Configurer CSD sur Cisco IOS à l'aide de SDM

Contenu

Introduction

Bien que les sessions VPN SSL (Secure Sockets Layer) (Cisco WebVPN) soient sécurisées, il se peut que le client dispose encore de cookies, de fichiers de navigateur et de pièces jointes d'e-mail une fois la session terminée. Cisco Secure Desktop (CSD) étend la sécurité inhérente aux sessions VPN SSL en écrivant des données de session dans un format chiffré à une zone *coffre* spéciale du disque du client. En outre, ces données sont supprimées du disque à la fin de la session VPN SSL. Ce document présente un exemple de configuration pour CSD sur un routeur Cisco IOS®.

Le CSD est pris en charge sur les plates-formes de périphériques Cisco suivantes :

- Routeurs Cisco IOS version 12.4(6)T et ultérieure
- Cisco 870, 1811, 1841, 2801, 2811, 2821, 2851, 3725, 3745, 3825, 3845, 7200 et 730 1 routeurs
- Concentrateurs de la gamme Cisco VPN 3000, versions 4.7 et ultérieures
- Appareils de sécurité de la gamme Cisco ASA 5500, versions 7.1 et ultérieures
- Module de services Cisco WebVPN pour Cisco Catalyst et Cisco 7600, versions 1.2 et

ultérieures

Conditions préalables

Conditions requises

Assurez-vous que vous répondez à ces exigences avant d'essayer cette configuration :

Configuration requise pour le routeur Cisco IOS

- Routeur Cisco IOS avec image avancée 12.4(6T) ou ultérieure
- Cisco Router Secure Device Manager (SDM) 2.3 ou supérieur
- Une copie du package CSD pour IOS sur votre poste de gestion
- Certificat numérique ou authentification autosigné d'un routeur avec une autorité de certification (CA)**Remarque :** chaque fois que vous utilisez des certificats numériques, assurez-vous de définir correctement le nom d'hôte, le nom de domaine et la date/heure/fuseau horaire du routeur.
- Mot de passe secret actif sur le routeur
- DNS activé sur votre routeur. Plusieurs services WebVPN nécessitent que DNS fonctionne correctement.

Configuration requise pour les ordinateurs clients

- Les clients distants doivent disposer de privilèges d'administration locaux ; il n'est pas nécessaire, mais il est fortement suggéré.
- Les clients distants doivent disposer de Java Runtime Environment (JRE) version 1.4 ou ultérieure.
- Navigateurs clients distants : Internet Explorer 6.0, Netscape 7.1, Mozilla 1.7, Safari 1.2.2 ou Firefox 1.0
- Cookies activés et fenêtres publicitaires intempestives autorisées sur les clients distants

Components Used

Les informations contenues dans ce document sont basées sur les versions de matériel et de logiciel suivantes :

- Routeur Cisco IOS 3825 avec version 12.9(T)
- SDM version 2.3.1

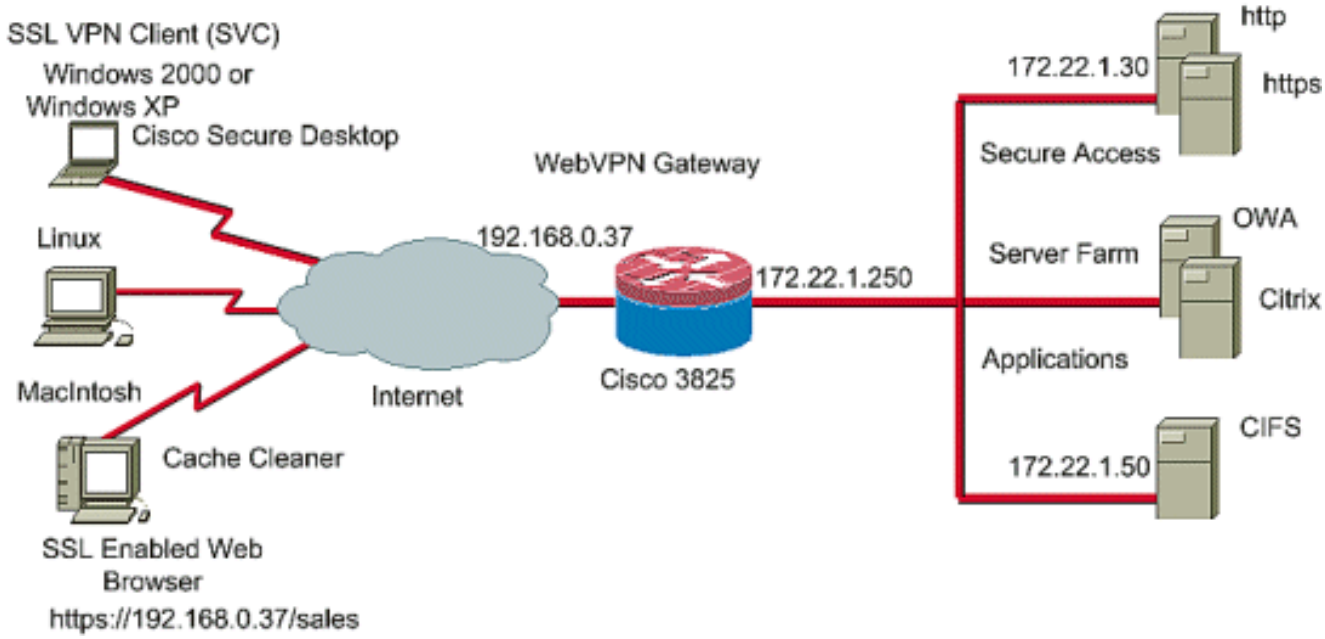
The information in this document was created from the devices in a specific lab environment. Tous les périphériques utilisés dans ce document ont commencé par une configuration effacée (par défaut). If your network is live, make sure that you understand the potential impact of any command.

Diagramme du réseau

Ce document utilise la configuration réseau suivante :

Cet exemple utilise un routeur de la gamme Cisco 3825 pour permettre un accès sécurisé à l'intranet de l'entreprise. Le routeur de la gamme Cisco 3825 renforce la sécurité des connexions

VPN SSL avec des fonctions et des caractéristiques CSD configurables. Les clients peuvent se connecter au routeur CSD via l'une des trois méthodes VPN SSL suivantes : VPN SSL sans client (WebVPN), VPN SSL client léger (transfert de port) ou client VPN SSL (SVC Full Tunneling).



Produits connexes

Cette configuration peut également être utilisée avec les versions de matériel et de logiciel suivantes :

- Plates-formes de routeurs Cisco 870,1811,1841,2801,2811,2821 2851,3725,3745,3825,3845, 720 et 7 01
- Image de sécurité avancée Cisco IOS version 12.4(6)T et ultérieure

Conventions

Reportez-vous aux Conventions des conseils techniques Cisco pour plus d'informations sur les conventions du document.

Configuration

Une passerelle WebVPN permet à un utilisateur de se connecter au routeur via l'une des technologies VPN SSL. Une seule passerelle WebVPN par adresse IP est autorisée sur le périphérique, bien que plusieurs contextes WebVPN puissent être connectés à une passerelle WebVPN. Chaque contexte est identifié par un nom unique. Les stratégies de groupe identifient les ressources configurées disponibles pour un contexte WebVPN particulier.

La configuration du CSD sur un routeur IOS se fait en deux phases :

Phase I : Préparez votre routeur à la configuration CSD avec SDM

1. Configurez une passerelle WebVPN, un contexte WebVPN et une stratégie de groupe.**Remarque :** Cette étape est facultative et n'est pas traitée en détail dans ce

document. Si vous avez déjà configuré votre routeur pour l'une des technologies VPN SSL, omettez cette étape.
2. Activez CSD dans un contexte WebVPN.

Phase II : Configurez CSD à l'aide d'un navigateur Web.

1. Définissez *les emplacements Windows*.
2. Identifier les critères de localisation .
3. Configurez les modules et les fonctions d'emplacement Windows.
4. Configurez les fonctionnalités Windows CE, Macintosh et Linux.

Phase I : Préparez votre routeur à la configuration CSD avec SDM.

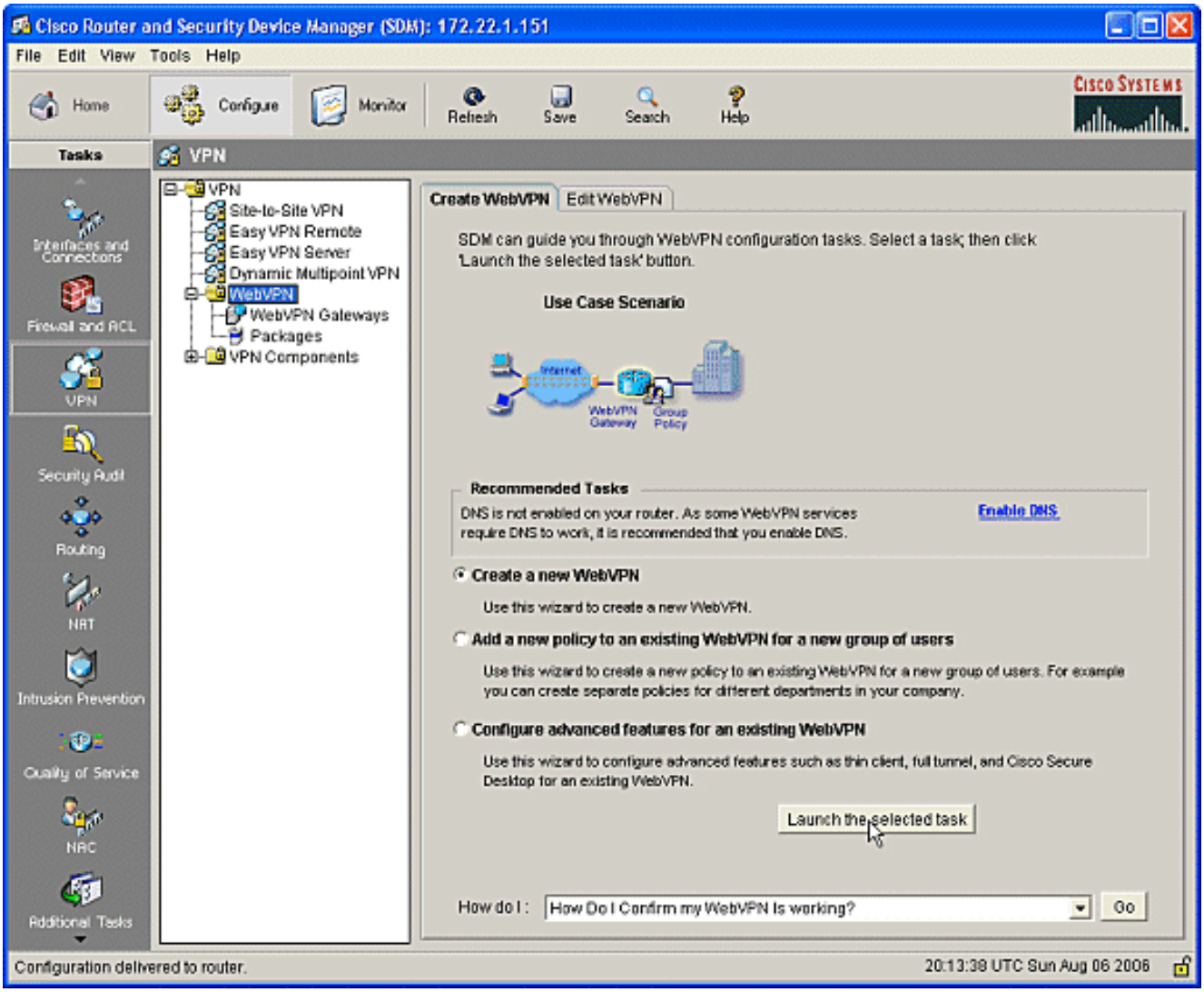
Le CSD peut être configuré avec SDM ou à partir de l'interface de ligne de commande (CLI). Cette configuration utilise SDM et un navigateur Web.

Ces étapes sont utilisées pour terminer la configuration de CSD sur votre routeur IOS.

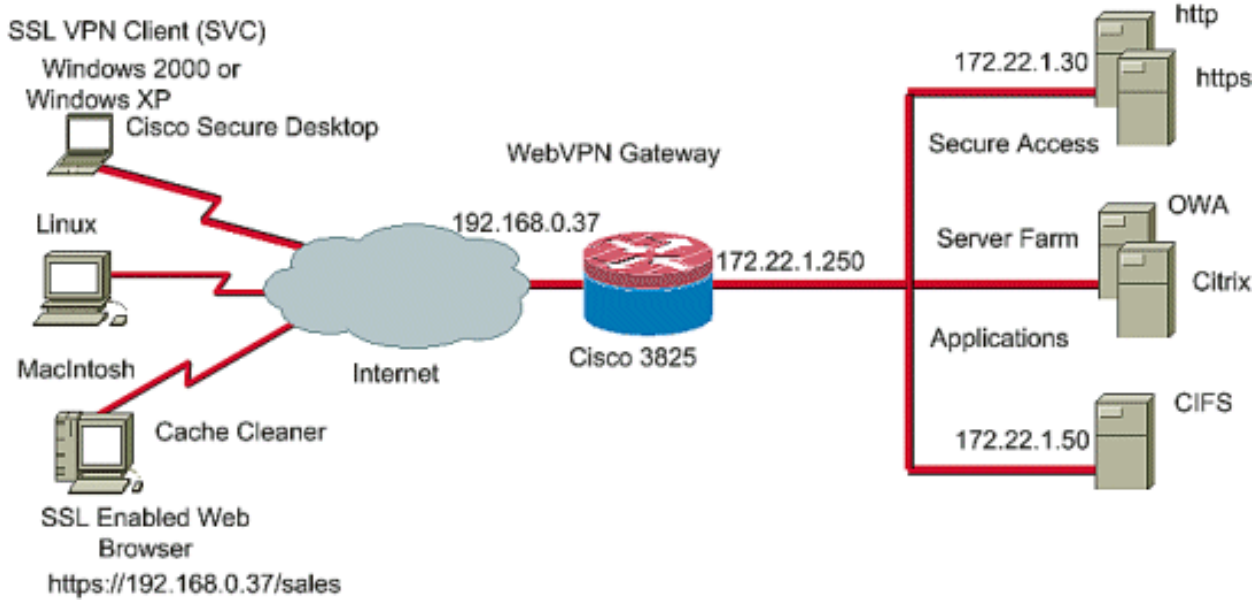
Phase I : Étape 1 : Configurez une passerelle WebVPN, un contexte WebVPN et une stratégie de groupe.

Vous pouvez utiliser l'Assistant WebVPN pour accomplir cette tâche.

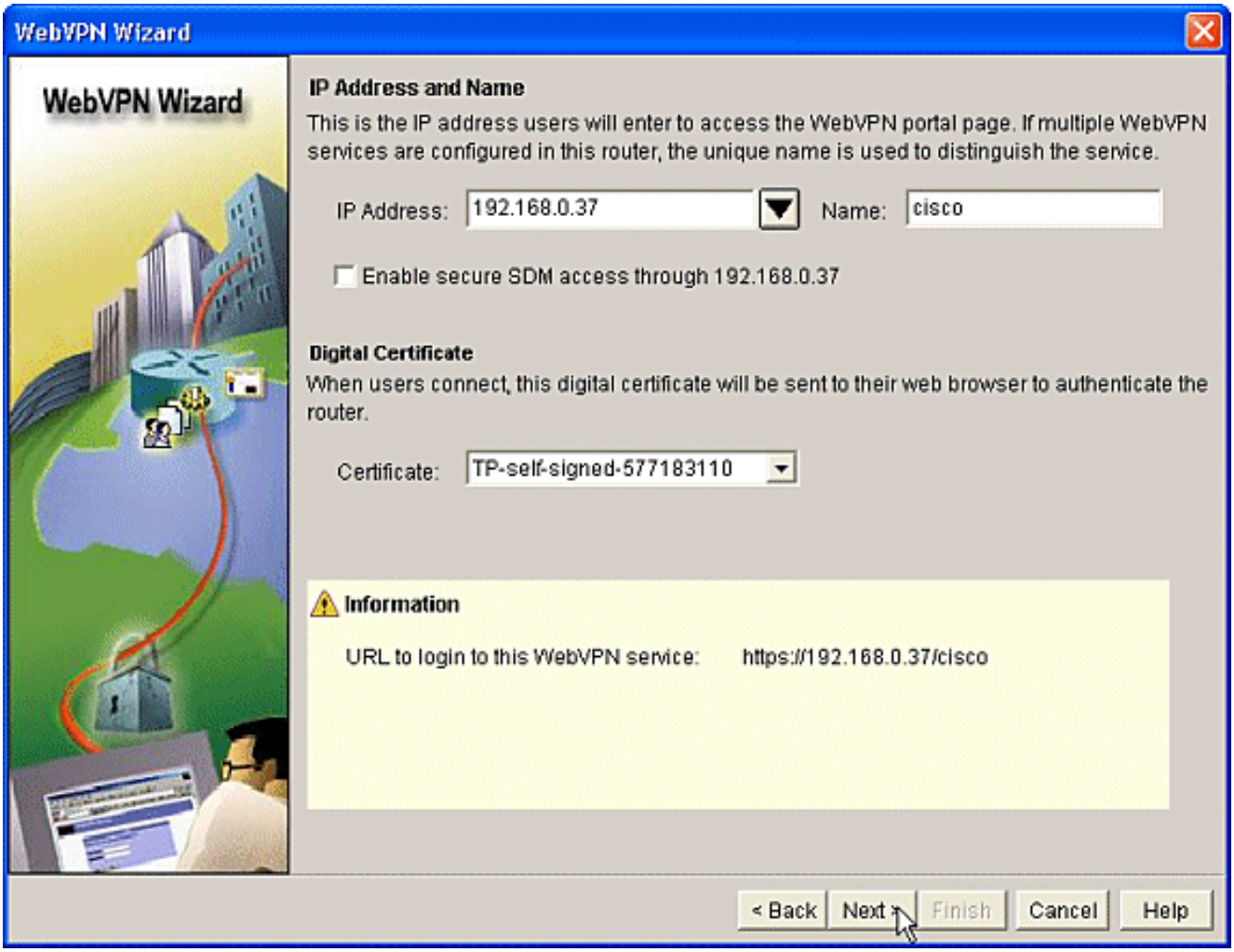
1. Ouvrez SDM et accédez à **Configurer > VPN > WebVPN**. Cliquez sur l'onglet **Create WebVPN** et cochez la case d'option **Create a new WebVPN**. Cliquez sur **Lancer la tâche sélectionnée**.



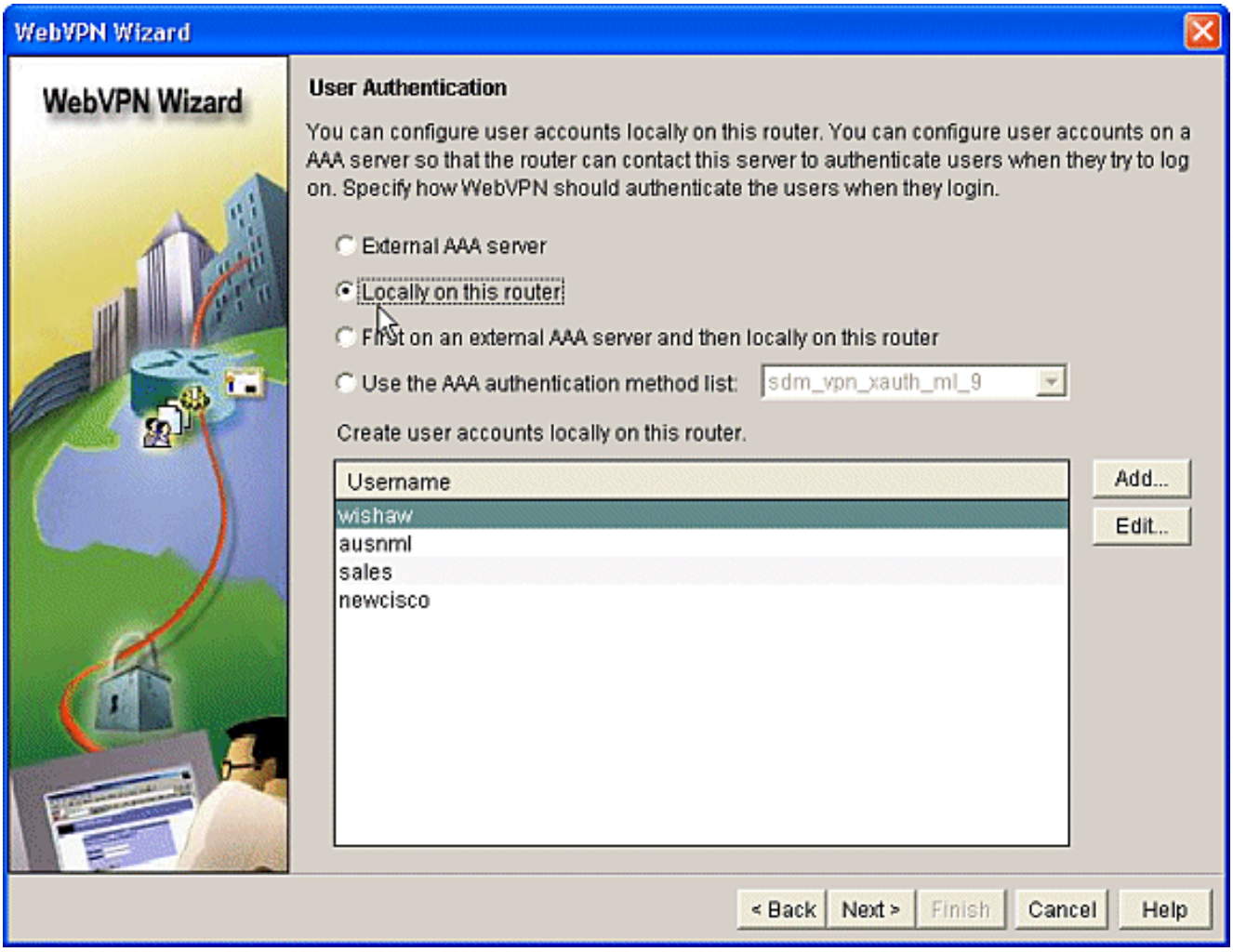
2. L'écran WebVPN Wizard répertorie les paramètres que vous pouvez configurer. Cliquez sur **Next**
(Suivant).



