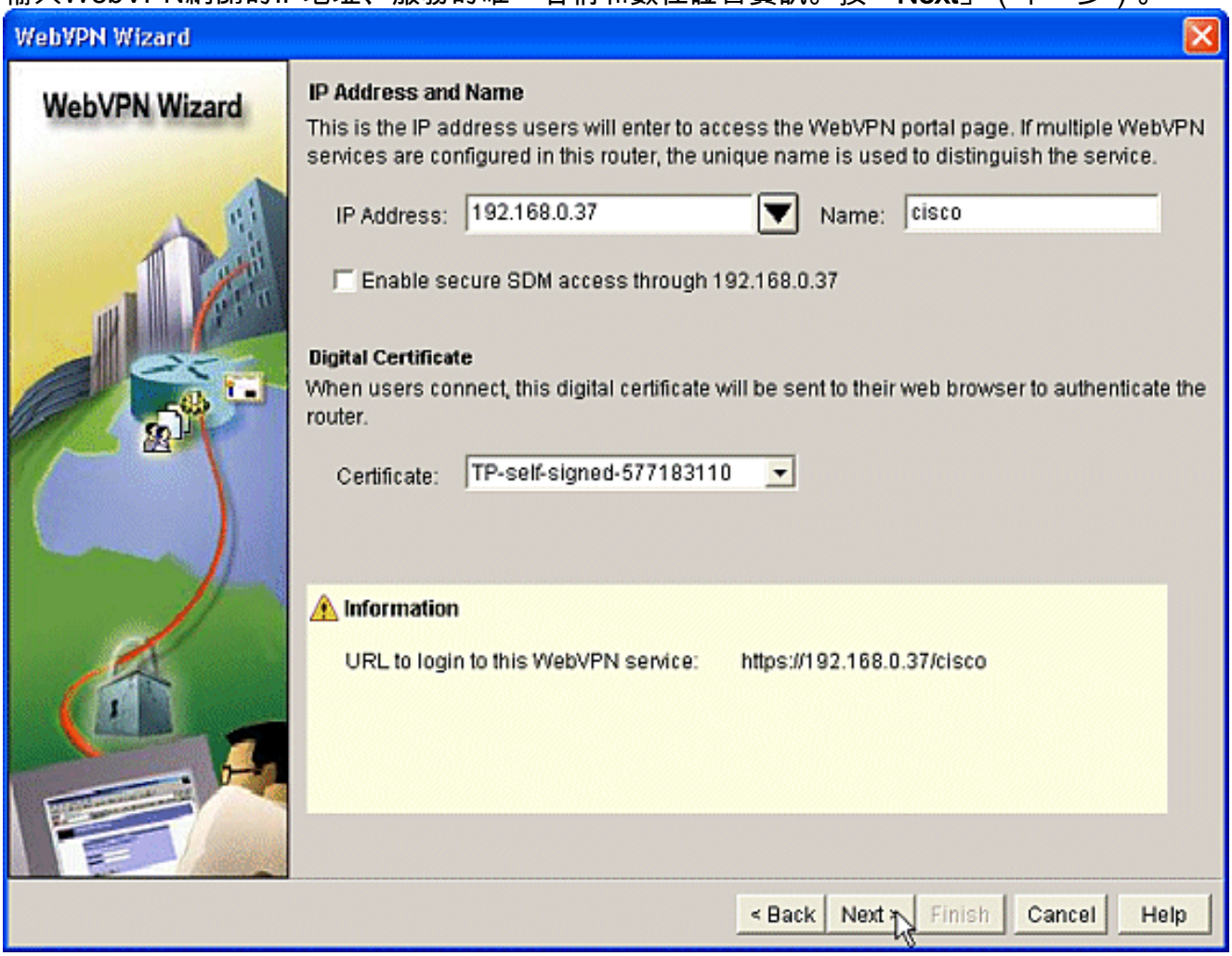
1. 開啟SDM，然後轉到**Configure > VPN > WebVPN**。按一下**Create WebVPN**頁籤並選中**Create a new WebVPN**單選按鈕。按一下**Launch the selected task**。



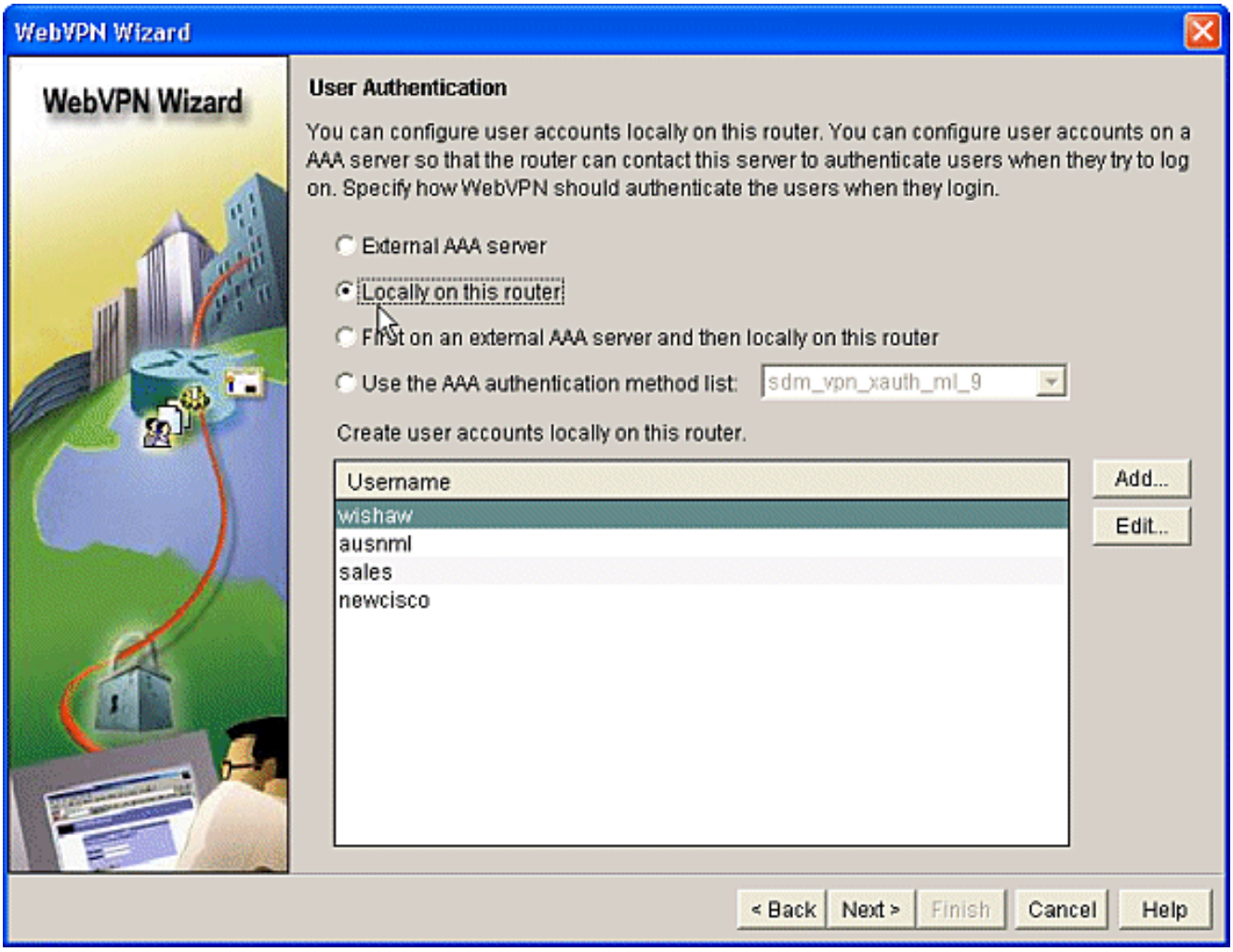
2. WebVPN嚮導螢幕列出了可以配置的引數。按「**Next**」（下一步）。



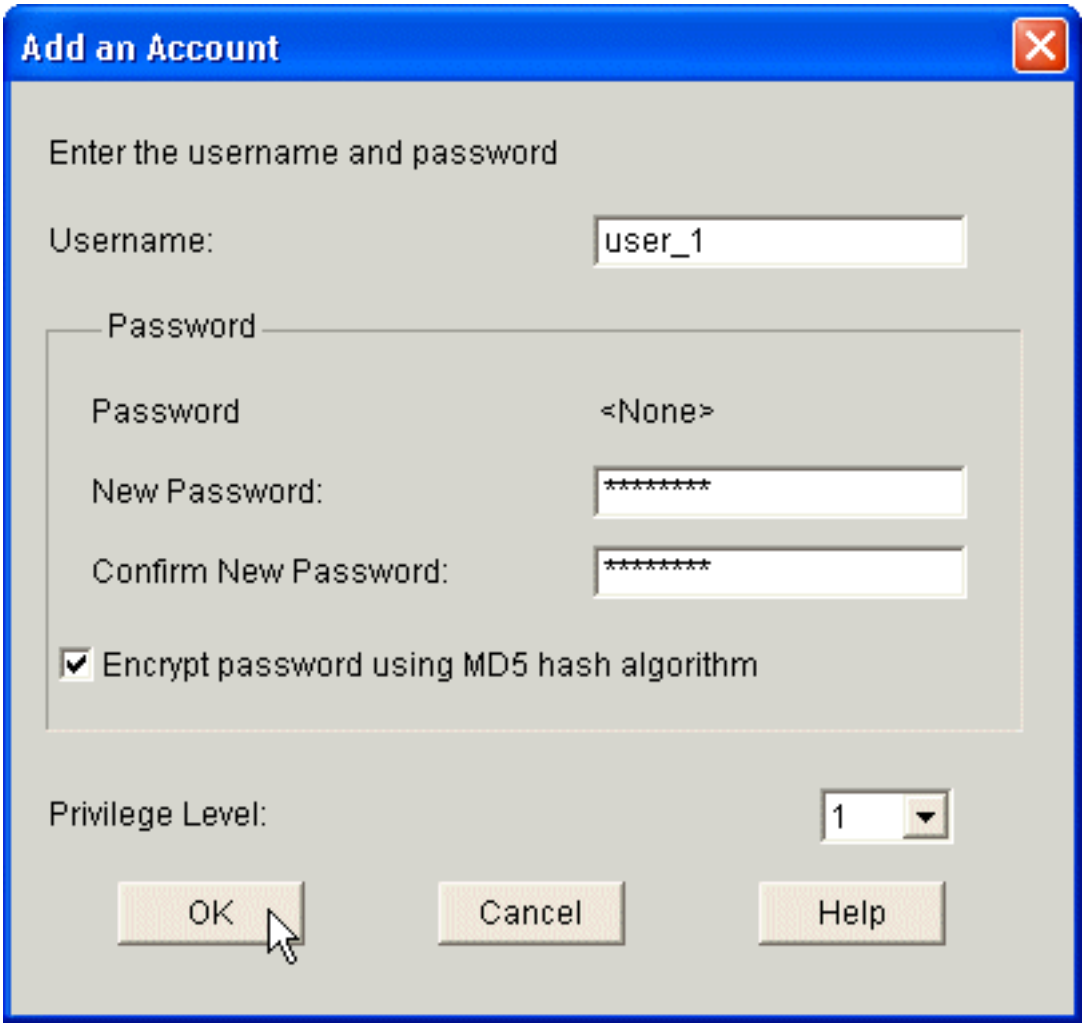
3. 輸入WebVPN網關的IP地址、服務的唯一名稱和數位證書資訊。按「**Next**」（下一步）。



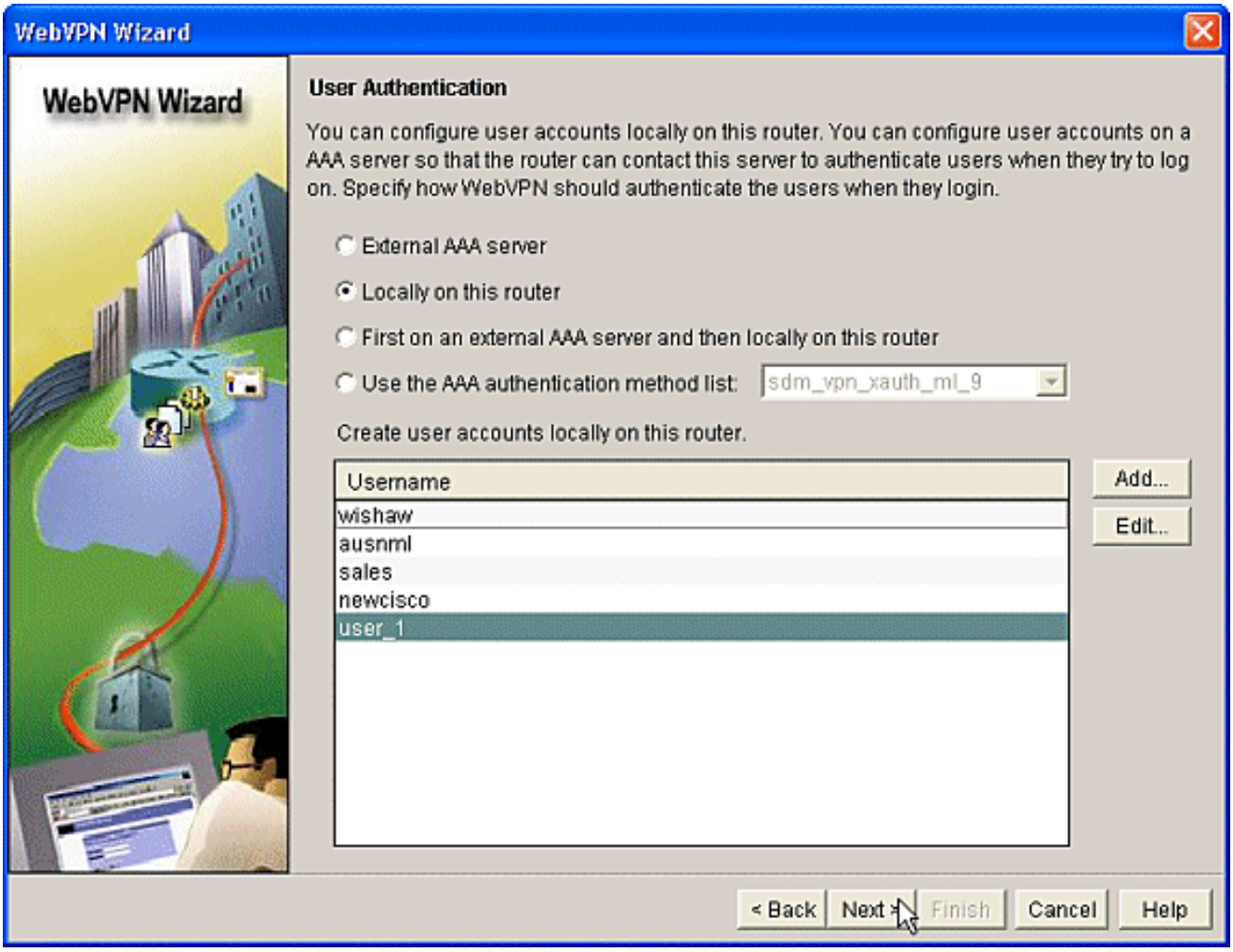
4. 可以建立使用者帳戶以驗證此WebVPN網關。您可以使用本地帳戶或在外部身份驗證、授權和記帳(AAA)伺服器上建立的帳戶。此示例使用路由器上的本地帳戶。選中**Locally on this router**單選按鈕，然後按一下**Add**。



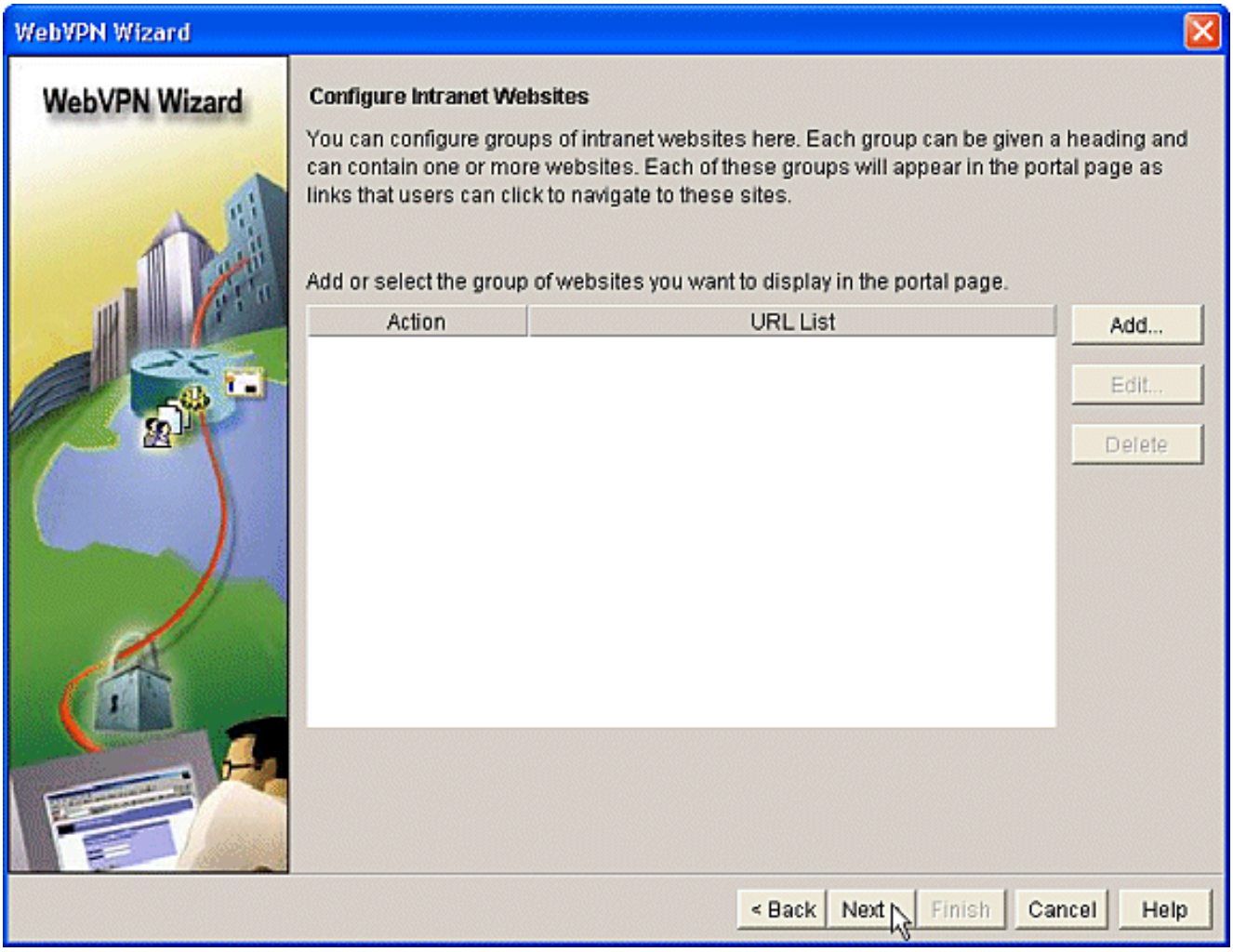
5. 在「新增帳戶」螢幕中輸入新使用者的帳戶資訊，然後按一下**確定**。



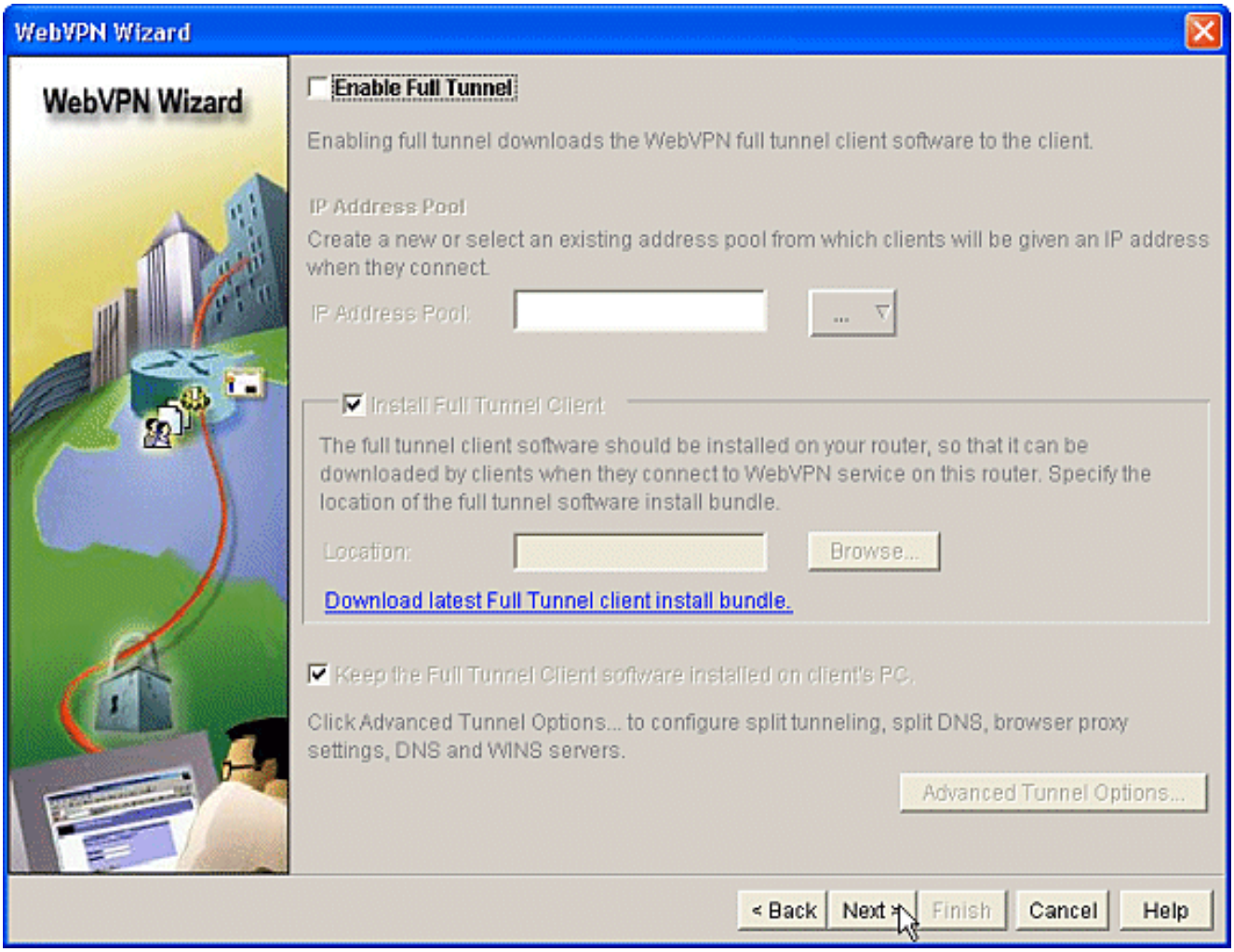
6. 建立使用者後，在User Authentication頁面上按一下**Next**。



