# Cisco Secure Desktop (CSD) on IOS Configuration Example using SDM

## Contents



## Introduction

Although Secure Sockets Layer (SSL) VPN (Cisco WebVPN) sessions are secure, the client may still have cookies, browser files, and email attachments remaining after a session is complete. Cisco Secure Desktop (CSD) extends the inherent security of SSL VPN sessions by writing session data in an encrypted format to a special *vault* area of the client's disk. In addition, this data is removed from the disk at the end of the SSL VPN session. This document presents a sample configuration for CSD on a Cisco IOS® router.

CSD is supported on the following Cisco device platforms:

- Cisco IOS Routers Version 12.4(6)T and later
- Cisco 870,1811,1841, 2801, 2811, 2821, 2851, 3725, 3745, 3825, 3845, 7200 and 7301 routers
- Cisco VPN 3000 Series Concentrators Version 4.7 and later
- Cisco ASA 5500 Series Security Appliances Version 7.1 and later
- Cisco WebVPN Services Module for Cisco Catalyst and Cisco 7600 Series Version 1.2 and

later

# Prerequisites

## Requirements

Ensure that you meet these requirements before you attempt this configuration:

**Requirements for the Cisco IOS router**

- Cisco IOS router with Advanced Image 12.4(6T) or later
- Cisco Router Secure Device Manager (SDM) 2.3 or higher
- A copy of the CSD for IOS package on your management station
- A router self-signed digital certificate or authentication with a Certificate Authority (CA)**Note:** Anytime you use digital certificates, make sure that you set the router's hostname, domain name, and date/time/timezone correctly.
- An enable secret password on the router
- DNS enabled on your router. Several WebVPN services require DNS to work properly.

**Requirements for Client computers**

- Remote clients should have local administrative privileges; it is not required, but it is highly suggested.
- Remote clients must have Java Runtime Environment (JRE) Version 1.4 or higher.
- Remote client browsers: Internet Explorer 6.0, Netscape 7.1, Mozilla 1.7, Safari 1.2.2, or Firefox 1.0
- Cookies enabled and Popups allowed on remote clients

## Components Used

The information in this document is based on these software and hardware versions:

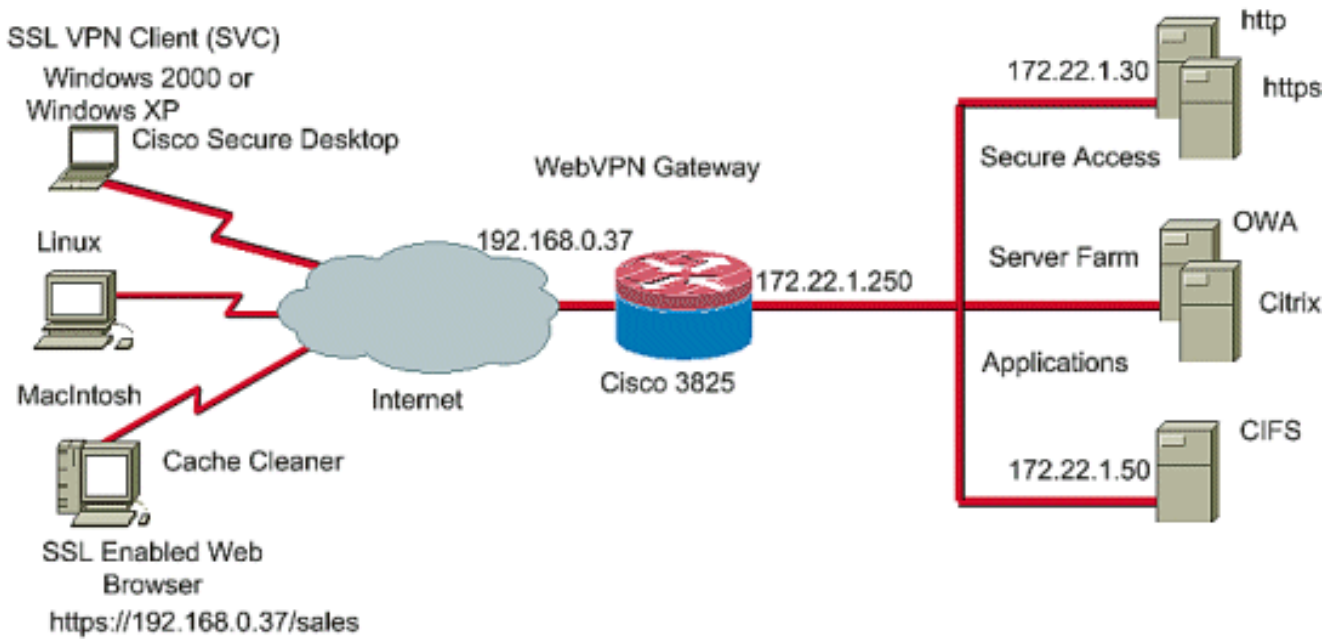
- Cisco IOS router 3825 with Version 12.9(T)
- SDM Version 2.3.1

The information in this document was created from the devices in a specific lab environment. All the devices used in this document began with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command.

## Network Diagram

This document uses this network setup:

This example uses a Cisco 3825 Series router to allow secure access to the company's intranet. The Cisco 3825 Series router enhances the security of SSL VPN connections with configurable CSD features and characteristics. Clients can connect to the CSD-enabled router via one of these three SSL VPN methods: Clientless SSL VPN (WebVPN), Thin-Client SSL VPN ( Port-Forwarding), or SSL VPN Client (Full Tunneling SVC).




### Related Products

This configuration can also be used with these hardware and software versions:

- Cisco router platforms 870,1811,1841,2801,2811,2821 2851,3725,3745.3825,3845, 7200 and 7301
- Cisco IOS Advanced Security Image Version 12.4(6)T and later

## Conventions

Refer to the Cisco Technical Tips Conventions for more information about document conventions.

## Configure

A WebVPN gateway allows a user to connect to the router via one of the SSL VPN technologies. Only one WebVPN gateway per IP address is allowed on the device, although more than one WebVPN context can be attached to a WebVPN gateway. Each context is identified by a unique name. Group Policies identify the configured resources available to a particular WebVPN context.

Configuration of CSD on an IOS router is accomplished in two phases:

**Phase I: Prepare your router for CSD configuration with SDM**

1. **Configure a WebVPN gateway, WebVPN context, and group policy** .**Note:** This step is optional and is not covered in great detail in this document. If you have already configured your router for one of the SSL VPN technologies, omit this step.
2. **Enable CSD in a WebVPN context** .

**Phase II: Configure CSD using a web browser.**

1. **Define *Windows Locations*** .
2. **Identify Location criteria** .
3. **Configure Windows location modules and features** .

4. [Configure Windows CE, Macintosh, and Linux features] .

## Phase I: Prepare your router for CSD configuration with SDM.

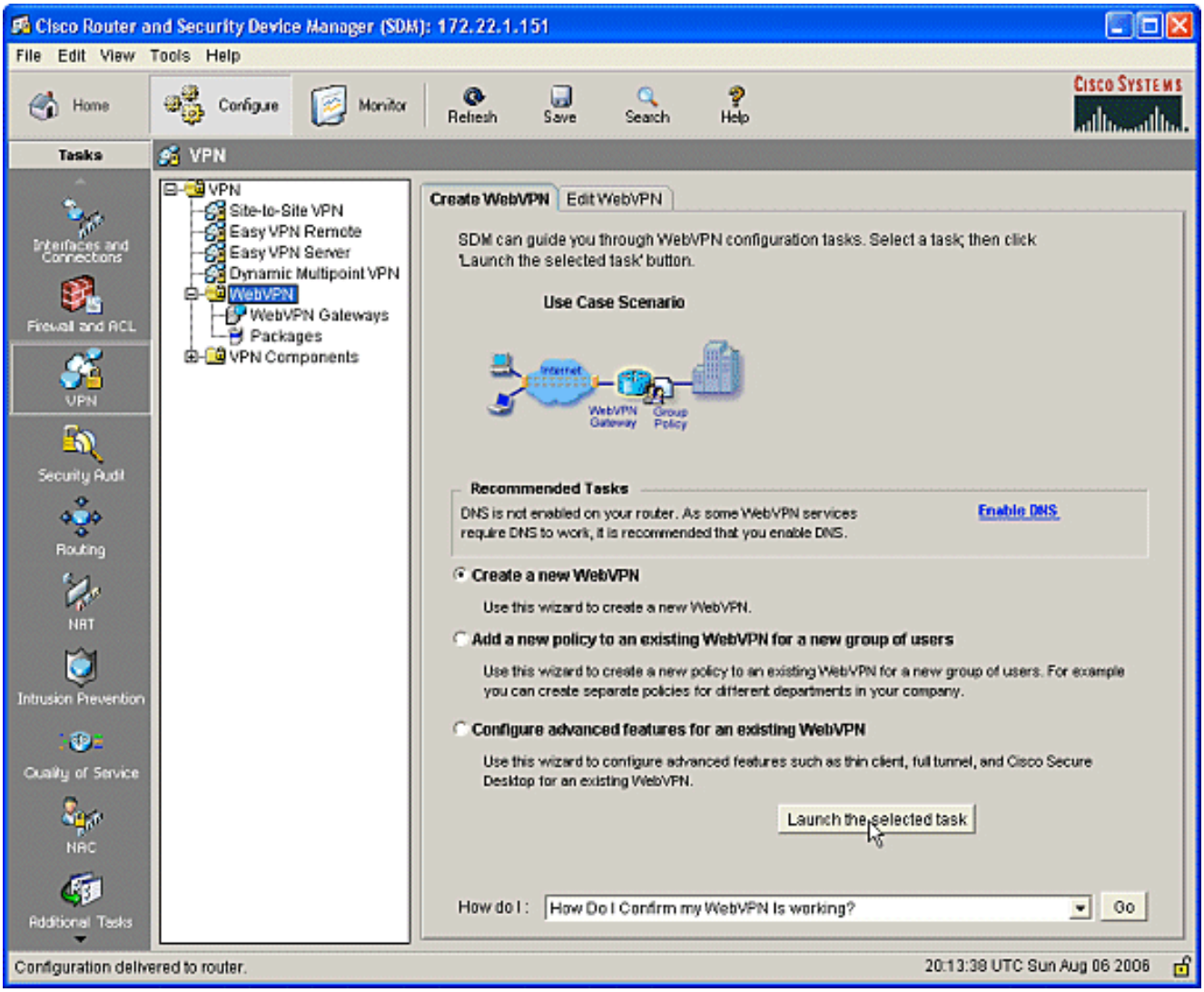
CSD can be configured with SDM or from the command-line interface (CLI). This configuration uses SDM and a web browser.

These steps are used to complete the configuration of CSD on your IOS router.

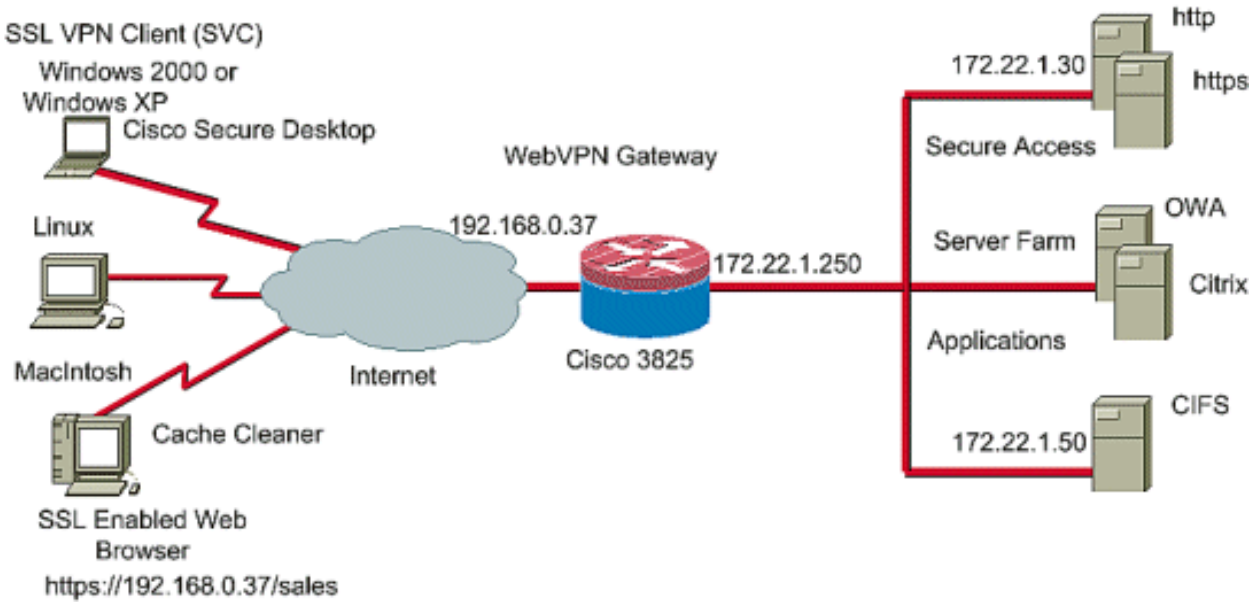
## Phase I: Step 1: Configure a WebVPN gateway, WebVPN context, and group policy.

You can use the WebVPN Wizard to accomplish this task.

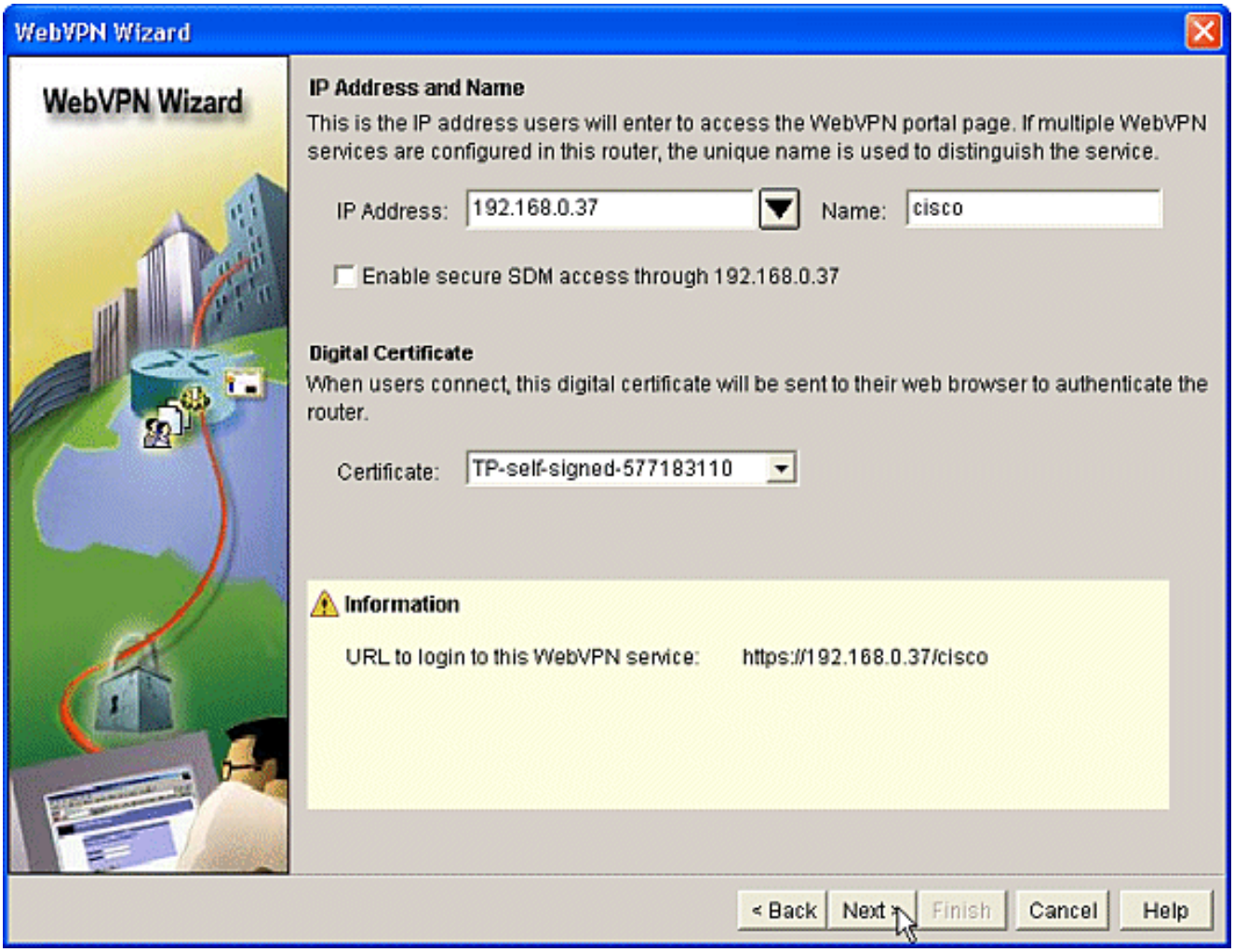
1. Open SDM and go to **Configure > VPN > WebVPN**. Click the **Create WebVPN** tab and check the **Create a new WebVPN** radio button. Click **Launch the selected task**.



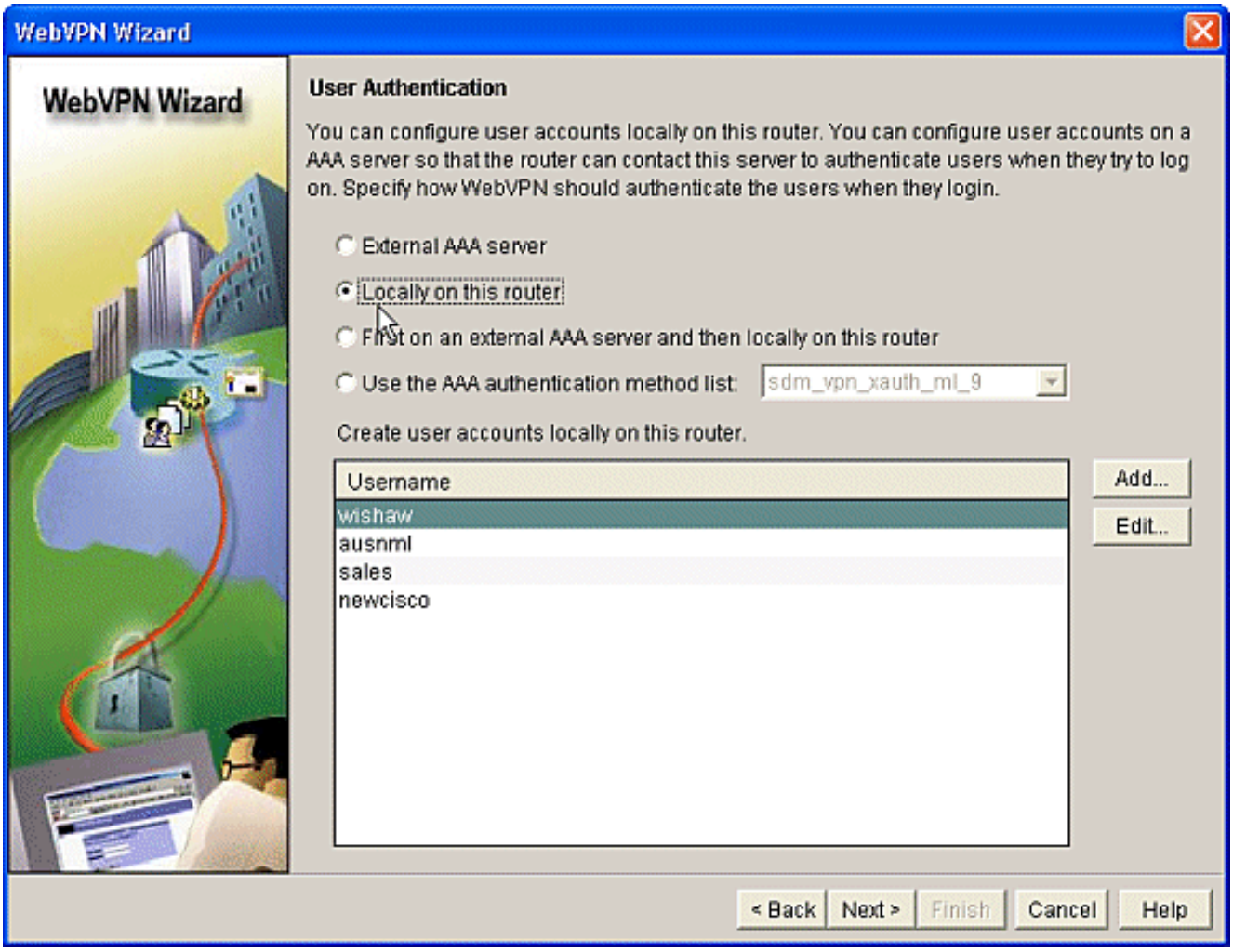

2. The WebVPN Wizard screen lists the parameters that you can configure. Click **Next**.



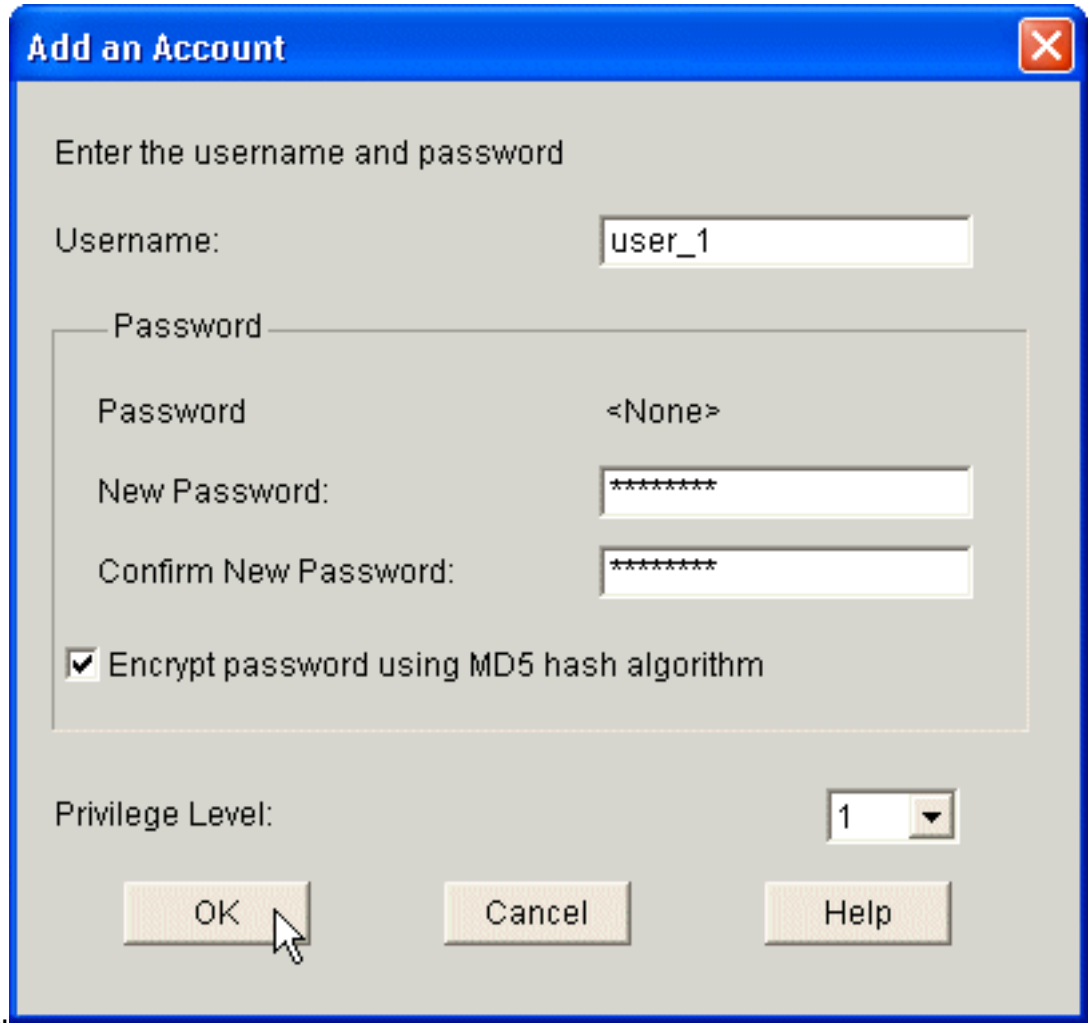

3. Enter the IP address for the WebVPN gateway, a unique name for the service, and Digital Certificate information. Click **Next**.




