ASA with WebVPN and Single Sign-on using ASDM and NTLMv1 Configuration Example

Contents

Introduction

This document describes how to configure the Cisco Adaptive Security Appliance (ASA) to automatically pass WebVPN user login credentials, as well as secondary authentication, to servers that require additional login validation against Windows Active Directory running NT LAN Manager version 1 (NTLMv1). This feature is known as single-sign-on (SSO). It gives links configured for a specific WebVPN group the capability to pass on this user authentication information, thus eliminating multiple authentication prompts. This feature can also be used at the global or user configuration level.

Prerequisites

Requirements

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

- Ensure that NTLMv1 and Windows permissions for the target VPN users are configured. Consult your Microsoft documentation for more information on Windows domain access rights.

Components Used

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

- Cisco ASA 7.1(1)
- Cisco Adaptive Security Device Manager (ASDM) 5.1(2)
- Microsoft Internet Information Services (IIS)

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.

Conventions

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

Configure

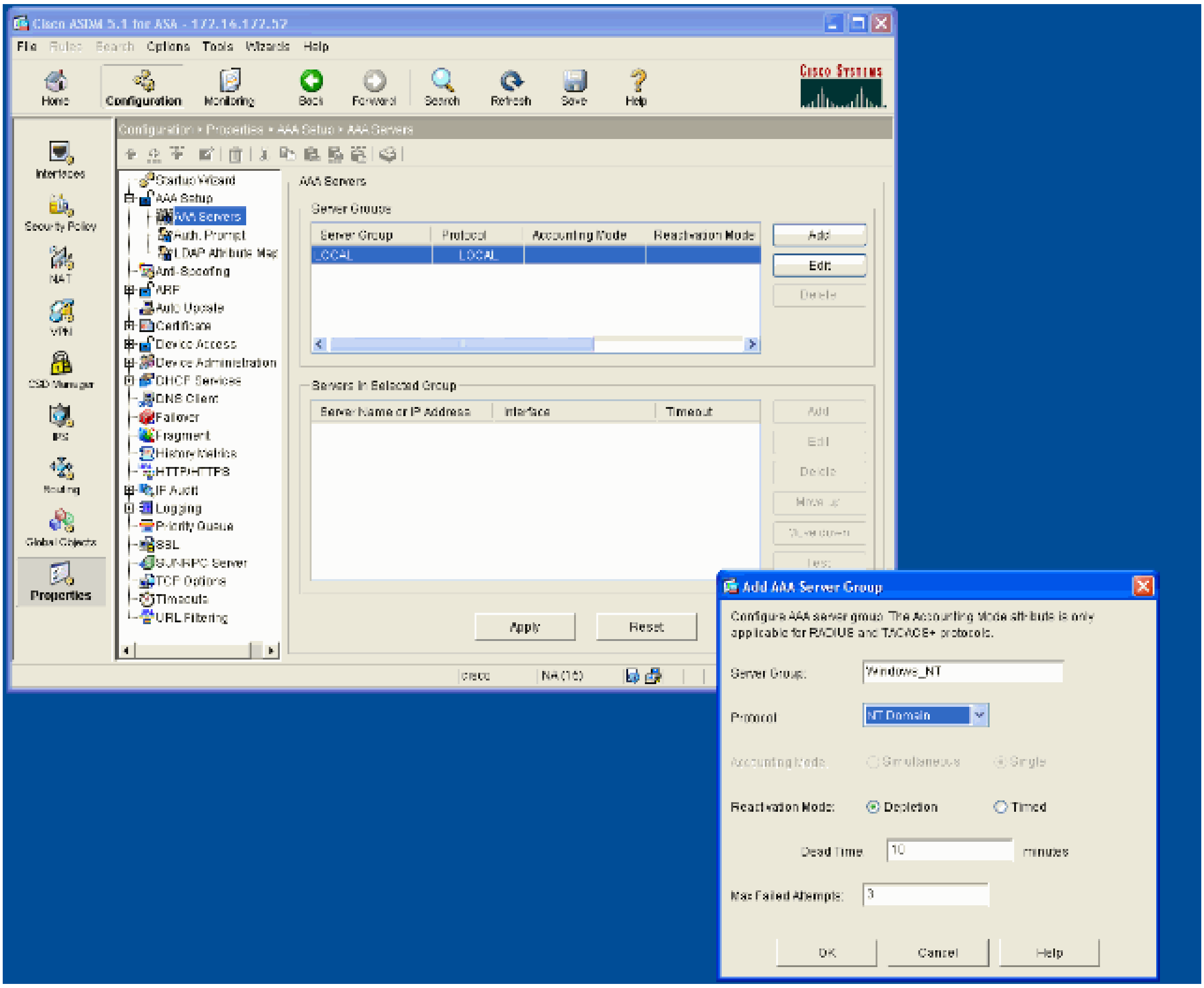
In this section, you are presented with the information to configure the ASA as a WebVPN server with SSO.

Note: Use the Command Lookup Tool (registered customers only) to obtain more information on the commands used in this section.

Add an AAA Server for Windows Domain Authentication

Complete these steps to configure the ASA to use a domain controller for authentication.

1. Select **Configuration > Properties > AAA Setup > AAA Servers** and click **Add**. Provide a name for the server group, such as Windows_NT, and choose **NT Domain** as the protocol.



Server Group	Protocol	Accounting Mode	Reactivation Mode
LOCAL	LOCAL		

Server Name or IP Address	Interface	Timeout

Add AAA Server Group

Configure AAA server group. The Accounting Mode attribute is only applicable for RADIUS and TACACS+ protocols.

Server Group: Windows_NT

Protocol: NT Domain

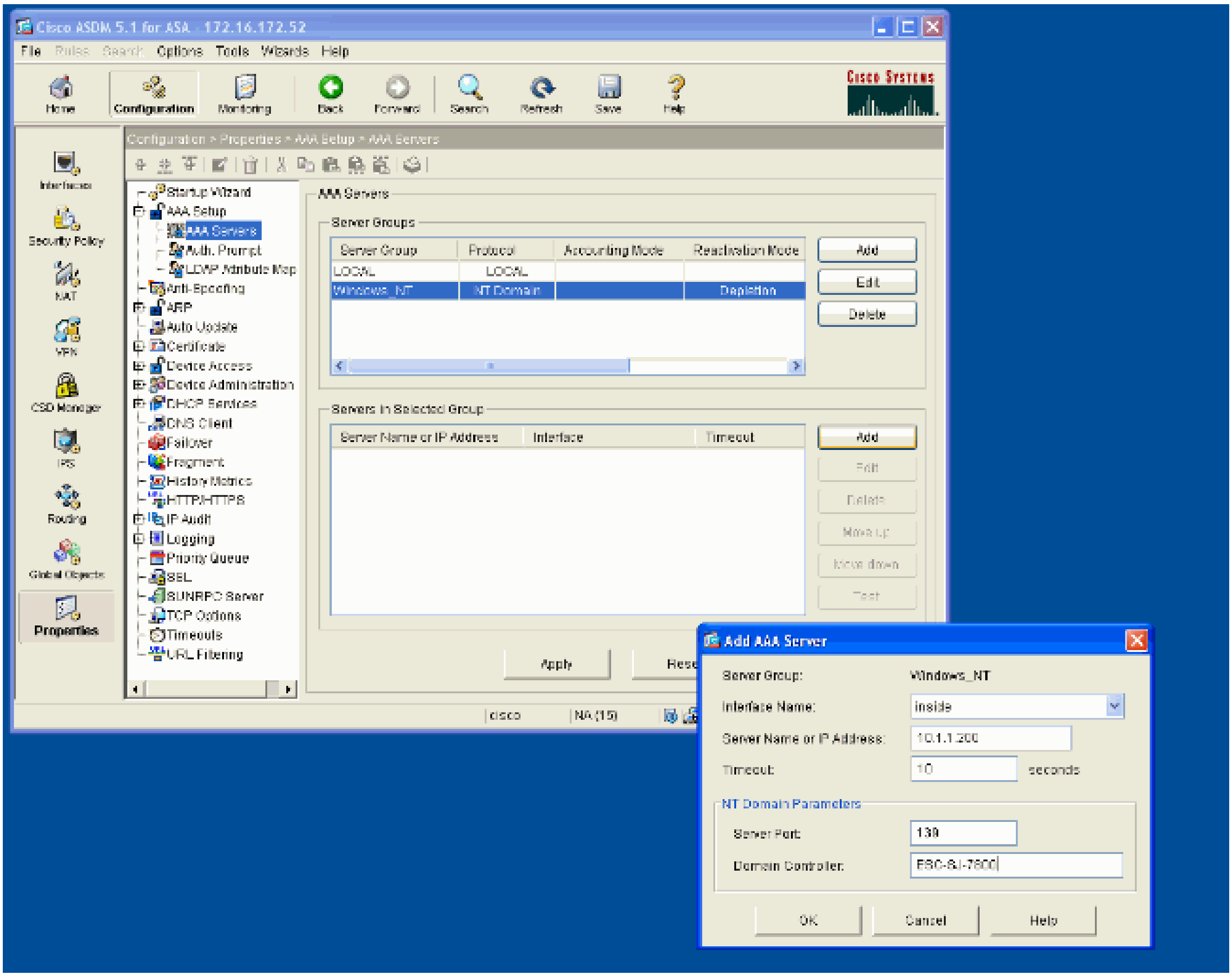
Accounting Mode: ○ Simultaneous ● Single

Reactivation Mode: ● Depletion ○ Timed

Dead Time: 10 minutes

Max Failed Attempts: 3

2. Add a Windows server.Select the newly created group and click **Add**. Select the interface where the server is located and enter the IP address and domain controller name. Be sure that the domain controller name is entered in all capital letters. Click **OK** when you are done.