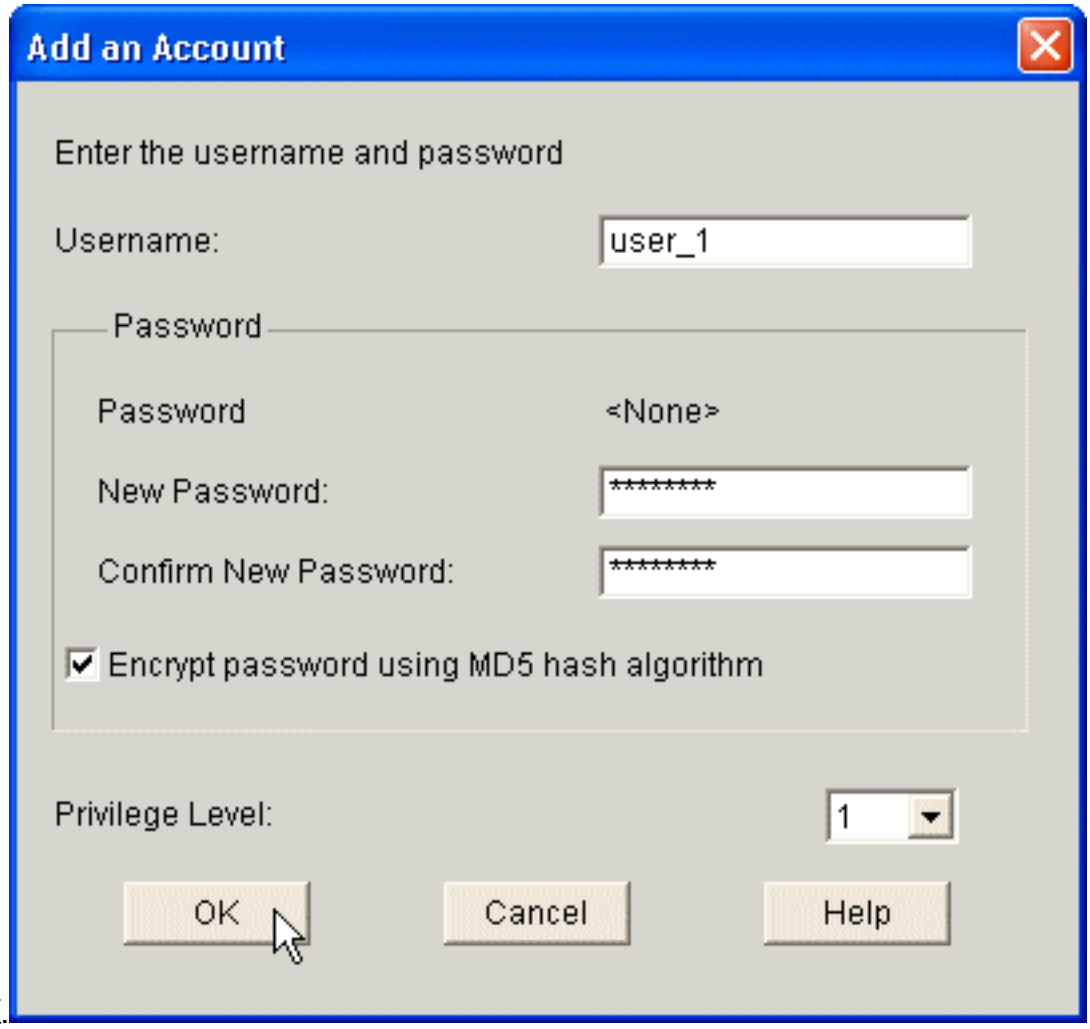
3. Saisissez l'adresse IP de la passerelle WebVPN, un nom unique pour le service et des informations de certificat numérique. Cliquez sur **Next**
(Suivant).



4. Vous pouvez créer des comptes utilisateur pour l'authentification de cette passerelle WebVPN. Vous pouvez utiliser des comptes locaux ou des comptes créés sur un serveur AAA (Authentication, Authorization, and Accounting) externe. Cet exemple utilise des comptes locaux sur le routeur. Cochez la case d'option **Locally sur ce routeur** et cliquez sur **Add**.

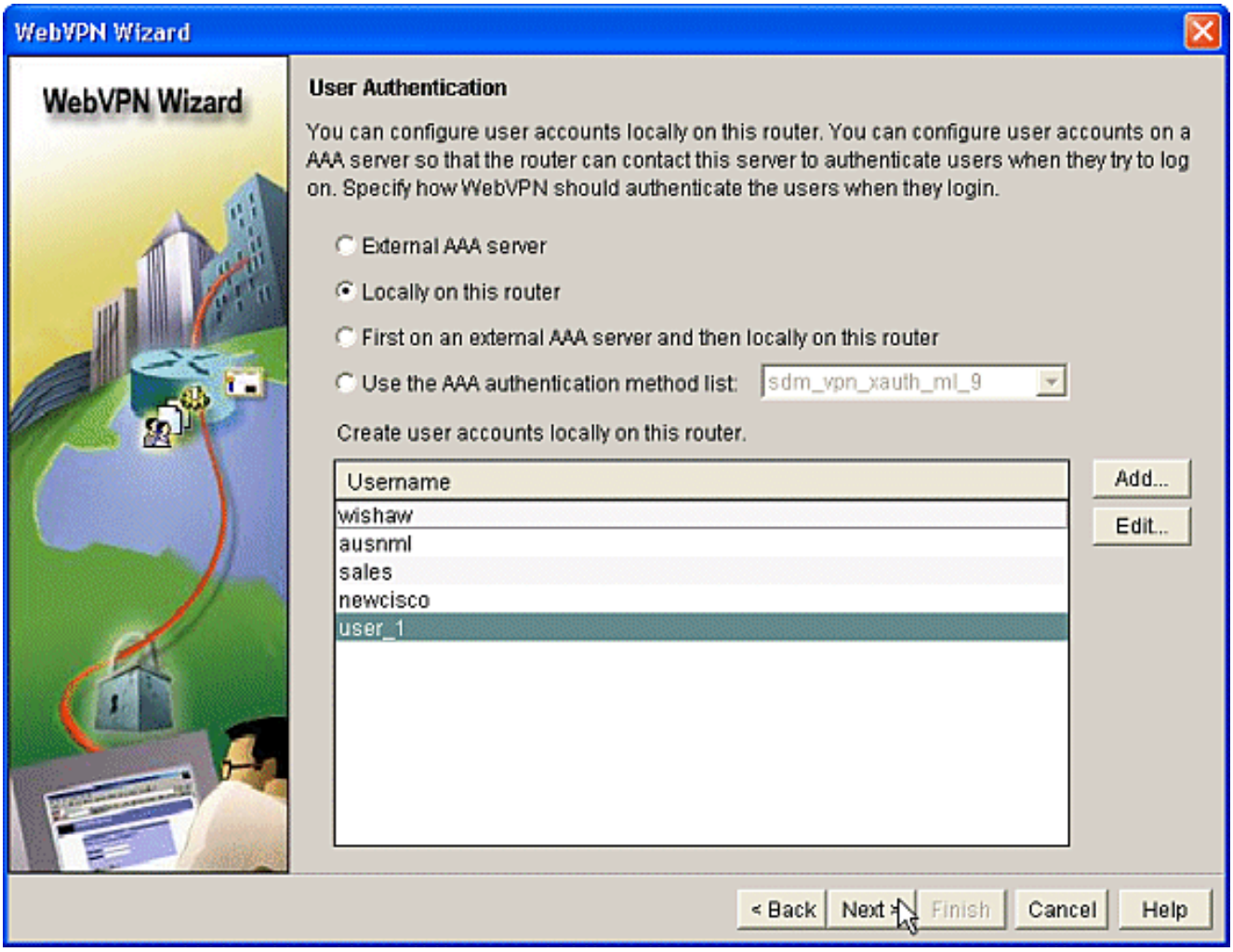


5. Entrez les informations de compte du nouvel utilisateur dans l'écran Ajouter un compte et

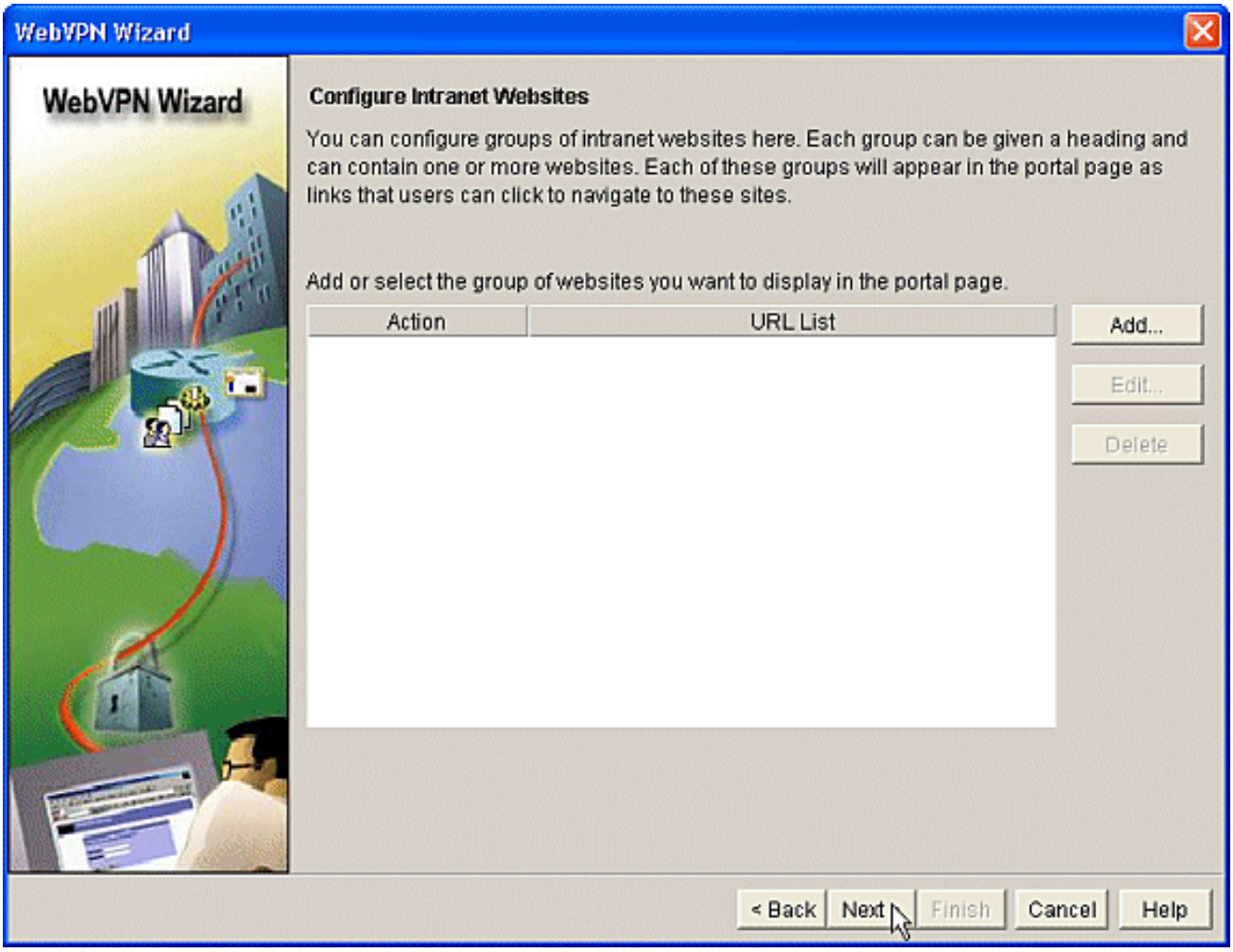


cliquez sur **OK**.

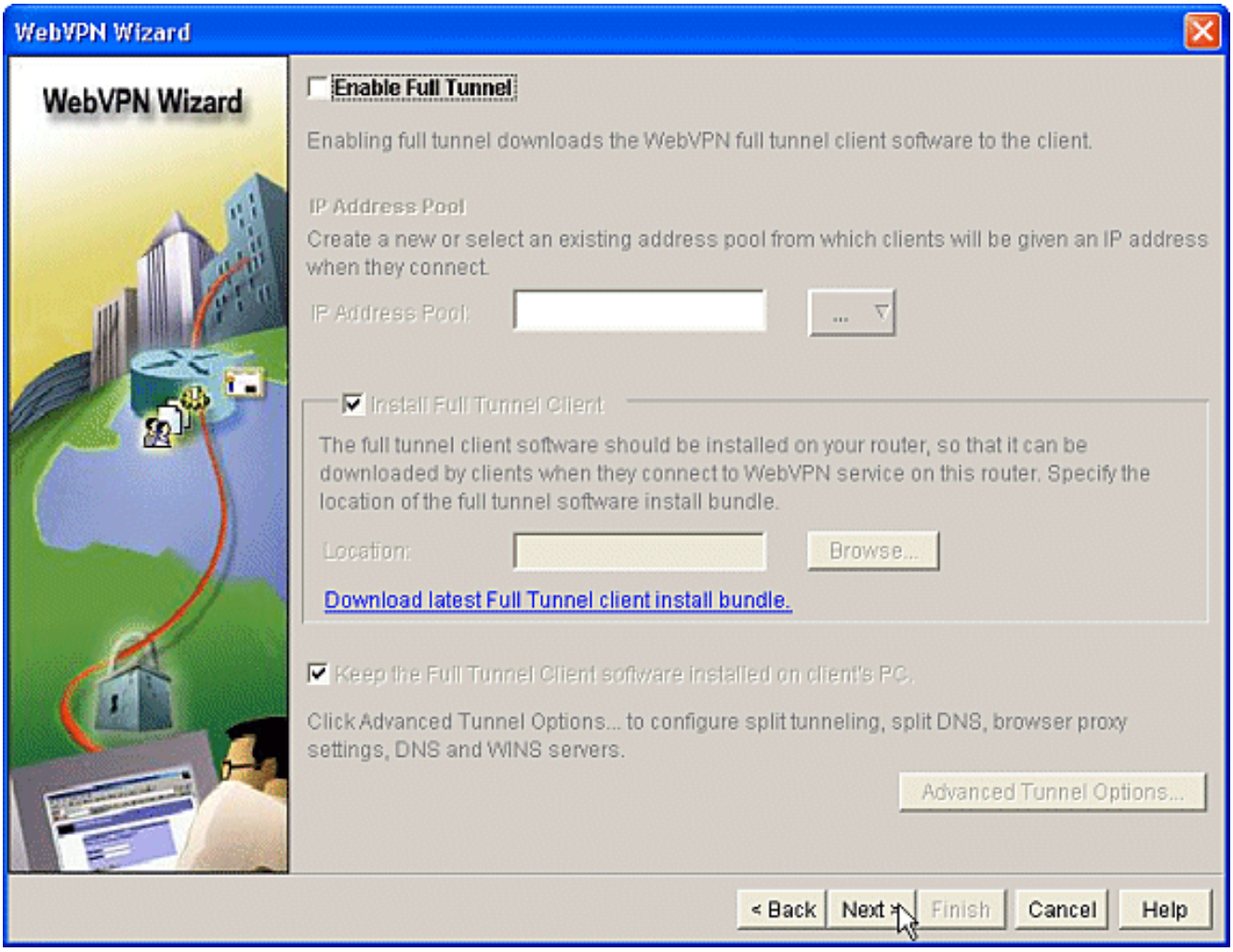
6. Après avoir créé vos utilisateurs, cliquez sur **Suivant** dans la page Authentification utilisateur.



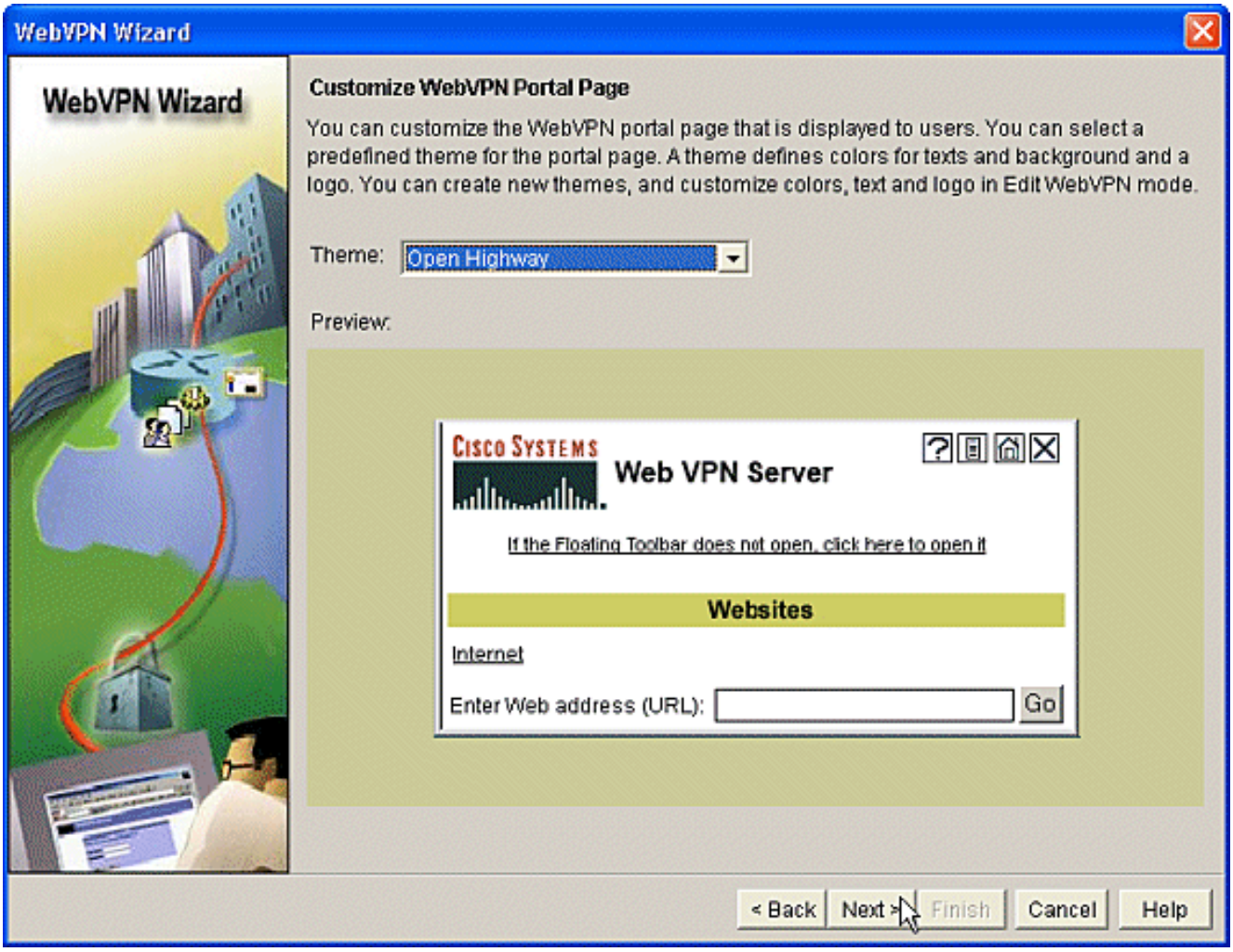
7. L'écran Configurer les sites Web intranet vous permet de configurer le site Web disponible pour les utilisateurs de la passerelle WebVPN. Puisque ce document est axé sur la configuration de CSD, ignorez cette page. Cliquez sur **Next** (Suivant).



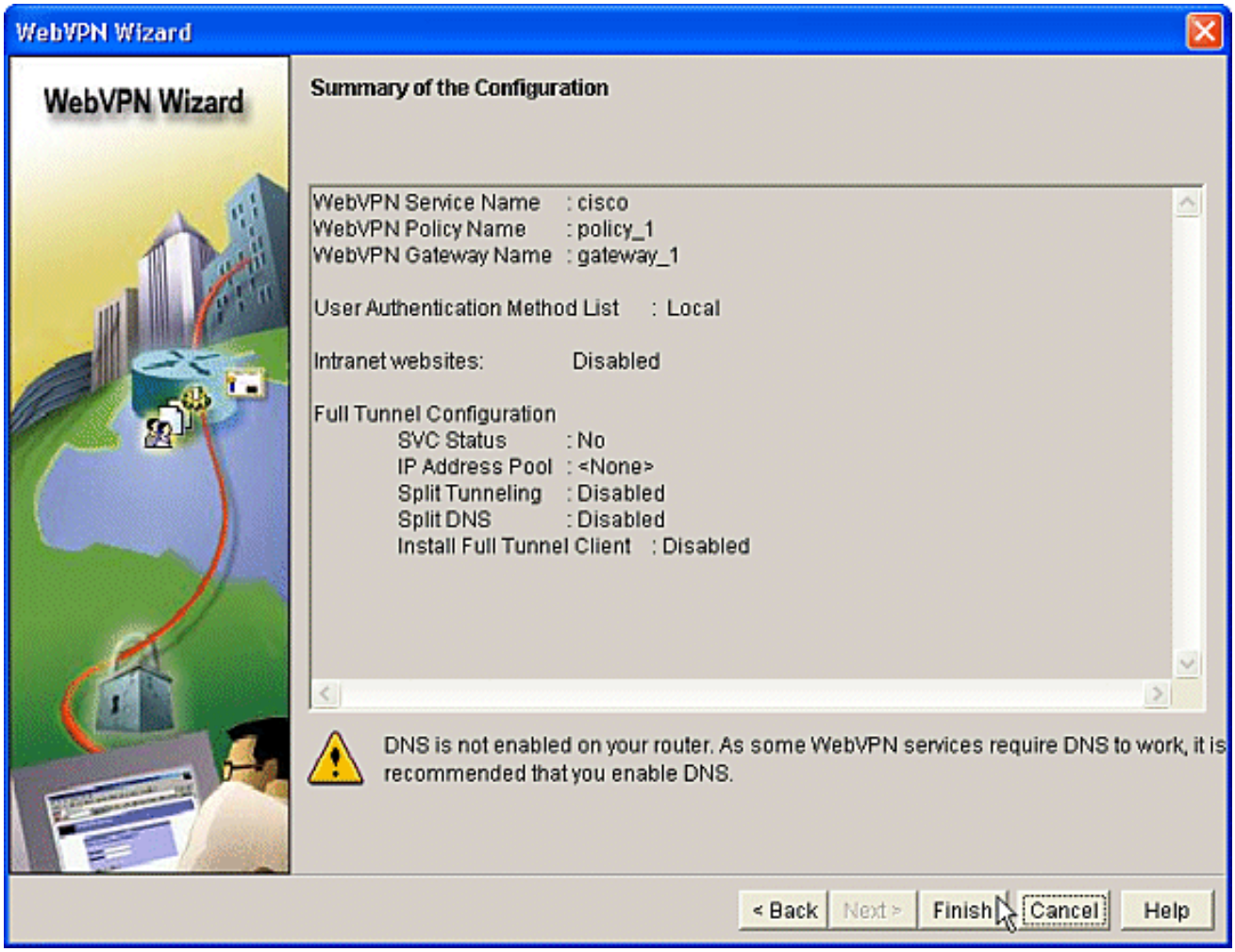
8. Bien que l'écran suivant de l'Assistant WebVPN vous permette de choisir d'activer le client VPN SSL Full Tunnel, l'objectif de ce document est d'activer CSD. Désélectionnez **Enable Full Tunnel** et cliquez sur **Next**.



