Configurazione di CSD su Cisco IOS con SDM

Sommario

Introduzione

Sebbene le sessioni VPN (Cisco WebVPN) Secure Sockets Layer (SSL) siano protette, il client potrebbe comunque disporre di cookie, file del browser e allegati di posta elettronica rimanenti al termine di una sessione. Cisco Secure Desktop (CSD) estende la sicurezza intrinseca delle sessioni VPN SSL scrivendo i dati della sessione in formato crittografato in una speciale area di vaulting del disco del client. Inoltre, questi dati vengono rimossi dal disco al termine della sessione VPN SSL. Questo documento presenta una configurazione di esempio per CSD su un router Cisco IOS®.

CSD è supportato sulle seguenti piattaforme per dispositivi Cisco:

- Router Cisco IOS versione 12.4(6)T e successive
- Cisco 870,1811,1841, 2801, 2811, 2821, 2851, 3725, 3745, 3825, 3845, 7200 e 7301 router

- Cisco VPN serie 3000 concentrator versione 4.7 e successive
- Cisco ASA serie 5500 Security Appliance versione 7.1 e successive
- Cisco WebVPN Services Module per Cisco Catalyst e Cisco serie 7600 versione 1.2 e successive

Prerequisiti

Requisiti

Prima di provare questa configurazione, accertarsi di soddisfare i seguenti requisiti:

Requisiti per il router Cisco IOS

- Router Cisco IOS con Advanced Image 12.4(6T) o versioni successive
- Cisco Router Secure Device Manager (SDM) 2.3 o superiore
- Una copia del pacchetto CSD per IOS sulla stazione di gestione
- Certificato digitale autofirmato o autenticazione del router con un'Autorità di certificazione (CA)

  Nota: ogni volta che si utilizzano certificati digitali, accertarsi di impostare correttamente il nome host, il nome di dominio e il fuso orario/data del router.
- Una password segreta enable sul router
- DNS abilitato sul router. Diversi servizi WebVPN richiedono DNS per funzionare correttamente.

Requisiti per i computer client

- I client remoti devono disporre di privilegi amministrativi locali; non è necessario, ma è consigliabile.
- I client remoti devono disporre di Java Runtime Environment (JRE) versione 1.4 o successiva.
- Browser client remoti: Internet Explorer 6.0, Netscape 7.1, Mozilla 1.7, Safari 1.2.2 o Firefox 1.0
- Cookie attivati e popup consentiti su client remoti

Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

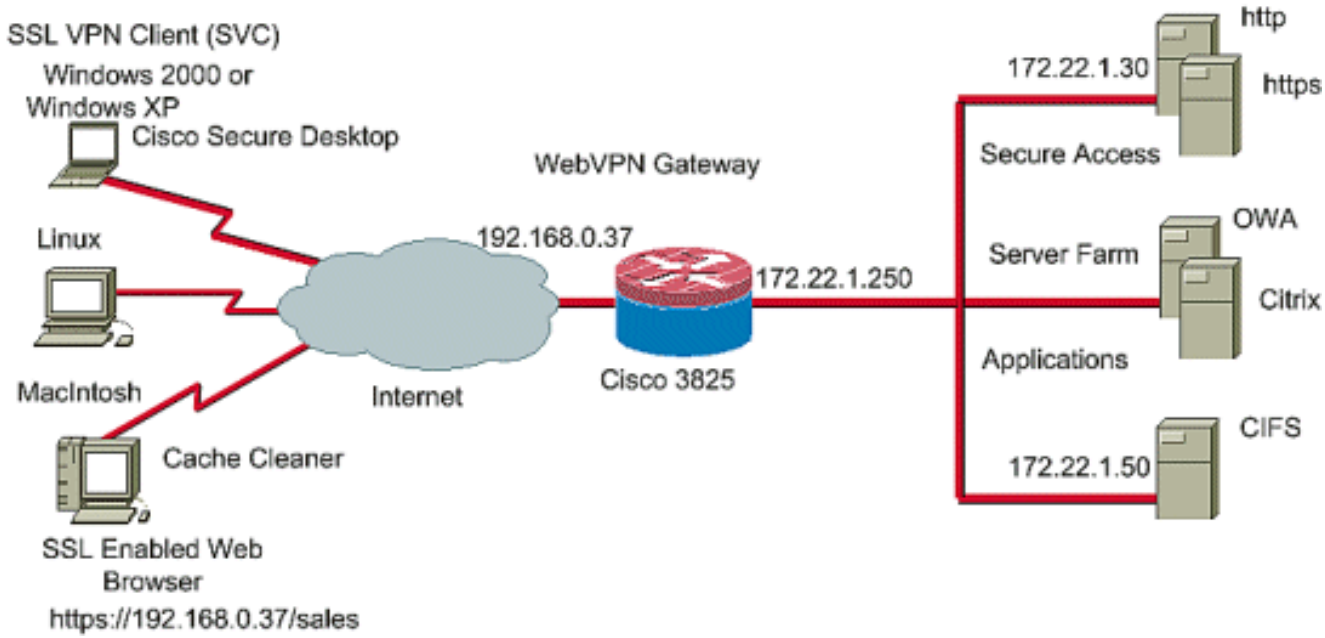
- Cisco IOS router 3825 con versione 12.9(T)
- SDM versione 2.3.1

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

Esempio di rete

Il documento usa la seguente configurazione di rete:

In questo esempio viene usato un router Cisco serie 3825 per consentire l'accesso sicuro alla Intranet aziendale. Il router Cisco serie 3825 migliora la sicurezza delle connessioni VPN SSL con caratteristiche e funzionalità CSD configurabili. I client possono connettersi al router abilitato per CSD tramite uno dei tre metodi VPN SSL seguenti: VPN SSL senza client (WebVPN), VPN SSL thin client (Port-Forwarding) o client VPN SSL (Full Tunneling SVC).



Prodotti correlati

La configurazione illustrata in questo documento può essere utilizzata nelle seguenti versioni hardware e software:

- piattaforme router Cisco 870,1811,1841,2801,2811,2821,2851,3725,3745,3825,3845, 7200 e 7301
- Cisco IOS Advanced Security Image versione 12.4(6)T e successive

Convenzioni

Fare riferimento a Cisco Technical Tips Conventions per ulteriori informazioni sulle convenzioni dei documenti.

Configurazione

Un gateway WebVPN consente a un utente di connettersi al router tramite una delle tecnologie VPN SSL. Nel dispositivo è consentito un solo gateway WebVPN per indirizzo IP, sebbene sia possibile collegare più contesti WebVPN a un gateway WebVPN. Ogni contesto è identificato da un nome univoco. I Criteri di gruppo identificano le risorse configurate disponibili per un particolare contesto WebVPN.

La configurazione del CSD su un router IOS è effettuata in due fasi:

Fase I: preparare il router per la configurazione del CSD con SDM

1. Configurare un gateway WebVPN, il contesto WebVPN e i Criteri di gruppo.

   Nota: questo passaggio è facoltativo e non viene descritto in dettaglio nel presente documento. Se il router è già stato configurato per una delle tecnologie VPN SSL, omettere questo passaggio.

2. Abilita CSD in un contesto WebVPN.

Fase II: configurare CSD utilizzando un browser Web.

1. Definisci percorsi Windows.
2. Identificare i criteri di posizione.
3. Configurare i moduli e le funzionalità di posizione di Windows.
4. Configurare le funzionalità di Windows CE, Macintosh e Linux.

Fase I: preparare il router per la configurazione del CSD con SDM.

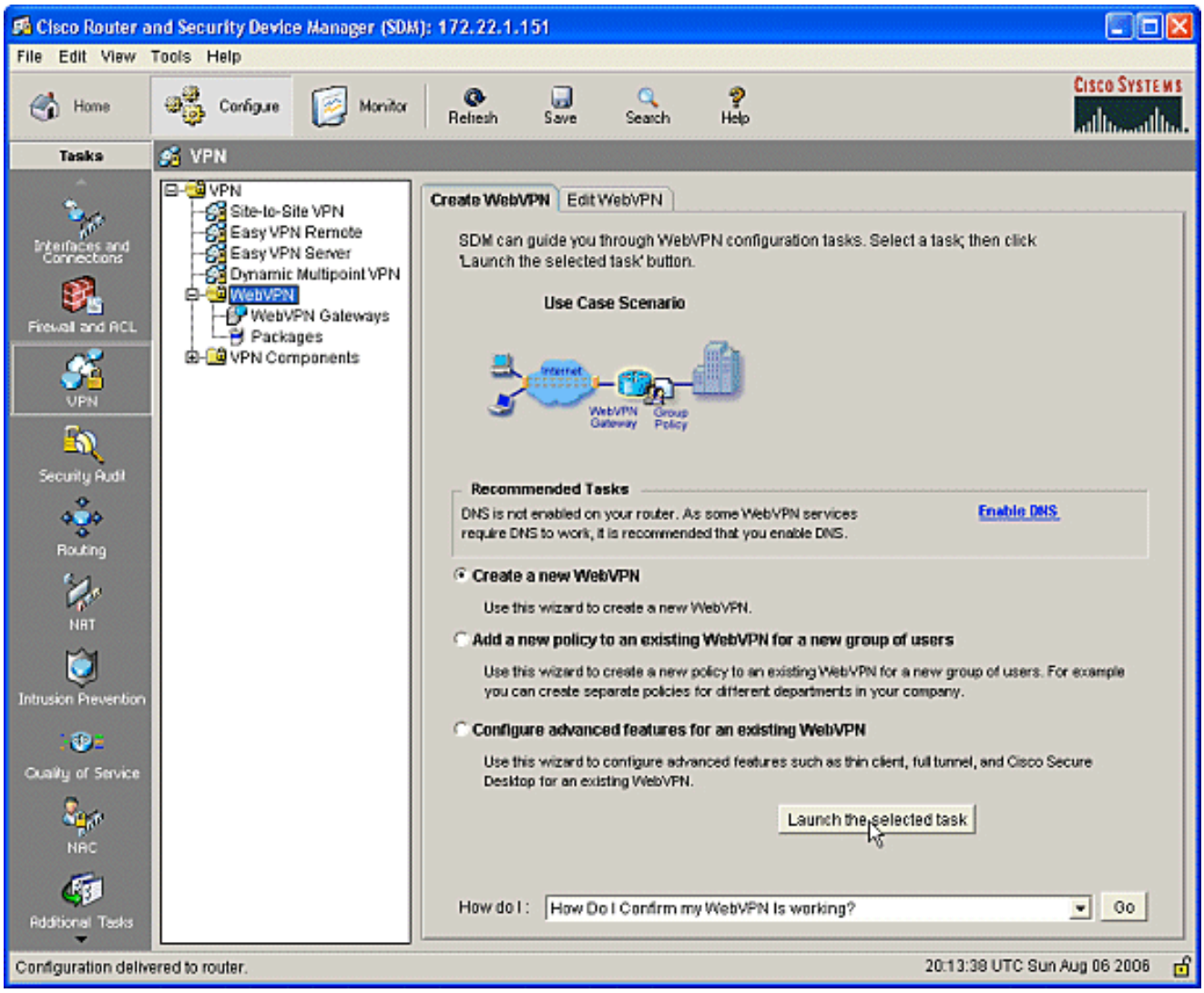
CSD può essere configurato con SDM o dall'interfaccia della riga di comando (CLI). Questa configurazione utilizza SDM e un browser Web.

Questa procedura viene utilizzata per completare la configurazione del CSD sul router IOS.

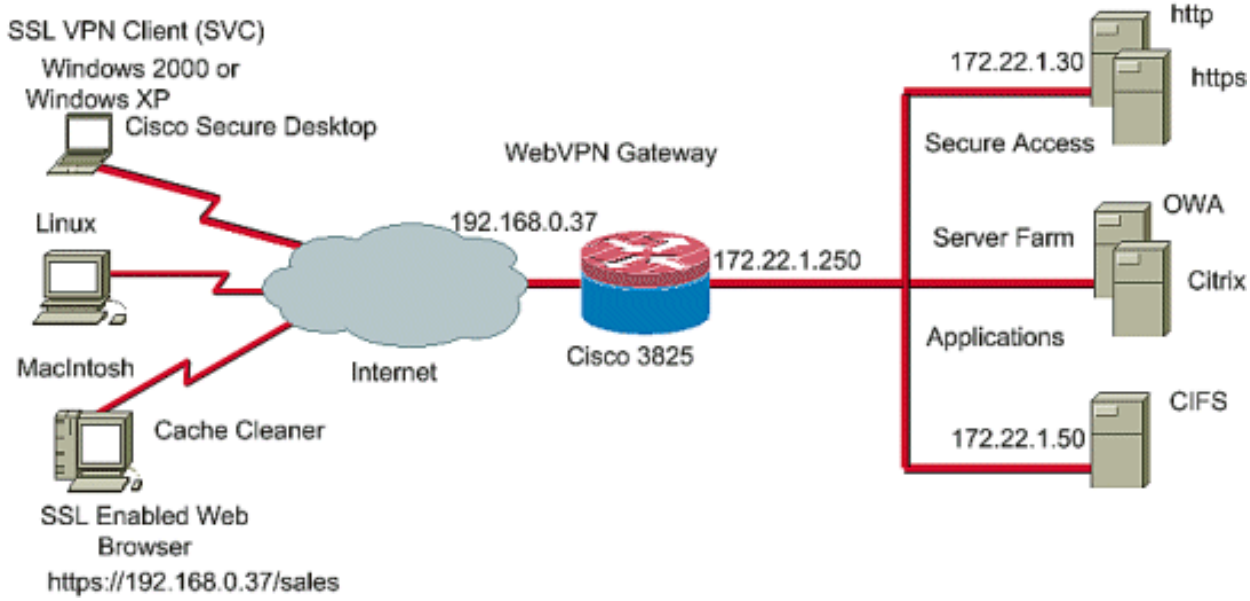
Fase I: configurare un gateway WebVPN, un contesto WebVPN e criteri di gruppo.

Per eseguire questa operazione, è possibile utilizzare la Creazione guidata WebVPN.

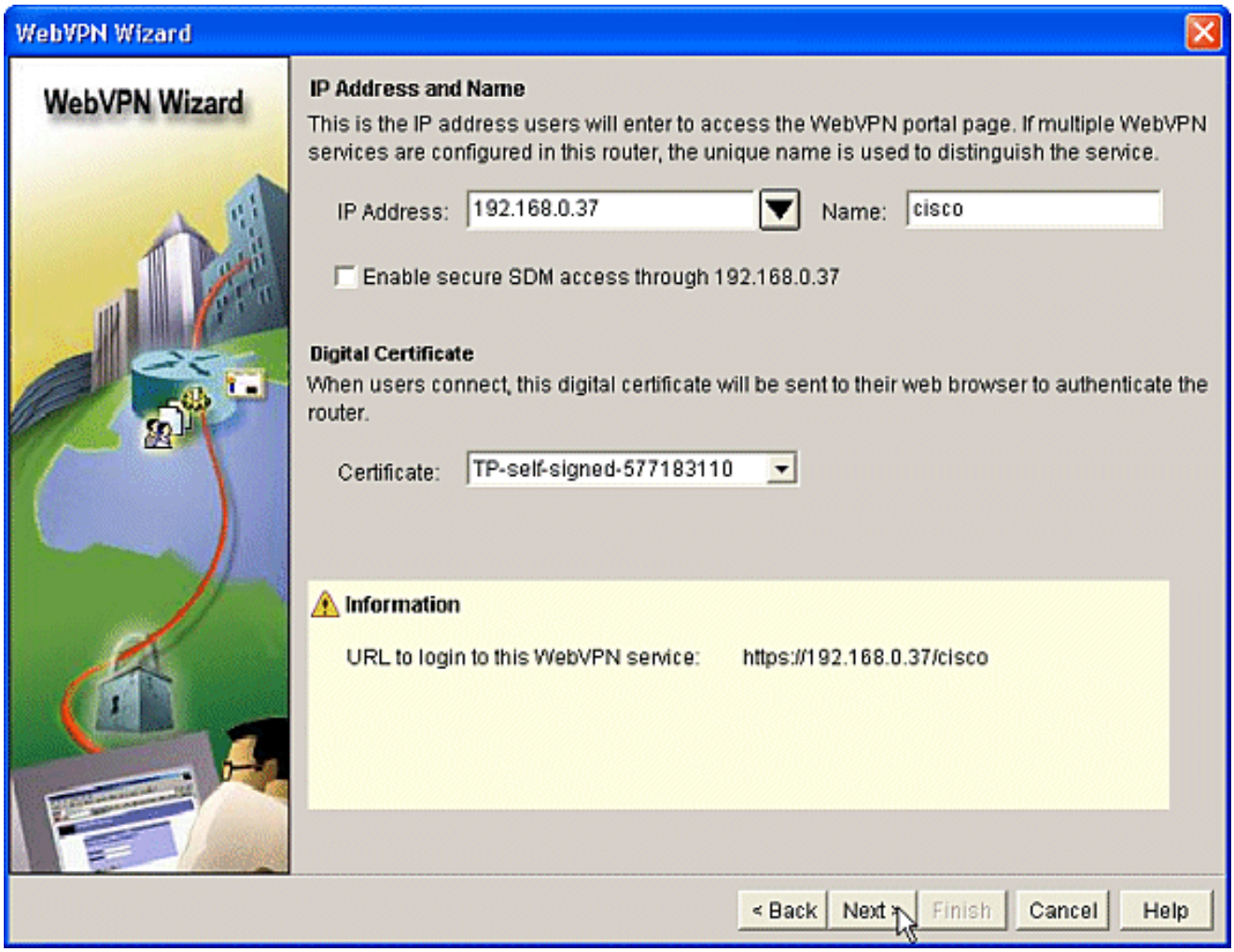
1. Aprire SDM e selezionare Configure > VPN > WebVPN. Fare clic sulla scheda Create WebVPN (Crea VPN Web) e selezionare il pulsante di opzione Create a new WebVPN (Crea una nuova VPN Web). Fare clic su Avvia l'attività selezionata.



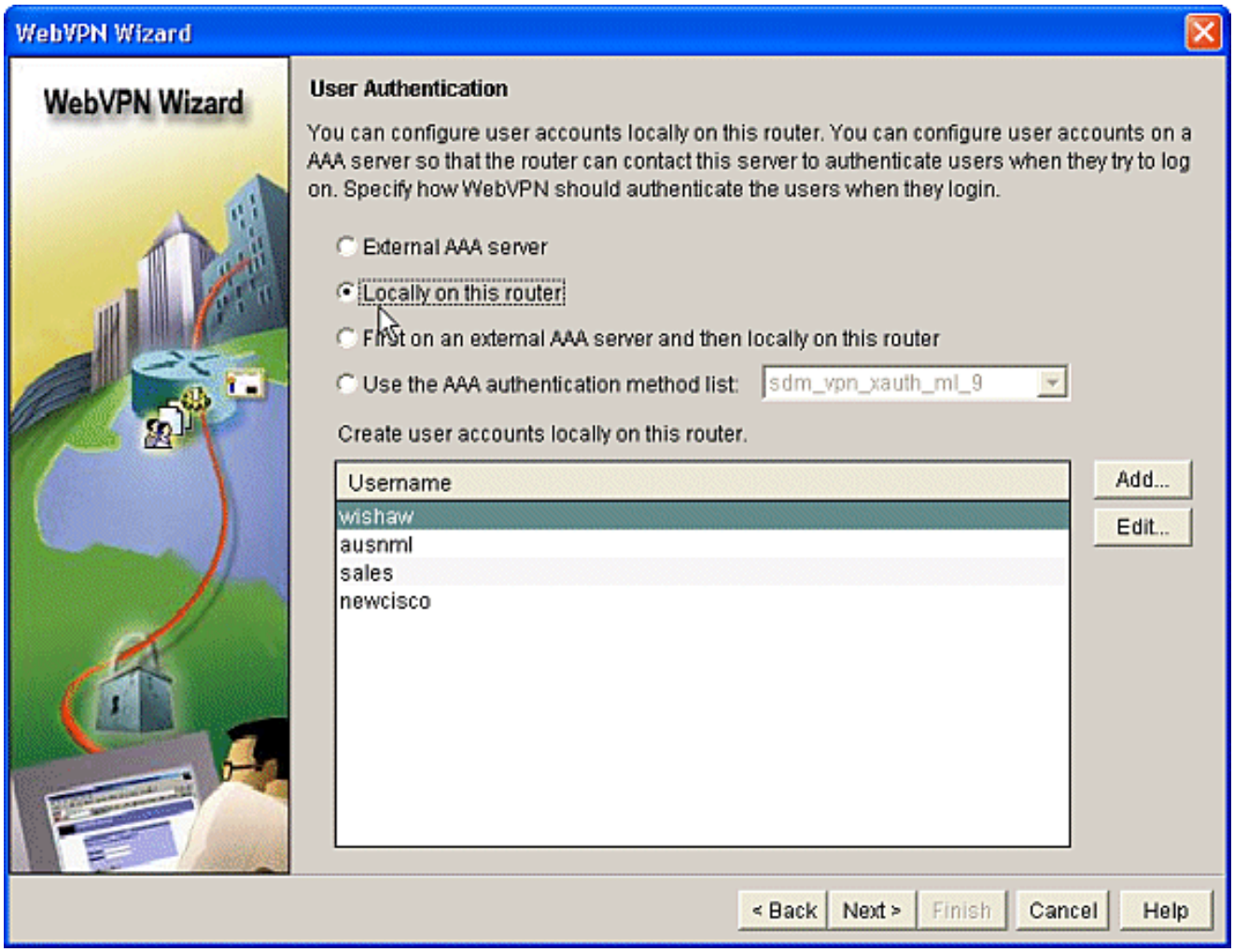
2. Nella schermata Creazione guidata WebVPN sono elencati i parametri che è possibile configurare. Fare clic su Next (Avanti).



