Cisco Secure Desktop (CSD) auf IOS - Konfigurationsbeispiel mit SDM

Inhalt

Einführung

Obwohl Secure Sockets Layer (SSL) VPN-Sitzungen (Cisco WebVPN) sicher sind, verfügt der Client möglicherweise weiterhin über Cookies, Browserdateien und E-Mail-Anhänge, die nach Abschluss einer Sitzung verbleiben. Cisco Secure Desktop (CSD) erweitert die inhärente Sicherheit von SSL VPN-Sitzungen, indem Sitzungsdaten in verschlüsselter Form in einen speziellen *Vault*-Bereich auf der Client-Festplatte geschrieben werden. Darüber hinaus werden diese Daten am Ende der SSL VPN-Sitzung von der Festplatte entfernt. Dieses Dokument enthält eine Beispielkonfiguration für CSD auf einem Cisco IOS®-Router.

Der CSD wird auf den folgenden Cisco Geräteplattformen unterstützt:

- Cisco IOS Router Version 12.4(6)T und höher
- Cisco 870, 1811, 1841, 2801, 2811, 2821, 2851, 3725, 3745, 3825, 3845, 7200 und 730 1 Router
- Cisco VPN Concentrators der Serie 3000 ab Version 4.7

- Cisco Security Appliances der Serie ASA 5500 ab Version 7.1
- Cisco WebVPN Services Module für Cisco Catalyst und Cisco Serie 7600, Version 1.2 und höher

Voraussetzungen

Anforderungen

Stellen Sie sicher, dass Sie diese Anforderungen erfüllen, bevor Sie versuchen, diese Konfiguration durchzuführen:

Anforderungen für den Cisco IOS-Router

- Cisco IOS-Router mit Advanced Image 12.4(6T) oder höher
- Cisco Router Secure Device Manager (SDM) 2.3 oder höher
- Eine Kopie des CSD für IOS-Pakets auf Ihrer Managementkonsole
- Ein selbstsigniertes digitales Zertifikat oder eine Authentifizierung mit einer Zertifizierungsstelle (Certificate Authority, CA)**Hinweis:** Stellen Sie bei jeder Verwendung digitaler Zertifikate sicher, dass Sie den Hostnamen, den Domänennamen und das Datum/die Uhrzeit/die Zeitzone des Routers korrekt festgelegt haben.
- Ein enable secret-Kennwort auf dem Router
- DNS auf Ihrem Router aktiviert. Für mehrere WebVPN-Dienste muss DNS ordnungsgemäß funktionieren.

Anforderungen an Client-Computer

- Remote-Clients sollten über lokale Administratorberechtigungen verfügen. Sie ist nicht erforderlich, wird jedoch nachdrücklich empfohlen.
- Remote-Clients müssen über Java Runtime Environment (JRE) Version 1.4 oder höher verfügen.
- Remote-Client-Browser: Internet Explorer 6.0, Netscape 7.1, Mozilla 1.7, Safari 1.2.2 oder Firefox 1.0
- Cookies aktiviert und Popups auf Remote-Clients zugelassen

Verwendete Komponenten

Die Informationen in diesem Dokument basierend auf folgenden Software- und Hardware-Versionen:

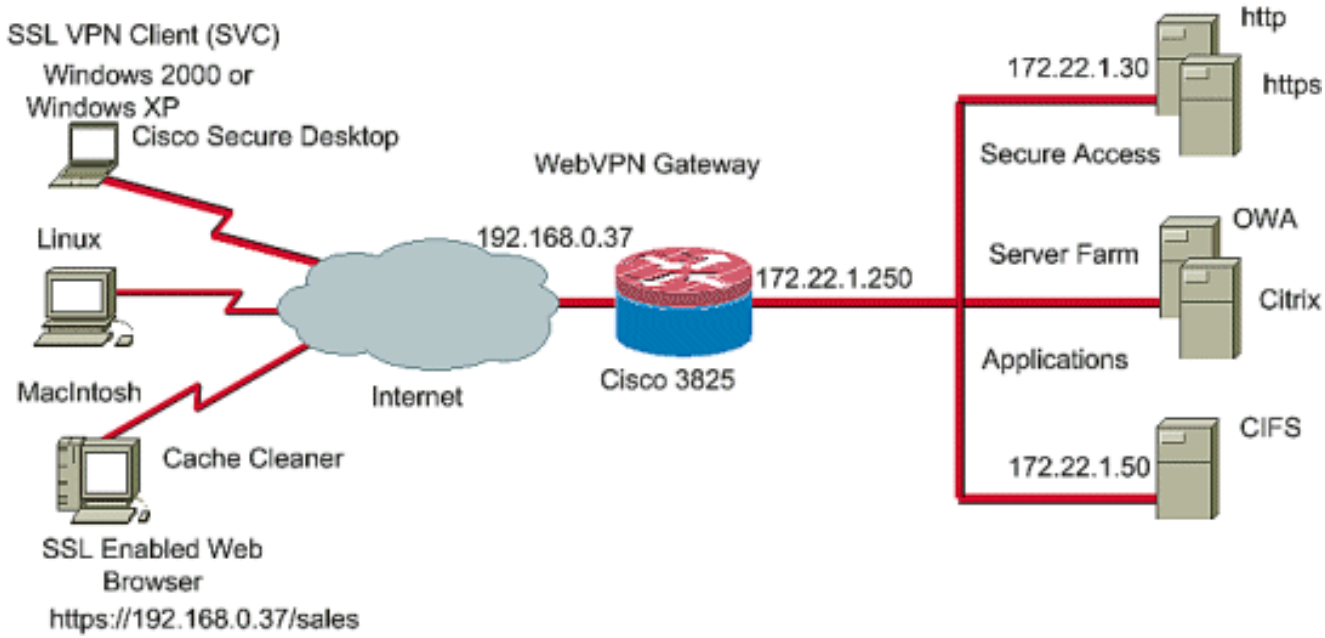
- Cisco IOS-Router 3825 mit Version 12.9(T)
- SDM Version 2.3.1

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle in diesem Dokument verwendeten Geräte begannen mit einer leeren (Standard-)Konfiguration. Wenn Ihr Netz Live ist, überprüfen Sie, ob Sie die mögliche Auswirkung jedes möglichen Befehls verstehen.

Netzwerkdiagramm

In diesem Dokument wird die folgende Netzwerkeinrichtung verwendet:

In diesem Beispiel wird ein Cisco Router der Serie 3825 verwendet, um den sicheren Zugriff auf das Intranet des Unternehmens zu ermöglichen. Der Cisco Router der Serie 3825 erhöht die Sicherheit von SSL VPN-Verbindungen durch konfigurierbare CSD-Funktionen und -Merkmale. Clients können über eine der folgenden drei SSL VPN-Methoden eine Verbindung zum CSD-fähigen Router herstellen: Clientless SSL VPN (WebVPN), Thin-Client SSL VPN (Port-Forwarding) oder SSL VPN Client (Full Tunneling SVC).



Verwandte Produkte

Diese Konfiguration kann auch mit den folgenden Hardware- und Softwareversionen verwendet werden:

- Cisco Router-Plattformen 870,1811,1841,2801,2811,2821 2851,3725,3745.3825,3845, 7200 und 73 01
- Cisco IOS Advanced Security Image Version 12.4(6)T und höher

Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie in den Cisco Technical Tips Conventions (Technische Tipps zu Konventionen von Cisco).

Konfiguration

Ein WebVPN-Gateway ermöglicht es Benutzern, über eine der SSL VPN-Technologien eine Verbindung zum Router herzustellen. Auf dem Gerät ist nur ein WebVPN-Gateway pro IP-Adresse zulässig, obwohl mehrere WebVPN-Kontexte an ein WebVPN-Gateway angeschlossen werden können. Jeder Kontext wird durch einen eindeutigen Namen identifiziert. Gruppenrichtlinien identifizieren die konfigurierten Ressourcen, die für einen bestimmten WebVPN-Kontext verfügbar sind.

Die Konfiguration des CSD auf einem IOS-Router erfolgt in zwei Phasen:

Phase I: Vorbereiten des Routers für die CSD-Konfiguration mit SDM

1. Konfigurieren eines WebVPN-Gateways, eines WebVPN-Kontexts und einer Gruppenrichtlinie.**Hinweis:** Dieser Schritt ist optional und wird in diesem Dokument nicht ausführlich behandelt. Wenn Sie Ihren Router bereits für eine der SSL VPN-Technologien konfiguriert haben, lassen Sie diesen Schritt aus.
2. Aktivieren Sie CSD in einem WebVPN-Kontext.

Phase II: Konfigurieren Sie den CSD mithilfe eines Webbrowsers.

1. Definieren Sie *Windows-Speicherorte*.
2. Identifizieren Sie Standortkriterien.
3. Konfigurieren Sie die Windows-Standortmodule und -Funktionen.
4. Konfigurieren der Funktionen von Windows CE, Macintosh und Linux.

Phase I: Bereiten Sie Ihren Router mit SDM auf die CSD-Konfiguration vor.

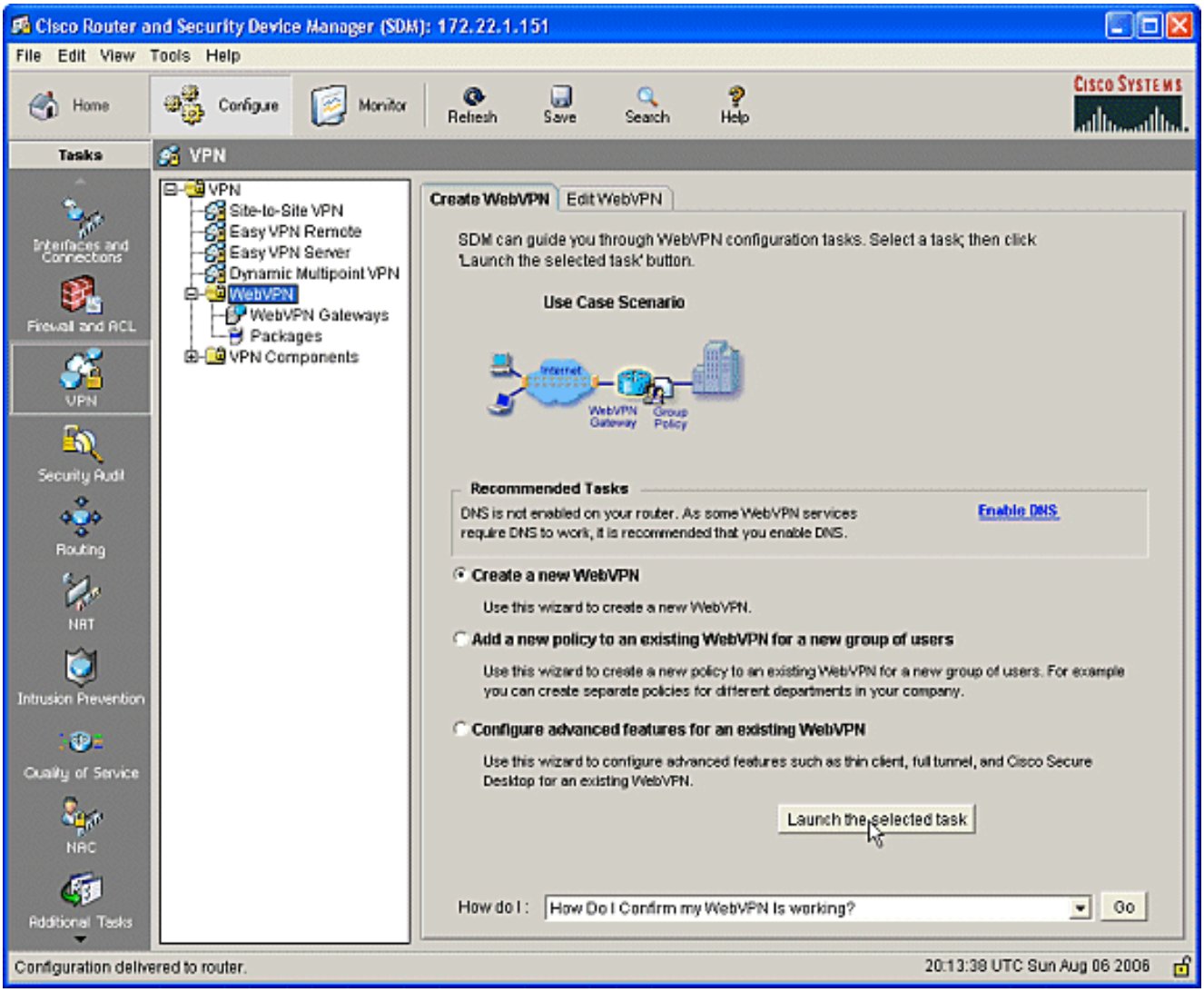
Der CSD kann mit SDM oder über die Befehlszeilenschnittstelle (CLI) konfiguriert werden. Diese Konfiguration verwendet SDM und einen Webbrowser.

Diese Schritte werden verwendet, um die Konfiguration des CSD auf Ihrem IOS-Router abzuschließen.

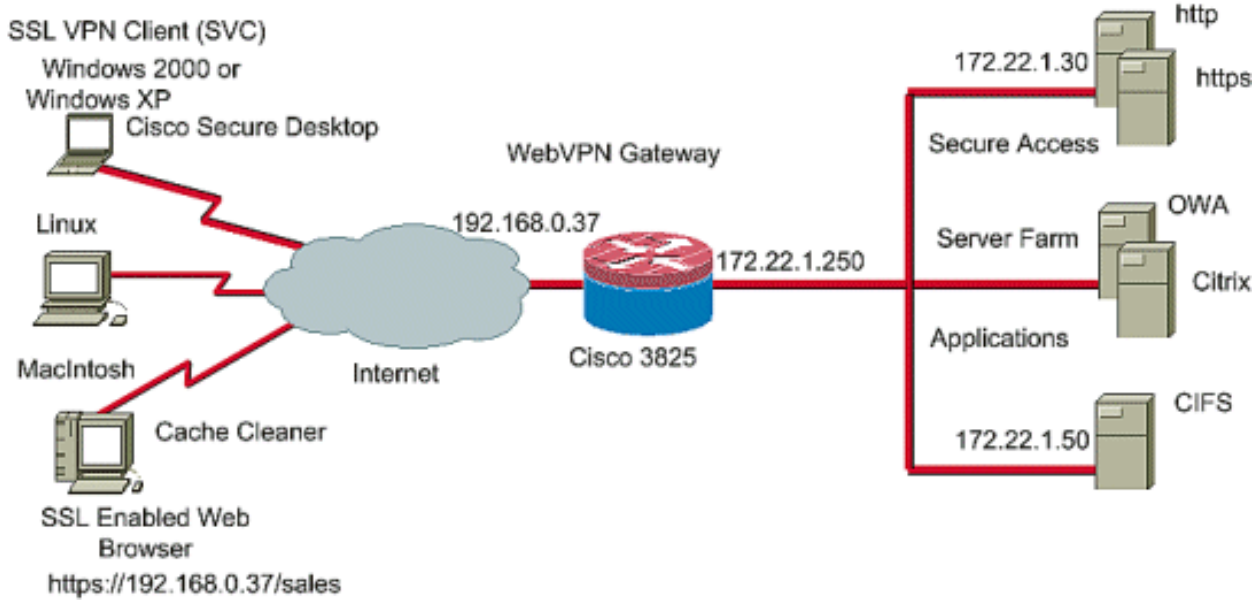
Phase I: Schritt 1: Konfigurieren eines WebVPN-Gateways, eines WebVPN-Kontexts und einer Gruppenrichtlinie

Sie können den WebVPN-Assistenten verwenden, um diese Aufgabe durchzuführen.

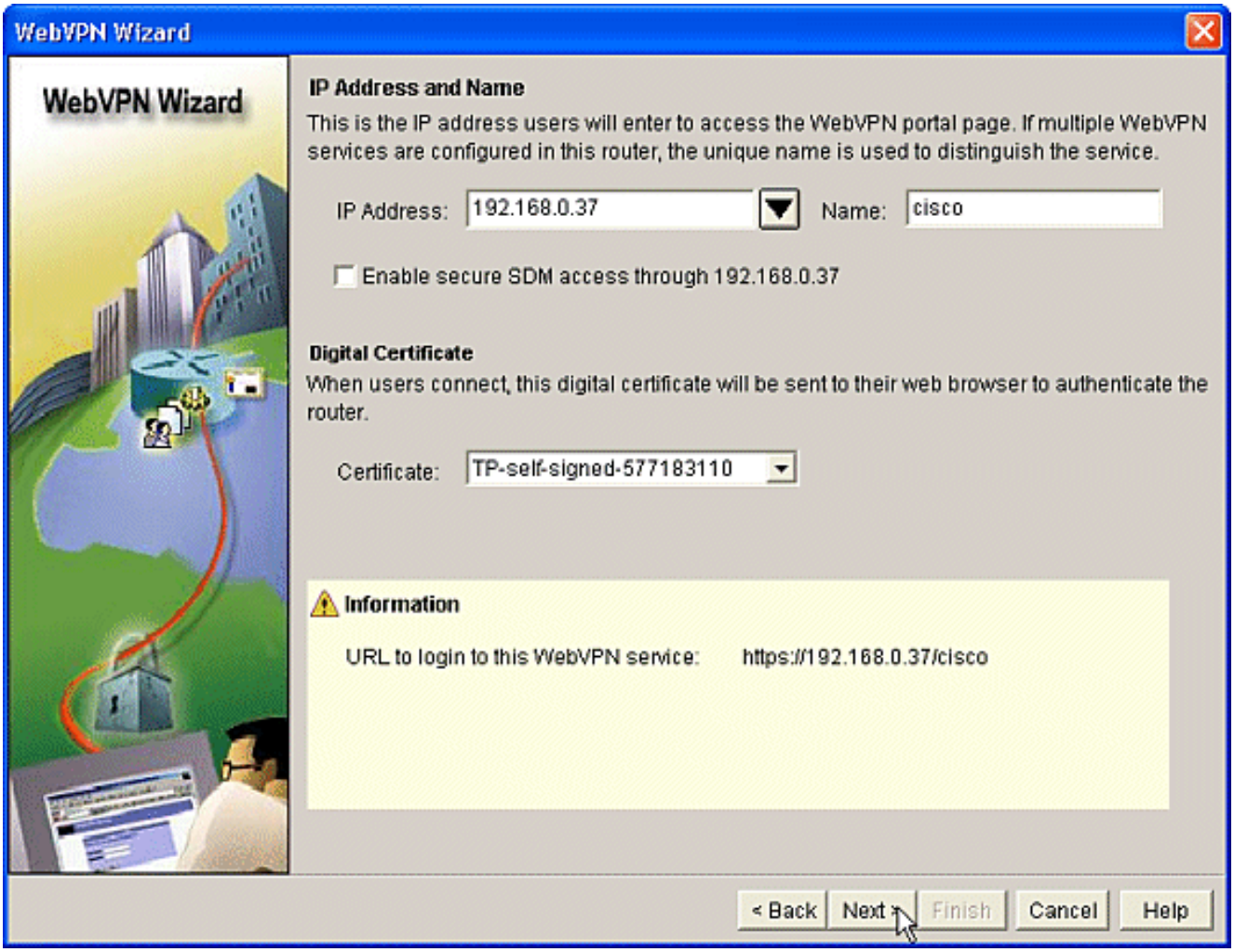
1. Öffnen Sie SDM, und wählen Sie **Configure > VPN > WebVPN aus**. Klicken Sie auf die Registerkarte **Create WebVPN (WebVPN erstellen)**, und aktivieren Sie das Optionsfeld **Create a new WebVPN (Neues WebVPN erstellen).** Klicken Sie auf **Ausgewählte Aufgabe starten**.



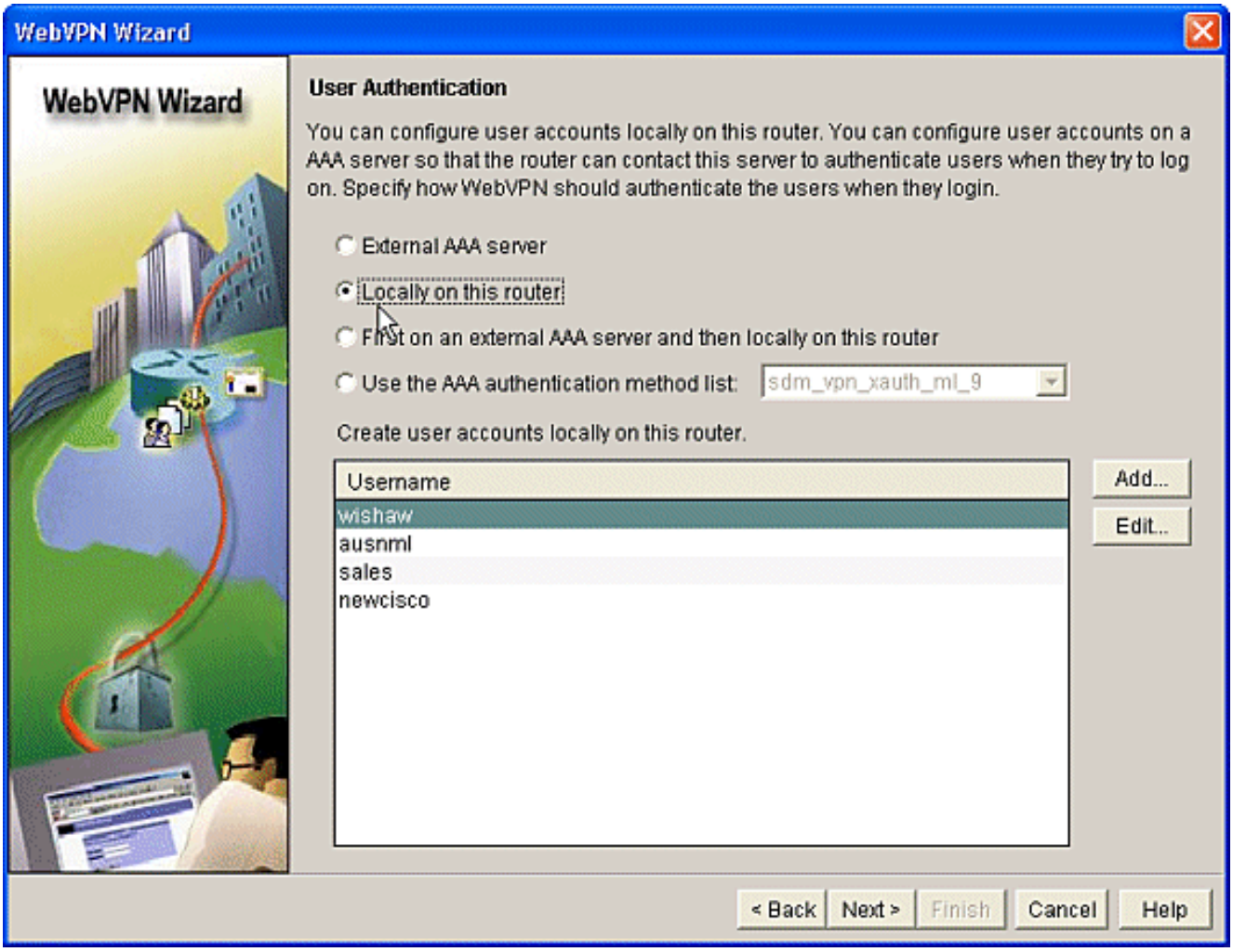
2. Im Bildschirm WebVPN Wizard (WebVPN-Assistent) werden die Parameter aufgelistet, die Sie konfigurieren können. Klicken Sie auf **Weiter**.



