ASA 8.x SSL VPN Deployment Guide

Document version number 1.0
Created by Robert Potts & Nelson Rodrigues

Introduction

This document demonstrates key SSL VPN features and capabilities of the ASA 5500 Adaptive Security Appliance. It can help you evaluate the security appliance for your own network security needs.

The Cisco ASA 5500 offers two types of SSL VPN, a key technology for remote access to corporate resources:

- Clientless SSL VPN provides access to Web applications, such as email, and corporate portals via Web browsers and Java components. It requires no client software.
- The AnyConnect SSL VPN Client provides direct access to corporate resources, just like an IPsec client.

Both clientless and AnyConnect client connections use posture assessment policies. You can define these policies to evaluate whether an endpoint is a corporate or public entity with the properly configured operating systems, firewall, antivirus software, and antispyware that you require.

Additional Information

This document provides configuration tasks for Dynamic Access Policies (DAP)—a powerful tool for controlling access to corporate resources regardless of the location or security posture of the end user device. For a more in-depth discussion about DAP, see the white paper *Dynamic Access Policies* at this URL:

http://wwwin.cisco.com/data-shared/stg/pmtool/VPN-Edition/dapwhitepaper.pdf

For detailed DAP configuration information, see the Understanding Policy Enforcement of Permissions and Attributes section of the *Cisco Security Appliance Command Line Configuration Guide, Version 8.0* at this URL:

http://www.cisco.com/en/US/partner/docs/security/asa/asa80/configuration/guide/extsvr.html#wp1598961

We continue to document additional use cases and publish them under Selected ASDM Configuration Tasks at the following URL:

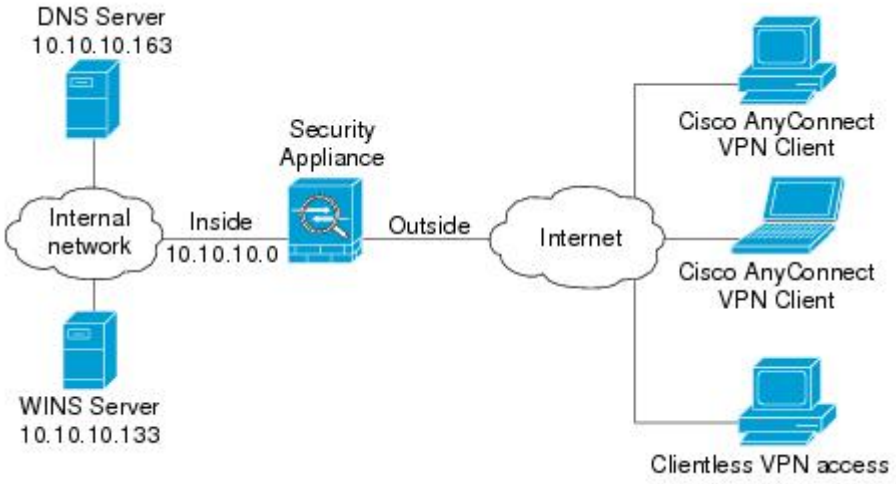
http://www.cisco.com/en/US/products/ps6121/products_installation_and_configuration_guides_list.html

Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

This document contains the following sections:

Example Network Topology

This document assumes the following network topology:



Initial Setup

This section provides instructions for setting up ASDM to manage the security appliance, configuring basic settings, and adding users.

Preparing for ASDM Access

To use ASDM, perform the following steps:

Step 1 Use an Ethernet cable to connect the MGMT interface to a switch or hub. To this same switch, connect a PC that will run ASDM to configure the security appliance.

Note You can use other interfaces inside for ASDM access if you choose.

Step 2 Configure your PC to use DHCP. This enables the PC to obtain an IP address automatically from the security appliance. It can then communicate with the security appliance and the Internet as well as run ASDM for configuration and management tasks.

Note Alternatively, you can assign a static IP address to your PC by selecting an address in the 192.168.1.0 subnet.

Valid addresses are 192.168.1.2 through 192.168.1.254, with a mask of 255.255.255.0 and default route of 192.168.1.1. When you connect other devices to any of the inside ports, make sure that they do not have the same IP address. The MGMT interface of the adaptive security appliance is assigned the IP address 192.168.1.1 by default, so this address is unavailable.

Step 3 Check the LINK LED on the MGMT interface.

When a connection is established, the LINK LED interface on the adaptive security appliance and the corresponding LINK LED on the switch or hub are solid green.

Step 4 Connect the console for CLI access, enabling ASDM access, assigning IP addresses to other interfaces and, if necessary, for debugging.

Step 5 To configure CLI commands you must be in global configuration mode. To enter config mode, at the prompt type **config t**.

```
asa# config t
asa(config)#
```

Note To display the running configuration, type **show runn** for the complete configuration or **show runn <command>** for specific output.

Step 6 To enable default ASDM access, enter the **http** commands.

```
asa(config)# http server enable
asa(config)# http 0.0.0.0 0.0.0.0  management
```