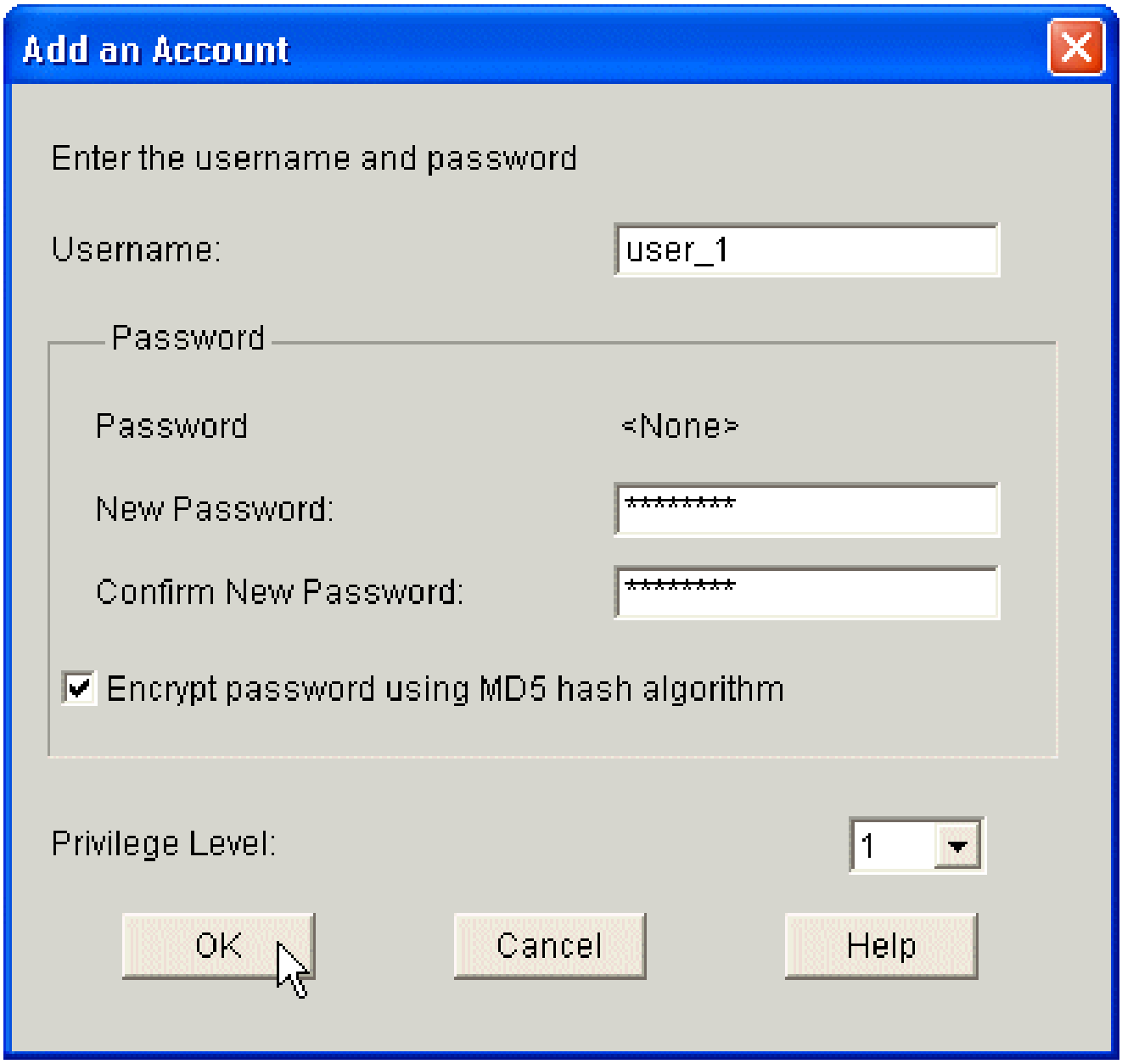
3. Immettere l'indirizzo IP del gateway WebVPN, un nome univoco per il servizio e le informazioni sul certificato digitale. Fare clic su Next (Avanti).



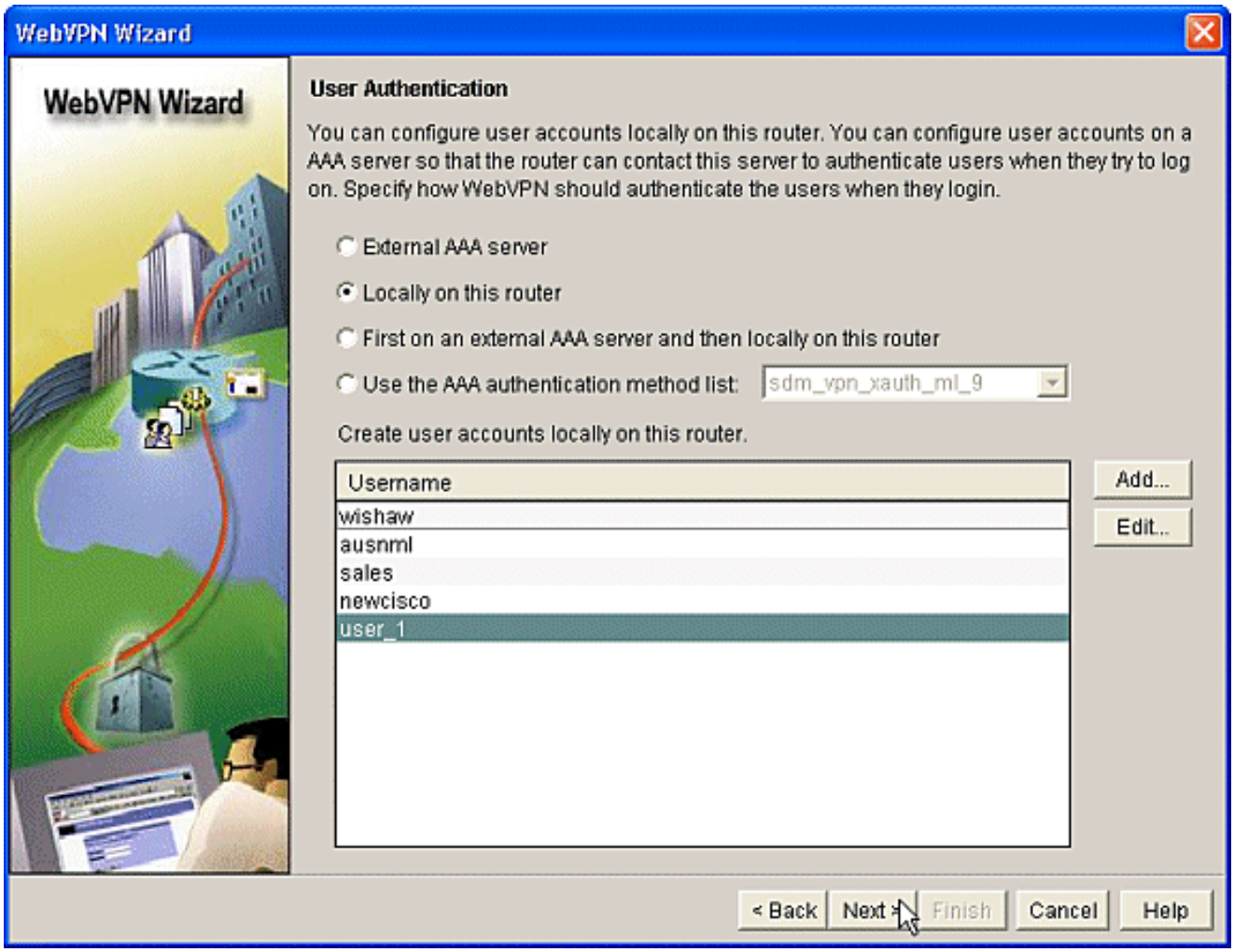
4. È possibile creare account utente per l'autenticazione in questo gateway WebVPN. È possibile utilizzare account locali o account creati in un server esterno di autenticazione, autorizzazione e accounting (AAA). In questo esempio vengono utilizzati gli account locali sul router. Selezionare il pulsante di opzione Localmente sul router e fare clic su Aggiungi.



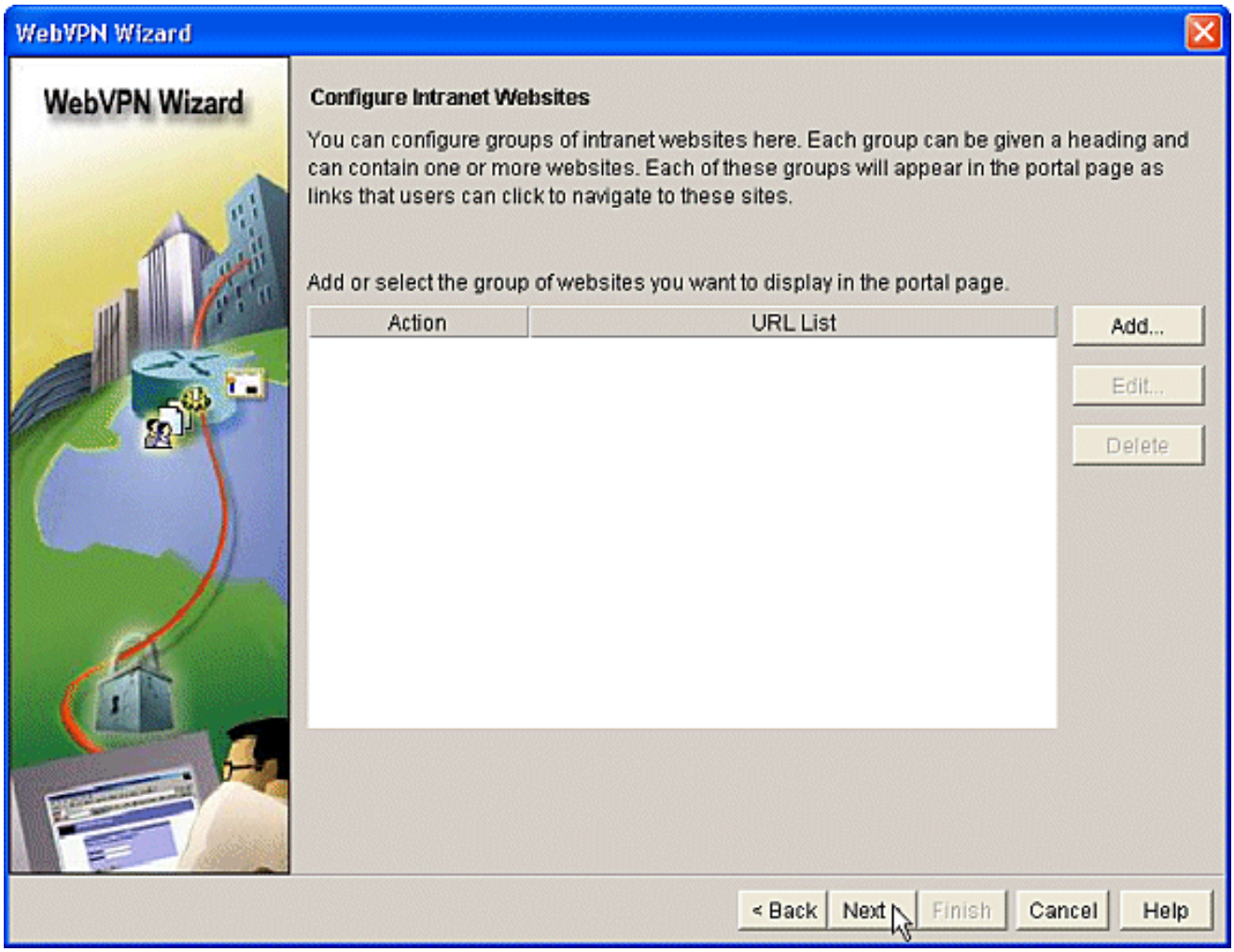
5. Immettere le informazioni sull'account per il nuovo utente nella schermata Aggiungi account e fare clic su OK.



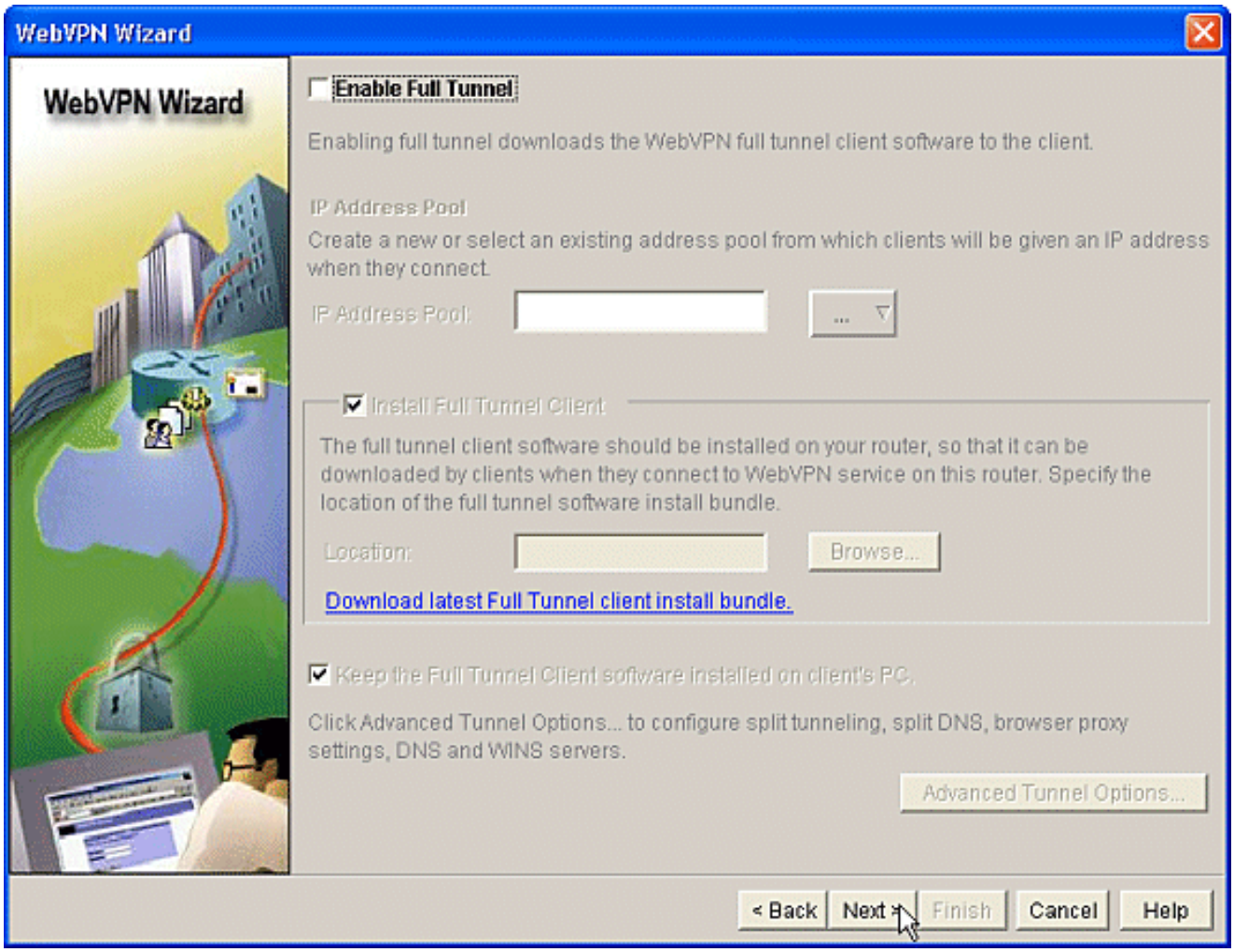
6. Dopo aver creato gli utenti, fare clic su Avanti nella pagina Autenticazione utente.



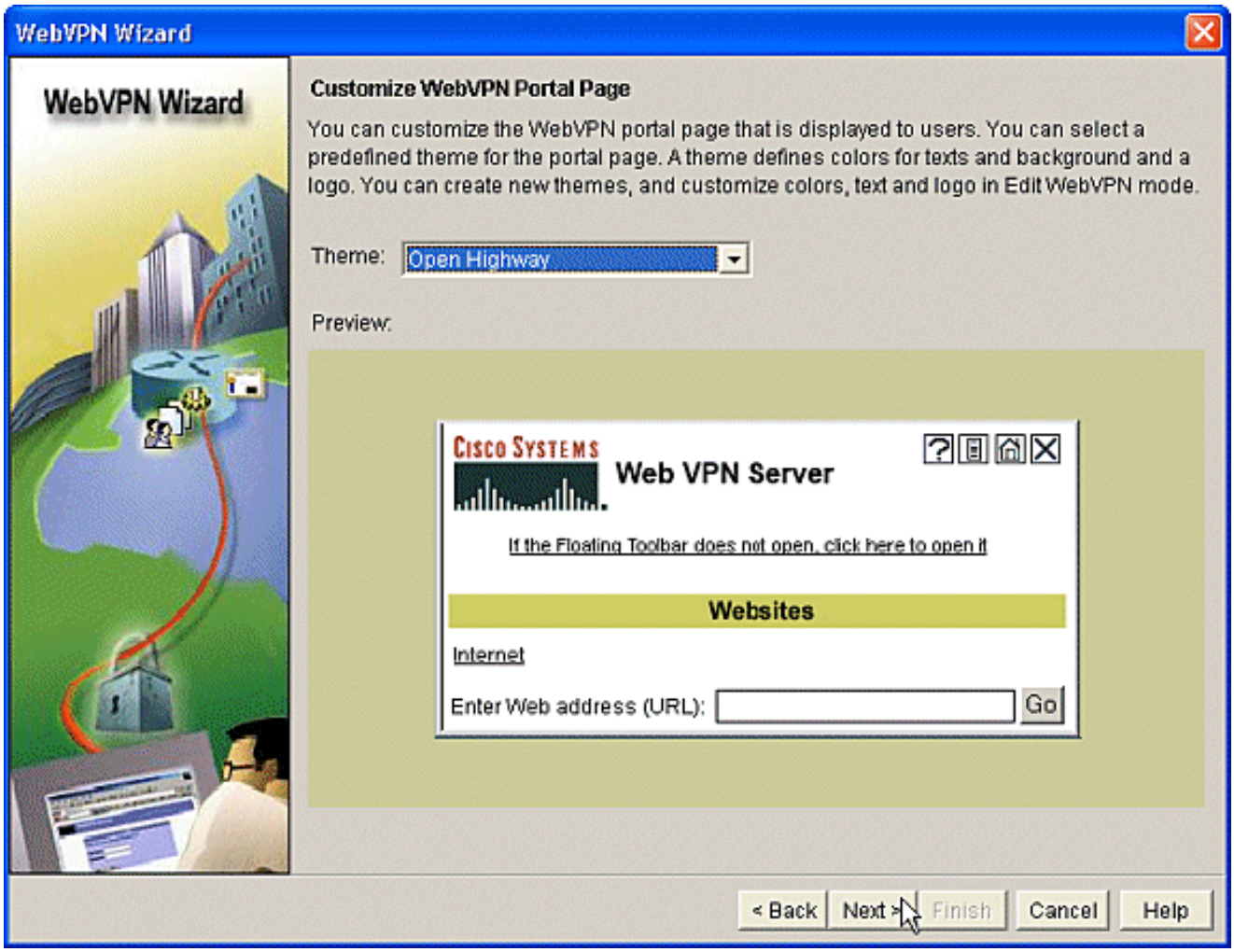
7. La schermata Configura siti Web Intranet consente di configurare il sito Web disponibile per gli utenti del gateway WebVPN. Poiché lo stato attivo di questo documento è la configurazione di CSD, ignorare questa pagina. Fare clic su Next (Avanti).



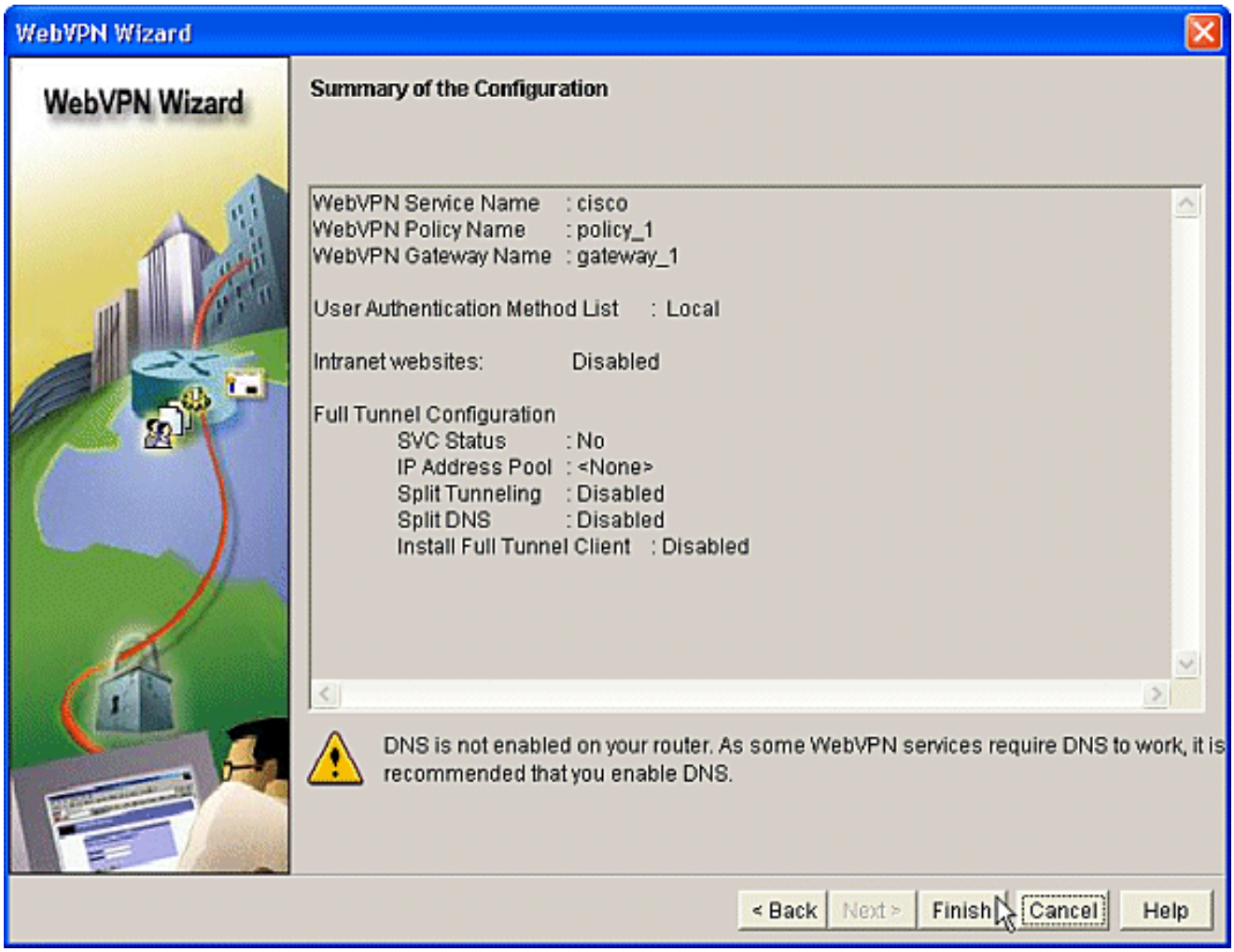
8. Sebbene la schermata successiva della Creazione guidata WebVPN consenta di abilitare il client VPN SSL a tunnel completo, in questo documento viene illustrato come abilitare CSD. Deselezionare Abilita tunnel completo e fare clic su Avanti.



