Configuración de CSD en Cisco IOS mediante SDM

Contenido

Introducción

Aunque las sesiones VPN de Secure Sockets Layer (SSL) (WebVPN de Cisco) sean seguras, el cliente puede tener todavía cookies, archivos del navegador y adjuntos de correo electrónico después de completarse una sesión. Cisco Secure Desktop (CSD) amplía la seguridad inherente de las sesiones de SSL VPN escribiendo los datos de sesión en un formato cifrado en un área *vault* especial del disco del cliente. Además, estos datos se quitan del disco al final de la sesión VPN de SSL. Este documento presenta una configuración de ejemplo para CSD en un Cisco IOS® router.

CSD es compatible con las siguientes plataformas de dispositivos de Cisco:

- Routers Cisco IOS versión 12.4(6)T y posteriores
- Cisco 870, 1811, 1841, 2801, 2811, 2821, 2851, 3725, 3745, 3825, 3845, 7200 y 730 Routers1
- Concentradores de la serie Cisco VPN 3000 versión 4.7 y posteriores
- Dispositivos de seguridad Cisco ASA serie 5500 versión 7.1 y posteriores

- Cisco WebVPN Services Module para Cisco Catalyst y Cisco 7600 Series versión 1.2 y posteriores

Prerequisites

Requirements

Asegúrese de cumplir estos requisitos antes de intentar esta configuración:

Requisitos para el router Cisco IOS

- Router Cisco IOS con imagen avanzada 12.4(6T) o posterior
- Cisco Router Secure Device Manager (SDM) 2.3 o superior
- Una copia del paquete CSD para IOS en su estación de administración
- Certificado digital autofirmado o autenticación con una autoridad de certificación (CA)**Nota:** Cuando utilice certificados digitales, asegúrese de establecer correctamente el nombre de host, el nombre de dominio y la fecha/hora/zona horaria del router.
- Una contraseña secreta de habilitación en el router
- DNS activado en el router. Varios servicios WebVPN requieren que DNS funcione correctamente.

Requisitos para ordenadores cliente

- Los clientes remotos deben tener privilegios administrativos locales; no es obligatorio, pero se sugiere con sumo cuidado.
- Los clientes remotos deben tener Java Runtime Environment (JRE) versión 1.4 o superior.
- Exploradores de clientes remotos: Internet Explorer 6.0, Netscape 7.1, Mozilla 1.7, Safari 1.2.2 o Firefox 1.0
- Cookies activadas y Popups permitidas en clientes remotos

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- Router Cisco IOS 3825 con versión 12.9(T)
- SDM versión 2.3.1

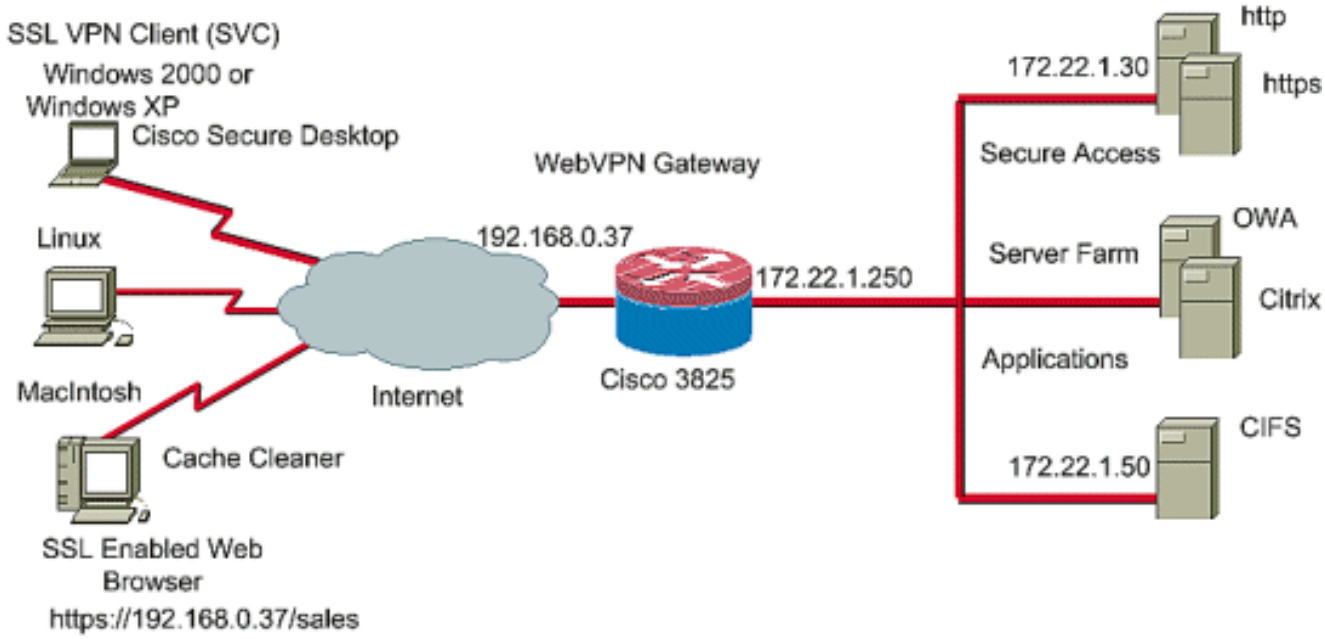
The information in this document was created from the devices in a specific lab environment. Todos los dispositivos usados en este documento comenzaron con una configuración despejada (predeterminada). If your network is live, make sure that you understand the potential impact of any command.

Diagrama de la red

En este documento, se utiliza esta configuración de red:

Este ejemplo utiliza un router Cisco serie 3825 para permitir el acceso seguro a la intranet de la empresa. El router Cisco serie 3825 mejora la seguridad de las conexiones VPN SSL con características y características CSD configurables. Los clientes pueden conectarse al router

habilitado para CSD a través de uno de estos tres métodos SSL VPN: Clientless SSL VPN (WebVPN), Thin-Client SSL VPN (Port-Forwarding) o SSL VPN Client (SVC de tunelación completa).



Productos Relacionados

Esta configuración también se puede utilizar con las siguientes versiones de hardware y software:

- Plataformas de router de Cisco 870, 1811, 1841, 2801, 2811, 2821 2851, 3725, 3745.3825, 3845, 7200 y 73 01
- Imagen de seguridad avanzada de Cisco IOS versión 12.4(6)T y posteriores

Convenciones

Consulte Convenciones de Consejos Técnicos de Cisco para obtener más información sobre las convenciones de los documentos.

Configurar

Un gateway WebVPN permite al usuario conectarse al router a través de una de las tecnologías SSL VPN. Sólo se permite un gateway WebVPN por dirección IP en el dispositivo, aunque se puede conectar más de un contexto WebVPN a un gateway WebVPN. Cada contexto se identifica con un nombre único. Las políticas de grupo identifican los recursos configurados disponibles para un contexto WebVPN determinado.

La configuración de CSD en un router IOS se realiza en dos fases:

Fase I: Prepare su router para la configuración de CSD con SDM

1. Configure un gateway WebVPN, un contexto WebVPN y una política de grupo.**Nota:** Este paso es opcional y no se trata con detalle en este documento. Si ya ha configurado el router para una de las tecnologías SSL VPN, omita este paso.

2. Habilite CSD en un contexto WebVPN.

Fase II: Configure CSD mediante un navegador web.

1. Definir *ubicaciones de Windows*.
2. Identificar los criterios de ubicación.
3. Configure las funciones y los módulos de ubicación de Windows.
4. Configure las funciones de Windows CE, Macintosh y Linux.

Fase I: Prepare su router para la configuración de CSD con SDM.

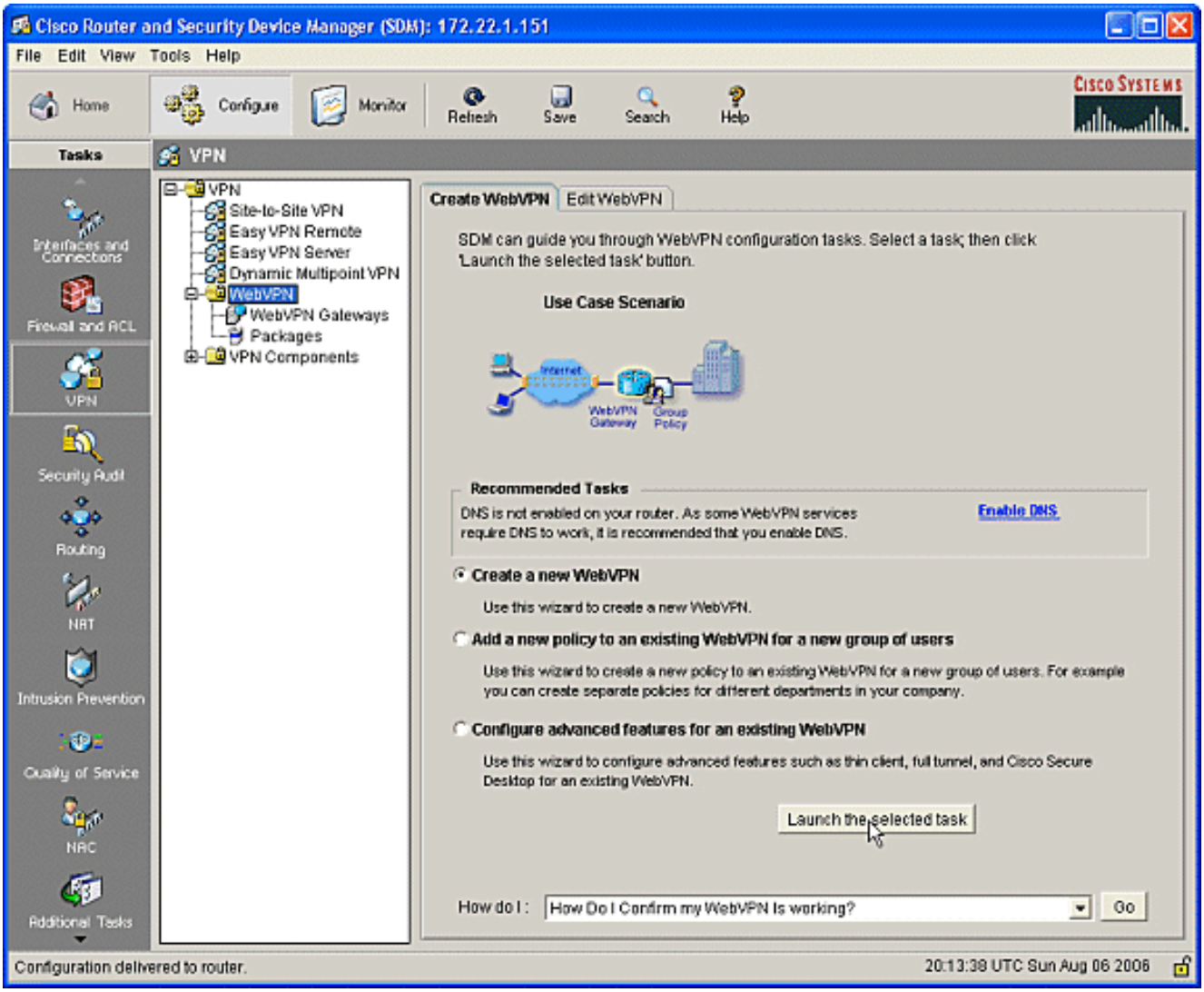
CSD se puede configurar con SDM o desde la interfaz de línea de comandos (CLI). Esta configuración utiliza SDM y un navegador web.

Estos pasos se utilizan para completar la configuración de CSD en su router IOS.

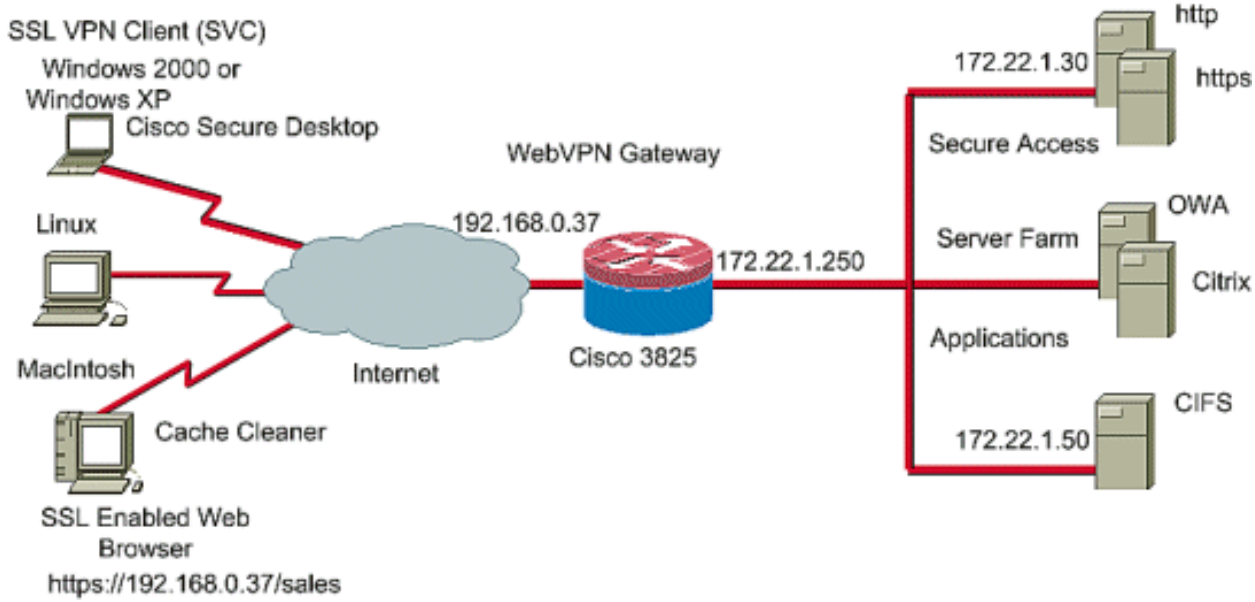
Fase I: Paso 1: Configure un gateway WebVPN, un contexto WebVPN y una política de grupo.

Puede utilizar el Asistente para WebVPN para realizar esta tarea.

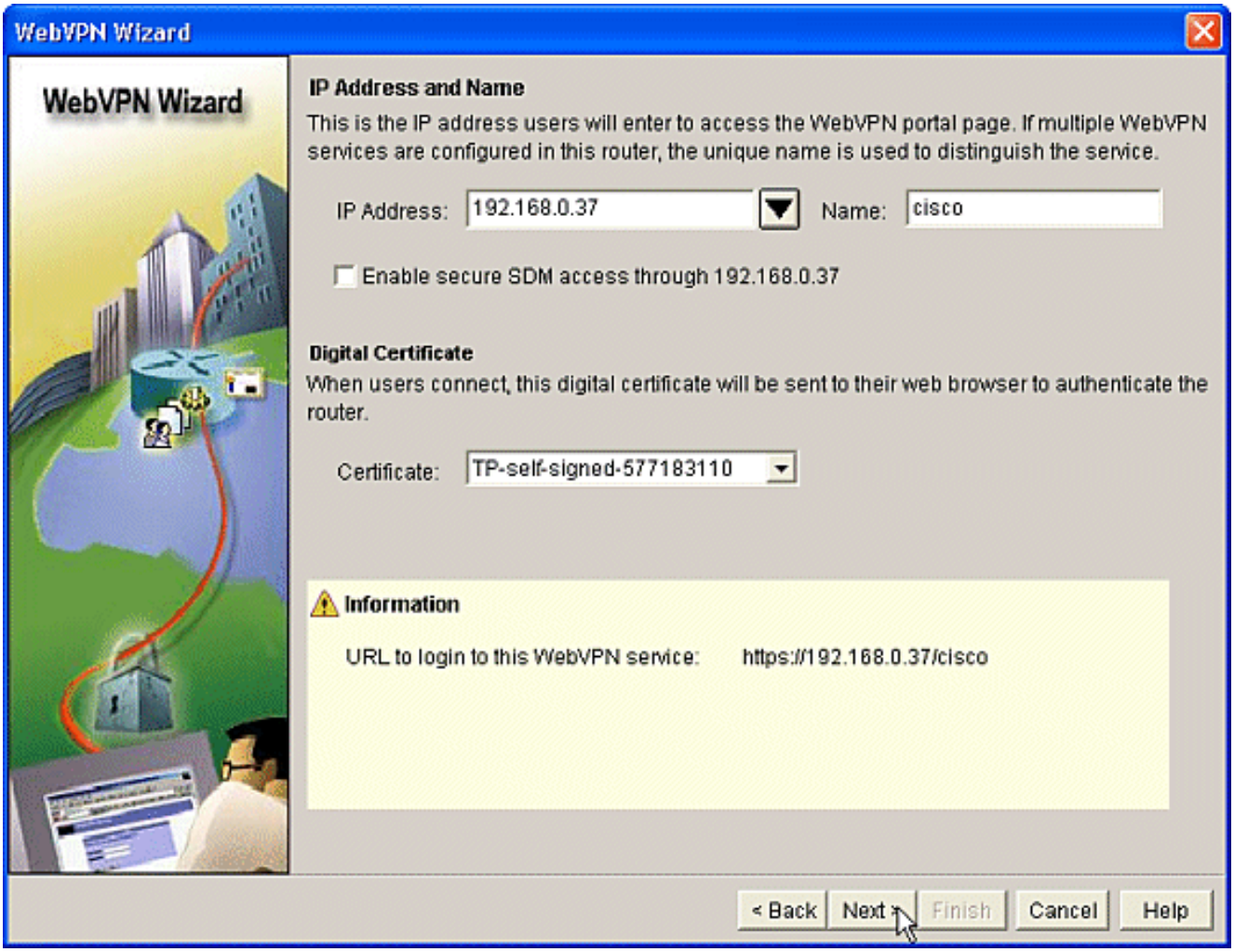
1. Abra SDM y vaya a **Configure > VPN > WebVPN**. Haga clic en la ficha **Create WebVPN** y marque el botón de opción **Create a new WebVPN**. Haga clic en **Iniciar la tarea seleccionada**.



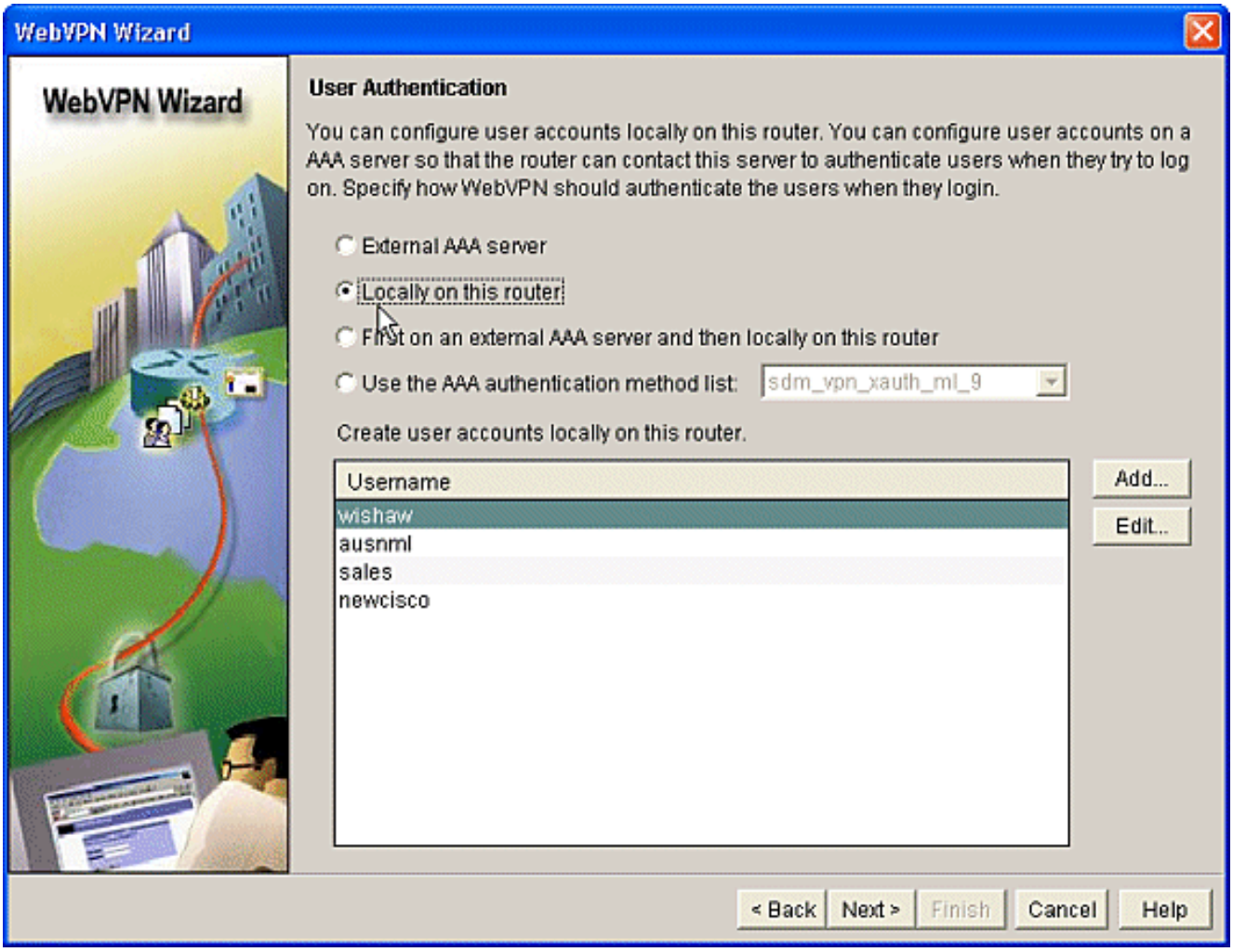
2. La pantalla Asistente para WebVPN muestra los parámetros que puede configurar. Haga clic en Next
(Siguiente).



