SDMを使用したCisco IOSでのCSDの設定

内容

概要
前提条件
要件
使用するコンポーネント
ネットワーク図
関連製品
表記法
設定
フェーズ 1：SDM を使用してルータを CSD 設定用に準備する。
フェーズ 1：ステップ 1：WebVPN ゲートウェイ、WebVPN コンテキスト、およびグループ ポリシーを設定する。
フェーズ 1：ステップ 2：WebVPN のコンテキストで CSD を有効にする。
フェーズ 2：Web ブラウザを使用して CSD を設定する。
フェーズ 2：ステップ 1：Windows の口ケーションを定義する。
フェーズ 2：ステップ 2：口ケーションの基準を識別する。
フェーズ 2：ステップ 3：Windows の口ケーションのモジュールと機能を設定する。
フェーズ 2：ステップ 4：Windows CE、Macintosh、および Linux の機能を設定する。
確認
CSD の動作テスト
コマンド
トラブルシュート
コマンド
関連情報

概要

Secure Sockets Layer（SSL）VPN（Cisco WebVPN）のセッションがセキュアであっても、クッキー、ブラウザ ファイル、E メールの添付ファイルが、セッション完了後もクライアントに残ったままになっています。Cisco Secure Desktop（CSD）では、セッションのデータを暗号化した形式でクライアントのディスクの特別な vault 領域に書き込んで、SSL VPN セッションの本来のセキュリティを強化します。さらに、このデータは SSL VPN セッションが終了したときにディスクから削除されます。このドキュメントでは、Cisco IOS(R) ルータでの CSD の設定例について説明します。

CSD をサポートするシスコのデバイス プラットフォームには次のものがあります。

- Cisco IOS ルータ バージョン 12.4(6)T 以降
- Cisco 870、1811、1841、2801、2811、2821、2851、3725、3745、3825、3845、7200、および 7301 ルータ
- Cisco VPN 3000 シリーズ コンセントレータ バージョン 4.7 以降
- Cisco ASA 5500 シリーズ セキュリティ アプライアンス バージョン 7.1 以降
- Cisco Catalyst および Cisco 7600 シリーズ用 Cisco WebVPN サービス モジュール バージョ

ン 1.2 以降

前提条件

要件

この設定を行う前に、次の要件が満たされていることを確認します。

Cisco IOS ルータの要件

- Advanced Image 12.4(6T) 以降が導入された Cisco IOS ルータ
- Cisco Router Secure Device Manager（SDM）2.3 以降
- 管理ステーションに IOS パッケージ用の CSD
- ルータの自己署名デジタル証明書または認証局（CA）による認証**注：デジタル**証明書を使用する場合は、必ずルータのホスト名、ドメイン名、日付/時刻/タイムゾーンを正しく設定してください。
- ルータのイネーブル シークレット パスワード
- ルータで DNS がイネーブルになっている。一部の WebVPN サービスが正しく動作するためには、DNS が必要です。

クライアント コンピュータの要件

- リモート クライアントには、ローカルの管理者権限があること。これは必須事項ではありませんが、重要な推奨事項です。
- リモート クライアントには、Java Runtime Environment（JRE）バージョン 1.4 以降が必要です。
- リモート クライアント ブラウザ：Internet Explorer 6.0、Netscape 7.1、Mozilla 1.7、Safari 1.2.2、Firefox 1.0 のいずれか
- リモート クライアントでクッキーがイネーブルにされており、ポップアップが許可されていること。

使用するコンポーネント

このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づいています。

- バージョン 12.9(T) の Cisco IOS ルータ 3825
- SDM バージョン 2.3.1

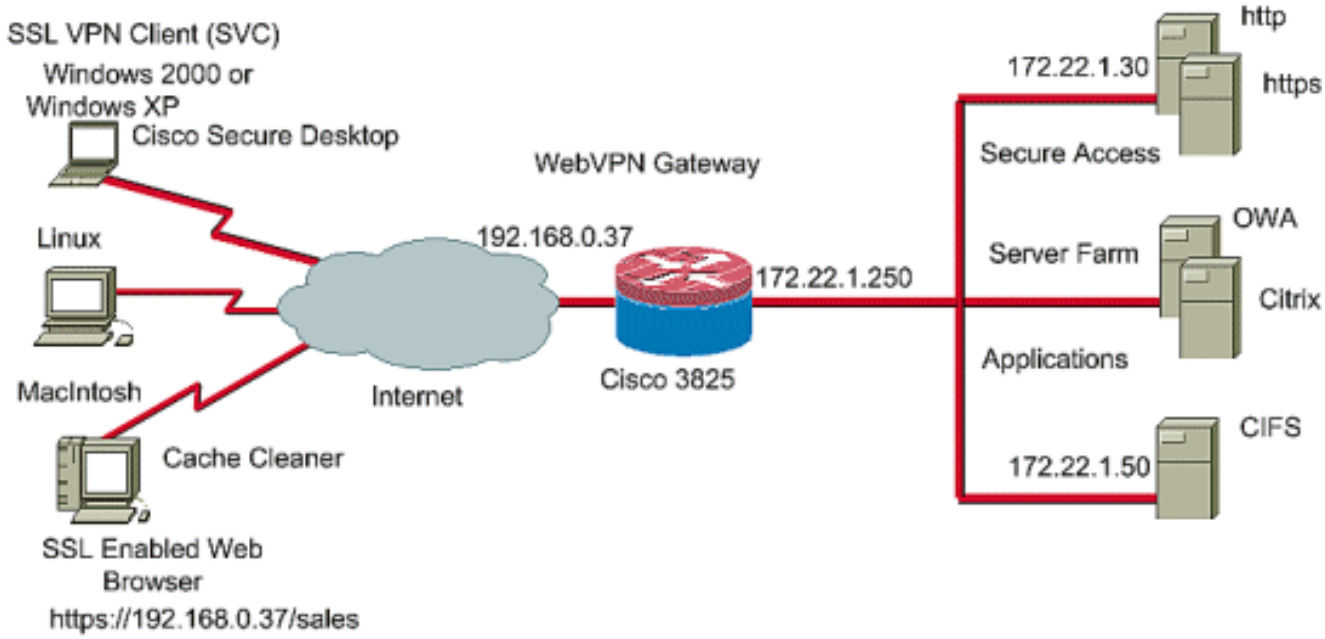
このドキュメントの情報は、特定のラボ環境にあるデバイスに基づいて作成されました。このドキュメントで使用するすべてのデバイスは、クリアな（デフォルト）設定で作業を開始しています。対象のネットワークが実稼働中である場合には、どのようなコマンドについても、その潜在的な影響について確実に理解しておく必要があります。

ネットワーク図

このドキュメントでは、次のネットワーク セットアップを使用します。

この例では、Cisco 3825 シリーズ ルータを使用して、社内のイントラネットに安全にアクセスできるようにしています。Cisco 3825 シリーズ ルータでは、設定可能な CSD 機能とその特性により SSL VPN 接続のセキュリティが向上しています。クライアントは、次の3つのSSL VPN方式の

いずれかを使用してCSD対応ルータに接続できます。クライアントレスSSL VPN(WebVPN)、シンクライアントSSL VPN（ポートフォワーディング）、またはSSL VPNクライアント（フルトンネリングSVC）。



関連製品

この設定は、次のバージョンのハードウェアとソフトウェアにも使用できます。

- Cisco ルータ プラットフォーム 870、1811、1841、2801、2811、2821、2851、3725、3745、3825、3845、7200、および 7301
- Cisco IOS Advanced Security Image バージョン 12.4(6)T 以降

表記法

ドキュメント表記の詳細は、『シスコ テクニカル ティップスの表記法』を参照してください。

設定

WebVPN ゲートウェイを使用すると、ユーザはいずれかの SSL VPN テクノロジーでルータに接続できるようになります。WebVPN ゲートウェイには複数の WebVPN コンテキストを割り当てることができますが、各デバイスで IP アドレスごとに指定できる WebVPN ゲートウェイは 1 つだけです。各コンテキストは、一意の名前で識別します。グループ ポリシーによって、特定の WebVPN コンテキストで使用可能な設定済みリソースが識別されます。

IOS ルータでの CSD の設定は、次の 2 つのフェーズで行います。

フェーズ 1：SDM を使用してルータを CSD 設定用に準備する。

1. **WebVPN ゲートウェイ、WebVPN コンテキスト、およびグループ ポリシーを設定する。注：この手順はオプションであり、このドキュメントでは詳しく説明していません。使用しているルータにすでに SSL VPN テクノロジーのいずれかが設定されている場合は、このステップを省略してください。**

2. WebVPN のコンテキストで CSD を有効にする。
フェーズ 2：Web ブラウザを使用して CSD を設定する。

1. Windows のロケーションを定義する。
2. ロケーションの基準を識別する。
3. Windows のロケーションのモジュールと機能を設定する。
4. Windows CE、Macintosh、および Linux の機能を設定する。

フェーズ 1：SDM を使用してルータを CSD 設定用に準備する。

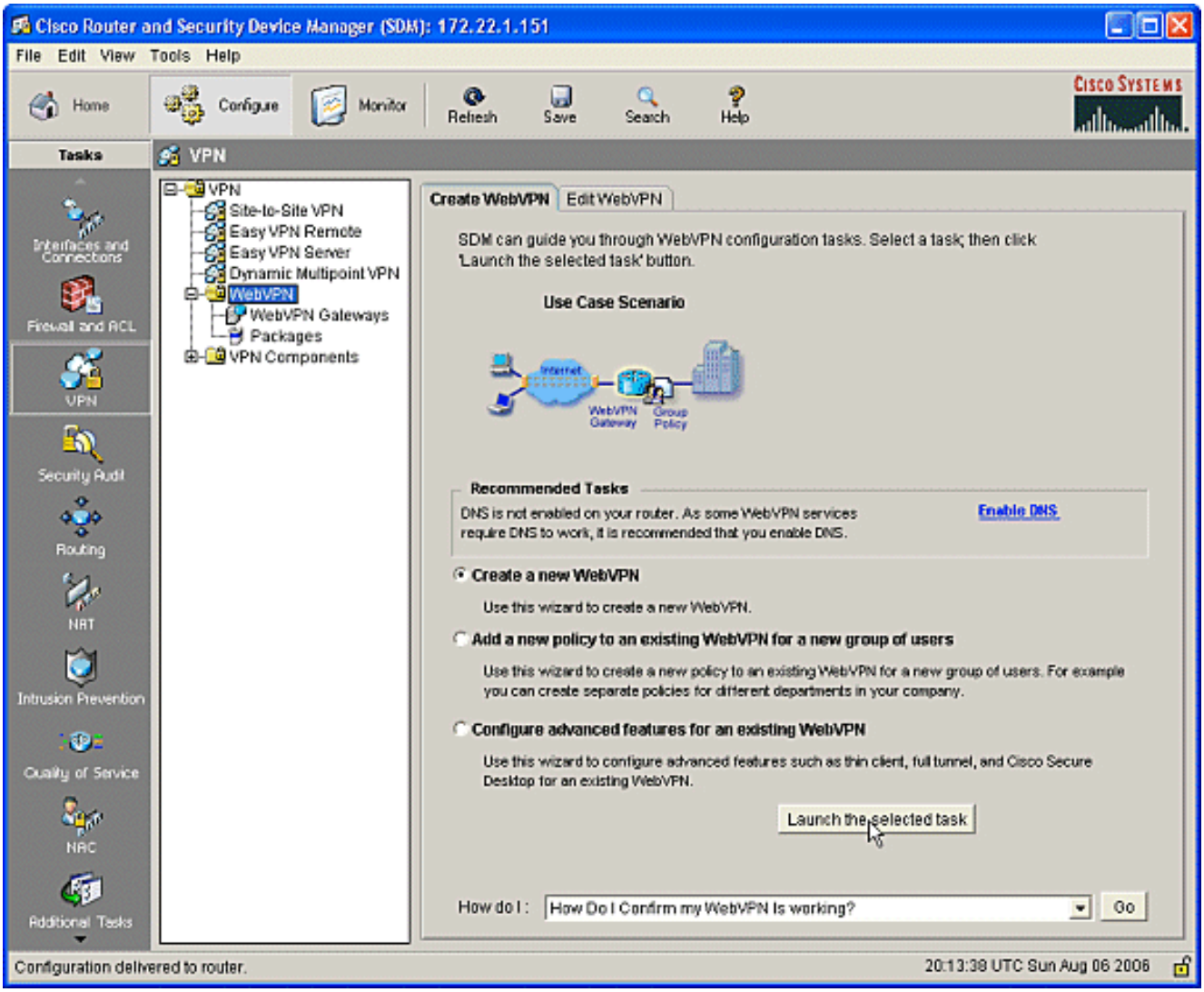
CSD は、SDM を使用して、または command-line interface (CLI; コマンドライン インターフェイス) から設定できます。 この設定では、SDM と Web ブラウザを使用します。

これらのステップは、使用している IOS ルータで CSD を設定するために実行します。

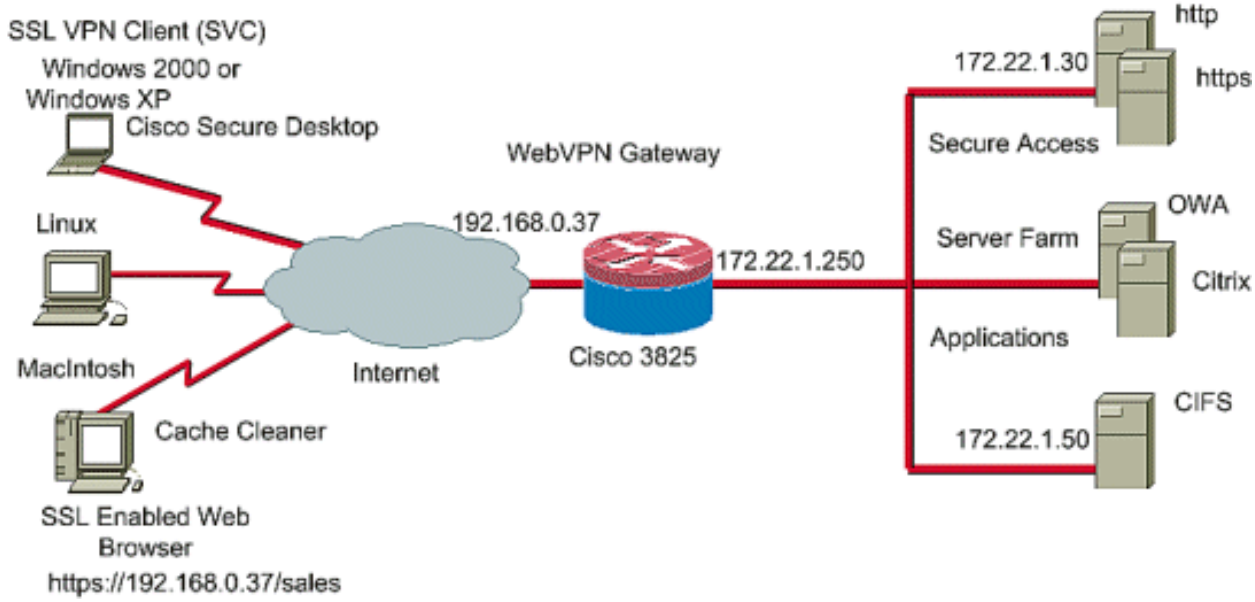
フェーズ 1：ステップ 1：WebVPN ゲートウェイ、WebVPN コンテキスト、およびグループ ポリシーを設定する。

この操作は、WebVPN Wizard を使用して行います。

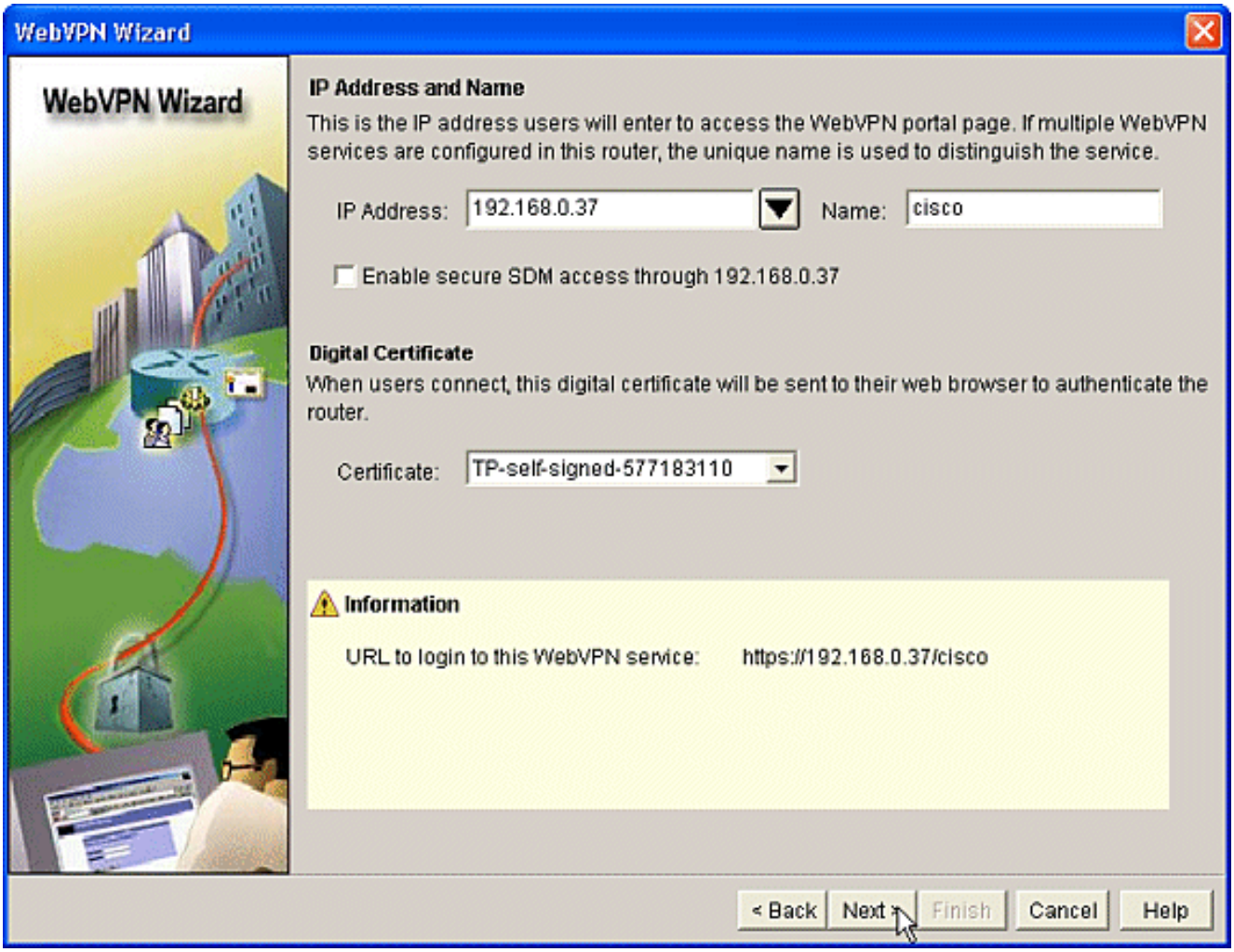
1. SDMを開き、[**Configure] > [VPN] > [WebVPN]に移動します。**Create WebVPN タブをクリックして、Create a new WebVPN オプション ボタンをチェックします。[Launch the selected task] をクリックします。



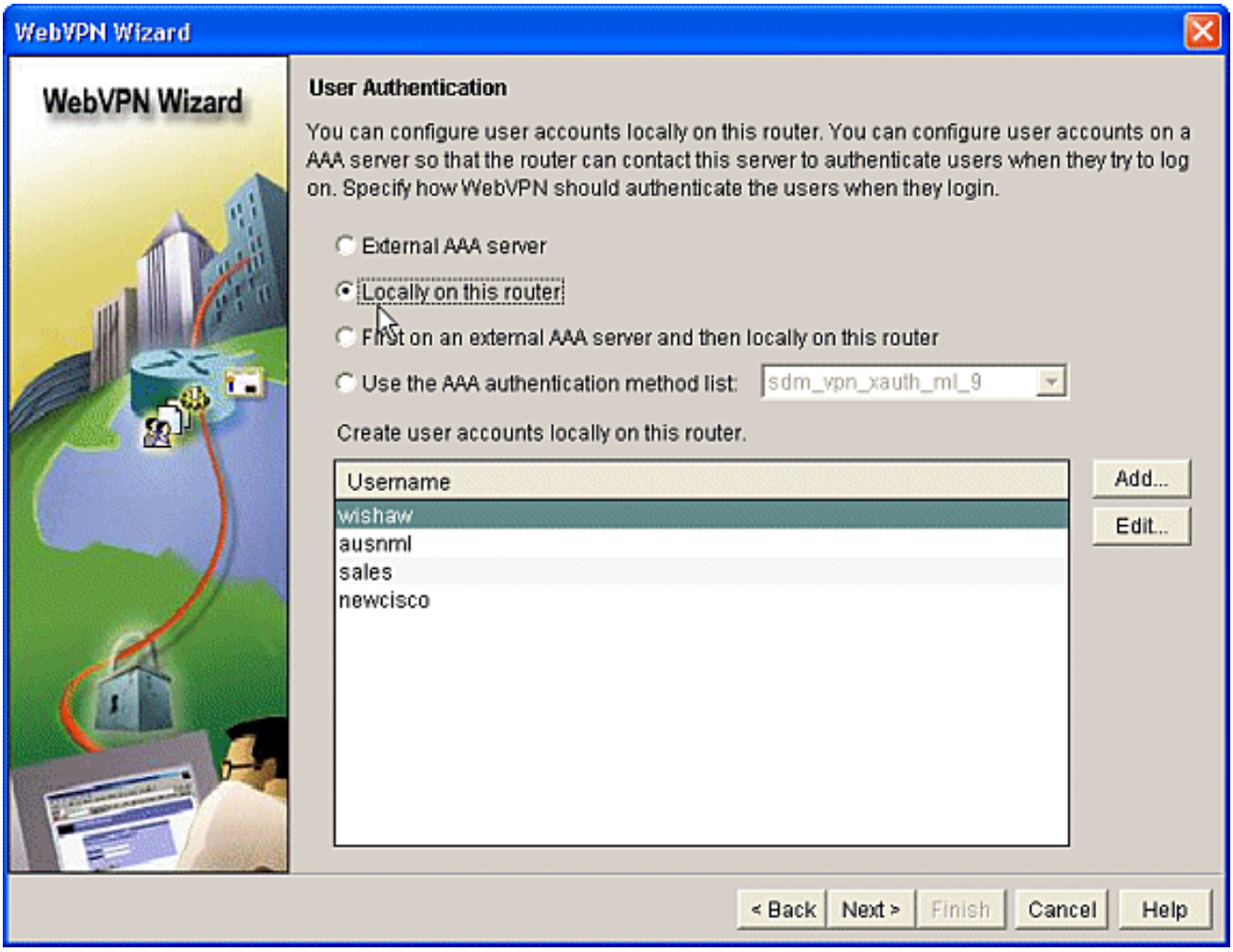
2. WebVPN Wizard の画面に、設定可能なパラメータのリストが表示されます。[next] をクリックします。