9. È possibile personalizzare l'aspetto della pagina del portale WebVPN per gli utenti. In questo caso, viene accettato l'aspetto di default. Fare clic su Next (Avanti).



10. Verrà visualizzata l'ultima schermata della serie. Mostra un riepilogo della configurazione per il gateway WebVPN. Fare clic su Finish (Fine) e, quando richiesto, su OK.



Fase I: abilitare CSD in un contesto WebVPN.

Utilizzare la Creazione guidata WebVPN per abilitare CSD in un contesto WebVPN.

1. Utilizzare le funzionalità avanzate della Creazione guidata WebVPN per abilitare CSD per il nuovo contesto creato. La procedura guidata consente di installare il pacchetto CSD, se non è già installato.

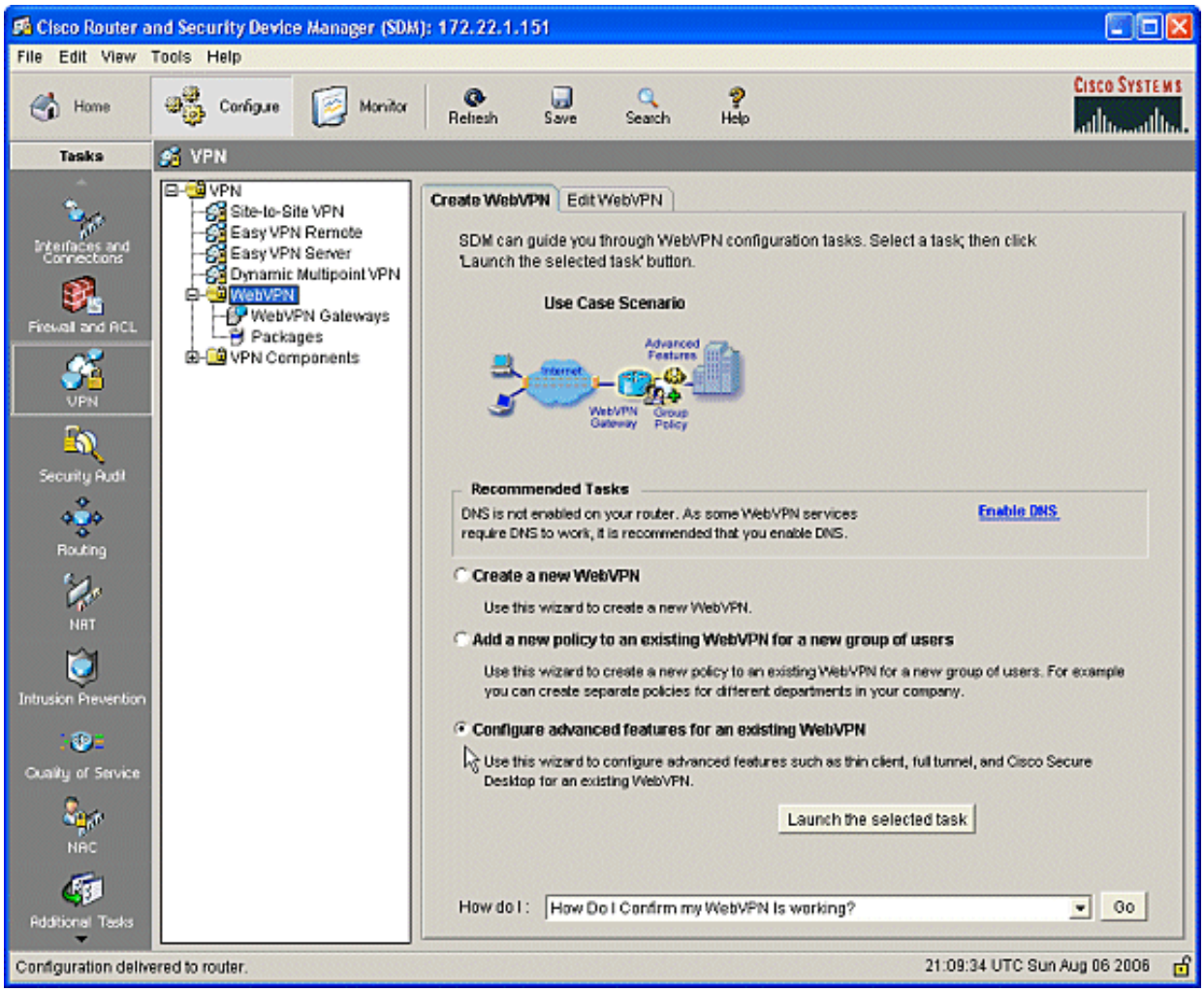
    a. In SDM, fare clic sulla scheda Configure (Configura).

    b. Nel riquadro di navigazione, fare clic su VPN > WebVPN.

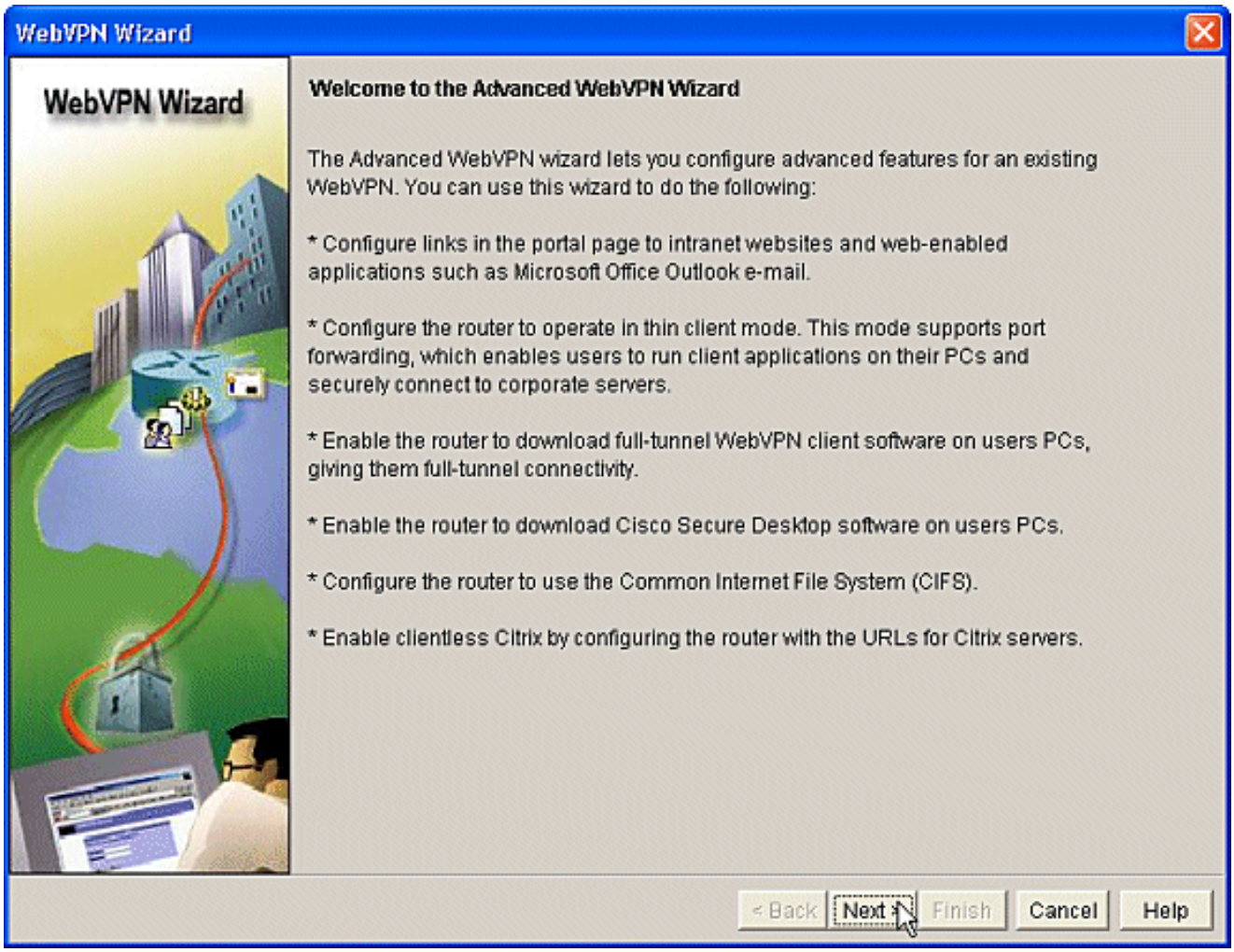
    c. Fare clic sulla scheda Crea WebVPN.

    d. Selezionare il pulsante di opzione Configura funzionalità avanzate per una WebVPN esistente.

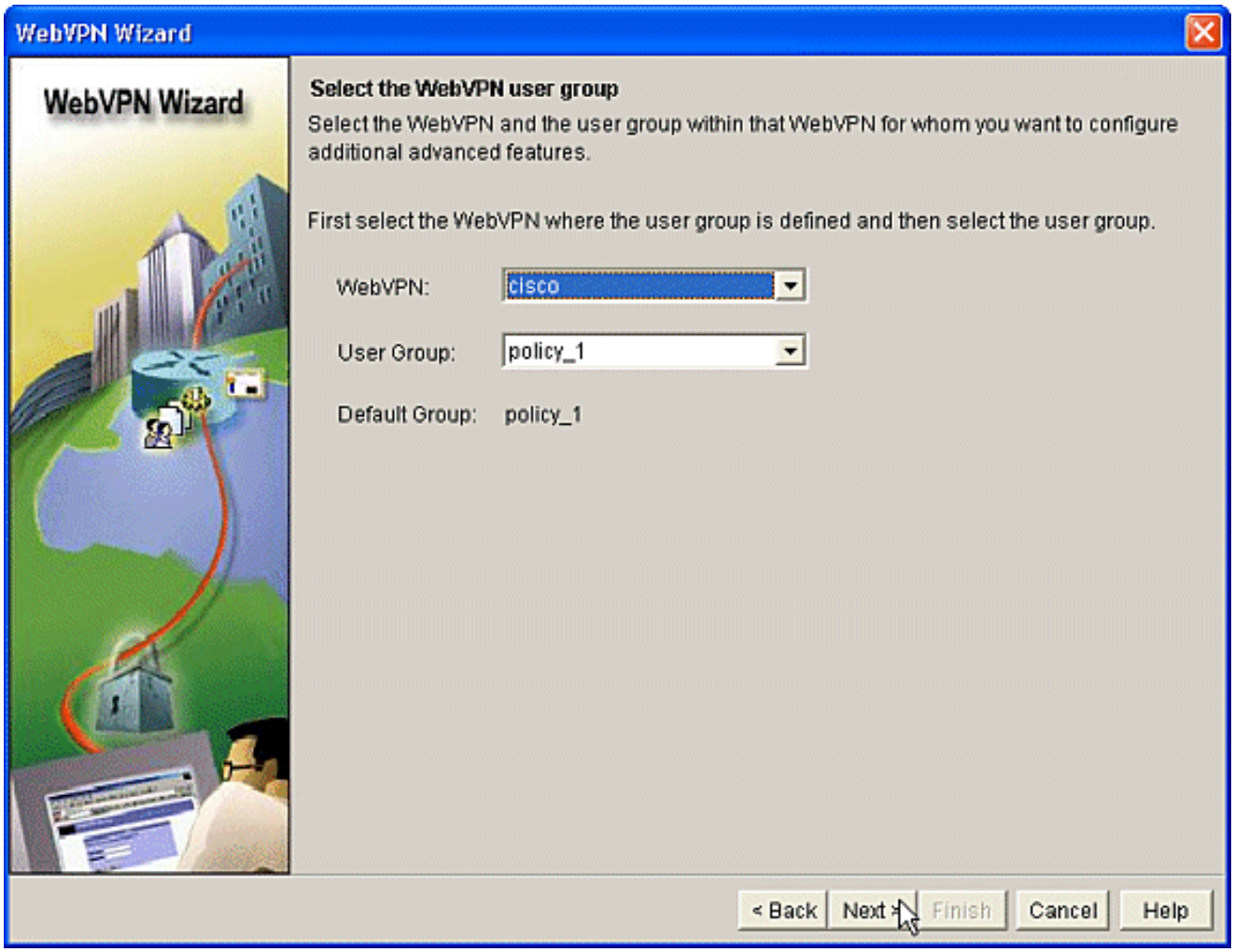
    e. Fare clic sul pulsante Avvia il task selezionato.



2. Verrà visualizzata la pagina iniziale della Creazione guidata WebVPN avanzata. Fare clic su Next (Avanti).



3. Scegliere WebVPN e il gruppo di utenti dalle caselle a discesa dei campi. Le funzionalità della Creazione guidata WebVPN avanzata verranno applicate alle scelte effettuate. Fare clic su Next (Avanti).



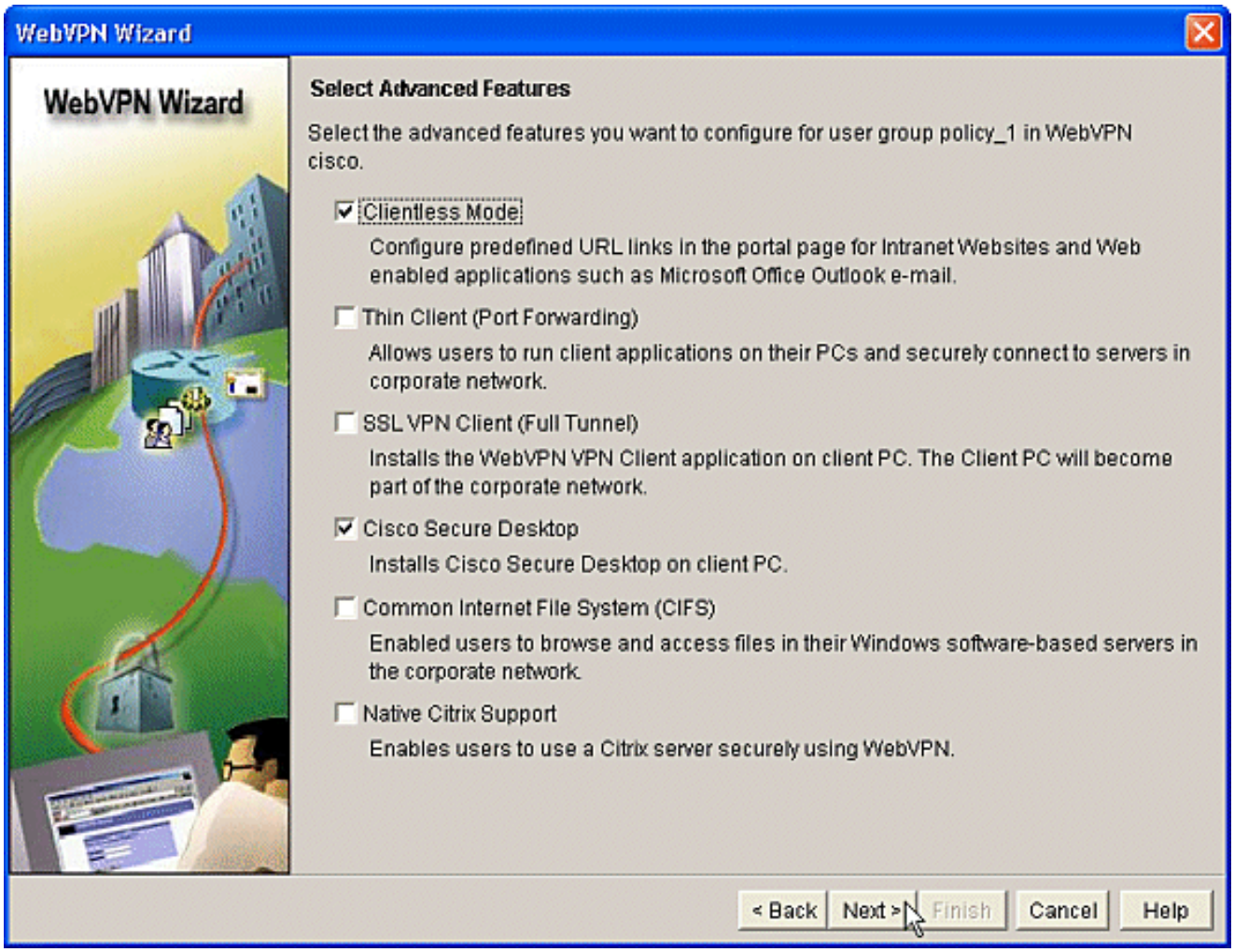
4. La schermata Seleziona caratteristiche avanzate consente di scegliere tra le tecnologie elencate.

    a. Controllare Cisco Secure Desktop.

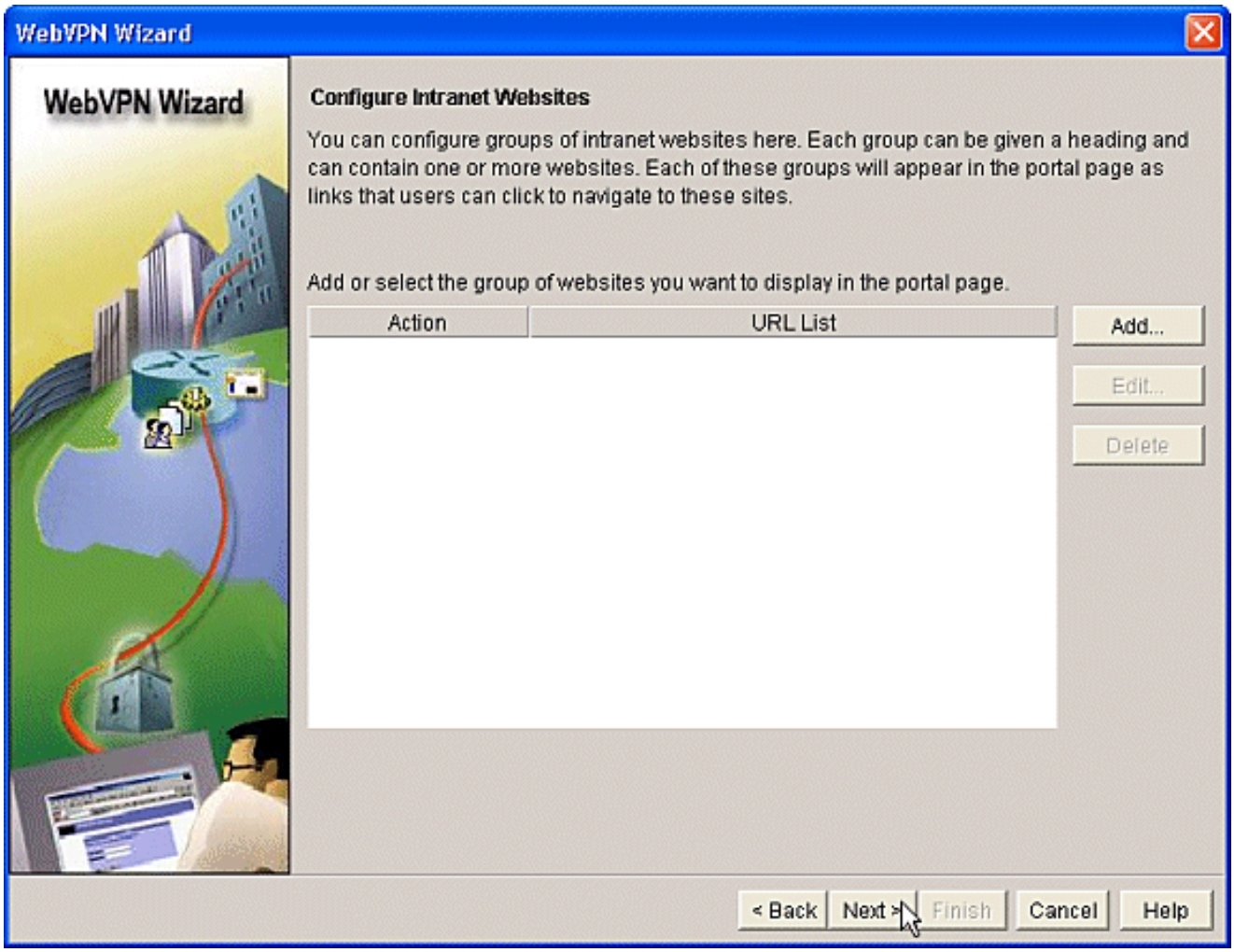
    b. Nell'esempio, la scelta è Modalità senza client.

    c. Se si sceglie una delle altre tecnologie elencate, vengono aperte finestre aggiuntive per consentire l'input di informazioni correlate.

    d. Fare clic sul pulsante Avanti.



5. La schermata Configura siti Web Intranet consente di configurare le risorse del sito Web da rendere disponibili agli utenti. È possibile aggiungere i siti Web interni della società, ad esempio Outlook Web Access (OWA).



6. Nella schermata Abilita Cisco Secure Desktop (CSD) è possibile abilitare il CSD per questo contesto. Selezionare la casella accanto a Installa Cisco Secure Desktop (CSD) e fare clic su Sfoglia.