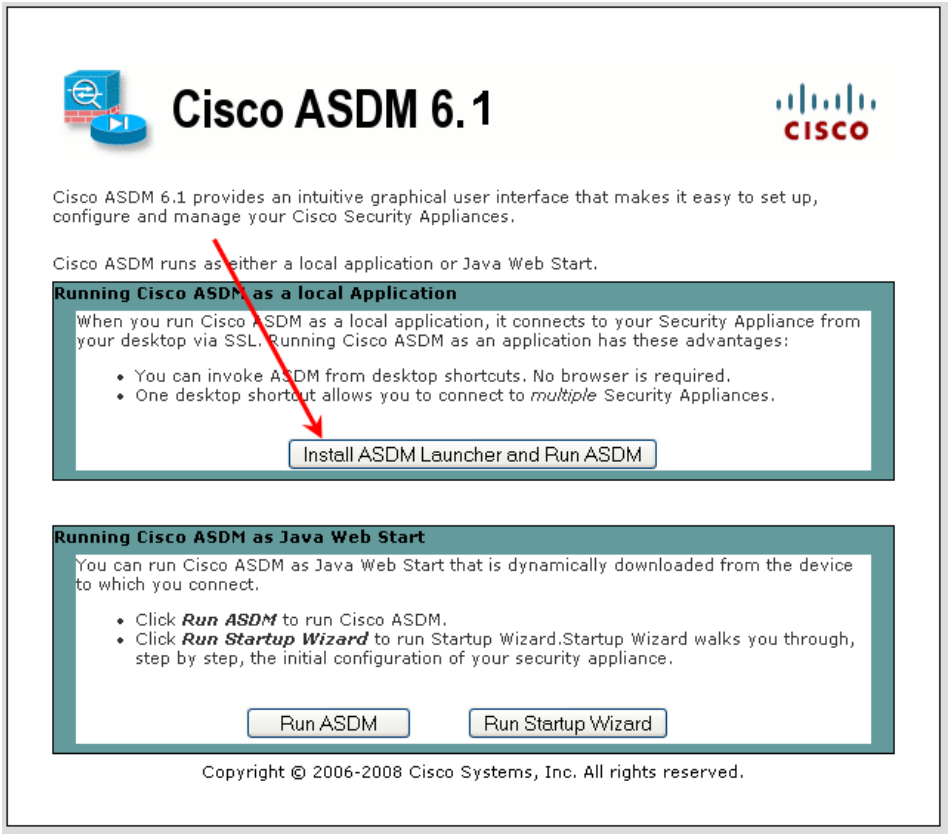
Step 7 Verify that the browser uses the same SSL version and encryption as the security appliance. The default ssl-server-version is any (SSL3.0 and TLSv1) and AES, 3DES and RC4 encryption ciphers.

```
asa(config)# show runn ssl    - displays the SSL encryption and server versions
asa(config)# ssl <options>     - sets the SSL configuration
```

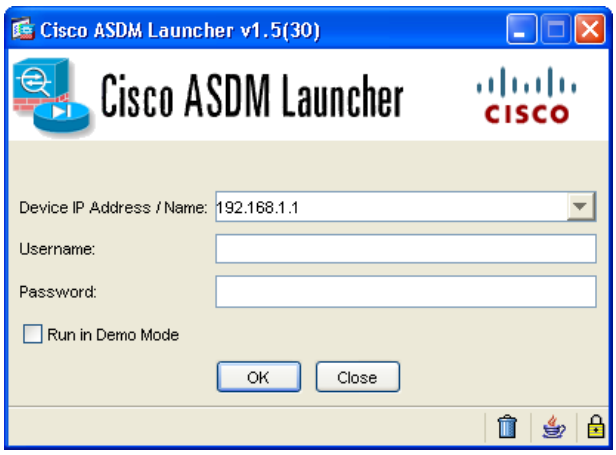
Step 8 The security appliance generates an SSL self-signed certificate for each interface when booting. For most lab environments you can use this certificate. Third party certificates (for example, Verisign) are also supported. For instructions on enrolling the security appliance for third party certificates, see Configuring Certs section in the *Cisco Security Appliance Command Line Configuration Guide* at http://www.cisco.com/en/US/docs/security/asa/asa80/configuration/guide/cert_cfg.html

Step 9 Launch ASDM by entering https://192.168.1.1/admin in the browser.

Step 10 The initial ASDM screen offers three operational options. Select **Install ASDM and Run ASDM**:



The security appliance downloads an ASDM .msi file to your PC. Double-click the .msi file to launch the ASDM installer. After installing, the Launcher window displays:



Step 11 Enter the username and password. The main ASDM screen displays.

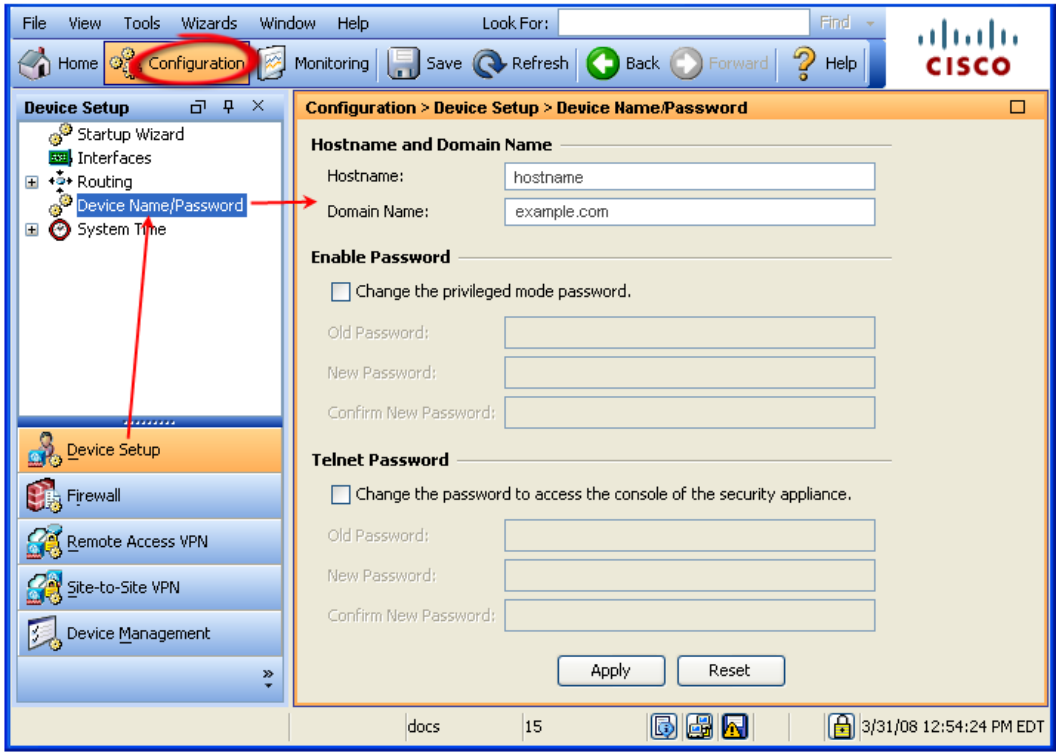
Step 12 To see the commands that ASDM sends to the security appliance, in the toolbar at the top of the main ASDM screen, go to Tools > Preferences > General tab, and check **Preview commands before sending them to the device**.