9. Vous pouvez personnaliser l'apparence de la page WebVPN Portal pour les utilisateurs. Dans ce cas, l'apparence par défaut est acceptée. Cliquez sur **Next** (Suivant).



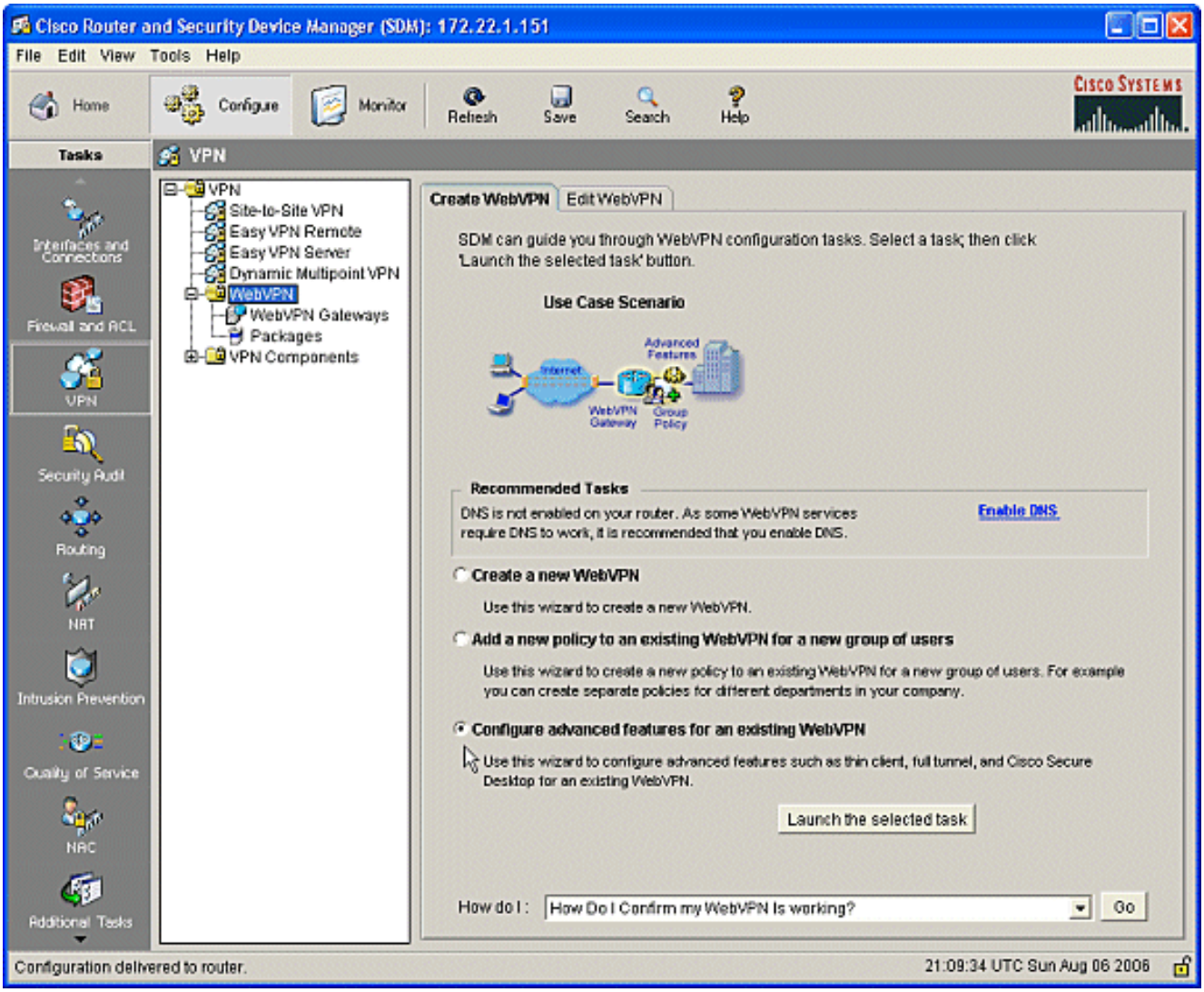
10. L'Assistant affiche le dernier écran de cette série. Il présente un résumé de la configuration de la passerelle WebVPN. Cliquez sur **Terminer** et, lorsque vous y êtes invité, cliquez sur **OK**.



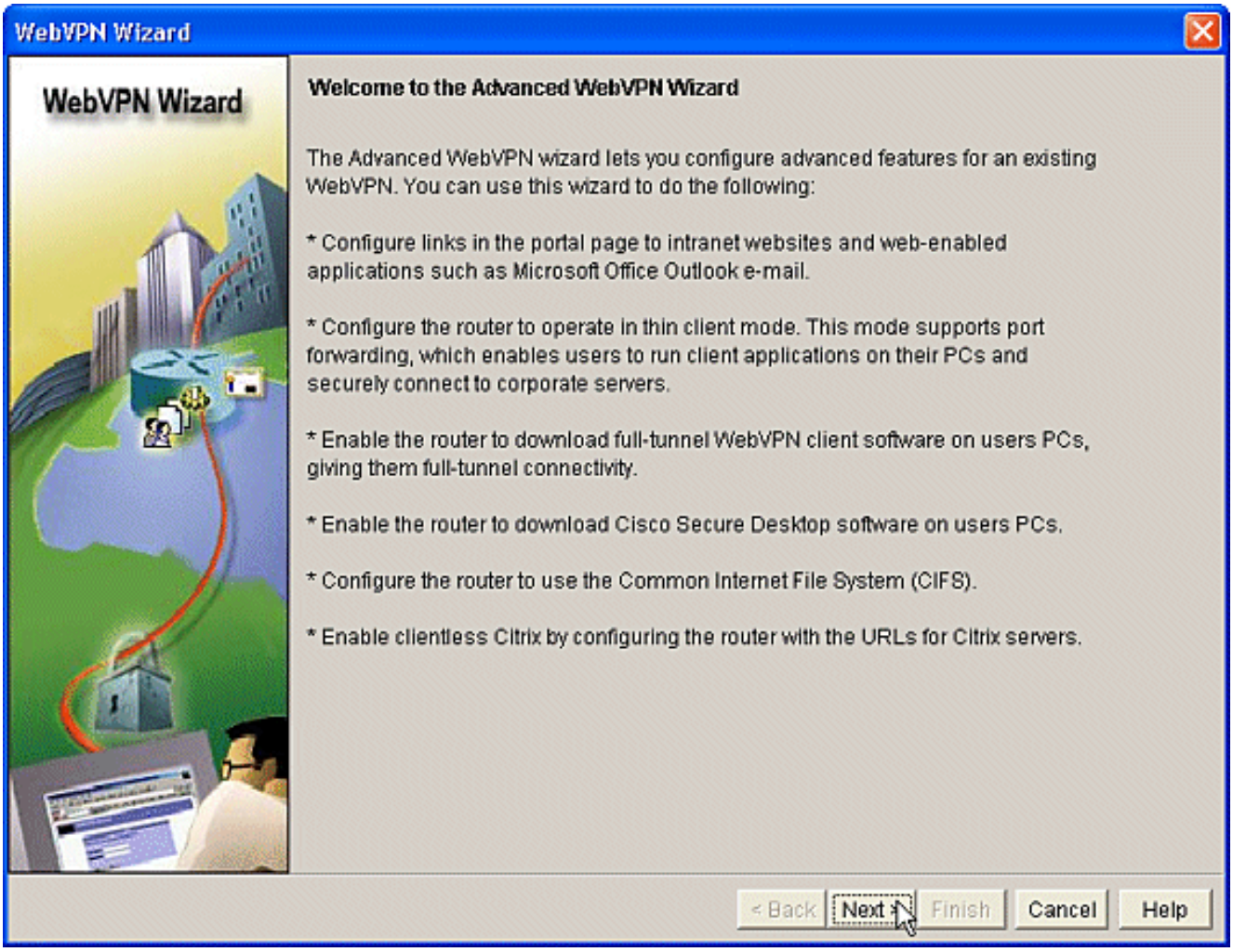
Phase I : Étape 2 : Activez CSD dans un contexte WebVPN.

Utilisez l'Assistant WebVPN pour activer CSD dans un contexte WebVPN.

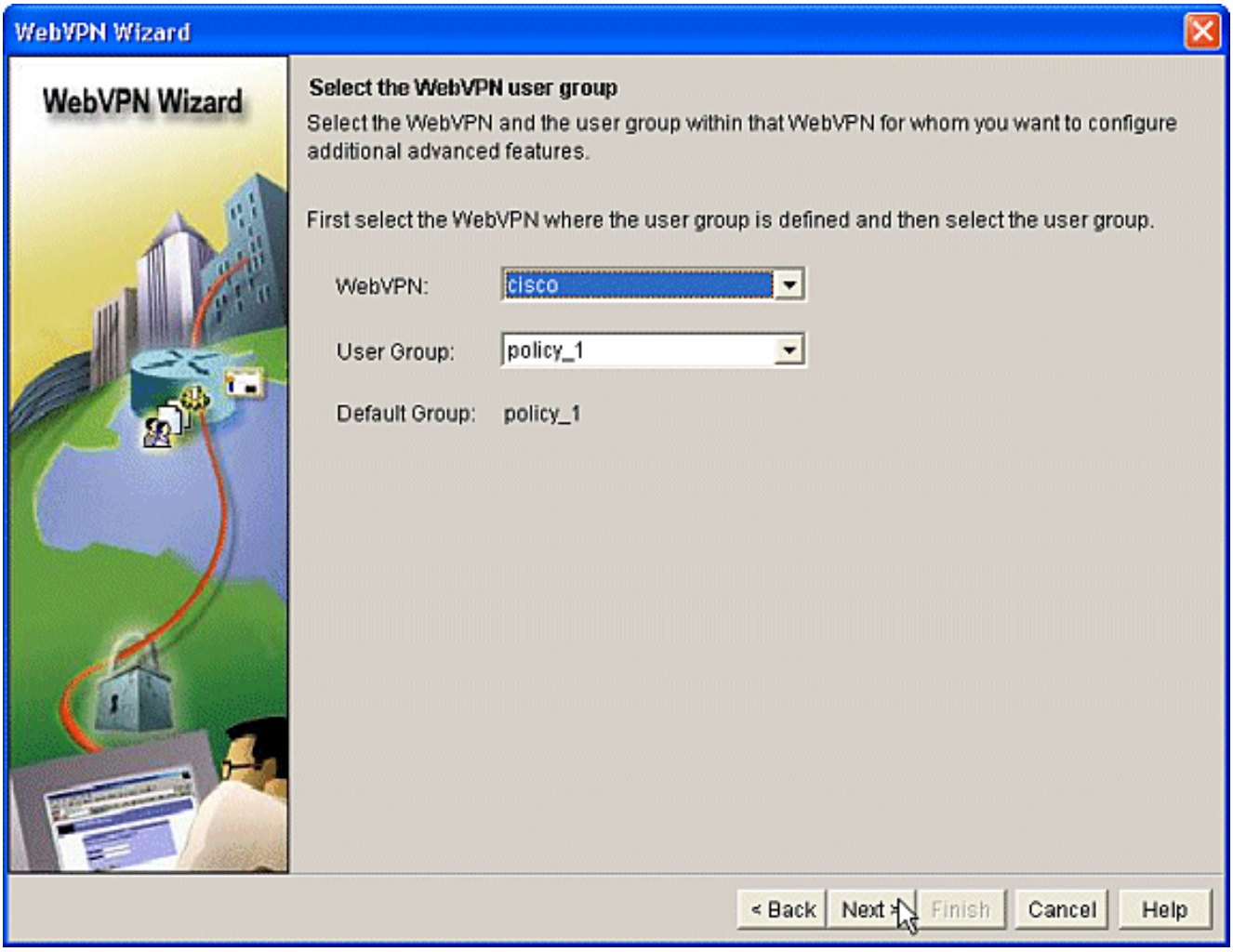
1. Utilisez les fonctionnalités avancées de l'Assistant WebVPN pour activer CSD pour le contexte nouvellement créé. L'Assistant vous donne la possibilité d'installer le package CSD s'il n'est pas déjà installé.Dans SDM, cliquez sur l'onglet **Configurer**.Dans le volet de navigation, cliquez sur **VPN > WebVPN**.Cliquez sur l'onglet **Create WebVPN**.Cochez la case d'option **Configurer les fonctionnalités avancées pour un WebVPN existant**.Cliquez sur le bouton **Lancer la tâche sélectionnée**.



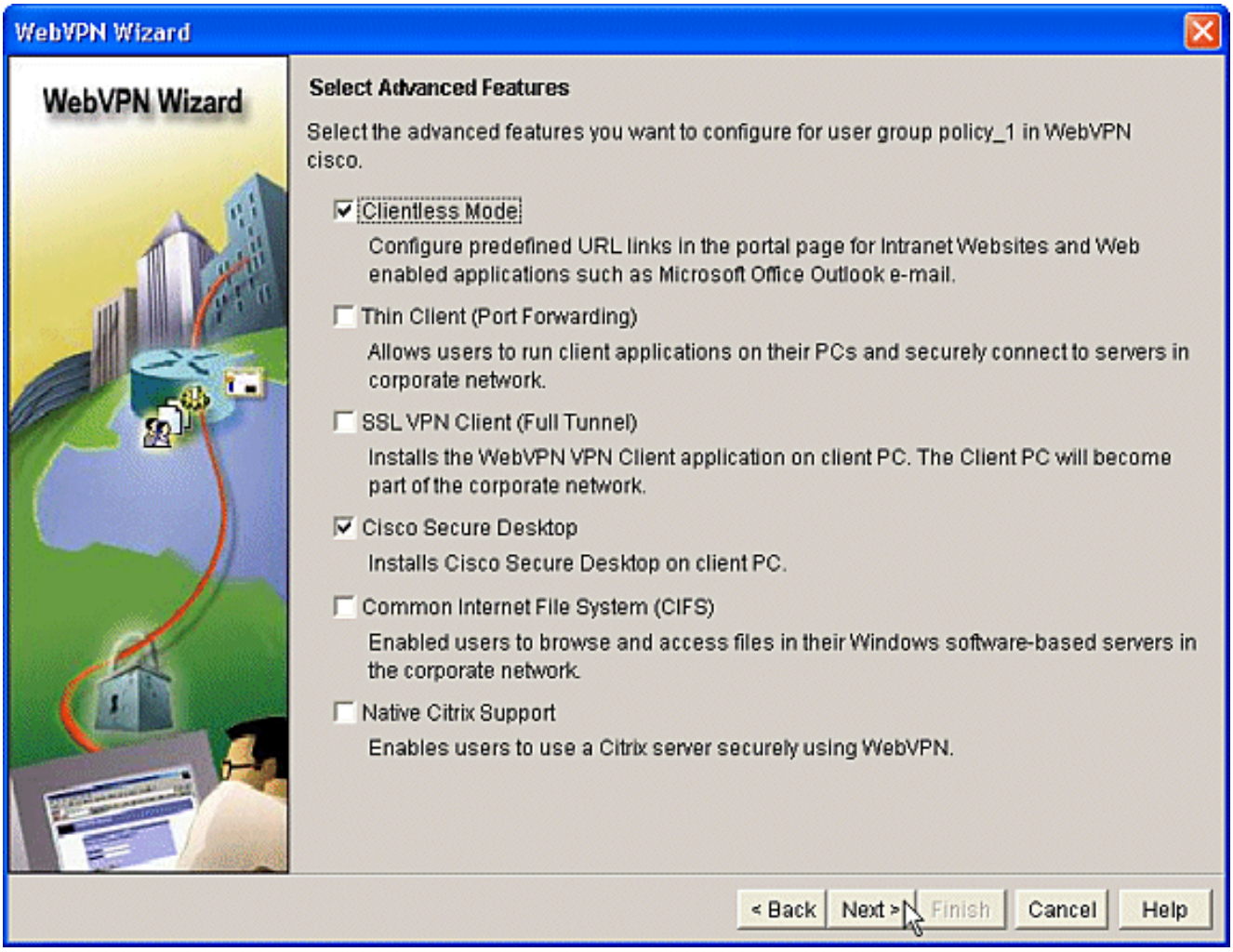
2. La page d'accueil de l'assistant WebVPN avancé s'affiche. Cliquez sur **Next** (Suivant).



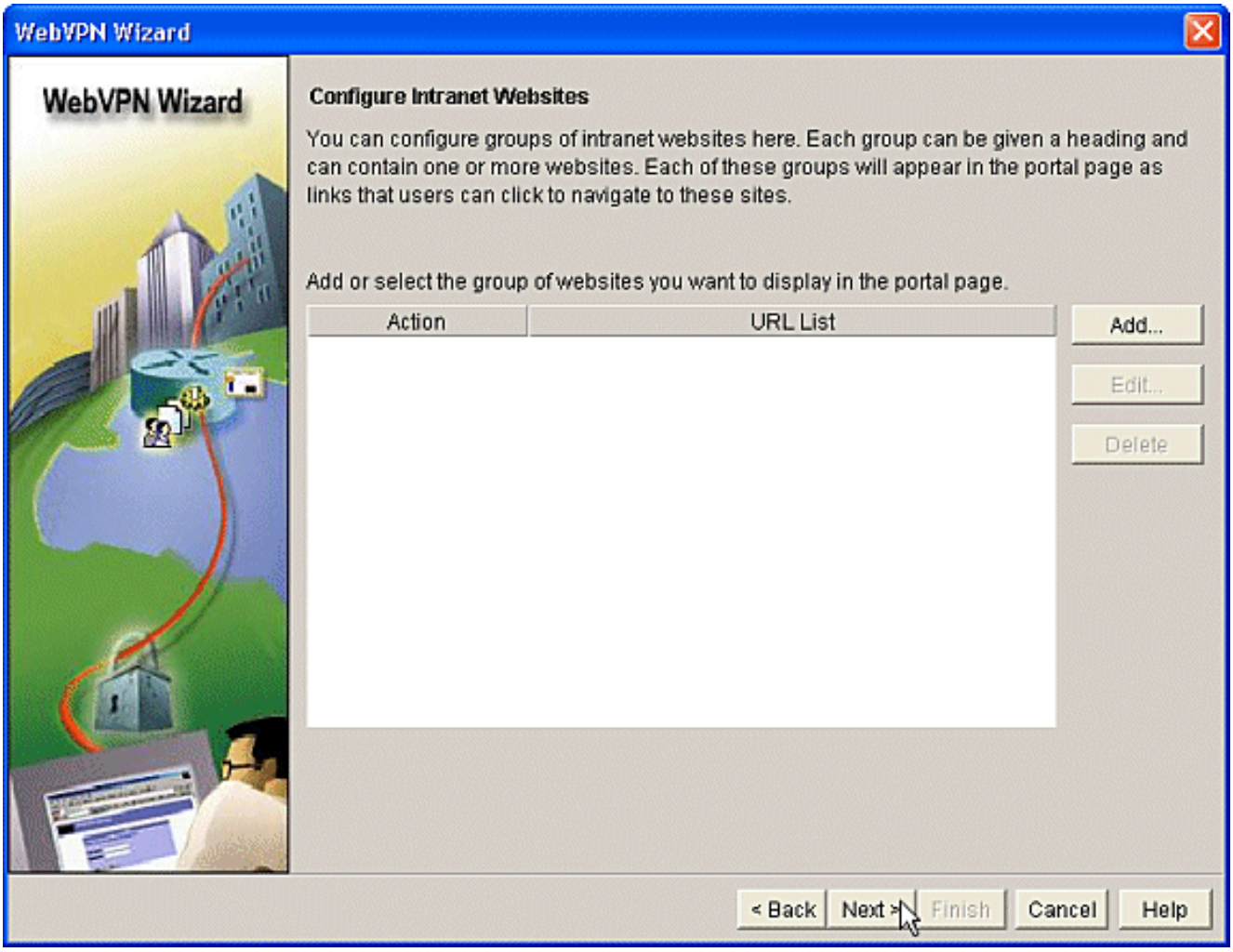
3. Sélectionnez WebVPN et le groupe d'utilisateurs dans les zones déroulantes des champs. Les fonctions de l'assistant WebVPN avancé seront appliquées à vos choix. Cliquez sur **Next** (Suivant).



4. L'écran Sélectionner les fonctionnalités avancées vous permet de choisir parmi les technologies répertoriées.Vérifiez **Cisco Secure Desktop**.Dans cet exemple, le choix est **Mode sans client**.Si vous choisissez l'une des autres technologies répertoriées, des fenêtres supplémentaires s'ouvrent pour permettre l'entrée des informations associées.Cliquez sur le bouton
Suivant.

