# Índice



# Introdução

As VPNs SSL sem clientes (WebVPN) permitem que um usuário acesse recursos de forma segura na LAN corporativa de qualquer lugar com um navegador Web habilitado para SSL. Primeiro, o usuário autentica com um gateway WebVPN que permitirá o seu acesso a recursos de rede pré-configurados. Os gateways WebVPN podem ser configurados no Roteadores do ® do Cisco IOS, nas ferramentas de segurança adaptáveis de Cisco (ASA), nos concentradores do Cisco VPN 3000, e no Módulo de serviços de Cisco WebVPN para os Catalyst 6500 e 7600 Router.

A tecnologia Virtual Private Network (VPN) Secure Socket Layer (SSL) pode ser configurada em dispositivos Cisco em três modos principais: VPN SSL Sem Clientes (WebVPN), VPN SSL Thin-Client (Encaminhamento de Portas), e Cliente VPN SSL (modo SVC). Este documento demonstra a configuração da WebVPN em Cisco IOS Routers.

**Nota:** Não altere o nome do domínio IP ou o nome de host do roteador, pois isso acionará uma regeneração do certificado autoassinado e substituirá o ponto de confiança configurado. A regeneração do certificado autoassinado utilizará problemas de conexão se o roteador tiver sido configurado para WebVPN. A WebVPN vincula o nome do ponto de confiança SSL à configuração de gateway WebVPN. Portanto, se um certificado autoassinado novo for emitido, o nome novo do ponto de confiança não corresponderá à configuração da WebVPN e os usuários

não conseguirão conectar.

**Nota:** Se você executar o **comando ip https-secure server** em um roteador WebVPN que use um certificado autoassinado persistente, uma nova chave RSA será gerada e o certificado se tornará inválido. Um novo ponto de confiança será criado, o que quebra a WebVPN SSL. Se o roteador que usa o certificado autoassinado persistente reinicializar após você executar o **comando ip https-secure server**, o mesmo problema ocorrerá.

Consulte o Exemplo de Configuração do IOS da VPN SSL Thin-Client (WebVPN) com SDM para obter mais informações sobre a VPN SSL thin-client.

Consulte o Exemplo de Configuração de Cliente VPN SSL (SVC) no IOS com SDM para obter mais informações sobre o Cliente VPN SSL.

A VPN SSL pode ser executada nestas plataformas de Cisco Routers:

- Cisco 870, 1811, 1841, 2801, 2811, 2821 e 2851 Series Routers
- Cisco 3725, 3745, 3825, 3845, 7200 e 7301 Series Routers

# Pré-requisitos

## Requisitos

Certifique-se de atender a estes requisitos antes de tentar esta configuração:

- Uma imagem avançada do Cisco IOS Software Release 12.4(6)T ou posterior
- Uma das plataformas de Cisco Routers listadas na Introdução

## Componentes Utilizados

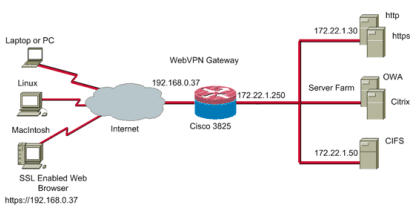
As informações neste documento são baseadas nestas versões de software e hardware:

- Cisco 3825 Router
- Imagem do software Advanced Enterprise - Cisco IOS Software Release 12.4(9)T
- Cisco Router and Security Device Manager (SDM) - versão 2.3.1

As informações neste documento foram criadas a partir de dispositivos em um ambiente de laboratório específico. Todos os dispositivos utilizados neste documento foram iniciados com uma configuração (padrão) inicial. Se a sua rede estiver ativa, certifique-se de que entende o impacto potencial de qualquer comando. Os endereços IP utilizados neste exemplo foram obtidos de endereços RFC 1918 que são privados e ilegais para uso na Internet.

## Diagrama de Rede

Este documento utiliza a seguinte configuração de rede:



## Convenções

Consulte as Convenções de Dicas Técnicas da Cisco para obter mais informações sobre convenções de documentos.

## Tarefas de Pré-configuração

Antes de iniciar, execute estas tarefas:

1. Configure um nome de host e um nome de domínio.
2. Configure o roteador para SDM. A Cisco envia alguns roteadores com uma cópia pré-instalada do SDM.Se o Cisco SDM já não estiver carregado em seu roteador, você poderá obter uma cópia gratuita do software de Download de Software (somente clientes registrados). Você deve possuir uma conta CCO com um contrato de serviço. Para obter informações detalhadas sobre a instalação e a configuração do SDM, consulte Cisco Router and Security Device Manager.
3. Configure a data, a hora e o fuso horário corretos para seu roteador.

# Configurar a WebVPN no Cisco IOS

Você pode ter mais de um gateway WebVPN associado a um dispositivo. Cada gateway WebVPN é vinculado somente a um endereço IP no roteador. Você pode criar mais de um contexto WebVPN para um gateway WebVPN específico. Para identificar contextos individuais, forneça cada contexto com um nome exclusivo. Um grupo de políticas pode ser associado somente a um contexto WebVPN. O grupo de políticas descreve quais recursos estão disponíveis em um contexto WebVPN específico.

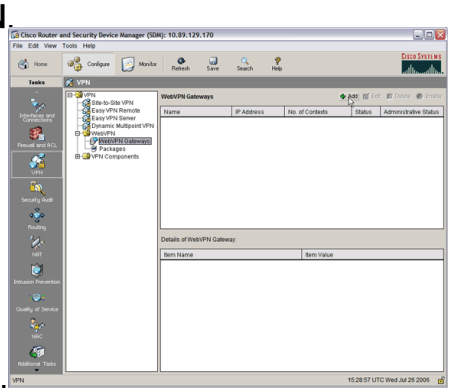
Execute estes passos para configurar a WebVPN no Cisco IOS:

1. Configurar o Gateway WebVPN
2. Configurar os Recursos Permitidos o Grupo de Políticas
3. Configurar o Grupo de Políticas WebVPN e Selecionar os Recursos
4. Configurar o Contexto WebVPN
5. Configurar o Banco de Dados de Usuários e o Método de Autenticação