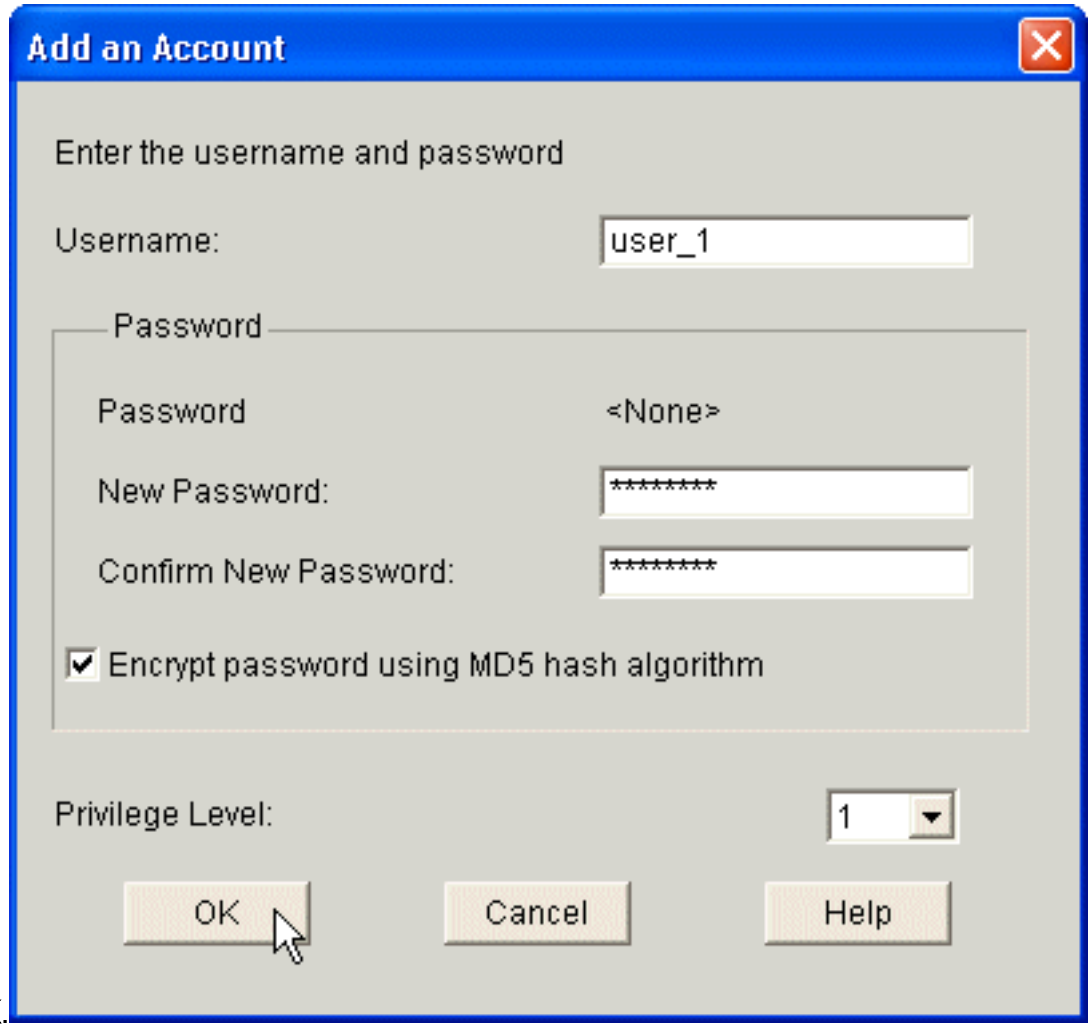
3. Geben Sie die IP-Adresse für das WebVPN-Gateway, einen eindeutigen Namen für den Dienst und Informationen zum digitalen Zertifikat ein. Klicken Sie auf **Weiter**.



4. Benutzerkonten können für die Authentifizierung zu diesem WebVPN-Gateway erstellt werden. Sie können lokale Konten oder Konten verwenden, die auf einem externen AAA-Server (Authentication, Authorization, Accounting) erstellt wurden. In diesem Beispiel werden lokale Konten auf dem Router verwendet. Aktivieren Sie das Optionsfeld **Lokal auf diesem Router** und klicken Sie auf **Hinzufügen**.

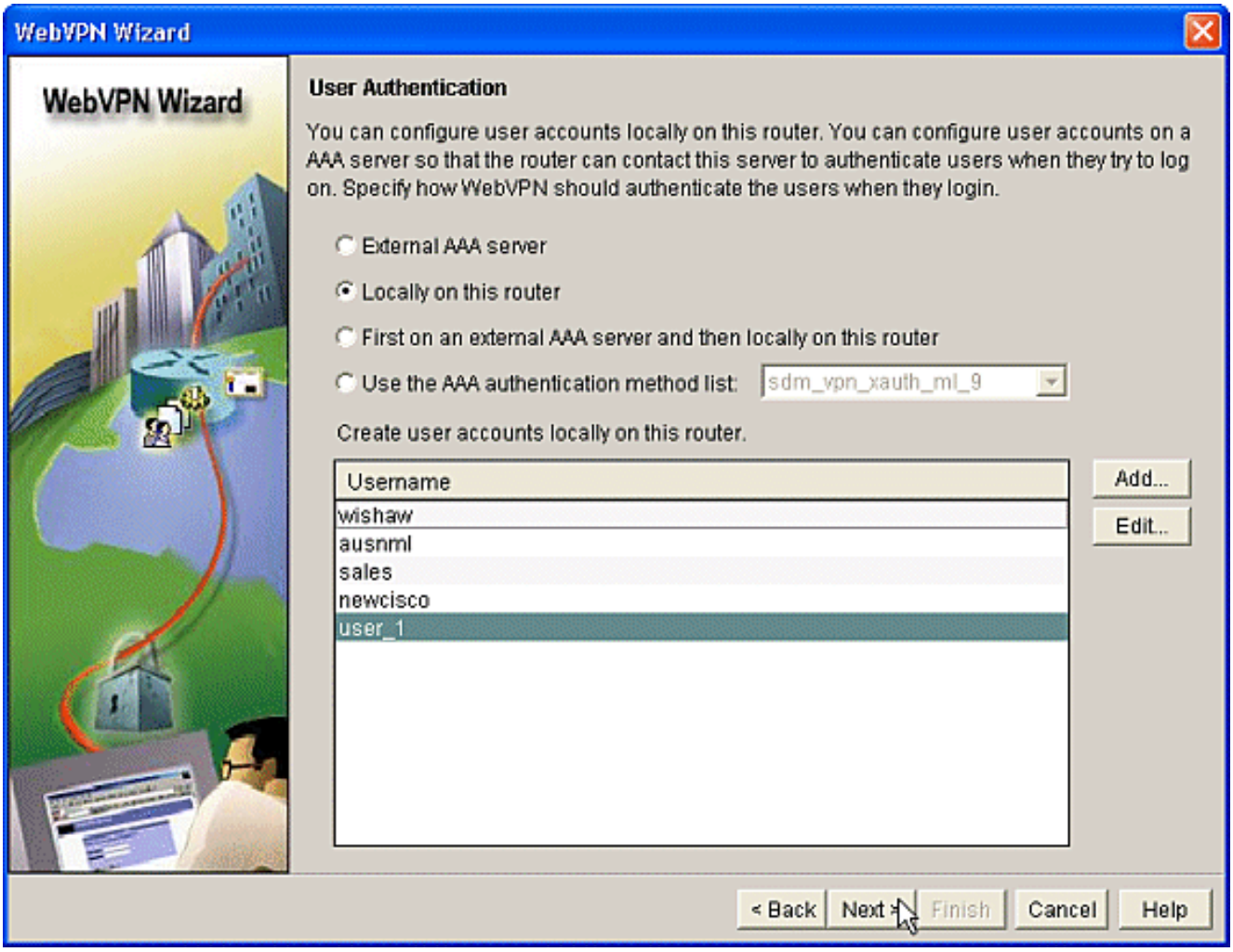


5. Geben Sie die Kontoinformationen für den neuen Benutzer im Bildschirm Konto hinzufügen ein, und klicken Sie auf

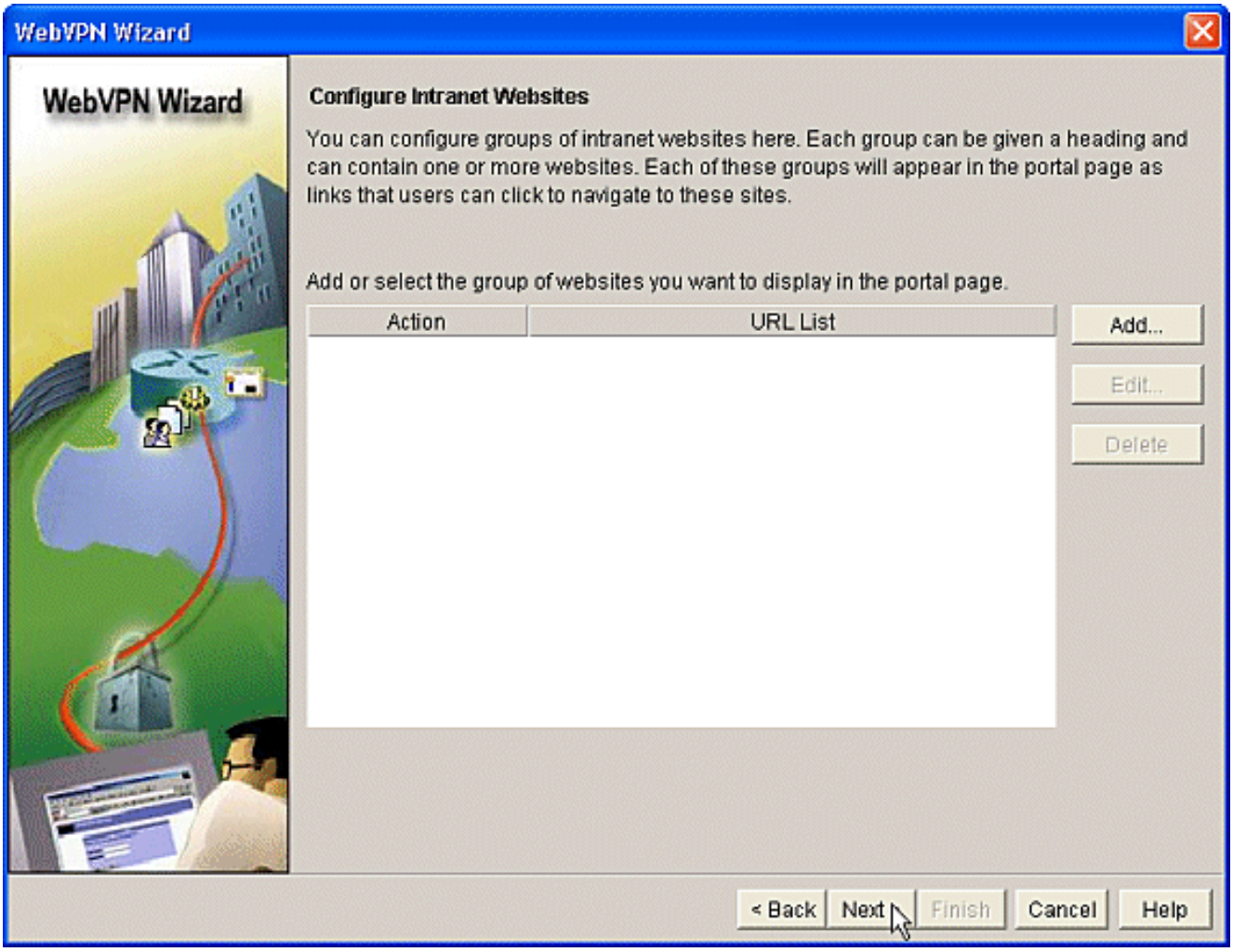


OK.

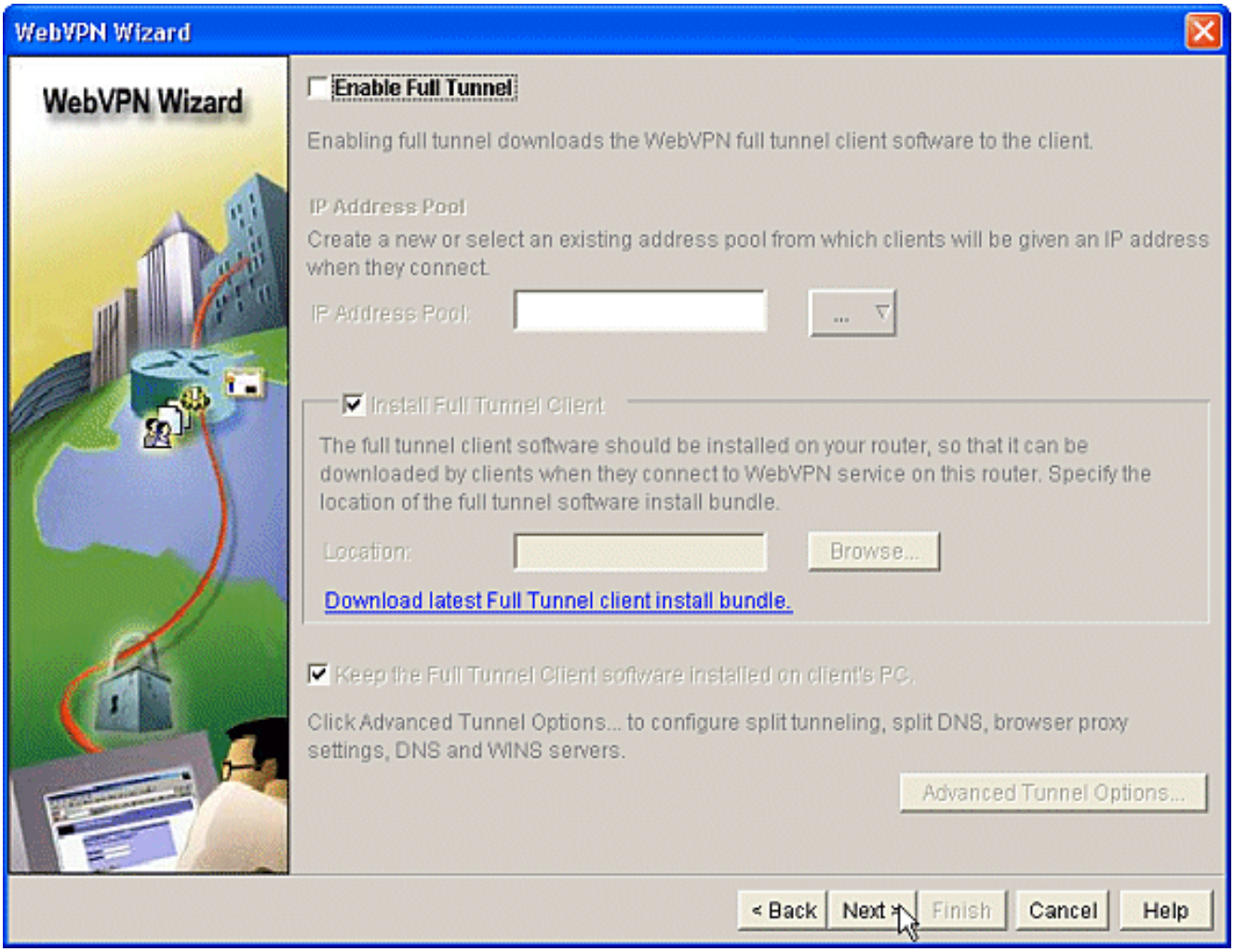
6. Nachdem Sie die Benutzer erstellt haben, klicken Sie auf der Seite "Benutzerauthentifizierung" auf **Weiter**.



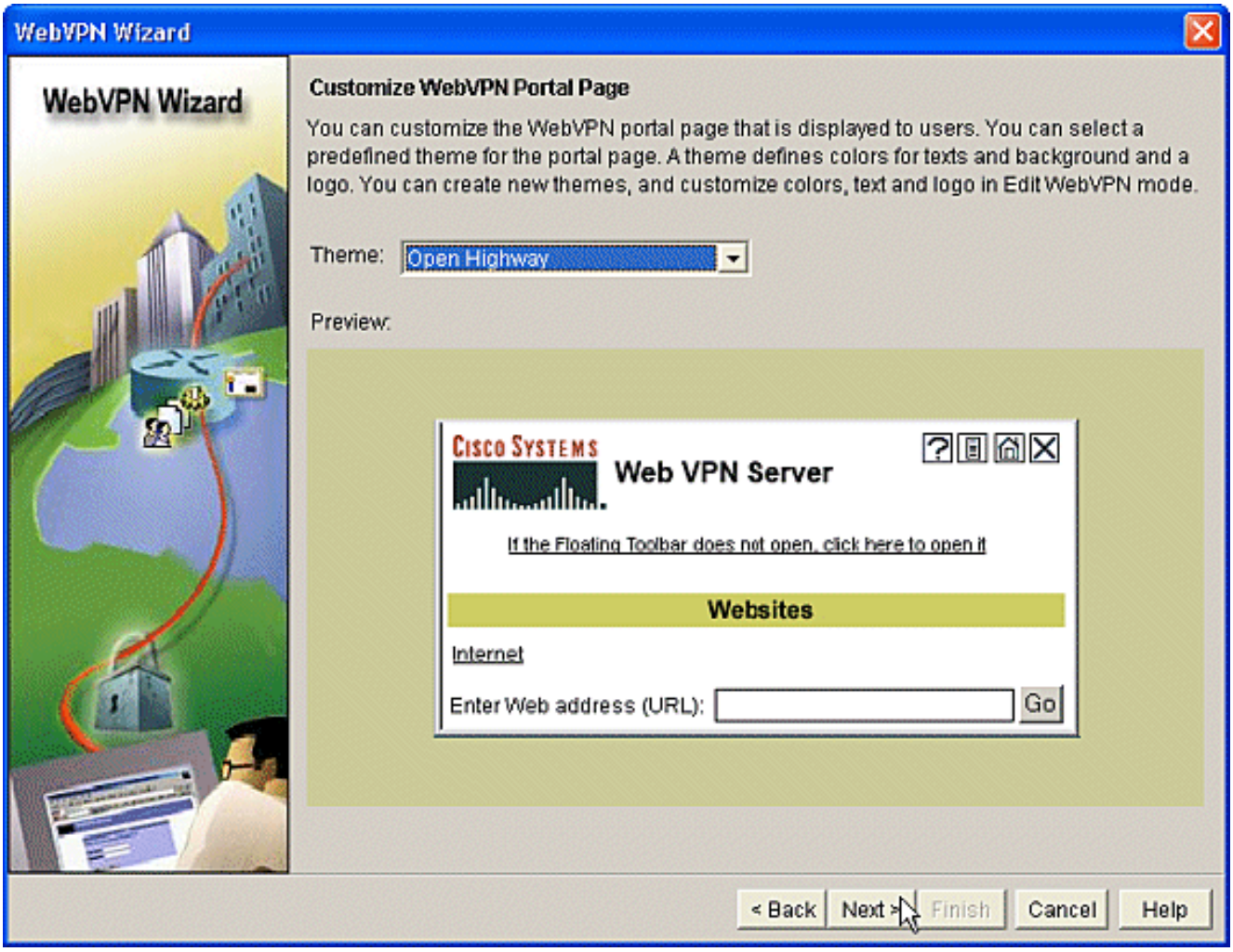
7. Im Bildschirm Configure Intranet Websites (Intranet-Websites konfigurieren) können Sie die Website konfigurieren, die Benutzern des WebVPN-Gateways zur Verfügung steht. Da das Thema dieses Dokuments die Konfiguration von CSD ist, ignorieren Sie diese Seite. Klicken Sie auf
Weiter.



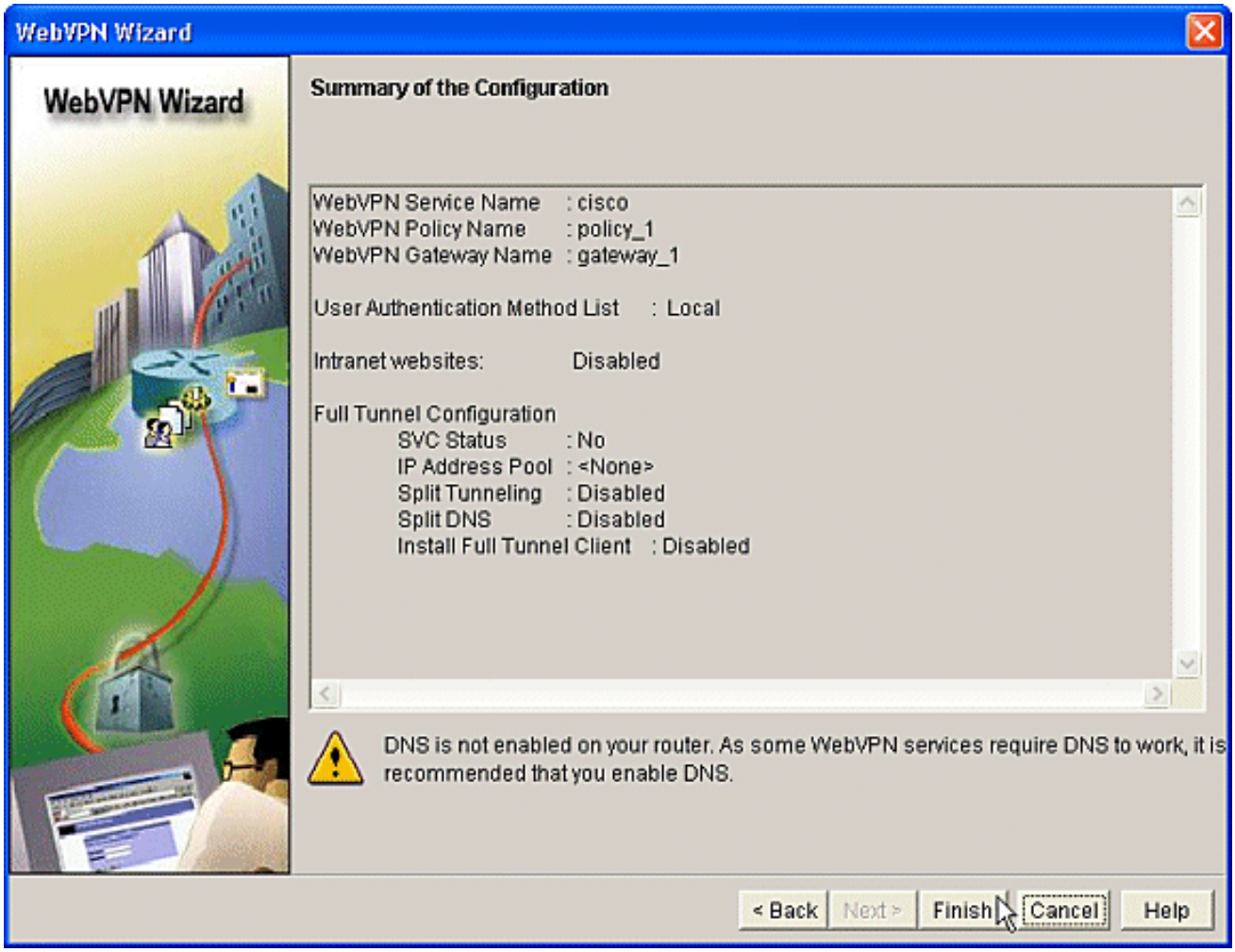
8. Obwohl Sie im nächsten Bildschirm des WebVPN-Assistenten wählen können, ob Sie den SSL VPN-Client für Full-Tunnel aktivieren möchten, wird in diesem Dokument die Aktivierung des CSD behandelt. Deaktivieren Sie **Vollständigen Tunnel aktivieren** und klicken Sie auf **Weiter**.