Configuring Hostname, DNS, Basic Routing

The hostname provides a name for the security appliance. Domain Name Server (DNS) provides name resolution for clientless SSL VPN connections. To configure a hostname, DNS, and basic routing on the security appliance, perform the following steps.

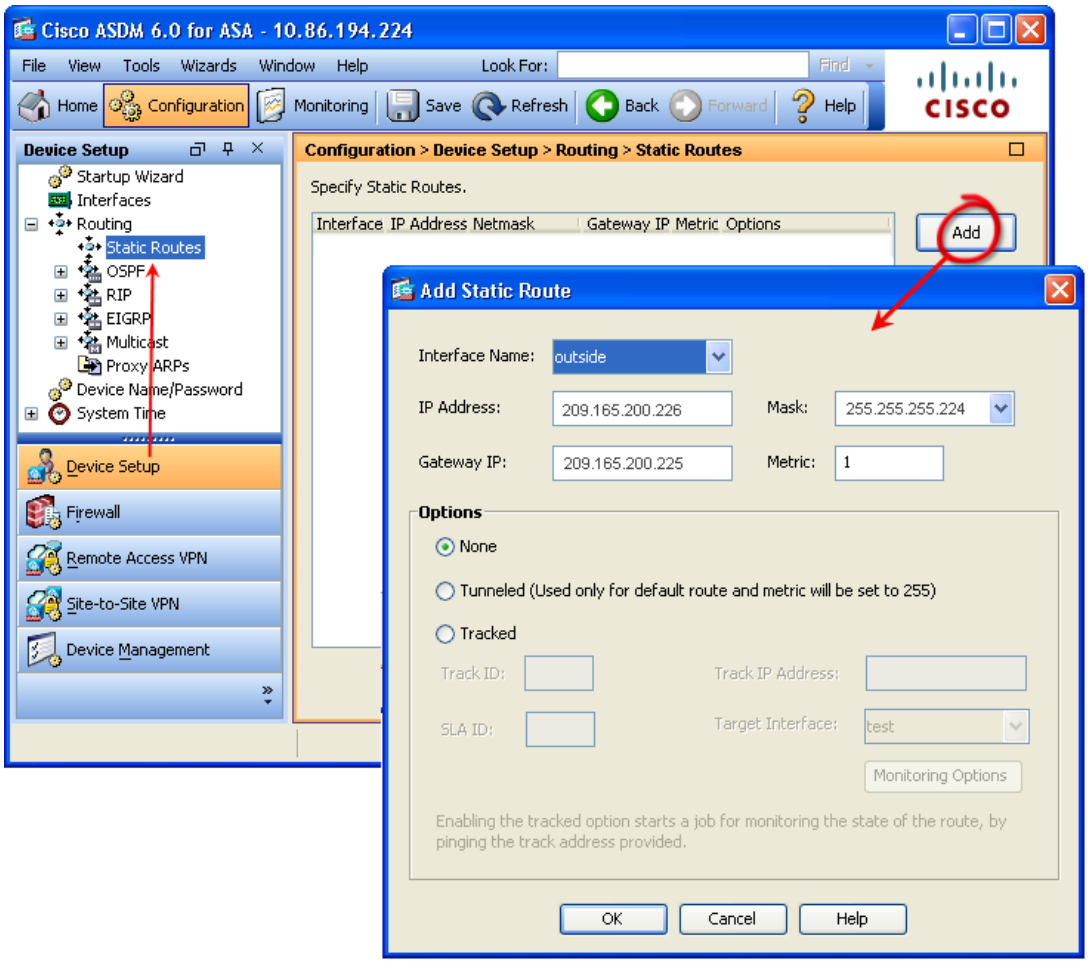
Step 1 Configure the ASA Hostname and Domain Name.

Navigate to Configuration > Device Setup > Device Name/Password. Enter the hostname and domain name:



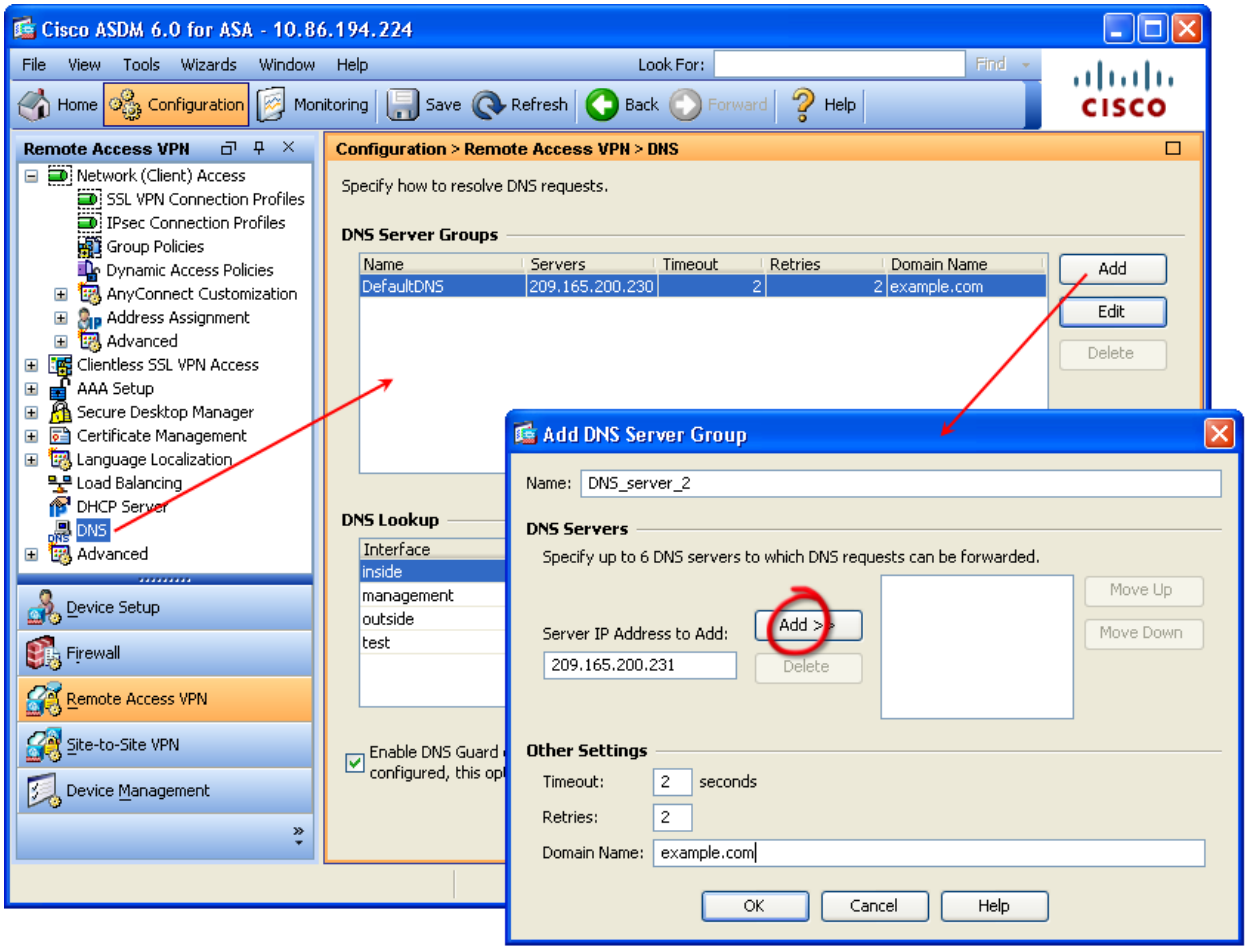
Step 2 Configure routing to access your internal resources. For lab environments we recommend you use static routes.

