Clientless SSL VPN (WebVPN) on Cisco IOS Using SDM Configuration Example

Document ID: 70663

Contents

Introduction

Clientless SSL VPN (WebVPN) allows a user to securely access resources on the corporate LAN from anywhere with an SSL−enabled Web browser. The user first authenticates with a WebVPN gateway which then allows the user access to pre−configured network resources. WebVPN gateways can be configured on Cisco IOS® routers, Cisco Adaptive Security Appliances (ASA), Cisco VPN 3000 Concentrators, and the Cisco WebVPN Services Module for the Catalyst 6500 and 7600 Routers.

Secure Socket Layer (SSL) Virtual Private Network (VPN) technology can be configured on Cisco devices in three main modes: Clientless SSL VPN (WebVPN), Thin−Client SSL VPN (Port Forwarding), and SSL VPN Client (SVC) mode. This document demonstrates the configuration of theWebVPN on Cisco IOS routers.

Note: Do not to change either the IP domain name or the host name of the router as this will trigger a regeneration of the self−signed certificate and will override the configured trustpoint. Regeneration of the self−signed certificate causes connection issues if the router has been configured for WebVPN. WebVPN ties the SSL trustpoint name to the WebVPN gateway configuration. Therefore, if a new self−signed certificate is issued, the new trustpoint name does not match the WebVPN configuration and users are unable to connect.

Note: If you run the **ip https−secure server** command on a WebVPN router that uses a persistent self−signed certificate, a new RSA key is generated and the certificate becomes invalid. A new trustpoint is created, which breaks SSL WebVPN. If the router that uses the persistent self−signed certificate reboots after you run the **ip https−secure server** command, the same issue occurs.

Refer to Thin−Client SSL VPN (WebVPN) IOS Configuration Example with SDM in order to learn more about the thin−client SSL VPN.

Refer to SSL VPN Client (SVC) on IOS with SDM Configuration Example in order to learn more about the SSL VPN Client.

SSL VPN runs on these Cisco Router platforms:

- Cisco 870, 1811, 1841, 2801, 2811, 2821 and 2851 series routers
- Cisco 3725, 3745, 3825, 3845, 7200 and 7301 series routers

Prerequisites

Requirements

Ensure that you meet these requirements before you attempt this configuration:

- An advanced image of Cisco IOS Software Release 12.4(6)T or later
- One of the Cisco router platforms listed in the Introduction

Components Used

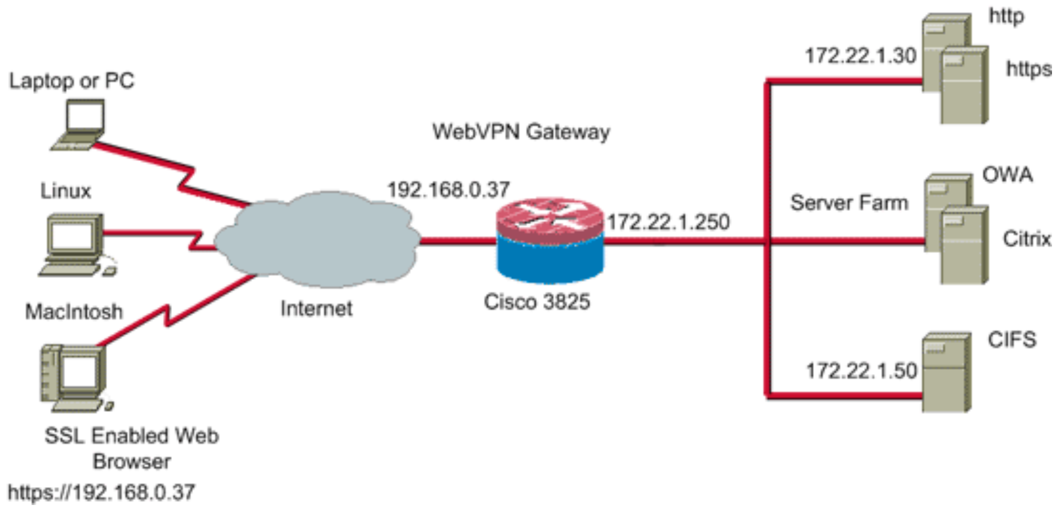
The information in this document is based on these software and hardware versions:

- Cisco 3825 router
- Advanced Enterprise software image − Cisco IOS Software Release 12.4(9)T
- Cisco Router and Security Device Manager (SDM) − version 2.3.1

The information in this document was created from the devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If your network is live, make sure that you understand the potential impact of any command. The IP addresses used in this example are taken from RFC 1918 addresses which are private and not legal to use on the Internet.

Network Diagram

This document uses this network setup:



Conventions

Refer to the Cisco Technical Tips Conventions for more information on document conventions.

Preconfiguration Tasks

Before you begin, complete these tasks:

1. Configure a host name and domain name.
2. Configure the router for SDM. Cisco ships some routers with a preinstalled copy of SDM.

   If the Cisco SDM is not already loaded on your router, you can obtain a free copy of the software from Software Download (registered customers only) . You must have a CCO account with a service contract. For detailed information on the installation and configuration of SDM, refer to Cisco Router and Security Device Manager.
3. Configure the correct date, time, and time zone for your router.

Configure WebVPN on Cisco IOS

You can have more than one WebVPN gateway associated with a device. Each WebVPN gateway is linked to only one IP address on the router. You can create more than one WebVPN context for a particular WebVPN gateway. To identify individual contexts, provide each context with a unique name. One policy group can be associated with only one WebVPN context. The policy group describes which resources are available in a particular WebVPN context.

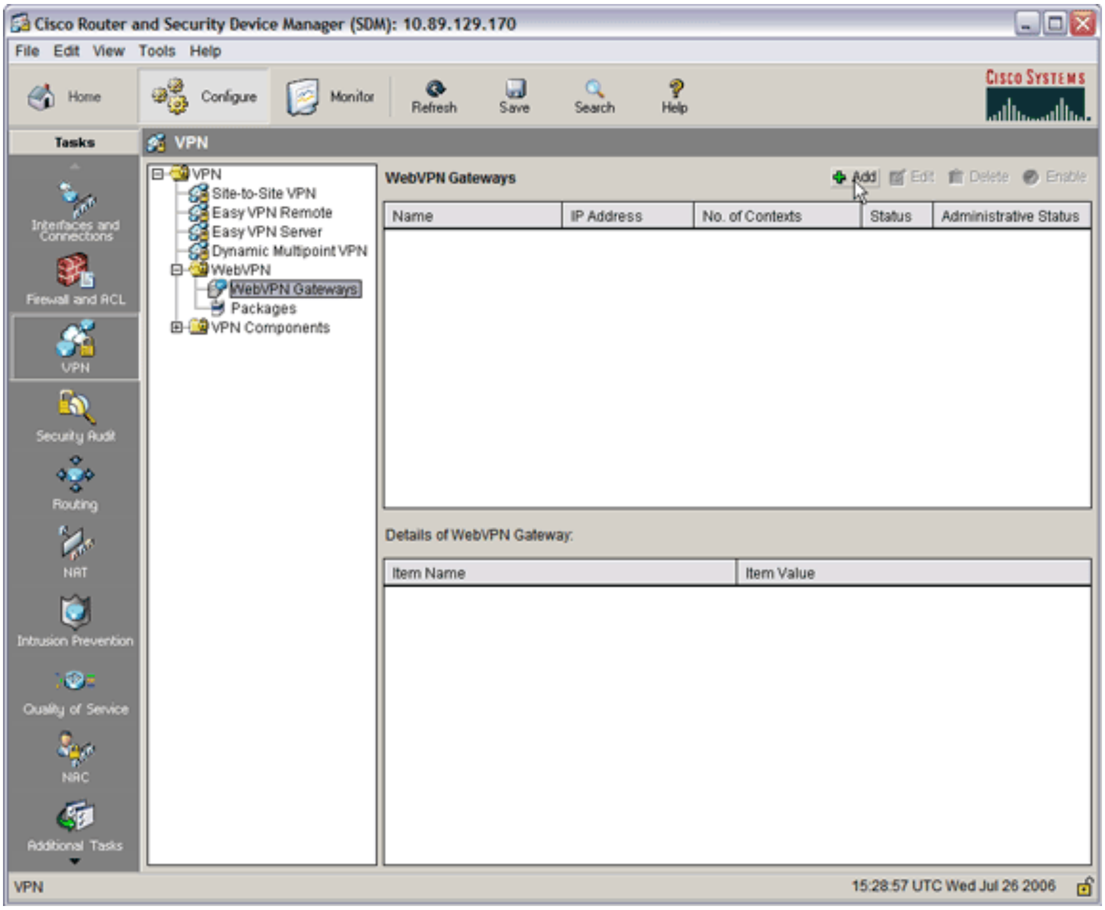
Complete these steps in order to configure WebVPN on Cisco IOS:

1. Configure the WebVPN Gateway
2. Configure the Resources Allowed for the Policy Group
3. Configure the WebVPN Policy Group and Select the Resources
4. Configure the WebVPN Context
5. Configure the User Database and Authentication Method