4. User accounts can be created for authentication to this WebVPN gateway. You can use either local accounts or accounts created on an external Authentication, Authorization, and Accounting (AAA) server. This example uses local accounts on the router. Check the radio button **Locally on this router** and click **Add**.

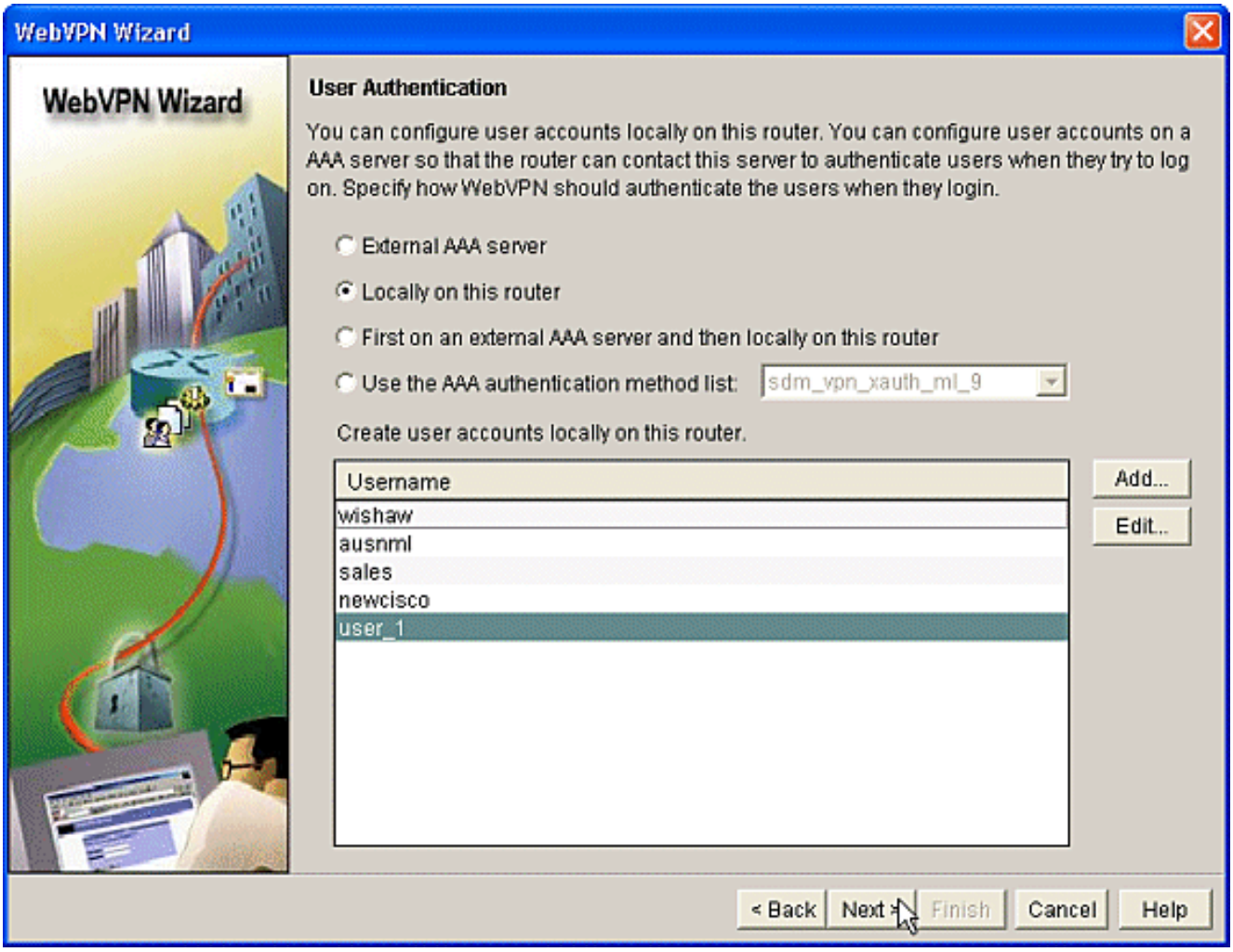



5. Enter the account information for the new user on the Add an Account screen and click

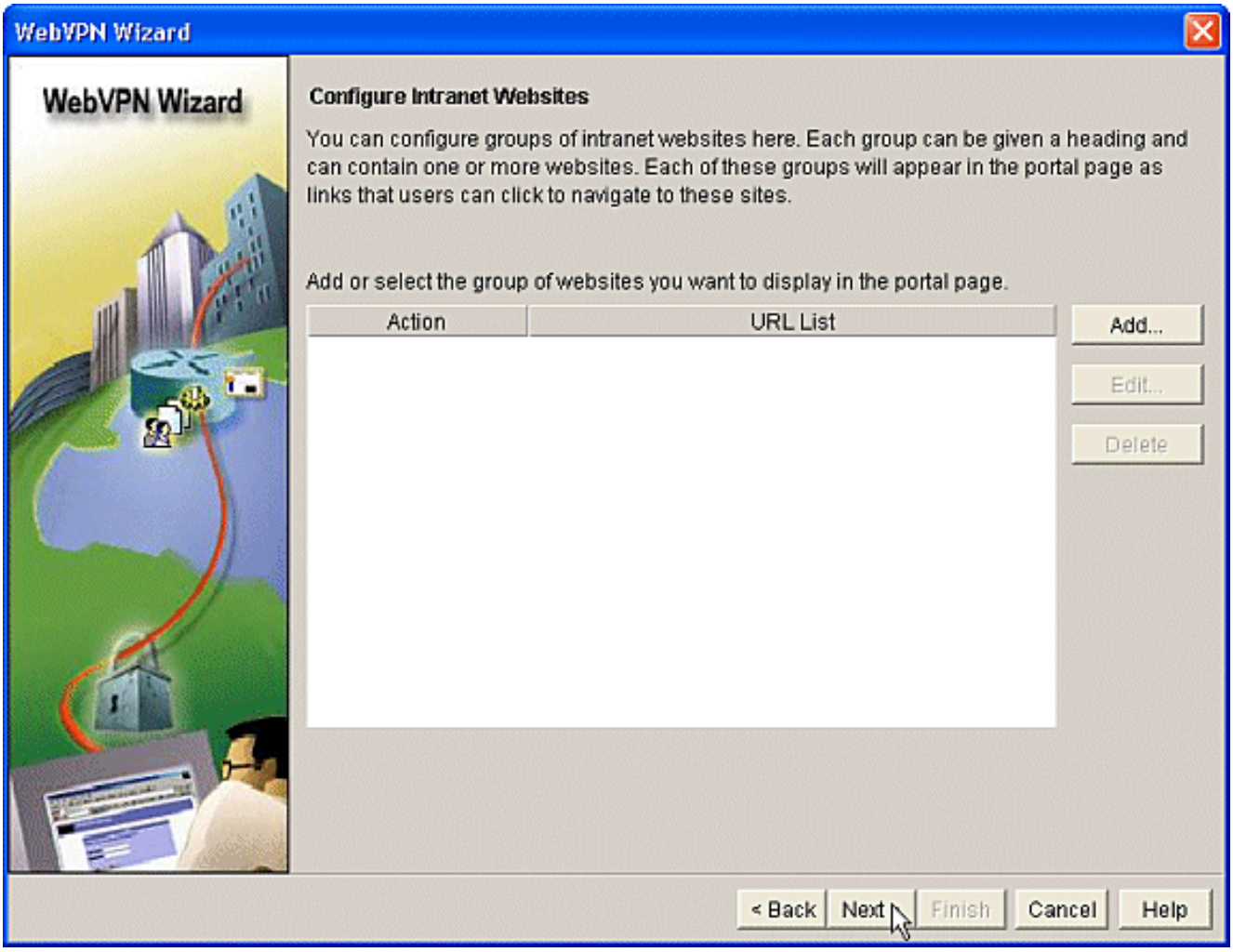



**OK**.

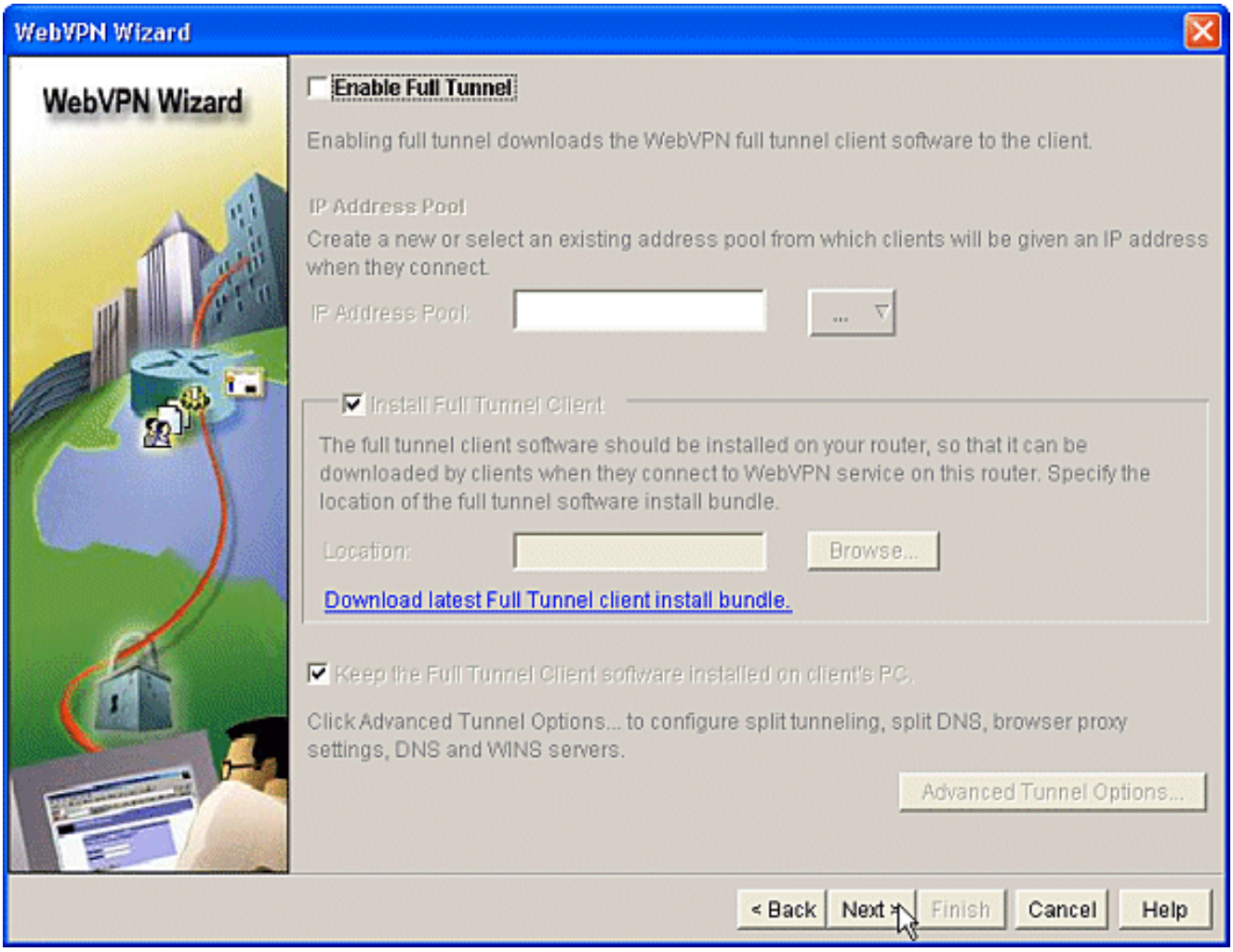
6. After you have created your users, click **Next** on the User Authentication page.



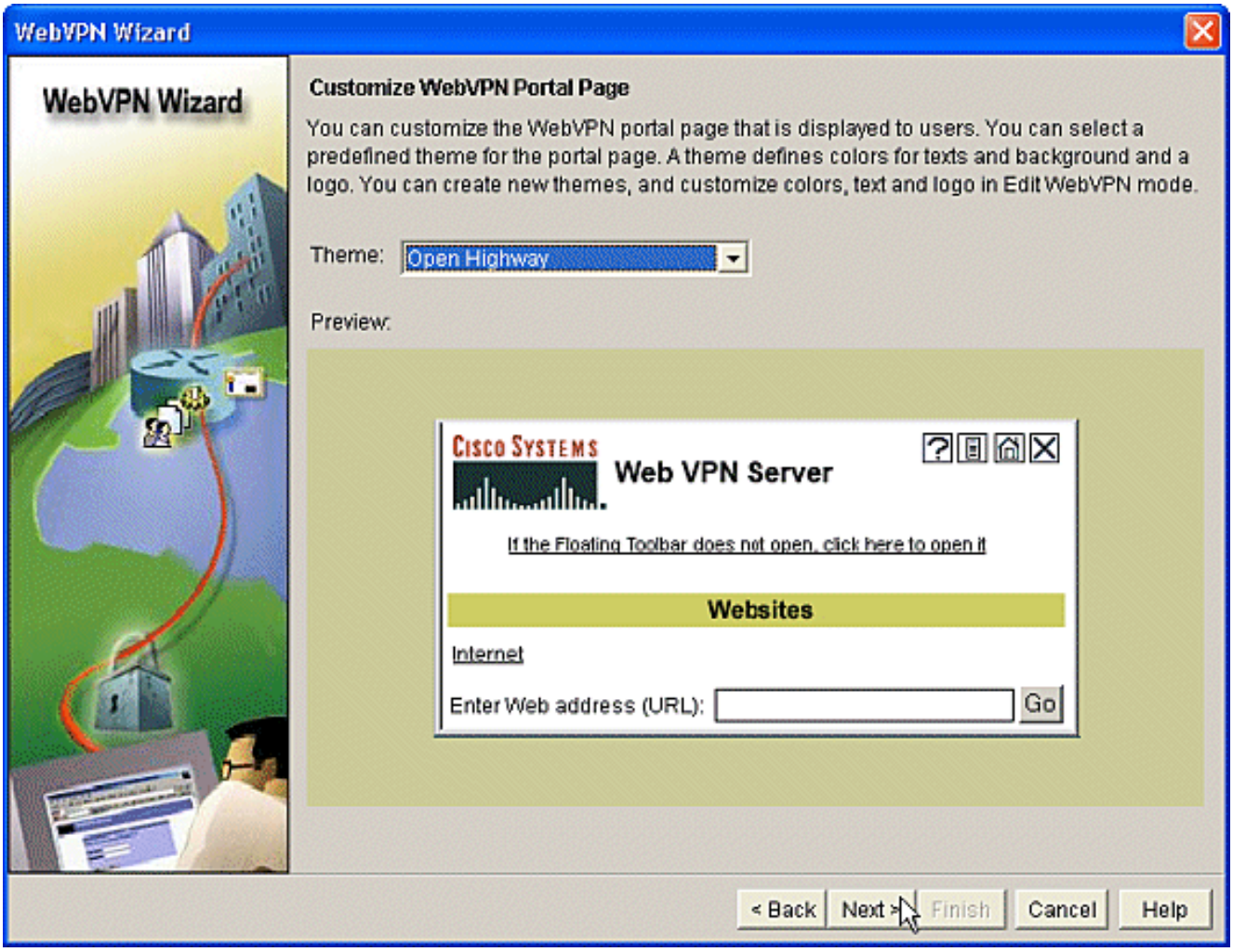

7. The Configure Intranet Websites screen allows you to configure the website available to users of the WebVPN gateway. Since this document's focus is the configuration of CSD, disregard this page. Click **Next**.



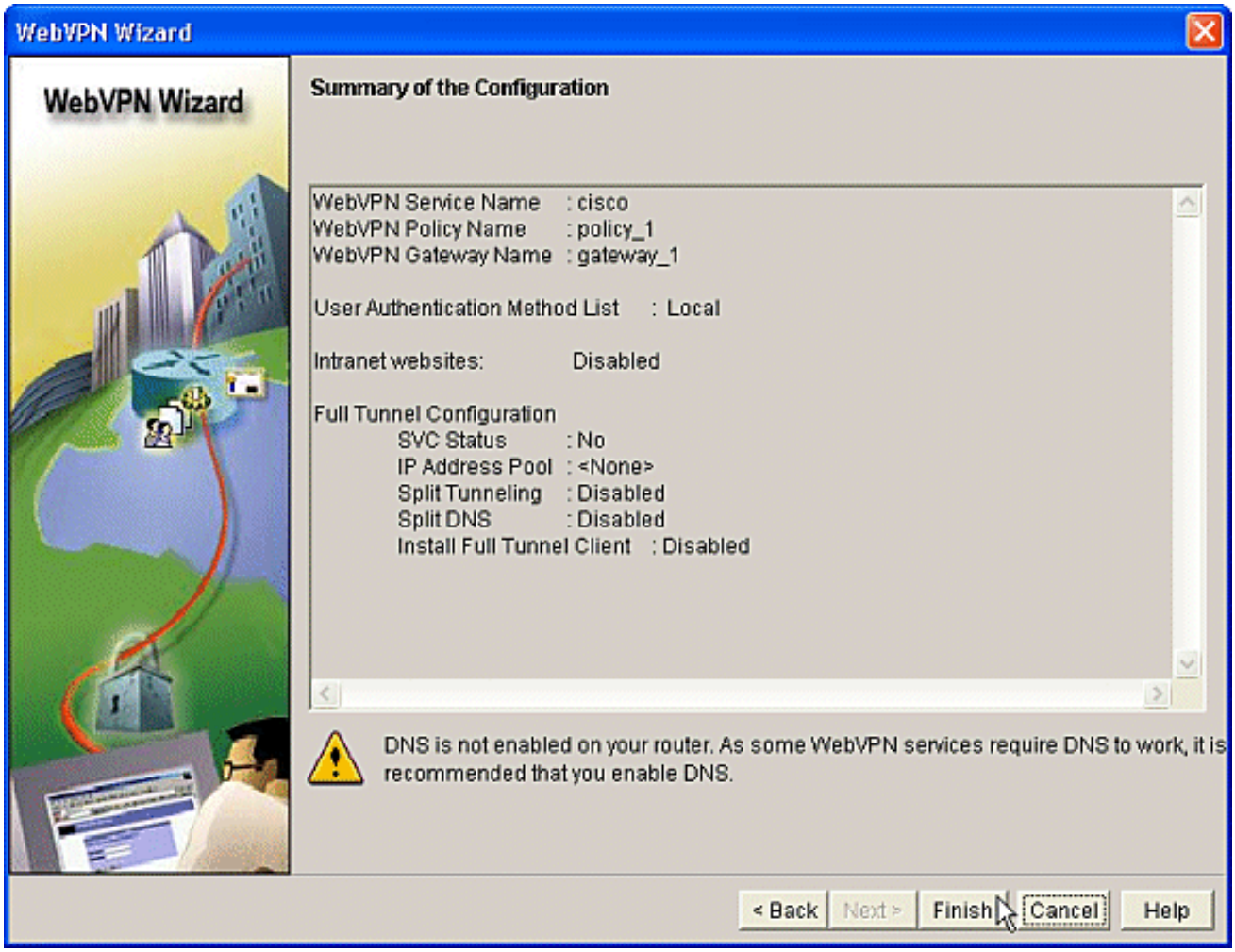

8. Although the next WebVPN Wizard screen allows you the choice to enable the Full Tunnel SSL VPN Client, the focus of this document is how to enable CSD. Uncheck **Enable Full Tunnel** and click
**Next**.