Navigate to: Configuration > Device Setup > Routing > Static Routes**.** Click Add and enter the static route information:



Step 3 Configure the DNS settings to use for clientless SSL VPN hostname resolution.

Navigate to Configuration> Remote Access VPN > DNS. Select To configure the DefaultDNS set of servers, select *DefaultDNS* and click **Add**. This is a global setting for all clientless sessions on the security appliance:

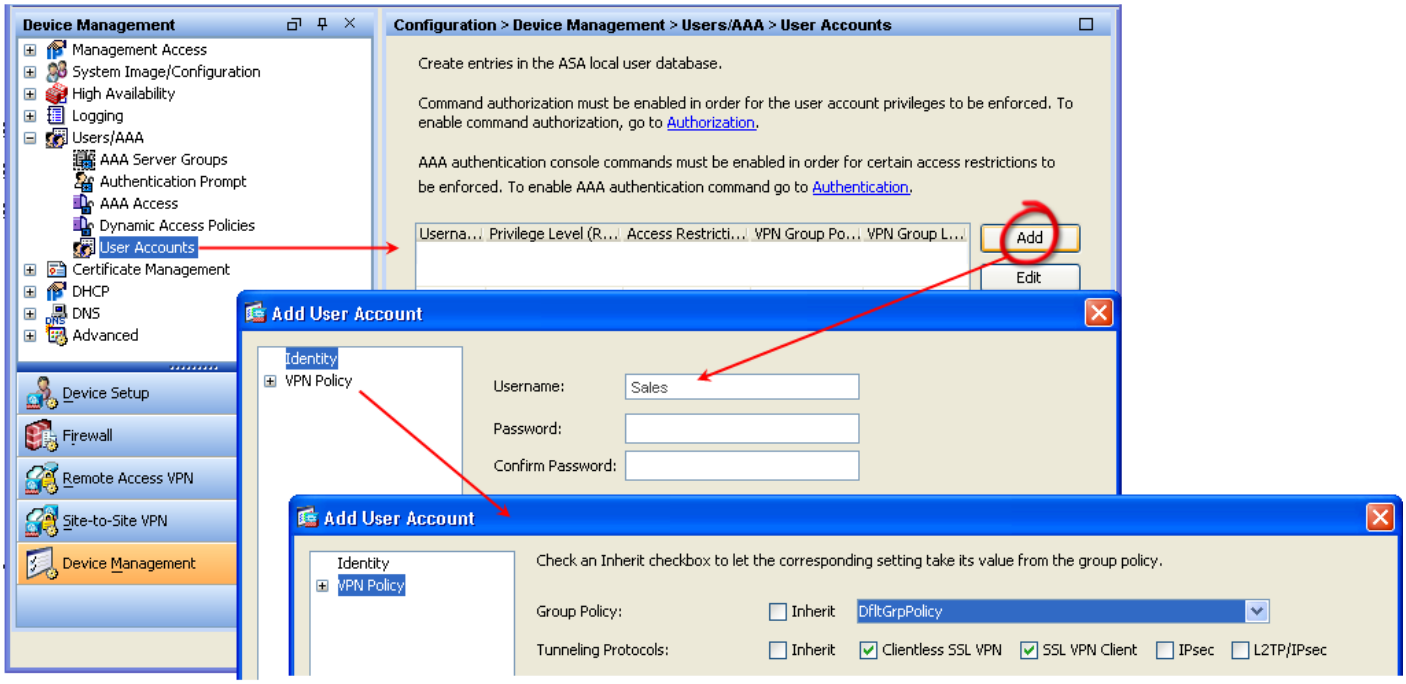


Configuring VPN Users in the Local Database

User accounts can be stored in a local database on the security appliance or on an external AAA server. This section shows how to configure VPN users in the local database:

Step 1 Navigate to Configuration> Device Management > Users/AAA > User Accounts. The Identify pane displays. Add three users: *Sales*, *Engineer*, and *Admin*.

Step 2 In the VPN Policy pane, assign these users to the default group-policy, *DfltGrpPolicy*. You can select the Tunneling Protocols in this screen or inherit the setting from DfltGrpPolicy.