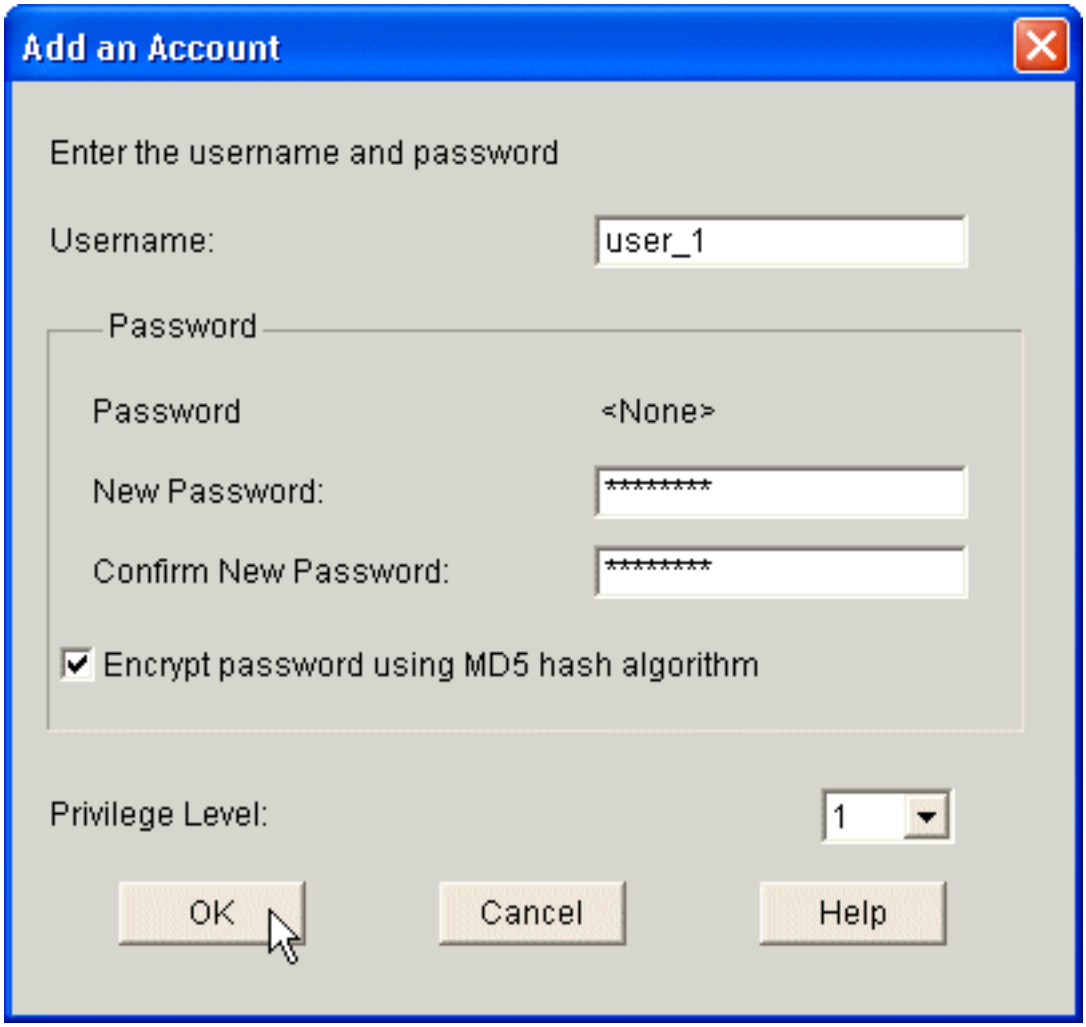
3. WebVPN ゲートウェイの IP アドレス、サービスの一意の名前、デジタル証明書の情報を入力します。[next] をクリックします。



4. この WebVPN ゲートウェイに対する認証のためのユーザ アカウントが作成できます。ローカルのアカウント、あるいは、外部の Authentication, Authorization, and Accounting (AAA; 認証、認可、アカウンティング) サーバで作成されたアカウントのいずれも使用できます。この例では、ルータでローカルのアカウントを使用しています。Locally on this router オプション ボタンをチェックして、Add をクリックします。

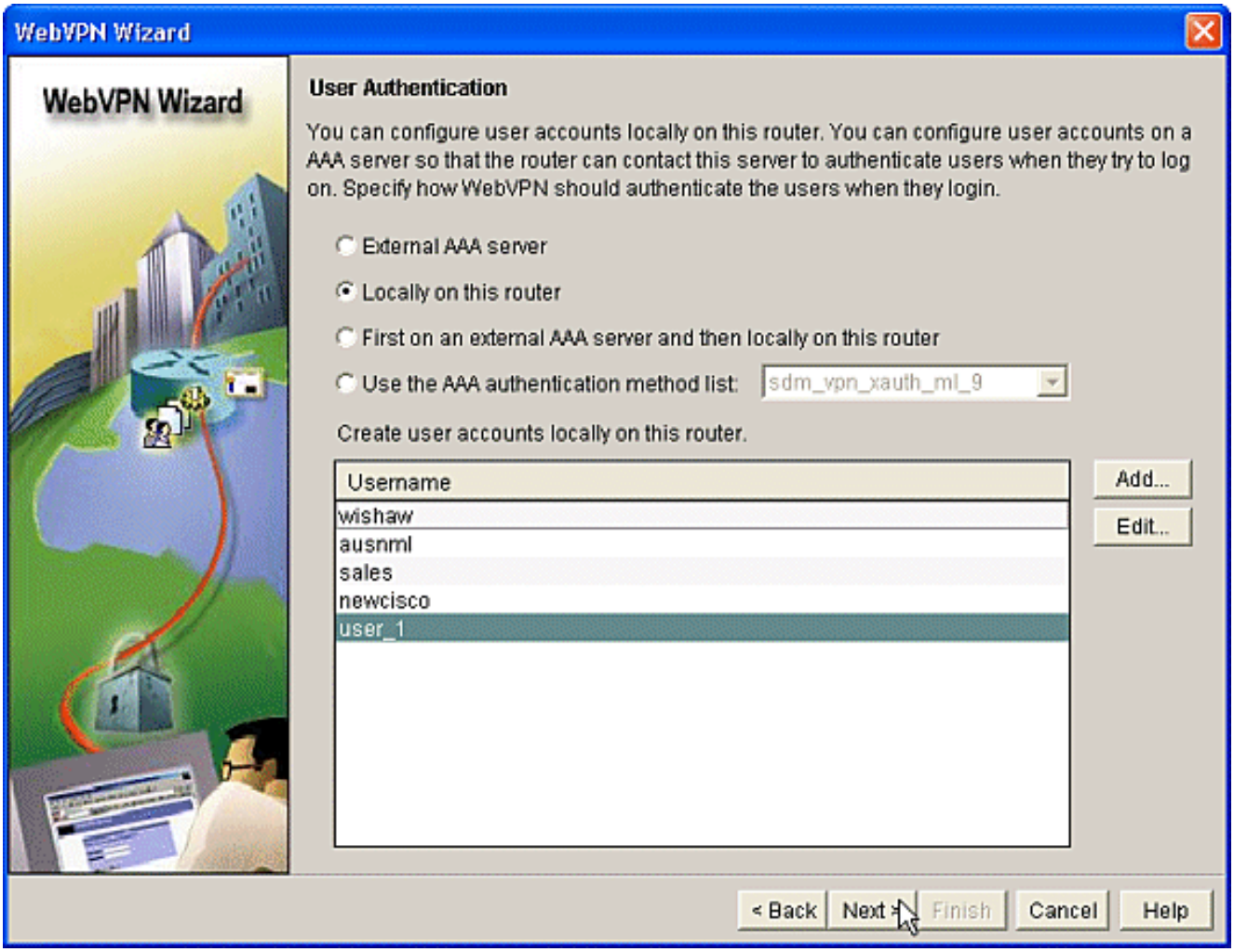


5. Add an Account の画面で新しいユーザのアカウント情報を入力して、OK をクリックします

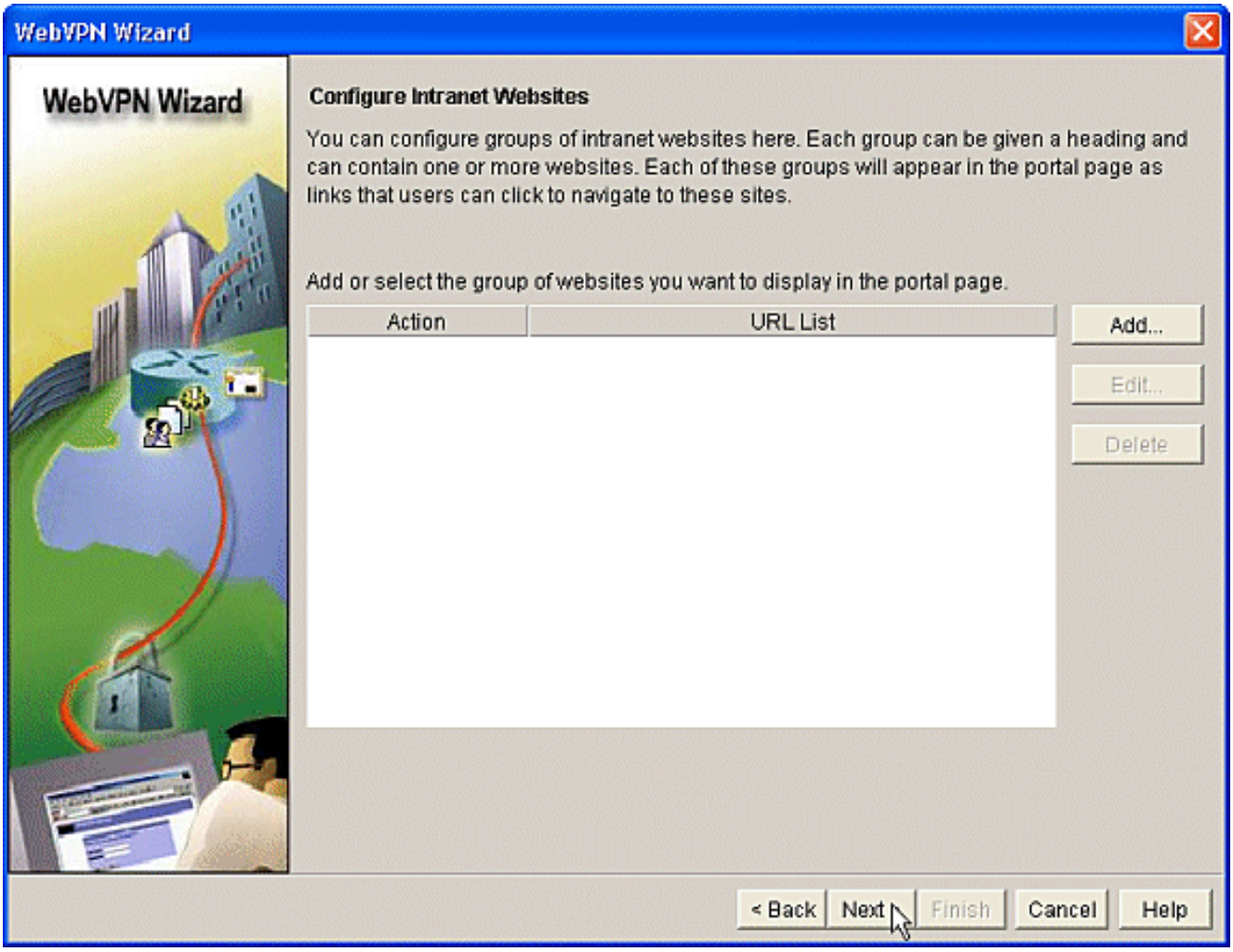


。

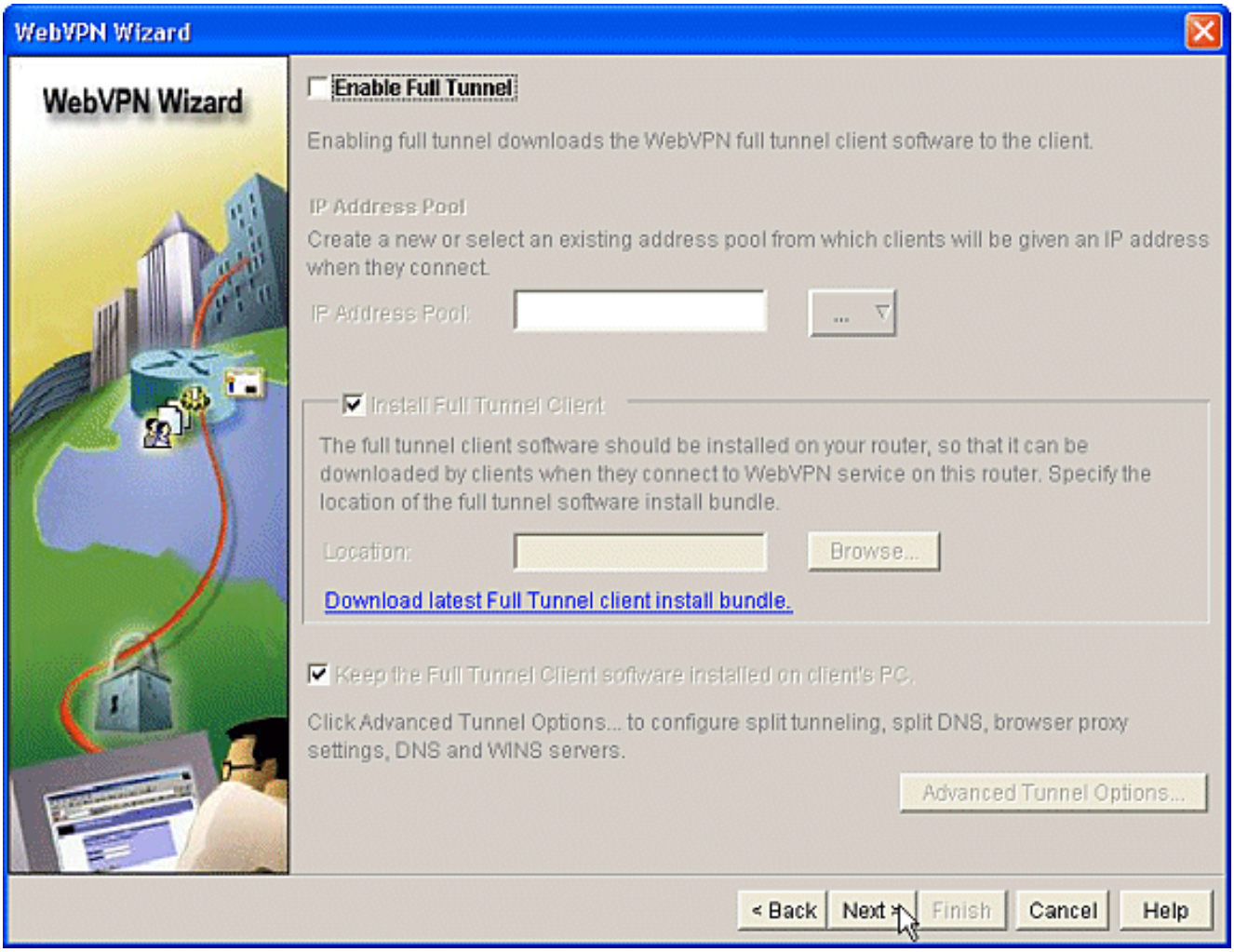
6. ユーザを作成したら、User Authentication のページで Next をクリックします。



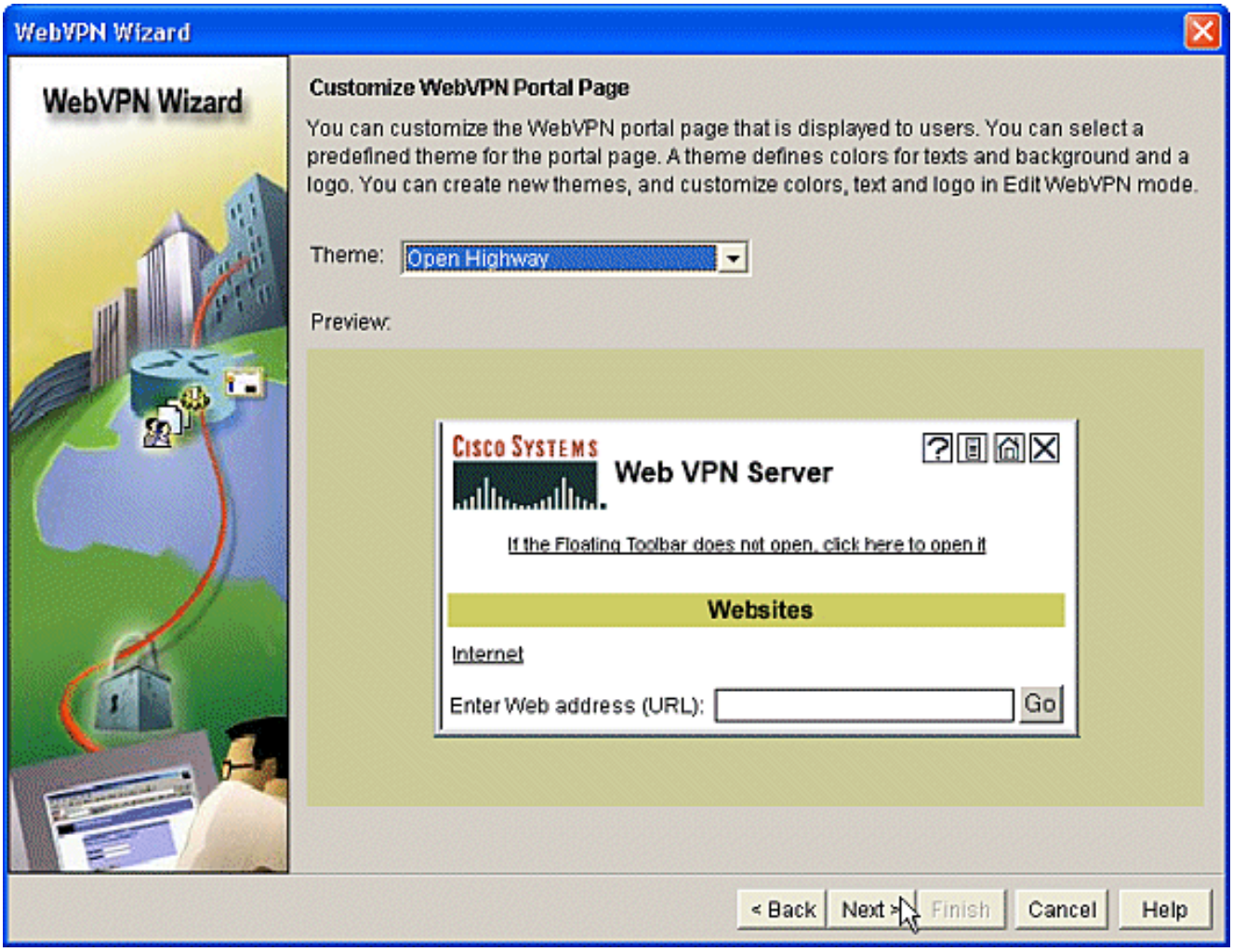
7. Configure Intranet Websites の画面では、WebVPN ゲートウェイのユーザがアクセスできる Web サイトを設定できます。このドキュメントでは CSD の設定に重点を置いているため、このページの説明については割愛します。[next] をクリックします。