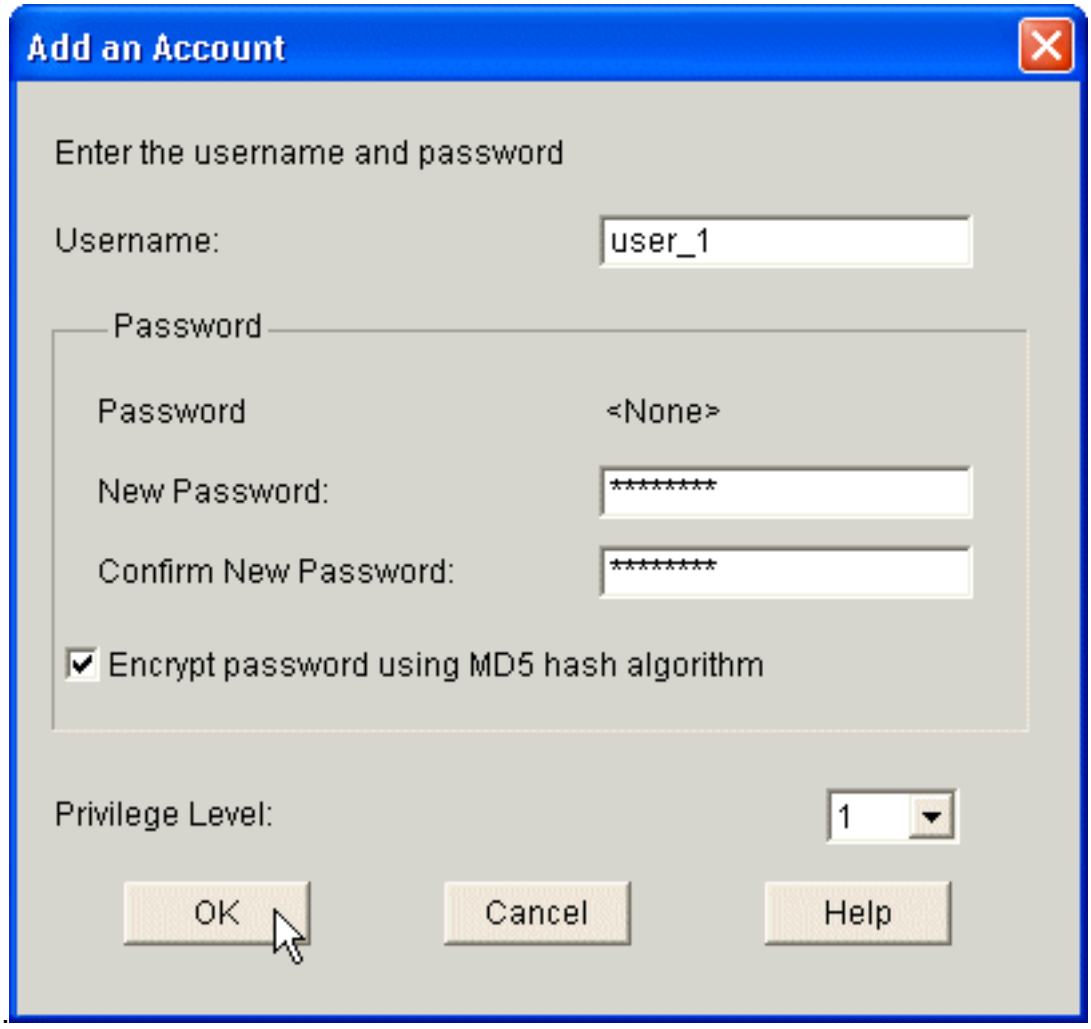
3. Introduzca la dirección IP del gateway de WebVPN, un nombre único para el servicio e información de certificado digital. Haga clic en Next
(Siguiente).



4. Se pueden crear cuentas de usuario para la autenticación en este gateway de WebVPN. Puede utilizar cuentas locales o cuentas creadas en un servidor externo de autenticación, autorización y contabilidad (AAA). Este ejemplo utiliza cuentas locales en el router. Verifique el botón de opción **Localmente en este router** y haga clic en **Agregar**.

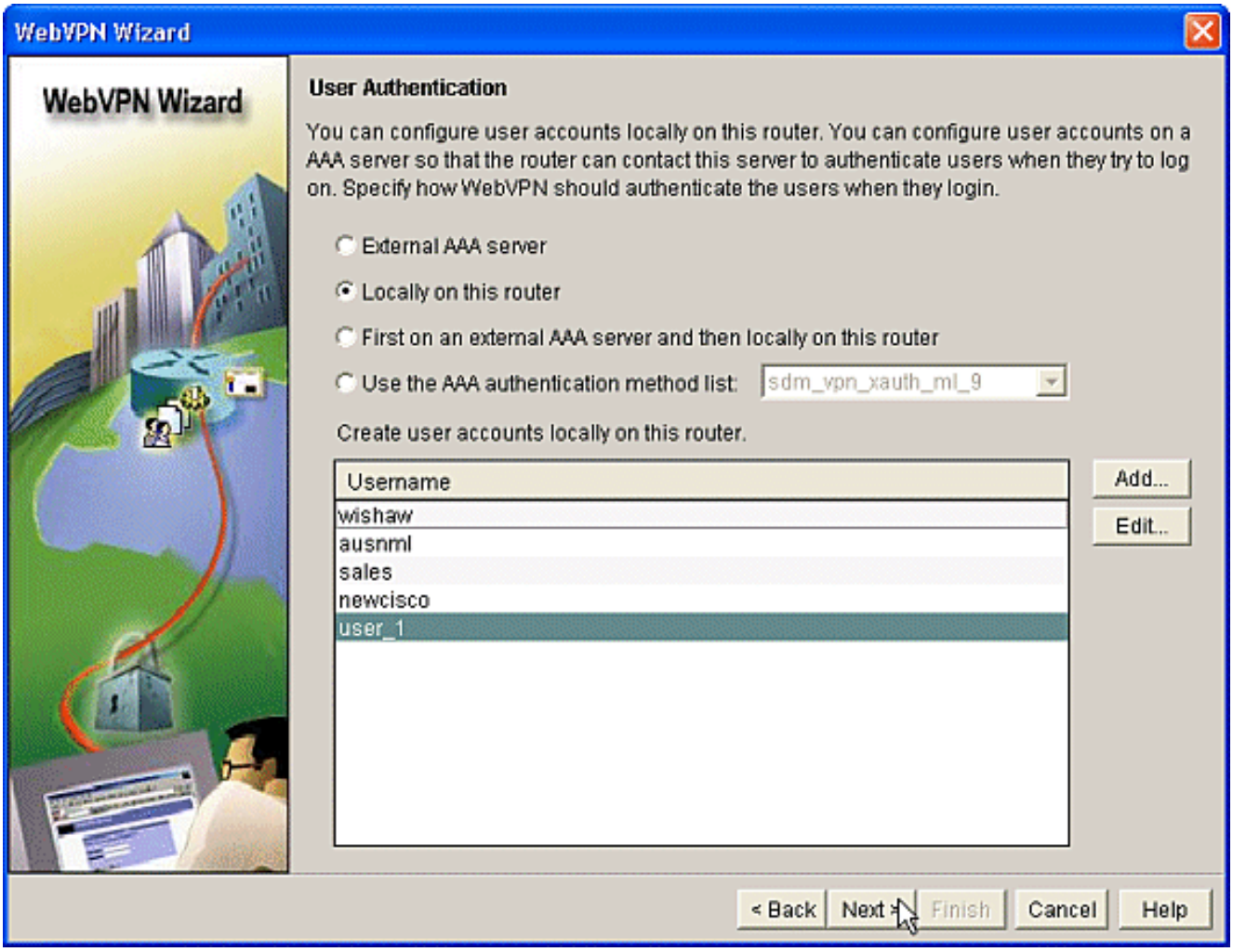


5. Introduzca la información de cuenta del nuevo usuario en la pantalla Add an Account (Agregar una cuenta) y haga clic en **OK**

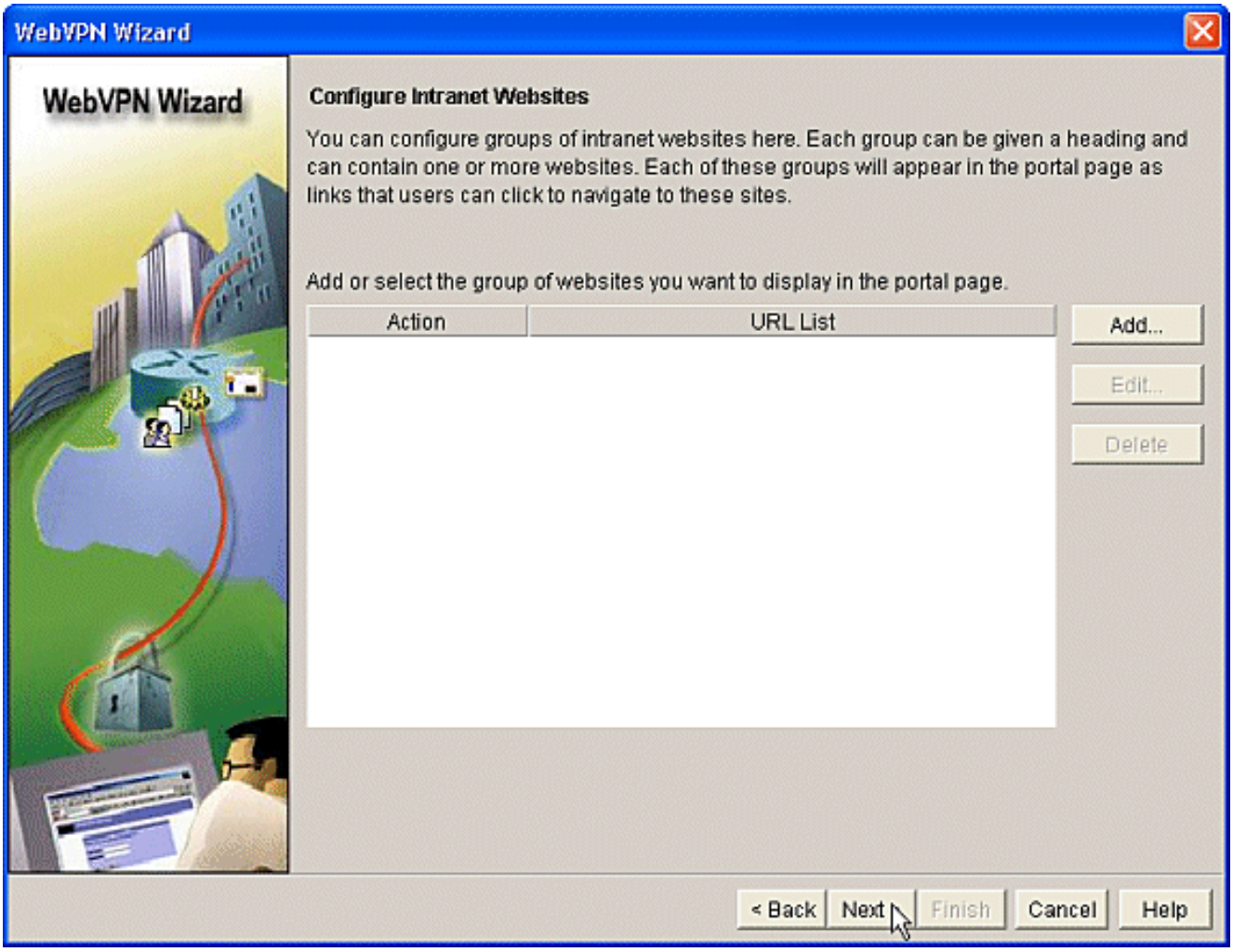


(Aceptar).

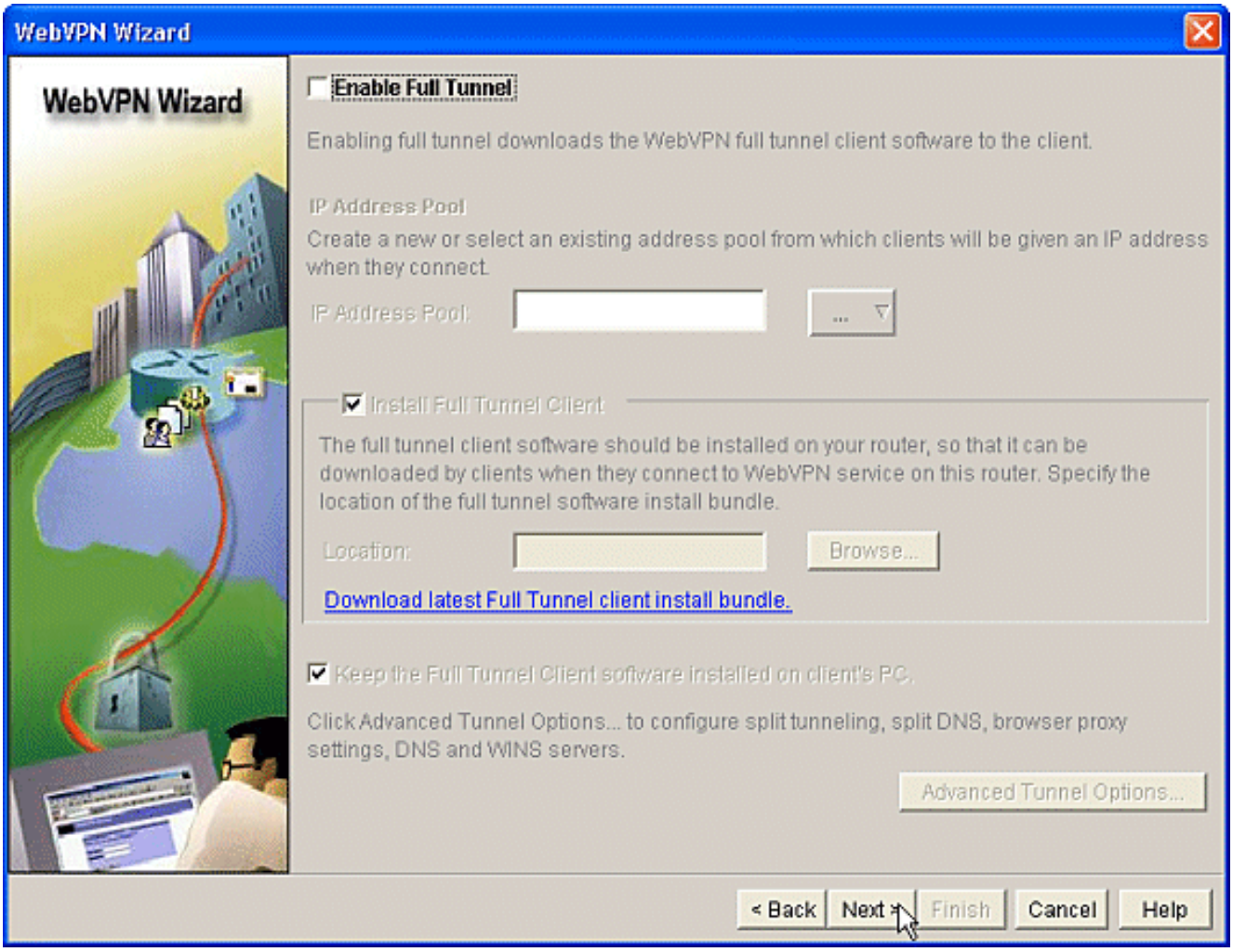
6. Después de haber creado los usuarios, haga clic en **Siguiente** en la página Autenticación de usuario.



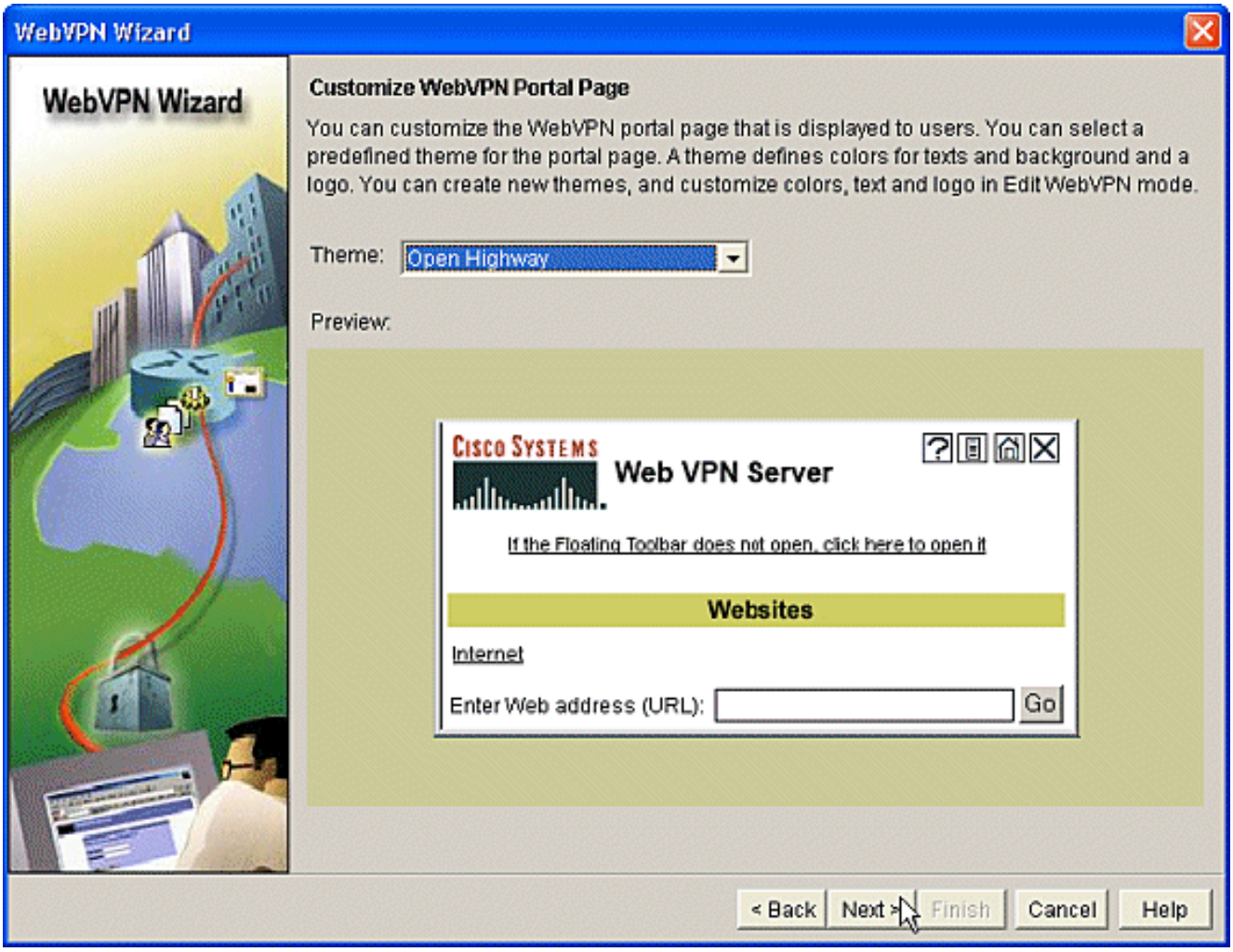
7. La pantalla Configure Intranet Websites (Configurar sitios web de la intranet) permite configurar el sitio web disponible para los usuarios del gateway de WebVPN. Dado que el foco de este documento es la configuración de CSD, ignore esta página. Haga clic en Next (Siguiente).



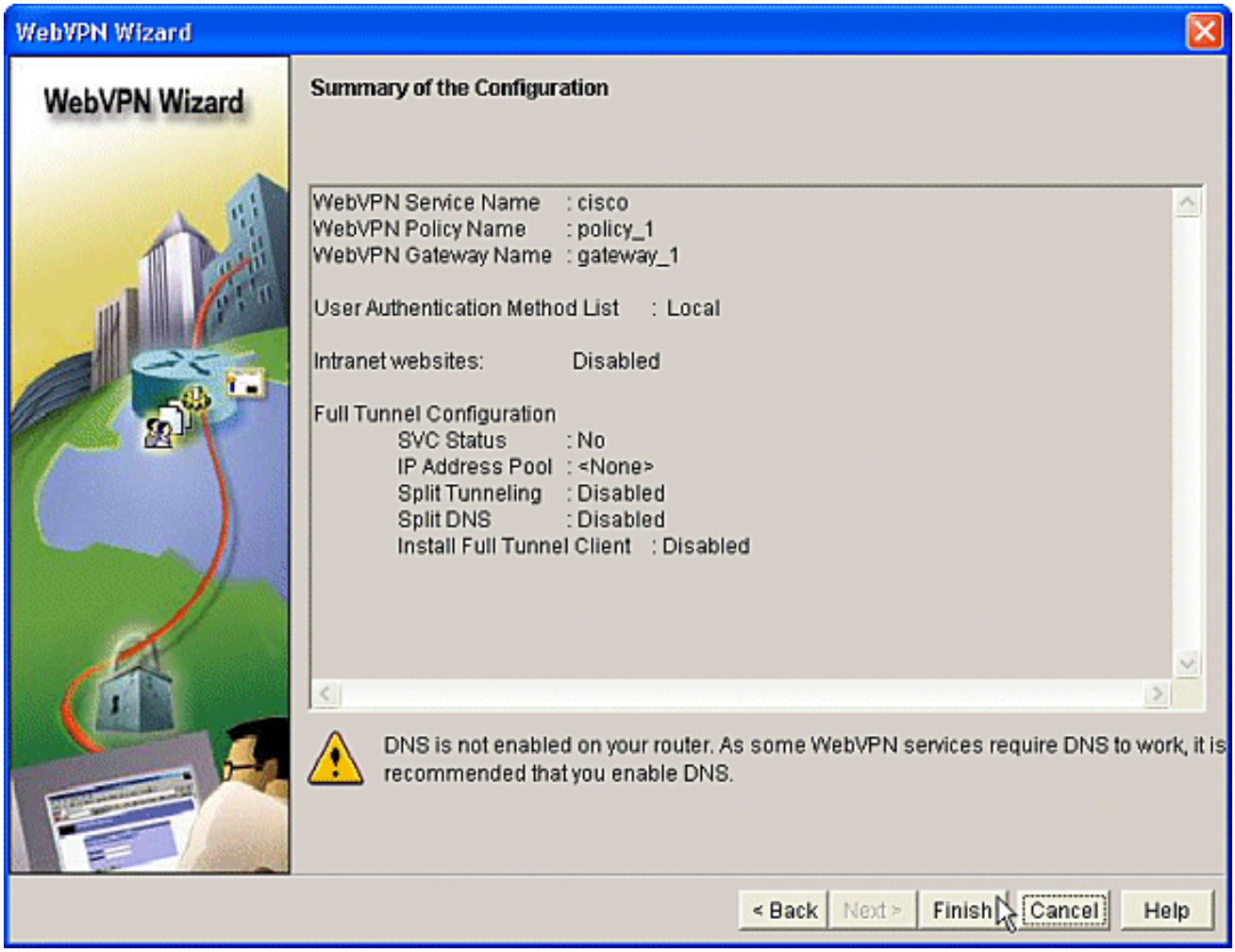
8. Aunque la siguiente pantalla WebVPN Wizard le permite elegir habilitar Full Tunnel SSL VPN Client, el foco de este documento es cómo habilitar CSD. Desmarque **Enable Full Tunnel** y haga clic en
Next.