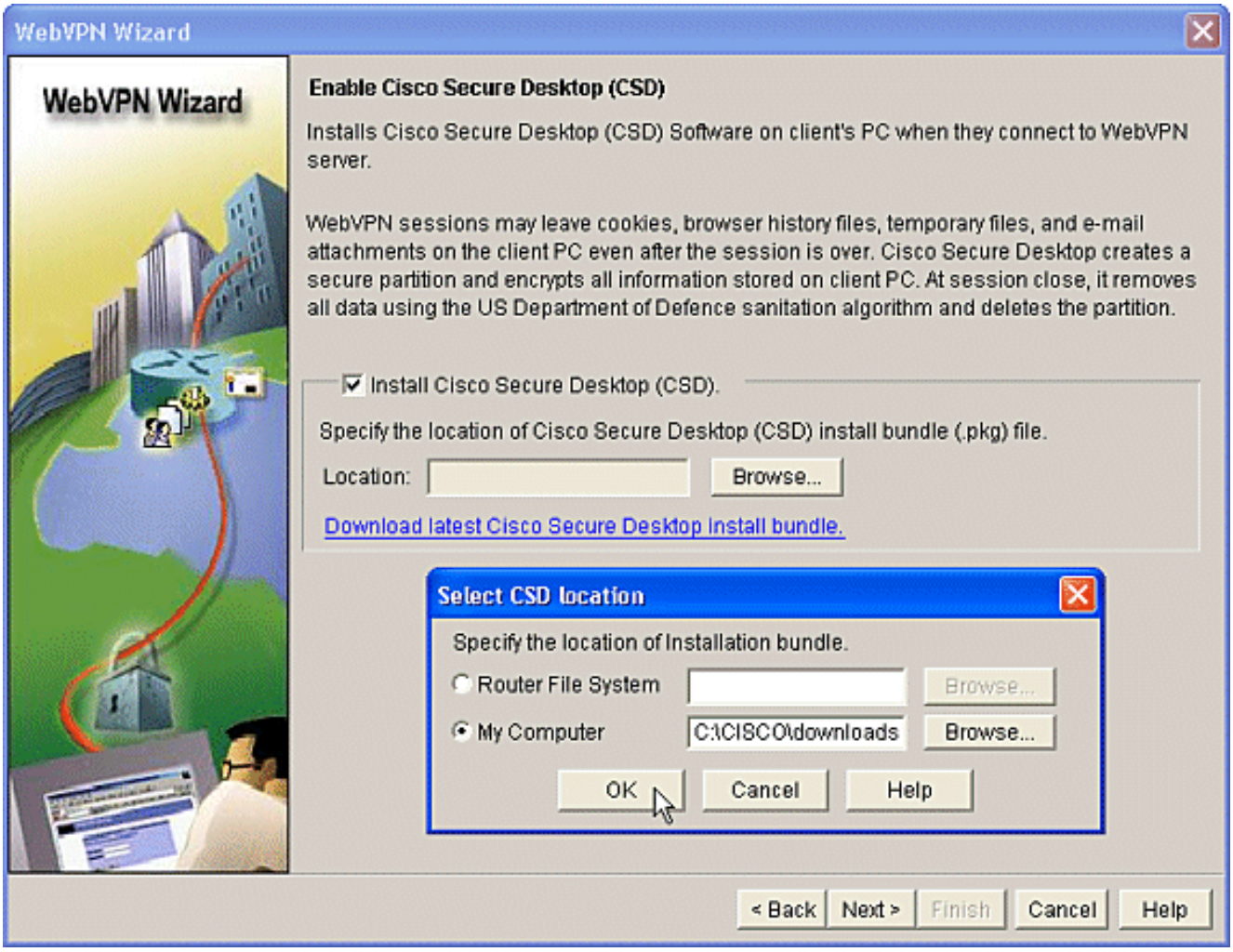


5. L'écran Configurer les sites Web intranet vous permet de configurer les ressources Web que vous souhaitez mettre à la disposition des utilisateurs. Vous pouvez ajouter les sites Web internes de la société, tels qu'Outlook Web Access (OWA).



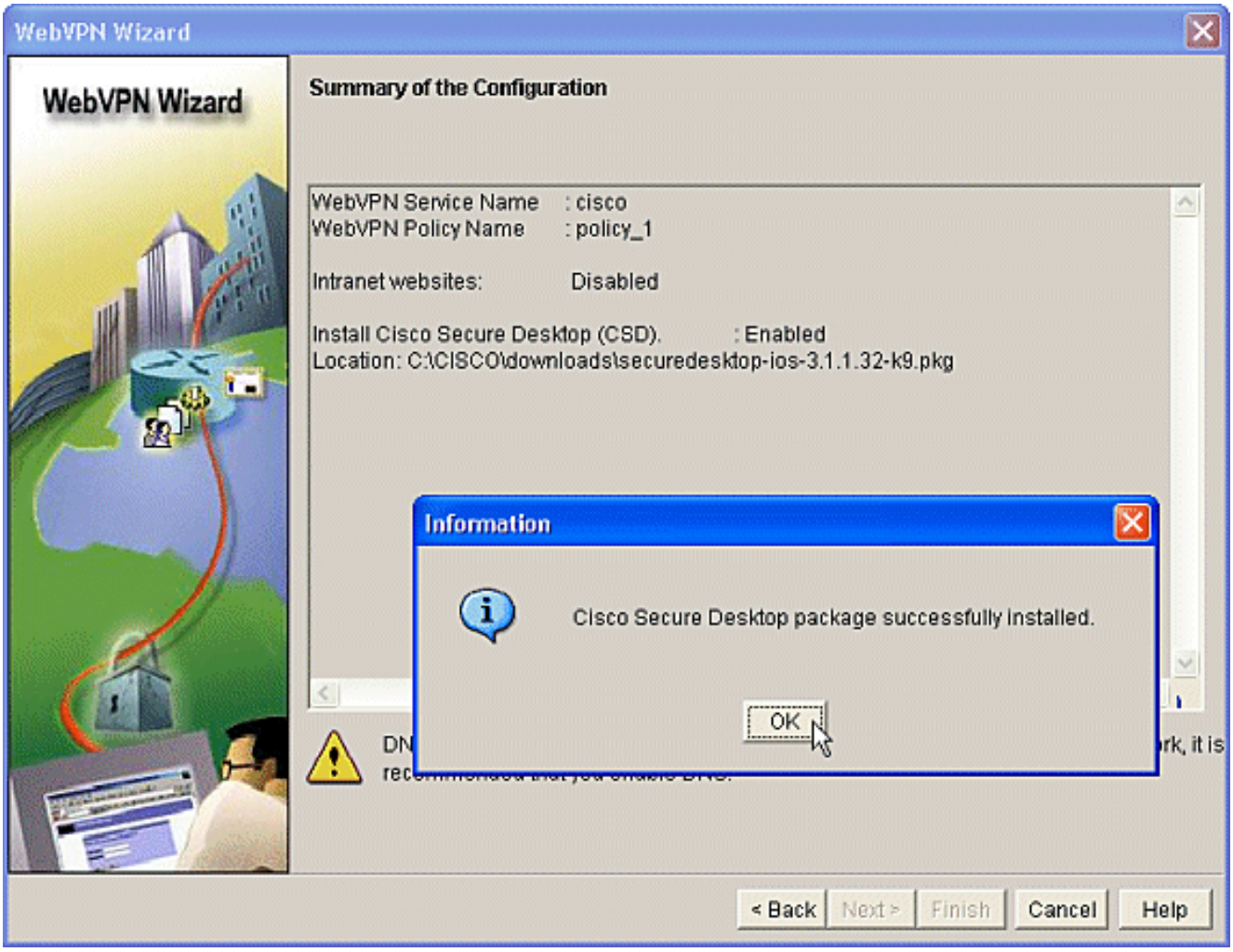
6. Dans l'écran Enable Cisco Secure Desktop (CSD), vous avez la possibilité d'activer le CSD pour ce contexte. Cochez la case en regard de **Installer Cisco Secure Desktop (CSD)** et cliquez sur
Parcourir.

7. Dans la zone Sélectionner un emplacement CSD, cochez **Poste de travail**.Cliquez sur le bouton **Parcourir**.Choisissez le fichier de package CSD IOS sur votre station de travail de gestion.Cliquez sur le bouton **OK**.Cliquez sur le bouton **Suivant**.



8. Un récapitulatif de l'écran Configuration s'affiche. Cliquez sur le bouton **Terminer**.

9. Cliquez sur **OK** lorsque vous voyez que le fichier de package CSD a été correctement installé.



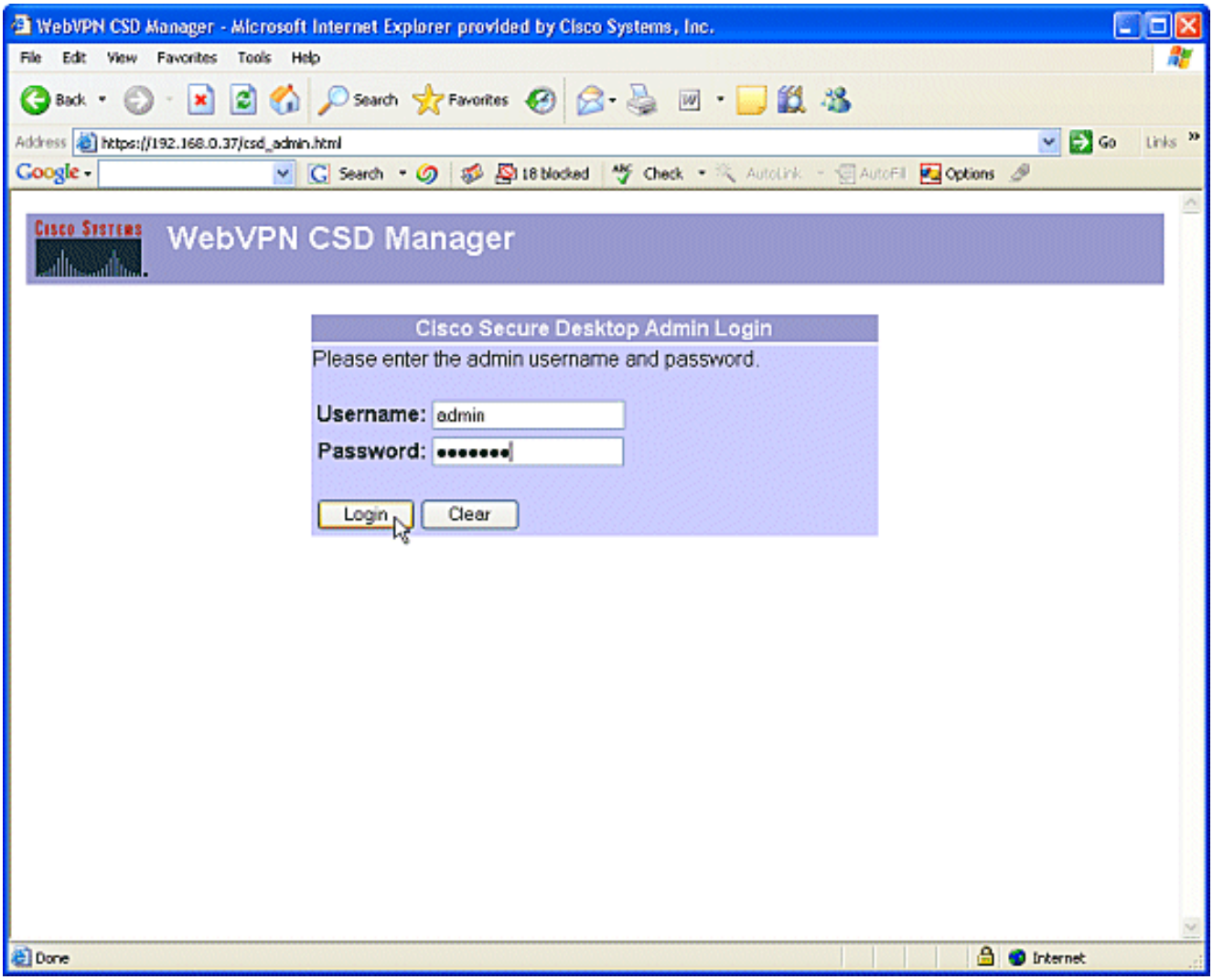
Phase II : Configurez CSD à l'aide d'un navigateur Web.

Ces étapes sont utilisées pour terminer la configuration de CSD sur votre navigateur Web.

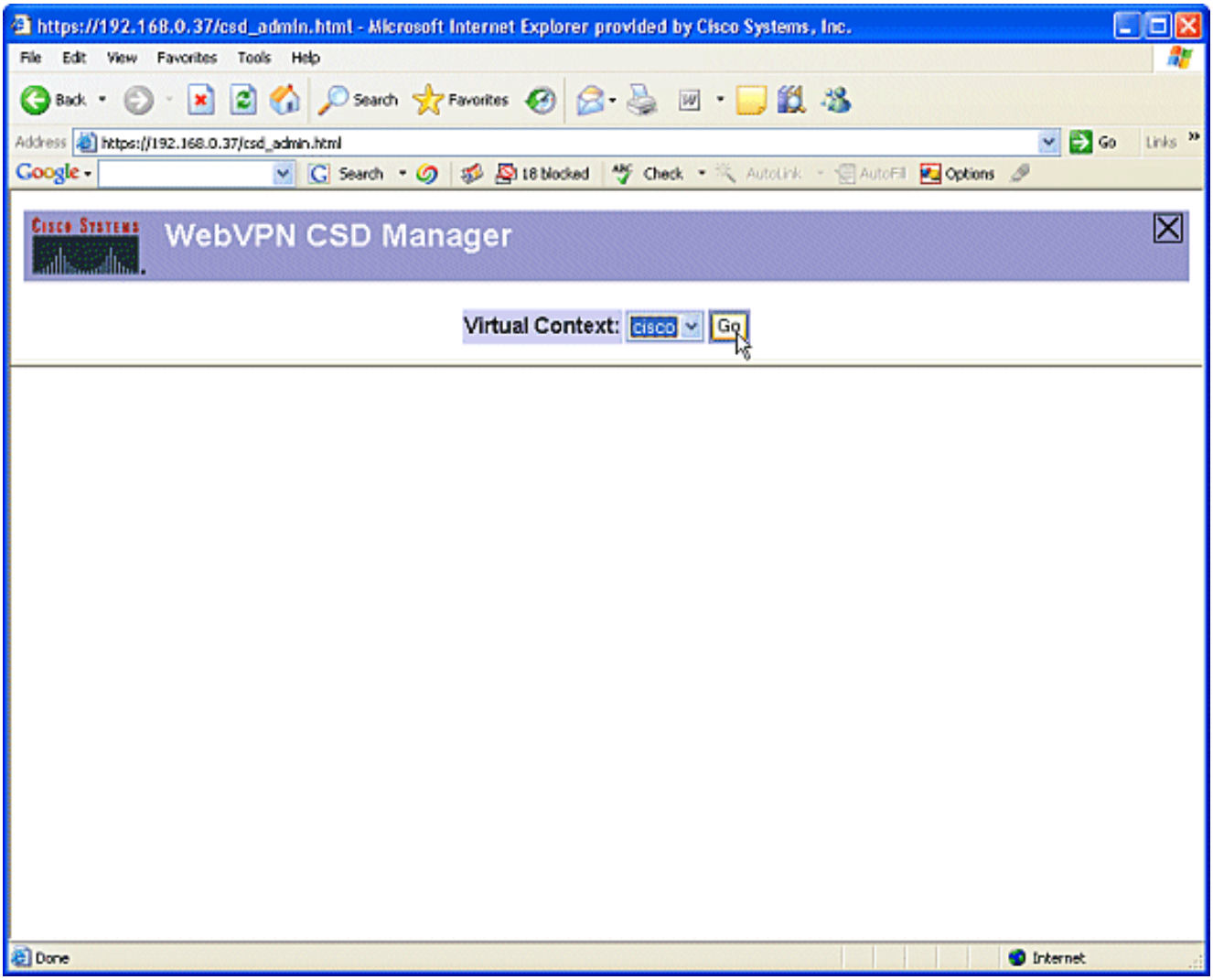
Phase II : Étape 1 : Définissez les emplacements Windows.

Définissez les emplacements Windows.

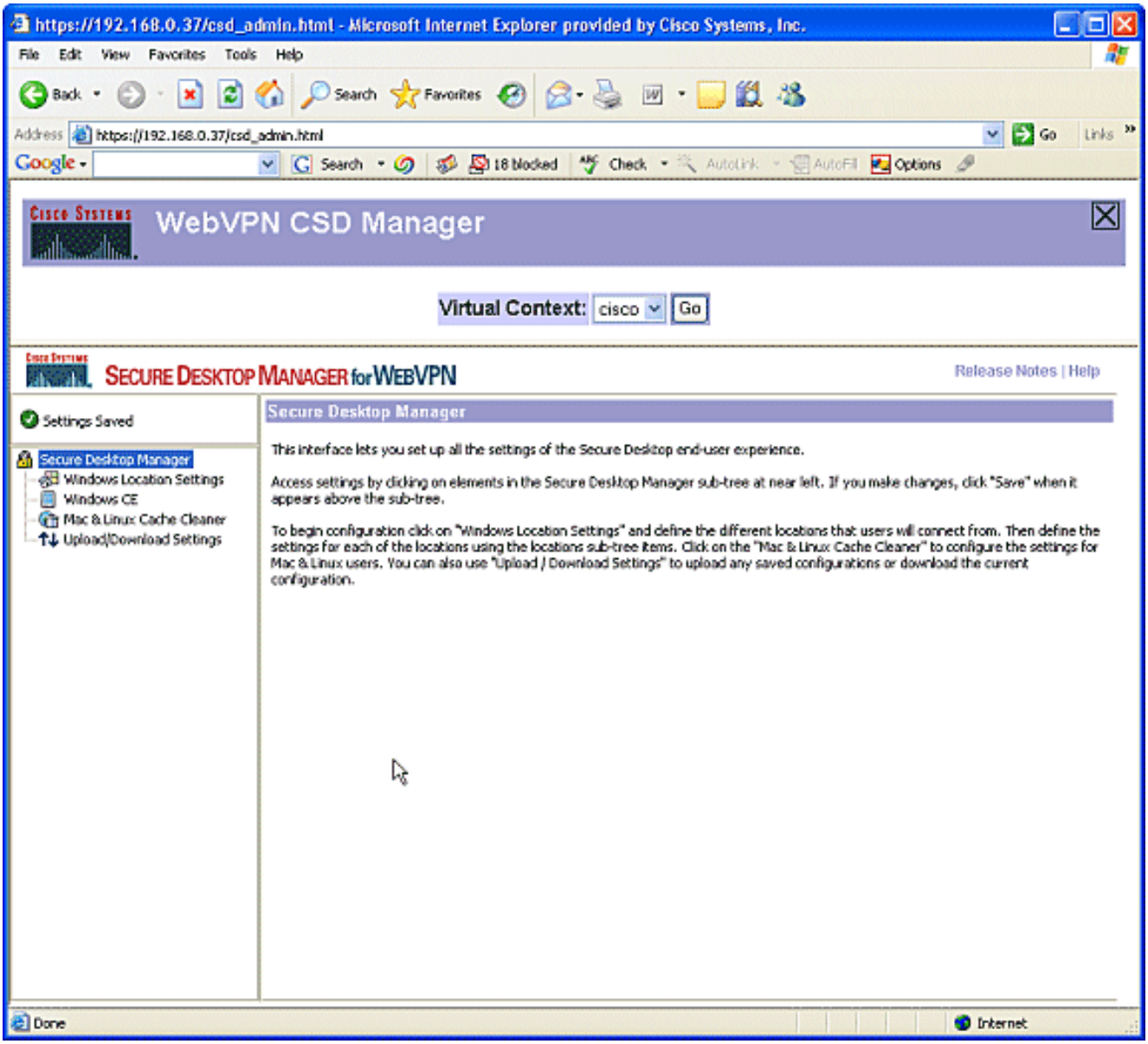
1. Ouvrez votre navigateur Web à l'adresse **https://WebVPNgateway_IP Address/csd_admin.html**, par exemple, **https:/192.168.0.37/csd_admin.html**.
2. Entrez le nom d'utilisateur **admin**.Entrez le mot de passe, qui est le secret d’activation du routeur.Cliquez sur **Connexion**.



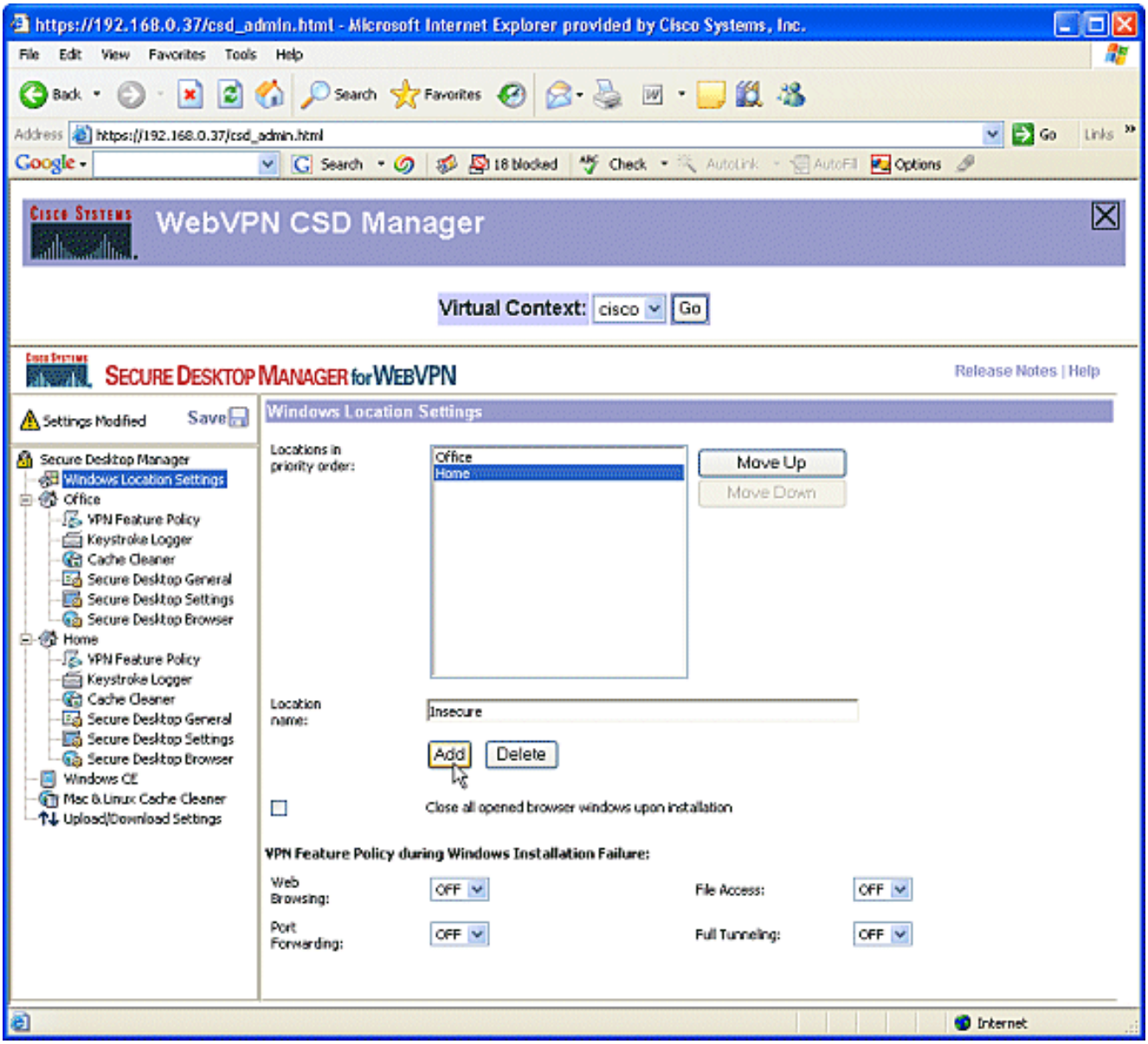
3. Acceptez le certificat offert par le routeur, sélectionnez le contexte dans la liste déroulante, puis cliquez sur
Go.