Step 1. Configure the WebVPN Gateway

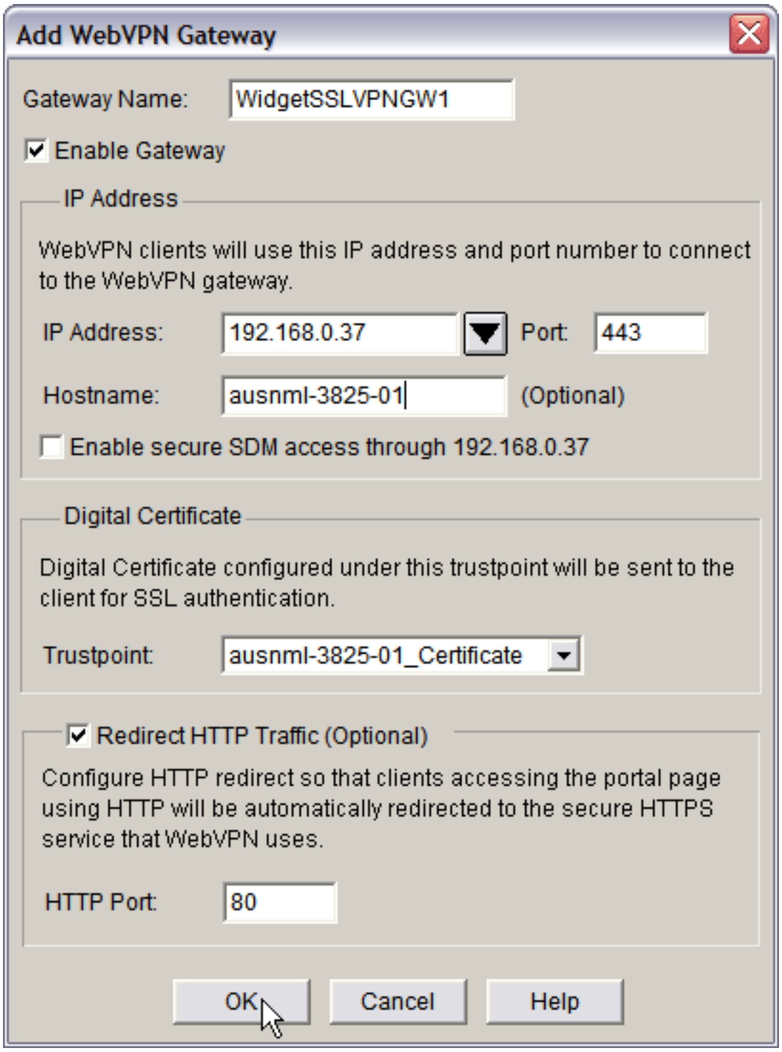
Complete these steps in order to configure the WebVPN Gateway:

1. Within the SDM application, click **Configure**, and then click **VPN**.
2. Expand **WebVPN**, and choose **WebVPN Gateways**.



3. Click **Add**.

   The Add WebVPN Gateway dialog box appears.



Add WebVPN Gateway

Gateway Name: WidgetSSLVPNGW1

☑ Enable Gateway

IP Address

WebVPN clients will use this IP address and port number to connect to the WebVPN gateway.

IP Address: 192.168.0.37 Port: 443

Hostname: ausnml-3825-01 (Optional)

☐ Enable secure SDM access through 192.168.0.37

Digital Certificate

Digital Certificate configured under this trustpoint will be sent to the client for SSL authentication.

Trustpoint: ausnml-3825-01_Certificate

☑ Redirect HTTP Traffic (Optional)

Configure HTTP redirect so that clients accessing the portal page using HTTP will be automatically redirected to the secure HTTPS service that WebVPN uses.

HTTP Port: 80

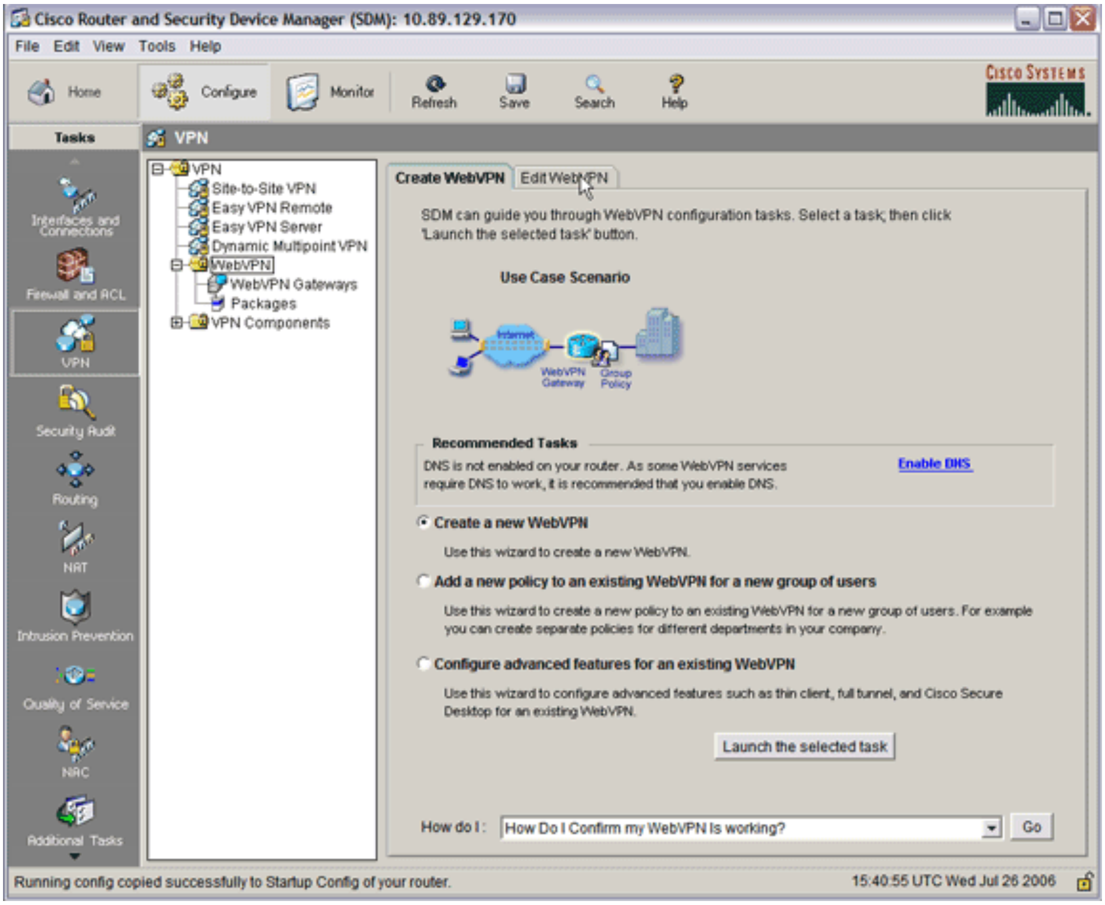
4. Enter values in the Gateway Name and IP Address fields, and then check the **Enable Gateway** check box.
5. Check the **Redirect HTTP Traffic** check box, and then click **OK**.
6. Click **Save**, and then click **Yes** to accept the changes.

Step 2. Configure the Resources Allowed for the Policy Group

In order to make it easier to add resources to a policy group, you can configure the resources before you create the policy group.

Complete these steps in order to configure the resources allowed for the policy group:

1. Click **Configure**, and then click **VPN**.



SDM can guide you through WebVPN configuration tasks. Select a task, then click 'Launch the selected task' button.

Use Case Scenario

Recommended Tasks

DNS is not enabled on your router. As some WebVPN services require DNS to work, it is recommended that you enable DNS. Enable DNS

● Create a new WebVPN

Use this wizard to create a new WebVPN.

○ Add a new policy to an existing WebVPN for a new group of users

Use this wizard to create a new policy to an existing WebVPN for a new group of users. For example you can create separate policies for different departments in your company.