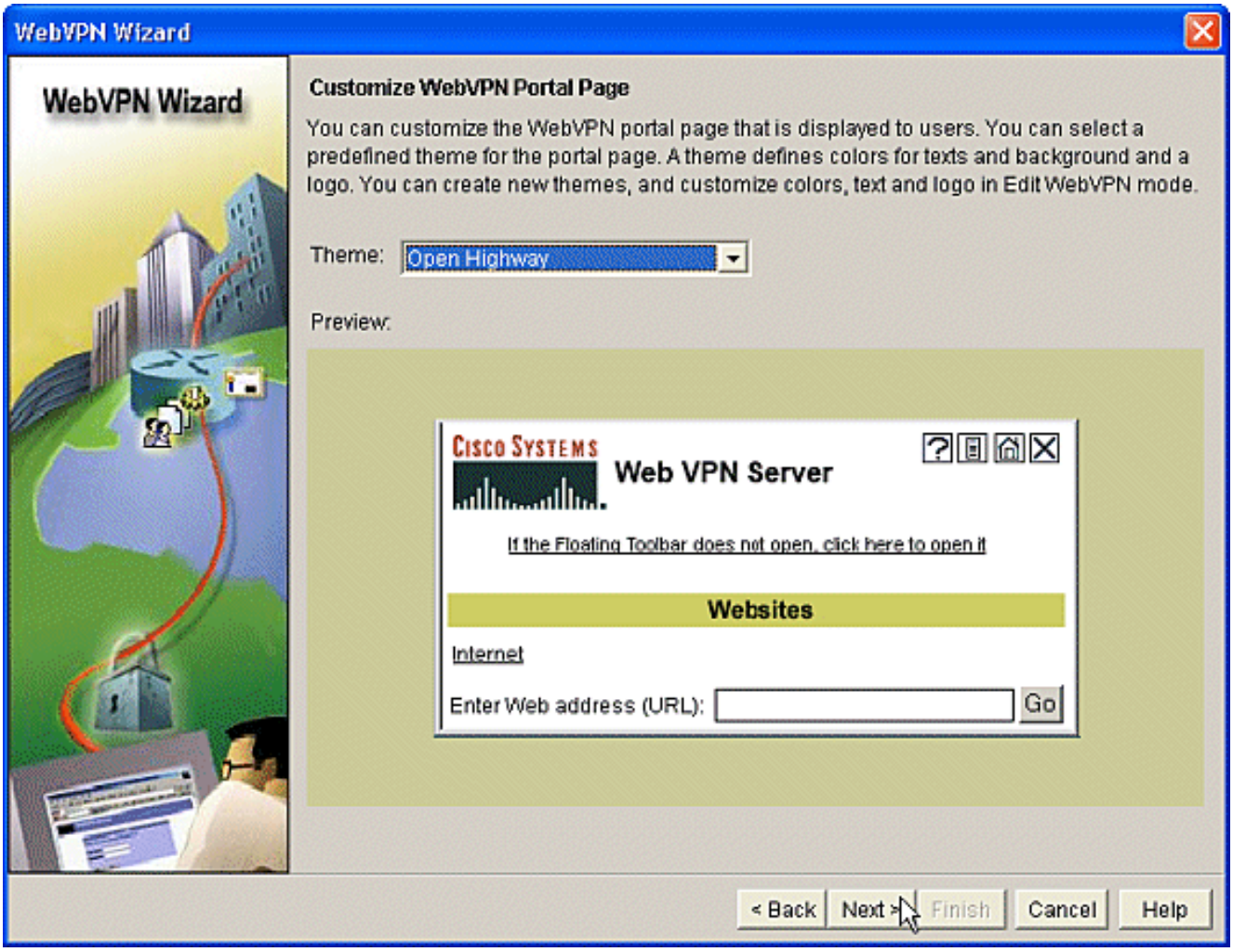
7. Configure Intranet Websites螢幕允許您配置WebVPN網關使用者可用的網站。由於本文檔重點是CSD的配置，請忽略此頁。按「**Next**」（下一步）。



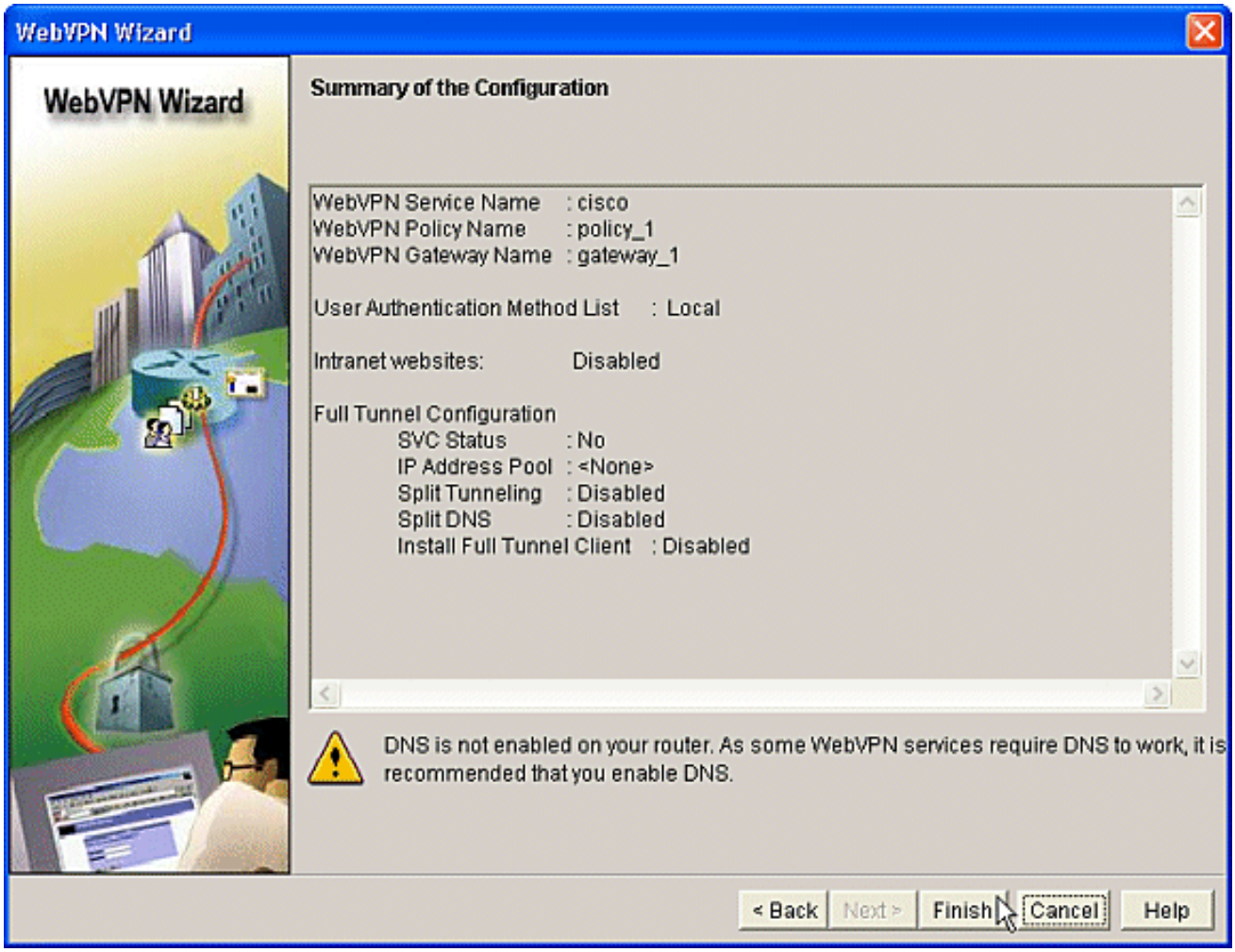
8. 雖然下一個WebVPN嚮導螢幕允許您選擇啟用全通道SSL VPN客戶端，但本文檔重點介紹如何啟用CSD。取消選中**Enable Full Tunnel**，然後按一下**Next**。



9. 您可以為使用者自定義WebVPN門戶頁面的外觀。在這種情況下，接受預設外觀。按「**Next**」（下一步）。



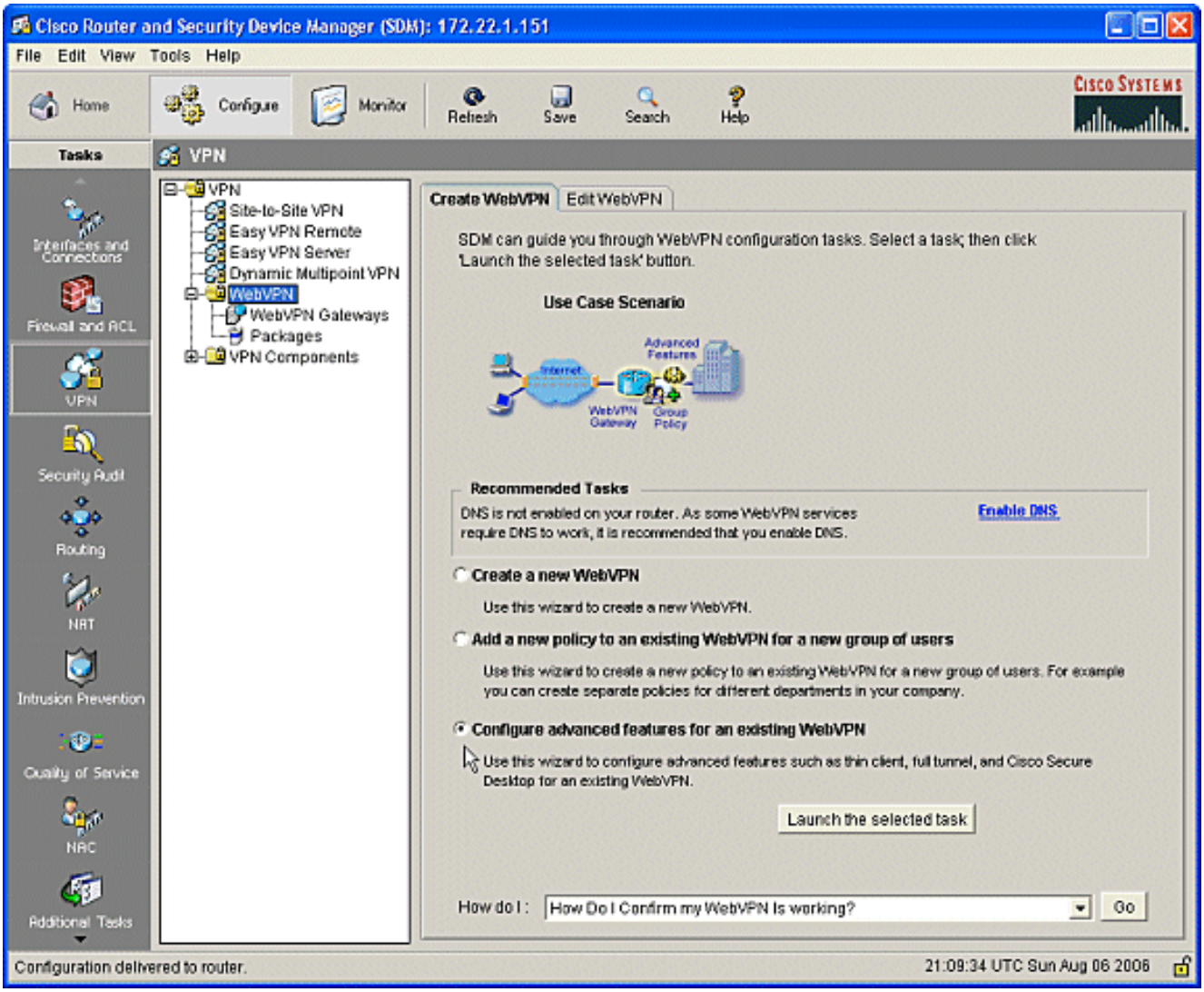
10. 嚮導會顯示此系列中的最後一個螢幕。其中顯示了WebVPN網關的配置摘要。按一下「Finish」，並在系統提示時按一下「OK」。



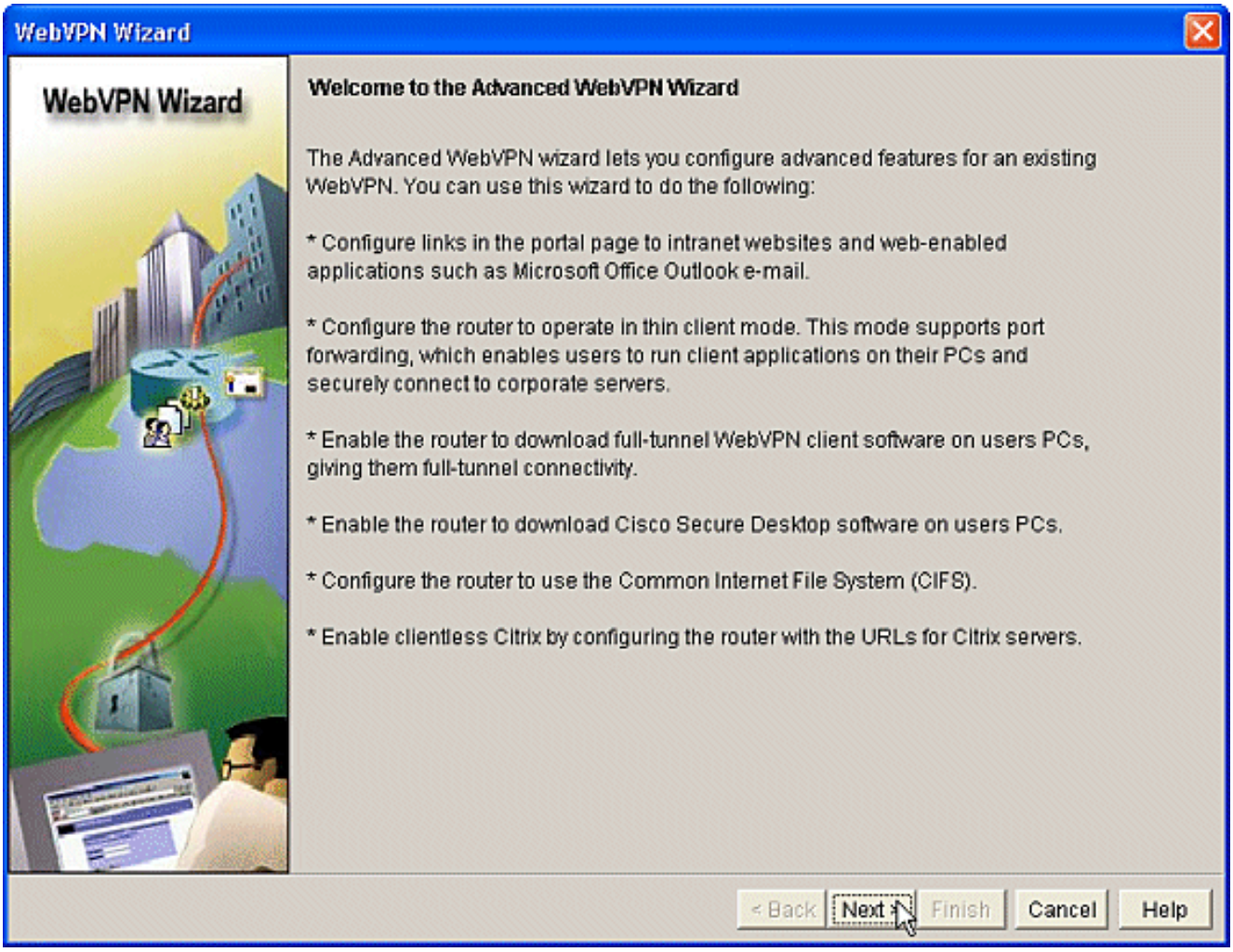
階段I:第2步：在WebVPN上下文中啟用CSD。

使用WebVPN嚮導在WebVPN上下文中啟用CSD。

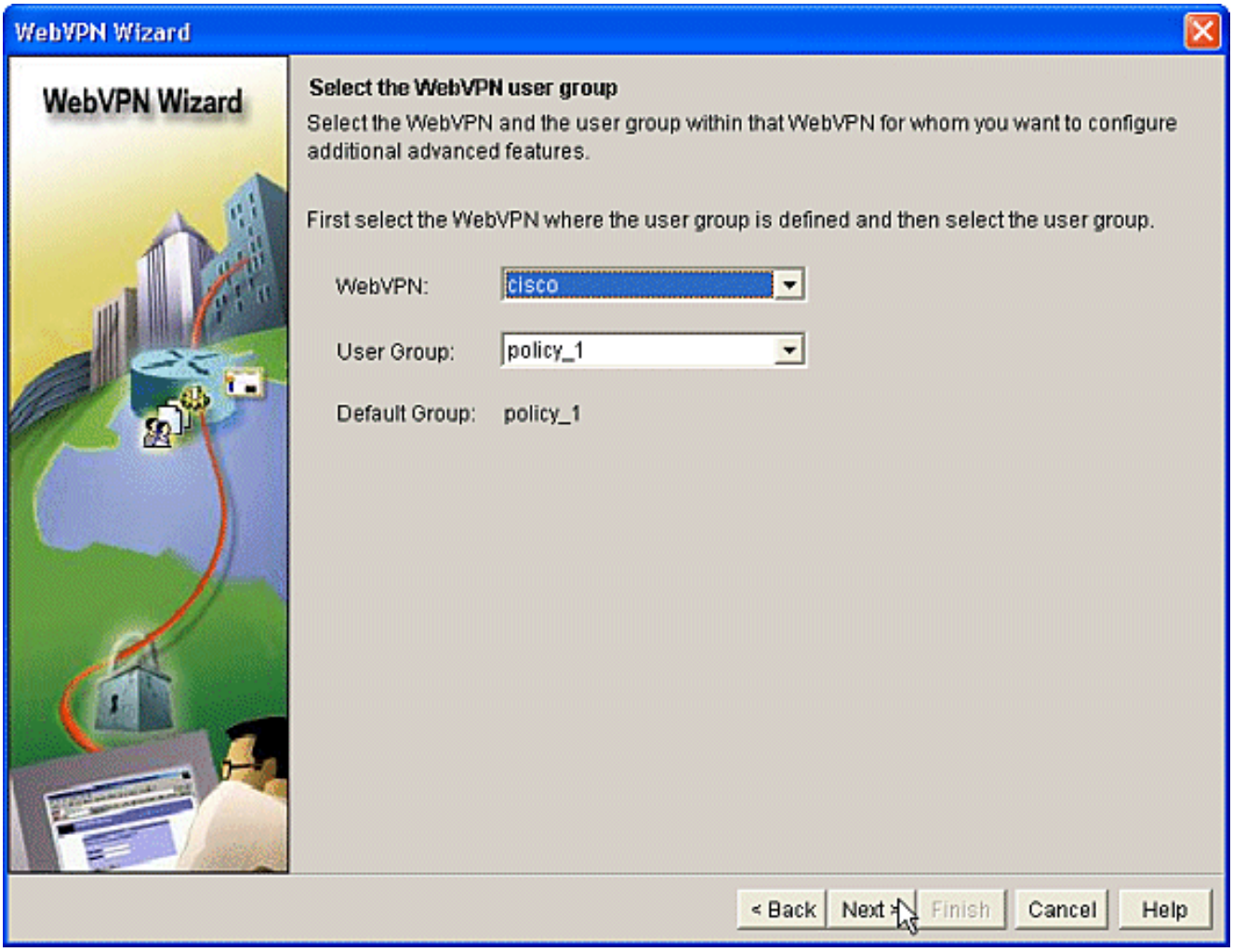
1. 使用WebVPN嚮導的高級功能為新建立的上下文啟用CSD。如果尚未安裝CSD軟體包，嚮導將為您提供安裝該軟體包的機會。在SDM中，按一下**Configure**頁籤。在導航窗格中，按一下**VPN > WebVPN**。按一下**Create WebVPN**頁籤。選中**Configure advance features for an existing WebVPN**單選按鈕。按一下**啟動所選任務**按鈕。



