使用SDM在Cisco IOS上配置無客戶端SSL VPN(WebVPN)

目錄

簡介

無客戶端SSL VPN(WebVPN)允許使用者使用啟用SSL的Web瀏覽器，從任何位置安全訪問公司LAN上的資源。使用者首先使用WebVPN網關進行身份驗證，然後允許使用者訪問預配置的網路資源。WebVPN網關可在Cisco IOS®路由器、思科自適應安全裝置(ASA)、Cisco VPN 3000集中器以及適用於Catalyst 6500和7600路由器的Cisco WebVPN服務模組上配置。

安全通訊端層(SSL)虛擬私人網路(VPN)技術可以在思科裝置上以三種主要模式設定：無客戶端SSL VPN(WebVPN)、瘦客戶端SSL VPN（埠轉發）和SSL VPN客戶端(SVC)模式。本文檔演示了Cisco IOS路由器上的WebVPN配置。

注意：請勿更改路由器的IP域名或主機名，因為這將觸發重新生成自簽名證書並覆蓋配置的信任點。如果路由器已配置為WebVPN，則重新生成自簽名證書會導致連線問題。WebVPN將SSL信任點名稱繫結到WebVPN網關配置。因此，如果頒發新的自簽名證書，則新的信任點名稱與WebVPN配置不匹配，使用者無法連線。

注意：如果在使用永久性自簽名證書的WebVPN路由器上運行**ip https-secure server命令，將生成新的RSA金鑰，並且證書將無效。**將建立一個新的信任點，該信任點會破壞SSL WebVPN。如果在運行**ip https-secure server**命令後使用永久性自簽名證書的路由器重新啟動，則會發生相同的問題。

請參閱使用SDM的瘦客戶端SSL VPN(WebVPN)IOS配置示例，瞭解有關瘦客戶端SSL VPN的詳細資訊。

請參閱使用SDM的IOS上的SSL VPN客戶端(SVC)配置示例，瞭解有關SSL VPN客戶端的詳細資訊。

SSL VPN在這些思科路由器平台上運行：

- Cisco 870、1811、1841、2801、2811、2821和2851系列路由器
- Cisco 3725、3745、3825、3845、7200和7301系列路由器

必要條件

需求

嘗試此組態之前，請確保符合以下要求：

- Cisco IOS軟體版本12.4(6)T或更新版本的進階映像
- 簡介中列出的其中一個思科路由器平台

採用元件

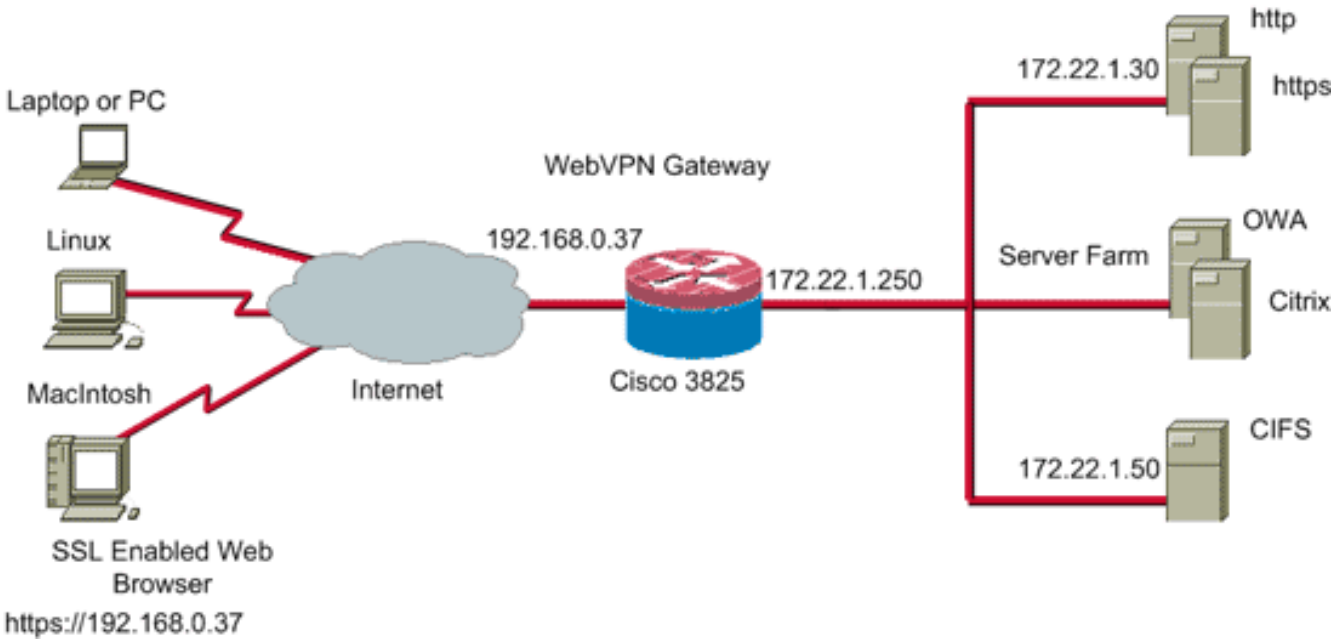
本文中的資訊係根據以下軟體和硬體版本：

- 思科3825路由器
- 進階企業軟體映像 — Cisco IOS軟體版本12.4(9)T
- Cisco路由器和安全裝置管理員(SDM)- 2.3.1版

本文中的資訊是根據特定實驗室環境內的裝置所建立。文中使用到的所有裝置皆從已清除（預設）的組態來啟動。如果您的網路正在作用，請確保您已瞭解任何指令可能造成的影響。本示例中使用的IP地址取自RFC 1918地址，這些地址是私有地址，不適合在Internet上使用。

網路圖表

本檔案會使用以下網路設定：



慣例

請參閱思科技術提示慣例以瞭解更多有關文件慣例的資訊。

預配置任務

開始之前，請完成以下任務：

1. 配置主機名和域名。
2. 為SDM配置路由器。Cisco為某些路由器預裝了SDM副本。如果路由器上尚未載入Cisco SDM，您可以從Software Download（僅限註冊客戶）獲取軟體的免費副本。 您必須擁有具有服務合約的CCO帳戶。有關安裝和配置SDM的詳細資訊，請參閱Cisco路由器和安全裝置管理器。
3. 為路由器配置正確的日期、時間和時區。

在Cisco IOS上配置WebVPN

一個裝置可以關聯多個WebVPN網關。每個WebVPN網關僅連結到路由器的一個IP地址。您可以為特定WebVPN網關建立多個WebVPN上下文。要標識各個上下文，請為每個上下文提供一個唯一的名稱。一個策略組只能與一個WebVPN上下文關聯。策略組描述特定的WebVPN環境中哪些資源可用。

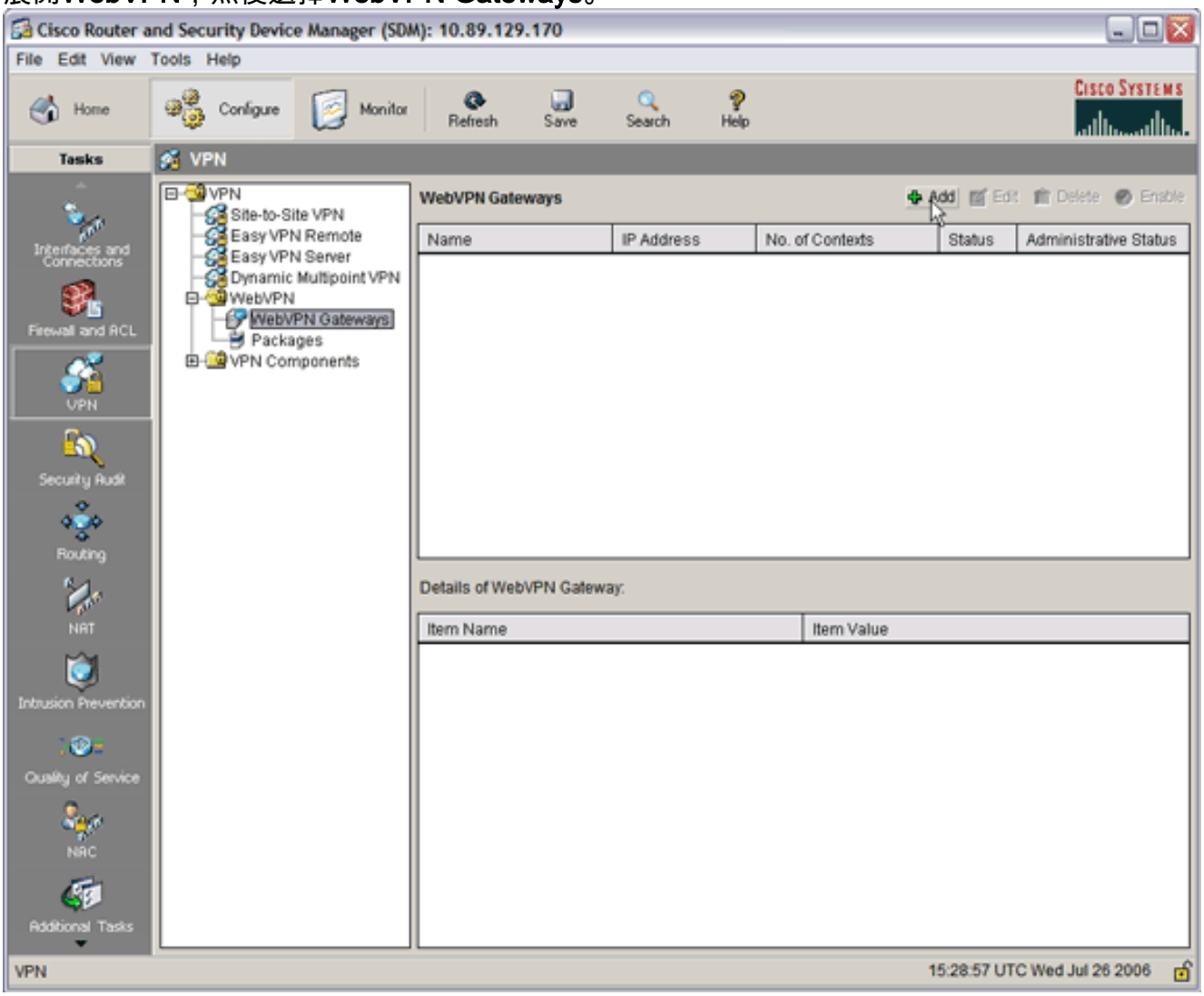
完成以下步驟，以便在Cisco IOS上設定WebVPN:

1. 配置WebVPN網關
2. 配置策略組允許的資源
3. 配置WebVPN策略組並選擇資源
4. 配置WebVPN上下文
5. 配置使用者資料庫和身份驗證方法

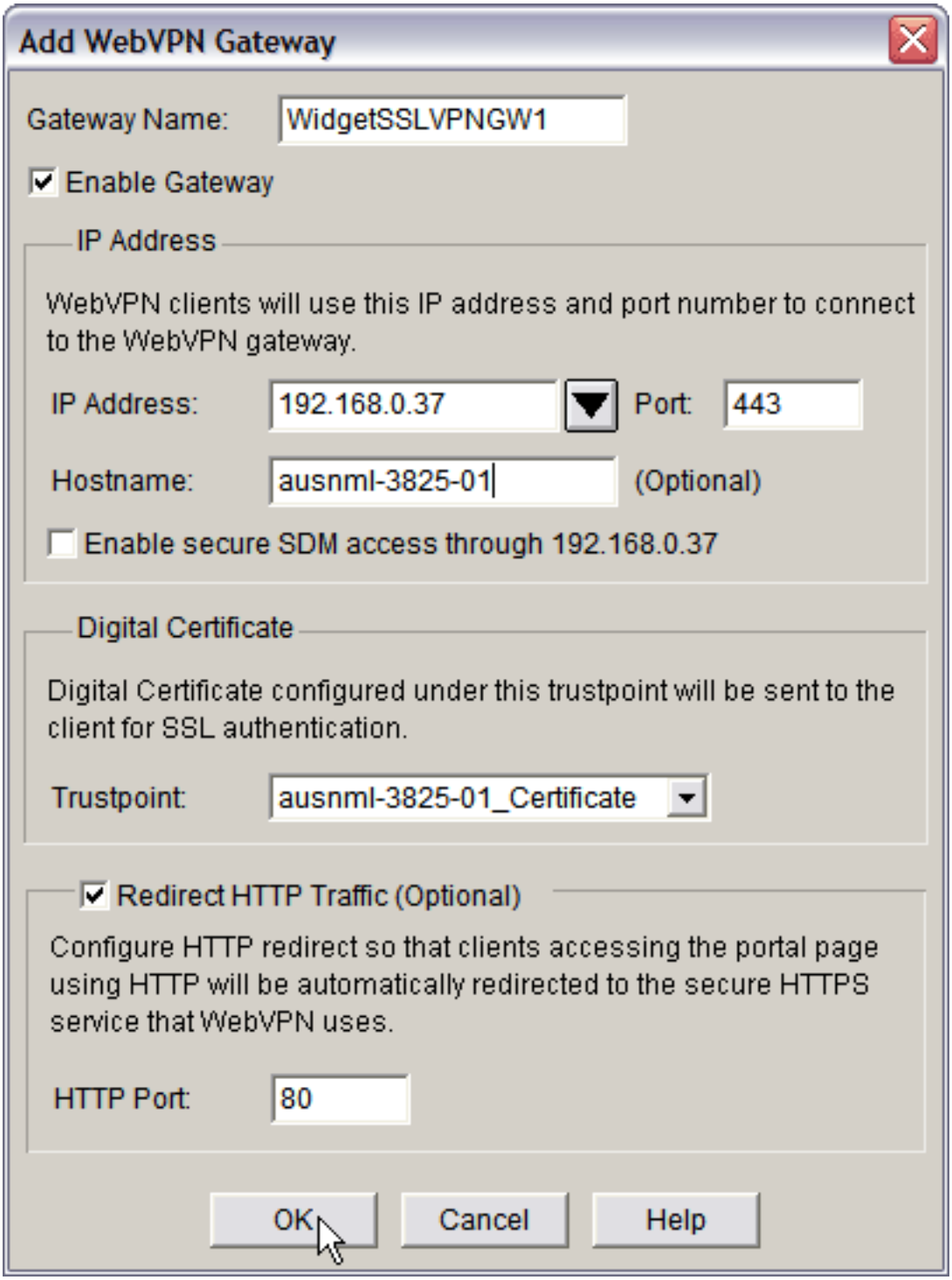
步驟1.配置WebVPN網關

完成以下步驟以配置WebVPN網關：

1. 在SDM應用程式中，按一下**Configure**，然後按一下**VPN**。
2. 展開**WebVPN**，然後選擇**WebVPN Gateways**。



3. 按一下「**Add**」。系統將顯示Add WebVPN Gateway對話方塊。



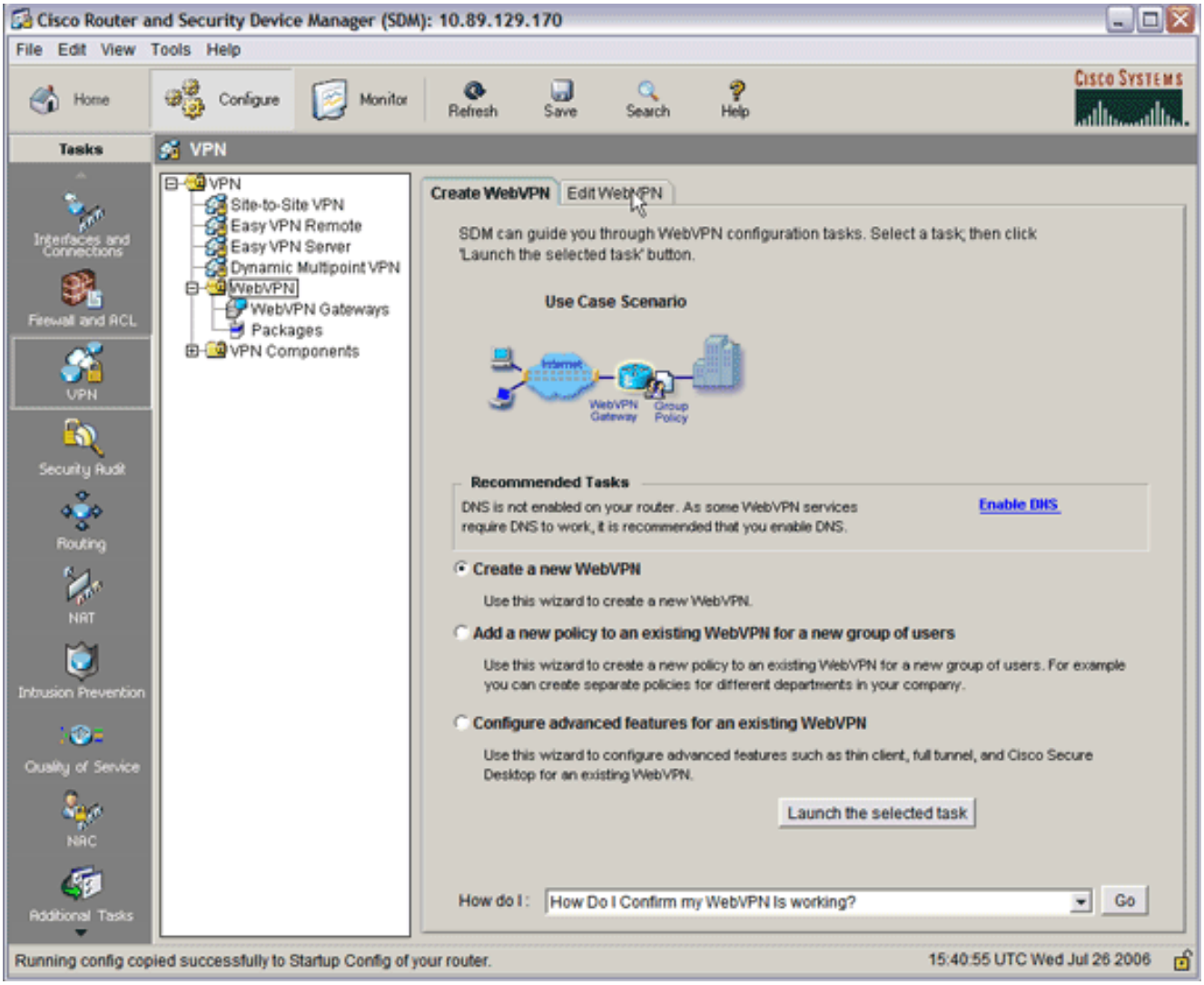
4. 在Gateway Name和IP Address欄位中輸入值，然後選中**Enable Gateway**覈取方塊。
5. 選中**Redirect HTTP Traffic**覈取方塊，然後按一下**OK**。
6. 按一下**Save**，然後按一下**Yes**接受更改。

