Configureer CSD op Cisco IOS met behulp van DSL

Inhoud

Inleiding

Hoewel Secure Socket Layer (SSL) VPN-sessies (Cisco WebVPN) veilig zijn, kan de client nog steeds koekjes, browser bestanden en e-mailbijlagen hebben na voltooiing van een sessie. Cisco Secure Desktop (CSD) breidt de inherente beveiliging van SSL VPN-sessies uit door sessiegegevens in een gecodeerde indeling te schrijven naar een speciaal gebied van de schijf van de client. Bovendien worden deze gegevens aan het einde van de SSL VPN-sessie van de schijf verwijderd. Dit document presenteert een voorbeeldconfiguratie voor CSD op een Cisco IOS® router.

CSD wordt ondersteund op de volgende Cisco-platforms:

- Cisco IOS-routers versie 12.4(6)T en hoger
- Cisco 870.181.1841, 2801, 2811, 2821, 2851, 3725, 3745, 3825, 3845, 7200 en 733 1 routers
- Cisco VPN 3000 Series Concentrators versie 4.7 en hoger
- Cisco ASA 5500 Series security applicaties versie 7.1 en hoger
- Cisco Webex VPN servicesmodule voor Cisco Catalyst en Cisco 7600 Series versie 1.2 en

hoger

Voorwaarden

Vereisten

Zorg ervoor dat u aan deze vereisten voldoet voordat u deze configuratie probeert:

Vereisten voor de Cisco IOS-router

- Cisco IOS-router met geavanceerde afbeelding 12.4(6T) of hoger
- Cisco Router Secure Devices Manager (DSM) 2.3 of hoger
- Een exemplaar van het CSD voor IOS-pakket op uw beheerstation
- Een router met zelfgetekend digitaal certificaat of verificatie met een certificaatinstantie (CA)**Opmerking:** Als u digitale certificaten gebruikt, zorg er dan voor dat u de hostname, domeinnaam en date/time/timezone van de router juist instelt.
- Kunt u een geheim wachtwoord op de router inschakelen
- DNS ingeschakeld op uw router. Voor meerdere WebVPN-services is DNS nodig om goed te werken.

Eisen voor clientcomputers

- Afstandsklanten dienen lokale administratieve rechten te hebben; het is niet nodig , maar het is zeer gesuggereerd .
- Afstandsklanten moeten beschikken over Java Runtime Environment (JRE) versie 1.4 of hoger.
- Afstandsbrowsers: Internet Explorer 6.0, Netscape 7.1, Mozilla 1.7, Safari 1.2.2 of Firefox 1.0
- Gebruikte koekjes en populaties toegestaan op externe klanten

Gebruikte componenten

De informatie in dit document is gebaseerd op de volgende software- en hardware-versies:

- Cisco IOS-router 3825 met versie 12.9(T)
- versie 2.3.1

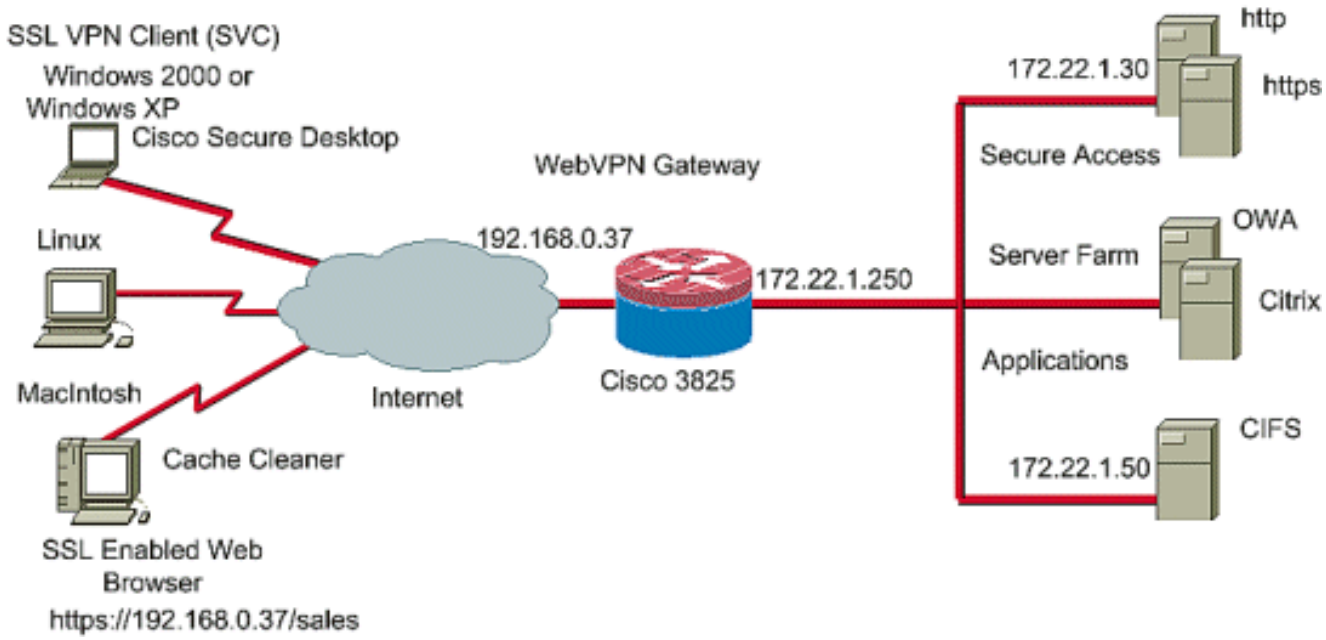
De informatie in dit document is gebaseerd op de apparaten in een specifieke laboratoriumomgeving. Alle apparaten die in dit document worden gebruikt, begonnen met een gewiste (standaard) configuratie. Als uw netwerk live is, moet u de potentiële impact van elke opdracht begrijpen.

Netwerkdiagram

Het netwerk in dit document is als volgt opgebouwd:

Dit voorbeeld gebruikt een router van Cisco 3825 Series om veilige toegang tot het intranet van het bedrijf toe te staan. De Cisco 3825 Series router verbetert de beveiliging van SSL VPN-verbindingen met configureerbare CSD-functies en -eigenschappen. Clients kunnen via een van deze drie SSL VPN-methoden een verbinding maken met de door CSD geactiveerd router: Clientloze SSL VPN (WebVPN), Thin-Client SSL VPN (Port-Forwarding) of SSL VPN-client (Full

Tunneling SVC).



Verwante producten

Deze configuratie kan ook worden gebruikt in combinatie met deze hardware- en softwareversies:

- Cisco-routerplatforms 870.1811.1841.2801.2811.2821 2851.3725.3745.3825.3845, 7200 en 73 01
- Cisco IOS geavanceerde security afbeelding 12.4(6)T en hoger

Conventies

Raadpleeg de Cisco Technical Tips Convention voor meer informatie over documentconventies.

Configureren

Een gateway van WebVPN staat een gebruiker toe om met de router via één van de SSL VPN technologieën te verbinden. Slechts één gateway van WebVPN per IP adres is toegestaan op het apparaat, alhoewel meer dan één context van WebVPN aan een gateway van WebVPN kan worden verbonden. Elke context is geïdentificeerd met een unieke naam. Groepsbeleid identificeert de geconfigureerde resources die beschikbaar zijn voor een bepaalde WebVPN-context.

Configuratie van CSD op een IOS-router wordt in twee fasen verwezenlijkt:

Fase I: Bereid uw router voor de configuratie van het CSD met ontwikkel

1. Configureer de gateway van WebVPN, de context van WebVPN en het groepsbeleid.**N.B.:** Deze stap is optioneel en wordt in dit document niet uitvoerig behandeld. Als u uw router voor een van de SSL VPN-technologieën al hebt ingesteld, laat u deze stap dan achter.
2. CSD in een WebVPN-context inschakelen.

Fase II: CSD configureren met behulp van een webbrowser.

1. Bepaal de *locaties van Windows*.
2. Identificeer locatiecriteria.
3. Configuratie van de modules en de eigenschappen van de Plaats van Windows.
4. Configuratie van de eigenschappen van Windows CE, Macintosh en Linux.

Fase I: Bereid uw router voor CSD configuratie voor met het middel.

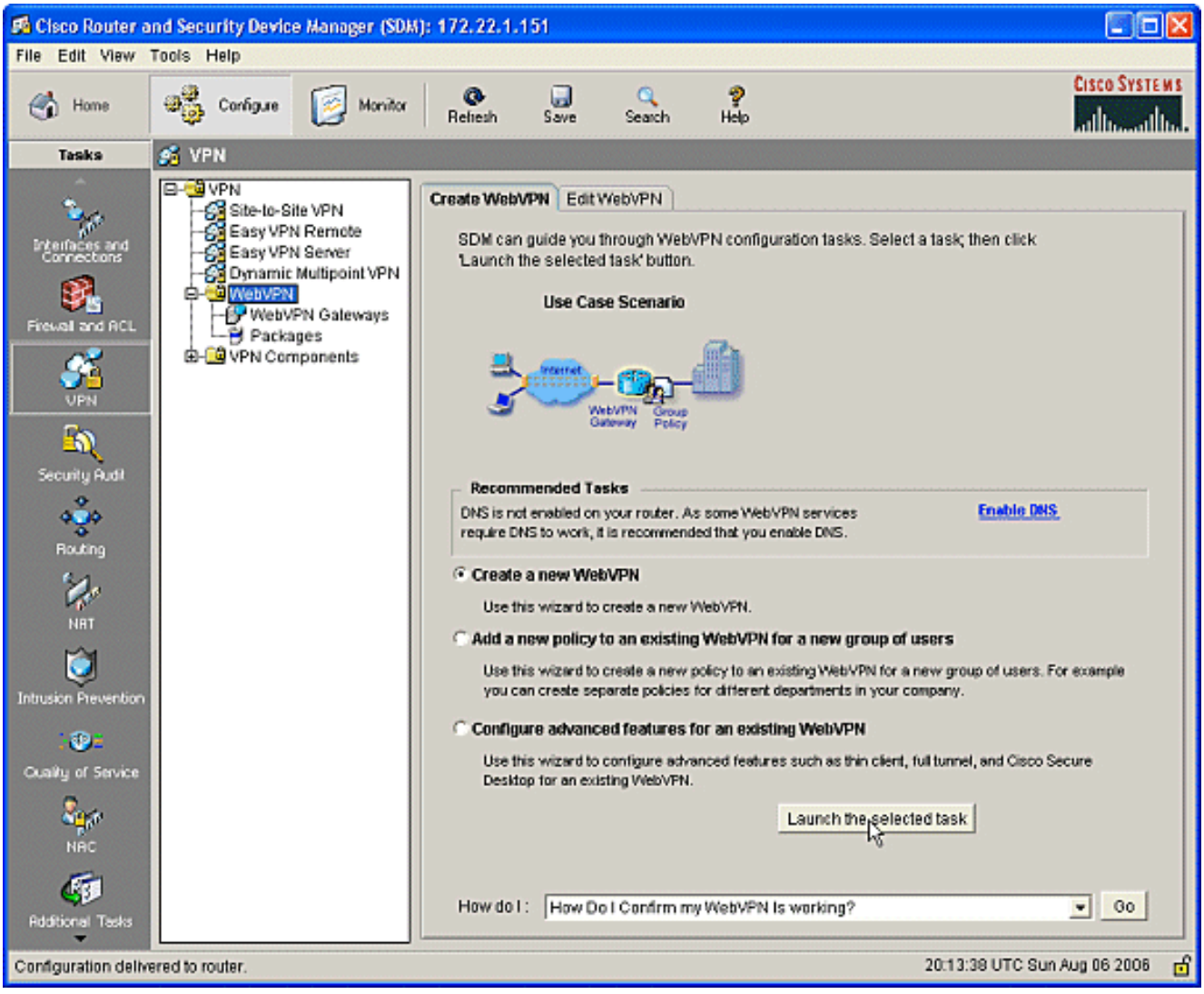
CSD kan worden ingesteld met een dm of van de opdrachtregel interface (CLI). Deze configuratie gebruikt een browser en een browser.

Deze stappen worden gebruikt om de configuratie van CSD op uw IOS-router te voltooien.

Fase I: Stap 1: Configureer de gateway van WebVPN, de context en het groepsbeleid.

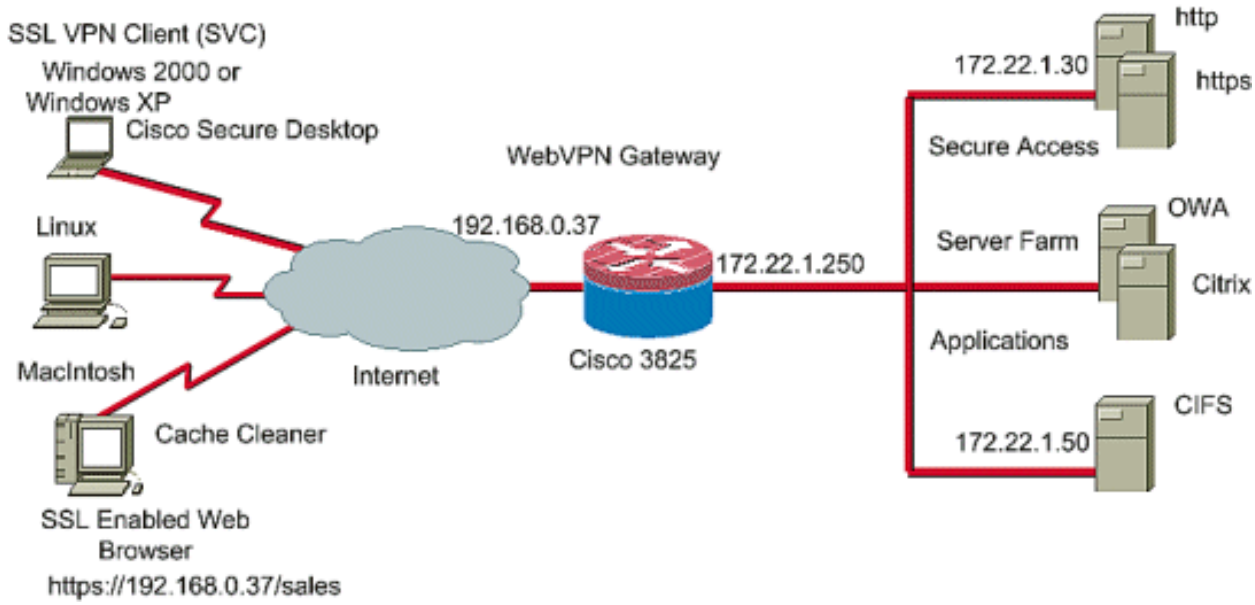
U kunt de WebVPN Wizard gebruiken om deze taak te volbrengen.

1. Open slechts ontwikkkeling en ga naar **het configureren > VPN > WebVPN**. Klik op het tabblad **WebVPN maken** en controleer de radioknop **Webex** maken. Klik op **De geselecteerde taak starten**.

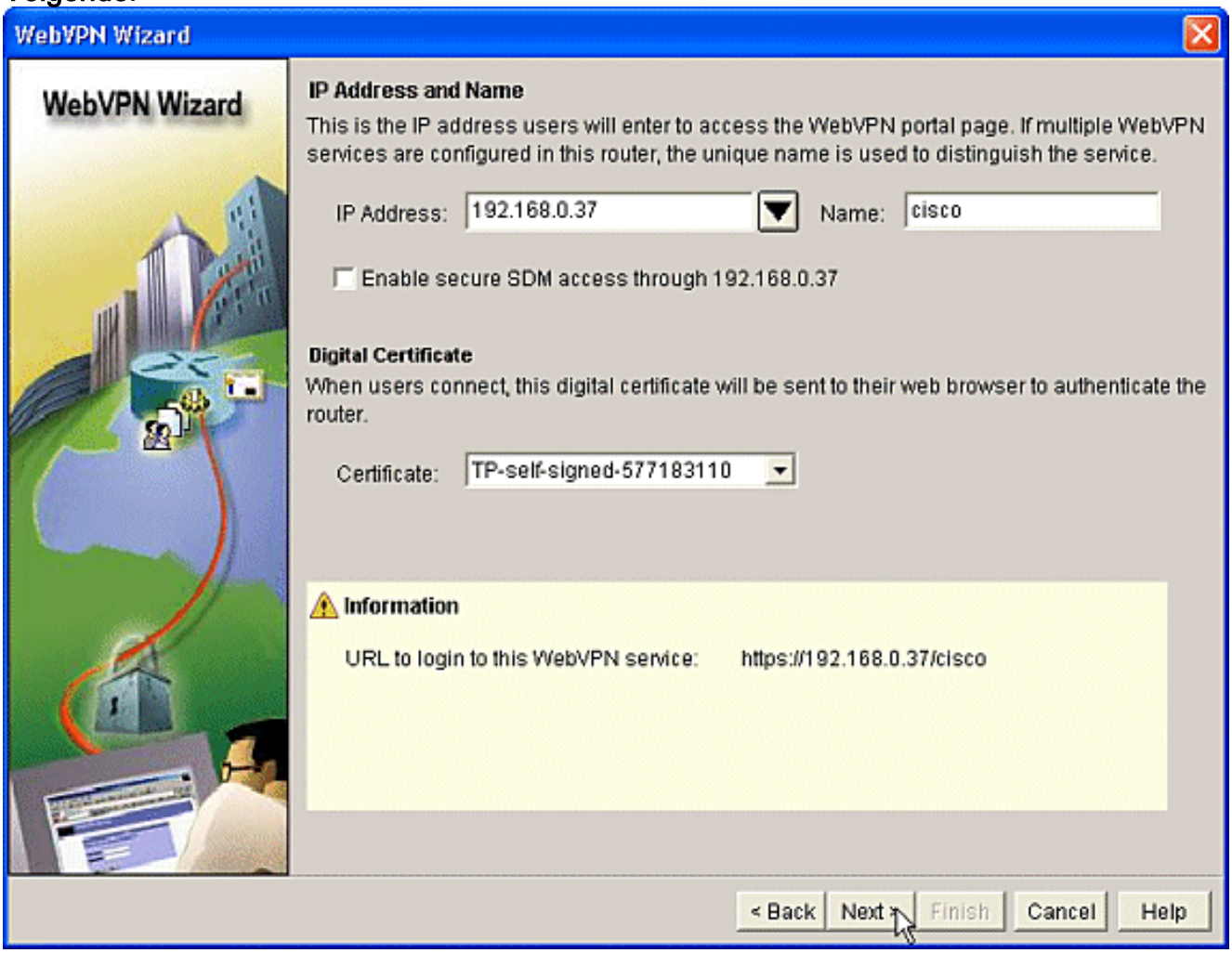


2. Het scherm van de Wizard Webex maakt een lijst van de parameters die u kunt configureren.

Klik op
Volgende.

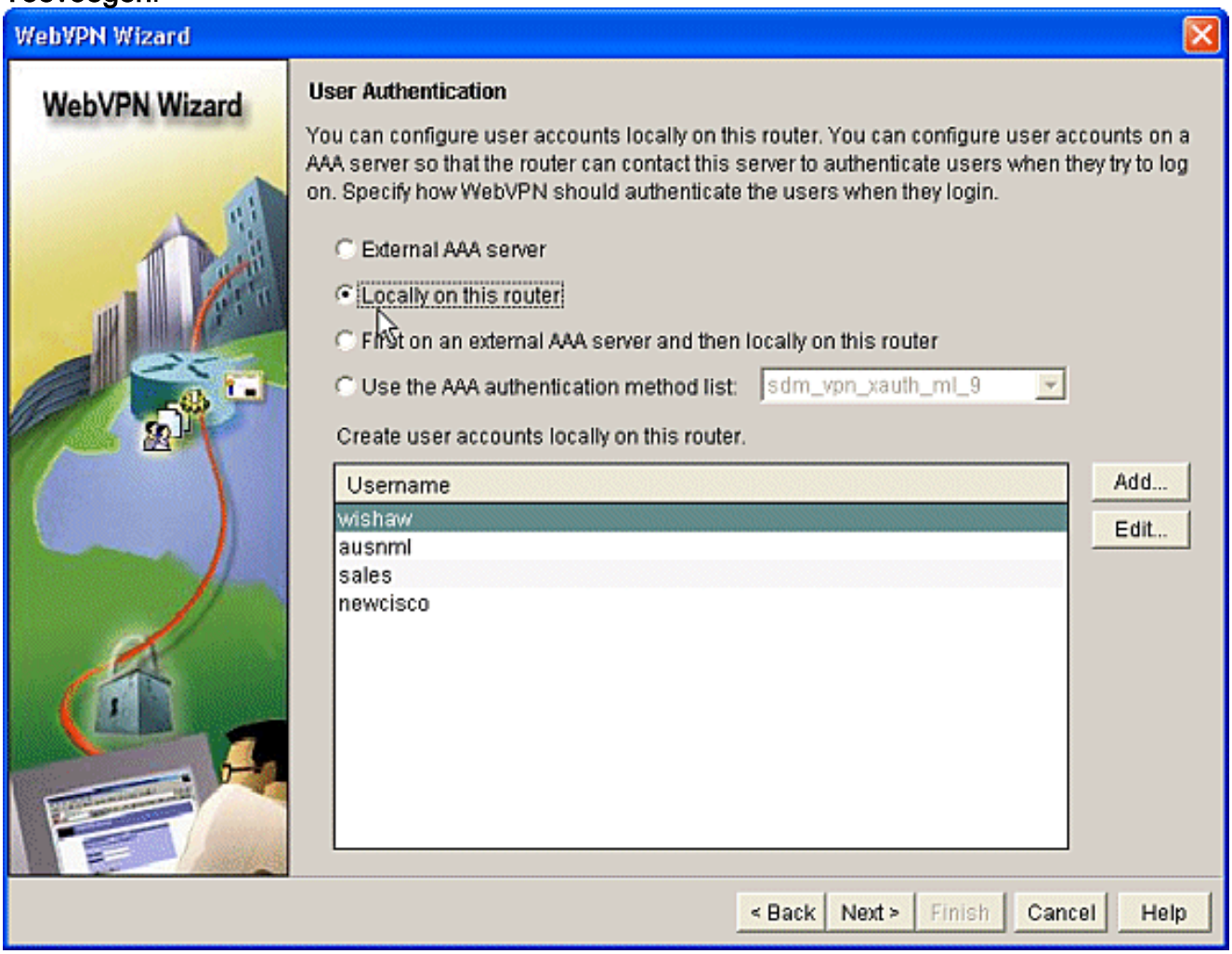


3. Voer het IP-adres in voor de WebVPN-gateway, een unieke naam voor de service en informatie over het digitale certificaat. Klik op
Volgende.