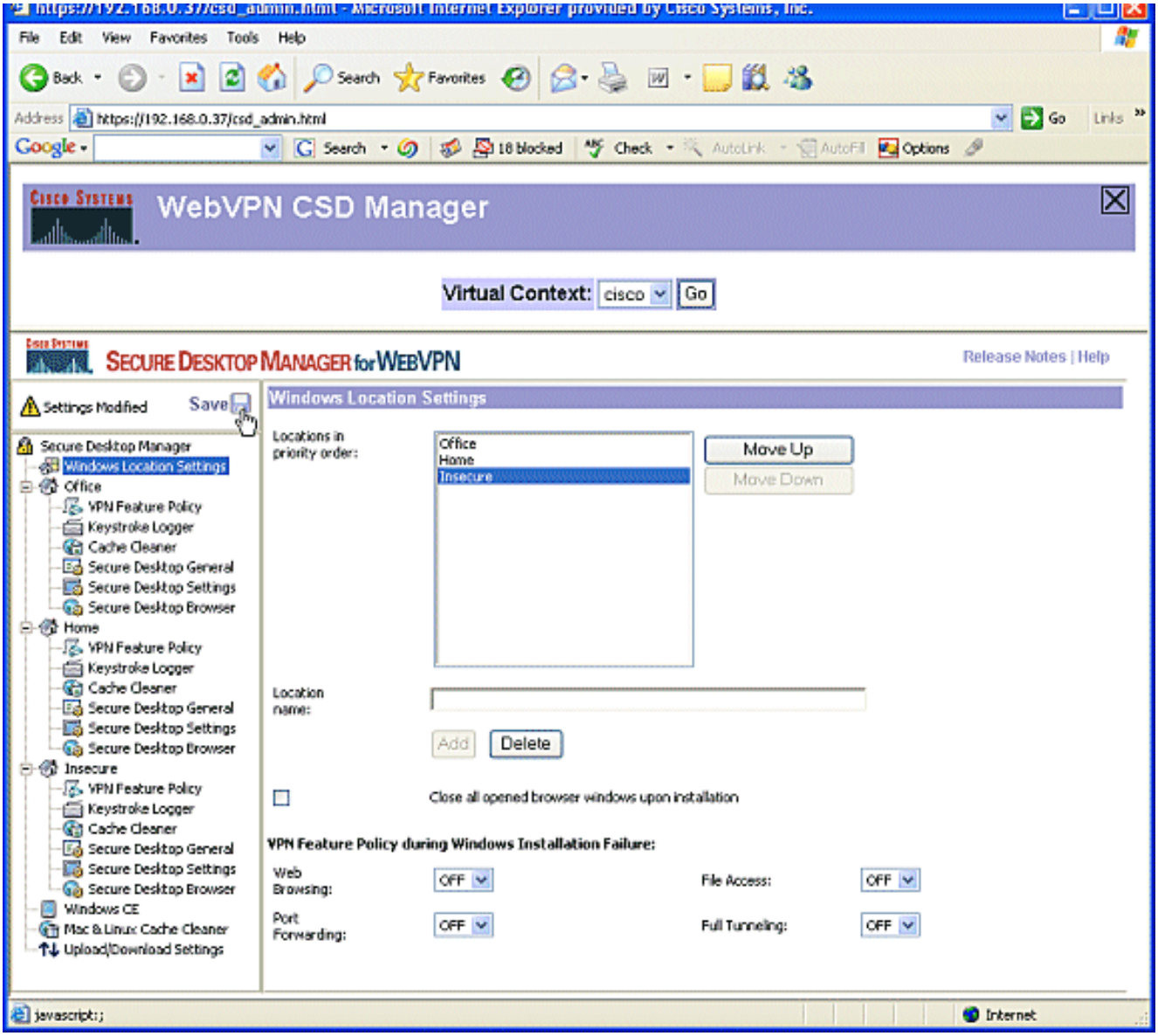
4. Secure Desktop Manager pour WebVPN s'ouvre.



5. Dans le volet gauche, sélectionnez **Paramètres de l'emplacement Windows**.Placez le curseur dans la zone en regard de Nom de l'emplacement, puis saisissez un nom d'emplacement.Cliquez sur **Add**.Dans cet exemple, trois noms d'emplacement sont affichés : Bureau, domicile et non sécurisé. Chaque fois qu'un nouvel emplacement est ajouté, le volet gauche s'étend avec les paramètres configurables de cet emplacement.



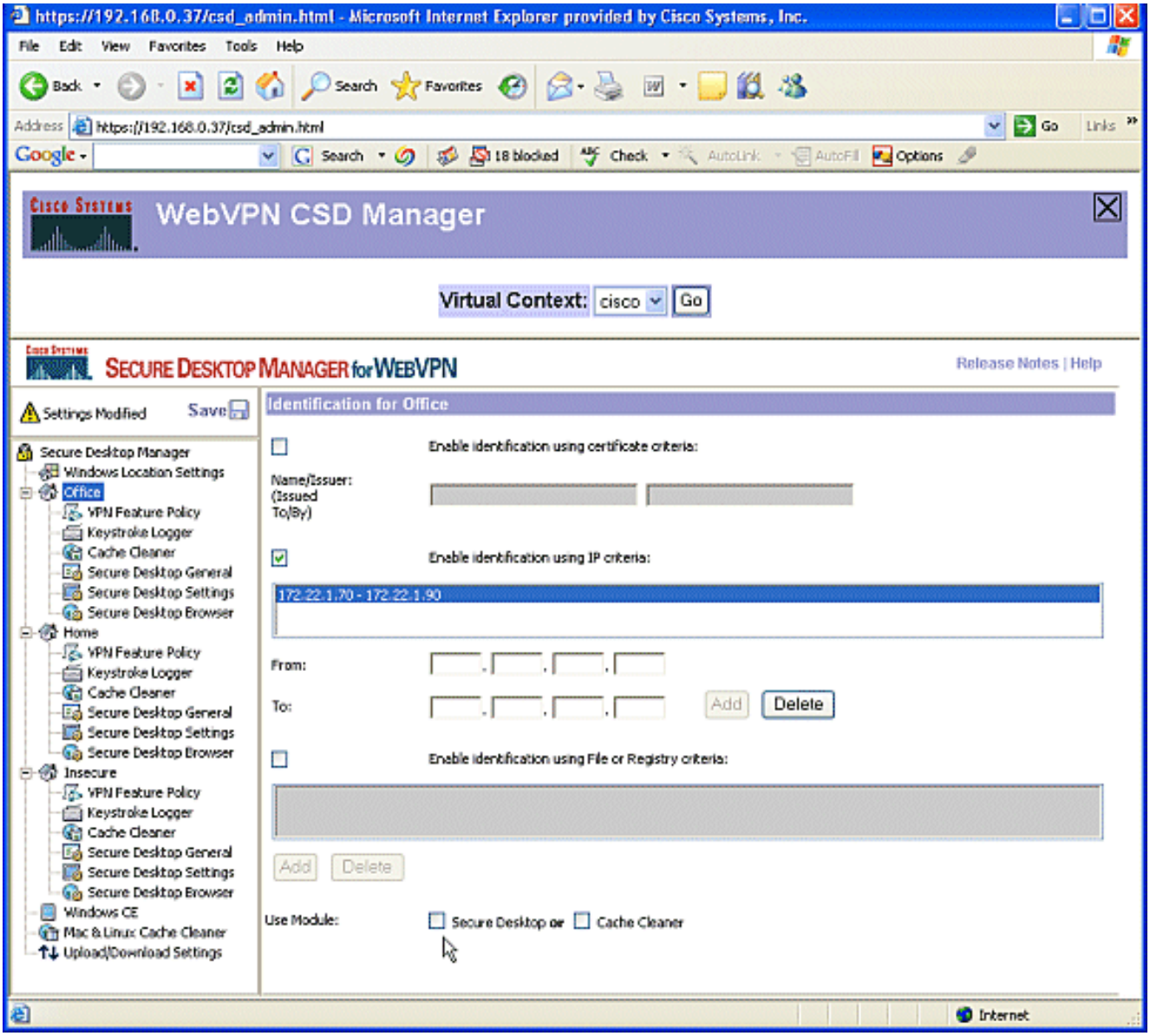
6. Après avoir créé les emplacements Windows, cliquez sur **Enregistrer** en haut du volet gauche.**Remarque :** Enregistrez vos configurations souvent car vos paramètres seront perdus si vous êtes déconnecté du navigateur
Web.



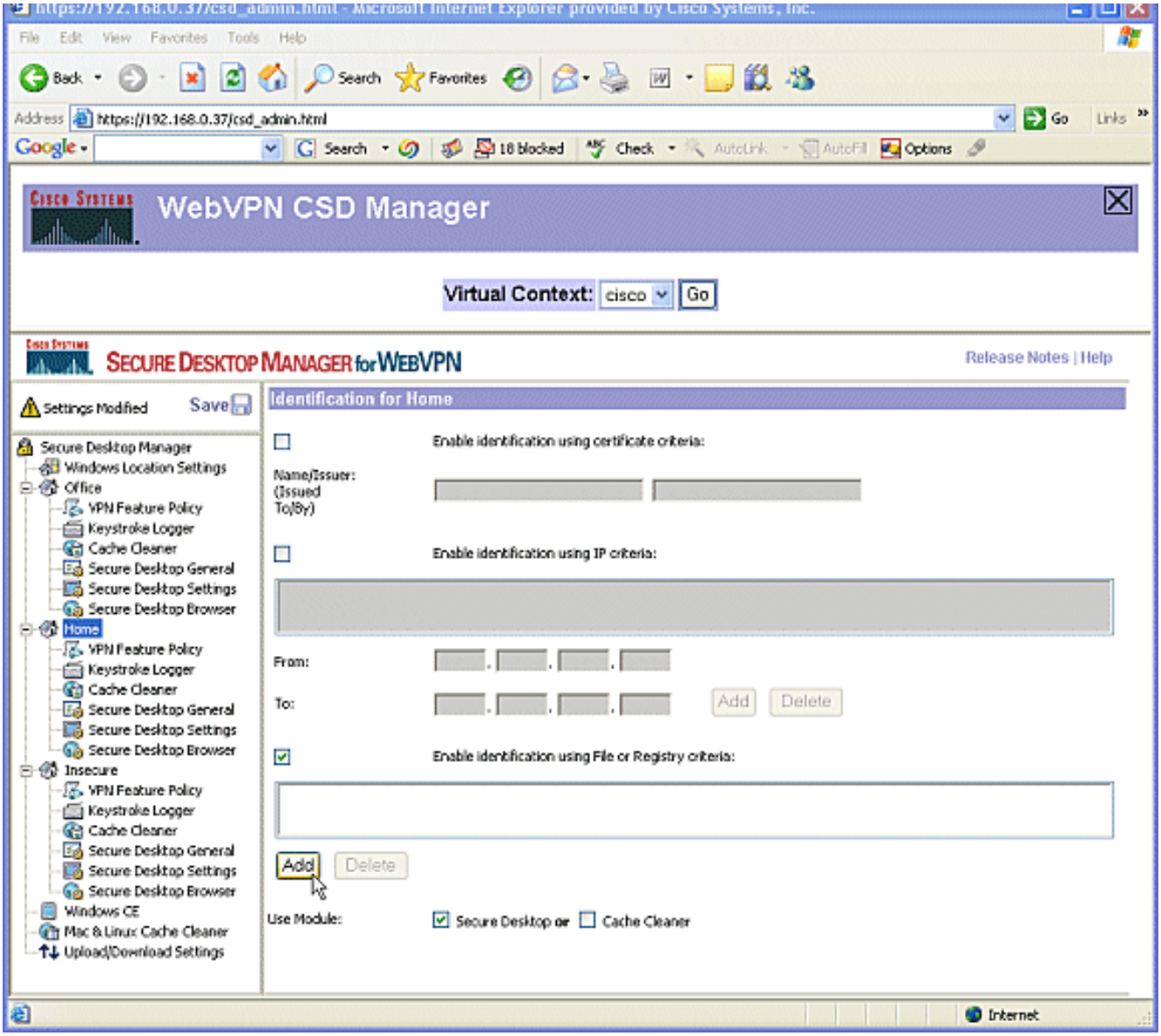
Phase II : Étape 2 : Identifier les critères de localisation

Afin de distinguer les emplacements Windows les uns des autres, affectez des critères spécifiques à chaque emplacement. Cela permet à CSD de déterminer quelles fonctionnalités s'appliquent à un emplacement Windows particulier.

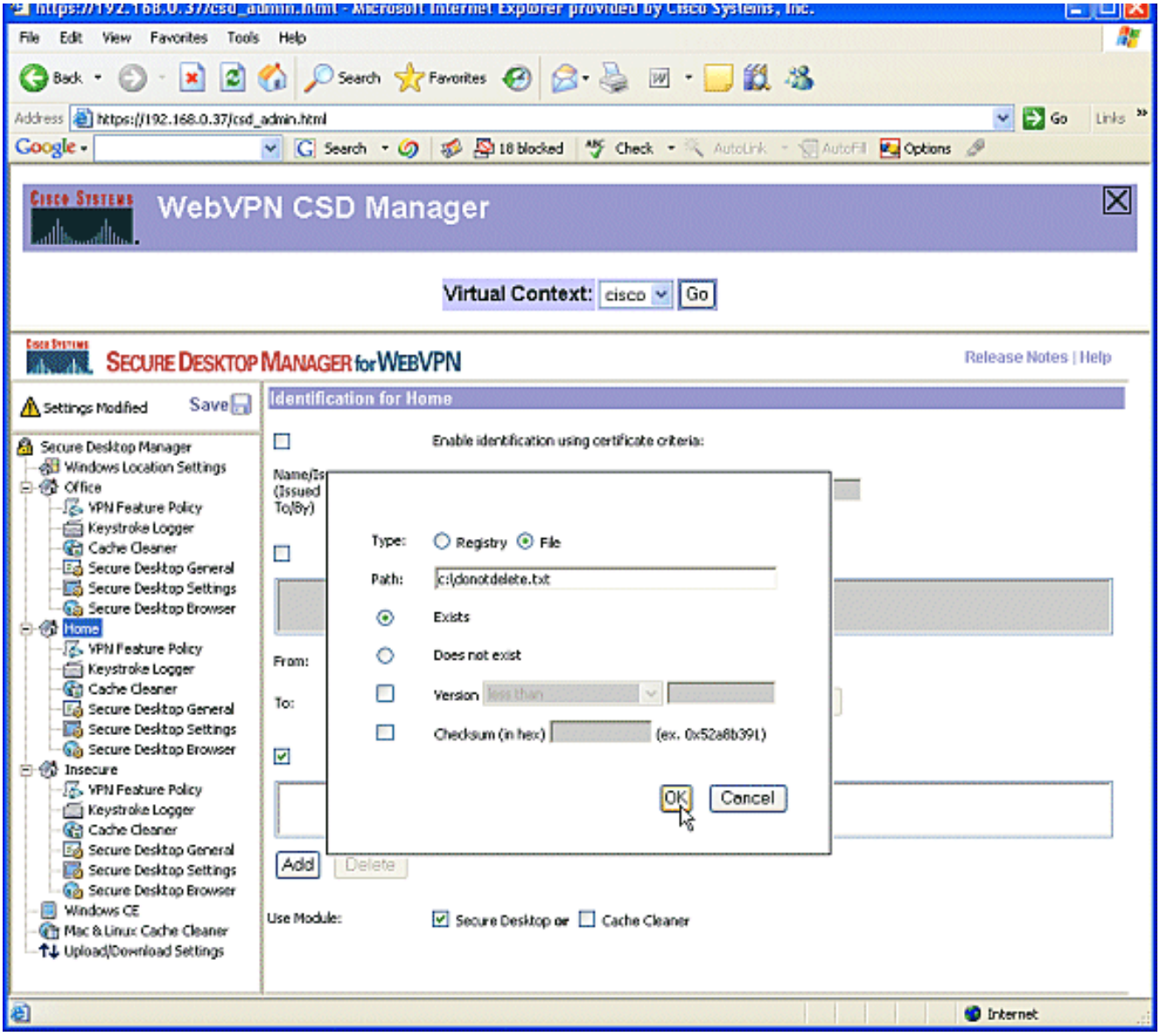
1. Dans le volet gauche, cliquez sur **Office**.Vous pouvez identifier un emplacement Windows avec des critères de certificat, des critères IP, un fichier ou des critères de Registre. Vous pouvez également choisir Secure Desktop ou Cache Cleaner pour ces clients. Ces utilisateurs étant des employés de bureau internes, identifiez-les avec des critères IP.Entrez les plages d'adresses IP dans les zones **De** et **À**.Cliquez sur **Add**. Décochez **Utiliser le module : Bureau sécurisé**.Lorsque vous y êtes invité, cliquez sur **Enregistrer**, puis sur **OK**.



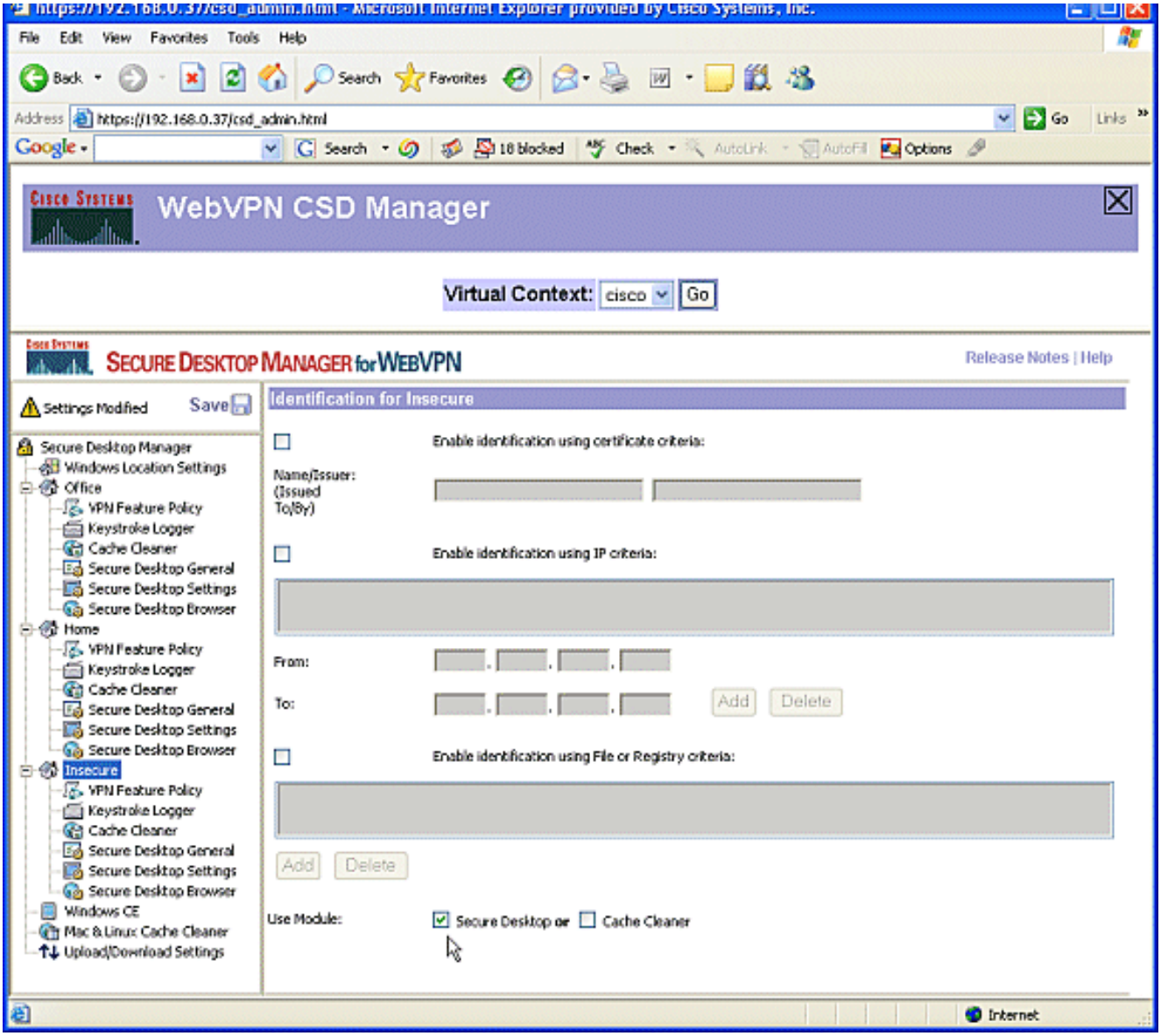
2. Dans le volet gauche, cliquez sur la deuxième **page d'accueil** des paramètres d'emplacement Windows.Assurez-vous **d'utiliser le module : Secure Desktop** est coché.Un fichier qui identifie ces clients sera distribué. Vous pouvez choisir de distribuer des certificats et/ou des critères de Registre pour ces utilisateurs.Cochez la case **Activer l'identification à l'aide des critères Fichier ou Registre**.Cliquez sur
Add.