Server Group	Protocol	Accounting Mode	Reactivation Mode
LOCAL	LOCAL		
Windows_NT	NT Domain		Depletion

Server Name or IP Address	Interface	Timeout

Add AAA Server

Server Group: Windows_NT

Interface Name: inside

Server Name or IP Address: 10.1.1.200

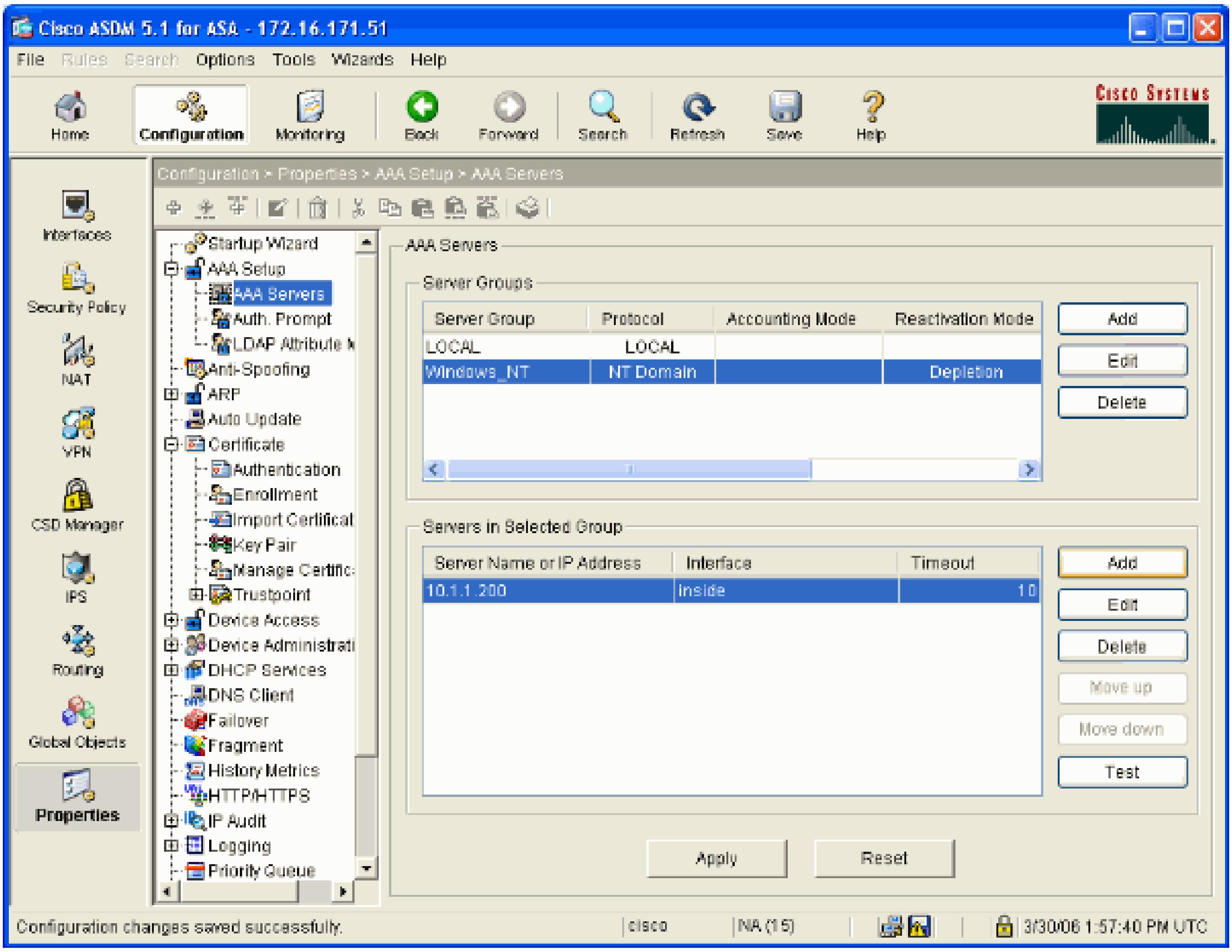
Timeout: 10 seconds

NT Domain Parameters

Server Port: 139

Domain Controller: ESC-SJ-7800

This window shows the completed AAA configuration:



Server Group	Protocol	Accounting Mode	Reactivation Mode
LOCAL	LOCAL		
Windows_NT	NT Domain		Depletion

Server Name or IP Address	Interface	Timeout
10.1.1.200	inside	10

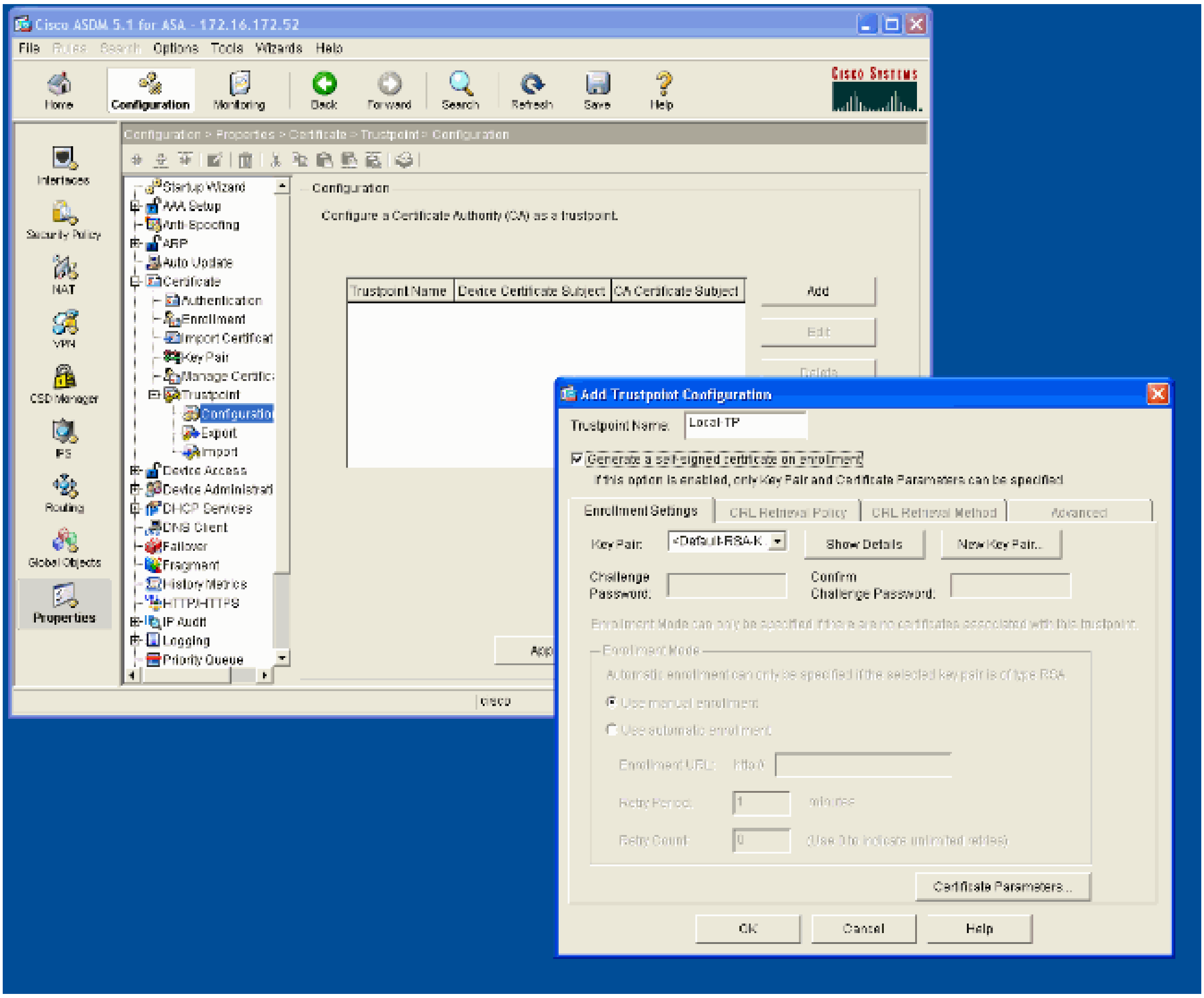
Configuration changes saved successfully. | cisco | NA (15) | 3/30/06 1:57:40 PM UTC

Create a Self-signed Certificate

Complete these steps to configure the ASA to use a self-signed certificate.

Note: In this example a self-signed certificate is used for simplicity. For other certificate enrollment options, such as enrolling with an external Certificate Authority, refer to Configuring Certificates.

1. Select **Configuration > Properties > Certificate > Trustpoint > Configuration** and click **Add**.
2. In the window that appears enter a Trustpoint Name such as Local-TP and check **Generate a self-signed certificate on enrollment**. Other options can be left with their default settings. Click **OK** when you are done.


Cisco ASDM 5.1 for ASA - 172.16.172.52
File Rules Search Options Tools Wizards Help
Home Configuration Monitoring Back Forward Search Refresh Save Help
Interfaces Security Policy NAT VPN CSD Manager IPS Routing Global Objects Properties
Startup Wizard AAA Setup Anti-Spoofing ARP Auto Update Certificate Authentication Enrollment Import Certificat Key Pair Manage Certific Trustpoint Configuratio Export Import Device Access Device Administrat DHCP Services DNS Client Failover Fragment History Metrics HTTP/HTTPS IP Audit Logging Priority Queue
Add Edit Delete
Enrollment Settings CRL Retrieval Policy CRL Retrieval Method Advanced
Show Details New Key Pair...
Certificate Parameters...
OK Cancel Help

Configuration > Properties > Certificate > Trustpoint > Configuration

Configuration

Configure a Certificate Authority (CA) as a trustpoint.

Trustpoint Name	Device Certificate Subject	CA Certificate Subject

Add Trustpoint Configuration

Trustpoint Name: Local-TP

☑ Generate a self-signed certificate on enrollment

If this option is enabled, only Key Pair and Certificate Parameters can be specified.

Key Pair: <Default-RSA-K

Challenge Password:

Confirm Challenge Password:

Enrollment Mode can only be specified if there are no certificates associated with this trustpoint.

Enrollment Mode

Automatic enrollment can only be specified if the selected key pair is of type RSA.

● Use manual enrollment

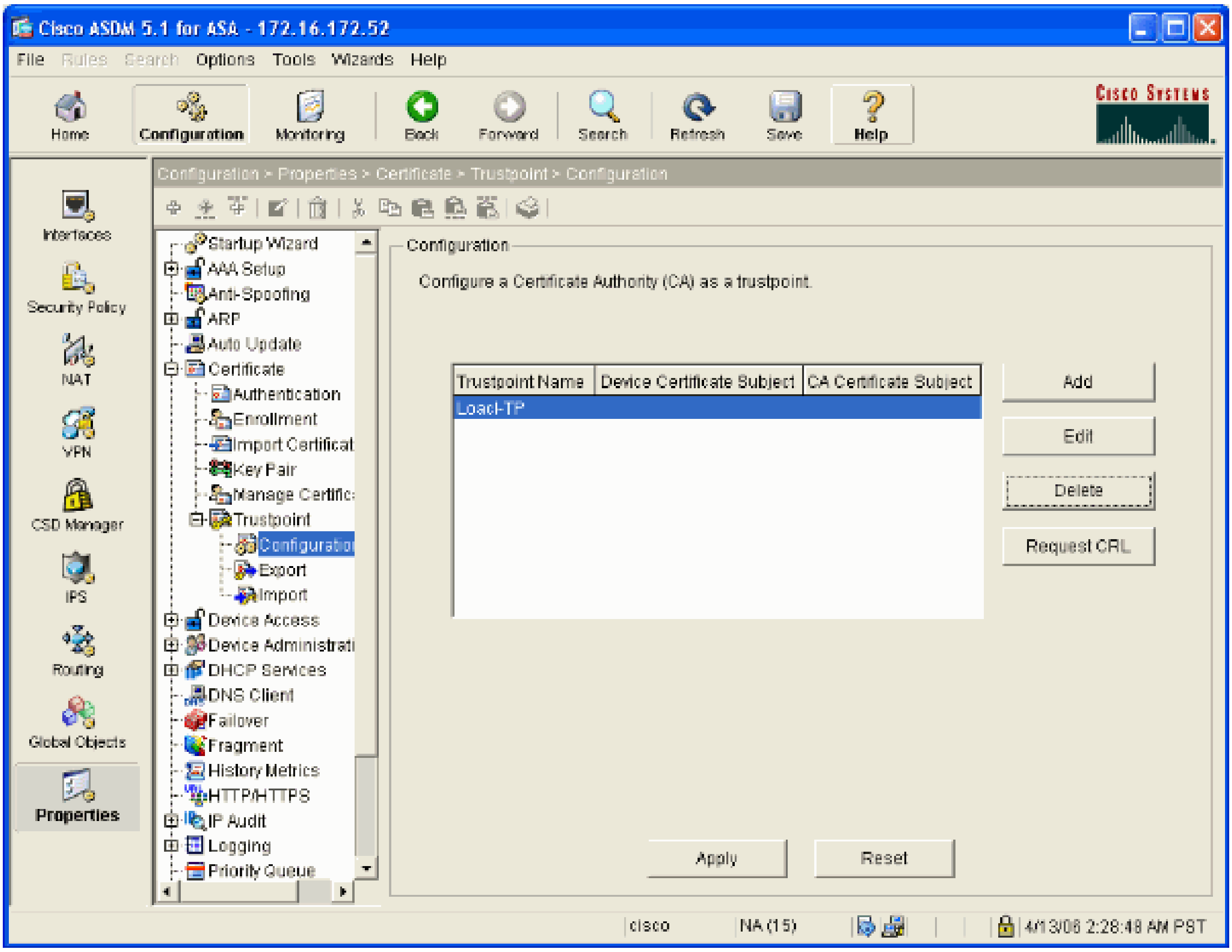
○ Use automatic enrollment

Enrollment URL: http://

Retry Period: 1 minutes

Retry Count: 0 (Use 0 to indicate unlimited retries)