9. Puede personalizar la apariencia de la página del portal WebVPN para los usuarios. En este caso, se acepta la apariencia predeterminada. Haga clic en Next (Siguiente).



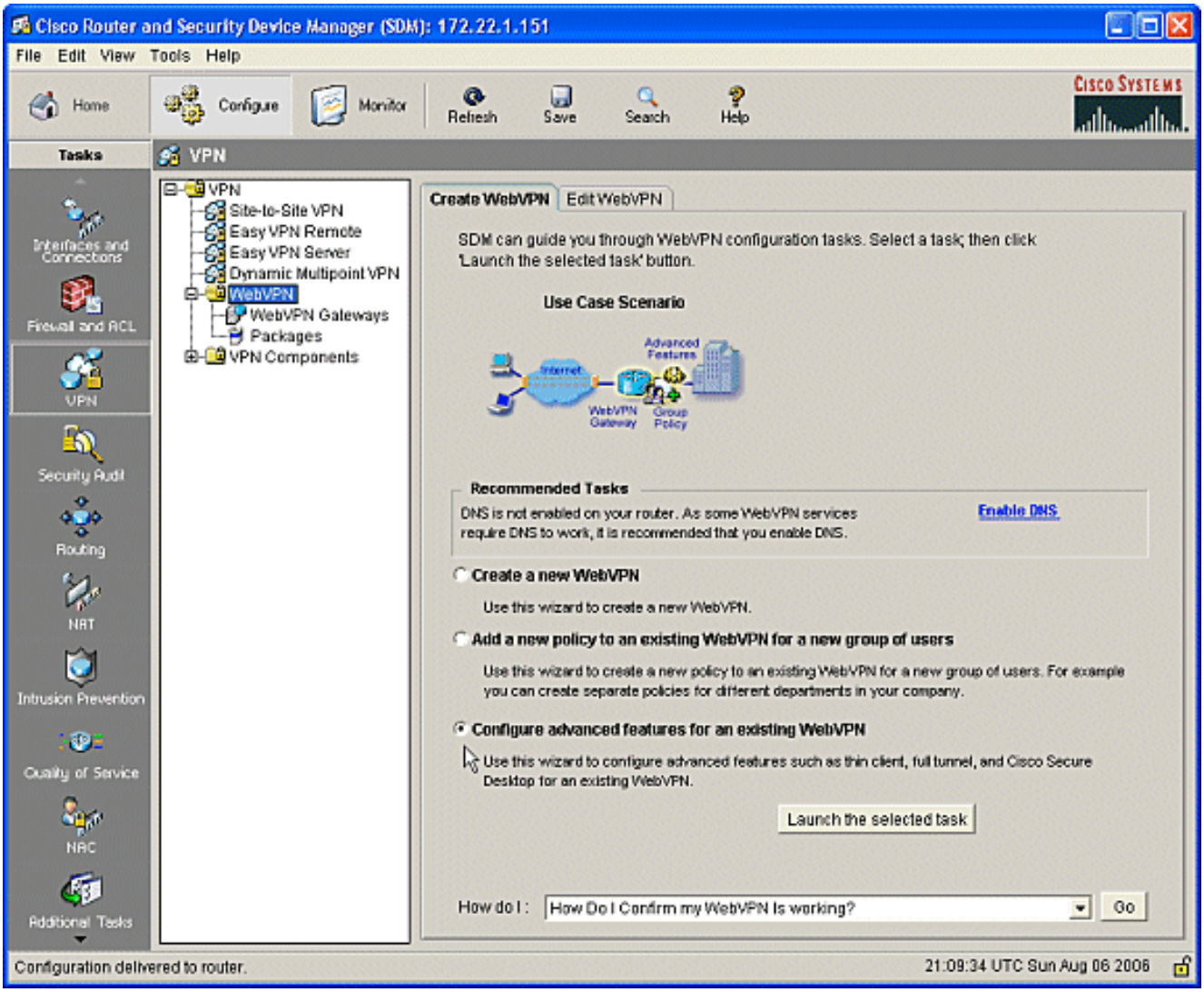
10. El asistente muestra la última pantalla de esta serie. Muestra un resumen de la configuración del gateway de WebVPN. Haga clic en **Finalizar** y, cuando se le solicite, haga clic en
Aceptar.



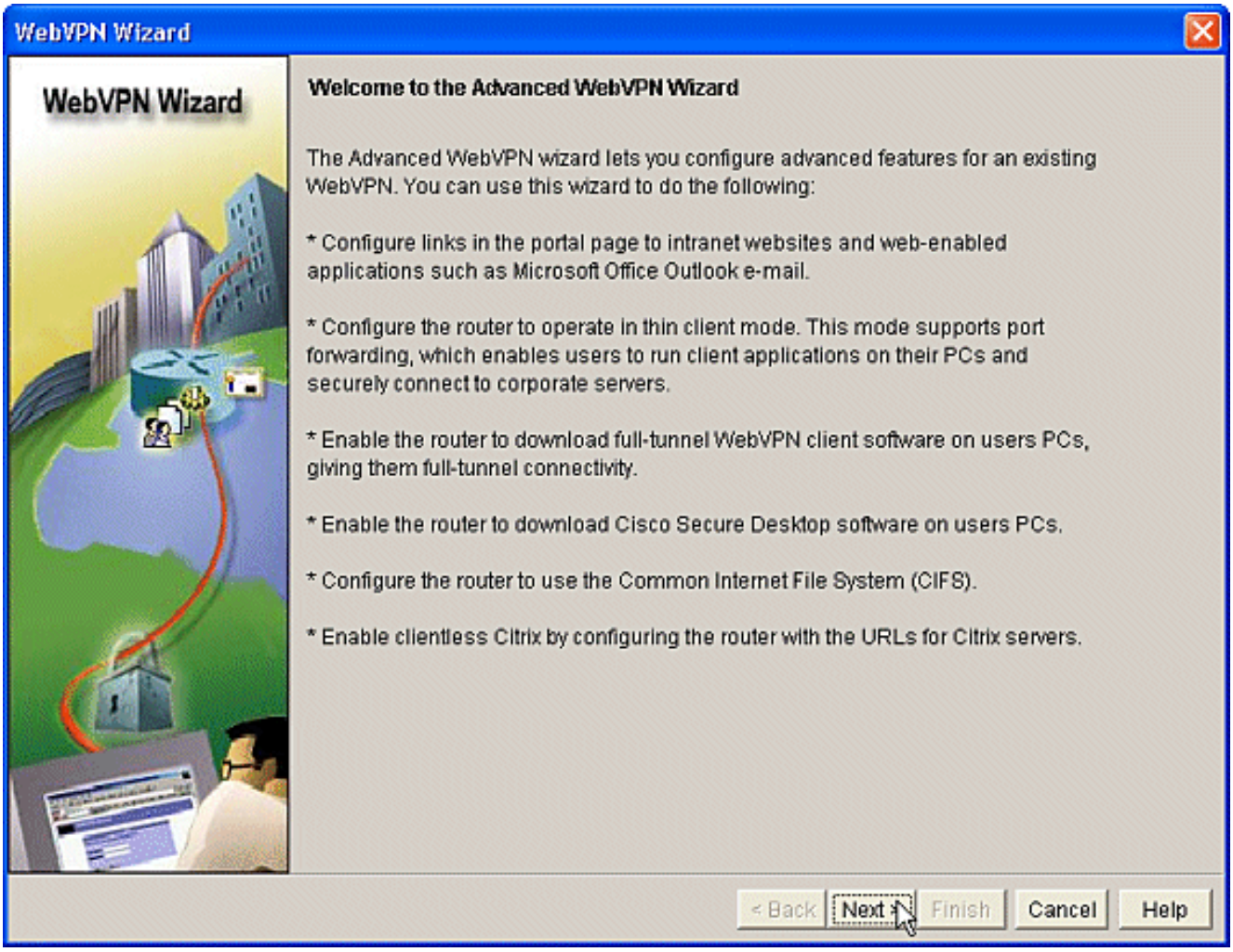
Fase I: Paso 2: Habilite CSD en un contexto WebVPN.

Utilice WebVPN Wizard para habilitar CSD en un contexto WebVPN.

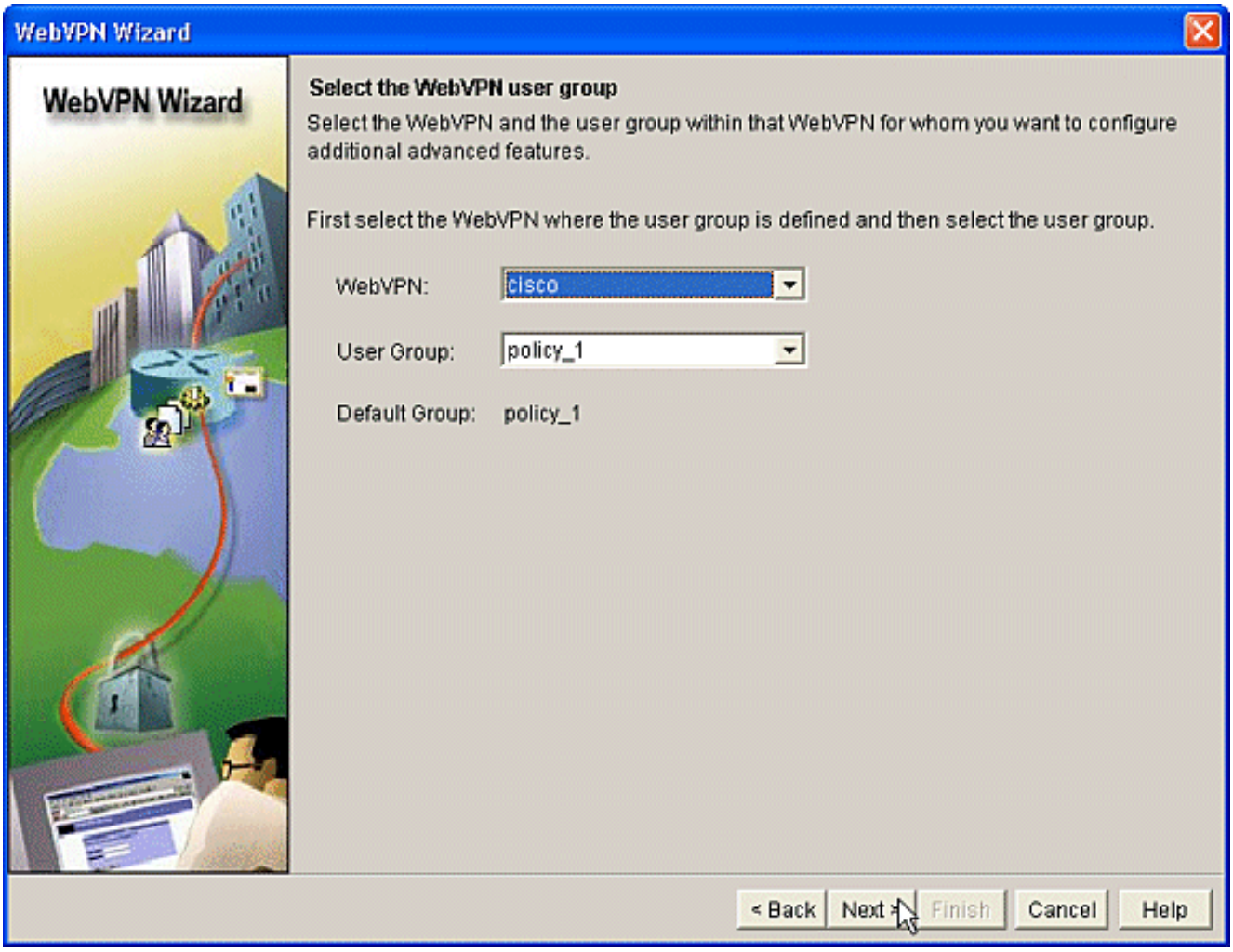
1. Utilice las funciones avanzadas del asistente de WebVPN para habilitar el CSD para el contexto recién creado. El asistente le da la oportunidad de instalar el paquete CSD si aún no está instalado.En SDM, haga clic en la ficha **Configurar**.En el panel de navegación, haga clic en **VPN > WebVPN**.Haga clic en la pestaña **Create WebVPN**.Marque el botón de opción **Configurar funciones avanzadas para un WebVPN existente**.Haga clic en el botón **Iniciar la tarea seleccionada**.



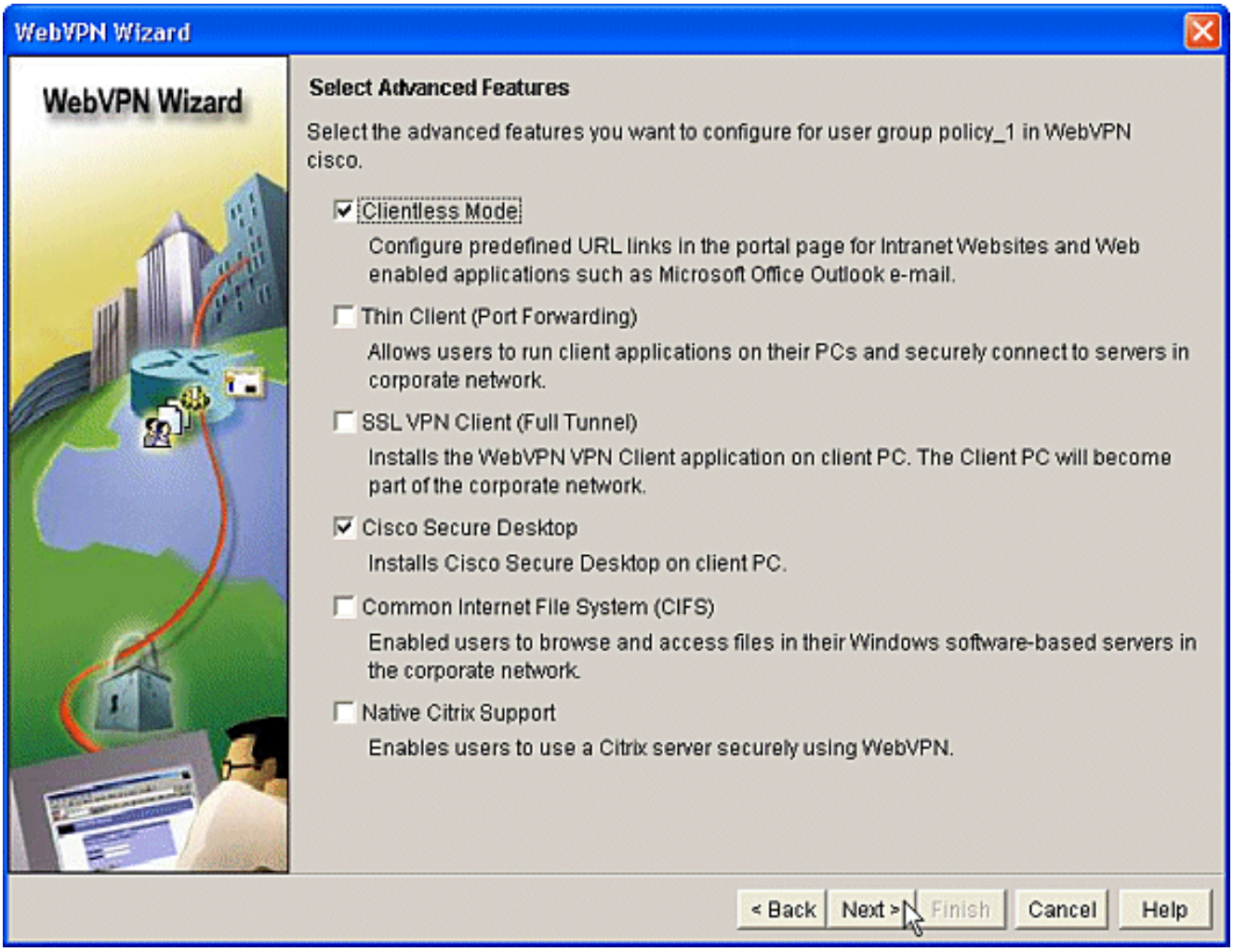
2. Se muestra la página de bienvenida del Asistente para WebVPN avanzado. Haga clic en Next
(Siguiente).



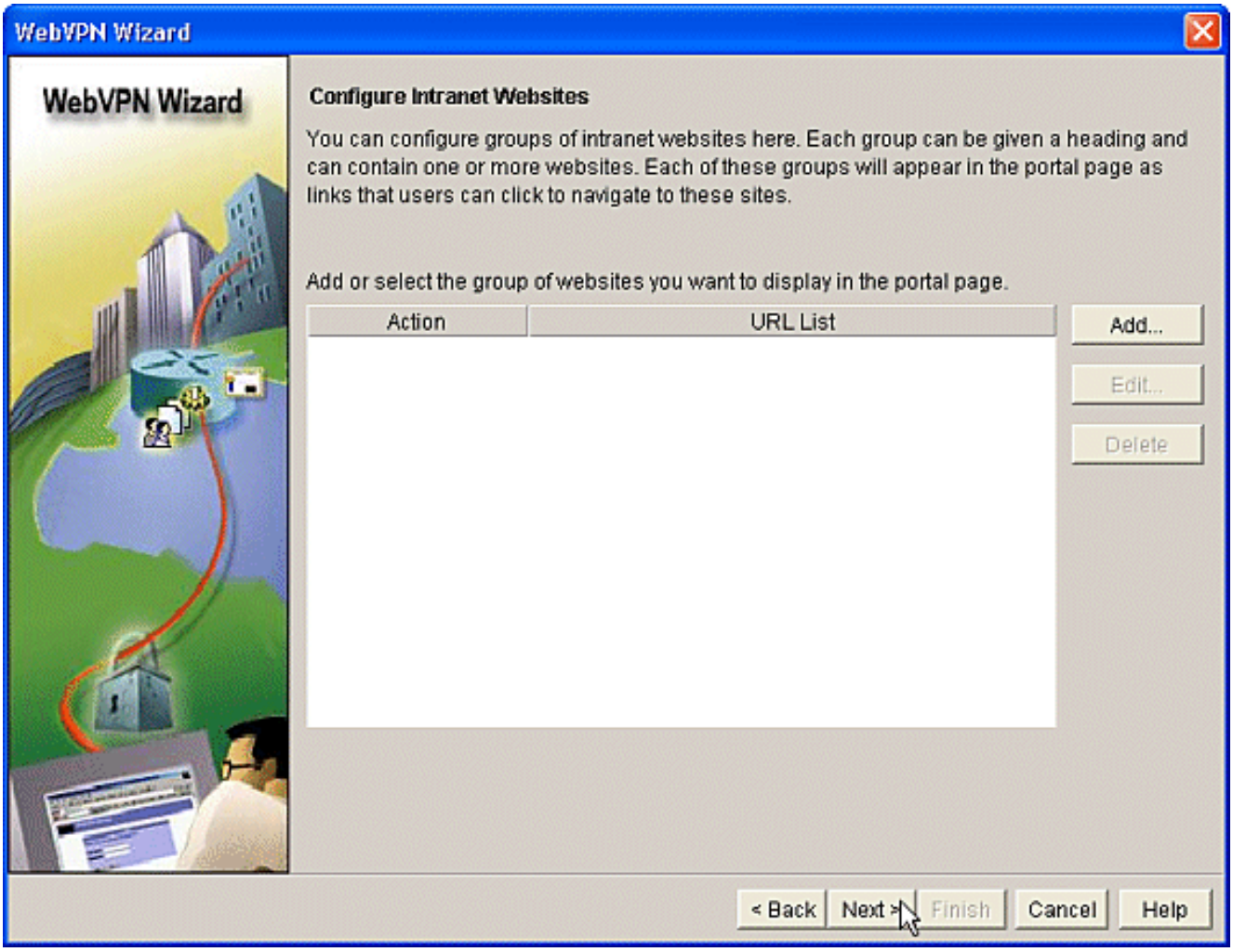
3. Elija WebVPN y el grupo de usuarios en los cuadros desplegables de los campos. Las funciones del Asistente para WebVPN avanzado se aplicarán a sus opciones. Haga clic en Next
(Siguiente).



4. La pantalla Select Advanced Features (Seleccionar funciones avanzadas) le permite elegir entre las tecnologías enumeradas.Verifique **Cisco Secure Desktop**.En este ejemplo, la opción es **Modo sin cliente**.Si elige alguna de las otras tecnologías enumeradas, se abrirán ventanas adicionales para permitir la entrada de información relacionada.Haga clic en el botón
Next.