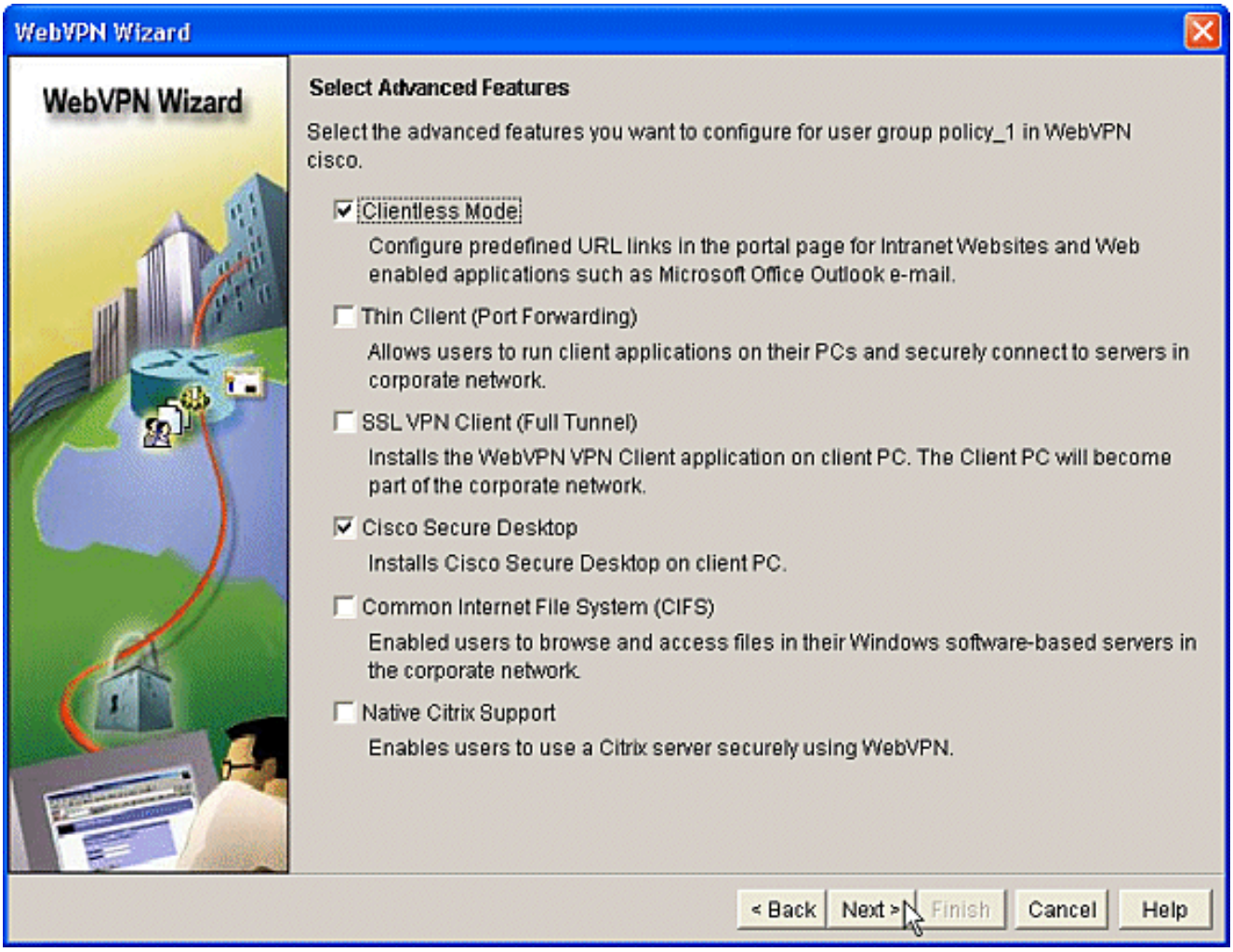
2. 系統將顯示高級WebVPN嚮導的歡迎頁面。按「**Next**」（下一步）。



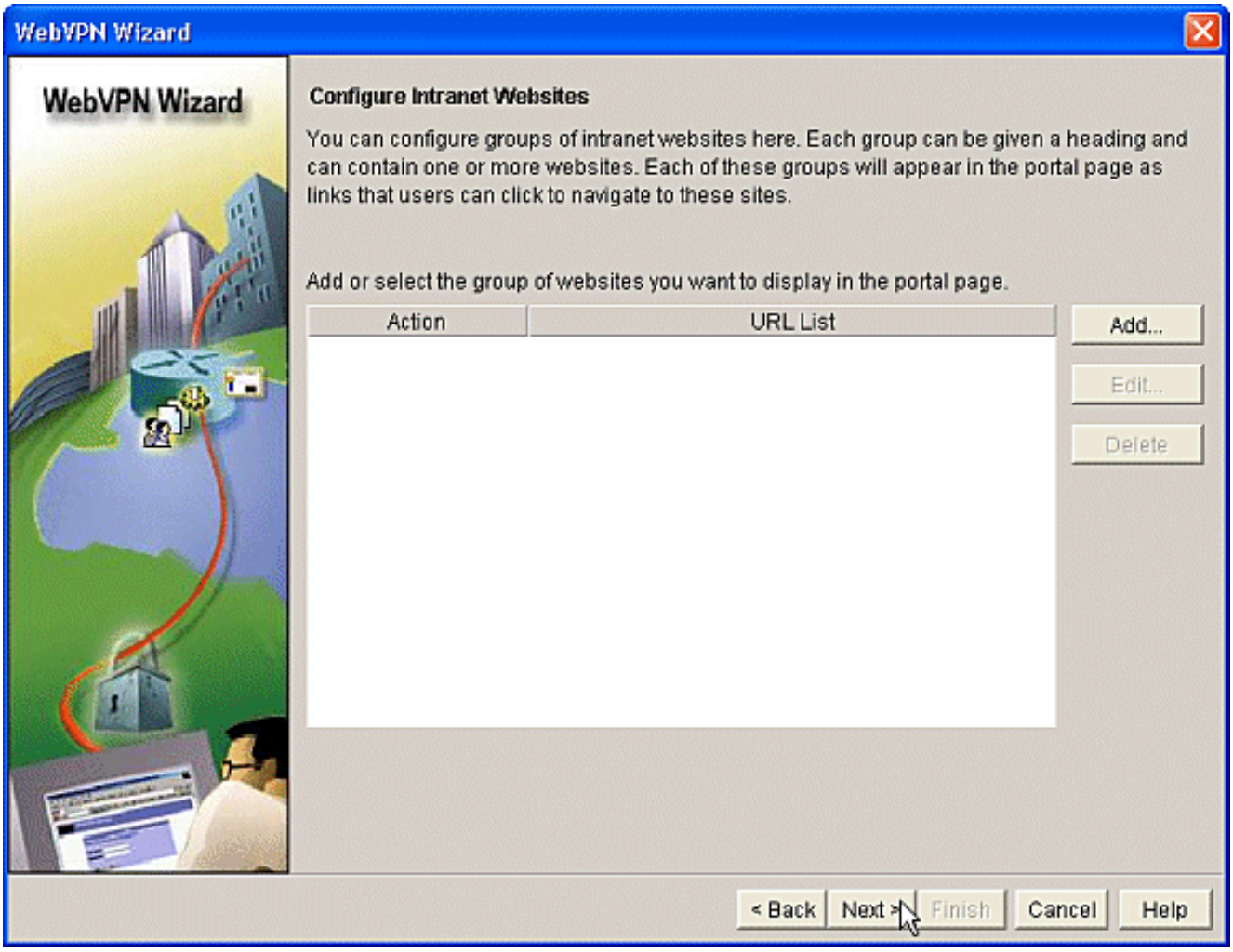
3. 從欄位的下拉框中選擇WebVPN和使用者組。高級WebVPN嚮導功能將應用於您的選擇。按「**Next**」（下一步）。



4. Select Advanced Features（選擇高級功能）螢幕允許您從列出的技術中進行選擇。檢查**Cisco Secure Desktop**。在本例中，選擇的是**Clientless Mode**。如果選擇其他列出的任何技術，則會開啟其他視窗以輸入相關資訊。按一下**Next**按鈕。

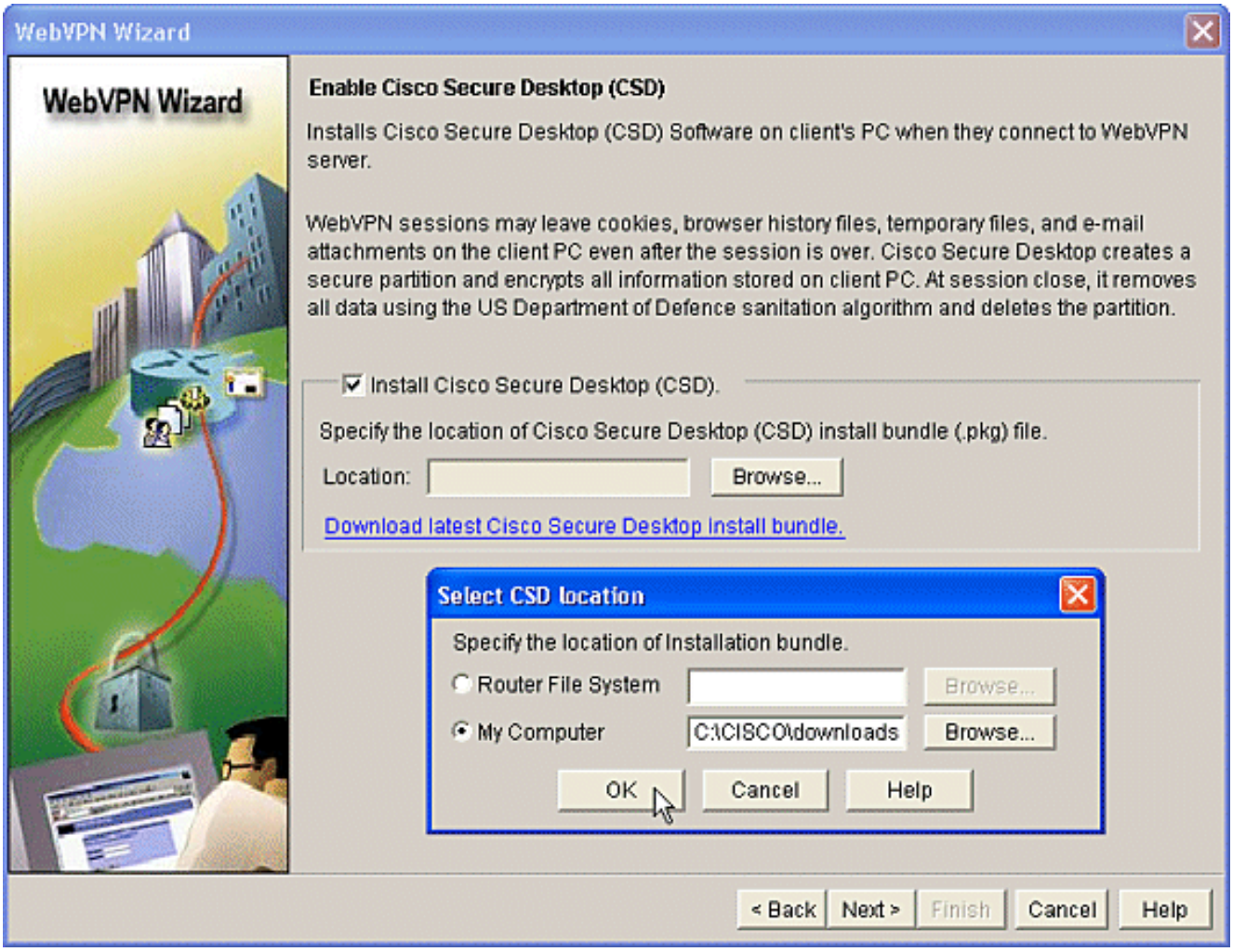


5. 通過「配置Intranet網站」螢幕，可以配置使用者想要使用的網站資源。您可以新增公司的內部網站，例如Outlook Web Access(OWA)。



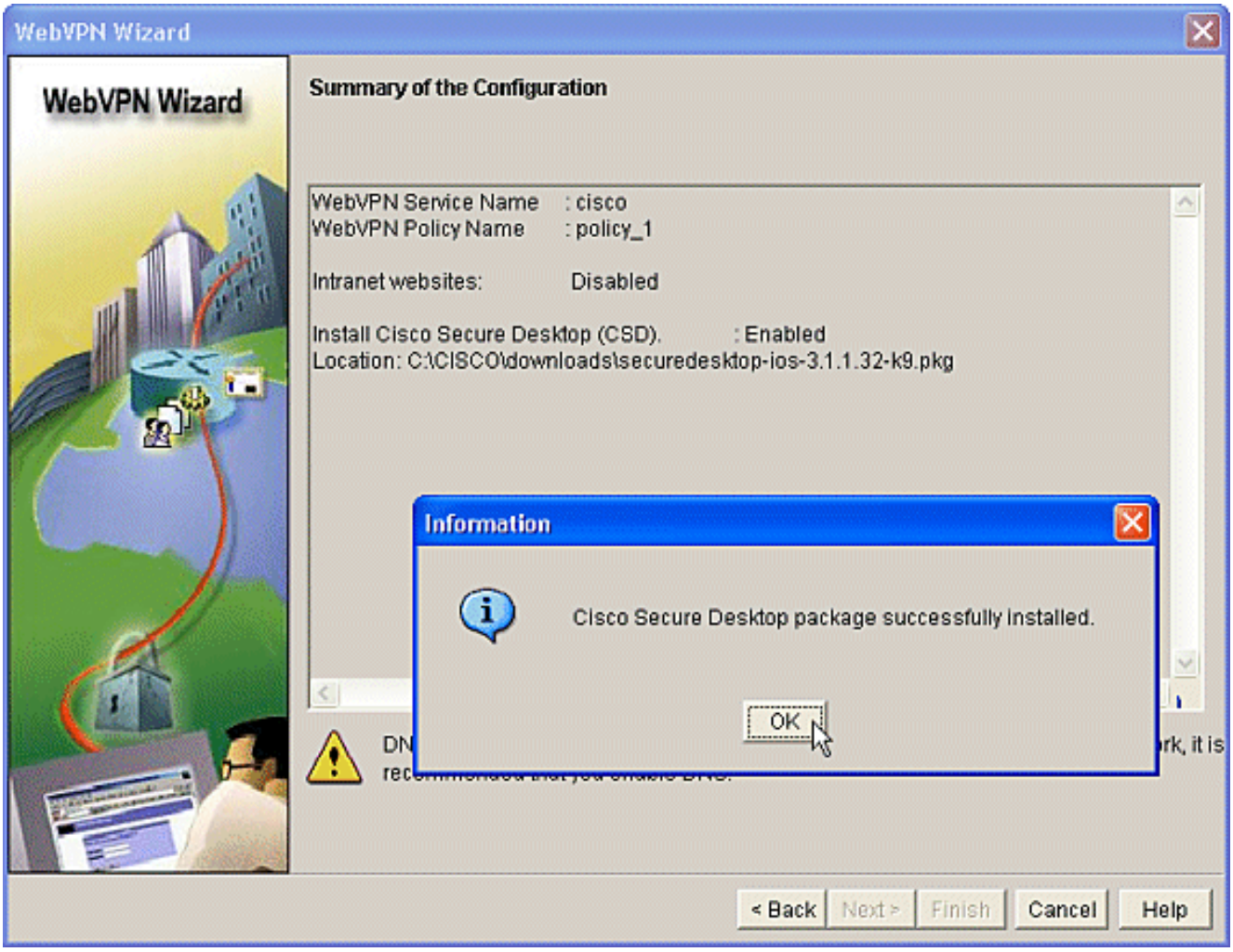
6. 在啟用Cisco Secure Desktop(CSD)螢幕中，您有機會為此情景啟用CSD。選中**安裝Cisco Secure Desktop(CSD)**旁邊的框，然後按一下**Browse**。

7. 在Select CSD Location區域，選中**My Computer**。按一下**Browse**按鈕。在管理工作站上選擇CSD IOS軟體包檔案。按一下**OK**按鈕。按一下**Next**按鈕。