9. Sie können die Darstellung der WebVPN-Portalseite für Benutzer anpassen. In diesem Fall wird die Standarddarstellung akzeptiert. Klicken Sie auf **Weiter**.



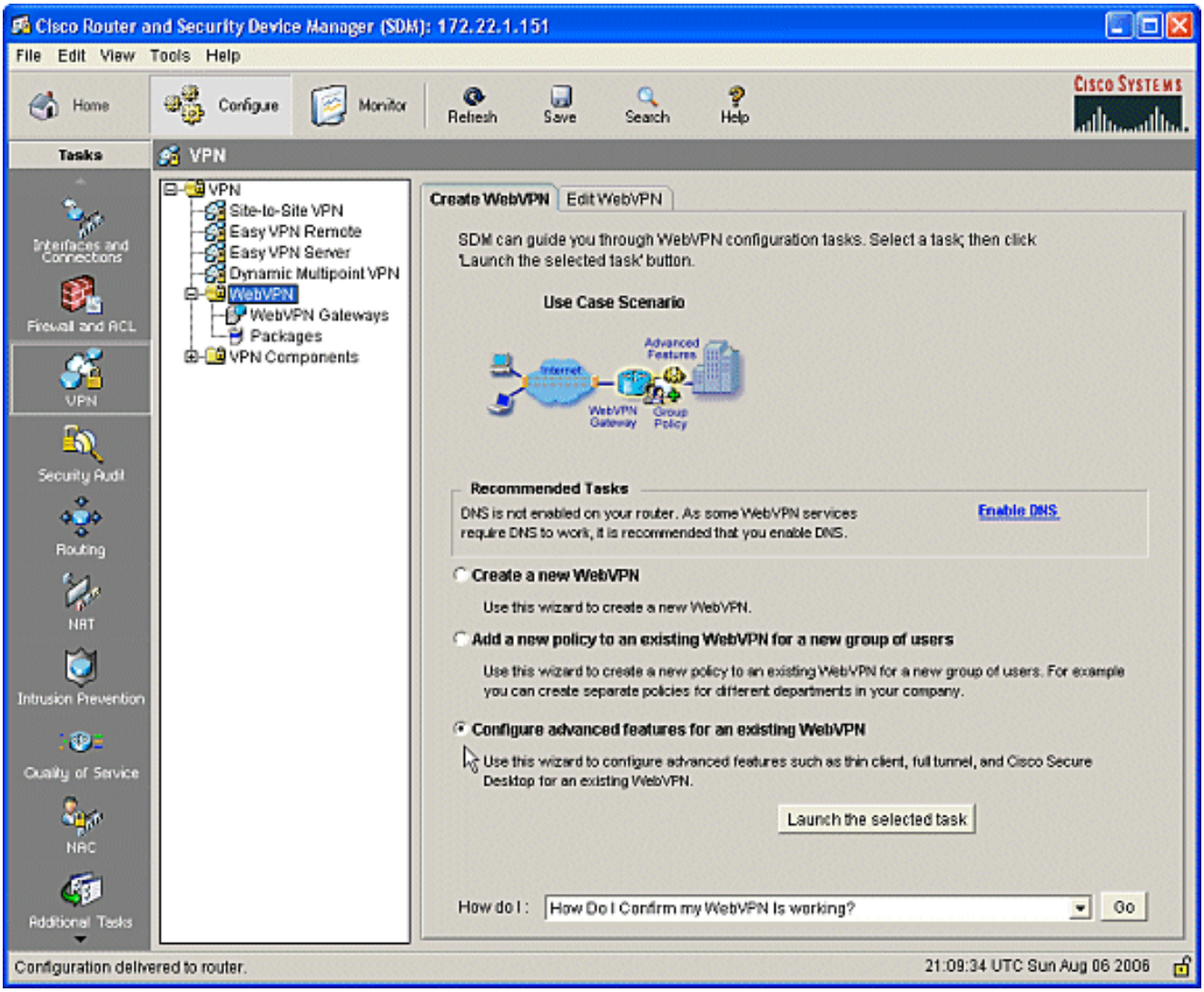
10. Der Assistent zeigt den letzten Bildschirm dieser Serie an. Es wird eine Zusammenfassung der Konfiguration für das WebVPN-Gateway angezeigt. Klicken Sie auf **Fertig stellen** und klicken Sie bei Aufforderung auf
OK.



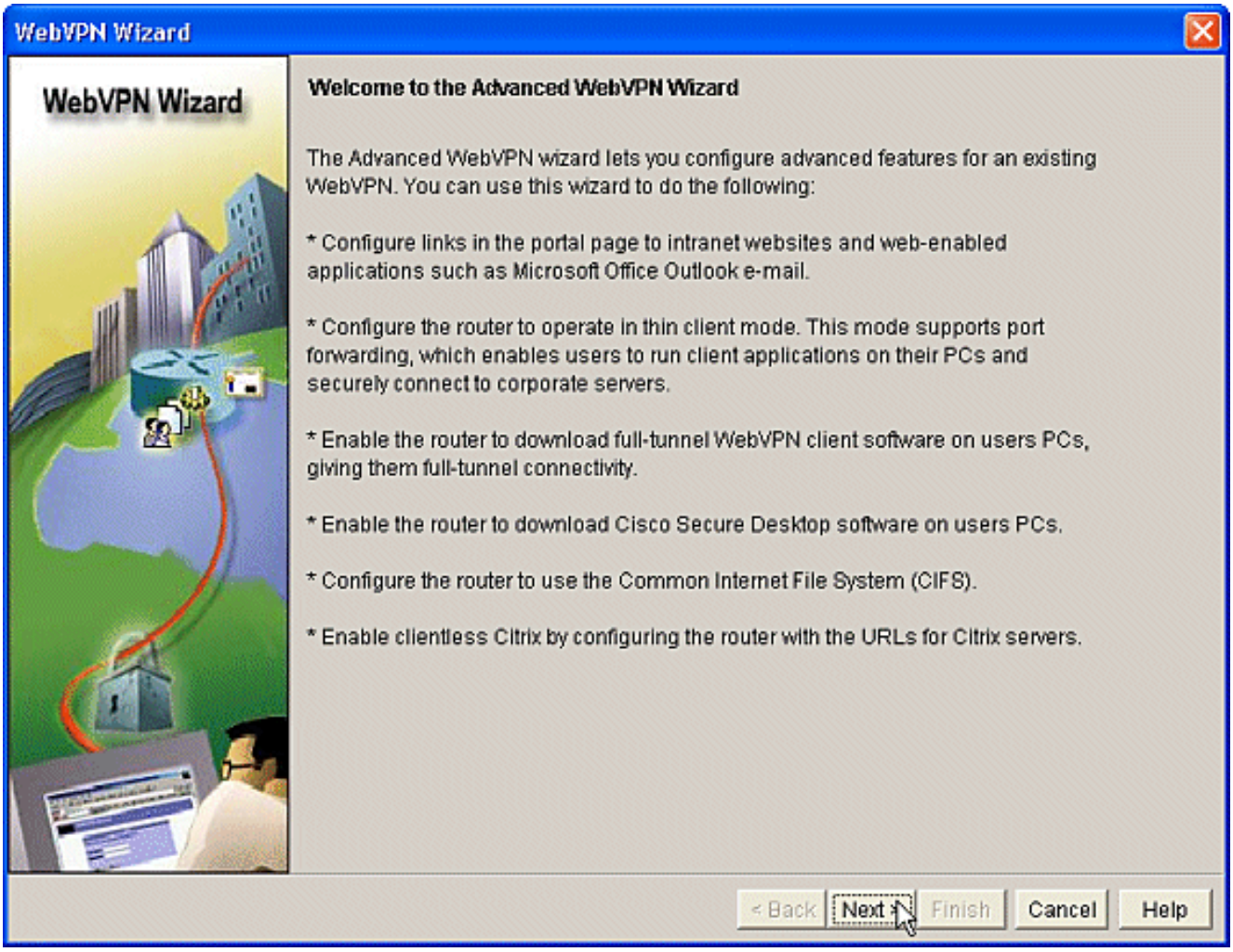
Phase I: Schritt 2: Aktivieren Sie CSD in einem WebVPN-Kontext.

Verwenden Sie den WebVPN-Assistenten, um CSD in einem WebVPN-Kontext zu aktivieren.

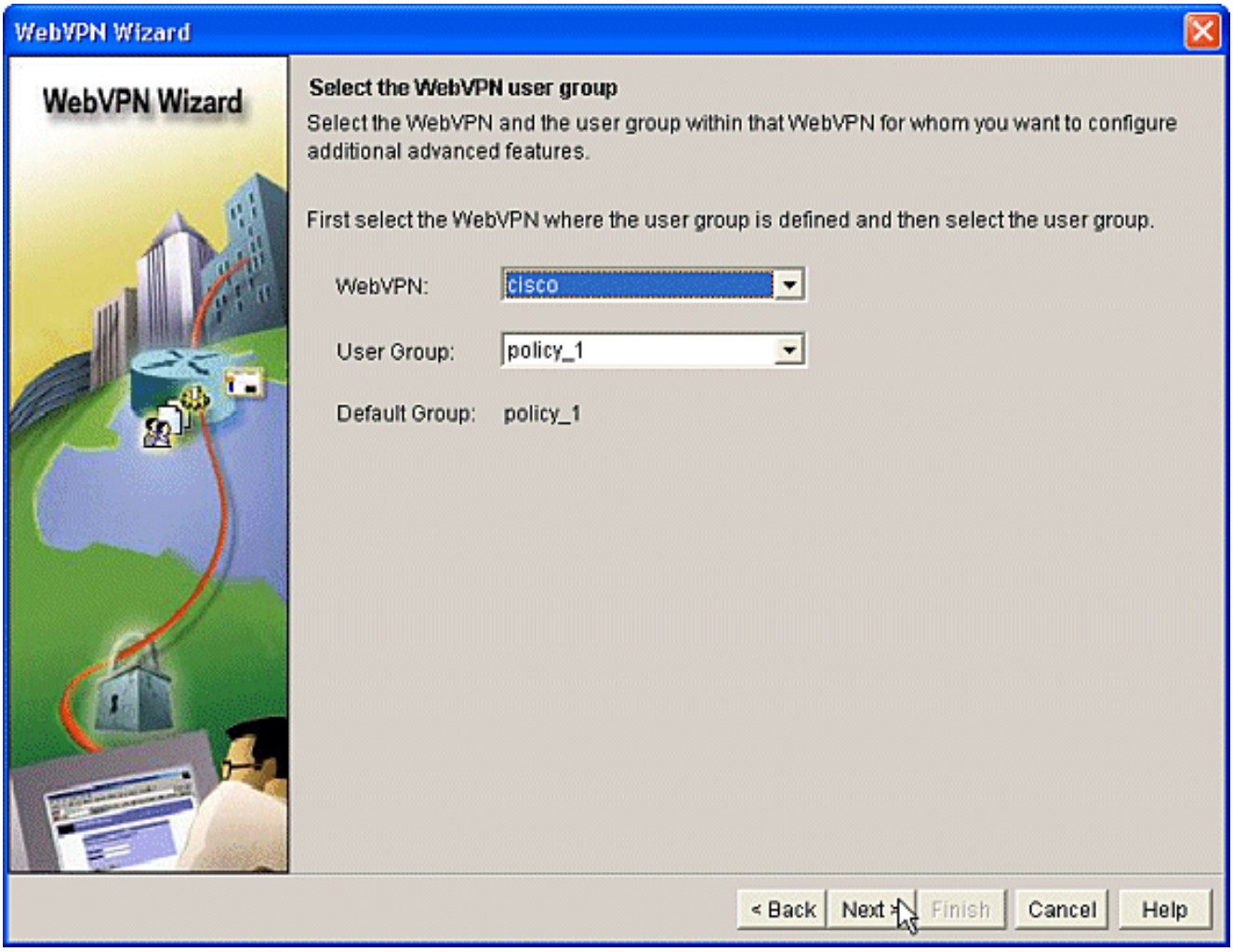
1. Verwenden Sie die erweiterten Funktionen des WebVPN-Assistenten, um CSD für den neu erstellten Kontext zu aktivieren. Der Assistent gibt Ihnen die Möglichkeit, das CSD-Paket zu installieren, wenn es noch nicht installiert ist.Klicken Sie in SDM auf die Registerkarte **Konfigurieren**.Klicken Sie im Navigationsbereich auf **VPN > WebVPN**.Klicken Sie auf die Registerkarte **WebVPN erstellen**.Aktivieren Sie das Optionsfeld **Erweiterte Funktionen für ein vorhandenes WebVPN konfigurieren**.Klicken Sie auf die Schaltfläche **Ausgewählte Aufgabe starten**.



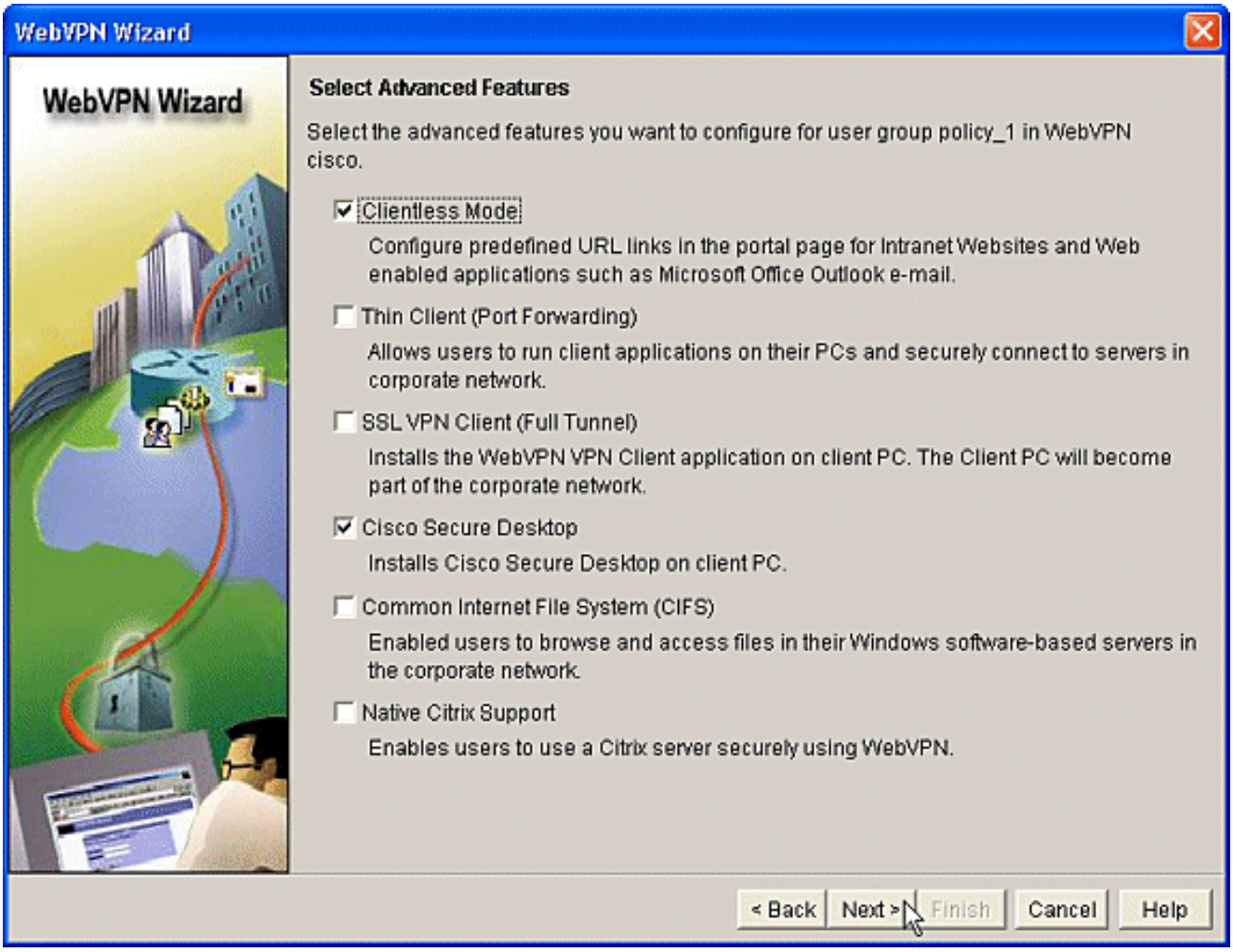
2. Die Willkommensseite für den erweiterten WebVPN-Assistenten wird angezeigt. Klicken Sie auf
Weiter.



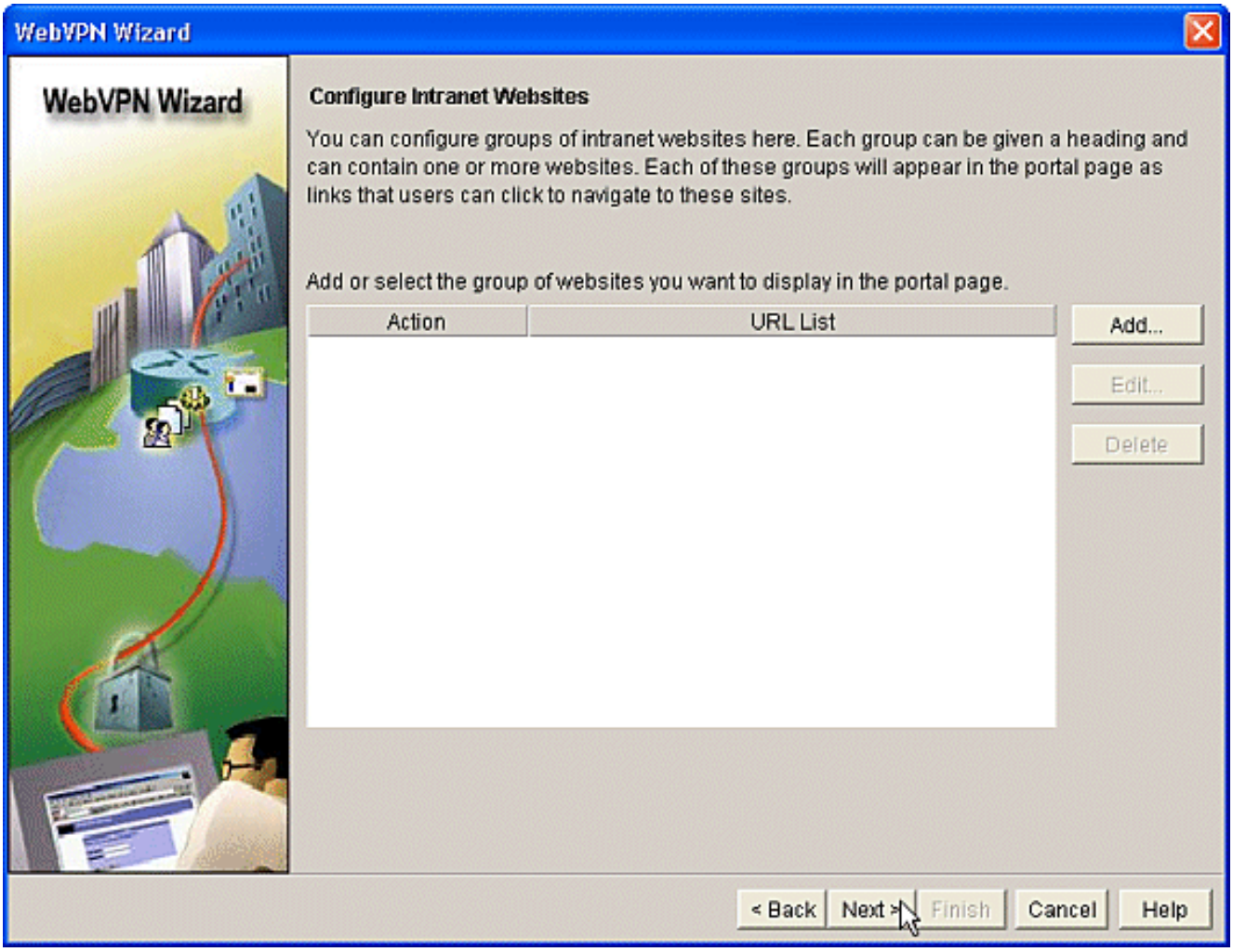
3. Wählen Sie in den Dropdown-Feldern das WebVPN und die Benutzergruppe aus. Die Funktionen des erweiterten WebVPN-Assistenten werden auf Ihre Auswahl angewendet. Klicken Sie auf
Weiter.



4. Im Bildschirm "Erweiterte Funktionen auswählen" können Sie aus den aufgeführten Technologien auswählen.Überprüfen Sie **Cisco Secure Desktop**.In diesem Beispiel wird der **Clientless-Modus** ausgewählt.Wenn Sie eine der anderen aufgelisteten Technologien auswählen, werden zusätzliche Fenster geöffnet, in denen Sie verwandte Informationen eingeben können.Klicken Sie auf die Schaltfläche **Weiter**.