This window shows the completed Trustpoint configuration:



Configuration

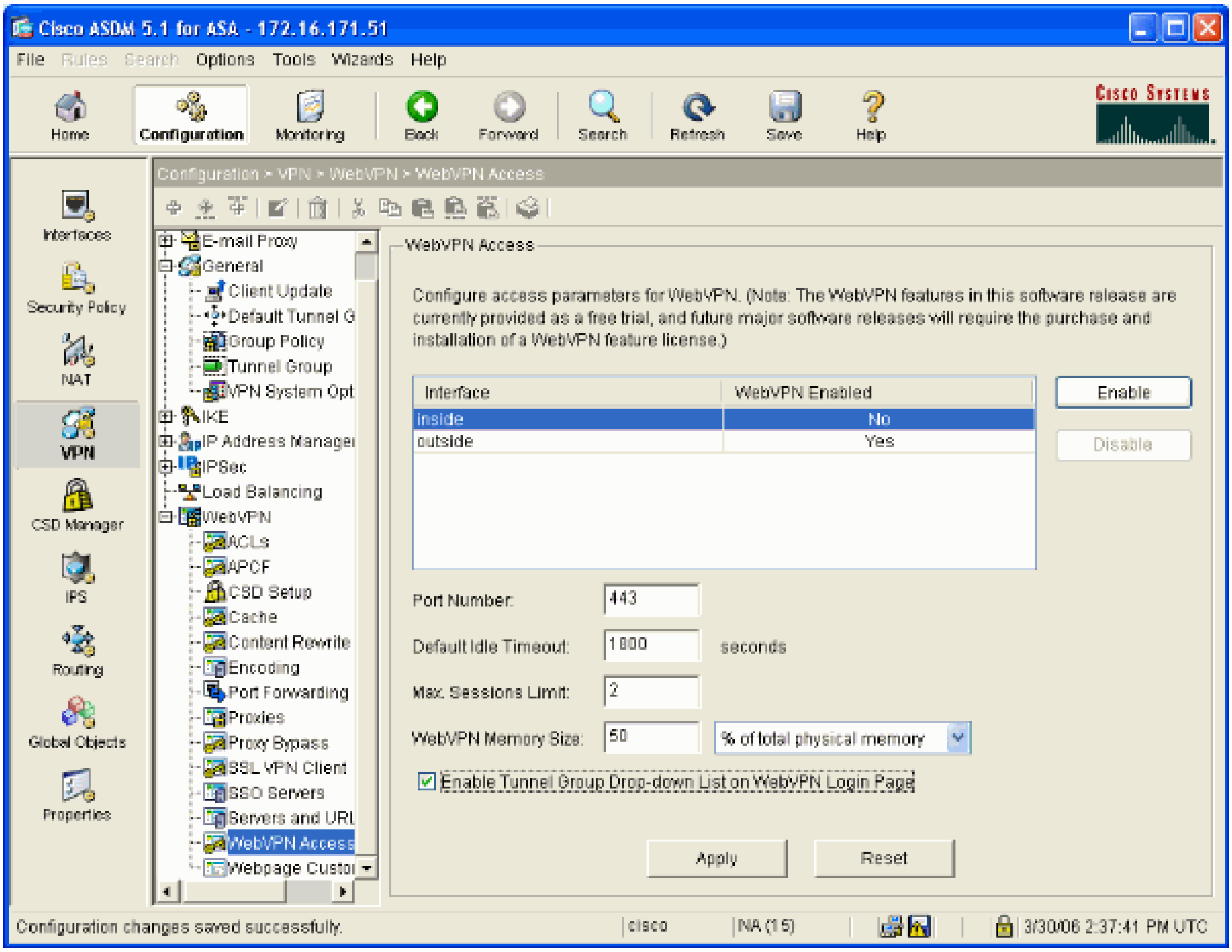
Configure a Certificate Authority (CA) as a trustpoint.

Trustpoint Name	Device Certificate Subject	CA Certificate Subject
Load-TP		

Enable WebVPN on the Outside Interface

Complete these steps to allow users outside your network to connect using WebVPN.

1. Select **Configuration > VPN > WebVPN > WebVPN Access**.
2. Select the desired interface, click **Enable**, and check **Enable Tunnel Group Drop-down List on WebVPN Login Page**.**Note:** If the same interface is used for WebVPN and ASDM access, you must change the default port for ASDM access from port 80 to a new port such as 8080. This is done under **Configuration > Properties > Device Access > HTTPS/ASDM**.**Note:** You can automatically redirect a user to port 443 in the event that a user navigates to **http://<ip_address>** instead of **https://<ip_address>**. Select **Configuration > Properties > HTTP/HTTPS**, choose the desired interface, click **Edit** and select **Redirect HTTP to HTTPS**.



WebVPN Access

Configure access parameters for WebVPN. (Note: The WebVPN features in this software release are currently provided as a free trial, and future major software releases will require the purchase and installation of a WebVPN feature license.)

Interface	WebVPN Enabled
inside	No
outside	Yes

Port Number: 443

Default Idle Timeout: 1800 seconds

Max. Sessions Limit: 2

WebVPN Memory Size: 50 % of total physical memory

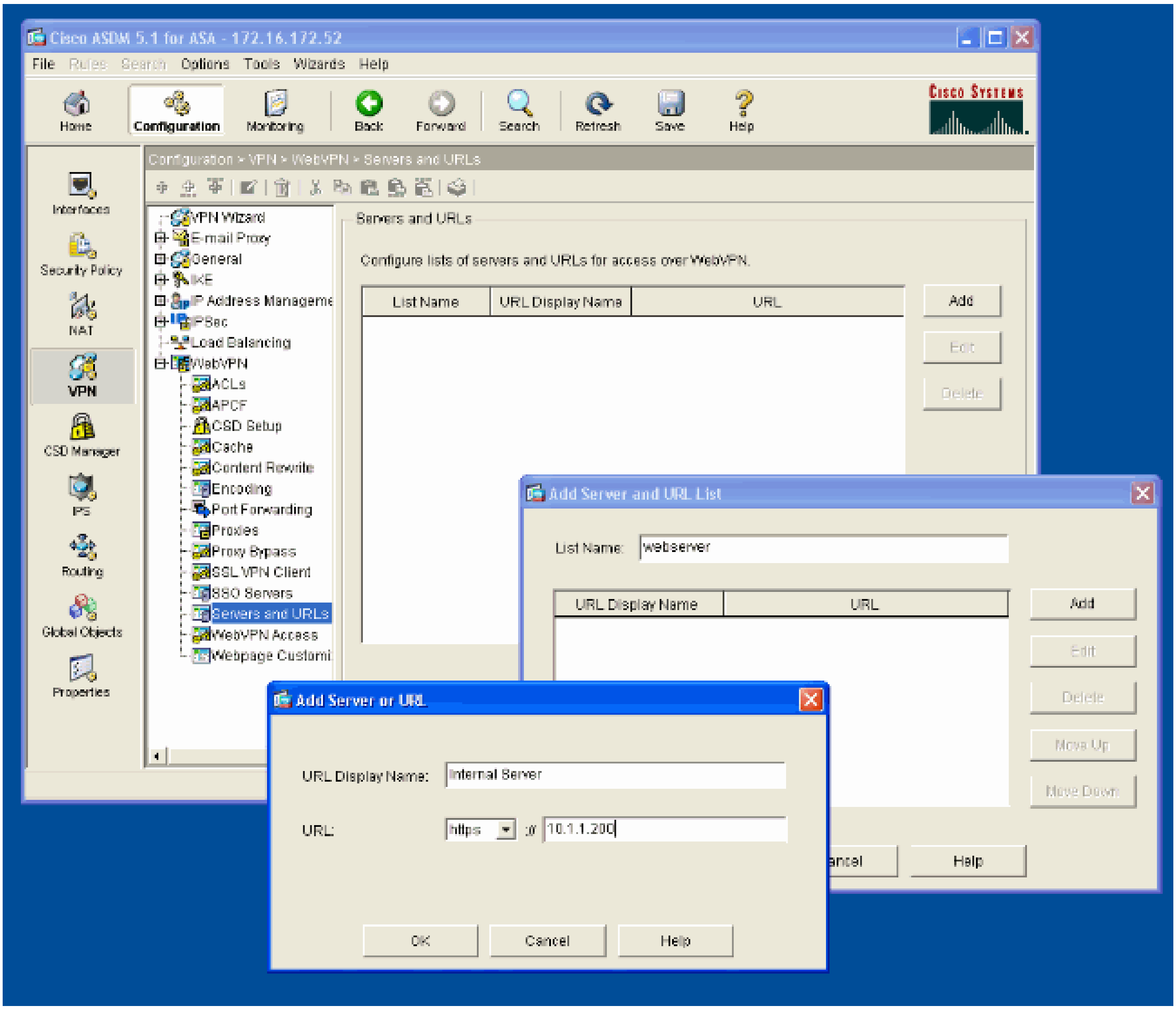
☑ Enable Tunnel Group Drop-down List on WebVPN Login Page

Configuration changes saved successfully. | cisco | NA (15) | 3/30/06 2:37:41 PM UTC

Configure a URL List for your Internal Server(s)

Complete these steps to create a list that contains the servers for which you want to grant your WebVPN users access.

1. Select **Configuration > VPN > WebVPN > Servers and URLs** and click **Add**.
2. Enter a name for the URL list. This name is not visible to end users. Click **Add**.
3. Enter the URL Display Name as it is to be displayed to users. Enter the URL information of the server. This should be how you normally access the server.