8. 系統隨即會顯示「配置」螢幕的摘要。按一下**Finish**按鈕。

9. 看到CSD軟體包檔案已成功安裝後，按一下**OK**。



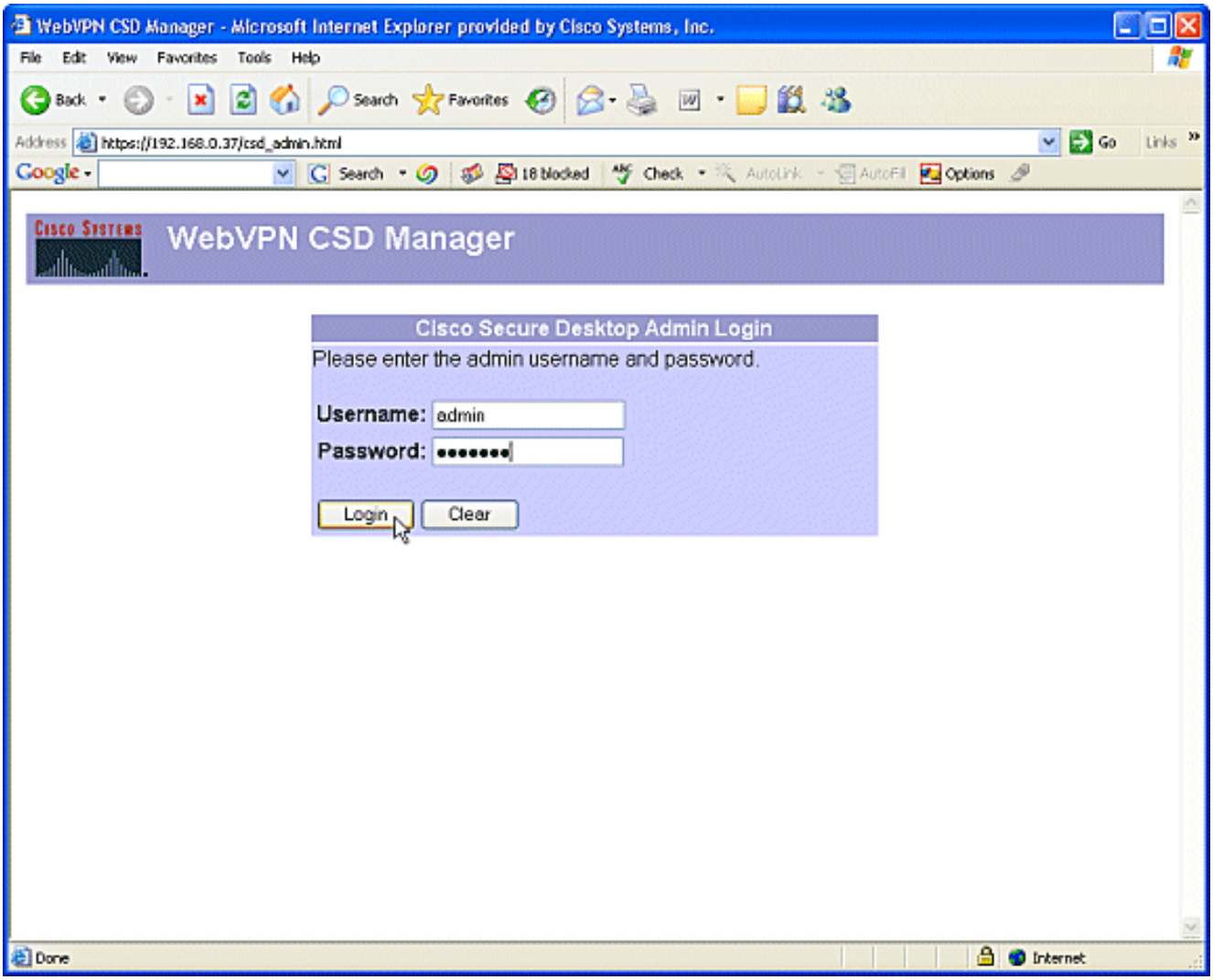
第二階段：使用Web瀏覽器配置CSD。

這些步驟用於在Web瀏覽器上完成CSD的配置。

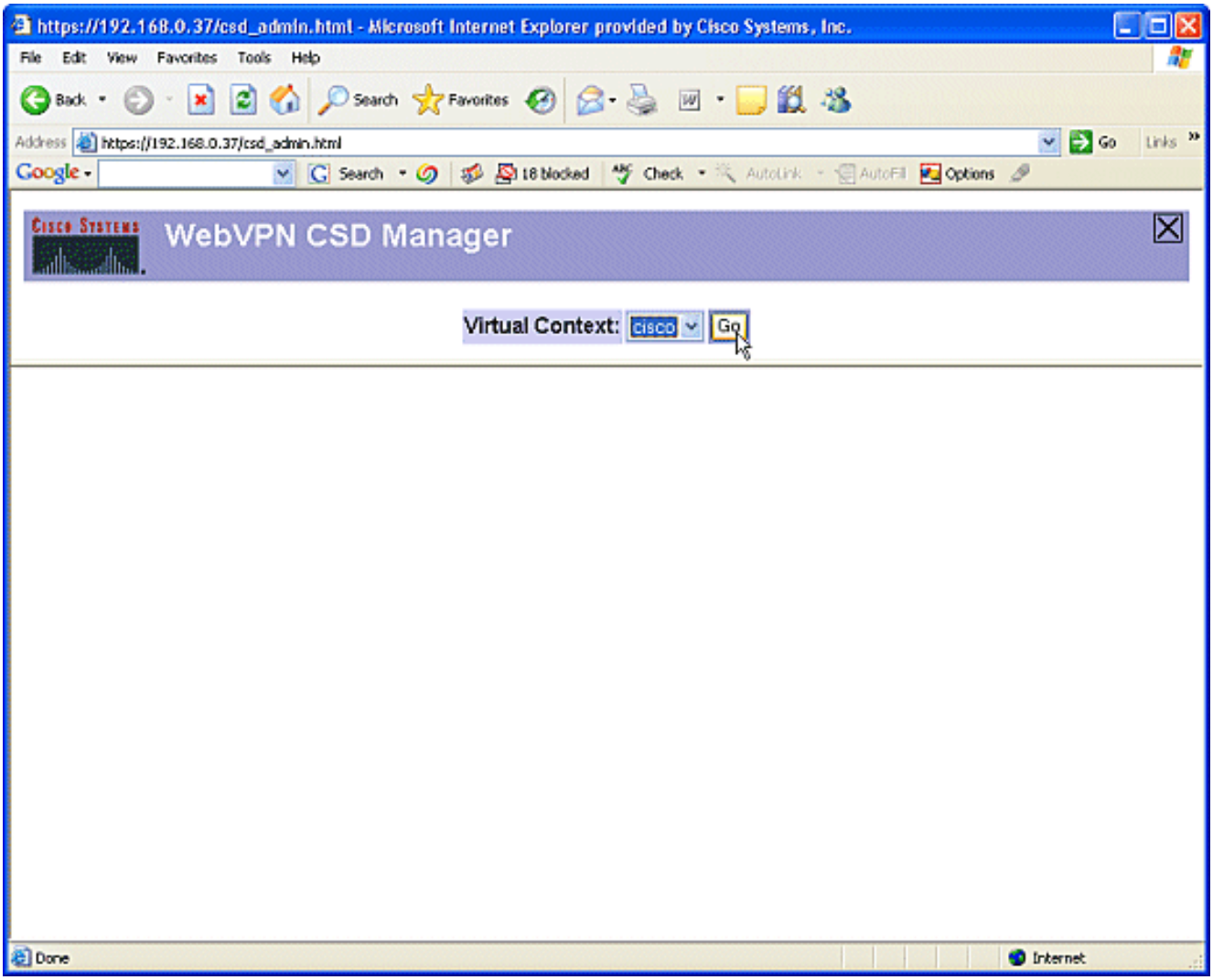
第二階段：第1步：定義Windows位置。

定義Windows位置。

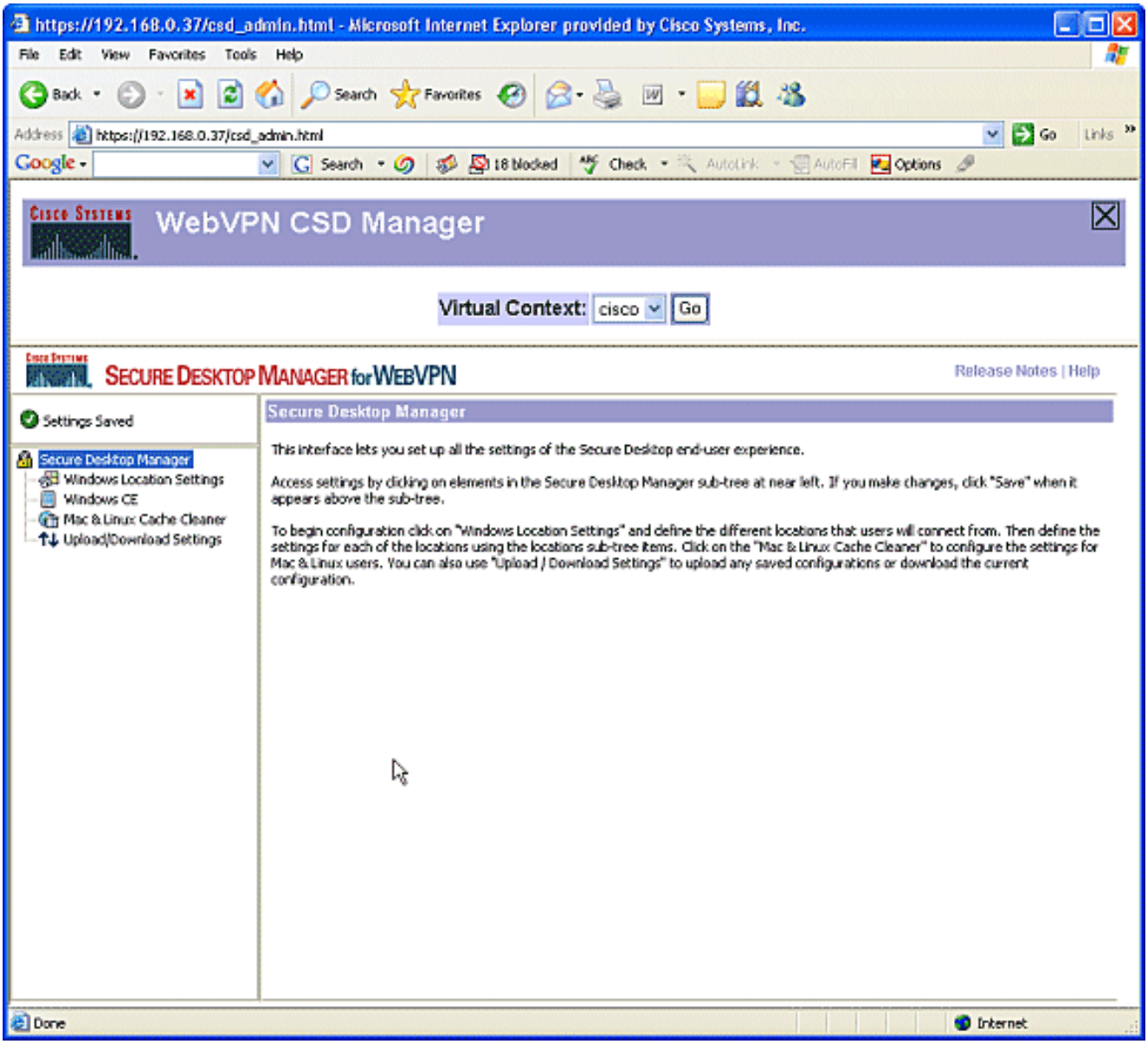
1. 在**https://WebVPNgateway_IP Address/csd_admin.html**上開啟您的Web瀏覽器，例如**https:/192.168.0.37/csd_admin.html**。
2. 輸入使用者名稱**admin**。輸入口令，即路由器的使能加密口令。按一下「**Login**」。



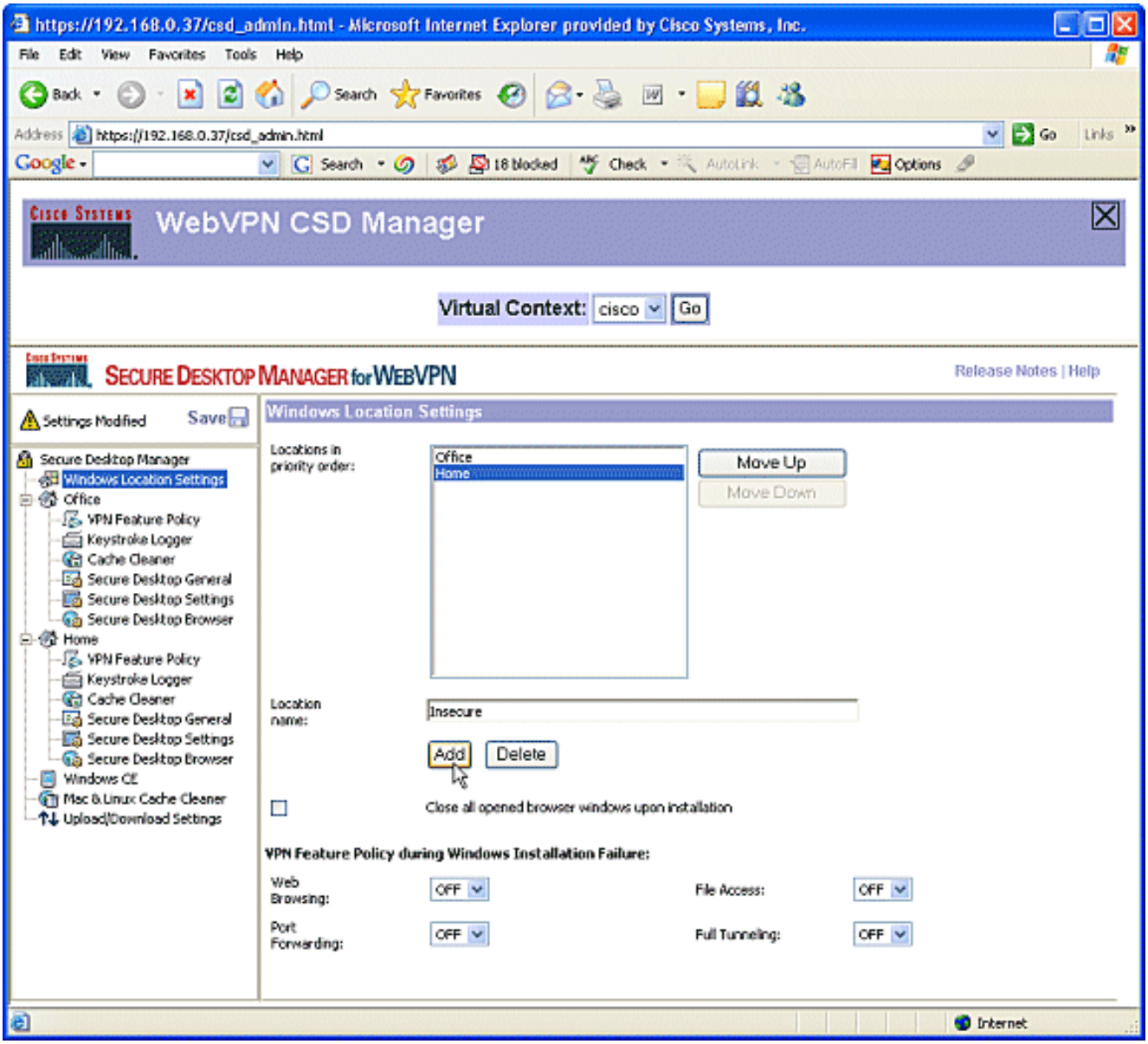
3. 接受路由器提供的證書，從下拉框中選擇上下文，然後按一下**Go**。



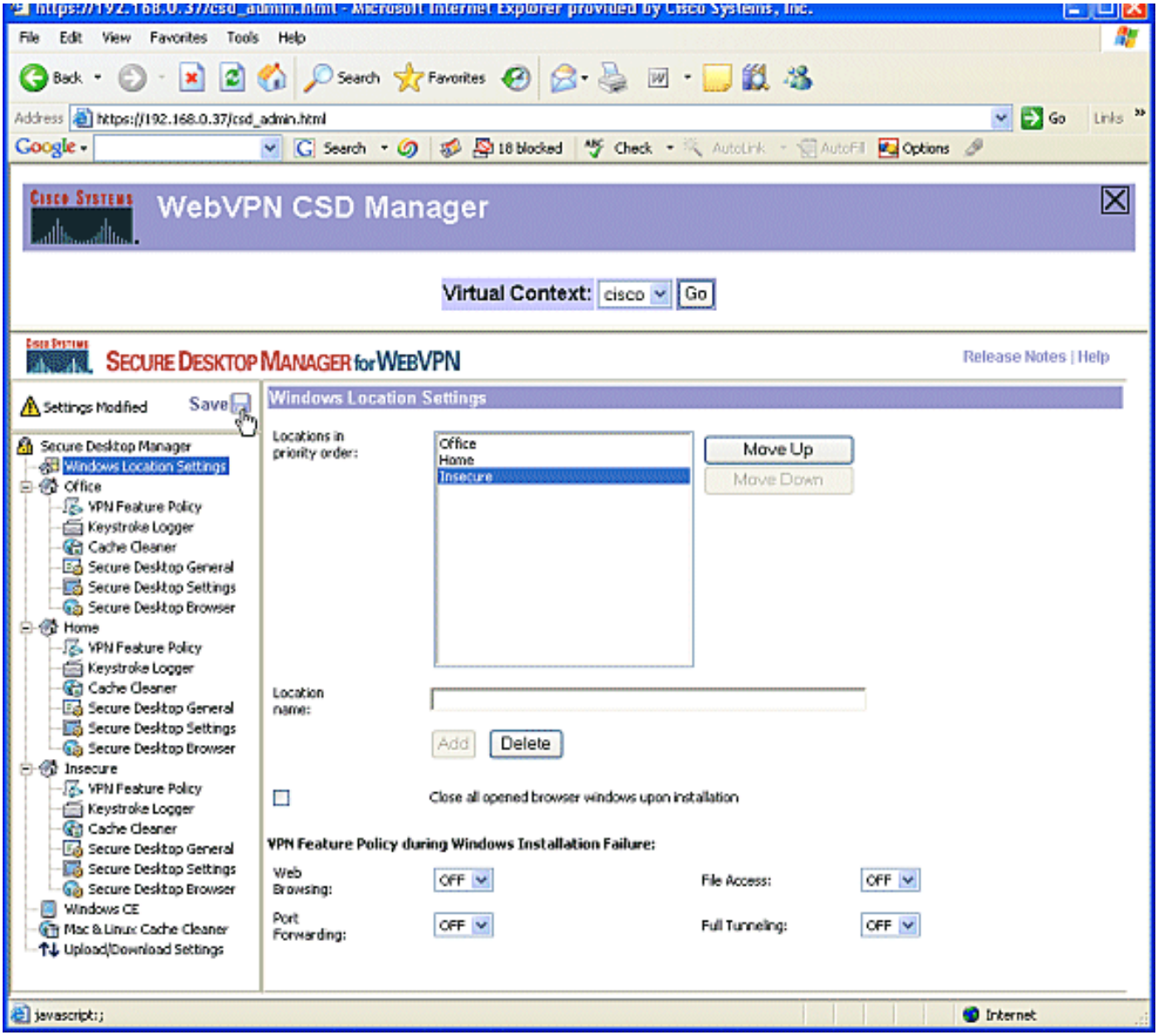
4. 將開啟Secure Desktop Manager for WebVPN。



5. 在左窗格中，選擇**Windows Location Settings**。將游標置於「位置名稱」(Location name)旁邊的框中，並輸入位置名稱。按一下「**Add**」。在此示例中，顯示了三個位置名稱：Office、Home和Insecure。每次新增新位置時，左窗格都會展開該位置的可配置引數。



