目次

概要

クライアントレス SSL VPN（WebVPN）では、SSL 対応ブラウザがあれば、ユーザはどんな場所からでも安全に企業 LAN のリソースへアクセスできます。 ユーザはまず WebVPN ゲートウェイで認証を受けますが、WebVPN ゲートウェイでは、あらかじめ設定されたネットワーク リソースへのユーザ アクセスが許可されます。 WebVPN ゲートウェイは、Cisco IOS® ルータ、Cisco Adaptive Security Appliances（ASA; 適応型セキュリティ アプライアンス）、Cisco VPN 3000 コンセントレータ、Catalyst 6500 および 7600 ルータ対応 Cisco WebVPN サービス モジュールに設定できます。

Secure Socket Layer（SSL）Virtual Private Network（VPN; 仮想プライベート ネットワーク）テクノロジーは、3 つの主要モードで Cisco デバイス上に設定できます。 3 つのモードとは、クライアントレス SSL VPN（WebVPN）、シンクライアント SSL VPN（ポート転送）、および SSL VPN クライアント（SVC）モードです。 このドキュメントでは、Cisco IOS ルータでの WebVPN の設定方法を紹介します。

注ルータの IP ドメイン名またはホスト名に変更を加えないでください。自己署名証明書が再生成され、設定済みのトラストポイントが無効になります。 ルータが WebVPN 用に設定されている場合、自己署名証明書が再生成されると、接続の問題が発生します。 WebVPN は、SSL トラストポイント名を WebVPN ゲートウェイ設定に結びつけます。 このため、新しい自己署名証明書が発行されると、新しいトラストポイント名が WebVPN の設定と一致せず、ユーザが接続できま

せん。

注永続的な自己署名証明書を使用する WebVPN ルータで **ip https-secure server** コマンドを実行すると、新しい RSA キーが生成されて、証明書が無効になります。 新しいトラストポイントが作成されて、このトラストポイントが SSL WebVPN を中断します。 **ip https-secure server** コマンドを実行した後に、永続的な自己署名証明書を使用するルータが再起動すると、同じ問題が発生します。

シンクライアント SSL VPN についての詳細は、『SDM によるシンクライアント SSL VPN (WebVPN) の IOS 設定例』を参照してください。

SSL VPN Client の詳細は、『SDM を使用した IOS での SSL VPN Client (SVC) の設定例』を参照してください。

SSL VPN は次の Cisco ルータ プラットフォームで動作します。

- Cisco 870、1811、1841、2801、2811、2821 および 2851 シリーズ ルータ
- Cisco 3725、3745、3825、3845、7200、および 7301 シリーズ ルータ

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 ソフトウェア リリース 12.4(6)T 以降の拡張イメージ
- 「概要」に記載されている Cisco ルータ プラットフォームのいずれか

使用するコンポーネント

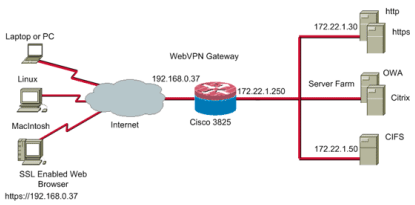
このドキュメントの情報は、次のソフトウェアとハードウェアのバージョンに基づくものです。

- Cisco 3825 ルータ
- 拡張 Enterprise ソフトウェア イメージ：Cisco IOS ソフトウェア リリース 12.4(9)T
- Cisco Router and Security Device Manager (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たものです。 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。 ネットワークが稼働中の場合は、コマンドが及ぼす潜在的な影響を十分に理解しておく必要があります。 次の例で使用する IP アドレスは、RFC 1918 から引用したプライベート アドレスで、インターネットでの使用には適格ではありません。

ネットワーク図

このドキュメントでは、次のネットワーク構成を使用しています。



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。

設定前の作業

開始する前に、次の作業を実行してください。

1. ホスト名とドメイン名を設定します。
2. ルータの SDM 設定を行います。 一部のシスコ ルータには、SDM がプリインストールされています。Cisco SDM がルータにロードされていない場合は、このソフトウェアの無償コピーを [Software Download] ページ（登録ユーザ専用）からダウンロードできます。 サービス契約を結んでいる Cisco.com アカウントが必要です。 SDM のインストールと設定についての詳細、『Cisco ルータとセキュリティ デバイス マネージャ』を参照してください。
3. ルータで正しい日付、時刻、および時間帯を設定します。

Cisco IOS での WebVPN の設定

1 つのデバイスに、複数の WebVPN ゲートウェイを関連付けることができます。 各 WebVPN ゲートウェイは、ルータ上の 1 つの IP アドレスにのみリンクされます。 特定の WebVPN ゲートウェイに複数の WebVPN コンテキストを作成できます。 各コンテキストを識別するため、コンテキストに一意の名前を付けます。 1 つのポリシー グループは、1 つの WebVPN コンテキストにのみ関連付けられます。 ポリシー グループは、特定の WebVPN コンテキストでどのリソースが利用可能かを説明します。

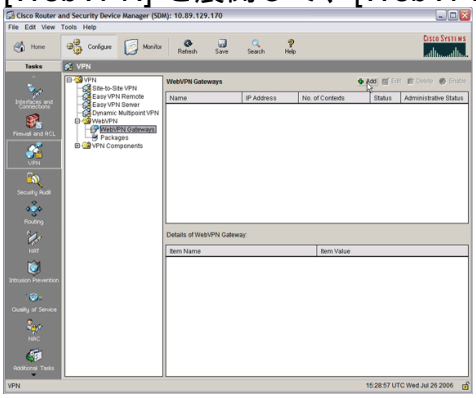
Cisco IOS に WebVPN を設定するには、次の手順を実行します。

1. WebVPN ゲートウェイの設定
2. ポリシー グループに対して許可されるリソースを設定する
3. WebVPN ポリシー グループの設定とリソースの選択
4. WebVPN コンテキストの設定
5. ユーザ データベースと認証方法の設定