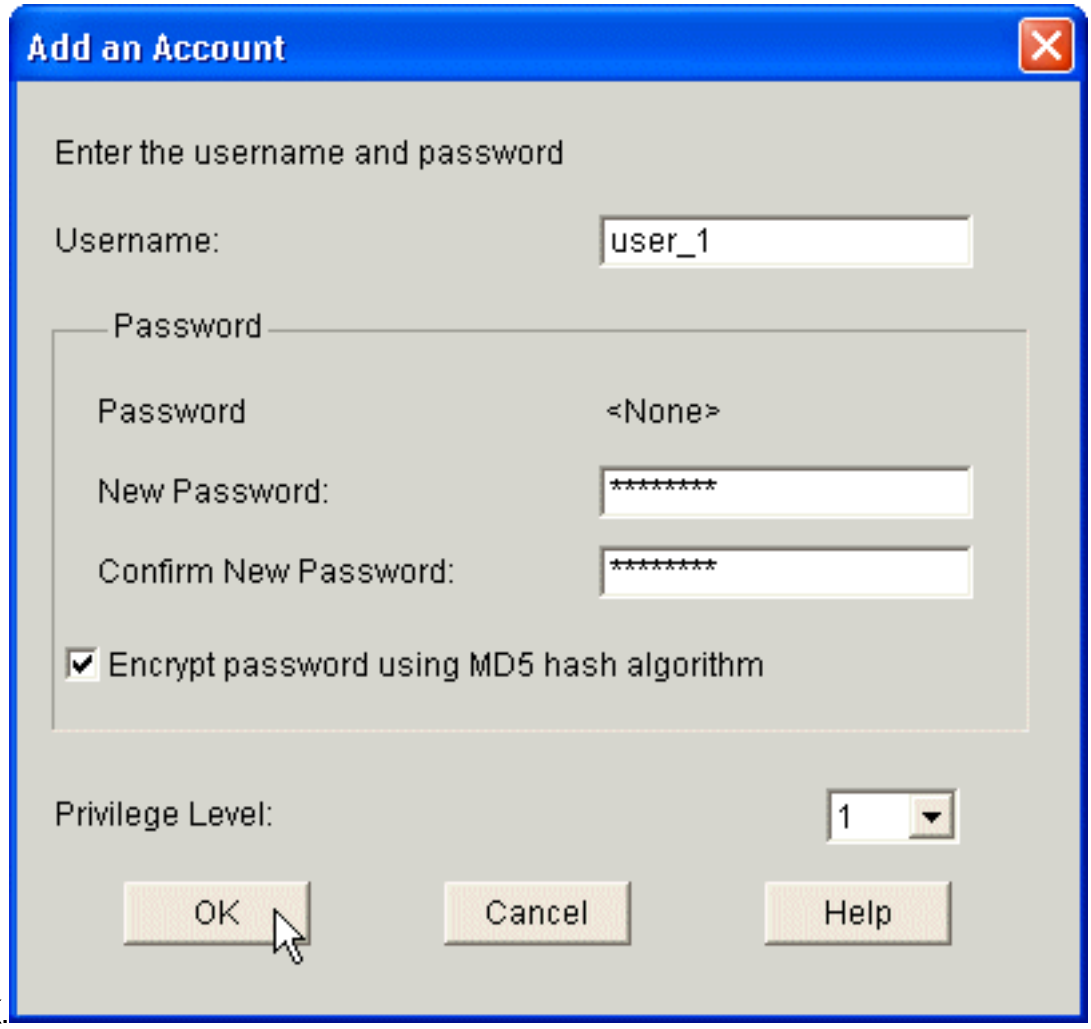


4. Gebruikersrekeningen kunnen worden gemaakt voor verificatie naar deze WebVPN-gateway. U kunt lokale rekeningen of rekeningen gebruiken die op een externe verificatie-, autorisatie- en accounting-server (AAA) zijn gemaakt. Dit voorbeeld gebruikt lokale rekeningen op de router. Controleer de radioknop **lokaal op deze router** en klik op

Toevoegen.

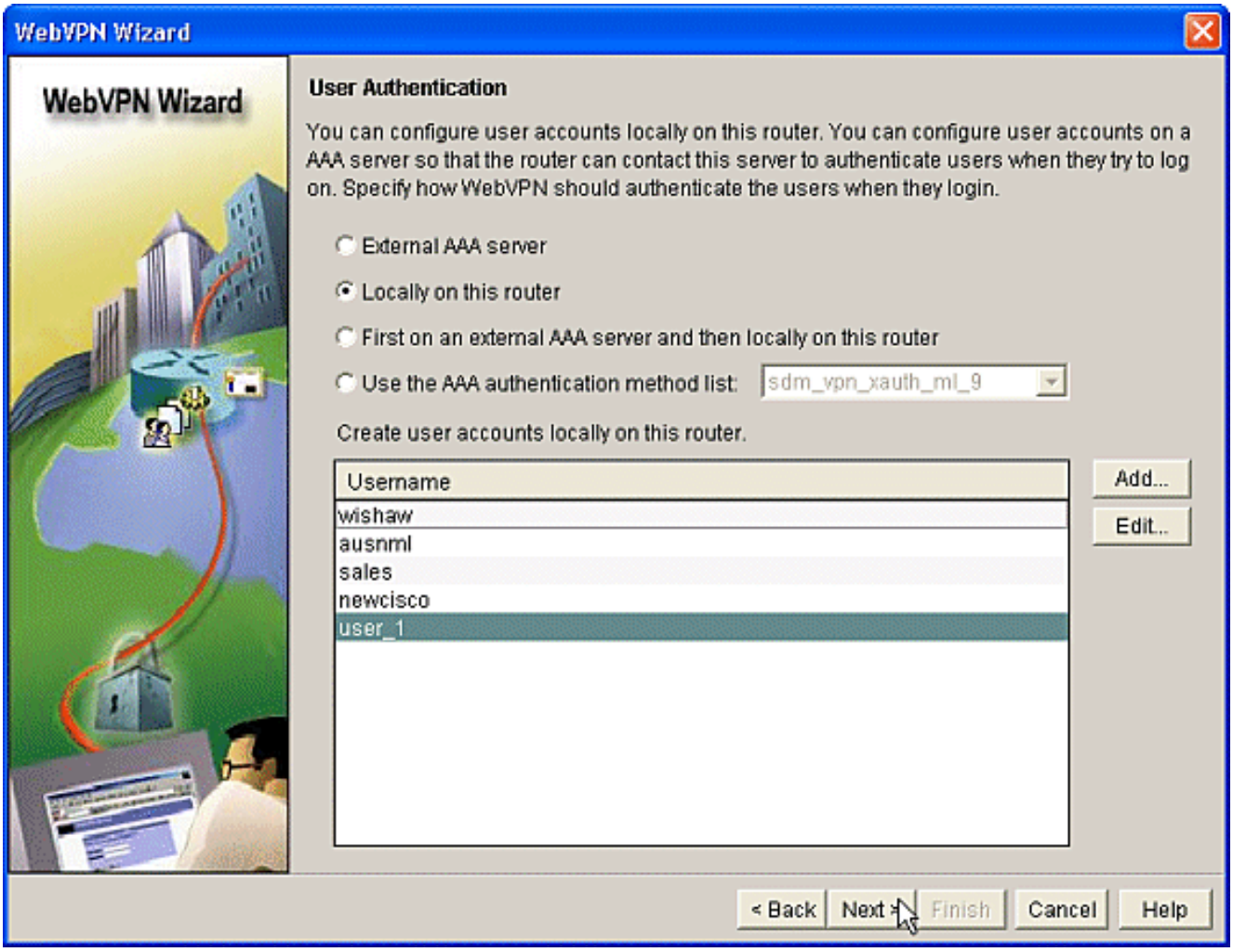


5. Voer de accountinformatie voor de nieuwe gebruiker in op het scherm Toevoegen en klik op

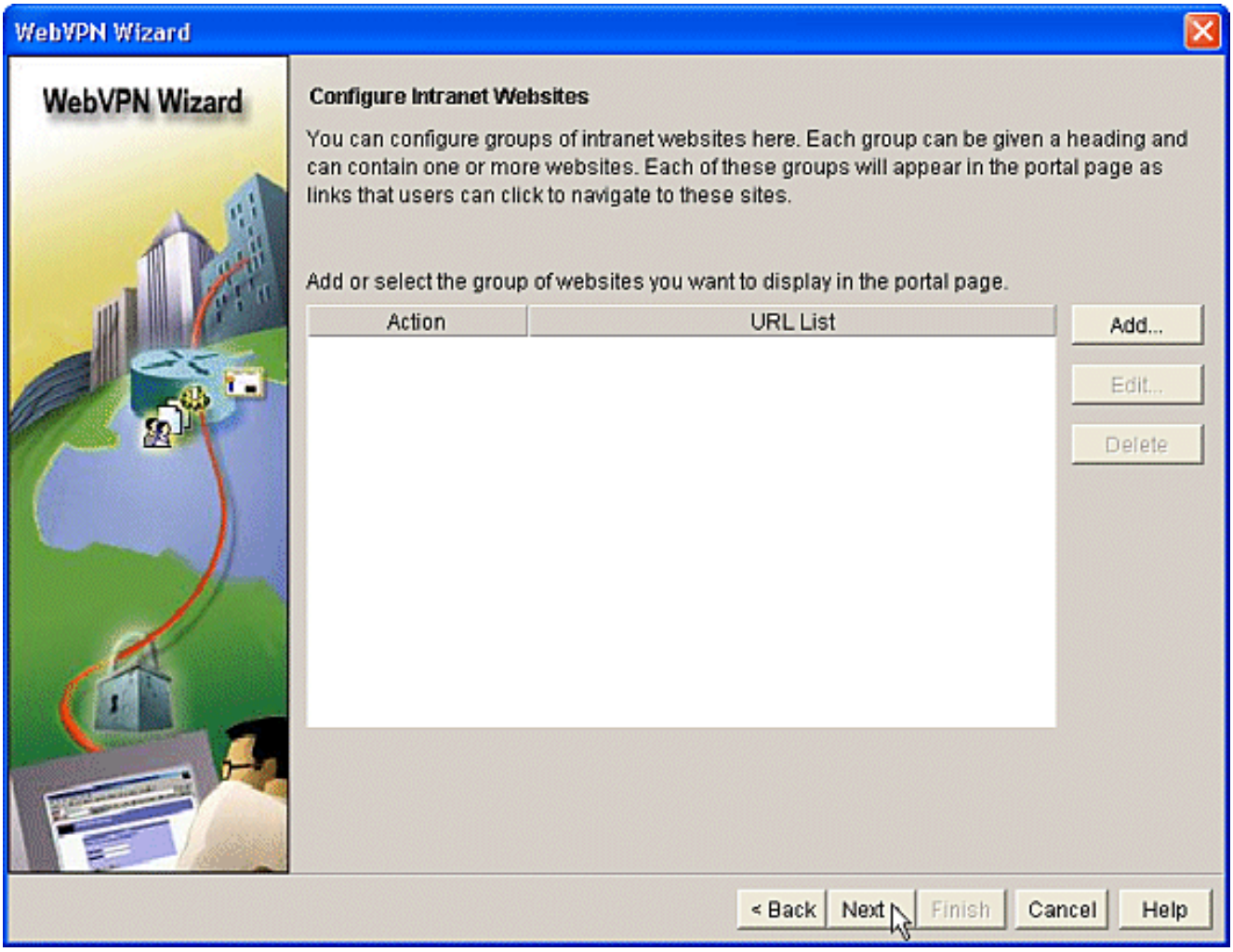


OK.

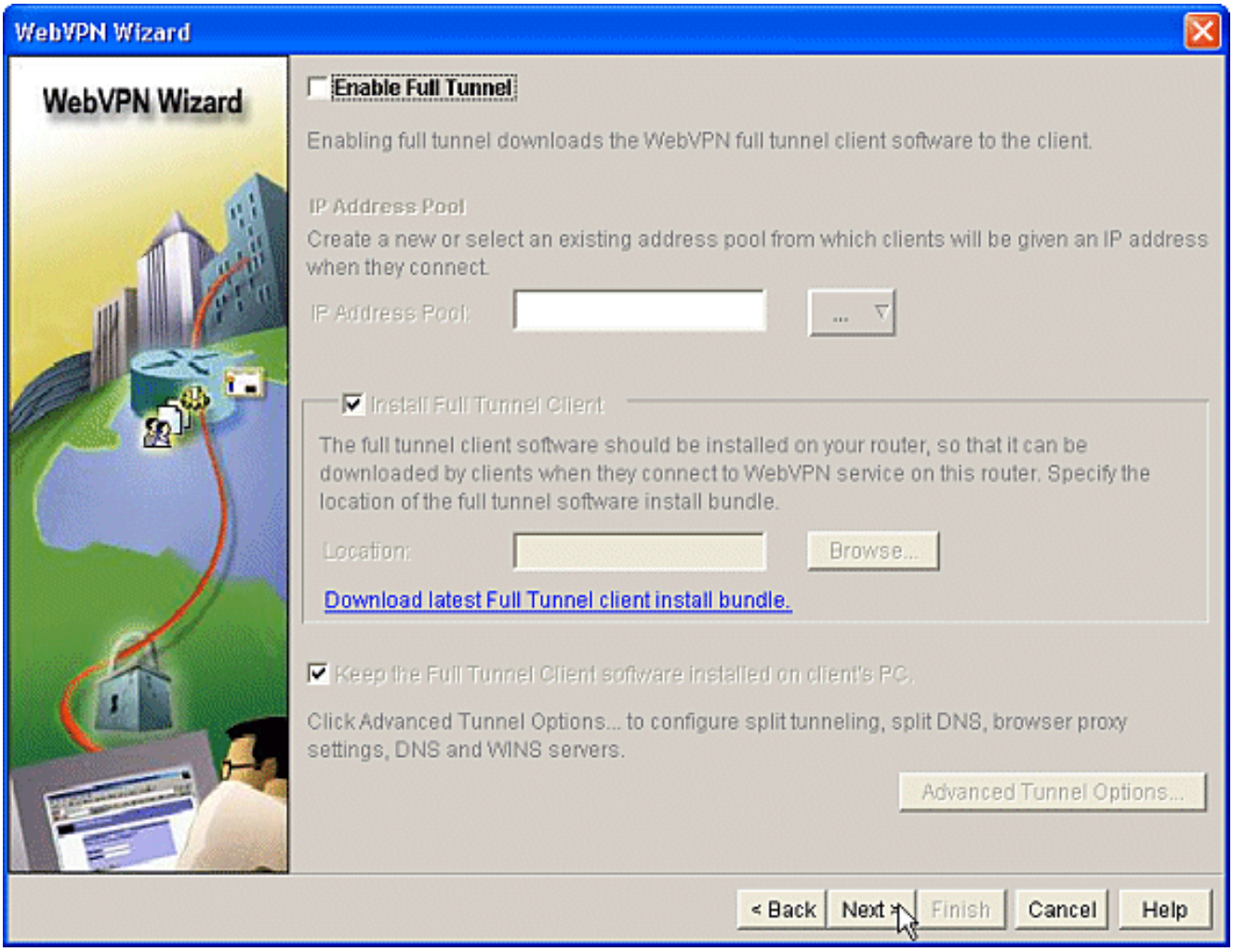
6. Nadat u uw gebruikers hebt gemaakt, klikt u op **Volgende** op de pagina Gebruikersverificatie.



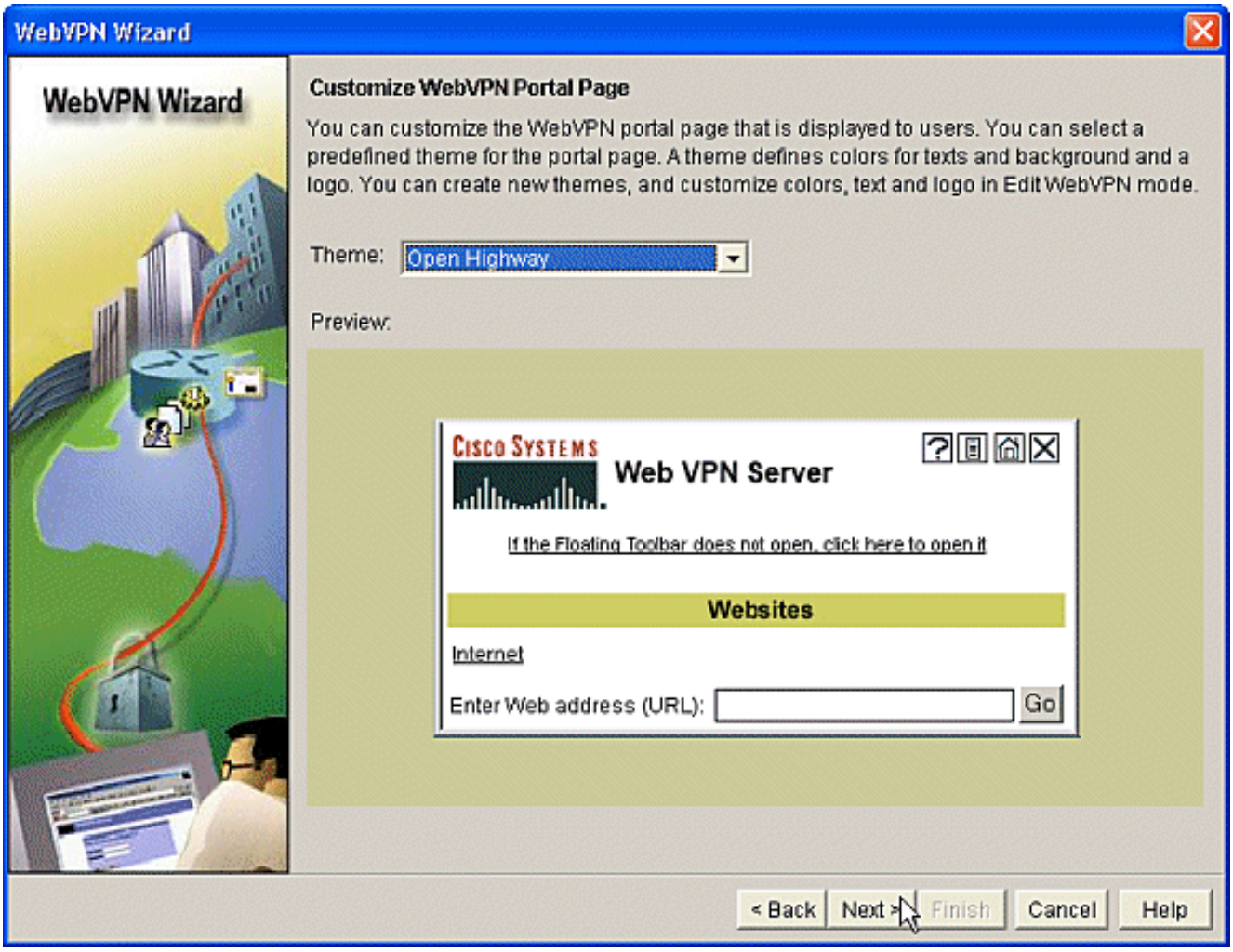
7. Met het scherm Intranet Websites configureren kunt u de website configureren die beschikbaar is voor gebruikers van de WebVPN-gateway. Aangezien dit document vooral gericht is op de configuratie van CSD, moet u deze pagina van de hand wijzen. Klik op **Volgende**.



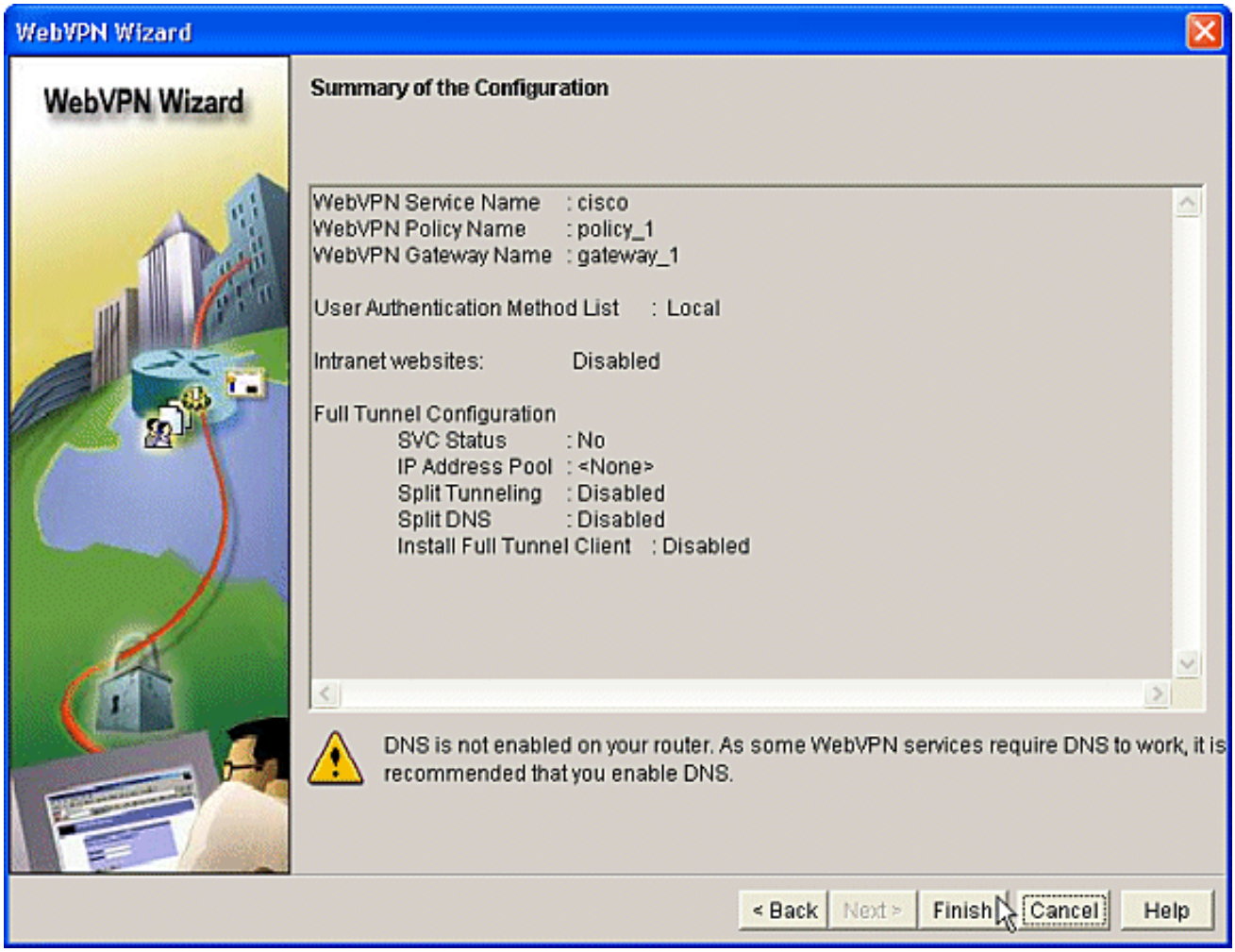
8. Hoewel u met het volgende WebVPN Wizard-scherm kunt kiezen om de Full Tunnel SSL VPN-client in te schakelen, is de focus van dit document hoe u CSD-effecten kunt inschakelen. Schakel de **optie Full Tunnel inschakelen uit** en klik op **Volgende**.