○ Configure advanced features for an existing WebVPN

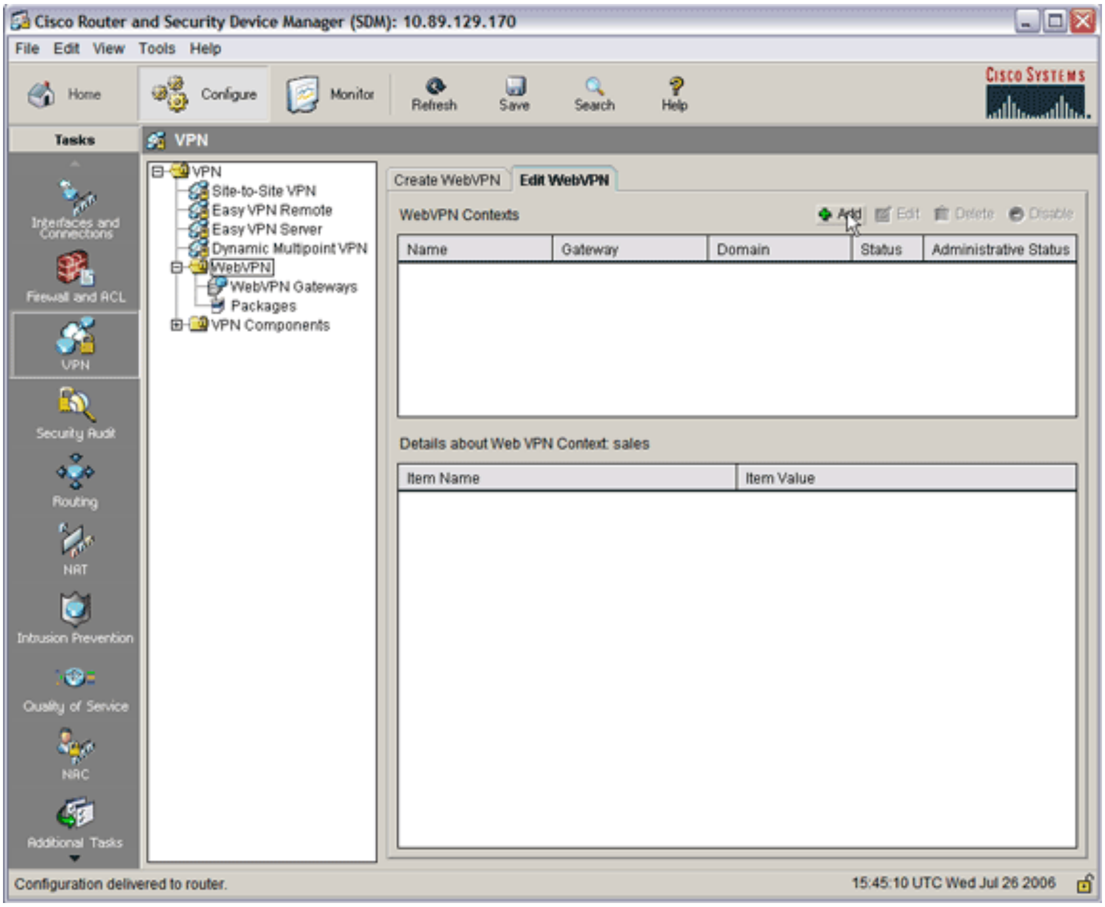
Use this wizard to configure advanced features such as thin client, full tunnel, and Cisco Secure Desktop for an existing WebVPN.

How do I: How Do I Confirm my WebVPN Is working?

Running config copied successfully to Startup Config of your router. 15:40:55 UTC Wed Jul 26 2006

2. Choose **WebVPN**, and then click the **Edit WebVPN** tab.

   Note: WebVPN allows you to configure access for HTTP, HTTPS, Windows file browsing through the Common Internet File System (CIFS) protocol, and Citrix.



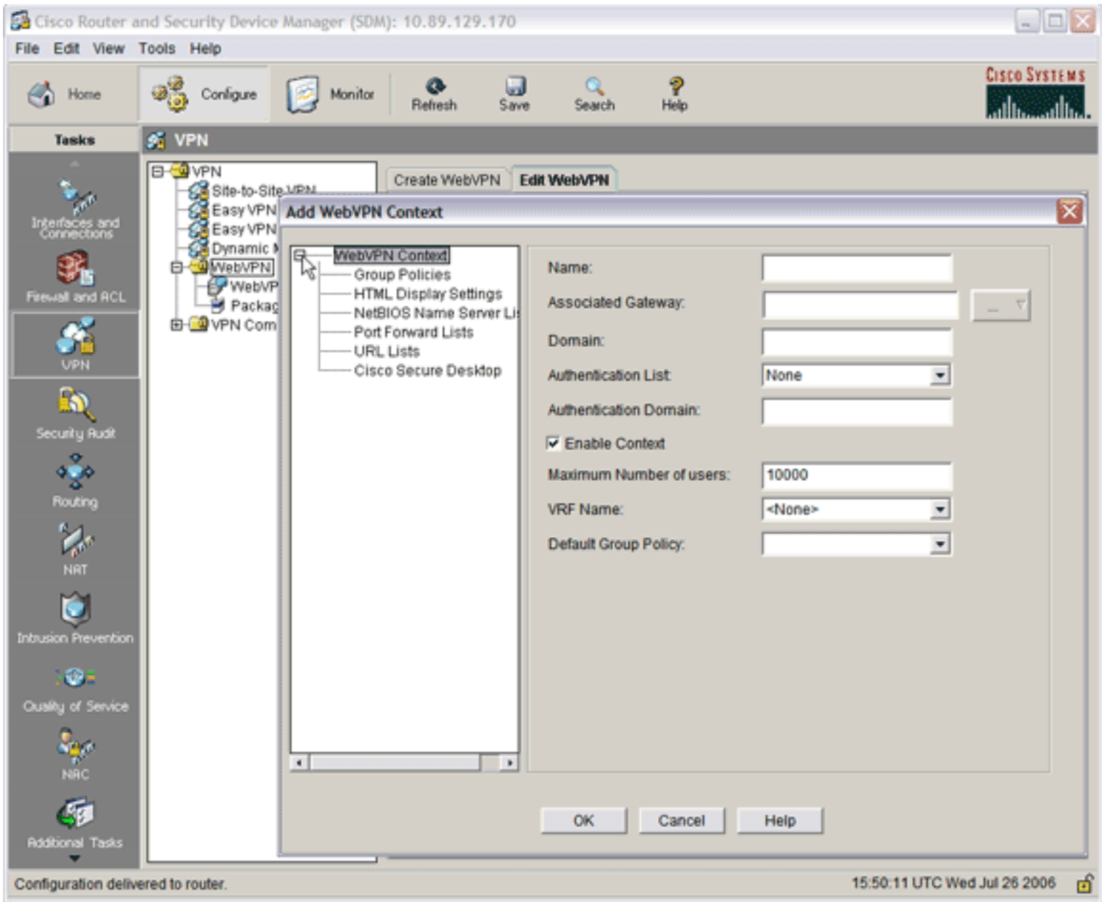
Details about Web VPN Context: sales

Configuration delivered to router.

15:45:10 UTC Wed Jul 26 2006

3. Click **Add**.

   The Add WebVPN Context dialog box appears.



Name:

Associated Gateway:

Domain:

Authentication List: None

Authentication Domain:

☑ Enable Context

Maximum Number of users: 10000

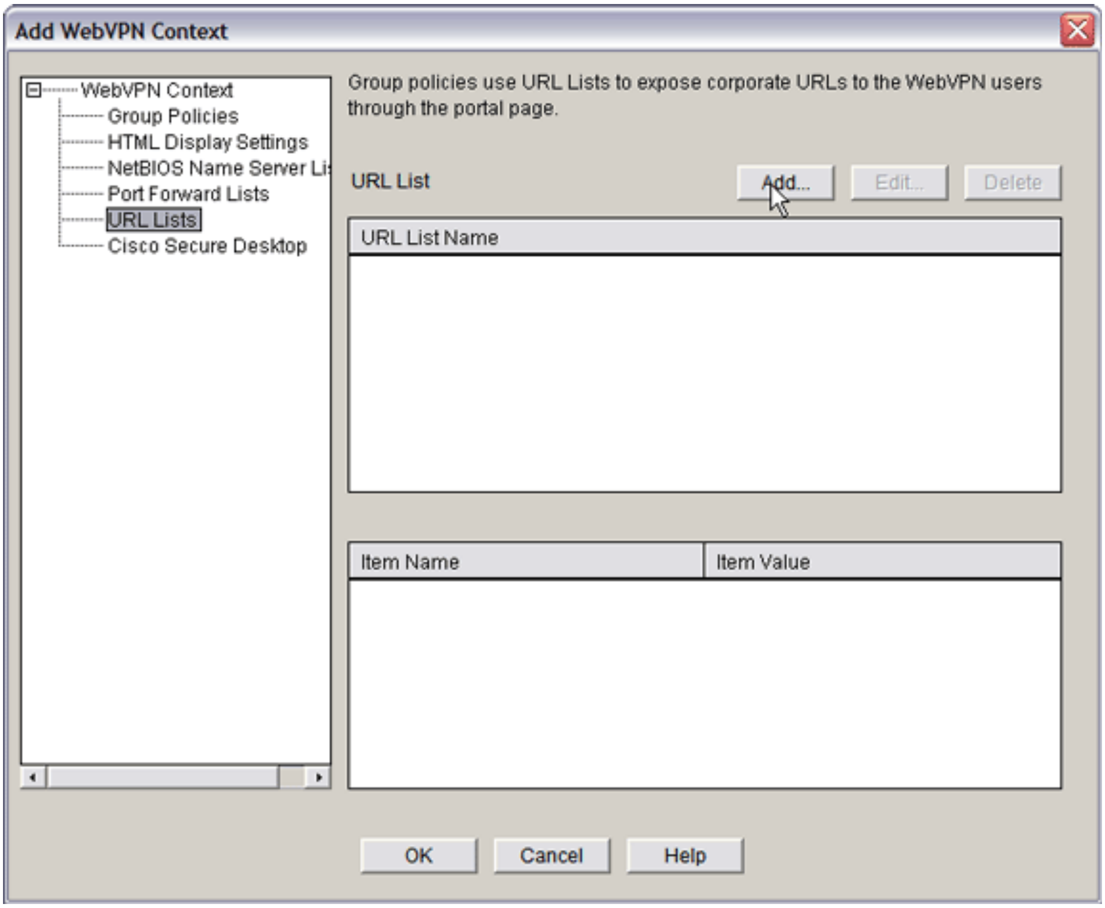
VRF Name: <None>

Default Group Policy:

Configuration delivered to router.