步驟2.配置策略組允許的資源

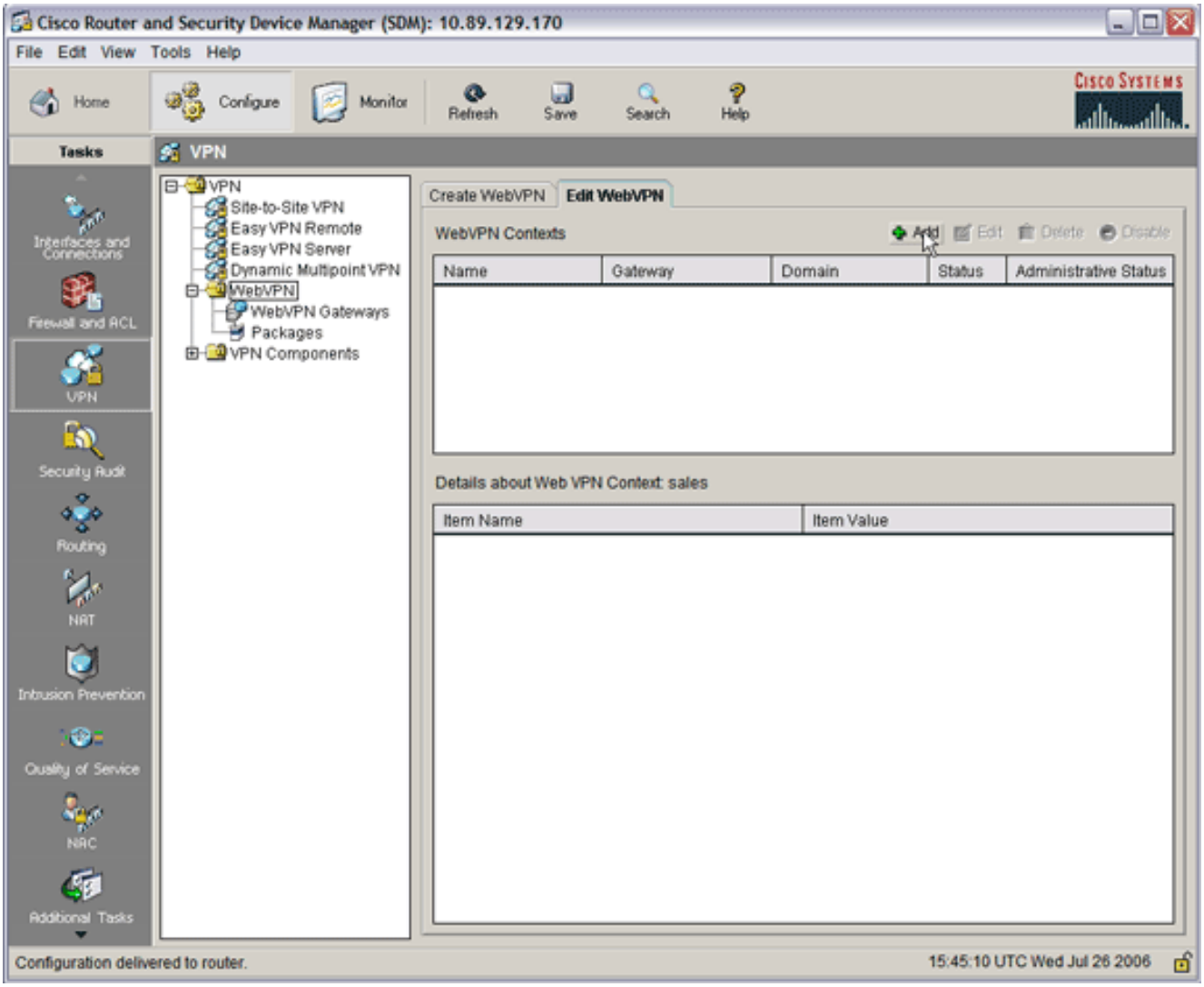
為了更輕鬆地向策略組新增資源，可以在建立策略組之前配置資源。

完成以下步驟，配置策略組允許的資源：

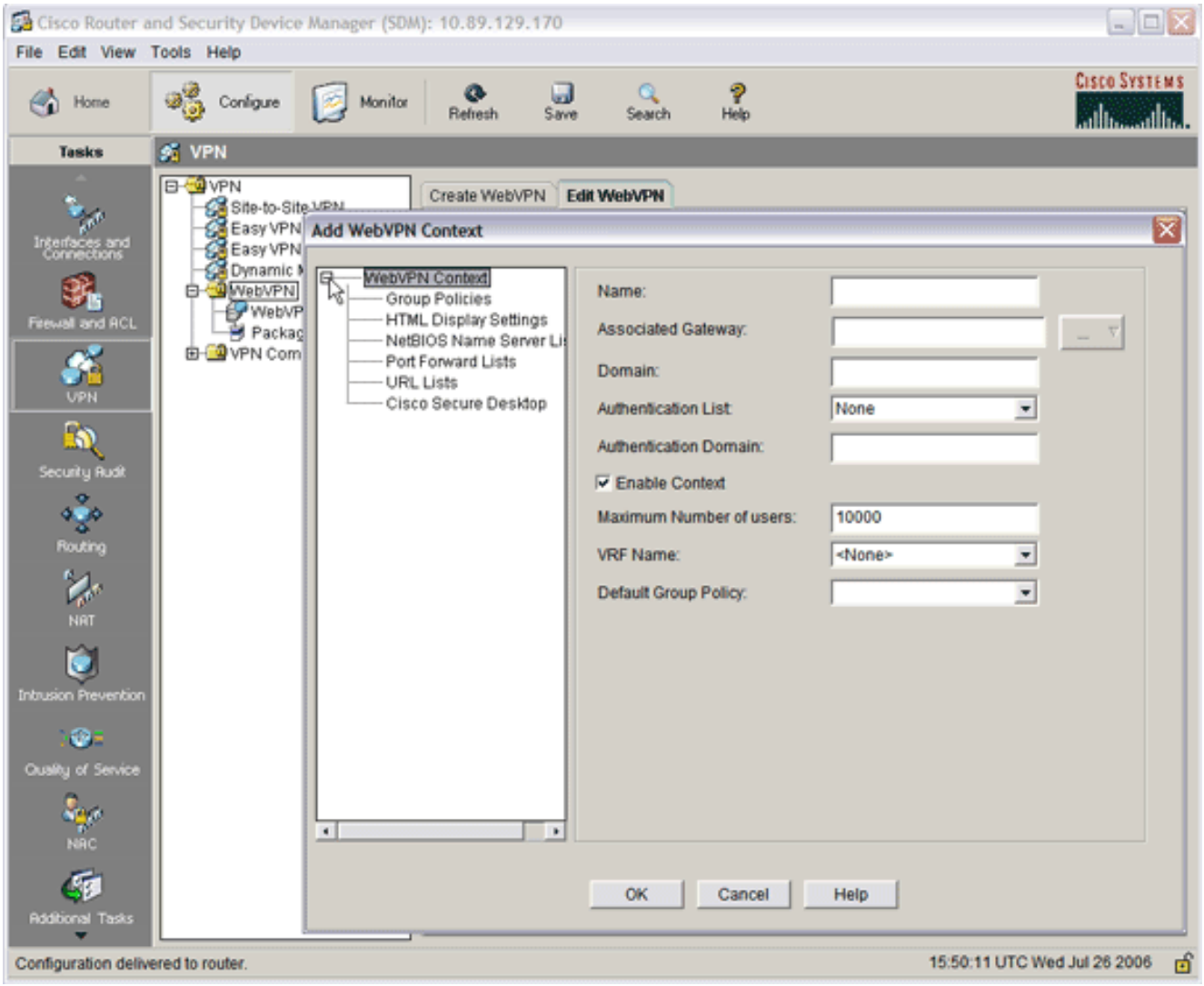
1. 按一下**Configure**，然後按一下**VPN**。



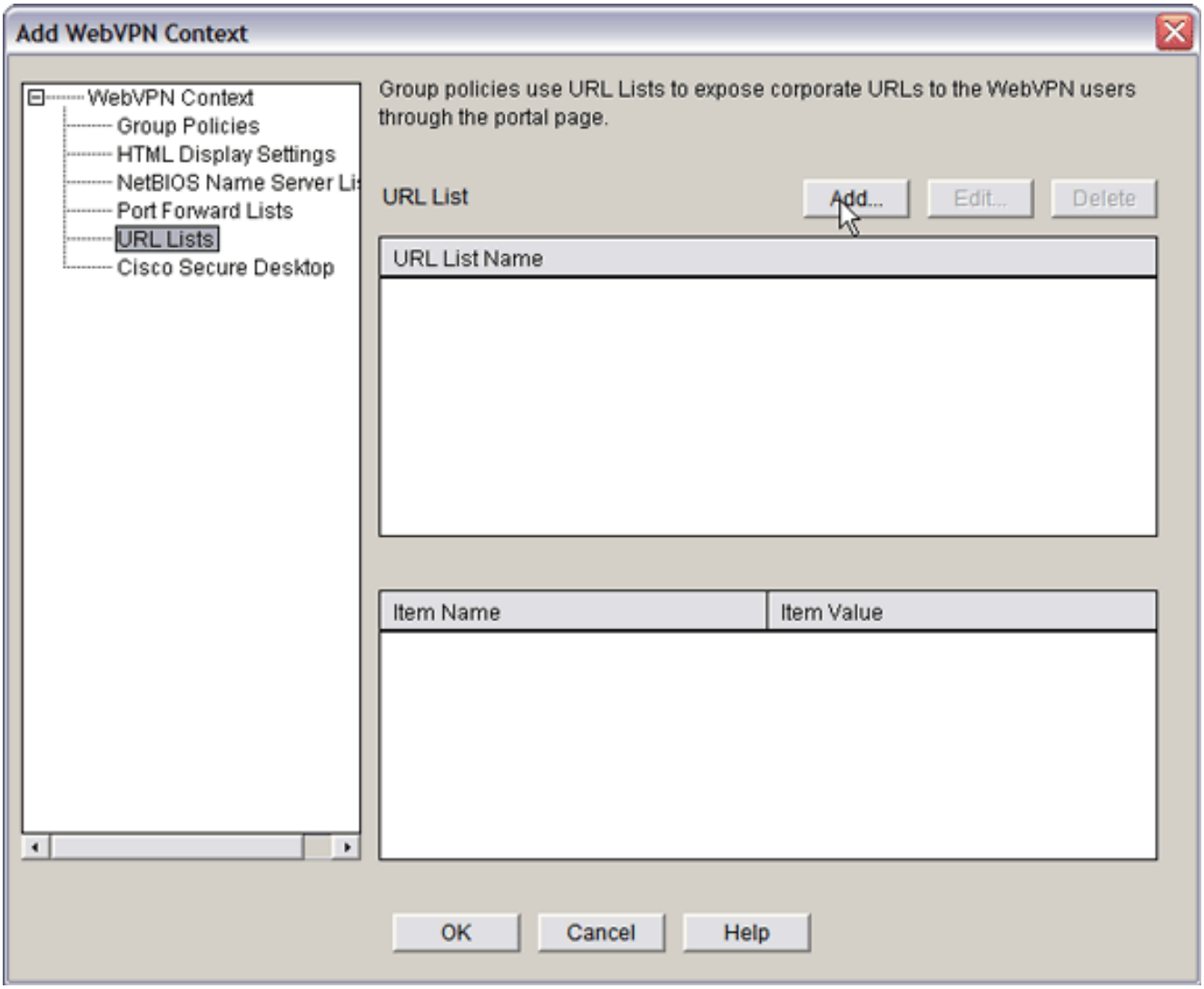