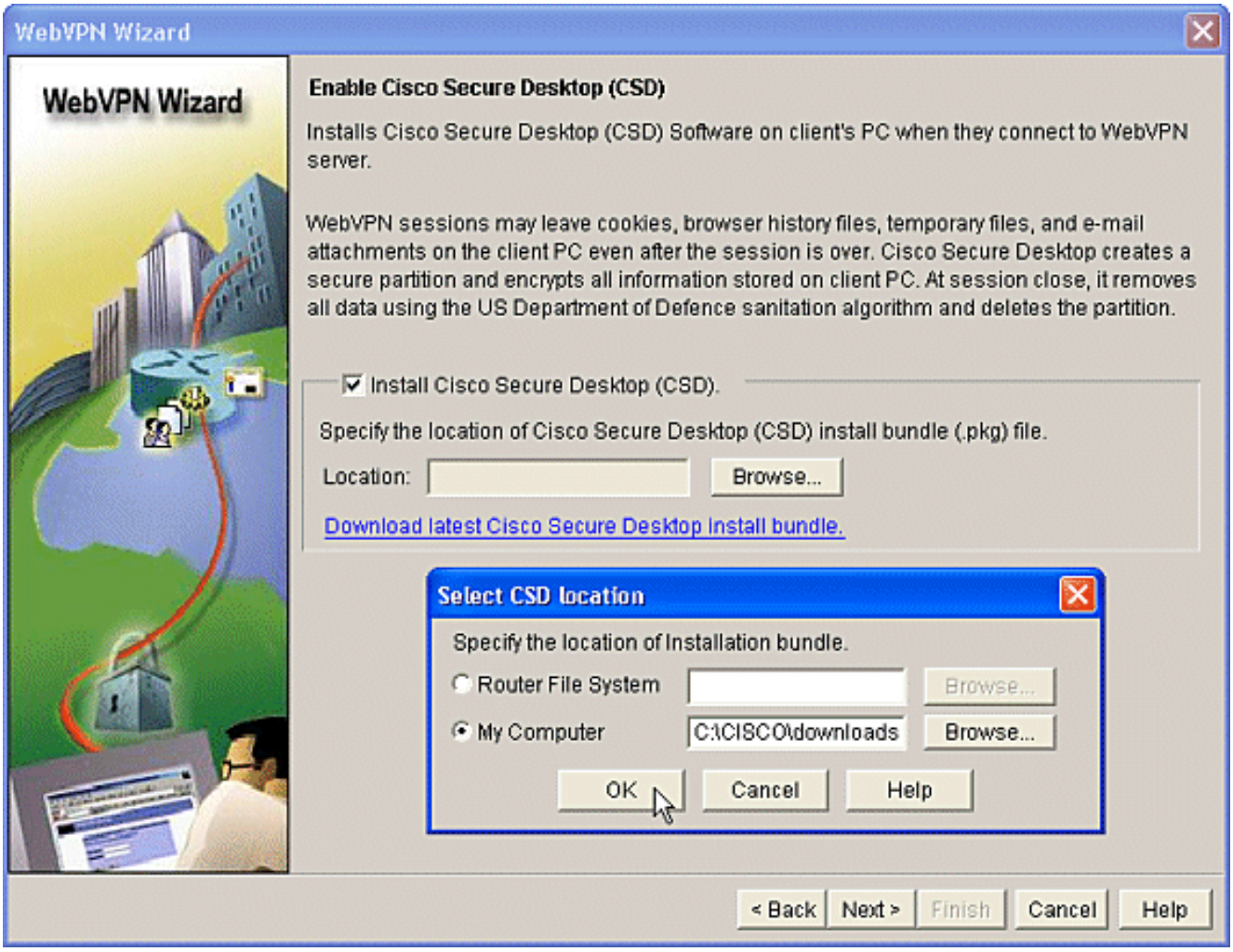


5. Der Bildschirm Configure Intranet Websites (Intranet-Websites konfigurieren) ermöglicht die Konfiguration der Website-Ressourcen, die Sie den Benutzern zur Verfügung stellen möchten. Sie können die internen Websites des Unternehmens wie Outlook Web Access (OWA)
hinzufügen.



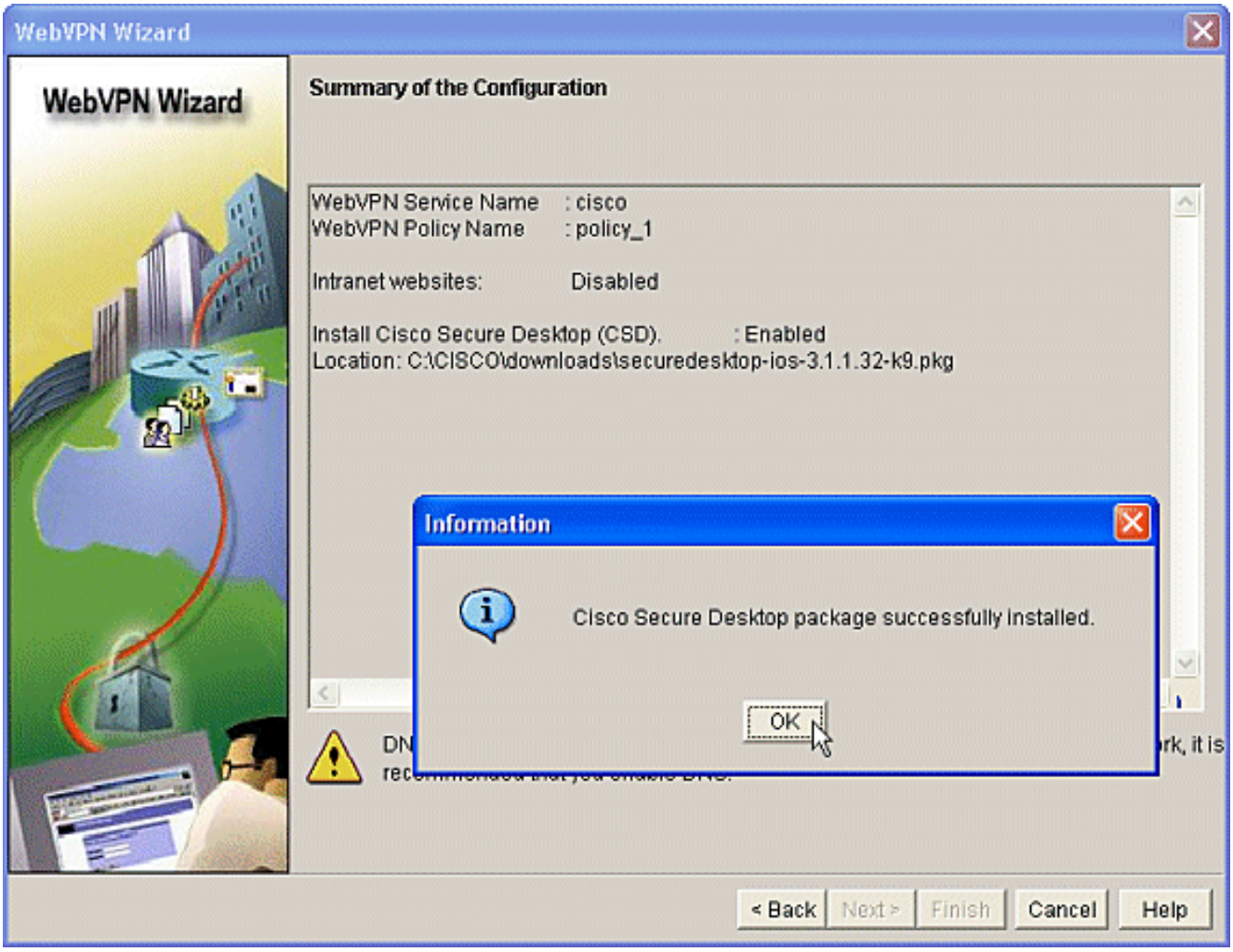
6. Im Bildschirm "Enable Cisco Secure Desktop (CSD)" können Sie den CSD für diesen Kontext aktivieren. Aktivieren Sie das Kontrollkästchen neben **Cisco Secure Desktop (CSD installieren),** und klicken Sie auf **Durchsuchen**.

7. Aktivieren Sie im Bereich Speicherort für CSD auswählen die Option **Arbeitsplatz**.Klicken Sie auf die Schaltfläche **Durchsuchen**.Wählen Sie die CSD IOS-Paketdatei auf Ihrer Management-Workstation aus.Klicken Sie auf die Schaltfläche **OK**.Klicken Sie auf die Schaltfläche
Weiter.



8. Eine Zusammenfassung des Konfigurationsbildschirms wird angezeigt. Klicken Sie auf die Schaltfläche **Fertig stellen**.

9. Klicken Sie auf **OK**, wenn Sie sehen, dass die CSD-Paketdatei erfolgreich installiert wurde.



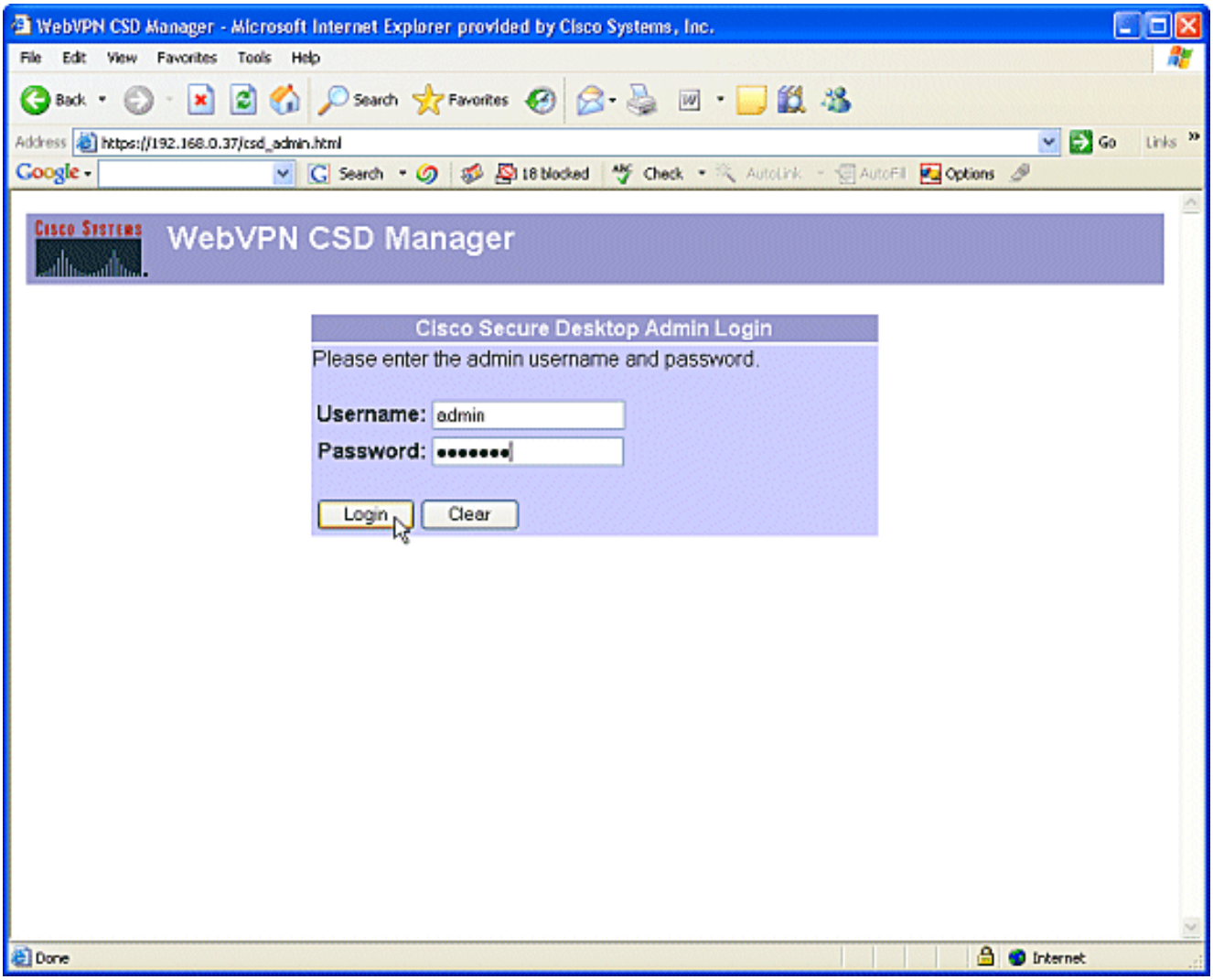
Phase II: Konfigurieren Sie den CSD mithilfe eines Webbrowsers.

Diese Schritte werden verwendet, um die Konfiguration des CSD in Ihrem Webbrowser abzuschließen.

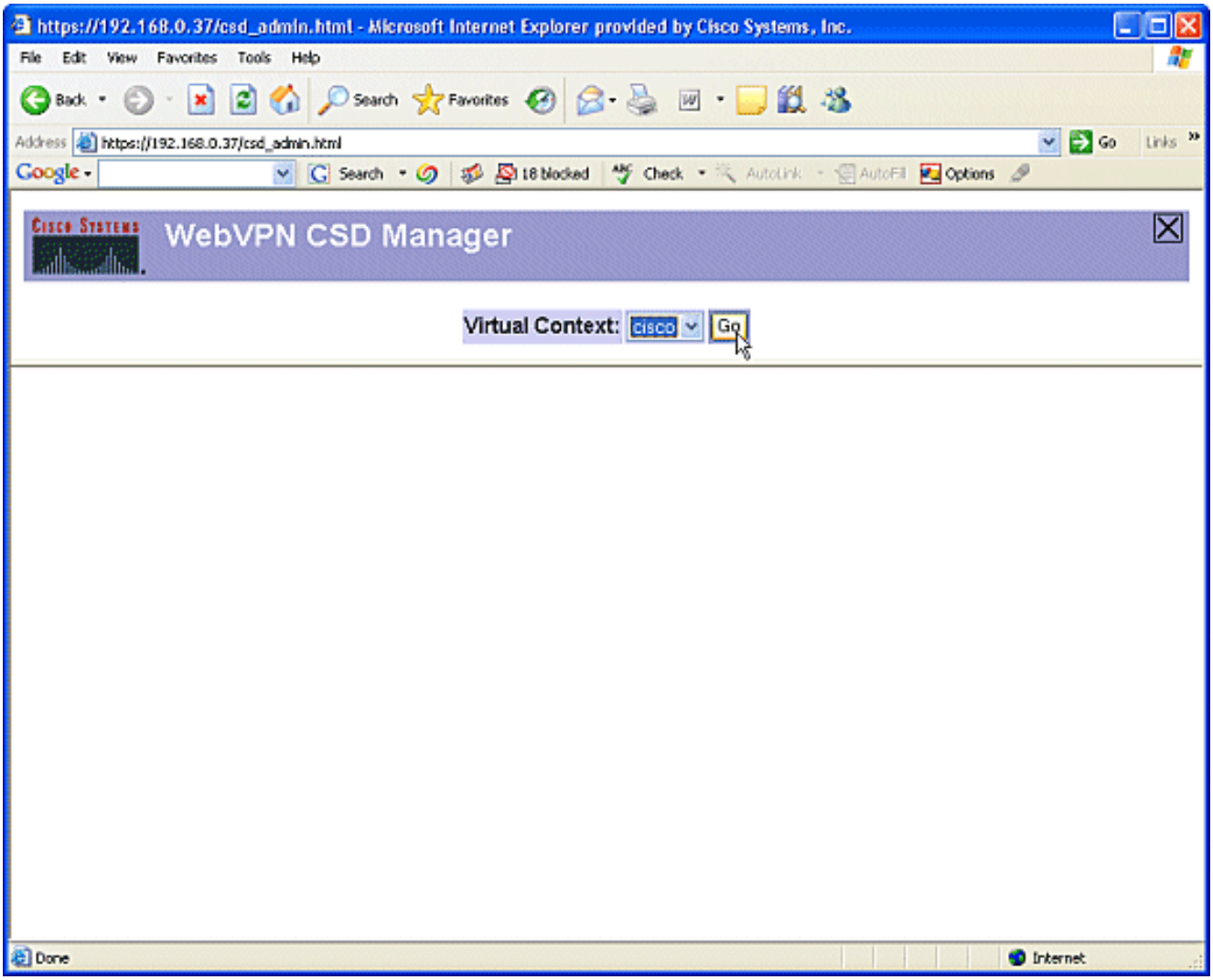
Phase II: Schritt 1: Definieren Sie Windows-Speicherorte.

Definieren Sie die Windows-Speicherorte.

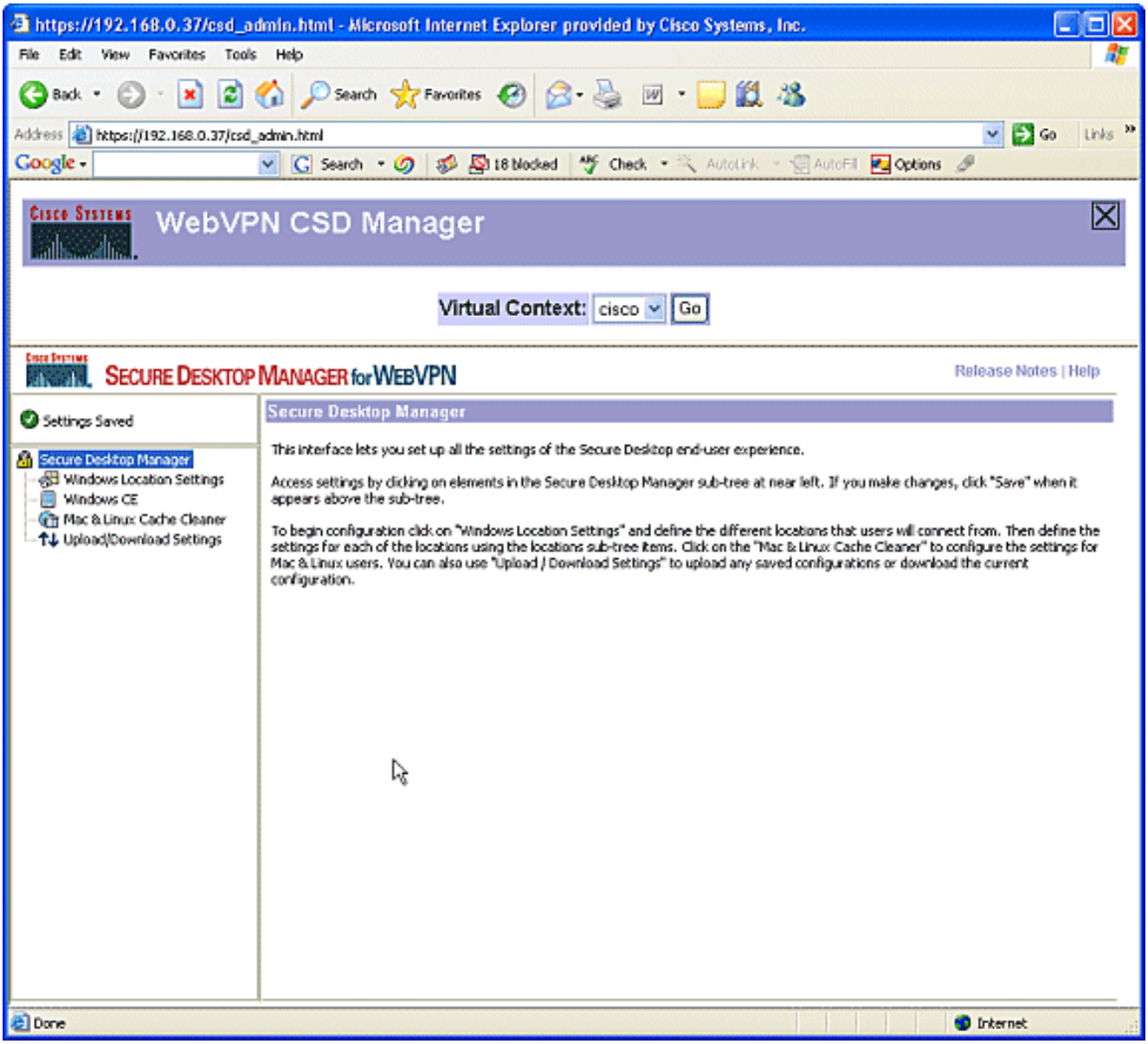
1. Öffnen Sie Ihren Webbrowser unter **https://WebVPNgateway_IP Address/csd_admin.html**, z. B. **https:/192.168.0.37/csd_admin.html**.
2. Geben Sie den Benutzernamen **admin ein**.Geben Sie das Kennwort ein, das den enable-geheimen Schlüssel des Routers darstellt.Klicken Sie auf **Anmelden**.



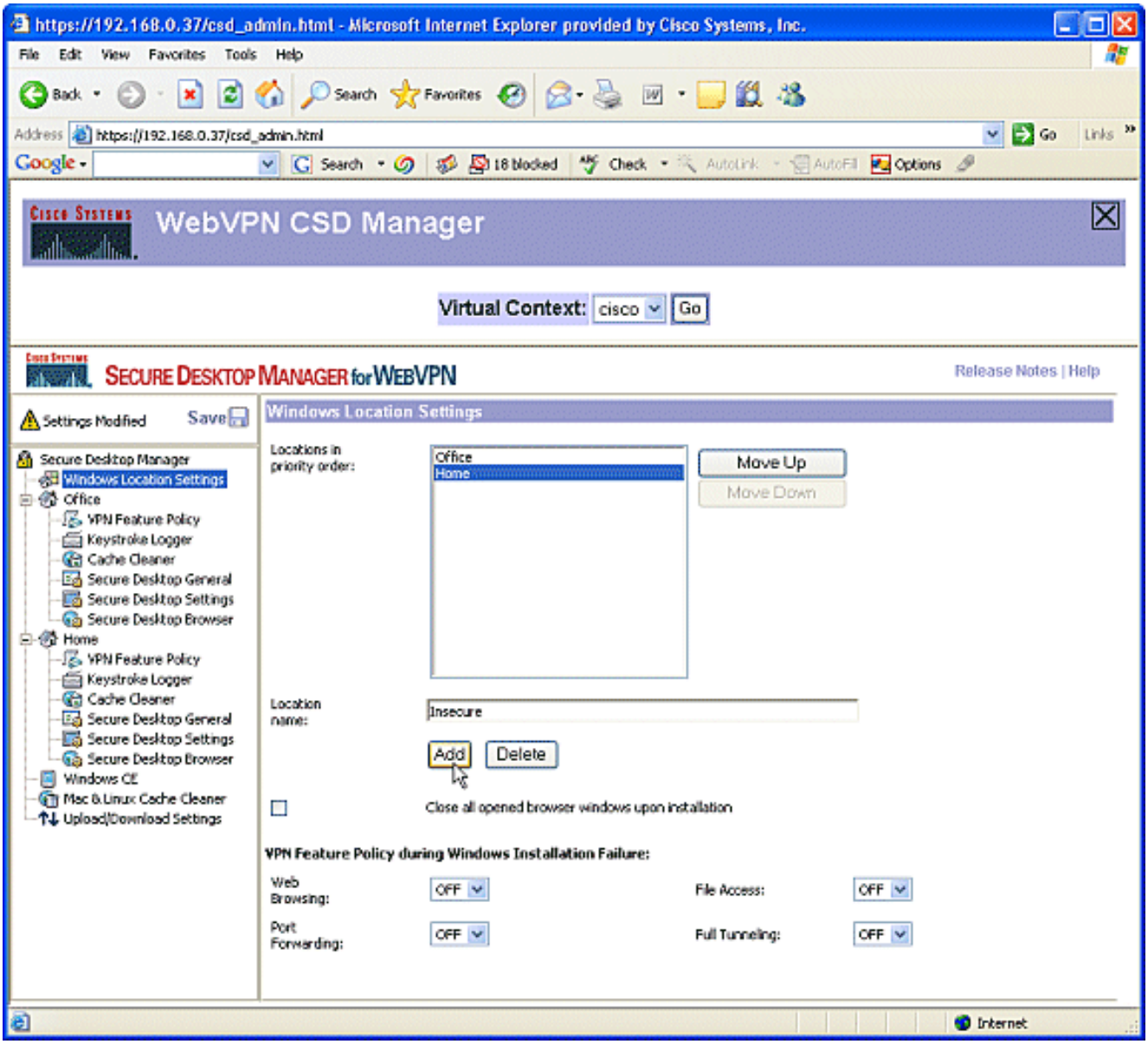
3. Akzeptieren Sie das vom Router angebotene Zertifikat, wählen Sie den Kontext aus dem Dropdown-Feld, und klicken Sie auf **Los**.