9. U kunt de weergave van de WebVPN Portal pagina aan gebruikers aanpassen. In dit geval wordt de standaardinstelling geaccepteerd. Klik op **Volgende**.



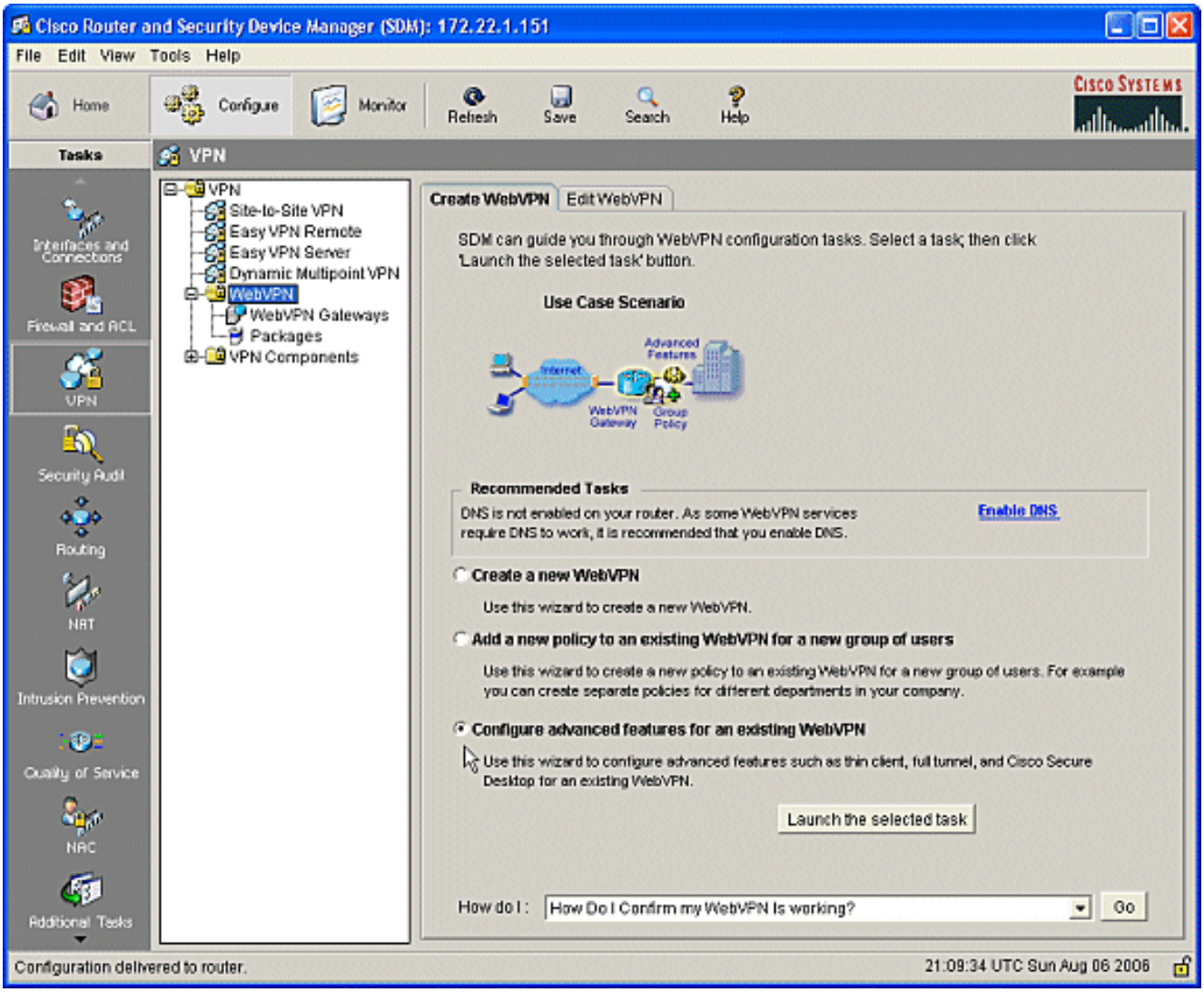
10. De wizard geeft het laatste scherm in deze serie weer. Het toont een samenvatting van de configuratie voor de gateway van WebVPN. Klik op **Voltooien** en klik, wanneer dit wordt gevraagd, op **OK**.



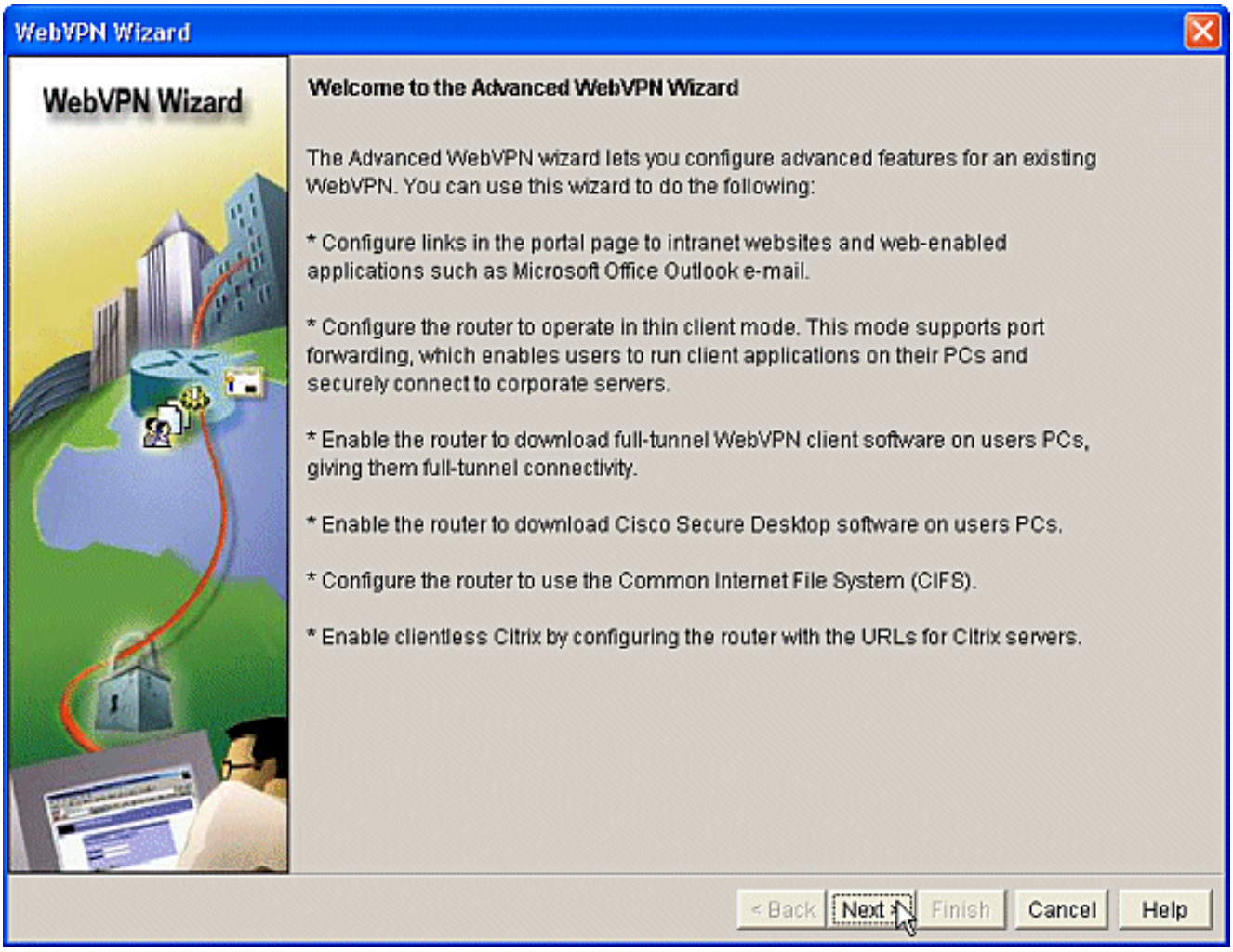
Fase I: Stap 2: CSD in een WebVPN-context inschakelen.

Gebruik de Wizard WebVPN om CSD in een WebVPN-context mogelijk te maken.

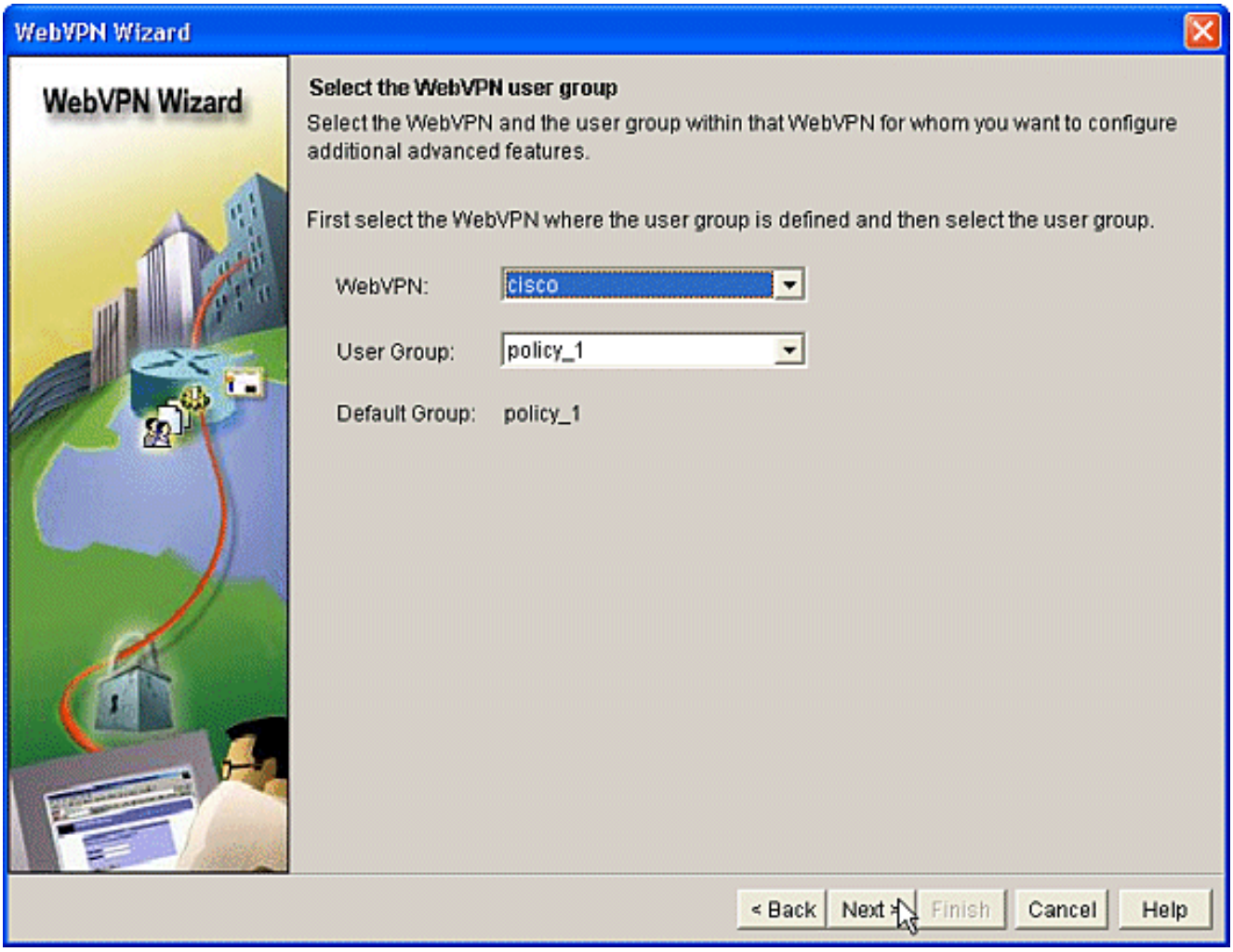
1. Gebruik de geavanceerde functies van de WebVPN Wizard om CSD voor de nieuwe context mogelijk te maken. De wizard geeft u de mogelijkheid om het CSD-pakket te installeren als het nog niet is geïnstalleerd.Klik op het tabblad **Configureren**.Klik in het navigatiedeelvenster op **VPN > WebVPN**.Klik op het tabblad **WebVPN maken**.Controleer de **configuratiescherm voor een bestaande WebVPN** radioknop.Klik op de knop **De geselecteerde taak** starten.



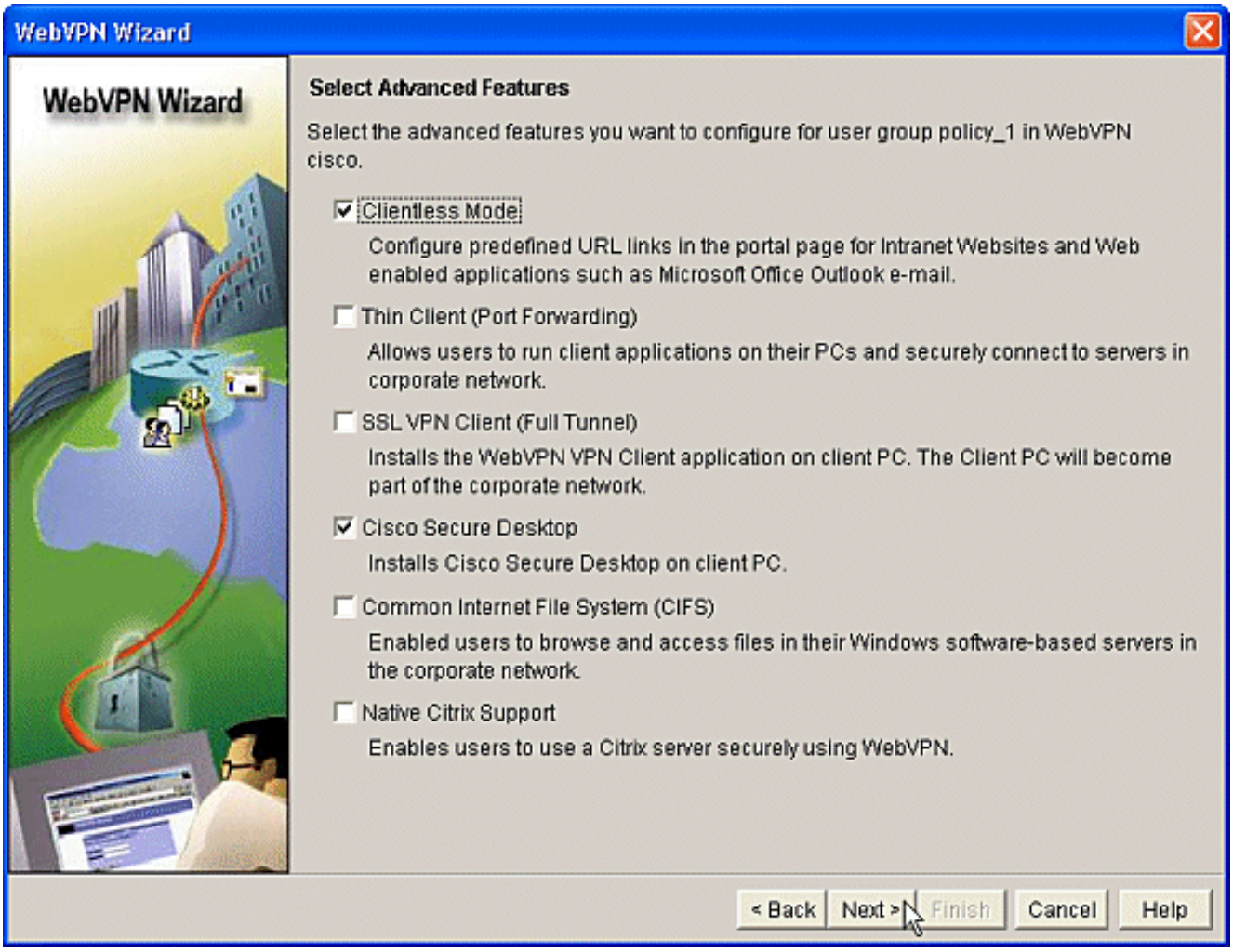
2. De welkomstpagina voor de geavanceerde WebVPN Wizard toont. Klik op **Volgende**.



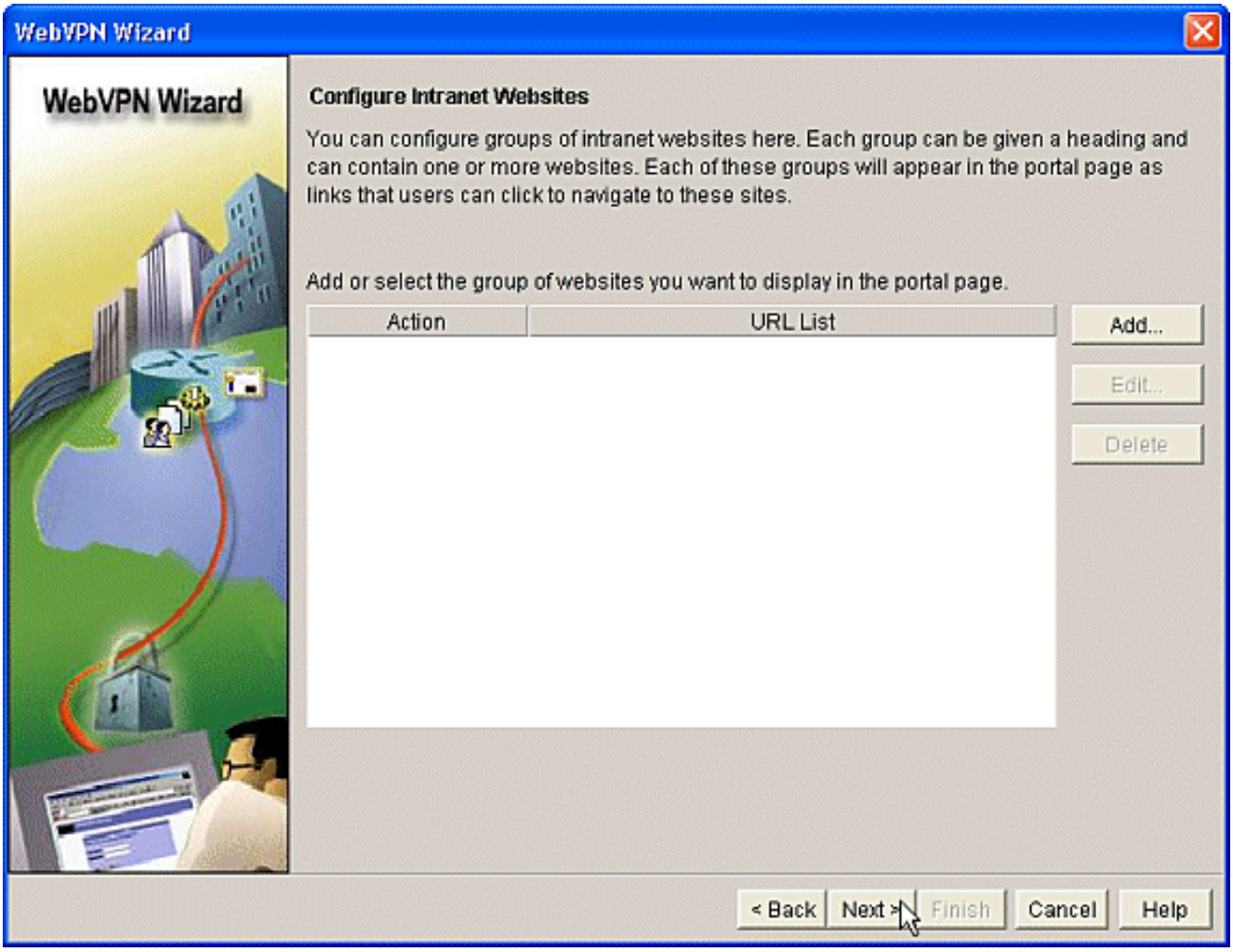
3. Kies het WebVPN en de gebruikersgroep van de vervolgkeuzelijsten van de velden. De geavanceerde WebVPN Wizard functies worden op uw keuzes toegepast. Klik op **Volgende**.



4. Met het scherm Geavanceerde functies kunt u kiezen uit de technologieën die in de lijst staan.Controleer **Cisco Secure-desktop**.In dit voorbeeld is de keuze **Clientloze modus**.Als u een van de andere genoemde technologieën kiest, staan er extra vensters open om invoer van verwante informatie toe te staan.Klik op de knop **Volgende**.