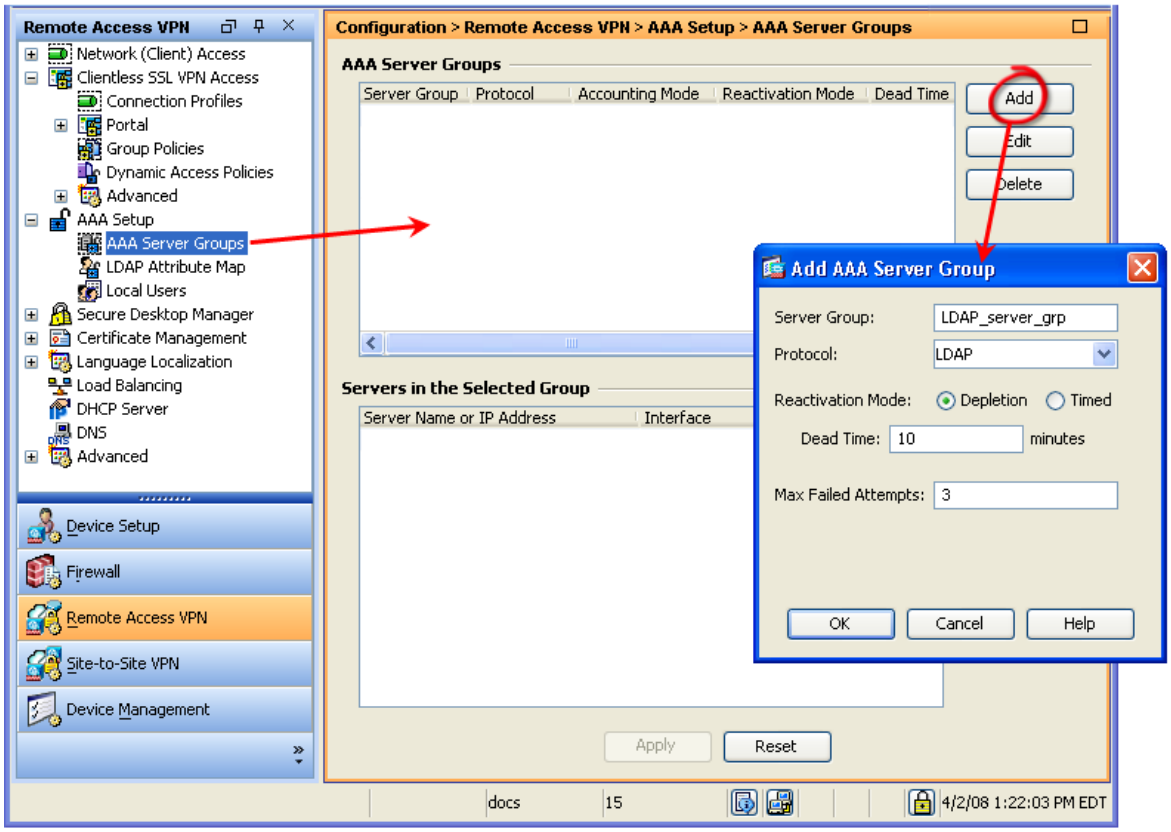
Configuring VPN Users on Active Directory/LDAP

The security appliance supports various authentication methods: RSA one-time passwords, Radius, Kerberos, LDAP, NT Domain, TACACS, Local/Internal, digital certificates, and a combination of both authentication and certificates.

To configure VPN users on an Active Directory LDAP AAA server, follow these steps.

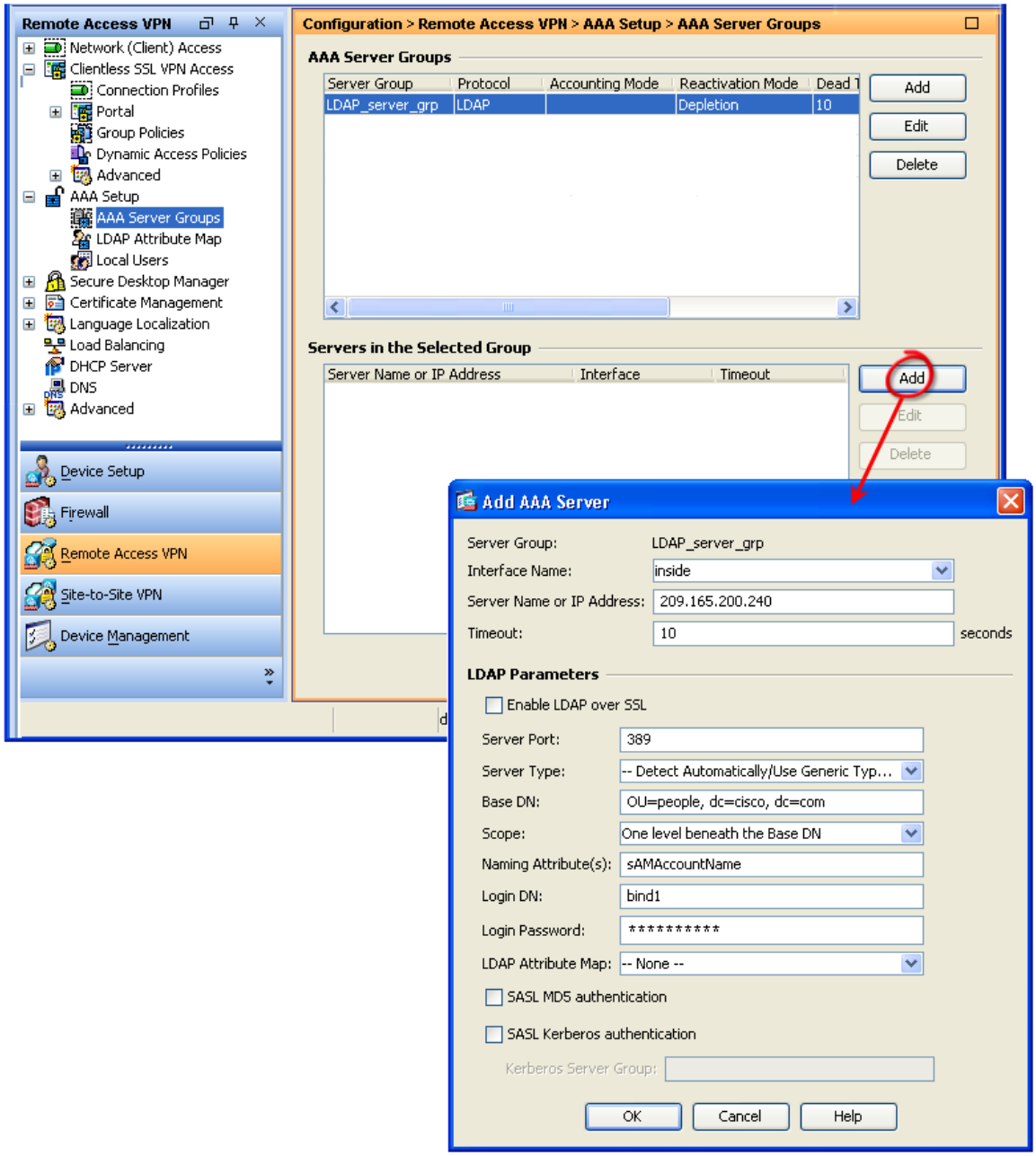
Step 1 Navigate to Configuration > Remote Access VPN > AAA/Local Users > AAA Server Groups.