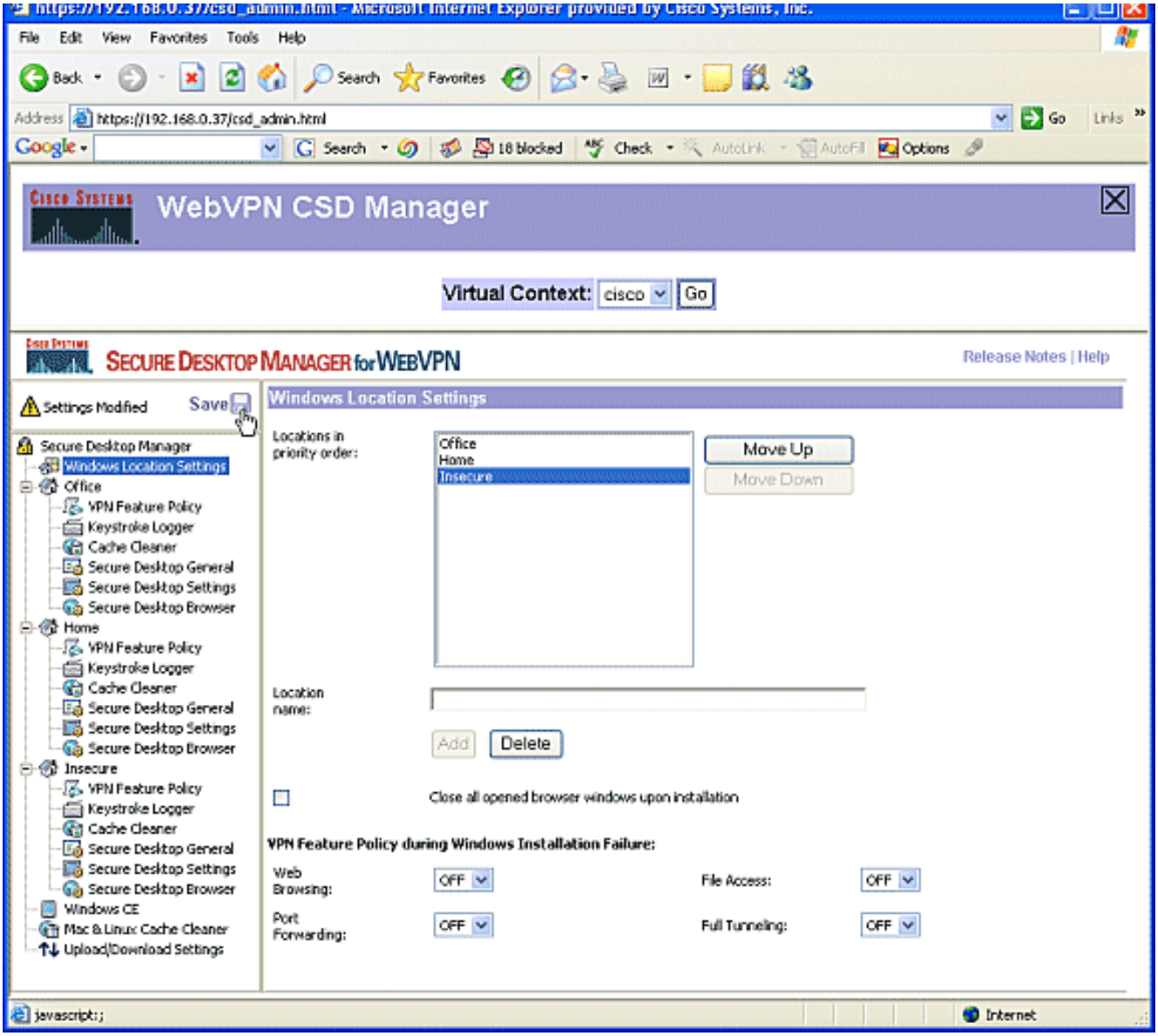
4. Der Secure Desktop Manager für WebVPN wird geöffnet.



5. Wählen Sie im linken Teilfenster die Option **Windows-Standorteinstellungen aus**.Platzieren Sie den Cursor in das Feld neben Standortname, und geben Sie einen Standortnamen ein.Klicken Sie auf **Hinzufügen**.In diesem Beispiel werden drei Standortnamen angezeigt: Büro, Home Office und unsicher. Wenn ein neuer Speicherort hinzugefügt wird, wird der linke Bereich mit den konfigurierbaren Parametern für diesen Speicherort erweitert.



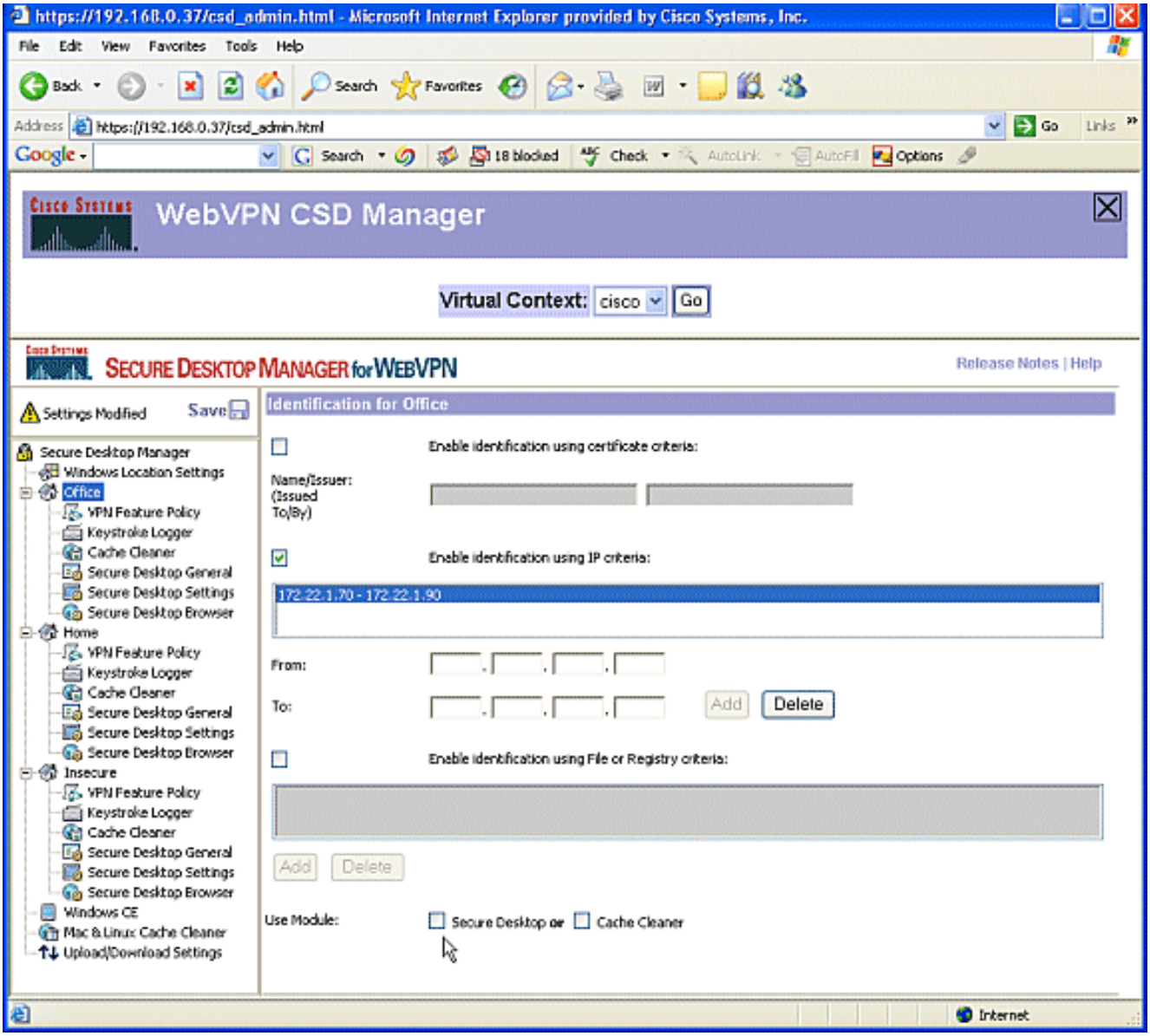
6. Nachdem Sie die Windows-Speicherorte erstellt haben, klicken Sie oben im linken Bereich auf **Speichern**.**Hinweis:** Speichern Sie Ihre Konfigurationen häufig, da Ihre Einstellungen verloren gehen, wenn Sie vom Webbrowser getrennt
werden.



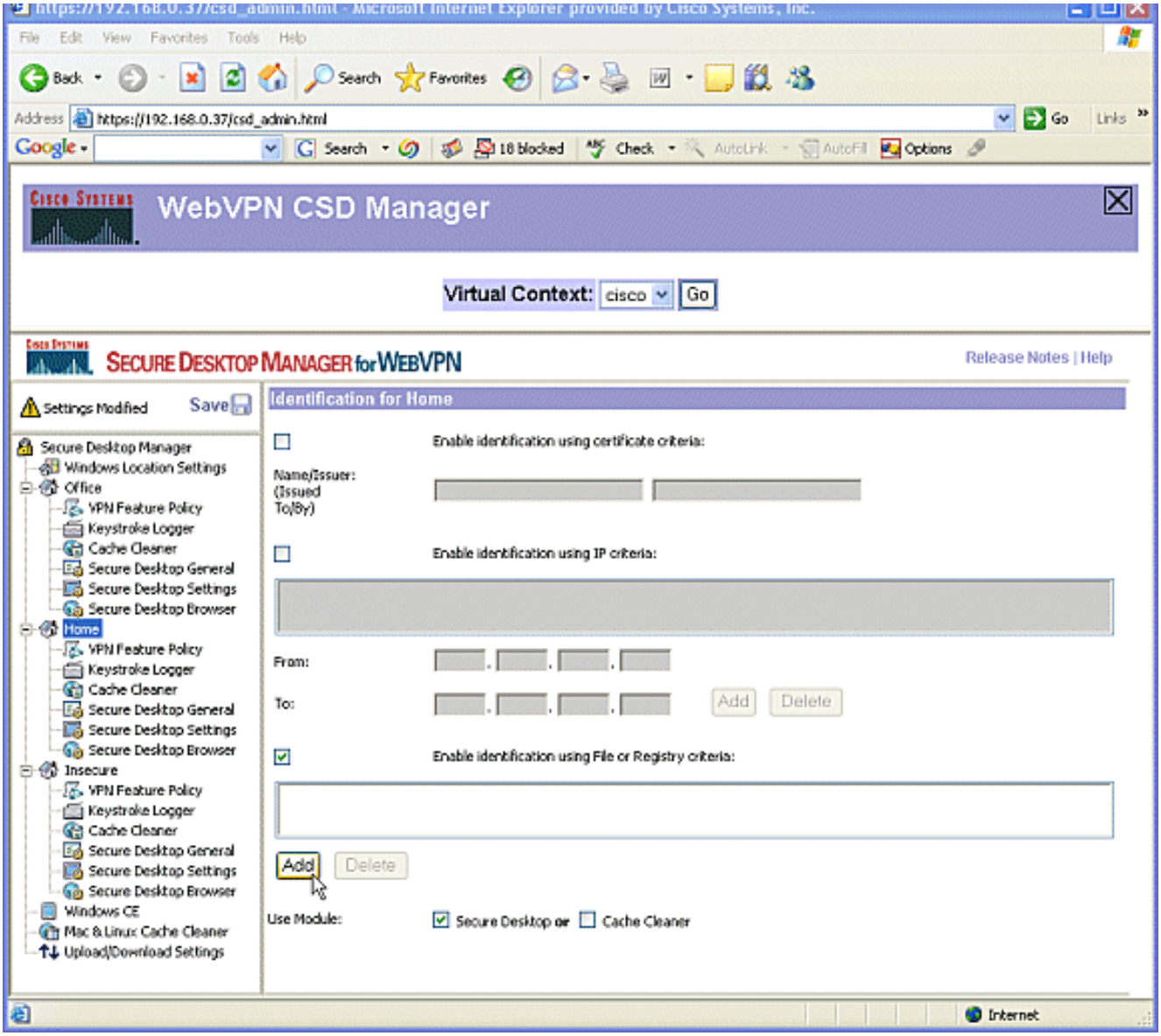
Phase II: Schritt 2: Identifizieren von Standortkriterien

Um Windows-Standorte voneinander zu unterscheiden, weisen Sie jedem Standort spezifische Kriterien zu. Dadurch kann der CSD bestimmen, welche seiner Funktionen auf einen bestimmten Windows-Speicherort angewendet werden sollen.

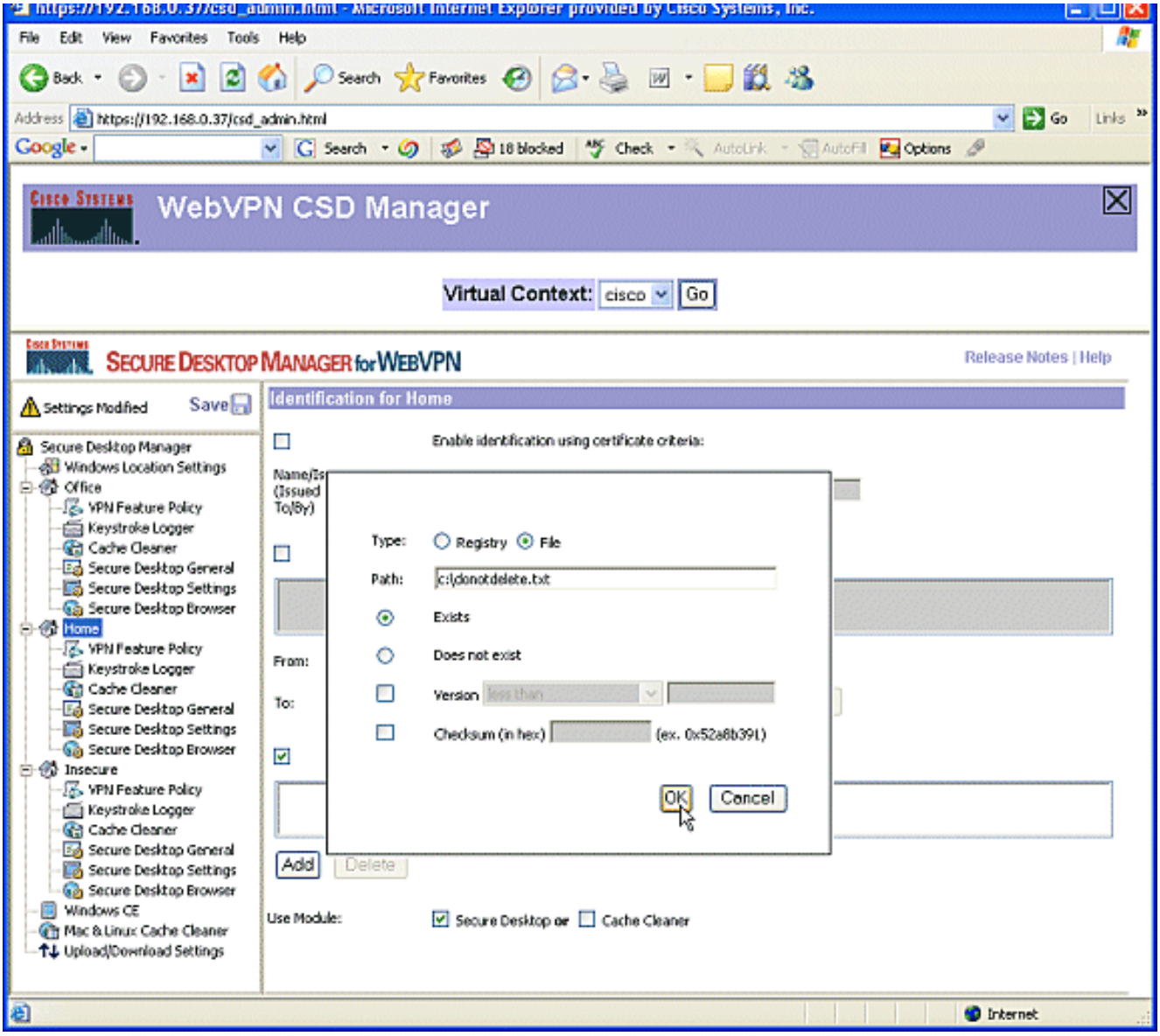
1. Klicken Sie im linken Teilfenster auf **Office**.Sie können einen Windows-Speicherort anhand von Zertifikatskriterien, IP-Kriterien, einer Datei oder Registrierungskriterien identifizieren. Sie können auch den Secure Desktop oder Cache Cleaner für diese Clients auswählen. Da es sich bei diesen Benutzern um interne Büroangestellte handelt, identifizieren Sie sie mit IP-Kriterien.Geben Sie die IP-Adressbereiche in die Felder **Von** und **Bis ein**.Klicken Sie auf **Hinzufügen**. Deaktivieren Sie **Modul verwenden: Sicherer Desktop**.Wenn Sie dazu aufgefordert werden, klicken Sie auf **Speichern** und dann auf **OK**.



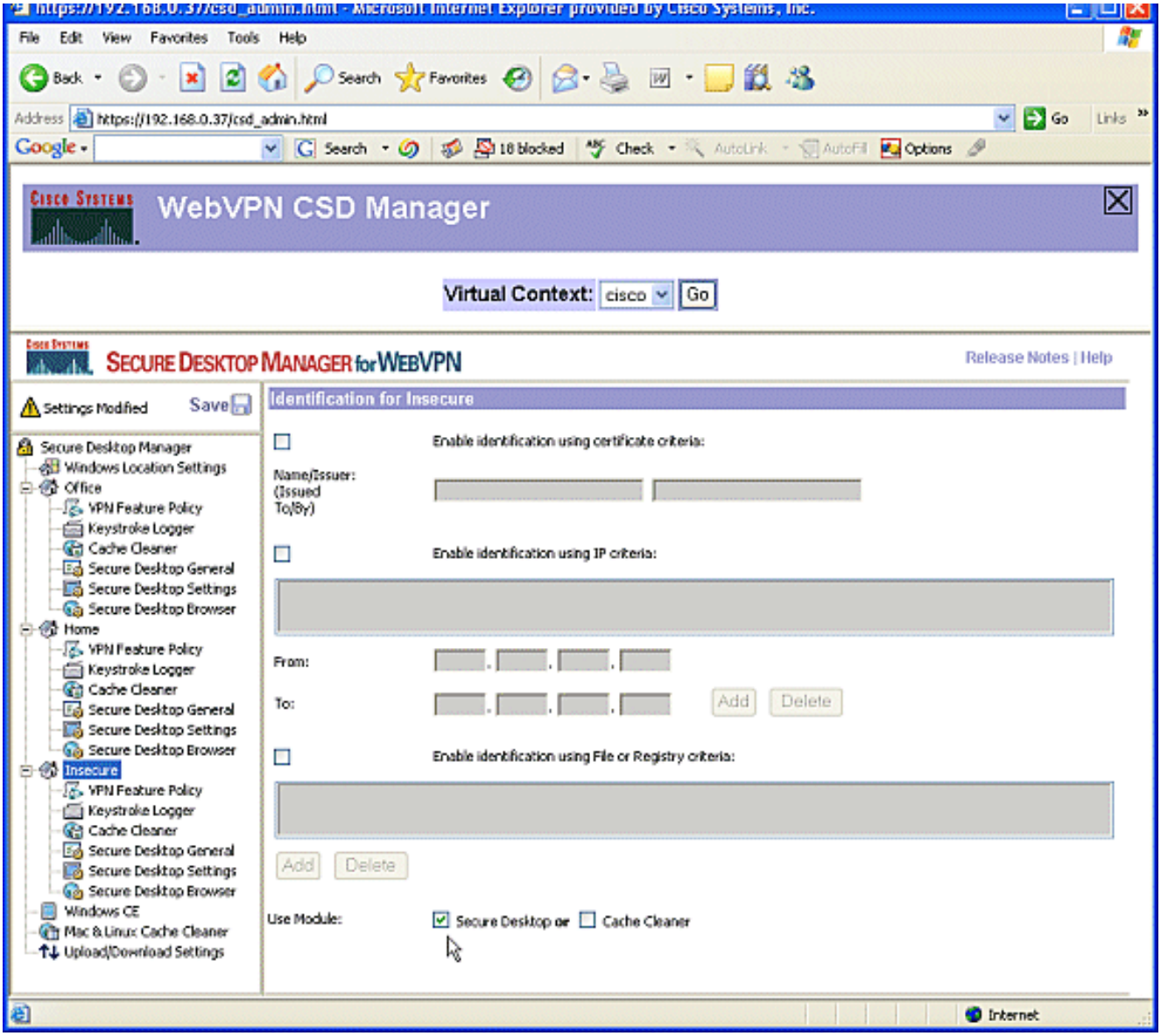
2. Klicken Sie im linken Teilfenster auf die zweite Windows-Standorteinstellung **Home**.**Modul verwenden: Secure Desktop** ist aktiviert.Es wird eine Datei verteilt, die diese Clients identifiziert. Sie können für diese Benutzer Zertifikate und/oder Registrierungskriterien verteilen.Aktivieren Sie **Identifikation mithilfe der Datei- oder Registrierungskriterien aktivieren**.Klicken Sie auf **Hinzufügen**.