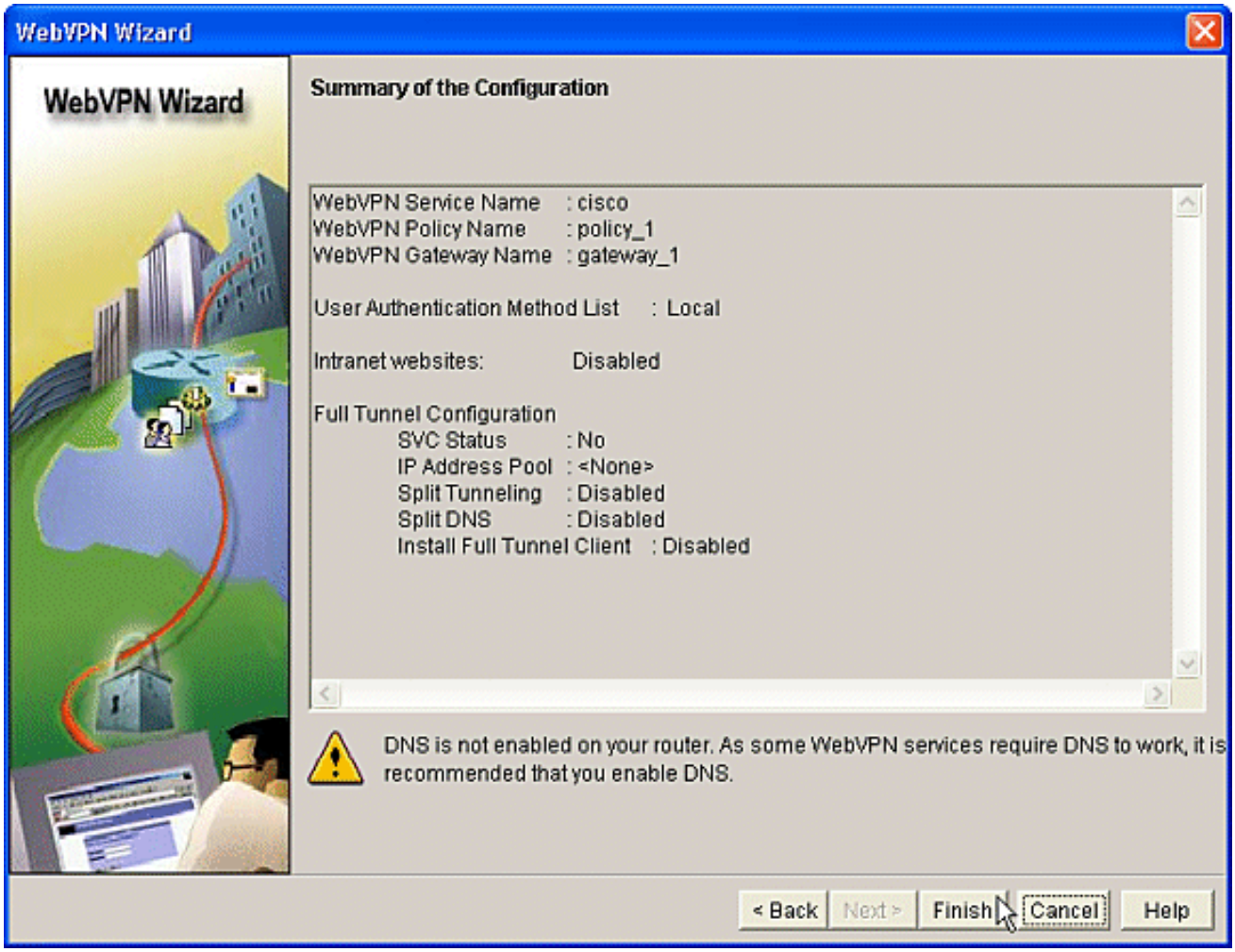
8. 次の WebVPN Wizard の画面では、フルトンネル SSL VPN クライアントをイネーブルにするための選択操作を行えますが、このドキュメントの目的は CSD をイネーブルにすることです。Enable Full Tunnel のチェックを外して、Next をクリックします。



9. ユーザに表示される WebVPN Portal Page の外観をカスタマイズできます。この場合はデフォルトのままにしています。[next] をクリックします。



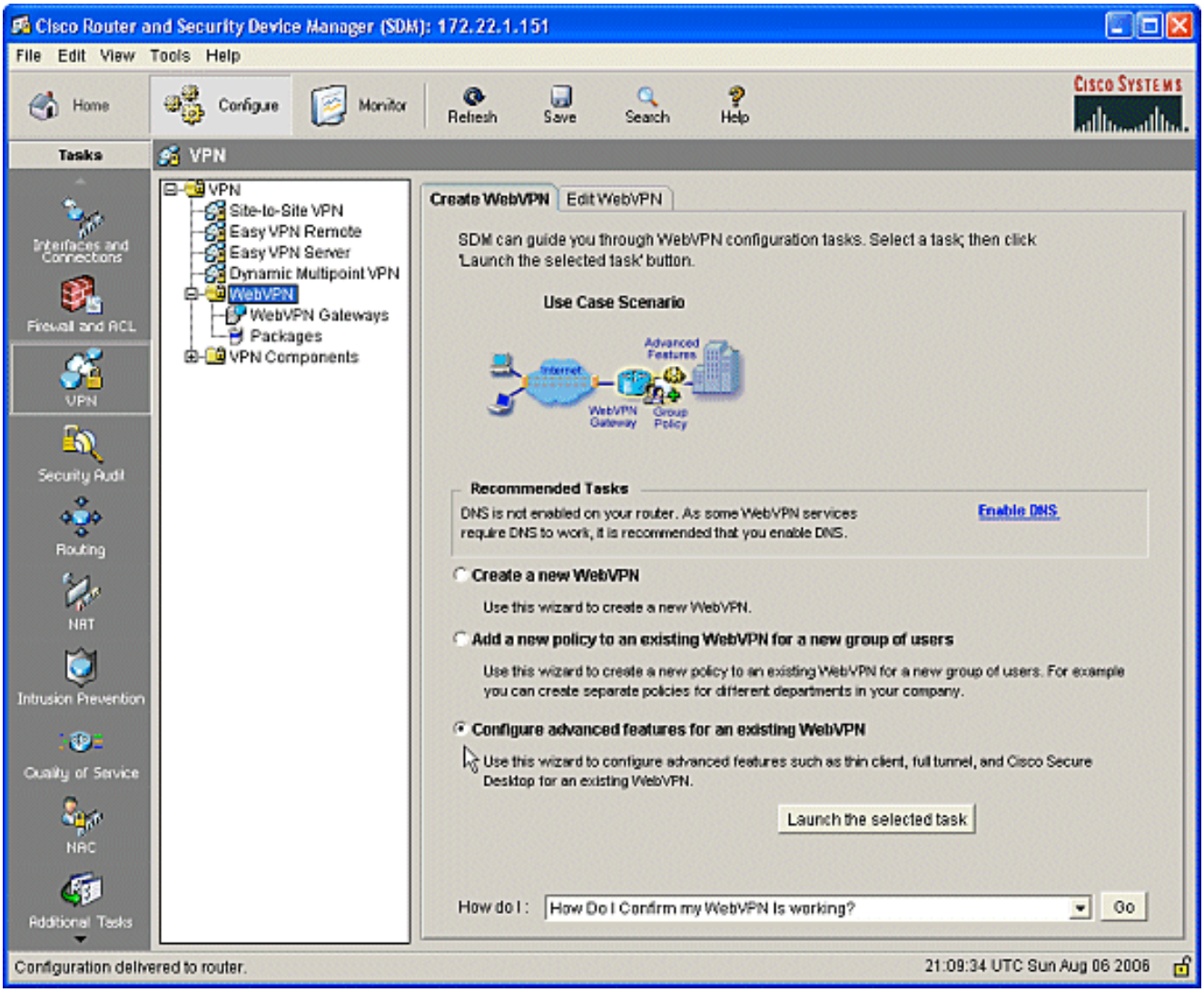
10. Wizard に、この一連の操作の最後の画面が表示されます。ここでは、WebVPN ゲートウェイの設定の要約が表示されます。Finish をクリックし、応答が表示されたら OK をクリックします。



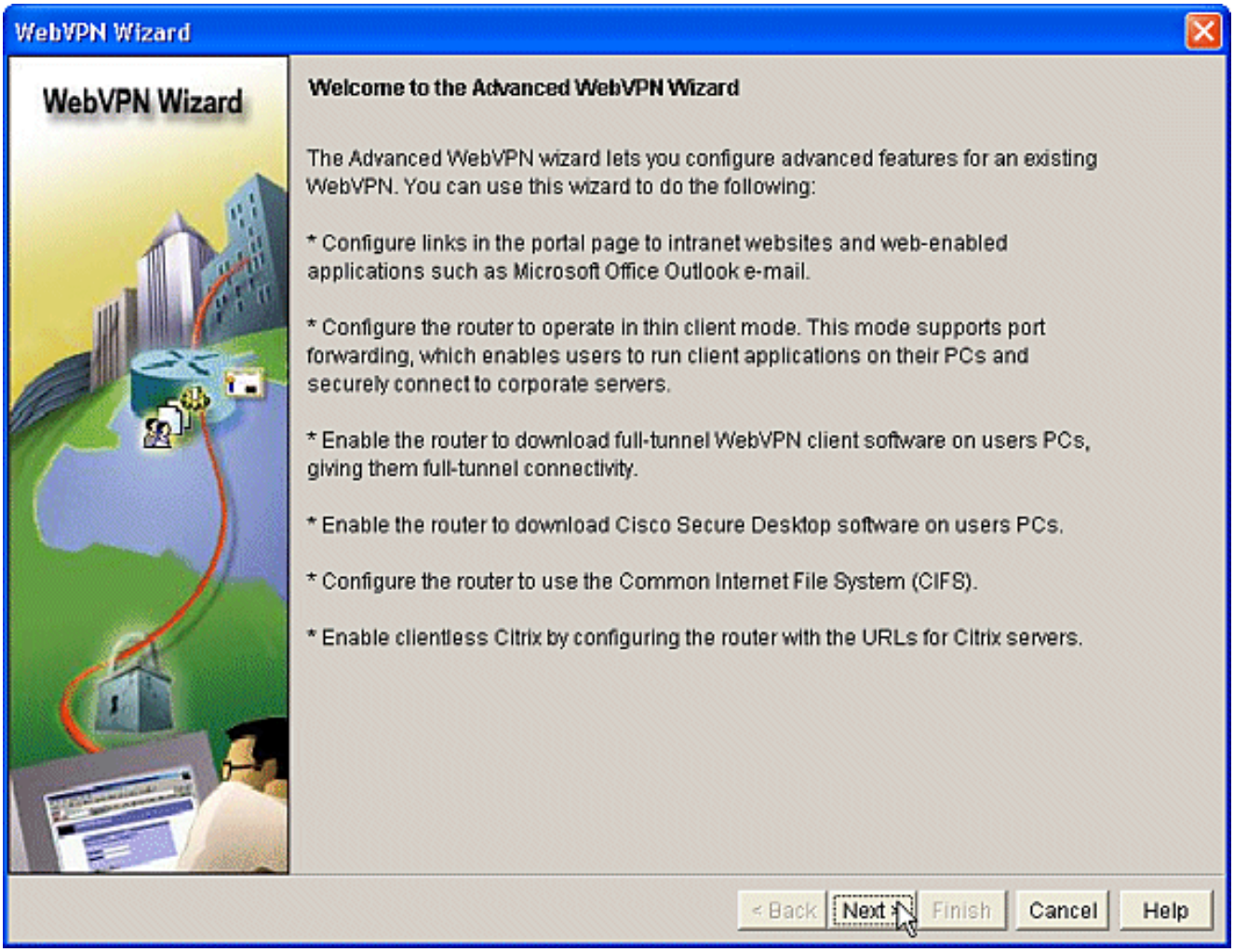
フェーズ 1：ステップ 2：WebVPN のコンテキストで CSD を有効にする。

WebVPN Wizard を使用して、WebVPN コンテキストの中で CSD をイネーブルにします。

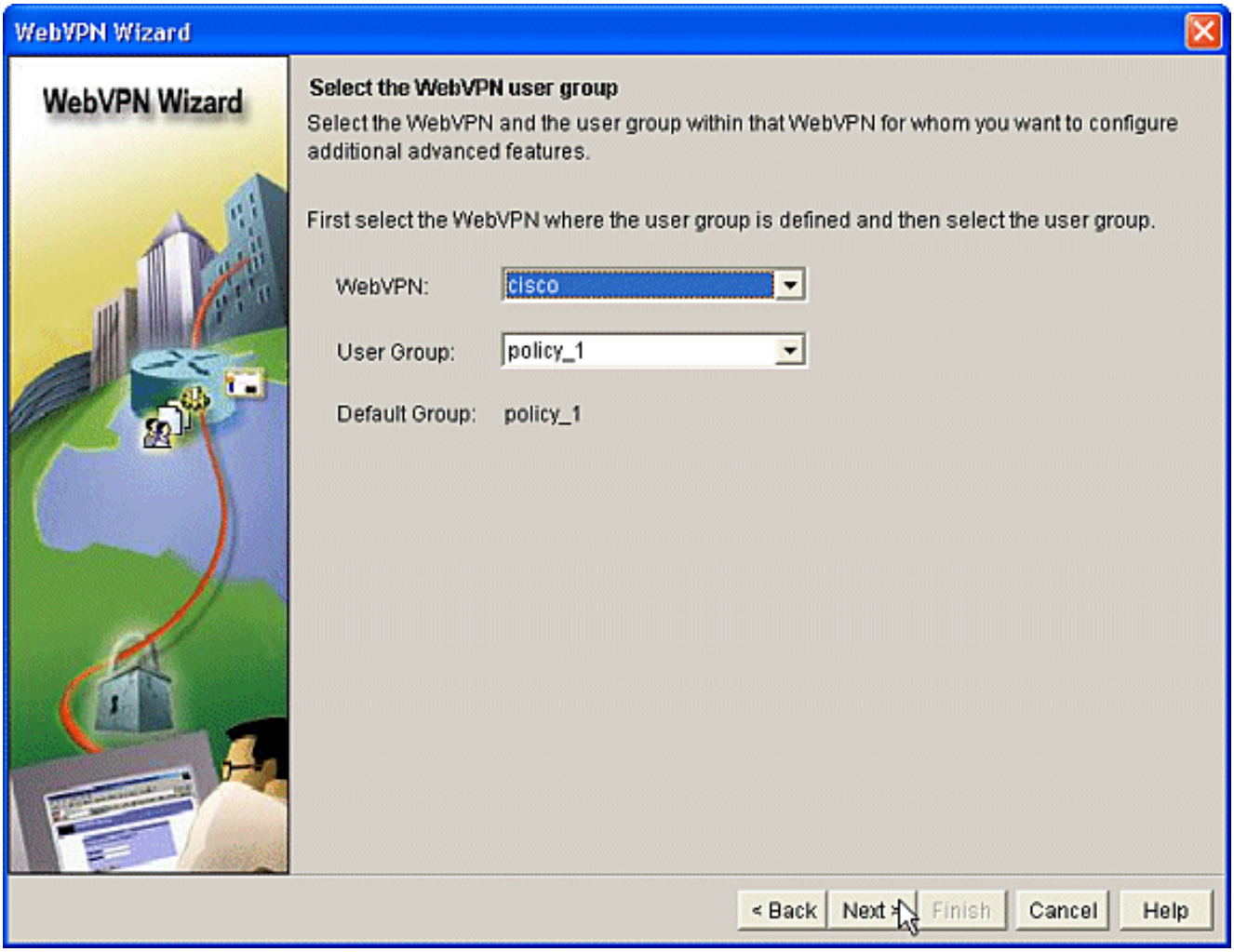
1. WebVPN Wizard の拡張機能を使用して、新しく作成したコンテキストで CSD をイネーブルにします。CSD のパッケージをまだインストールしていない場合は、この Wizard からインストールできます。SDM で Configuration タブをクリックします。ナビゲーションペインで、**[VPN] > [WebVPN]をクリックします。**[Create WebVPN] **タブをクリックします。** Configure advance features for an existing WebVPN オプション ボタンをチェックします。**[Launch the selected task]**ボタンをクリックします。



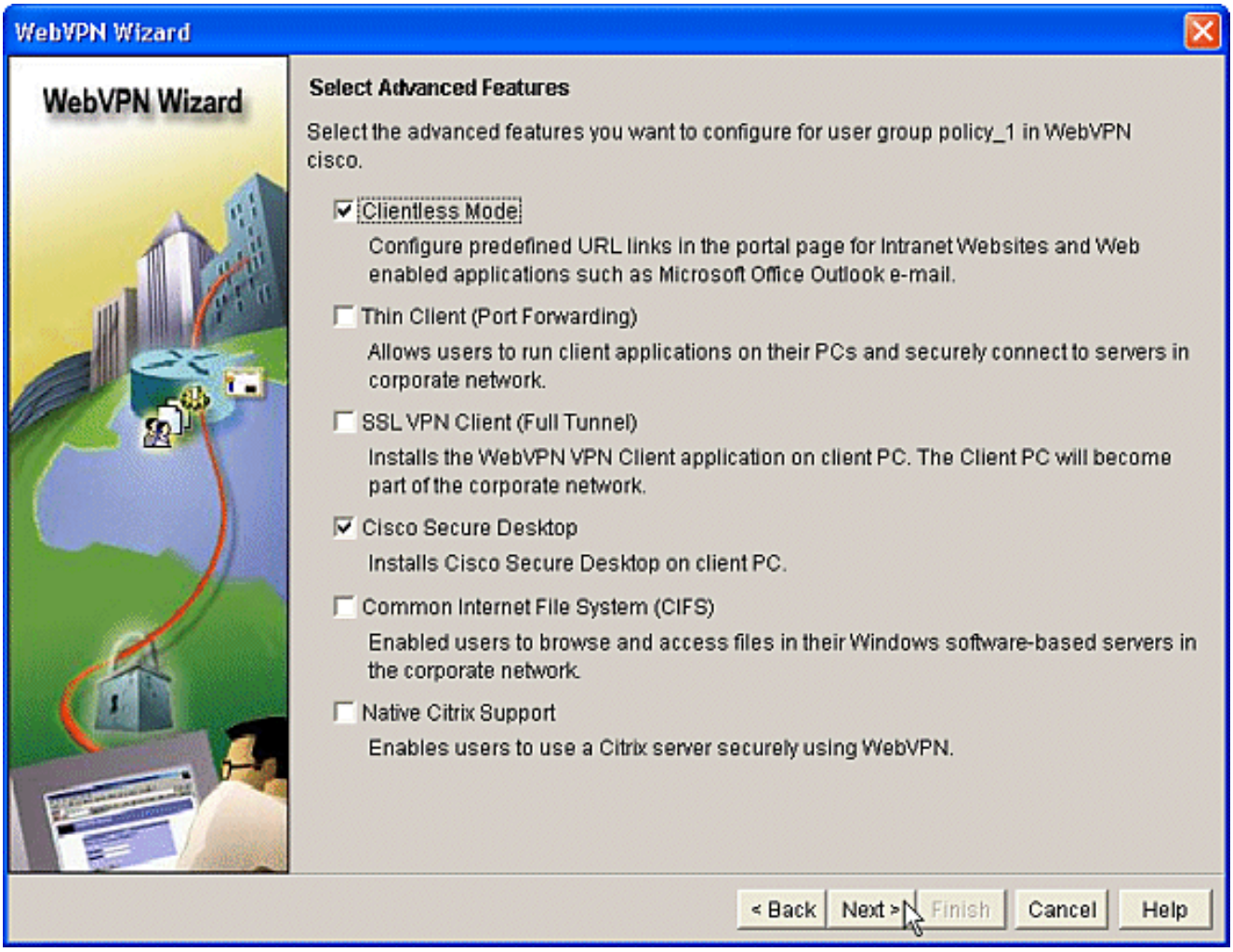
2. Advanced WebVPN Wizard の最初のページが表示されます。[next] をクリックします。



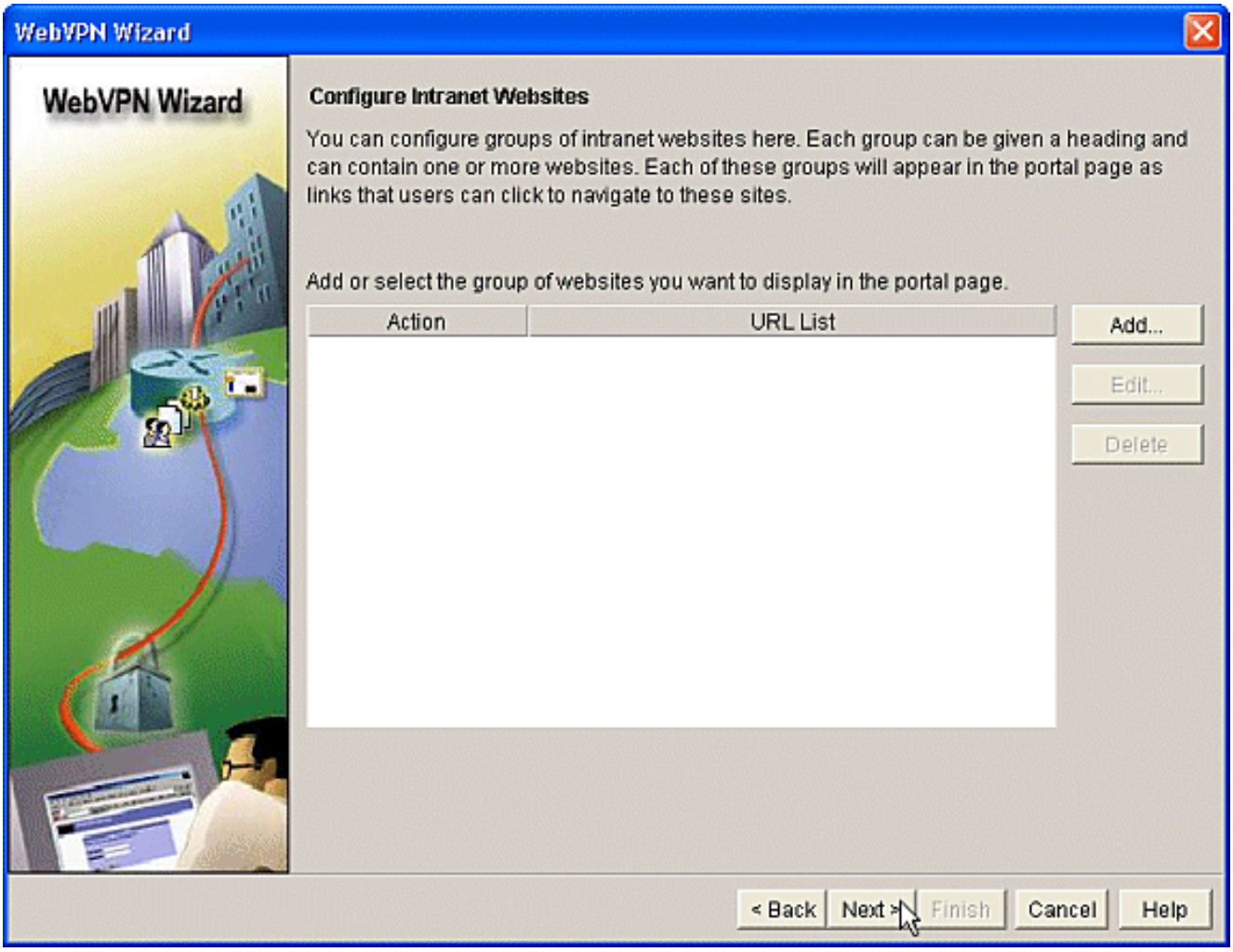
3. WebVPN とユーザ グループをフィールドのドロップダウン ボックスから選択します。選択した対象に Advanced WebVPN Wizard の機能が適用されます。[next] をクリックします。