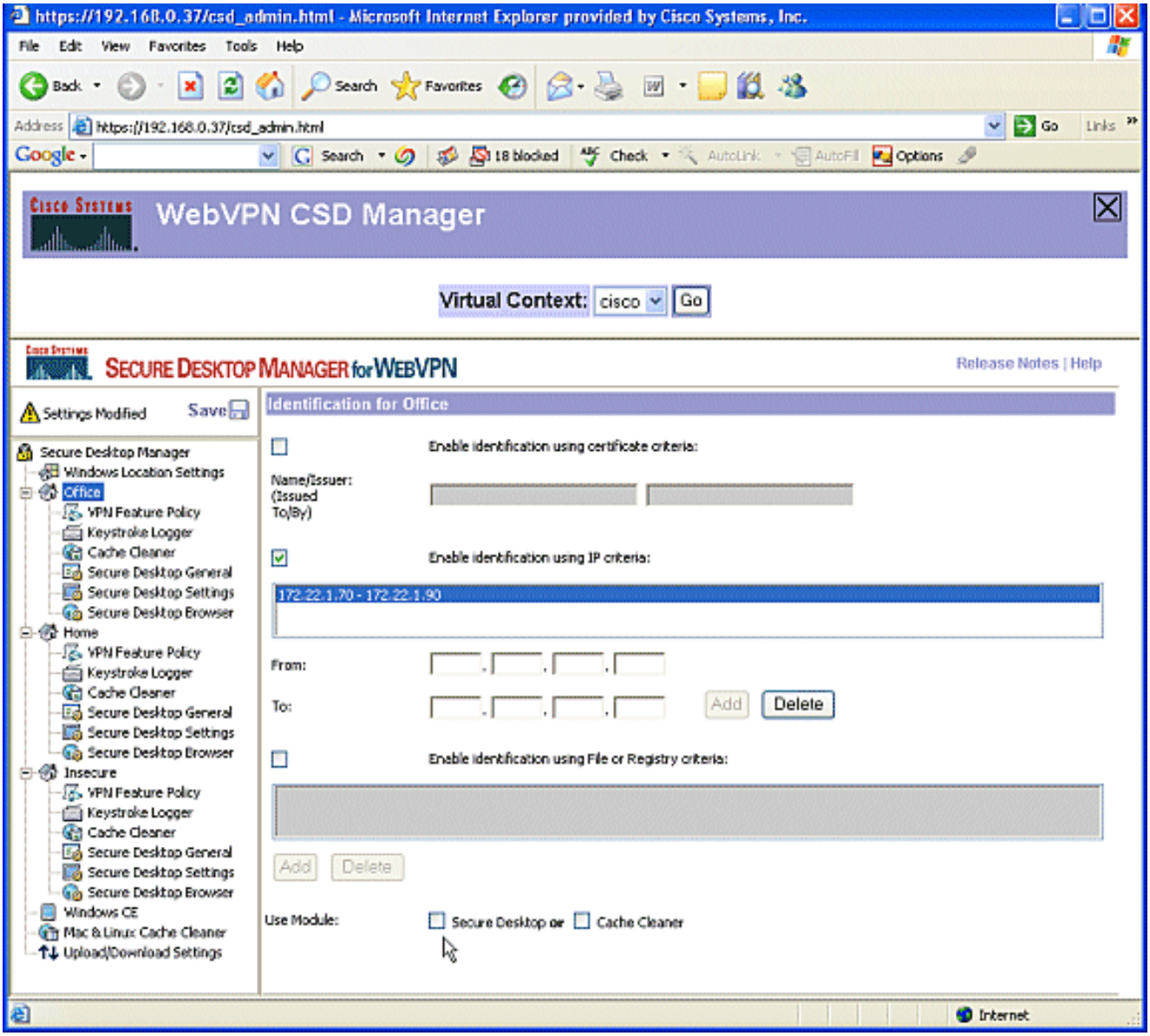
6. 建立Windows位置後，按一下左窗格頂部的**Save**。**附註：** 經常儲存您的配置，因為如果您斷開與Web瀏覽器的連線，您的設定將會丟失。



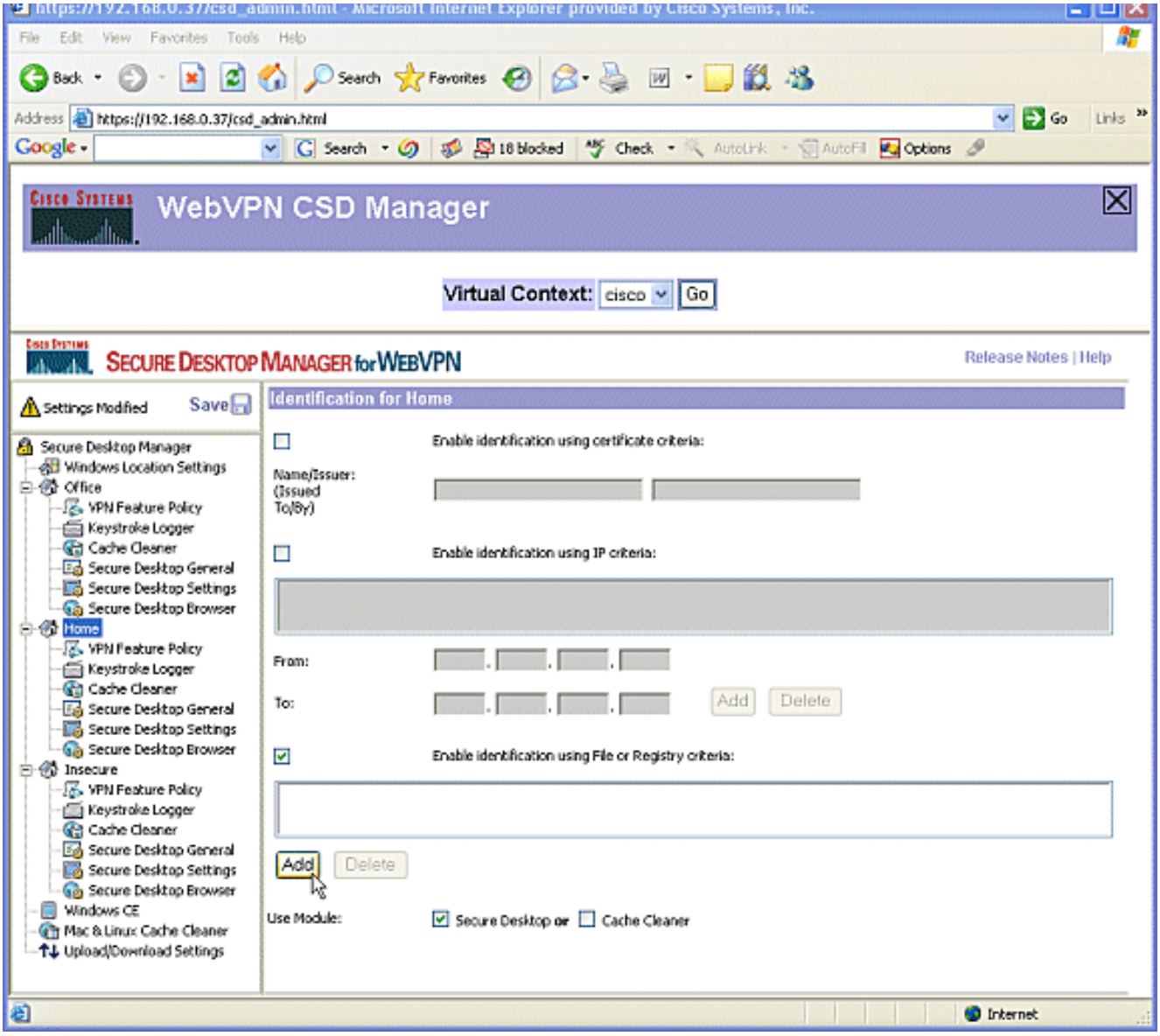
第二階段：第2步：確定位置條件

為了區分Windows位置，請為每個位置分配特定的條件。這允許CSD確定將哪些功能應用於特定Windows位置。

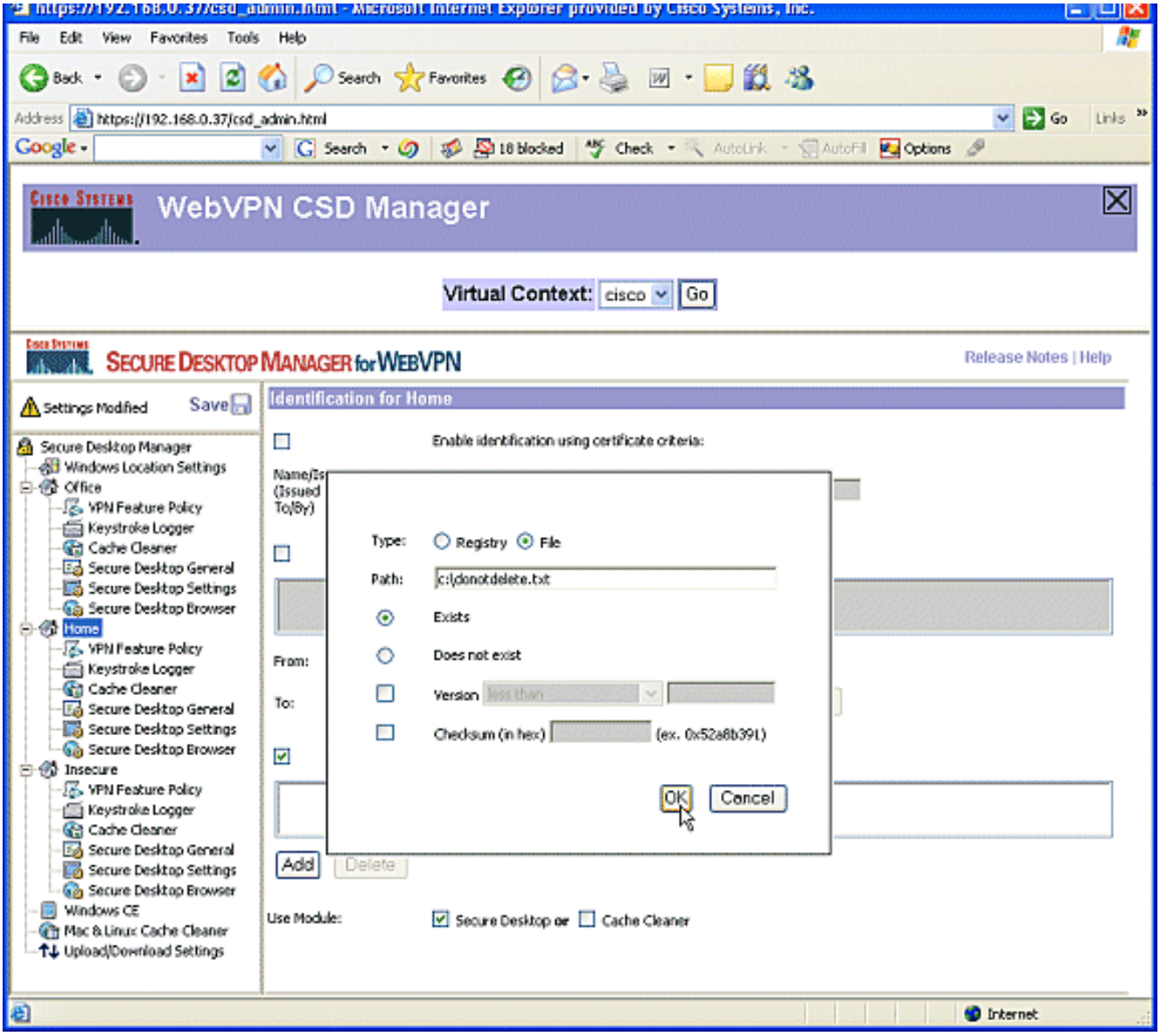
1. 在左窗格中，按一下**Office**。您可以使用證書條件、IP條件、檔案或登錄檔條件標識Windows位置。您還可以為這些客戶端選擇Secure Desktop或Cache Cleaner。由於這些使用者是內部辦公室員工，因此請通過IP標準識別他們。在**From**和**To**框中輸入IP地址範圍。按一下「**Add**」。取消選中**Use Module:安全案頭**。出現提示時，按一下**Save**，然後按一下**OK**。



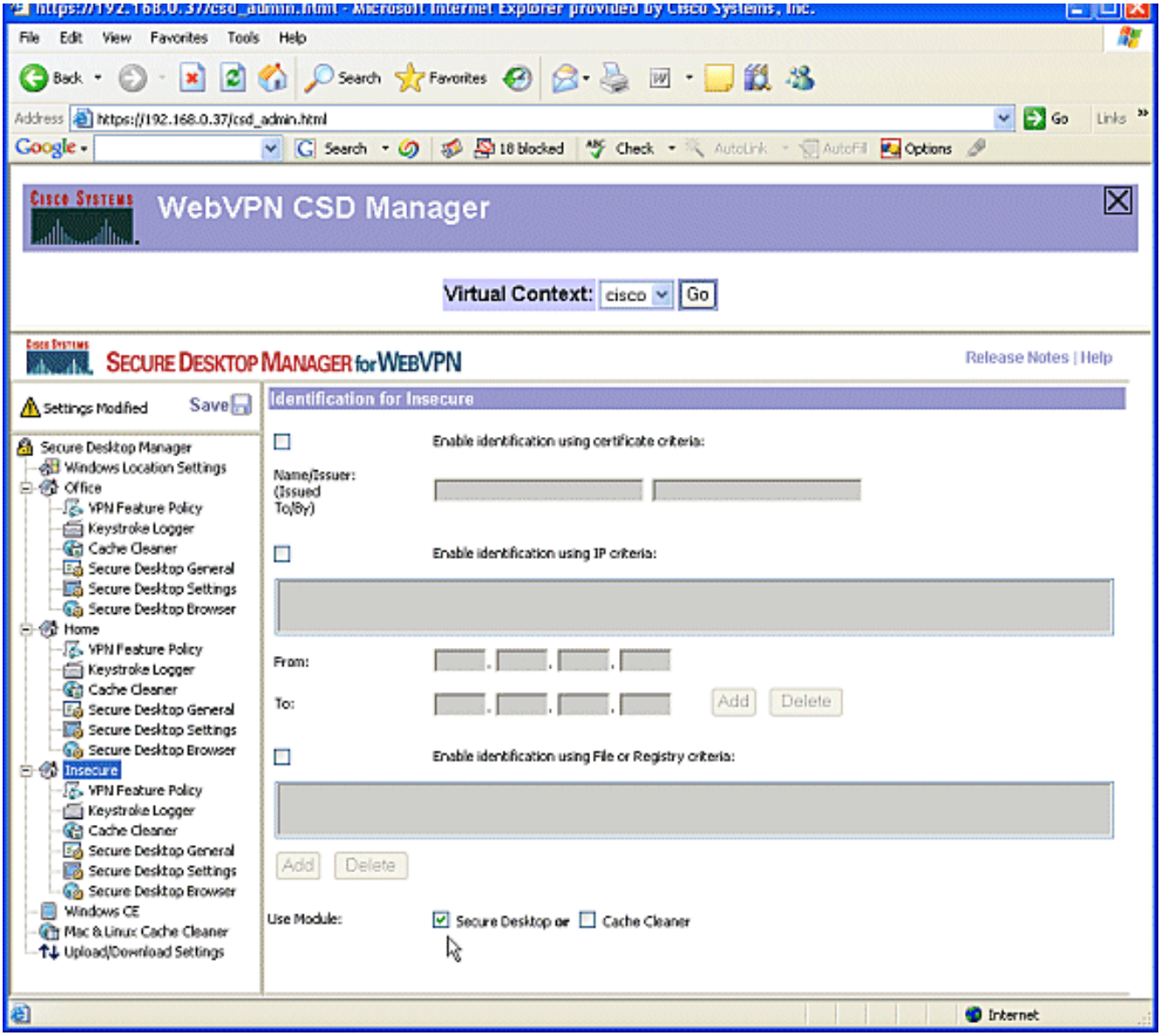
2. 在左窗格中，按一下第二個Windows位置設定**首頁**。確保使**用模組：已選中**Secure Desktop。將分發標識這些客戶機的檔案。您可以選擇為這些使用者分發證書和/或登錄檔條件。選中**Enable identification using File or Registry criteria**。按一下「**Add**」。



3. 在對話方塊中，選擇**檔案**，然後輸入檔案的路徑。此檔案必須分發給所有家庭客戶端。選中**Exists**單選按鈕。出現提示時，按一下**OK**，然後按一下**Save**。



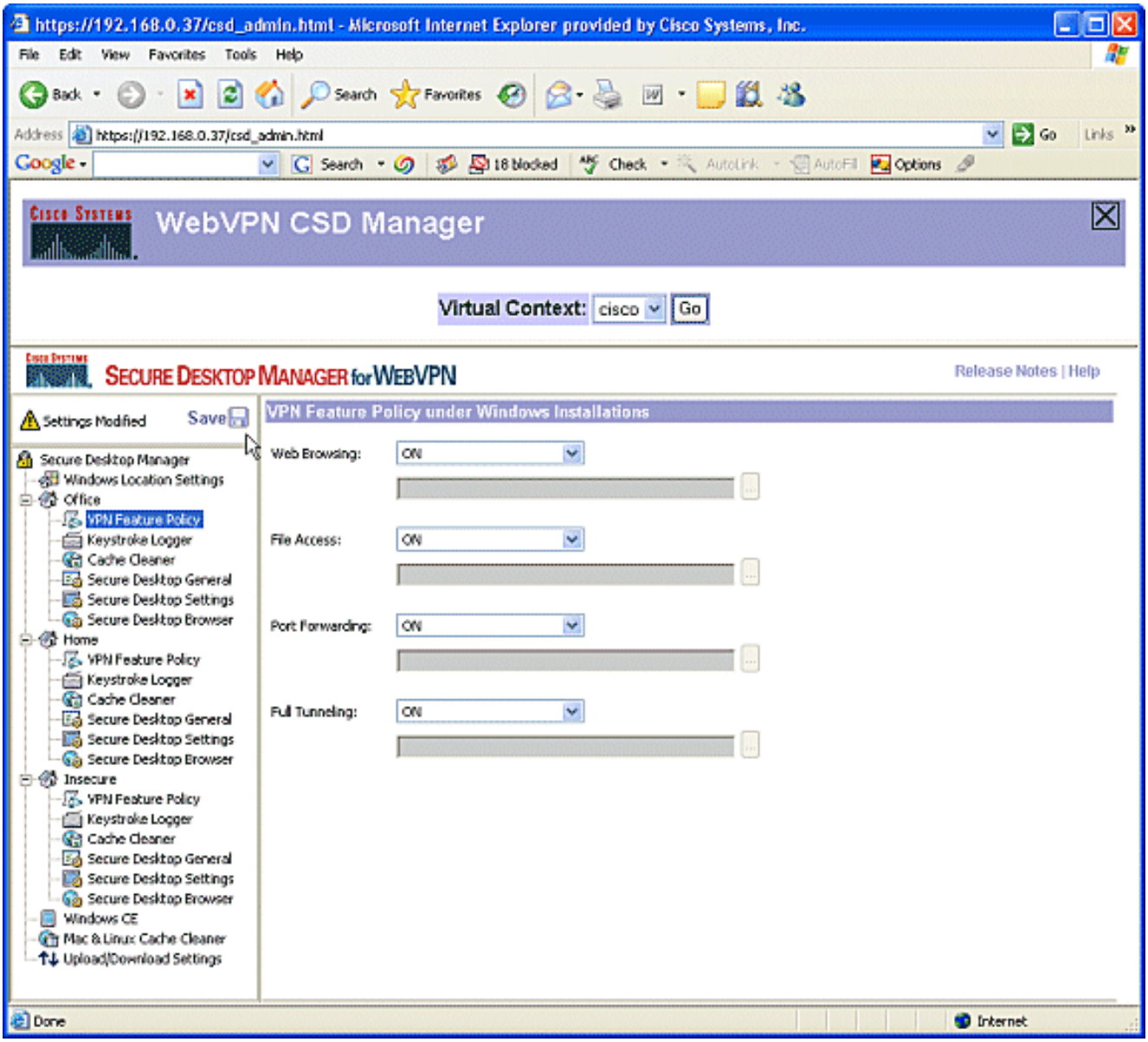
4. 要配置Insecure位置的標識，請不要應用任何標識標準。在左窗格中按一下Insecure。取消選中所有條件。選中Use Module:安全案頭。出現提示時，按一下Save，然後按一下OK。