9. You can customize the appearance of the WebVPN Portal Page to users. In this case, the default appearance is accepted. Click
**Next**.



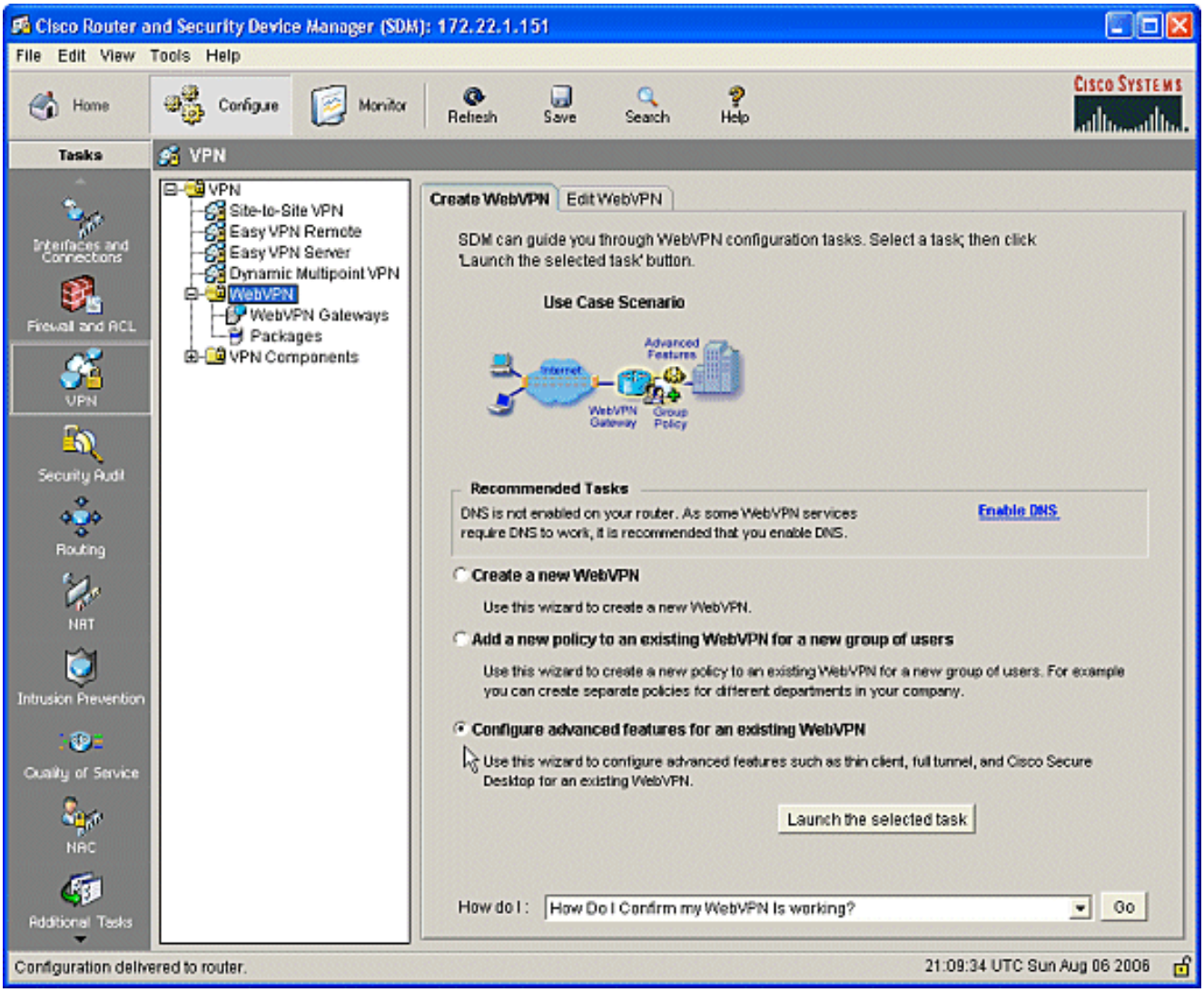

10. The Wizard displays the last screen in this series. It shows a summary of the configuration for the WebVPN gateway. Click **Finish** and, when prompted, click **OK**.



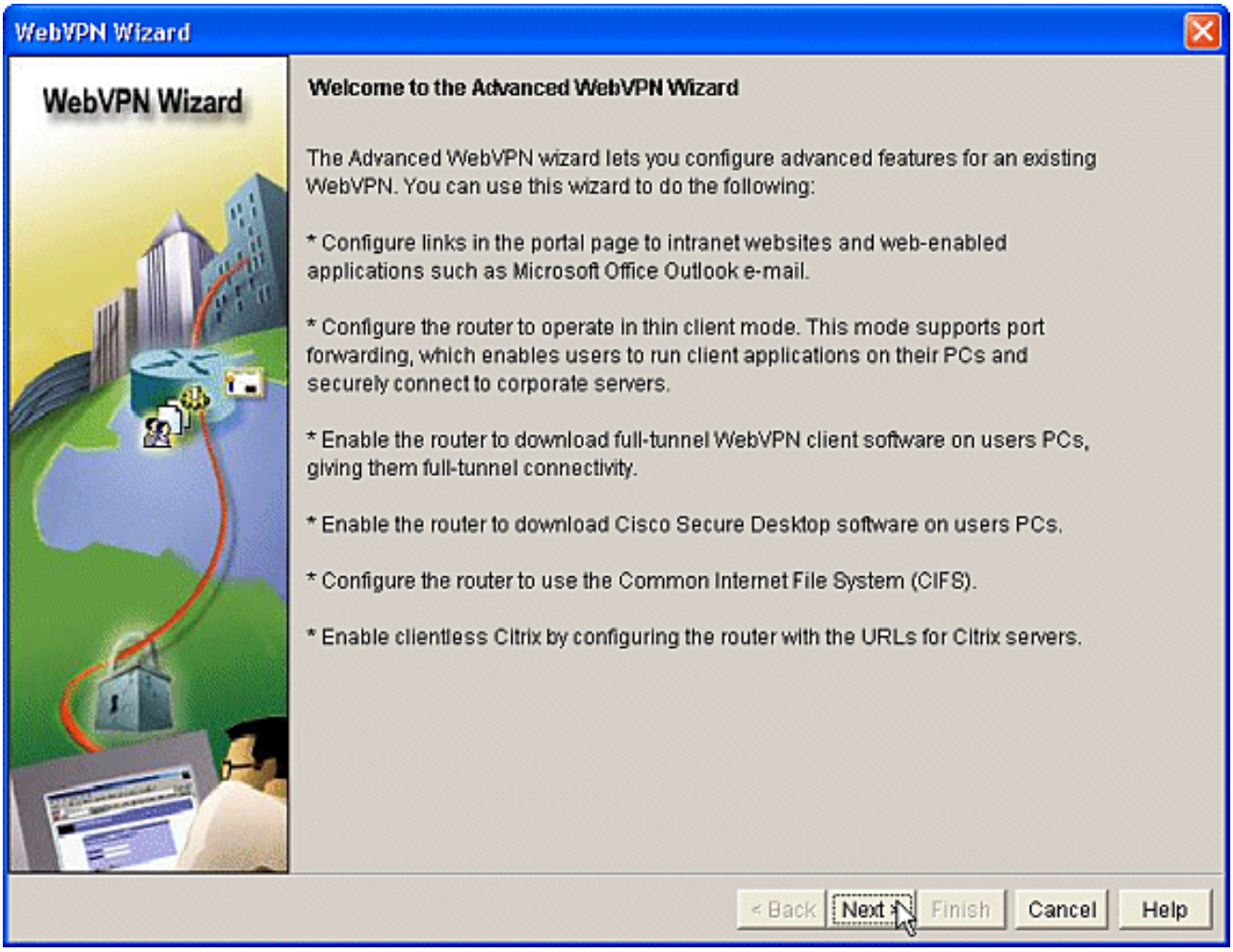

## Phase I: Step 2: Enable CSD in a WebVPN context.

Use WebVPN Wizard to enable CSD in a WebVPN context.

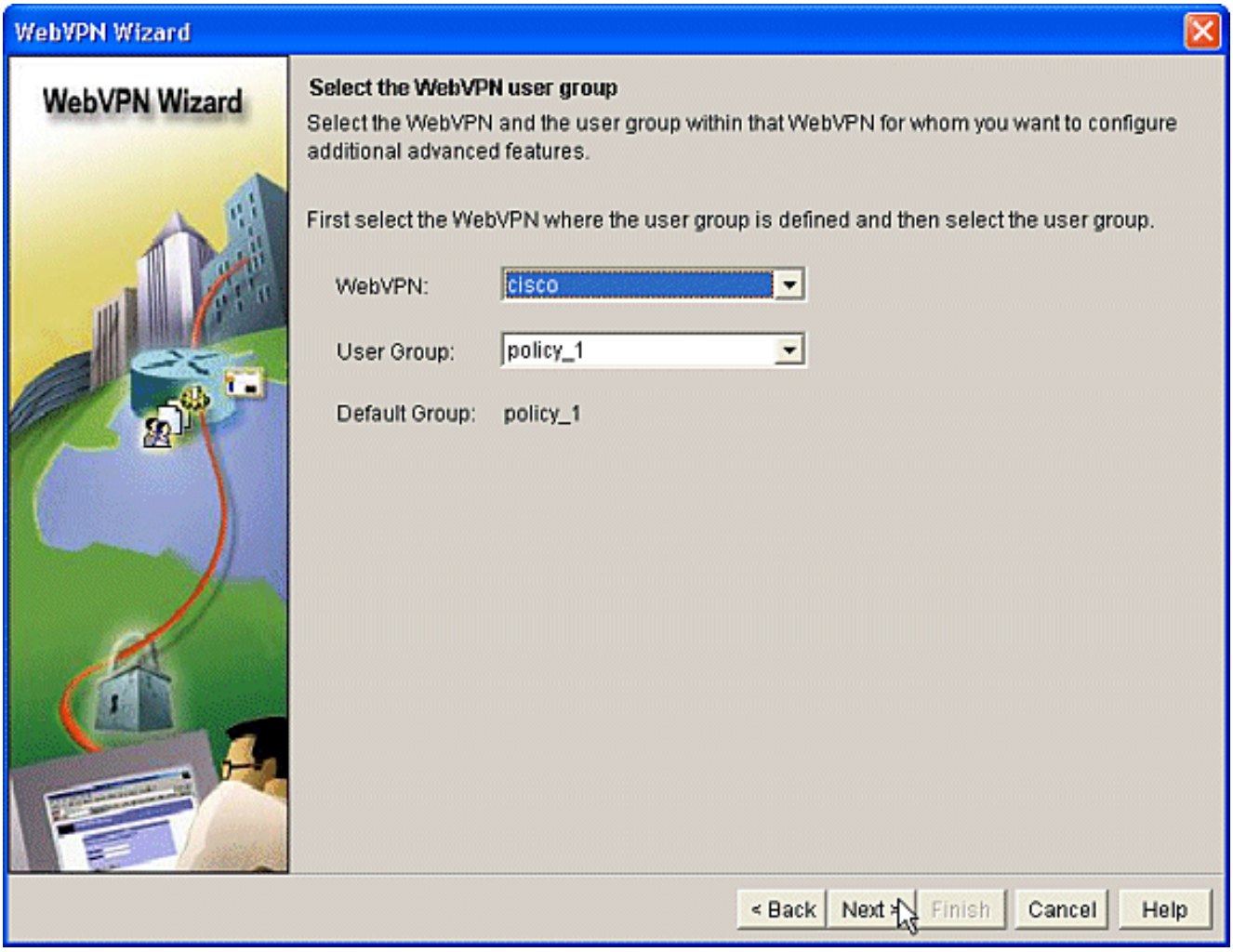
1. Use the advanced features of the WebVPN Wizard to enable CSD for the newly created context. The Wizard gives you the opportunity to install the CSD package if it is not already installed.In SDM, click the **Configure** tab.In the navigation pane, click **VPN > WebVPN**.Click the **Create WebVPN** tab.Check the **Configure advance features for an existing WebVPN** radio button.Click the **Launch the selected task**
   button.



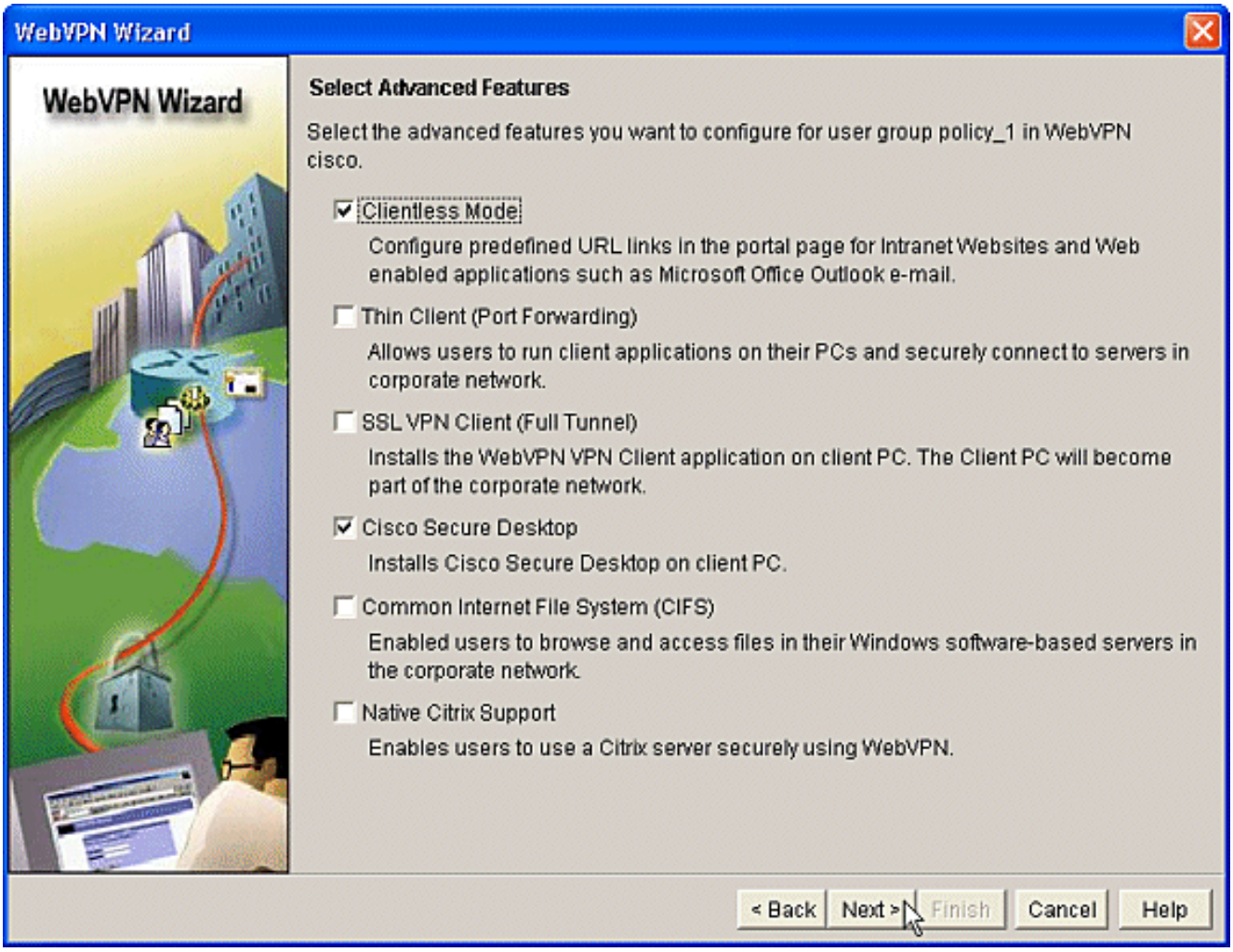

2. The welcome page for the Advanced WebVPN Wizard displays. Click **Next**.



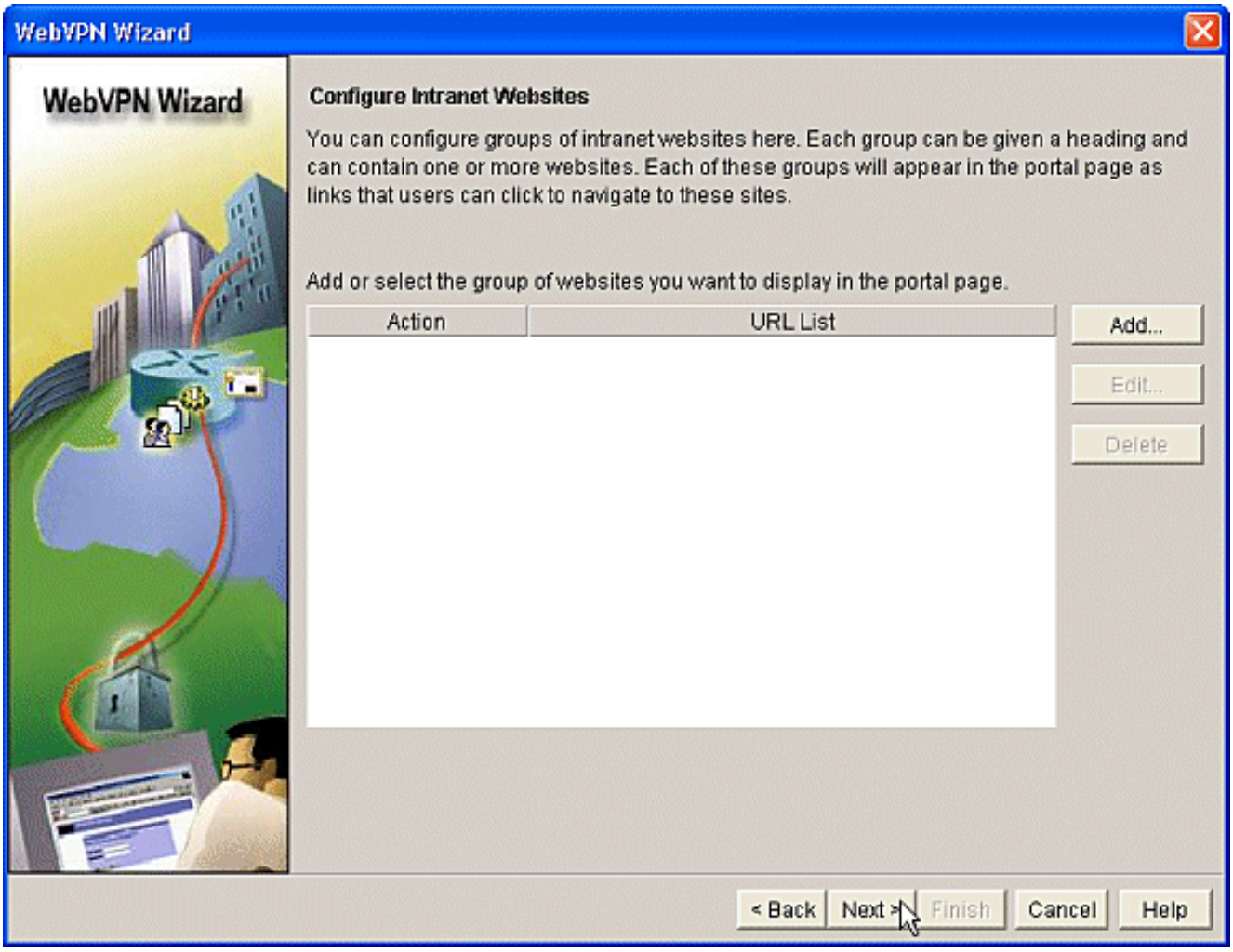

3. Choose the WebVPN and user group from the fields' drop-down boxes. The Advanced WebVPN Wizard features will be applied to your choices. Click **Next**.




4. The Select Advanced Features screen allows you to choose from the listed technologies.Check **Cisco Secure Desktop**.In this example, the choice is **Clientless Mode**.If you choose any of the other listed technologies, additional windows open to allow input of related information.Click the **Next**
button.