ステップ 1. WebVPN ゲートウェイの設定

WebVPN ゲートウェイを設定するには、次の手順を実行します。

1. SDM アプリケーションで、[Configure] をクリックし、次に [VPN] をクリックします。
2. [WebVPN] を展開して、[WebVPN Gateways] を選択します。



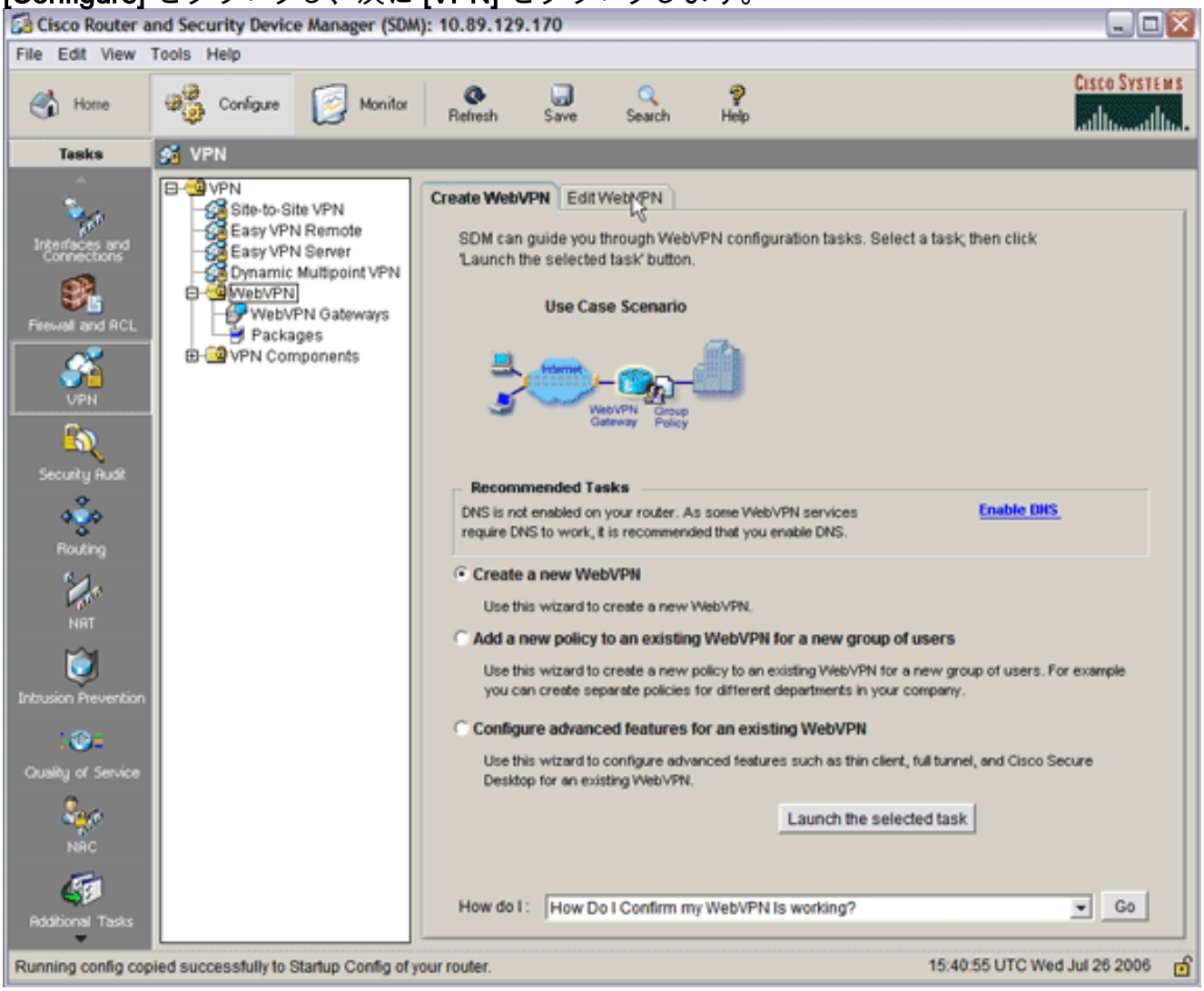
3. [Add] をクリックします。[Add WebVPN Gateway] ダイアログ ボックスが表示されます。
4. [Gateway Name] および [IP Address] フィールドに値を入力し、[Enable Gateway] チェック ボックスをオンにします。
5. [Redirect HTTP Traffic] チェック ボックスをオンにして、[OK] をクリックします。
6. [Save] をクリックし、[Yes] をクリックして変更を確定します。

ステップ 2. ポリシー グループに対して許可されるリソースの設定

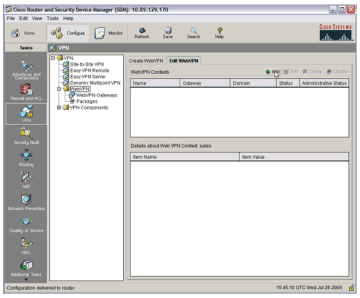
ポリシー グループを作成する前にリソースを設定すれば、ポリシー グループへ簡単にリソースを追加できます。