4. Select Advanced Features 画面では、リスト表示されたテクノロジーから必要なものを選択できます。Cisco Secure Desktop をチェックします。この例では、Clientless Mode を選択しています。表示されている他のテクノロジーを選択すると、別のウィンドウが開いて、関連する情報を入力できるようになります。[Next] **ボタンをクリックします。**

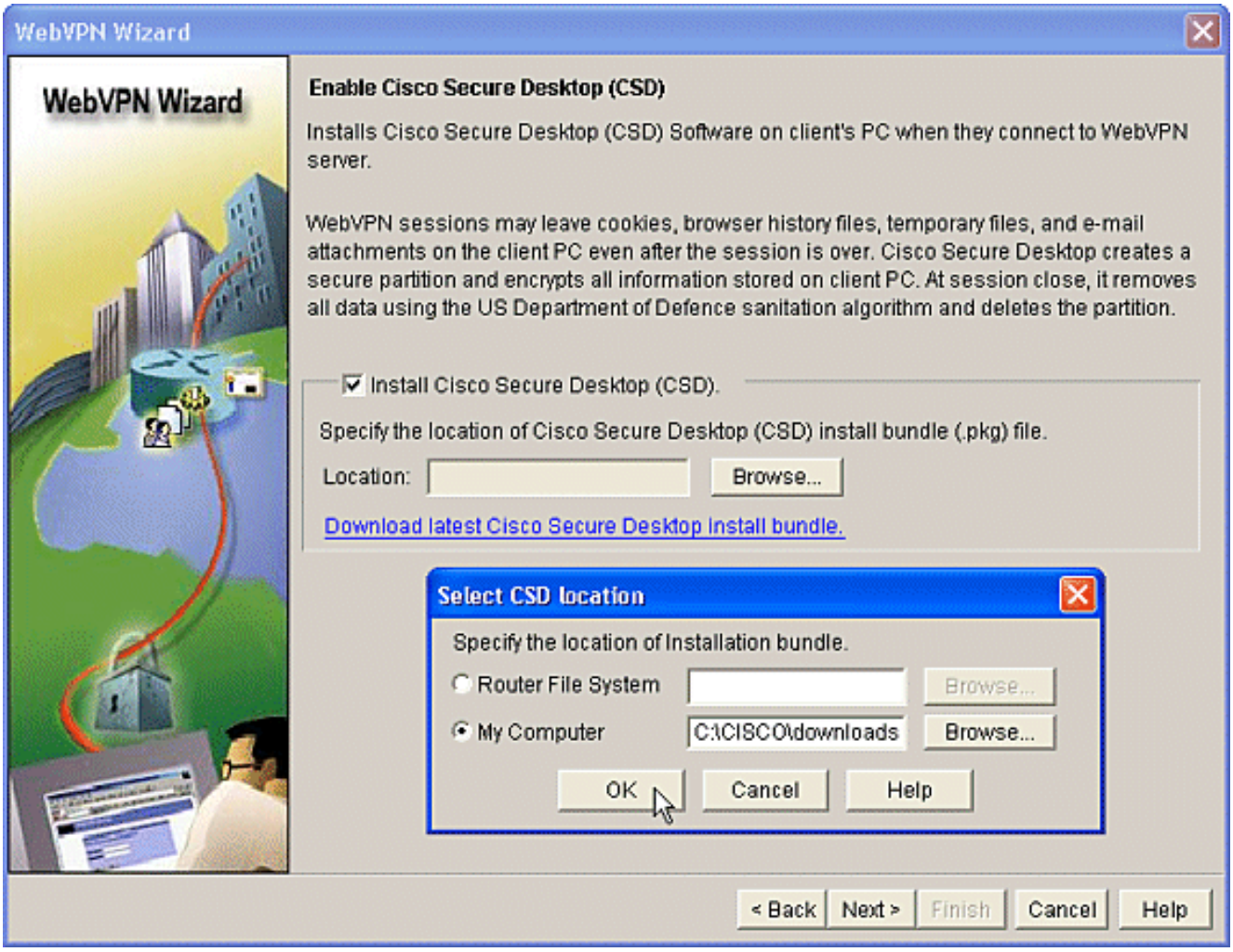


5. Configure Intranet Websites の画面では、ユーザがアクセスできる Web サイト リソースを設定できます。Outlook Web Access（OWA）などの社内の Web サイトを追加できます。



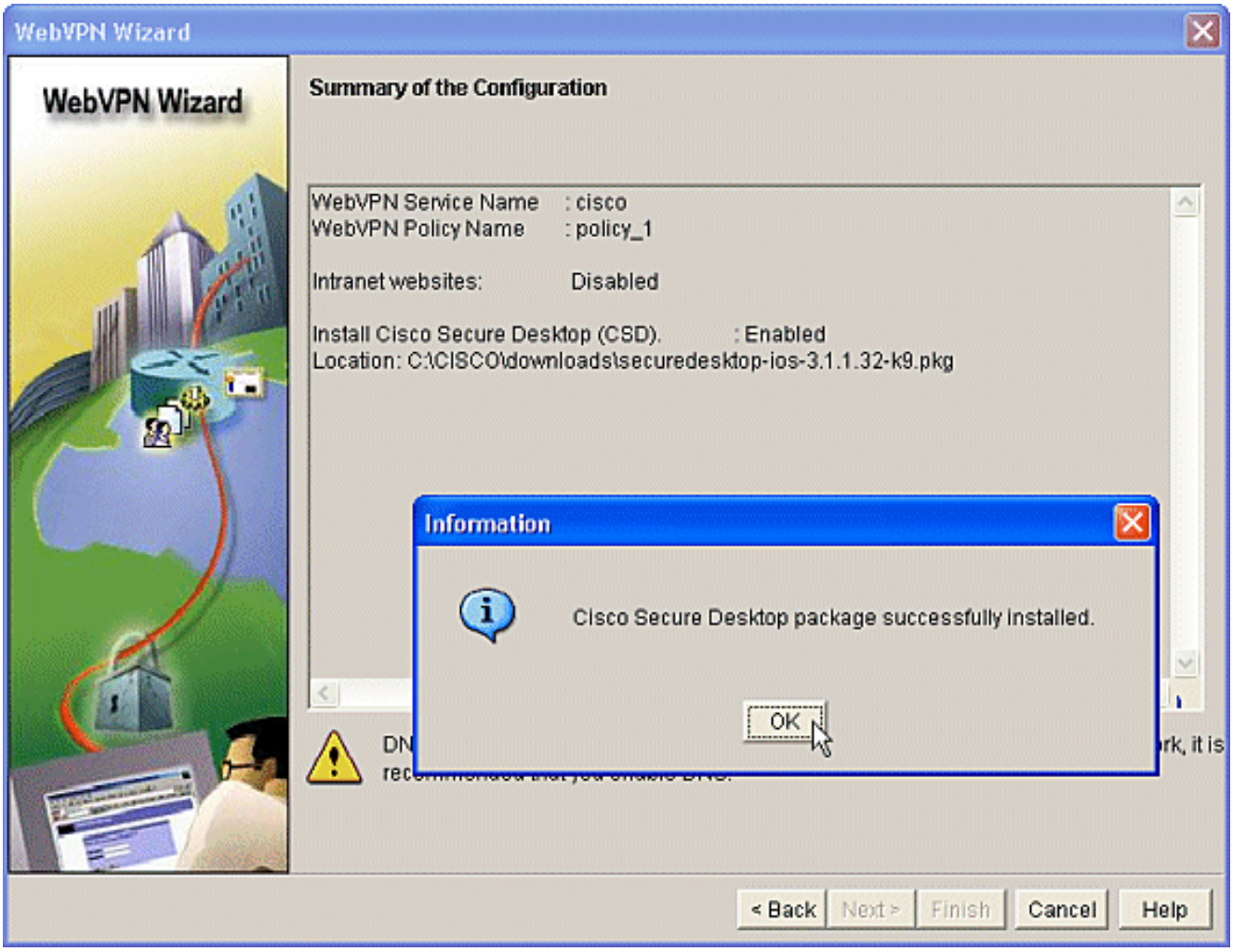
6. Enable Cisco Secure Desktop (CSD) 画面では、このコンテキストで CSD をイネーブルにできます。Install Cisco Secure Desktop (CSD) の隣のボックスをチェックして、Browse をクリックします。

7. Select CSD Location の領域で、My Computer をチェックします。Browse ボタンをクリックします。管理ワークステーションにある CSD IOS パッケージ ファイルを選択します。OK ボタンをクリックします。[Next] **ボタンをクリックします。**



8. Summary of the Configuration 画面が表示されます。Finish ボタンをクリックします。

9. CSD パッケージ ファイルが正しくインストールされたことを確認したら、OK をクリックします。



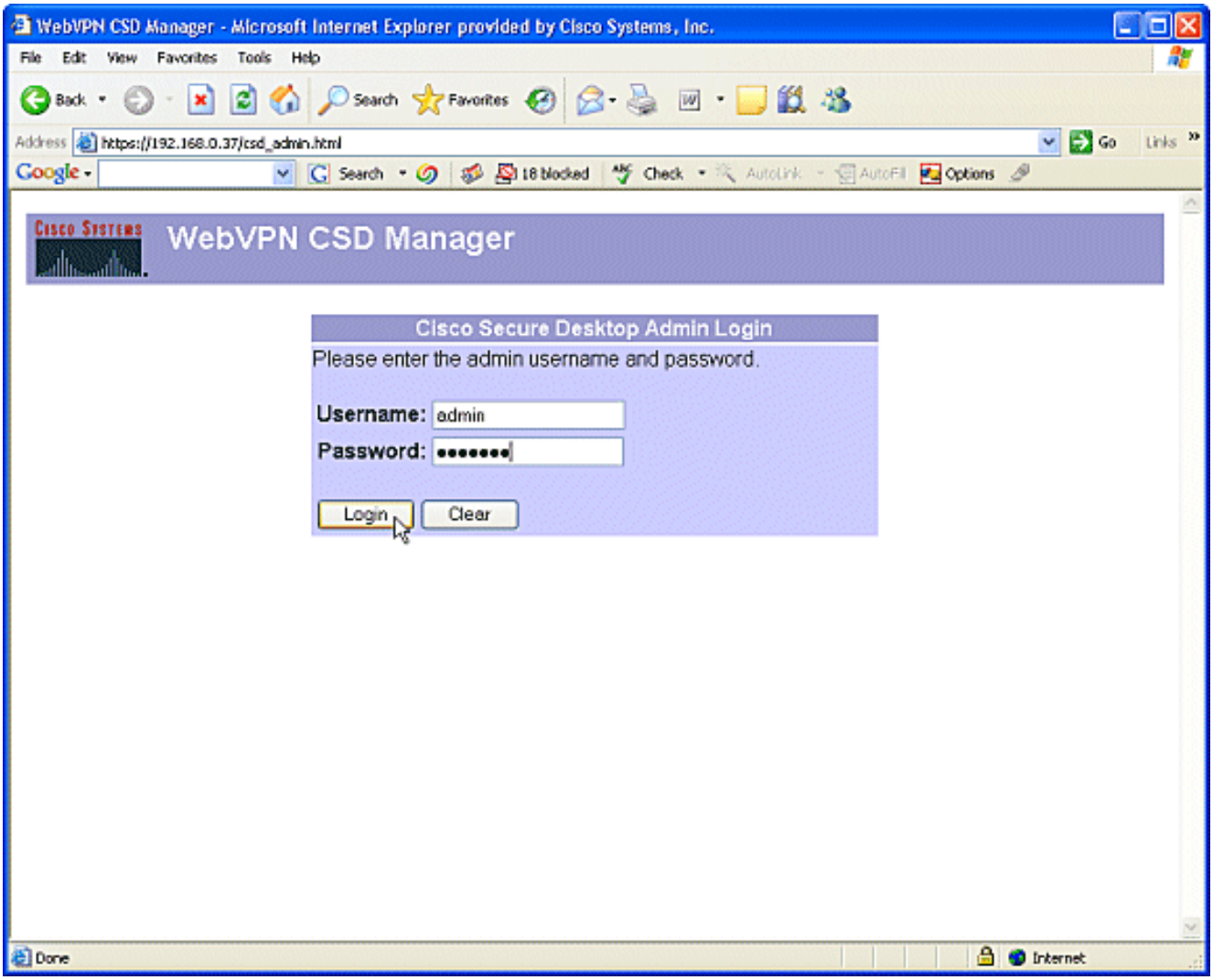
フェーズ 2：Web ブラウザを使用して CSD を設定する。

これらのステップは、使用している Web ブラウザで CSD を設定するために実行します。

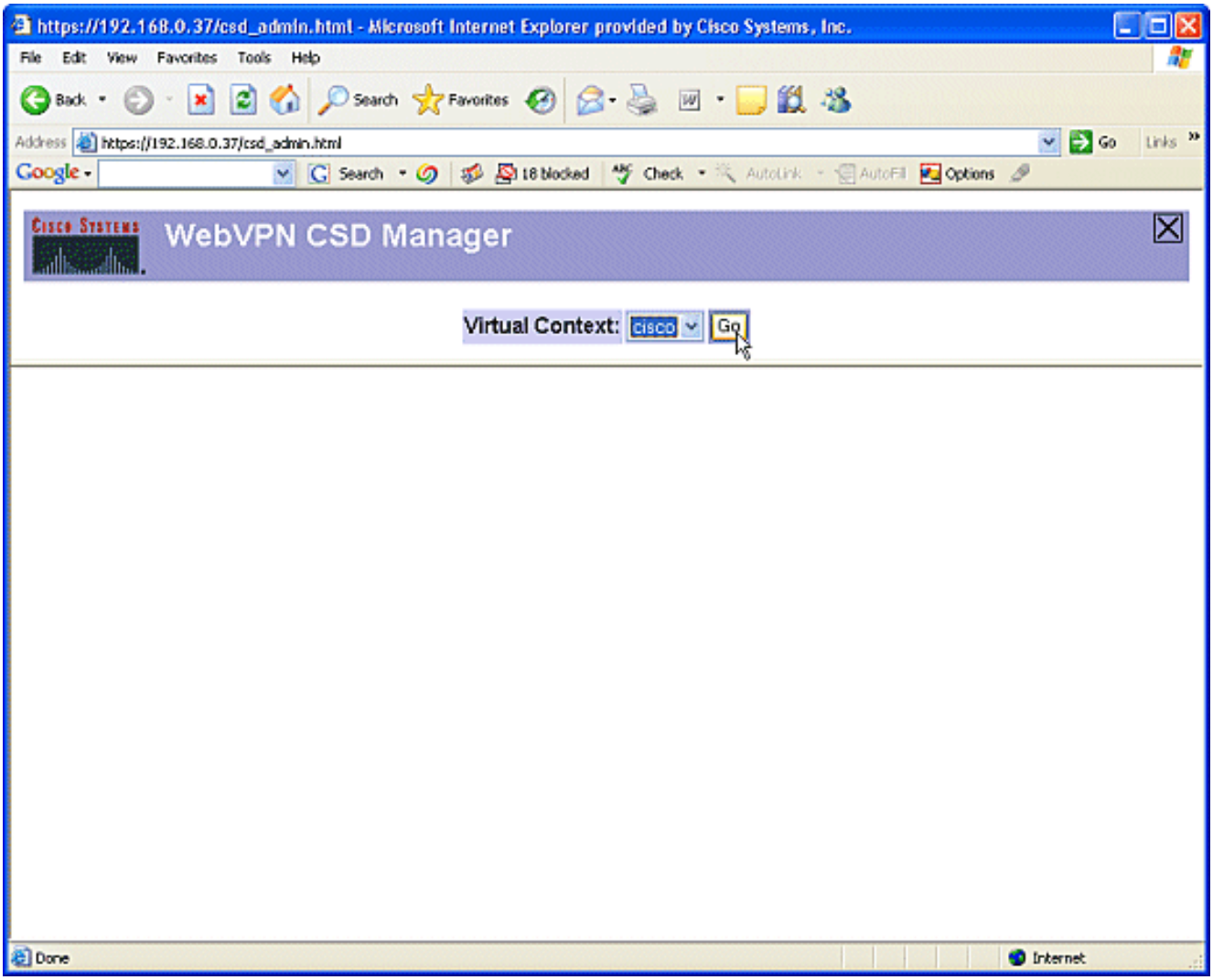
フェーズ 2：ステップ 1：Windows のロケーションを定義する。

Windows のロケーションを定義します。

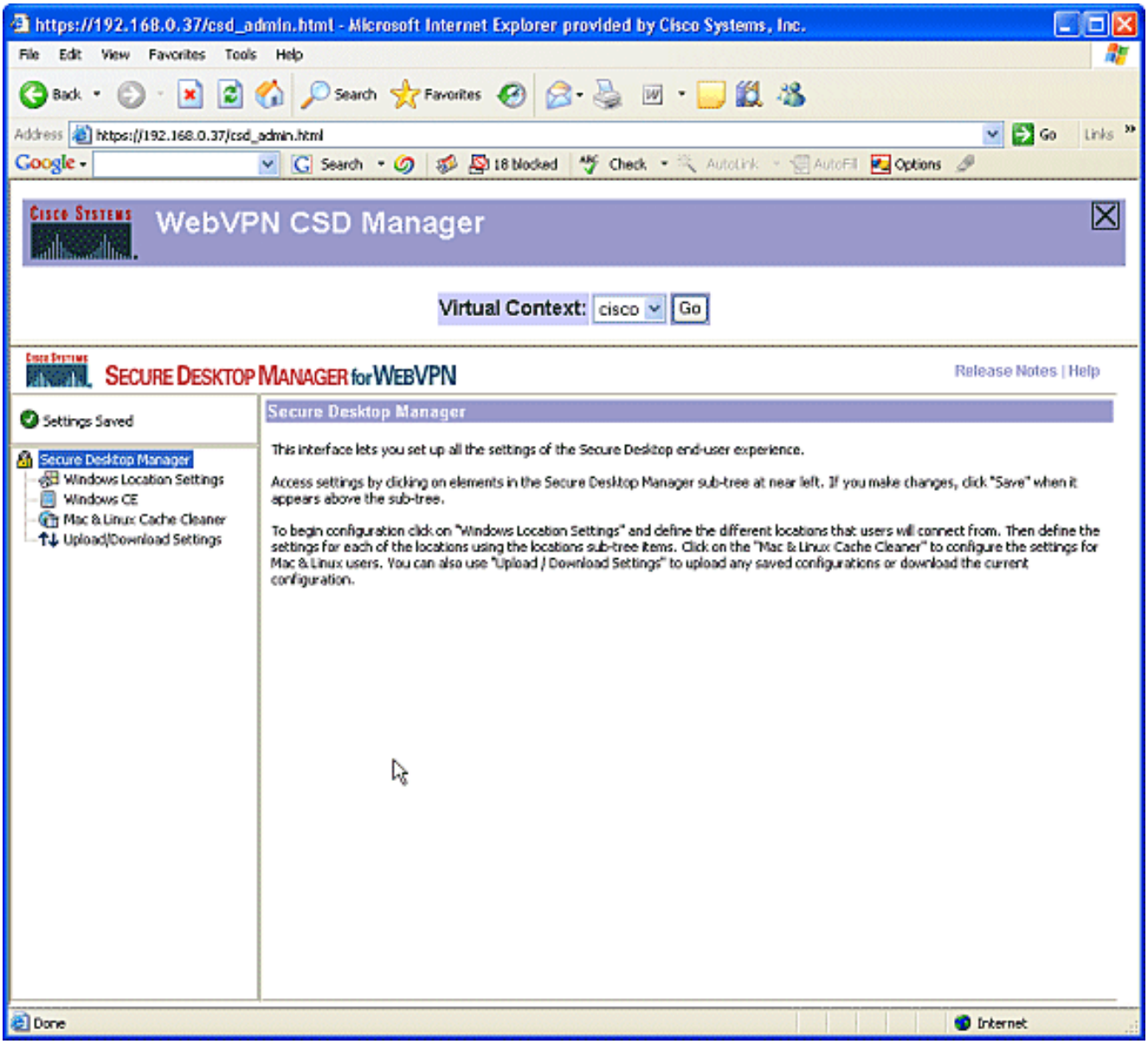
1. Web ブラウザで https://WebVPNgateway_IP Address/csd_admin.html を開きます。たとえば、https:/192.168.0.37/csd_admin.html になります。
2. ユーザ名として admin と入力します。パスワードを入力します。これはルータのイネーブル シークレット パスワードです。[Login] をクリックする。