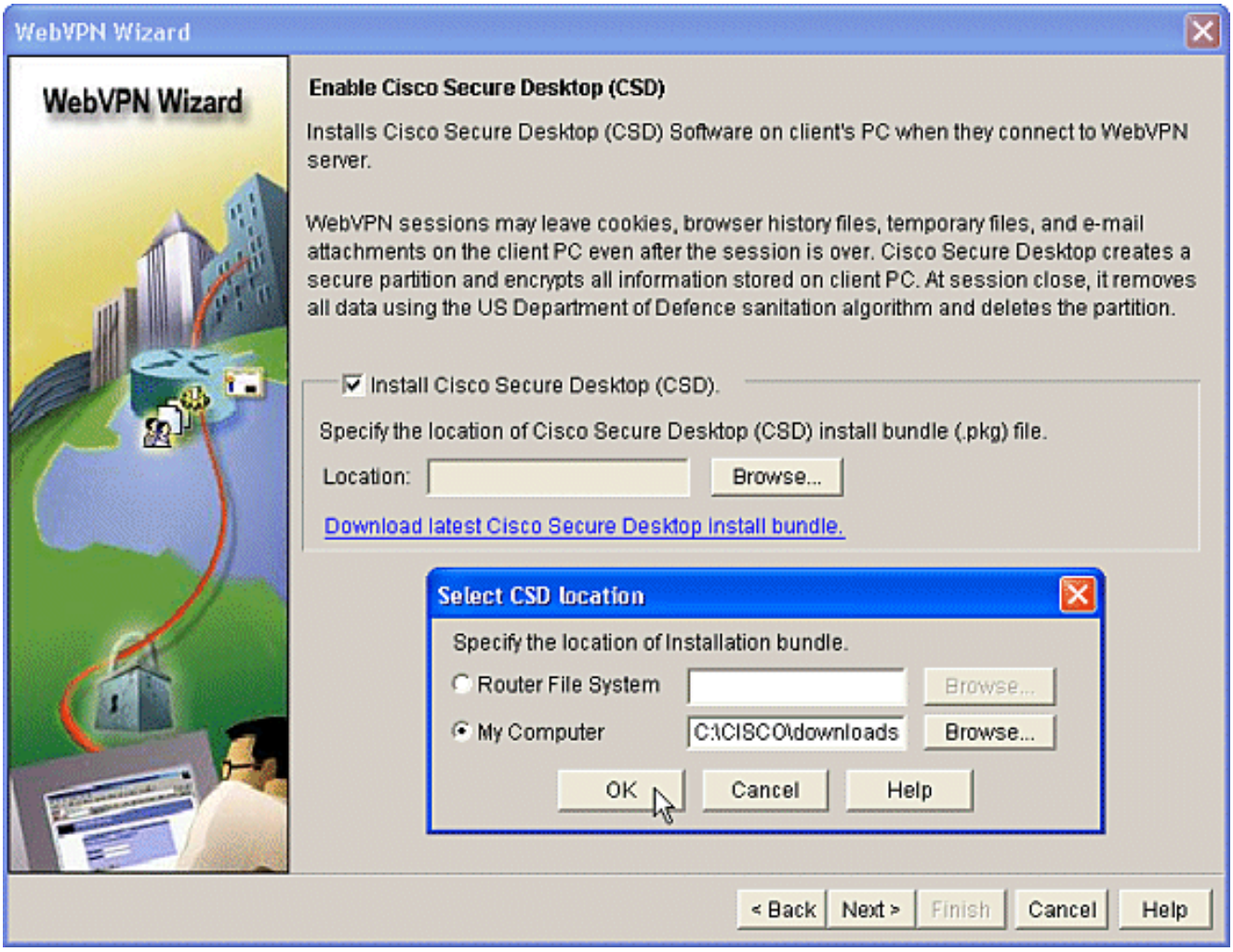



5. The Configure Intranet Websites screen allows you to configure the website resources you want available to the users. You can add the company's internal websites such as Outlook Web Access
(OWA).



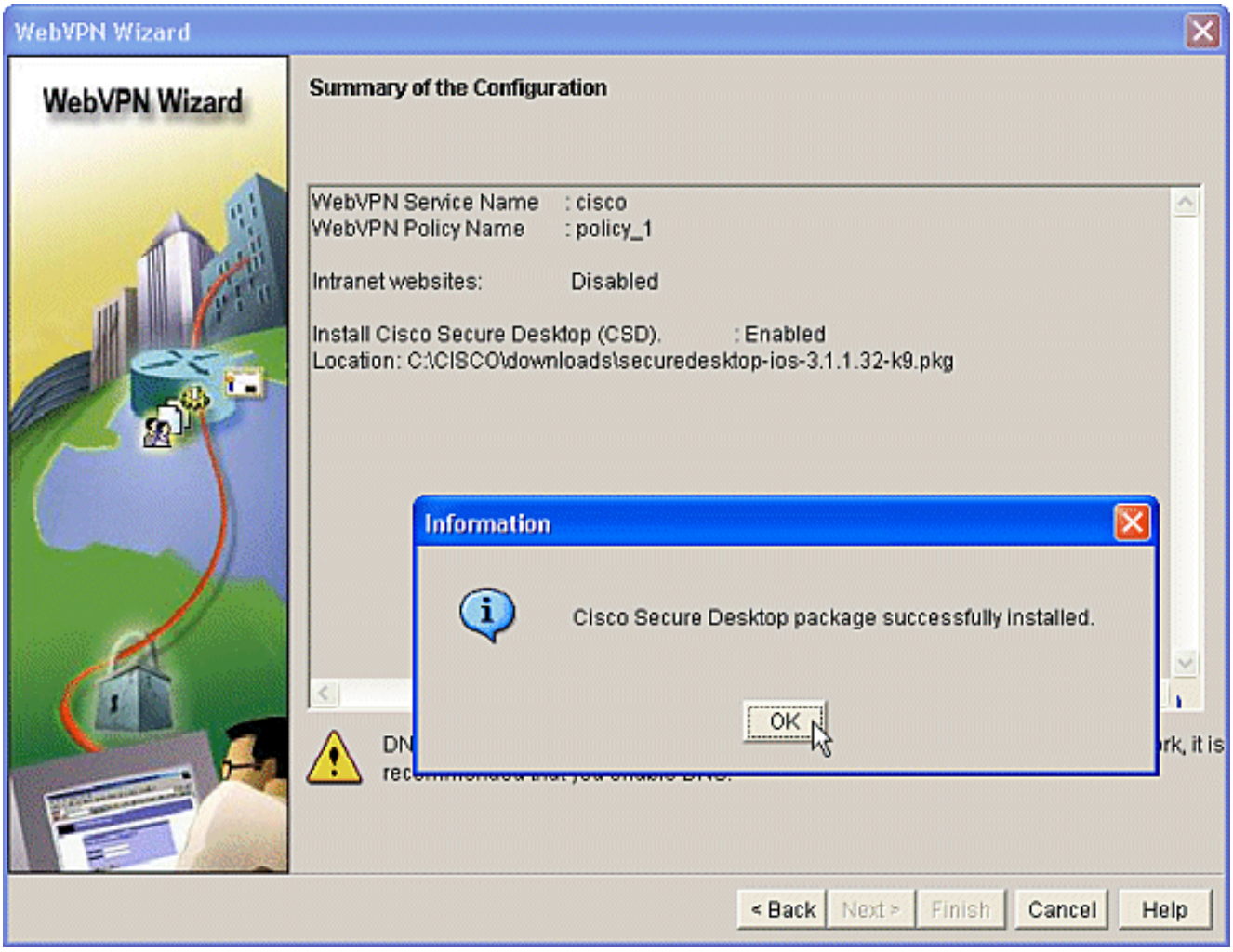

6. In the Enable Cisco Secure Desktop (CSD) screen, you have the opportunity to enable the CSD for this context. Check the box beside **Install Cisco Secure Desktop (CSD)** and click **Browse**.


7. From the Select CSD Location area, check **My Computer**.Click the **Browse** button.Choose the CSD IOS package file on your management workstation.Click the **OK** button.Click the **Next**
button.




8. A Summary of the Configuration screen displays. Click the **Finish** button.


9. Click **OK** when you see that the CSD package file has been successfully installed.



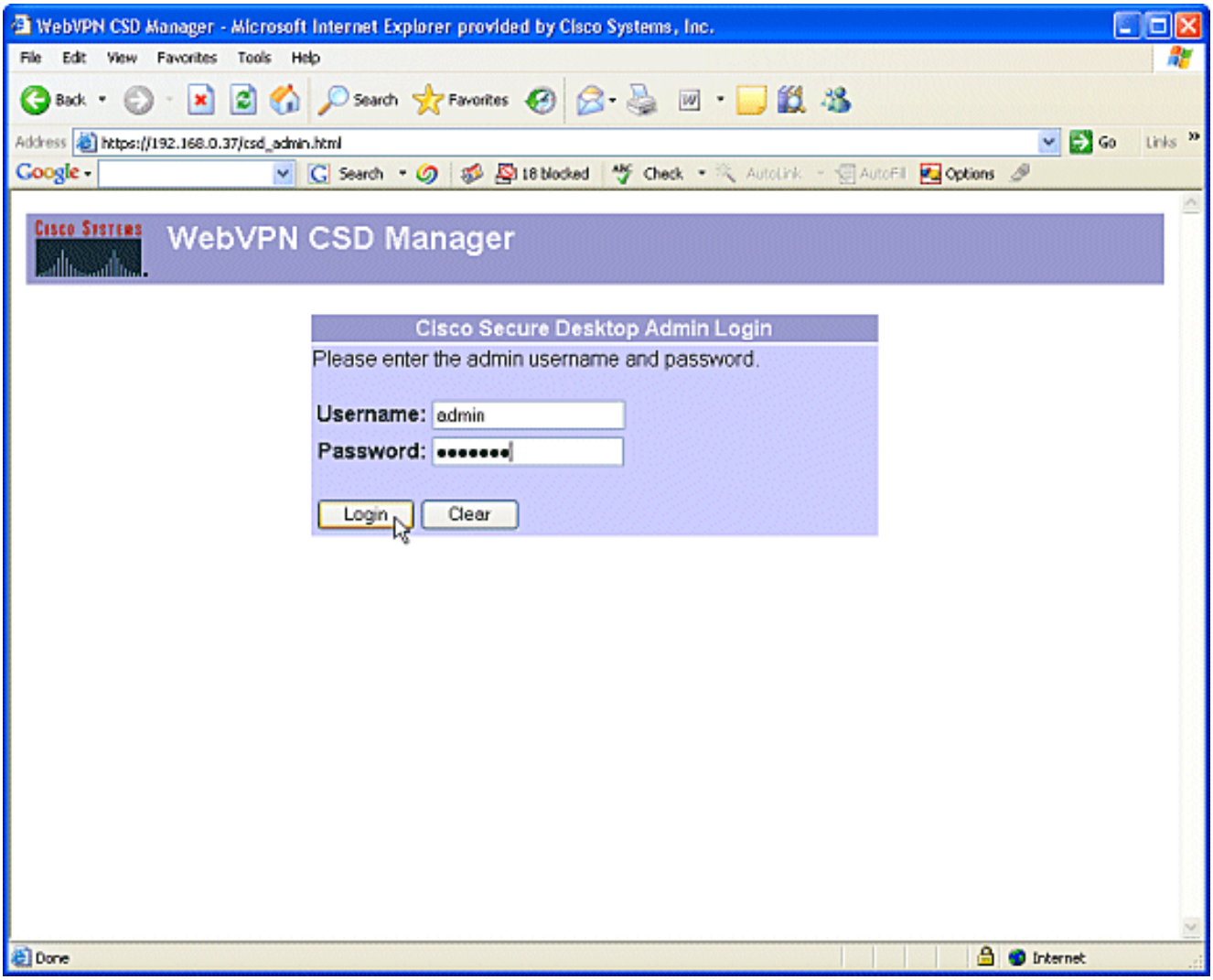

## Phase II: Configure CSD using a web browser.

These steps are used to complete the configuration of CSD on your web browser.

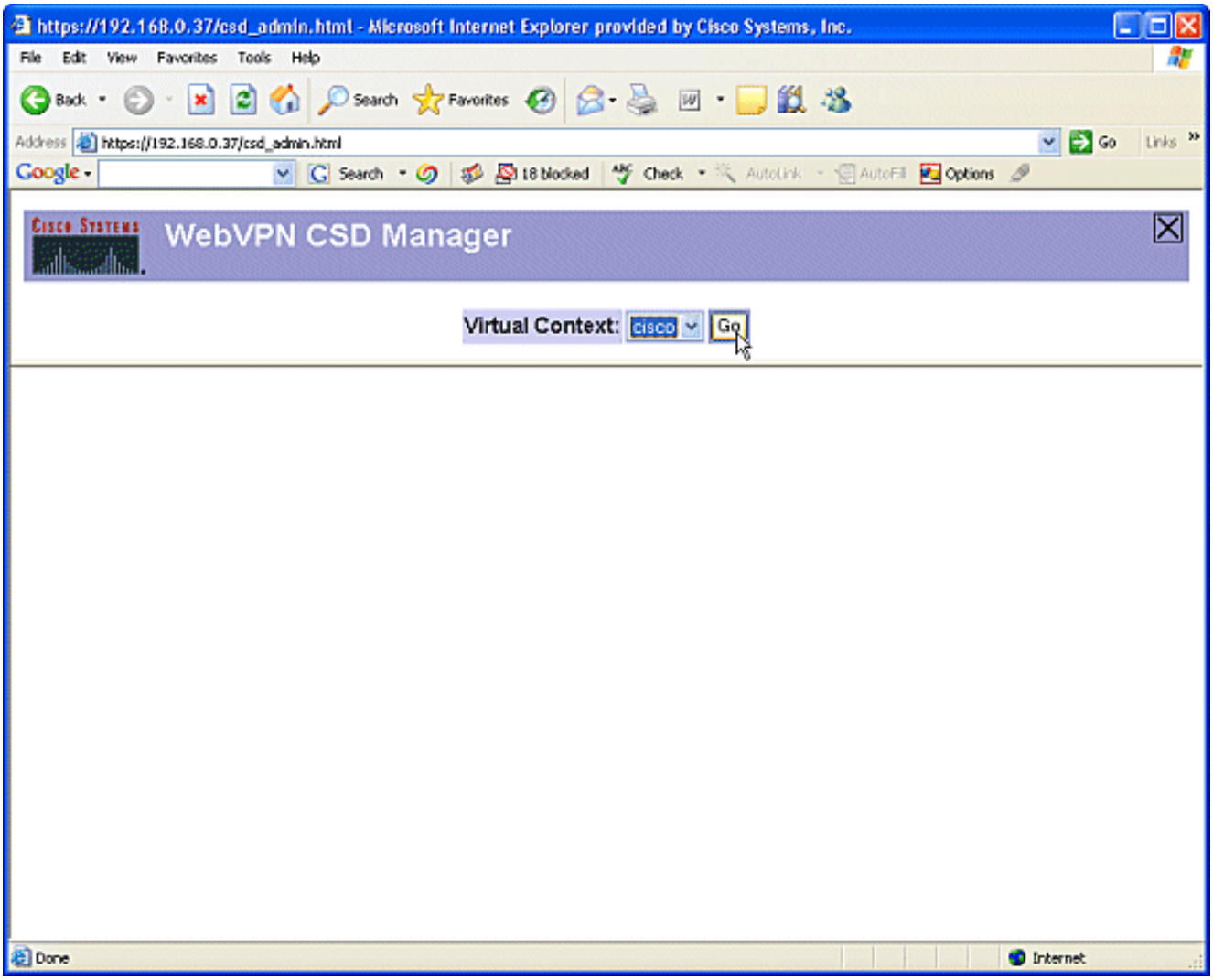
## Phase II: Step 1: Define Windows locations.

Define the Windows locations.

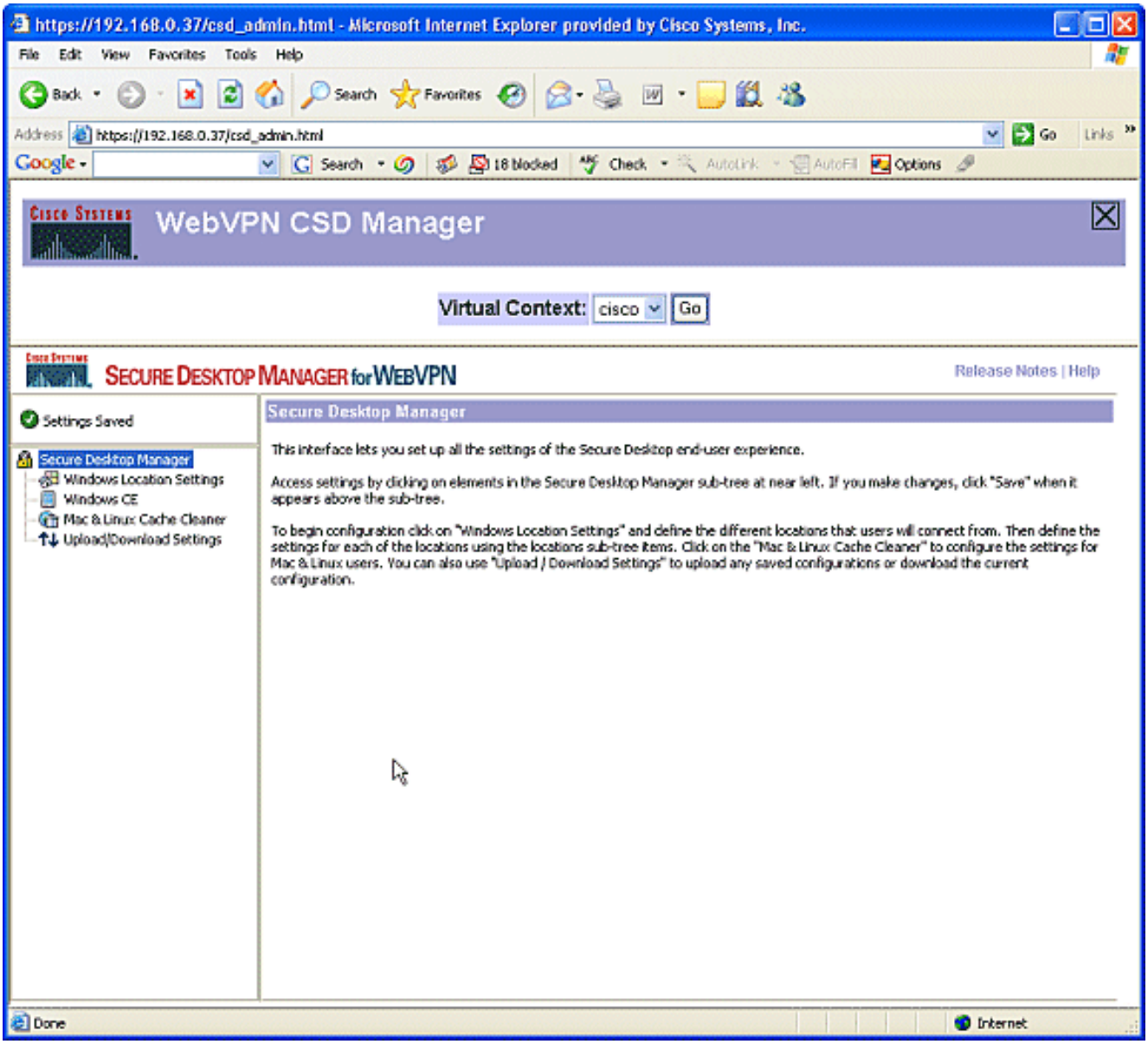
1. Open your web browser at **https://WebVPNgateway_IP Address/csd_admin.html**, for example, **https:/192.168.0.37/csd_admin.html**.
2. Enter the username **admin**.Enter the password, which is the enable secret of the router.Click **Login**.