Configuration > VPN > WebVPN > Servers and URLs

Servers and URLs

Configure lists of servers and URLs for access over WebVPN.

List Name	URL Display Name	URL

Add Server and URL List

List Name: webserver

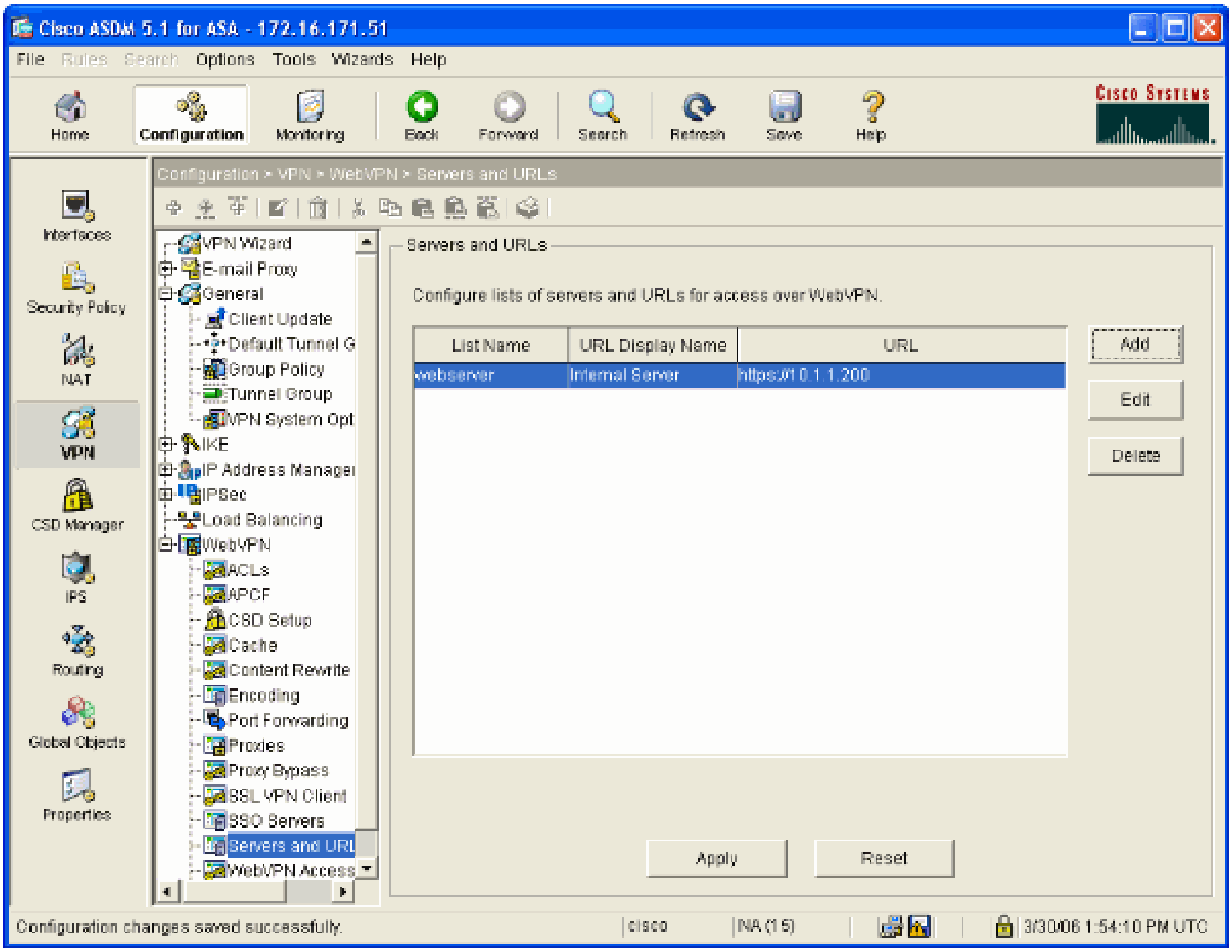
URL Display Name	URL

Add Server or URL

URL Display Name: Internal Server

URL: https ://10.1.1.200

4. Click **OK**, **OK**, and then **Apply**.



Configure lists of servers and URLs for access over WebVPN.

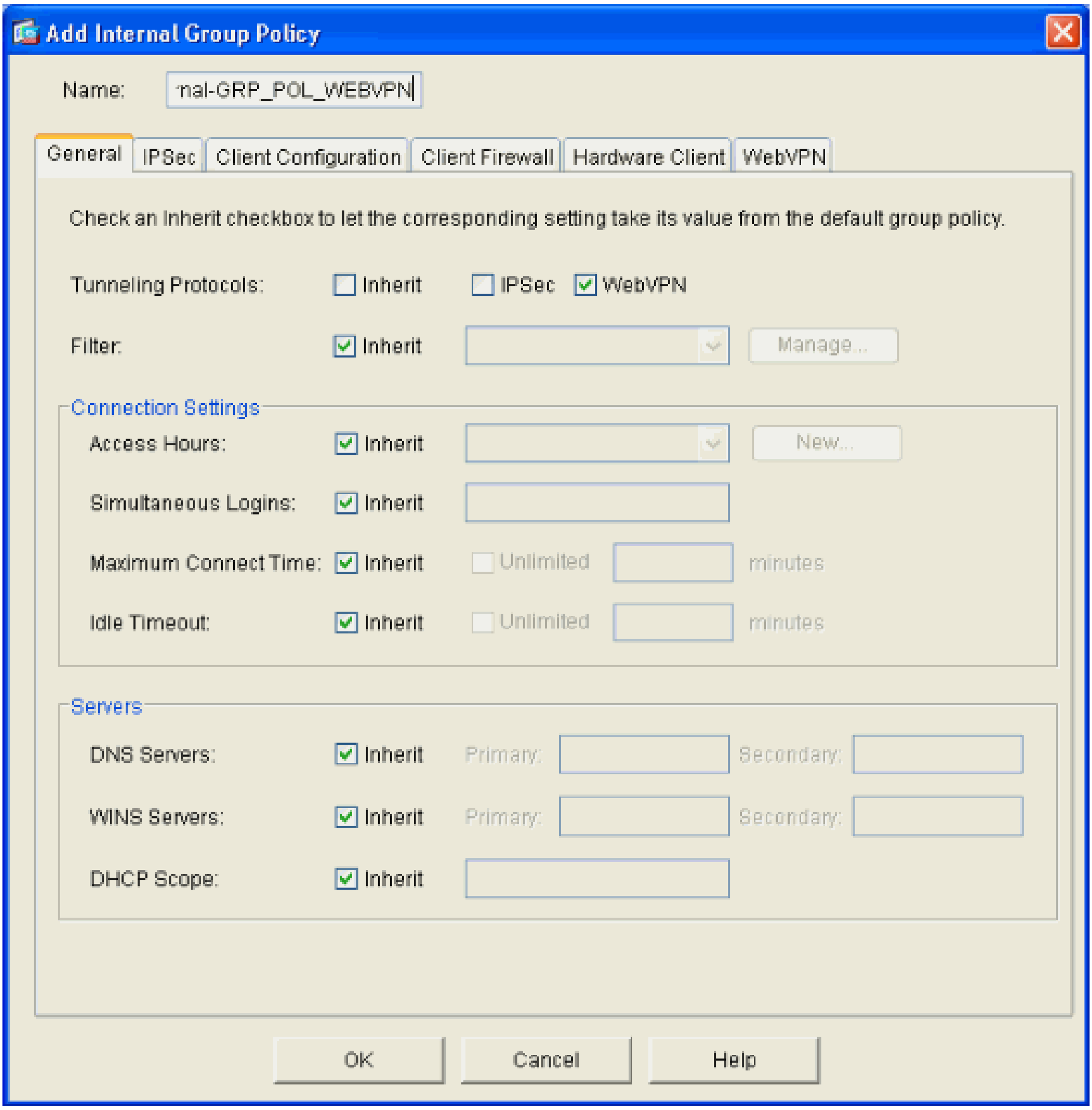
List Name	URL Display Name	URL
webserver	Internal Server	https://10.1.1.200

Configuration changes saved successfully.

Configure an Internal Group Policy

Complete these steps to configure a group policy for your WebVPN users.

1. Select **Configuration > VPN > General > Group Policy**, click **Add**, and select **Internal Group Policy**.
2. On the General tab, specify a policy name, such as Internal-Group_POL_WEBVPN. Then uncheck **Inherit** next to Tunneling Protocols and check
   WebVPN.



Name: nal-GRP_POL_WEBVPN

Check an Inherit checkbox to let the corresponding setting take its value from the default group policy.