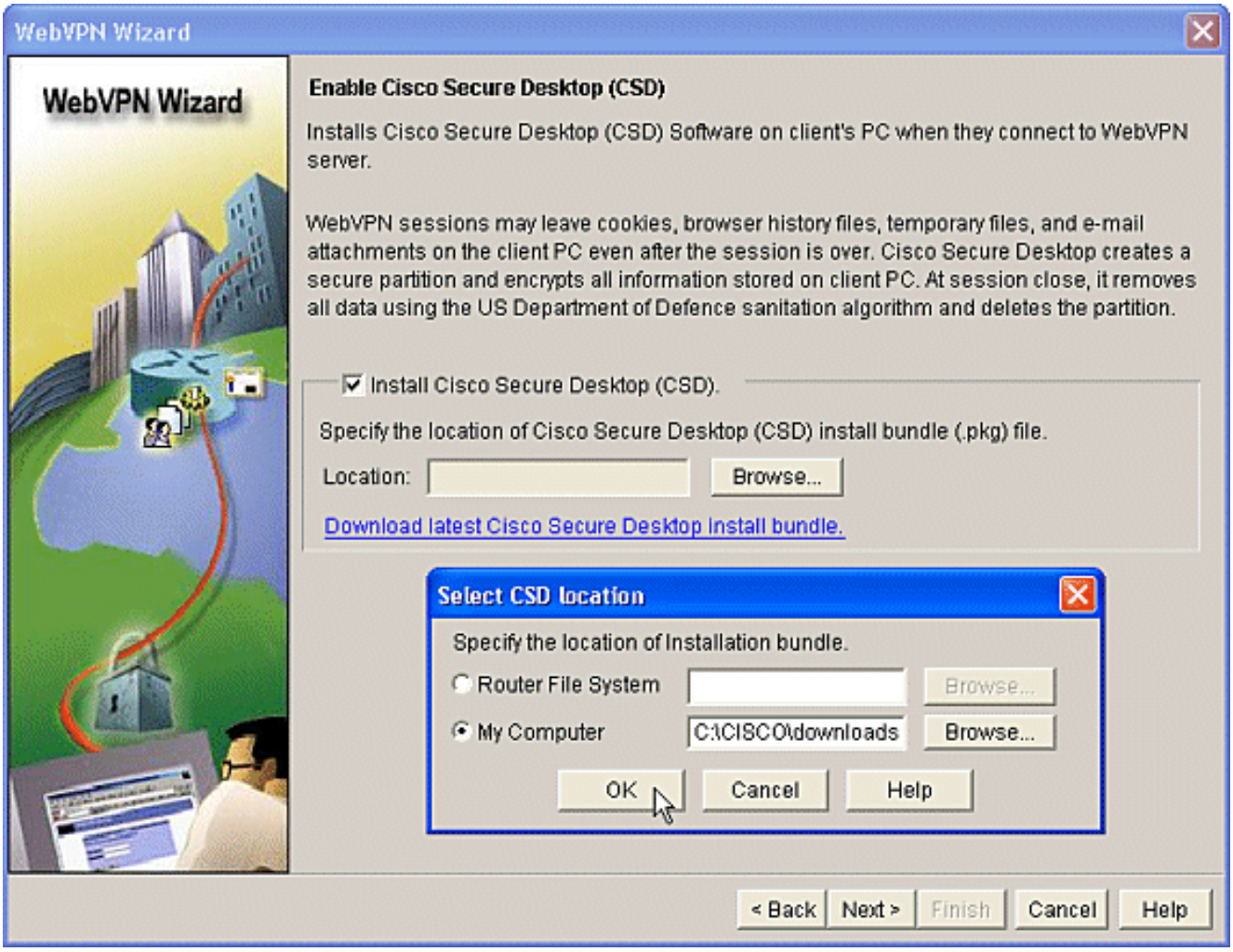


5. Met het scherm Intranet Websites configureren kunt u de website bronnen configureren die u voor de gebruikers beschikbaar wilt maken. U kunt de interne websites van het bedrijf toevoegen zoals Outlook Web Access
(OWA).



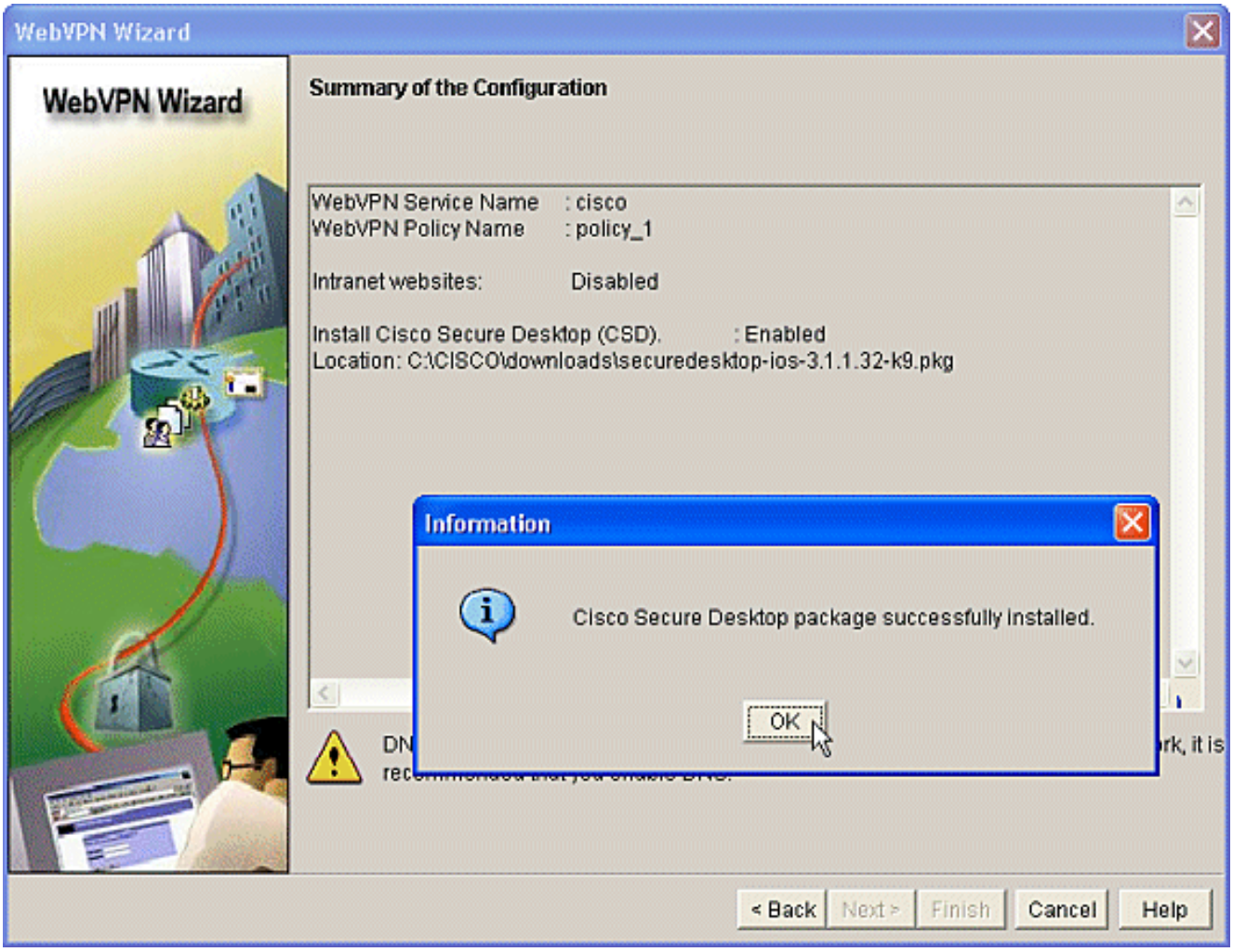
6. In het scherm Enable Cisco Secure Desktop (CEBI) hebt u de mogelijkheid om CSD voor deze context in te schakelen. Controleer het vakje naast **Installeer Cisco Secure Desktop (CSD)** en klik op **Bladeren**.

7. Controleer **Mijn computer** in het gedeelte **Locatie** selecteren.Klik op de knop **Bladeren**.Kies het CSD IOS-pakketbestand op uw beheerwerkstation.Klik op de knop **OK**.Klik op de knop **Volgende**.



8. Een samenvatting van het scherm Configuration verschijnt. Klik op de knop **Voltooien**.

9. Klik op **OK** wanneer u ziet dat het CSD-pakketbestand met succes is geïnstalleerd.



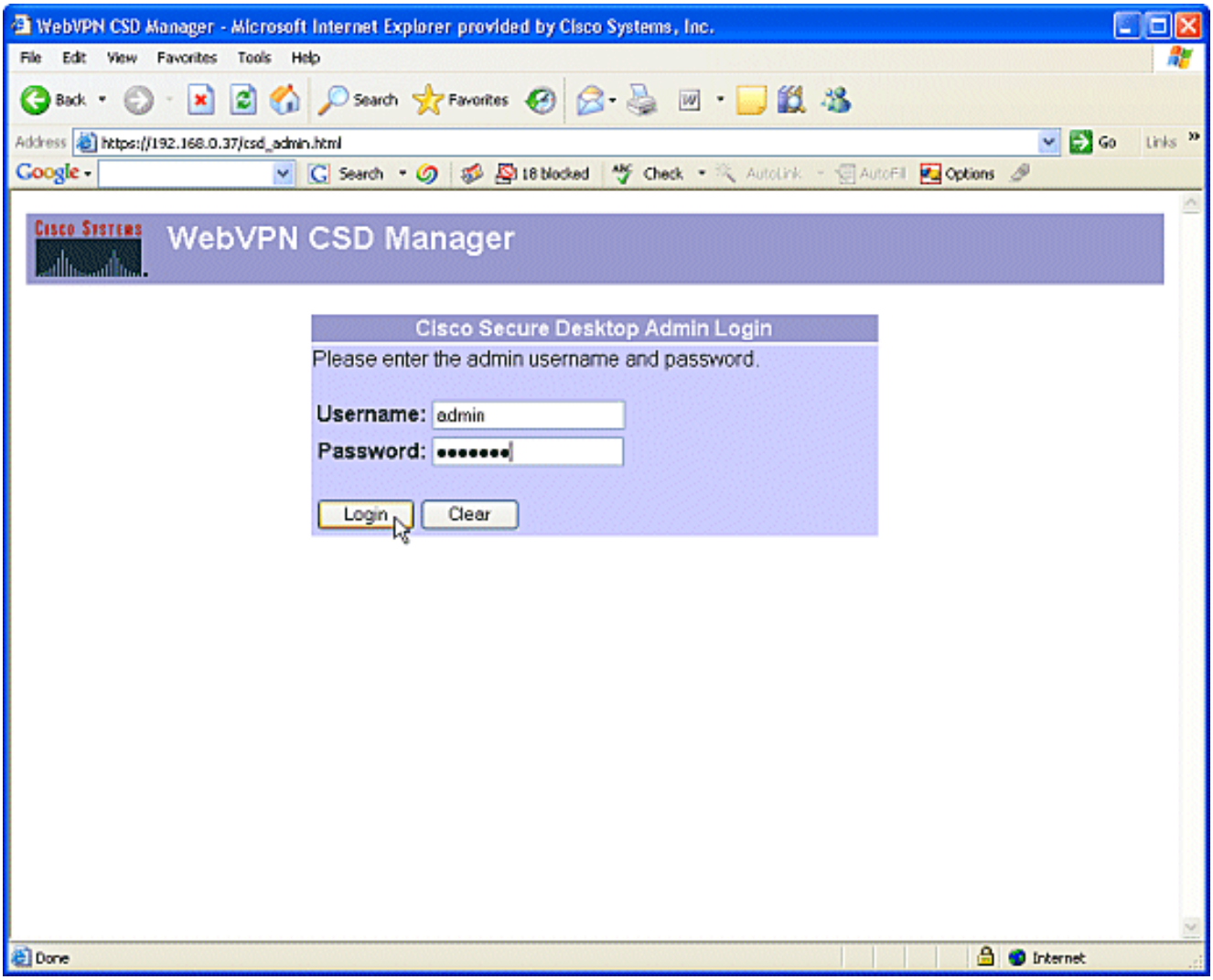
Fase II: CSD configureren met behulp van een webbrowser.

Deze stappen worden gebruikt om de configuratie van CSD op uw webbrowser te voltooien.

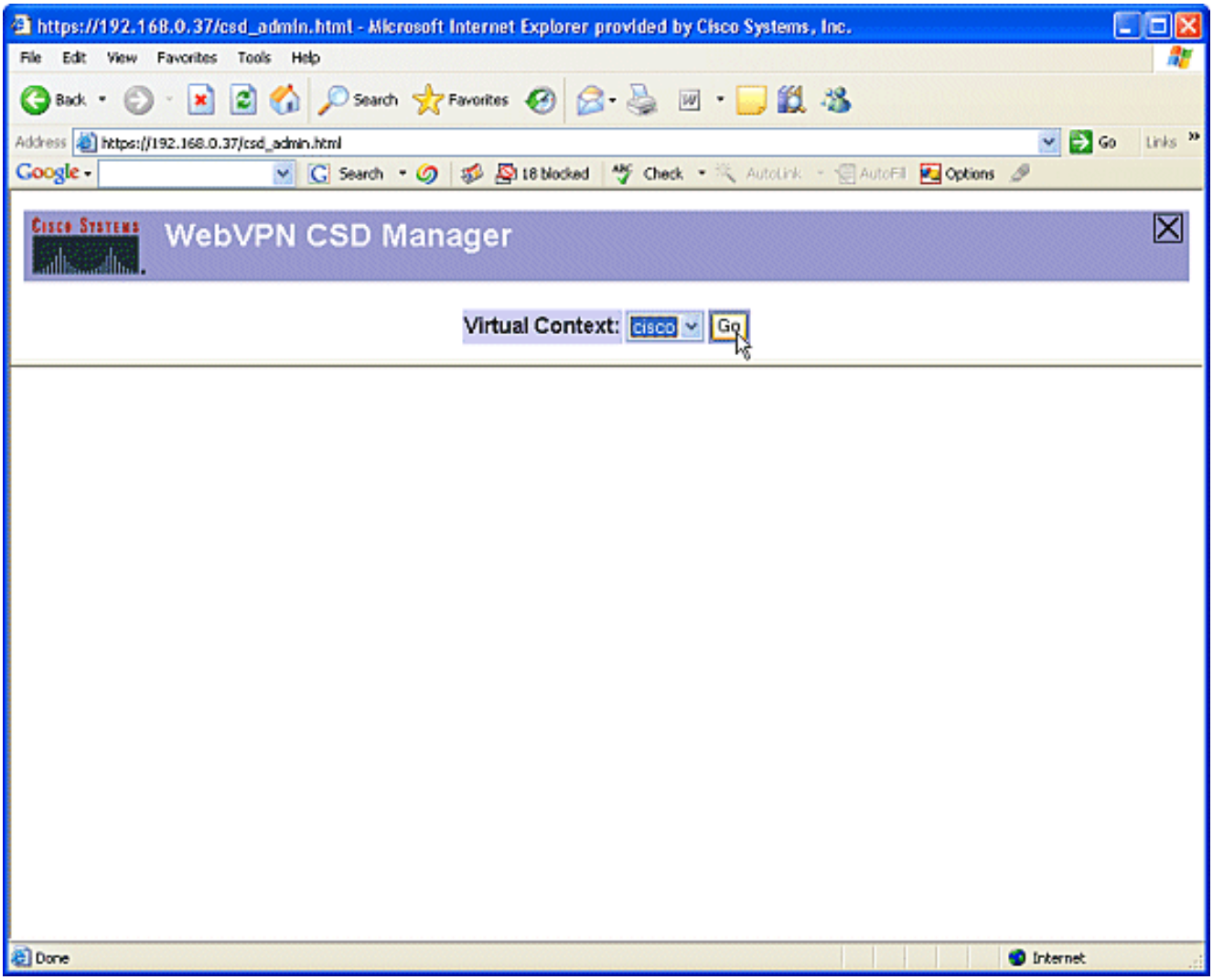
Fase II: Stap 1: Windows locaties definiëren

Bepaal de locaties van Windows.

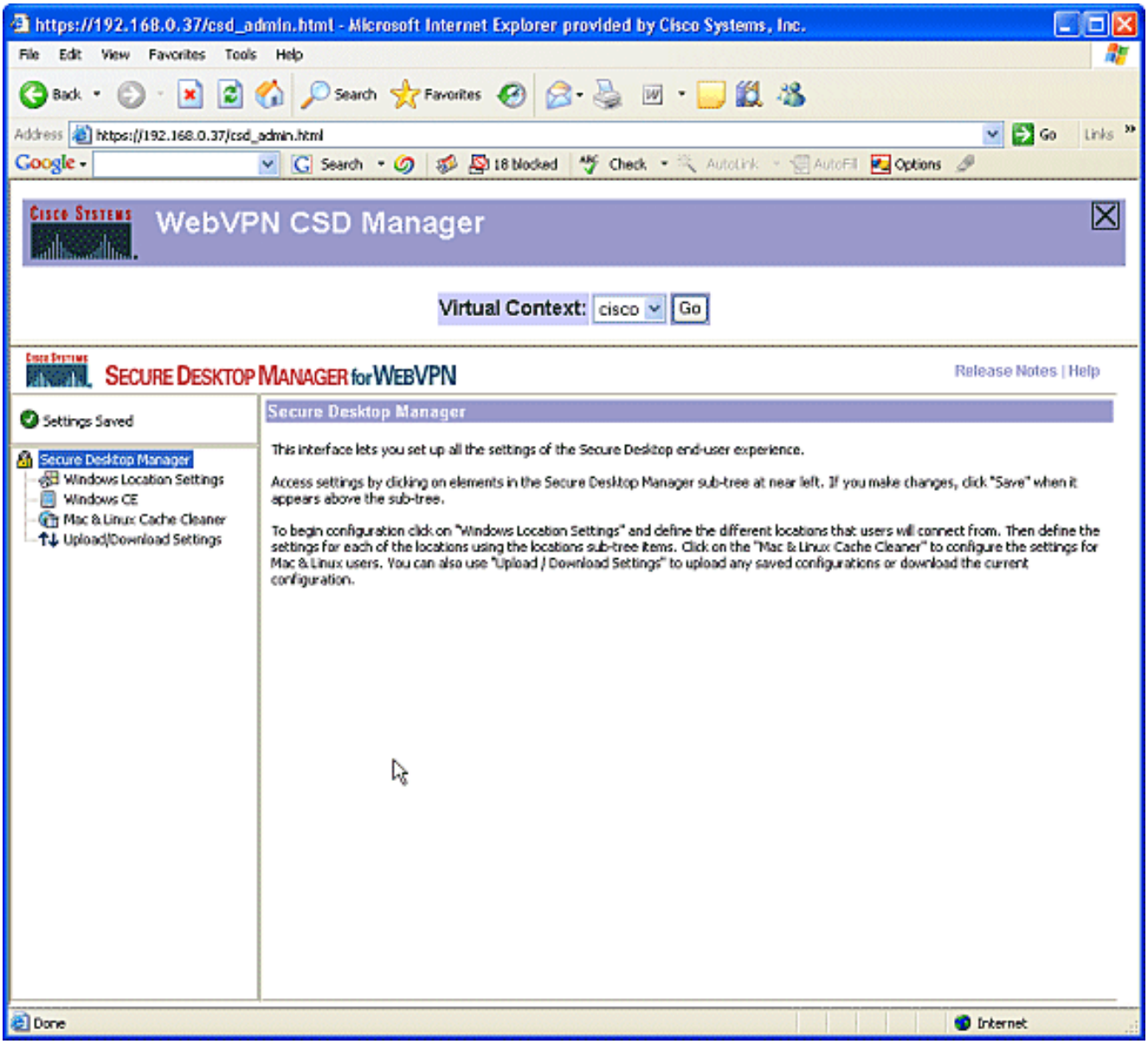
1. Open uw webbrowser op **https://WebVPNgateway_IP Address/csd_admin.html**, bijvoorbeeld, **https:/192.168.0.37/csd_admin.html**.
2. Voer de gebruikersnaam in **beheerder**.Voer het wachtwoord in dat het mogelijk geheim van de router is.Klik op **Aanmelden**.



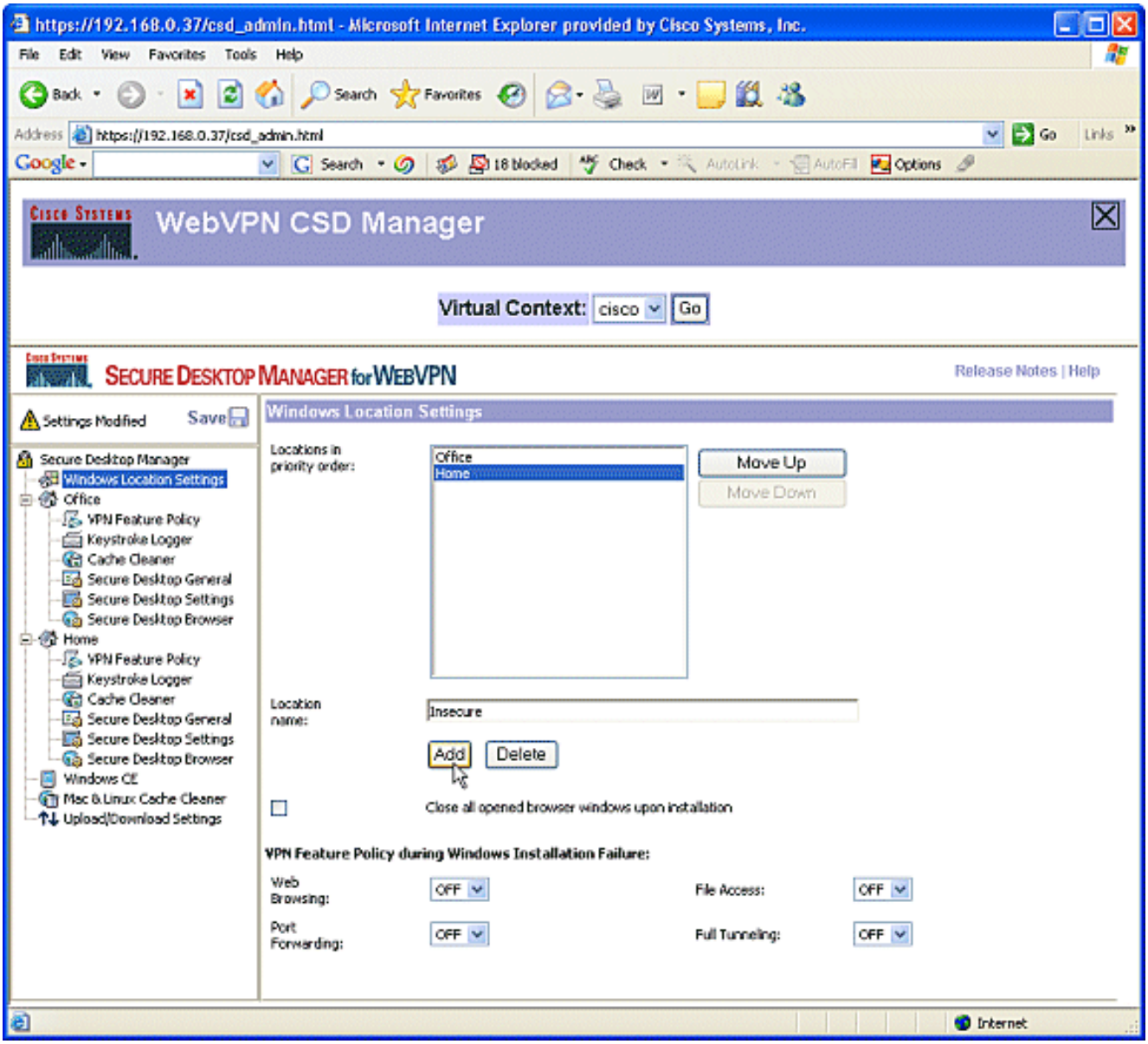
3. Accepteer het certificaat dat door de router is aangeboden, kies de context in het vervolgkeuzevenster en klik op
Ga.