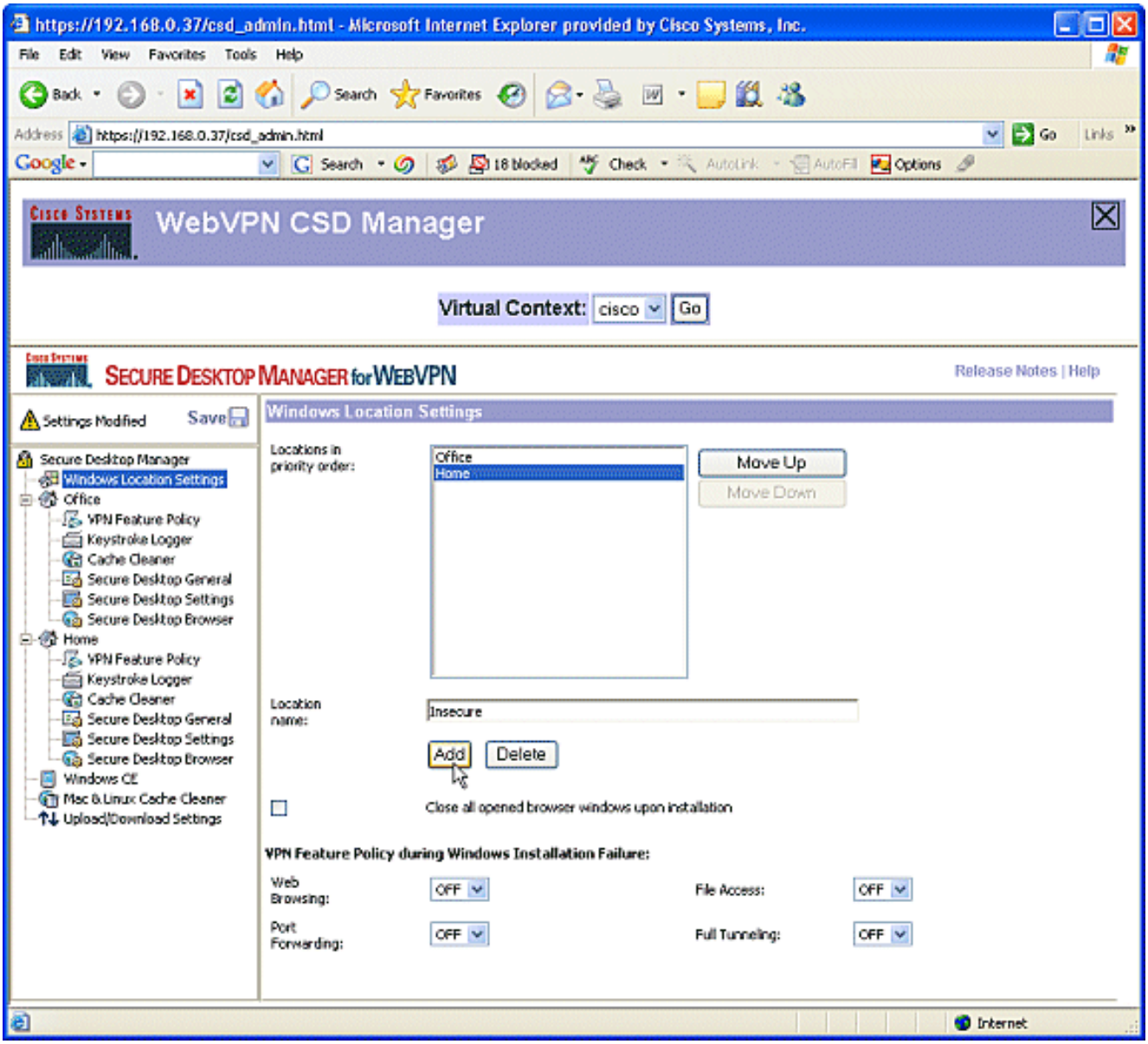

3. Accept the certificate offered by the router, choose the context from the drop-down box, and click
   **Go**.



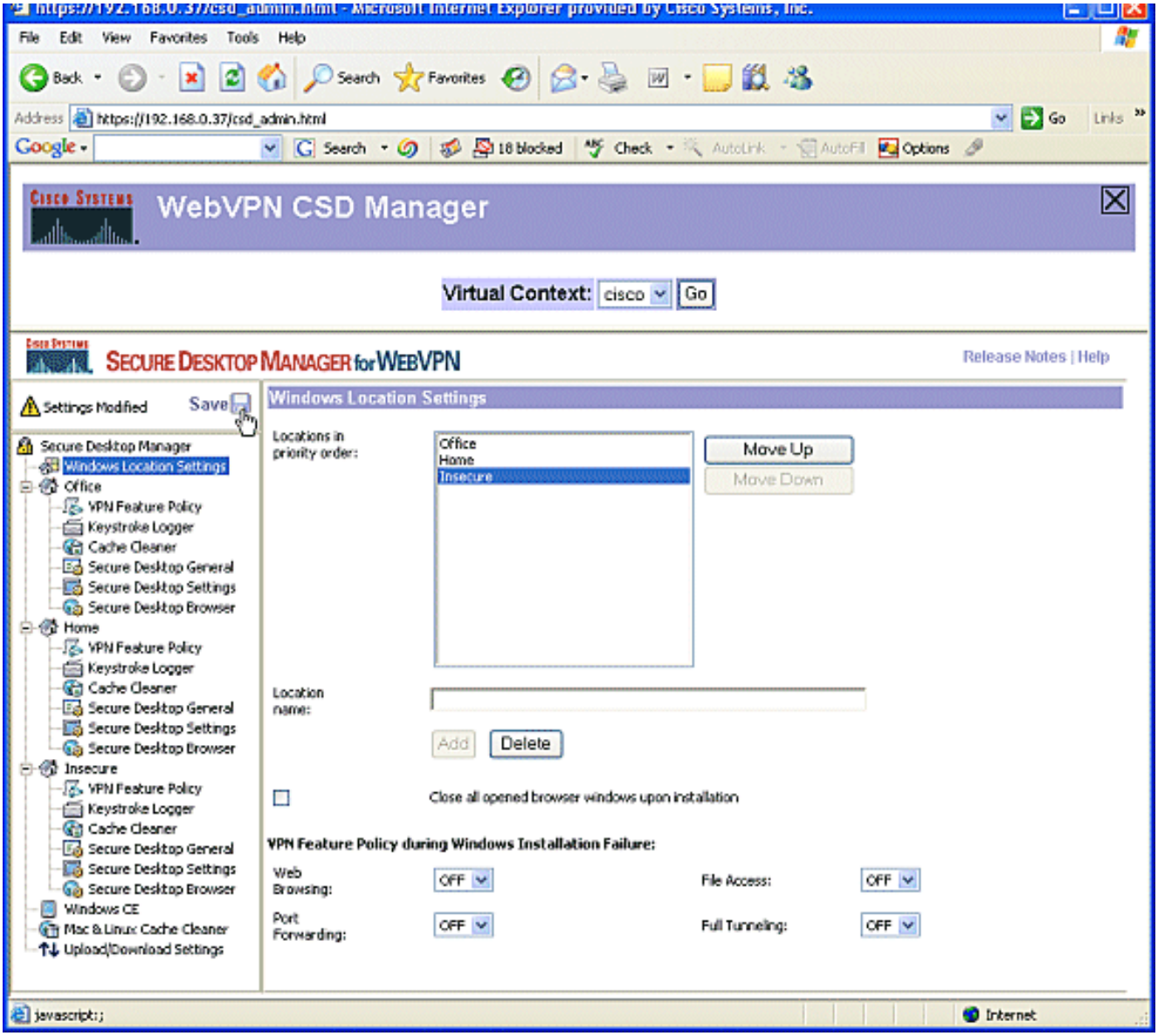

4. The Secure Desktop Manager for WebVPN opens.




5. From the left pane, choose **Windows Location Settings**.Place the cursor in the box next to Location name, and enter a location name.Click **Add**.In this example, three location names are shown: Office, Home, and Insecure. Each time a new location is added, the left pane expands with the configurable parameters for that location.



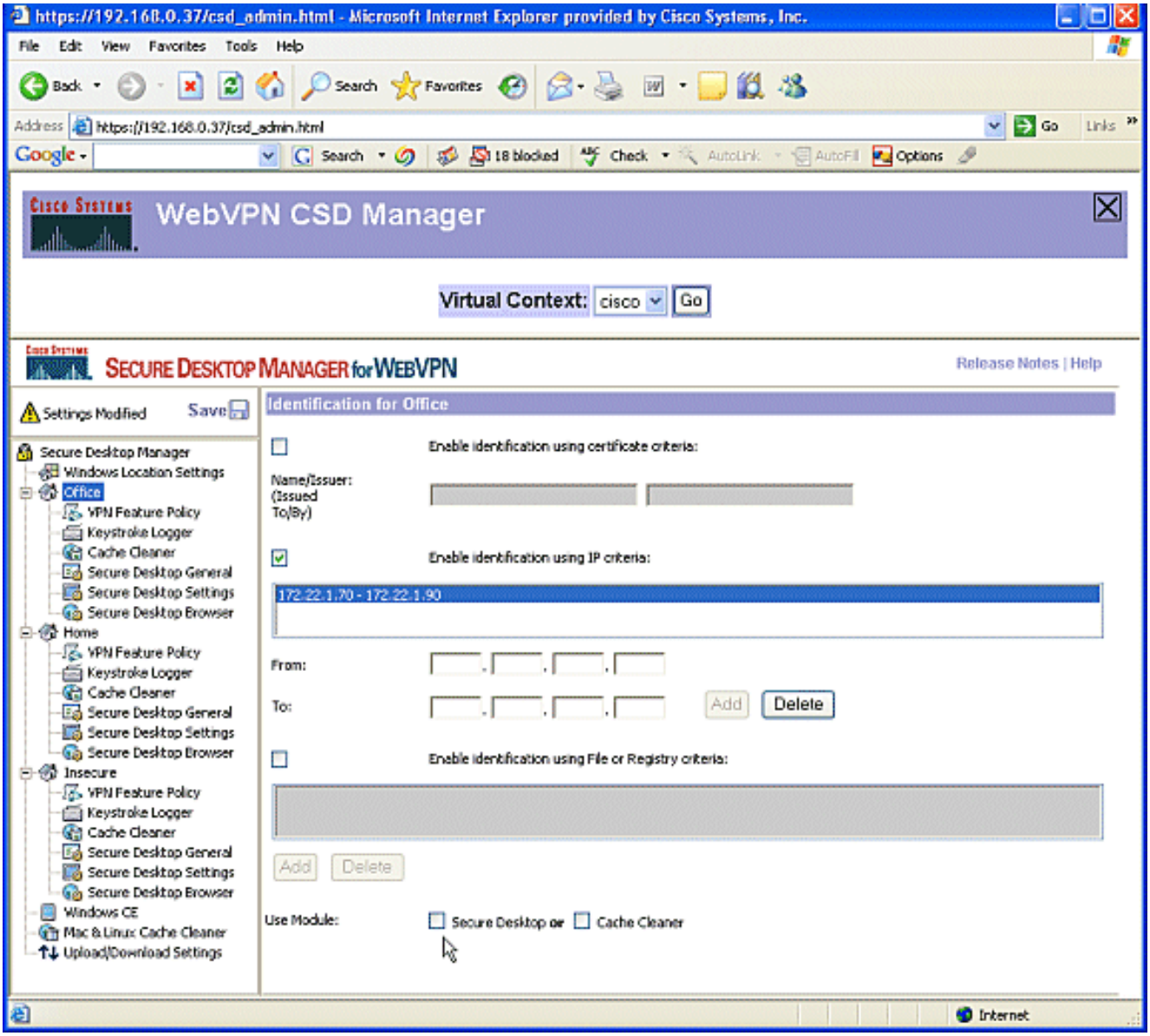

6. After you create the Windows locations, click **Save** at the top of the left pane.**Note:** Save your configurations often because your settings will be lost if you become disconnected from the web
browser.



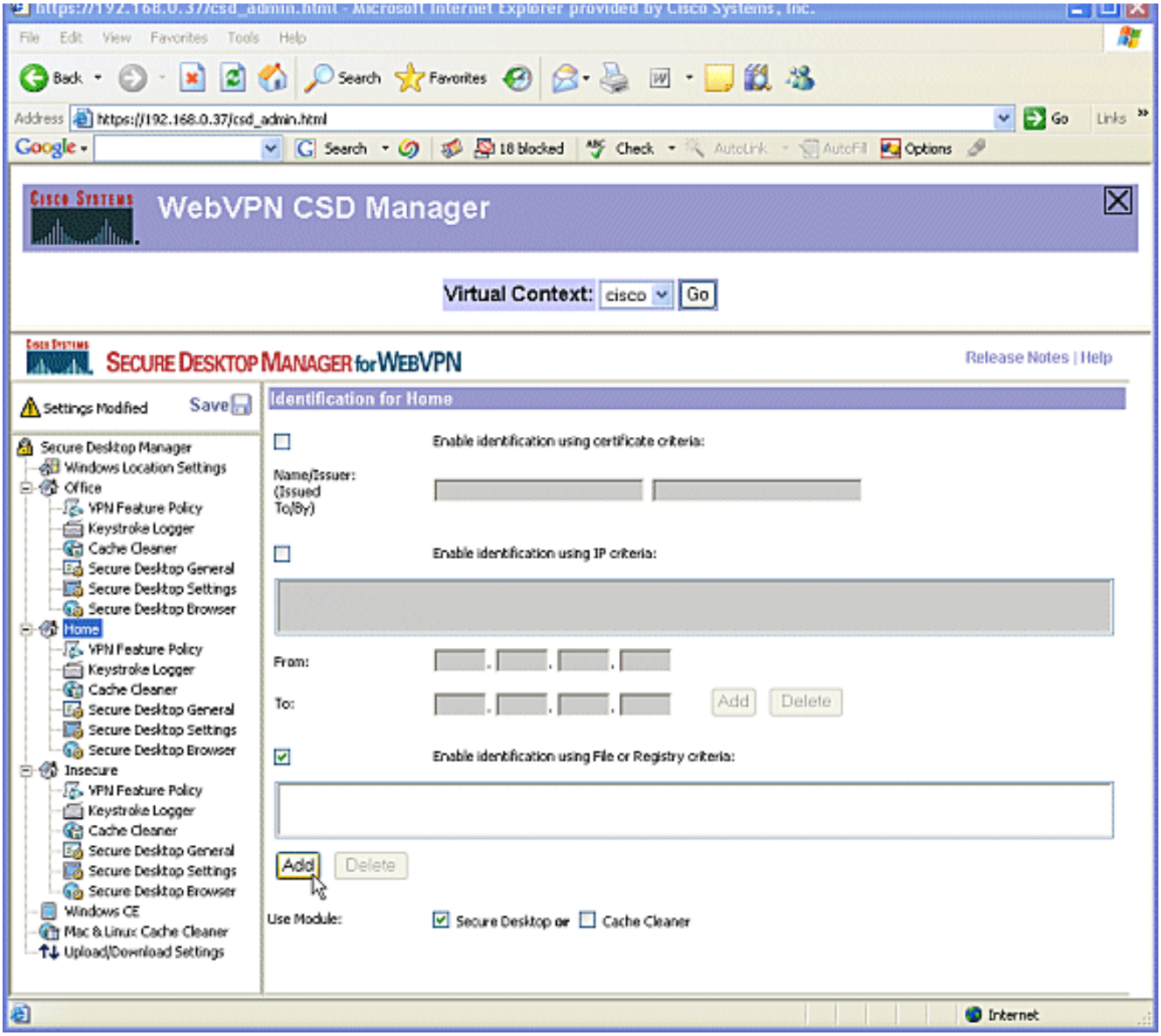

## Phase II: Step 2: Identify Location criteria

In order to distinguish Windows locations from each other, assign specific criteria to each location. This allows CSD to determine which of its features to apply to a particular Windows location.

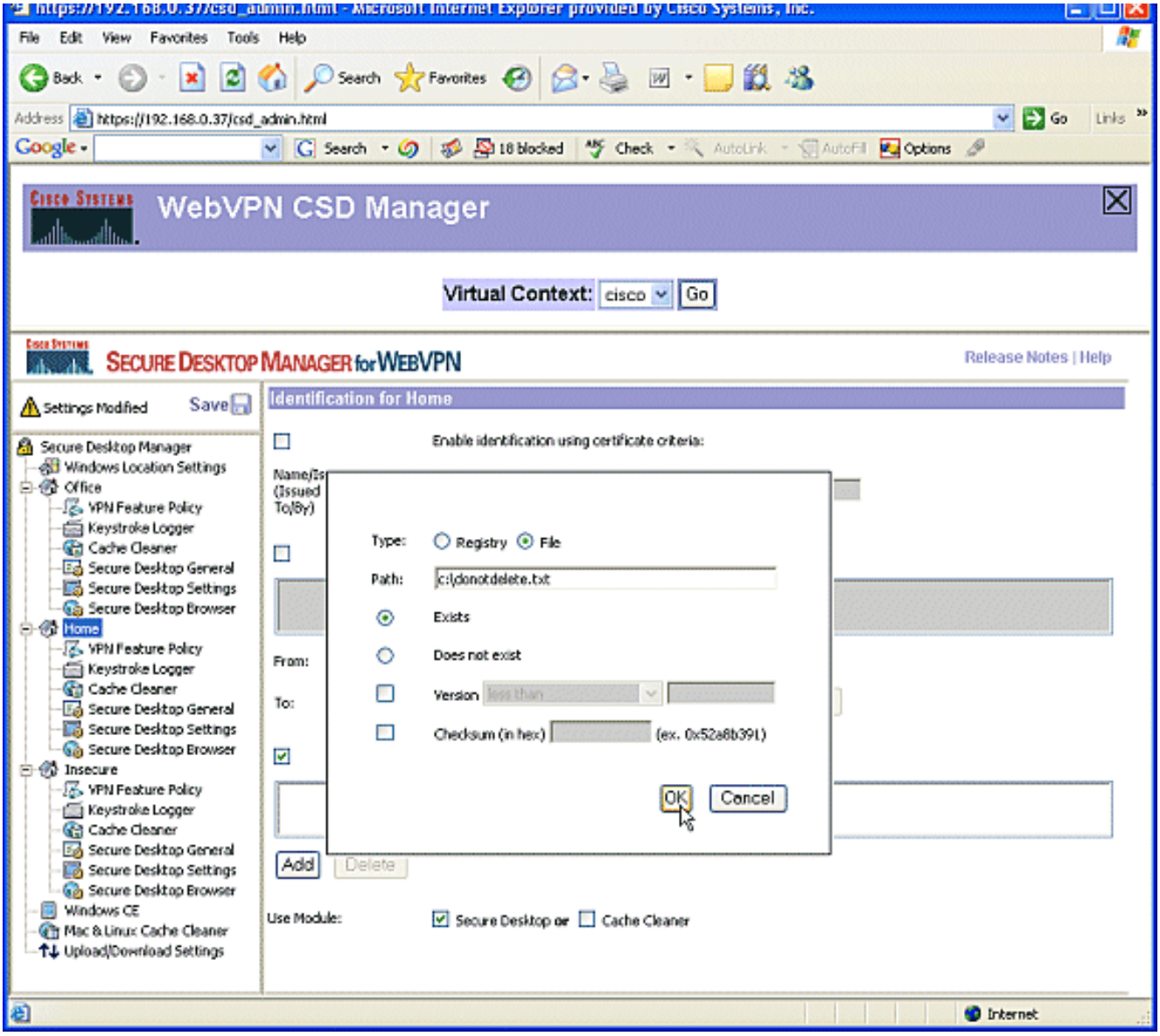
1. In the left pane, click **Office**.You can identify a Windows location with certificate criteria, IP criteria, a file, or registry criteria. You can also choose the Secure Desktop or Cache Cleaner for these clients. Since these users are internal office workers, identify them with IP criteria.Enter the IP address ranges in the **From** and **To** boxes.Click **Add**. Uncheck **Use Module: Secure Desktop**.When prompted, click **Save**, and click **OK**.



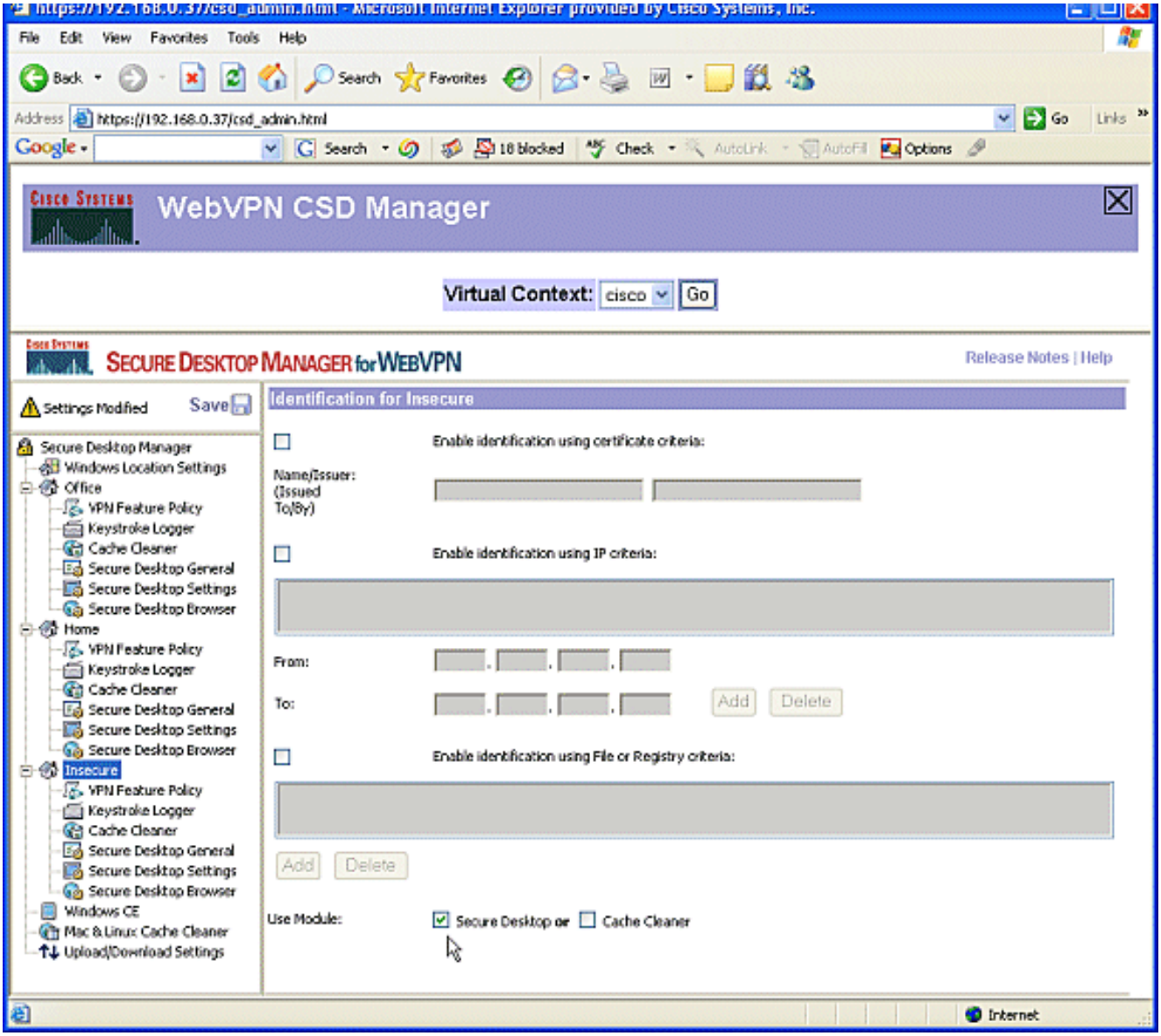

2. In the left pane, click the second Windows Location Setting **Home**.Make sure **Use Module: Secure Desktop** is checked.A file will be distributed that identifies these clients. You could choose to distribute certificates and/or registry criteria for these users.Check **Enable identification using File or Registry criteria**.Click **Add**.




3. In the dialog box, choose **File**, and enter the path to the file.This file must be distributed to all your home clients.Check the radio button **Exists**.When prompted, click **OK** , and click **Save**.