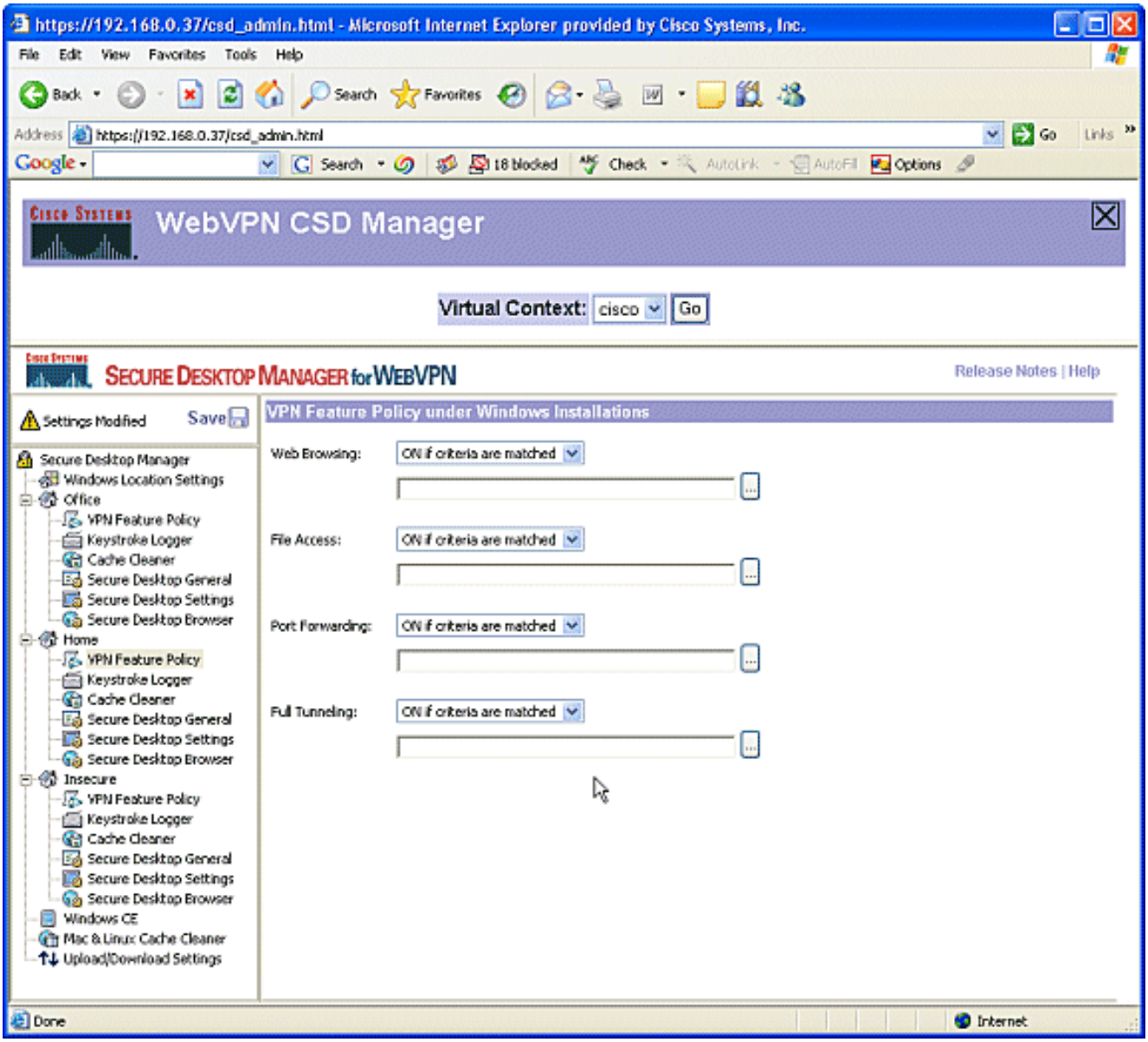
第二階段：步驟3:配置Windows位置模組和功能。

為每個Windows位置配置CSD功能。

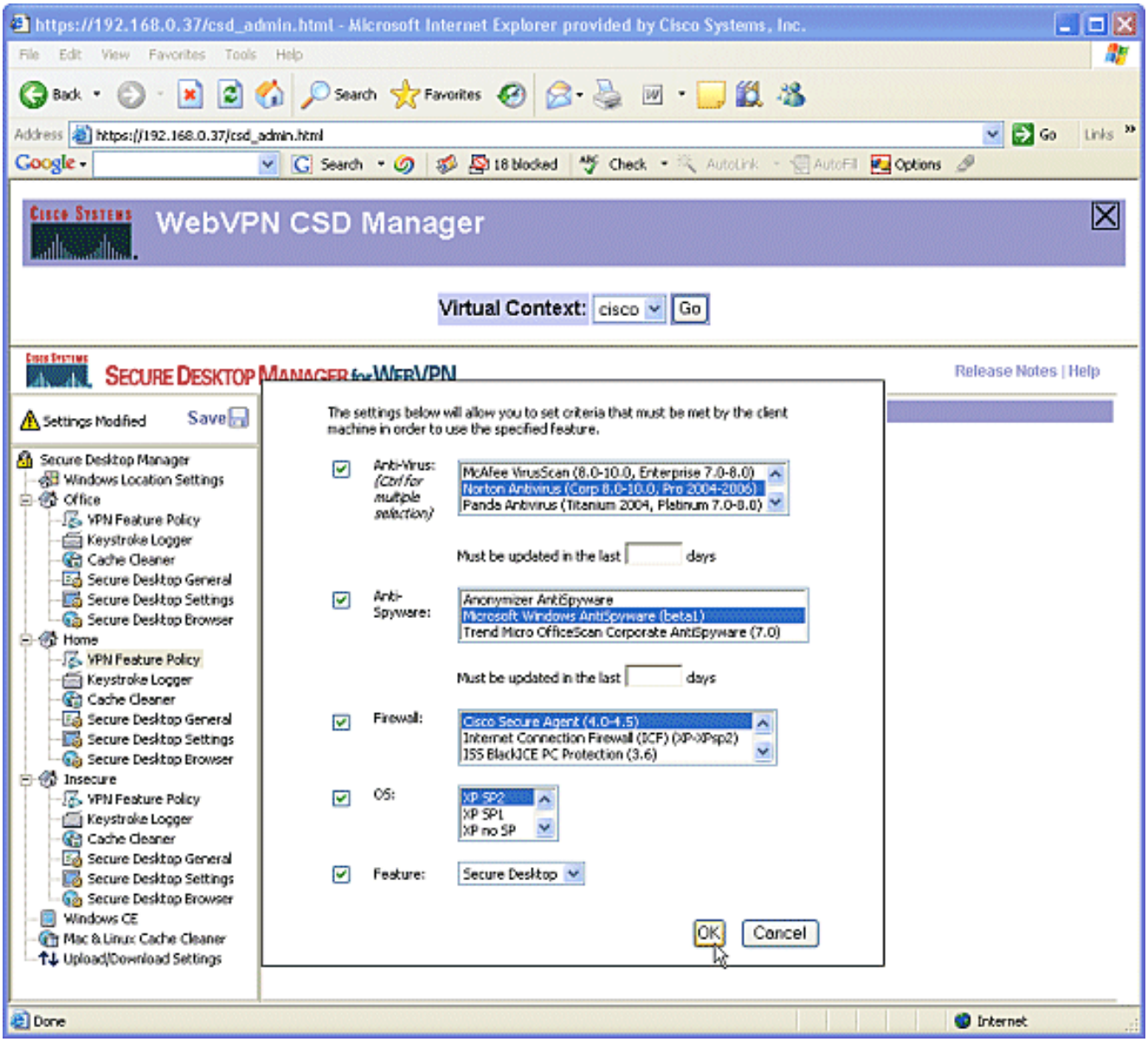
1. 在**Office**下，按一下**VPN Feature Policy**。由於這些客戶端是受信任的內部客戶端，因此既未啟用CSD也未啟用Cache Cleaner。其他引數均不可用。



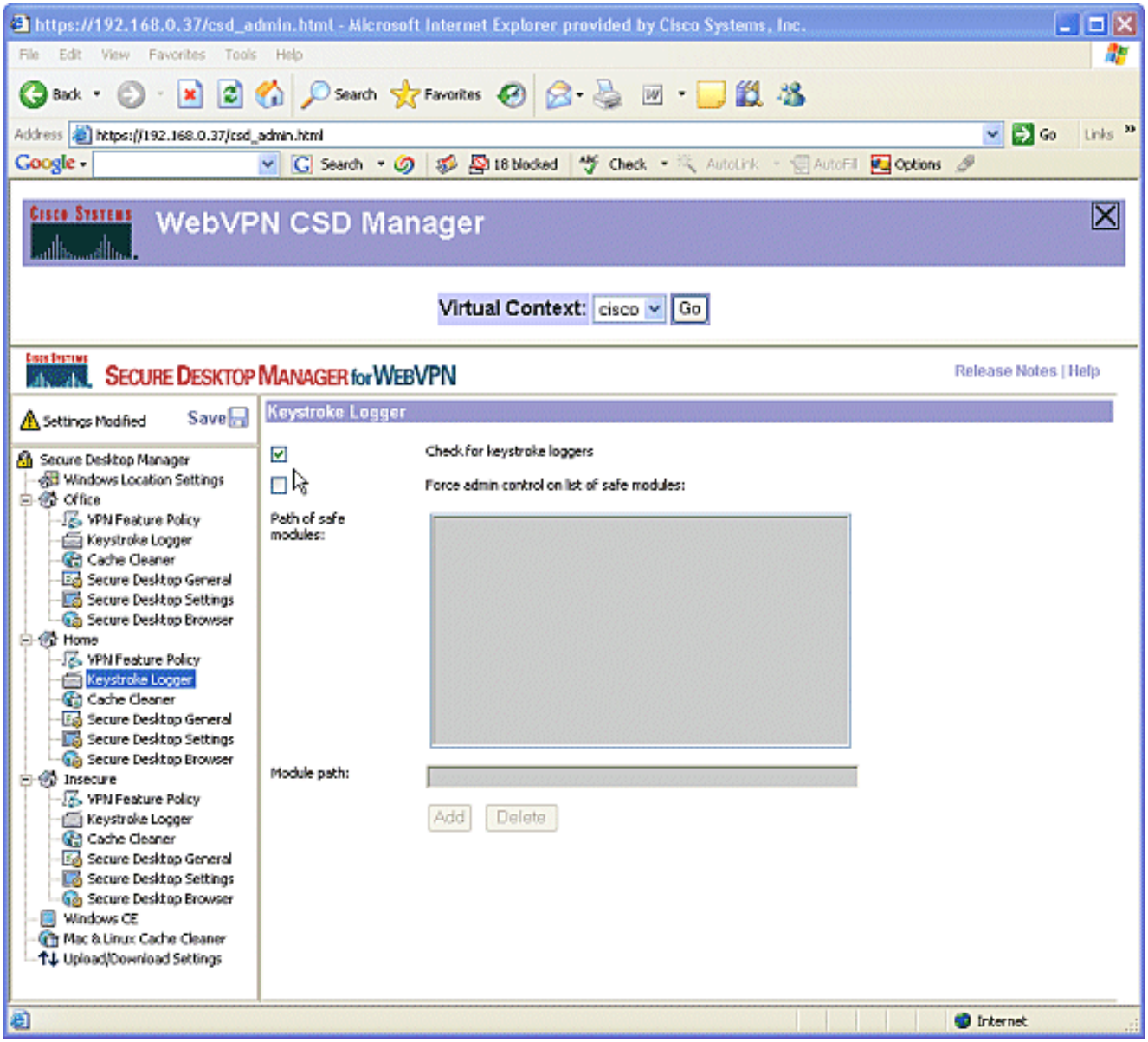
2. 如圖所示開啟功能。在左窗格中，選擇**Home**下的**VPN Feature Policy**。如果客戶端滿足特定標準，家庭使用者將可以訪問公司LAN。在每種訪問方法下，如果條件匹配，請選擇**ON**。



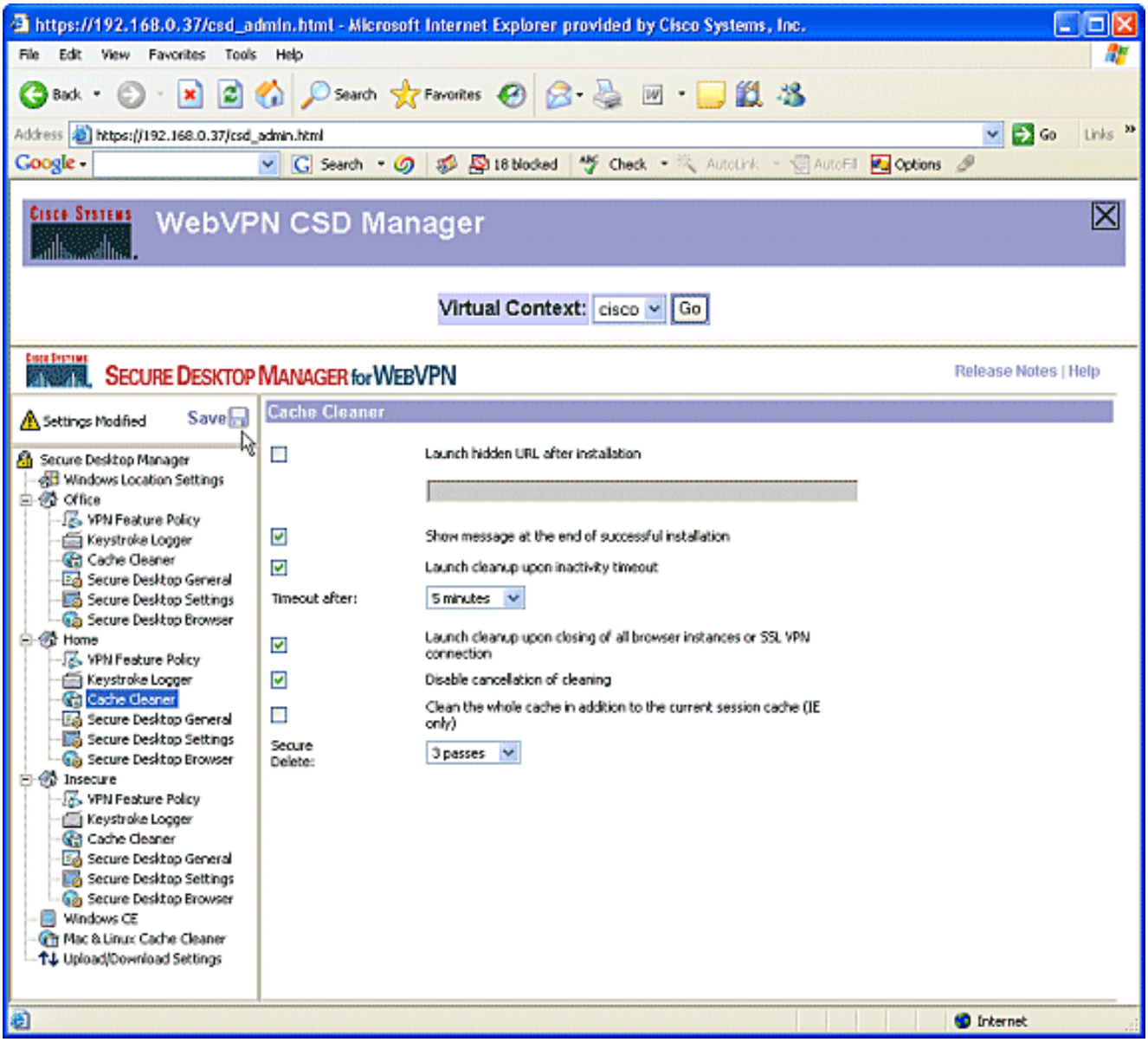
3. 對於Web瀏覽，按一下省略號按鈕並選擇必須匹配的條件。在對話方塊中按一下**OK**。



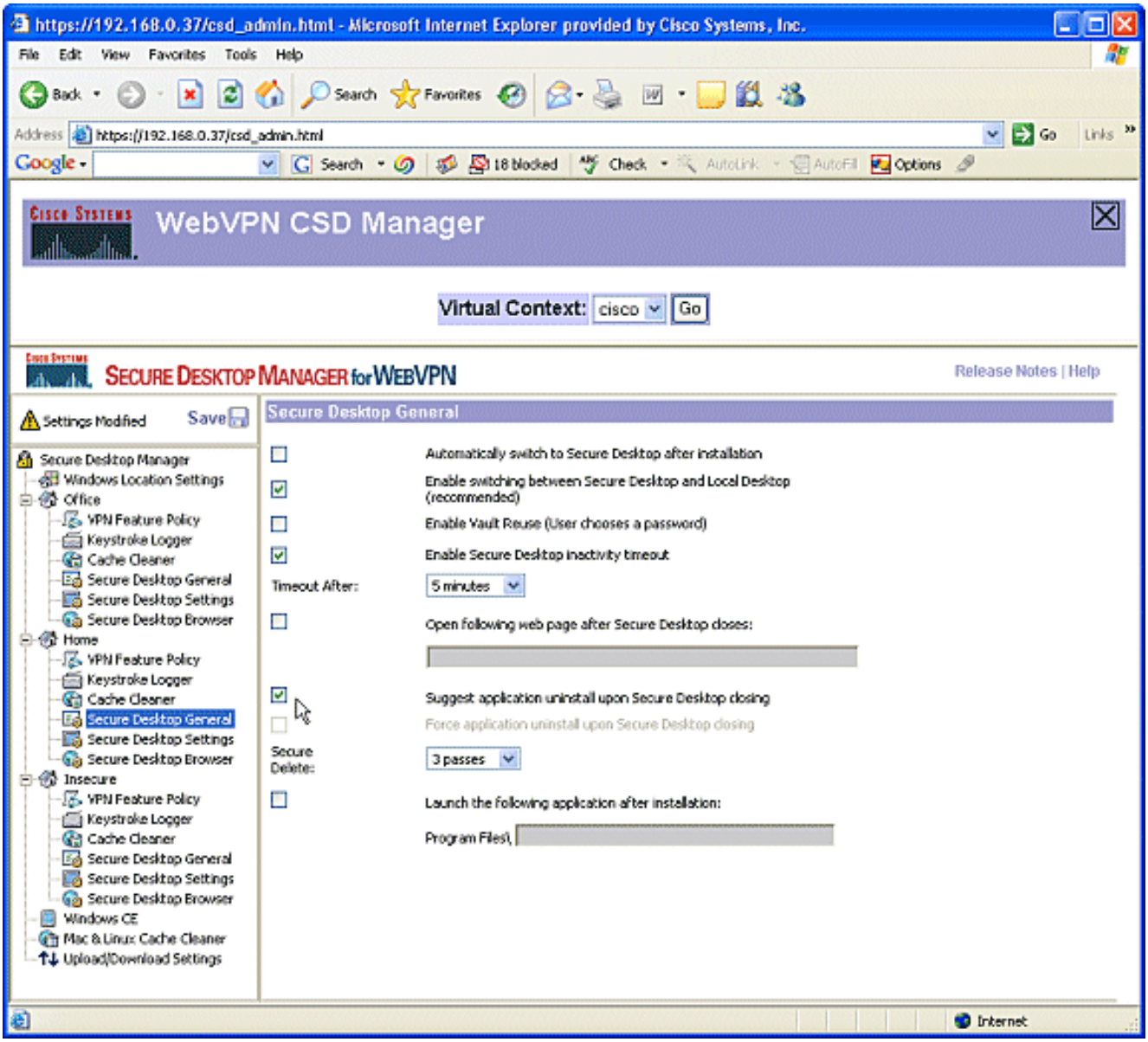
4. 您可以以類似的方式配置其他訪問方法。在**Home**下，選擇**Keystroke Logger**。在**Check for keystroke loggers**旁邊放置一個複選標籤。出現提示時，按一下**Save**，然後按一下**OK**。