15:50:11 UTC Wed Jul 26 2006

4. Expand **WebVPN Context**, and choose **URL Lists**.



Group policies use URL Lists to expose corporate URLs to the WebVPN users through the portal page.

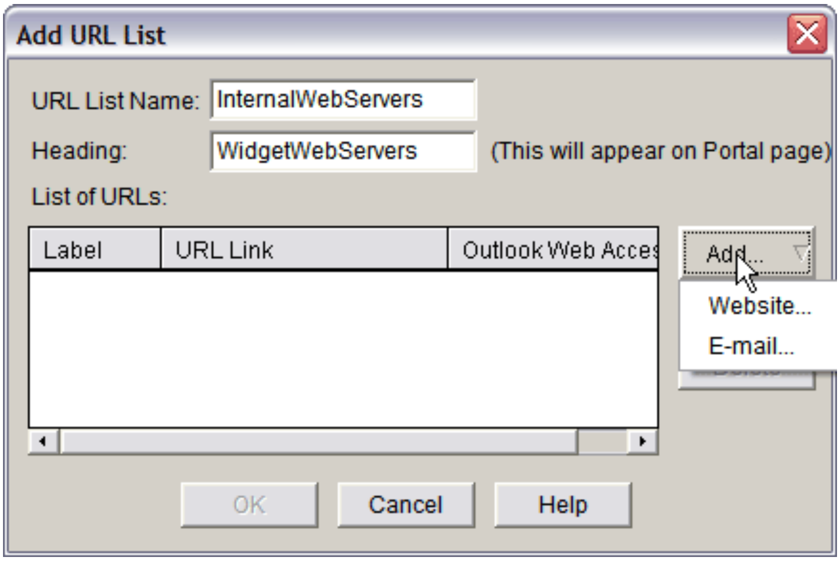
URL List

URL List Name

Item Name	Item Value

5. Click **Add**.

The Add URL List dialog box appears.



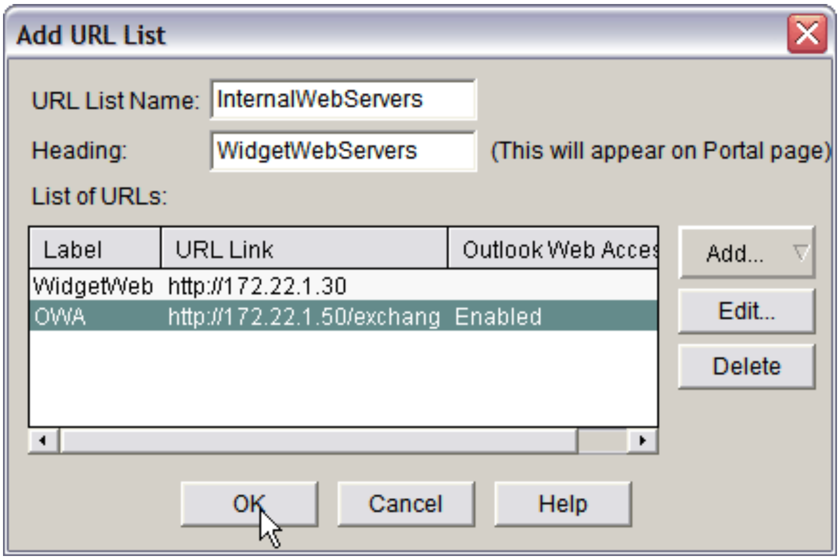
URL List Name: InternalWebServers

Heading: WidgetWebServers (This will appear on Portal page)

List of URLs:

Label	URL Link	Outlook Web Acces

6. Enter values in the URL List Name and Heading fields.
7. Click **Add**, and choose **Website**.



URL List Name: InternalWebServers

Heading: WidgetWebServers (This will appear on Portal page)

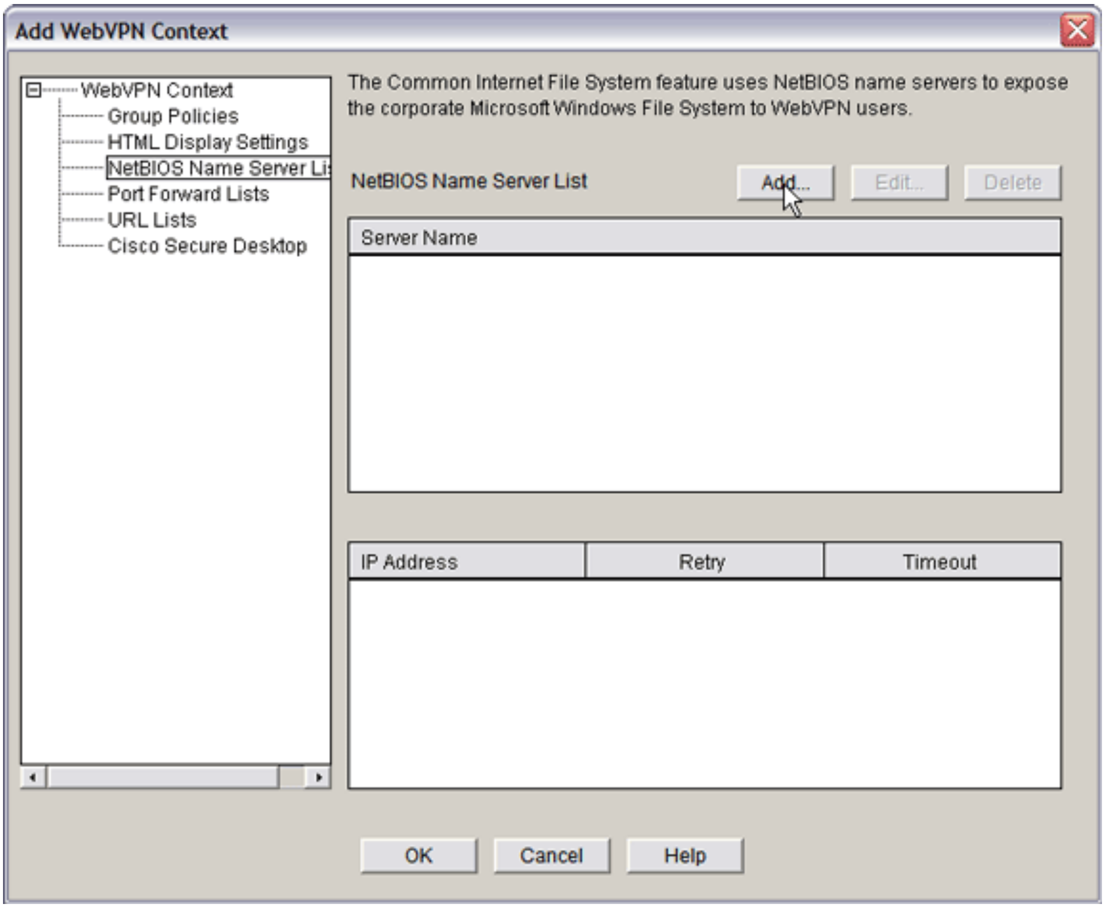
List of URLs:

Label	URL Link	Outlook Web Acces
WidgetWeb	http://172.22.1.30	
OWA	http://172.22.1.50/exchang	Enabled

This list contains all the HTTP and HTTPS Web servers that you want to be available for this WebVPN connection.

8. In order to add access for Outlook Web Access (OWA), click **Add**, choose **E−mail**, and then click **OK** after you have filled in all the desired fields.
9. In order to allow Windows file browsing through CIFS, you can designate an NetBIOS Name Service (NBNS) server and configure the appropriate shares in the Windows domain in order.

   a. From the WebVPN Context list, choose **NetBIOS Name Server Lists**.