ポリシー グループに対して許可されるリソースを設定するには、次の手順を実行します。

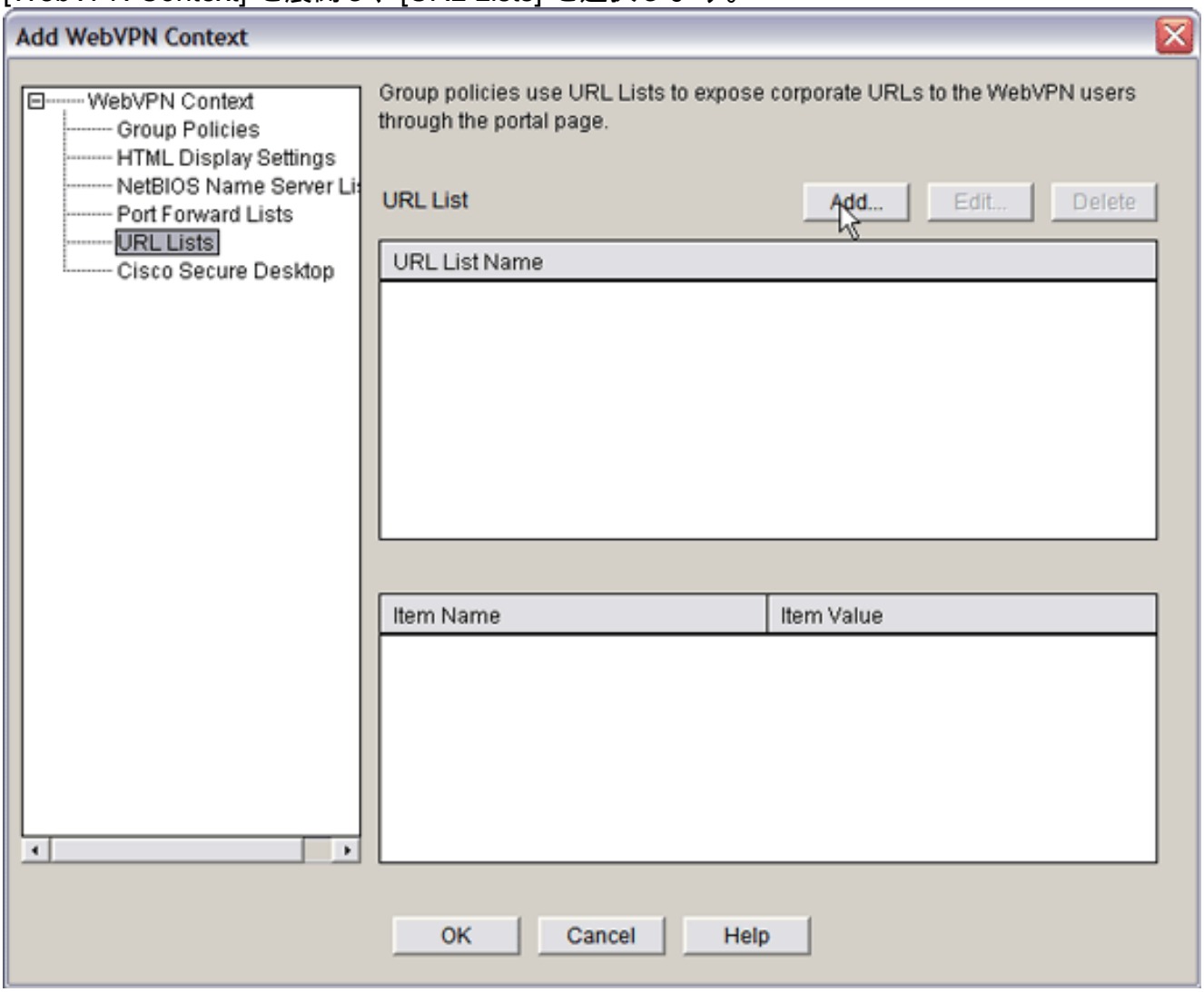
1. **[Configure]** をクリックし、次に **[VPN]** をクリックします。



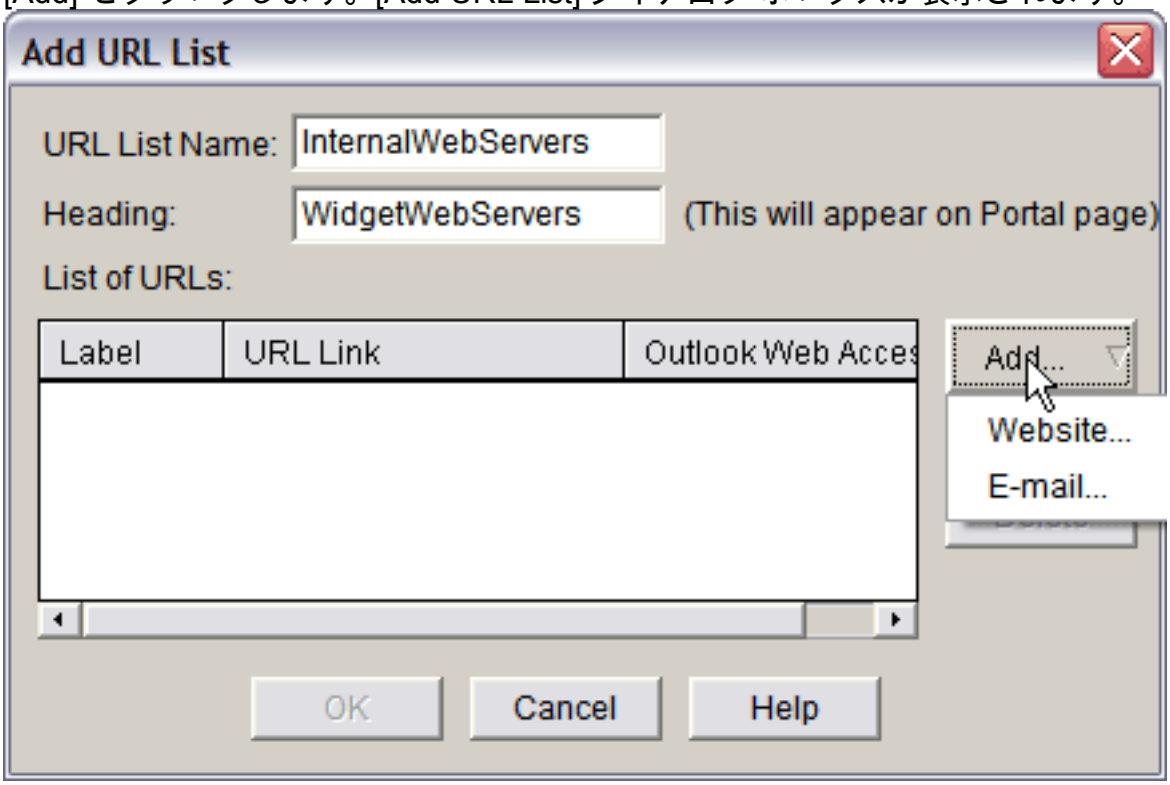
2. **WebVPN を**選択し、次に**編集 WebVPN タブを**クリックして下さい。**注**WebVPN では、HTTP、HTTPS、Common Internet File System（CIFS）プロトコルによる Windows ファイル ブラウジング、および Citrix のアクセスも設定できます。