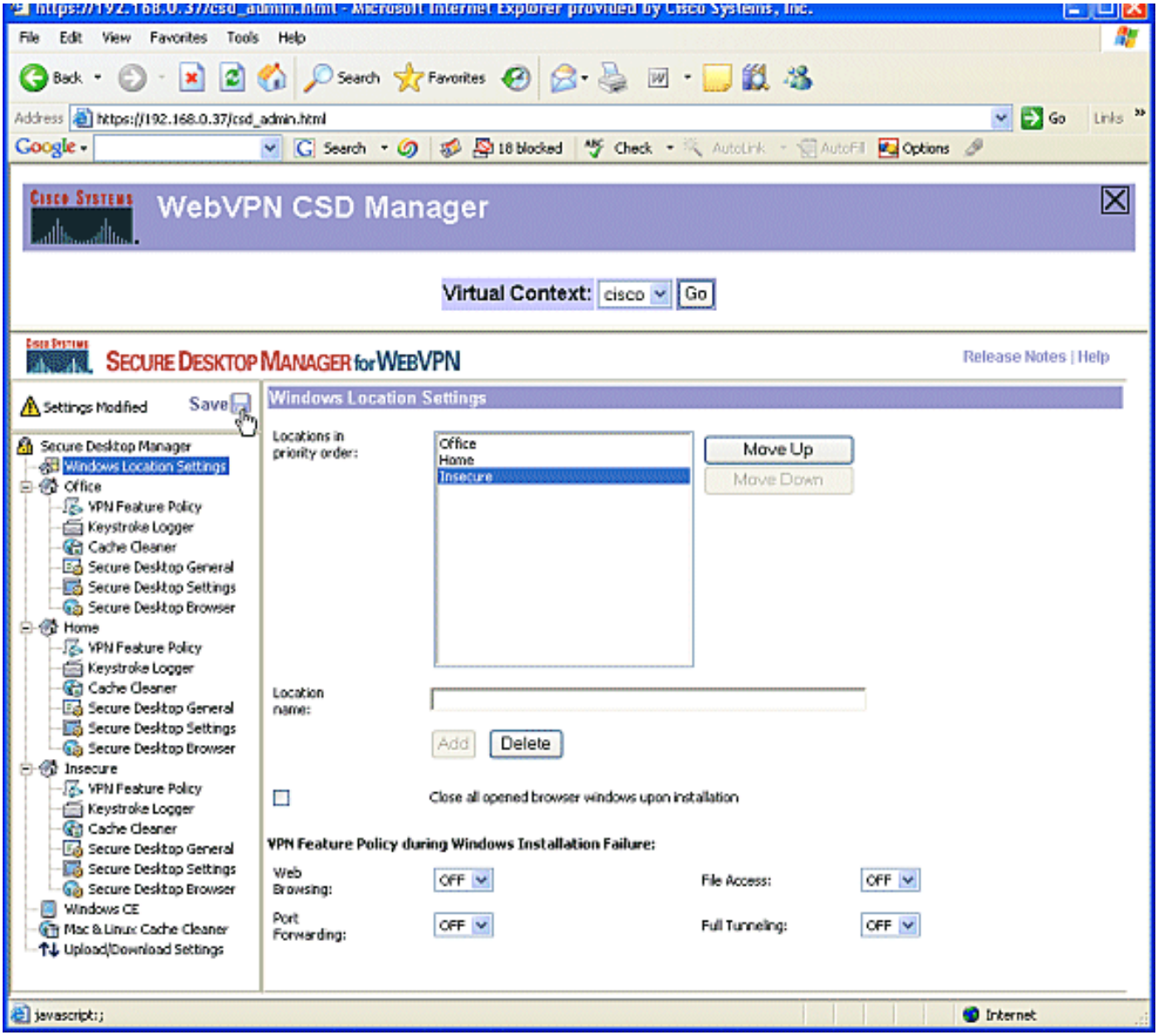
4. Secure Desktop Manager voor WebVPN wordt geopend.



5. Kies in het linker venster de **instellingen van de locatie van Windows**.Plaats de aanwijzer in het vakje naast de naam van de Plaats, en voer een plaatsnaam in.Klik op **Add** (Toevoegen).In dit voorbeeld worden drie locatienamen weergegeven: Office, Thuis en onzeker. Elke keer dat er een nieuwe locatie wordt toegevoegd, wordt het linker deelvenster uitgebreid met de configureerbare parameters voor die locatie.



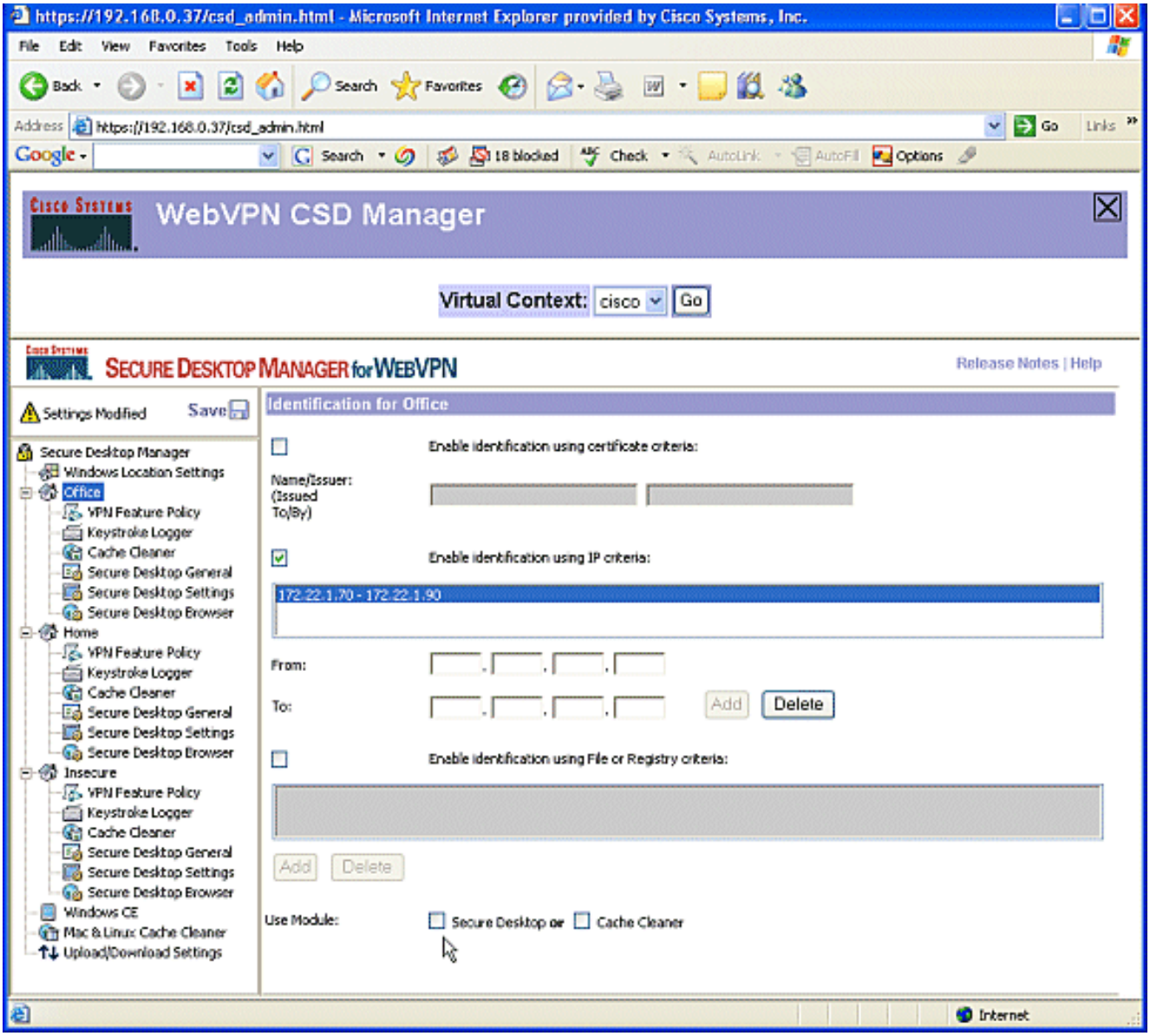
6. Nadat u de locaties van Windows hebt gemaakt, klikt u op **Opslaan** boven in het linker deelvenster.**OPMERKING:** Sla uw configuraties vaak op omdat uw instellingen verloren gaan als u niet meer verbinding maakt met de webbrowser.



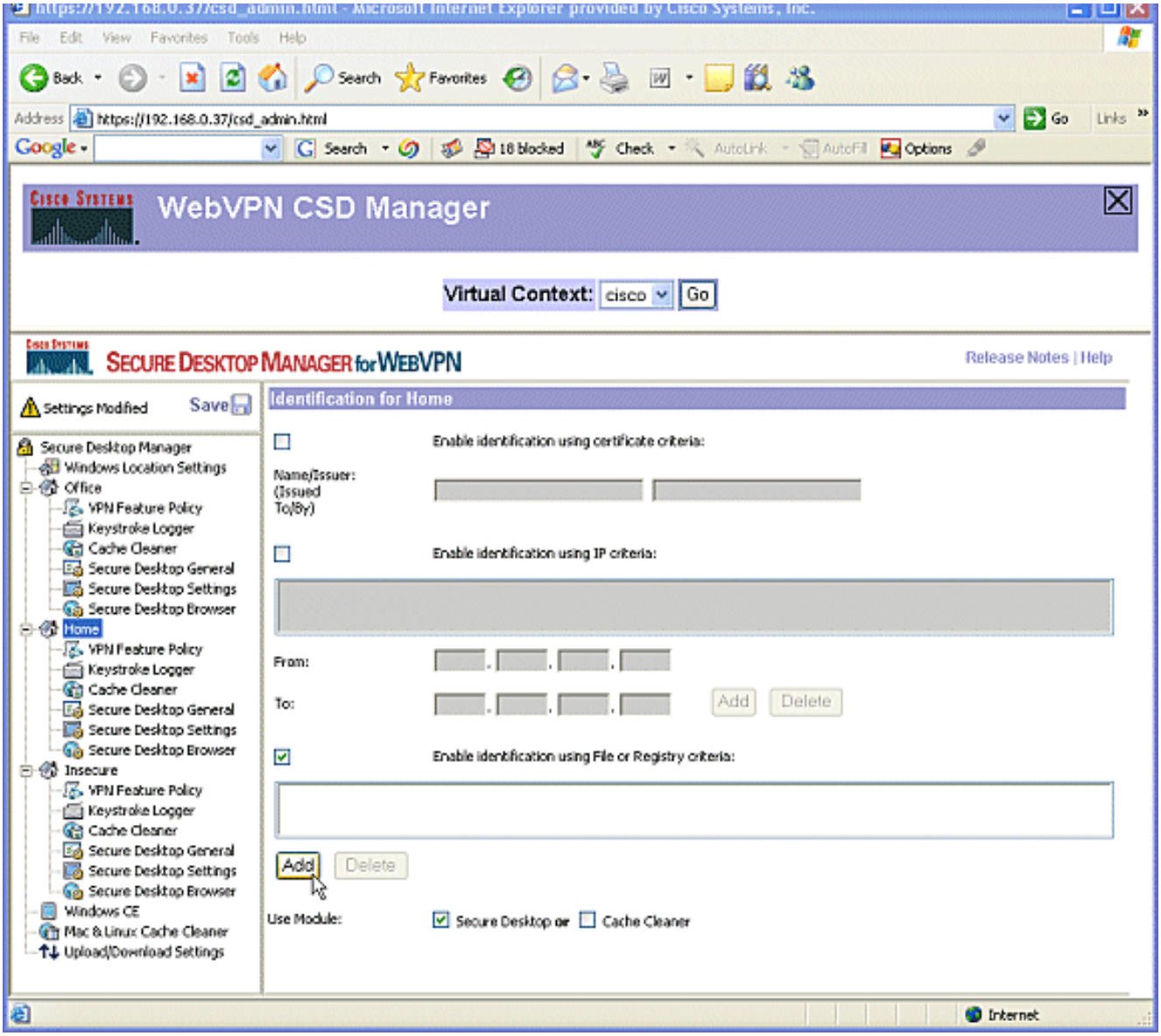
Fase II: Stap 2: Locatiecriteria identificeren

Om Windows locaties van elkaar te onderscheiden, moet u aan elke locatie specifieke criteria toewijzen. Dit stelt CSD in staat om te bepalen welke van zijn functies van toepassing zijn op een bepaalde Windows-locatie.

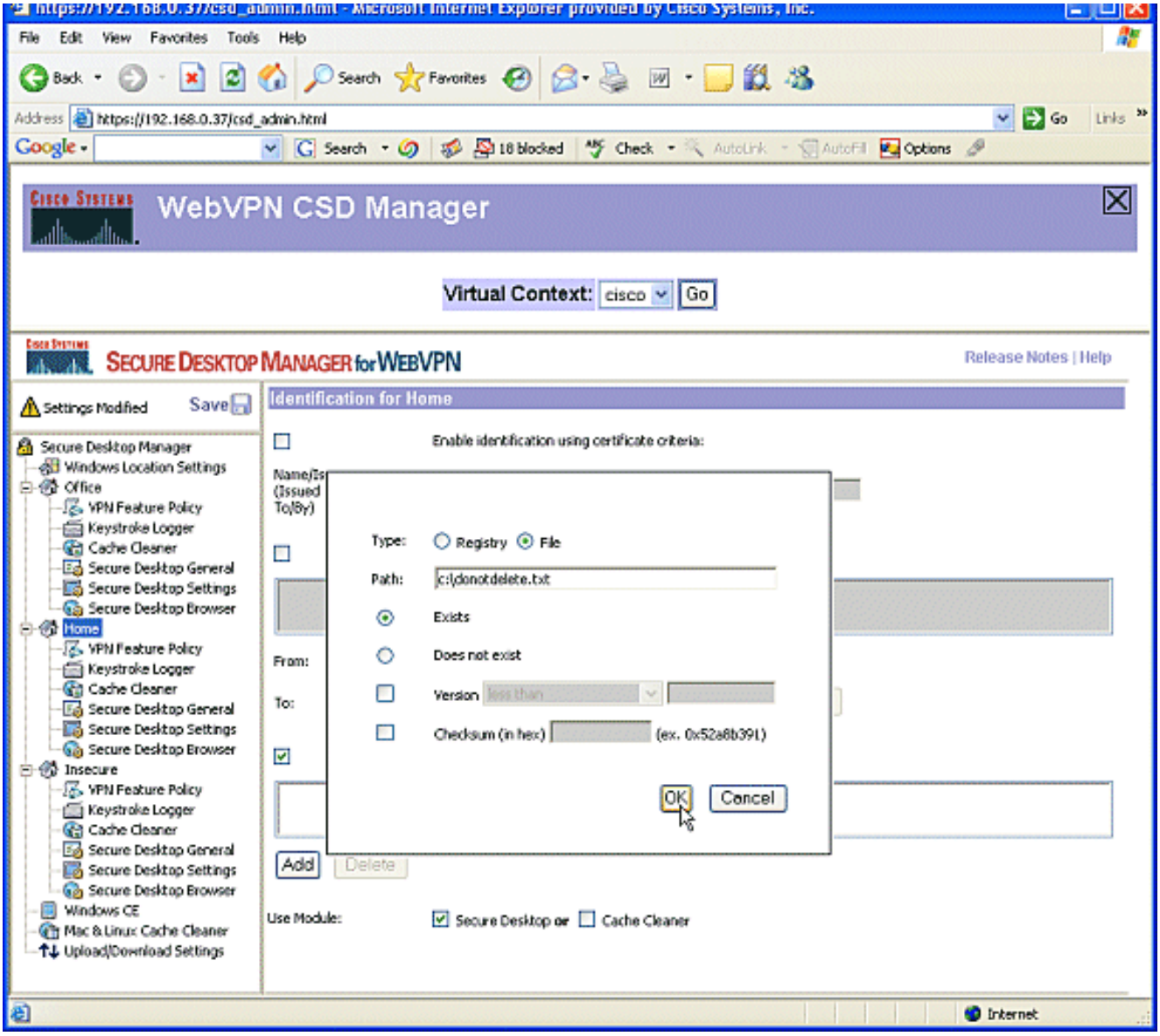
1. Klik in het linker deelvenster op **Office**.U kunt een Windows-locatie identificeren met certificeringscriteria, IP-criteria, een bestand of registratiecriteria. U kunt ook de Secure Desktop of Cache Cleaner voor deze klanten kiezen. Aangezien deze gebruikers interne kantoormedewerkers zijn, kunt u hen identificeren met IP-criteria.Voer de IP-adresbereiken in de vakjes **Van** en **Aan in**.Klik op **Add** (Toevoegen). **Gebruik module** niet **controleren: Secure-desktop**.Klik na de indiening op **Opslaan** en klik op **OK**.



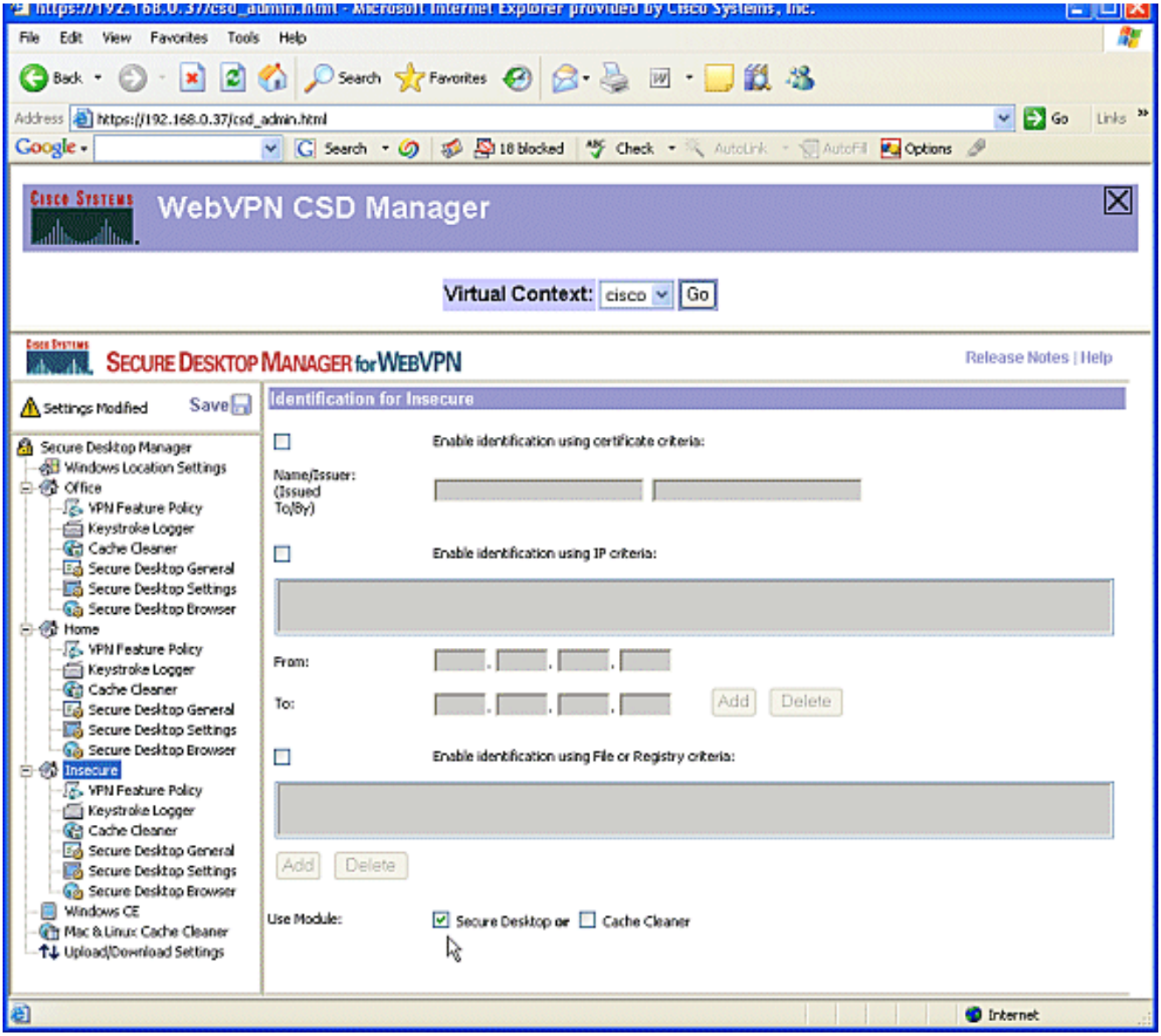
2. Klik in het linkervenster op het tweede **startpunt** van Windows Locatie.Zorg ervoor dat **u module gebruikt: Secure-desktop** is ingeschakeld.Er zal een bestand worden verspreid dat deze klanten identificeert. U kunt ervoor kiezen certificaten en/of registratiecriteria voor deze gebruikers te distribueren.Controleer **identificatie met behulp van criteria voor bestand of registratie**.Klik op **Add**
(Toevoegen).