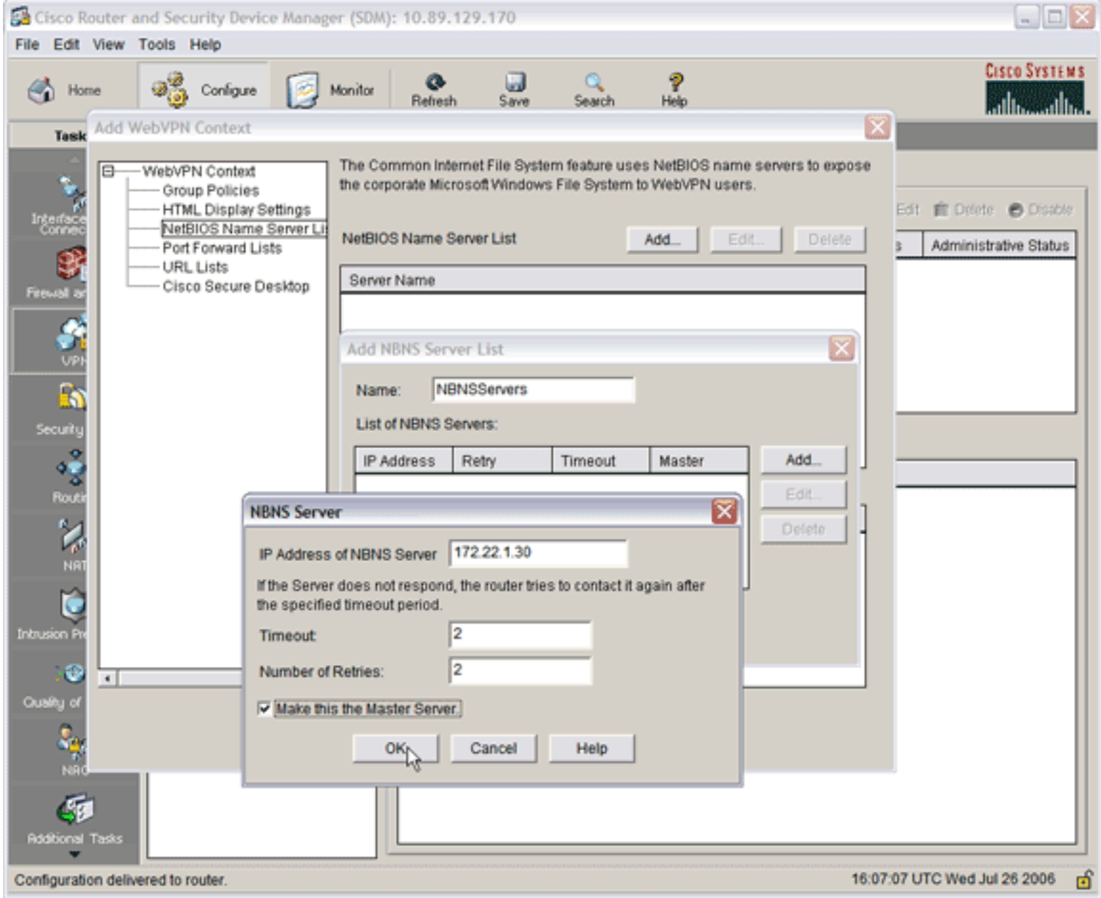
The Common Internet File System feature uses NetBIOS name servers to expose the corporate Microsoft Windows File System to WebVPN users.

b. Click **Add**.

The Add NBNS Server List dialog box appears.

c. Enter a name for the list, and click **Add**.

The NBNS Server dialog box appears.



The Common Internet File System feature uses NetBIOS name servers to expose the corporate Microsoft Windows File System to WebVPN users.

NetBIOS Name Server List

Name: NBNSServers

List of NBNS Servers:

IP Address of NBNS Server 172.22.1.30

If the Server does not respond, the router tries to contact it again after the specified timeout period.

Timeout 2

Number of Retries: 2

☑ Make this the Master Server.

Configuration delivered to router.

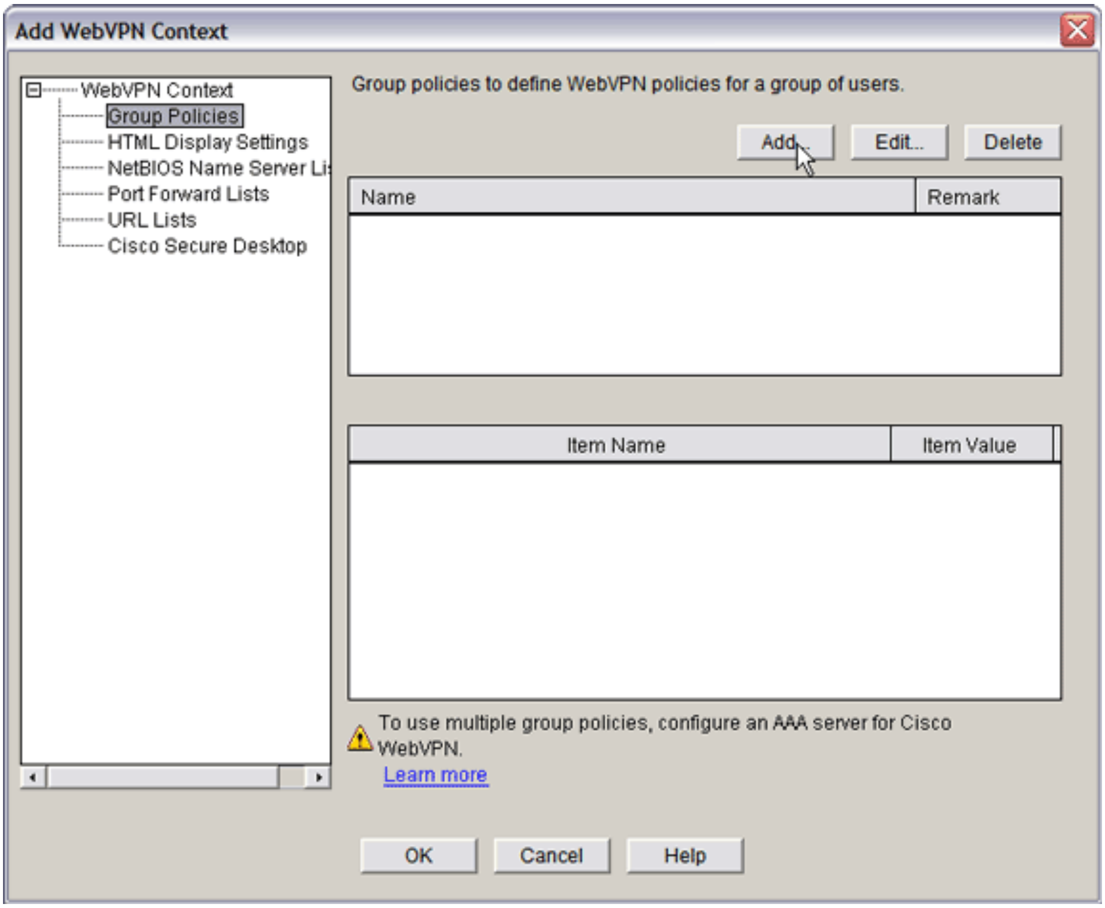
16:07:07 UTC Wed Jul 26 2006

d. If applicable, check the **Make This the Master Server** check box.
e. Click **OK**, and then click **OK**.

Step 3. Configure the WebVPN Policy Group and Select the Resources

Complete these steps in order to configure the WebVPN policy group and select the resources:

1. Click **Configure**, and then click **VPN**.
2. Expand **WebVPN**, and choose **WebVPN Context**.

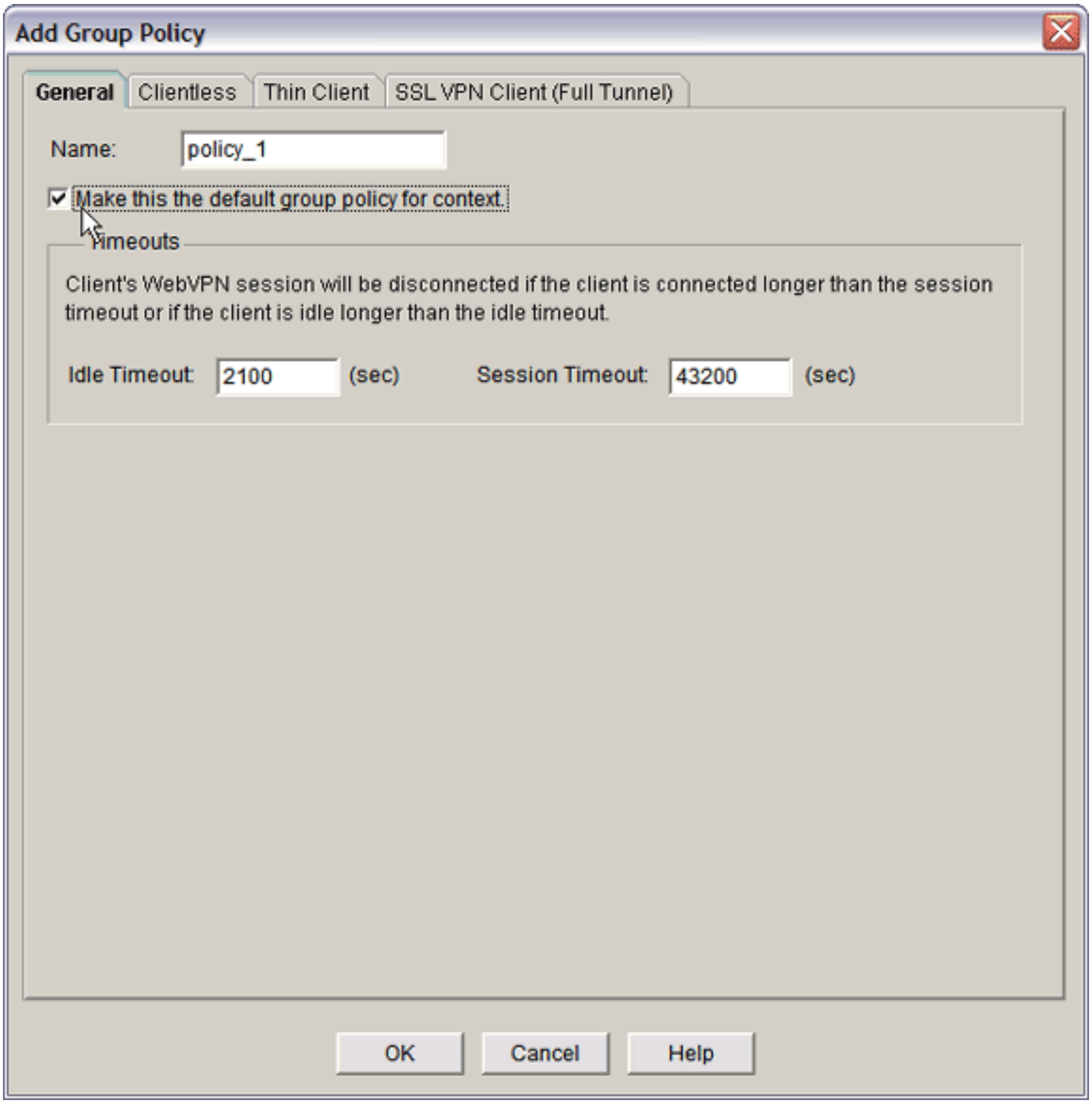


Group policies to define WebVPN policies for a group of users.