3. [Add] をクリックします。[Add WebVPN Context] ダイアログ ボックスが表示されます。
4. [WebVPN Context] を展開し、[URL Lists] を選択します。

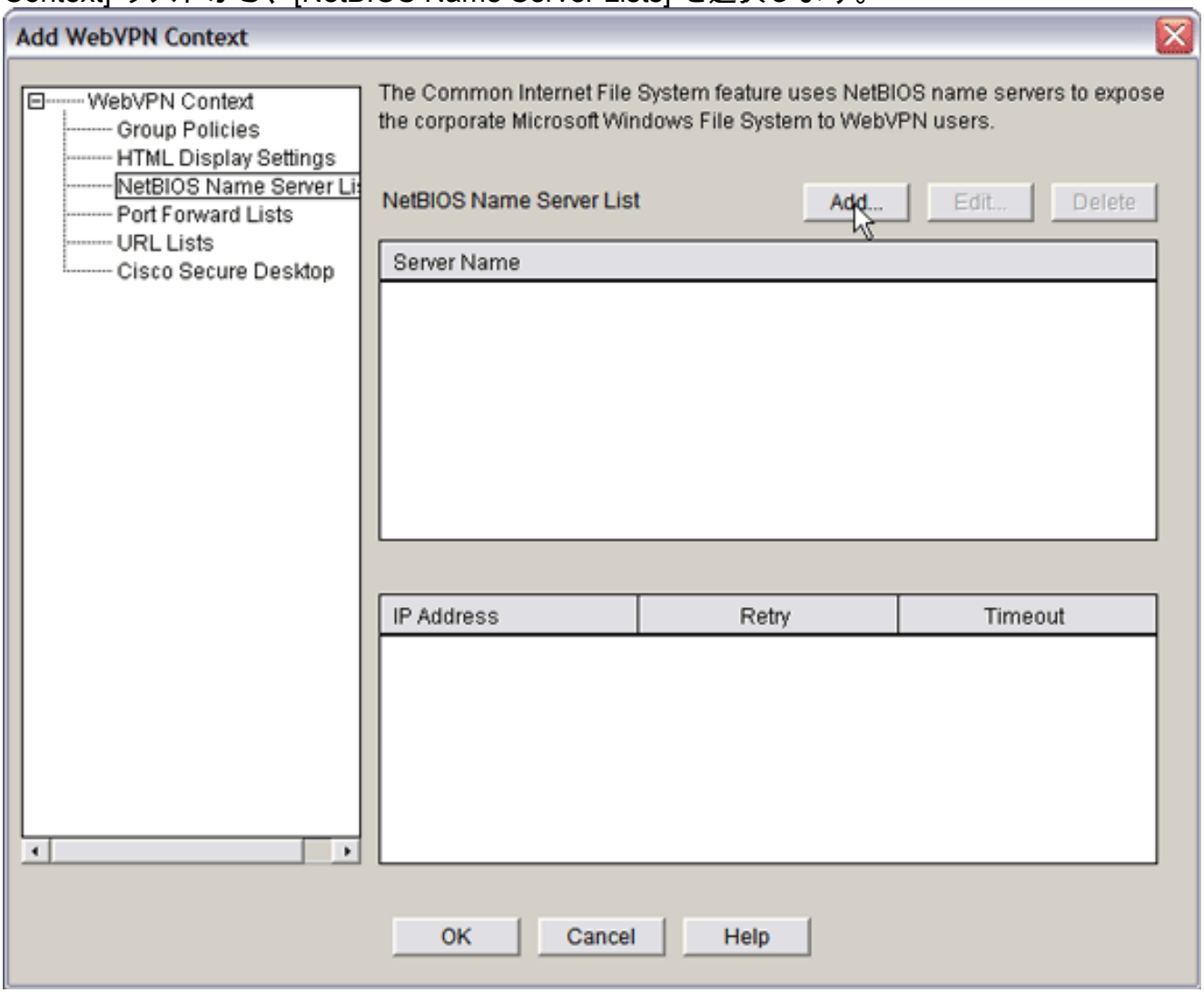


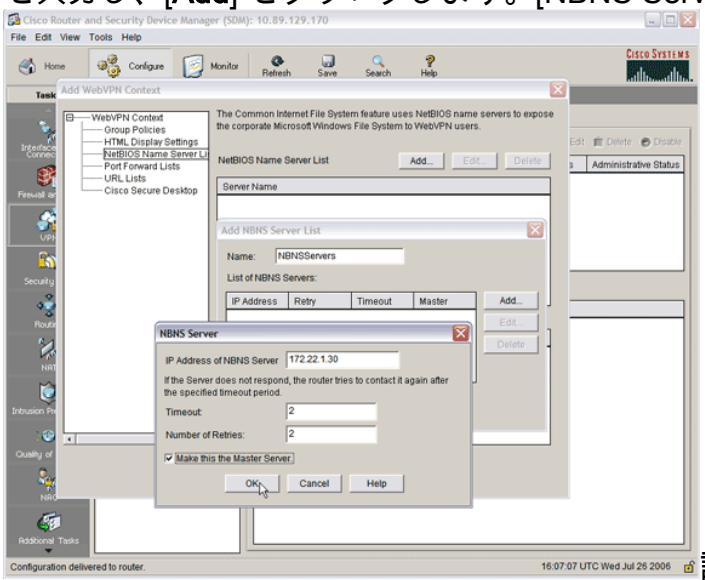
5. [Add] をクリックします。[Add URL List] ダイアログ ボックスが表示されます。