3. Wählen Sie im Dialogfeld die Option **Datei**, und geben Sie den Pfad zur Datei ein.Diese Datei muss an alle Ihre Home-Clients verteilt werden.Aktivieren Sie das Optionsfeld **Exists (Bestehen)**.Wenn Sie dazu aufgefordert werden, klicken Sie auf **OK** und dann auf **Speichern**.



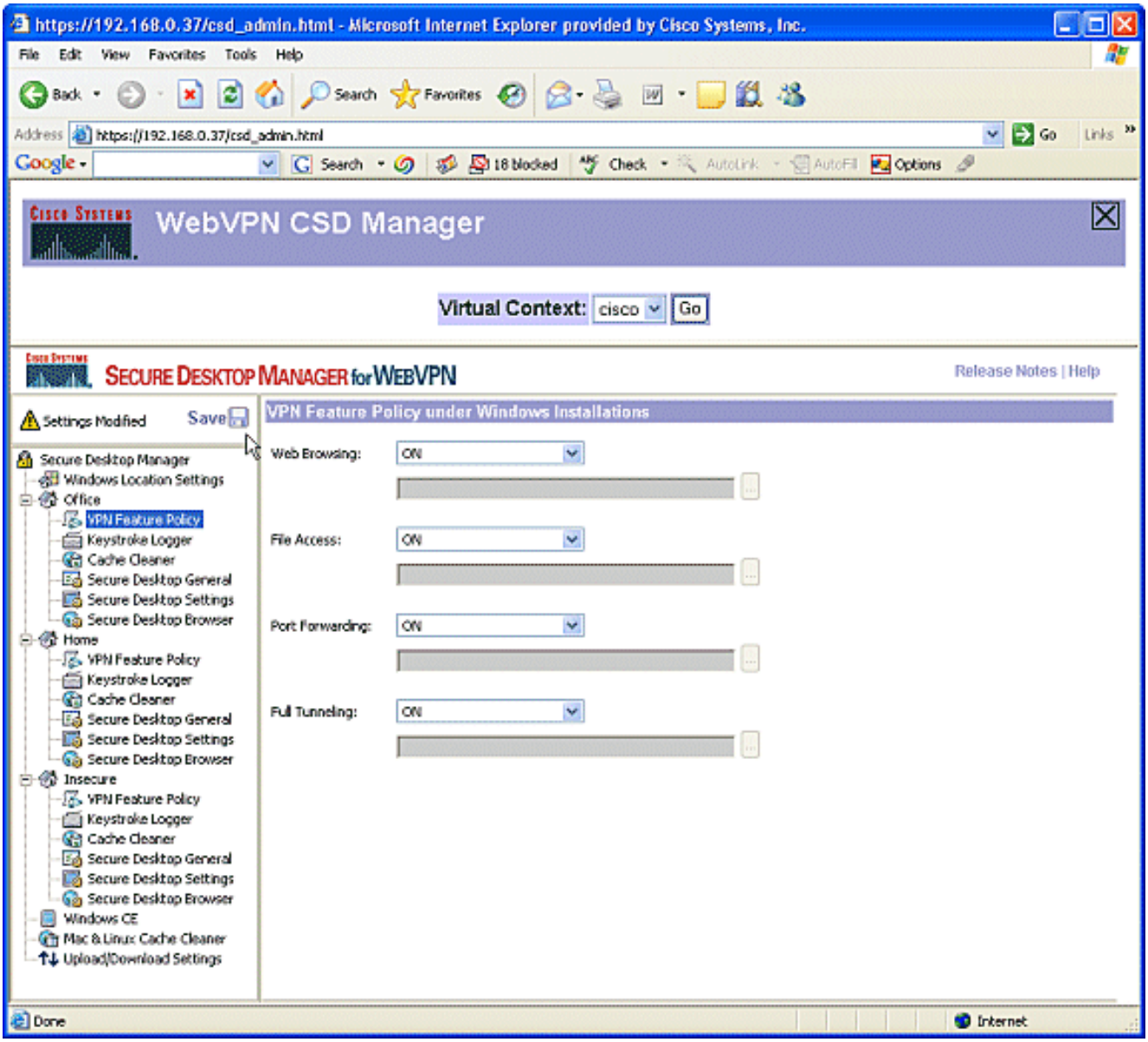
4. Um die Identifizierung **unsicherer** Standorte zu konfigurieren, wenden Sie einfach keine Identifikationskriterien an.Klicken Sie im linken Bereich auf **Unsicher**.Lassen Sie alle Kriterien deaktiviert.Aktivieren Sie **Modul verwenden: Sicherer Desktop**.Wenn Sie dazu aufgefordert werden, klicken Sie auf **Speichern** und dann auf **OK**.



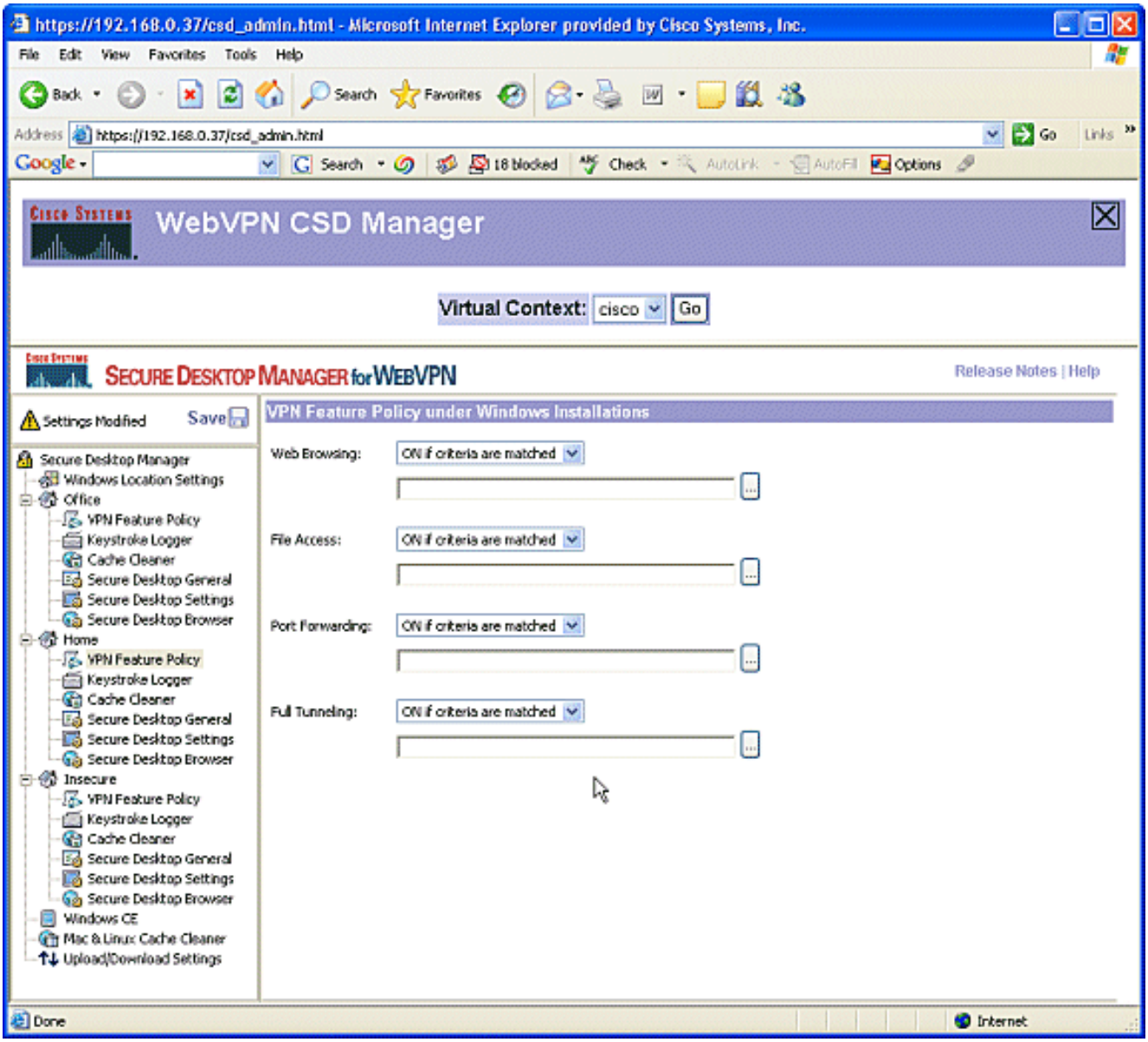
Phase II: Schritt 3: Konfigurieren Sie die Windows-Standortmodule und -Funktionen.

Konfigurieren Sie die CSD-Funktionen für jeden Windows-Standort.

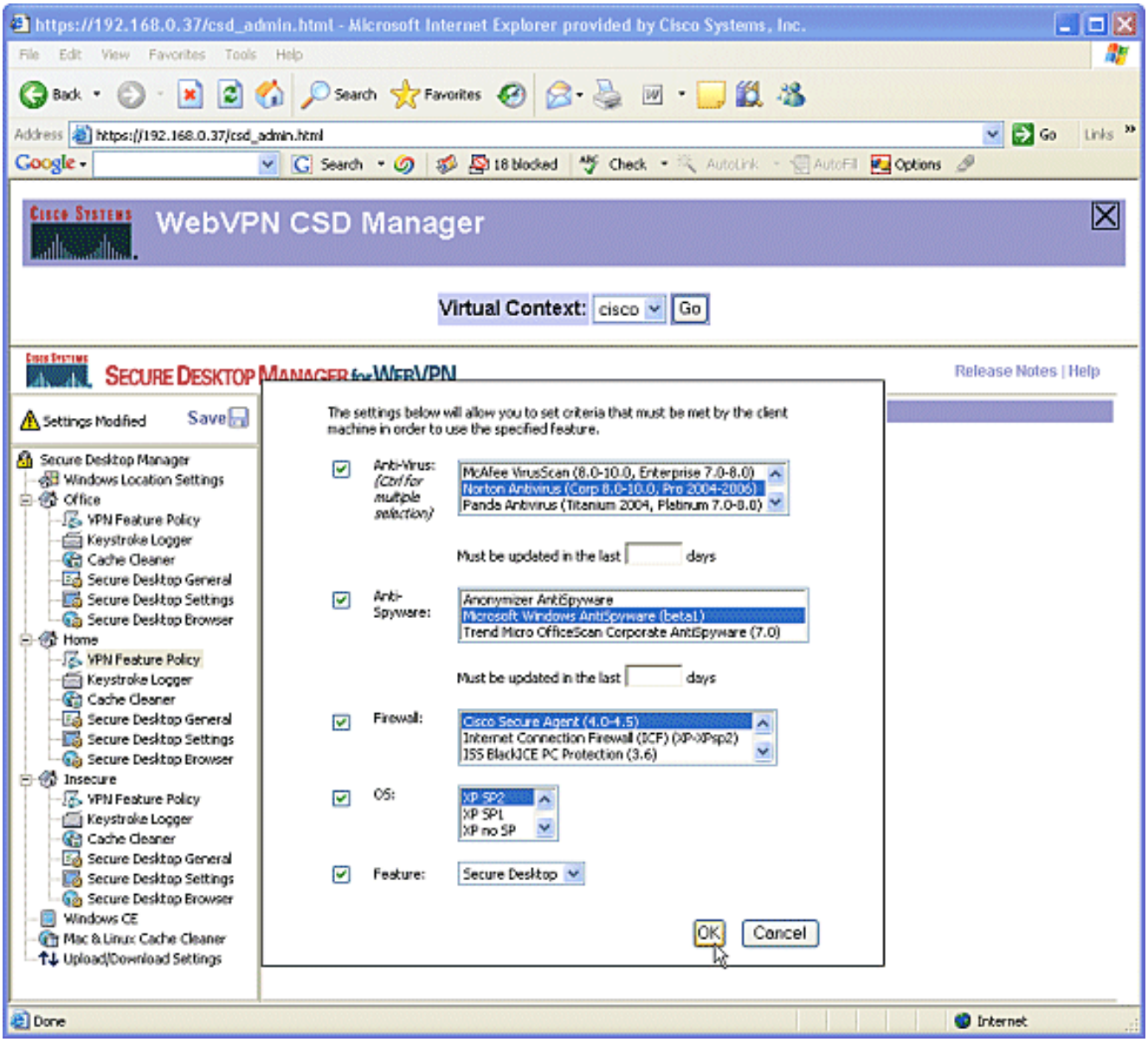
1. Klicken Sie unter **Office** auf **VPN-Funktionsrichtlinie**. Da es sich um vertrauenswürdige interne Clients handelt, wurden weder CSD noch Cache Cleaner aktiviert. Keine der anderen Parameter ist
verfügbar.



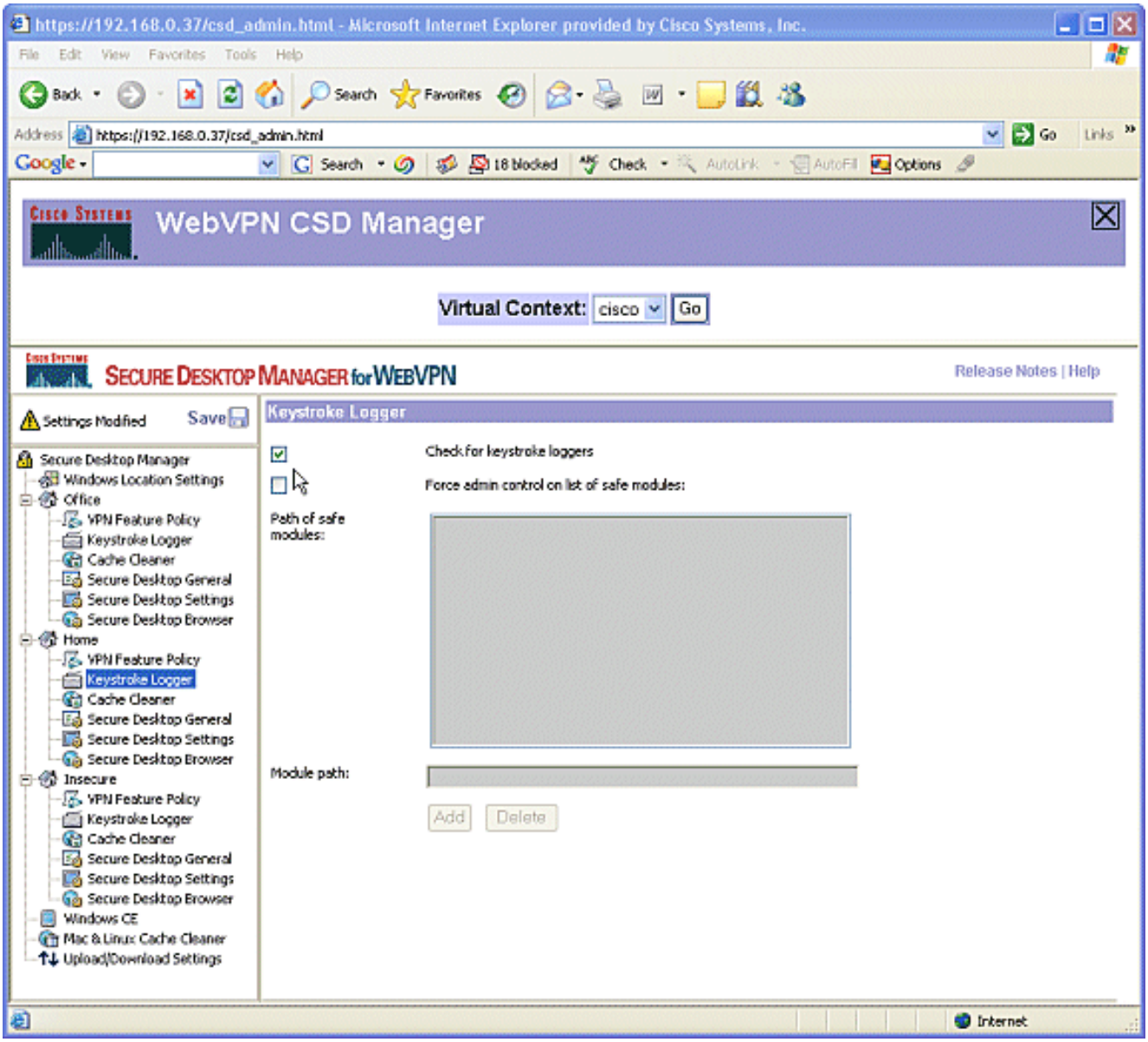
2. Aktivieren Sie die Funktionen wie gezeigt.Wählen Sie im linken Teilfenster unter **Home** die Option **VPN Feature Policy (VPN-Funktionsrichtlinie)**.Heimbenutzer erhalten Zugriff auf das Firmen-LAN, wenn sie bestimmte Kriterien erfüllen.Wählen Sie unter jeder Zugriffsmethode **ON** aus, **wenn die Kriterien zugeordnet sind**.



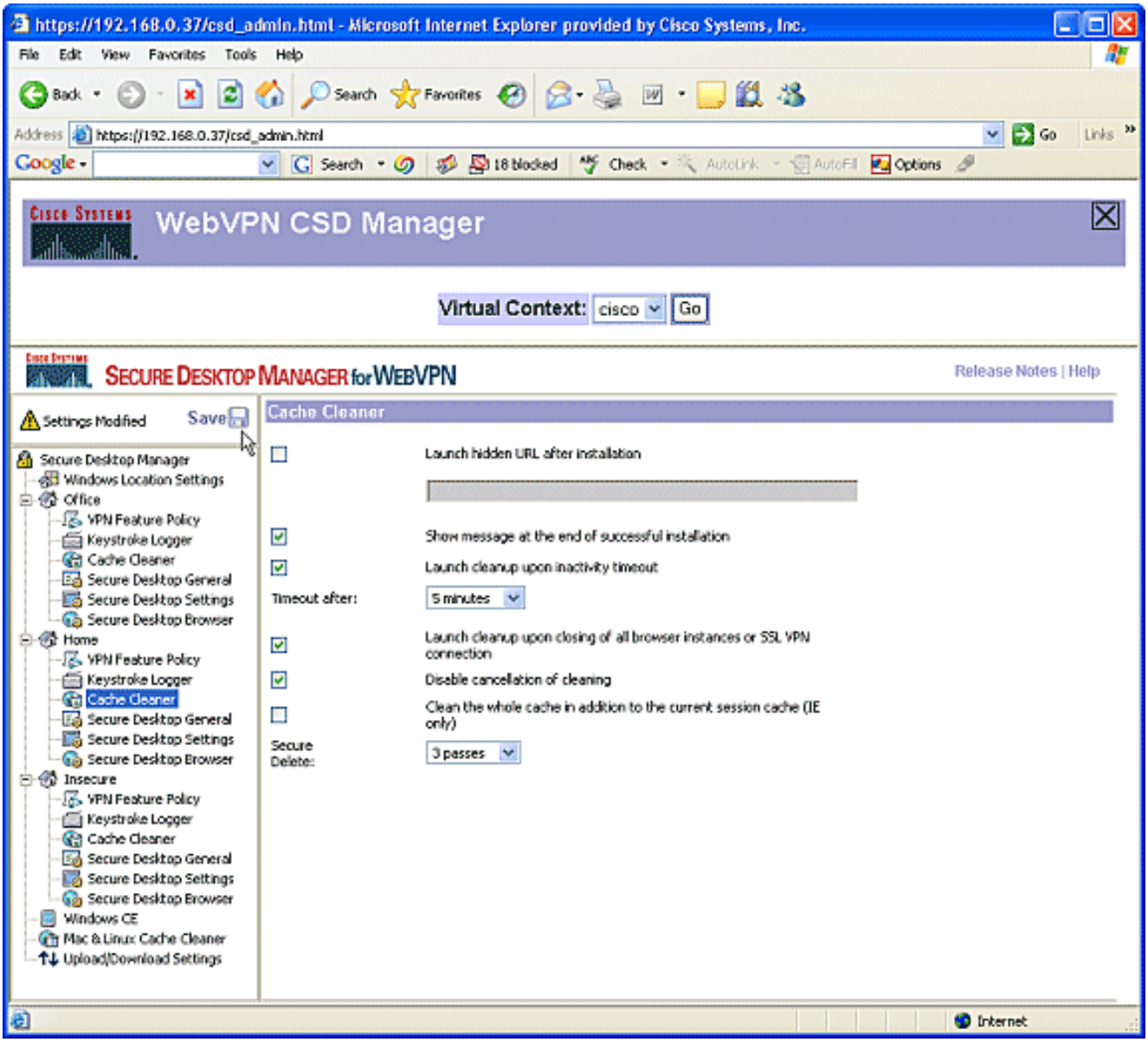
3. Klicken Sie für das Surfen im Internet auf die Schaltfläche mit den Auslassungszeichen, und wählen Sie die Kriterien aus, die übereinstimmen müssen. Klicken Sie im Dialogfeld auf **OK**.