2. 選擇**WebVPN**，然後按一下**Edit WebVPN**頁籤。**注意：**WebVPN允許您通過通用網際網路檔案系統(CIFS)協定和Citrix配置HTTP、HTTPS、Windows檔案瀏覽的訪問許可權。



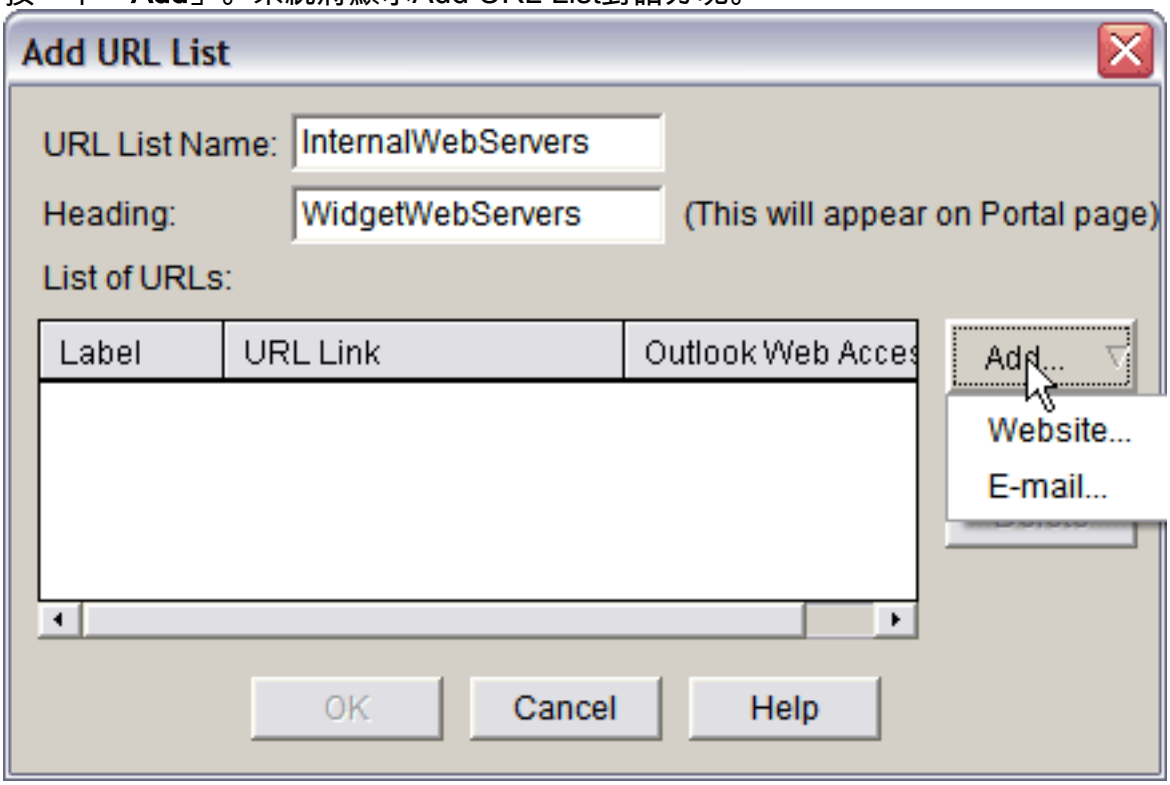
3. 按一下「**Add**」。系統將顯示Add WebVPN Context對話方塊。



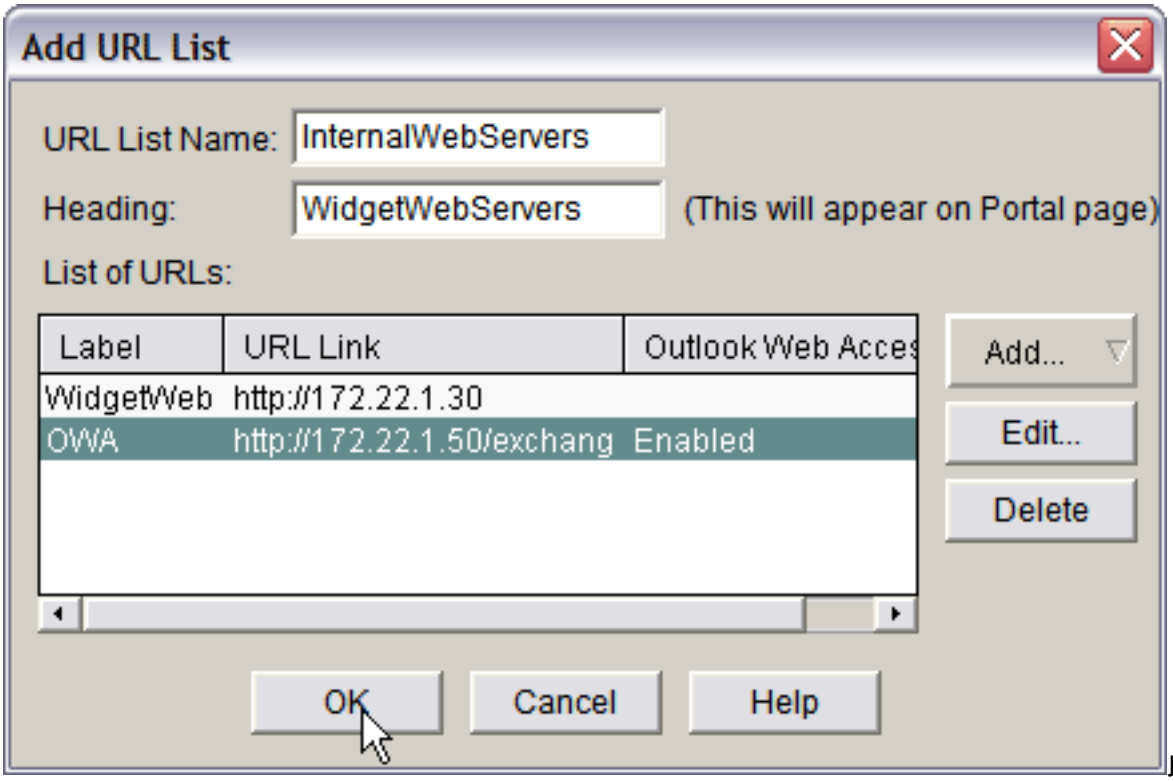
4. 展開**WebVPN Context**，然後選擇**URL Lists**。