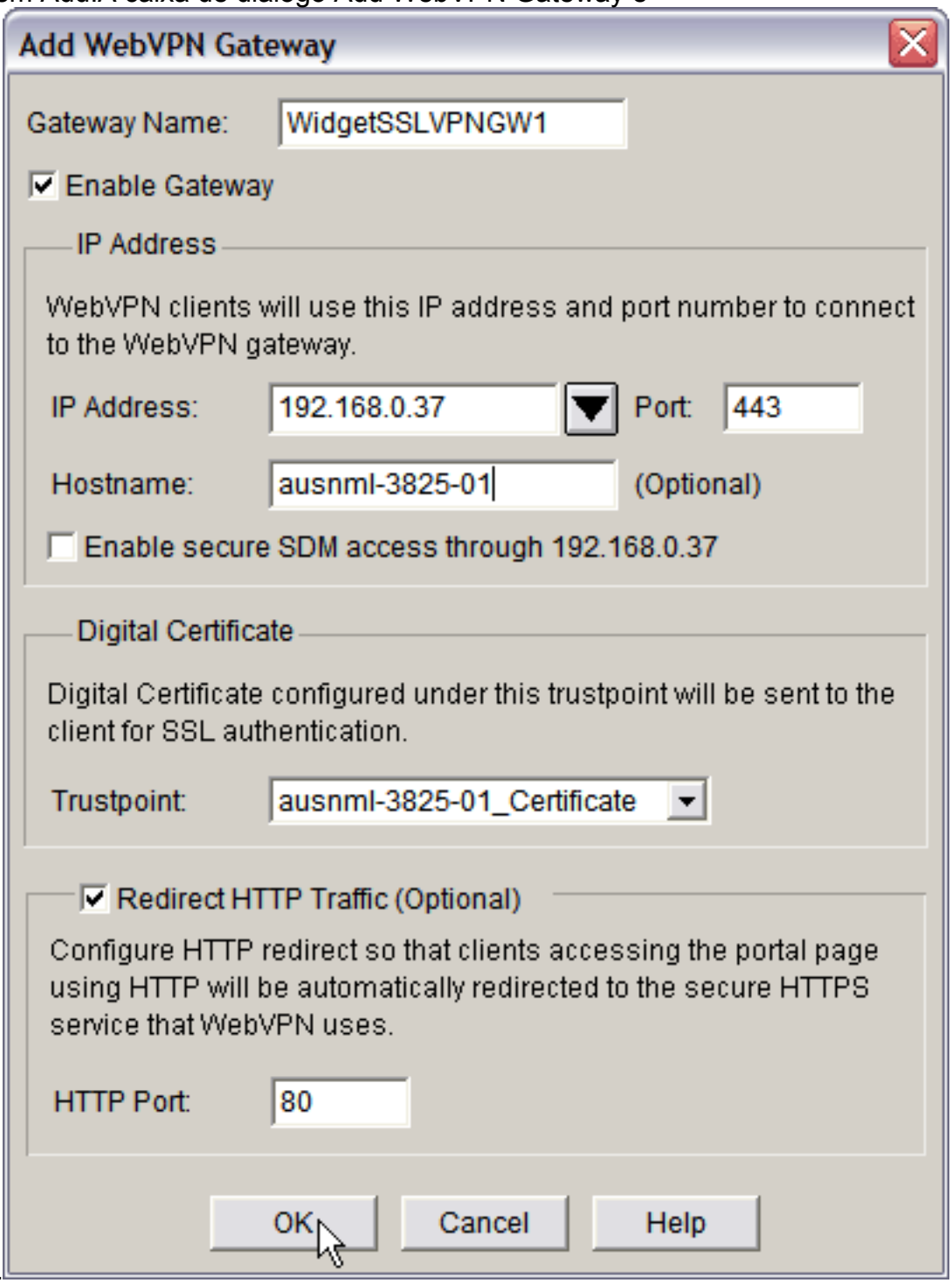
## Passo 1. Configurar o Gateway WebVPN

Execute estes passos para configurar o Gateway WebVPN:

1. No aplicativo SDM, clique em **Configure** e em **VPN**.
2. Expanda **WebVPN**, e escolha **Gateways WebVPN**.



3. Clique em Add.A caixa de diálogo Add WebVPN Gateway é exibida.




4. Insira valores nos campos Gateway Name e IP Address e marque a caixa de seleção **Enable Gateway**.
5. Marque a caixa de seleção **Redirect HTTP Traffic** e clique em **OK**.
6. Clique em **Save** e, em seguida, clique em **Yes** para aceitar as alterações.

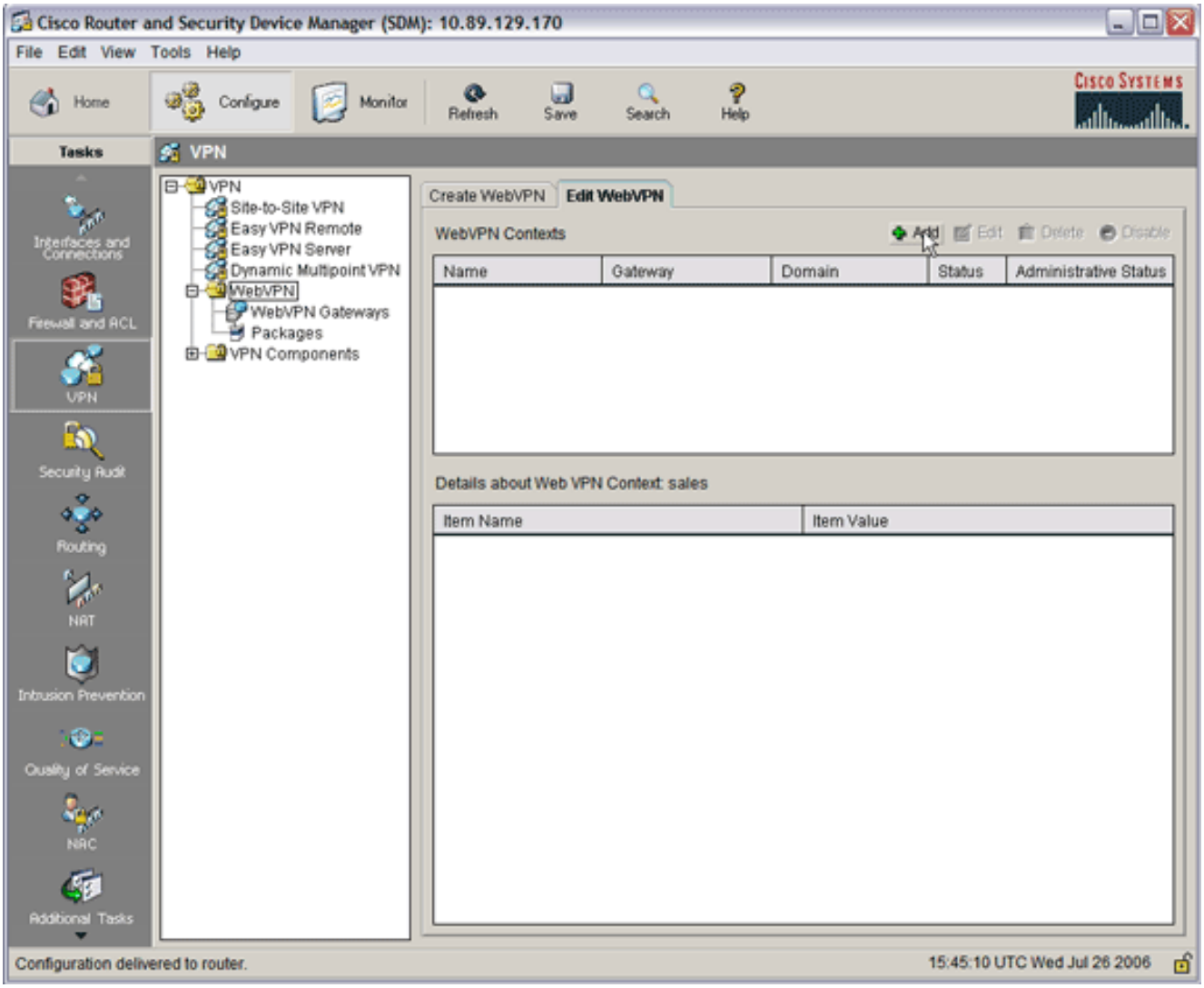
## Passo 2. Configurar os Recursos Permitidos para o Grupo de Políticas