Tunneling Protocols: □ Inherit □ IPSec ☑ WebVPN

Filter: ☑ Inherit

Connection Settings

Access Hours: ☑ Inherit

Simultaneous Logins: ☑ Inherit

Maximum Connect Time: ☑ Inherit □ Unlimited minutes

Idle Timeout: ☑ Inherit □ Unlimited minutes

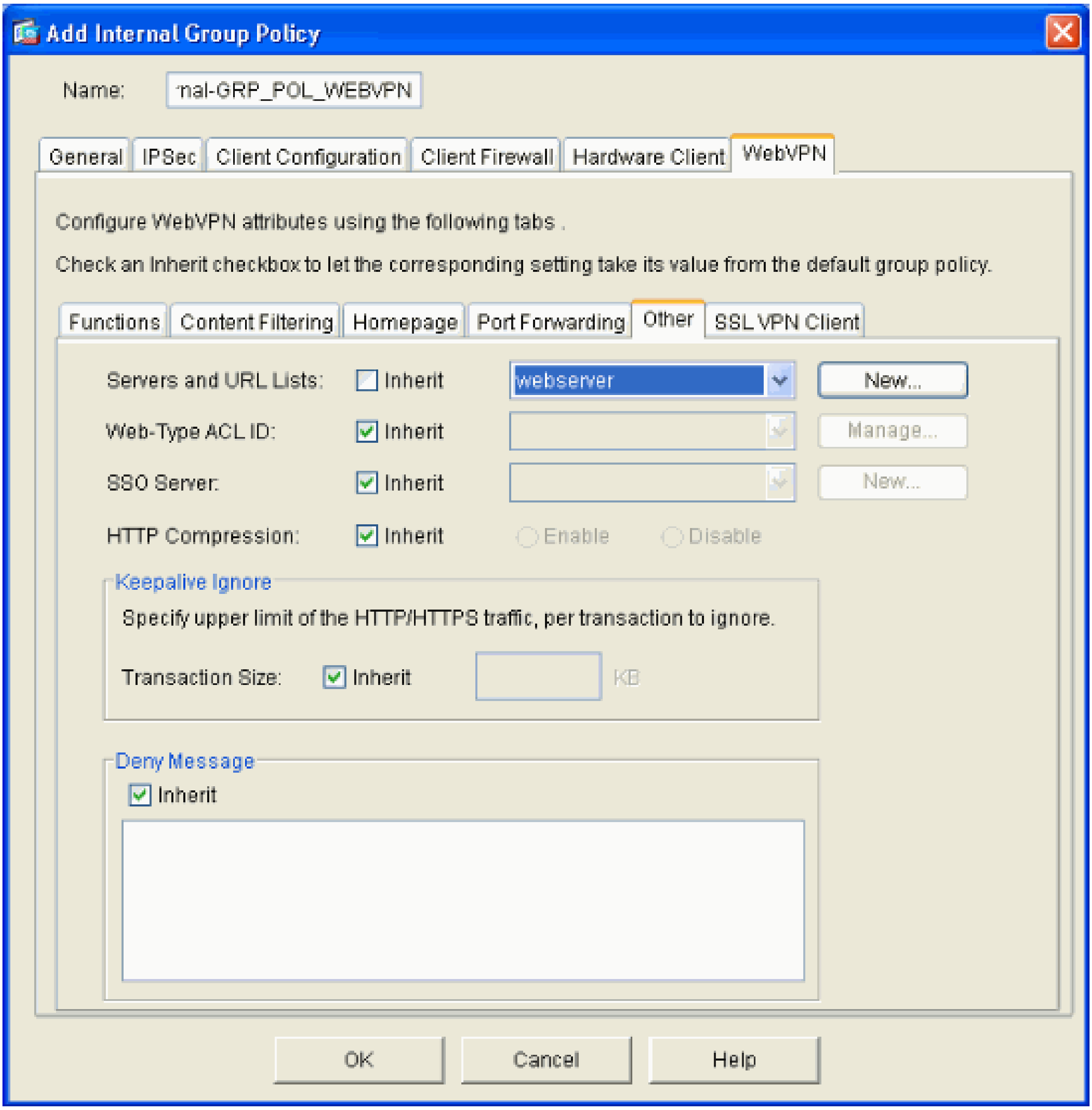
Servers

DNS Servers: ☑ Inherit Primary: Secondary:

WINS Servers: ☑ Inherit Primary: Secondary:

DHCP Scope: ☑ Inherit

3. On the WebVPN tab select the **Other** sub-tab. Uncheck **Inherit** next to Servers and URL Lists and select the URL List you configured from the drop-down list. Click **OK** when you are done.



Add Internal Group Policy

Name: nal-GRP_POL_WEBVPN

Configure WebVPN attributes using the following tabs .

Check an Inherit checkbox to let the corresponding setting take its value from the default group policy.

Servers and URL Lists: □ Inherit webserver New...

Web-Type ACL ID: ☑ Inherit Manage...

SSO Server: ☑ Inherit New...

HTTP Compression: ☑ Inherit ○ Enable ○ Disable

Keepalive Ignore

Specify upper limit of the HTTP/HTTPS traffic, per transaction to ignore.

Transaction Size: ☑ Inherit KB

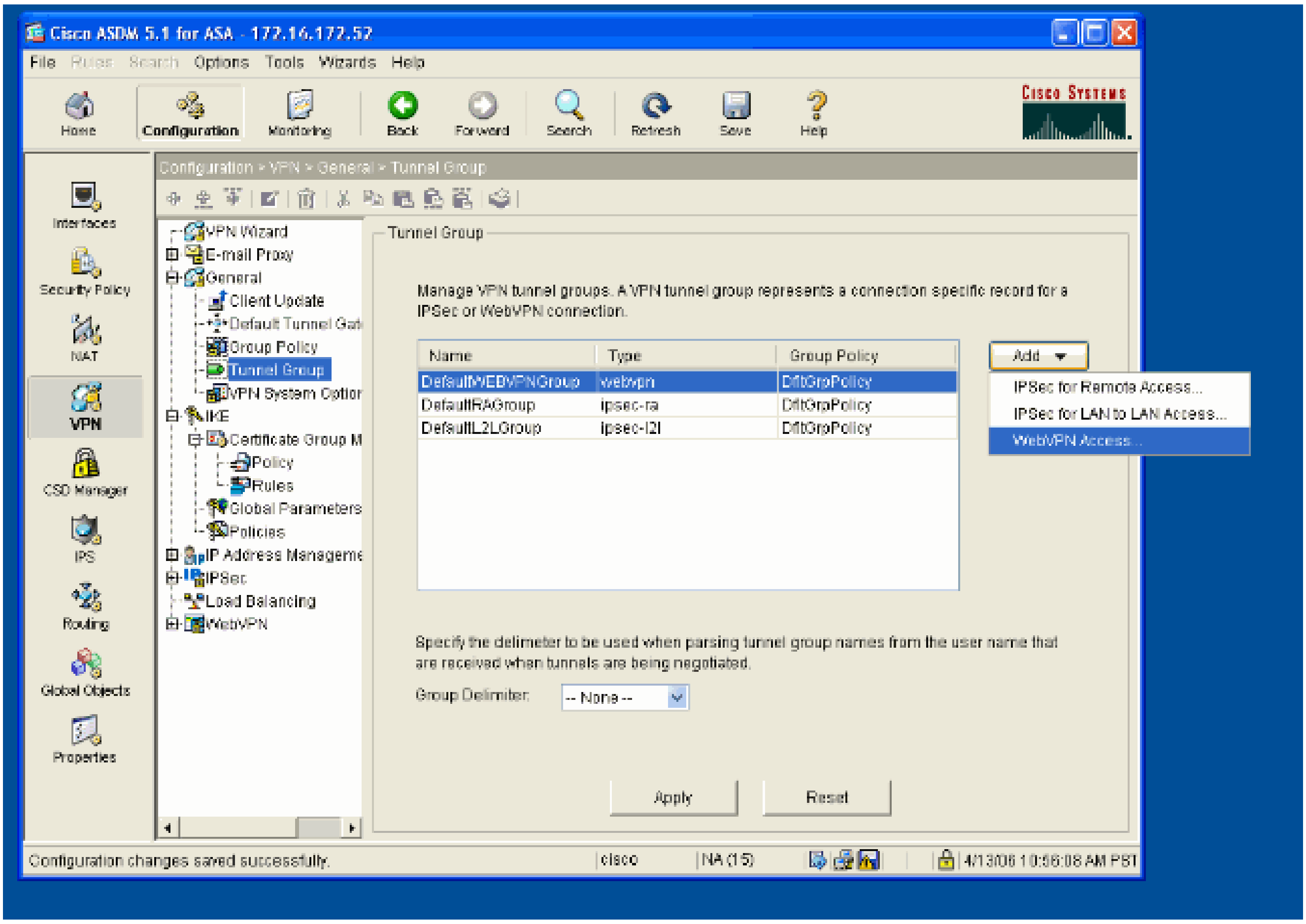
Deny Message

☑ Inherit

Configure a Tunnel Group

Complete these steps to configure a Tunnel Group for your WebVPN users.

1. Select **Configuration > VPN > General > Tunnel Group**, click **Add** and select **WebVPN Access...**



Tunnel Group

Manage VPN tunnel groups. A VPN tunnel group represents a connection specific record for a IPSec or WebVPN connection.

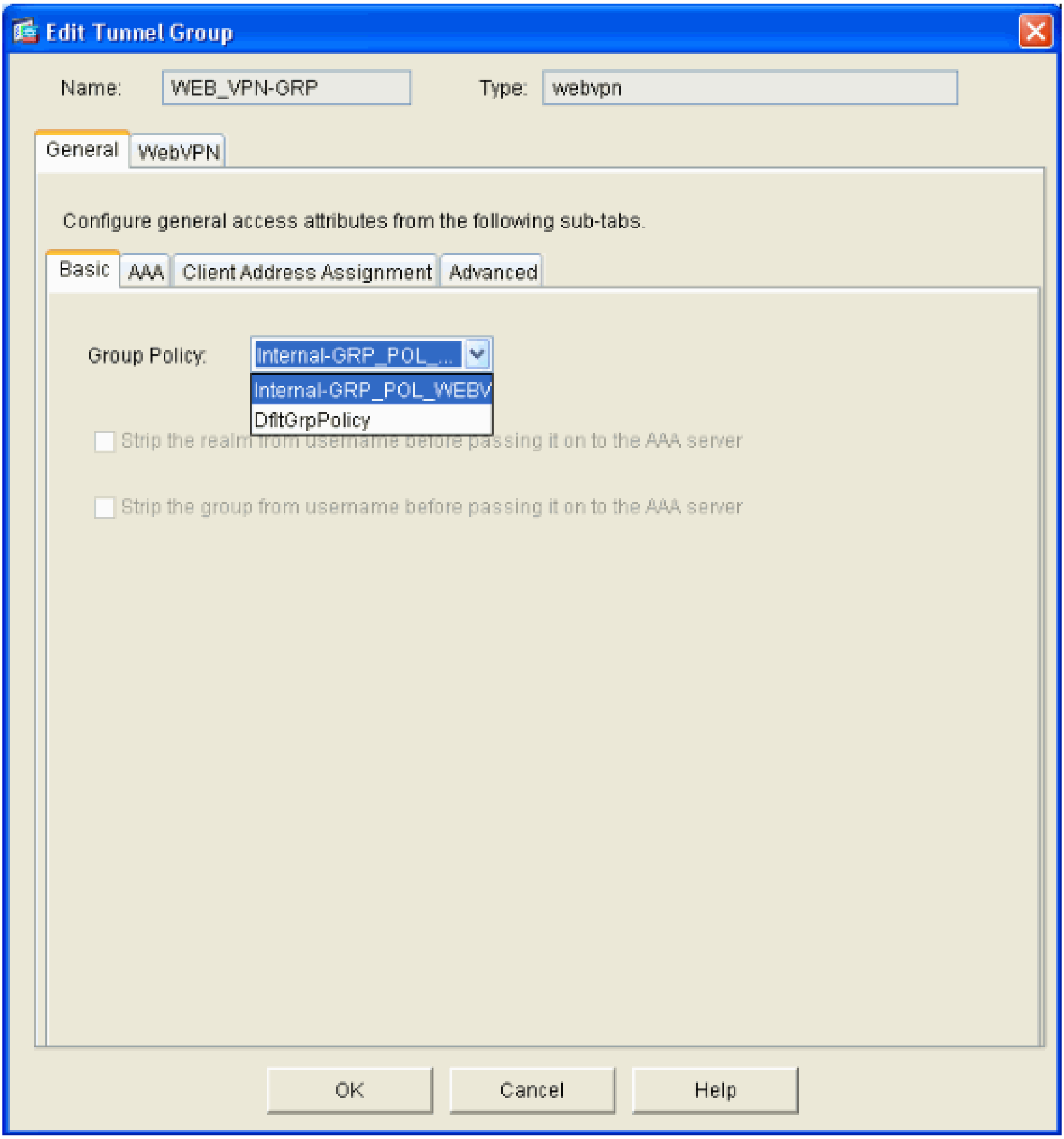
Name	Type	Group Policy
DefaultWEBVPNGroup	webvpn	DfltGrpPolicy
DefaultRAGroup	ipsec-ra	DfltGrpPolicy
DefaultL2LGroup	ipsec-l2l	DfltGrpPolicy

Specify the delimeter to be used when parsing tunnel group names from the user name that are received when tunnels are being negotiated.