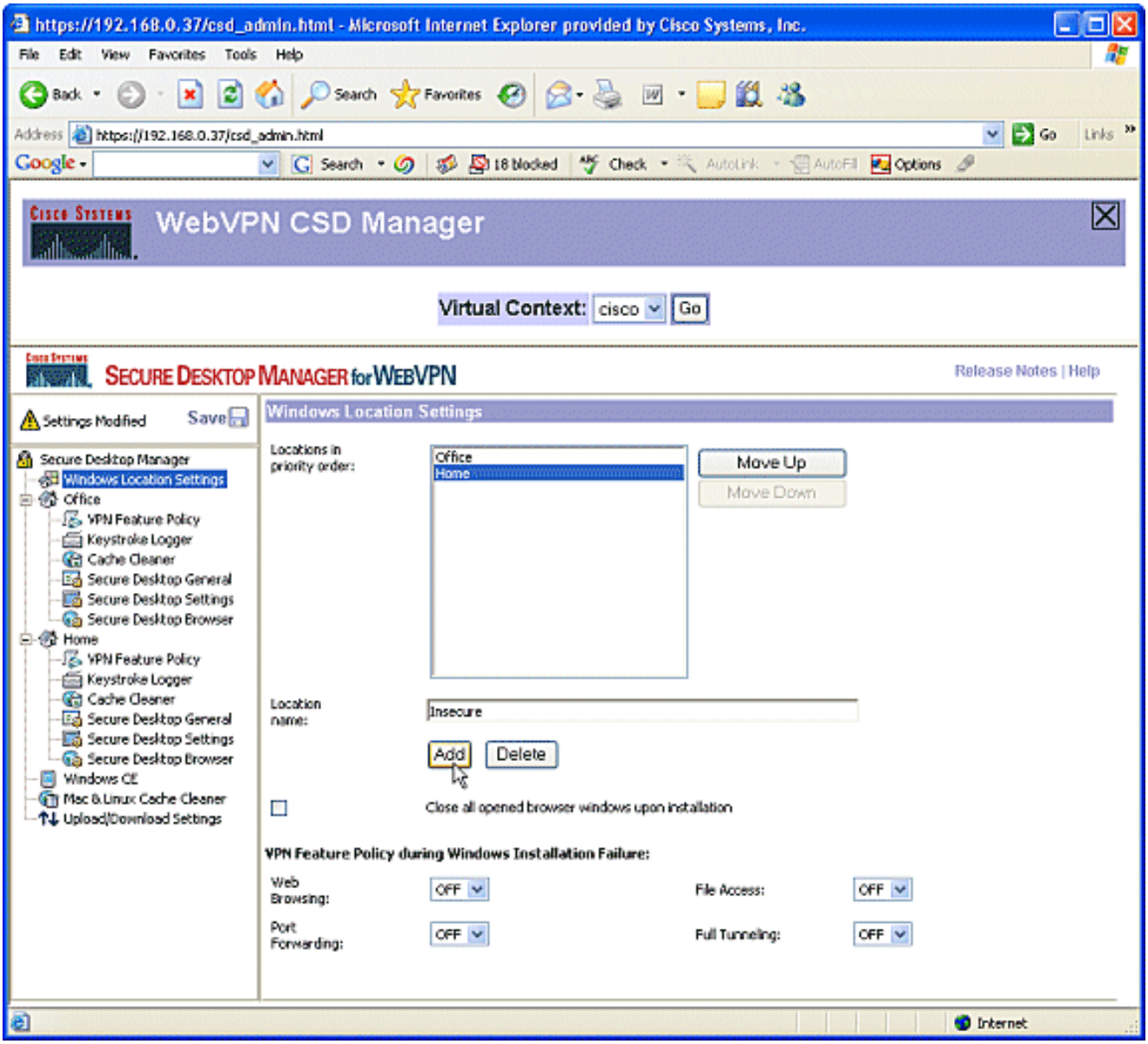
3. ルータから提示された証明書を受け入れ、ドロップダウン ボックスからコンテキストを選択して、Go をクリックします。



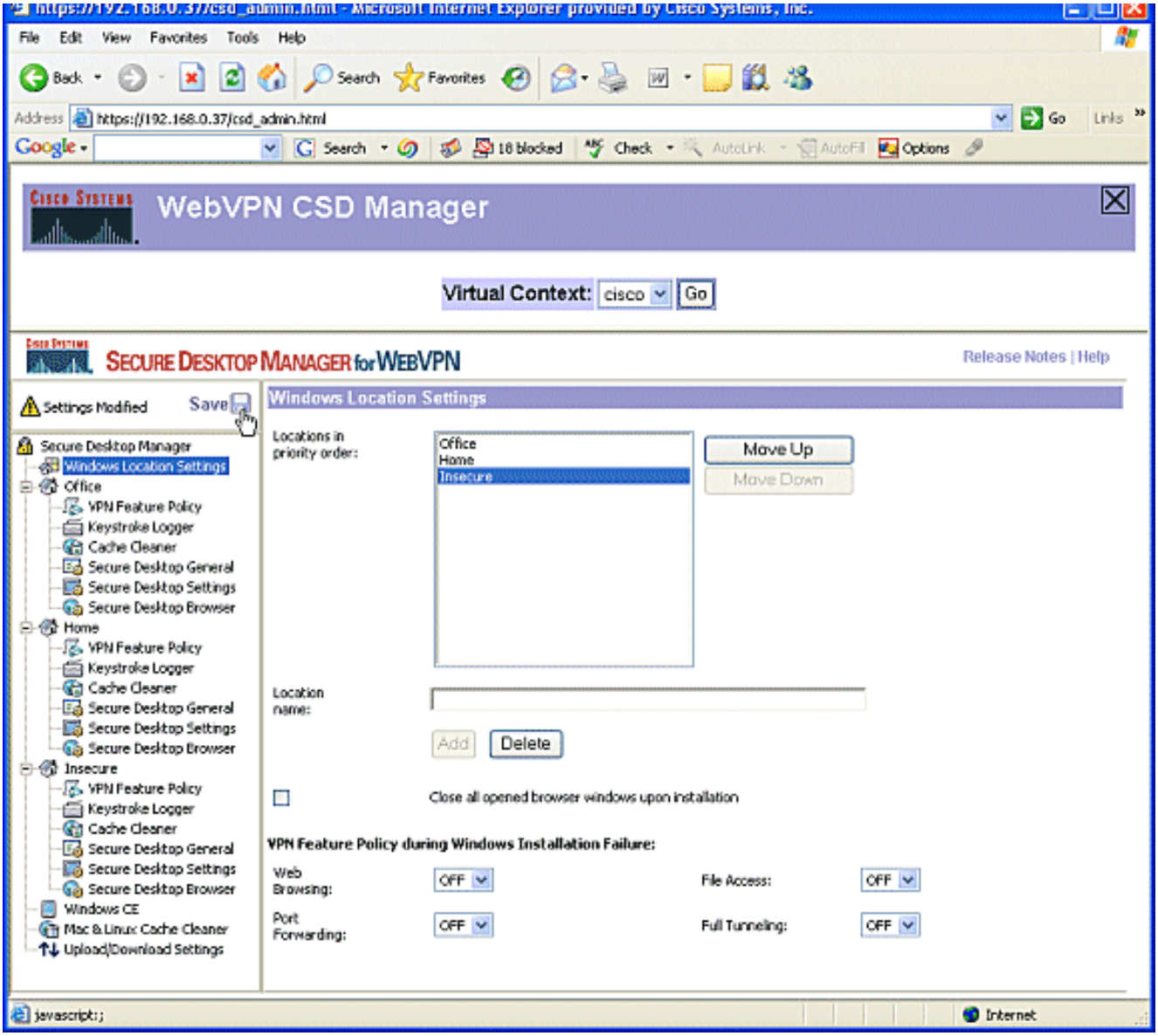
4. Secure Desktop Manager for WebVPN 画面が表示されます。



5. 左側のペインから Windows Location Settings を選択します。Location name の隣にあるボックスにカーソルを置き、ロケーション名を入力します。[Add] をクリックします。この例では、3つのロケーション名を示します。オフィス、自宅、および安全でない。新しいロケーションを追加するたびに、左側のペインが拡がって、そのロケーションの設定可能なパラメータが表示されます。



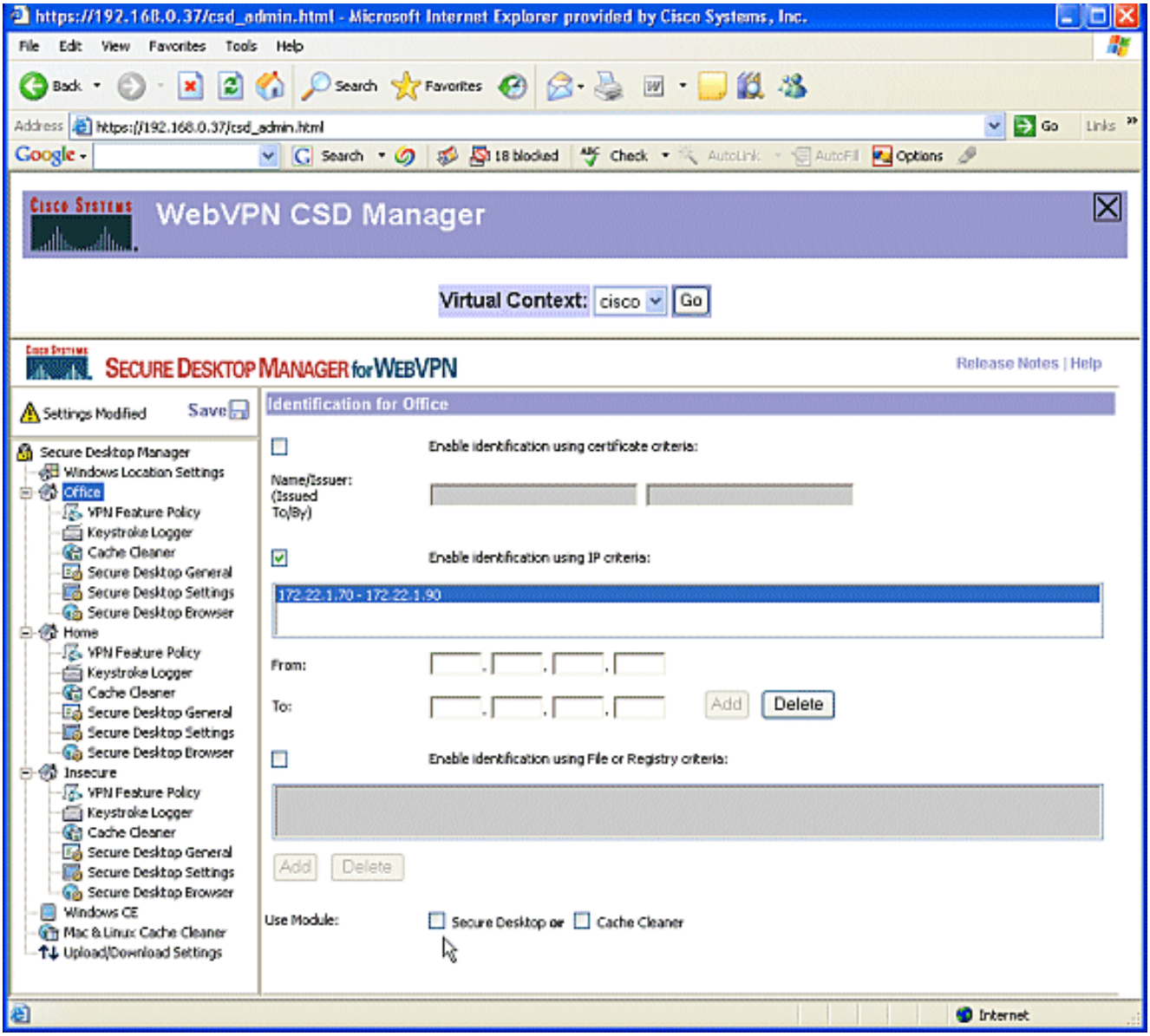
6. Windows ロケーションを作成したら、左側のペインの最上部にある Save をクリックします。**注：** Web ブラウザから接続解除されると設定が失われるため、設定は頻繁に保存するようにします。



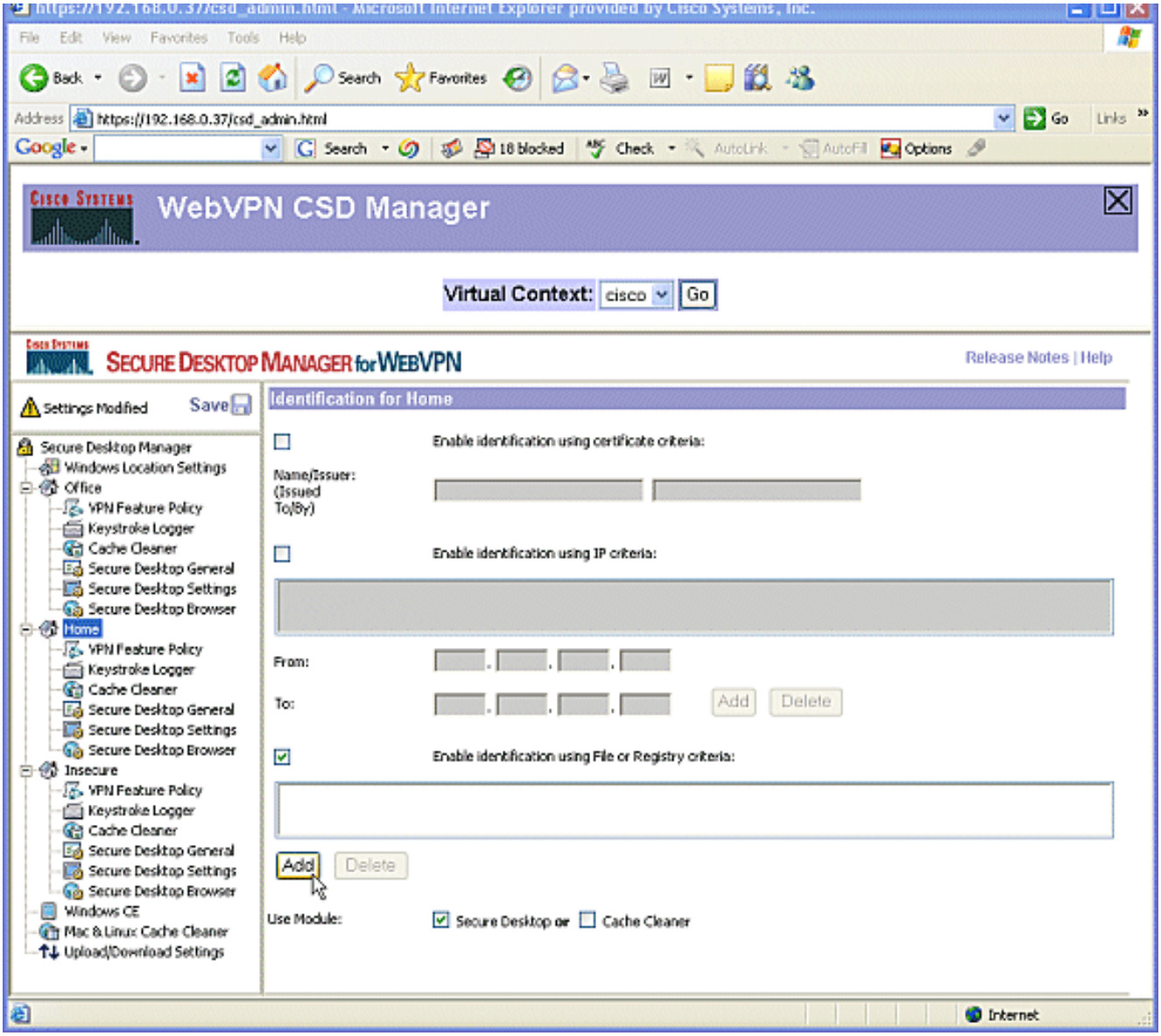
フェーズ 2：ステップ 2：ロケーションの基準を識別する。

Windows のロケーションを互いに区別するには、各ロケーションに特有の基準を割り当てます。これにより、CSD は、特定の Windows ロケーションにどの機能を割り当てるかが判断できます。

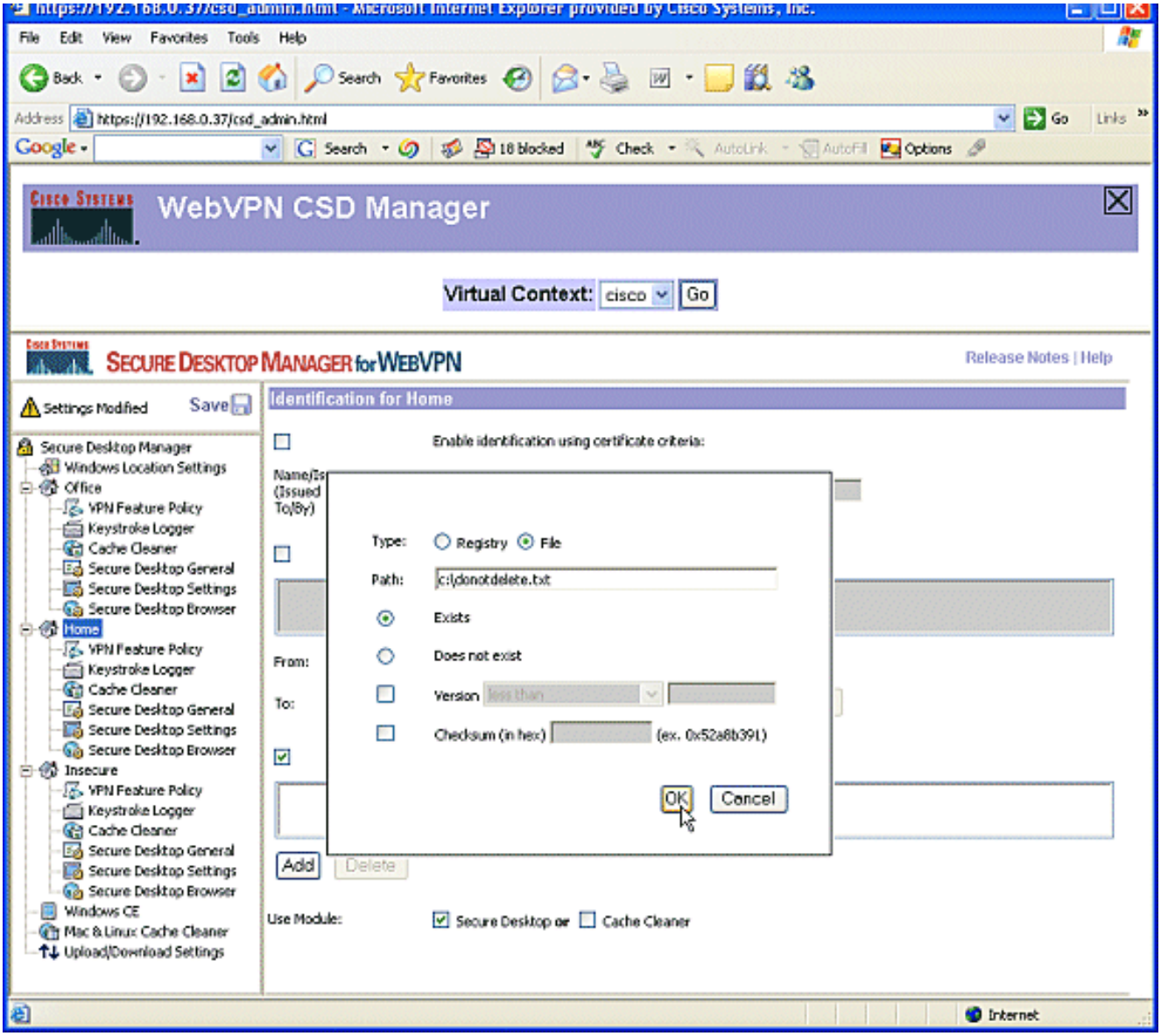
1. 左側のペインで Office をクリックします。Windows ロケーションは、証明書の基準、IP の基準、ファイル、レジストリの基準で識別できます。また、これらのクライアントに対して Secure Desktop や Cache Cleaner を選択することもできます。これらのユーザは社内のオフィスワーカーであるため、IP の基準で識別します。From ボックスと To ボックスに IP アドレスの範囲を入力します。[Add] をクリックします。[Use Module:Secure Desktop.応答が表示されたら、Save をクリックし、続いて OK をクリックします。



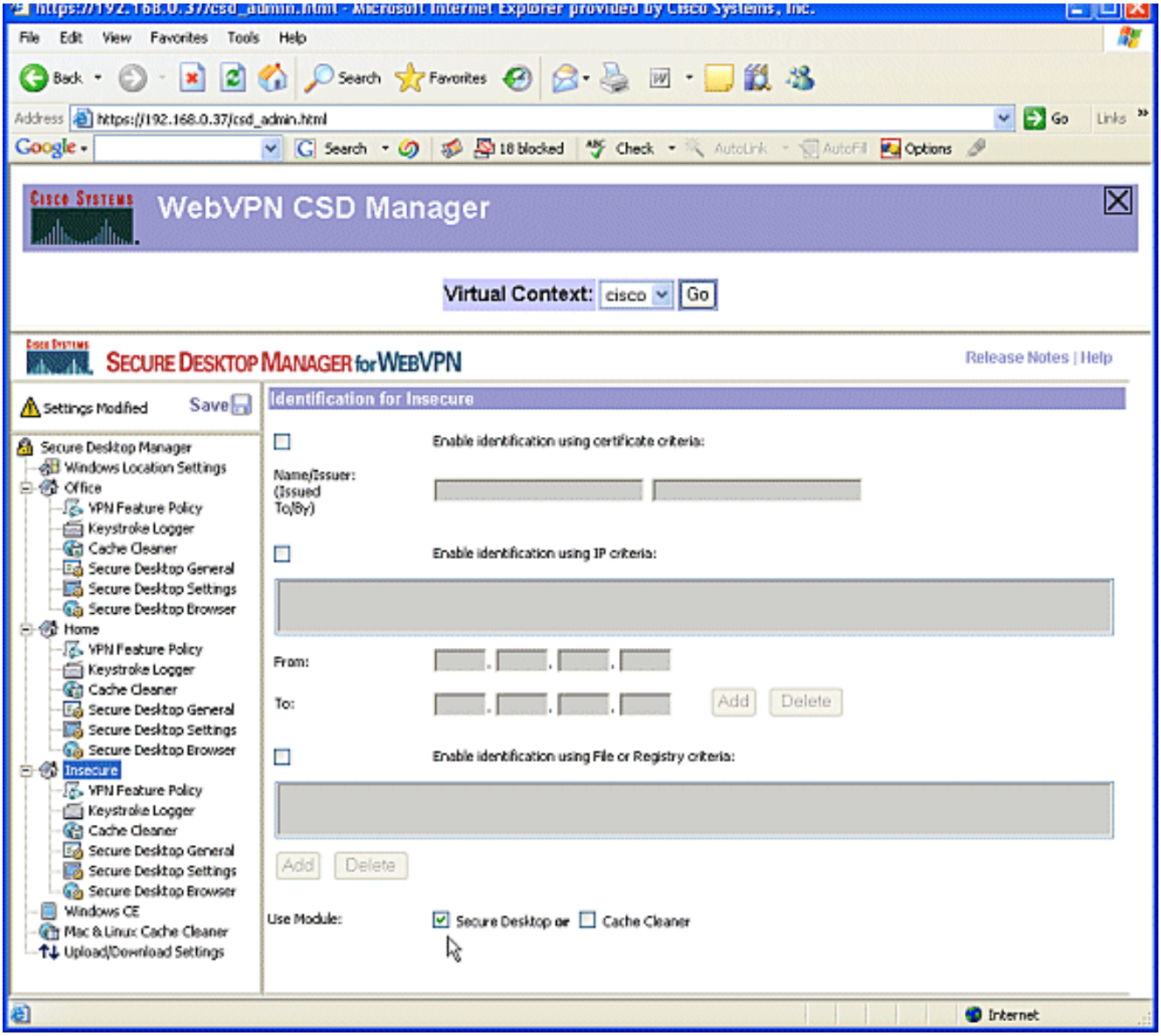
2. 左側のペインから 2 つ目の Windows ロケーション設定である Home をクリックします。使用モジュールを確認**してください：Secure Desktopがチェック**されています。これらのクライアントを識別するファイルが配布されます。これらのユーザに対して証明書やレジストリの基準を配布するように選択することもできます。Enable identification using File or Registry criteria をチェックします。[Add] をクリックします。