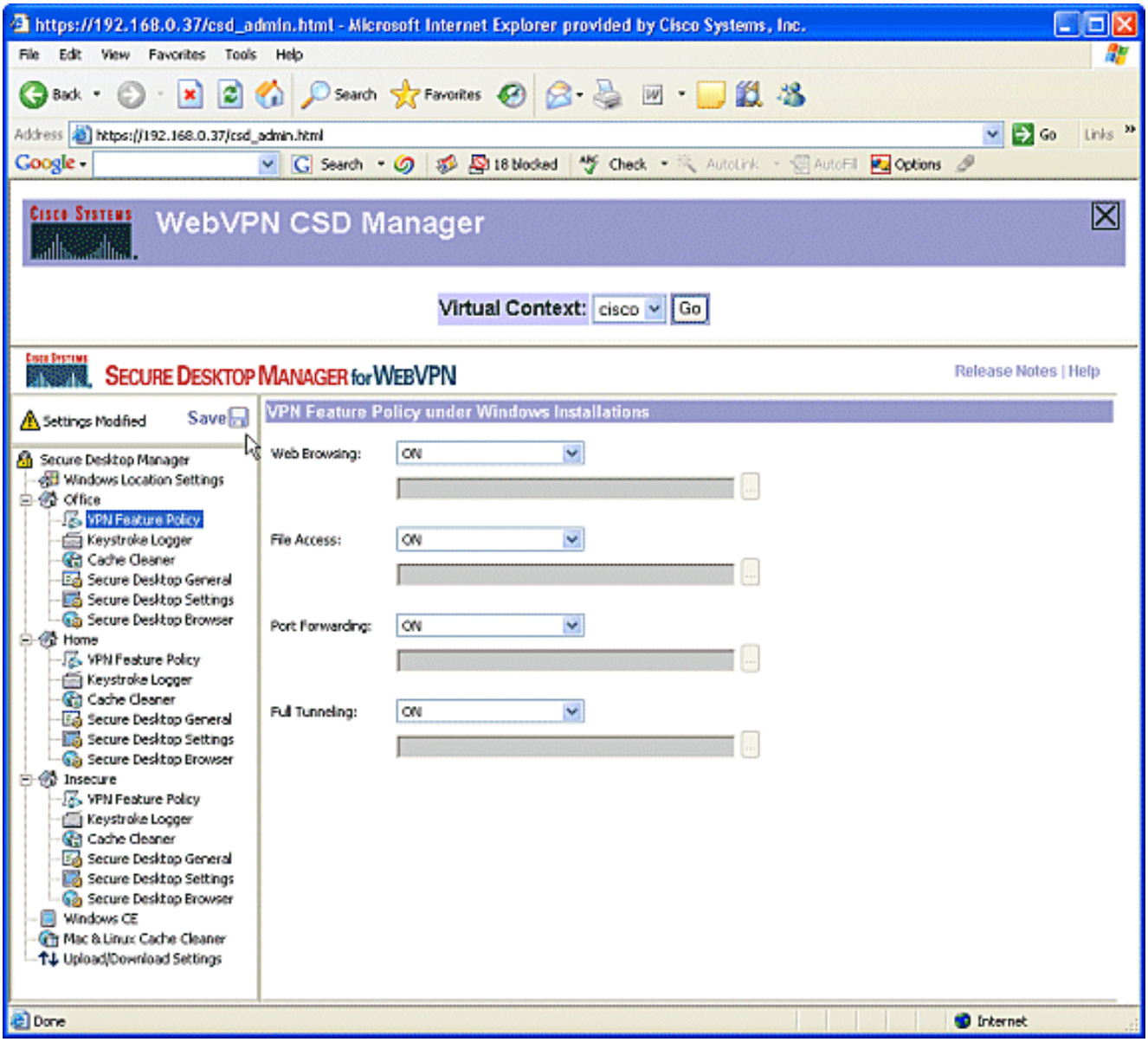

4. To configure the identification of **Insecure** locations, simply do not apply any identifying criteria.Click **Insecure** in the left pane.Leave all the criteria unchecked.Check **Use Module: Secure Desktop**.When prompted, click **Save**, and click **OK**.



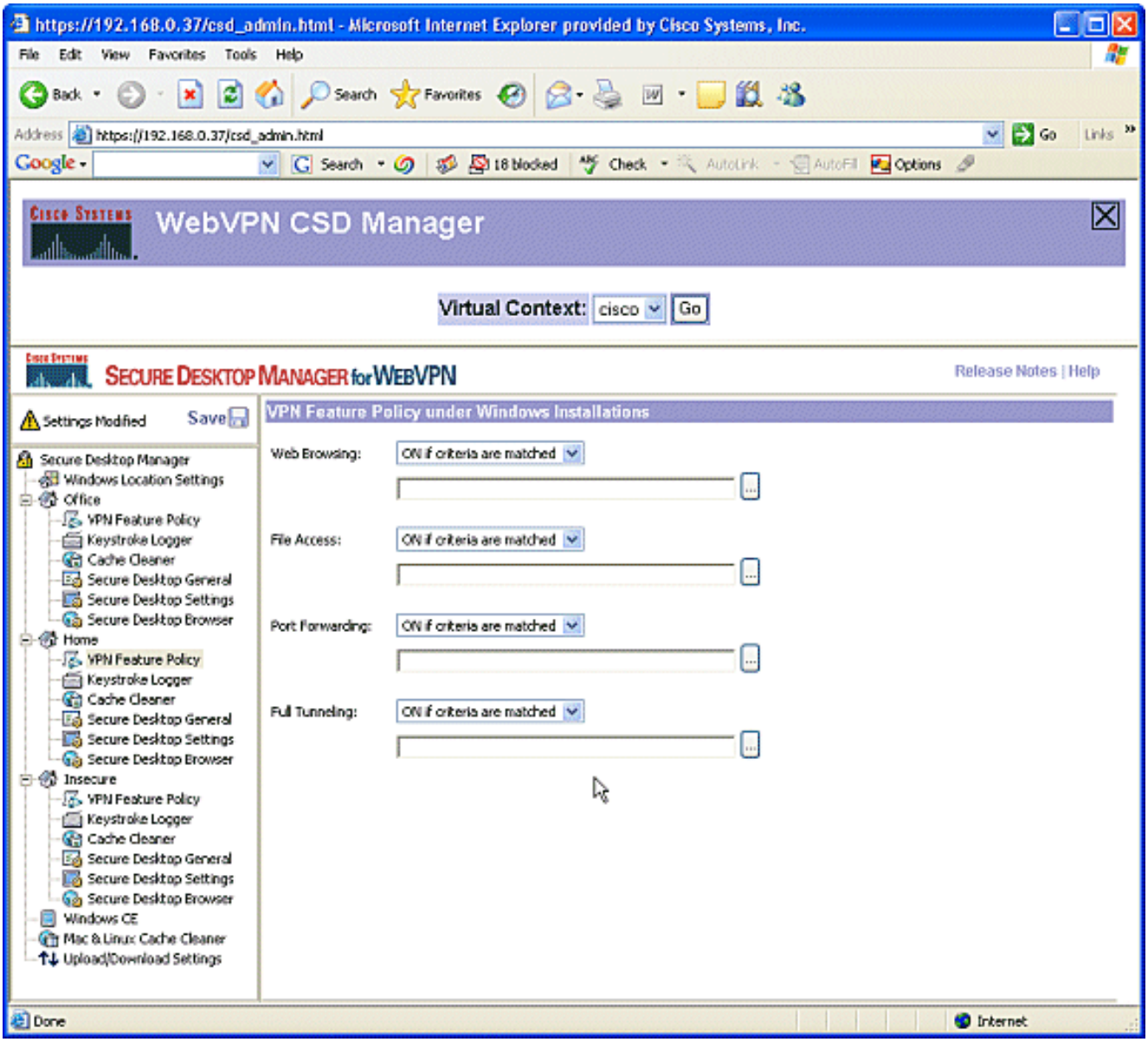

## Phase II: Step 3: Configure Windows location modules and features.

Configure the CSD features for each Windows location.

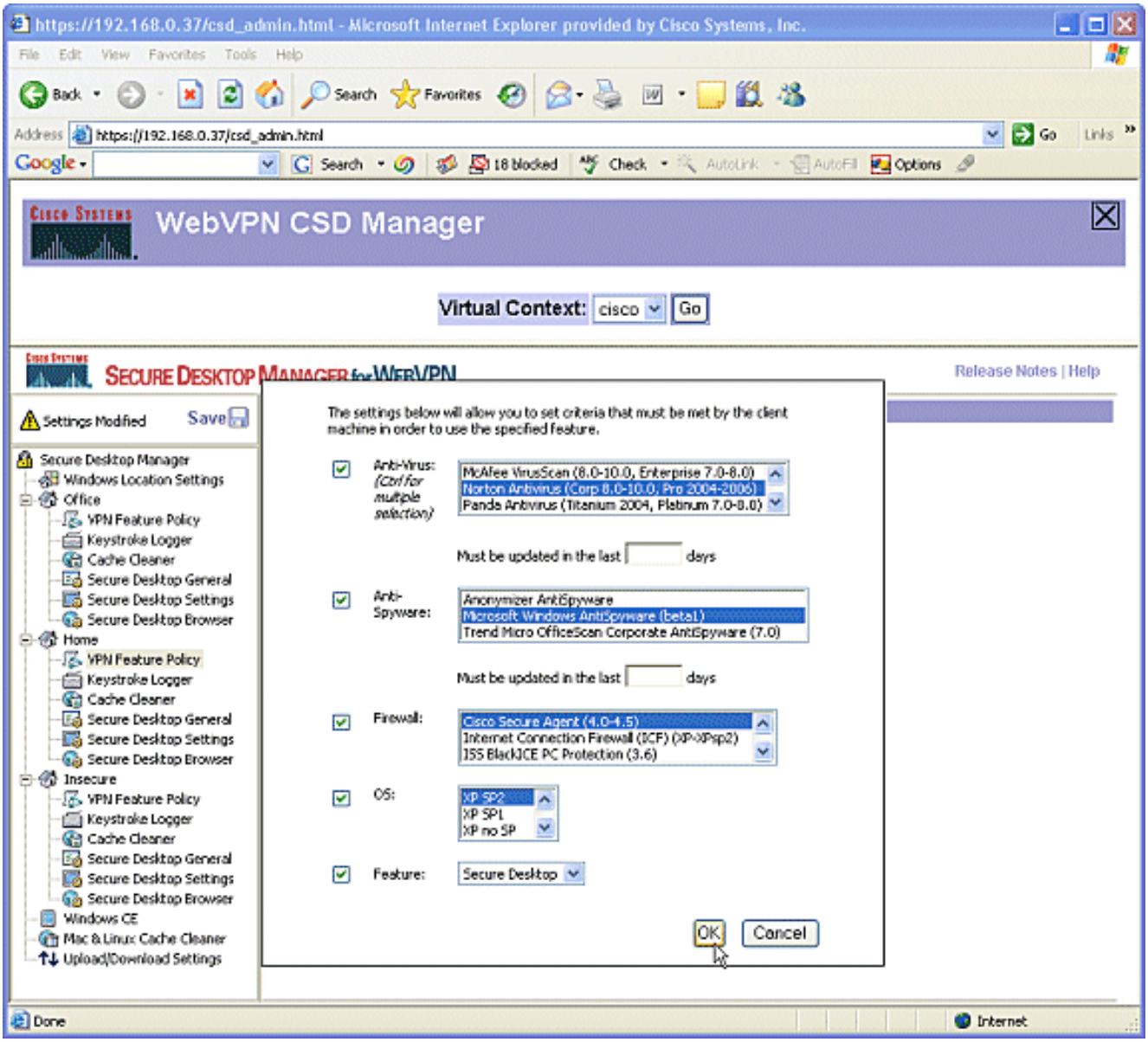
1. Under **Office**, click **VPN Feature Policy**. Since these are trusted internal clients, neither CSD nor Cache Cleaner was enabled. None of the other parameters is available.



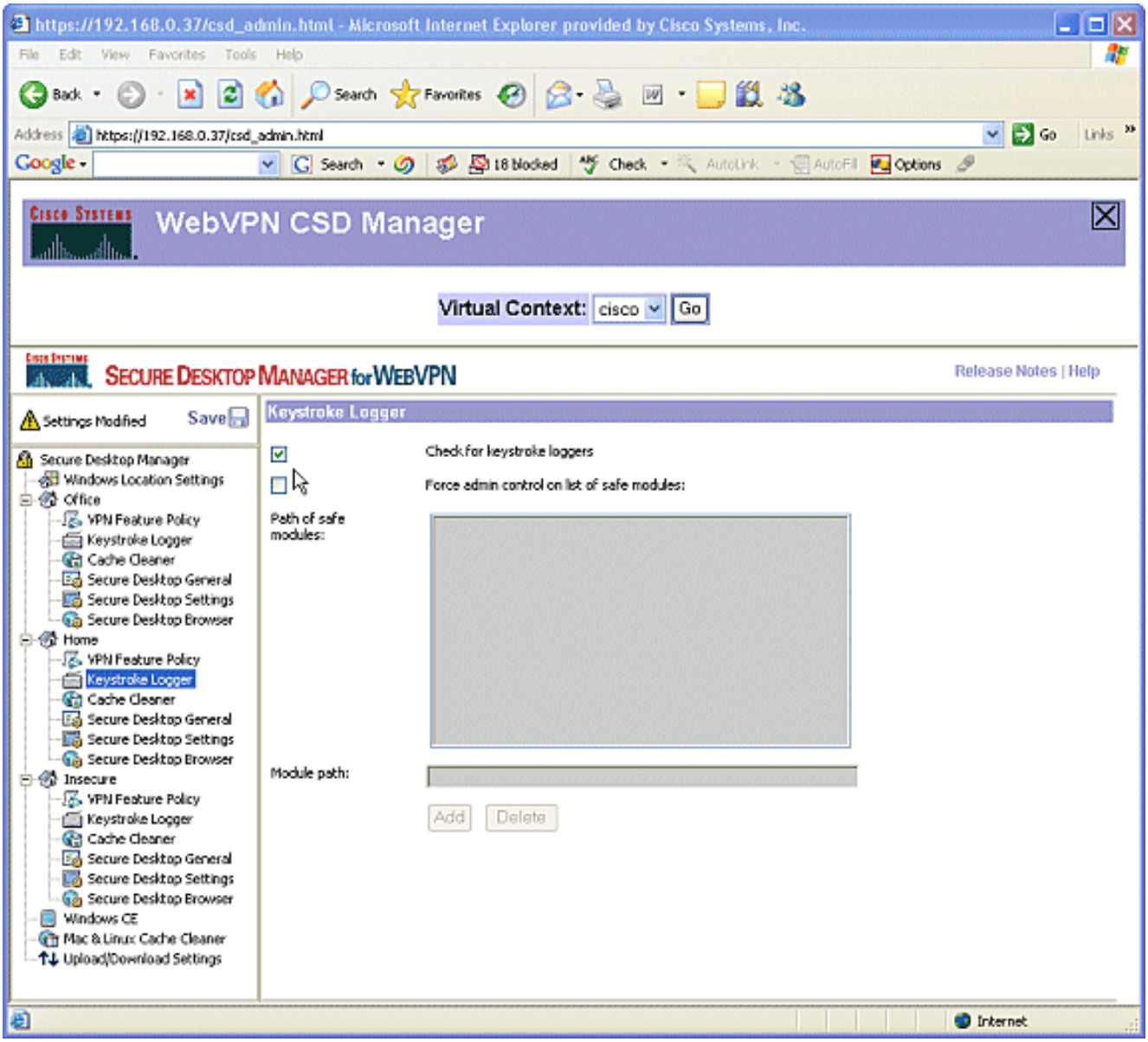

2. Turn on the features as shown.In the left pane, choose **VPN Feature Policy** under **Home**.Home users will be allowed access to the corporate LAN if the clients meet certain criteria.Under each method of access, choose **ON if criteria are matched**.



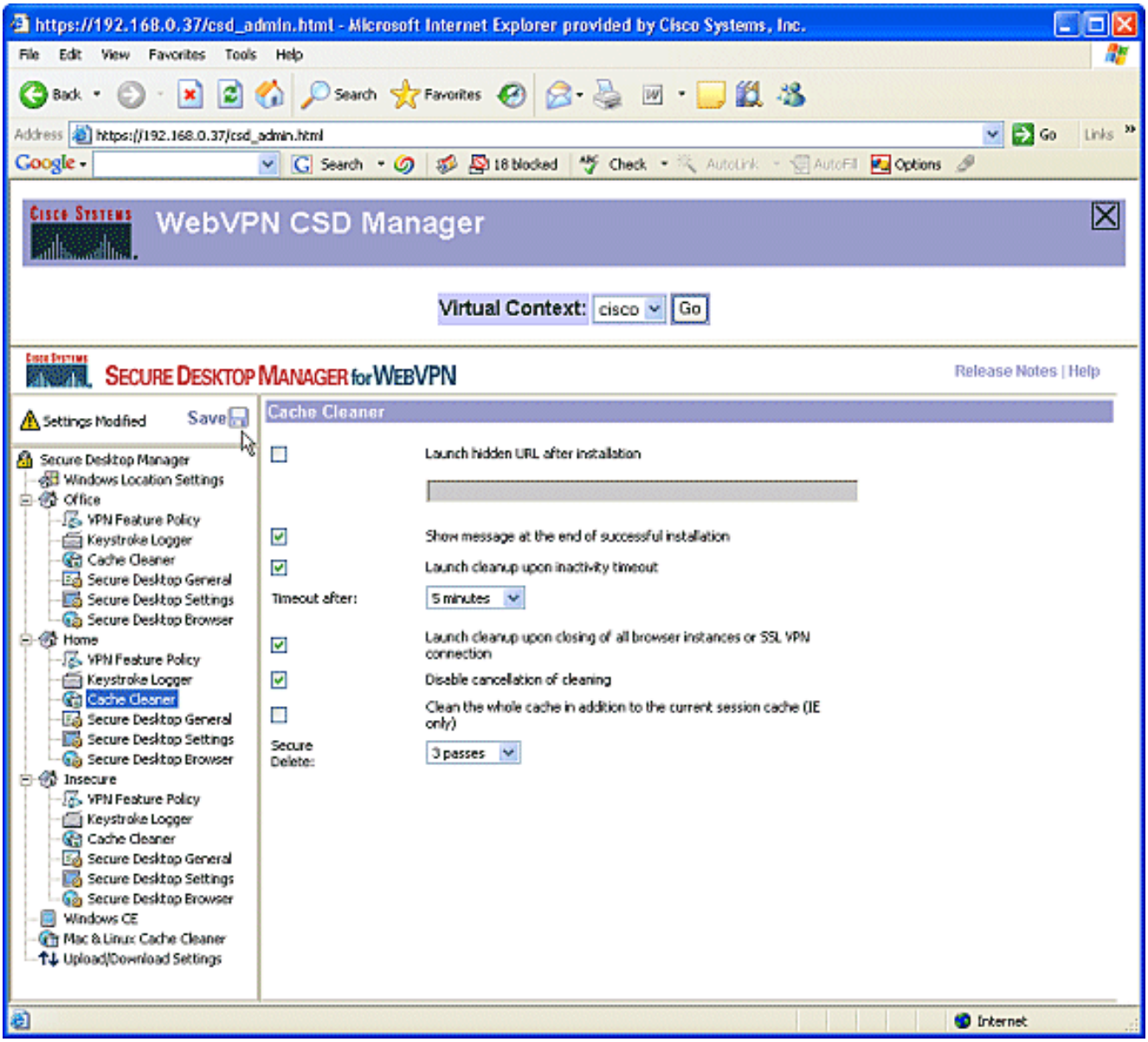

3. For Web Browsing, click the ellipsis button and choose the criteria that must match. Click **OK** in the dialog
box.



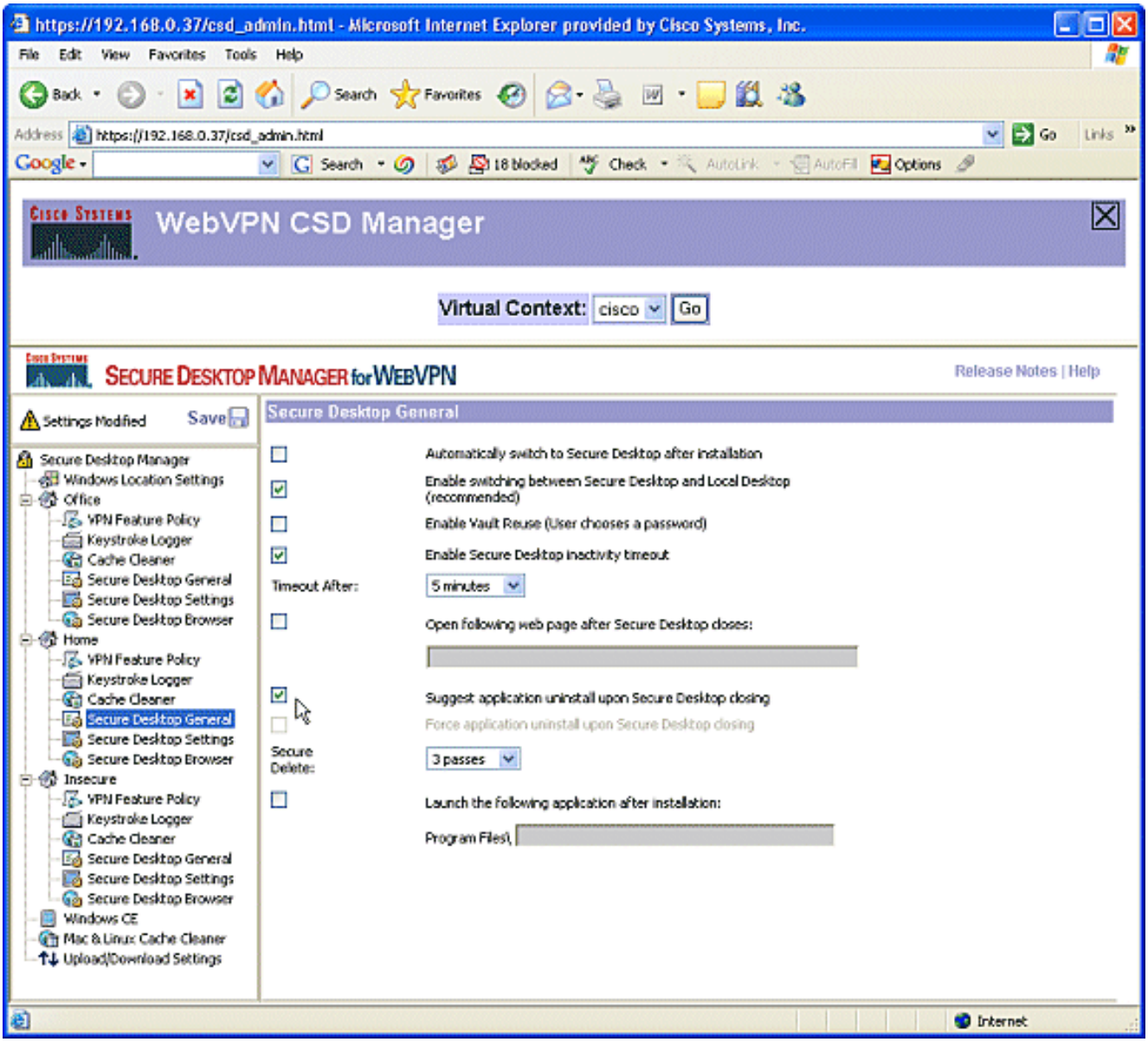

4. You can configure the other access methods in a similar fashion.Under **Home**, choose **Keystroke Logger**.Place a check mark next to **Check for keystroke loggers**.When prompted, click **Save**, and click **OK**.