Group Delimiter: -- None --

Configuration changes saved successfully. | cisco | NA (15) | 4/13/06 10:56:08 AM PST

2. Enter a name for the Tunnel Group, such as WEB_VPN-GRP. On the Basic tab select the Group Policy that you created and verify that the group Type is **webvpn**.



Name: WEB_VPN-GRP

Type: webvpn

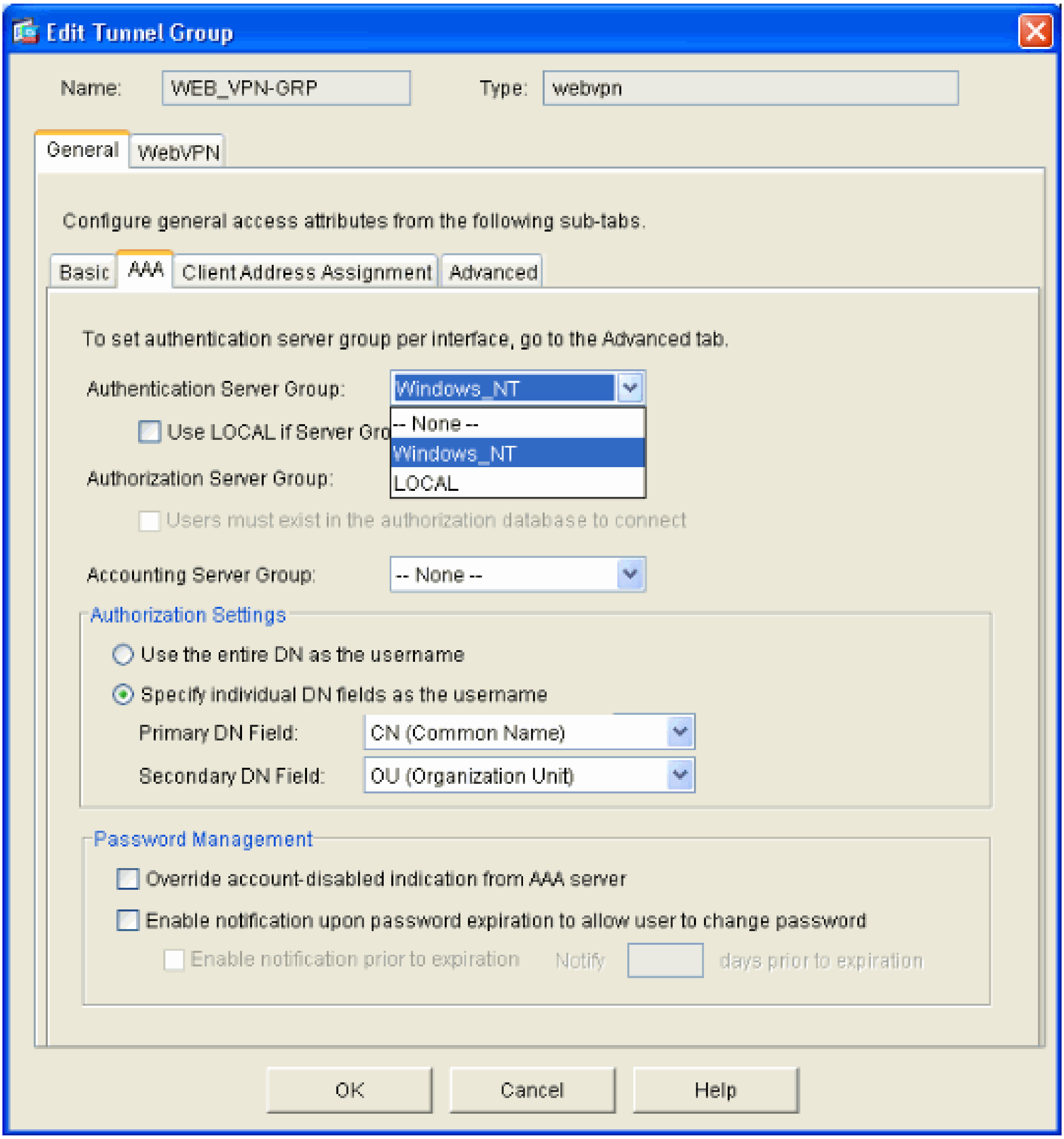
Configure general access attributes from the following sub-tabs.

Group Policy: Internal-GRP_POL_...

□ Strip the realm from username before passing it on to the AAA server

□ Strip the group from username before passing it on to the AAA server

3. Go to the AAA tab.For Authentication Server Group, choose the group you configured in order to enable NTLMv1 authentication with your domain controller.**Optional:** Check **Use LOCAL if Server Group Fails** to enable the use of the LOCAL user database in the event that the configured AAA group fails. This can help you troubleshoot at a later time.



Edit Tunnel Group

Name: WEB_VPN-GRP

Type: webvpn

General | WebVPN

Configure general access attributes from the following sub-tabs.

Basic | AAA | Client Address Assignment | Advanced

To set authentication server group per interface, go to the Advanced tab.

Authentication Server Group: Windows_NT

-- None --
Windows_NT
LOCAL

□ Use LOCAL if Server Gro

Authorization Server Group:

□ Users must exist in the authorization database to connect

Accounting Server Group: -- None --

Authorization Settings

○ Use the entire DN as the username

● Specify individual DN fields as the username

Primary DN Field: CN (Common Name)

Secondary DN Field: OU (Organization Unit)

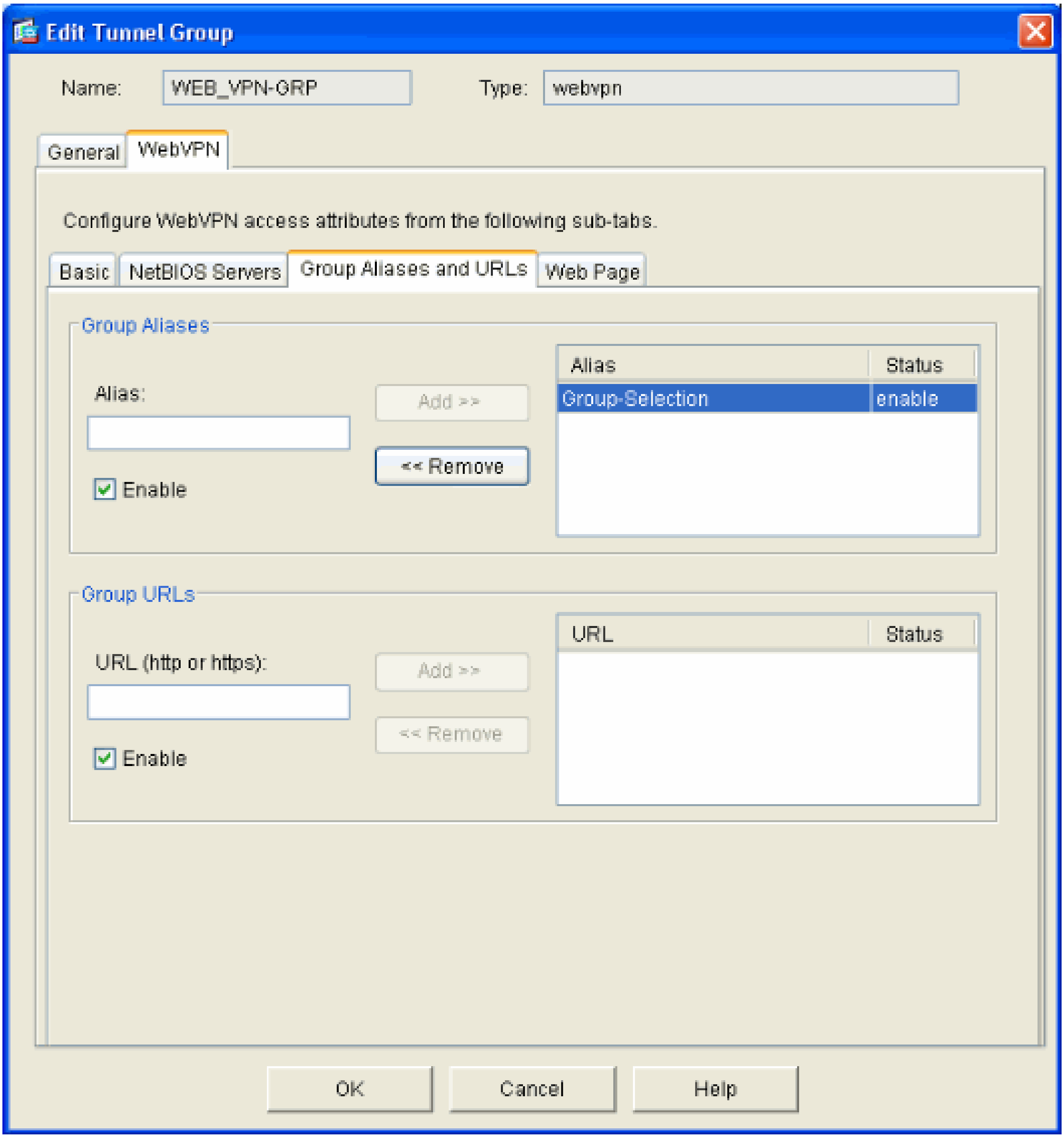
Password Management

□ Override account-disabled indication from AAA server

□ Enable notification upon password expiration to allow user to change password

□ Enable notification prior to expiration Notify days prior to expiration

4. Go to the WebVPN tab and then go to the **Group Aliases and URLs** sub-tab.
5. Enter an alias under Group Aliases and click **Add**. This alias appears in the drop-down list presented to WebVPN users at
login.



Name: WEB_VPN-GRP

Type: webvpn

Configure WebVPN access attributes from the following sub-tabs.

☑ Enable

Alias	Status
Group-Selection	enable

☑ Enable

URL	Status

6. Click **OK** and then **Apply**.

Configure Auto-Signon for a Server

Switch to the command line to enable SSO for your internal server(s).

Note: This step cannot be completed in the ASDM and must be accomplished using the command line. Refer to Accessing the Command-Line Interface for more information.

Use the **auto-signon** command to specify the network resource, such as a server, that you want to give your users access to. A single server IP address is configured here, but a network range such as **10.1.1.0 /24** can also be specified. Refer to the **auto-signon** command for more information.

```
ASA>enable ASA#configure terminal ASA(config)#webvpn ASA(config-webpvn)#auto-signon allow ip
10.1.1.200 255.255.255.255 auth-type ntlm ASA(config-webvpn)#quit ASA(config)#exit ASA#write
```

```
      memory
```

In this example output, the **auto-signon** command is configured for WebVPN globally. This command can also be used in WebVPN group configuration mode or WebVPN username configuration mode. The use of this command in WebVPN group configuration mode limits it to a particular group. Likewise, the use of this command in WebVPN username configuration mode limits it to an individual user. Refer to the **auto-signon** command for more information.