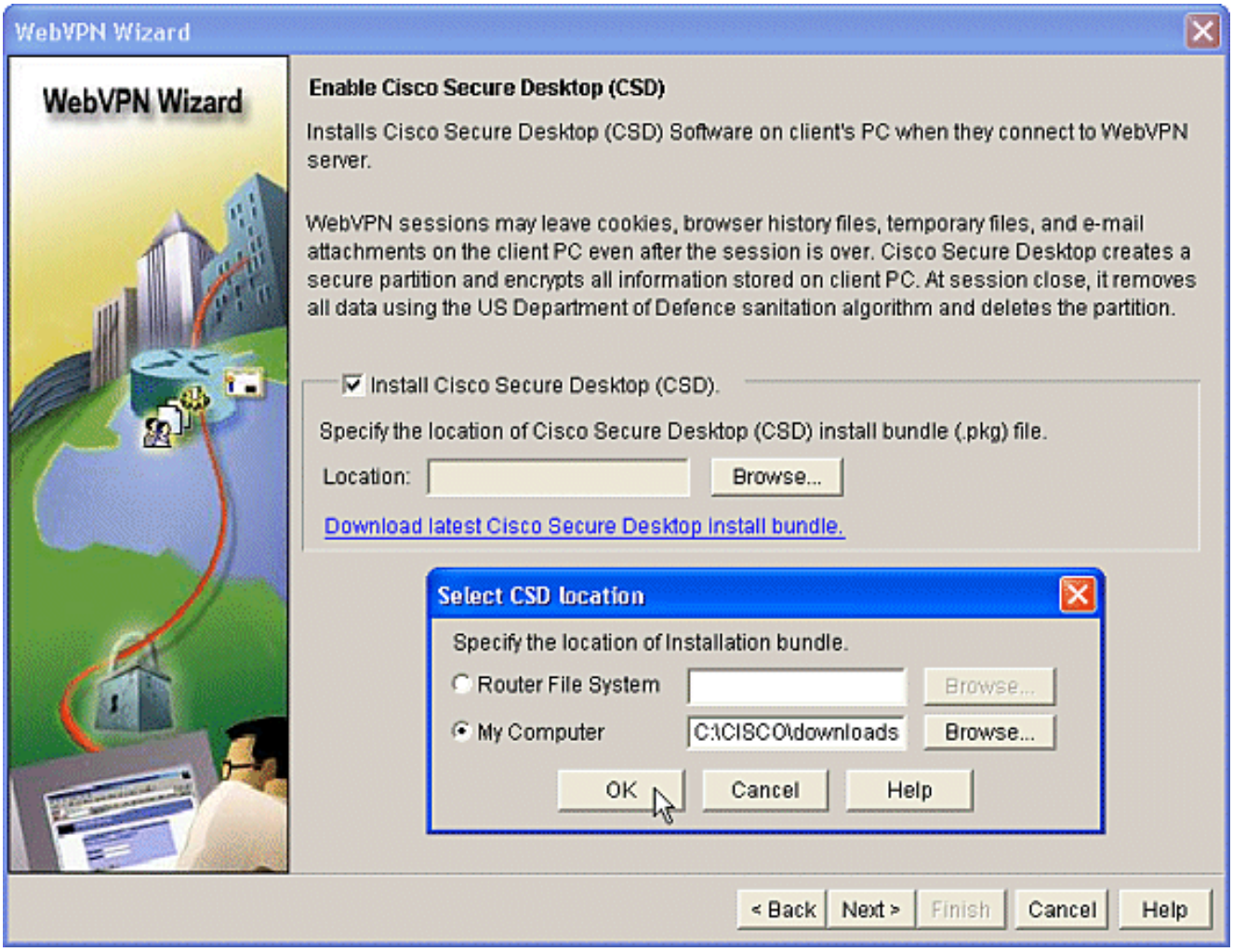


5. La pantalla Configure Intranet Websites (Configurar sitios web de intranet) permite configurar los recursos del sitio web que desea que estén disponibles para los usuarios. Puede agregar los sitios web internos de la empresa, como Outlook Web Access (OWA).



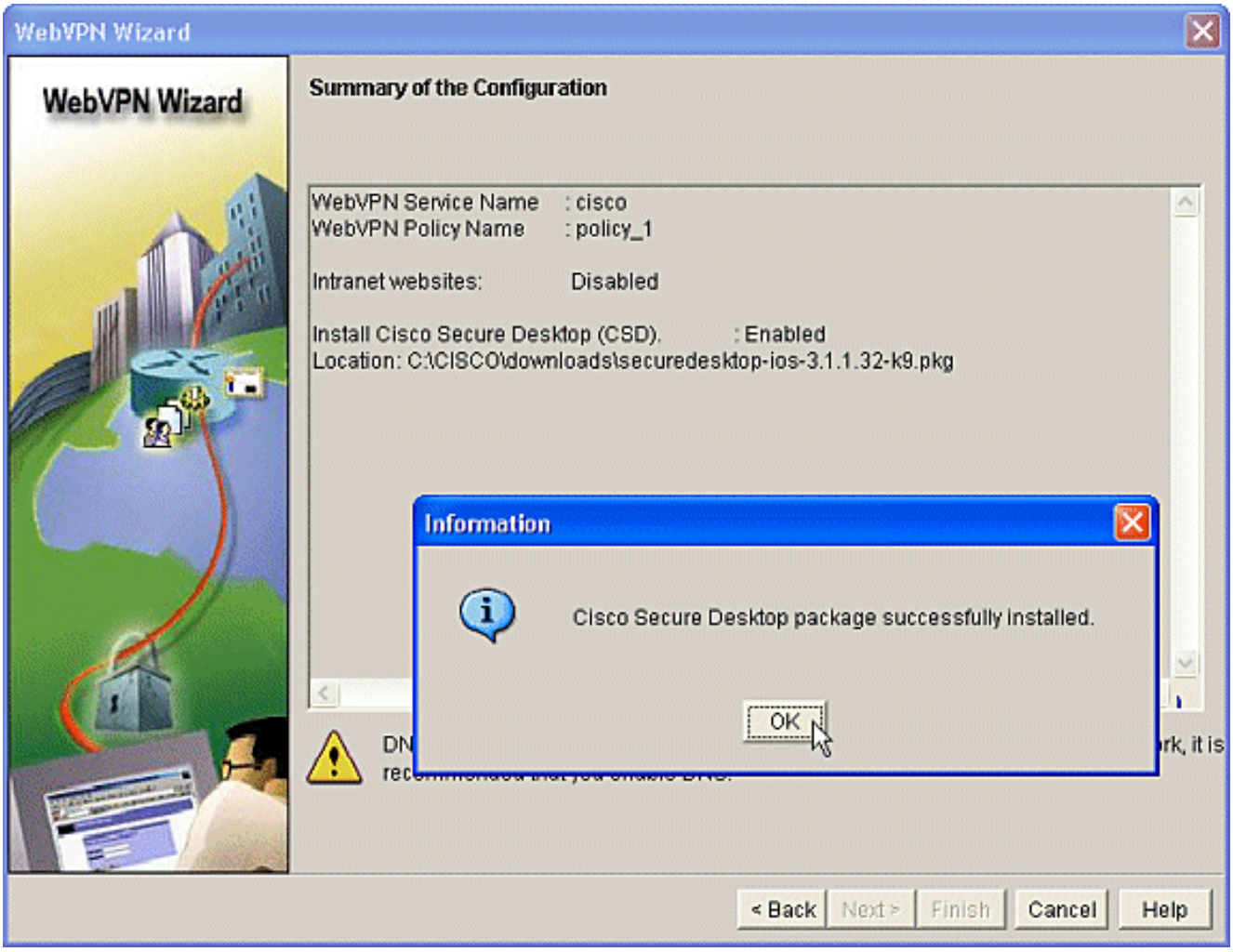
6. En la pantalla Enable Cisco Secure Desktop (CSD) (Habilitar Cisco Secure Desktop (CSD)), tiene la oportunidad de habilitar el CSD para este contexto. Marque la casilla junto a **Instalación de Cisco Secure Desktop (CSD)** y haga clic en **Examinar**.

7. En el área Seleccionar ubicación de CSD, marque **Mi PC**.Haga clic en el botón **Examinar**.Elija el archivo de paquete del IOS de CSD en su estación de trabajo de administración.Haga clic en el botón OK (Aceptar)Haga clic en el botón **Next**.



8. Se muestra un resumen de la pantalla Configuración. Haga clic en el botón **Finalizar**.

9. Haga clic en **Aceptar** cuando vea que el archivo del paquete CSD se ha instalado correctamente.



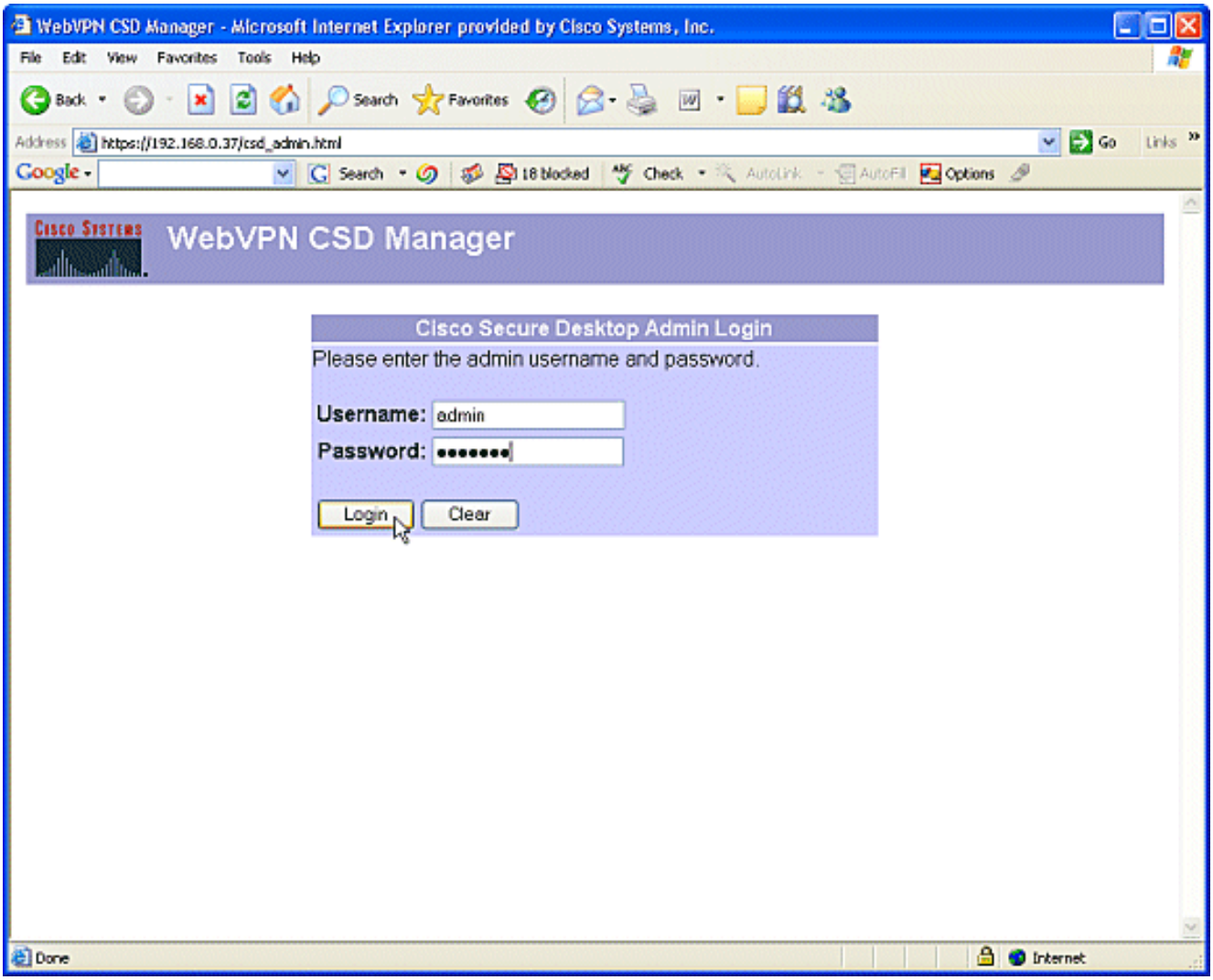
Fase II: Configure CSD mediante un navegador web.

Estos pasos se utilizan para completar la configuración de CSD en su navegador web.

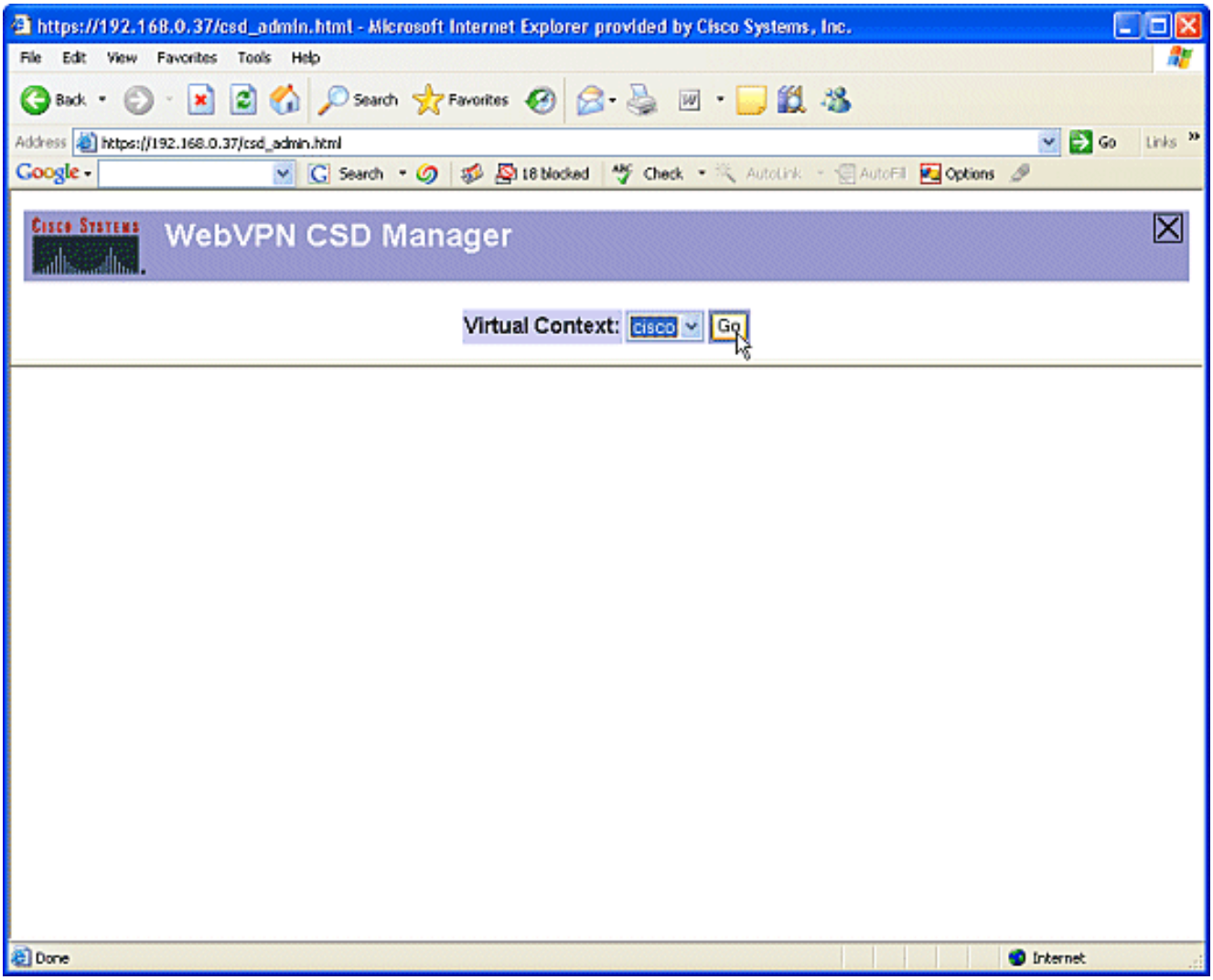
Fase II: Paso 1: Definir las ubicaciones de Windows.

Defina las ubicaciones de Windows.

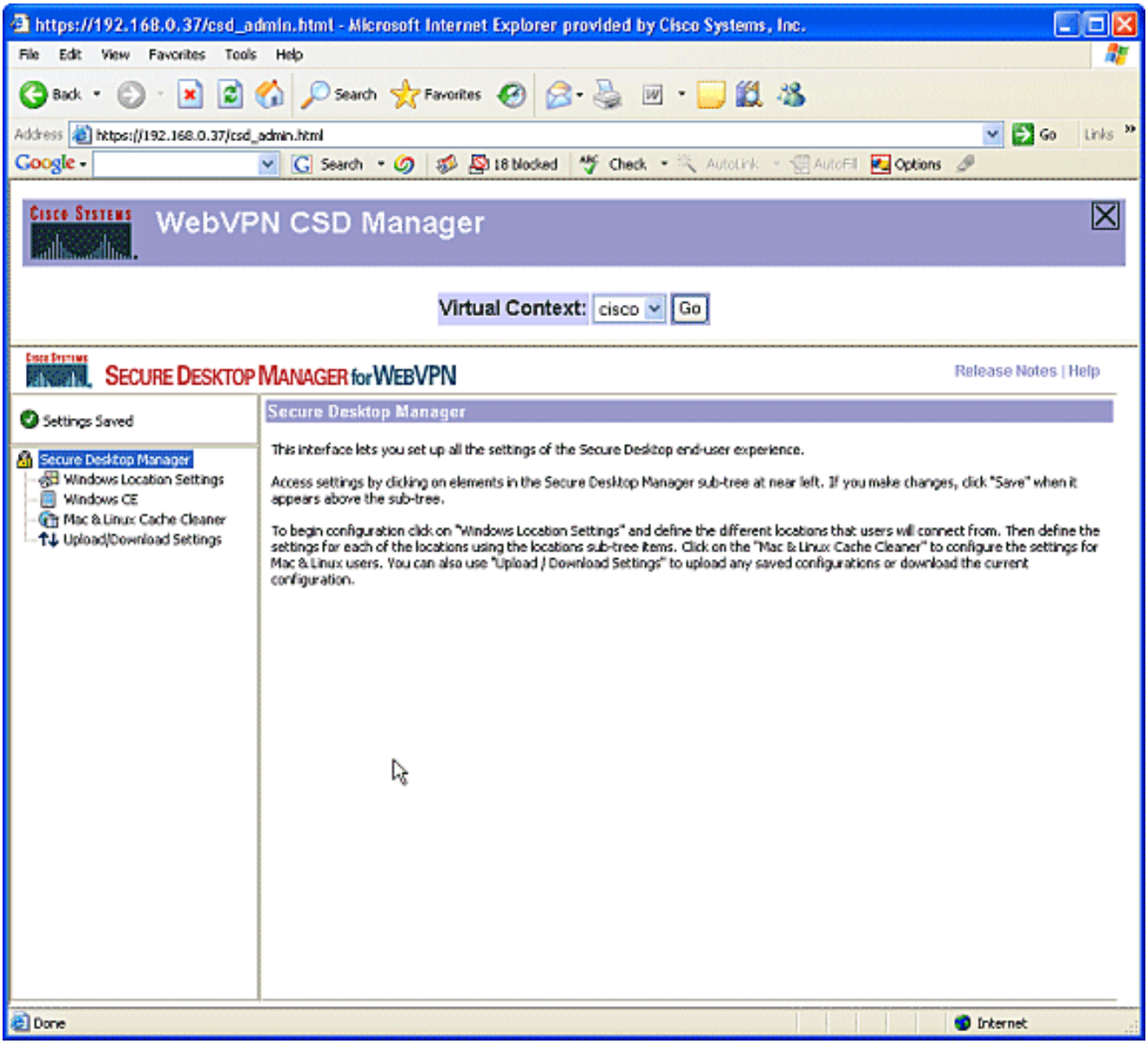
1. Abra su navegador web en **https://WebVPNgateway_IP Address/csd_admin.html**, por ejemplo, **https:/192.168.0.37/csd_admin.html**.
2. Introduzca el nombre de usuario **admin**.Introduzca la contraseña, que es el secreto de activación del router.Haga clic en Login
(Conexión).



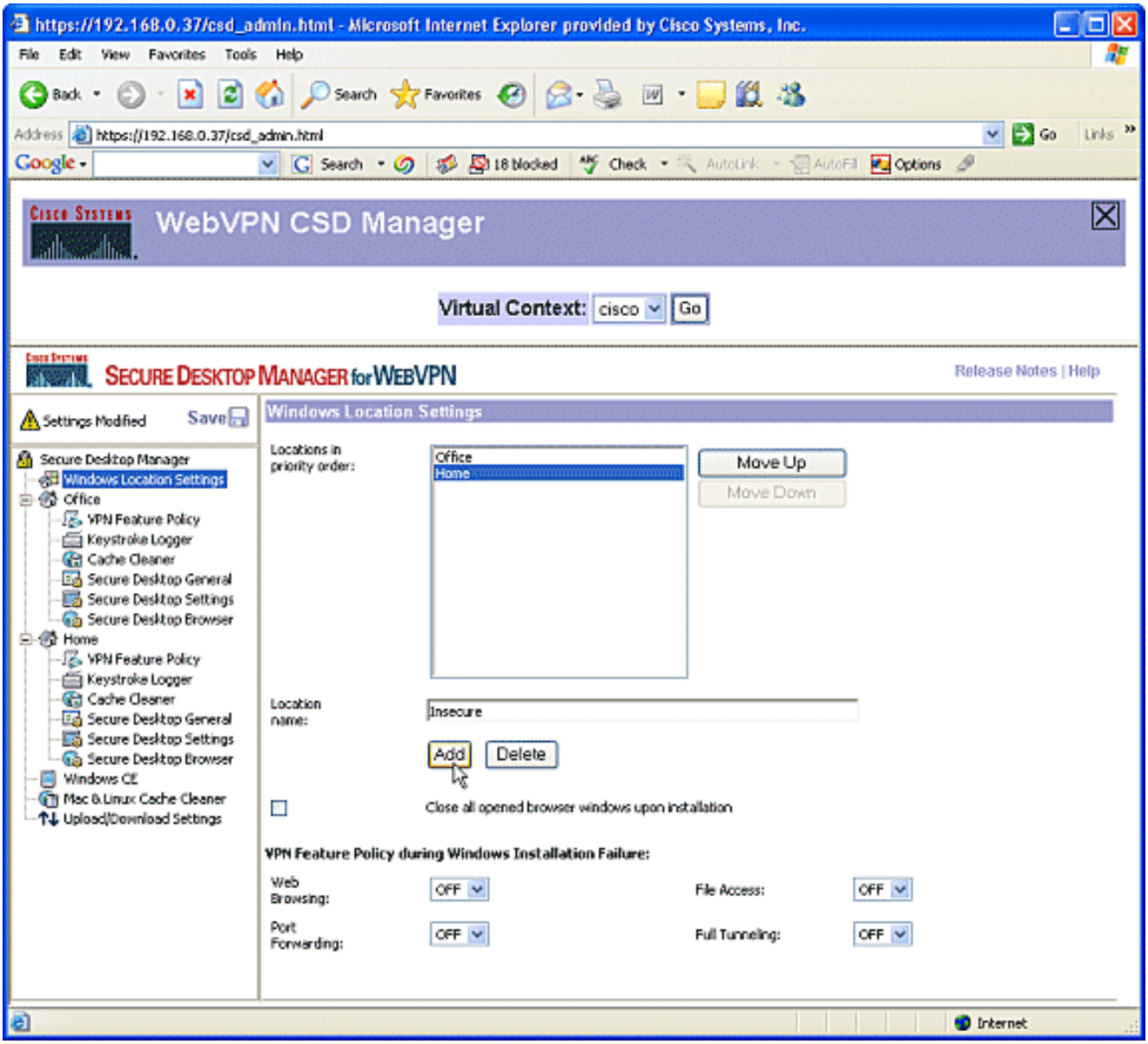
3. Acepte el certificado ofrecido por el router, elija el contexto en el cuadro desplegable y haga clic en
Ir.