5. 按一下「**Add**」。系統將顯示Add URL List對話方塊。

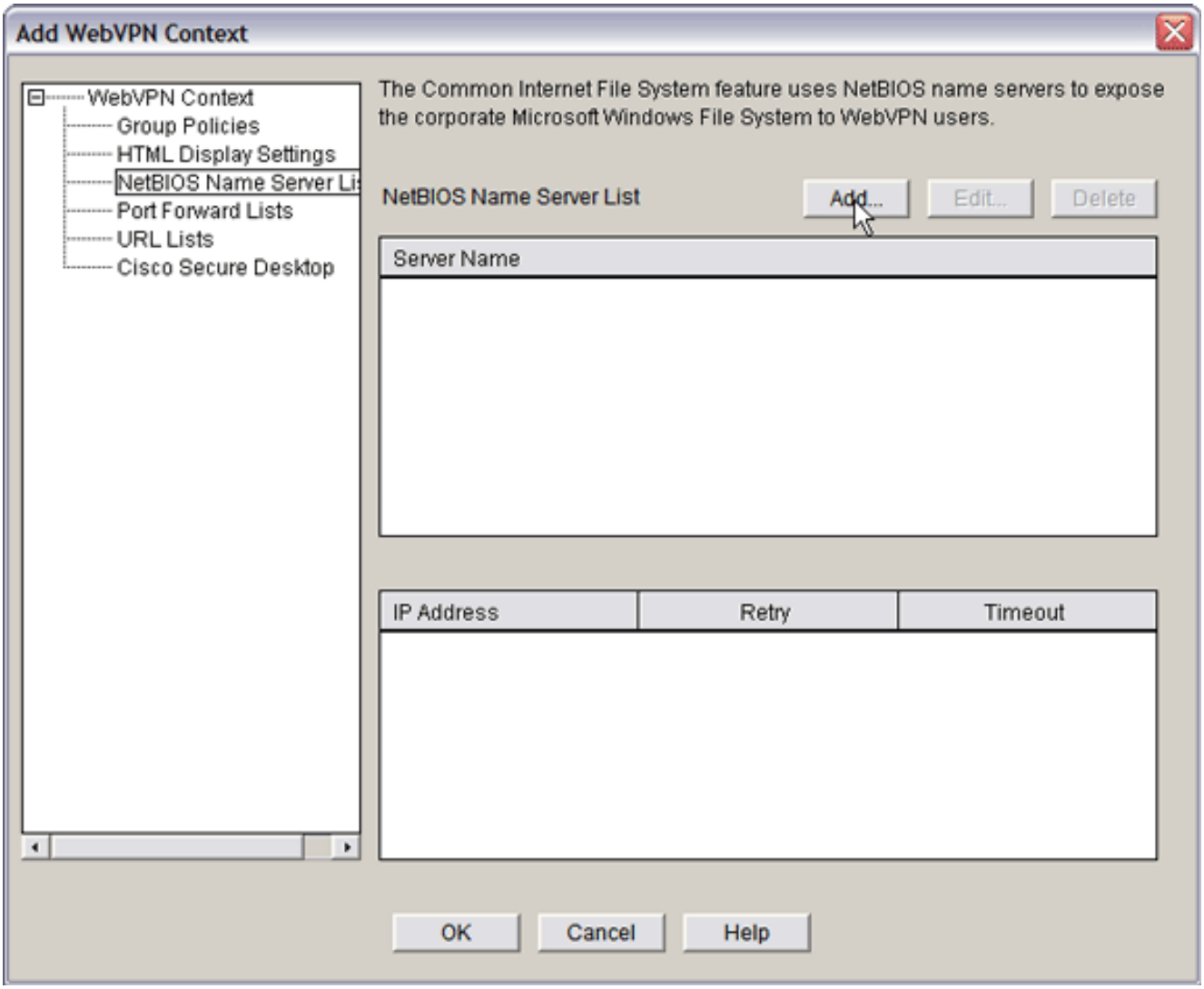


6. 在URL清單名稱和標題欄位中輸入值。
7. 按一下「**Add**」，然後選擇「**Website**」。

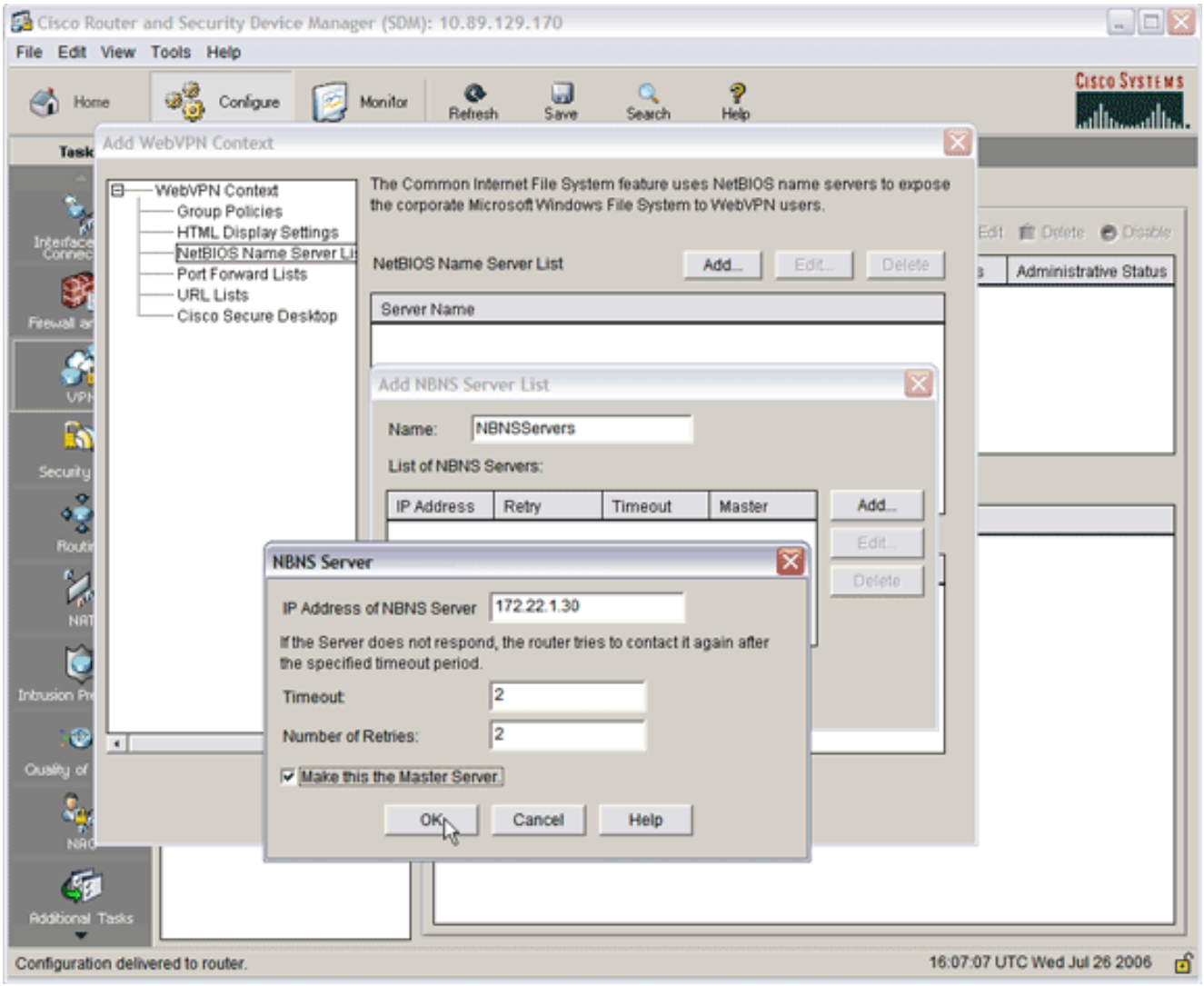


此清單包含希望可用於此WebVPN連線的所有HTTP和HTTPS Web伺服器。

8. 若要為Outlook Web Access(OWA)新增訪問許可權，請在填寫所有所需欄位後按一下**Add**，選擇**E-mail**，然後按一下**OK**。
9. 為了允許Windows檔案通過CIFS瀏覽，您可以指定一個NetBIOS名稱服務(NBNS)伺服器，並按順序在Windows域中配置適當的共用。在WebVPN Context清單中，選擇**NetBIOS Name Server Lists**。