Final ASA Configuration

This document uses this configuration:

ASA Version 7.1(1)

```
ASA#show running-config : Saved : ASA Version 7.1(1) !
terminal width 200 hostname ASA domain-name cisco.com enable
password 8Ry2YjIyt7RRXU24 encrypted names ! interface
GigabitEthernet0/0 nameif outside security-level 0 ip address
172.16.171.51 255.255.255.0 ! interface GigabitEthernet0/1
nameif inside security-level 100 ip address 10.1.1.1
255.255.255.0 ! interface GigabitEthernet0/2 shutdown no
nameif no security-level no ip address ! interface
GigabitEthernet0/3 shutdown no nameif no security-level no ip
address ! interface Management0/0 shutdown no nameif no
security-level no ip address ! passwd 2KFQnbNIdI.2KYOU
encrypted ftp mode passive dns server-group DefaultDNS
domain-name cisco.com pager lines 24 mtu inside 1500 mtu
outside 1500 no failover asdm image disk0:/asdm512.bin no
asdm history enable arp timeout 14400 route outside 0.0.0.0
0.0.0.0 172.16.171.1 1 timeout xlate 3:00:00 timeout conn
1:00:00 half-closed 0:10:00 udp 0:02:00 icmp 0:00:02 timeout
sunrpc 0:10:00 h323 0:05:00 h225 1:00:00 mgcp 0:05:00 timeout
mgcp-pat 0:05:00 sip 0:30:00 sip_media 0:02:00 timeout uauth
0:05:00 absolute !--- AAA server configuration aaa-server
Windows_NT protocol nt aaa-server Windows_NT host 10.1.1.200
nt-auth-domain-controller ESC-SJ-7800 !--- Internal group
policy configuration group-policy Internal-GRP_POL_WEBVPN
internal group-policy Internal-GRP_POL_WEBVPN attributes vpn-
tunnel-protocol webvpn webvpn url-list value webserver
username cisco password Q/odgwmtmVIw4Dcm encrypted privilege
15 aaa authentication http console LOCAL aaa authentication
ssh console LOCAL aaa authentication enable console LOCAL
http server enable 8181 http 0.0.0.0 0.0.0.0 outside no snmp-
server location no snmp-server contact snmp-server enable
traps snmp authentication linkup linkdown coldstart !---
Trustpoint/certificate configuration crypto ca trustpoint
Local-TP enrollment self crl configure crypto ca certificate
chain Local-TP certificate 31 308201b0 30820119 a0030201
02020131 300d0609 2a864886 f70d0101 04050030 1e311c30
1a06092a 864886f7 0d010902 160d4153 412e6369 73636f2e
636f6d30 1e170d30 36303333 30313334 3930345a 170d3136
30333237 31333439 30345a30 1e311c30 1a06092a 864886f7
0d010902 160d4153 412e6369 73636f2e 636f6d30 819f300d
06092a86 4886f70d 01010105 0003818d 00308189 02818100
e47a29cd 56becf8d 99d6d919 47892f5a 1b8fc5c0 c7d01ea6
58f3bec4 a60b2025 03748d5b 1226b434 561e5507 5b45f30e
9d65a03f 30add0b5 81f6801a 766c9404 9cabcbde 44b221f9
b6d6dc18 496fe5bb 4983927f adabfb17 68b4d22c cddfa6c3
d8802efc ec3af7c7 749f0aa2 3ea2c7e3 776d6d1d 6ce5f748
e4cda3b7 4f007d4f 02030100 01300d06 092a8648 86f70d01
01040500 03818100 c6f87c61 534bb544 59746bdb 4e01680f
```

```
06a88a15 e3ed8929 19c6c522 05ec273d 3e37f540 f433fb38
7f75928e 1b1b6300 940b8dff 69eac16b af551d7f 286bc79c
e6944e21 49bf15f3 c4ec82d8 8811b6de 775b0c57 e60a2700
fd6acc16 a77abee6 34cb0cad 81dfaf5a f544258d cc74fe2d
4c298076 294f843a edda3a0a 6e7f5b3c quit !--- Tunnel group
configuration tunnel-group WEB_VPN-GRP type webvpn tunnel-
group WEB_VPN-GRP general-attributes authentication-server-
group Windows_NT default-group-policy Internal-GRP_POL_WEBVPN
tunnel-group WEB_VPN-GRP webvpn-attributes group-alias Group-
Selection enable telnet timeout 5 ssh timeout 5 console
timeout 0 ! class-map inspection_default match default-
inspection-traffic ! ! policy-map global_policy class
inspection_default inspect dns maximum-length 512 inspect ftp
inspect h323 h225 inspect h323 ras inspect netbios inspect
rsh inspect rtsp inspect skinny inspect esmtp inspect sqlnet
inspect sunrpc inspect tftp inspect sip inspect xdmcp !
service-policy global_policy global !--- WebVPN Configuration
webvpn enable outside url-list webserver "Internal Server"
https://10.1.1.200 1 tunnel-group-list enable auto-signon
allow ip 10.1.1.200 255.255.255.255 auth-type ntlm
Cryptochecksum:c80ac5f6232df50fc1ecc915512c3cd6 : end
```

Verify

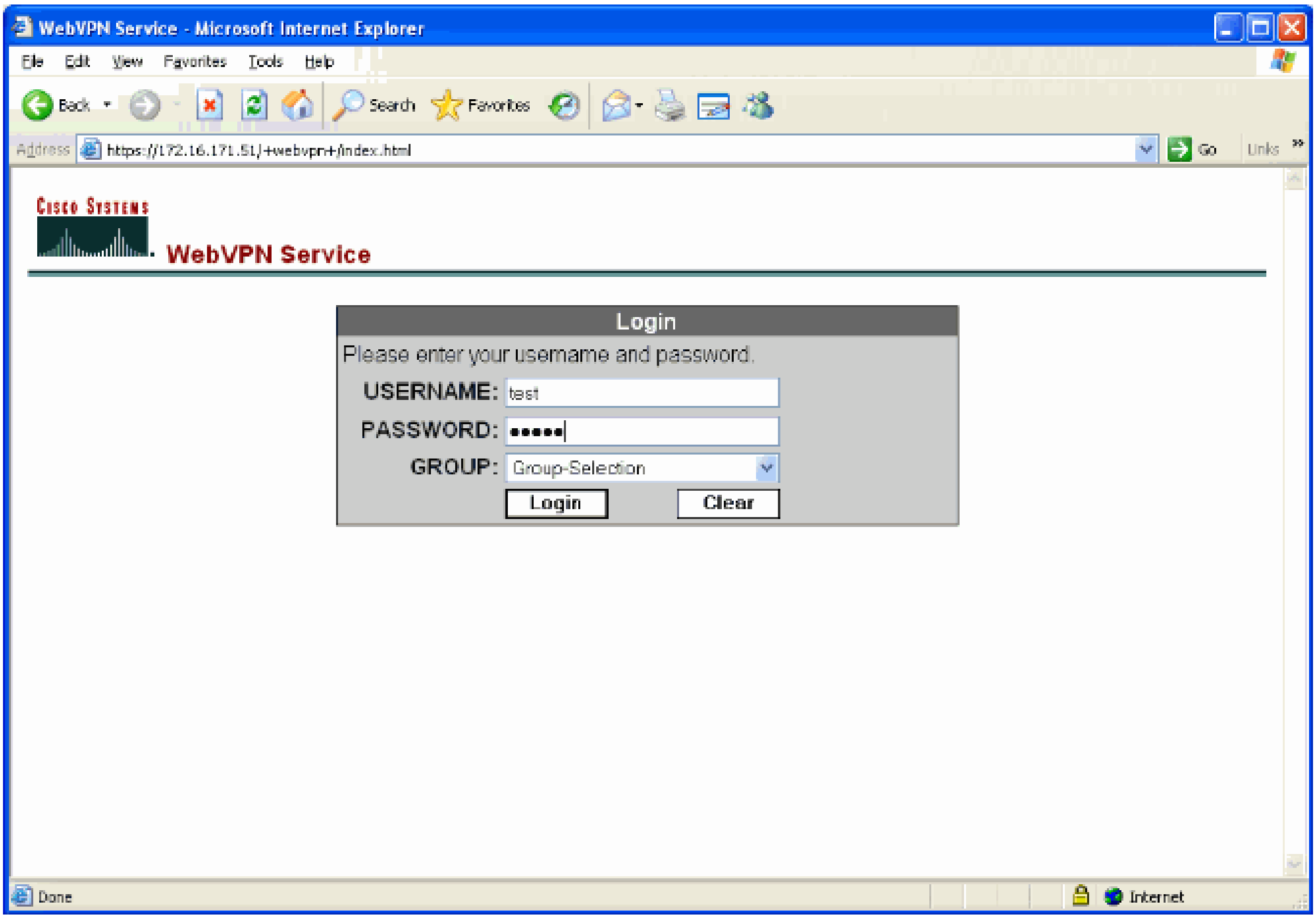
Use this section to confirm that your configuration works properly.

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

Test a WebVPN Login

Login as a user to test your configuration.

1. Attempt to login to the ASA with user information from your NT Domain. Select the group alias configured in step 5 under Configure a Tunnel Group.


WebVPN Service - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address
Go
Links
Cisco Systems
Done
Internet

https://172.16.171.51/+webvpn+/index.html

WebVPN Service

Login

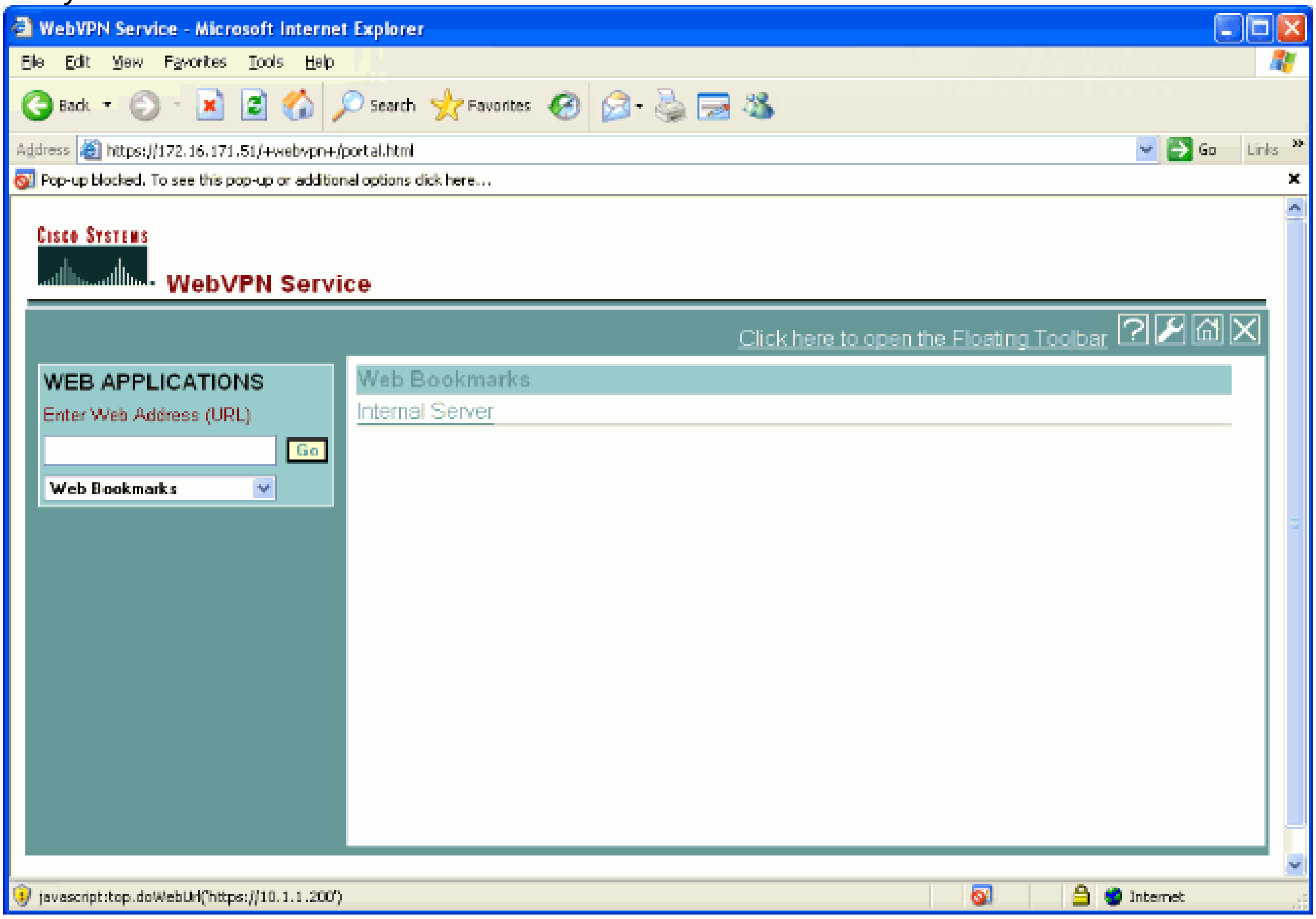
Please enter your username and password.