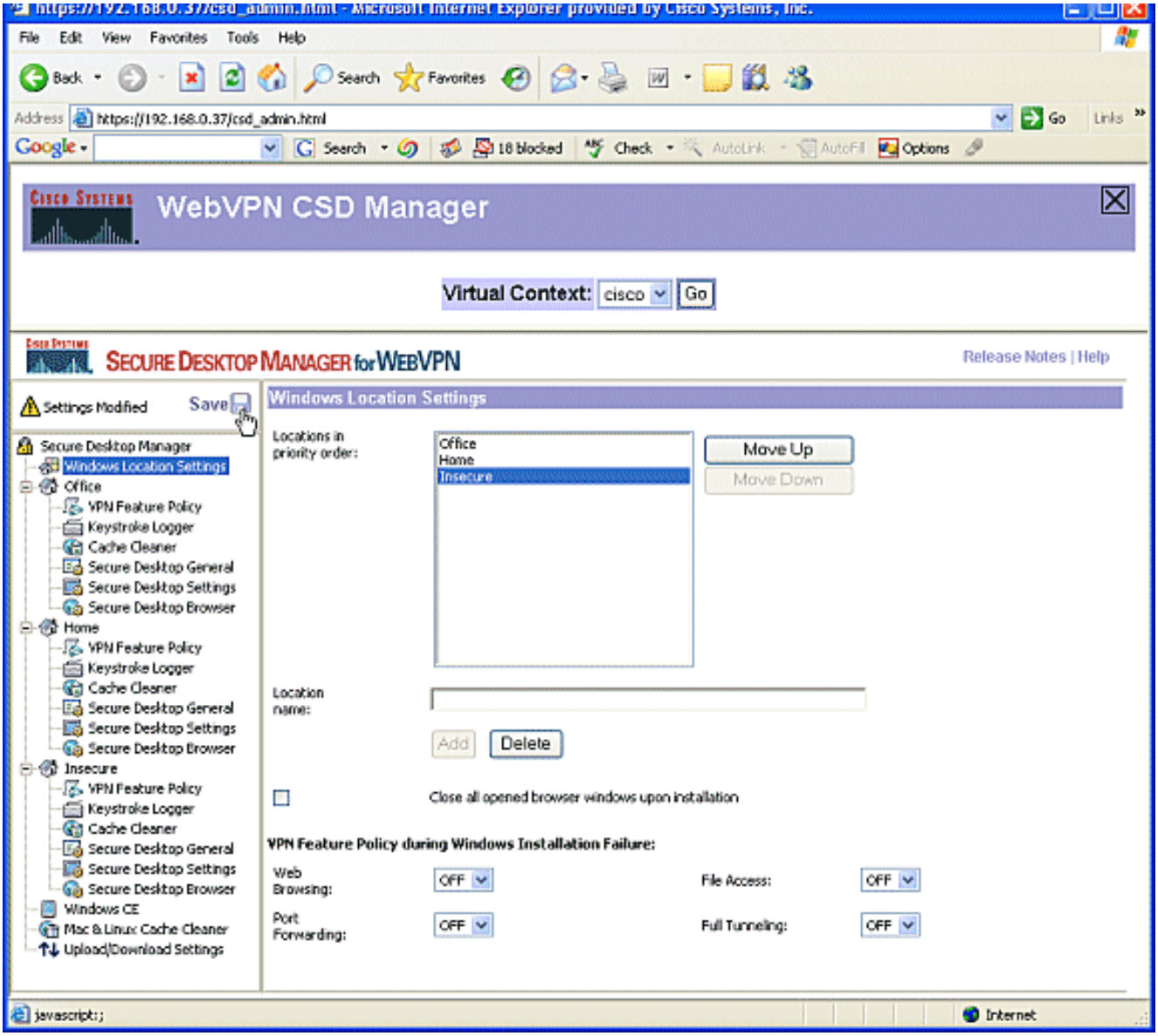
4. Se abrirá el Administrador de escritorio seguro para WebVPN.



5. En el panel izquierdo, elija **Configuración de ubicación de Windows**.Coloque el cursor en el cuadro situado junto al nombre de ubicación e introduzca un nombre de ubicación.Haga clic en Add (Agregar).En este ejemplo, se muestran tres nombres de ubicación: Office, Home e Insecure. Cada vez que se agrega una nueva ubicación, el panel izquierdo se expande con los parámetros configurables para esa
ubicación.



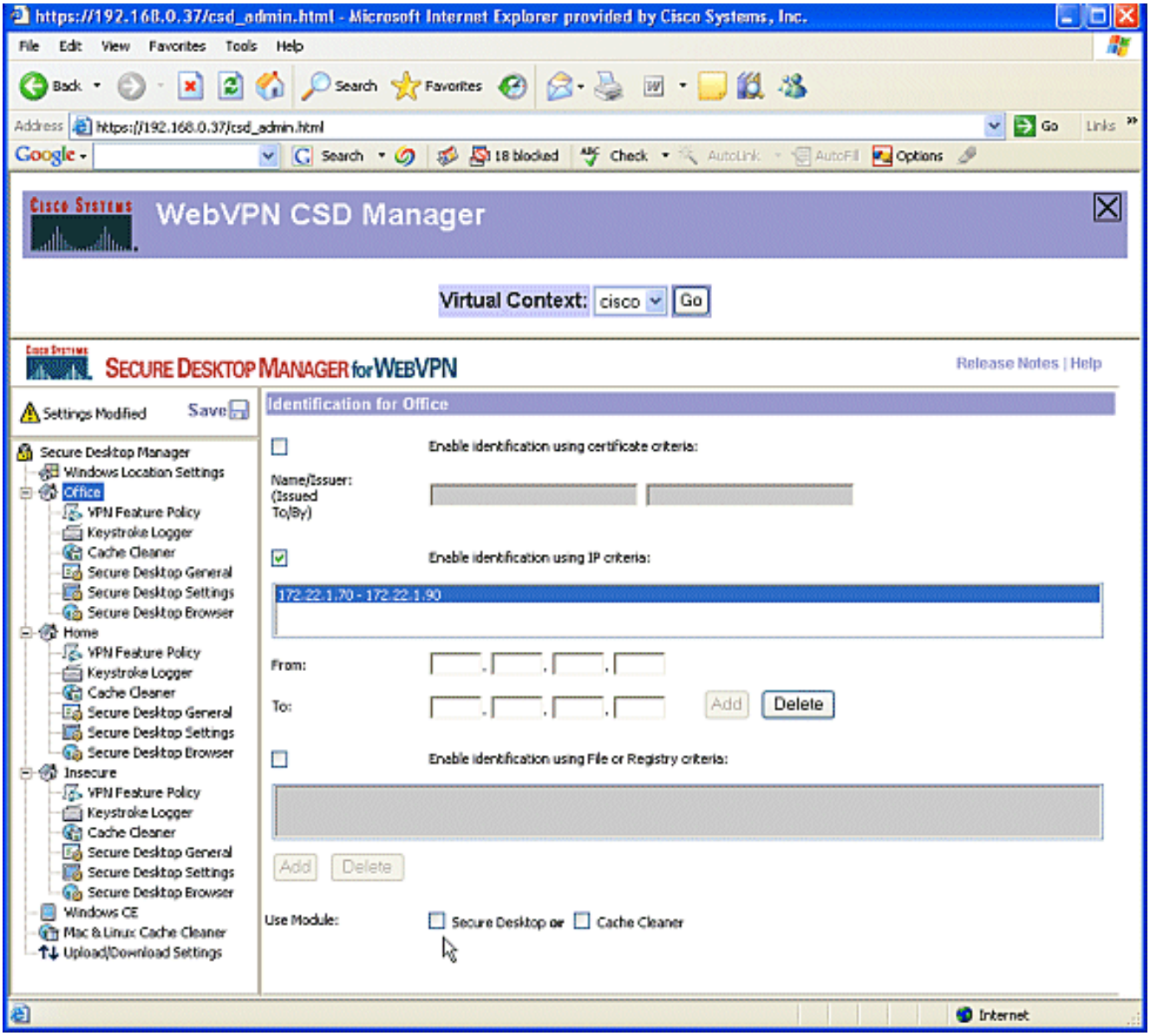
6. Después de crear las ubicaciones de Windows, haga clic en **Guardar** en la parte superior del panel izquierdo.**Nota:** Guarde sus configuraciones con frecuencia porque se perderán sus parámetros si se desconecta del navegador
web.



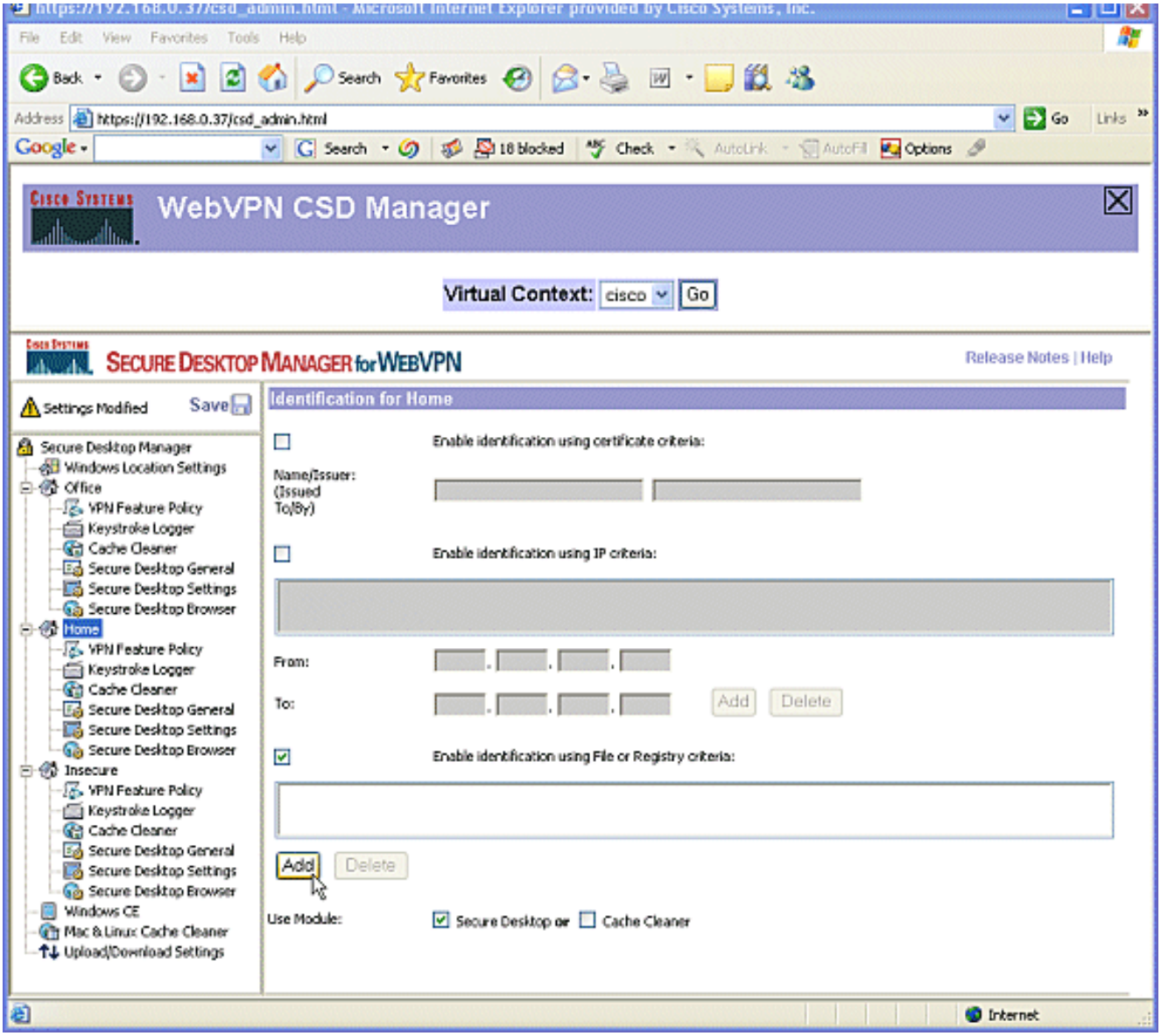
Fase II: Paso 2: Identificar los criterios de ubicación

Para distinguir las ubicaciones de Windows entre sí, asigne criterios específicos a cada ubicación. Esto permite a CSD determinar cuáles de sus funciones se aplicarán a una ubicación de Windows determinada.

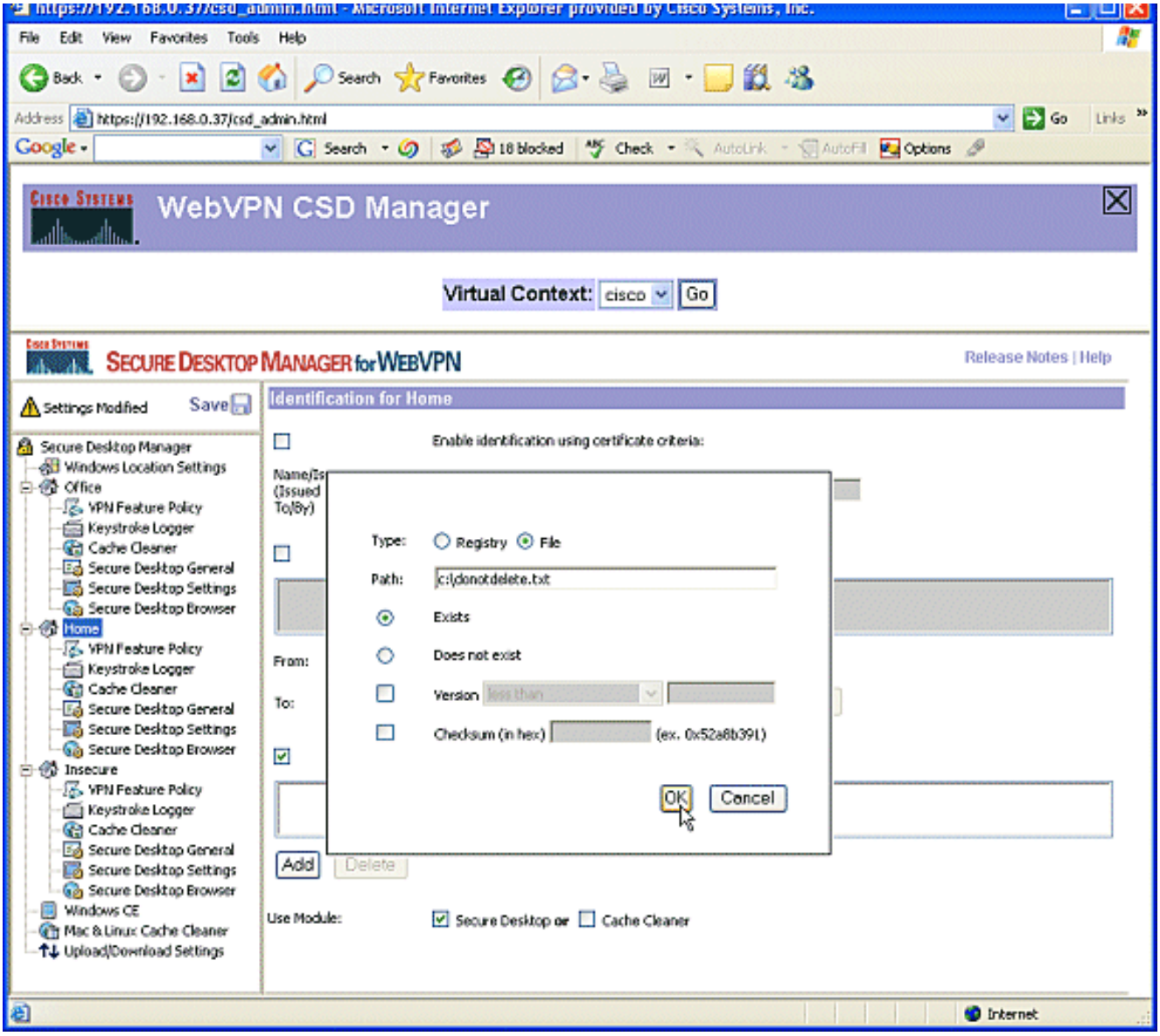
1. En el panel izquierdo, haga clic en **Office**.Puede identificar una ubicación de Windows con criterios de certificado, criterios IP, un archivo o criterios de registro. También puede elegir Secure Desktop o Cache Cleaner para estos clientes. Dado que estos usuarios son trabajadores internos de la oficina, identifíquelos con los criterios de IP.Ingrese los rangos de direcciones IP en los cuadros **De** y **A**.Haga clic en Add (Agregar). Desactive **Módulo de uso: Escritorio seguro**.Cuando se le solicite, haga clic en **Guardar** y haga clic en **Aceptar**.



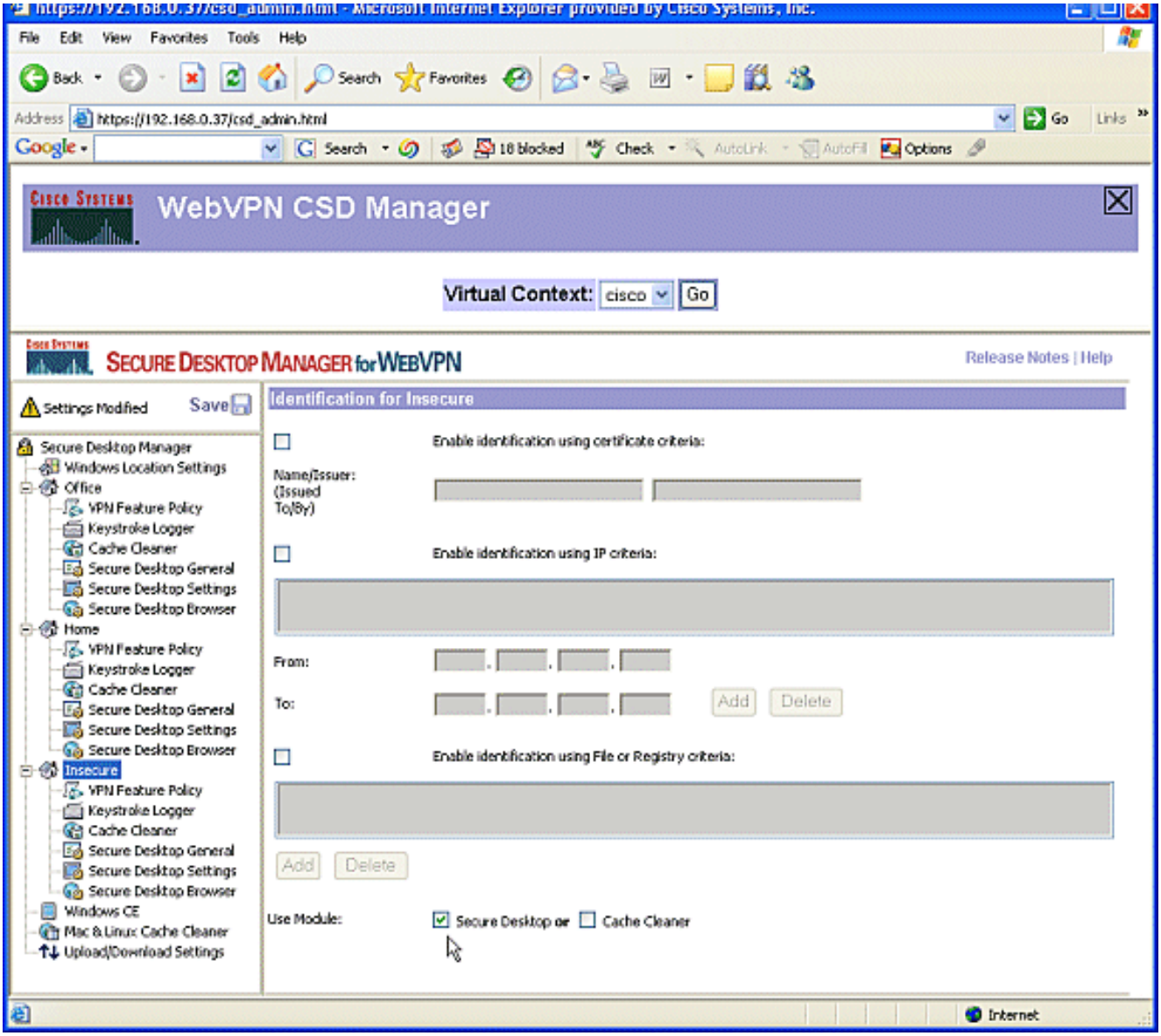
2. En el panel izquierdo, haga clic en el segundo **Inicio** de configuración de ubicación de Windows.Asegúrese de **Utilizar Módulo: Secure Desktop** está activado.Se distribuirá un archivo que identifica a estos clientes. Puede optar por distribuir certificados o criterios de registro para estos usuarios.Marque **Habilitar identificación usando criterios de archivo o registro**.Haga clic en Add
(Agregar).