6. [URL List Name] および [Heading] フィールドに値を入力します。

7. **[Add]** をクリックし、**[Website]** を選択します。このリストには、この WebVPN 接続で利用可能にする、すべての HTTP および HTTPS Web サーバが含まれています。
8. Outlook Web Access（OWA）へのアクセスを追加するには、[Add] をクリックし、[E-mail] を選択して、必要なすべてのフィールドへ入力してから [OK] をクリックします。
9. NetBIOS Name Service (NBNS) サーバを指定し、Windows ドメイン内の共有を順序通りに設定すれば、CIFS による Windows ファイル ブラウジングが可能になります。[WebVPN Context] リストから、[NetBIOS Name Server Lists] を選択します。



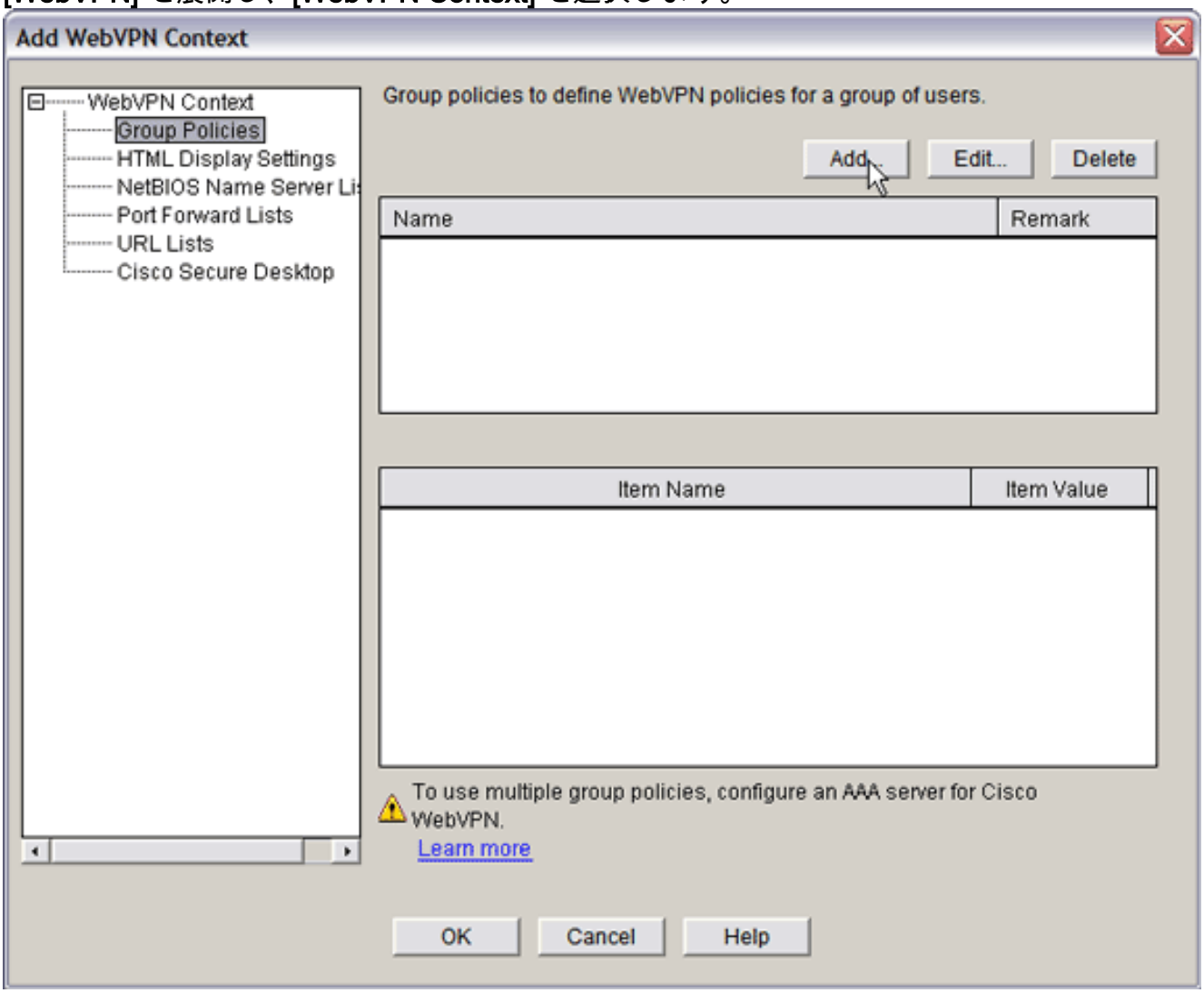
[Add] をクリックします。[Add NBNS Server List] ダイアログ ボックスが表示されます。リストの名前を入力し、**[Add]** をクリックします。[NBNS Server] ダイアログ ボックスが表示されます。  該当する場合、[Make This the