3. Dans la boîte de dialogue, sélectionnez **Fichier**, puis saisissez le chemin d'accès au fichier.Ce fichier doit être distribué à tous vos clients à domicile.Cochez la case d'option **Exists**.Lorsque vous y êtes invité, cliquez sur **OK**, puis sur **Enregistrer**.



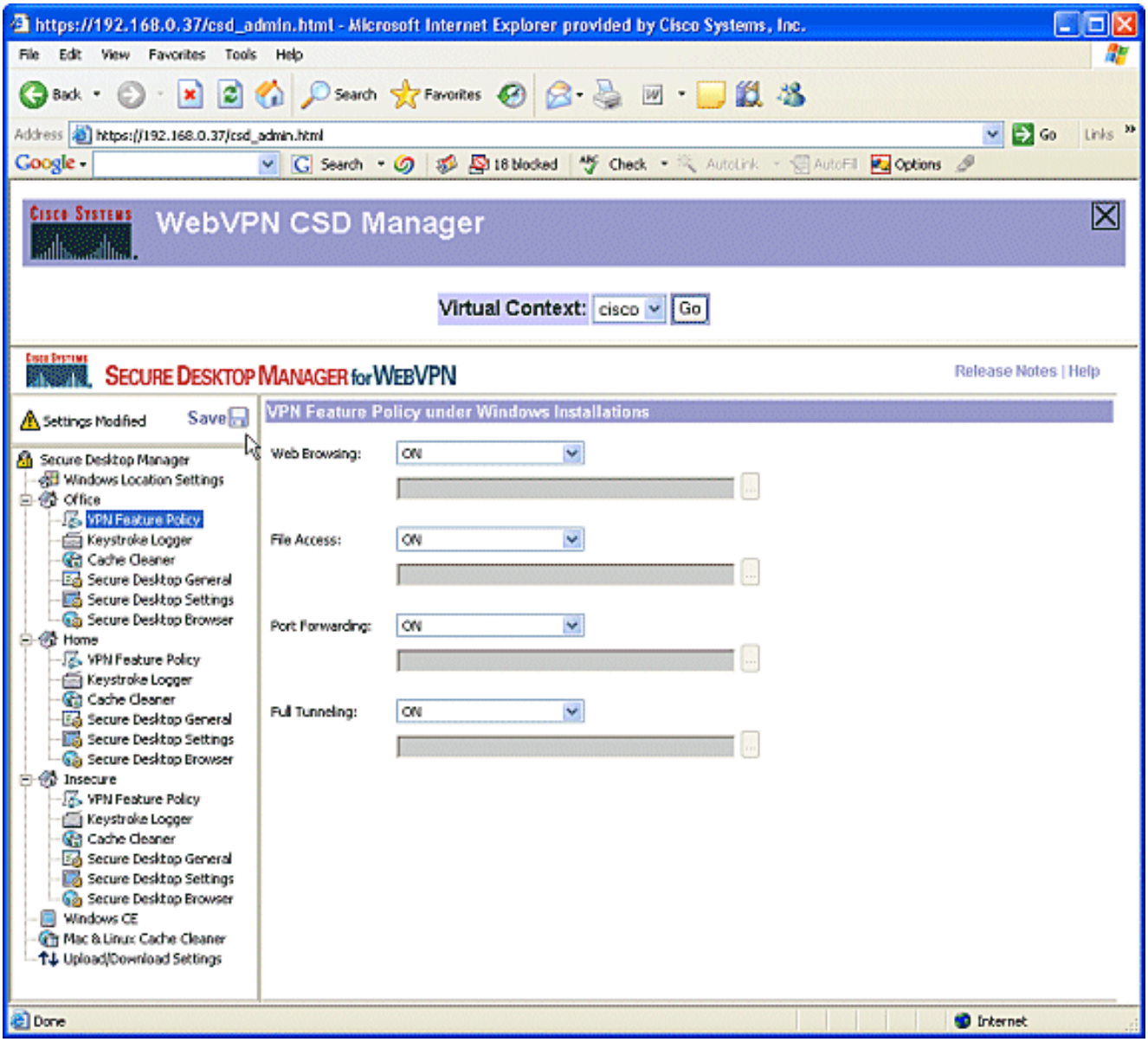
4. Pour configurer l'identification des emplacements **non sécurisés**, n'appliquez simplement aucun critère d'identification.Cliquez sur **Non sécurisé** dans le volet gauche.Ne cochez pas tous les critères.Cochez la case **Utiliser le module : Bureau sécurisé**.Lorsque vous y êtes invité, cliquez sur **Enregistrer**, puis sur **OK**.



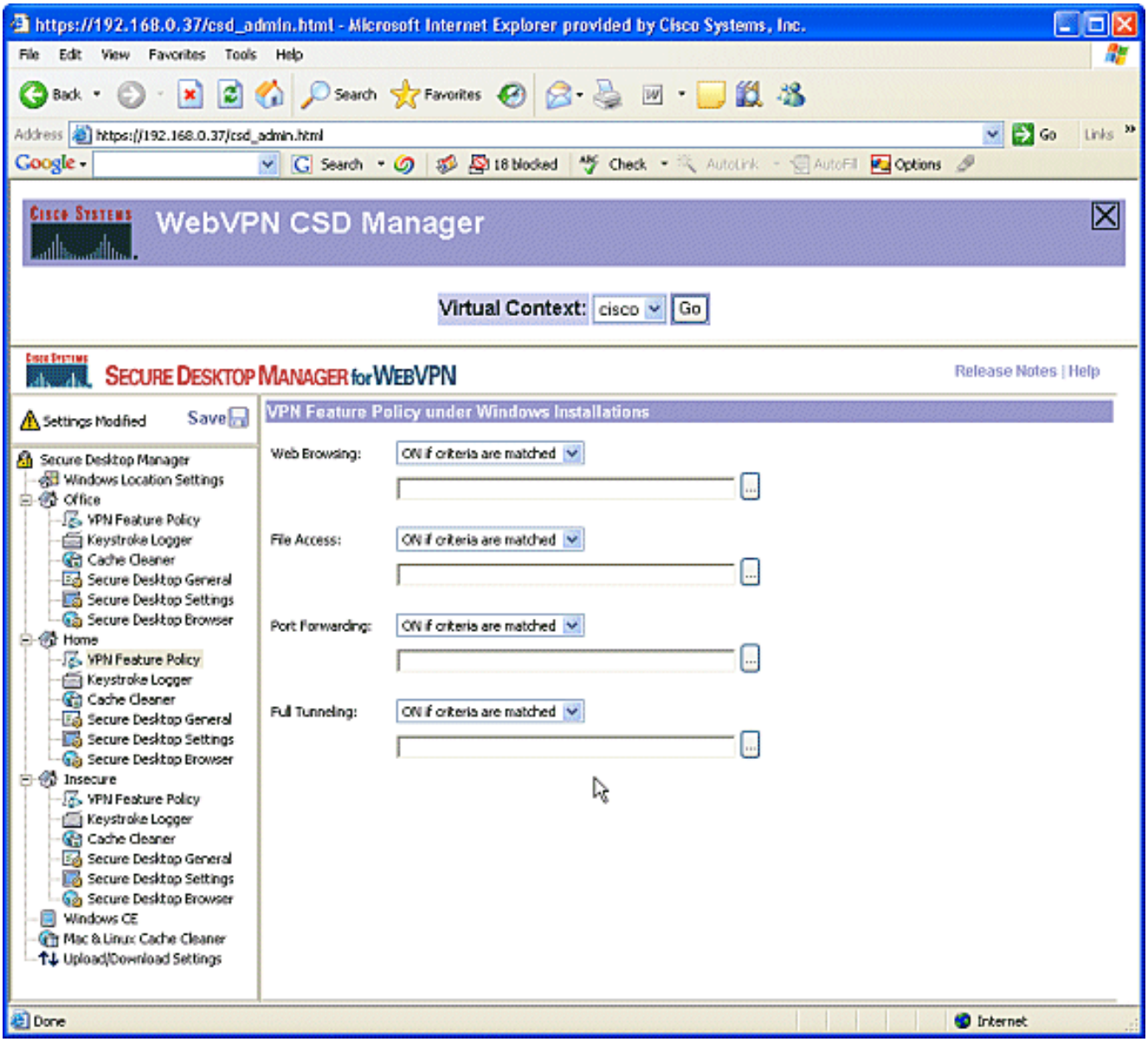
Phase II : Étape 3 : Configurez les modules et les fonctions d'emplacement Windows.

Configurez les fonctions CSD pour chaque emplacement Windows.

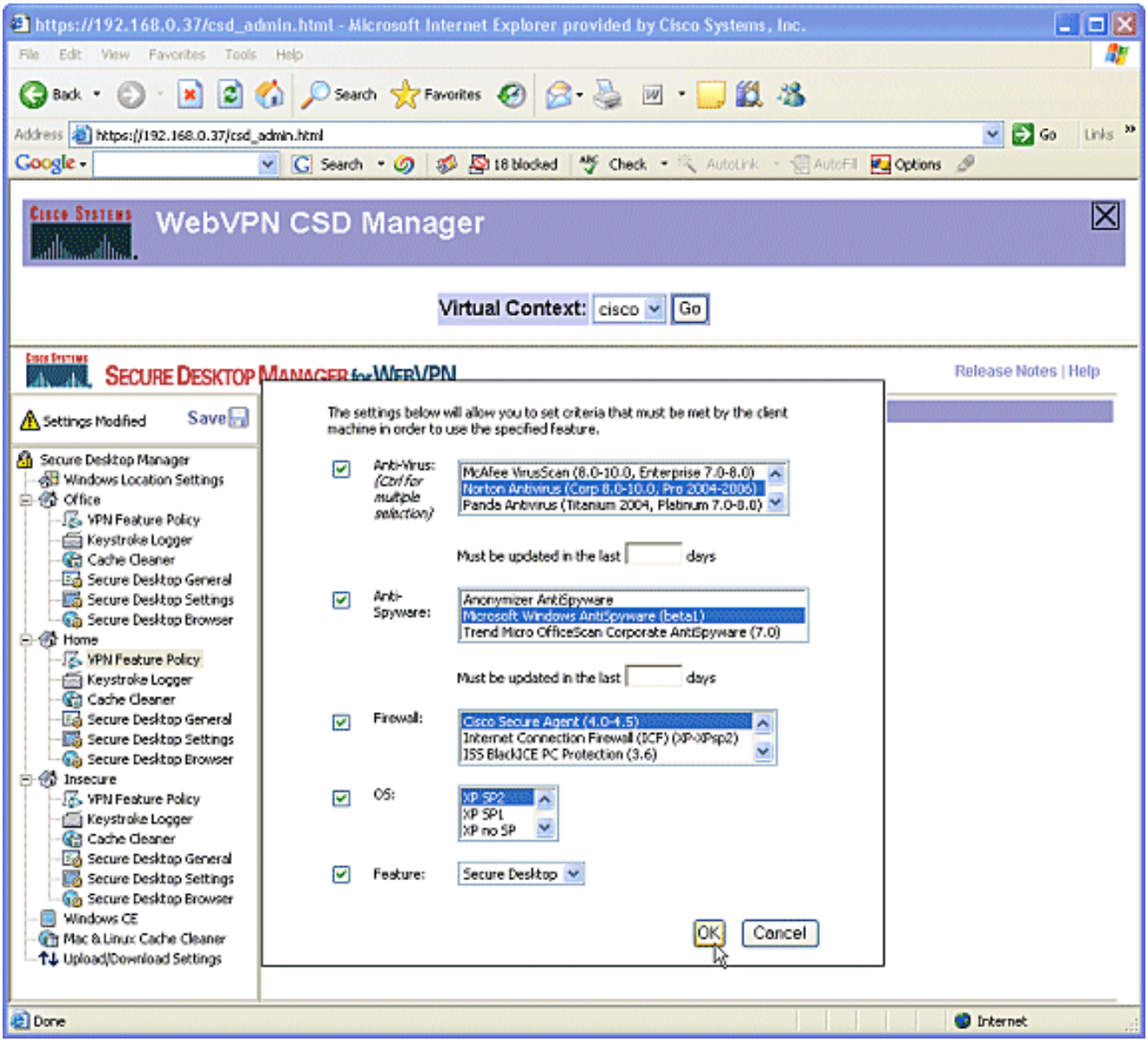
1. Sous **Office**, cliquez sur **Stratégie de fonctionnalité VPN**. Comme il s'agit de clients internes approuvés, ni CSD ni Cache Cleaner n'ont été activés. Aucun des autres paramètres n'est disponible.



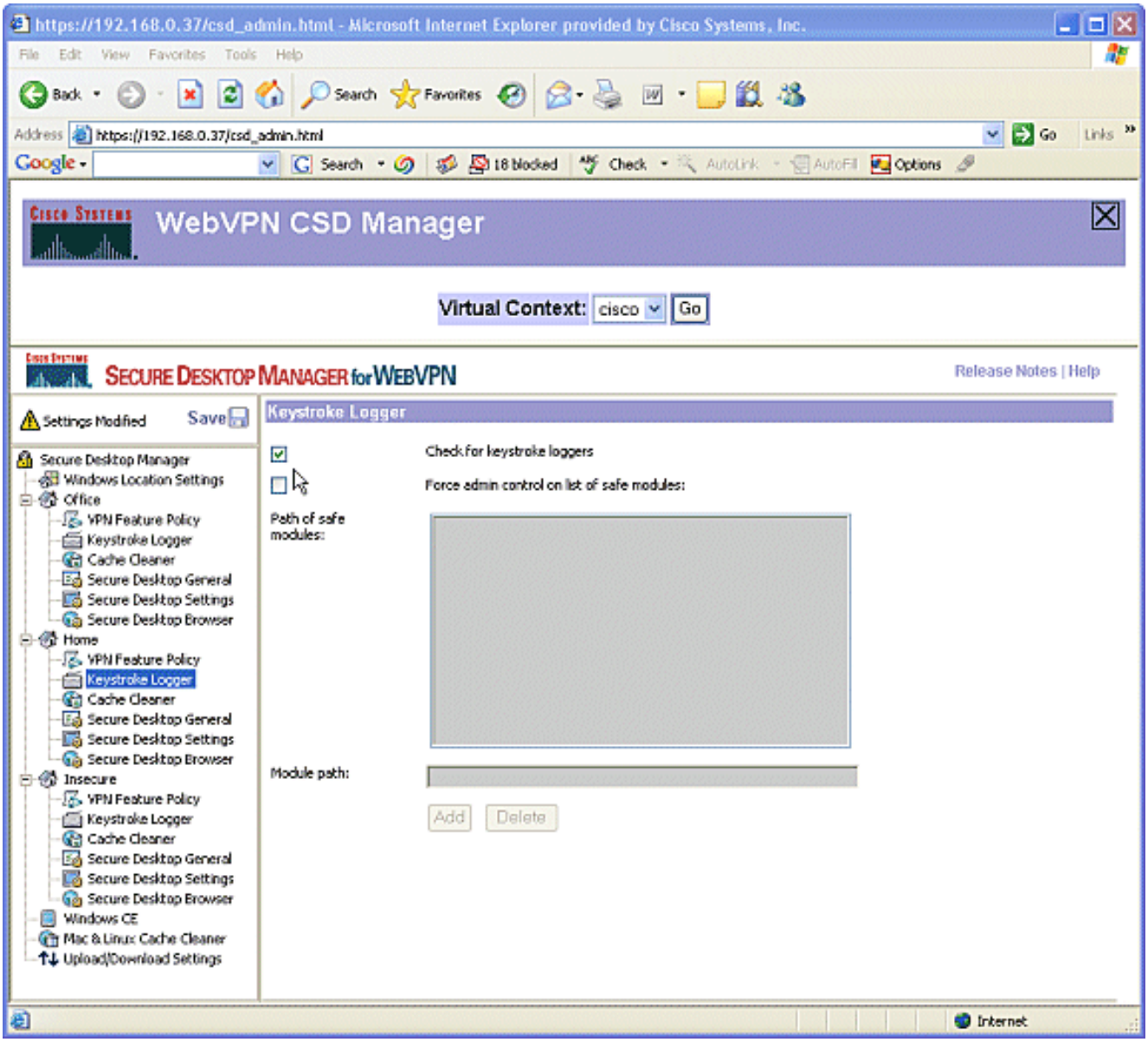
2. Activez les fonctions comme indiqué.Dans le volet gauche, sélectionnez **VPN Feature Policy** sous **Home**.Les utilisateurs à domicile pourront accéder au réseau local de l'entreprise si les clients répondent à certains critères.Sous chaque méthode d'accès, sélectionnez **ON si les critères correspondent**.



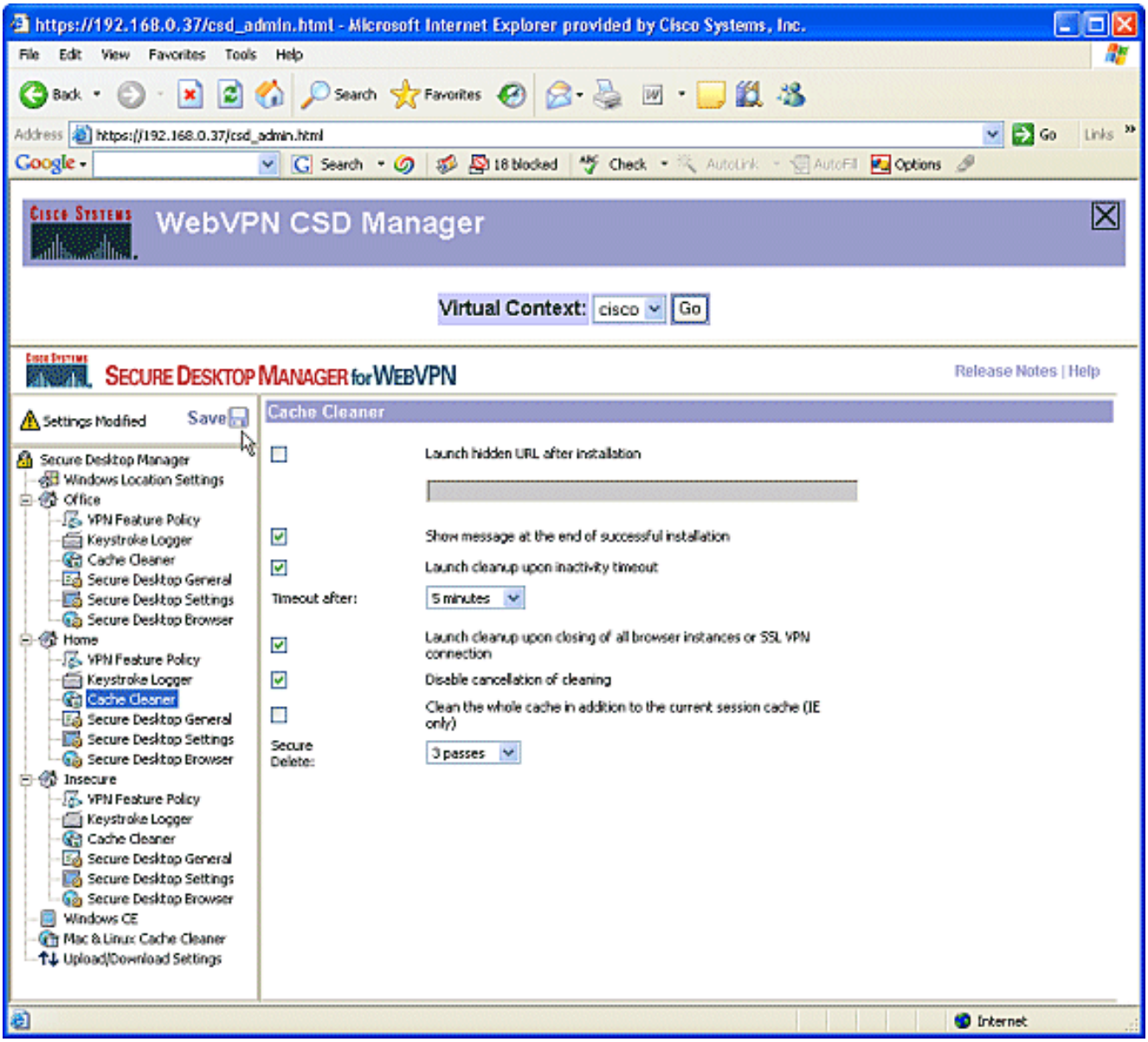
3. Pour la navigation Web, cliquez sur le bouton d'ellipse et choisissez les critères qui doivent correspondre. Cliquez sur **OK** dans la boîte de dialogue.