Para facilitar adicionar recursos a um grupo de políticas, você pode configurar os recursos antes de criar o grupo de políticas.

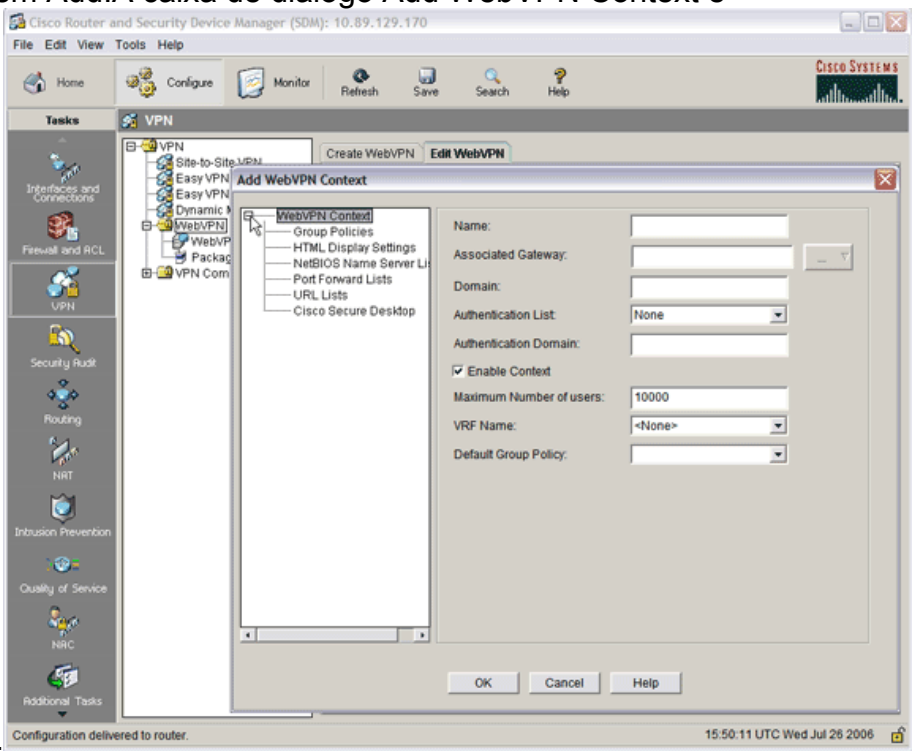
Execute estes passos para configurar os recursos permitidos o grupo de políticas:

1. Clique em **Configure** e clique em **VPN**. 

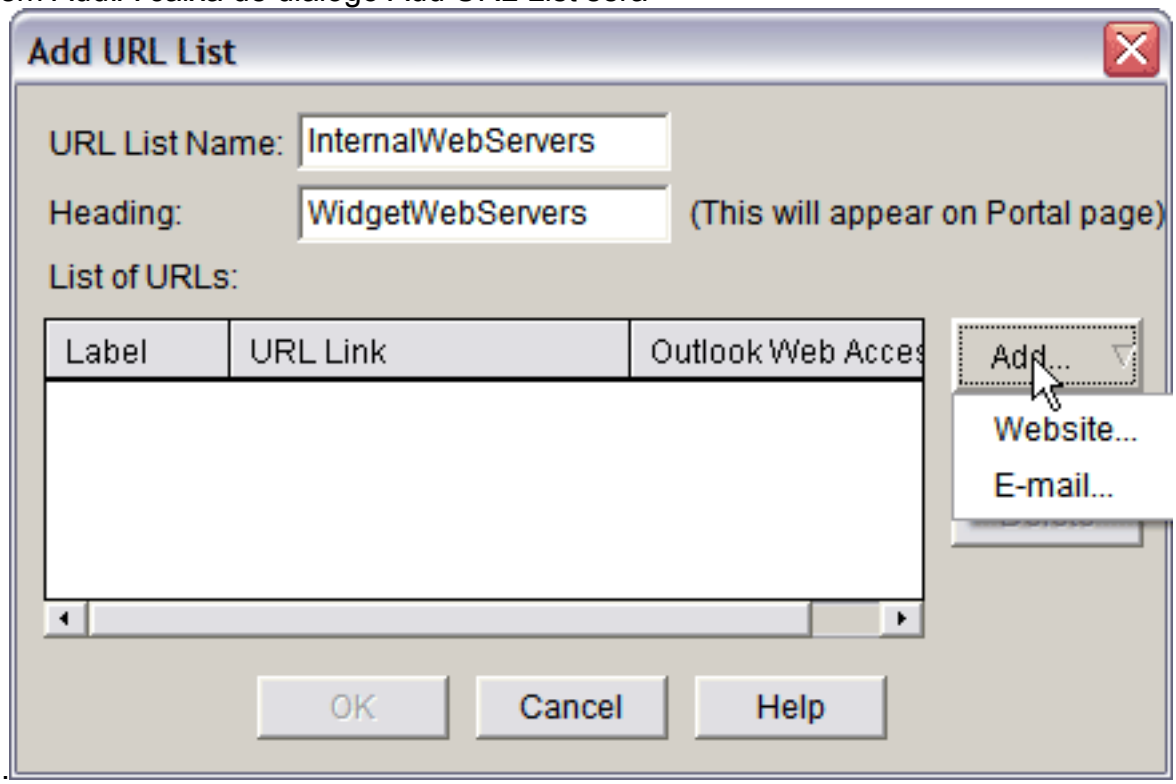
2. Escolha **WebVPN** e clique na guia **Edit WebVPN**.**Nota:** A WebVPN permite que você configure acesso para HTTP, HTTPS, navegação de arquivos do Windows através do protocolo Common Internet File System (CIFS) e Citrix.