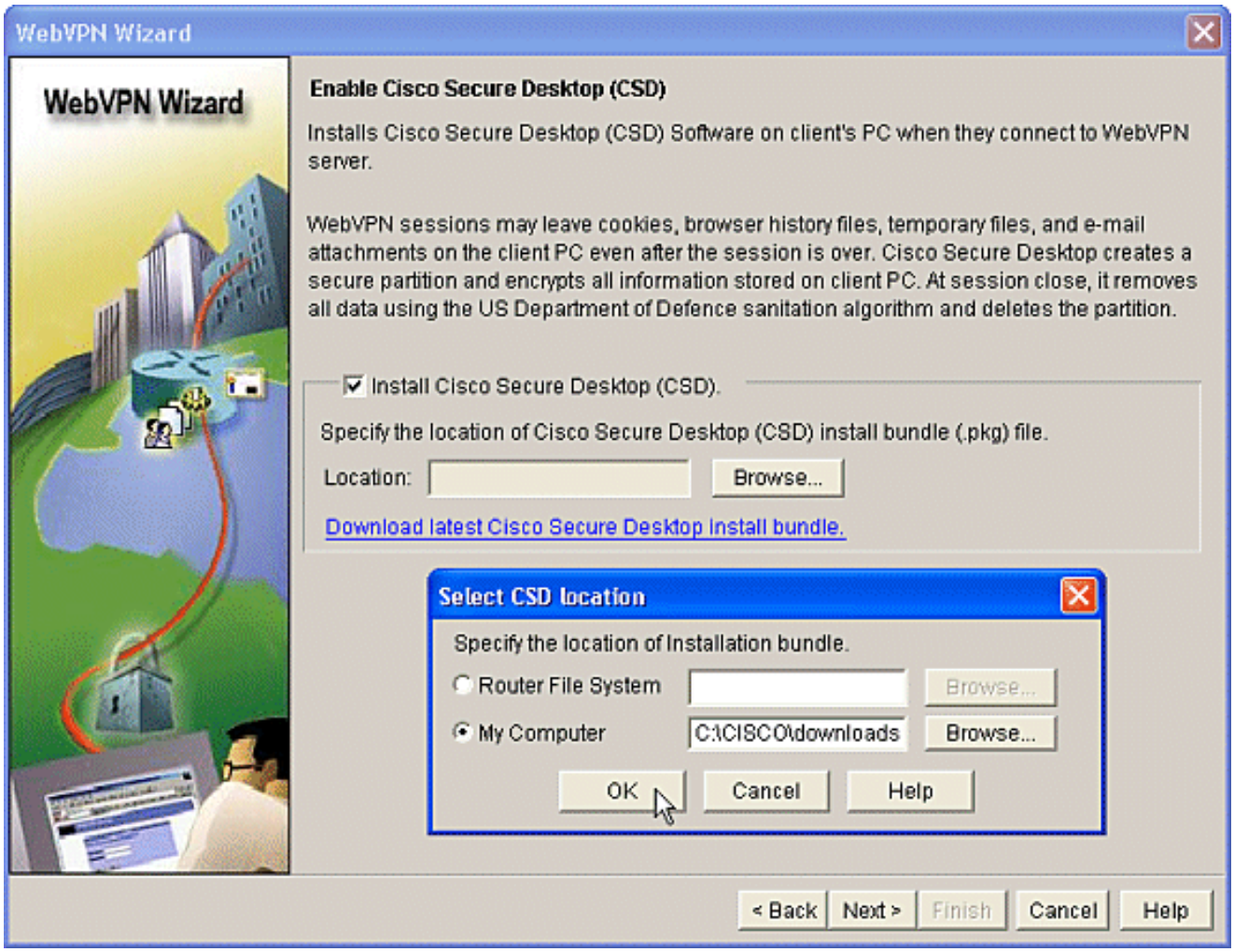
7. Nell'area Seleziona posizione CSD, selezionare Risorse del computer.

    a. Fare clic sul pulsante Sfoglia.

    b. Scegliere il file del pacchetto CSD IOS sulla workstation di gestione.

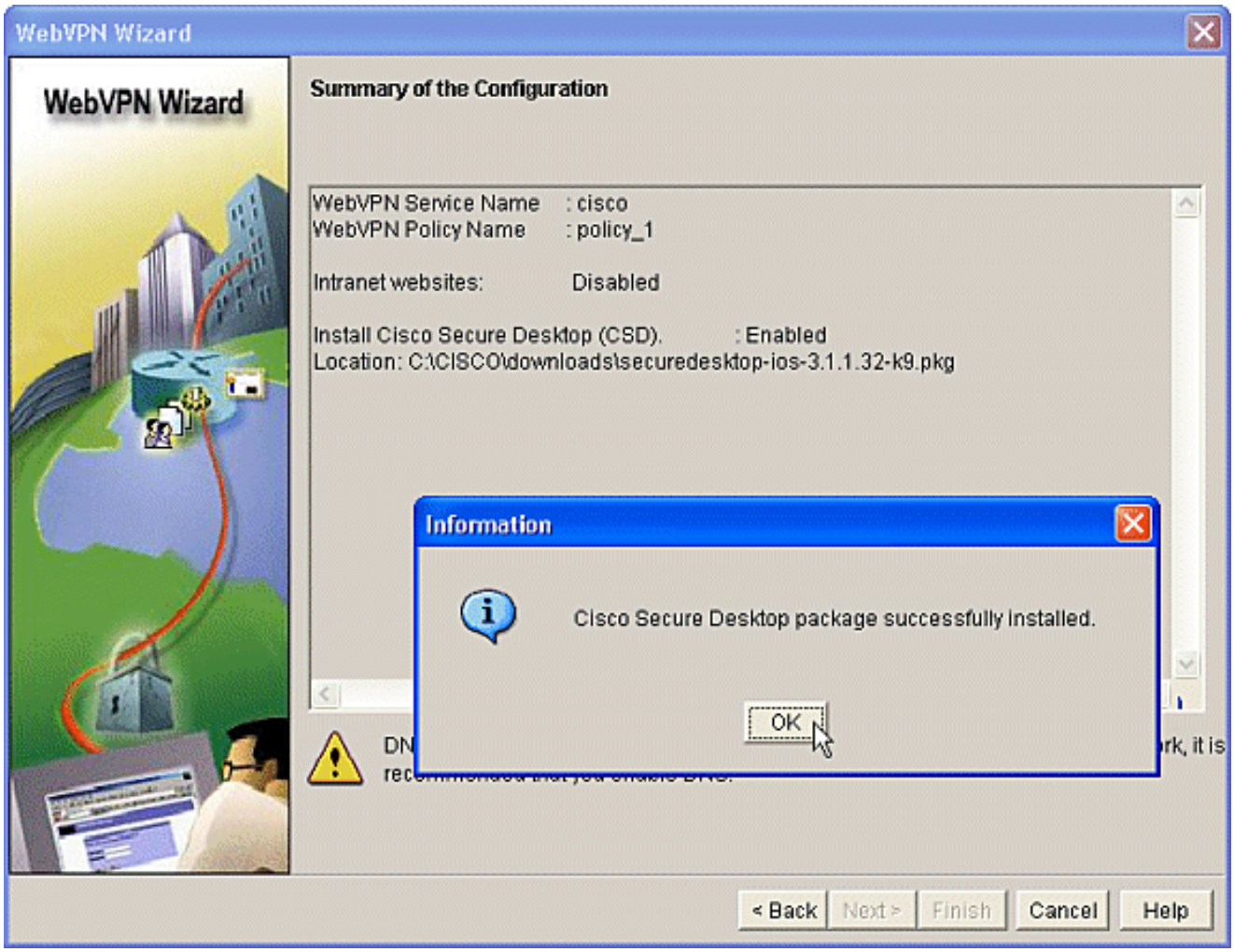
    c. Fare clic sul pulsante OK.

    d. Fare clic sul pulsante Avanti.



8. Viene visualizzato un riepilogo della schermata Configuration. Fare clic sul pulsante Fine.

9. Fare clic su OK quando si rileva che il file del pacchetto CSD è stato installato correttamente.



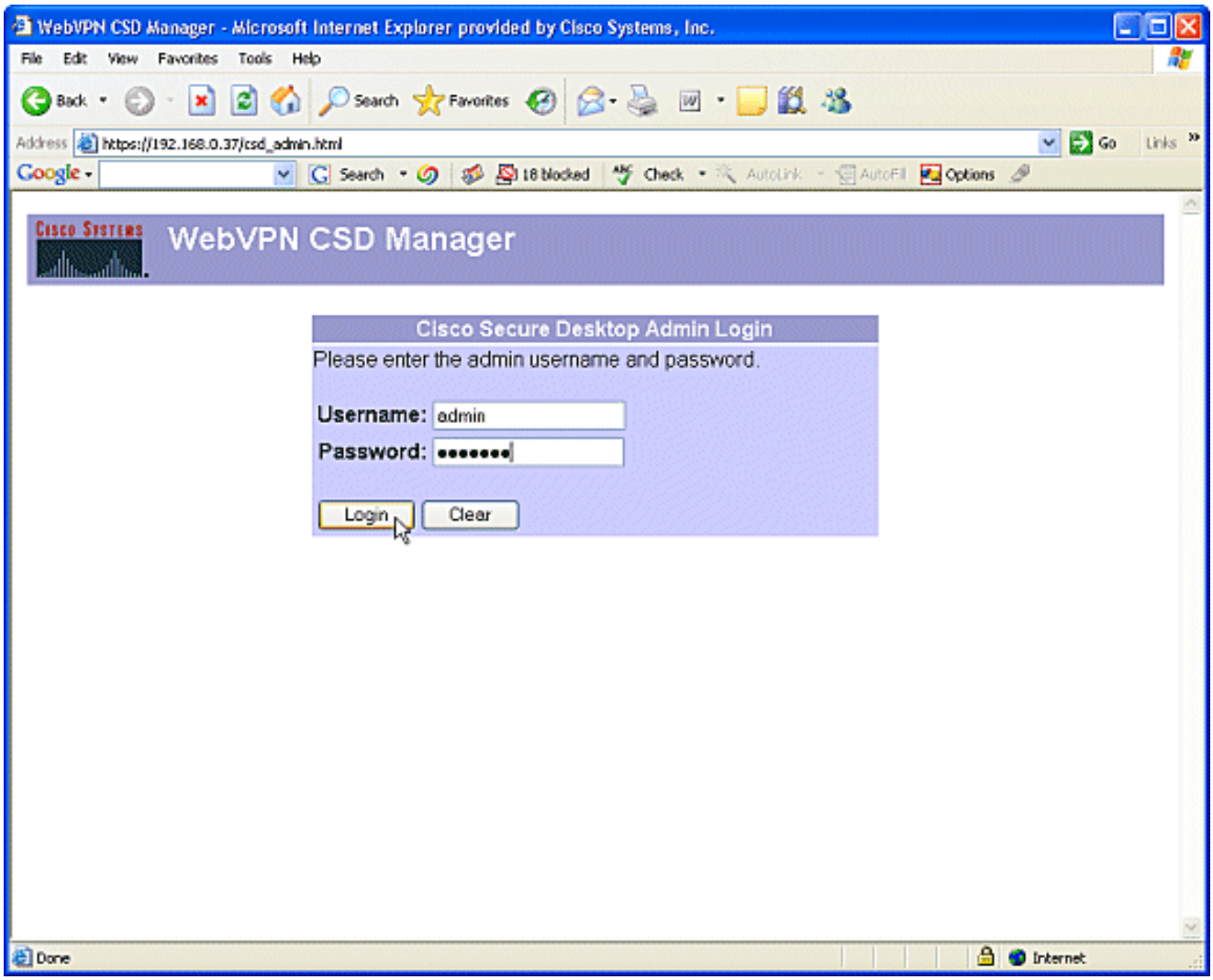
Fase II: configurare CSD utilizzando un browser Web.

Questi passaggi vengono utilizzati per completare la configurazione di CSD sul browser Web.

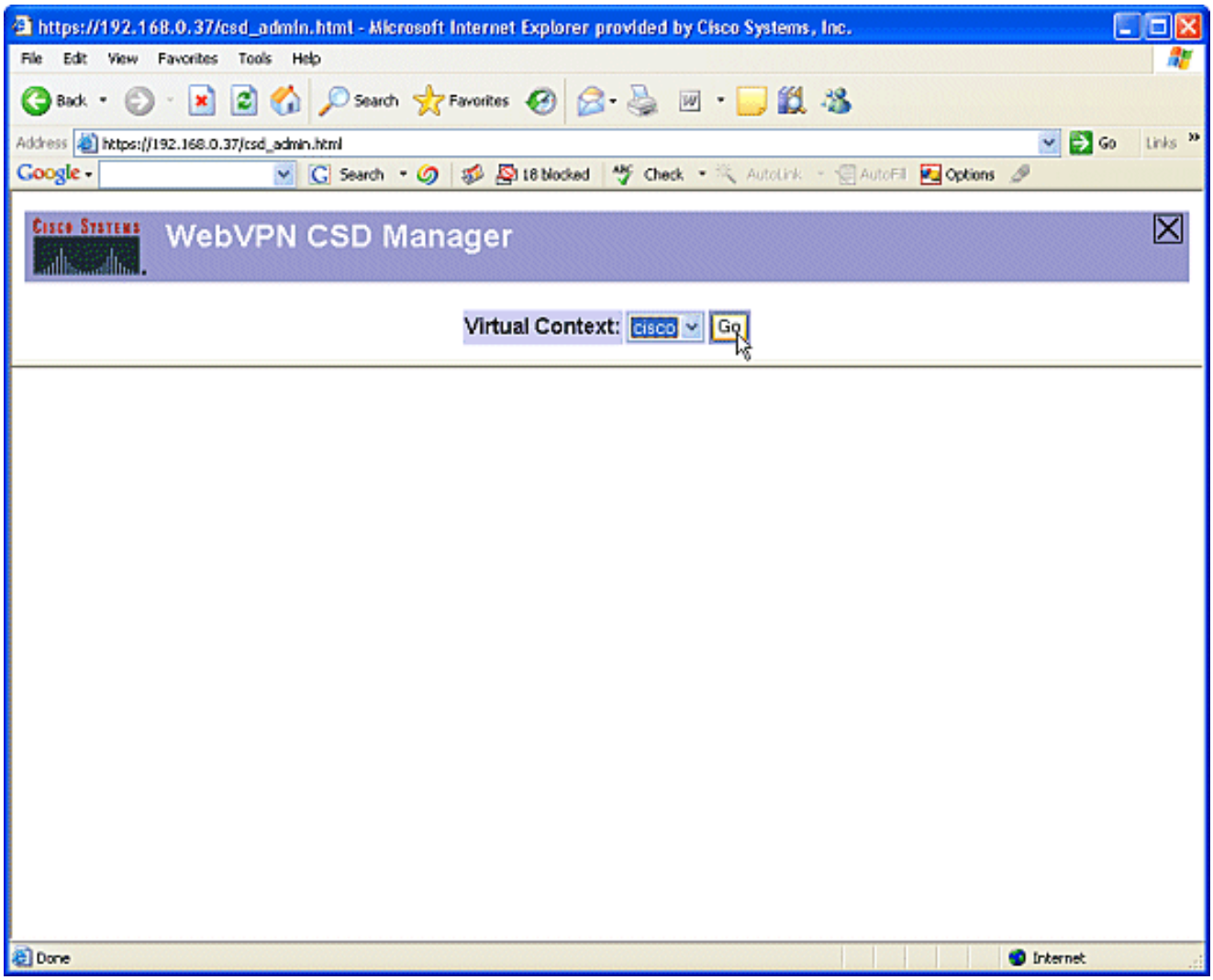
Fase II: definire i percorsi di Windows.

Definire i percorsi di Windows.

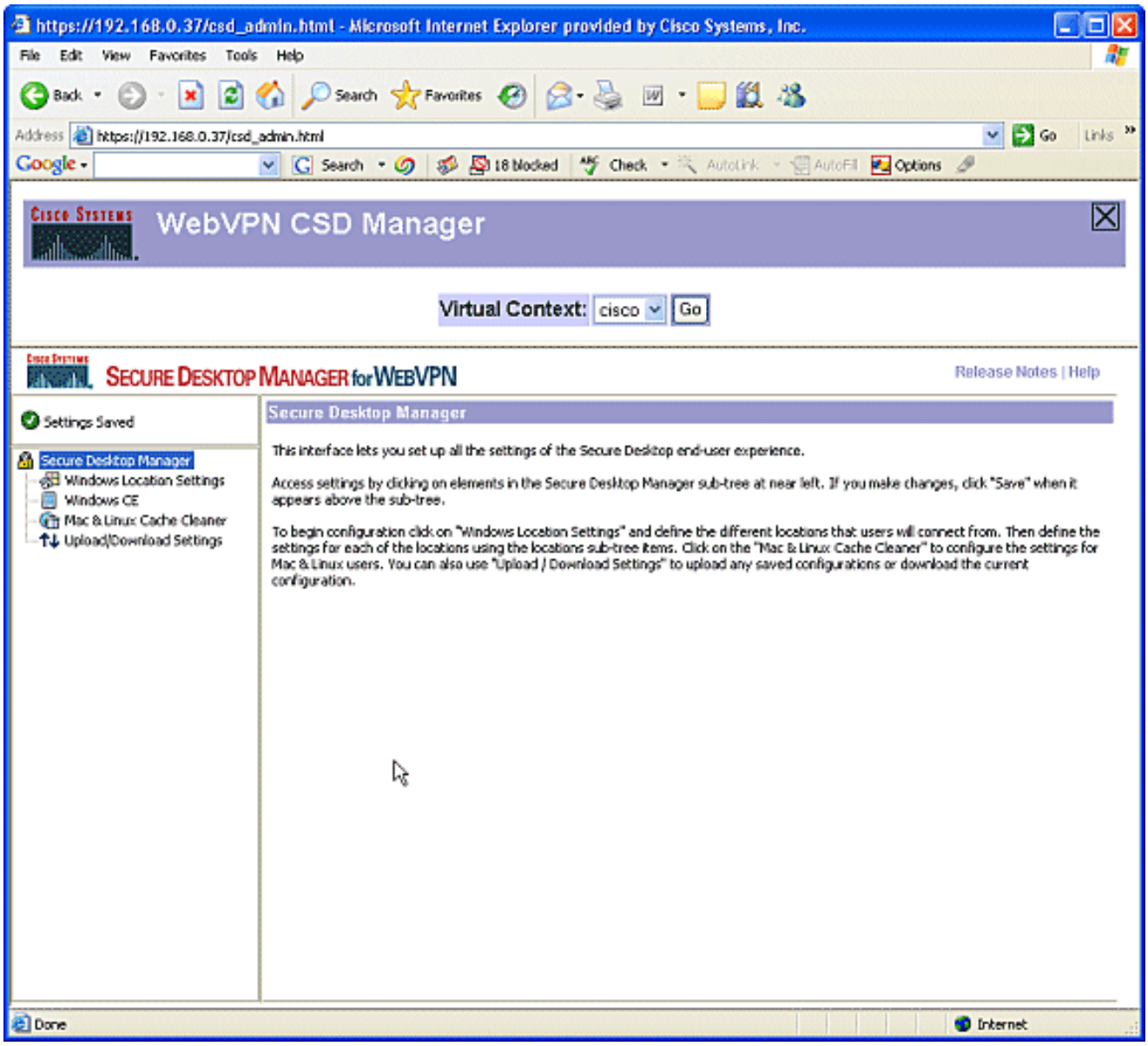
1. Aprire il browser Web all'indirizzo https://WebVPNgateway_IP Address/csd_admin.html, ad esempio https:/192.168.0.37/csd_admin.html.
2. Immettere il nome utente admin.
    a. Immettere la password, che è il segreto di abilitazione del router.
    b. Fare clic su Login.



3. Accettare il certificato offerto dal router, scegliere il contesto dalla casella a discesa e fare clic su Vai.



4. Viene aperto Secure Desktop Manager per WebVPN.

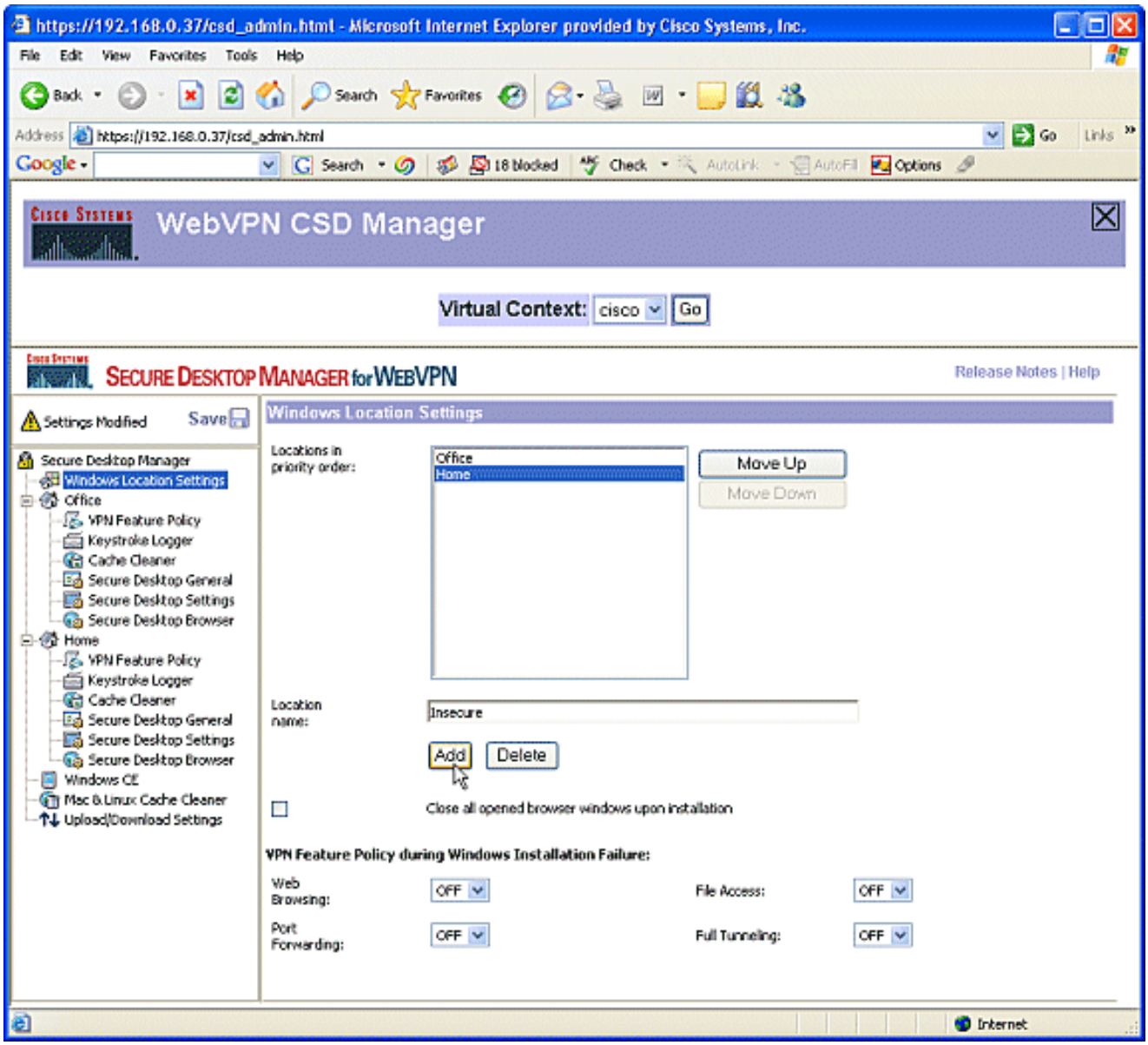


5. Nel riquadro sinistro scegliere Impostazioni percorso di Windows.

    a. Posizionare il cursore nella casella accanto a Nome posizione e immettere un nome di posizione.