3. En el cuadro de diálogo, elija **Archivo** e introduzca la ruta de acceso al archivo.Este archivo debe ser distribuido a todos sus clientes de casa.Compruebe que el botón de opción **Existe**.Cuando se le solicite, haga clic en **Aceptar** y haga clic en **Guardar**.



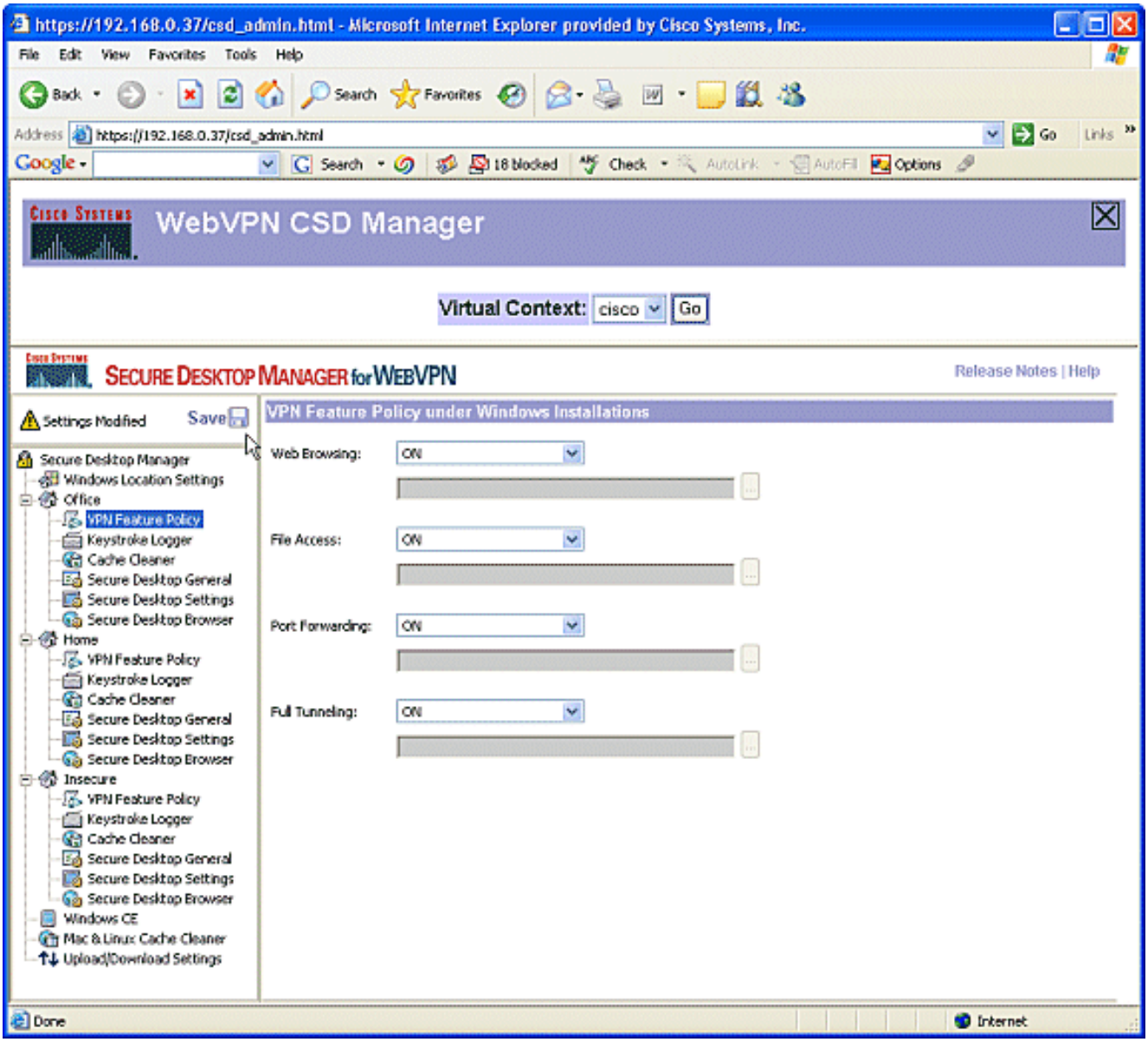
4. Para configurar la identificación de ubicaciones **inseguras**, simplemente no aplique ningún criterio de identificación.Haga clic en **Insecure** en el panel izquierdo.Deje todos los criterios sin marcar.Comprobar **módulo de uso: Escritorio seguro**.Cuando se le solicite, haga clic en **Guardar** y haga clic en
Aceptar.



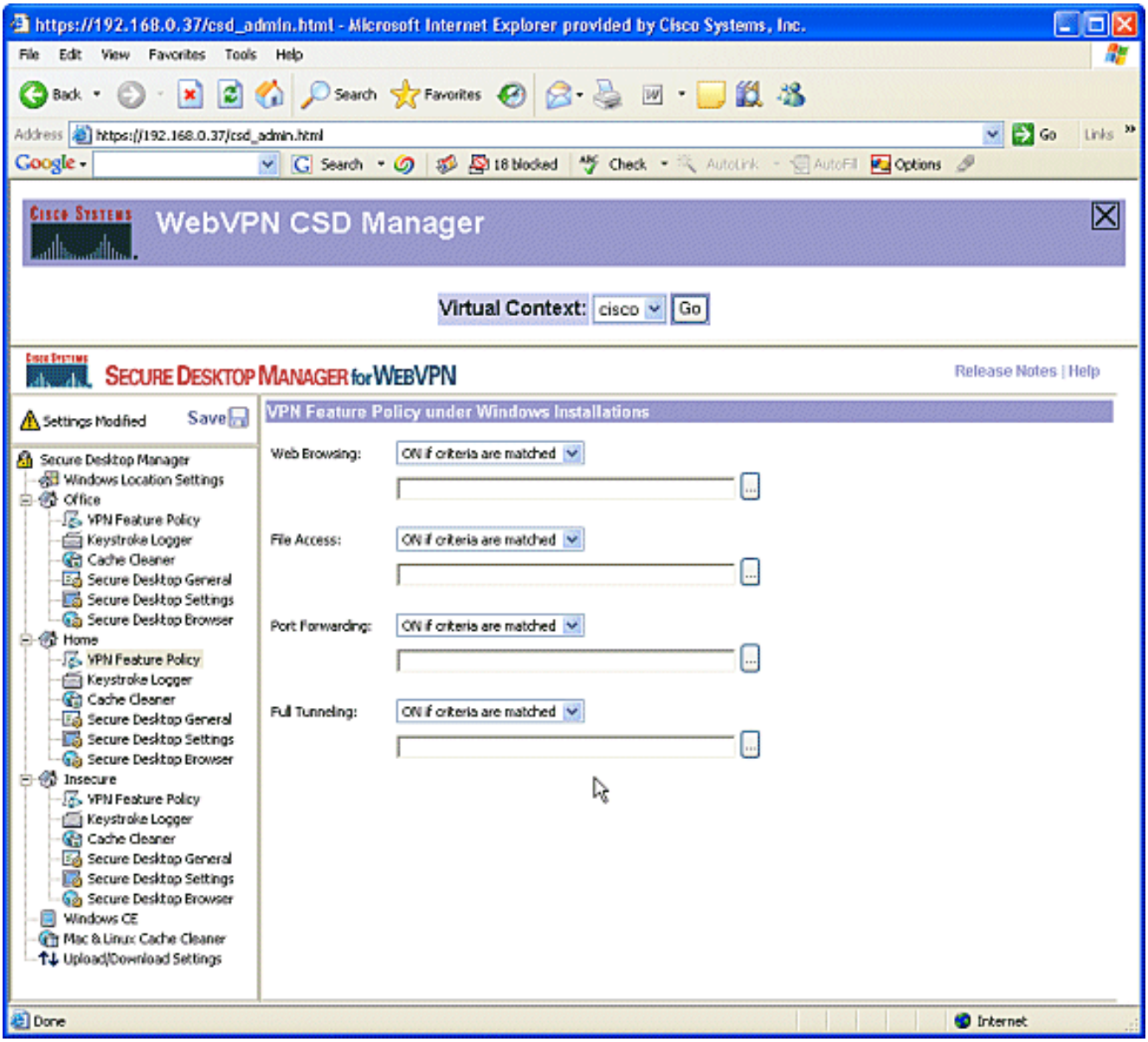
Fase II: Paso 3: Configure las funciones y los módulos de ubicación de Windows.

Configure las funciones de CSD para cada ubicación de Windows.

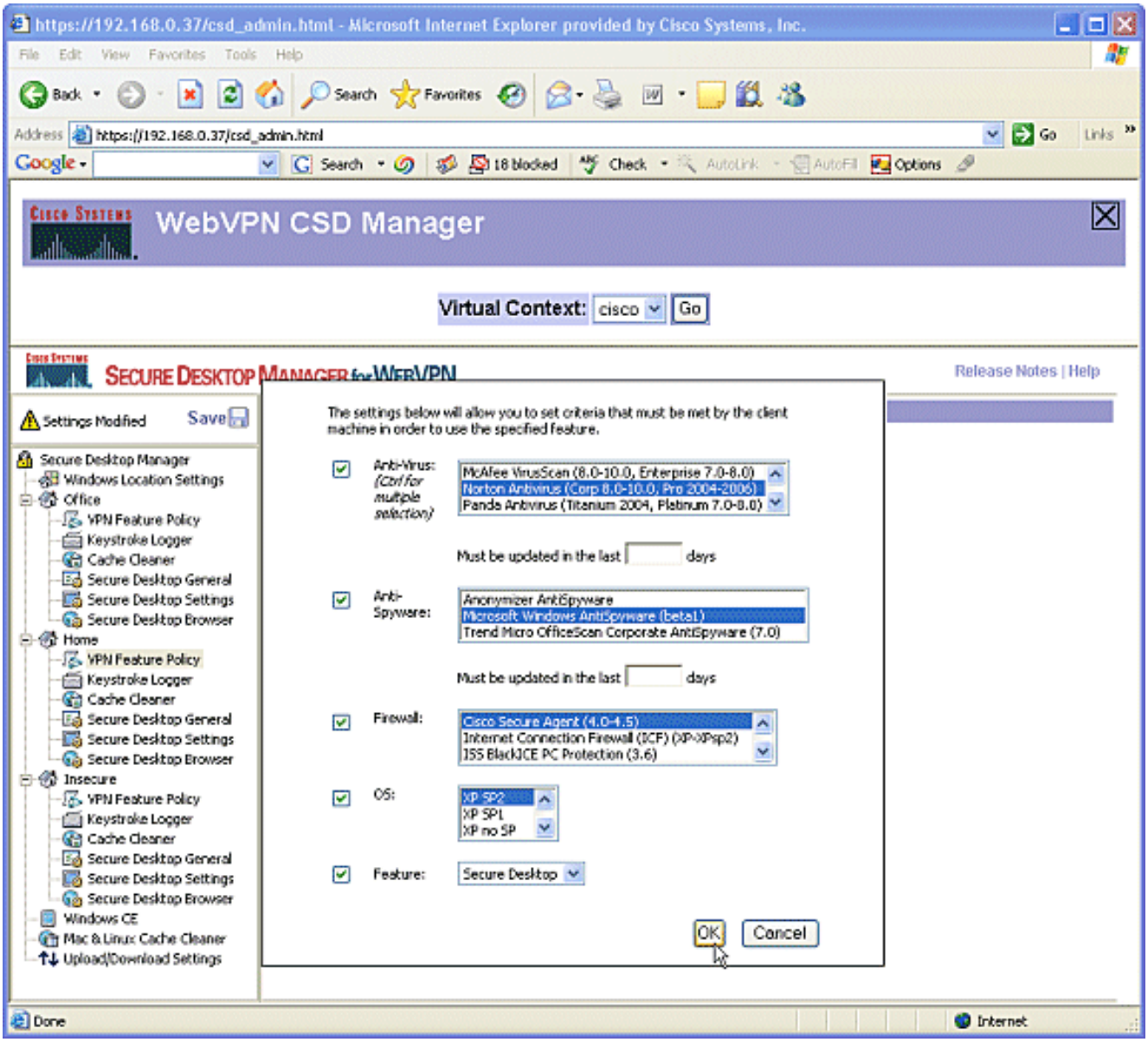
1. En **Office**, haga clic en **Política de funciones de VPN**. Dado que se trata de clientes internos de confianza, no se habilitó CSD ni Cache Cleaner. Ninguno de los otros parámetros está disponible.



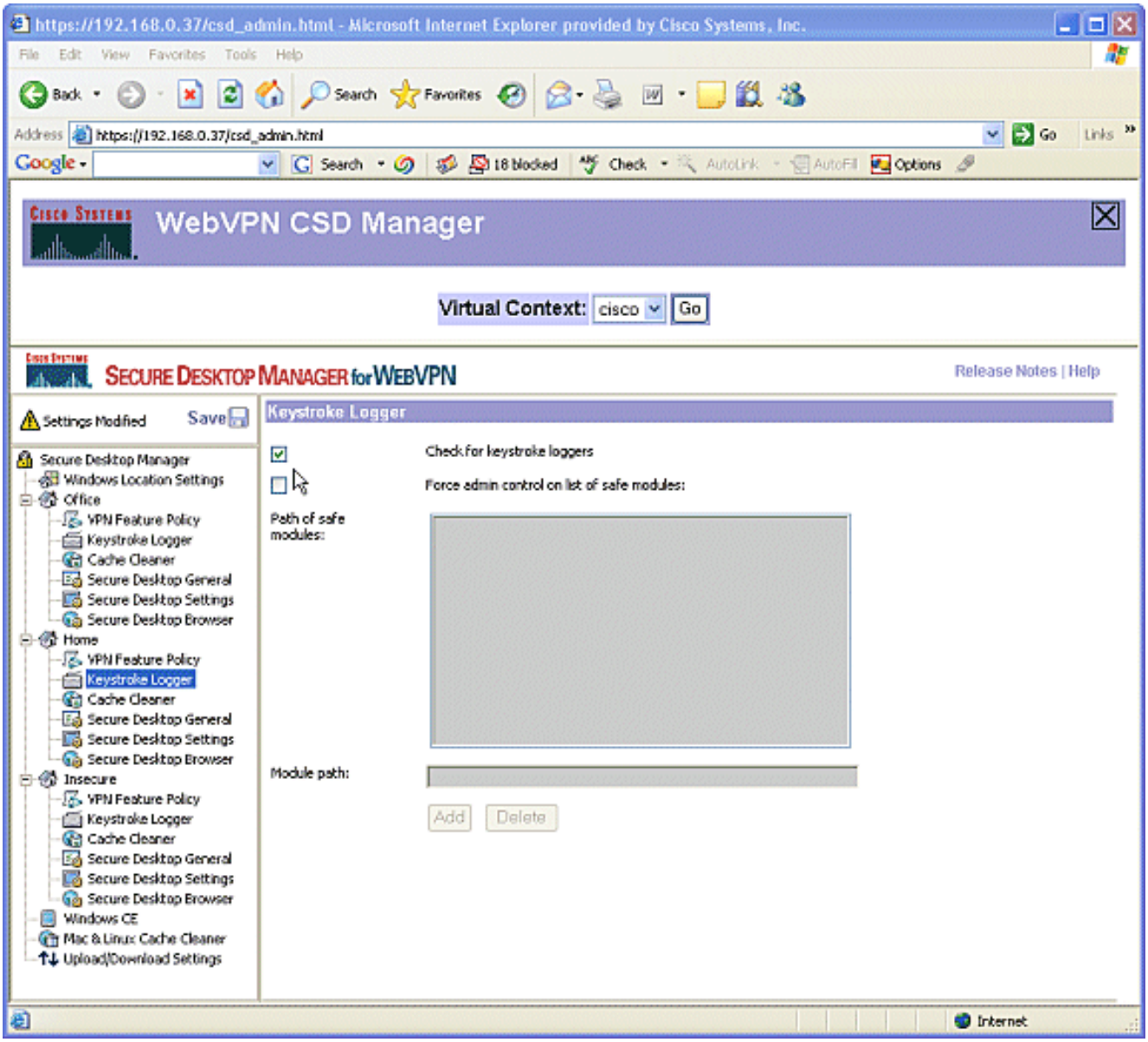
2. Active las funciones como se muestra.En el panel izquierdo, elija **Política de Funciones VPN** en **Inicio**.Los usuarios domésticos tendrán acceso a la LAN corporativa si los clientes cumplen ciertos criterios.En cada método de acceso, elija **ON si los criterios coinciden**.



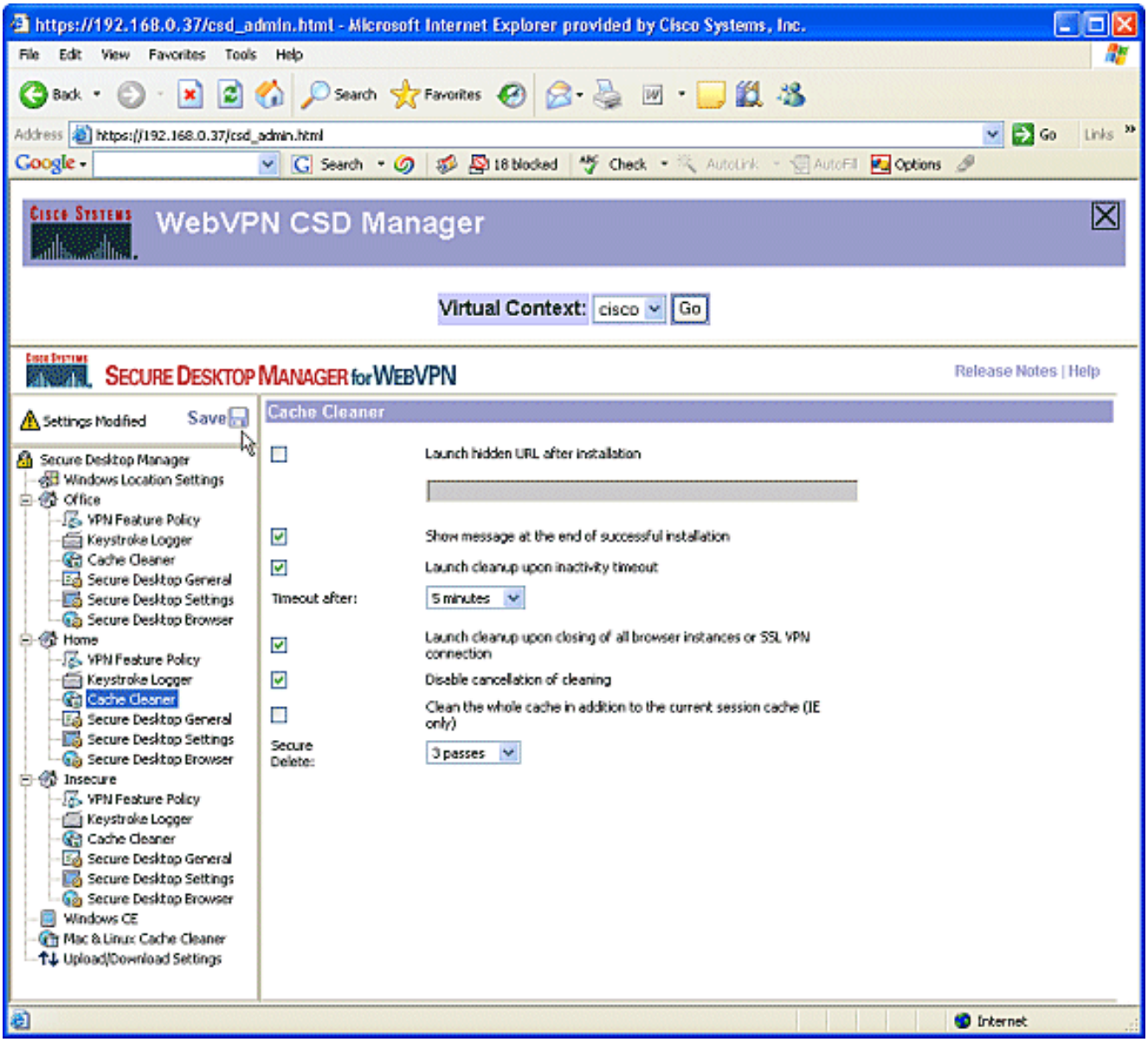
3. Para la exploración web, haga clic en el botón de puntos suspensivos y elija los criterios que deben coincidir. Haga clic en **Aceptar** en el cuadro de diálogo.