Master Server] チェック ボックスをオンにします。[OK] をクリックし、さらに [OK] をクリックします。

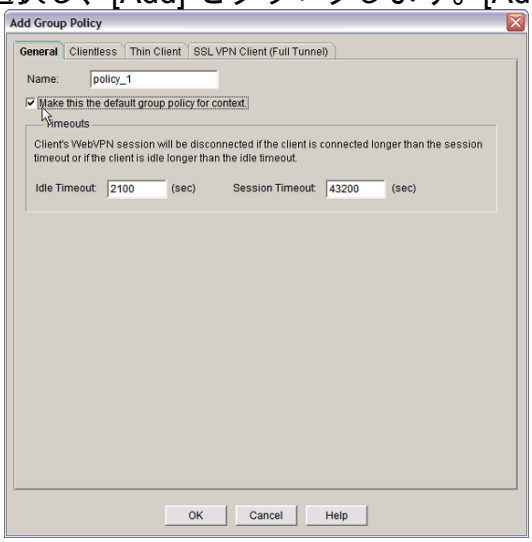
ステップ 3. WebVPN ポリシー グループの設定とリソースの選択

WebVPN ポリシー グループを設定し、リソースを選択するには、次の手順を実行します。

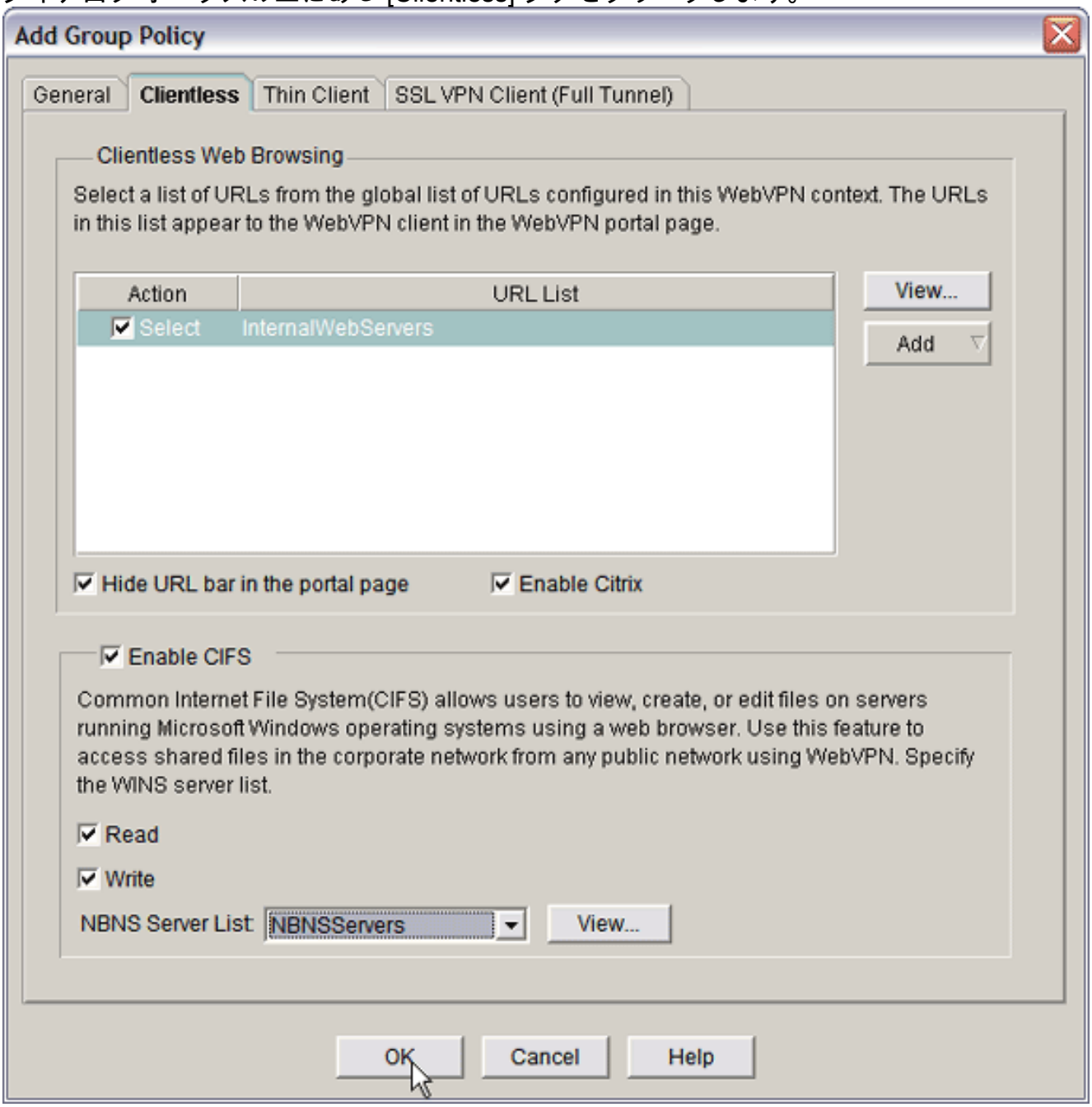
1. **[Configure]** をクリックし、次に **[VPN]** をクリックします。
2. **[WebVPN]** を展開し、**[WebVPN Context]** を選択します。



3. [Group Policies] を選択し、[Add] をクリックします。[Add Group Policy] ダイアログ ボックスが表示されます。



4. 新しいポリシーの名前を入力し、**[Make this the default group policy for context]** チェック ボックスにチェックマークを入れます。
5. ダイアログ ボックスの上にある [Clientless] タブをクリックします。



6. 選択する URL リストの [Select] チェック ボックスにチェックマークを付けます。
7. お客様が Citrix クライアントを使用するため、Citrix サーバへのアクセスが必要な場合は、[Enable Citrix] チェック ボックスをオンにします。
8. [Enable CIFS]、[Read]、および [Write] チェック ボックスをオンにします。
9. **[NBNS Server List]** ドロップダウンの矢印をクリックして、ステップ 2 で Windows ファイル ブラウジング用に作成した NBNS サーバ リストを選択します。
10. [OK] をクリックします。