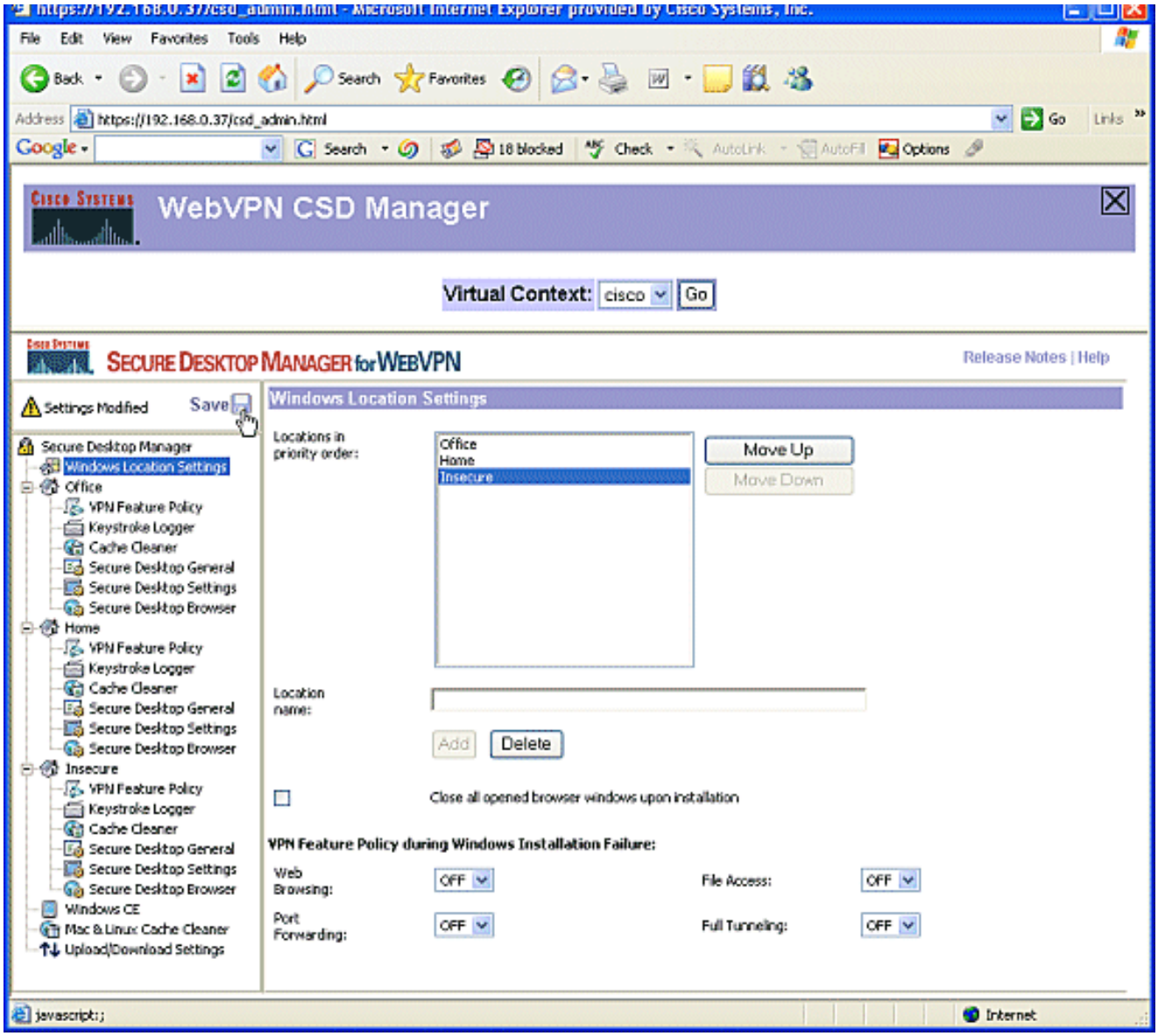
    b. Fare clic su Add.

    c. In questo esempio vengono visualizzati tre nomi di località: Office, Home e Insecure. Ogni volta che viene aggiunto un nuovo percorso, il riquadro di sinistra si espande con i parametri configurabili per tale percorso.



6. Dopo aver creato i percorsi di Windows, fare clic su Salva nella parte superiore del riquadro sinistro.

   Nota: salvare spesso le configurazioni perché le impostazioni andranno perse se si viene disconnessi dal browser Web.



Fase II: fase 2: identificazione dei criteri di ubicazione

Per distinguere i percorsi di Windows tra loro, assegnare criteri specifici a ogni percorso. In questo modo il CSD può determinare quali funzionalità applicare a una determinata posizione Windows.

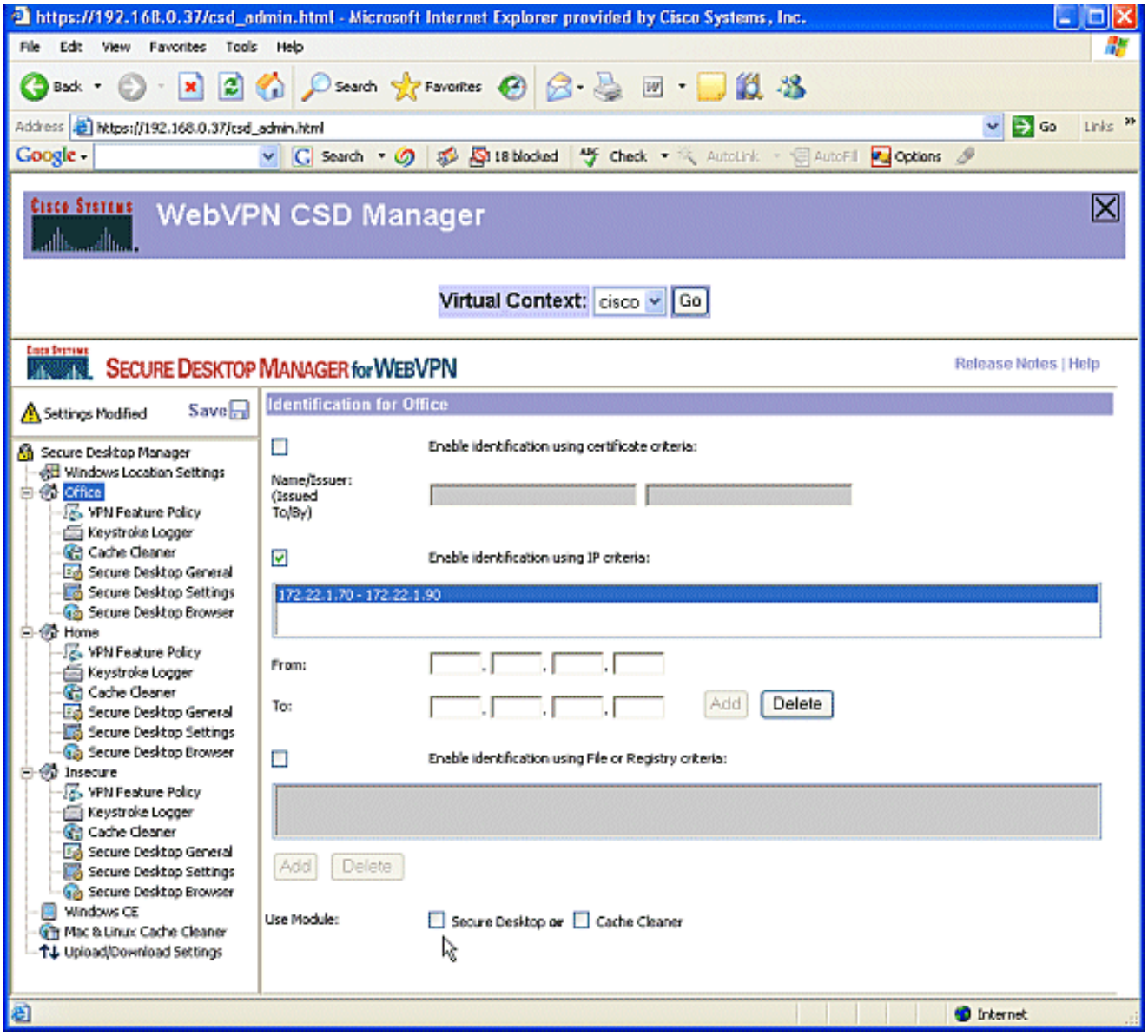
1. Nel riquadro sinistro fare clic su Office.

    a. È possibile identificare un percorso di Windows con criteri di certificato, criteri IP, un file o criteri del Registro di sistema. È inoltre possibile scegliere Secure Desktop o Cache Cleaner per questi client. Poiché questi utenti sono dipendenti dell'ufficio interno, identificarli con i criteri IP.

    b. Immettere gli intervalli di indirizzi IP nelle caselle Da e A.

    c. Fare clic su Add. Deselezionare Usa modulo: desktop sicuro.

    d. Quando richiesto, fare clic su Salva, quindi su OK.



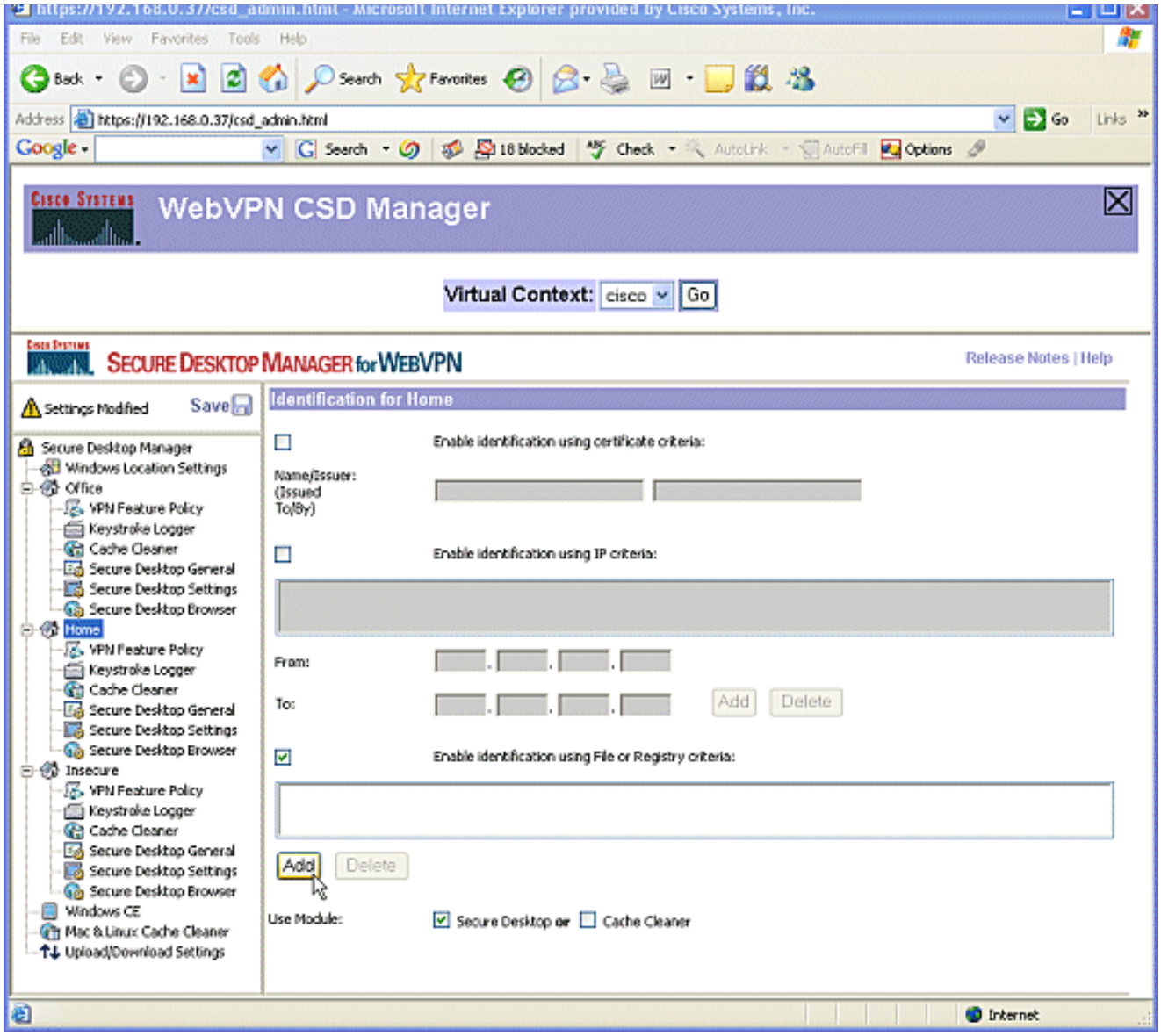
2. Nel riquadro di sinistra fare clic sulla seconda home page di Impostazioni percorso di Windows.

    a. Accertarsi che l'opzione Use Module: Secure Desktop sia selezionata.

    b. Verrà distribuito un file che identifica questi client. È possibile scegliere di distribuire i certificati e/o i criteri del Registro di sistema per questi utenti.

    c. Selezionare Abilita identificazione utilizzando i criteri File o Registro di sistema.

    d. Fare clic su Add.

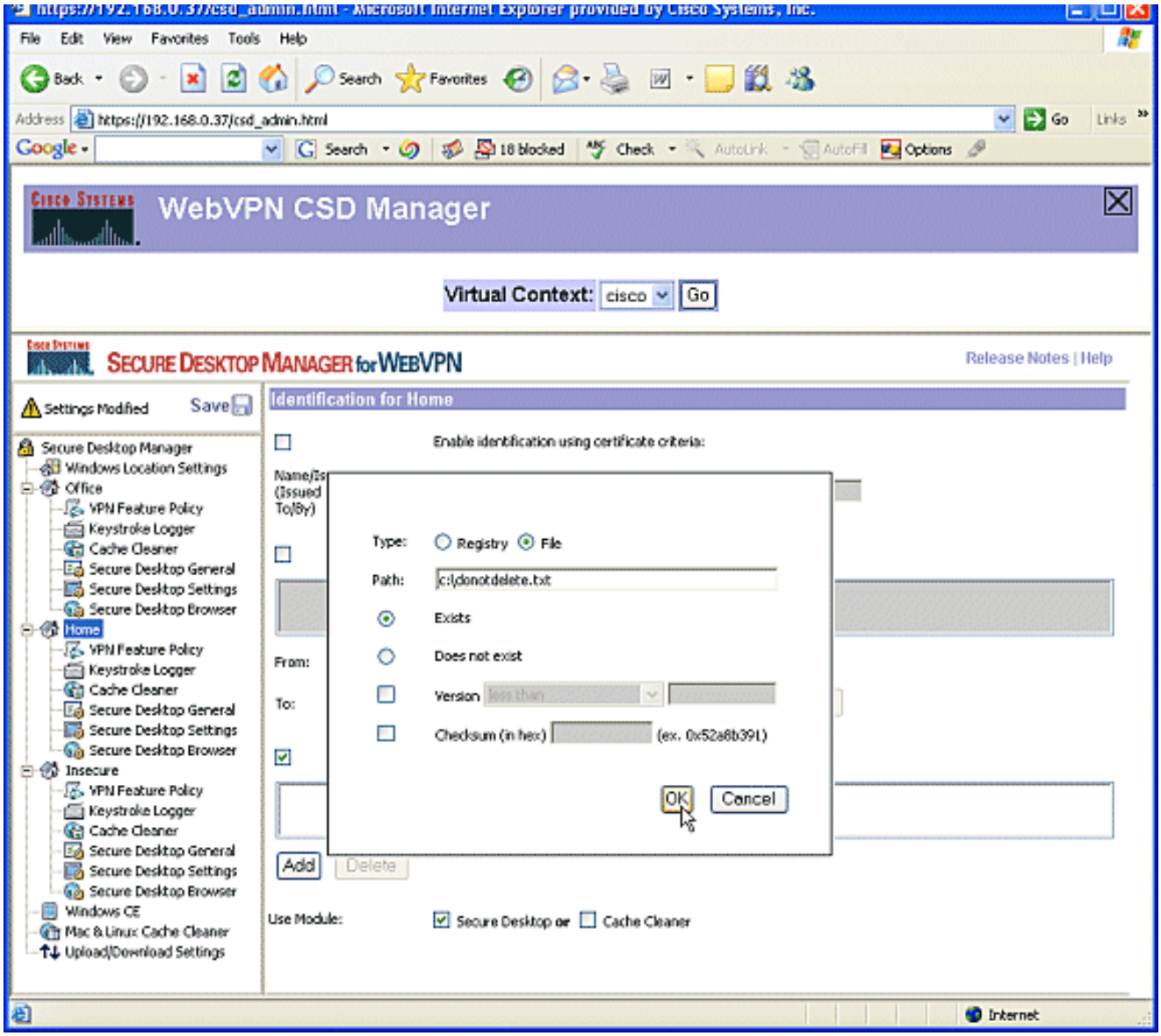


3. Nella finestra di dialogo, scegliere File, quindi immettere il percorso del file.

    a. Questo file deve essere distribuito a tutti i client di casa.

    b. Selezionare il pulsante di opzione Esiste.

    c. Quando richiesto, fare clic su OK, quindi su Salva.



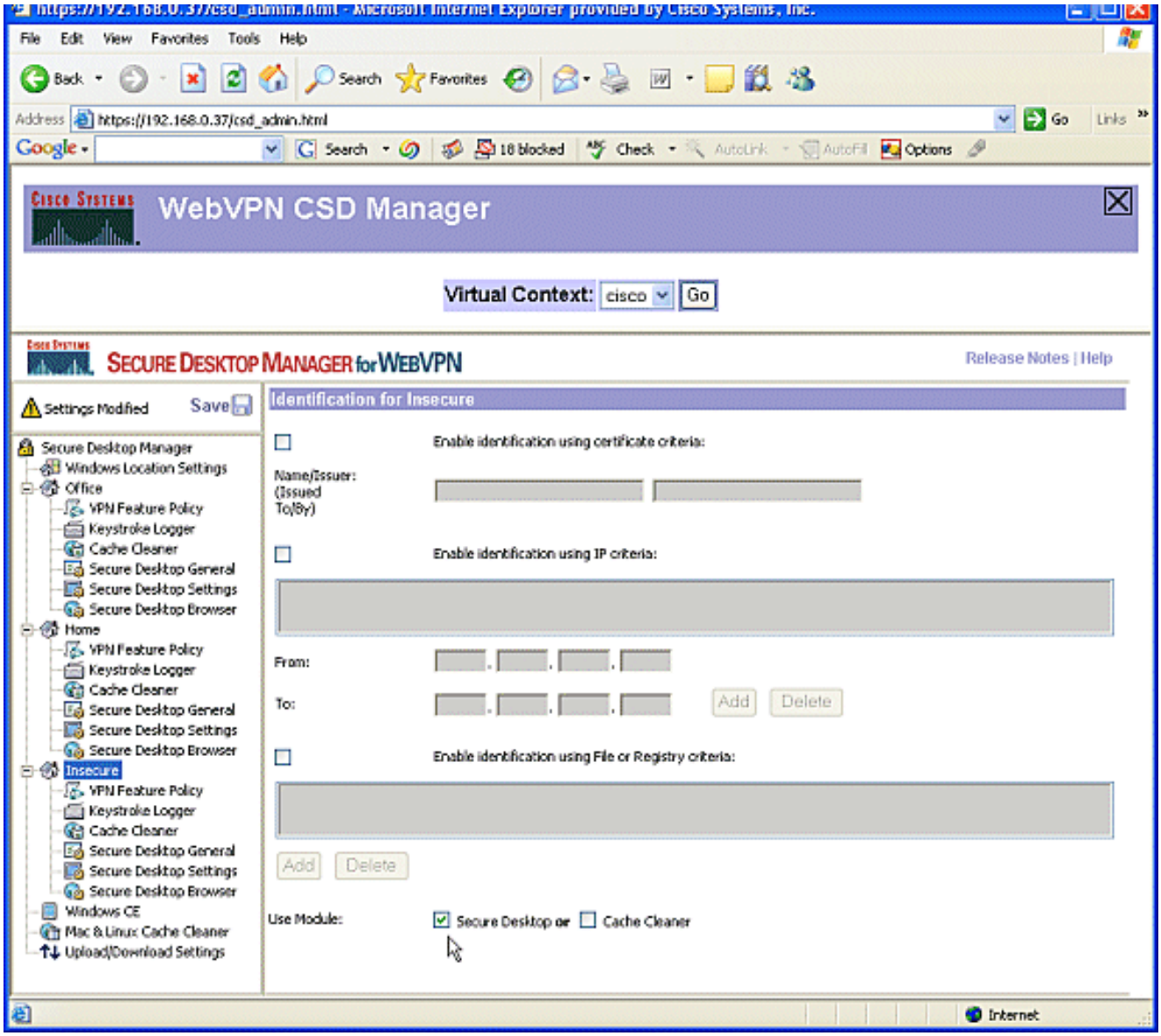
4. Per configurare l'identificazione delle posizioni non sicure, non applicare alcun criterio di identificazione.

    a. Fare clic su Non protetto nel riquadro di sinistra.

    b. Lasciare tutti i criteri non selezionati.

    c. Selezionare Use Module: Secure Desktop.