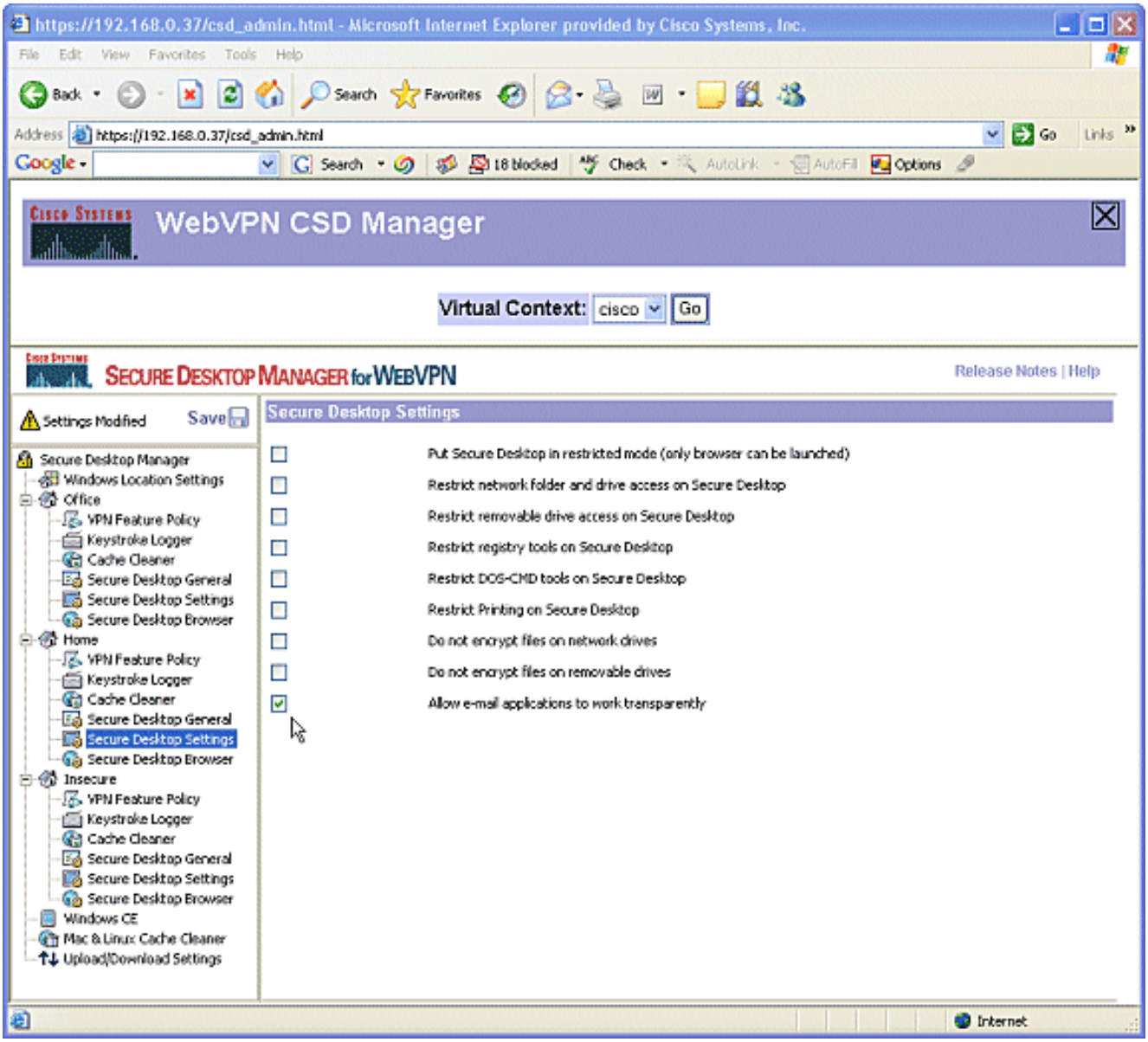
5. 在「首頁」視窗位置下，選擇**「快取清除器」**。保留預設設定如螢幕截圖所示。



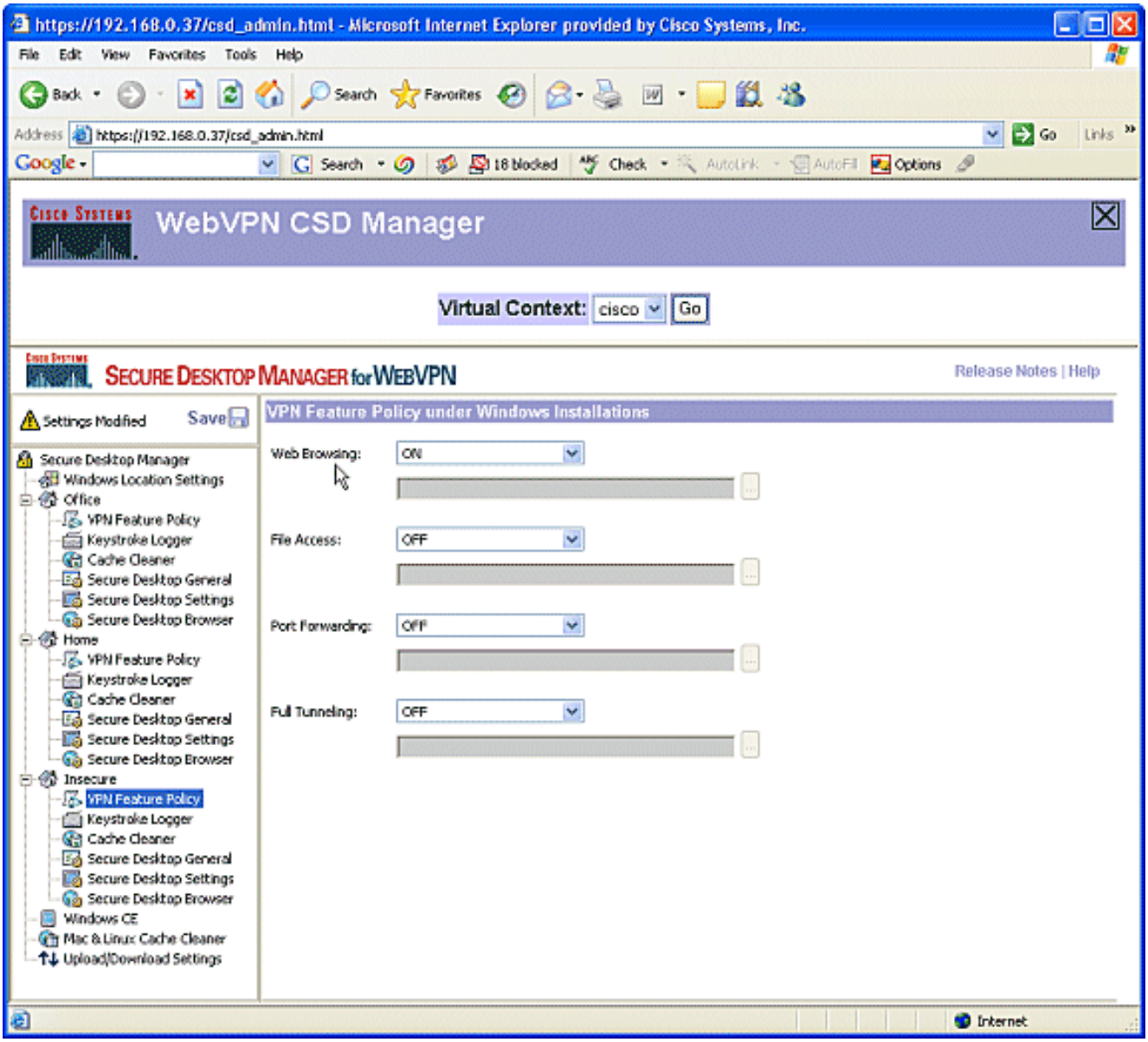
6. 在Home下，選擇**Secure Desktop General**。選中**在Secure Desktop關閉時建議解除安裝應用程式**。將所有其它引數保留為其預設設定，如螢幕截圖所示。



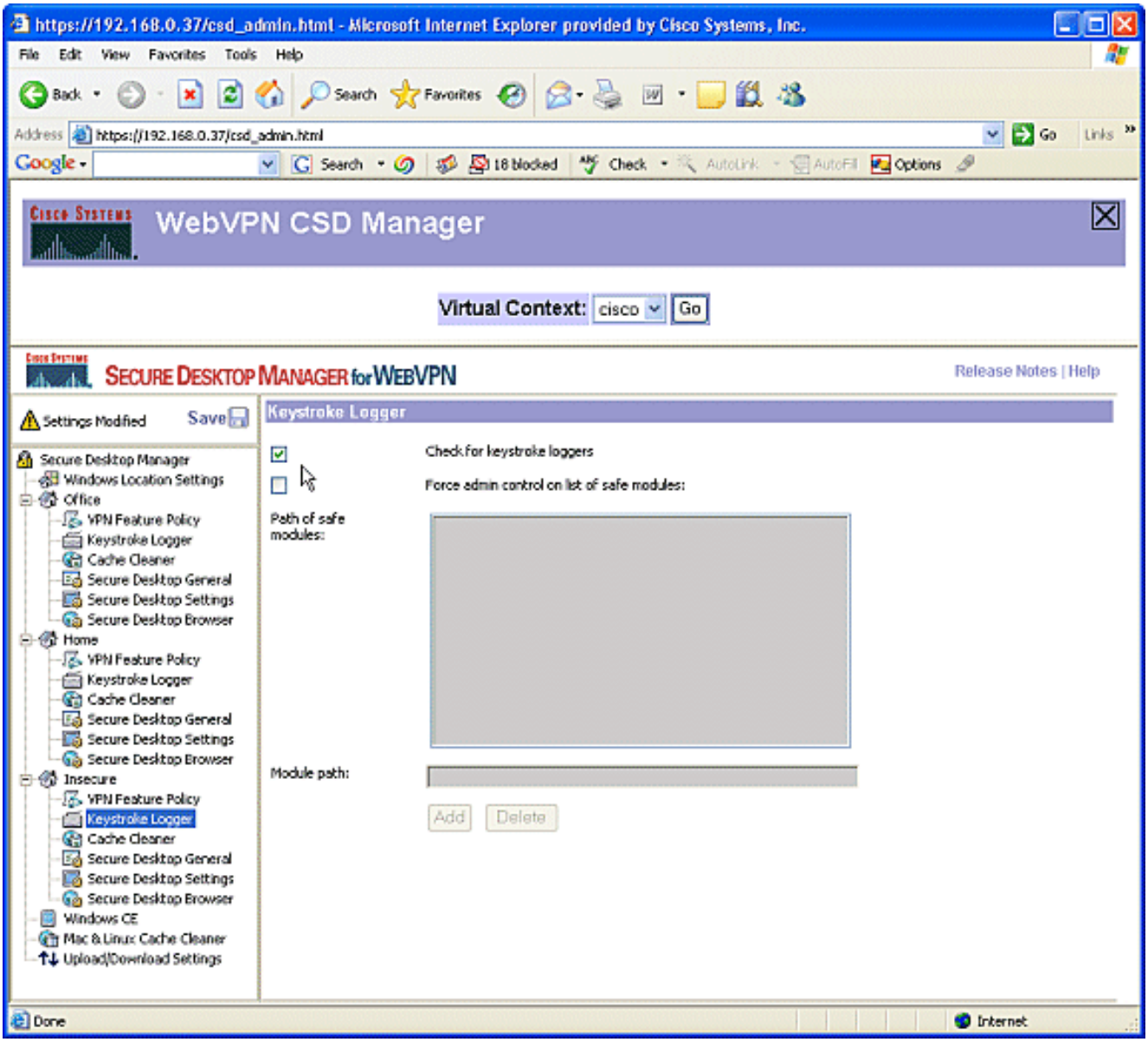
7. 對於「首頁」下的「安全案頭設定」，請選擇**「允許電子郵件應用程式透明工作」**。出現提示時，按一下**Save**，然後按一下**OK**。



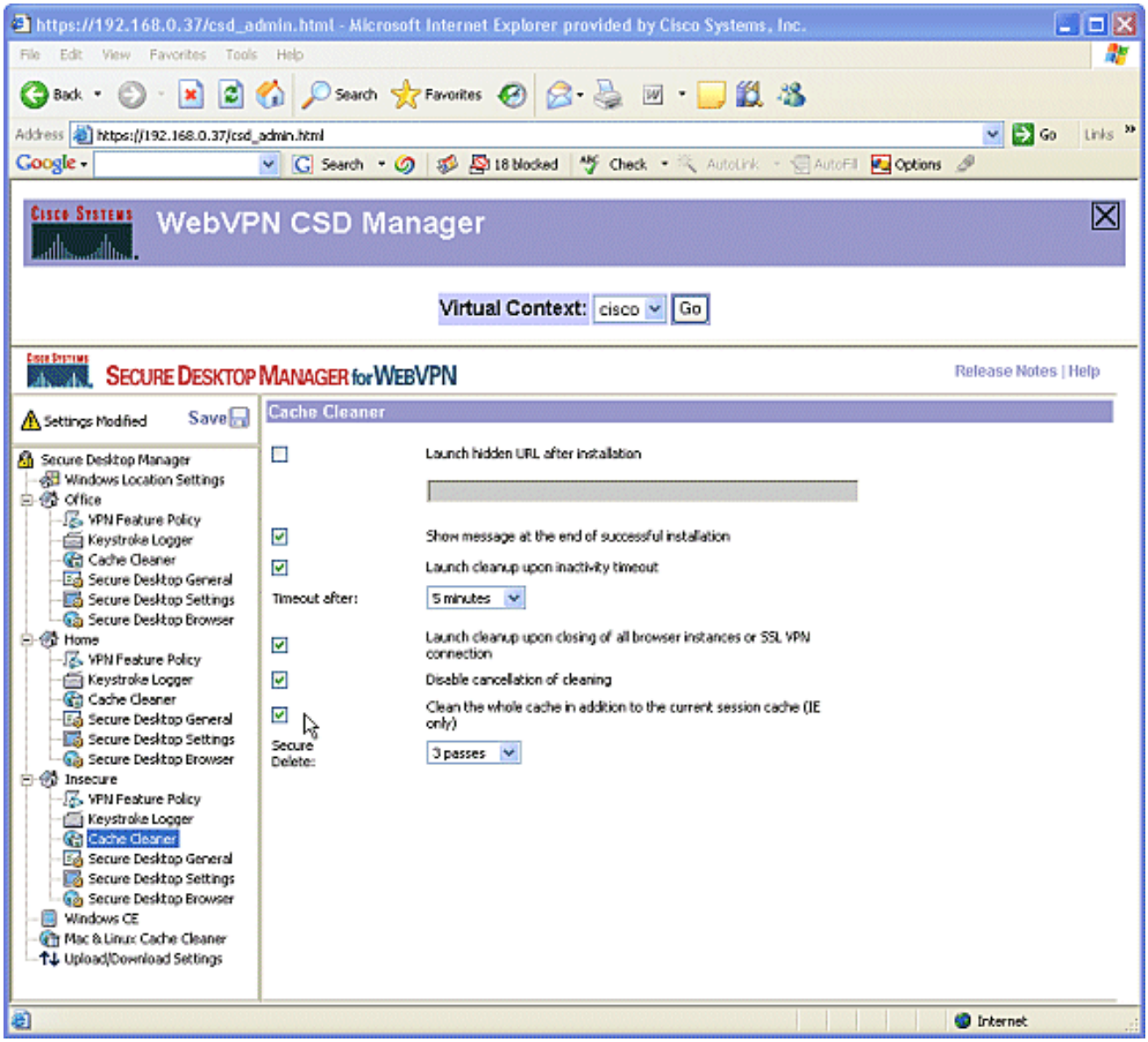
8. Secure Desktop Browser的配置取決於您是否希望這些使用者訪問具有預配置收藏夾的公司網站。在Insecure下，選擇VPN Feature Policy。由於這些使用者不可信，因此僅允許Web瀏覽。從Web Browsing下拉選單中選擇ON。所有其他訪問均設定為OFF。



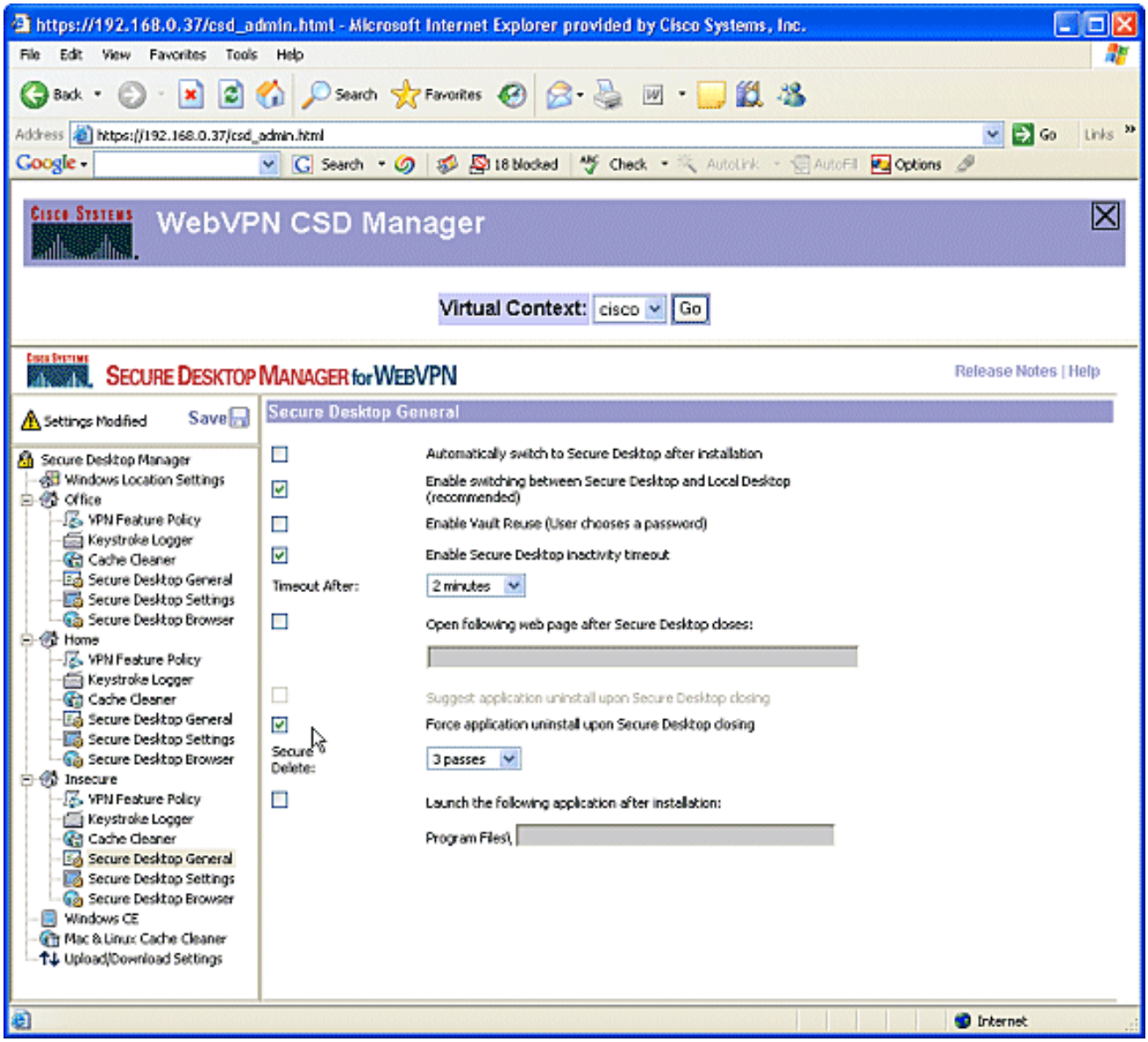
9. 選中**檢查按鍵記錄器**覈取方塊。



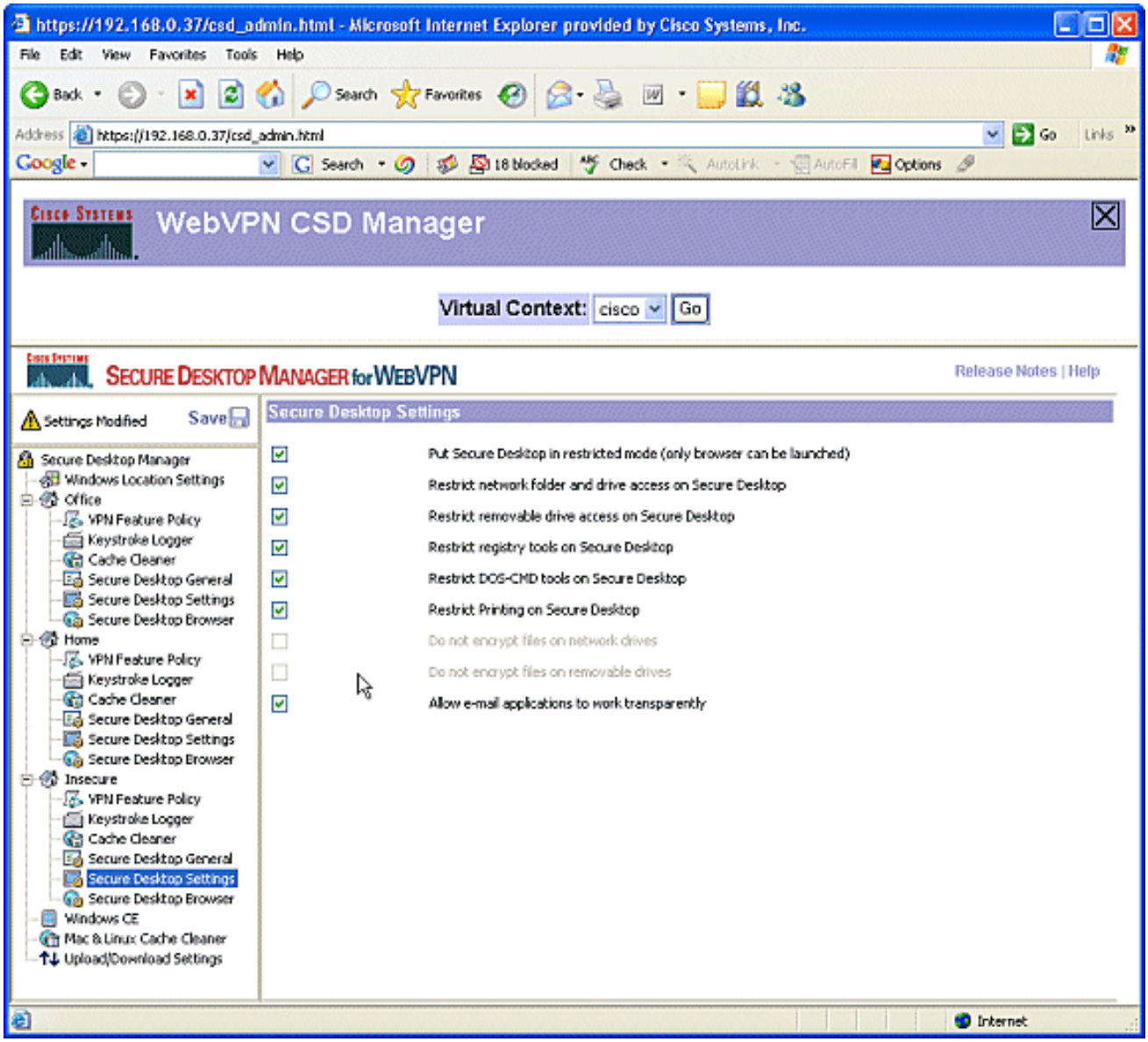
10. 為Insecure配置快取清理程式。選中**Clean the whole cache into the current session cache(IE only)**覈取方塊。將其他設定保留為預設值。