3. Selecteer in het dialoogvenster **Bestand** en voer het pad naar het bestand in.Dit bestand moet worden verdeeld onder al uw thuisklanten.Controleer of de radioknop **bestaat**.Klik na de ontvangst op **OK** en klik op **Opslaan**.



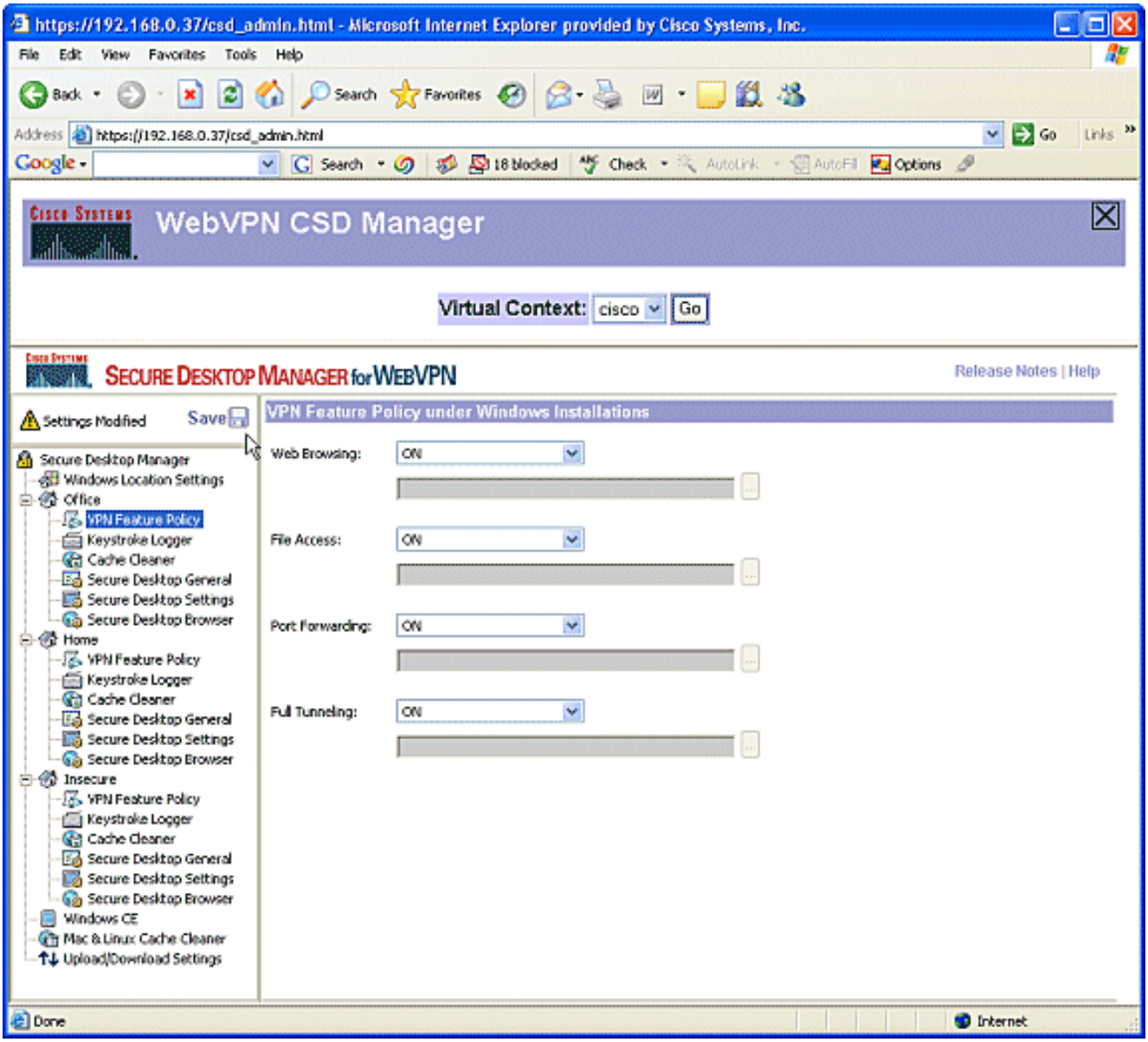
4. Om de identificatie van **onveilige** locaties te configureren, volgt u simpelweg geen identificatiecriteria.Klik **onveilig** in het linker deelvenster.Laat alle criteria ongecontroleerd.Controleer **de gebruiksmodule: Secure-desktop**.Klik na de indiening op **Opslaan** en klik op
OK.



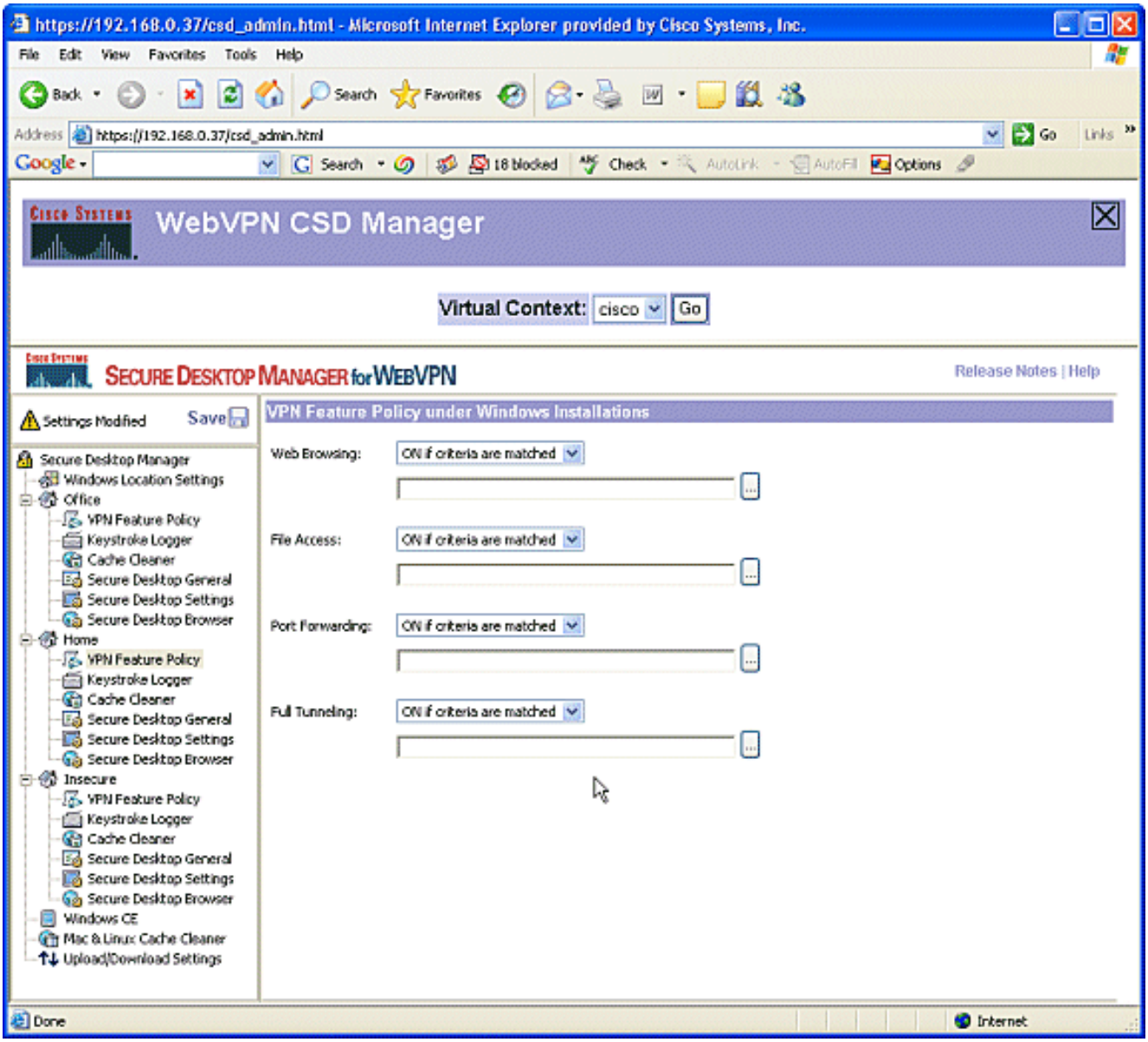
Fase II: Stap 3: Installeren van Windows.

Configureer de CSD-functies voor elke Windows-locatie.

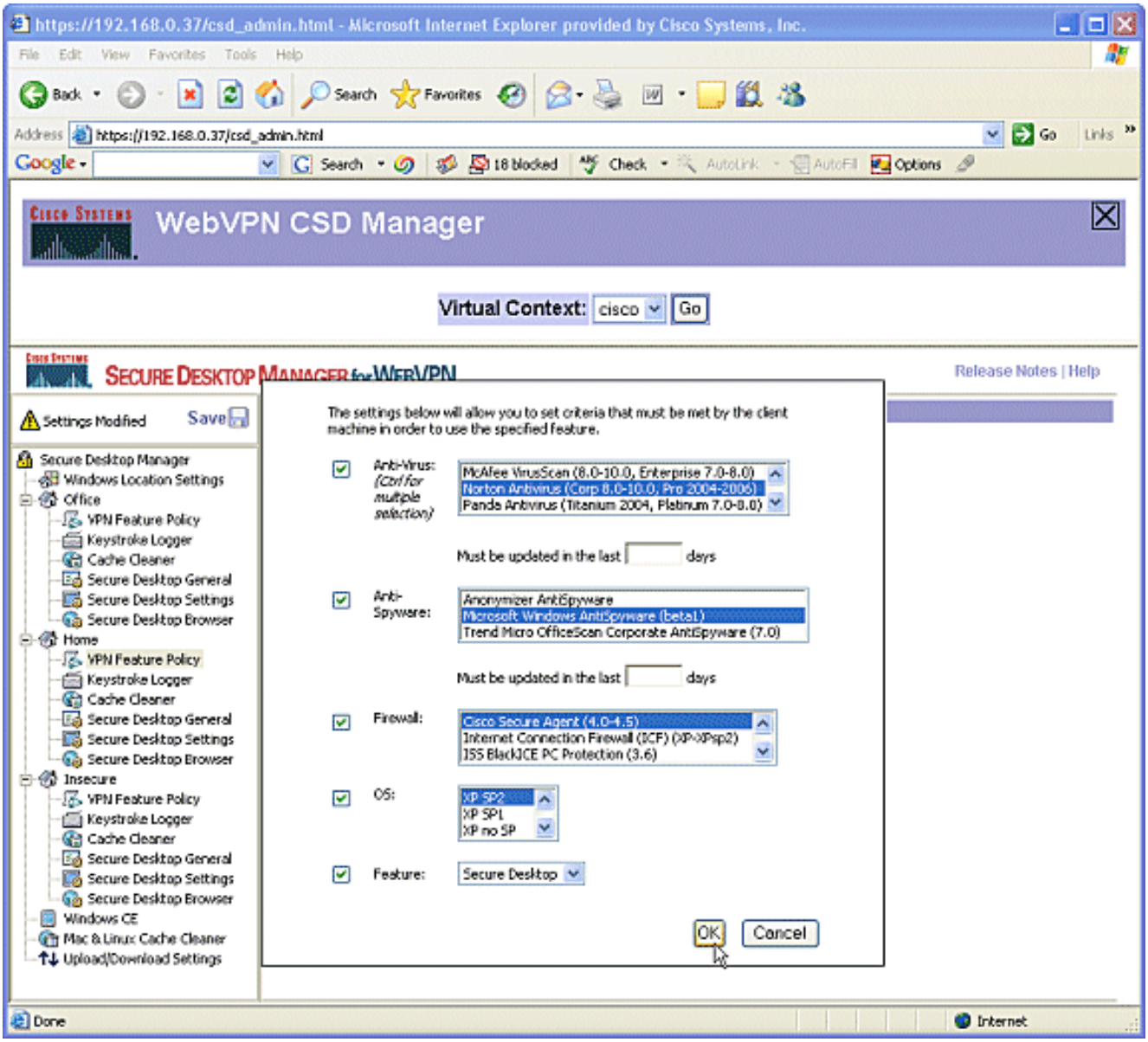
1. Klik onder **Office** op **VPN-functiebeleid**. Aangezien deze klanten vertrouwd zijn met de interne cliënten, werd noch CSD noch Cache Cleaner ingeschakeld. Geen van de andere parameters is
beschikbaar.



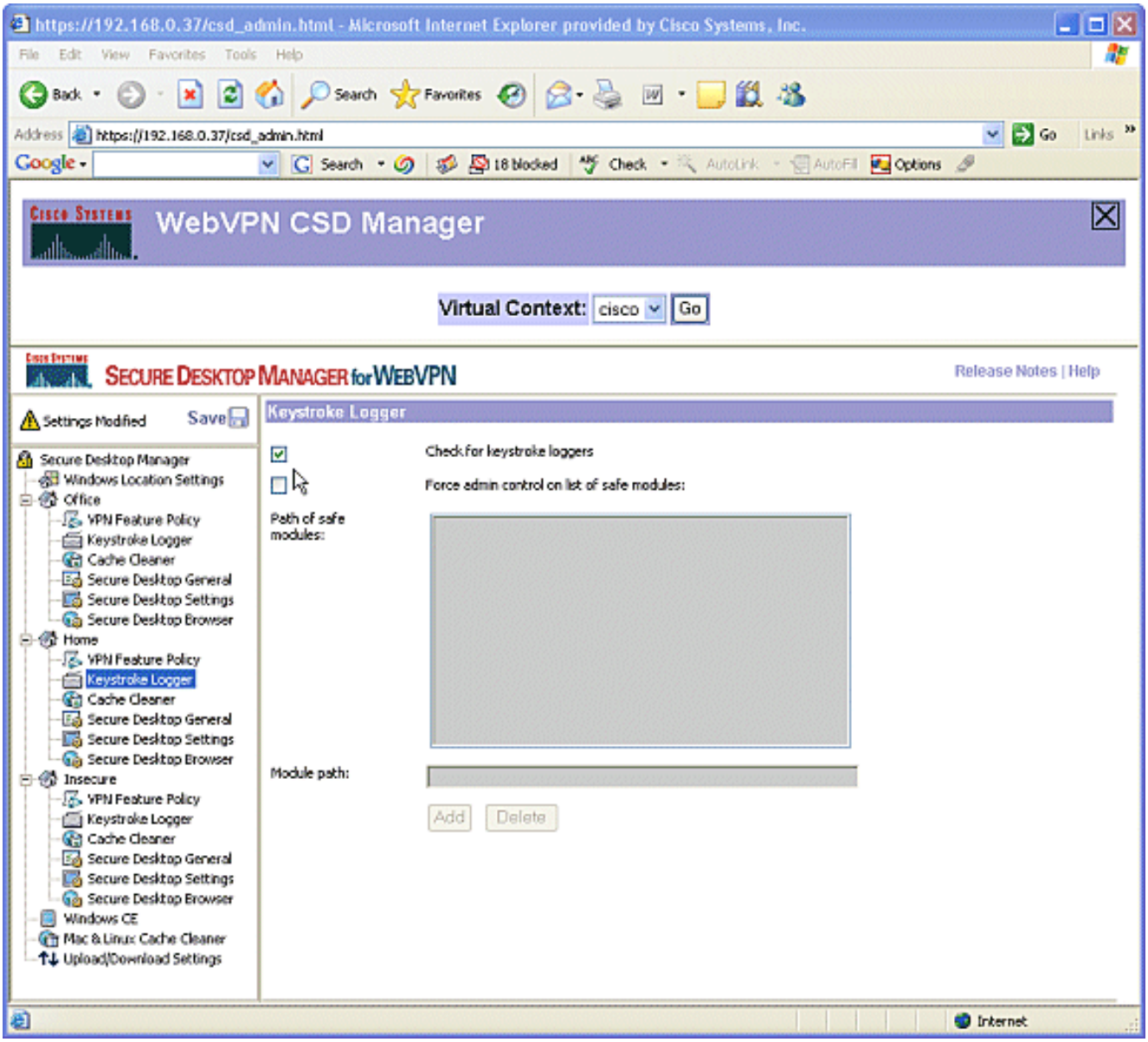
2. Schakel de functies in zoals aangegeven.Kies in het linker deelvenster **de optie VPN-functiebeleid** onder **Startpunt**.Thuisgebruikers krijgen toegang tot het LAN van de onderneming als de klanten aan bepaalde criteria voldoen.Kies **ON** bij elke toegangsmethode **als de criteria overeenkomen**.



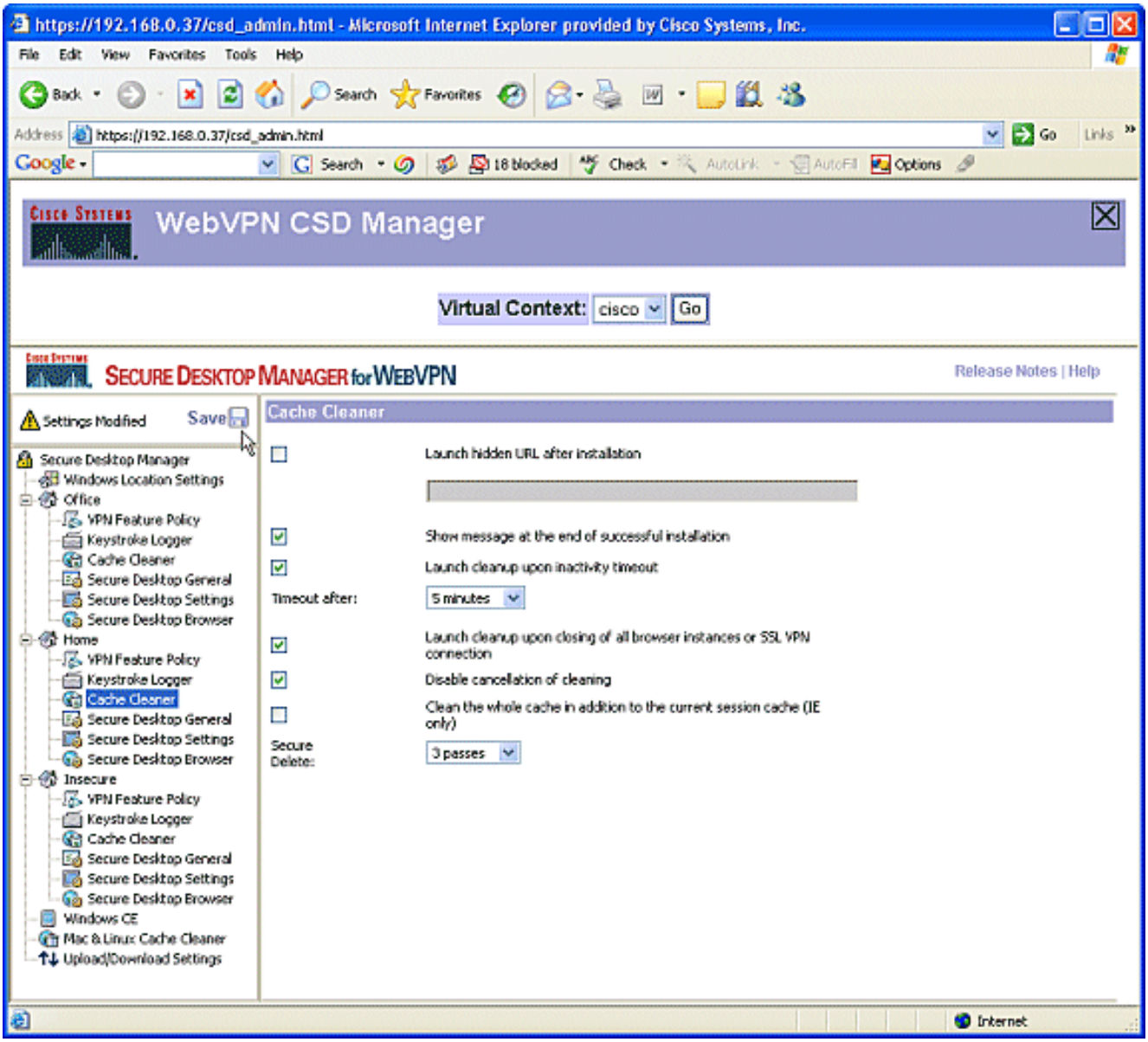
3. Voor Web Browsing, klik de ellips knop en kies de criteria die moeten aanpassen. Klik op **OK** in het dialoogvenster.