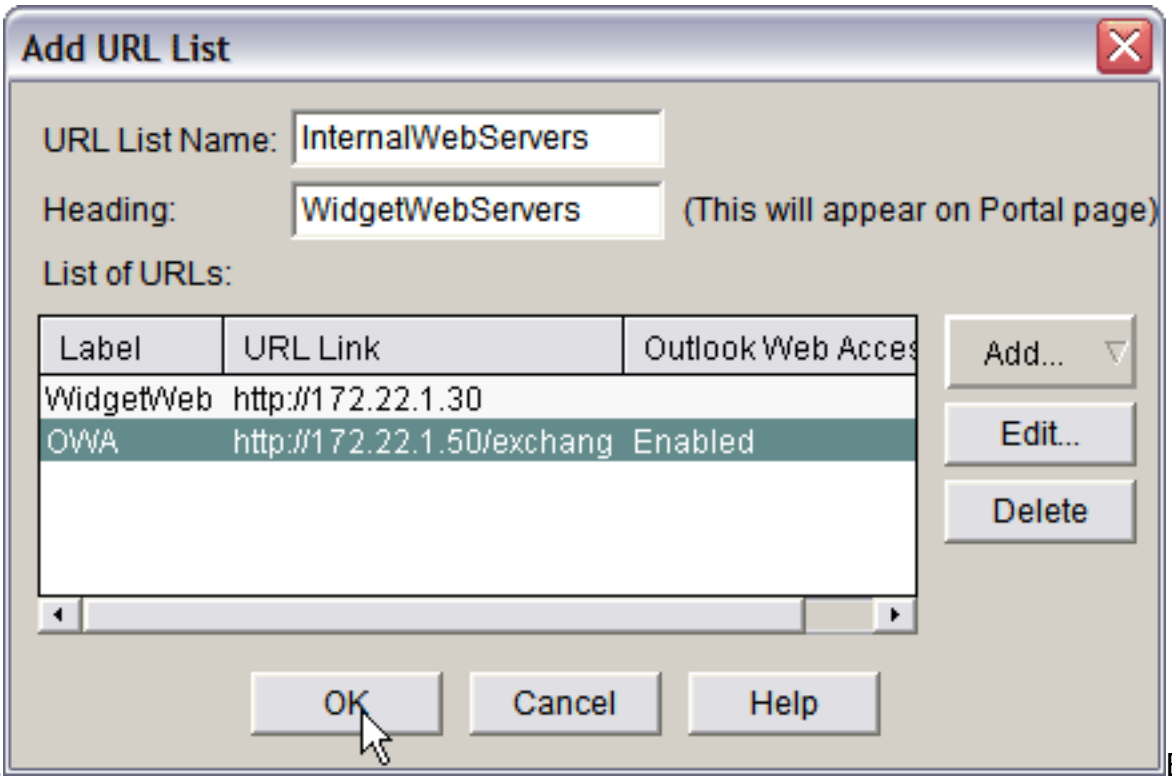

3. Clique em Add.A caixa de diálogo Add WebVPN Context é exibida.



4. Expanda **WebVPN Context** e escolha **URL Lists**.
5. Clique em Add.A caixa de diálogo Add URL List será exibida.

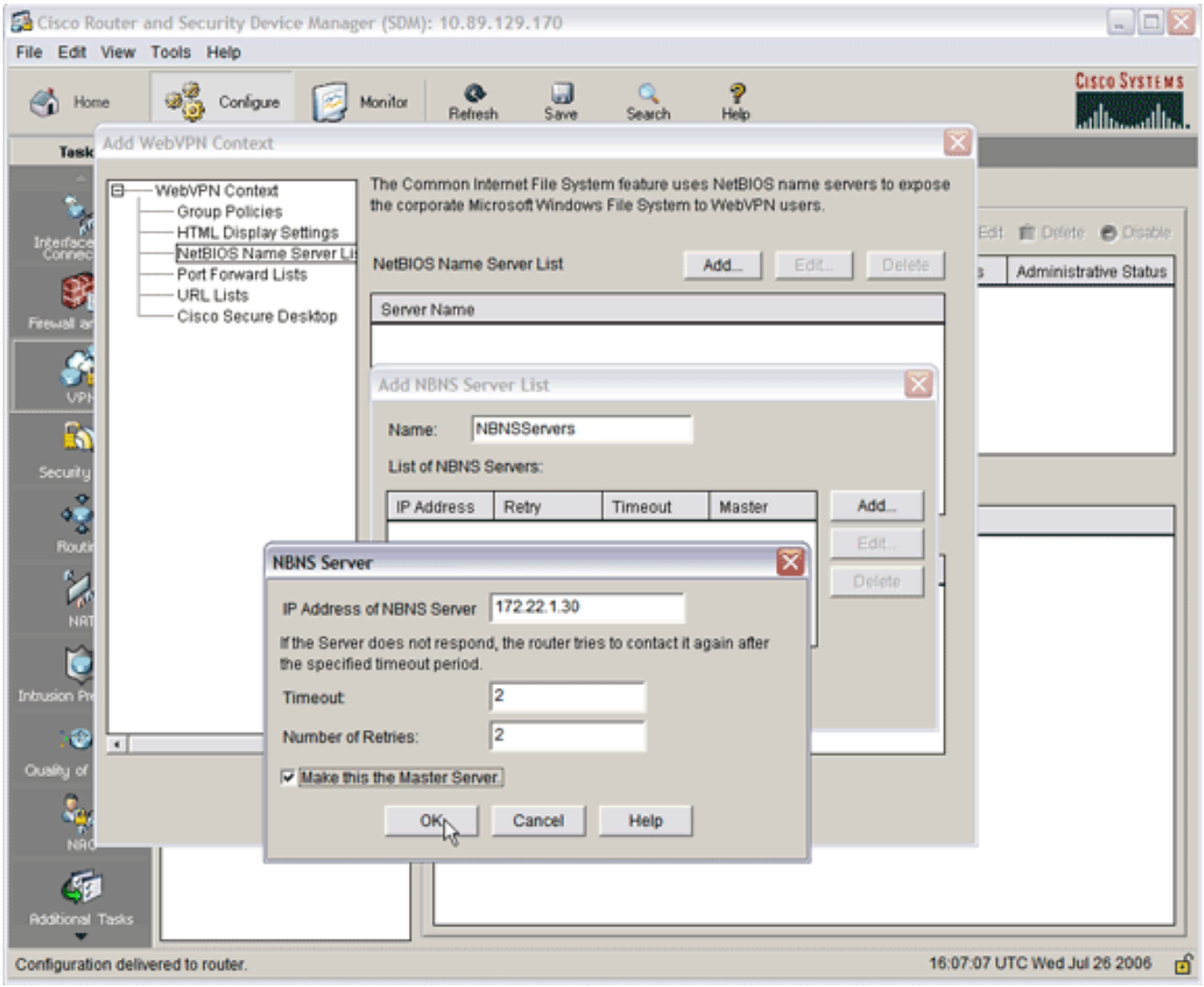



6. Insira valores nos campos URL List Name e Heading.
7. Clique em **Add** e escolha **Website**.




Esta lista contém todos os servidores Web HTTP e HTTPS que você deseja disponibilizar para esta conexão WebVPN.
8. Para adicionar acesso ao Outlook Web Access (OWA), clique em **Add**, escolha **E-mail** e clique em **OK** após preencher todos os campos desejados.