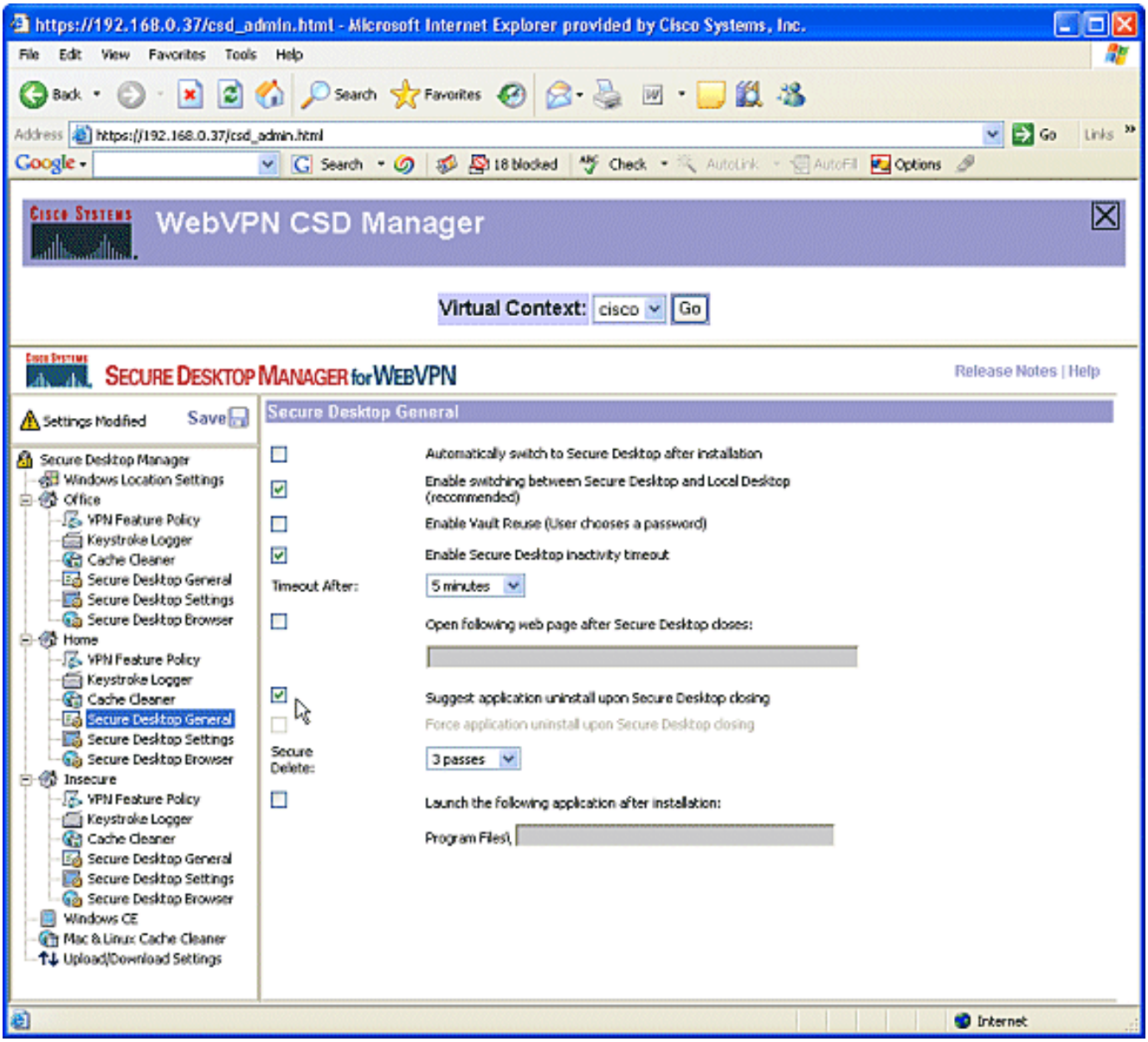
4. Puede configurar los otros métodos de acceso de forma similar.En **Inicio**, elija **Registrador de pulsaciones de tecla**.Coloque una marca de verificación junto a **Buscar registradores de pulsaciones de tecla**.Cuando se le solicite, haga clic en **Guardar** y haga clic en **Aceptar**.



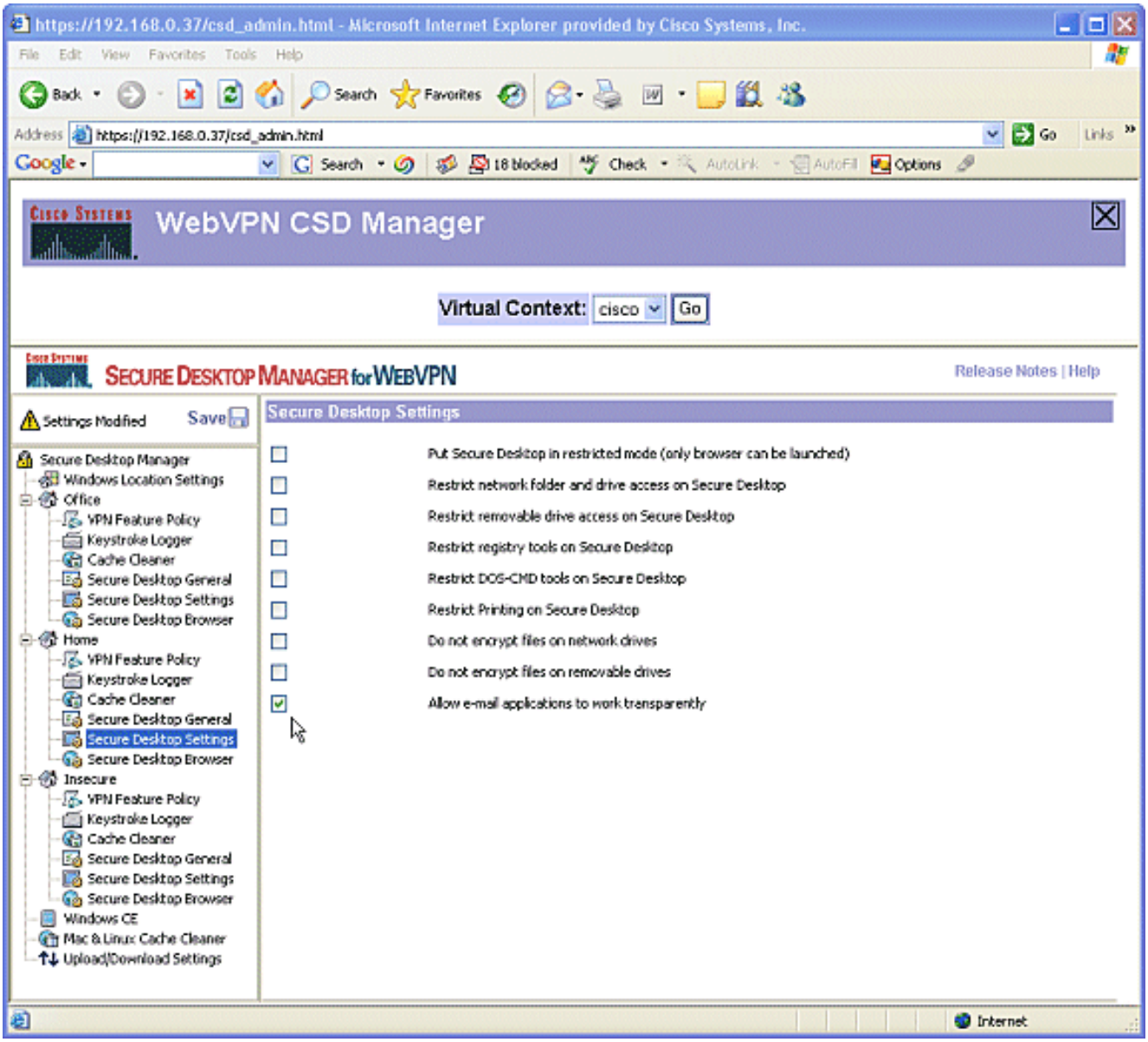
5. En la ubicación de las ventanas de inicio, elija **Limpiador de caché**. Deje los parámetros predeterminados como se muestra en la captura de pantalla.



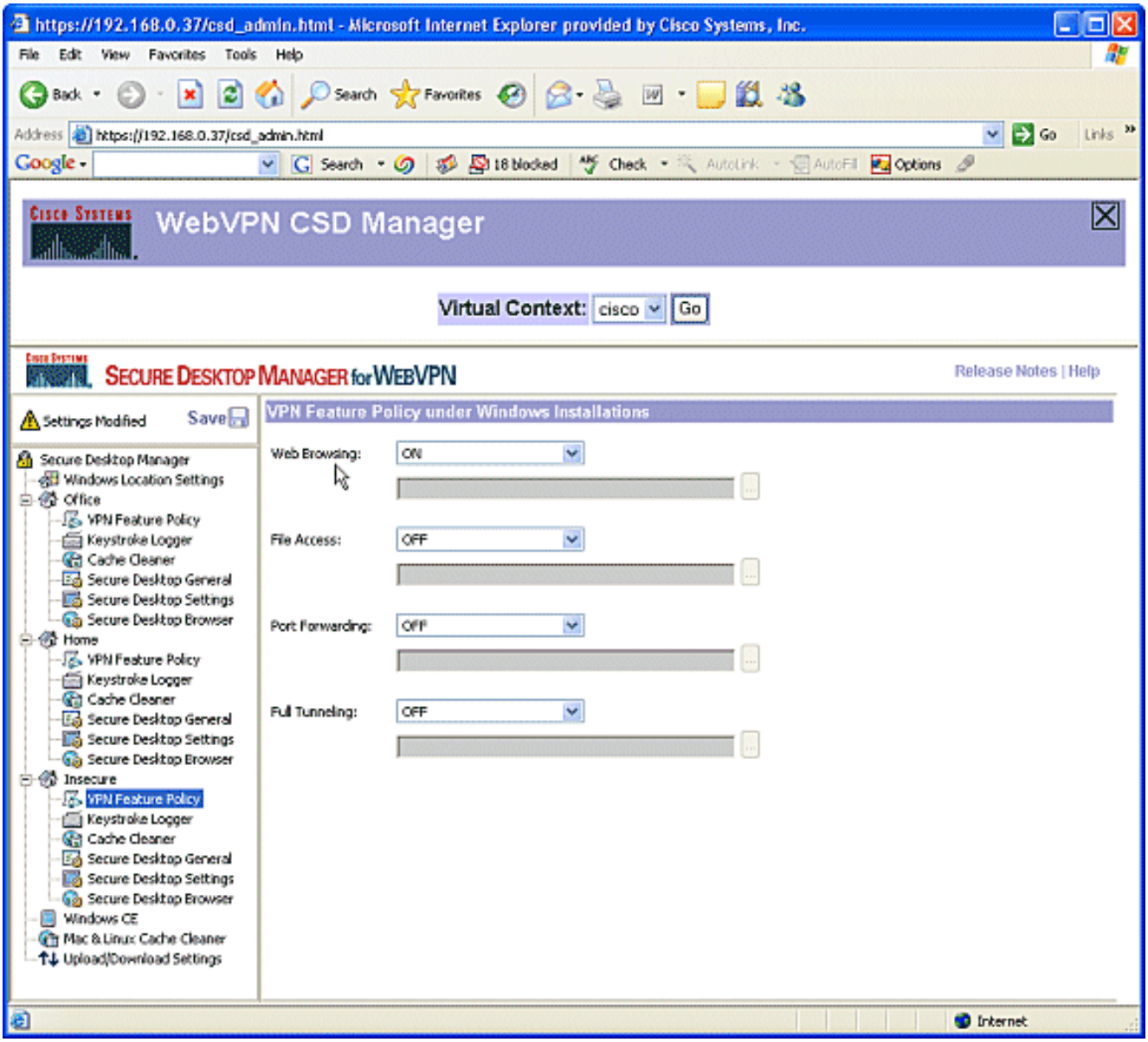
6. En Inicio, elija **Secure Desktop General**. Marque **Sugiera la desinstalación de la aplicación al cerrar Secure Desktop**. Deje el resto de parámetros en su configuración predeterminada, como se muestra en la captura de pantalla.



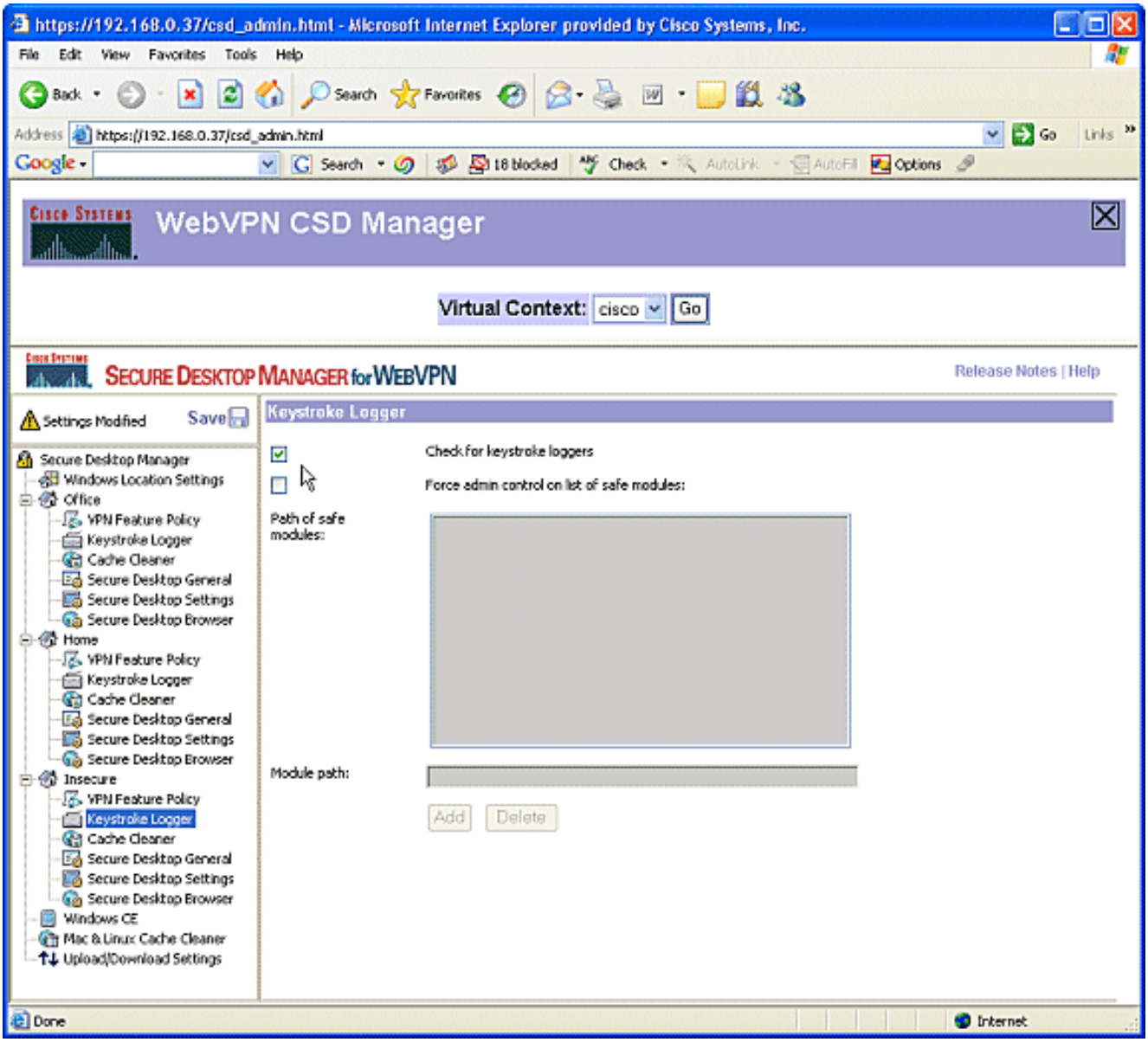
7. Para Secure Desktop Settings en Home, elija **Allow e-mail Applications to work transparent**. Cuando se le solicite, haga clic en **Guardar** y haga clic en **Aceptar**.



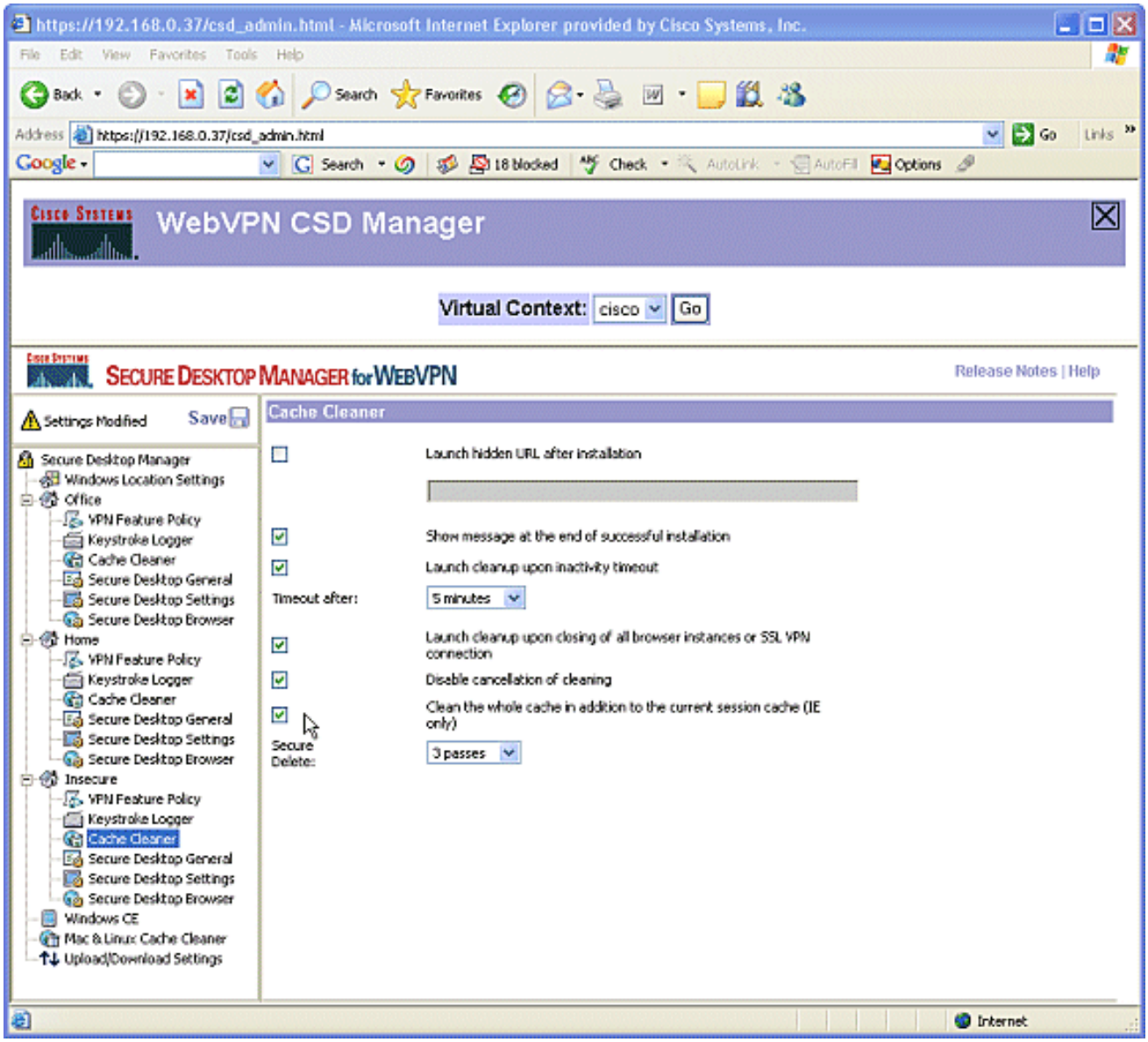
8. La configuración de **Secure Desktop Browser** depende de si desea o no que estos usuarios accedan a un sitio web de la empresa con favoritos preconfigurados.En Insecure , elija **VPN Feature Policy**.Dado que no son usuarios de confianza, permita sólo la navegación web.Elija **ON** en el menú desplegable para **Navegación Web**.El resto del acceso está configurado en **OFF**.



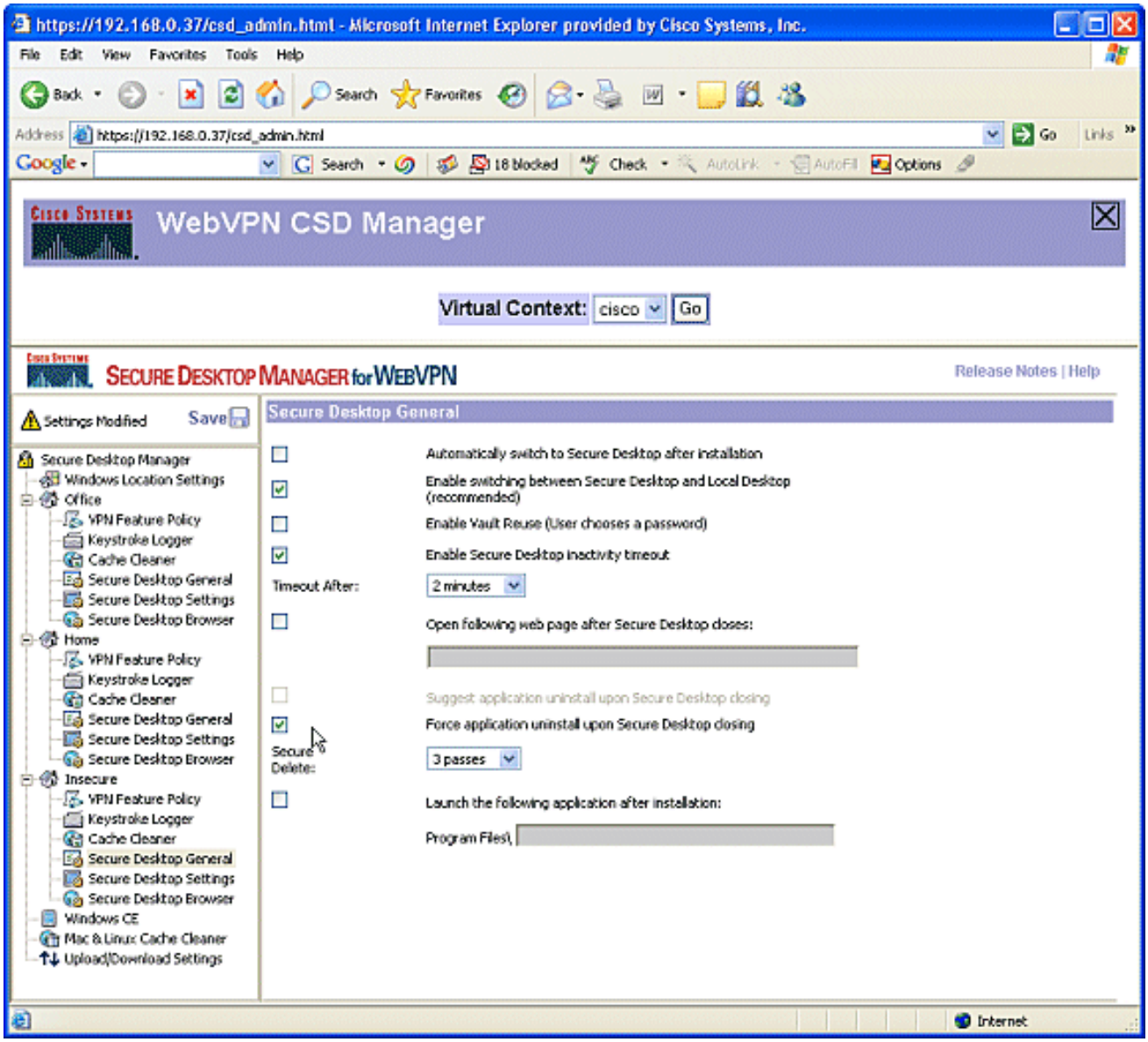
9. Marque la casilla de verificación **Comprobar si hay registradores de pulsaciones de teclas**.