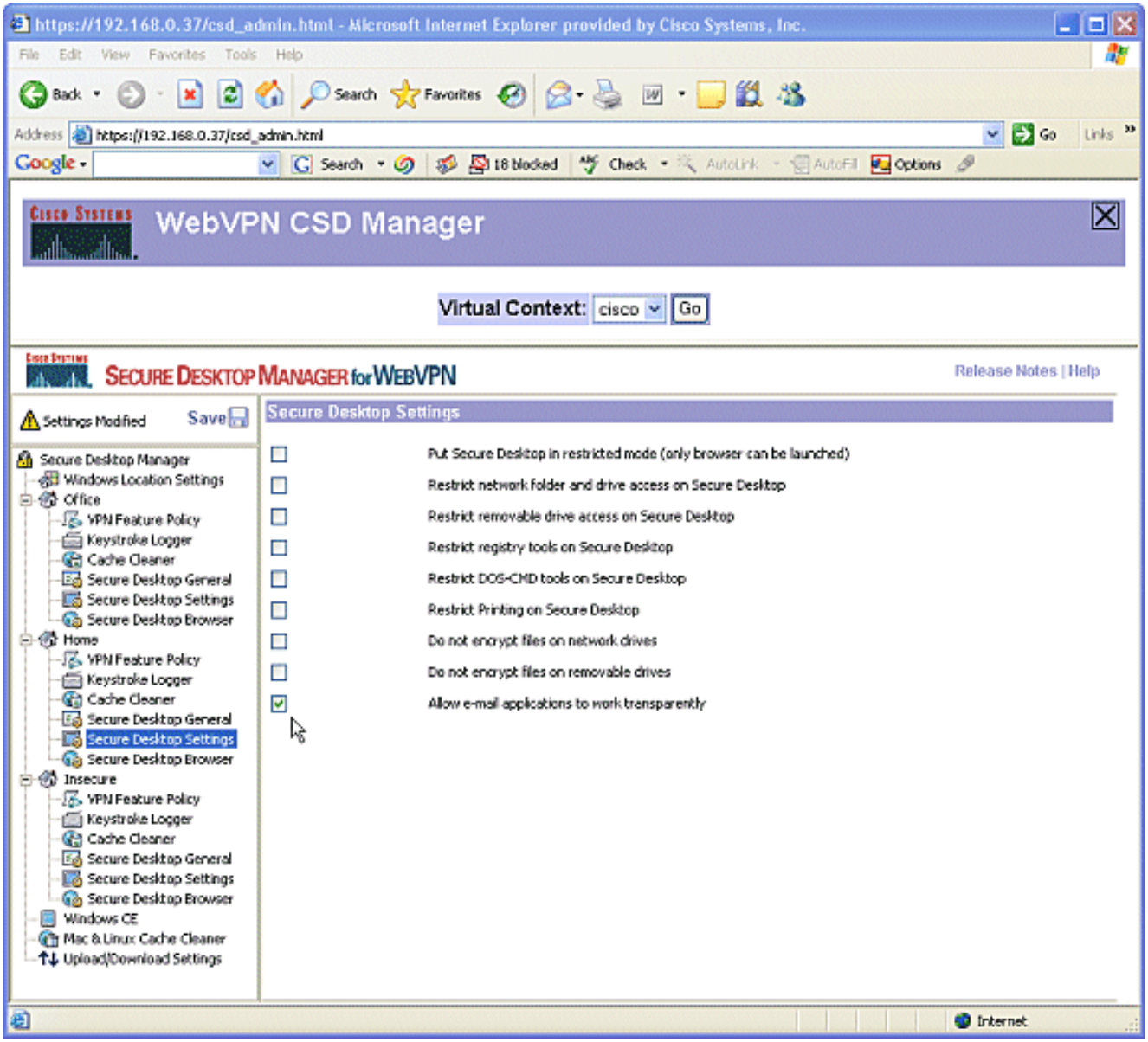

5. Under the Home windows location, choose **Cache Cleaner**. Leave the default settings as shown in the screen
shot.



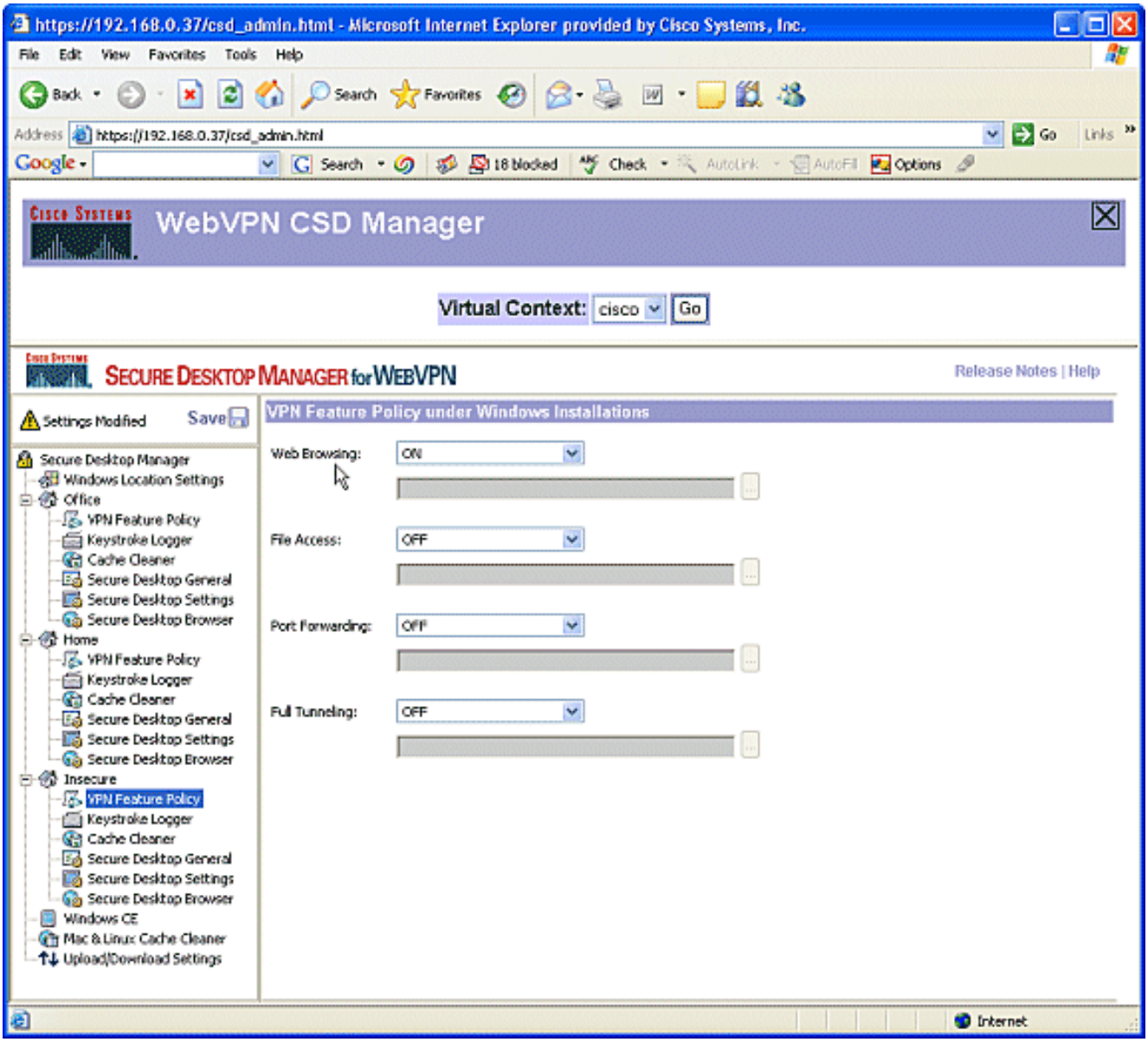

6. Under Home, choose **Secure Desktop General**. Check **Suggest application uninstall upon Secure Desktop closing**. Leave all other parameters at their default settings as shown in the screen
shot.



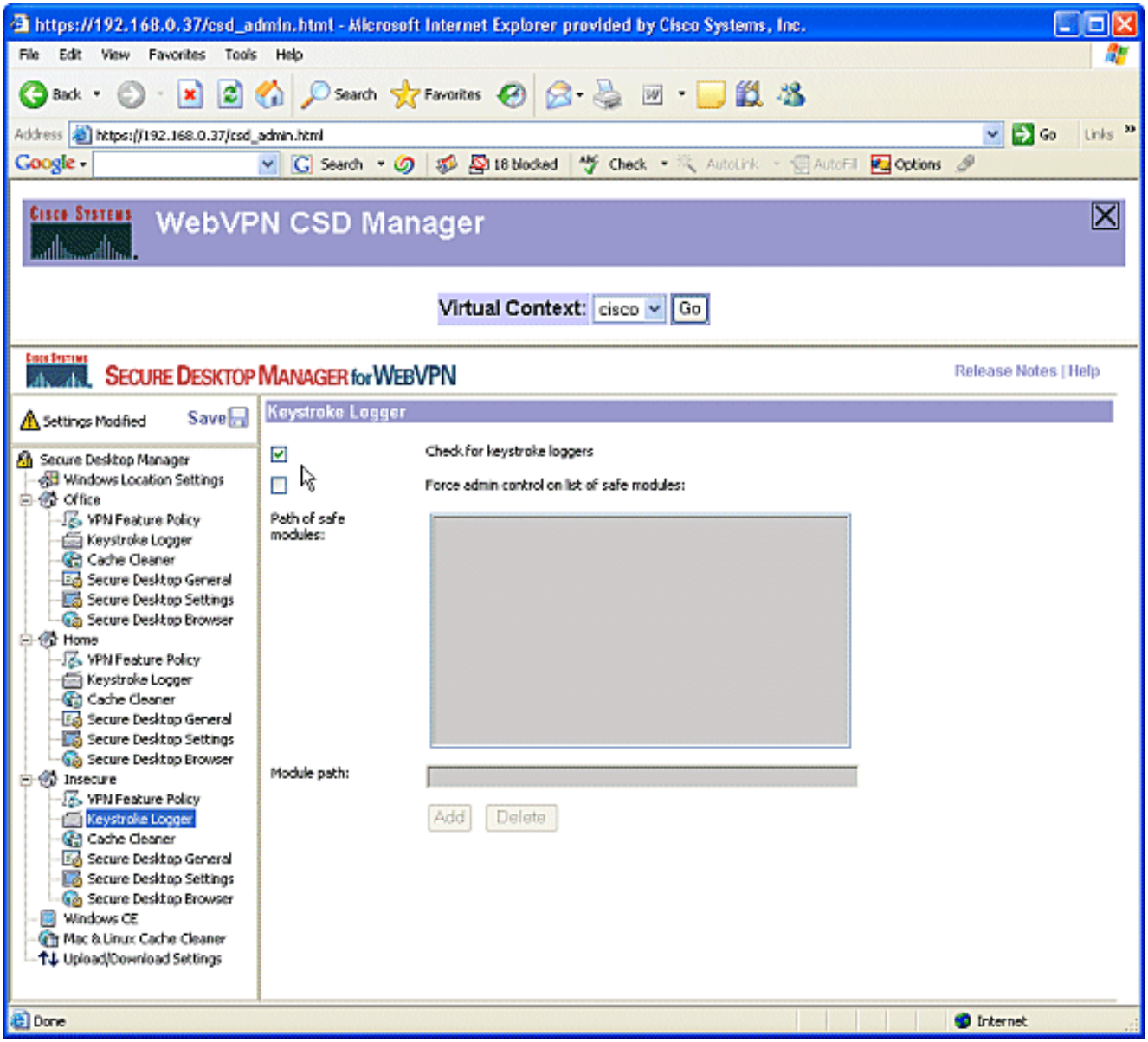

7. For Secure Desktop Settings under Home, choose **Allow e-mail applications to work transparently**. When prompted, click **Save**, and click **OK**.



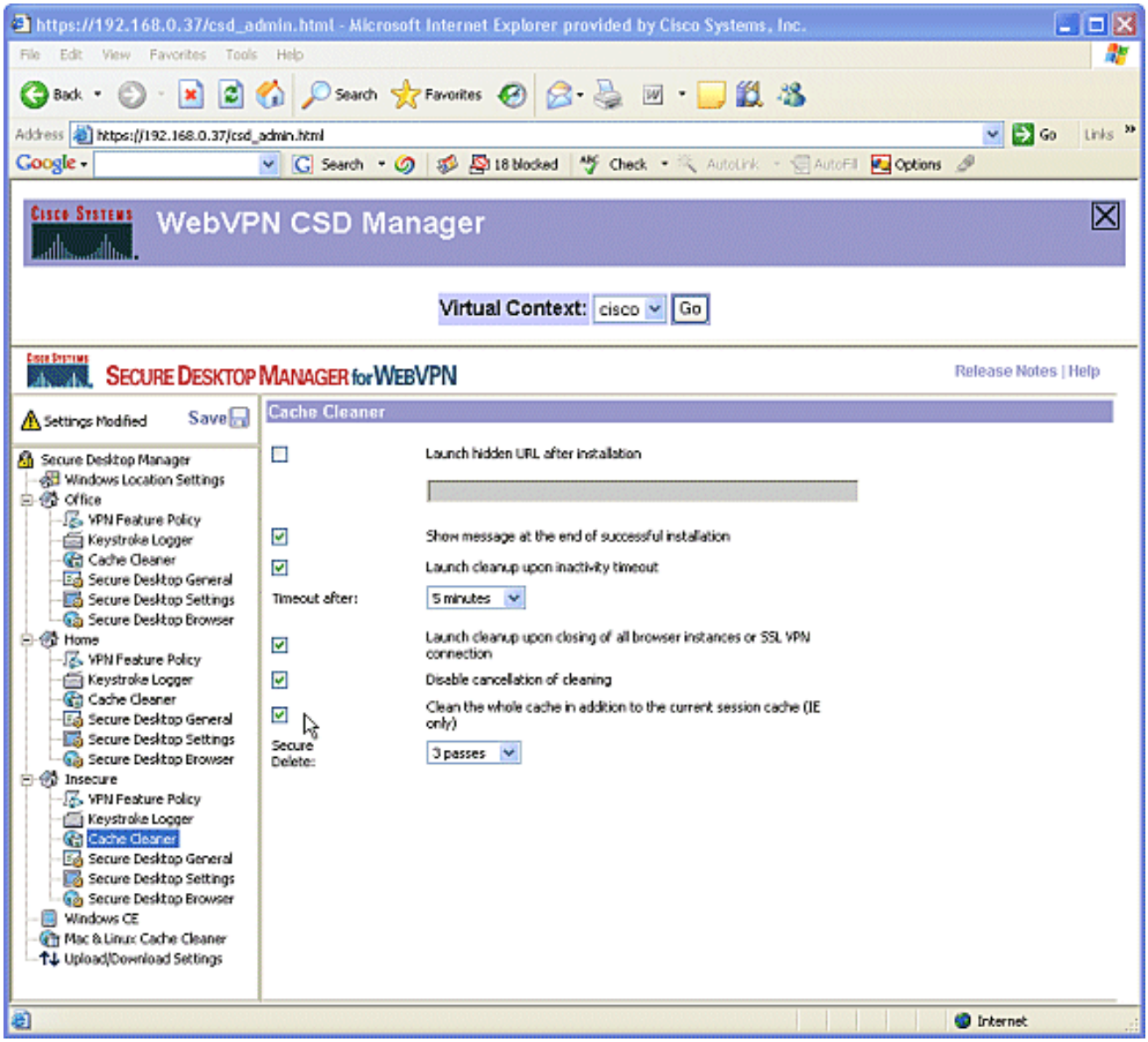

8. The configuration of **Secure Desktop Browser** is dependent upon whether or not you want these users to access a company website with preconfigured favorites.Under Insecure, choose **VPN Feature Policy**.Because these are not trusted users, allow only web browsing.Choose **ON** from the drop-down menu for **Web Browsing**.All other access is set to **OFF**.