Step 2 Add a server group and specify the Protocol as LDAP.

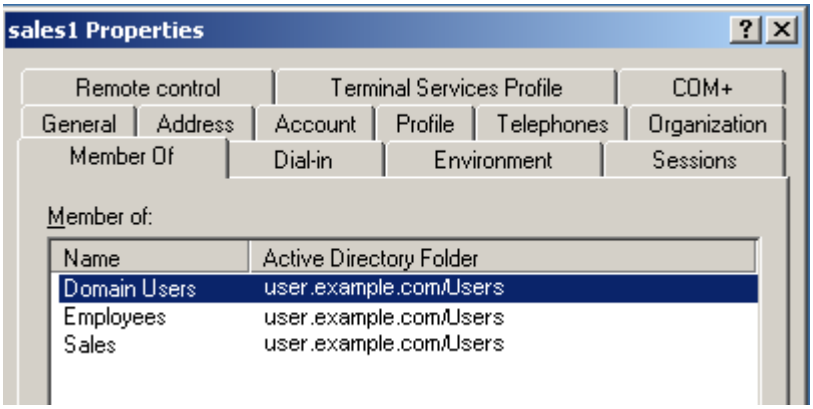


Step 3 Add a server entry with the minimum parameters defined. In the Servers in the Selected Group area, click **Add**. The Add AAA Server window displays:

Note Login DN is the user record used for binding operations. You must have at least read privileges to retrieve LDAP records.

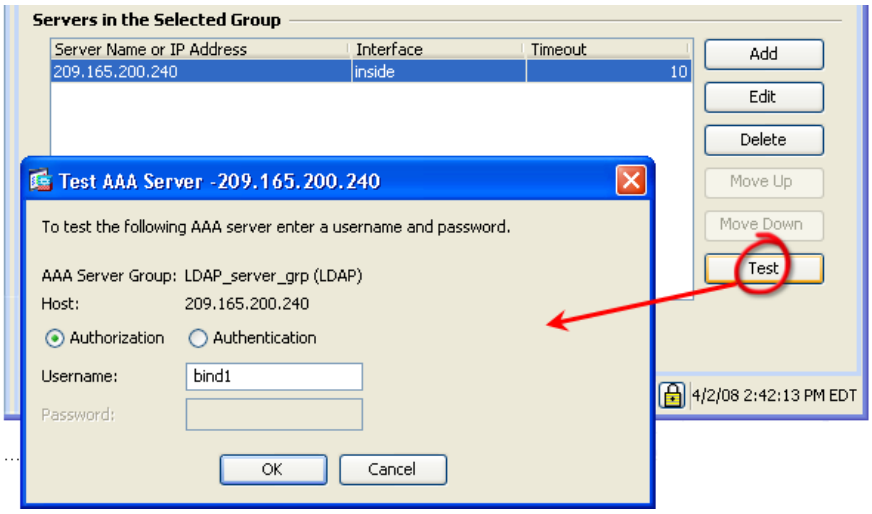


Step 4 Define users on Active Directory by assigning them to their appropriate AD Groups. The following screen is an example Active Directory screen:



Step 5 To test connectivity from the security appliance to the Active Directory authentication server, navigate to Configuration > Remote Access VPN > AAA/Local Users > AAA Server Groups.

Step 6 Select the server entry from the servers in the Selected Group area and click **Test**. Then enter the username and password to test.



When the test is complete, the security appliance displays a window indicating success or failure.

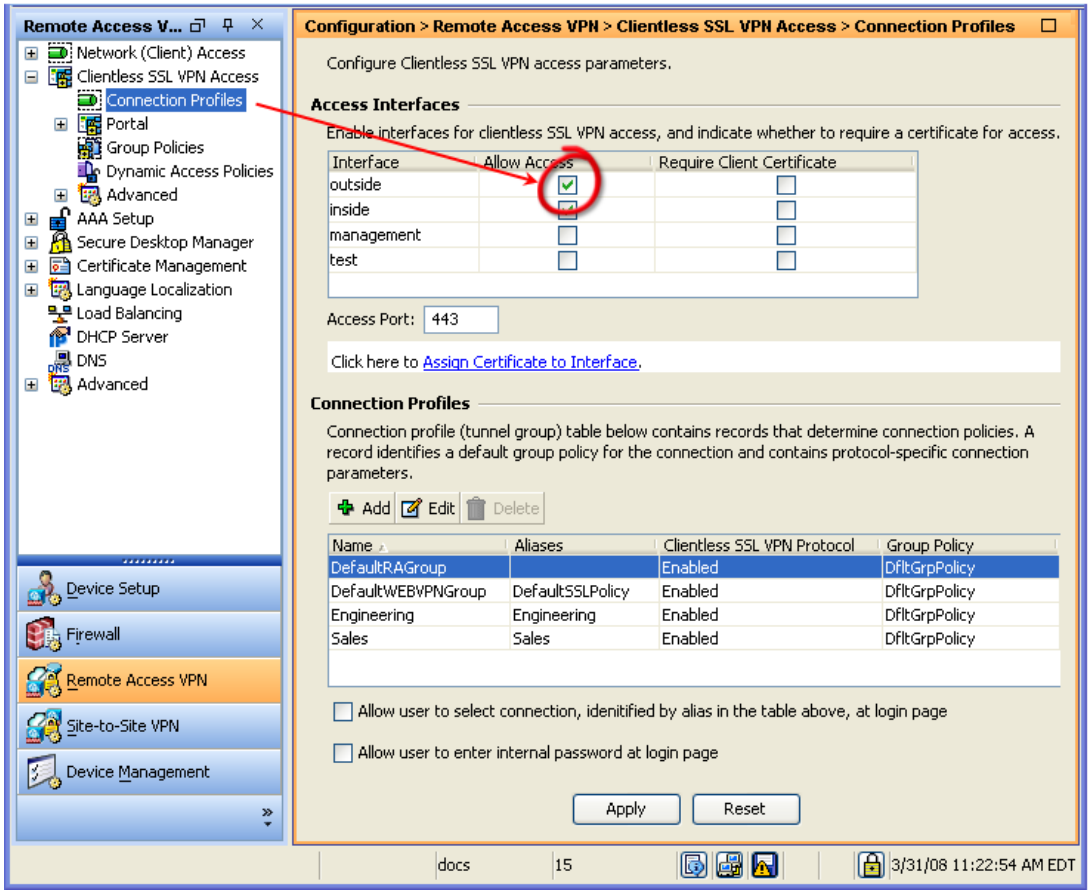
- If the test is successful, you can use the server for authentication/authorization.
- If the test fails, you can debug using the CLI command **debug ldap 255**. This command displays the information exchanged between the LDAP server and the security appliance.