To use multiple group policies, configure an AAA server for Cisco WebVPN.

3. Choose **Group Policies**, and click **Add**.

   The Add Group Policy dialog box appears.



Add Group Policy

Name: policy_1

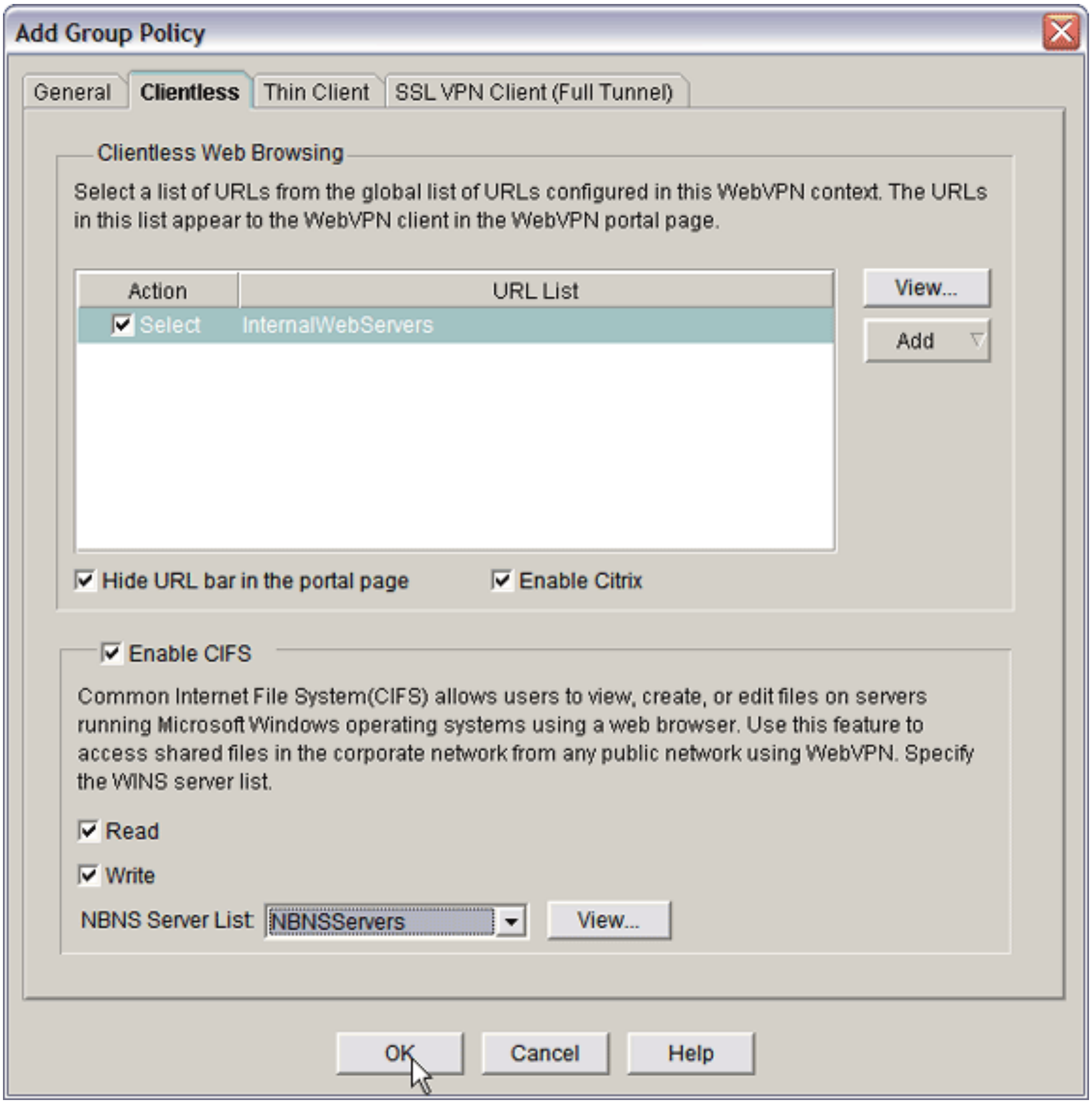
☑ Make this the default group policy for context.

Timeouts

Client's WebVPN session will be disconnected if the client is connected longer than the session timeout or if the client is idle longer than the idle timeout.

Idle Timeout: 2100 (sec) Session Timeout: 43200 (sec)

4. Enter a name for the new policy, and check the **Make this the default group policy for context** check box.
5. Click the **Clientless** tab located at the top of the dialog box.



Clientless Web Browsing

Select a list of URLs from the global list of URLs configured in this WebVPN context. The URLs in this list appear to the WebVPN client in the WebVPN portal page.

Action	URL List
☑ Select	InternalWebServers

☑ Hide URL bar in the portal page ☑ Enable Citrix

☑ Enable CIFS

Common Internet File System(CIFS) allows users to view, create, or edit files on servers running Microsoft Windows operating systems using a web browser. Use this feature to access shared files in the corporate network from any public network using WebVPN. Specify the WINS server list.

☑ Read

☑ Write

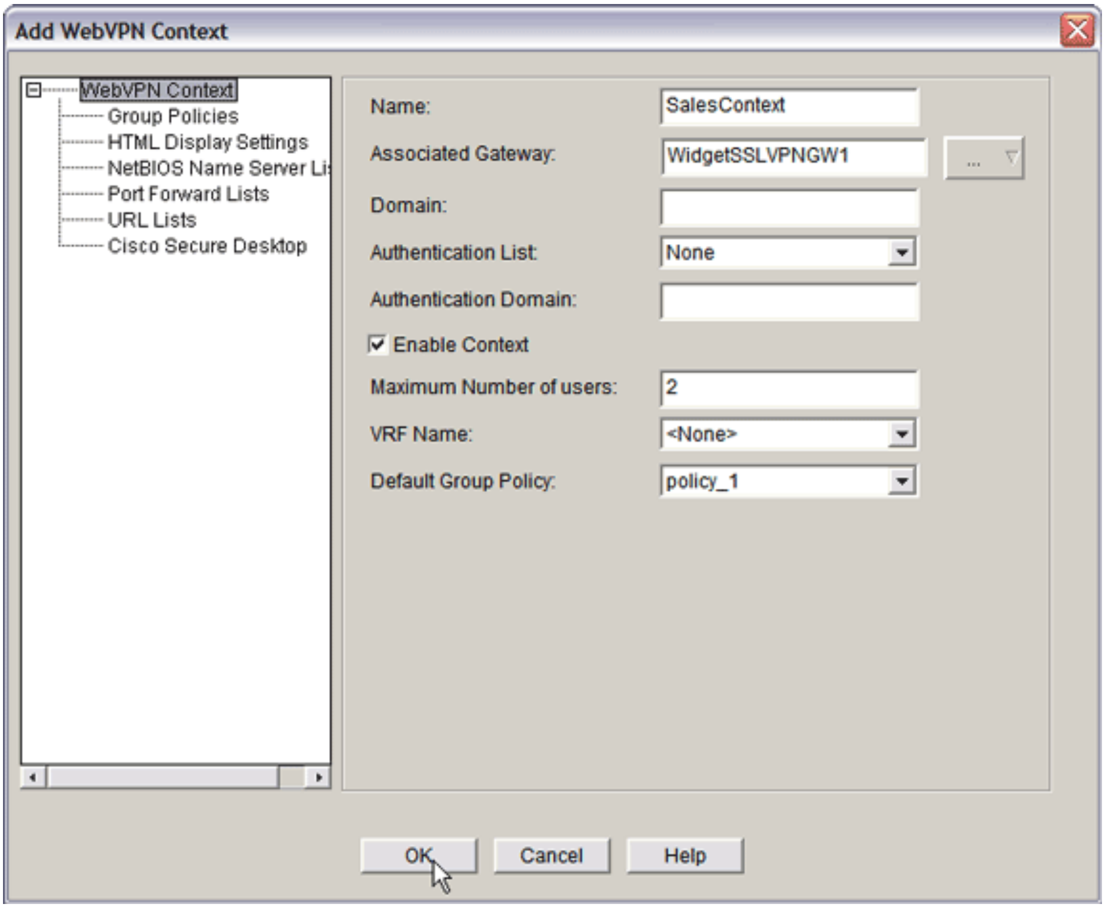
NBNS Server List: NBNSServers

6. Check the **Select** check box for the desired URL List.
7. If your customers use Citrix clients that need access to Citrix servers, check the **Enable Citrix** check box.
8. Check the **Enable CIFS**, **Read**, and **Write** check boxes.
9. Click the **NBNS Server List** drop−down arrow, and choose the NBNS server list that you created for Windows file browsing in Step 2.
10. Click **OK**.