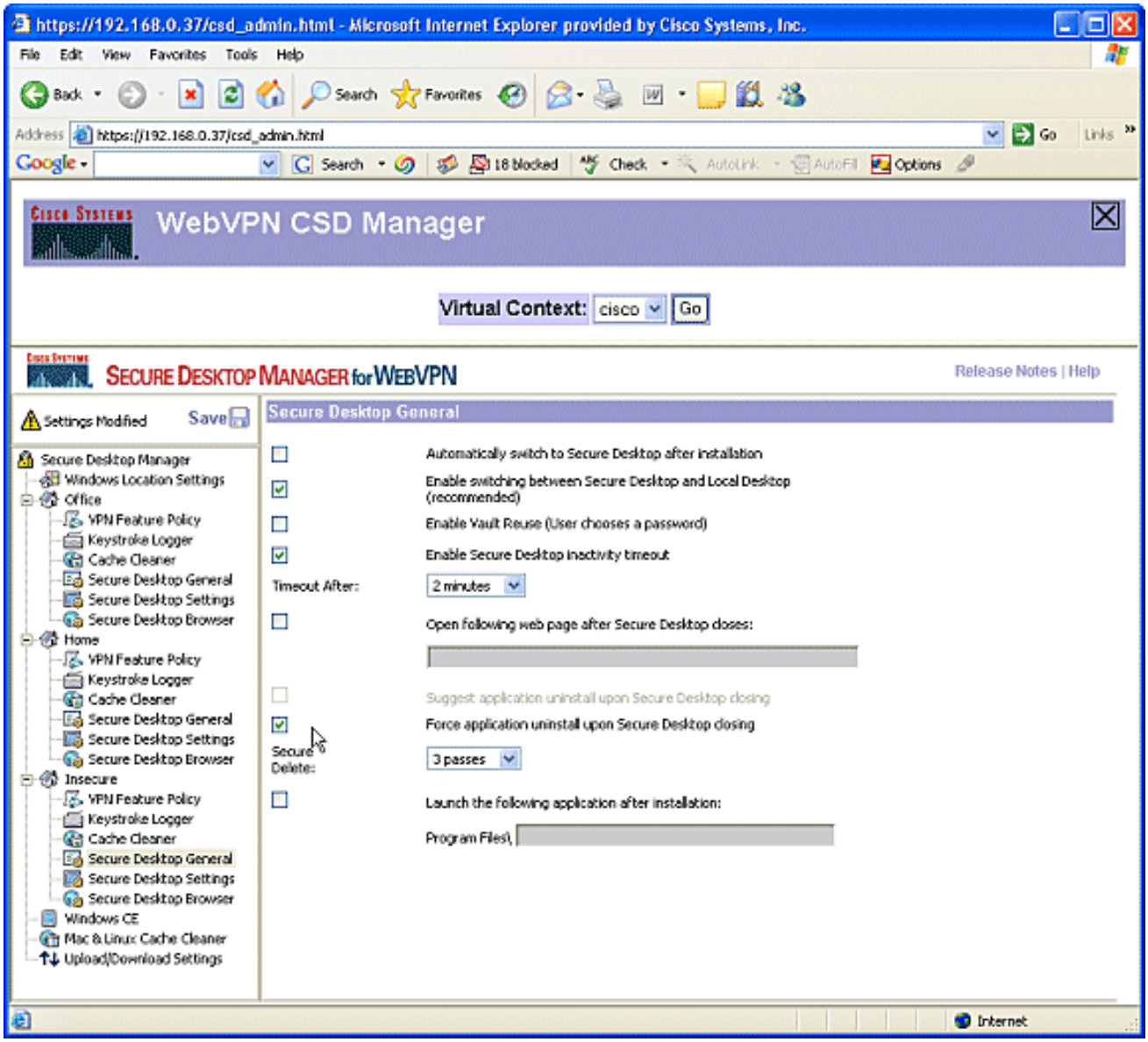

9. Check the **Check for keystroke loggers** check box.



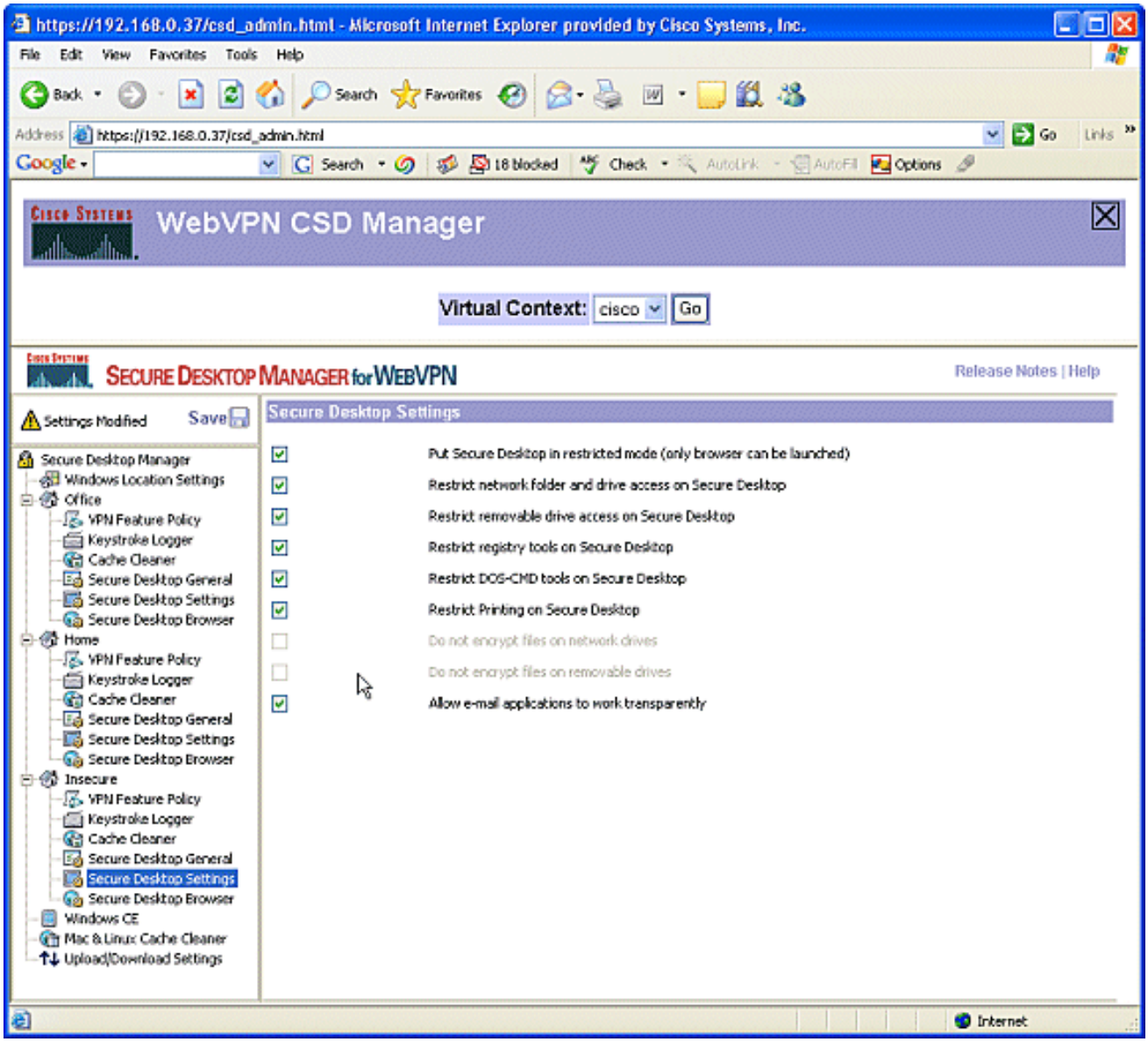

10. Configure the Cache Cleaner for Insecure.Check the **Clean the whole cache in addition to the current session cache (IE only)** check box.Leave the other settings at their defaults.



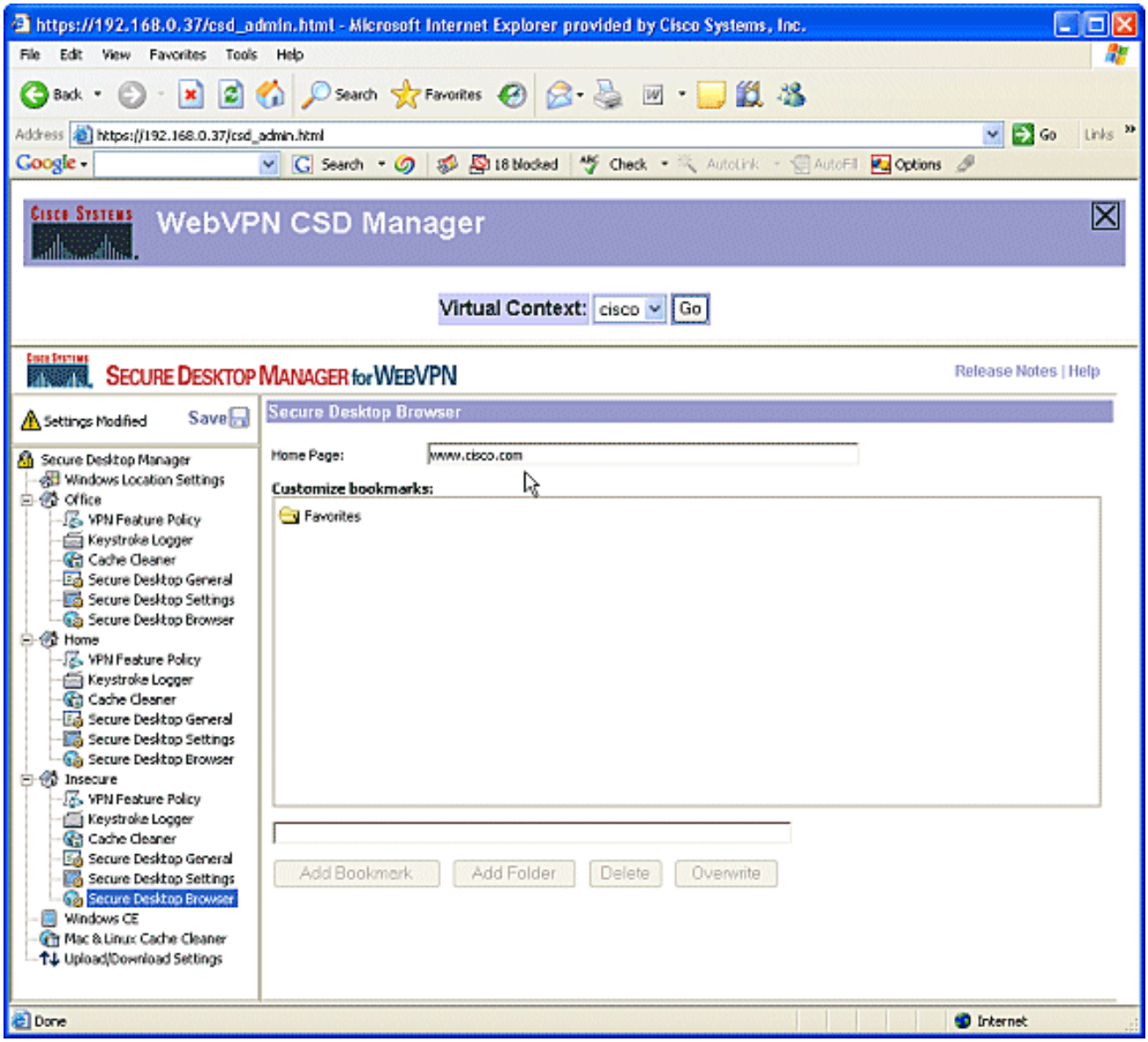

11. Under Insecure, choose **Secure Desktop General**.Reduce the time-out inactivity to 2 minutes.Check the **Force application uninstall upon Secure Desktop closing** check box.




12. Choose **Secure Desktop Settings** under Insecure, and configure very restrictive settings as
shown.



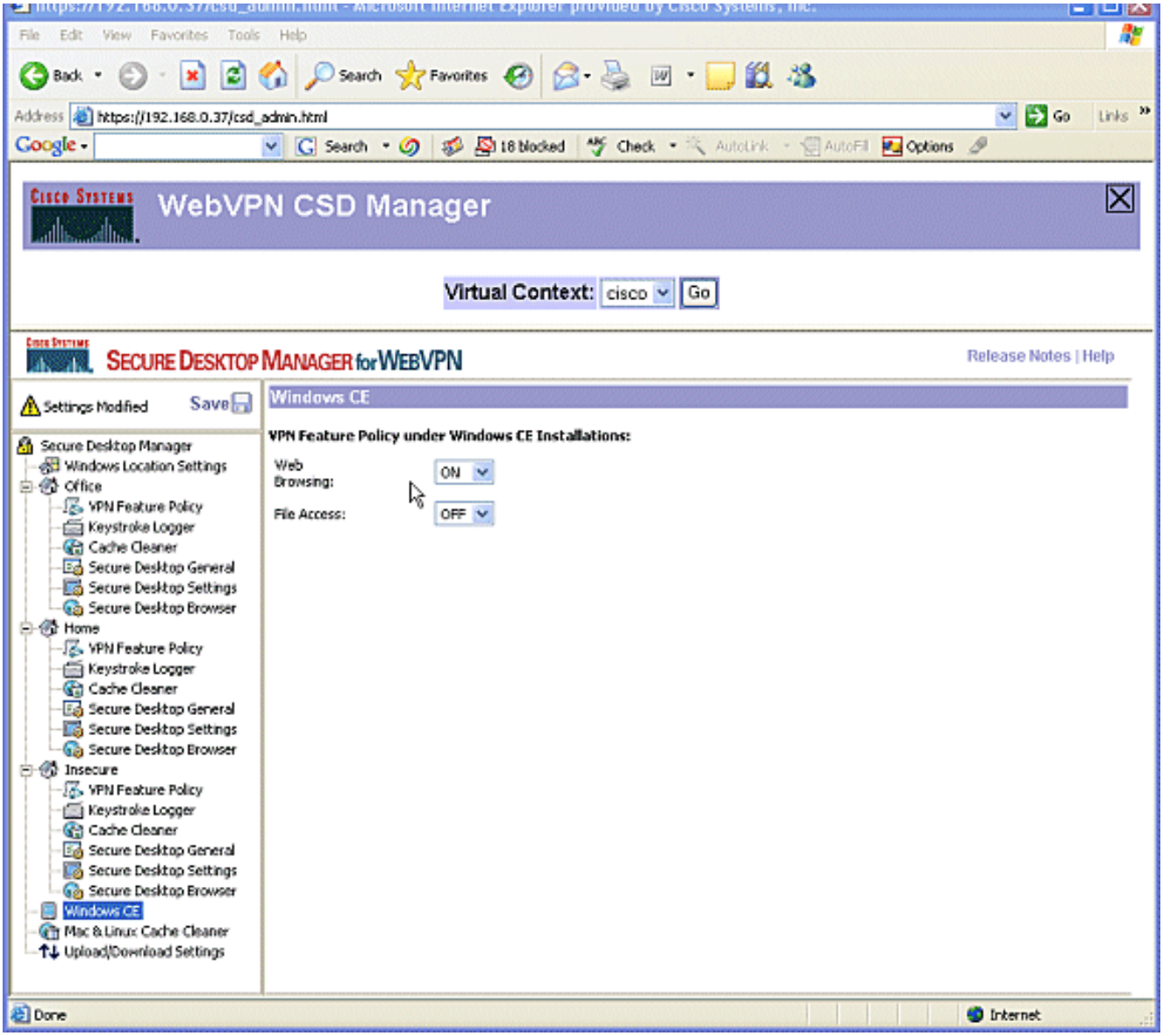

13. Choose **Secure Desktop Browser**. In the Home Page field, enter the website to which these clients will be guided for their home page.



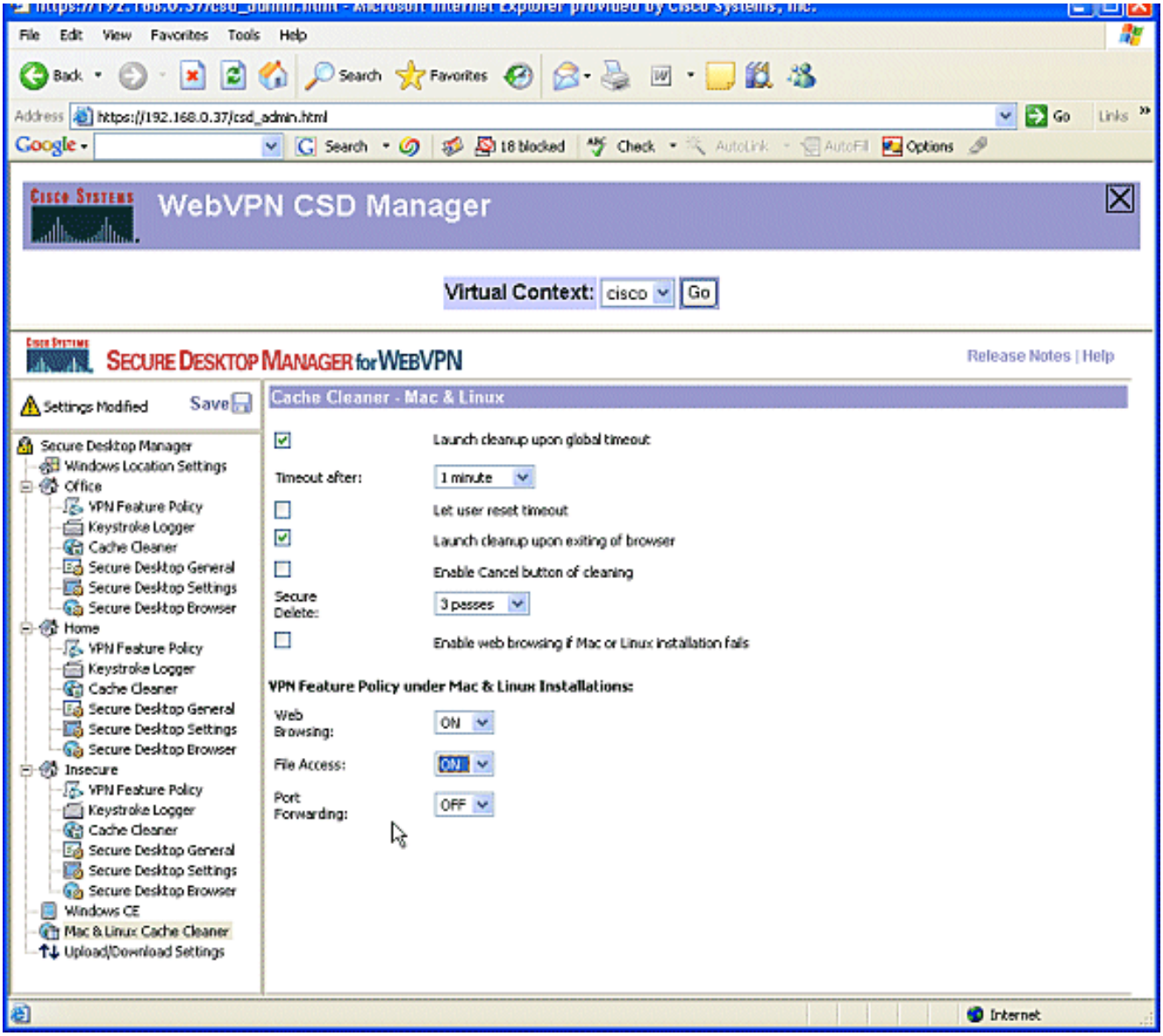

## Phase II: Step 4: Configure Windows CE, Macintosh, and Linux features.

Configure the CSD features for Windows CE, Macintosh, and Linux.

1. Choose **Windows CE** under Secure Desktop Manager. Windows CE has limited VPN features. Turn **Web Browsing to ON**.




2. Choose **Mac & Linux Cache Cleaner**.The Macintosh and Linux Operating Systems have access only to the cache cleaner aspects of CSD. Configure them as shown in the graphic.When prompted, click **Save**, and click **OK**.

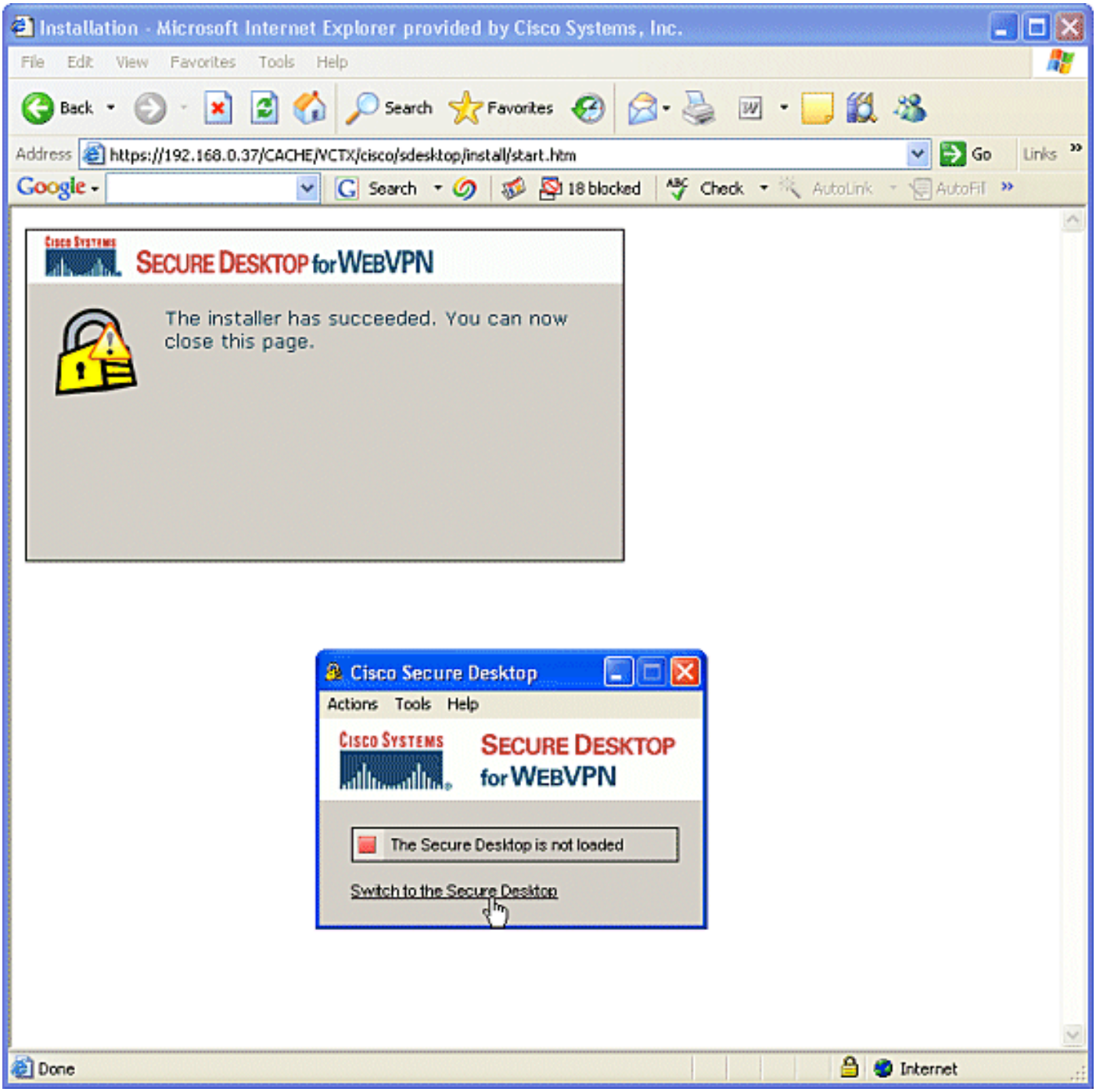



# Verify

## Test the CSD Operation

Test the operation of CSD by connecting to the WebVPN gateway with an SSL enabled browser at **https://WebVPN_Gateway_IP Address**.

**Note:** Remember to use the unique name of the context if you created different WebVPN contexts, for example, **https://192.168.0.37/cisco**.




### Commands

Several **show** commands are associated with WebVPN. You can execute these commands at the command-line interface (CLI) to show statistics and other information. For detailed information about **show** commands, refer to Verifying WebVPN Configuration.

**Note:** The CLI Analyzer (registered customers only) supports certain **show** commands. Use the CLI Analyzer to view an analysis of **show** command output.

## Troubleshoot

### Commands

Several **debug** commands are associated with WebVPN. For detailed information about these

commands, refer to Using WebVPN Debug Commands.

**Note:** The use of **debug** commands can adversely impact your Cisco device. Before you use **debug** commands, refer to Important Information on Debug Commands.

For more information about **clear** commands, refer to Using WebVPN Clear commands.

## Related Information

- **WebVPN and DMVPN Convergence Deployment Guide**
- **SSL VPN - WebVPN**
- **Cisco IOS SSLVPN**
- **Technical Support & Documentation - Cisco Systems**