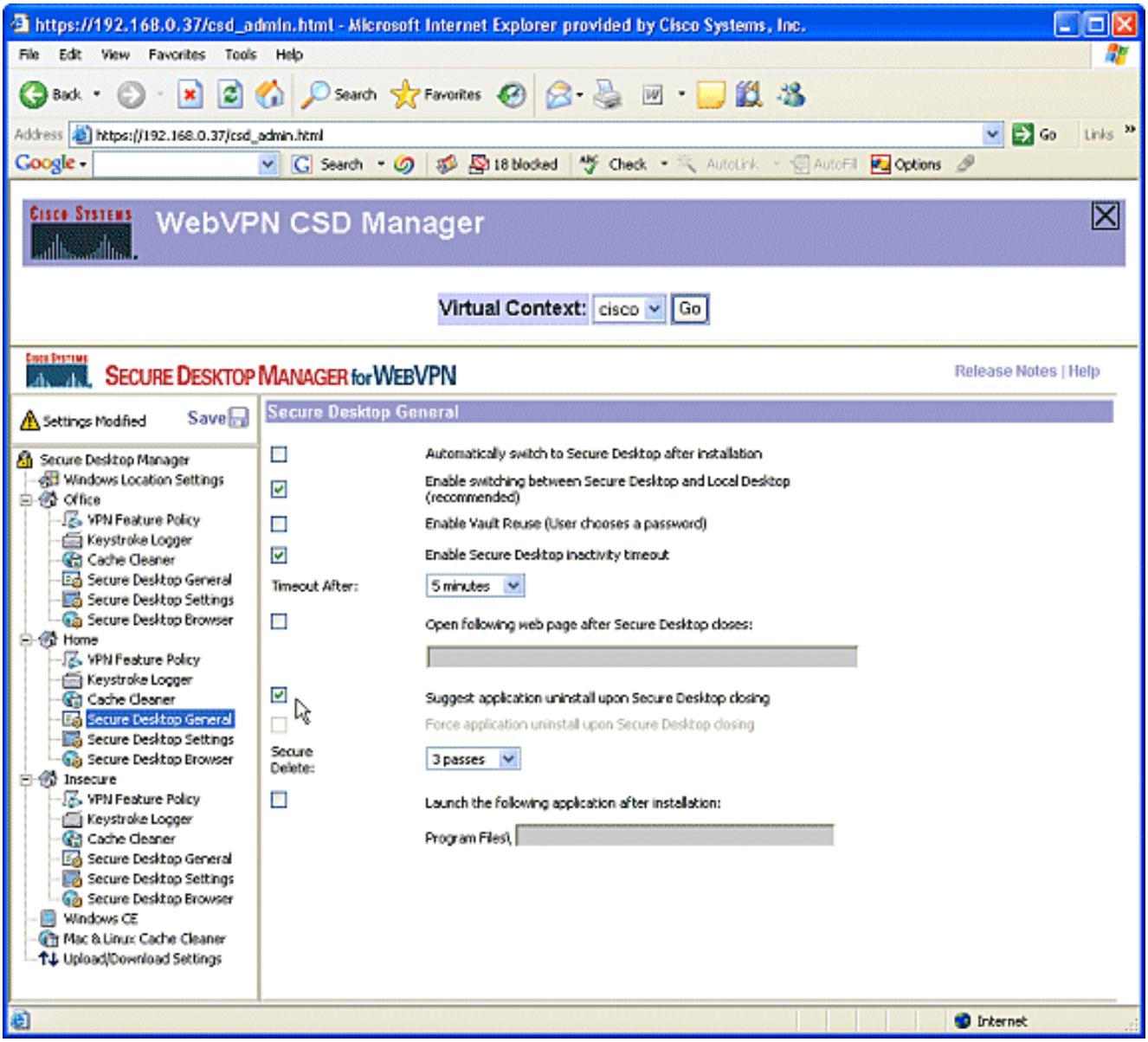
4. Vous pouvez configurer les autres méthodes d'accès de la même manière.Sous **Accueil**, sélectionnez **Clavier Logger**.Cochez la case **Rechercher les enregistreurs de frappe**.Lorsque vous y êtes invité, cliquez sur **Enregistrer**, puis sur **OK**.



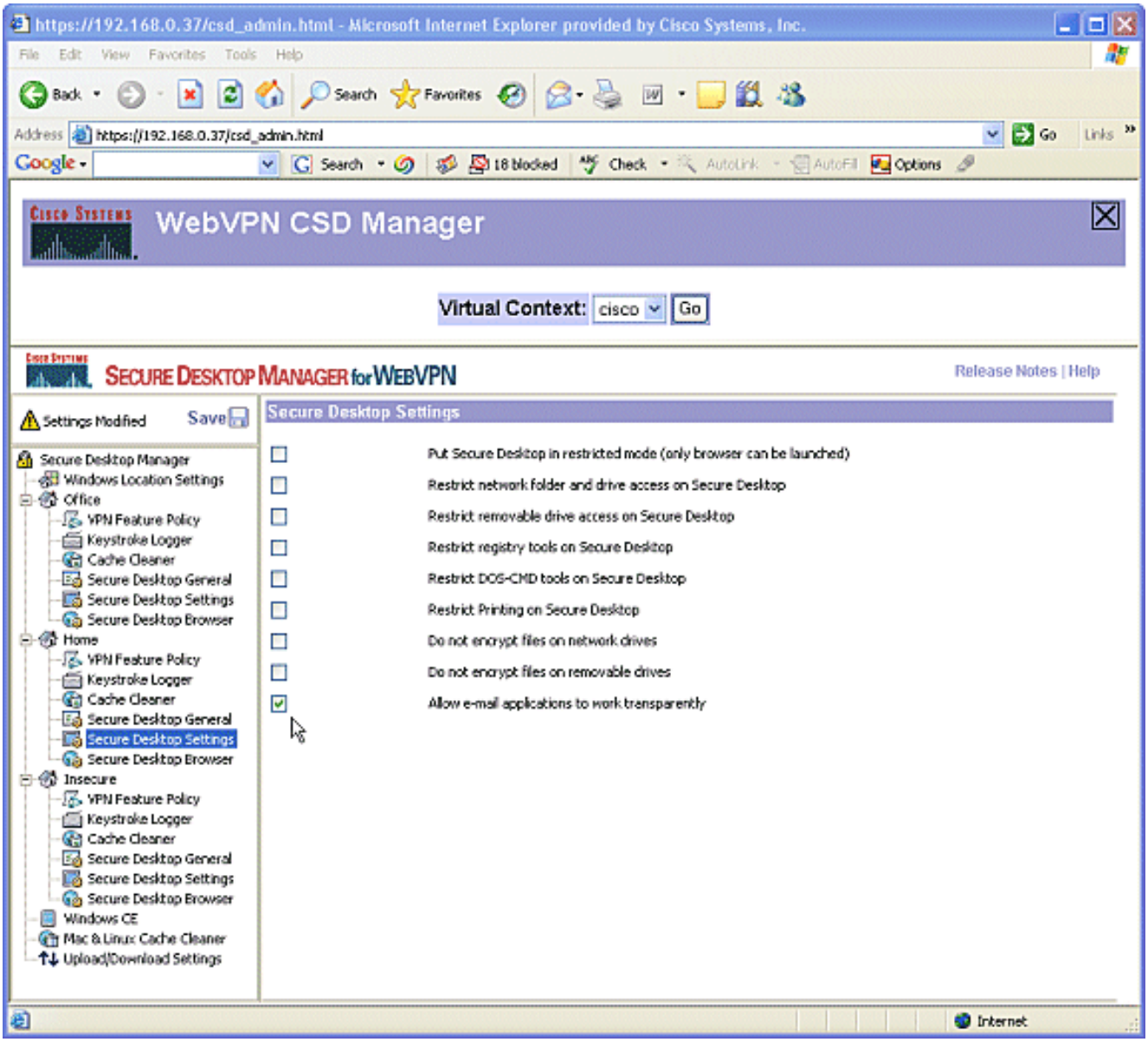
5. Sous l'emplacement des fenêtres d'accueil, sélectionnez **Nettoyeur de cache**. Laissez les paramètres par défaut comme indiqué dans la capture d'écran.



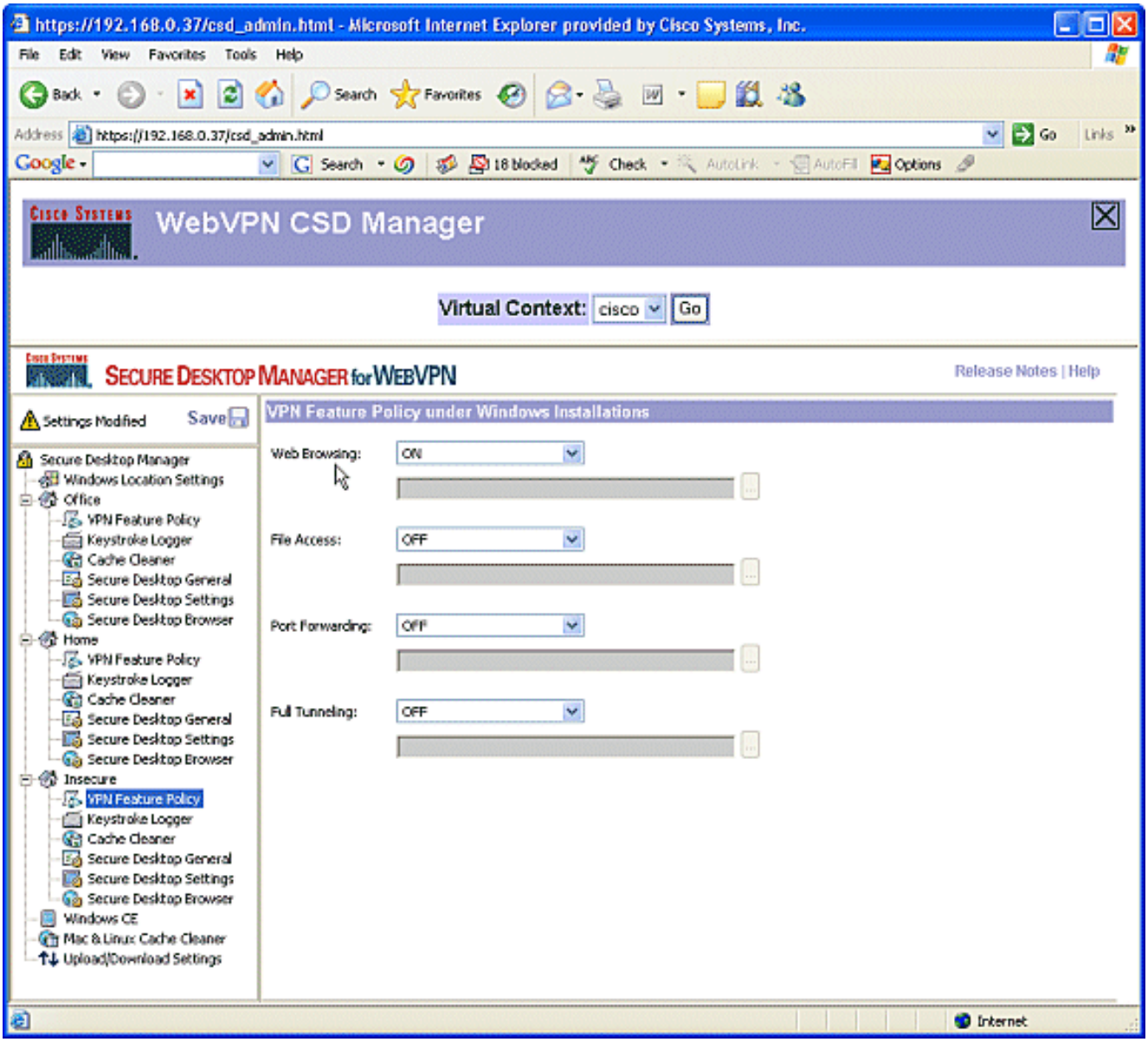
6. Sous Accueil, sélectionnez **Secure Desktop General**. Cochez **la case Suggérer la désinstallation de l'application lors de la fermeture de Secure Desktop**. Laissez tous les autres paramètres à leurs paramètres par défaut, comme indiqué dans la capture d'écran.



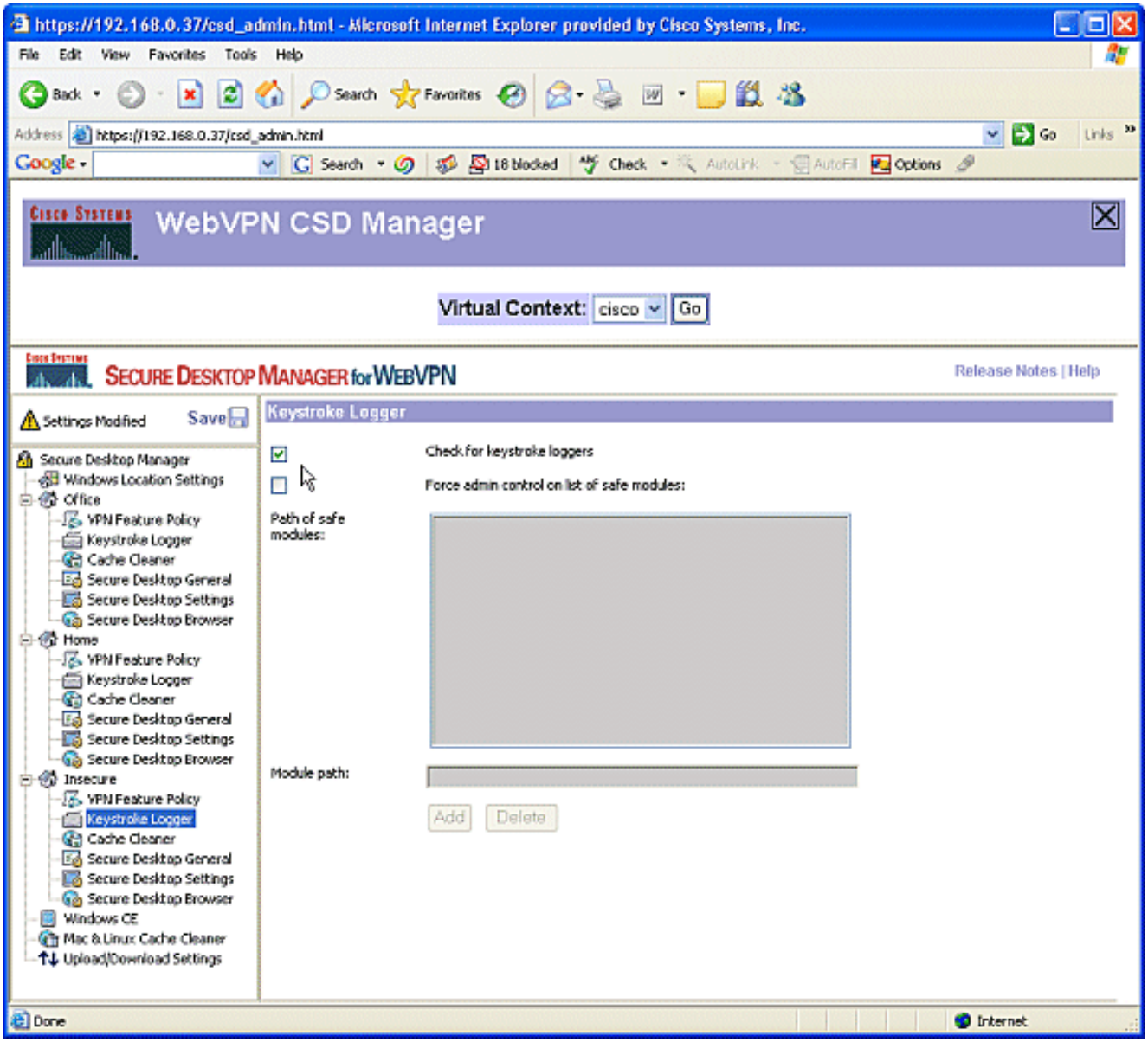
7. Dans Paramètres du bureau sécurisé sous Accueil, sélectionnez **Autoriser le fonctionnement transparent des applications de messagerie électronique**. Lorsque vous y êtes invité, cliquez sur **Enregistrer**, puis sur **OK**.



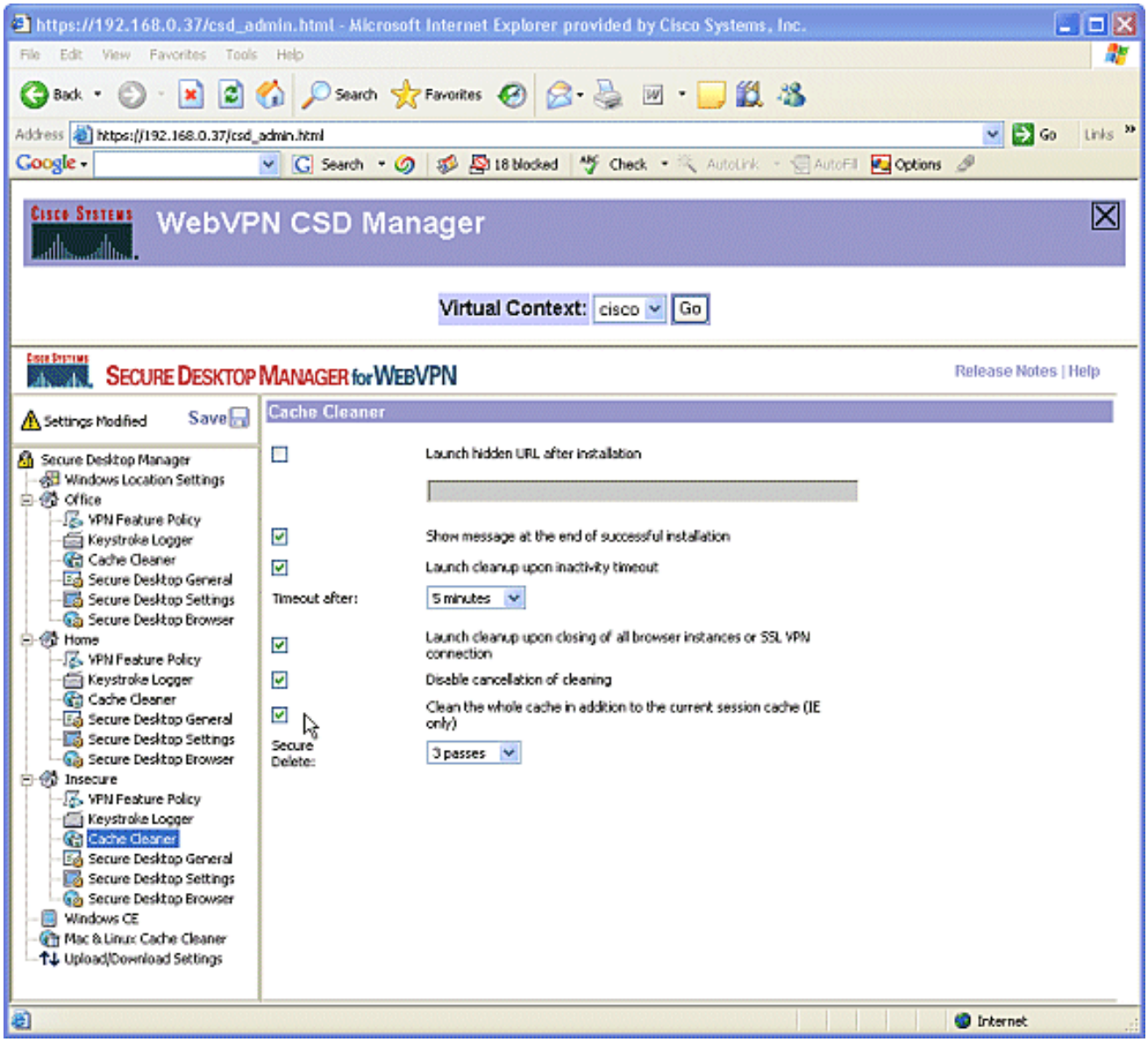
8. La configuration de **Secure Desktop Browser** dépend du fait que vous souhaitiez ou non que ces utilisateurs accèdent à un site Web d'entreprise avec des favoris préconfigurés.Sous Insecure, sélectionnez **VPN Feature Policy**.Étant donné que ces utilisateurs ne sont pas fiables, autorisez uniquement la navigation sur le Web.Choisissez **ON** dans le menu déroulant **Navigation Web**.Tous les autres accès sont définis sur **OFF**.



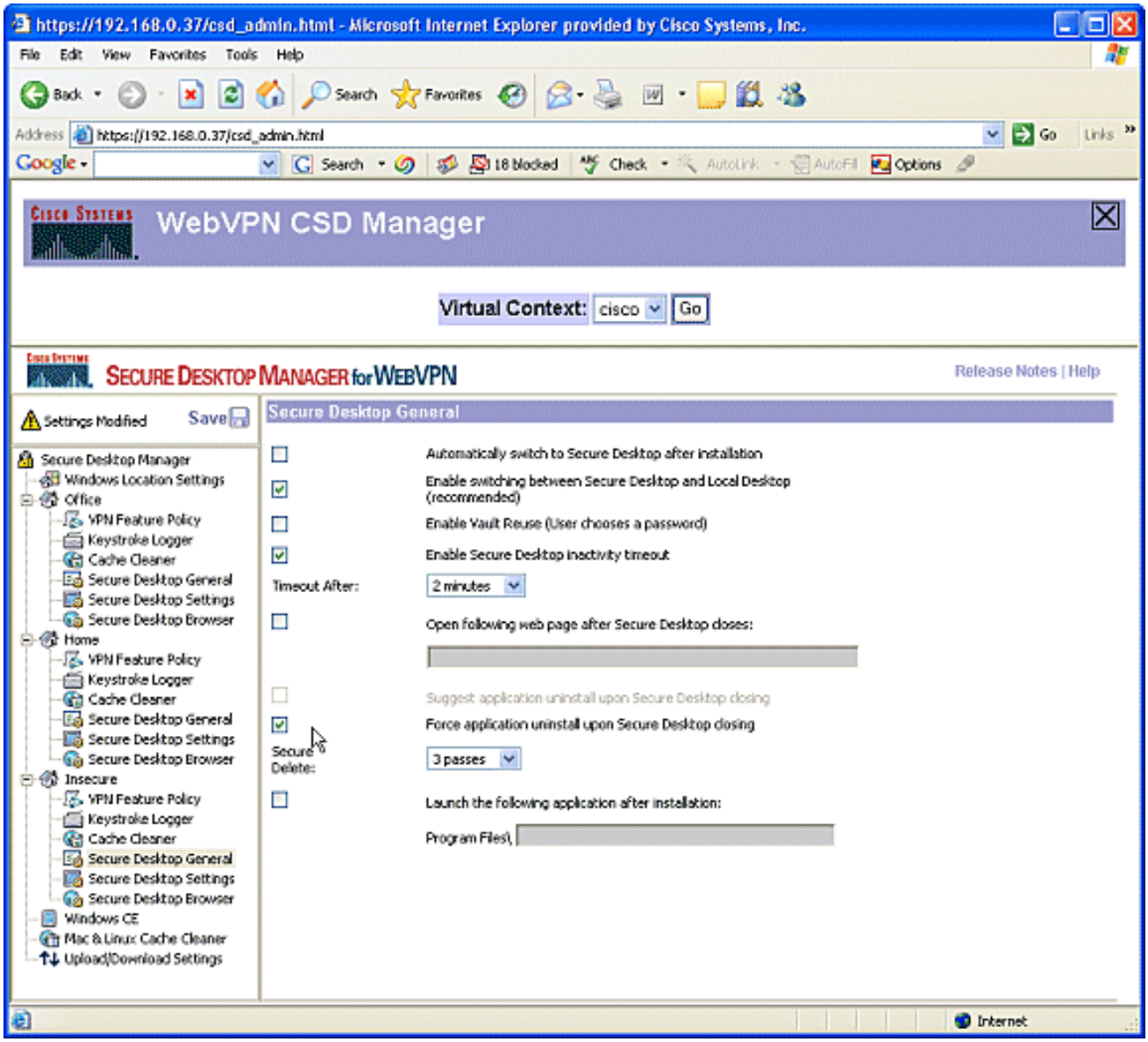
9. Cochez la case **Vérifier les enregistreurs de frappe**.