USERNAME: test

PASSWORD: •••••

GROUP: Group-Selection

2. Look for the link(s) configured to the internal server(s). Click on the link to verify.


WebVPN Service - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address
Go
Links
Cisco Systems
Go
Internet

https://172.16.171.51/+webvpn+/portal.html

Pop-up blocked. To see this pop-up or additional options click here...

WebVPN Service

Click here to open the Floating Toolbar

WEB APPLICATIONS

Enter Web Address (URL)

Web Bookmarks

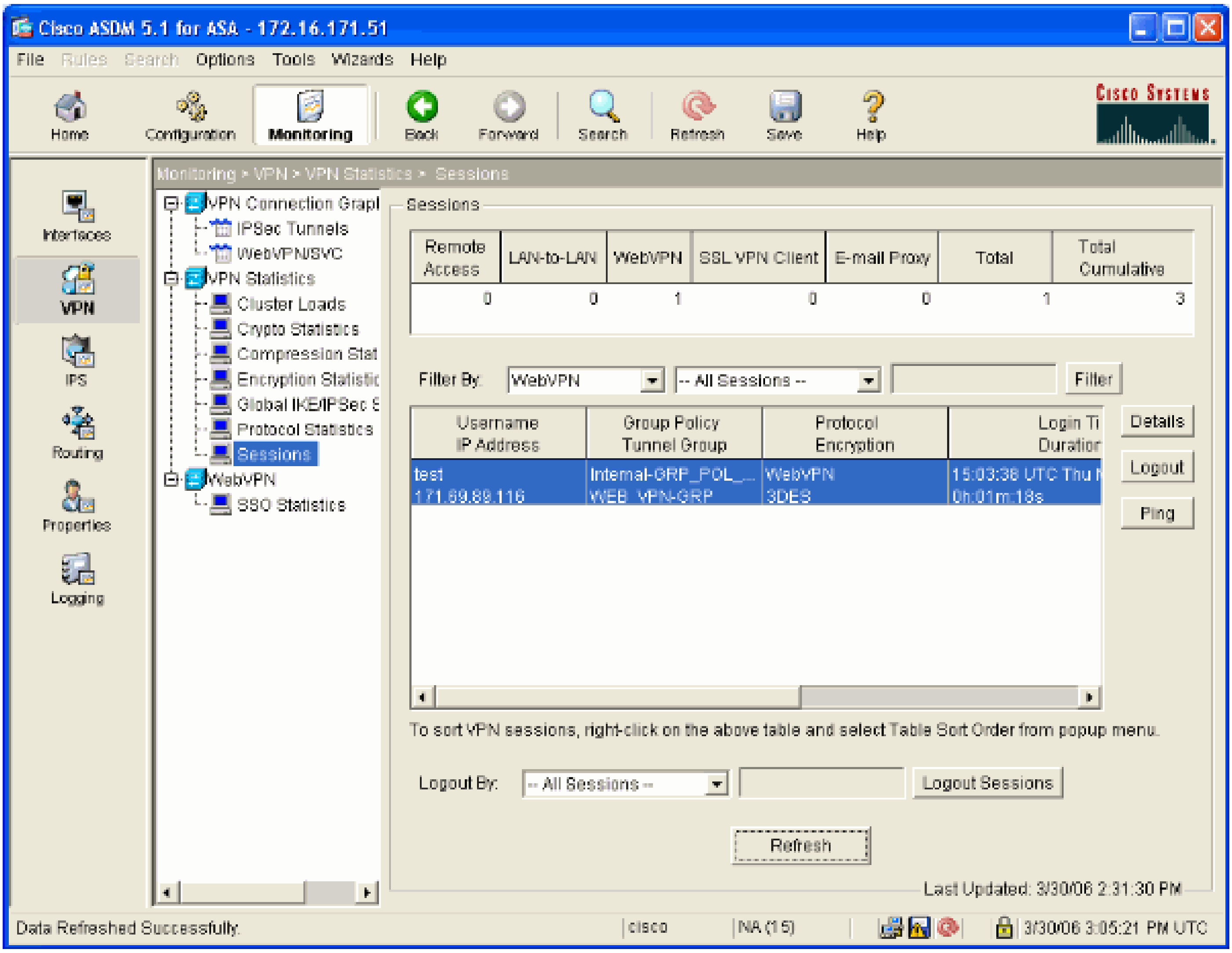
Web Bookmarks

Internal Server

javascript:top.doWebUrl('https://10.1.1.200')

Monitor Sessions

Select **Monitoring > VPN > VPN Statistics > Sessions** and look for a WebVPN session that belongs to the group configured in this document.



Sessions

Remote Access	LAN-to-LAN	WebVPN	SSL VPN Client	E-mail Proxy	Total	Total Cumulative
0	0	1	0	0	1	3

Filter By: WebVPN ▾ -- All Sessions -- ▾

Username IP Address	Group Policy Tunnel Group	Protocol Encryption	Login Ti Duratior
test 171.69.89.116	Internal-GRP_POL_... WEB_VPN-GRP	WebVPN 3DES	15:03:38 UTC Thu N 0h:01m:18s

To sort VPN sessions, right-click on the above table and select Table Sort Order from popup menu.

Logout By: -- All Sessions -- ▾

Last Updated: 3/30/06 2:31:30 PM

Data Refreshed Successfully. | cisco | NA (15) | 3/30/06 3:05:21 PM UTC

Debug a WebVPN Session

This output is a sample debug of a successful WebVPN session.

Note: Refer to Important Information on Debug Commands before you use **debug** commands.

```
ASA#debug webvpn 255 INFO: debug webvpn enabled at level 255 ASA# ASA#
webvpn_portal.c:ewaFormServe_webvpn_login[1570] webvpn_portal.c:http_webvpn_kill_cookie[385]
webvpn_auth.c:webvpn_auth[286] WebVPN: no cookie present!!
webvpn_portal.c:ewaFormSubmit_webvpn_login[1640] webvpn_portal.c:http_webvpn_kill_cookie[385]
webvpn_auth.c:http_webvpn_pre_authentication[1782] !--- Begin AAA WebVPN: calling AAA with
ewsContext (78986968) and nh (78960800)! WebVPN: started user authentication...
webvpn_auth.c:webvpn_aaa_callback[3422] WebVPN: AAA status = (ACCEPT)
webvpn_portal.c:ewaFormSubmit_webvpn_login[1640]
webvpn_auth.c:http_webvpn_post_authentication[1095] WebVPN: user: (test) authenticated. !---
End AAA webvpn_auth.c:http_webvpn_auth_accept[2093]
webvpn_session.c:http_webvpn_create_session[159]
webvpn_session.c:http_webvpn_find_session[136] WebVPN session created!
webvpn_session.c:http_webvpn_find_session[136] webvpn_db.c:webvpn_get_server_db_first[161]
webvpn_db.c:webvpn_get_server_db_next[202] traversing list: (webserver)
webvpn_portal.c:ewaFormServe_webvpn_cookie[1421] webvpn_auth.c:webvpn_auth[286]
webvpn_session.c:http_webvpn_find_session[136] webvpn_session.c:webvpn_update_idle_time[924]
WebVPN: session has been authenticated. webvpn_auth.c:webvpn_auth[286]
webvpn_session.c:http_webvpn_find_session[136] webvpn_session.c:webvpn_update_idle_time[924]
```

```
WebVPN: session has been authenticated. !--- Output supressed webvpn_auth.c:webvpn_auth[286]
webvpn_session.c:http_webvpn_find_session[136] webvpn_session.c:webvpn_update_idle_time[924]
WebVPN: session has been authenticated. webvpn_auth.c:webvpn_auth[286]
webvpn_session.c:http_webvpn_find_session[136] webvpn_session.c:webvpn_update_idle_time[924]
WebVPN: session has been authenticated. webvpn_auth.c:webvpn_auth[286]
webvpn_session.c:http_webvpn_find_session[136] webvpn_session.c:webvpn_update_idle_time[924]
WebVPN: session has been authenticated. webvpn_auth.c:webvpn_auth[286]
webvpn_session.c:http_webvpn_find_session[136] webvpn_session.c:webvpn_update_idle_time[924]
WebVPN: session has been authenticated. webvpn_auth.c:webvpn_auth[286]
webvpn_session.c:http_webvpn_find_session[136] webvpn_session.c:webvpn_update_idle_time[924]
WebVPN: session has been authenticated. webvpn_session.c:http_webvpn_find_session[136]
webvpn_session.c:webvpn_update_idle_time[924]
```

Troubleshoot

This section provides information you can use to troubleshoot your configuration.

- If the Group drop-down box is not present on the WebVPN login page, be sure that you have completed step 2 under Enable WebVPN on the Outside Interface and step 5 under Configure a Tunnel Group. If these steps are not completed and the drop-down is missing, authentication falls under the Default Group and likely fails.
- Although you cannot assign access rights to the user in ASDM or on the ASA, you can restrict users with Microsoft Windows access rights on your domain controller. Add the necessary NT group permissions for the web page the user authenticates to. Once the user logs into WebVPN with the permissions of the group, access to the specified pages is granted or denied accordingly. The ASA only acts as a proxy authentication host on behalf of the domain controller and all communications here are NTLMv1.
- You cannot configure SSO for Sharepoint over WebVPN because the Sharepoint Server does not support forms based authentication. As a result, the bookmarks with post or the post plugin procedure is not applicable here.

Related Information

- **Cisco ASA 5500 Series Adaptive Security Appliances**
- **Technical Support & Documentation - Cisco Systems**