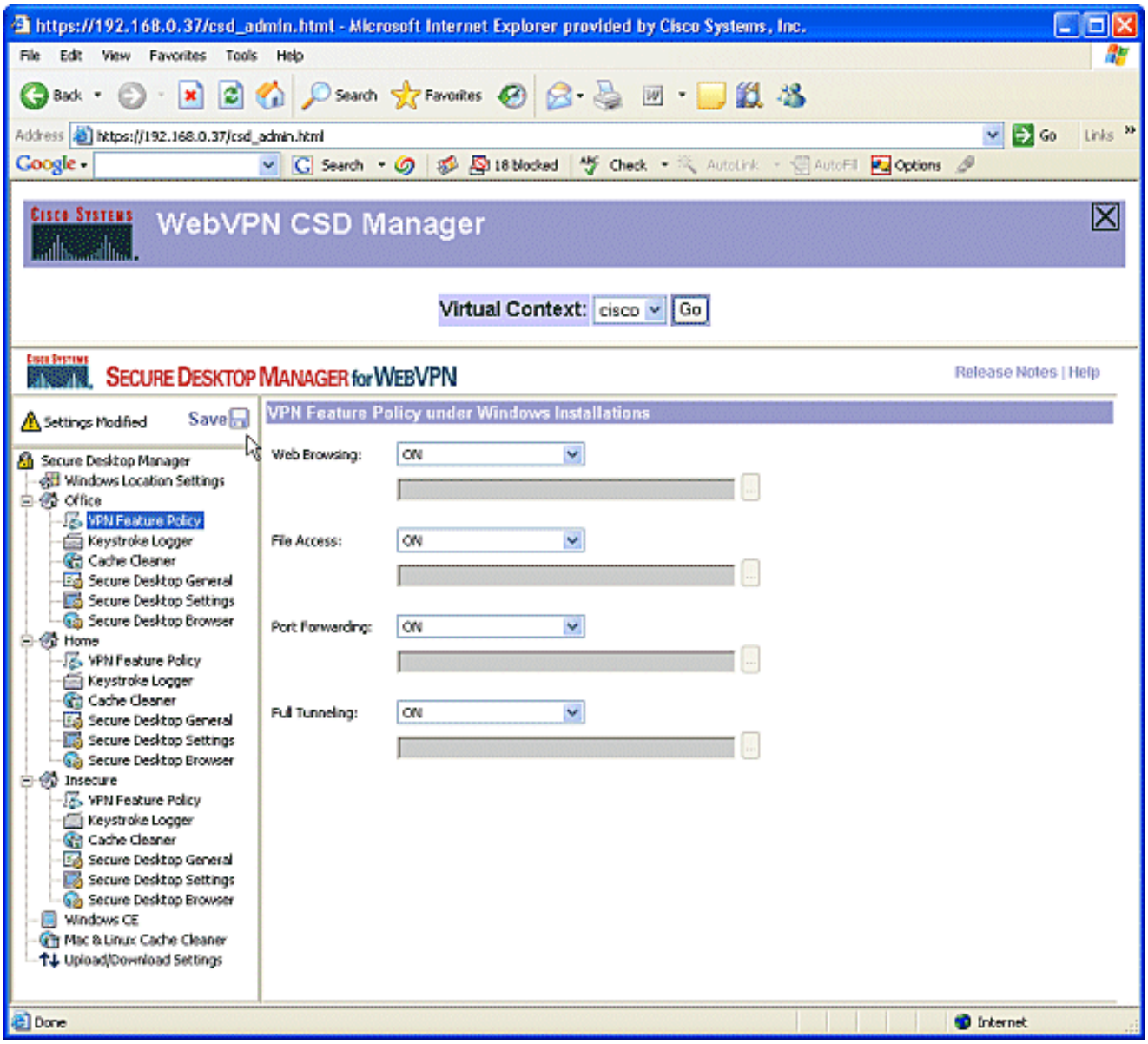
    d. Quando richiesto, fare clic su Salva, quindi su OK.



Fase II: configurare i moduli e le funzionalità di posizione di Windows.

Configurare le funzionalità CSD per ogni percorso di Windows.

1. In Office fare clic su Criteri funzionalità VPN. Poiché si tratta di client interni attendibili, non è stato abilitato né CSD né Cache Cleaner. Nessun altro parametro disponibile.

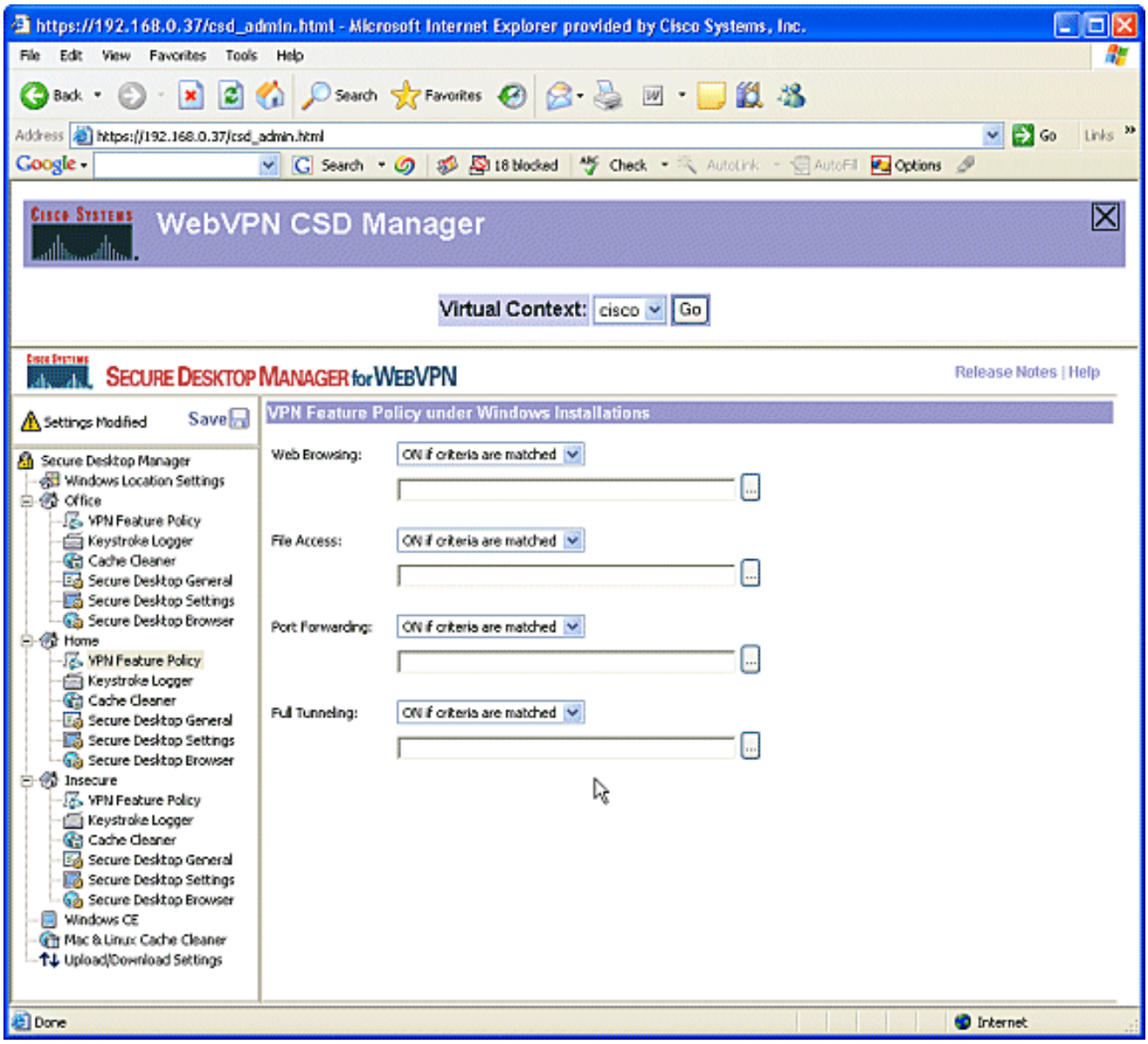


2. Attivate le feature come mostrato.

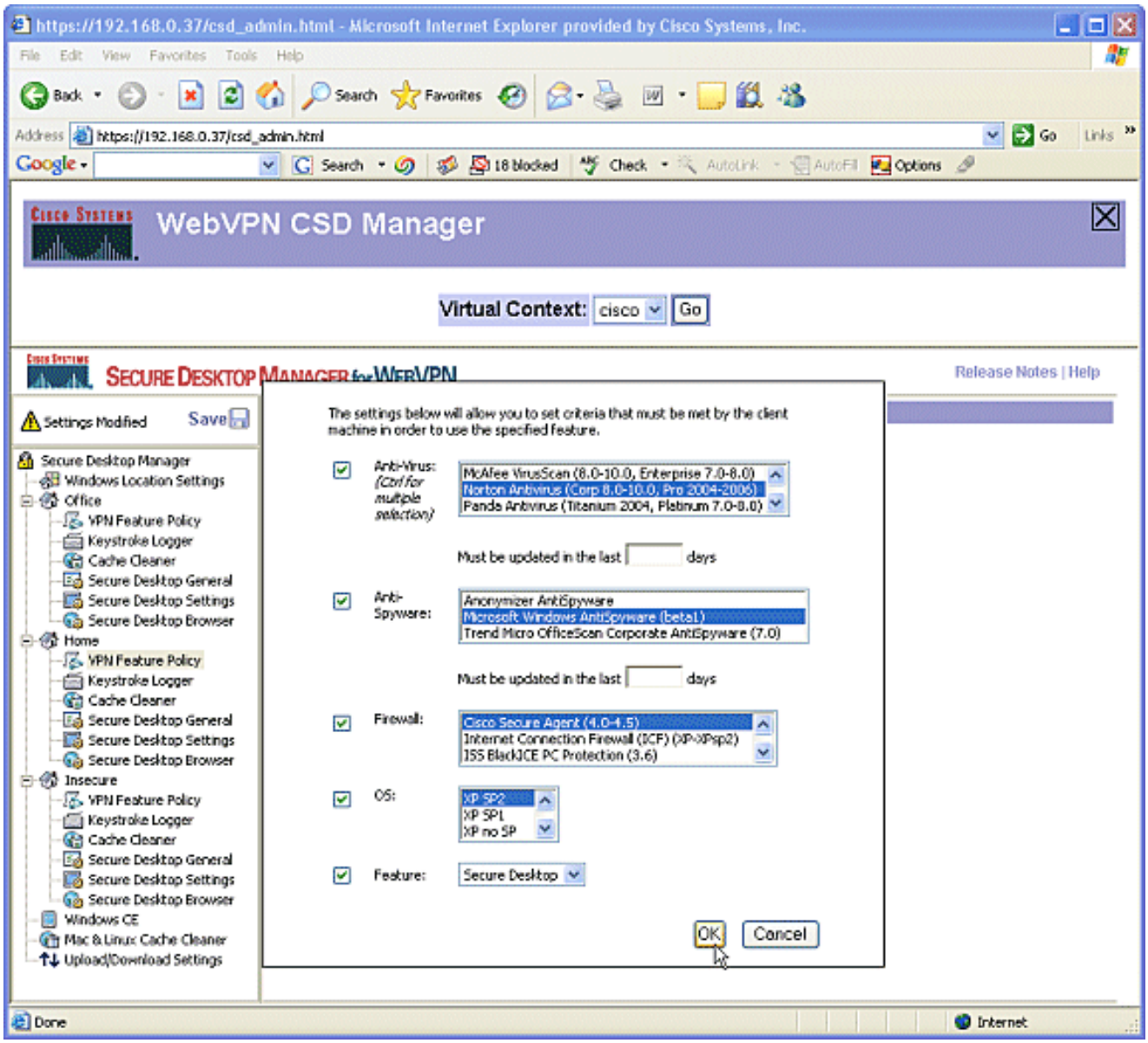
    a. Nel riquadro sinistro, scegliere VPN Feature Policy (Policy funzionalità VPN) in Home (Home).

    b. Gli utenti privati potranno accedere alla LAN aziendale se i client soddisfano determinati criteri.

    c. In ogni metodo di accesso, scegliere ON se i criteri vengono soddisfatti.



3. Per l'esplorazione del Web, fare clic sul pulsante con i puntini di sospensione e scegliere i criteri che devono corrispondere. Fate clic su OK nella finestra di dialogo.

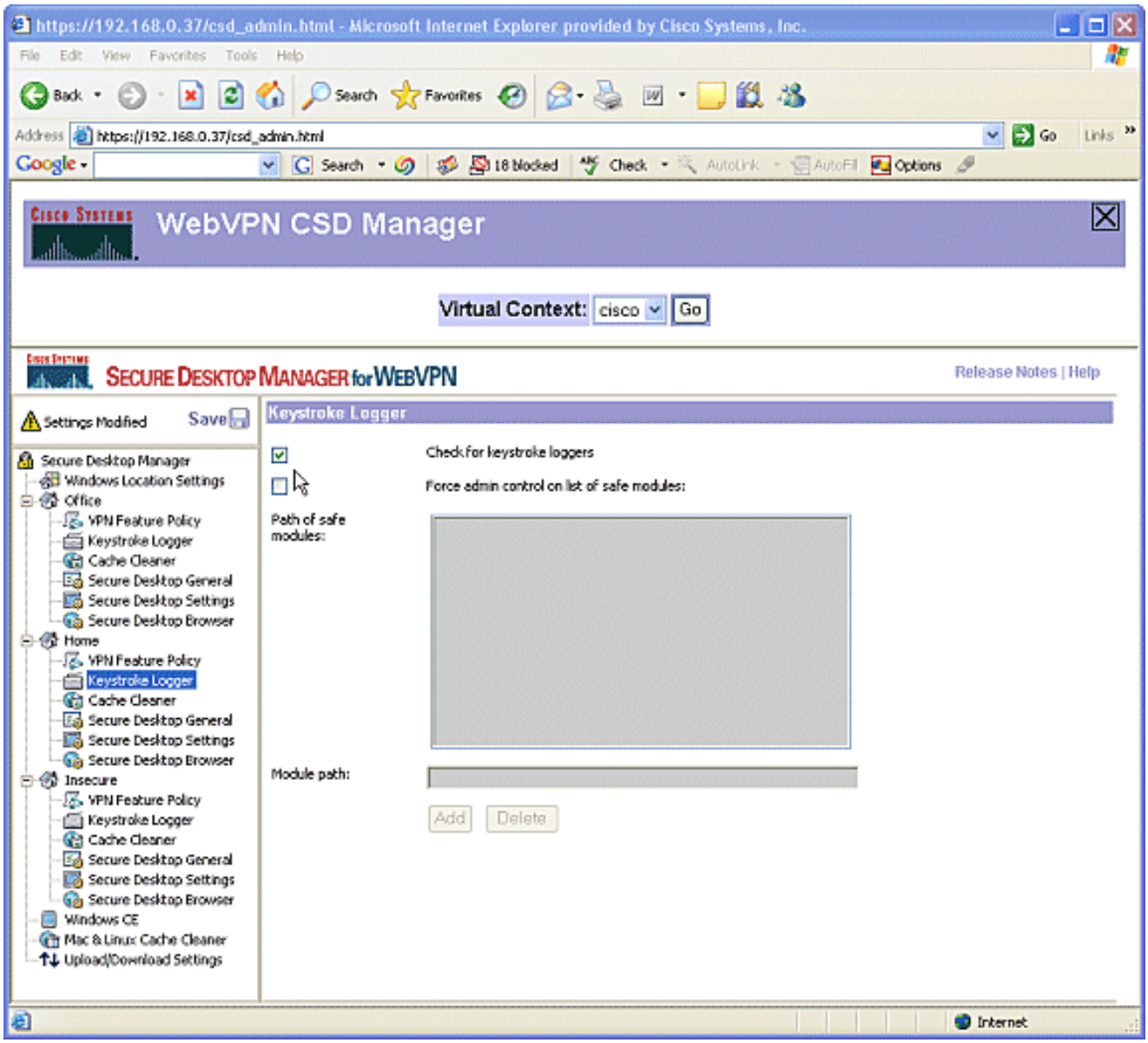


4. Analogamente, è possibile configurare gli altri metodi di accesso.

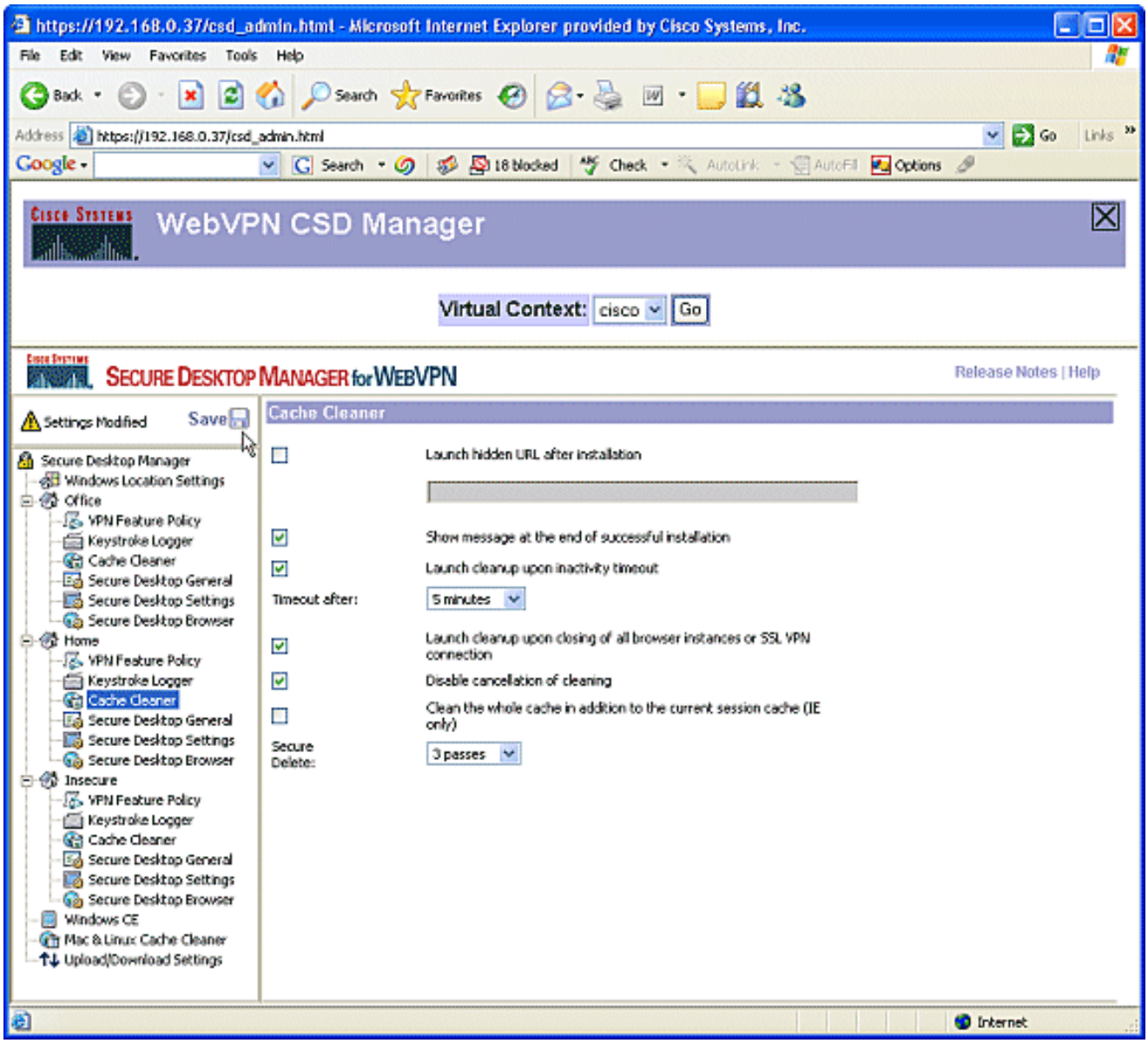
    a. In Home, scegliere Registratore tasti.

    b. Selezionare la casella di controllo Controlla registratori di tasti.