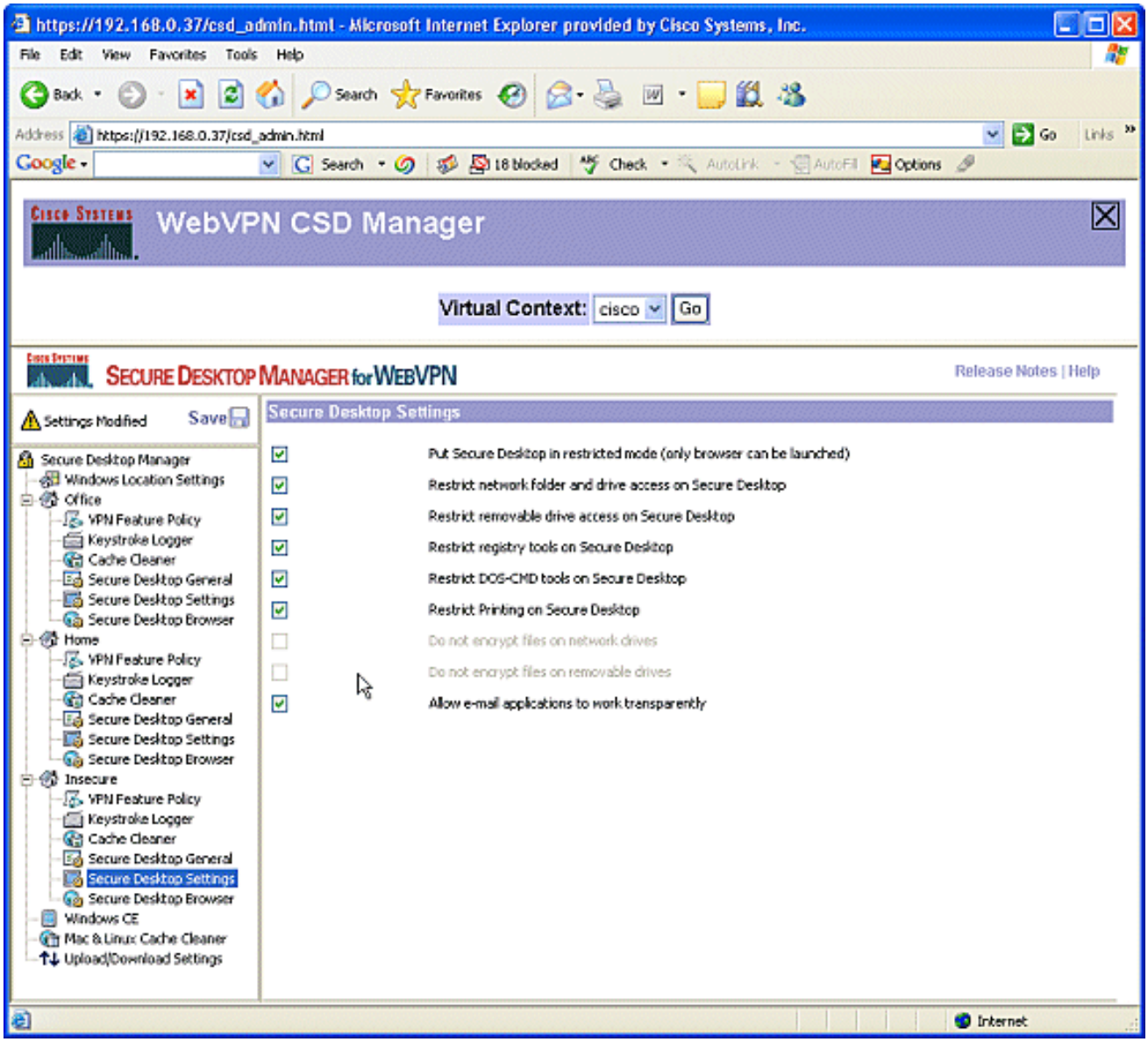
10. Configurez le Nettoyeur de cache pour l'absence de sécurité.Cochez la case **Nettoyer l'intégralité du cache en plus du cache de session en cours (IE uniquement)**.Laissez les autres paramètres par
défaut.



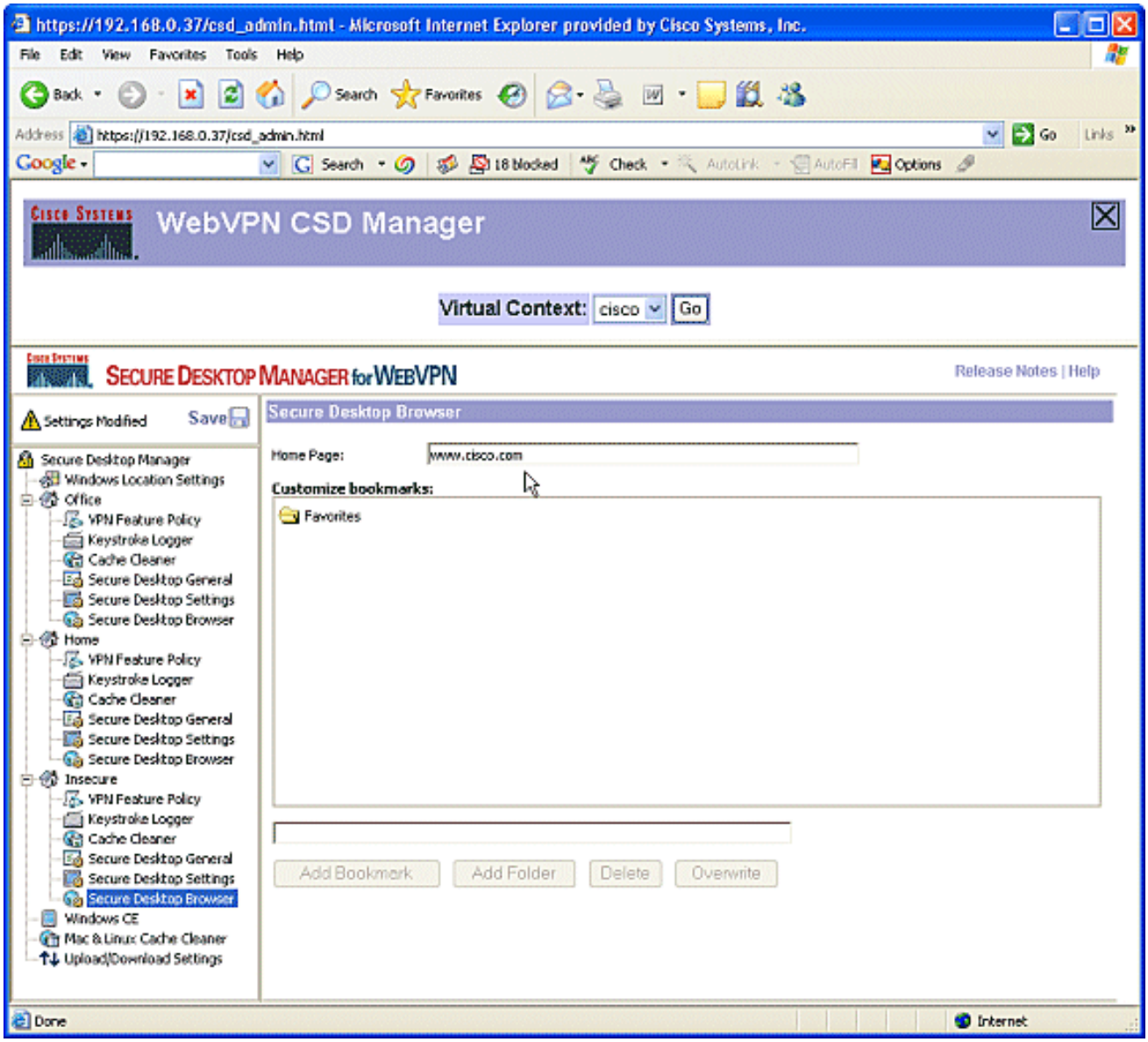
11. Sous Insecure, sélectionnez **Secure Desktop General**.Réduire le délai d'inactivité à 2 minutes.Cochez la case **Forcer la désinstallation de l'application lors de la fermeture de Secure Desktop**.



12. Choisissez **Secure Desktop Settings** sous Insecure, et configurez des paramètres très restrictifs comme
indiqué.



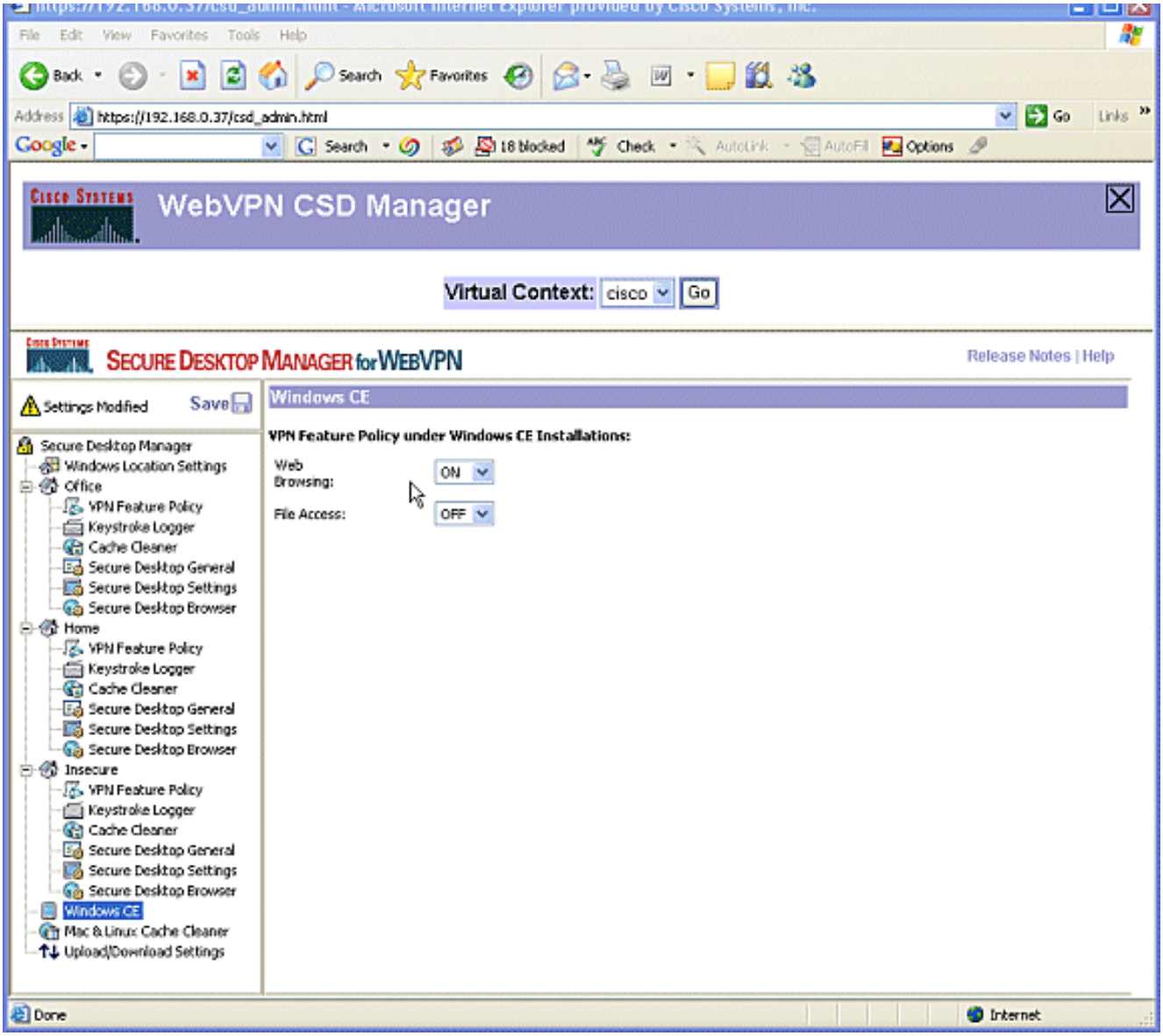
13. Choisissez **Secure Desktop Browser**. Dans le champ Page d'accueil, saisissez le site Web vers lequel ces clients seront guidés pour leur page d'accueil.



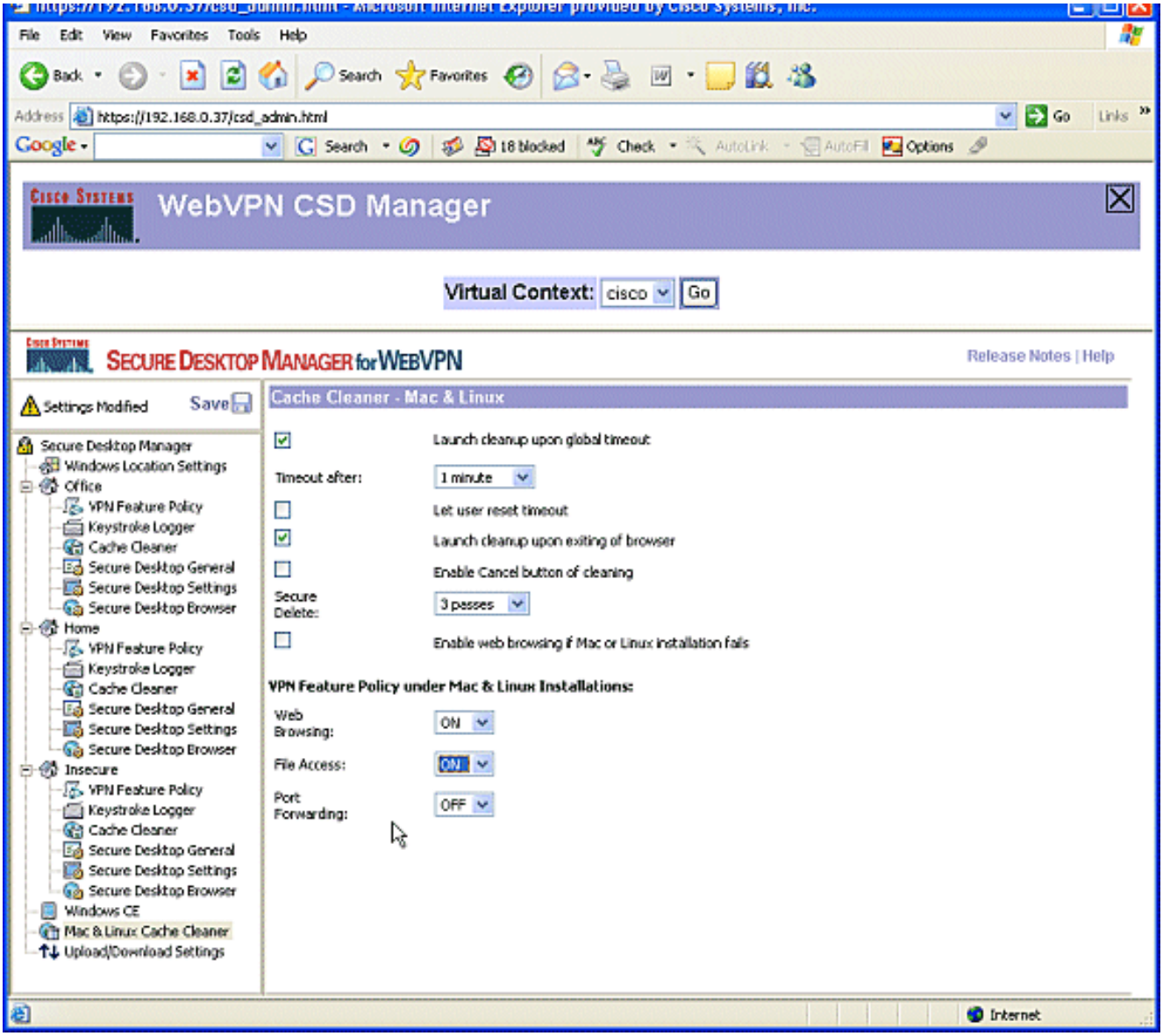
Phase II : Étape 4 : Configurez les fonctionnalités Windows CE, Macintosh et Linux.

Configurez les fonctionnalités CSD pour Windows CE, Macintosh et Linux.

1. Choisissez **Windows CE** sous Secure Desktop Manager. Windows CE a des fonctionnalités VPN limitées. Activez **la navigation Web**.



2. Choisissez **Nettoyeur de cache Mac & Linux**.Les systèmes d'exploitation Macintosh et Linux n'ont accès qu'aux aspects de nettoyage de cache de CSD. Configurez-les comme indiqué sur le schéma.Lorsque vous y êtes invité, cliquez sur **Enregistrer**, puis sur **OK**.

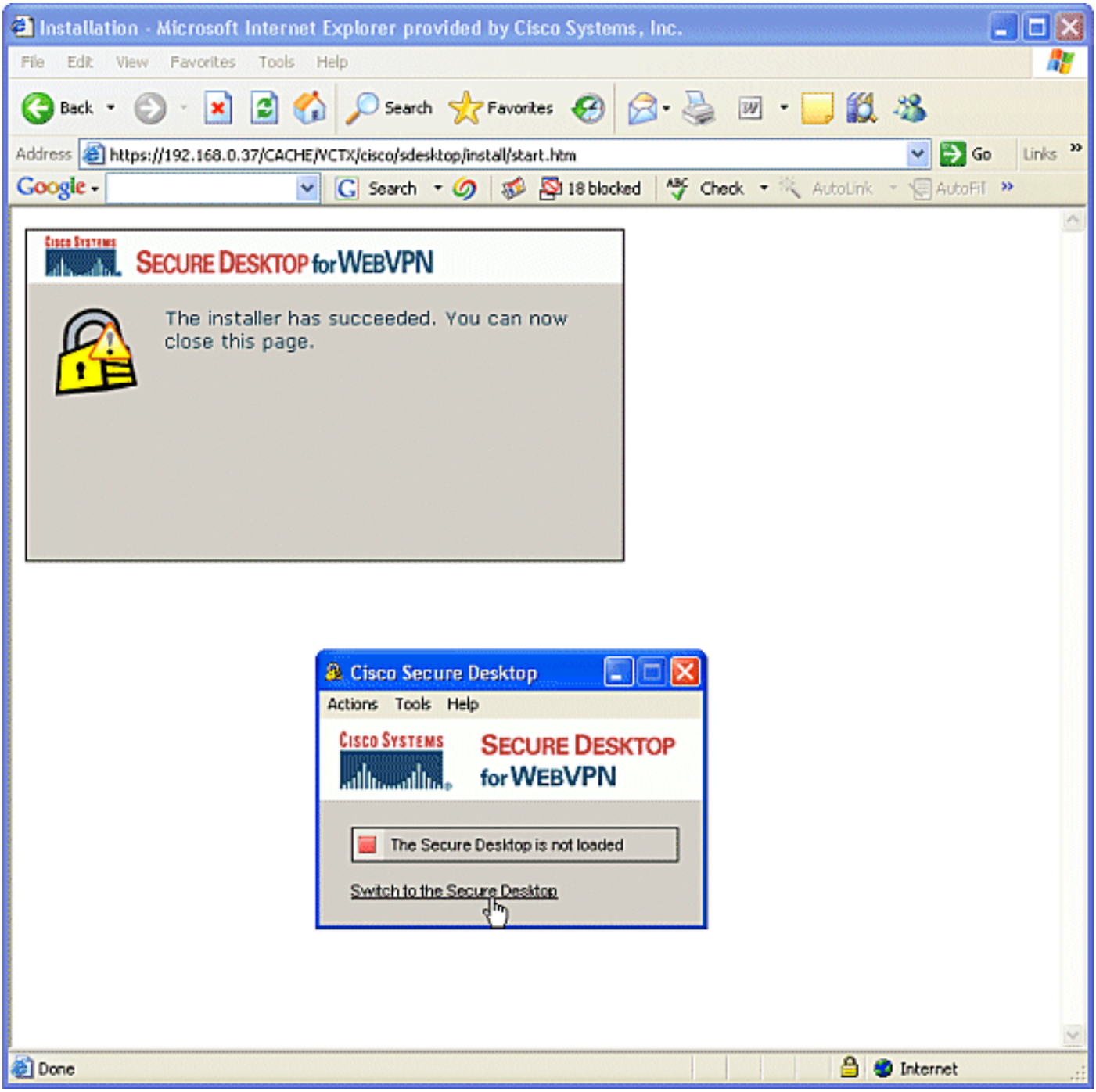


Vérification

Tester le fonctionnement du CSD

Testez le fonctionnement du CSD en vous connectant à la passerelle WebVPN avec un navigateur compatible SSL à l'adresse **https://WebVPN_Gateway_IP**.

Remarque : N'oubliez pas d'utiliser le nom unique du contexte si vous avez créé des contextes WebVPN différents, par exemple, **https://192.168.0.37/cisco**.



Commandes

Plusieurs **commandes show sont associées à WebVPN.** Vous pouvez exécuter ces commandes dans l'interface de ligne de commande (CLI) afin d'afficher les statistiques et autres informations. Pour obtenir des informations détaillées à propos des commandes **show, reportez-vous à** Vérification de la configuration de WebVPN.

Remarque : L'analyseur CLI (clients enregistrés uniquement) prend en charge certaines commandes **show**. Utilisez l'analyseur CLI pour afficher une analyse de la sortie de la commande **show**.

Dépannage

Commandes

Plusieurs commandes **debug sont associées à WebVPN.** Pour obtenir des informations détaillées à propos de ces commandes, reportez-vous à Utilisation des commandes Debug WebVPN.

Remarque : l'utilisation des commandes **debug** peut avoir un impact négatif sur votre périphérique Cisco. Avant d'utiliser les commandes **debug , référez-vous à la section** Informations importantes sur les commandes Debug.

Pour plus d'informations sur les commandes **clear**, référez-vous à Utilisation des commandes Clear de WebVPN.

Informations connexes

- Guide de déploiement de convergence WebVPN et DMVPN
- VPN SSL - WebVPN
- Cisco IOS SSLVPN
- Support et documentation techniques - Cisco Systems