ステップ 4. WebVPN コンテキストの設定

WebVPN ゲートウェイ、グループ ポリシー、およびリソースをリンクさせるには、WebVPN コンテキストを設定する必要があります。 WebVPN コンテキストを設定するには、次の手順を実行します。

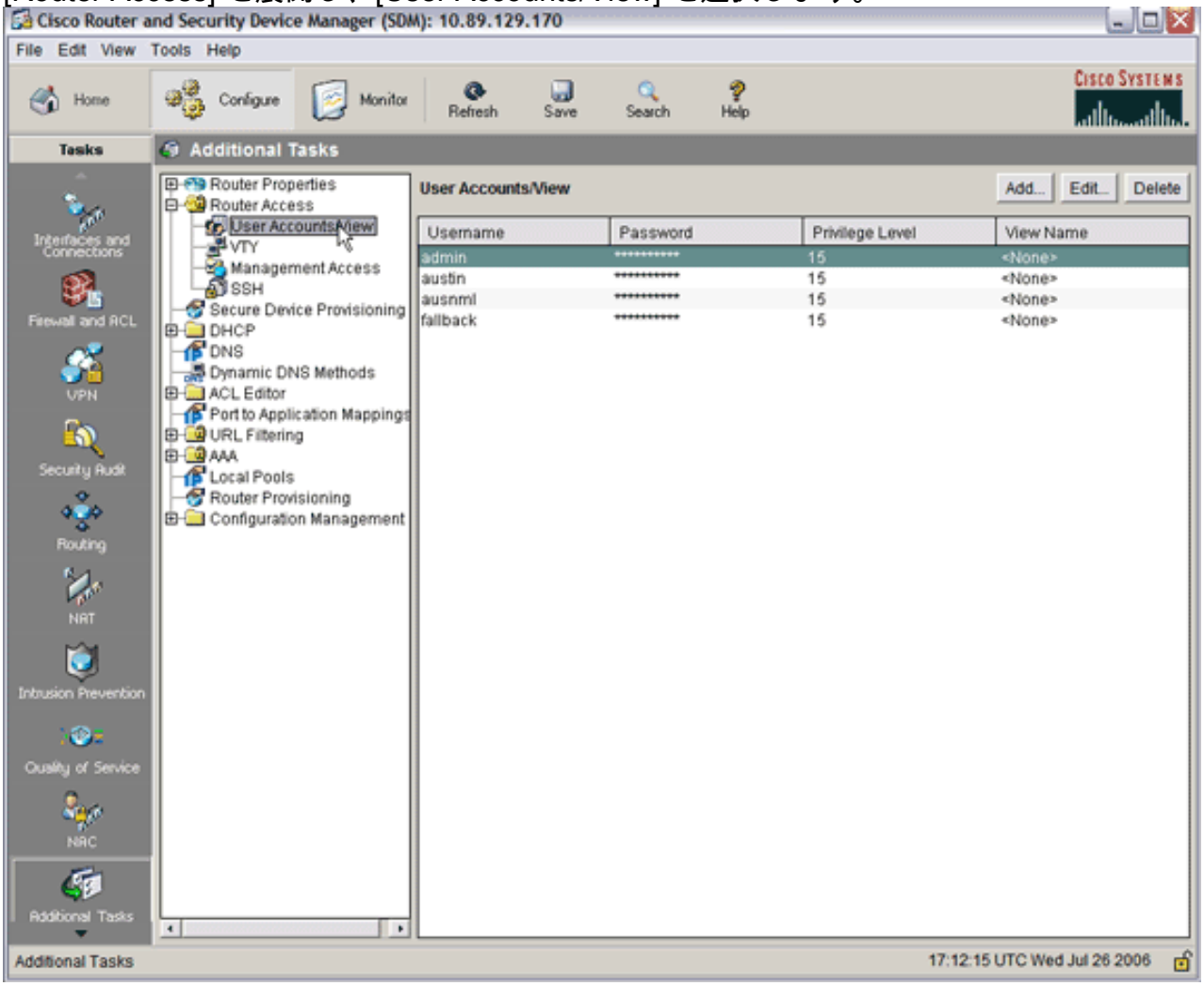
1. [WebVPN Context] を選択し、コンテキストの名前を入力します。
2. [Associated Gateway] ドロップダウンの矢印をクリックして、関連付けられているゲートウェイを選択します。
3. 複数のコンテキストを作成する場合は、このコンテキストを識別する一意の名前を [Domain] フィールドに入力します。 [Domain] フィールドを空欄にすると、ユーザは **https://*IPAddress*** で WebVPN にアクセスすることになります。 ドメイン名（たとえば、*Sales*）を入力すると、ユーザは **https://*IPAddress*/Sales** で接続することになります。
4. [Enable Context] チェック ボックスをオンにします。
5. [Maximum Number of Users] フィールドで、デバイスのライセンスで許可されている最大のユーザ数を入力します。
6. [Default Group policy] ドロップダウンの矢印をクリックし、グループ ポリシーを選択してこのコンテキストに関連付けます。
7. [OK] をクリックし、さらに [OK] をクリックします。

ステップ 5. ユーザ データベースと認証方法の設定

Radius、Cisco AAA サーバ、またはローカル データベースで認証を行うように、クライアントレス SSL VPN（WebVPN）セッションを設定できます。 次の例では、ローカル データベースを使用します。

ユーザ データベースと認証方法を設定するには、次の手順を実行します。

1. [Configuration] をクリックし、[Additional Tasks] をクリックします。
2. [Router Access] を展開し、[User Accounts/View] を選択します。



3. [Add] ボタンをクリックします。[Add an Account] ダイアログ ボックスが表示されます。
4. ユーザ アカウントとパスワードを入力します。
5. [OK] をクリックし、さらに [OK] をクリックします。
6. [Save] をクリックし、[Yes] をクリックして変更を確定します。