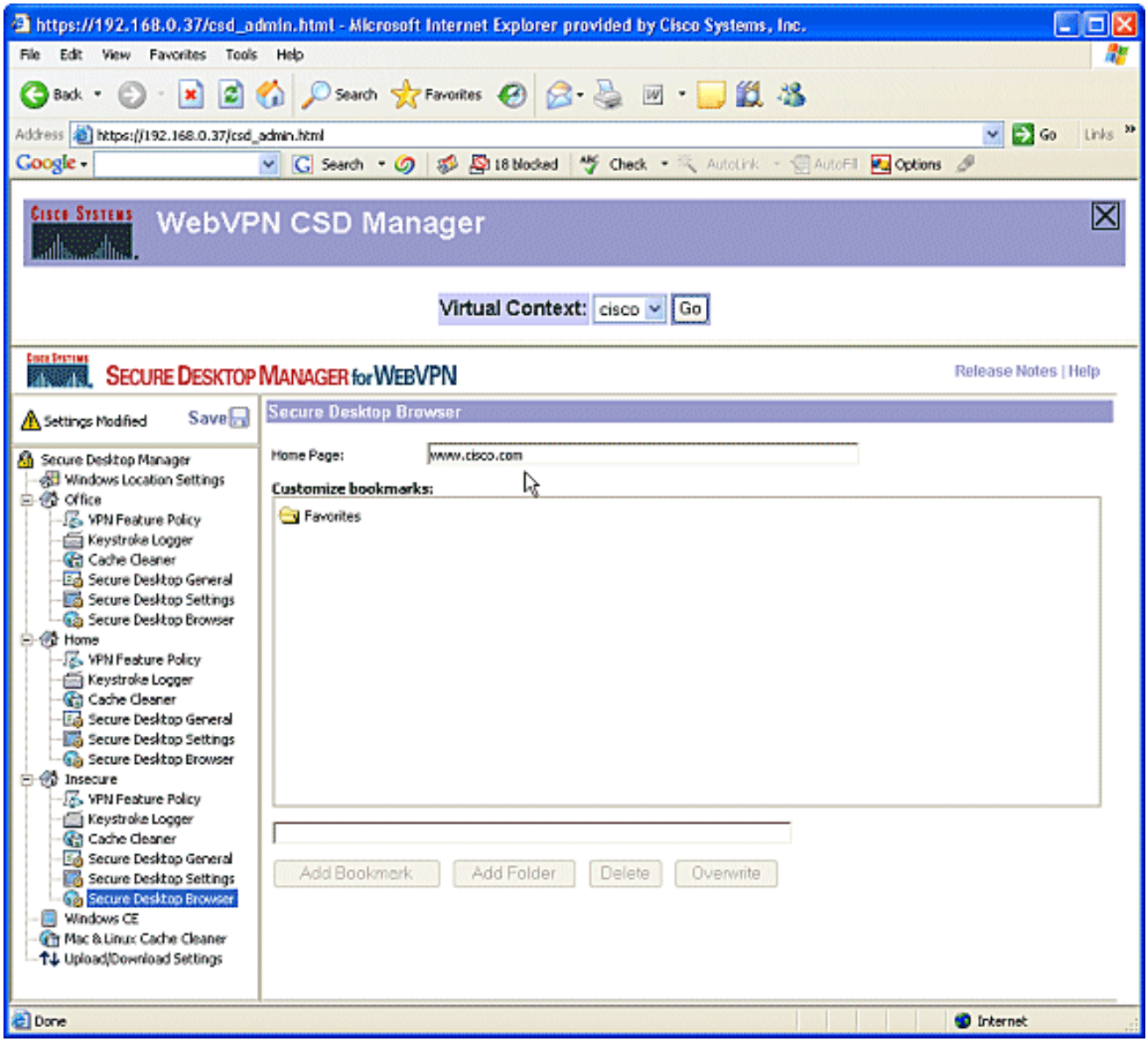
11. 在Insecure下，選擇**Secure Desktop General**。將超時非活動時間縮短為2分鐘。選中**Force application uninstall upon Secure Desktop closing**覈取方塊。



12. 在Insecure下選擇**Secure Desktop Settings**，然後配置非常嚴格的設定，如下所示。



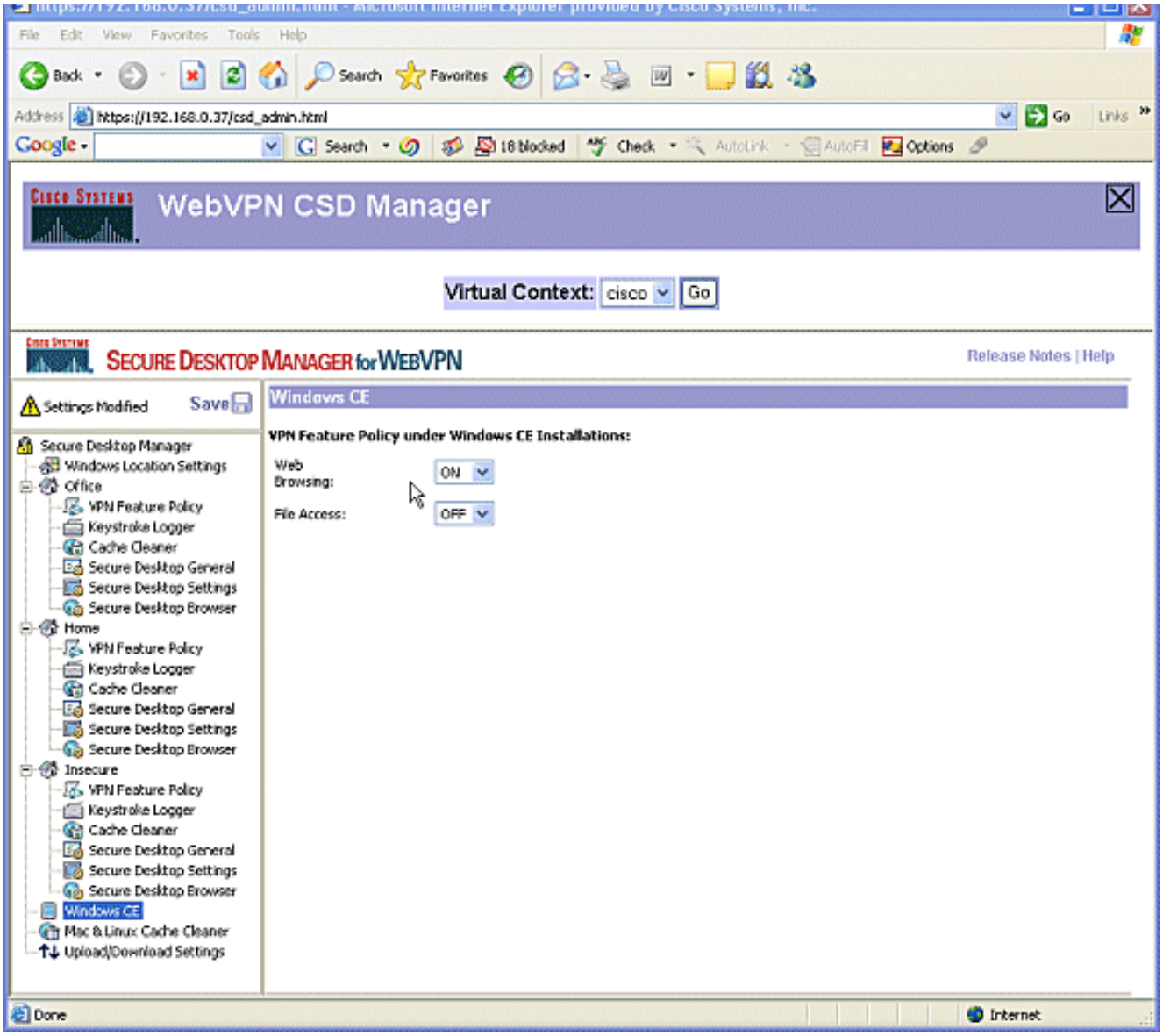
13. 選擇**Secure Desktop Browser**。在Home Page欄位中，輸入這些客戶端的首頁將引導到的網站。



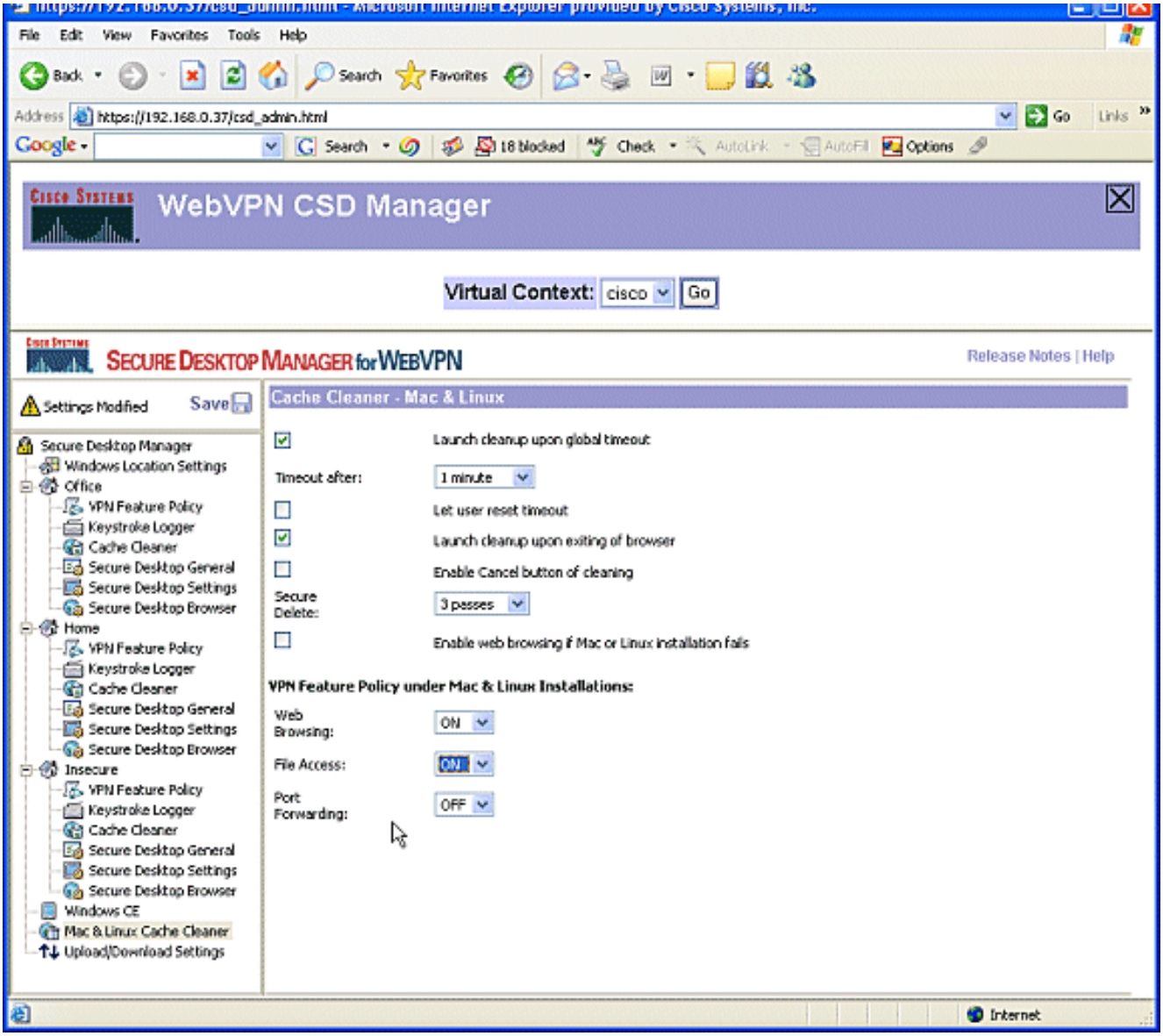
第二階段：第4步：配置Windows CE、Macintosh和Linux功能。

為Windows CE、Macintosh和Linux配置CSD功能。

1. 在Secure Desktop Manager下選擇**Windows CE**。Windows CE的VPN功能有限。將**Web Browsing設定為ON**。



2. 選擇**Mac & Linux Cache Cleaner**。Macintosh和Linux作業系統只能訪問CSD的快取清理器方面。如圖所示配置。出現提示時，按一下**Save**，然後按一下**OK**。

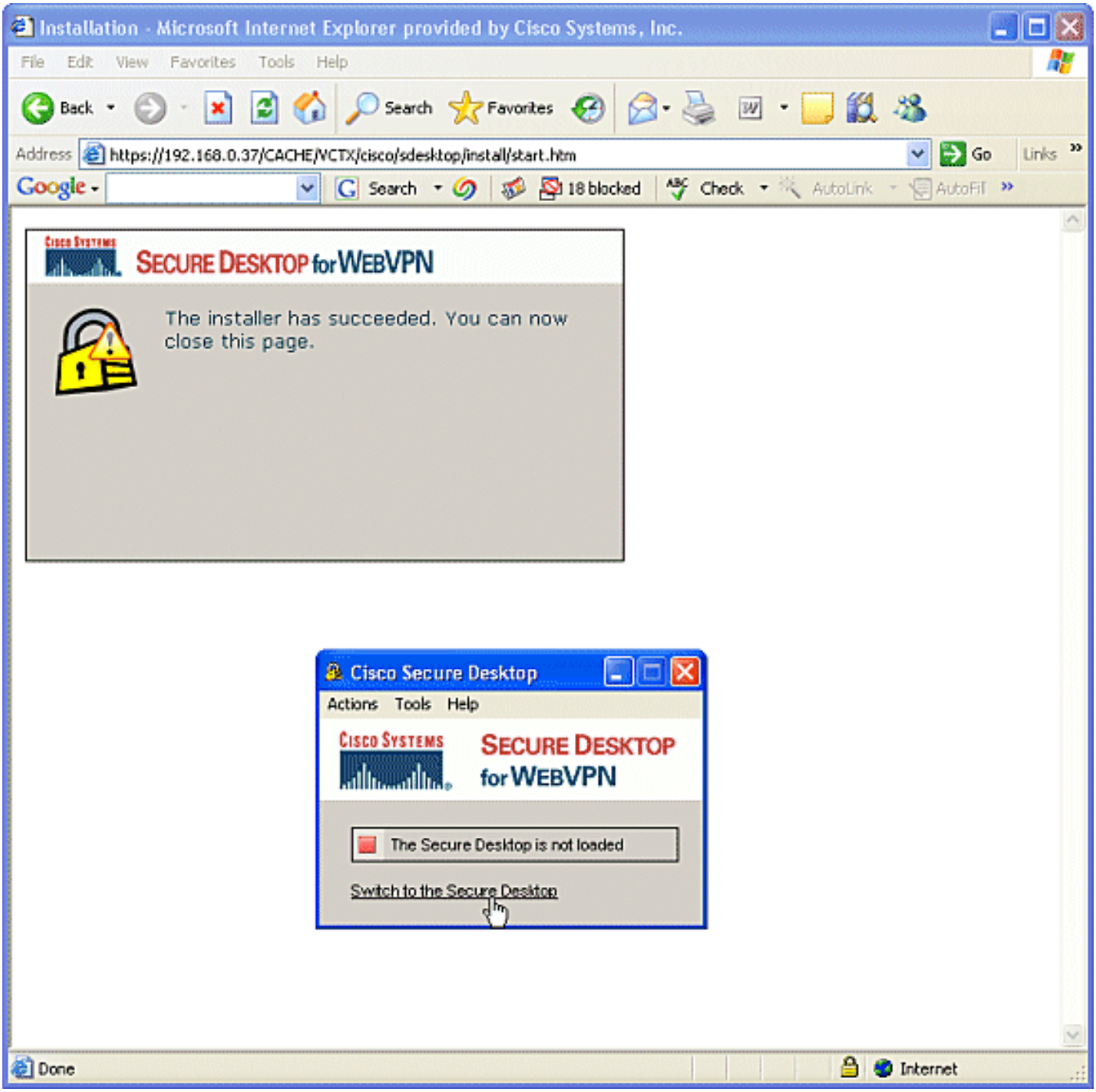


驗證

測試CSD操作

使用啟用了SSL的瀏覽器連線到WebVPN網關(地址為**https://WebVPN_Gateway_IP**)，測試CSD的運行。

注意：如果您建立了不同的WebVPN上下文，請記住使用上下文的唯一名稱，例如**https://192.168.0.37/cisco**。



指令

有幾個**show**命令與WebVPN關聯。您可以在命令列介面(CLI)上執行這些命令，以顯示統計資訊和其他資訊。有關**show**命令的詳細資訊，請參閱驗證WebVPN配置。

注意：CLI Analyzer(僅供已註冊客戶使用)支援某些**show**命令。使用CLI Analyzer檢視**show**指令輸出的分析。

疑難排解

指令

有幾個**debug**命令與WebVPN關聯。有關這些命令的詳細資訊，請參閱使用WebVPN Debug命令。

注意：使用**debug**指令可能會對思科裝置造成負面影響。使用**debug**指令之前，請先參閱有關Debug指令的重要資訊。

有關**clear**命令的詳細資訊，請參閱使用WebVPN Clear命令。

相關資訊

- **WebVPN和DMVPN融合部署指南**
- **SSL VPN - WebVPN**
- **Cisco IOS SSLVPN**
- **技術支援與文件 - Cisco Systems**