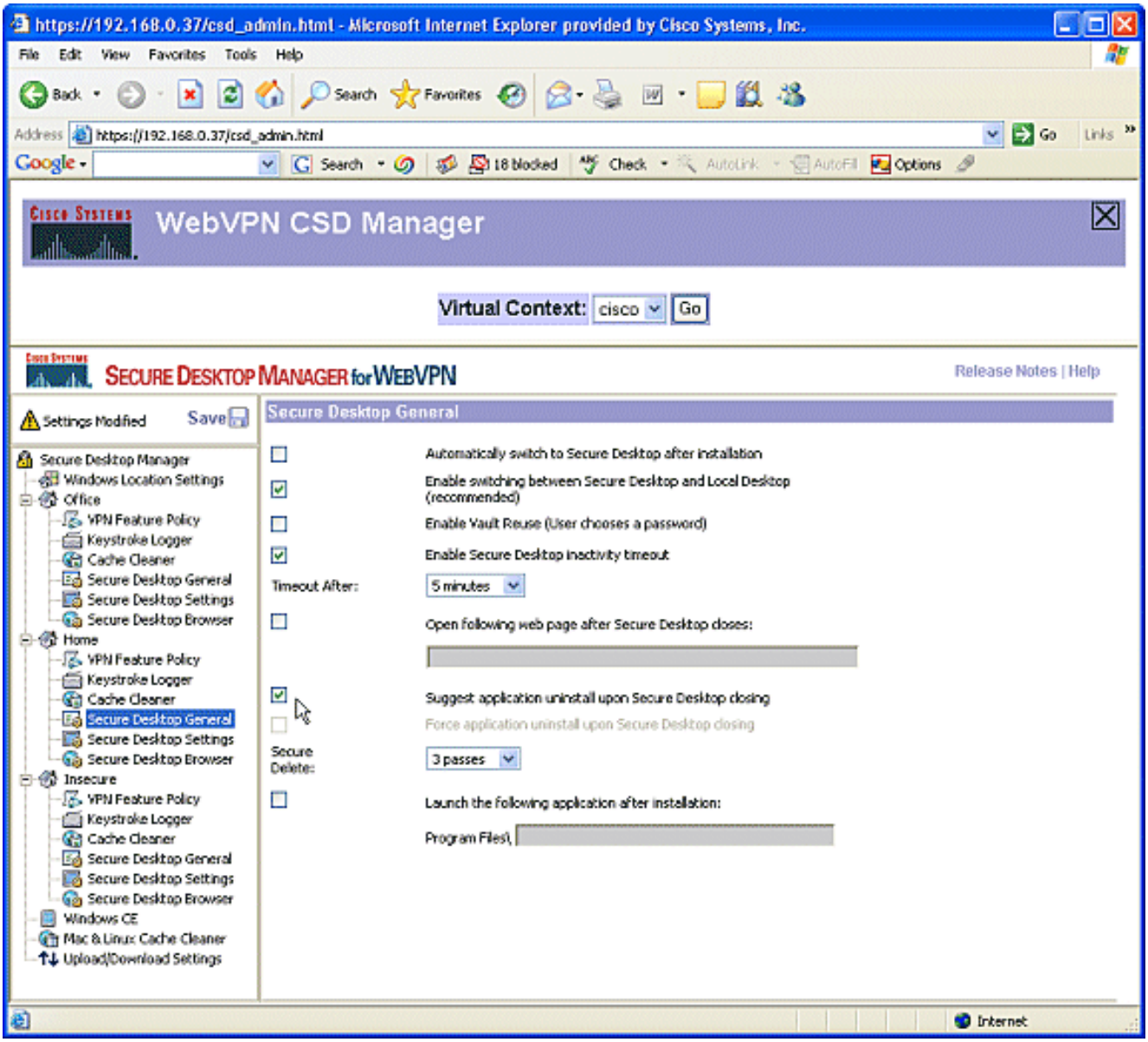
4. Sie können die anderen Zugriffsmethoden auf ähnliche Weise konfigurieren.Wählen Sie unter **Home** die Option **Keystroke Logger aus**.Aktivieren Sie das Kontrollkästchen neben **Nach Tastaturprotokollern suchen**.Wenn Sie dazu aufgefordert werden, klicken Sie auf **Speichern** und dann auf
OK.



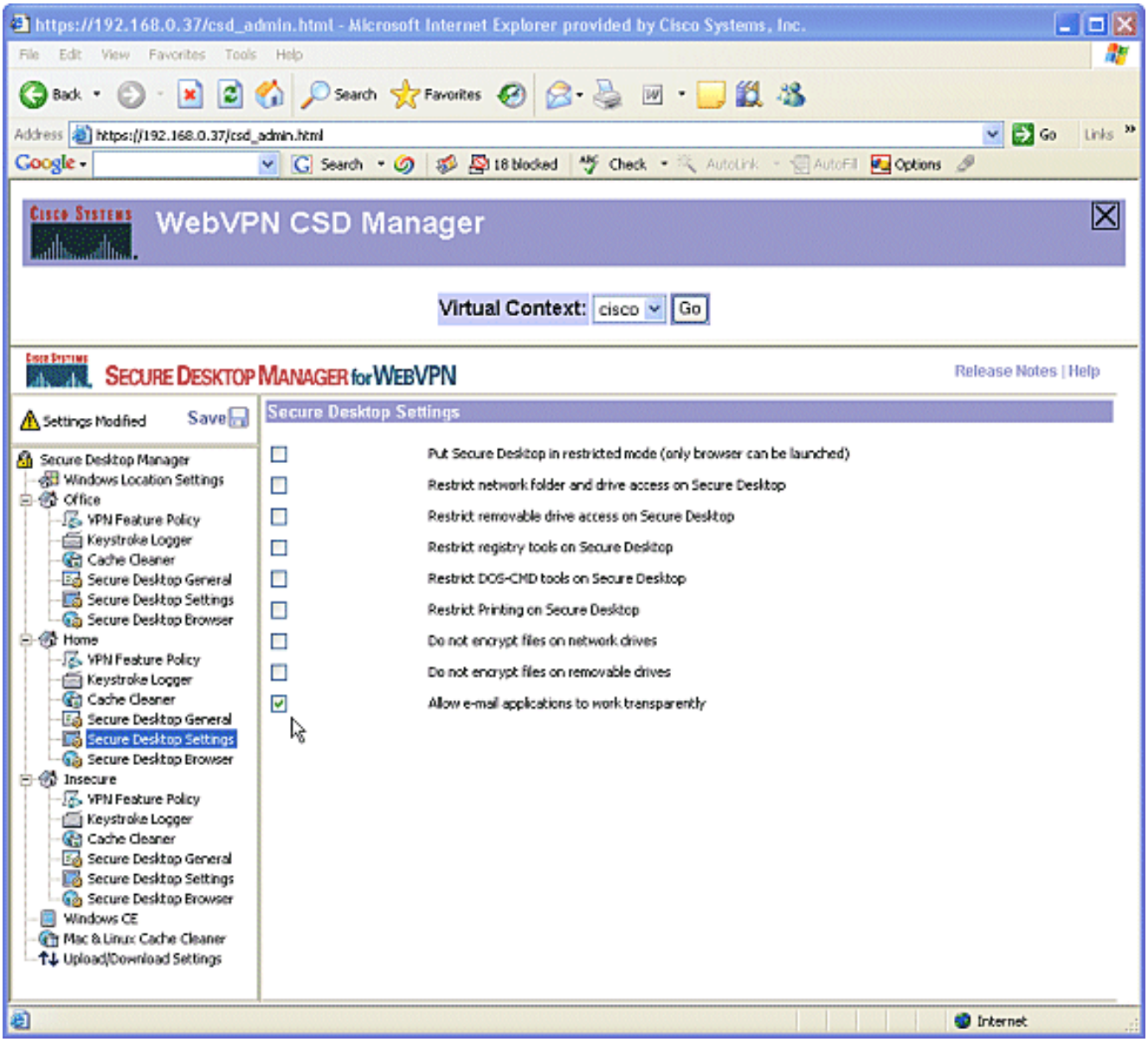
5. Wählen Sie unter "Home windows location" die Option **Cache Cleaner aus**. Lassen Sie die Standardeinstellungen unverändert, wie im Screenshot gezeigt.



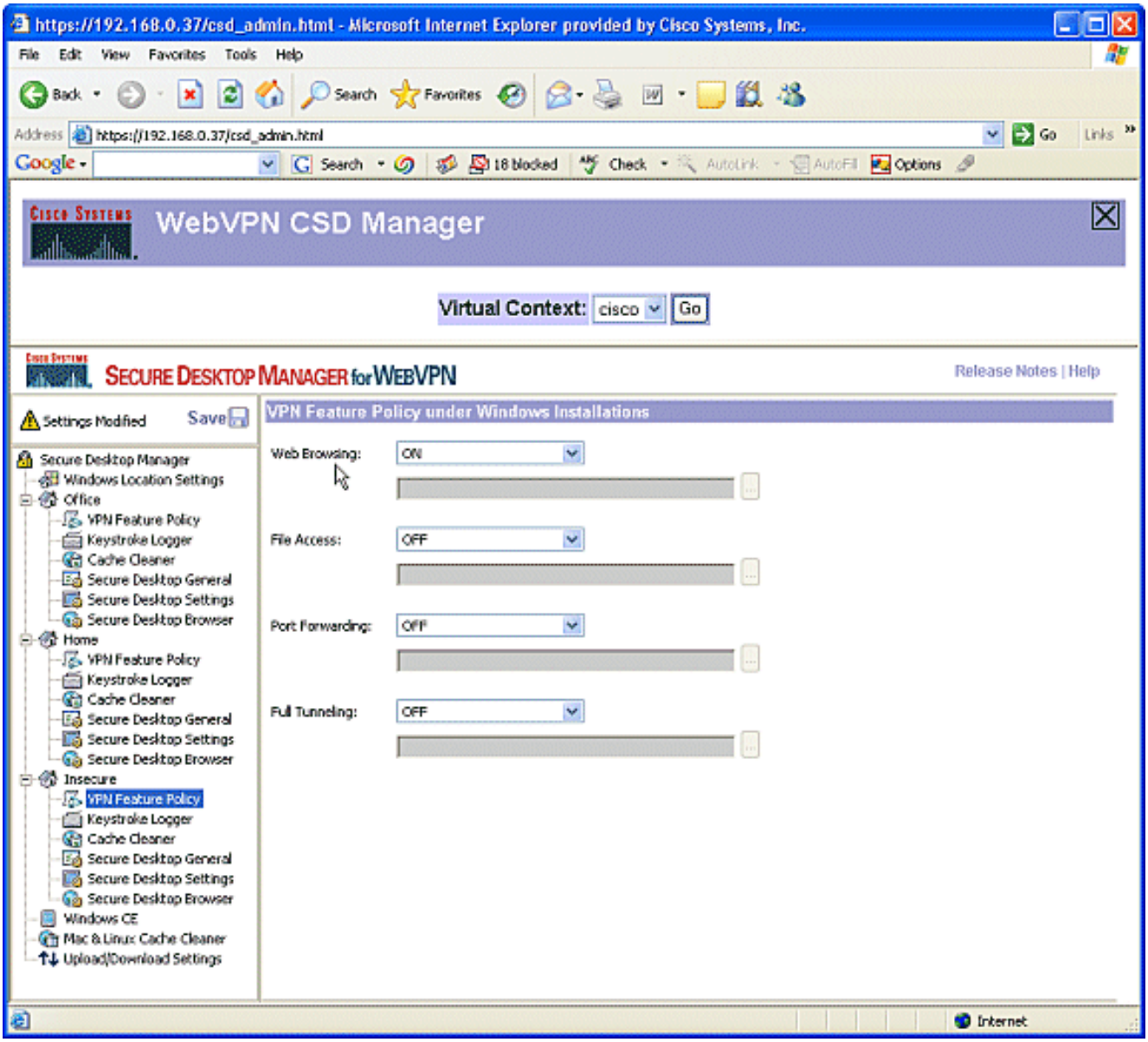
6. Wählen Sie unter Home die Option **Sicherer Desktop-Allgemein aus**. Aktivieren Sie die Option **Anwendungsdeinstallation beim Schließen des sicheren Desktops vorschlagen**. Lassen Sie alle anderen Parameter wie im Screenshot gezeigt in den Standardeinstellungen.



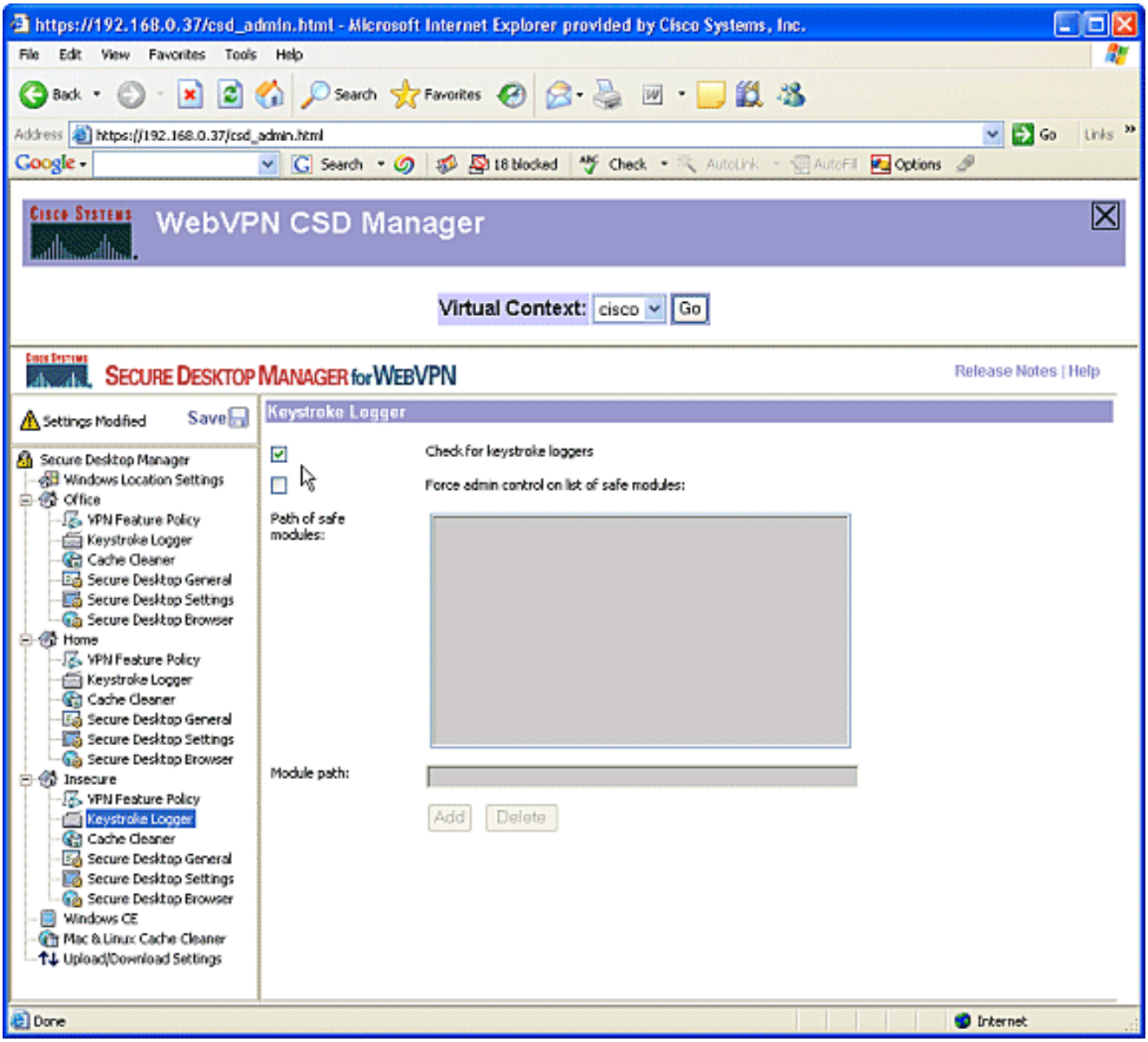
7. Wählen Sie für sichere Desktop-Einstellungen unter Home die Option **E-Mail-Anwendungen für ein transparentes Arbeiten zulassen aus**. Wenn Sie dazu aufgefordert werden, klicken Sie auf **Speichern** und dann auf **OK**.



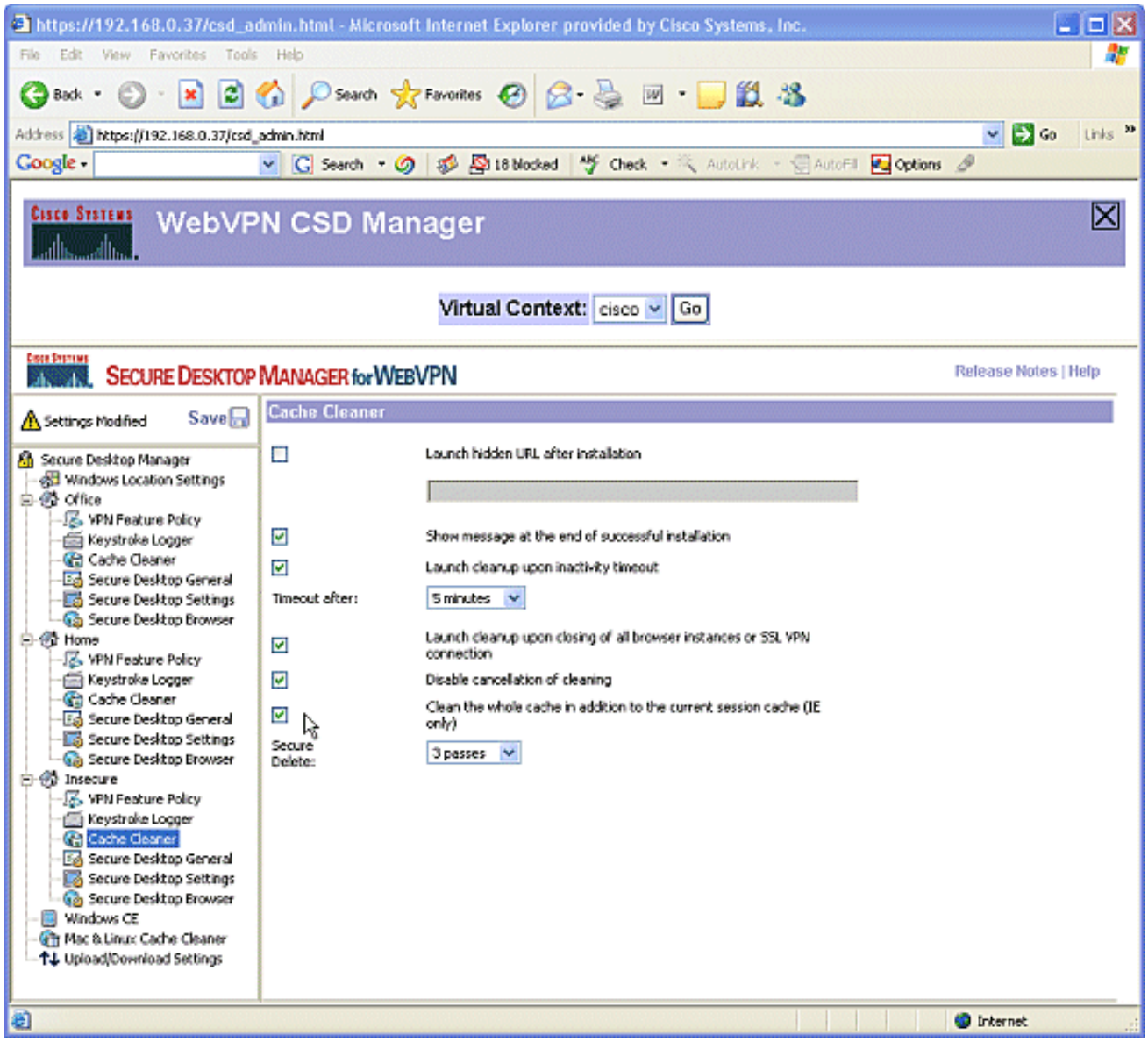
8. Die Konfiguration des **Secure Desktop Browsers** hängt davon ab, ob diese Benutzer auf eine Firmenwebsite mit vorkonfigurierten Favoriten zugreifen möchten.Wählen Sie unter Unsicher die Option **VPN Feature Policy (VPN-Funktionsrichtlinie)** aus.Da es sich nicht um vertrauenswürdige Benutzer handelt, erlauben Sie nur das Surfen im Internet.Wählen Sie **EIN** aus dem Dropdown-Menü für **Web Browsing aus**.Alle anderen Zugriffsrechte sind auf **OFF (AUS)**
eingestellt.



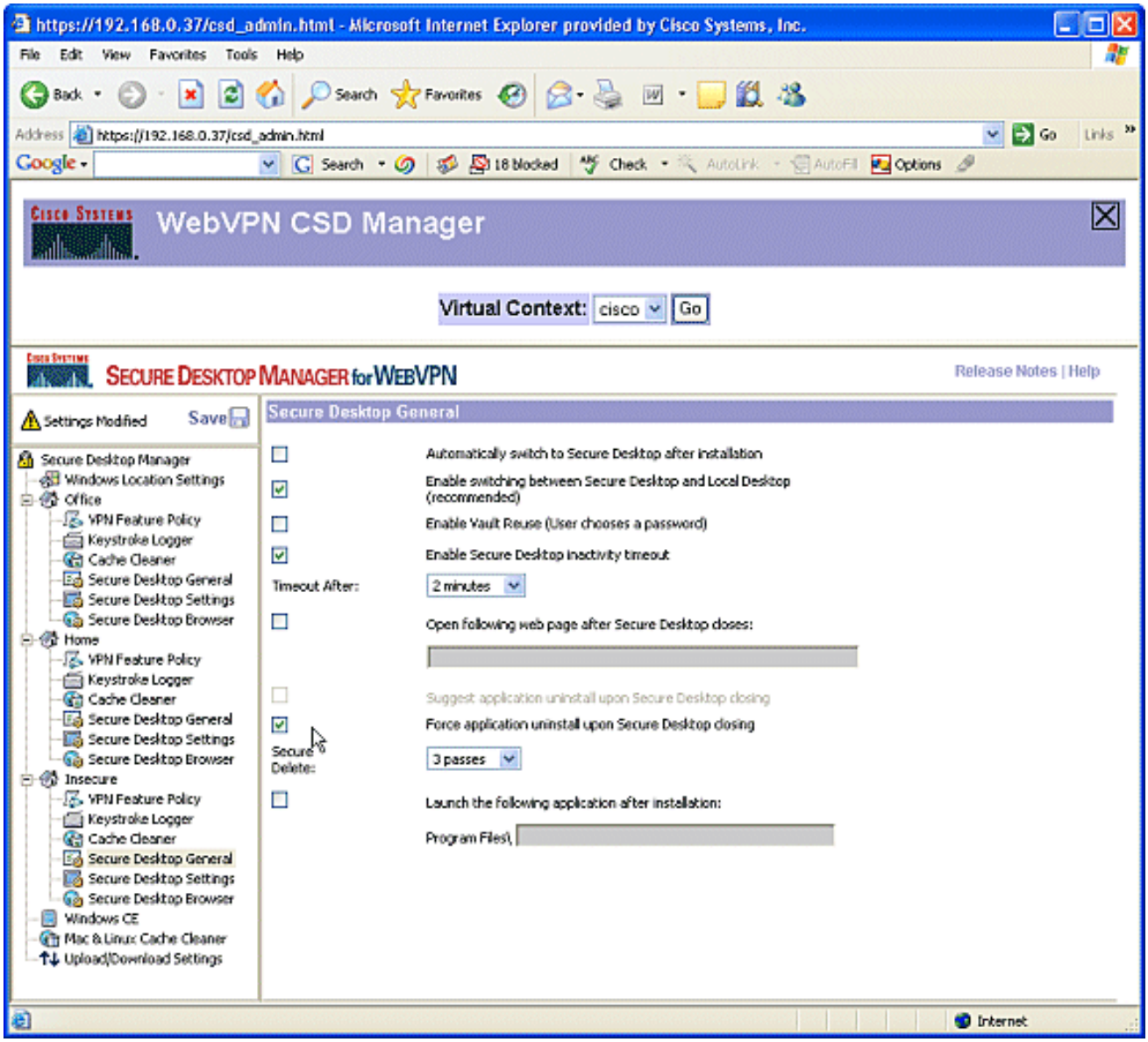
9. Aktivieren Sie das Kontrollkästchen **Nach Tastaturprotokollern suchen**.