3. ダイアログ ボックスで、File を選択して、ファイルのパスを入力します。このファイルは、Home のクライアントすべてに配布する必要があります。Exists オプション ボタンをチェックします。応答が表示されたら、OK をクリックし、続いて Save をクリックします。



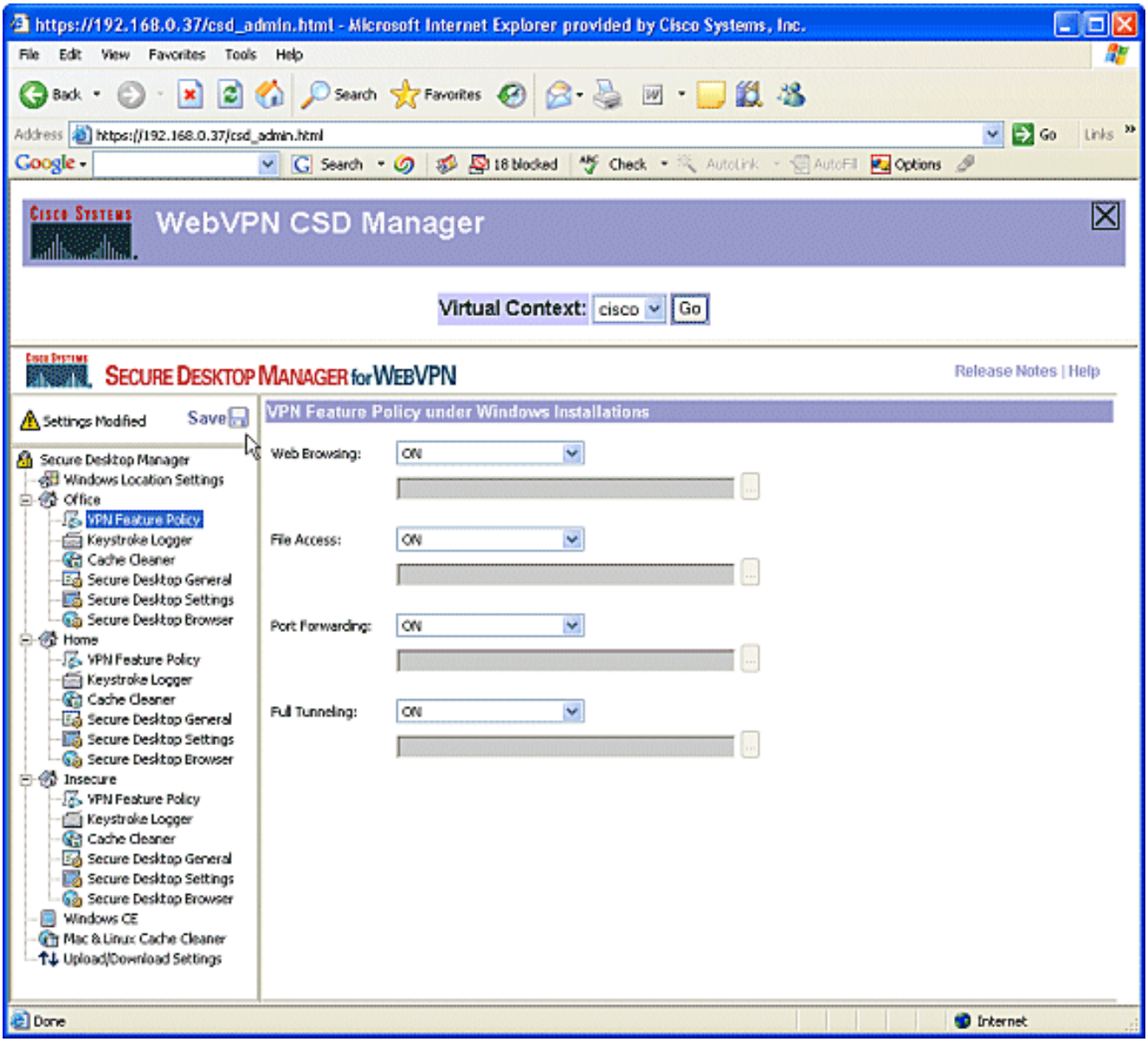
4. Insecure ロケーションの識別情報を設定するには、識別のための基準を何も割り当てないようにするだけです。左側のペインで Insecure をクリックします。すべての基準のチェックを外した状態にします。[**Use Module:Secure Desktop.**応答が表示されたら、Save をクリックし、続いて OK をクリックします。



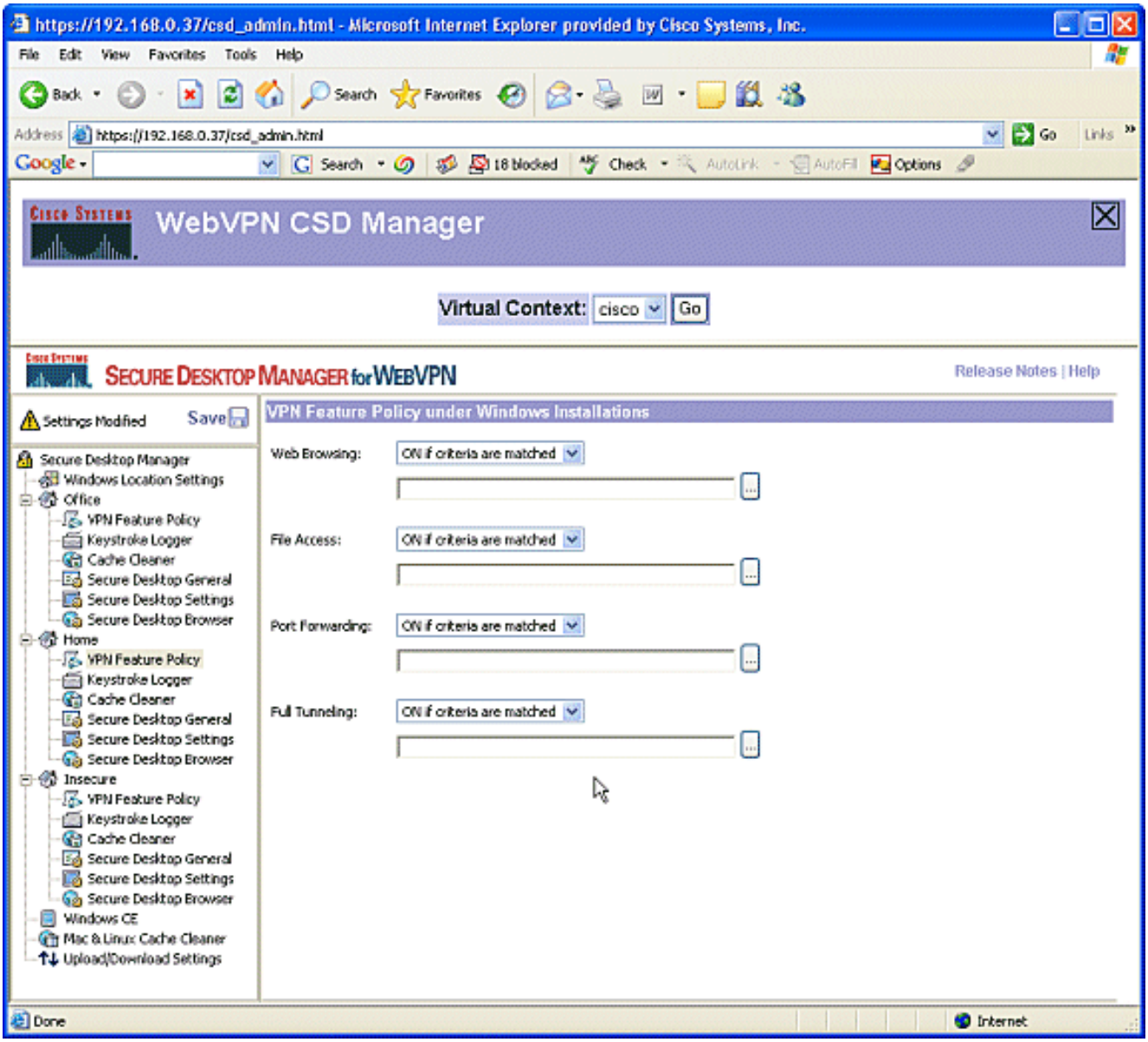
フェーズ 2：ステップ 3：Windows の口ケーションのモジュールと機能を設定する。

各 Windows 口ケーションに対して CSD 機能を設定します。

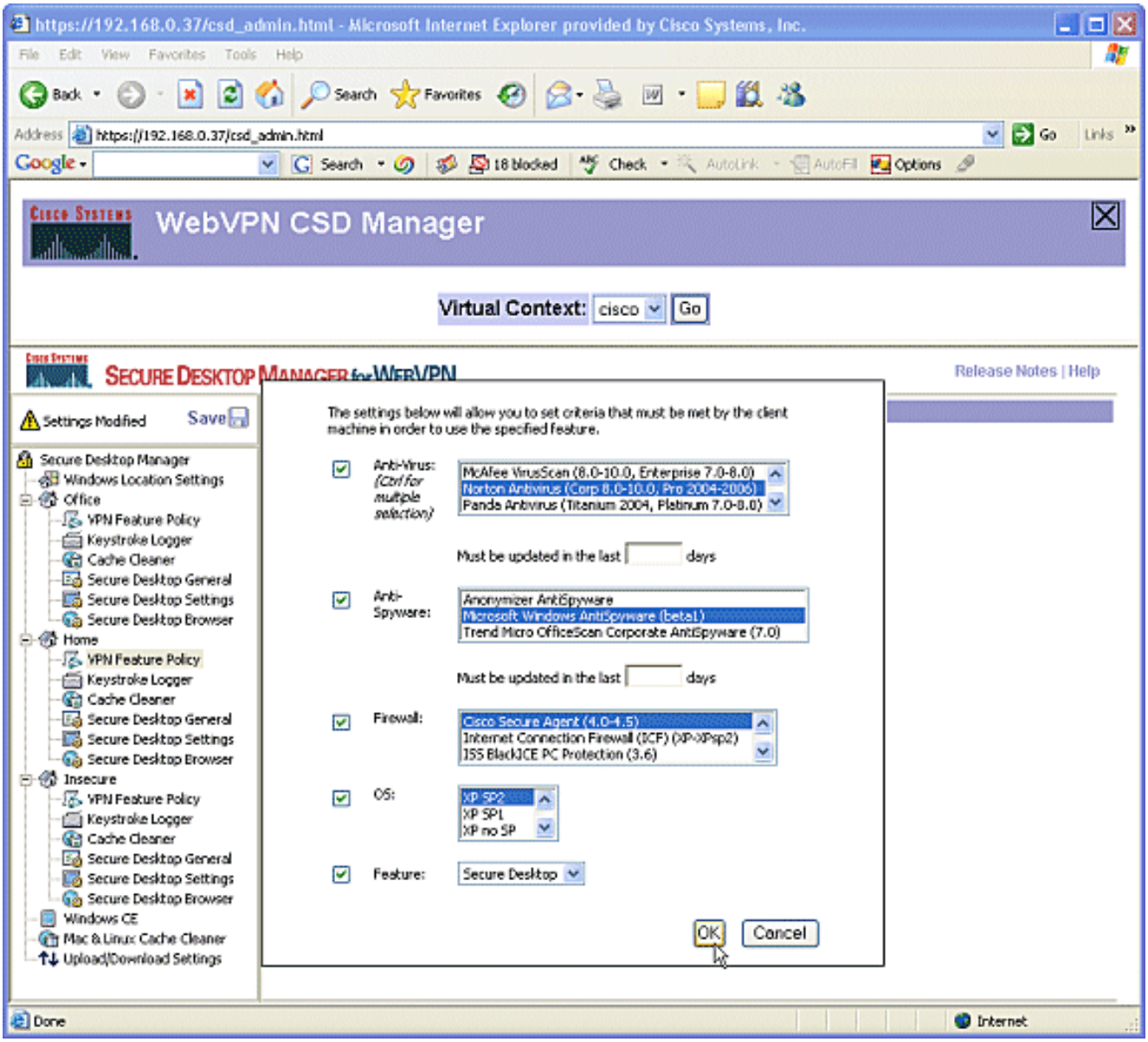
1. Office の下にある VPN Feature Policy をクリックします。これらは信頼されている社内クライアントであるため、CSD もキャッシュ クリーナもイネーブルになっていません。設定できる他のパラメータはありません。



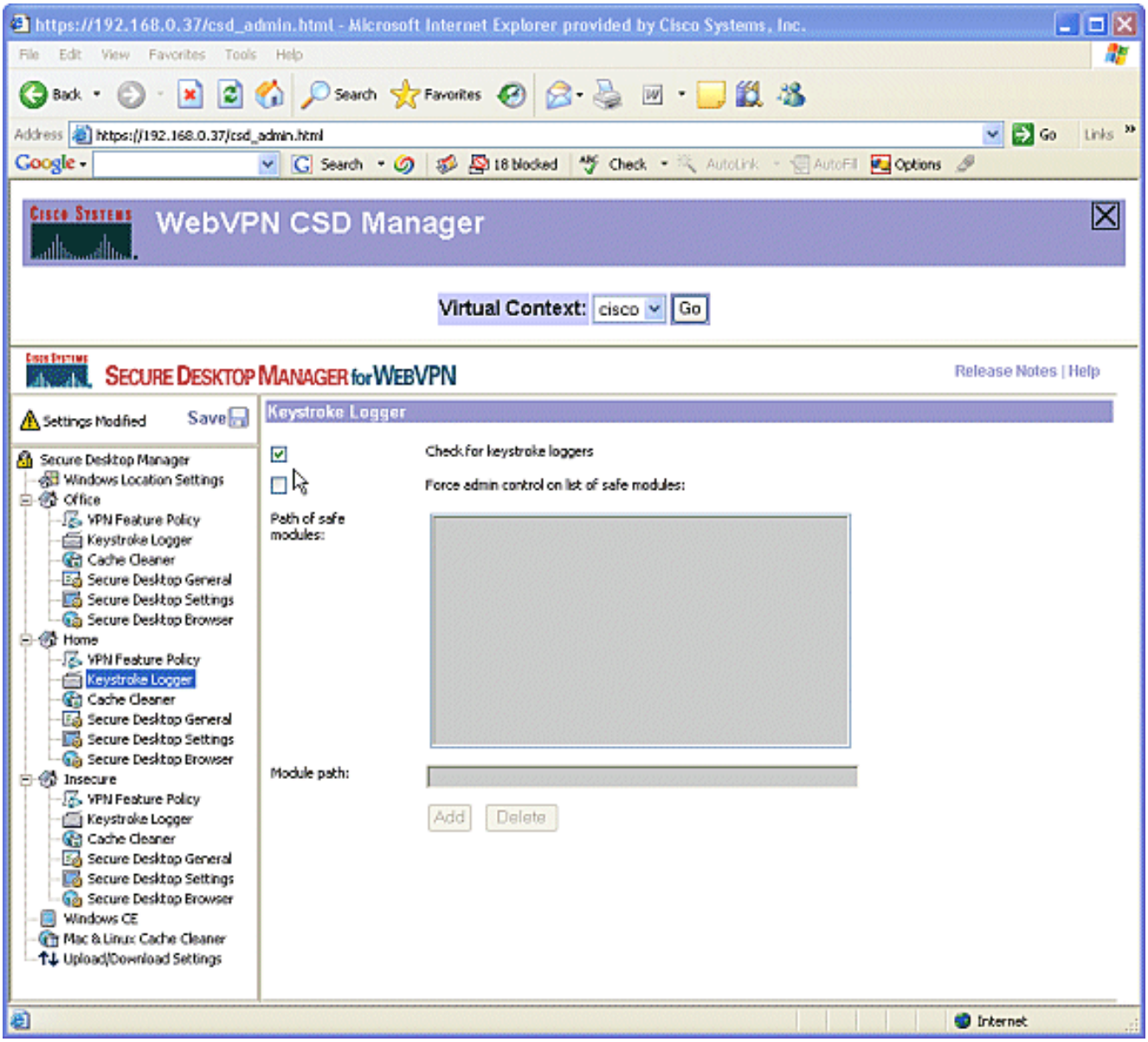
2. 次のように機能を有効にします。左側のペインで、Home の下の VPN Feature Policy を選択します。Home ユーザは、ある基準を満たせば会社の LAN へのアクセスが許可されます。各アクセス方式の下で、ON if criteria are matched を選択します。



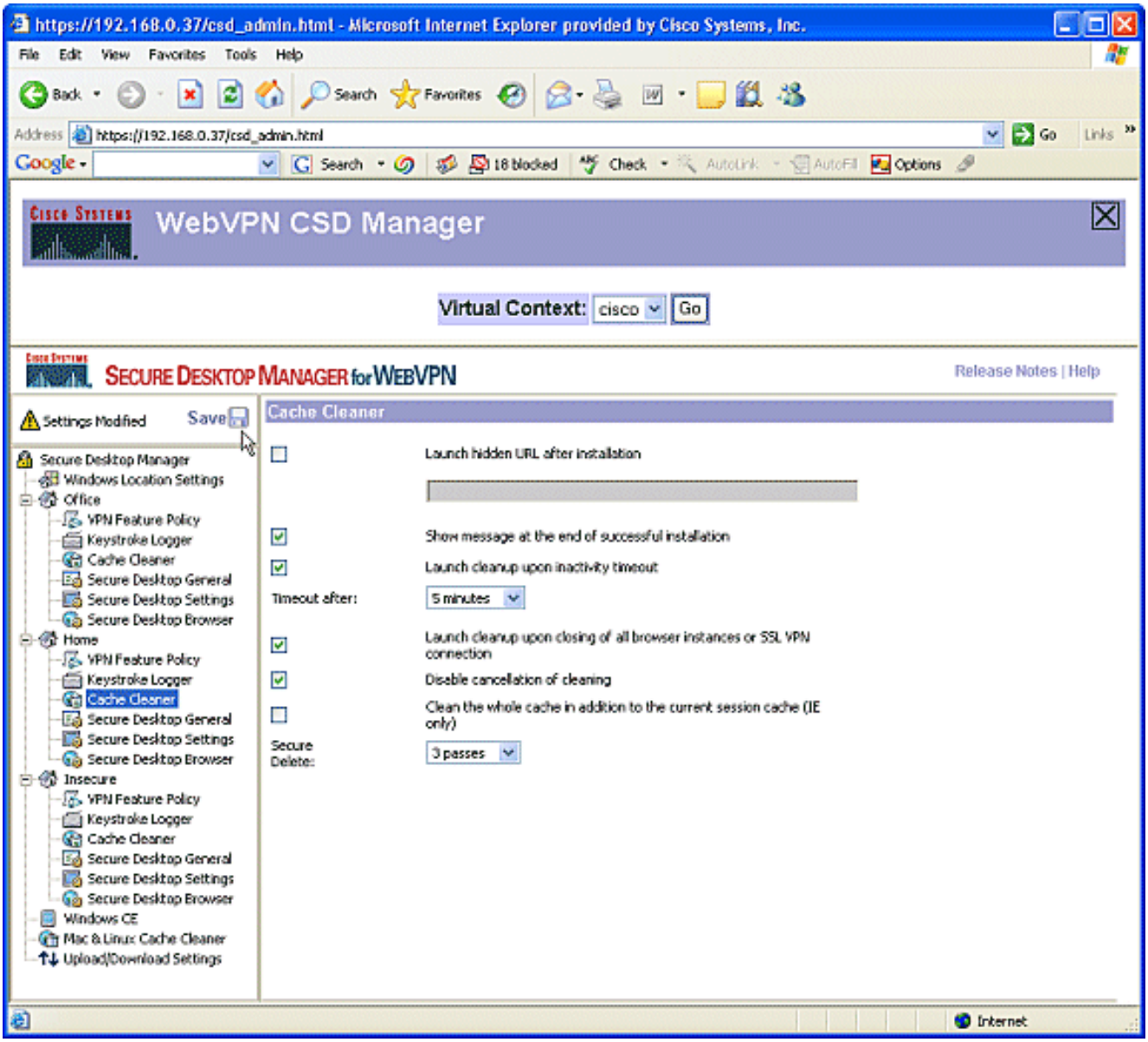
3. Web Browsing について、省略記号のボタンをクリックして、該当する基準を選択します。ダイアログボックスで [OK] をクリックします。