Enabling SSL VPN on Interfaces

You must enable SSL VPN on the interface(s) for remote users to establish connections. This is done in the Connection Profiles pane. Follow these steps to enable SSL VPN:

Step 1 Navigate to Clientless SSL VPN Access > Connection Profiles.

Step 2 In the Access Interfaces section, check the appropriate **Allow Access** boxes.

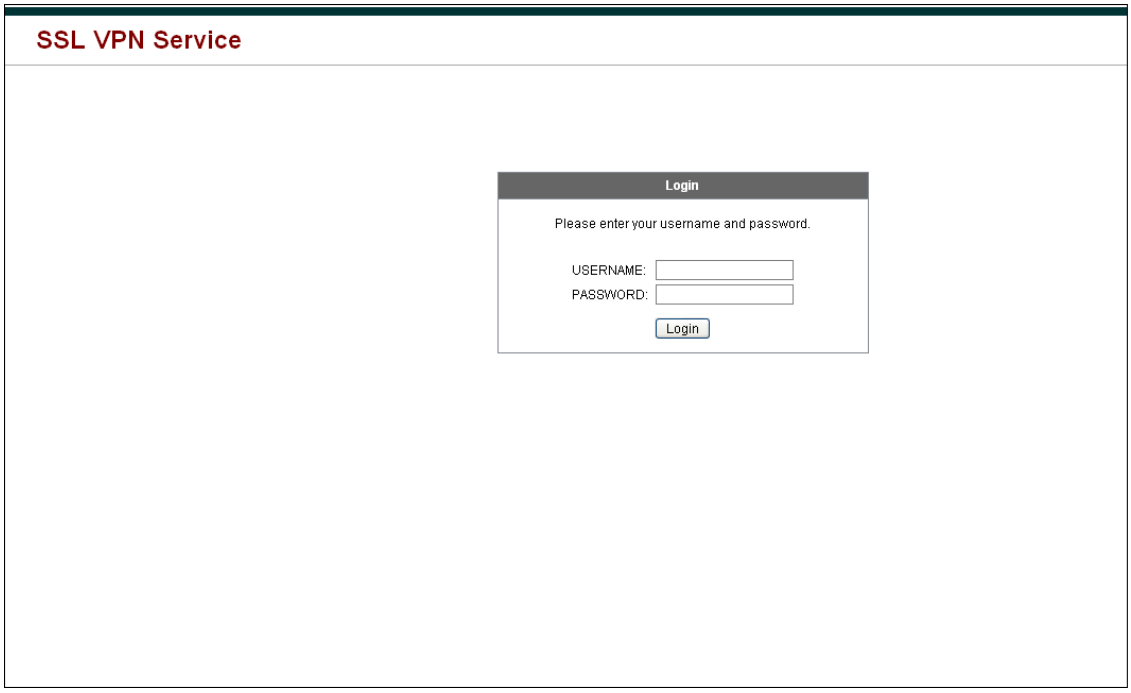


Establishing a Clientless SSL VPN session

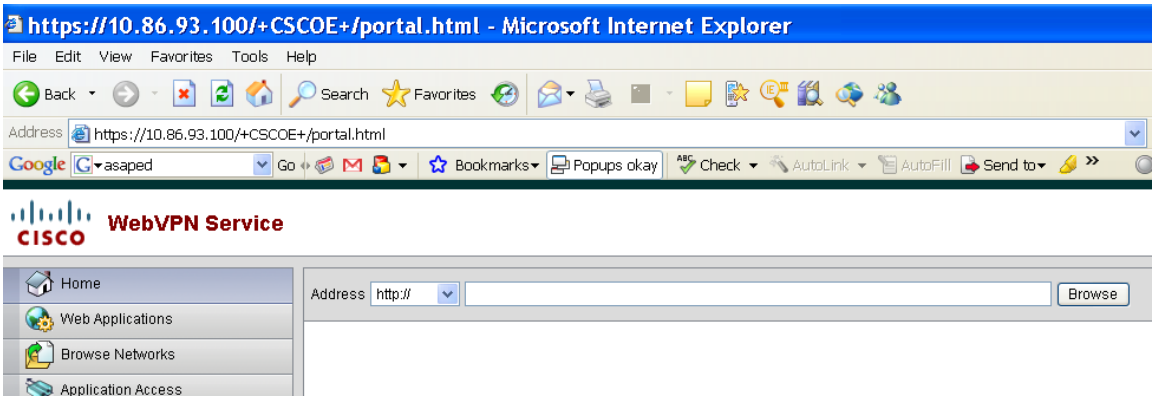
To establish a clientless SSL VPN session, perform the following steps.

Step 1 Clear your browser cache and cookies and also the Java RunTime Environment (JRE) cache.