結果

ASDM は次のコマンドライン設定を作成します。

```
ausnml-3825-01
```

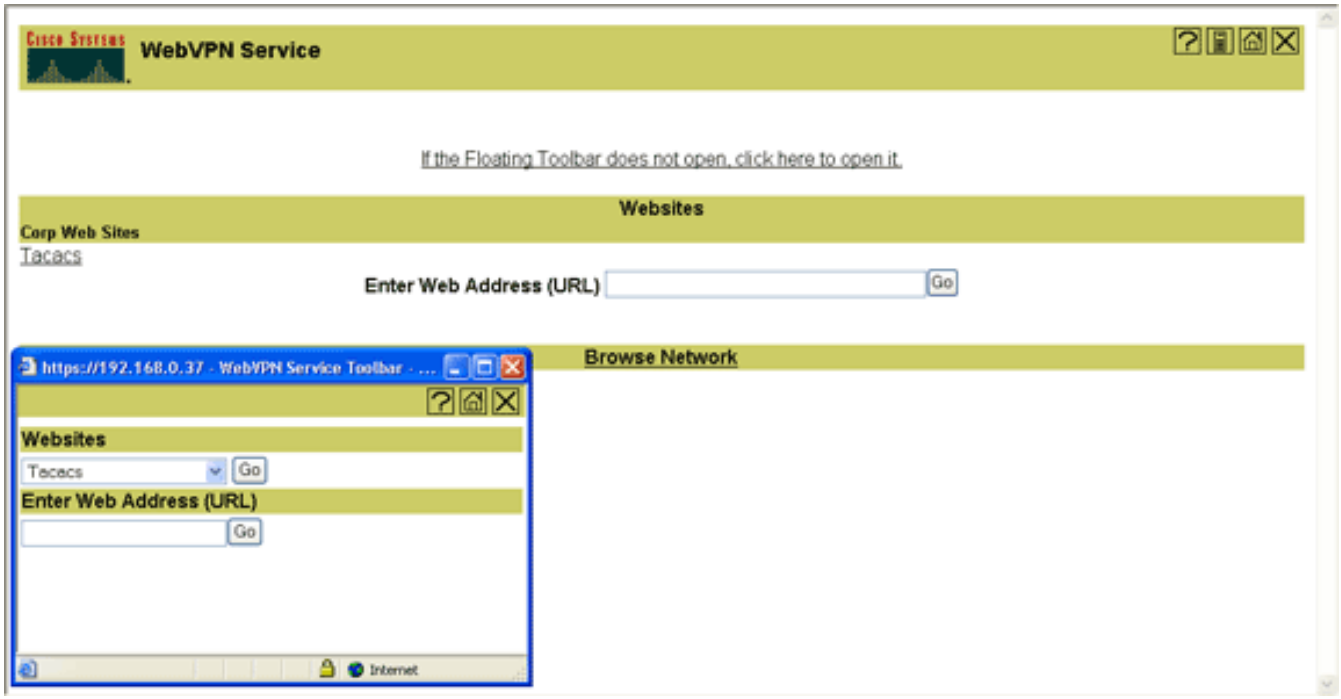
確認

ここでは、設定が正常に動作していることを確認します。

手順

設定が正常に動作していることを確認するには、次の手順を実行します。

- ユーザを使用して設定をテストします。 SSL 対応 Web ブラウザに、**https://*WebVPN_Gateway_IP_Address*** と入力します。 この場合、*WebVPN_Gateway_IP_Address* は WebVPN サービスの IP アドレスです。 証明書を承認してユーザ名とパスワードを入力すると、次のイメージのようなイメージが表示されます。



- SSL VPN セッションをチェックします。 SDM アプリケーションで、[Monitor] ボタンをクリックし、次に [VPN Status] をクリックします。 [WebVPN (All Contexts)] を展開し、適切なコンテキストを展開して、[Users] を選択します。
- エラー メッセージを確認します。 SDM アプリケーションで、[Monitor] ボタンをクリックし、[Logging] をクリックして、次に [Syslog] タブをクリックします。
- デバイスの実行コンフィギュレーションを表示します。 SDM アプリケーションで [Configure] ボタンをクリックし、[Additional Tasks] をクリックします。 [**Configuration Management**] を展開し、[**Config Editor**] を選択します。

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** コマンドの詳細は、『WebVPN 設定の確認』を参照してください。

注Output Interpreter Tool (OIT) (登録ユーザ専用) では、特定の **show** コマンドがサポートされています。 OIT を使用して、**show** コマンド出力の解析を表示できます。

トラブルシューティング

ここでは、設定に関するトラブルシューティングについて説明します。

注コピー処理が行われている間は、**Copy File to Server** コマンドを中断したり、別のウィンドウに移動しないでください。 操作を中断すると、不完全なファイルがサーバに保存される可能性があります。

注ユーザは WebVPN クライアントを使用して新しいファイルをアップロードしたり、ダウンロードしたりすることができますが、**Copy File to Server** コマンドを使用して、WebVPN の Common Internet File System (CIFS) のファイルを上書きすることはできません。 ユーザがサーバ上のファイルを置き換えようとすると、次のメッセージが表示されます。

手順

設定をトラブルシューティングするには、次の手順を実行します。

1. クライアントでポップアップ ブロッカーが無効になっていることを確認します。
2. クライアントで cookie が有効になっていることを確認します。
3. クライアントで Netscape、Internet Explorer、Firefox、または Mozilla ブラウザが使用されていることを確認します。

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 コマンドを使用すると、Cisco 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。

関連情報

- Cisco IOS SSLVPN
- Cisco IOS SSLVPN Q&A
- SDM によるシンクライアント SSL VPN (WebVPN) の IOS 設定例
- SDM を使用した IOS での SSL VPN Client (SVC) の設定例
- テクニカルサポートとドキュメント - Cisco Systems