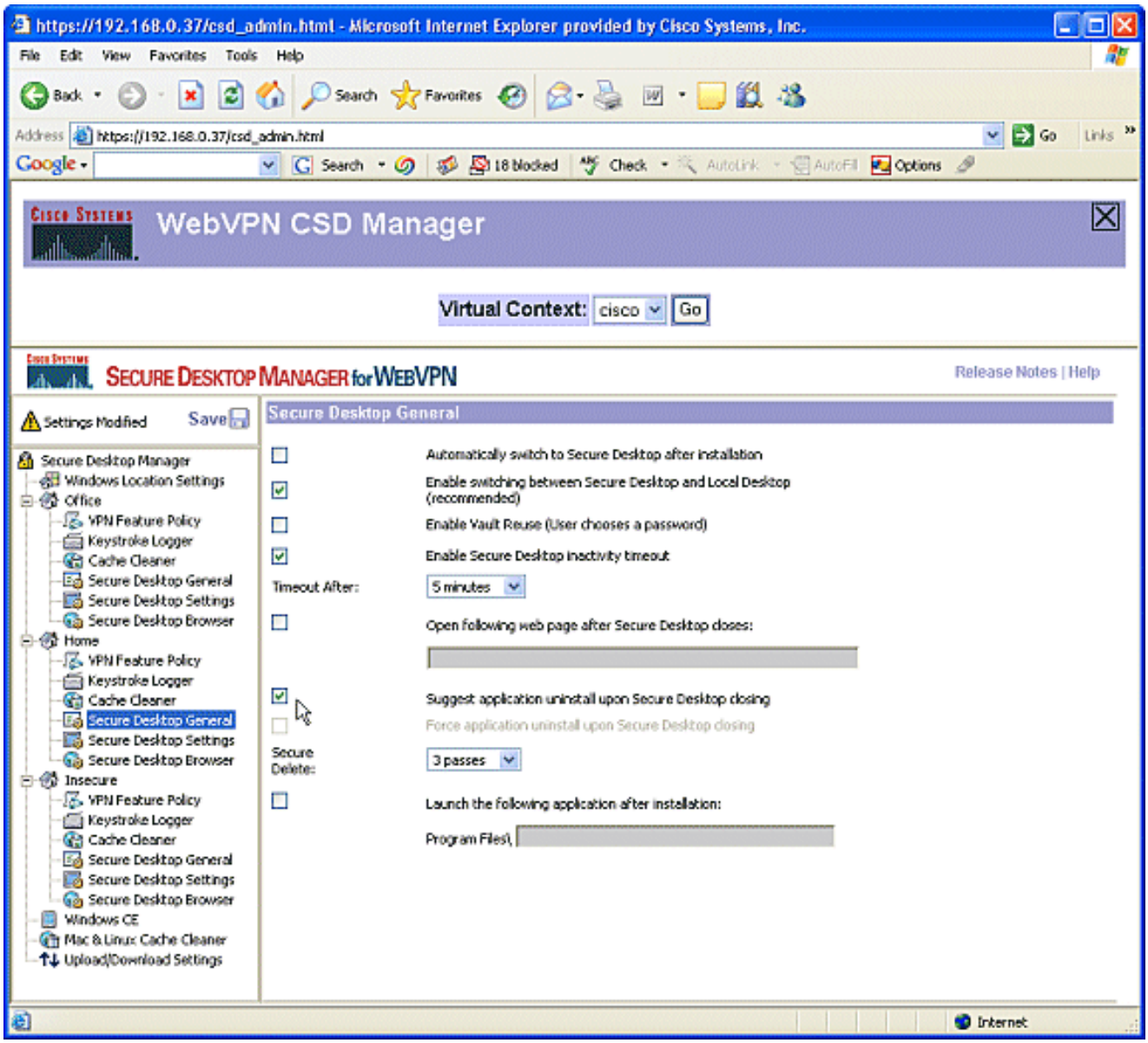
    c. Quando richiesto, fare clic su Salva, quindi su OK.



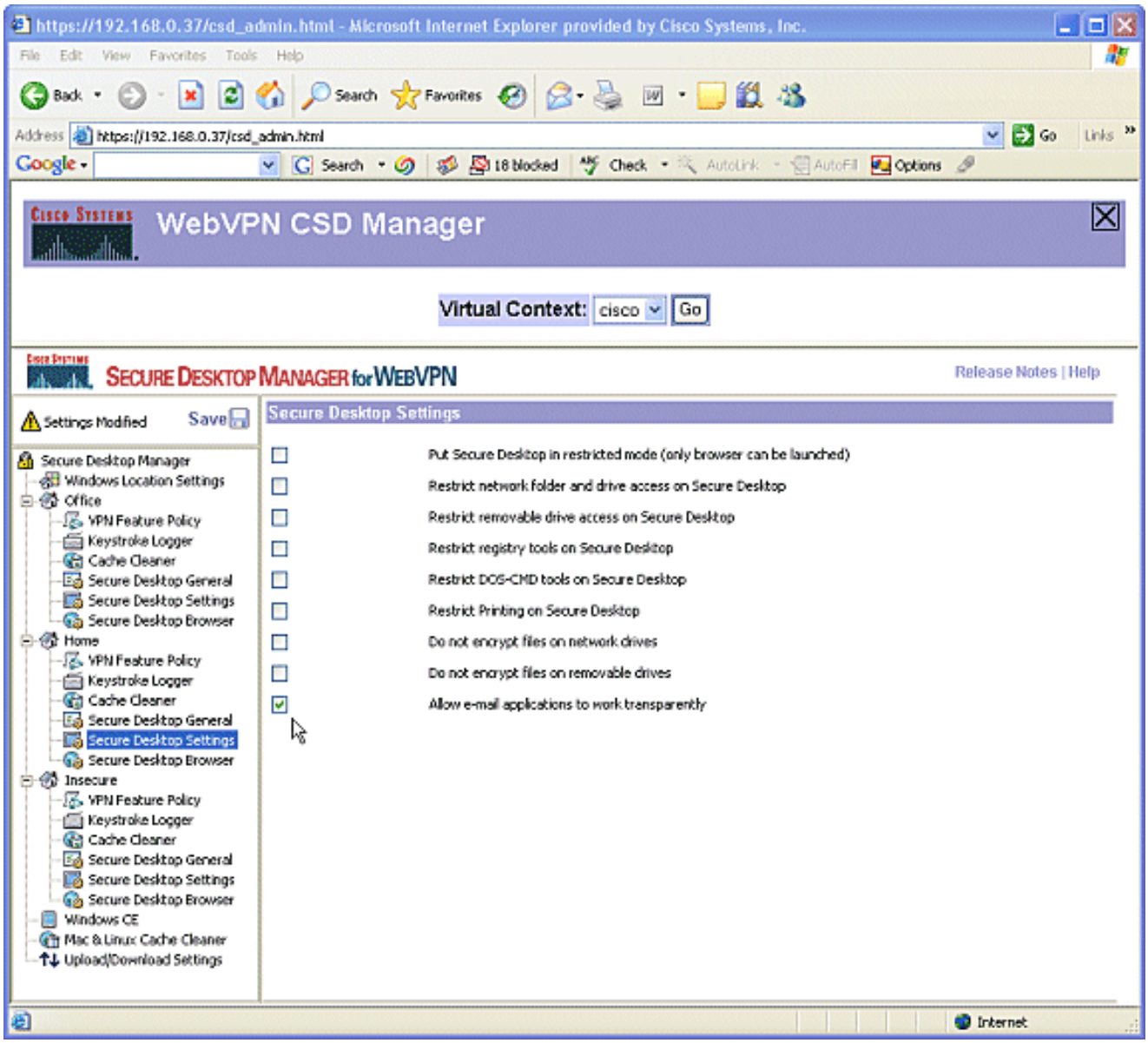
5. Nella posizione delle finestre Home, scegliere Cache Cleaner (Pulitura cache). Mantenere le impostazioni predefinite come illustrato nella schermata.



6. In Home, scegliere Secure Desktop General. Selezionare Suggerisci disinstallazione applicazione alla chiusura di Secure Desktop. Mantenere tutti gli altri parametri nelle impostazioni predefinite, come mostrato nella schermata.



7. Per Impostazioni desktop sicuro in Home, scegliere Consenti alle applicazioni di posta elettronica di funzionare in modo trasparente. Quando richiesto, fare clic su Salva, quindi su OK.



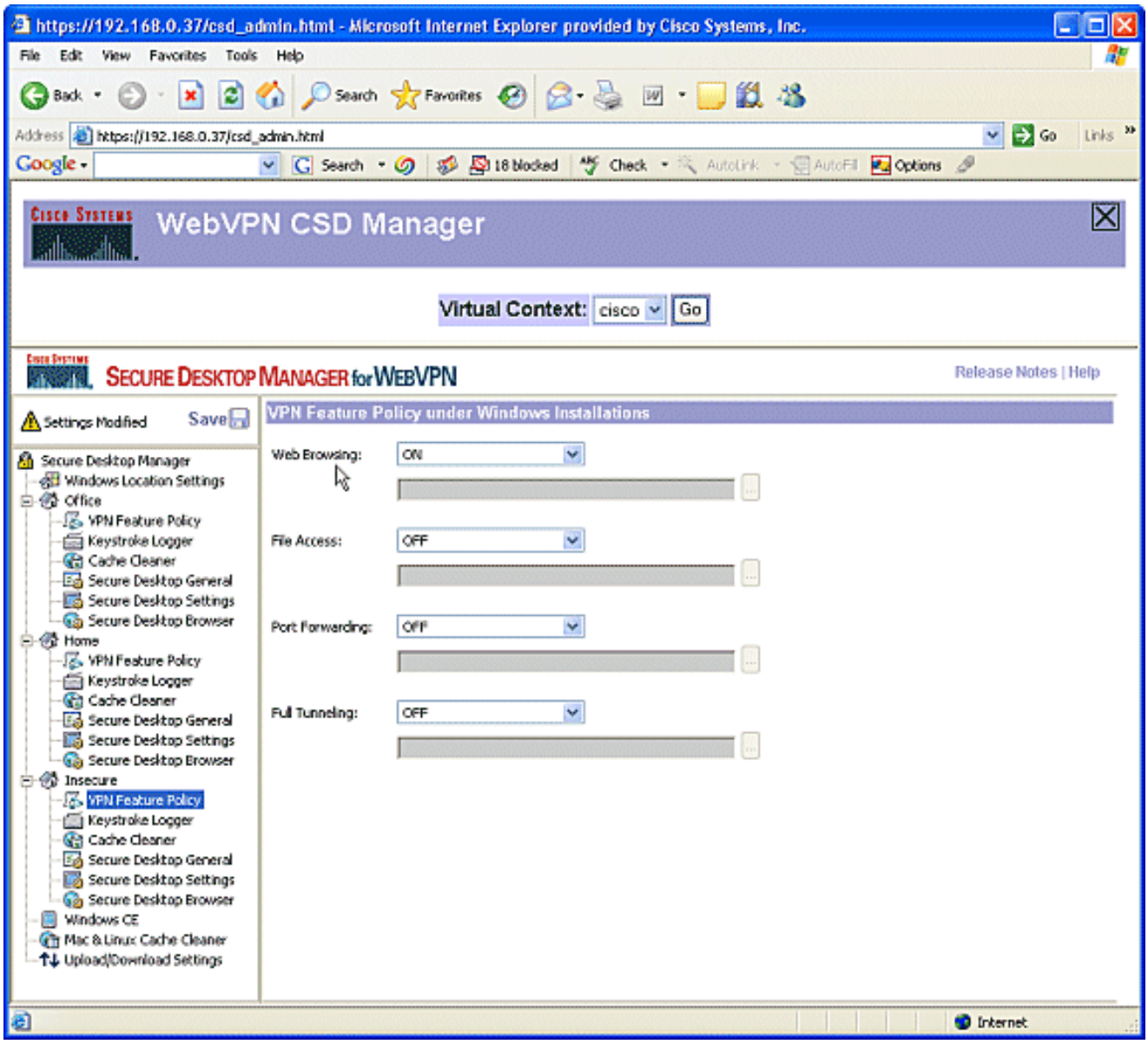
8. La configurazione di Secure Desktop Browser dipende dal fatto che gli utenti desiderino o meno accedere a un sito Web aziendale con i siti preferiti preconfigurati.

    a. In Non sicuro, scegliere VPN Feature Policy (Policy funzionalità VPN).

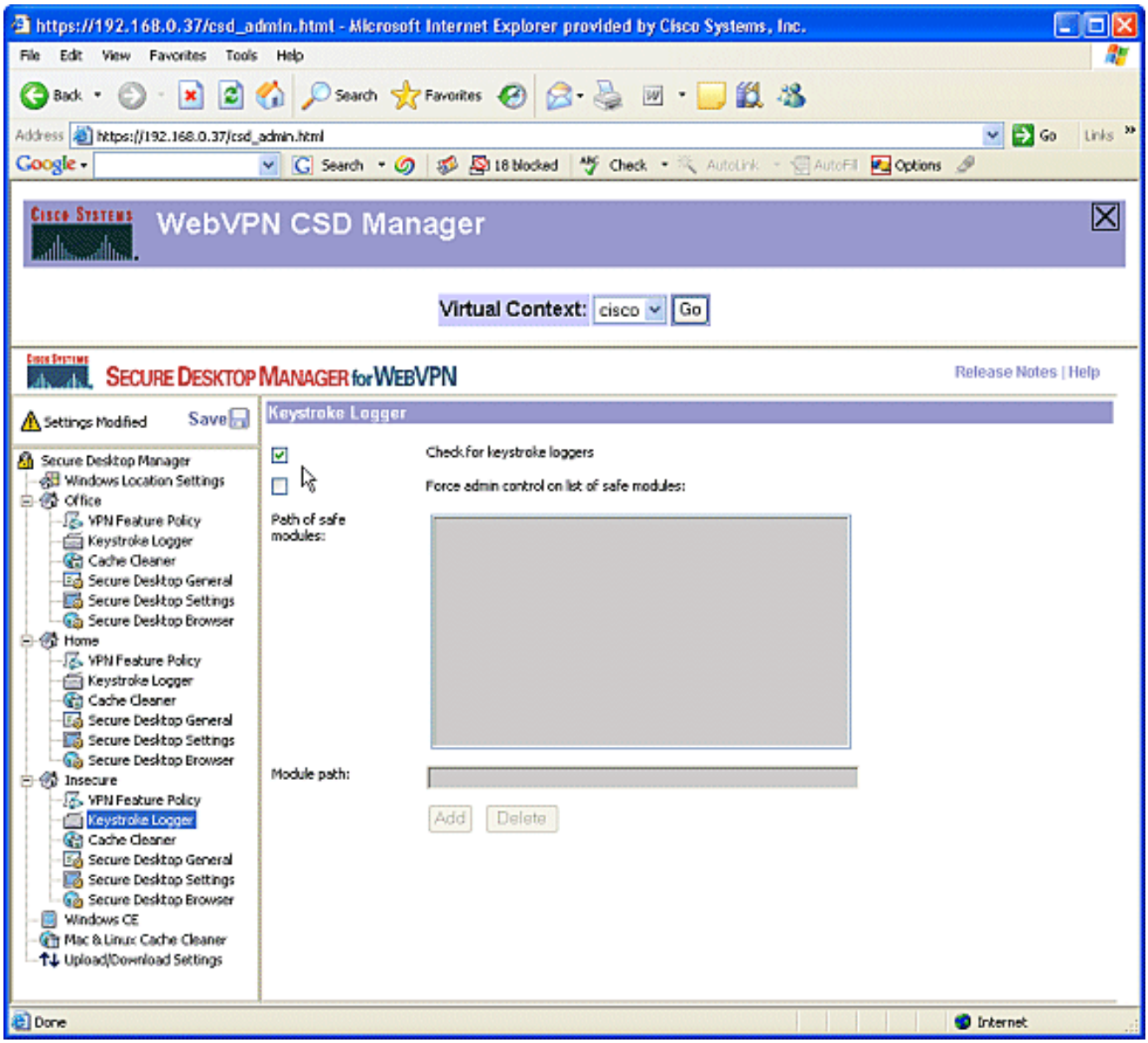
    b. Poiché non si tratta di utenti attendibili, consentire solo l'esplorazione del Web.

    c. Scegliere ON dal menu a discesa per Esplorazione Web.

    d. Tutti gli altri accessi sono impostati su OFF.



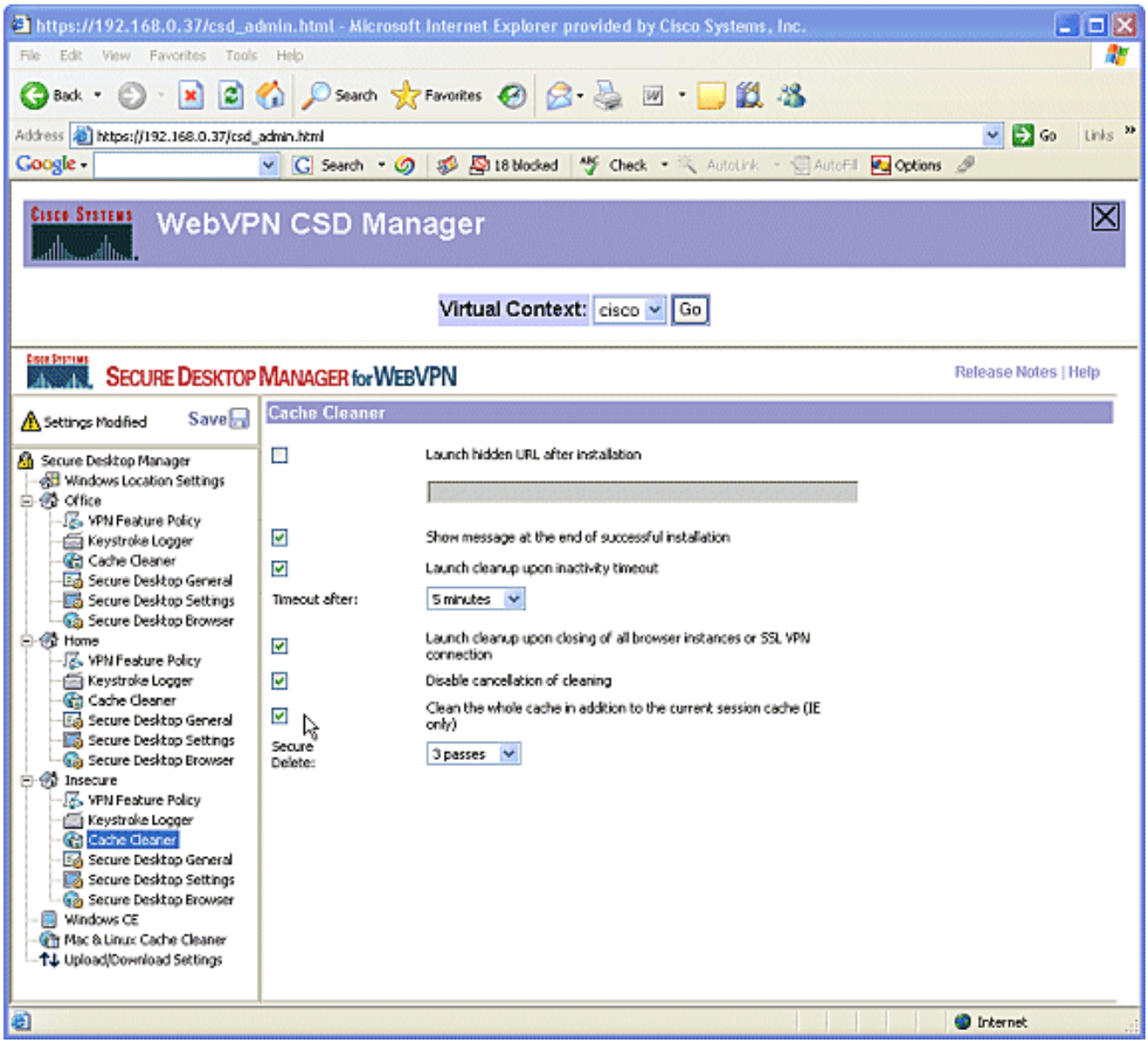
9. Selezionare la casella di controllo Controlla registratori di tasti.



10. Configurare Cache Cleaner per Insecure.

    a. Selezionare la casella di controllo Pulisci l'intera cache oltre alla cache della sessione corrente (solo IE).

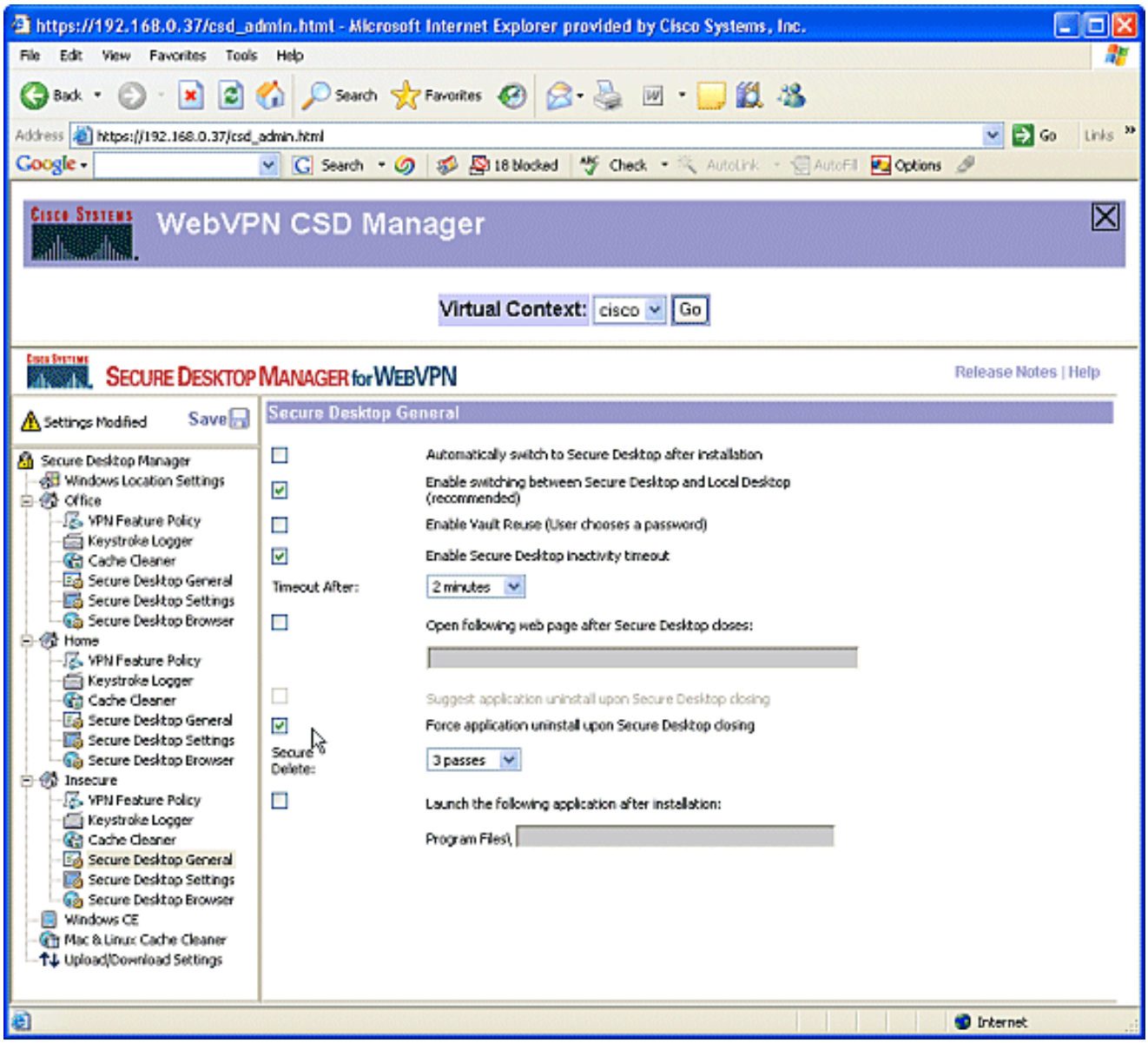
    b. Mantenere le altre impostazioni predefinite.