按一下「**Add**」。系統將顯示Add NBNS Server List對話方塊。輸入清單的名稱，然後按一下**Add**。出現「NBNS伺服器」對話方塊。

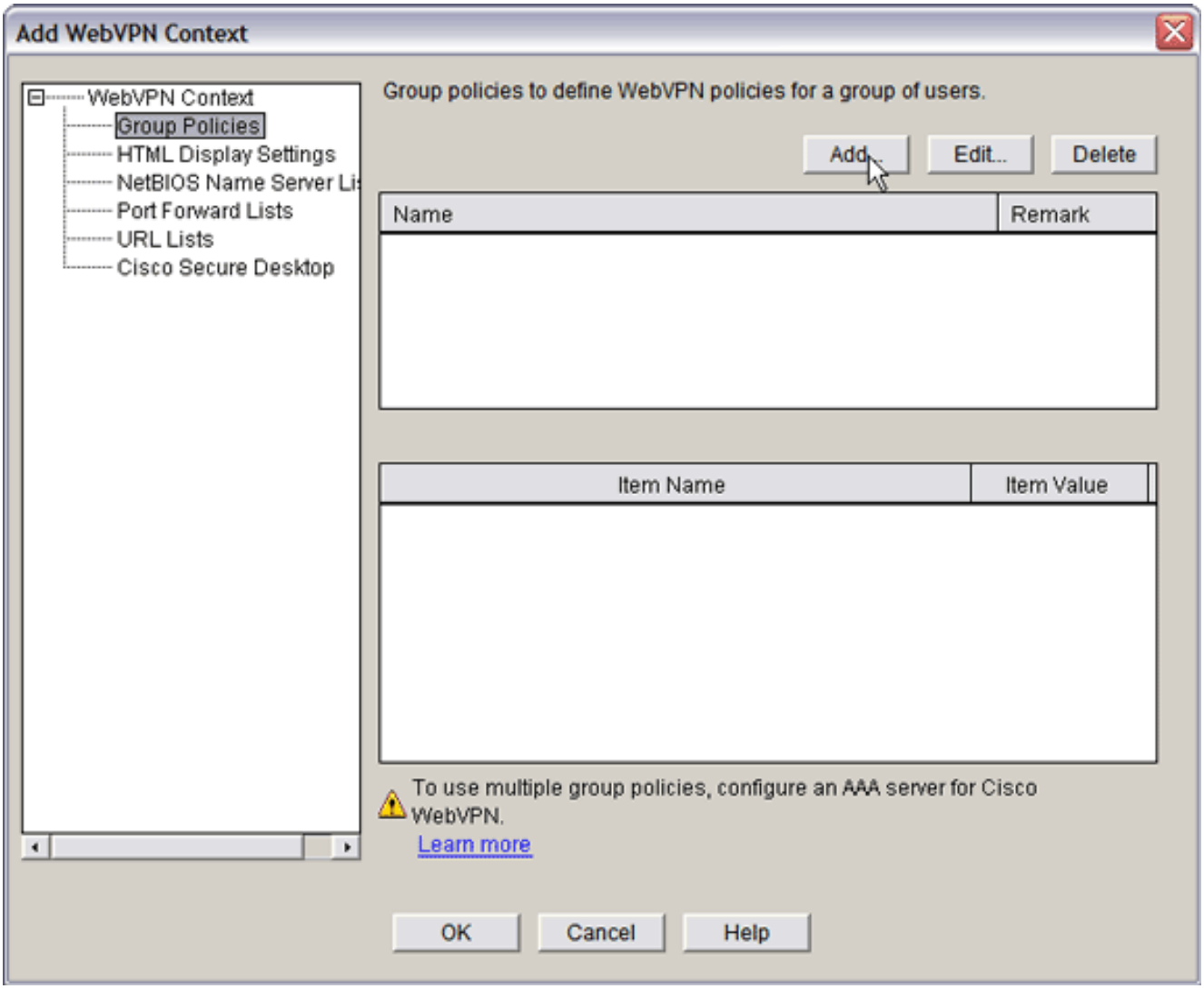


如果適用，請選中**Make This the Master Server**覈取方塊。按一下「**OK**」，然後按一下「**OK**」。

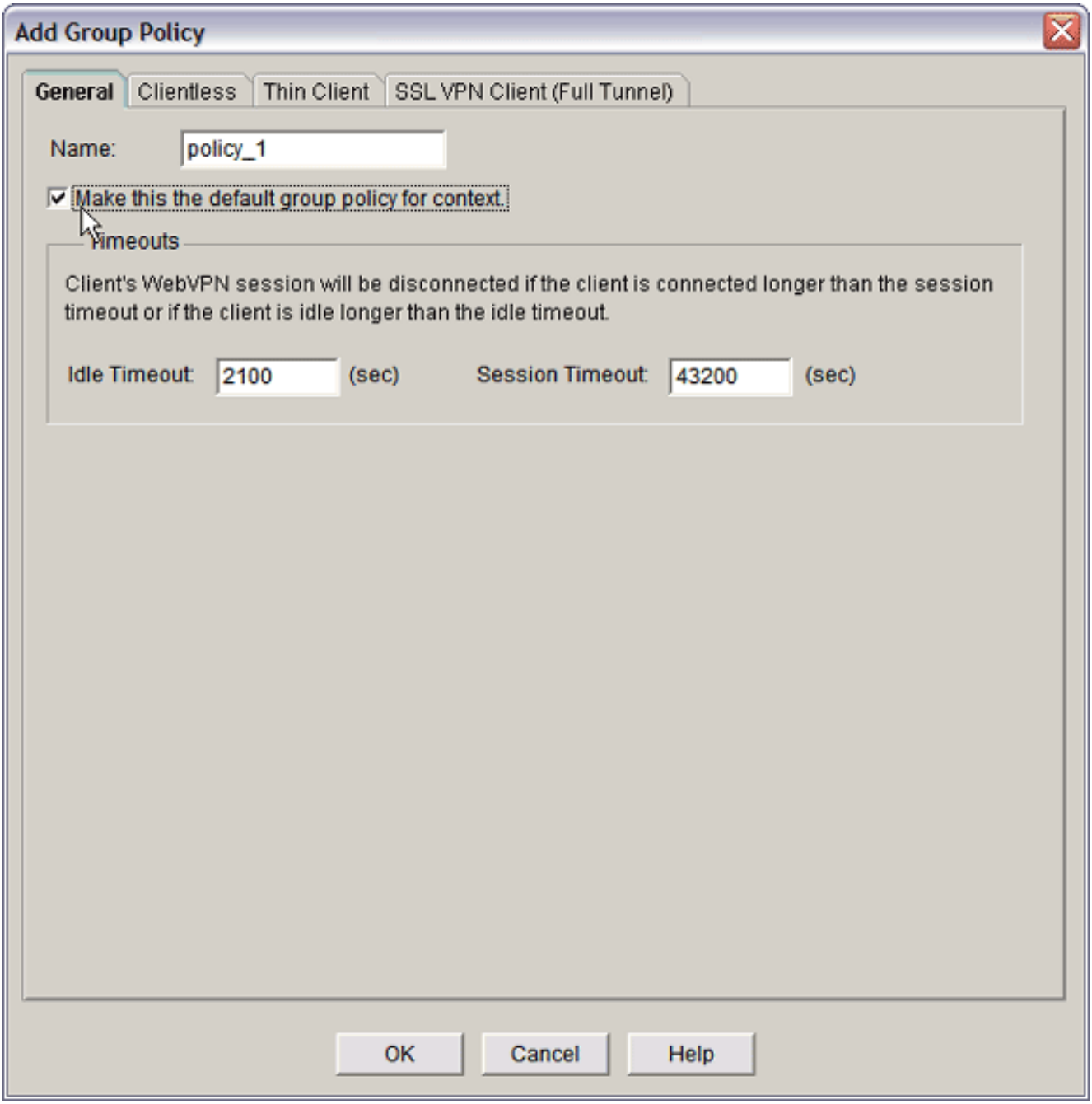
步驟3.配置WebVPN策略組並選擇資源

完成以下步驟以配置WebVPN策略組並選擇資源：

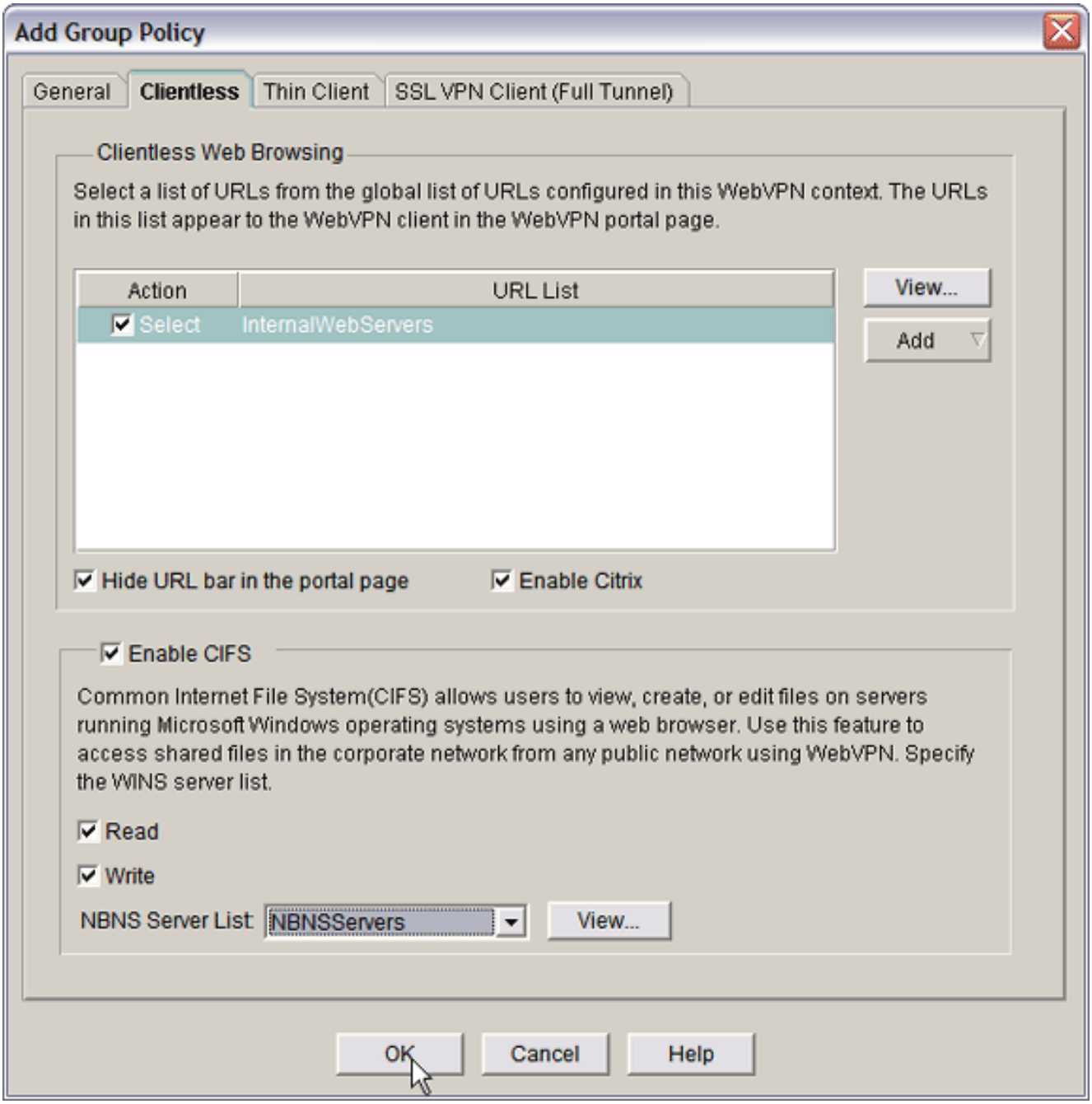
1. 按一下**Configure**，然後按一下**VPN**。
2. 展開**WebVPN**，然後選擇**WebVPN Context**。



3. 選擇**Group Policies**，然後按一下**Add**。系統將顯示Add Group Policy對話方塊。



4. 輸入新策略的名稱，並選中**Make this as default group policy for context**覈取方塊。
5. 按一下位於對話方塊頂部的**Clientless**頁籤。