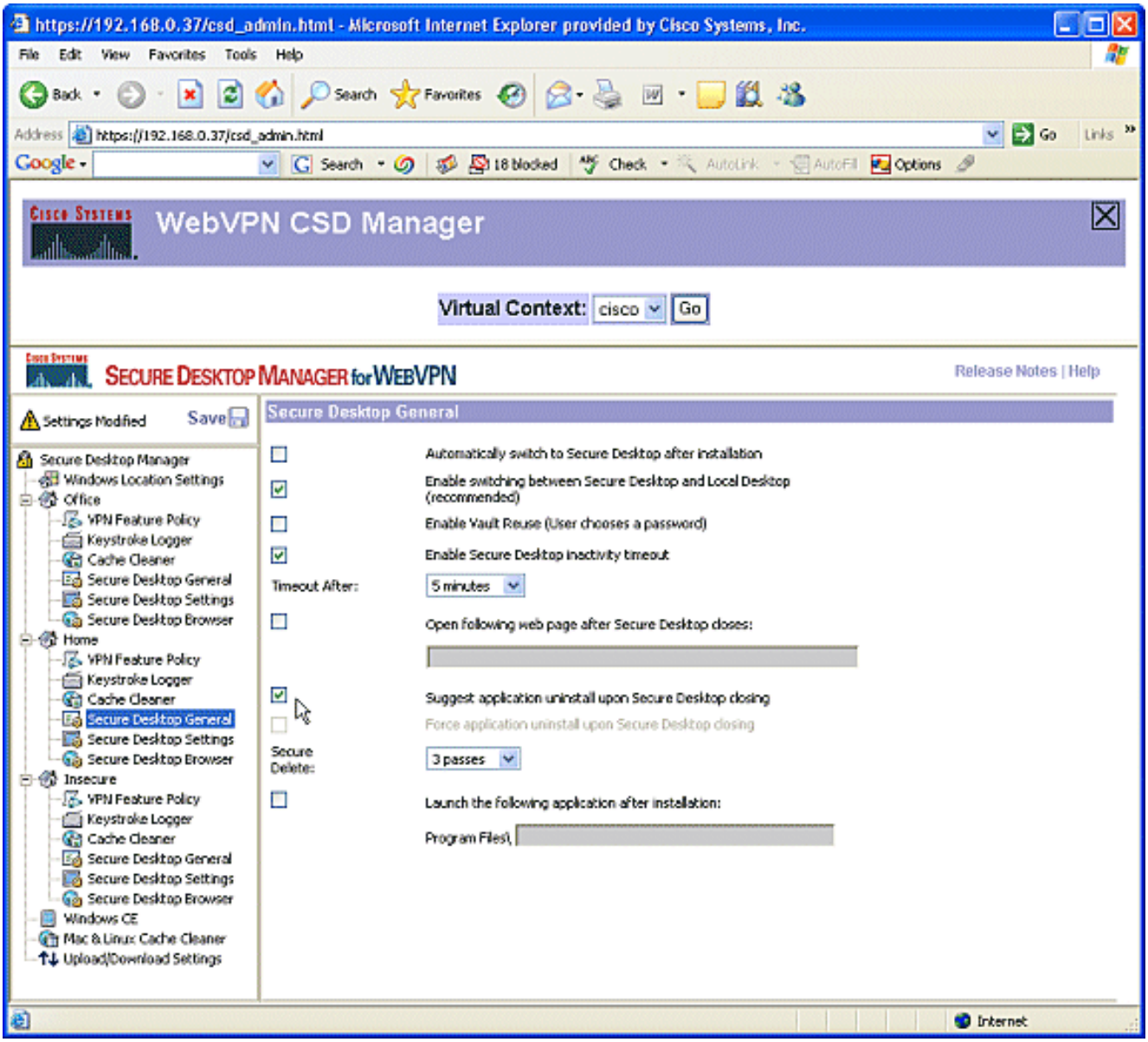
4. U kunt de andere toegangsmethoden op een zelfde manier configureren.Selecteer onder **Begin** de optie **Trefslag registreren**.Plaats een selectieteken naast **Controleer op loggers**.Klik na de indiening op **Opslaan** en klik op **OK**.



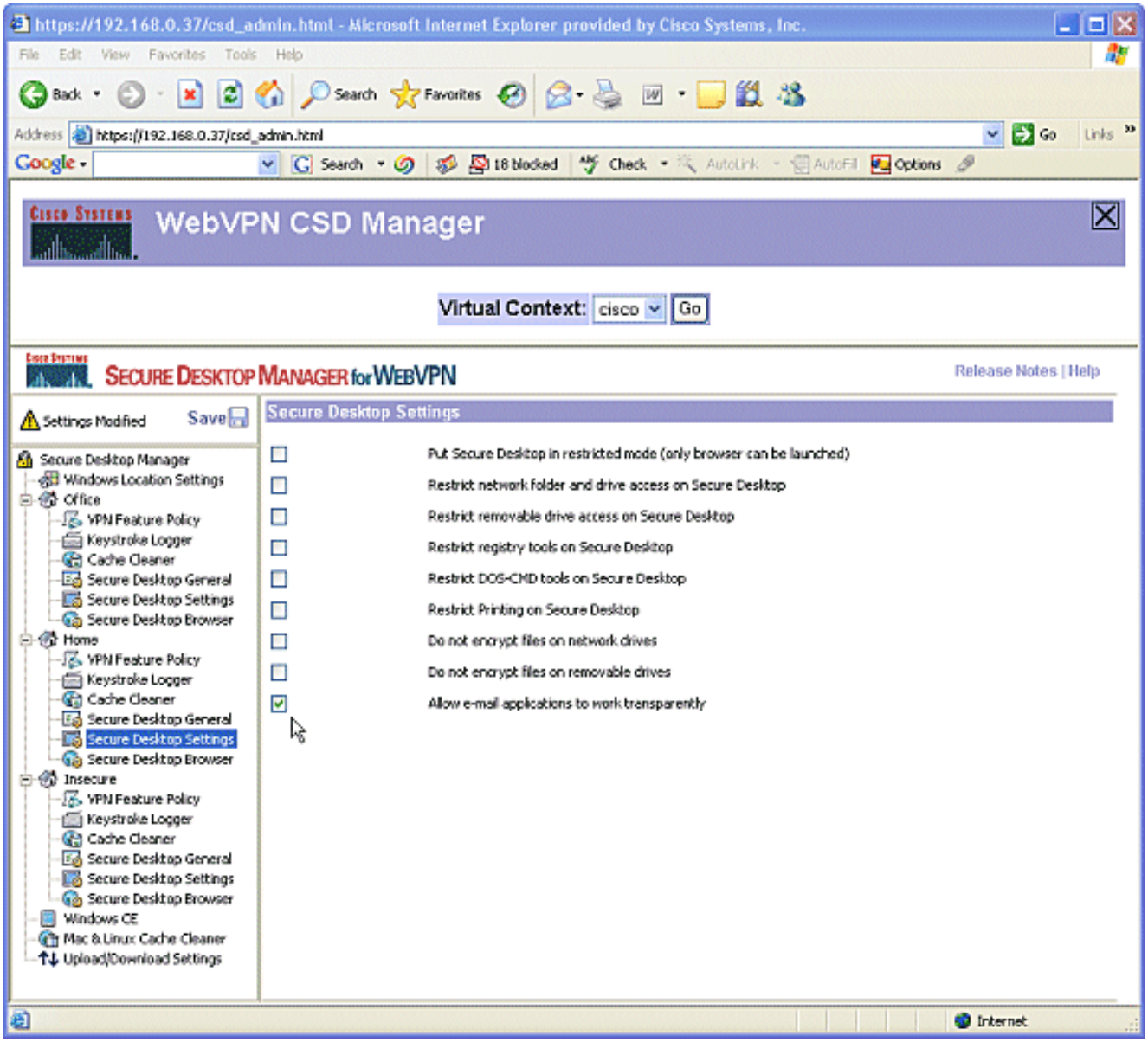
5. Selecteer onder de locatie Start Windows de optie **Cache Cleaner**. Laat de standaardinstellingen zoals weergegeven in de schermopname.



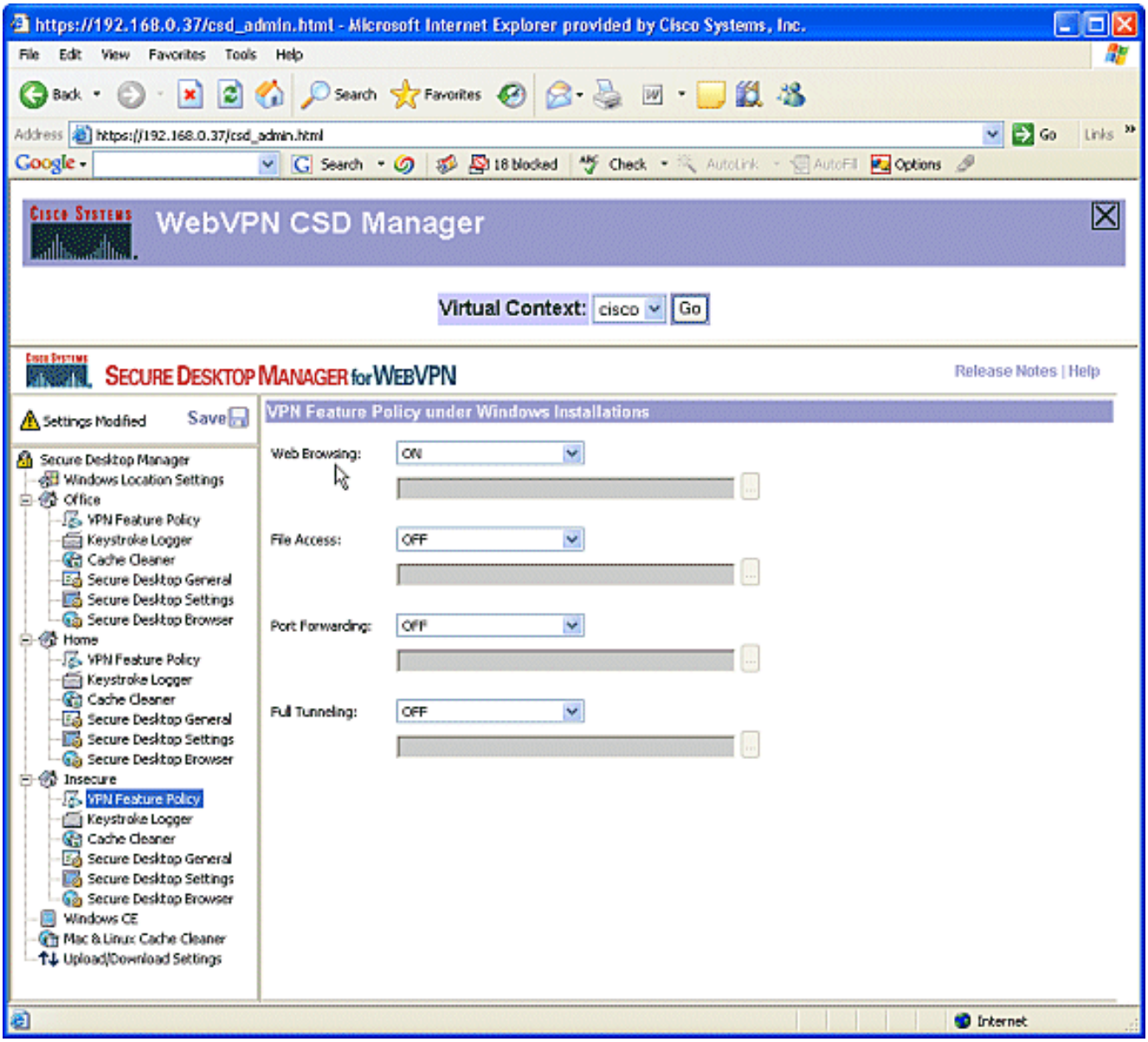
6. Selecteer onder Home de optie **Secure Desktop General**. Controleer **de toepassing desinstalleren nadat het bureaublad is gesloten**. Laat alle andere parameters bij hun standaardinstellingen zoals weergegeven in de schermopname.



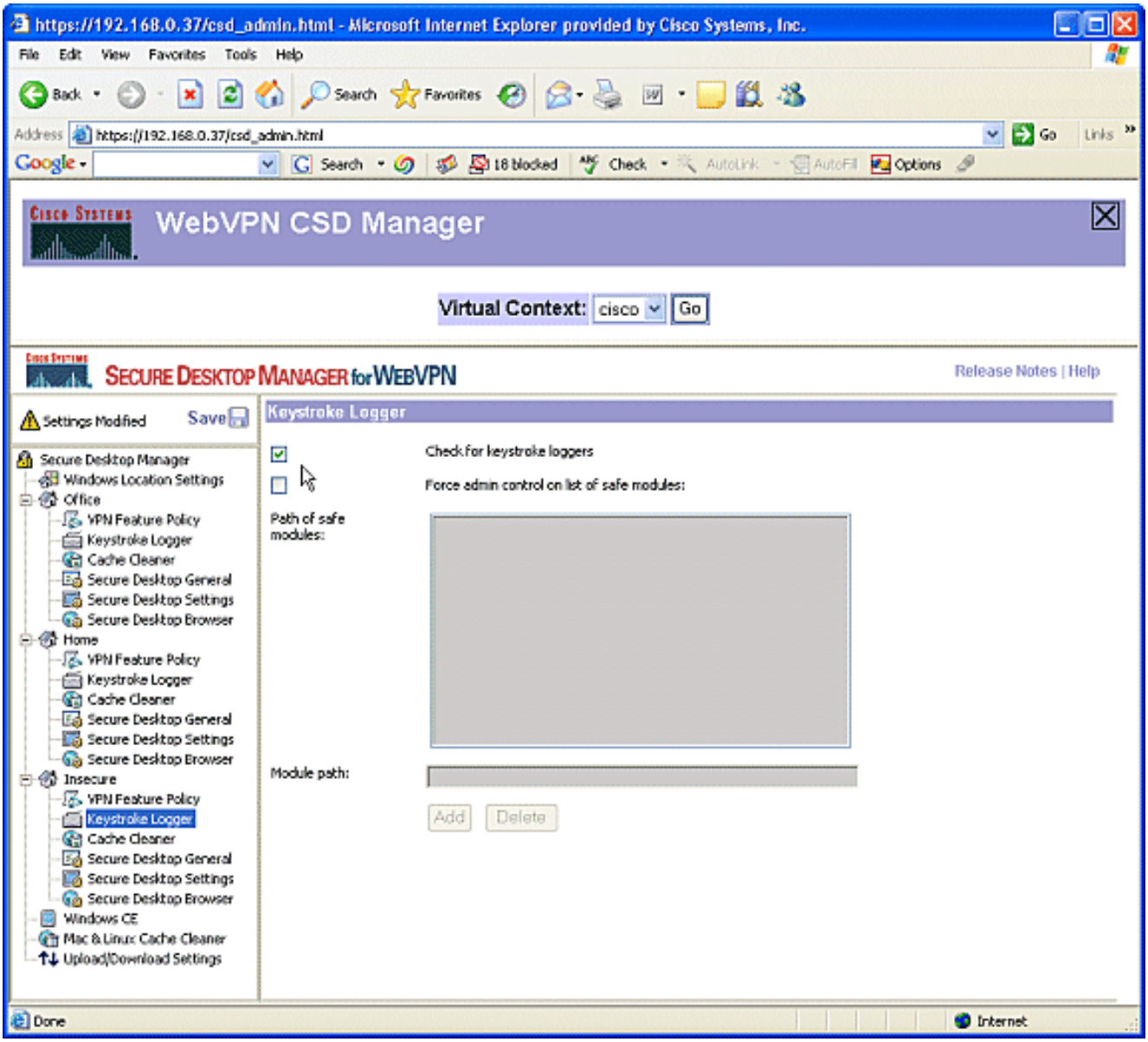
7. Selecteer voor beveiligde desktopinstellingen onder Start de optie **E-mailtoepassingen op transparante wijze laten werken**. Klik na de indiening op **Opslaan** en klik op **OK**.



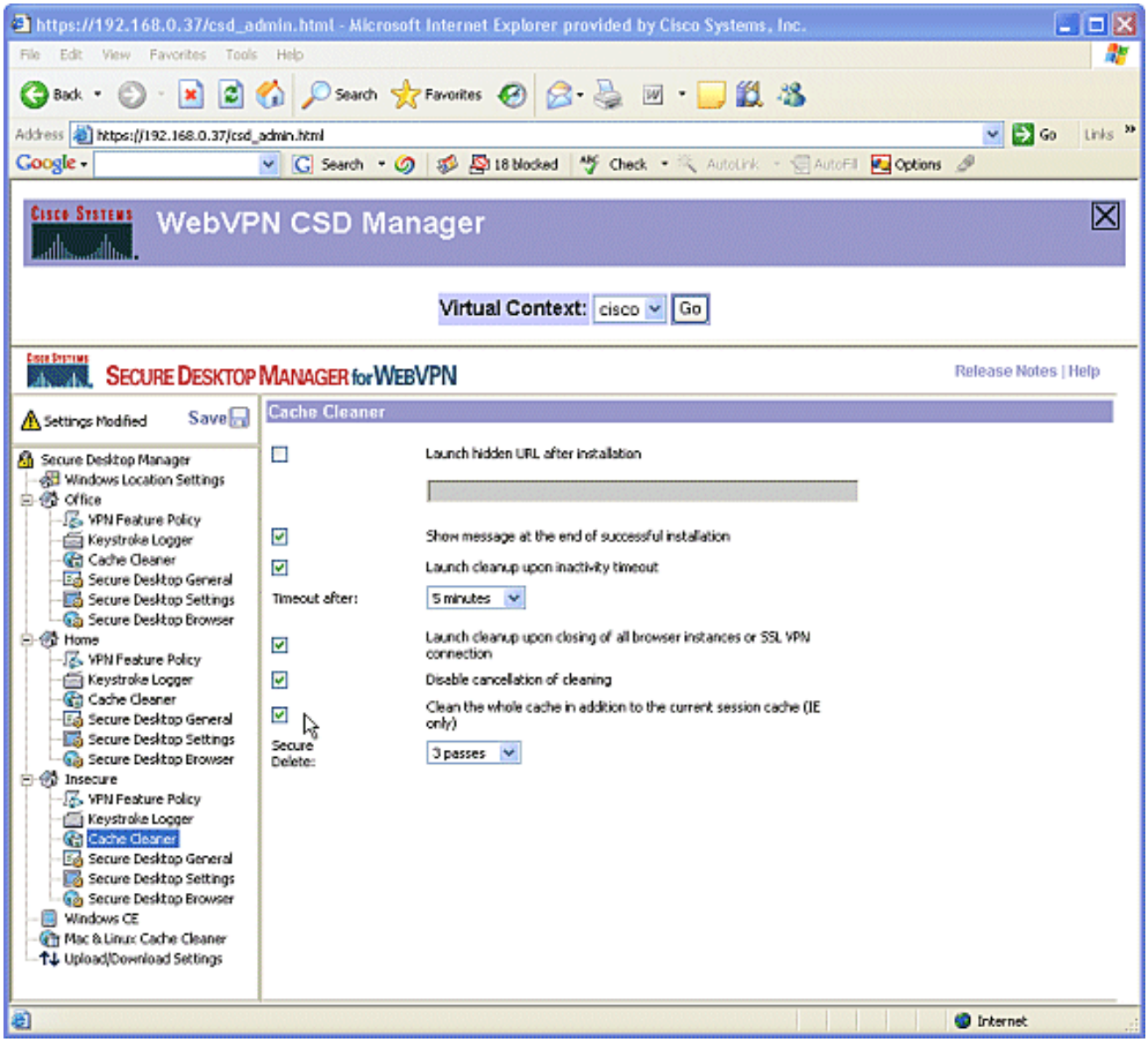
8. De configuratie van **Secure Desktop browser** is afhankelijk van of u deze gebruikers al dan niet toegang wilt hebben tot een bedrijfswebsite met vooraf ingestelde favorieten.Kies onder onveilig **VPN-functiebeleid**.Omdat dit geen vertrouwde gebruikers zijn, staat u alleen webbrowsen toe.Kies **ON** in het vervolgkeuzemenu voor **Web Browsing**.Alle andere toegang is ingesteld op
OFF.



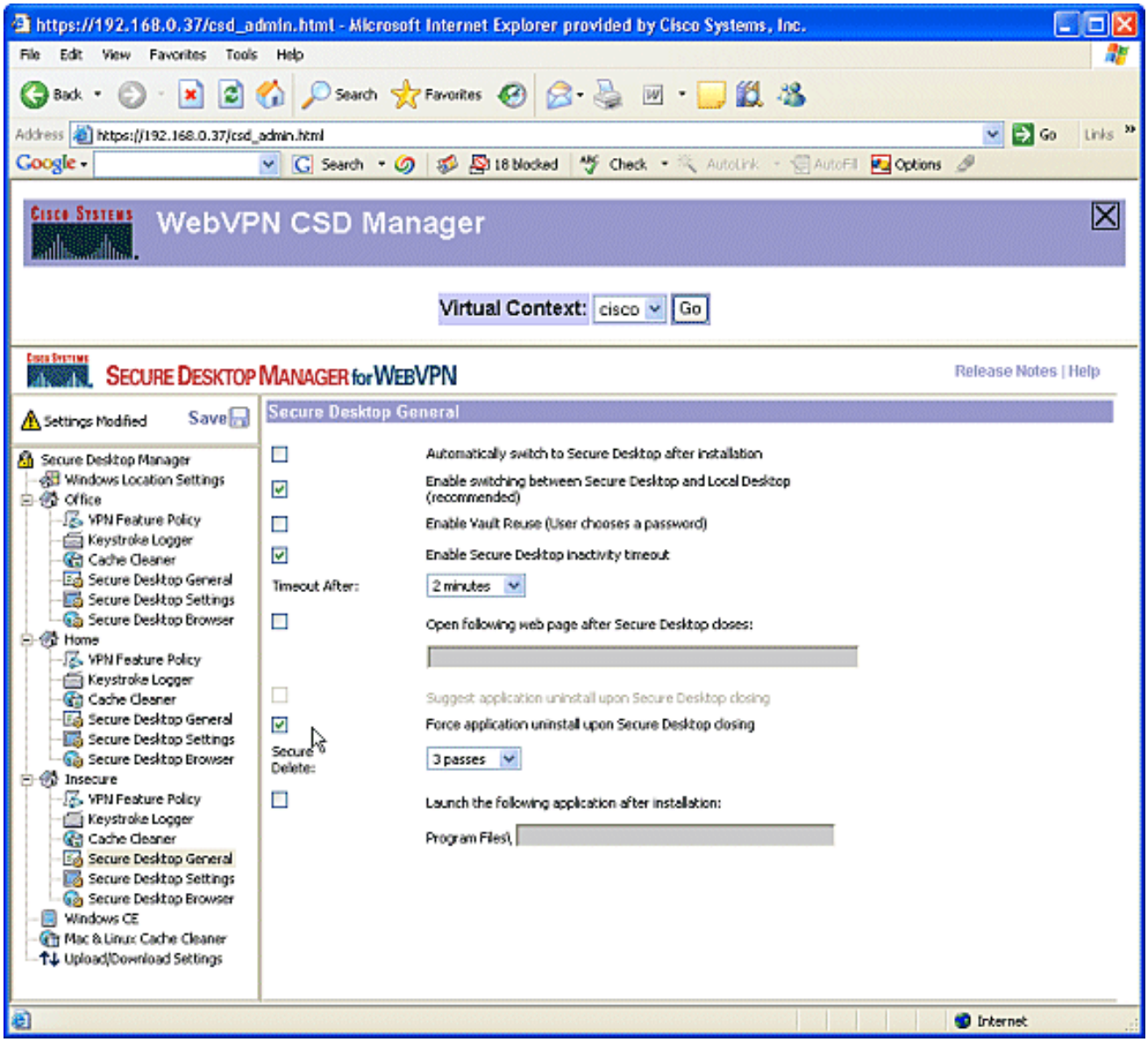
9. Controleer het aanvinkvakje **voor loggers** op **toetsenbord**.