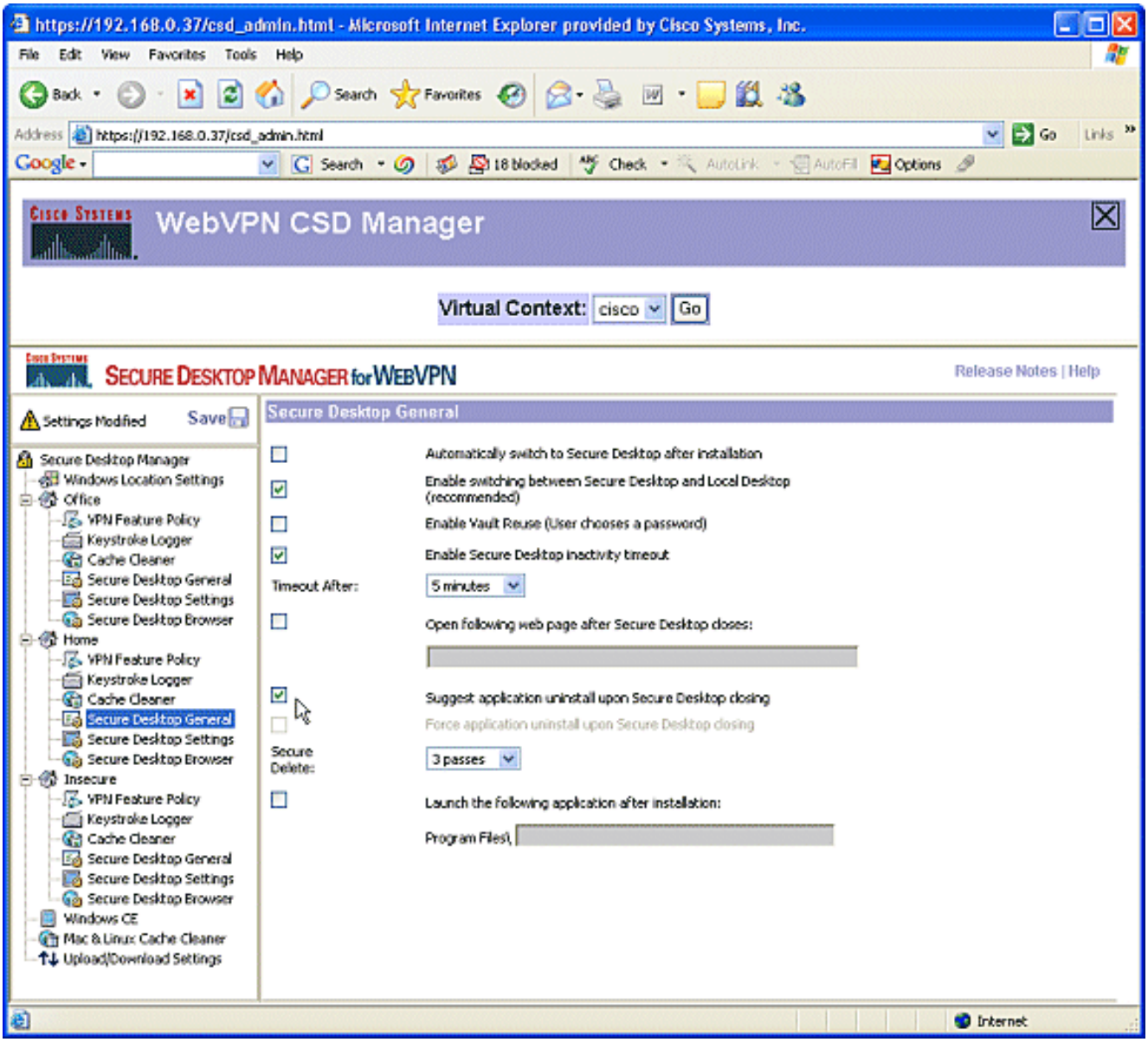
4. 同様の方法で、他のアクセス方法についても設定できます。Home の下で、Keystroke Logger を選択します。Check for keystroke loggers をチェックします。応答が表示されたら、Save をクリックし、続いて OK をクリックします。



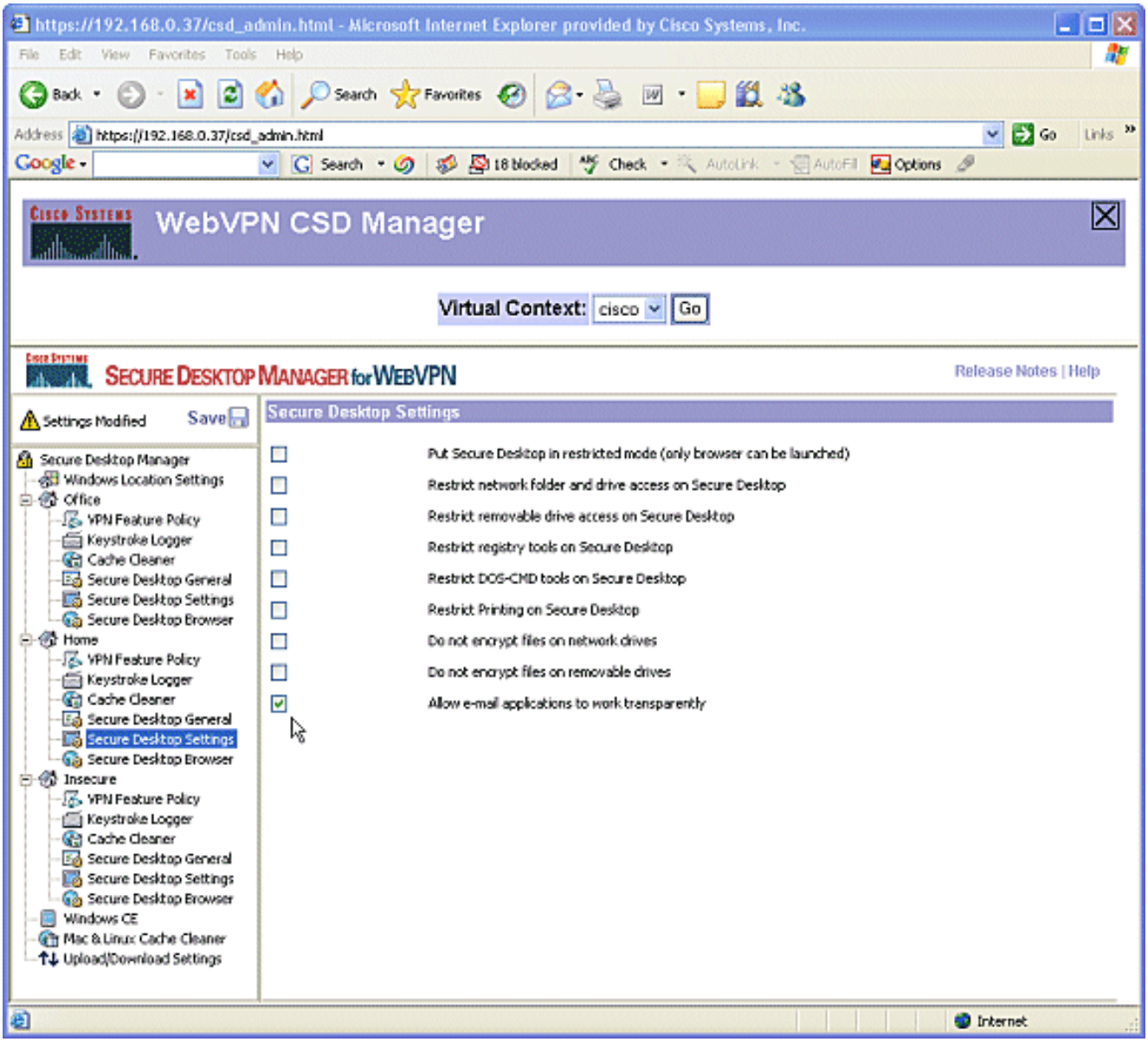
5. Windows ロケーション Home の下で、Cache Cleaner を選択します。このスクリーン ショットに表示されているように、デフォルトの設定のままにします。



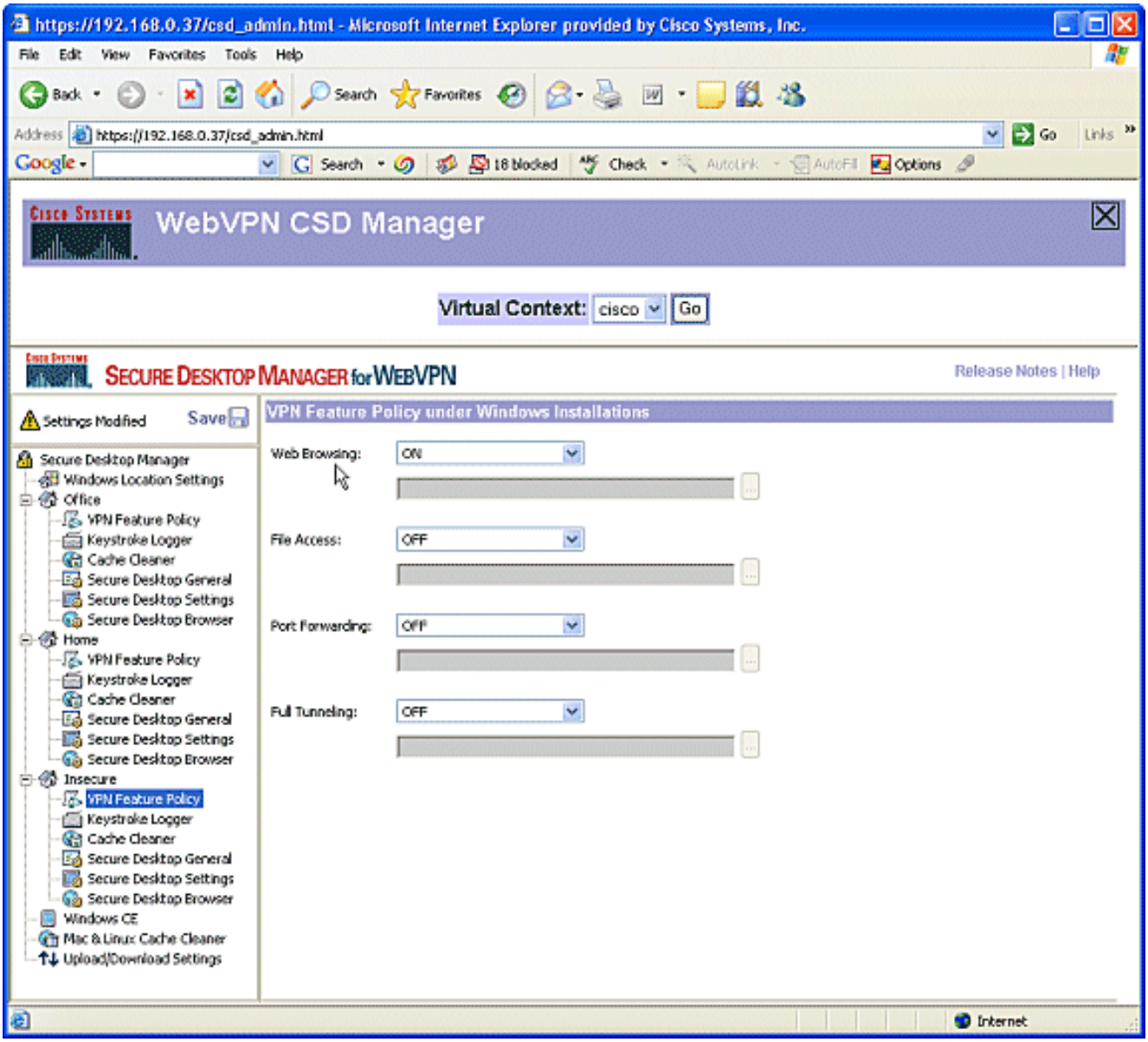
6. Home の下で、Secure Desktop General を選択します。Suggest application uninstall upon Secure Desktop closing をチェックします。このスクリーン ショットに表示されているように、他のパラメータはすべてデフォルトの設定のままにします。



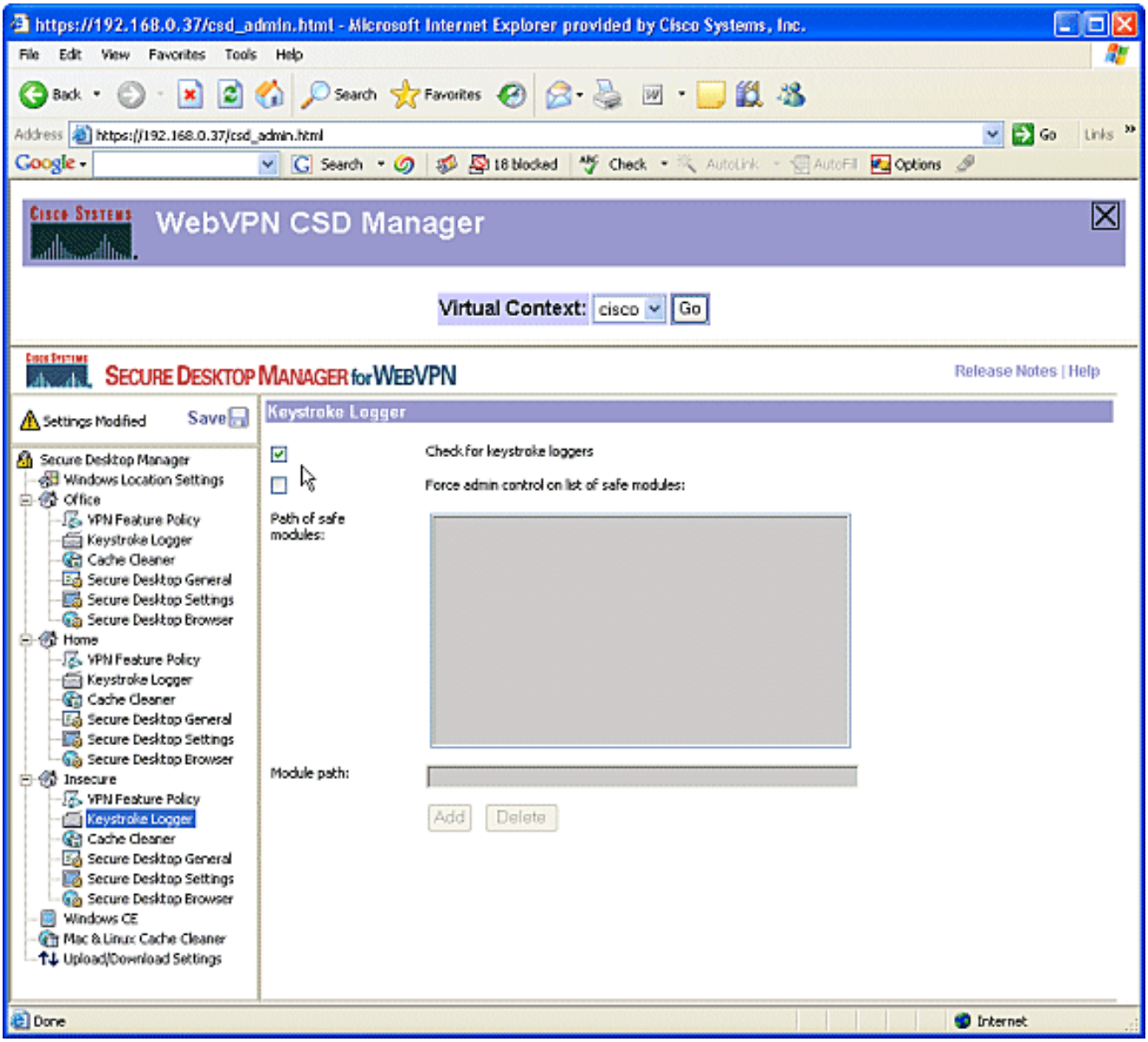
7. Home の Secure Desktop Settings について、Allow e-mail applications to work transparently を選択します。応答が表示されたら、Save をクリックし、続いて OK をクリックします。



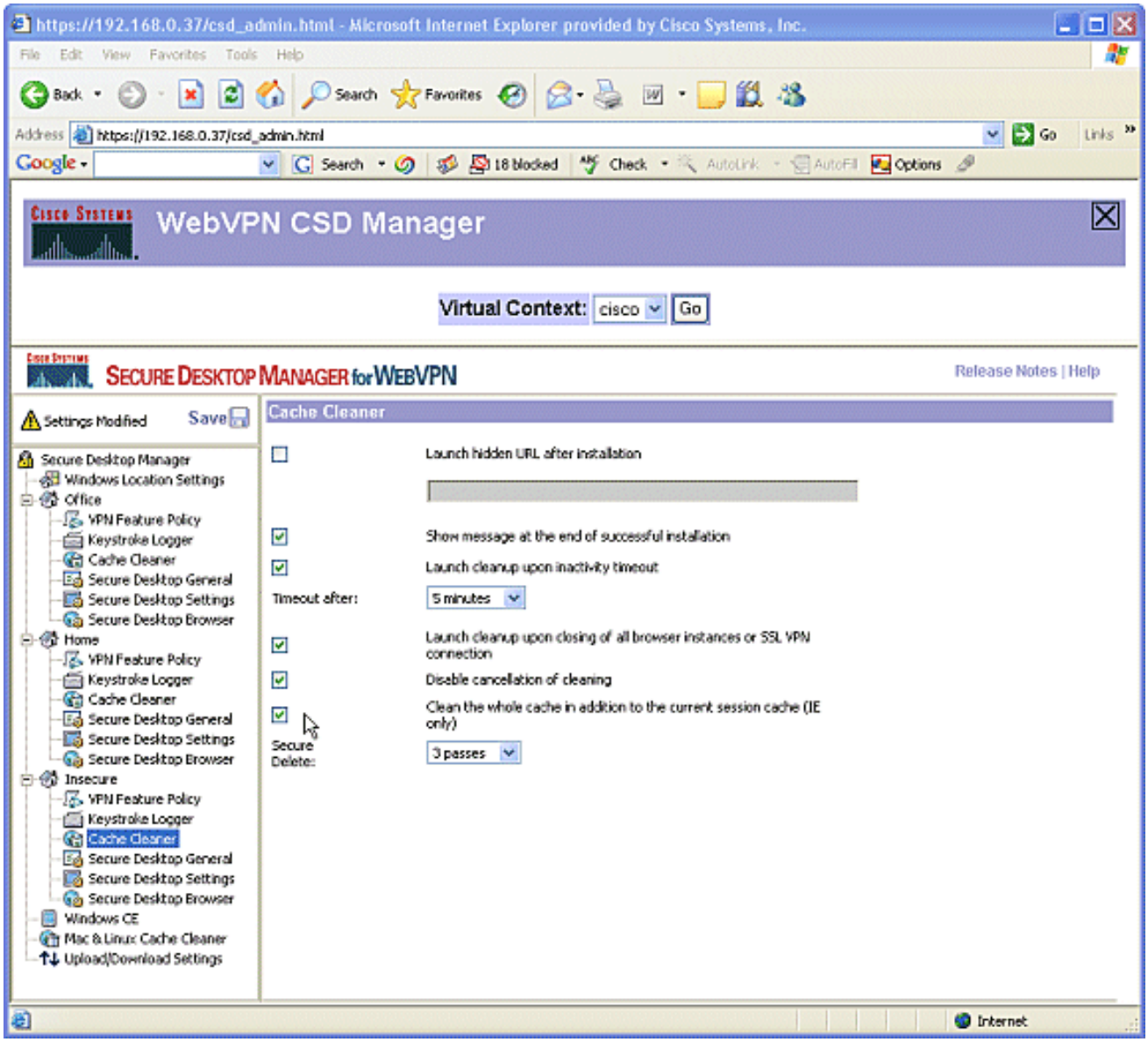
8. Secure Desktop Browser の設定は、これらのユーザに会社の Web サイトをお気に入りに事前設定してアクセスさせたいかどうかによって変わります。Insecure の下にある VPN Feature Policy をクリックします。これらは信頼されているユーザではないため、Web ブラウジングだけを許可します。Web Browsing のドロップダウン メニューから ON を選択します。他のアクセスについては、OFF に設定します。



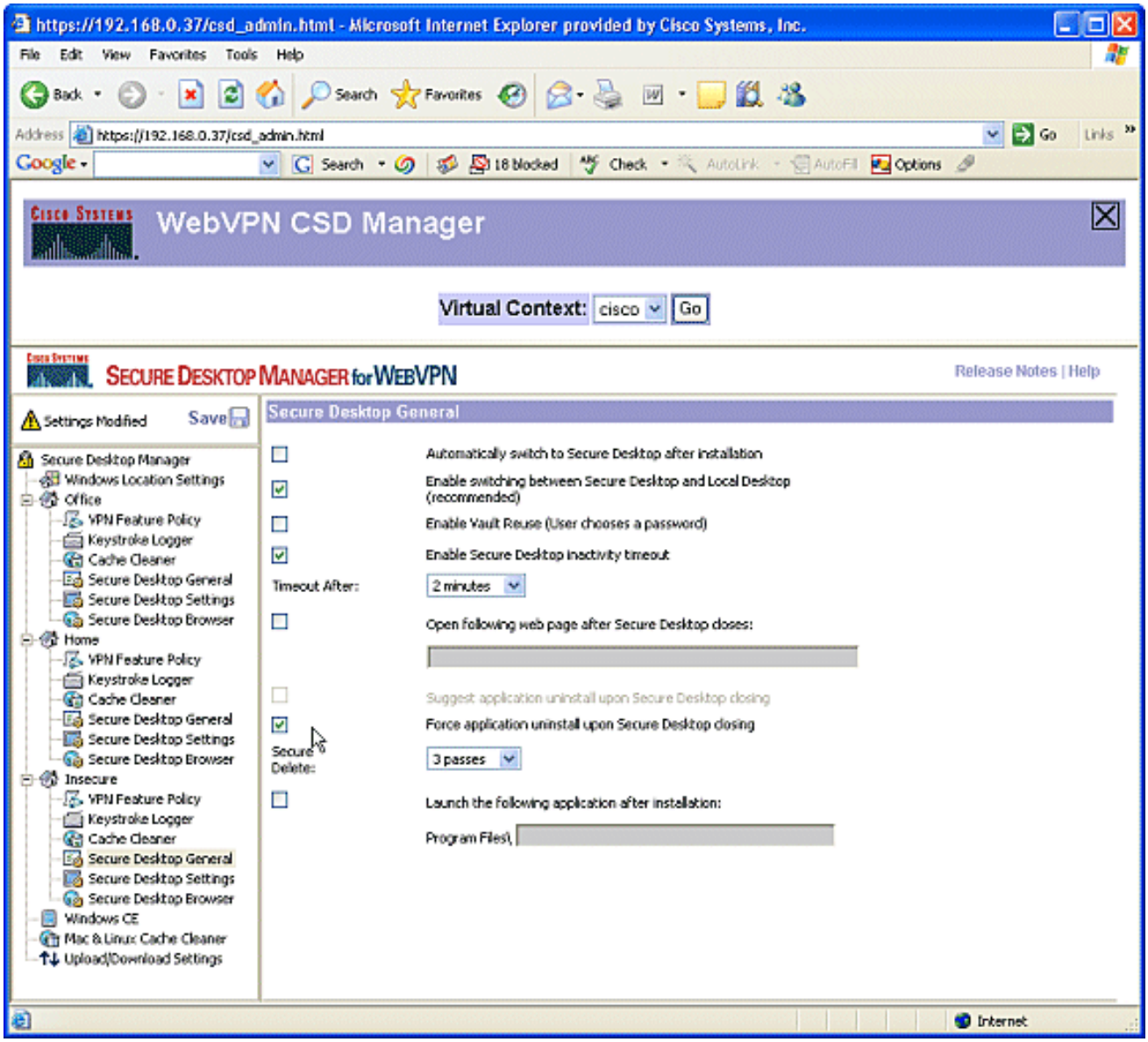
9. Check for keystroke loggers チェック ボックスをチェックします。