9. Para permitir a navegação de arquivos do Windows através do CIFS, você pode designar um servidor NetBIOS Name Service (NBNS) e configurar os compartilhamentos apropriados no domínio do Windows em ordem.Na lista WebVPN Context, escolha **NetBIOS Name**

**Server Lists**.Clique em Add.A caixa de diálogo Add NBNS Server List é exibida.Insira um nome para a lista e clique em **Add**.A caixa de diálogo NBNS Server será exibida.

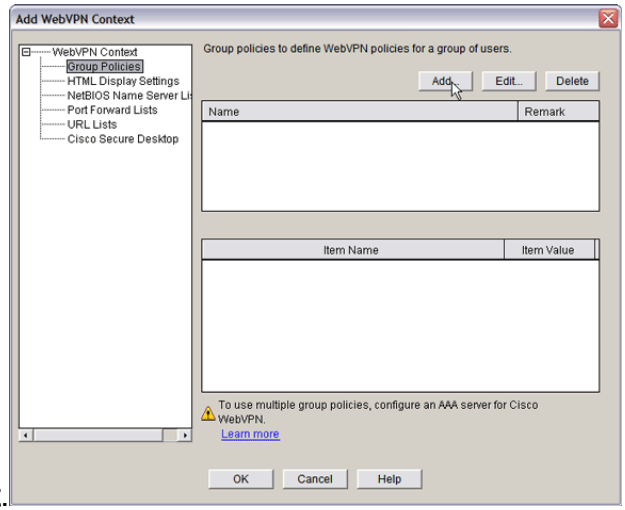



Se aplicável, marque a caixa de seleção **Make This the Master Server**.Clique em **OK** e, em seguida, clique em **OK**.

## Passo 3. Configurar o Grupo de Políticas WebVPN e Selecionar os Recursos

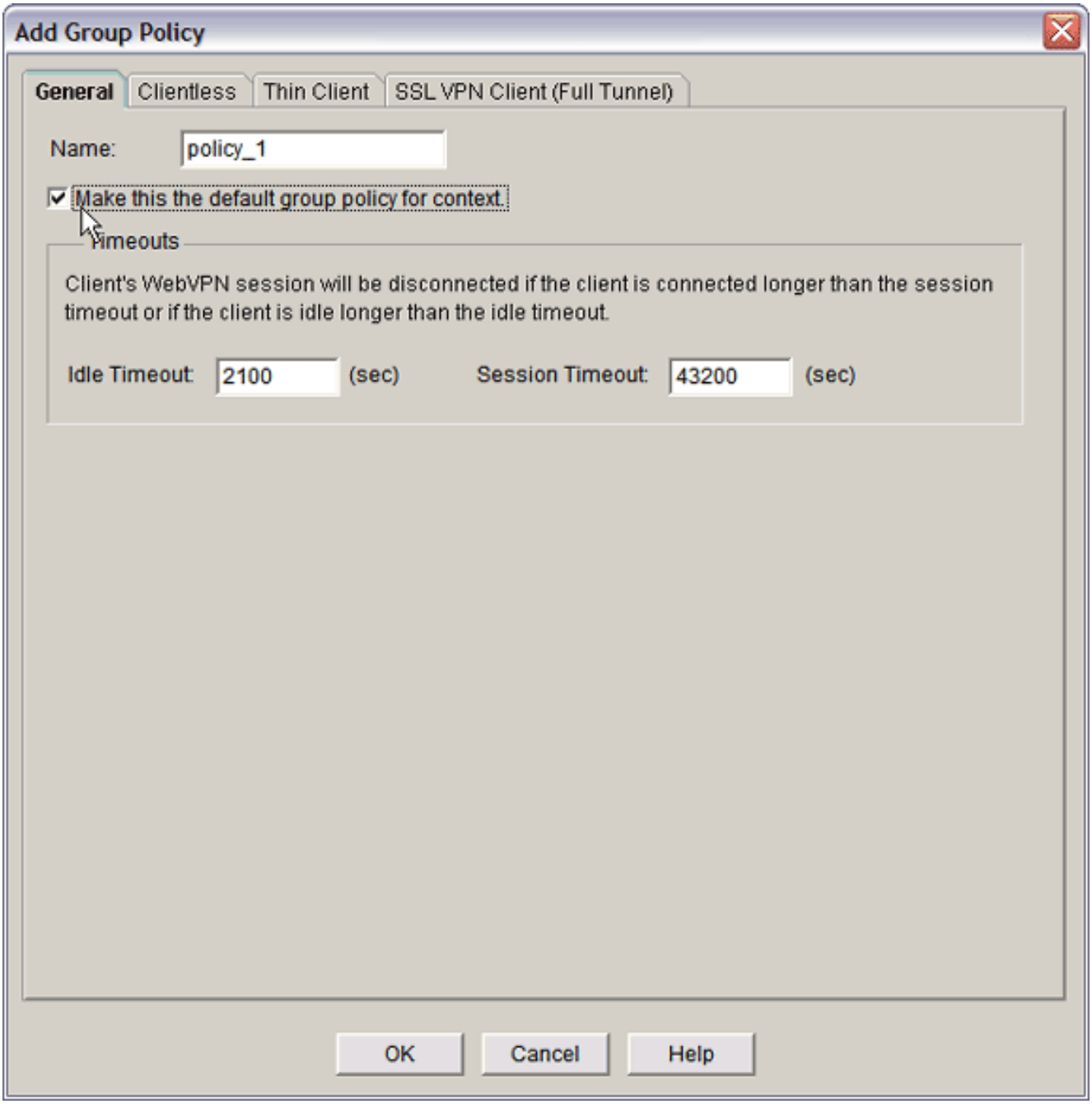
Execute estes passos para configurar o grupo de políticas WebVPN e selecionar os recursos:

1. Clique em **Configure** e clique em **VPN**.

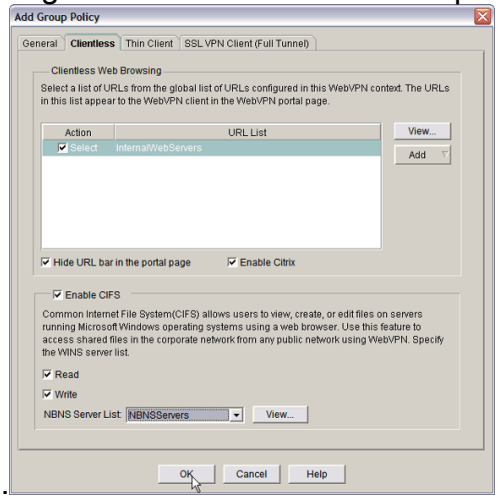



2. Expanda **WebVPN** e escolha **WebVPN Context**.

3. Escolha **Group Policies** e o clique em **Add**.A caixa de diálogo Add Group Policy é exibida.




4. Insira um nome para a nova política e selecione **Make this the default group policy para a** caixa de seleção de **contexto**.
5. Clique na guia **Clientless** localizada na parte superior da caixa de diálogo.

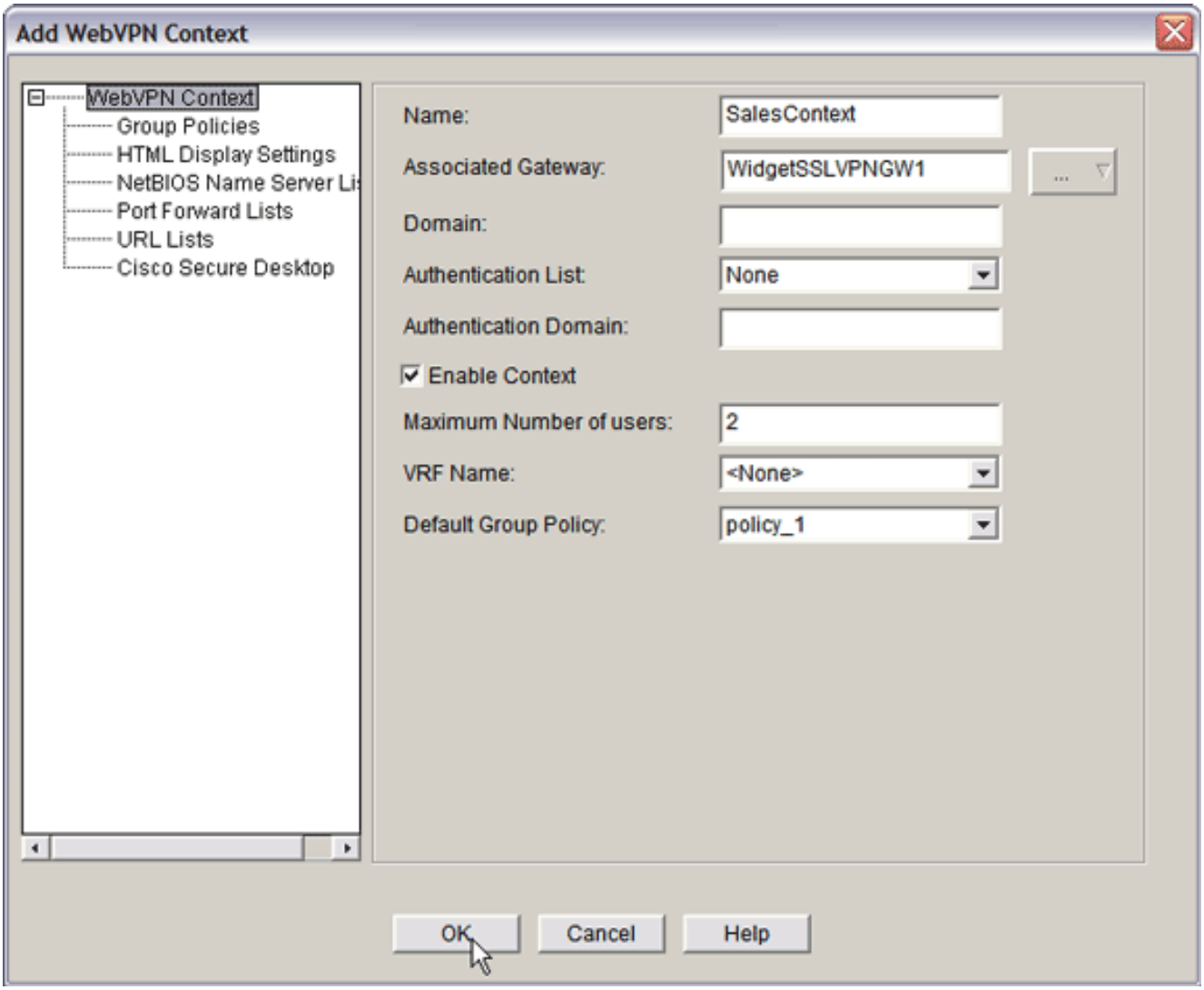


6. Marque a caixa de seleção **Select** para a URL List desejada.
7. Se seus clientes usam clientes Citrix que precisam de acesso a servidores Citrix, marque a caixa de seleção **Enable Citrix**.
8. Marque as caixas de seleção **Enable CIFS**, **Read** e **Write** .
9. Clique na seta suspensa **NBNS Server Lista**, e escolha a lista de servidores NBNS que você criou para a navegação de arquivos do Windows no Passo 2.
10. Clique em **OK**.