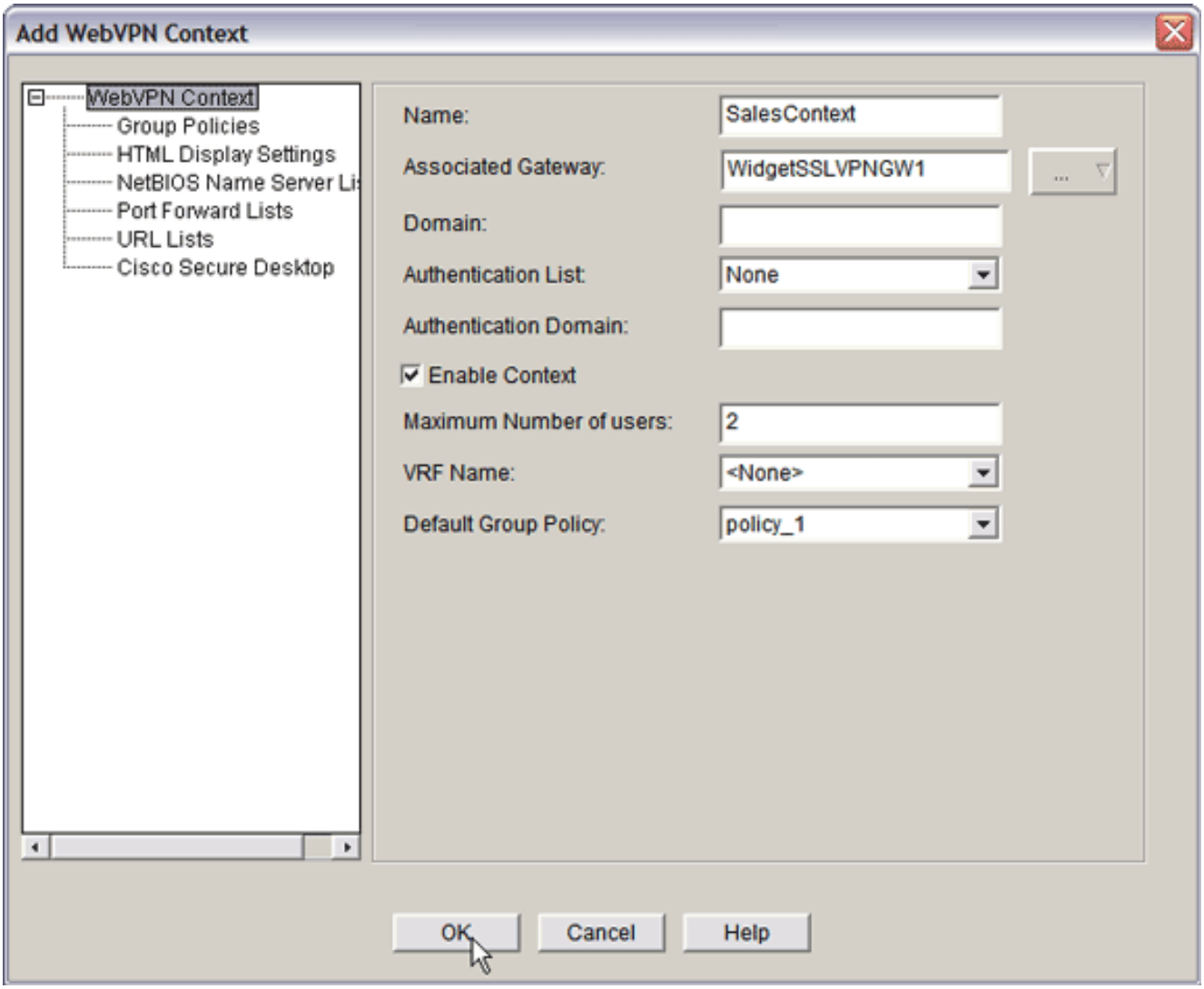


6. 選中所需的URL清單的**Select**覈取方塊。
7. 如果您的客戶使用需要訪問Citrix伺服器的Citrix客戶端，請選中**啟用Citrix**覈取方塊。
8. 選中**Enable CIFS**、**Read**和**Write**覈取方塊。
9. 按一下**NBNS Server List**下拉箭頭，然後選擇您在第2步中為Windows檔案瀏覽建立的NBNS伺服器清單。
10. 按一下「**OK**」（確定）。

步驟4.配置WebVPN上下文

若要將WebVPN網關、組策略和資源連結在一起，您必須配置WebVPN上下文。要配置WebVPN上下文，請完成以下步驟：

1. 選擇**WebVPN Context**，然後輸入上下文的名稱。



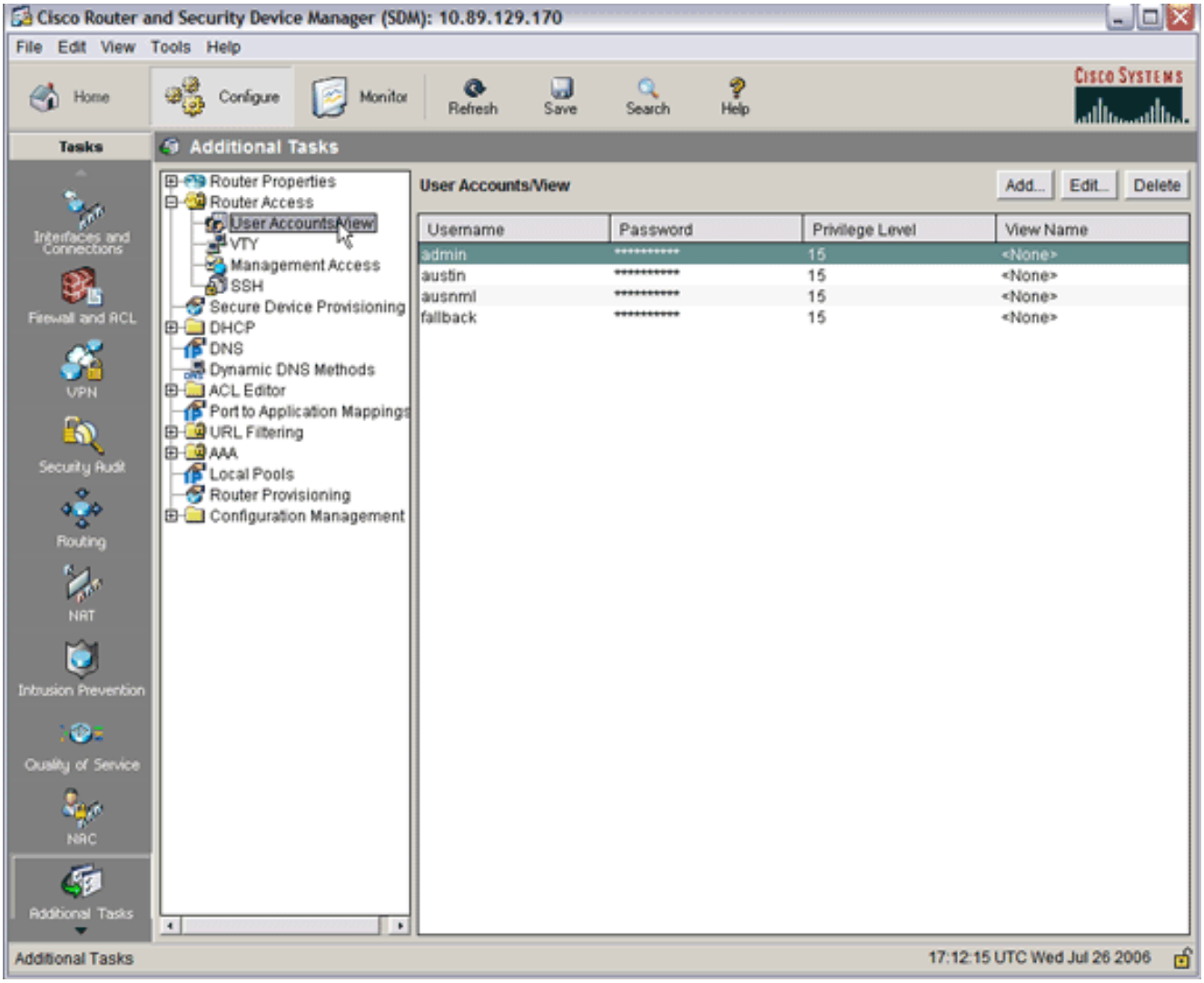
2. 點選Associated Gateway下拉箭頭，然後選擇關聯的網關。
3. 如果您打算建立多個上下文，請在「域」(Domain)欄位中輸入唯一名稱以標識此上下文。如果將「域」欄位留空，則使用者必須使用**https://*IPAddress*** 訪問WebVPN。如果您輸入域名(例如*Sales*)，則使用者必須使用**https://**IPAddress/Sales進行連線。
4. 選中**Enable Context**覈取方塊。
5. 在Maximum Number of Users欄位中，輸入裝置許可證允許的最大使用者數。
6. 按一下**Default Group policy**下拉箭頭，然後選擇要與此上下文關聯的組策略。
7. 按一下「**OK**」，然後按一下「**OK**」。