Step 4. Configure the WebVPN Context

In order to link the WebVPN gateway, group policy, and resources together, you must configure the WebVPN context. In order to configure the WebVPN context, complete these steps:

1. Choose **WebVPN Context**, and enter a name for the context.



Name: SalesContext
Associated Gateway: WidgetSSLVPNGW1
Domain:
Authentication List: None
Authentication Domain:
☑ Enable Context
Maximum Number of users: 2
VRF Name: <None>
Default Group Policy: policy_1

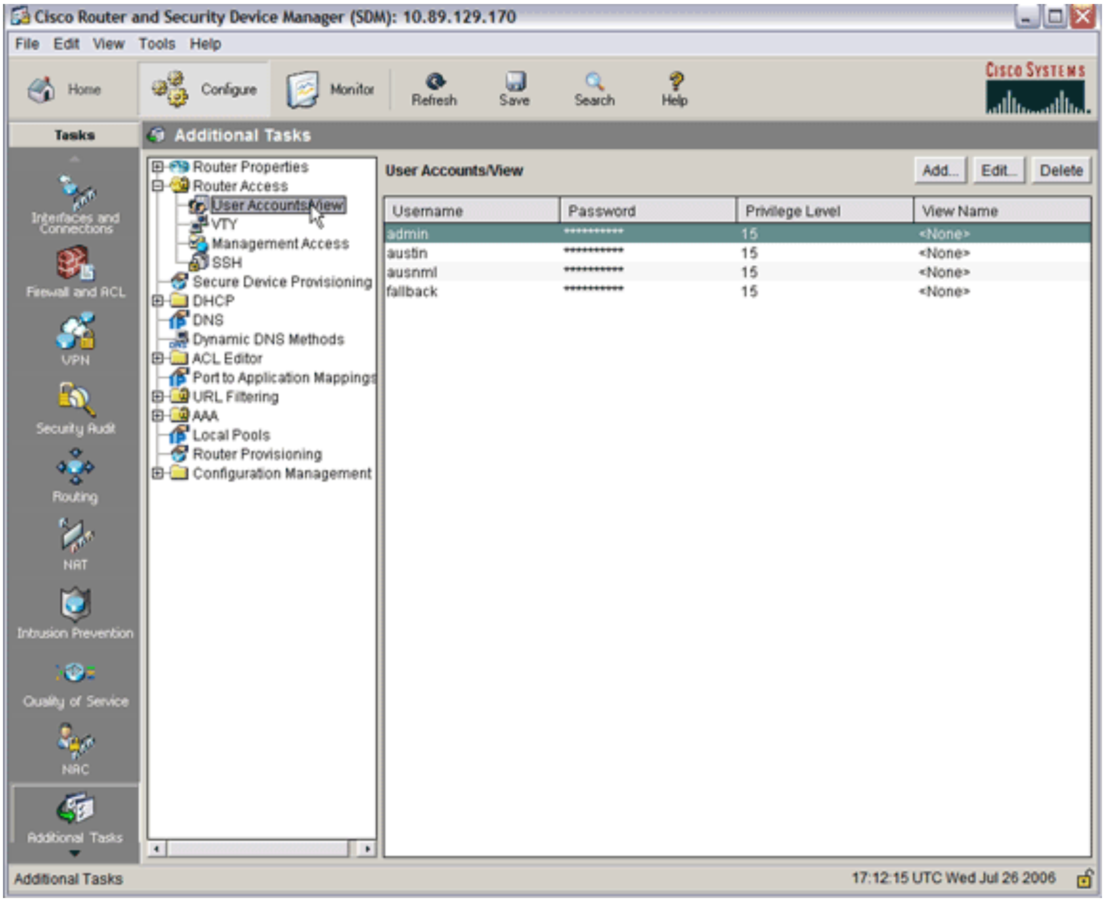
2. Click the Associated Gateway drop−down arrow, and choose an associated gateway.
3. If you intend to create more than one context, enter a unique name in the Domain field to identify this context. If you leave the Domain field blank, users must access the WebVPN with **https://*IPAddress*** . If you enter a domain name (for example, *Sales*), users must connect with **https://*IPAddress*/Sales**.
4. Check the **Enable Context** check box.
5. In the Maximum Number of Users field, enter the maximum number of users allowed by the device license.
6. Click the **Default Group policy** drop−down arrow, and select the group policy to associate with this context.
7. Click **OK**, and then click **OK**.

Step 5. Configure the User Database and Authentication Method

You can configure Clientless SSL VPN (WebVPN) sessions to authenticate with Radius, the Cisco AAA Server, or a local database. This example uses a local database.

Complete these steps in order to configure the user database and authentication method:

1. Click **Configuration**, and then click **Additional Tasks**.
2. Expand **Router Access**, and choose **User Accounts/View**.

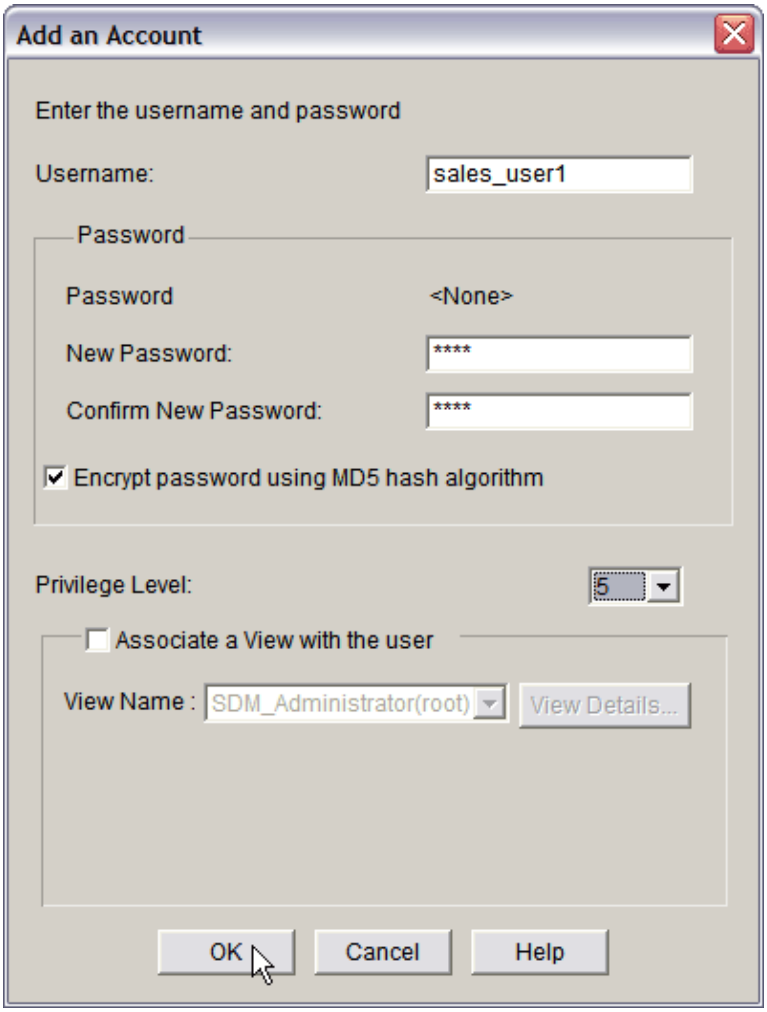


User Accounts/View

Username	Password	Privilege Level	View Name
admin	***********	15	<None>
austin	***********	15	<None>
ausnml	***********	15	<None>
fallback	***********	15	<None>

3. Click the **Add** button.

   The Add an Account dialog box appears.



Add an Account

Enter the username and password

Username: sales_user1

Password

Password <None>

New Password: ****

Confirm New Password: ****

☑ Encrypt password using MD5 hash algorithm

Privilege Level: 5

□ Associate a View with the user

View Name : SDM_Administrator(root)

4. Enter a user account and a password.
5. Click **OK**, and then click **OK**.
6. Click **Save**, and then click **Yes** to accept the changes.