## Passo 4. Configurar o Contexto WebVPN

Para vincular gateway WebVPN, política do grupos e recursos, você deve configurar o contexto WebVPN. Para configurar o contexto WebVPN, execute estes passos:

1. Escolha **WebVPN Context** e insira um nome para o contexto.




2. Clique na seta suspensa de Associates Gateway e escolha um gateway associado.
3. Se você pretende criar mais de um contexto, insira um nome exclusivo no campo Domain para identificar este contexto. Se você deixar o campo Domain em branco, os usuários deverão acessar a WebVPN com **https://EndereçoIP**. Se você inserir um nome de domínio (por exemplo, *Vendas*), os usuários deverão conectar com **https://EndereçoIP/Vendas**.
4. Marque a caixa de seleção **Enable Context**.
5. No campo Maximum Number of Users, insira o número máximo de usuários permitido pela

licença de dispositivos.

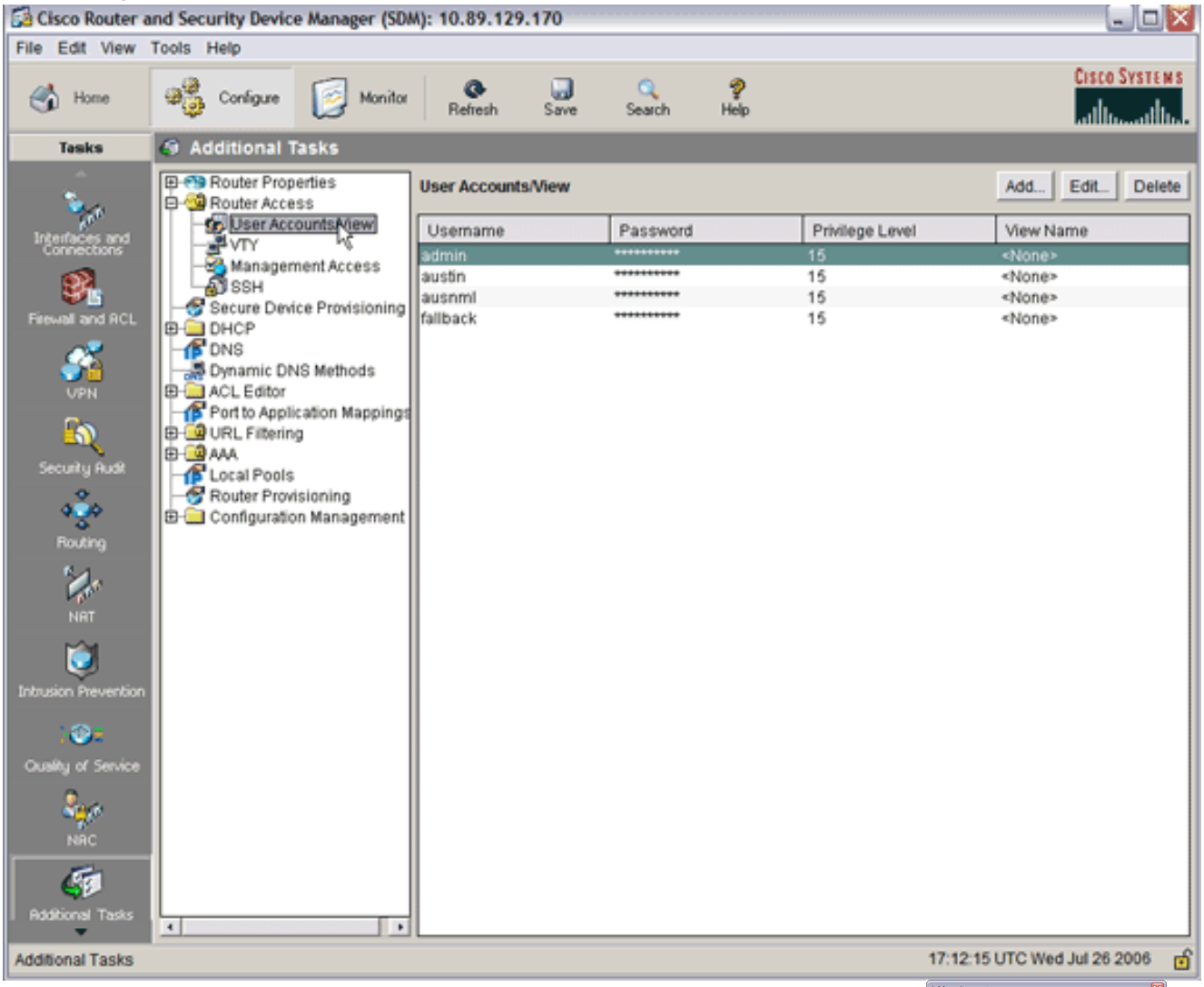
6. Clique na seta suspensa **Default Group policy** e selecione a política de grupo a ser associada a este contexto.
7. Clique em **OK** e, em seguida, clique em **OK**.

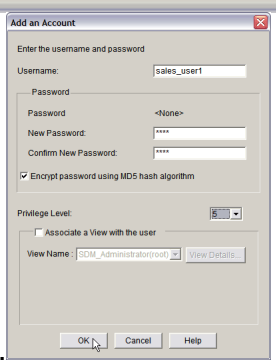
## Passo 5. Configurar o Banco de Dados de Usuários e o Método de Autenticação

Você pode configurar sessões VPN SSL Sem Clientes (WebVPN) para autenticar com o Radius, o Cisco AAA Server ou um banco de dados local. Este exemplo usa um banco de dados local.

Execute estes passos para configurar o banco de dados de usuários e o método de autenticação:

1. Clique em **Configuration** e em **Additional Tasks**.
2. Expanda **Router Access** e escolha **User Accounts/View**.




3. Clique no botão Adicionar.A caixa de diálogo Add an Account é exibida.

4. Insira uma conta de usuário e uma senha.
5. Clique em **OK** e, em seguida, clique em **OK**.
6. Clique em **Save** e, em seguida, clique em **Yes** para aceitar as alterações.