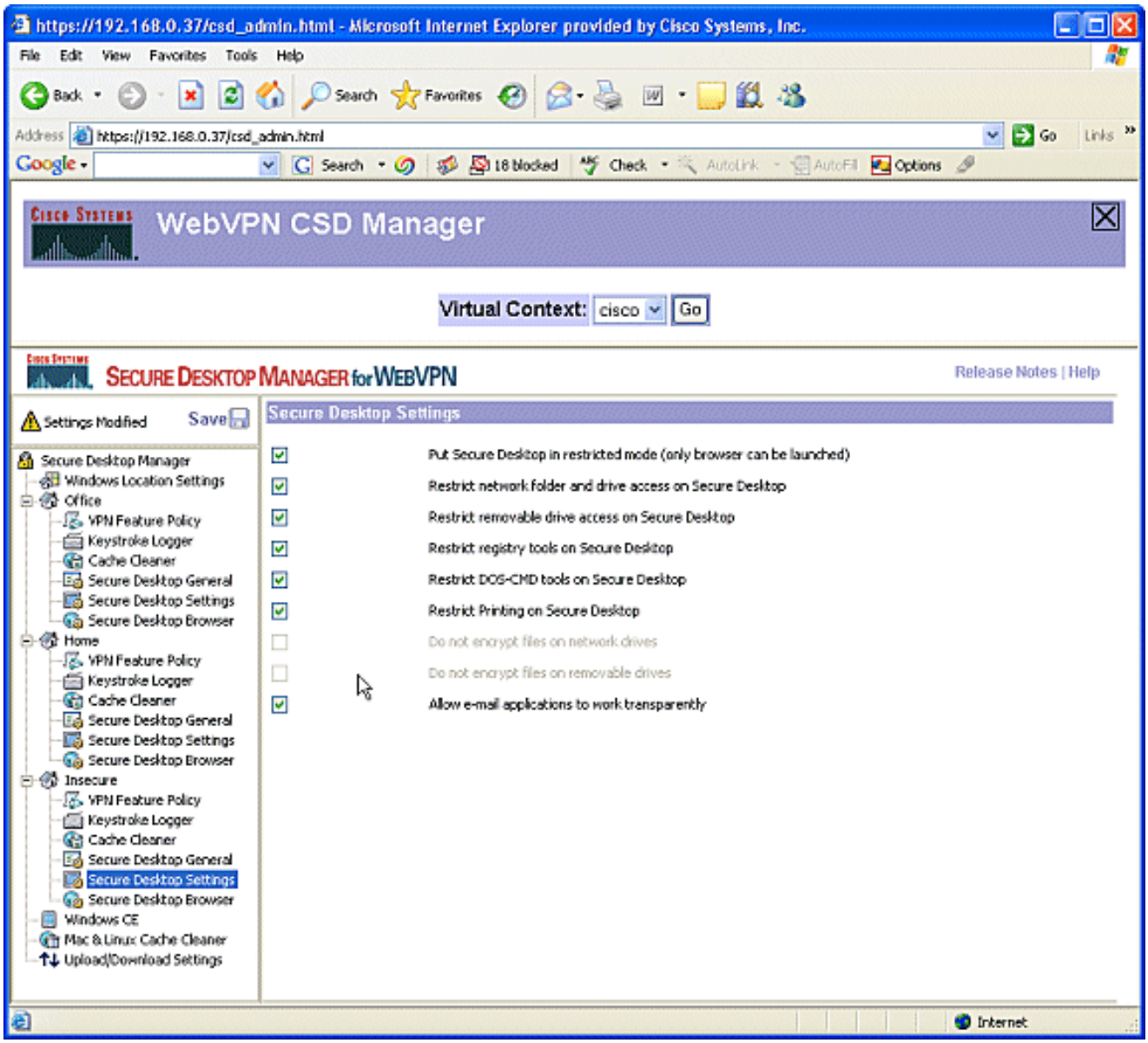
11. In Non sicuro scegliere Desktop sicuro generale.

    a. Ridurre il timeout di inattività a 2 minuti.

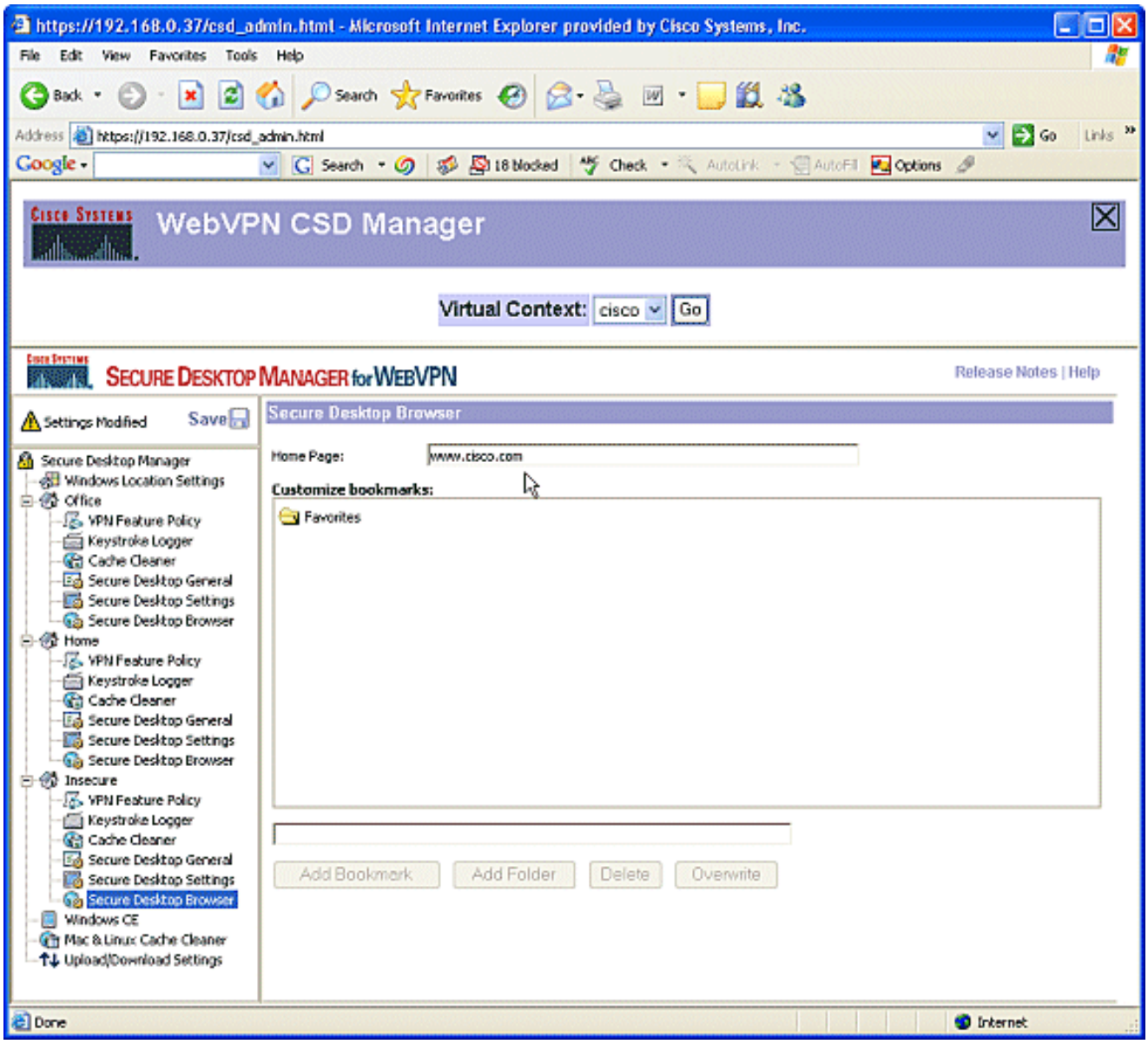
    b. Selezionare la casella di controllo Forza disinstallazione applicazione alla chiusura di Secure Desktop.



12. Scegliere Impostazioni desktop sicuro in Non sicuro e configurare le impostazioni molto restrittive come mostrato.



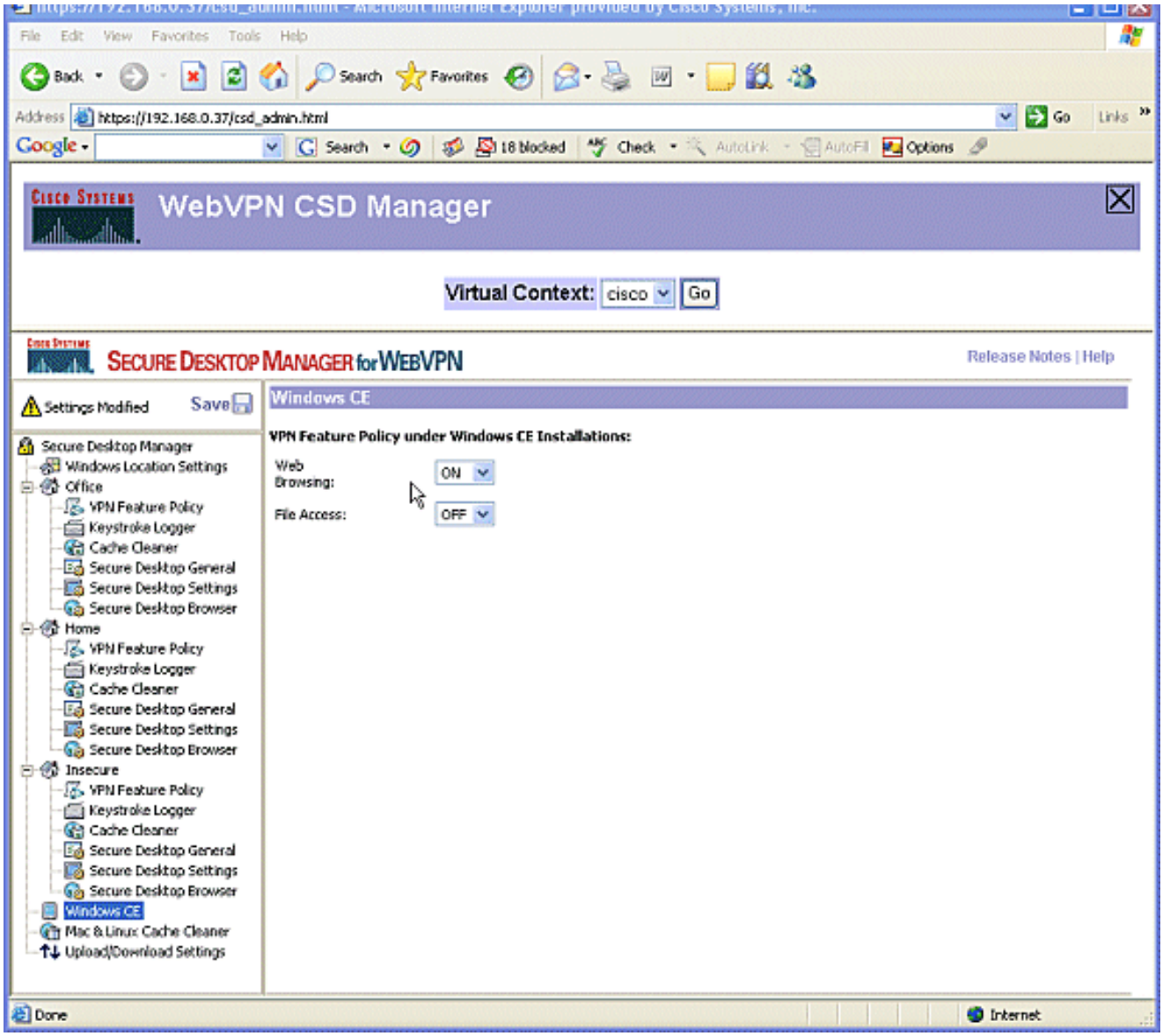
13. Scegliere Secure Desktop Browser. Nel campo Home page, immettere il sito Web a cui i client verranno indirizzati per la home page.



Fase II: configurare le funzionalità di Windows CE, Macintosh e Linux.

Configurare le funzionalità CSD per Windows CE, Macintosh e Linux.

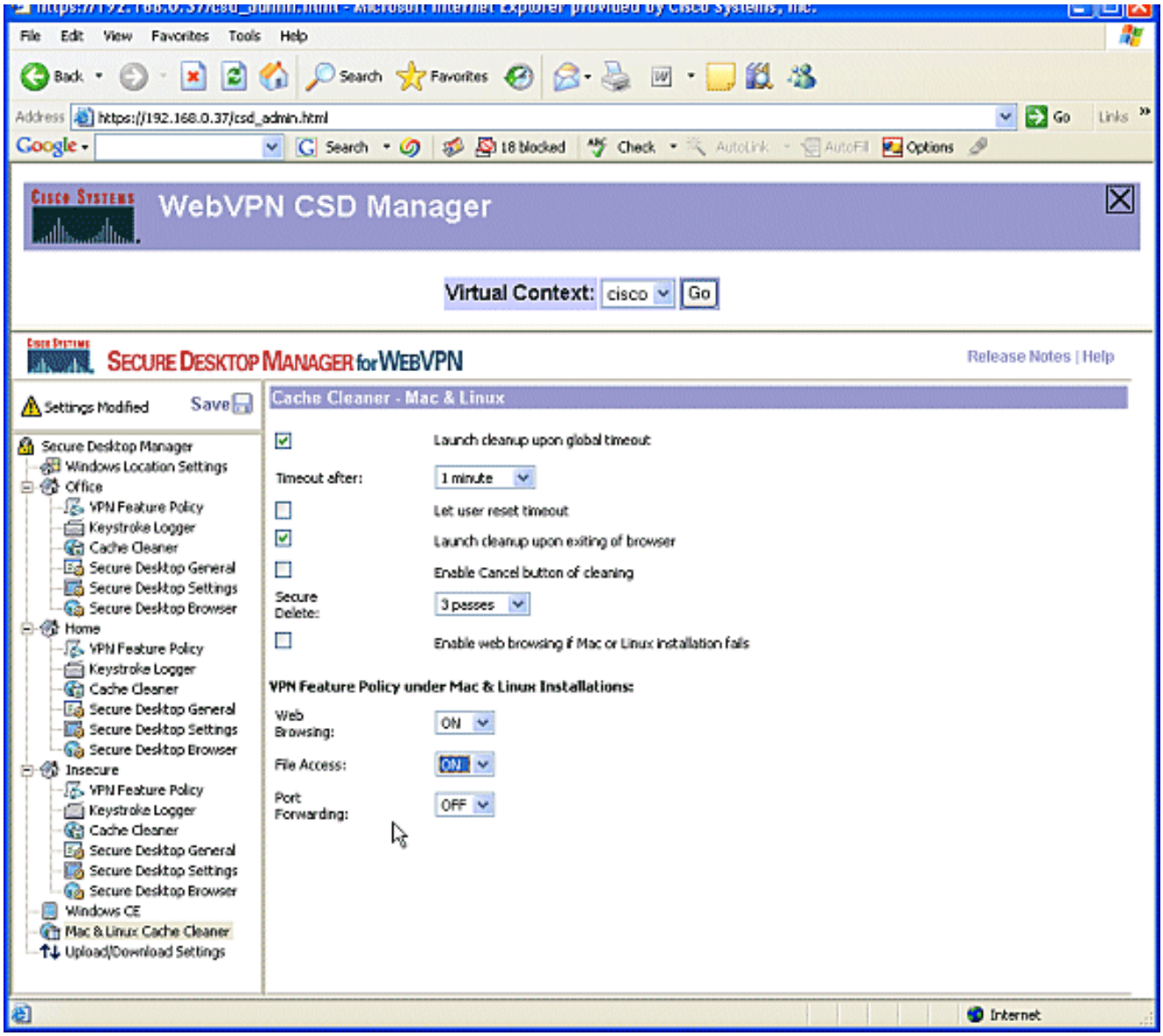
1. Scegliere Windows CE in Secure Desktop Manager. Windows CE dispone di funzionalità VPN limitate. Attivare Esplorazione Web.



2. Scegliere Mac & Linux Cache Cleaner.

    a. I sistemi operativi Macintosh e Linux hanno accesso solo agli aspetti di eliminazione della cache di CSD. Configurarle come illustrato nell'immagine.

    b. Quando richiesto, fare clic su Salva, quindi su OK.

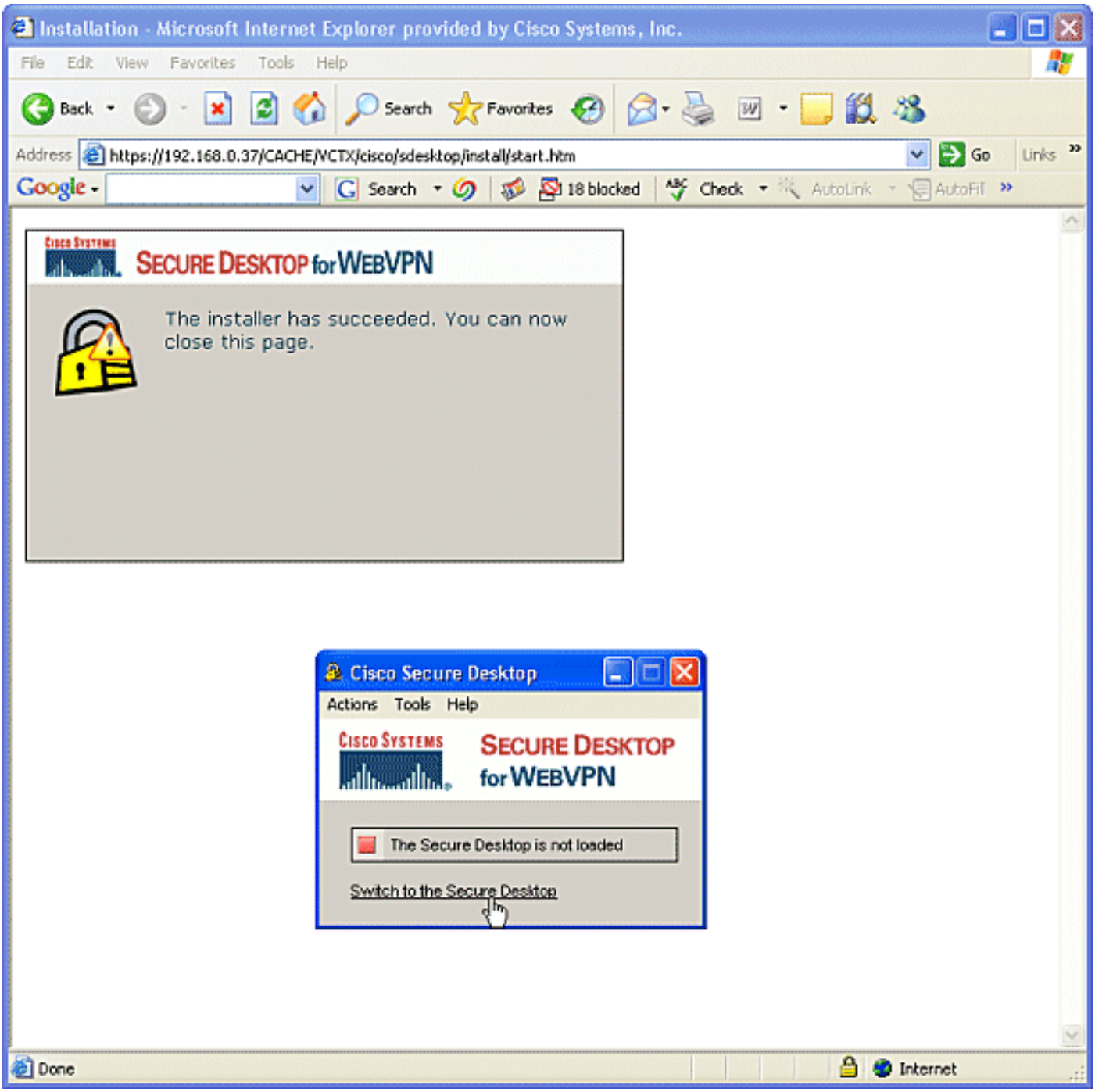


Verifica

Testare il funzionamento del CSD

Verificare il funzionamento del CSD connettendosi al gateway WebVPN con un browser abilitato per SSL all'indirizzo https://WebVPN_Gateway_IP Address.

Nota: ricordarsi di utilizzare il nome univoco del contesto se sono stati creati contesti WebVPN diversi, ad esempio https://192.168.0.37/cisco.



Comandi

Diversi comandi show sono associati a WebVPN. È possibile eseguire questi comandi dall'interfaccia della riga di comando (CLI) per visualizzare le statistiche e altre informazioni. Per informazioni dettagliate sui comandi show, consultare il documento sulla verifica della configurazione di WebVPN.

Nota: CLI Analyzer (solo utenti registrati) supporta alcuni comandi show. Usare CLI Analyzer per visualizzare un'analisi dell'output del comando show.

Risoluzione dei problemi

Comandi

Diversi comandi debug sono associati a WebVPN. Per informazioni dettagliate su questi comandi, consultare il documento sull'uso dei comandi di debug di WebVPN.

Nota: l'uso dei comandi di debug può avere un impatto negativo sul dispositivo Cisco. Prima di usare i comandi di debug, consultare la sezione Informazioni importanti sui comandi di debug.

Per ulteriori informazioni sui comandi clear, consultare il documento sull'utilizzo dei comandi WebVPN Clear.

Informazioni correlate

- Guida all'installazione di WebVPN e DMVPN Convergence
- SSL VPN - WebVPN
- Cisco IOS SSLVPN
- Documentazione e supporto tecnico – Cisco Systems

Informazioni su questa traduzione

Cisco ha tradotto questo documento utilizzando una combinazione di tecnologie automatiche e umane per offrire ai nostri utenti in tutto il mondo contenuti di supporto nella propria lingua. Si noti che anche la migliore traduzione automatica non sarà mai accurata come quella fornita da un traduttore professionista. Cisco Systems, Inc. non si assume alcuna responsabilità per l’accuratezza di queste traduzioni e consiglia di consultare sempre il documento originale in inglese (disponibile al link fornito).