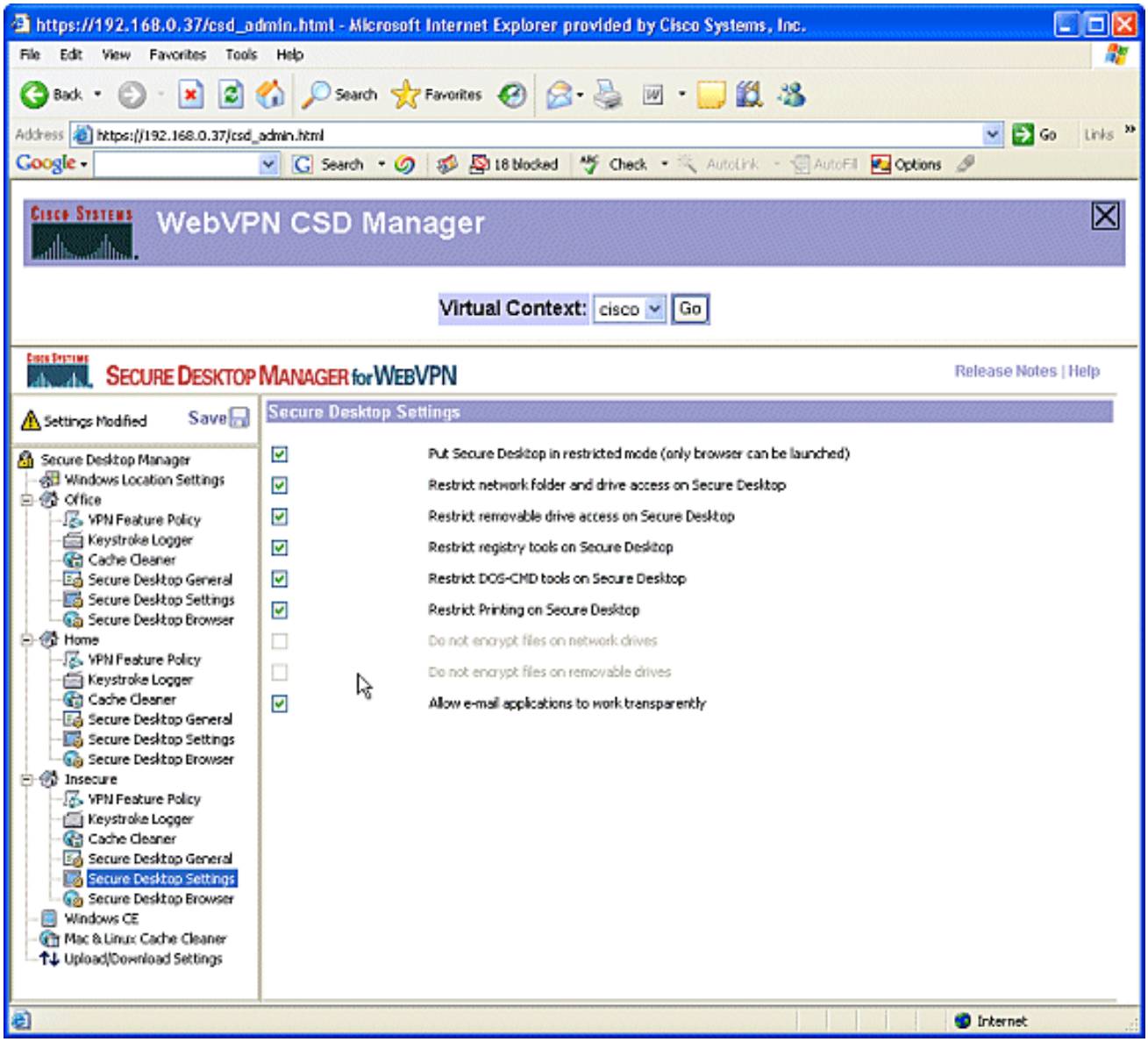
10. Insecure にキャッシュ クリーナを設定します。Clean the whole cache in addition to the current session cache (IE only) チェック ボックスをチェックします。他の設定はデフォルトのままにしておきます。



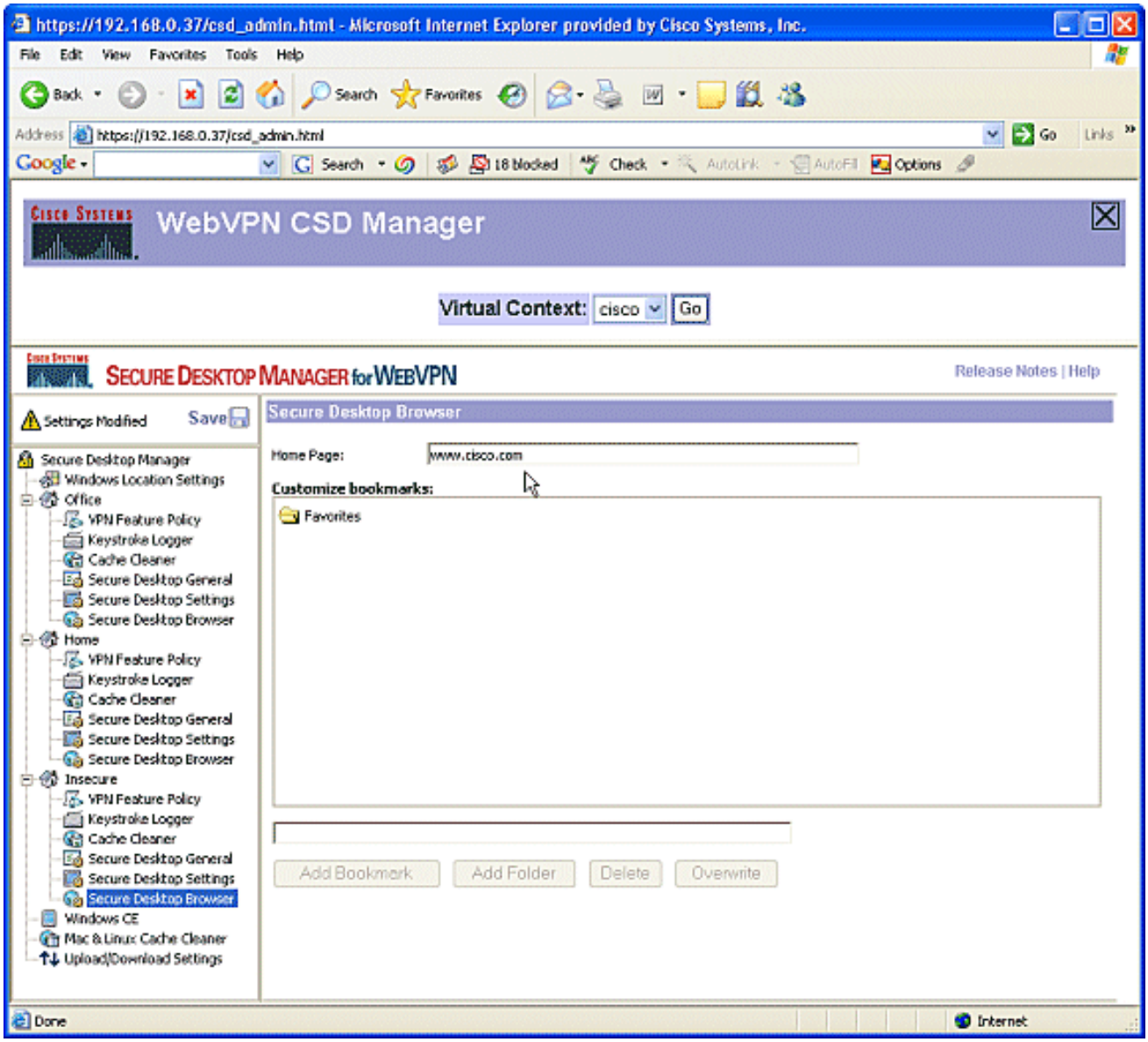
11. Insecure の下で、Secure Desktop General を選択します。無活動タイムアウトを 2 分に減らします。Force application uninstall upon Secure Desktop closing チェック ボックスをチェックします。



12. Insecure の下で Secure Desktop Settings を選択し、次に示すように非常に制限された設定を行います。



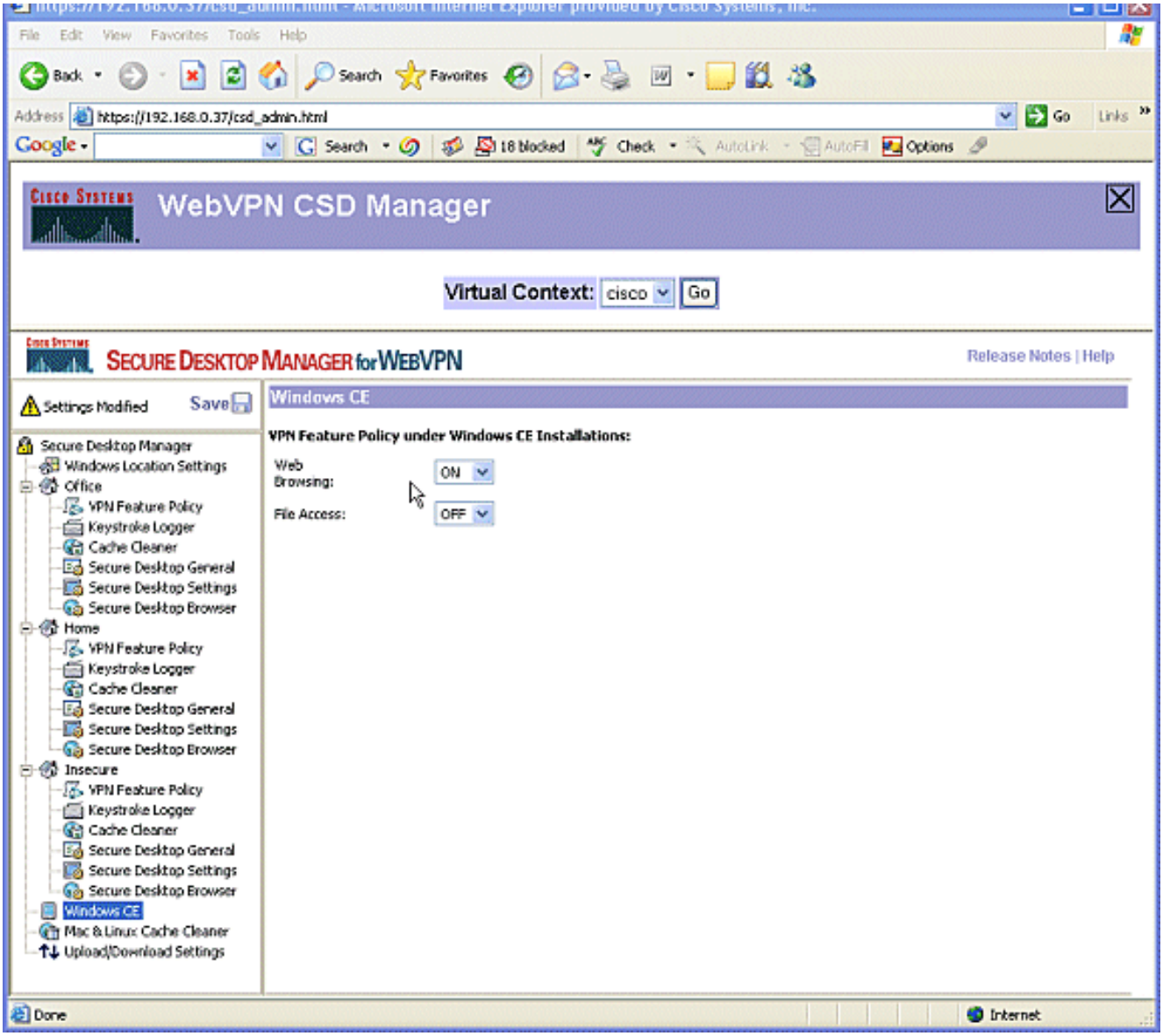
13. Secure Desktop Browser を選択します。Home Page フィールドに、これらのクライアントがホーム ページとする Web サイトを入力します。



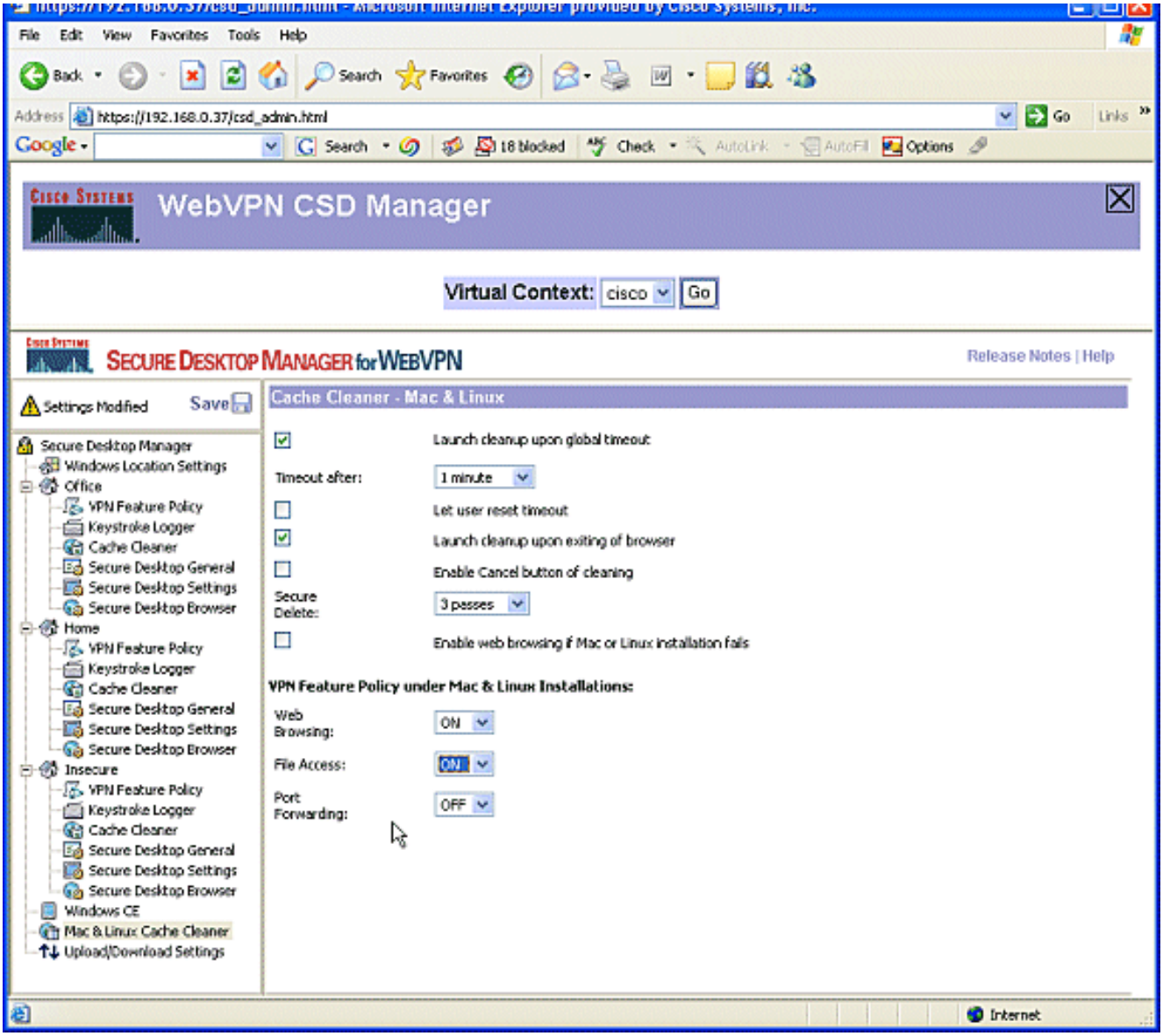
フェーズ 2：ステップ 4：Windows CE、Macintosh、および Linux の機能を設定する。

Windows CE、Macintosh、および Linux 向けに CSD 機能を設定します。

1. Secure Desktop Manager の下で Windows CE を選択します。Windows CE には一部の VPN 機能しかありません。Web Browsing を ON に設定します。



2. **Mac & Linux Cache Cleanerを選択します。**Macintosh と Linux のオペレーティングシステムがアクセスできるのは、CSD のキャッシュ クリーナとしての機能だけです。これらは次の図で示すように設定します。応答が表示されたら、Save をクリックし、続いて OK をクリックします。

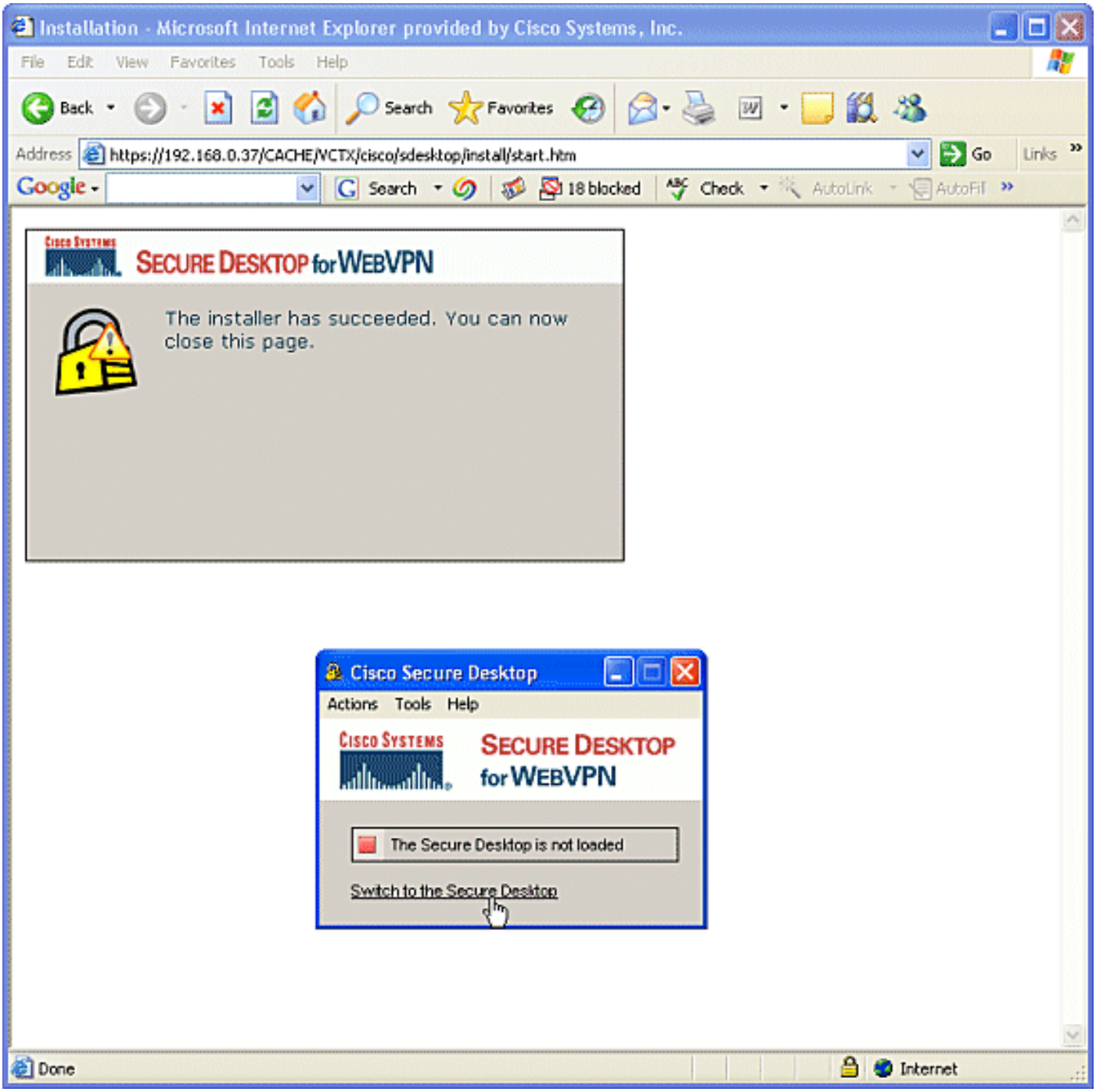


確認

CSD の動作テスト

SSL をイネーブルにしたブラウザで https://WebVPN_Gateway_IP Address にアクセスして WebVPN ゲートウェイに接続し、CSD の動作をテストします。

注：異なる WebVPNコンテキスト(例：https://192.168.0.37/cisco)を作成した場合は、コンテキストの一意の名前を必ず使用**してください**。



コマンド

いくつかの **show** コマンドは WebVPN に関連しています。これらのコマンドをコマンドライン インターフェイス（CLI）で実行して、統計情報や他の情報を表示できます。show コマンドの詳細については、「WebVPN 設定の検証」を参照してください。

注：CLI Analyzer(登録[ユーザ](#)専用)では、特定のshowコマンドが**サポート**されます。CLIアナライザを使用して、**show**コマンド出力の**分析を**表示します。

トラブルシュート

コマンド

いくつかの debug コマンドは、WebVPN に関連しています。これらのコマンドの詳細について

は、「WebVPN の Debug コマンドの使用」を参照してください。

注：debugコマンドを使用すると、シスコデバイスに悪影響が及ぶ可能性があります。debug コマンドを使用する前に、「debug コマンドの重要な情報」を参照してください。

clear コマンドの詳細については、『WebVPN clear コマンドの使用方法』を参照してください。

関連情報

- **WebVPN および DMVPN コンバージェンス導入ガイド**
- **SSL VPN - WebVPN**
- **Cisco IOS SSLVPN**
- **テクニカル サポートとドキュメント – Cisco Systems**