Results

The ASDM creates these command−line configurations:

ausnml−3825−01

```
Building configuration...

Current configuration : 4190 bytes
!
! Last configuration change at 17:22:23 UTC Wed Jul 26 2006 by ausnml
! NVRAM config last updated at 17:22:31 UTC Wed Jul 26 2006 by ausnml
!
version 12.4
service timestamps debug datetime msec
service timestamps log datetime msec
service password−encryption
!
hostname ausnml−3825−01
!
boot−start−marker
boot system flash c3825−adventerprisek9−mz.124−9.T.bin
boot−end−marker
!
no logging buffered
```

```
enable secret 5 $1$KbIu$5o8qKYAVpWvyv9rYbrJLi/
!
aaa new-model
!
aaa authentication login default local
aaa authentication login sdm_vpn_xauth_ml_1 local
aaa authorization exec default local
!
aaa session-id common
!
resource policy
!
ip cef
!
ip domain name cisco.com
!
voice-card 0
 no dspfarm
!

!--- Self-Signed Certificate Information

crypto pki trustpoint ausnml-3825-01_Certificate
 enrollment selfsigned
 serial-number none
 ip-address none
 revocation-check crl
 rsakeypair ausnml-3825-01_Certificate_RSAKey 1024
!
crypto pki certificate chain ausnml-3825-01_Certificate
 certificate self-signed 02
  30820240 308201A9 A0030201 02020102 300D0609 2A864886 F70D0101 04050030
  29312730 2506092A 864886F7 0D010902 16186175 736E6D6C 2D333832 352D3031
  2E636973 636F2E63 6F6D301E 170D3036 30373133 32333230 34375A17 0D323030
  31303130 30303030 305A3029 31273025 06092A86 4886F70D 01090216 18617573
  6E6D6C2D 33383235 2D30312E 63697363 6F2E636F 6D30819F 300D0609 2A864886
  F70D0101 01050003 818D0030 81890281 8100C97D 3D259BB7 3A48F877 2C83222A
  A1E9E42C 5A71452F 9107900B 911C0479 4D31F42A 13E0F63B E44753E4 0BEFDA42
  FE6ED321 8EE7E811 4DEEC4E4 319C0093 C1026C0F 38D91236 6D92D931 AC3A84D4
  185D220F D45A411B 09BED541 27F38EF5 1CC01D25 76D559AE D9284A74 8B52856D
  BCBBF677 0F444401 D0AD542C 67BA06AC A9030203 010001A3 78307630 0F060355
  1D130101 FF040530 030101FF 30230603 551D1104 1C301A82 18617573 6E6D6C2D
  33383235 2D30312E 63697363 6F2E636F 6D301F06 03551D23 04183016 801403E1
  5EAABA47 79F6C70C FBC61B08 90B26C2E 3D4E301D 0603551D 0E041604 1403E15E
  AABA4779 F6C70CFB C61B0890 B26C2E3D 4E300D06 092A8648 86F70D01 01040500
  03818100 6938CEA4 2E56CDFF CF4F2A01 BCD585C7 D6B01665 595C3413 6B7A7B6C
  F0A14383 4DA09C30 FB621F29 8A098FA4 F3A7F046 595F51E6 7C038112 0934A369
  D44C0CF4 718A8972 2DA33C43 46E35DC6 5DCAE7E0 B0D85987 A0D116A4 600C0C60
  71BB1136 486952FC 55DE6A96 1135C9D6 8C5855ED 4CD3AE55 BDA966D4 BE183920 88A8A55E
  quit
username admin privilege 15 secret 5 $1$jm6N$2xNfhupbAinq3BQZMRzrW0
username ausnml privilege 15 password 7 15071F5A5D292421
username fallback privilege 15 password 7 08345818501A0A12
username austin privilege 15 secret 5 $1$3xFv$W0YUsKDx1adDc.cVQF2Ei0
username sales_user1 privilege 5 secret 5 $1$2/SX$ep4fsCpodeyKaRji2mJkX/
!
interface GigabitEthernet0/0
 ip address 192.168.0.37 255.255.255.0
 duplex auto
 speed auto
 media-type rj45
!
interface GigabitEthernet0/1
 ip address 172.22.1.151 255.255.255.0
 duplex auto
 speed auto
 media-type rj45
!
ip route 0.0.0.0 0.0.0.0 172.22.1.1
!
ip http server
ip http authentication local

ip http timeout-policy idle 600 life 86400 requests 100
!
control-plane
!
line con 0
 stopbits 1
line aux 0
 stopbits 1
line vty 0 4
 exec-timeout 40 0
 privilege level 15
 password 7 071A351A170A1600
 transport input telnet ssh
line vty 5 15
 exec-timeout 40 0
 password 7 001107505D580403
 transport input telnet ssh
!
scheduler allocate 20000 1000
!

!--- WebVPN Gateway

webvpn gateway WidgetSSLVPNGW1
 hostname ausnml-3825-01
 ip address 192.168.0.37 port 443
 http-redirect port 80
 ssl trustpoint ausnml-3825-01_Certificate
 inservice
 !
webvpn context SalesContext
 ssl authenticate verify all
 !

!--- Identify resources for the SSL VPN session

 url-list "InternalWebServers"
   heading "WidgetWebServers"
   url-text "WidgetWeb" url-value "http://172.22.1.30"
   url-text "OWA" url-value "http://172.22.1.50/exchange"
 !
 nbns-list NBNSServers
   nbns-server 172.22.1.30
 !

!--- Identify the policy which controls the resources available

 policy group policy_1
   url-list "InternalWebServers"
   nbns-list "NBNSServers"
   functions file-access
   functions file-browse
   functions file-entry
   hide-url-bar
   citrix enabled
 default-group-policy policy_1
 gateway WidgetSSLVPNGW1
 max-users 2
 inservice
```

```
!
end
```

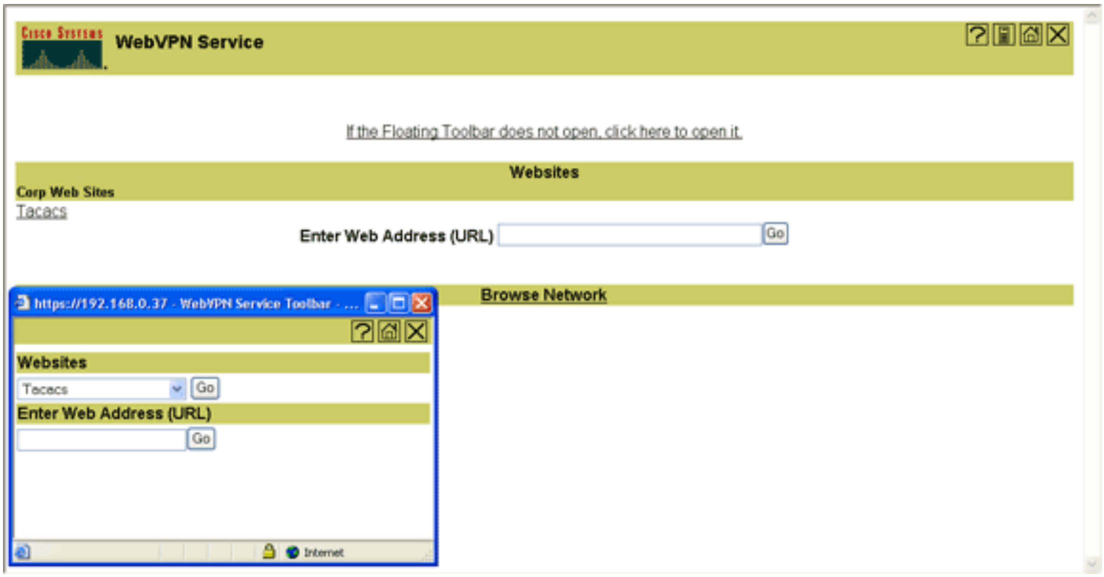
Verify

Use this section to confirm that your configuration works properly.

Procedure

Complete these procedures in order to confirm your configuration works properly:

- Test your configuration with a user. Enter **https://*WebVPN_Gateway_IP_Address*** into an SSL−enabled Web browser; where *WebVPN_Gateway_IP_Address* is the IP address of the WebVPN service. After you accept the certificate and enter a user name and password, a screen similar to this image should appear.



- Check the SSL VPN session. Within the SDM application, click the **Monitor** button, and then click **VPN Status**. Expand **WebVPN (All Contexts)**, expand the appropriate context, and choose **Users**.
- Check error messages. Within the SDM application, click the **Monitor** button, click **Logging**, and then click the **Syslog** tab.
- View the running configuration for the device. Within the SDM application, click the **Configure** button, and then click **Additional Tasks**. Expand **Configuration Management**, and choose **Config Editor**.

Commands

Several **show** commands are associated with WebVPN. You can execute these commands at the command−line interface (CLI) to show statistics and other information. For detailed information about **show** commands, refer to Verifying WebVPN Configuration.

Note: The Output Interpreter Tool (registered customers only) (OIT) supports certain **show** commands. Use the OIT to view an analysis of **show** command output.

Troubleshoot

Use this section to troubleshoot your configuration.

Note: Do not interrupt the **Copy File to Server** command or navigate to a different window while the copying is in progress. Interruption of the operation can cause an incomplete file to be saved on the server.

Note: Users can upload and download the new files using the WebVPN client, but the user is not allowed to overwrite the files in the Common Internet File System (CIFS) on WebVPN using the **Copy File to Server** command. The user receives this message when the user attempts to replace a file on the server:

```
Unable to add the file
```

Procedure

Complete these steps in order to troubleshoot your configuration:

1. Ensure clients disable pop−up blockers.
2. Ensure clients have cookies enabled.
3. Ensure clients use Netscape, Internet Explorer, Firefox, or Mozilla Web browsers.

Commands

Several **debug** commands are associated with WebVPN. Refer to Using WebVPN Debug Commands for detailed information about these commands.

Note: The use of **debug** commands can adversely impact your Cisco device. Before you use **debug** commands, refer to Important Information on Debug Commands.

Related Information

- **Cisco IOS SSLVPN**
- **Cisco IOS SSLVPN Q&A**
- **Thin−Client SSL VPN (WebVPN) IOS Configuration Example with SDM**
- **SSL VPN Client (SVC) on IOS with SDM Configuration Example**
- **Technical Support & Documentation − Cisco Systems**

Contacts & Feedback | Help | Site Map

Updated: Jun 02, 2009 Document ID: 70663