步驟5.配置使用者資料庫和身份驗證方法

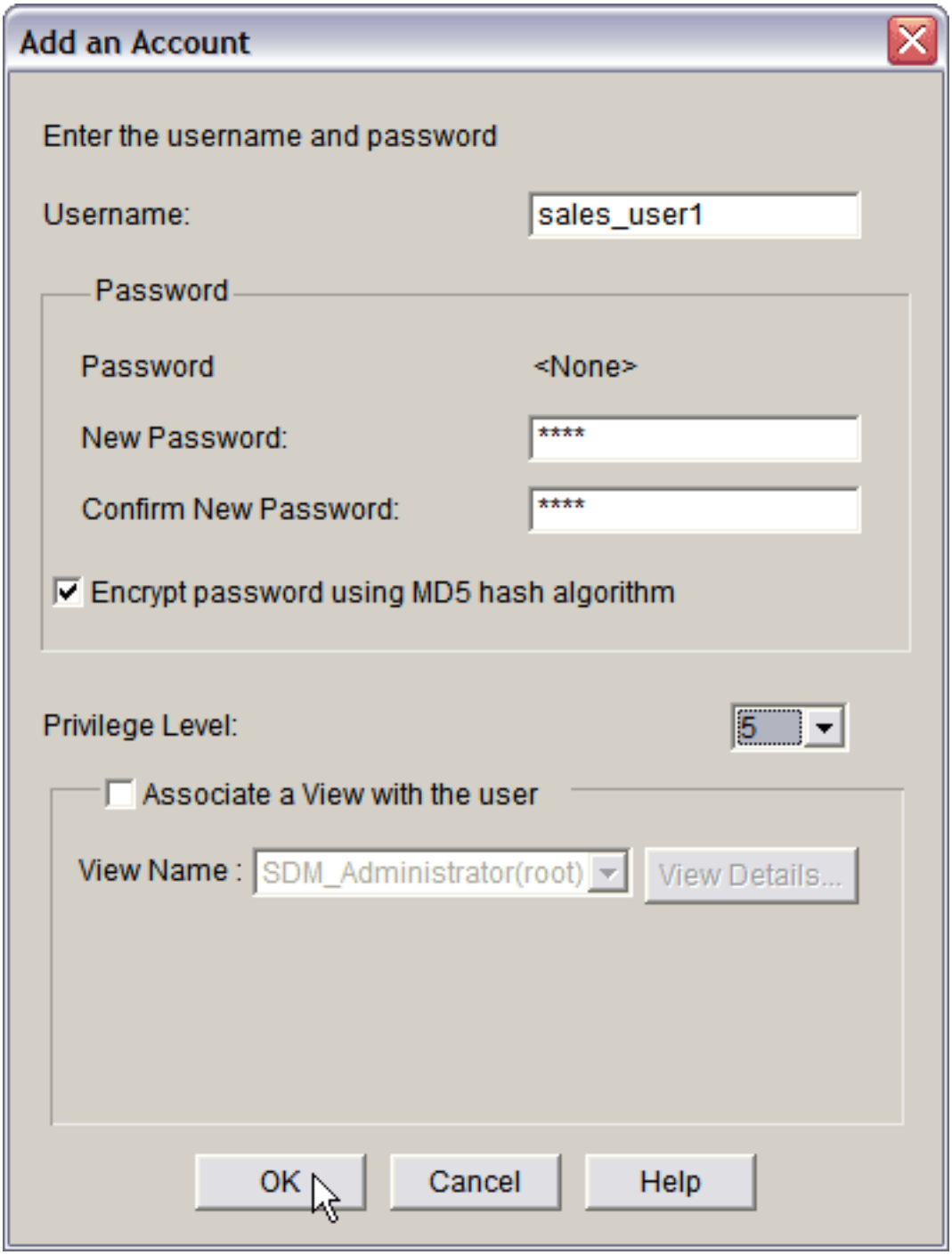
您可以配置無客戶端SSL VPN(WebVPN)會話以使用Radius、Cisco AAA伺服器或本地資料庫進行身份驗證。此示例使用本地資料庫。

完成以下步驟以配置使用者資料庫和身份驗證方法：

1. 按一下**Configuration**，然後按一下**Additional Tasks**。
2. 展開**Router Access**，然後選擇**User Accounts/View**。



3. 按一下**Add**按鈕。系統將顯示Add an Account對話方塊。



4. 輸入使用者帳戶和密碼。
5. 按一下「**OK**」，然後按一下「**OK**」。
6. 按一下**Save**，然後按一下**Yes**接受更改。

結果

ASDM建立以下命令列配置：

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
```

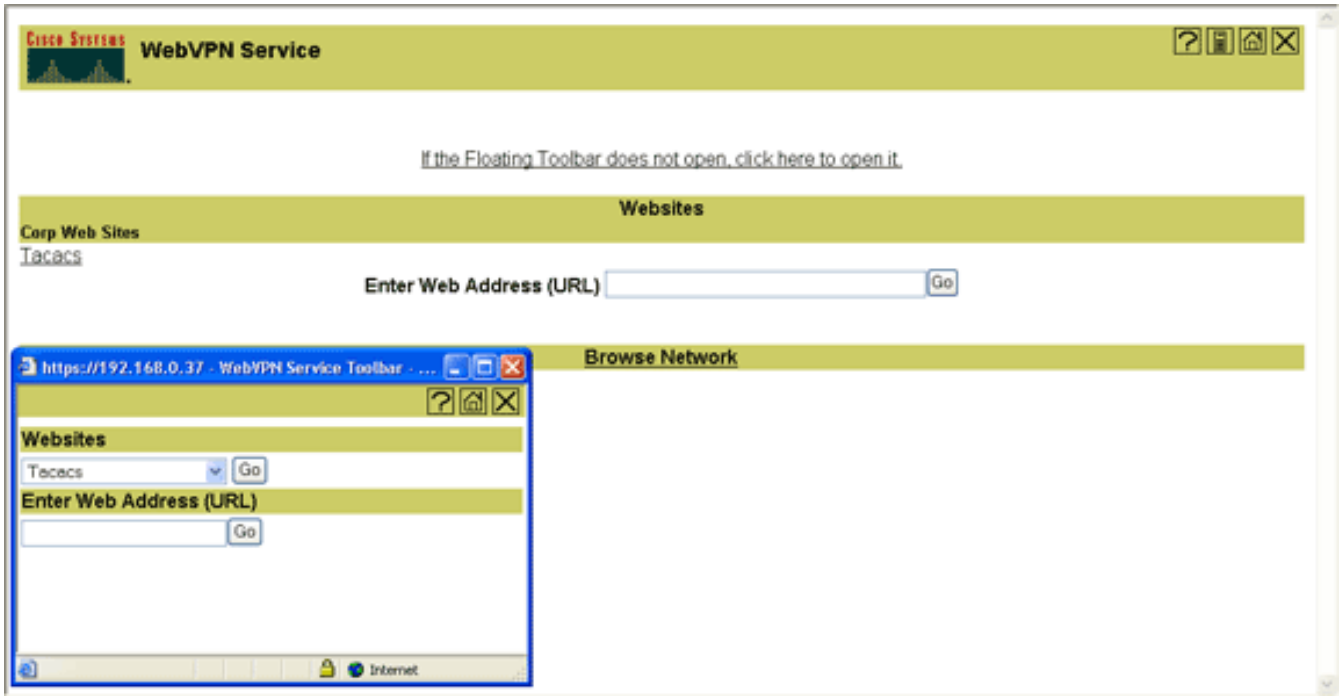
驗證

使用本節內容，確認您的組態是否正常運作。

程式

完成以下步驟以確認您的組態是否正常運作：

- 使用使用者測試您的組態。在已啟用SSL的Web瀏覽器中輸入 **https://*WebVPN_Gateway_IP_Address***;其中*WebVPN_Gateway_IP_Address*是WebVPN服務的IP地址。接受憑證並輸入使用者名稱和密碼後，系統會顯示類似此圖片的畫面。



- 檢查SSL VPN會話。在SDM應用中，按一下**Monitor**按鈕，然後按一下**VPN Status**。展開**WebVPN（所有上下文）**，展開相應的上下文，然後選擇**Users**。
- 檢查錯誤消息。在SDM應用中，按一下**Monitor**按鈕，按一下**Logging**，然後按一下**Syslog**頁籤。
- 檢視裝置的運行配置。在SDM應用程式中，按一下**Configure**按鈕，然後按一下**Additional Tasks**。展開**Configuration Management**，然後選擇**Config Editor**。

指令

有幾個**show**命令與WebVPN關聯。您可以在命令列介面(CLI)上執行這些命令，以顯示統計資訊和其他資訊。有關**show**命令的詳細資訊，請參閱驗證WebVPN配置。

註：Output Interpreter Tool(僅限註冊客戶)(OIT)支援某些**show**命令。使用OIT檢視**show**命令輸出的分析。

疑難排解

使用本節內容，對組態進行疑難排解。

註：復制過程中，**請勿中斷「將**檔案複製到伺服器」命令，或導航到其他視窗。操作中斷可能導致不完整的檔案儲存在伺服器上。

注意：使用者可以使用WebVPN客戶端上傳和下載新文件，但不允許使用者使用「將檔案複製到伺服器」命令覆蓋WebVPN上公共Internet檔案系統(CIFS)中的文件。當使用者嘗試替換伺服器上的檔案時，使用者會收到此消息：

```
Unable to add the file
```

程式

完成以下步驟，對組態進行疑難排解：

1. 確保客戶端禁用彈出視窗阻止程式。
2. 確保客戶端已啟用cookie。
3. 確保客戶端使用Netscape、Internet Explorer、Firefox或Mozilla Web瀏覽器。

指令

有幾個**debug**命令與WebVPN關聯。有關這些命令的詳細資訊，請參閱使用WebVPN Debug命令。

注意：使用**debug**指令可能會對思科裝置造成負面影響。使用**debug**指令之前，請先參閱有關Debug指令的重要資訊。

相關資訊

- Cisco IOS SSLVPN
- Cisco IOS SSLVPN問答
- 使用SDM的瘦客戶端SSL VPN(WebVPN)IOS配置示例
- 使用SDM的IOS上的SSL VPN客戶端(SVC)配置示例
- 技術支援與文件 - Cisco Systems