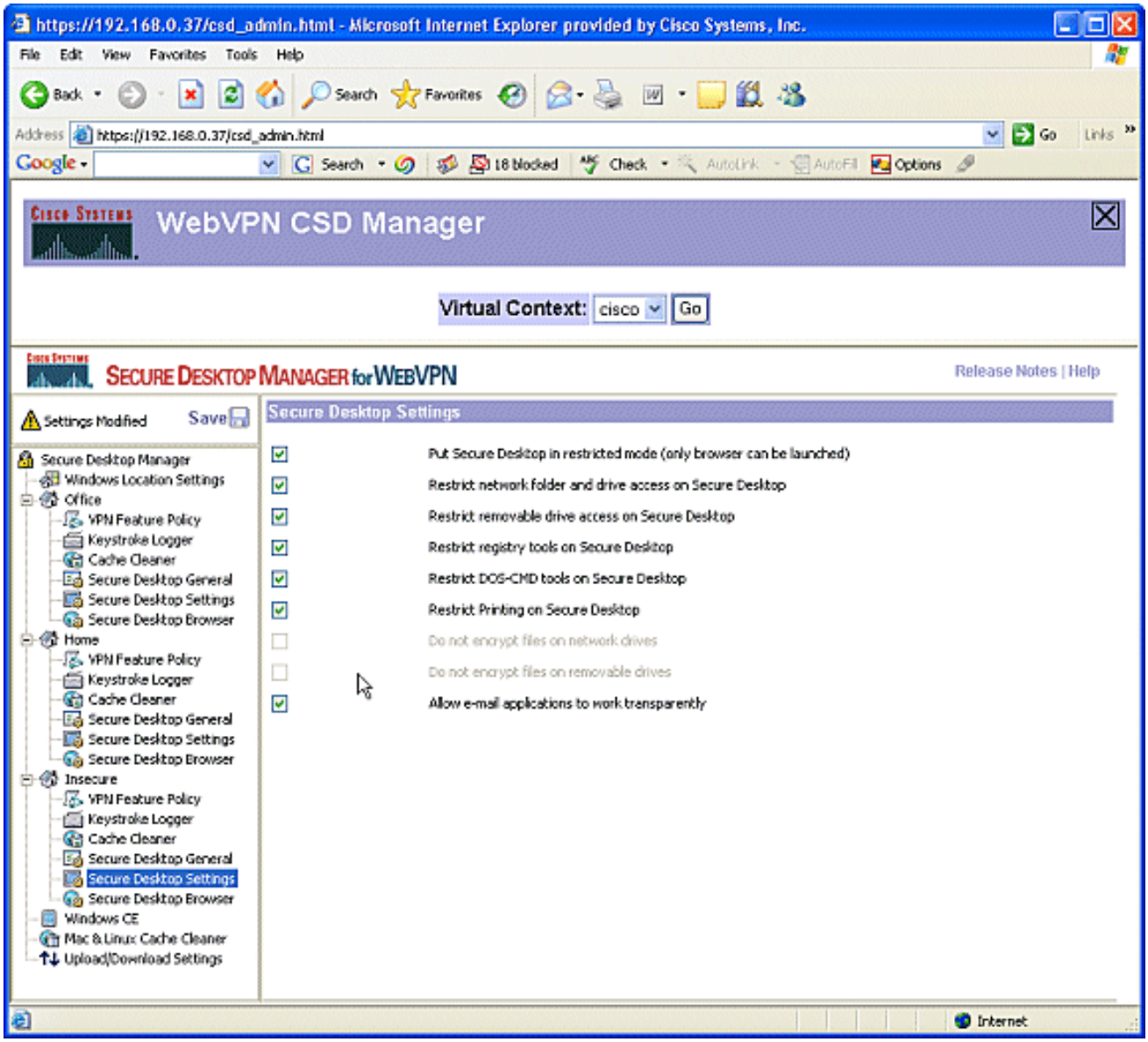
10. Configure el Limpiador de Caché para Inseguro.Marque la **casilla de verificación Limpiar toda la memoria caché además de la memoria caché de sesión actual (sólo IE)**.Deje el resto de configuraciones en sus valores predeterminados.



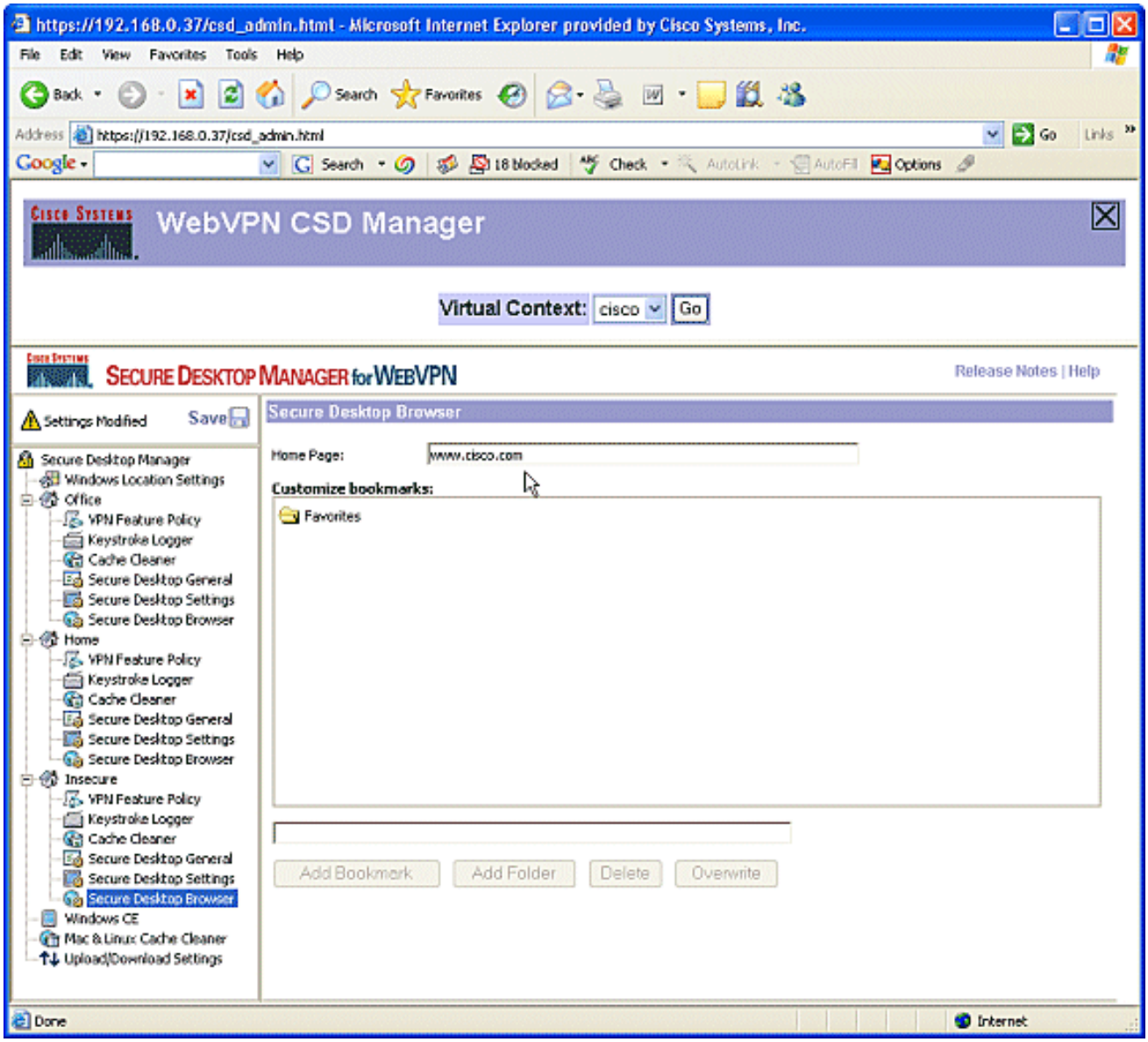
11. En Insecure , elija **Secure Desktop General**.Reduzca el tiempo de inactividad a 2 minutos.Active la casilla de verificación **Forzar la desinstalación de la aplicación al cerrar Secure Desktop**.



12. Elija **Secure Desktop Settings** en Insecure, y configure configuraciones muy restrictivas como se
muestra.



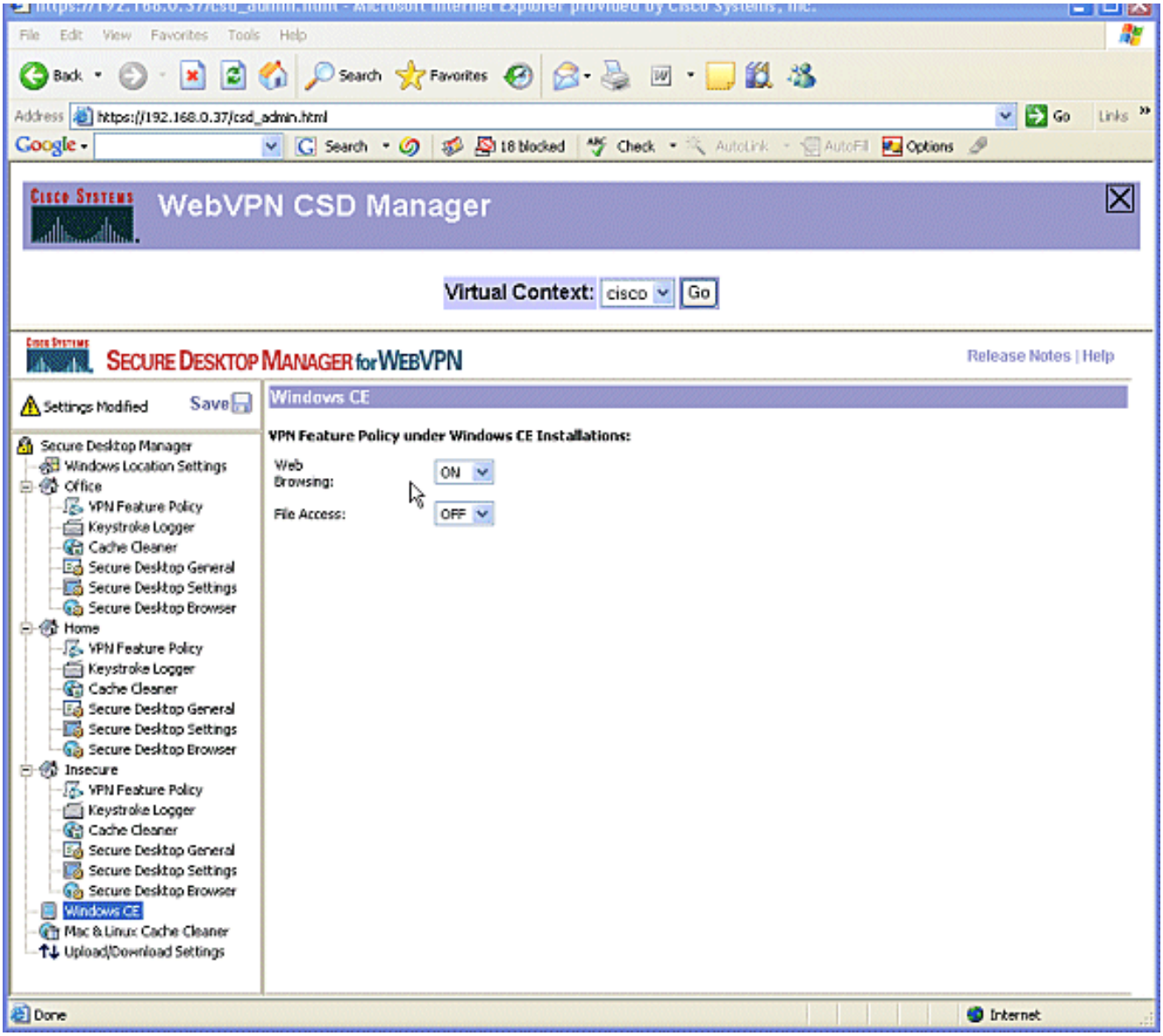
13. Elija **Secure Desktop Browser**. En el campo Página de inicio, introduzca el sitio web al que se guiarán estos clientes para su página de inicio.



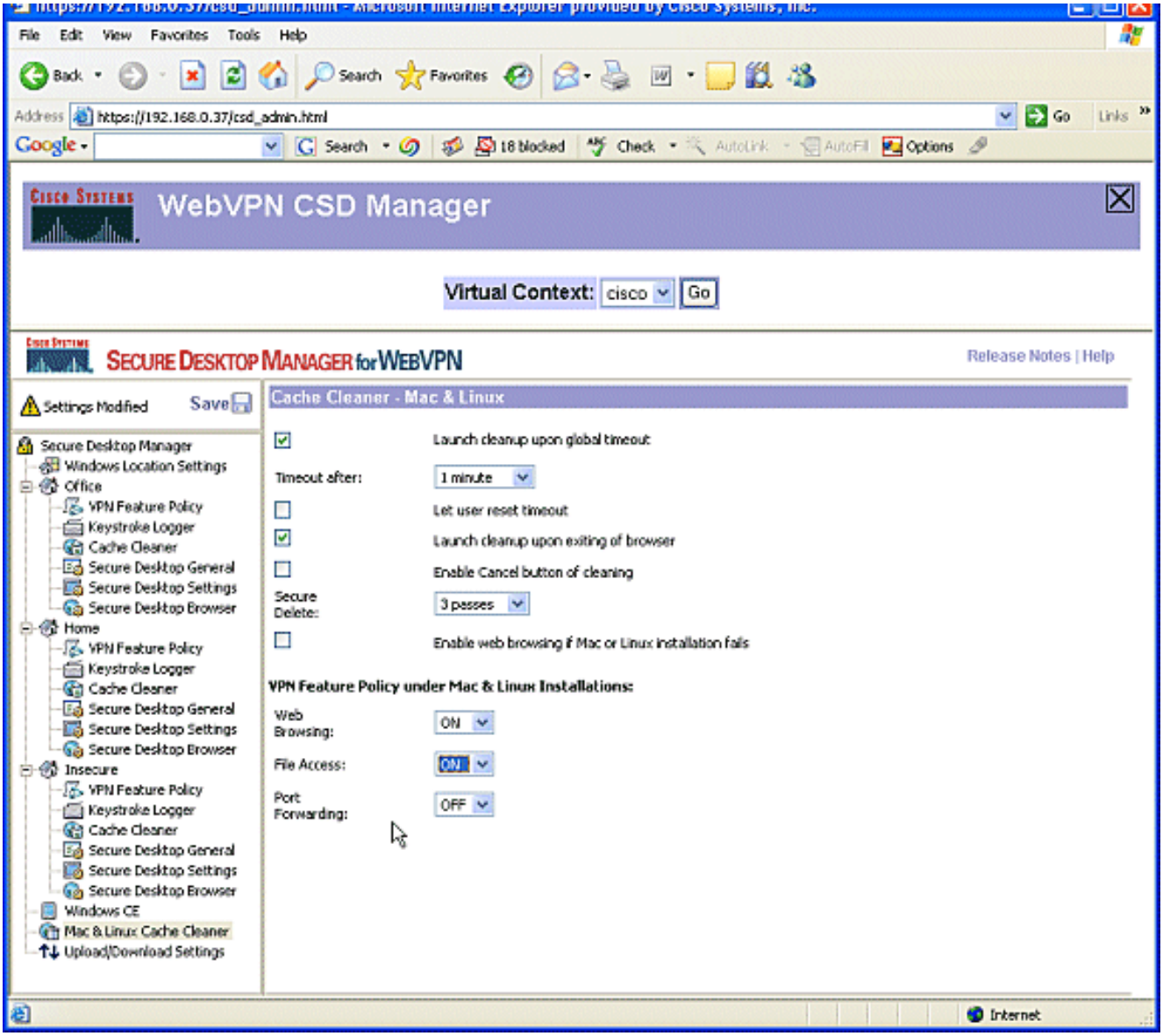
Fase II: Paso 4: Configure las funciones de Windows CE, Macintosh y Linux.

Configure las funciones CSD para Windows CE, Macintosh y Linux.

1. Elija **Windows CE** en Secure Desktop Manager. Windows CE tiene funciones de VPN limitadas. Active **Exploración Web**.



2. Elija **Limpiador de caché Mac y Linux**.Los Sistemas Operativos Macintosh y Linux tienen acceso sólo a los aspectos de limpieza de caché de CSD. Configure las opciones como se muestra en el gráfico.Cuando se le solicite, haga clic en **Guardar** y haga clic en **Aceptar**.

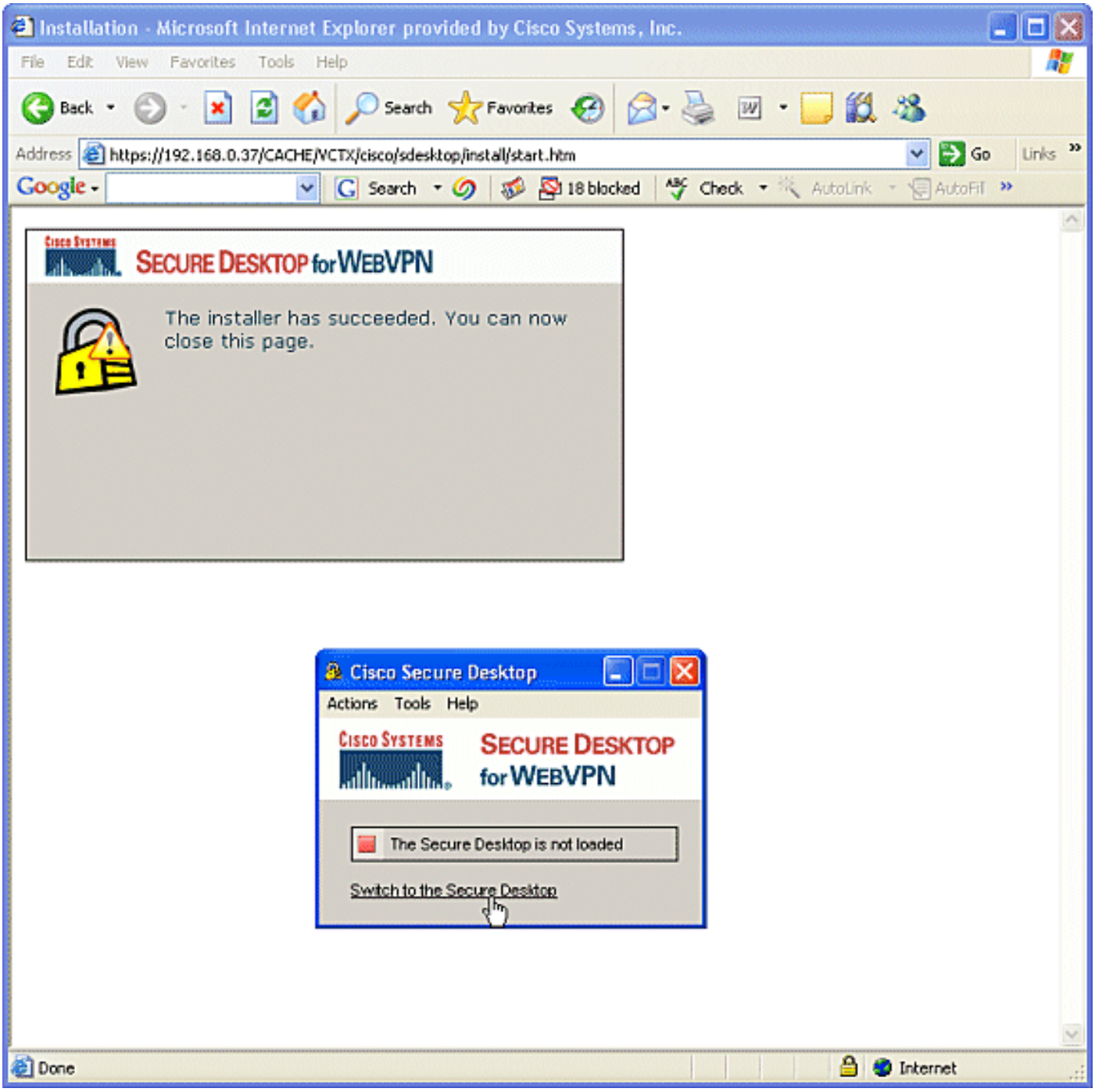


Verificación

Prueba de la Operación CSD

Pruebe el funcionamiento del CSD conectándose al gateway WebVPN con un navegador habilitado para SSL en **https://WebVPN_Gateway_IP Address**.

Nota: Recuerde utilizar el nombre único del contexto si creó diferentes contextos WebVPN, por ejemplo, **https://192.168.0.37/cisco**.



Comandos

Varios **comandos show se asocian a WebVPN.** Puede ejecutar estos comandos en command-line interface (CLI) para mostrar las estadísticas y otra información. Para obtener información detallada sobre los **comandos show, consulte** Verificar la Configuración WebVPN.

Nota: El Analizador CLI (sólo clientes registrados) admite determinados **comandos show**. Utilice el Analizador CLI para ver un análisis del resultado del comando **show**.

Troubleshoot

Comandos

Varios **comandos debug se asocian a WebVPN.** Para obtener información detallada sobre estos

comandos, consulte Uso de los Comandos Debug de WebVPN.

Nota: El uso de los comandos **debug** puede afectar negativamente a su dispositivo Cisco. Antes de que utilice los **comandos debug, consulte** Información Importante sobre los Comandos Debug.

Para obtener más información sobre los comandos **clear**, consulte Uso de los comandos WebVPN Clear.

Información Relacionada

- Guía de Implementación y Convergencia de WebVPN y DMVPN
- SSL VPN - WebVPN
- Cisco IOS SSLVPN
- Soporte Técnico y Documentación - Cisco Systems