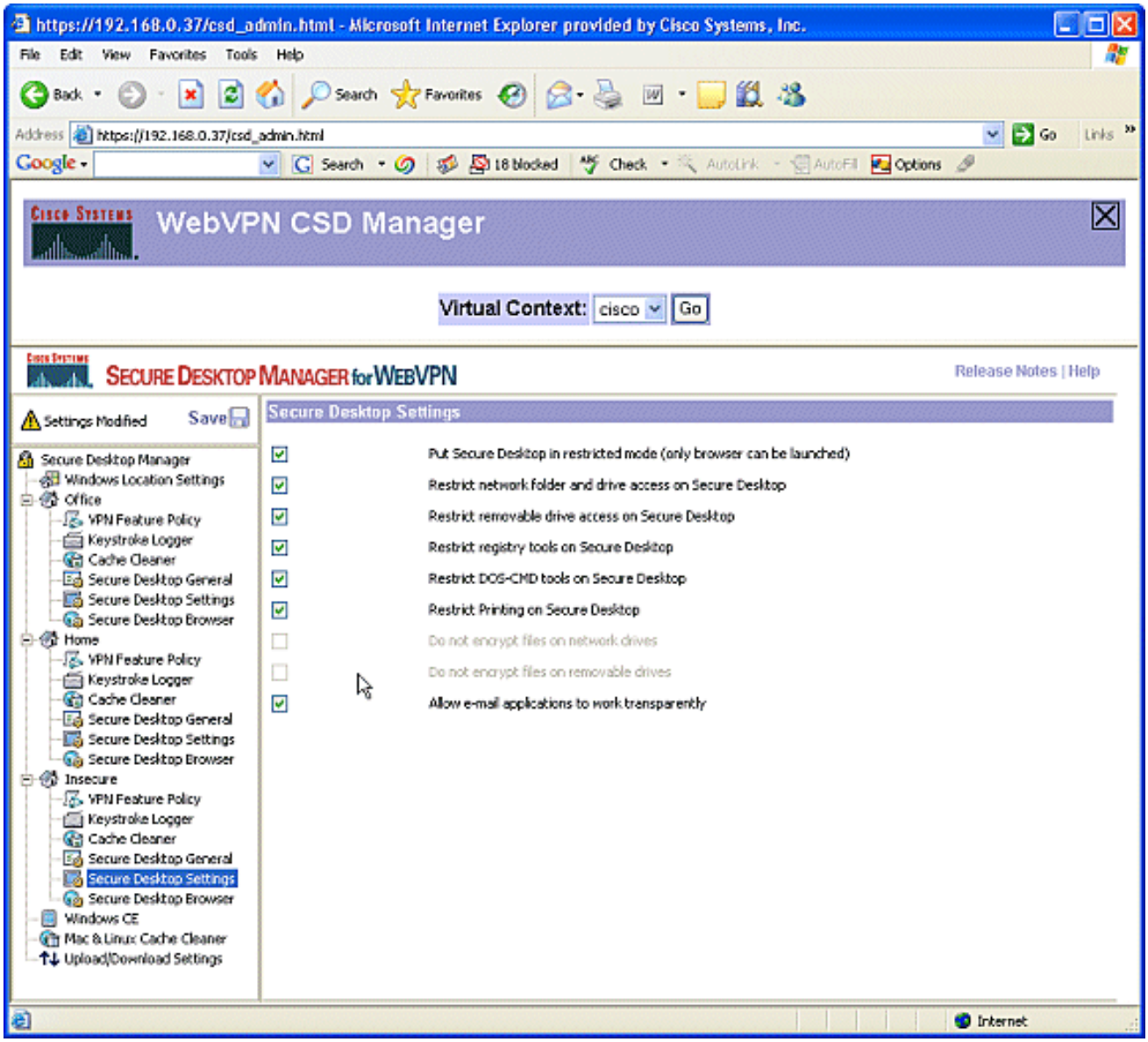
10. Configuratie van de Schoonmaakmachine voor onveilig.Controleer het **inlogvakje Clean the complete cache naast het huidige sessiecache (alleen IE)**.Laat de andere instellingen standaard
uit.



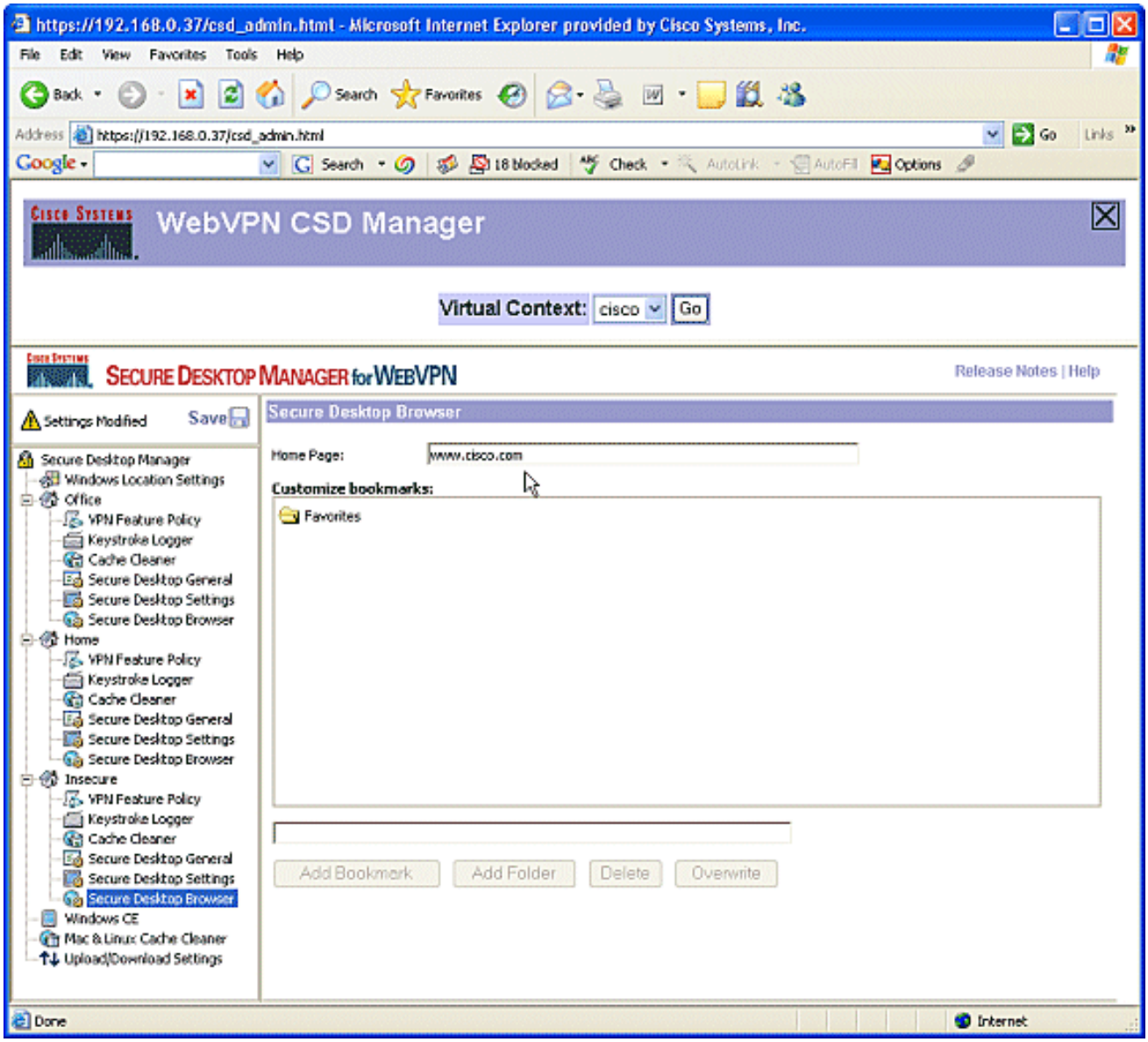
11. Selecteer onder Onveilig de optie **Secure Desktop General**.Verminder de time-out inactiviteit tot 2 minuten.Controleer de **toepassing Force** verwijderen **bij het** aanvinkvakje **Secure Desktop sluiten**.



12. Kies **Beveiligde desktopinstellingen** onder onveilig en stel de zeer beperkende instellingen in zoals wordt weergegeven.



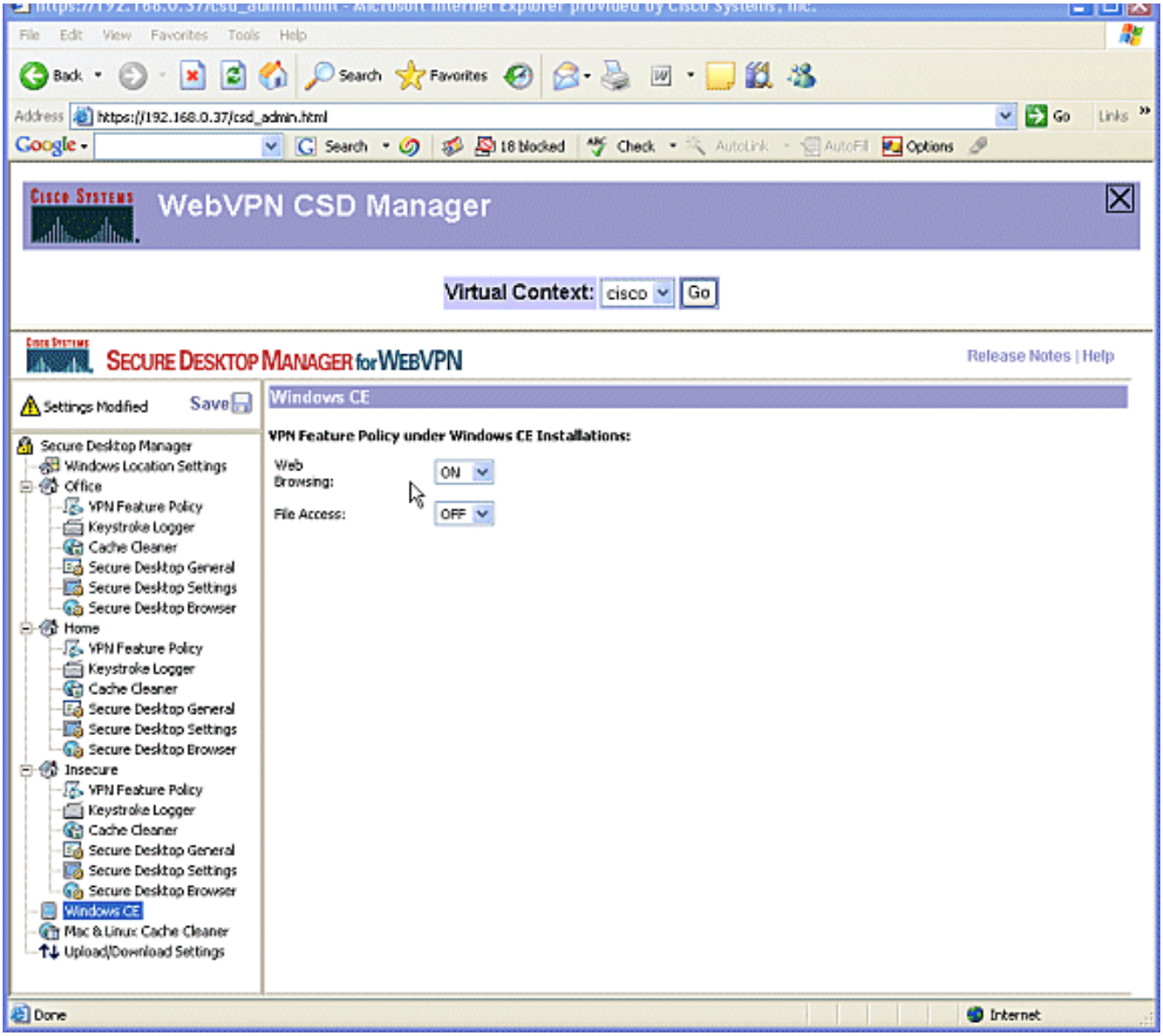
13. Kies **Secure Desktop browser**. Voer in het veld Thuispagina de website in waarop deze klanten voor hun startpagina zijn ingeschakeld.



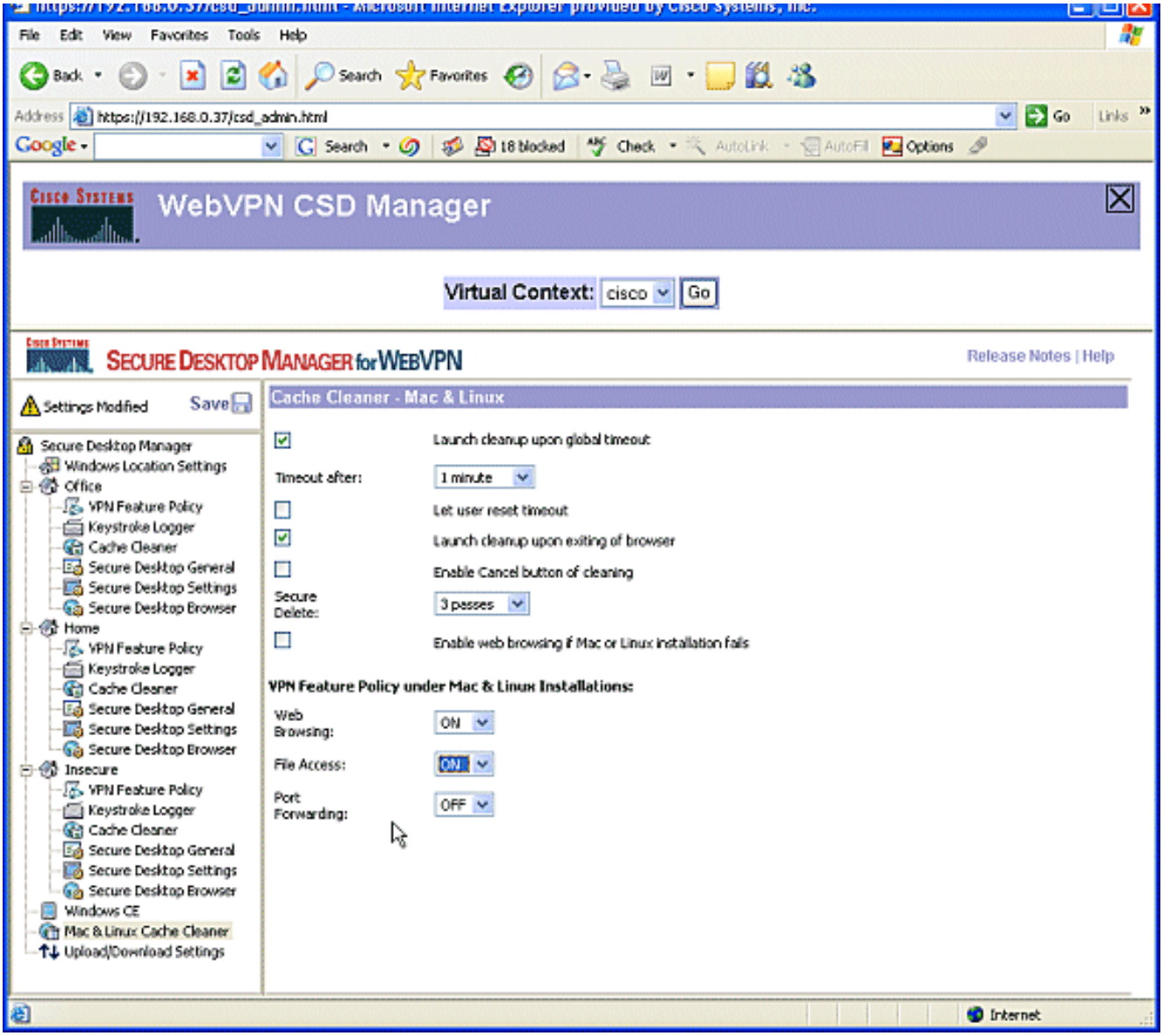
Fase II: Stap 4: Configureren Windows CE-, Macintosh- en Linux-functies.

Configureer de CSD-functies voor Windows CE, Macintosh en Linux.

1. Kies **Windows CE** onder Secure Desktop Manager. Windows CE heeft beperkte VPN-functies. Zet **Web Browsing in ON**.



2. Kies **Mac en Linux Cache Cleaner**.De Macintosh- en Linux-besturingssystemen hebben alleen toegang tot de cachestratieaspecten van CSD. Configureer ze zoals in de afbeelding.Klik na de indiening op **Opslaan** en klik op **OK**.

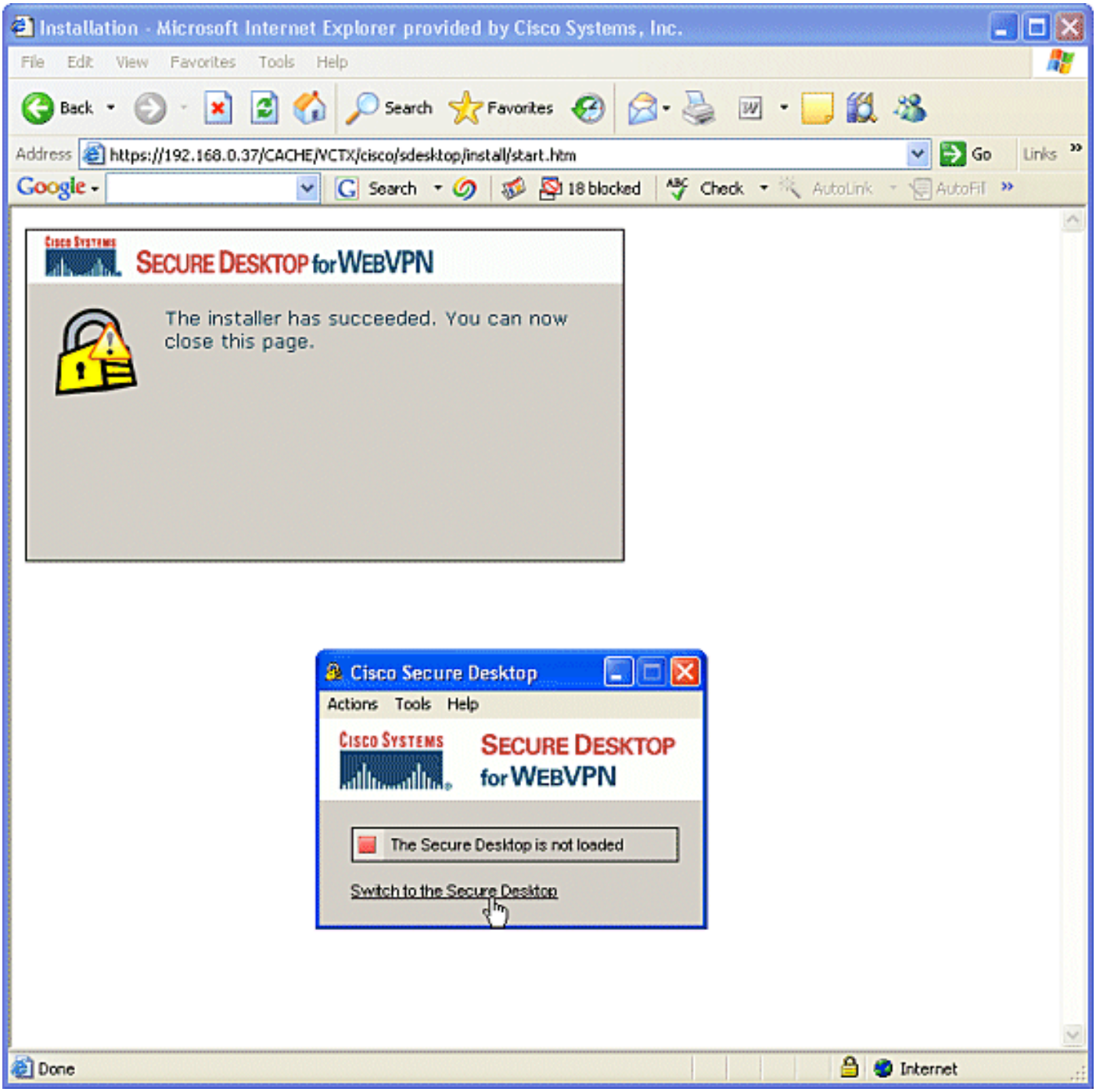


Verifiëren

Test van de CSD-werking

Test de bediening van CSD door verbinding te maken met de WebVPN gateway met een SSL-enabled browser op **https://WebVPN_Gateway_IP Address**.

Opmerking: Vergeet niet de unieke naam van de context te gebruiken als u verschillende WebVPN-contexten hebt gecreëerd, bijvoorbeeld **https://192.168.0.37/cisco**.



Opdrachten

Verschillende **tonen** opdrachten worden geassocieerd met WebVPN. U kunt deze opdrachten uitvoeren op de opdrachtregel-interface (CLI) om statistieken en andere informatie weer te geven. Raadpleeg voor gedetailleerde informatie over opdrachten **voor het** weergeven van de configuratie van WebVPN.

Opmerking: De CLI Analyzer (alleen geregistreerde klanten) ondersteunt bepaalde opdrachten voor de **show**. Gebruik de CLI Analyzer om een analyse van de opdrachtoutput **te** bekijken.

Problemen oplossen

Opdrachten

Meerdere **debug** opdrachten zijn gekoppeld aan WebVPN. Raadpleeg voor gedetailleerde informatie over deze opdrachten het gebruik van Debug Commands van WebVPN.

Opmerking: het gebruik van **debug-**opdrachten kan een negatieve invloed hebben op uw Cisco-apparaat. Voordat u **debug**-opdrachten gebruikt, raadpleegt u Belangrijke informatie over Debug Commands.

Raadpleeg voor meer informatie over **duidelijke** opdrachten de opdrachten WebVPN wissen.

Gerelateerde informatie

- Implementatiegids voor Webex en DMVPN-conversie
- SSL VPN - WebVPN
- Cisco IOS VPN-SLVPN
- Technische ondersteuning en documentatie – Cisco Systems