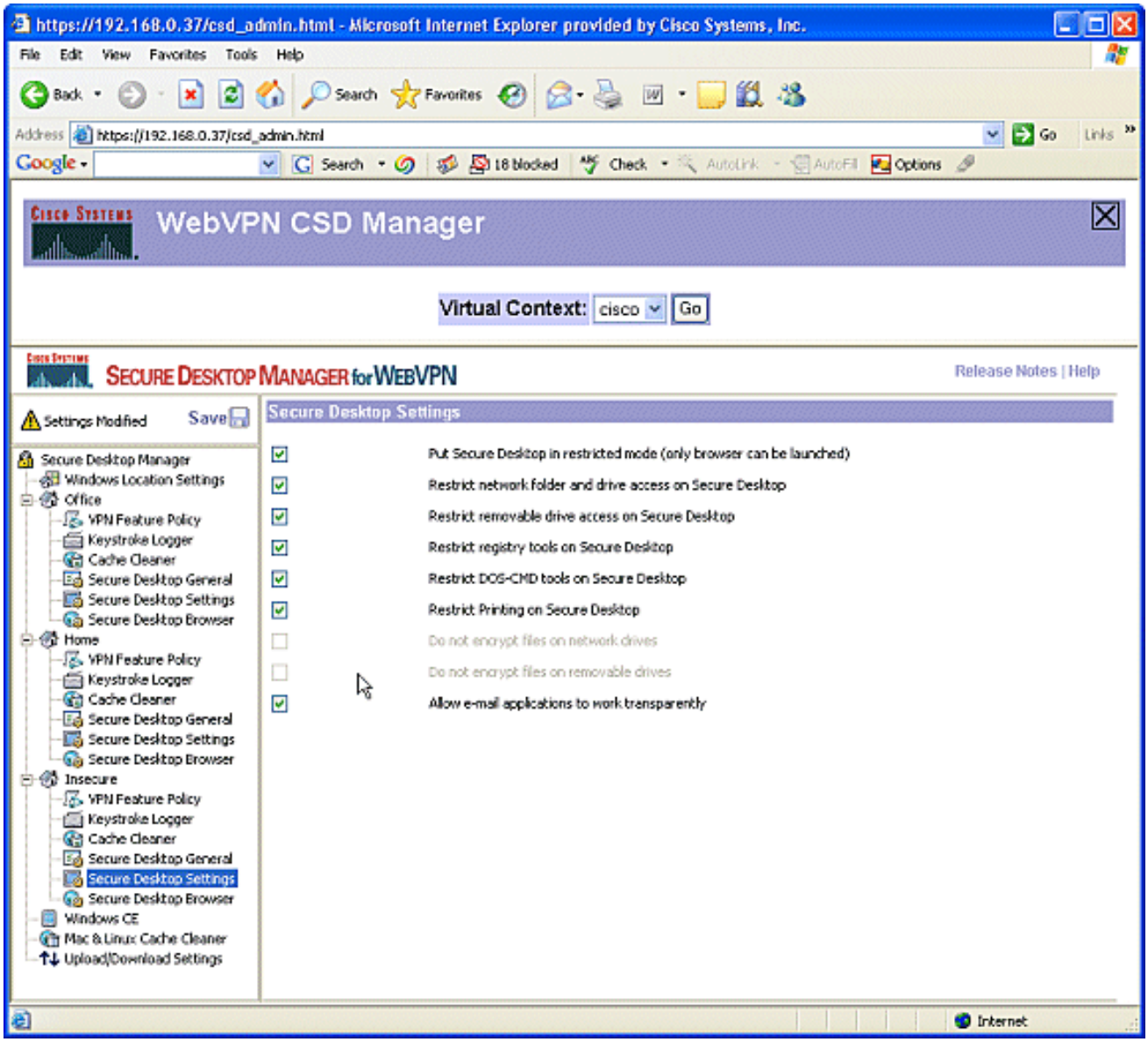
10. Konfigurieren Sie den Cache Cleaner für unsicher.Aktivieren Sie das Kontrollkästchen **Gesamten Cache über den aktuellen Sitzungscache (nur IE)** hinaus **reinigen**.Behalten Sie die anderen Standardeinstellungen
bei.



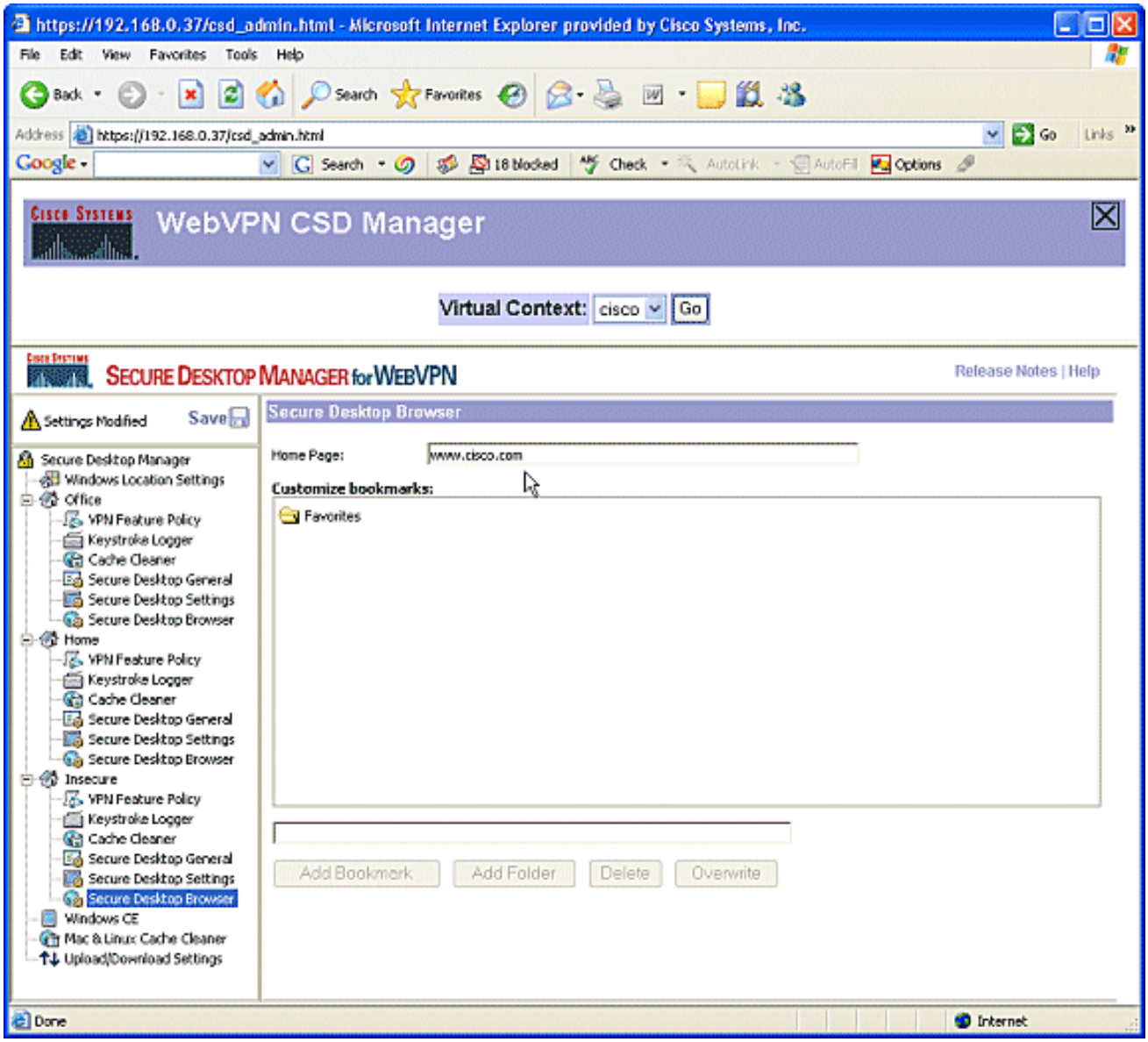
11. Wählen Sie unter Unsicher die Option **Sicherer Desktop-Allgemein aus**.Reduzieren Sie die Timeout-Inaktivität auf 2 Minuten.Aktivieren Sie das Kontrollkästchen **Anwendung erzwingen beim Schließen von sicherem Desktop deinstallieren**.



12. Wählen Sie **Sichere Desktop-Einstellungen** unter Unsicher, und konfigurieren Sie sehr restriktive Einstellungen wie
gezeigt.



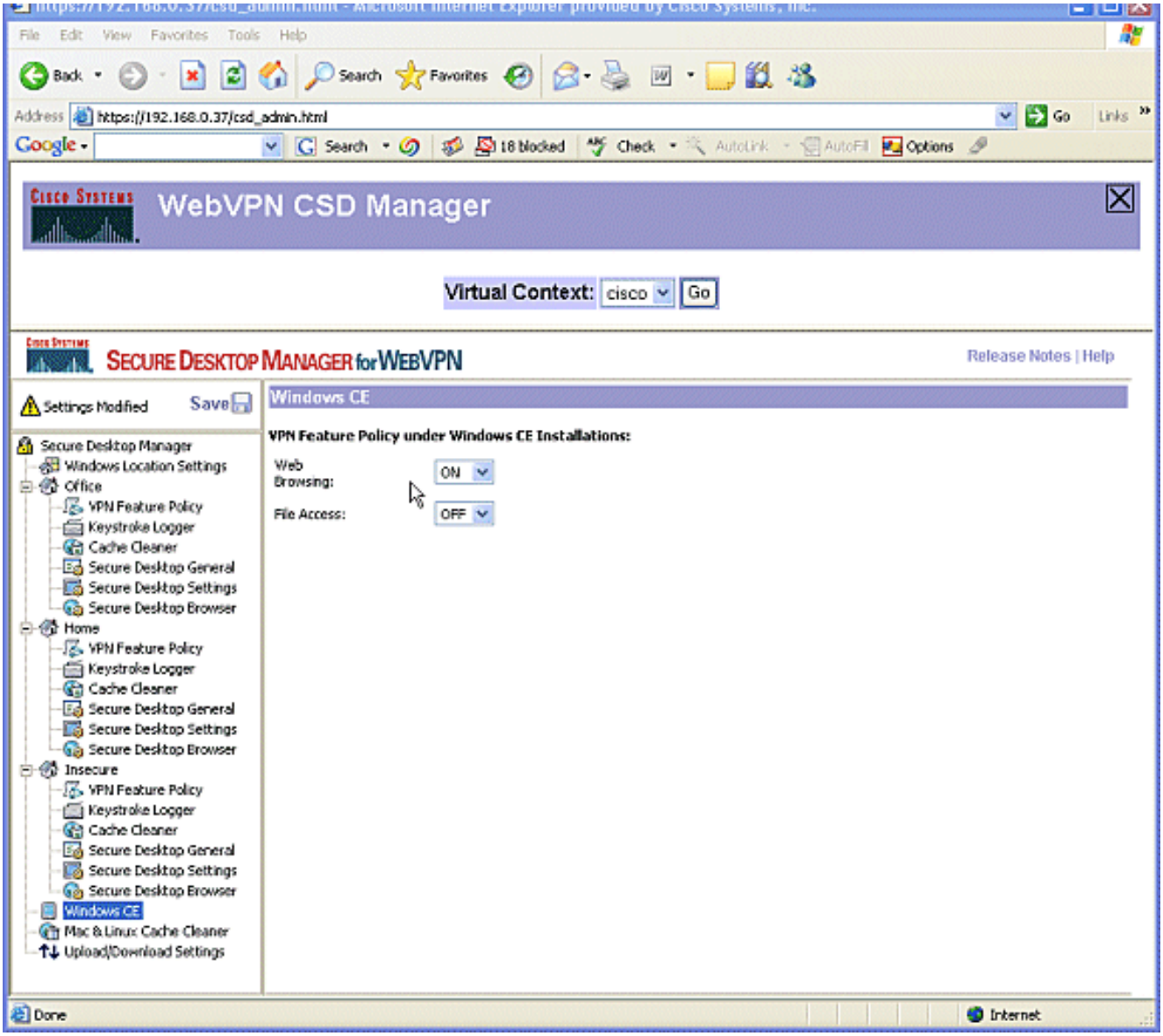
13. Wählen Sie **Sicherer Desktop-Browser aus**. Geben Sie im Feld Startseite (Startseite) die Website ein, zu der diese Clients für ihre Startseite geleitet werden sollen.



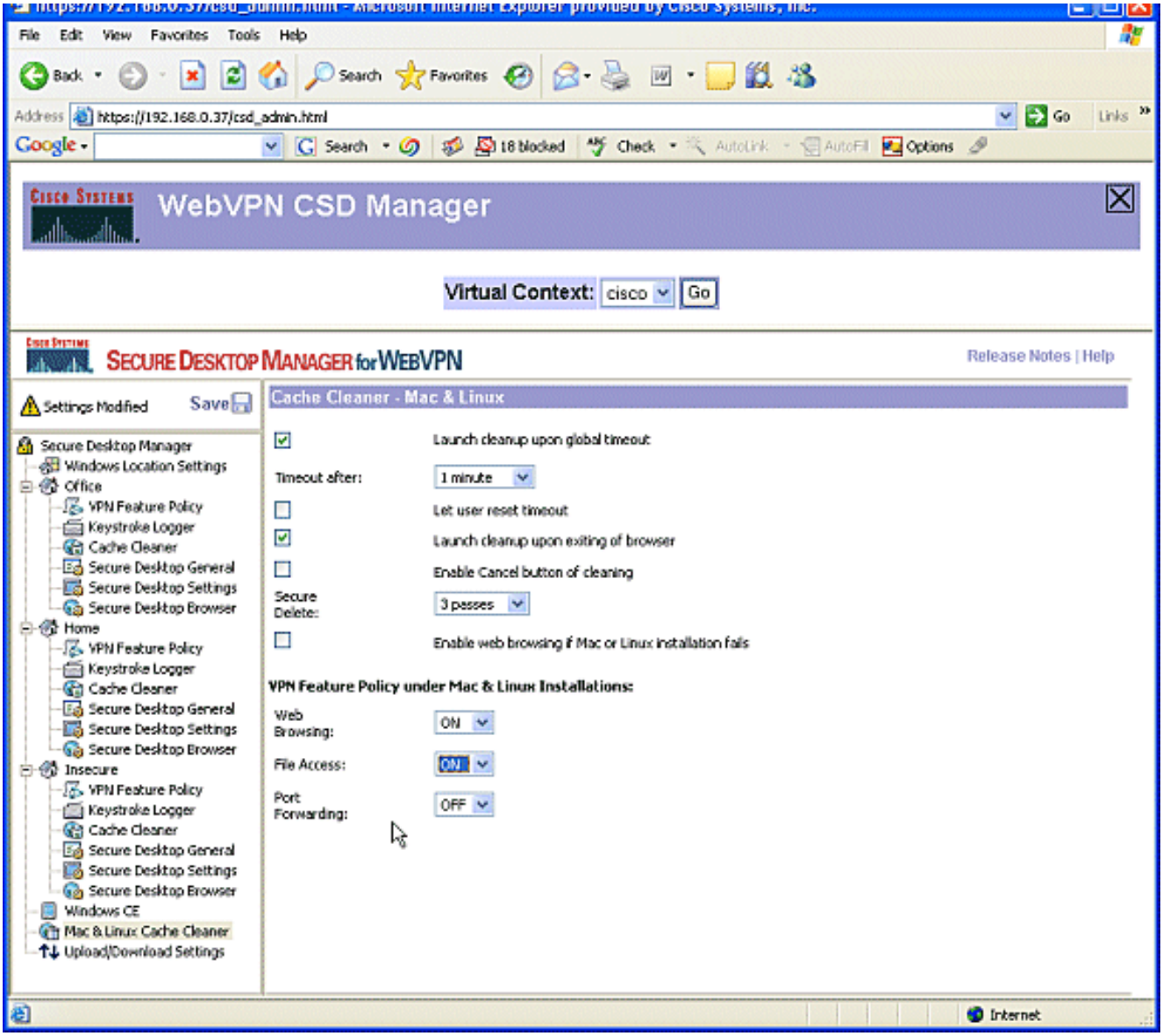
Phase II: Schritt 4: Konfigurieren Sie Windows CE-, Macintosh- und Linux-Features.

Konfigurieren Sie die CSD-Funktionen für Windows CE, Macintosh und Linux.

1. Wählen Sie **Windows CE** unter Sicherer Desktop-Manager aus. Windows CE verfügt über eingeschränkte VPN-Funktionen. Aktivieren Sie **die Option Internet-Browsen**.



2. Wählen Sie **Mac & Linux Cache Cleaner aus**.Die Macintosh- und Linux-Betriebssysteme haben nur Zugriff auf die Cache-Cleaner-Aspekte des CSD. Konfigurieren Sie sie wie in der Grafik dargestellt.Wenn Sie dazu aufgefordert werden, klicken Sie auf **Speichern** und dann auf
OK.

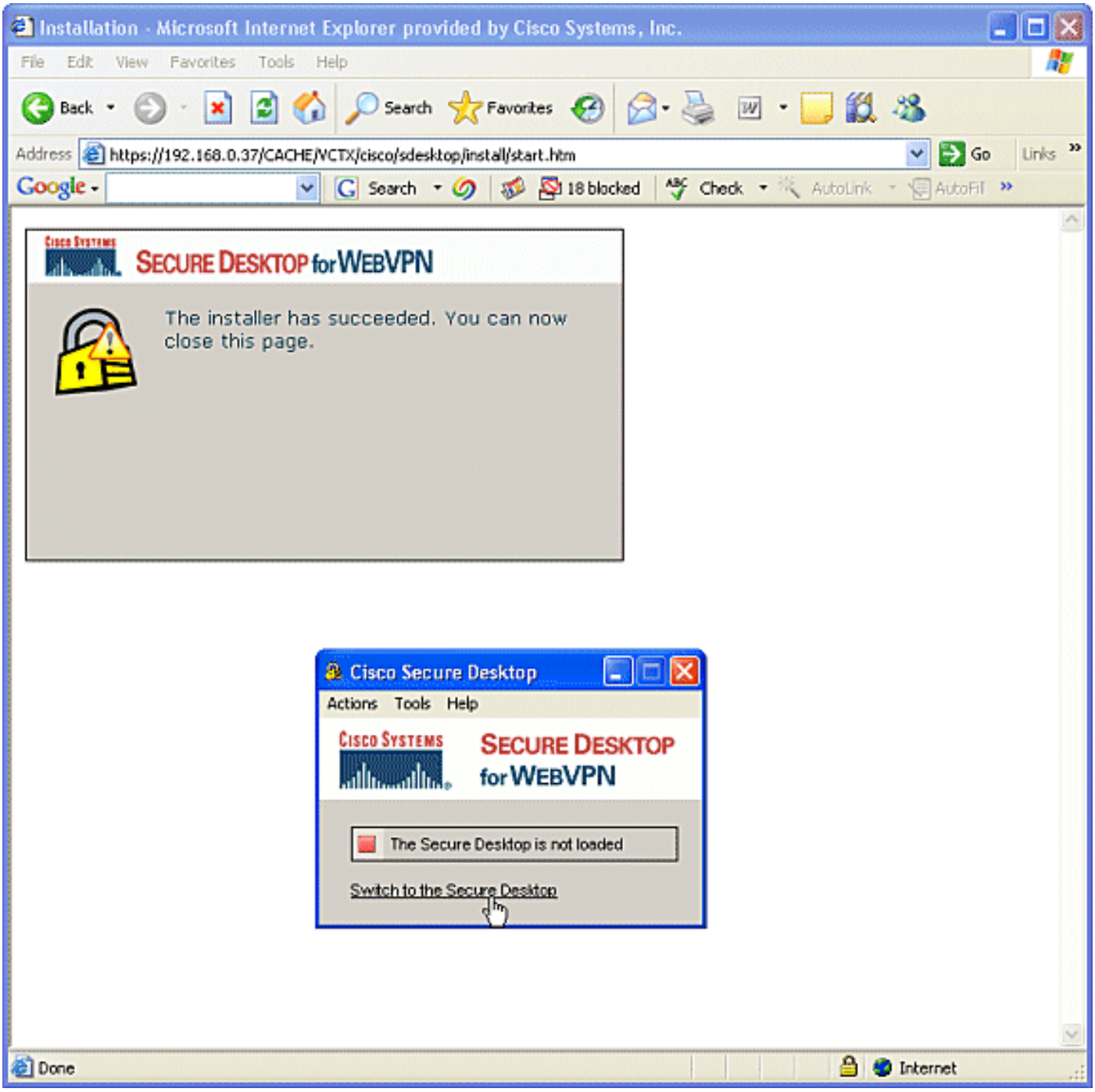


Überprüfung

CSD-Vorgang testen

Testen Sie den Betrieb des CSD, indem Sie eine Verbindung zum WebVPN-Gateway über einen SSL-fähigen Browser unter **https://WebVPN_Gateway_IP** herstellen.

Hinweis: Denken Sie daran, den eindeutigen Namen des Kontexts zu verwenden, wenn Sie unterschiedliche WebVPN-Kontexte erstellt haben, z. B. **https://192.168.0.37/cisco**.



Befehle

Mehrere **show**-Befehle sind WebVPN zugeordnet. Sie können diese Befehle in der Befehlszeilenschnittstelle (CLI) ausführen, um Statistiken und andere Informationen anzuzeigen. Detaillierte Informationen zu **show**-Befehlen finden Sie unter Verifying WebVPN Configuration.

Hinweis: Der CLI Analyzer (nur registrierte Kunden) unterstützt bestimmte **show**-Befehle. Verwenden Sie den CLI Analyzer, um eine Analyse der **Ausgabe** des **Befehls show** anzuzeigen.

Fehlerbehebung

Befehle

Dem WebVPN sind mehrere **Debugbefehle** zugeordnet. Ausführliche Informationen zu diesen

Befehlen finden Sie unter Verwenden von WebVPN-Debug-Befehlen.

Hinweis: Die Verwendung von **Debug-**Befehlen kann sich negativ auf Ihr Cisco Gerät auswirken. Bevor Sie **Debug-**Befehle verwenden, lesen Sie die Informationen unter Wichtige Informationen über Debug-Befehle.

Weitere Informationen zu **Clear** Befehlen finden Sie unter Verwenden von WebVPN Clear-Befehlen.

Zugehörige Informationen

- Implementierungsleitfaden für WebVPN- und DMVPN-Konvergenz
- SSL VPN - WebVPN
- Cisco IOS SSL VPN
- Technischer Support und Dokumentation für Cisco Systeme