### Resultados

O ASDM cria estas configurações de linha de comando:

```
ausnml-3825-01
```

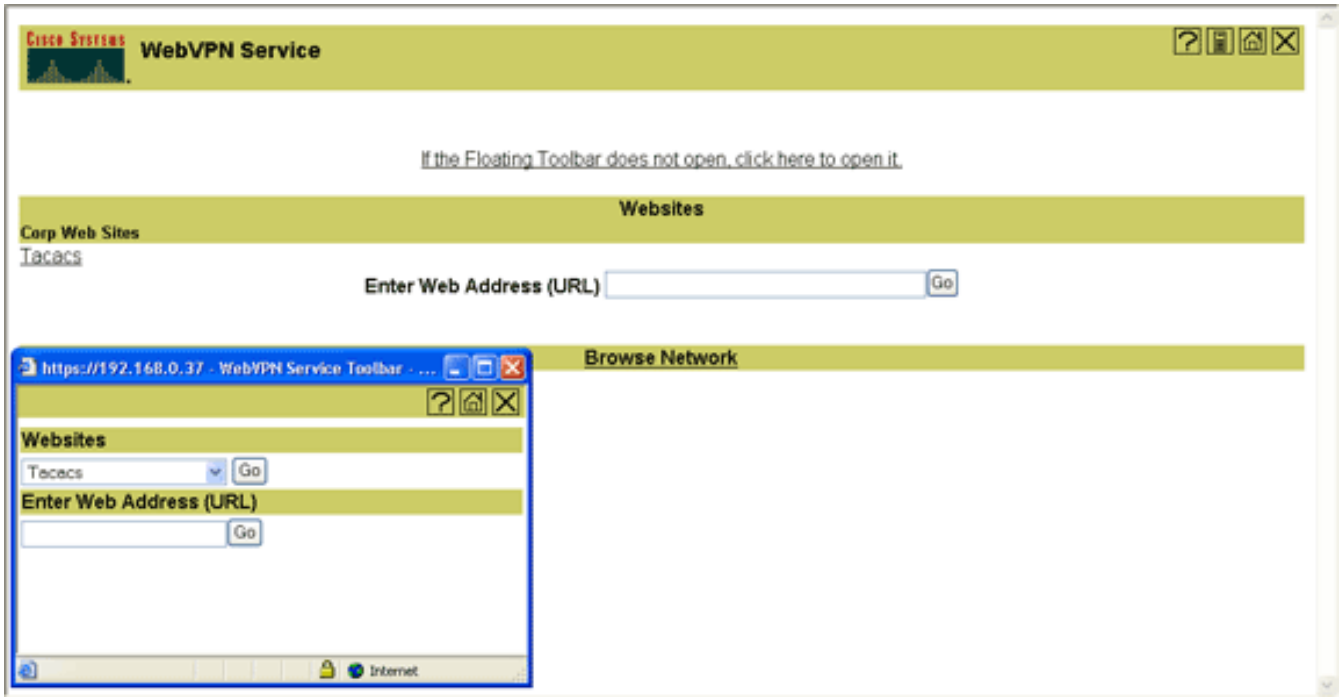
## Verificar

Use esta seção para confirmar se a sua configuração funciona corretamente.

### Procedimento

Execute estes procedimentos para confirmar se a sua configuração está funcionando corretamente:

- Teste sua configuração com um usuário. Insira **https://WebVPN_Gateway_Endereço_IP em um** navegador da Web com SSL habilitado; onde *WebVPN_Gateway_Endereço_IP* é o endereço IP do serviço WebVPN. Após você aceitar o certificado e inserir um nome de usuário e uma senha, uma tela semelhante a esta imagem deverá ser exibida.




- Verifique a sessão VPN SSL. No aplicativo SDM, clique no botão **Monitor** e, em seguida, clique em **VPN Status**. Expanda **WebVPN (All Contexts)**, expanda o contexto apropriado e escolha **Users**.
- Verifique as mensagens de erro. No aplicativo SDM, clique no botão **Monitor**, clique em **Logging** e clique na guia **Syslog**.
- Consulte a configuração running para o dispositivo. No aplicativo SDM, clique no **botão Configure** e clique em **Additional Tasks**. Expanda **Configuration Management** e escolha

Config Editor.

### Comandos

Vários **comandos show** estão associados ao WebVPN. Você pode executar estes comandos na interface de linha de comando (CLI) para mostrar estatísticas e outras informações. Para obter informações detalhadas sobre os **comandos show**, consulte Verificação da Configuração do WebVPN.

**Nota:** A Output Interpreter Tool (apenas para clientes registrados) (OIT) suporta determinados comandos show. Use a OIT para exibir uma análise da saída do comando show.

## Troubleshooting

Use esta seção para resolver problemas de configuração.

**Nota:** Não interrompa o comando **Copy File to Server** ou navegue para uma janela diferente enquanto a cópia estiver em andamento. A interrupção da operação pode fazer com que um arquivo incompleto seja salvo no servidor.

**Nota:** Os usuários podem carregar e baixar os novos arquivos usando o cliente WebVPN, mas o usuário não pode substituir os arquivos no Common Internet File System (CIFS) na WebVPN usando o comando **Copy File to Server**. O usuário recebe esta mensagem quando ele tenta substituir um arquivo no servidor:

### Procedimento

Execute estes passos para fazer troubleshoot da sua configuração:

1. Certifique-se de que os clientes desabilitem bloqueadores de pop-up.
2. Certifique-se de que os clientes possuam cookies habilitados.
3. Certifique-se de que os clientes usem os navegadores da Web Netscape, Internet Explorer, Firefox ou Mozilla.

### Comandos

Vários **comandos debug** estão associados ao WebVPN. Consulte Usando Comandos de Depuração da WebVPN para obter informações detalhadas sobre esses comandos.

**Nota:** O uso de **comandos debug** pode afetar negativamente seu dispositivo Cisco. Antes de utilizar **comandos debug**, consulte Informações Importantes sobre Comandos Debug.

## Informações Relacionadas

- Cisco IOS SSLVPN
- Perguntas e Respostas sobre a VPN SSL do Cisco IOS
- Exemplo de Configuração de VPN SSL com Thin-Client (WebVPN) no Cisco IOS com SDM
- Exemplo de Configuração de Cliente VPN SSL (SVC) no IOS com SDM

- Suporte Técnico e Documentação - Cisco Systems