Step 2 Enter **https://<web-interface-IP>** or **https://<ASA-FQDN>** in the browser address bar to initiate the session. The Login window displays:

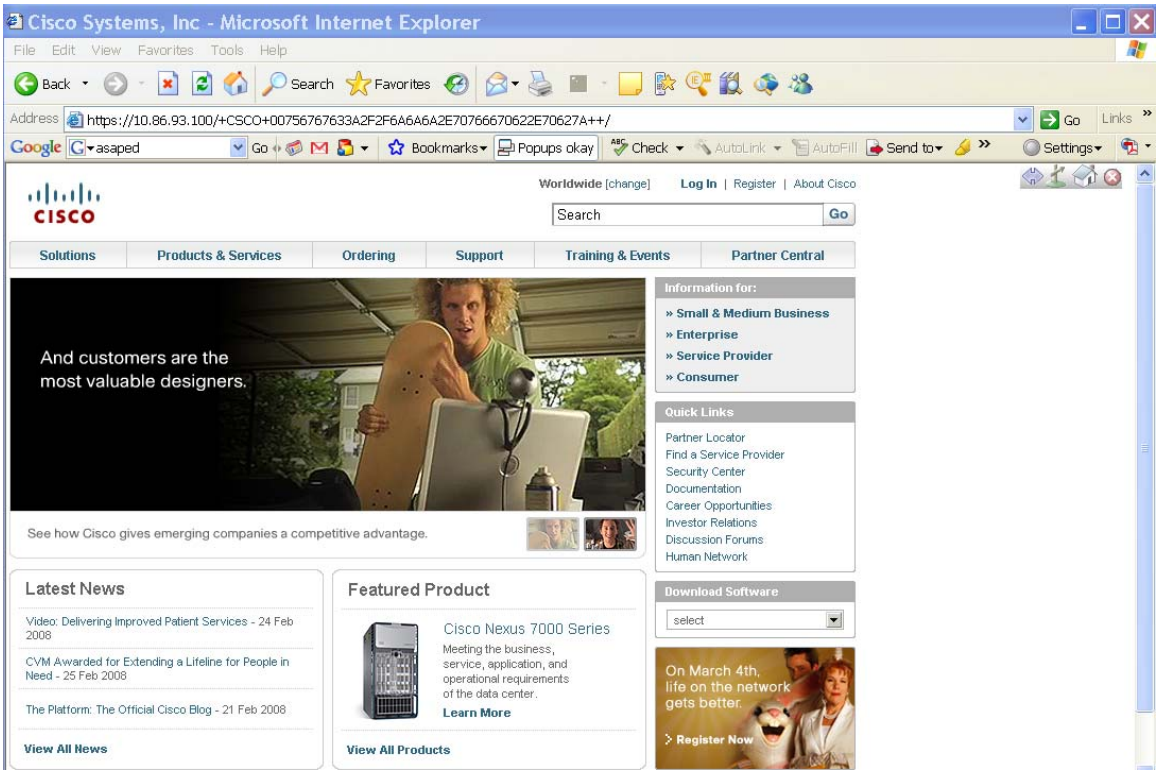


Step 3 Enter the user credentials and verify that the default clientless SSL VPN portal displays:



Step 4 Browse to a website (for example, https://our-internal-portal).

No Bookmark/URL-Lists are defined at this point. Enter the website and verify it is processed by SSL VPN.


Cisco Systems, Inc - Microsoft Internet Explorer
File Edit View Favorites Tools Help
Back Search Favorites
Address https://10.86.93.100/+CSCO+0075676763 3A2F2F6A6A6A2E70766670622E70627A++/
Go Links
Google asaped Go Bookmarks Popups okay Check AutoLink AutoFill Send to Settings
Worldwide [change] Log In | Register | About Cisco
Search Go
Solutions Products & Services Ordering Support Training & Events Partner Central
And customers are the most valuable designers.
See how Cisco gives emerging companies a competitive advantage.
Information for:
» Small & Medium Business
» Enterprise
» Service Provider
» Consumer
Quick Links
Partner Locator
Find a Service Provider
Security Center
Documentation
Career Opportunities
Investor Relations
Discussion Forums
Human Network
Download Software
select
Latest News
Video: Delivering Improved Patient Services - 24 Feb 2008
CVM Awarded for Extending a Lifeline for People in Need - 25 Feb 2008
The Platform: The Official Cisco Blog - 21 Feb 2008
View All News
Featured Product
Cisco Nexus 7000 Series
Meeting the business, service, application, and operational requirements of the data center.
Learn More
View All Products
On March 4th, life on the network gets better.
Register Now

Enforcing VPN Access via Connection Profiles, Group Policies, and Customization Objects

You can configure and enforce VPN access policies by configuring connection profiles and group policies, or by configuring dynamic access policies. The following procedure provides instructions on configuring group policies and connection profiles.

Understanding Policy Enforcement of Permissions and Attributes

You can configure the security appliance to apply user attributes obtained from a RADIUS/LDAP authentication /authorization server, user attributes set in group policies on the security appliance, or both. If the security appliance receives attributes from both sources, the attributes are aggregated and applied to the user policy. If there are conflicts between attributes coming from the server and from a group policy, those attributes obtained from the DAP always take precedence.

To summarize, the VPN permission policy for user authorization is the aggregate of the DAP access attributes and the group-policy inheritance hierarchy.

1. The security appliance applies attributes in the following order:
2. Dynamic Access Policy attributes—Take precedence over all others.
3. User attributes—The AAA server returns these after successful user authentication or authorization.
4. Group policy attributes —These attributes come from the group policy associated with the user. You identify the user group policy name in the local database by the vpn-group-policy attribute or from a RADIUS/LDAP server by the value of the RADIUS CLASS attribute (25) in the OU=GroupName. The group policy provides any attributes that are missing from the DAP or user attributes.
5. Connection profile (tunnel group) default-group-policy attributes —These attributes come from the default group policy associated with the connection profile. This group policy provides any attributes that are missing from the DAP, user or group policy.
6. System default attributes—System default attributes provide any values that are missing from the DAP, user, group policy, or connection profile.

Configuring an Engineering and a Sales Connection Profile

To configure a connection profile, perform the following steps.

Step 1 Navigate to Configuration > Remote Access VPN > Clientless SSL VPN Access > Connection Profiles.

Step 2 In the Connection Profiles section, add the connection profiles *Engineering* and *Sales*.

Step 3 Click **OK** and **Apply** the changes.

Step 4 Select the Engineering connection profile and click **Edit**. The Edit Clientless SSL VPN Connection Profile screen opens.

Step 5 Enter *Engineering* as an alias of in the Aliases field.

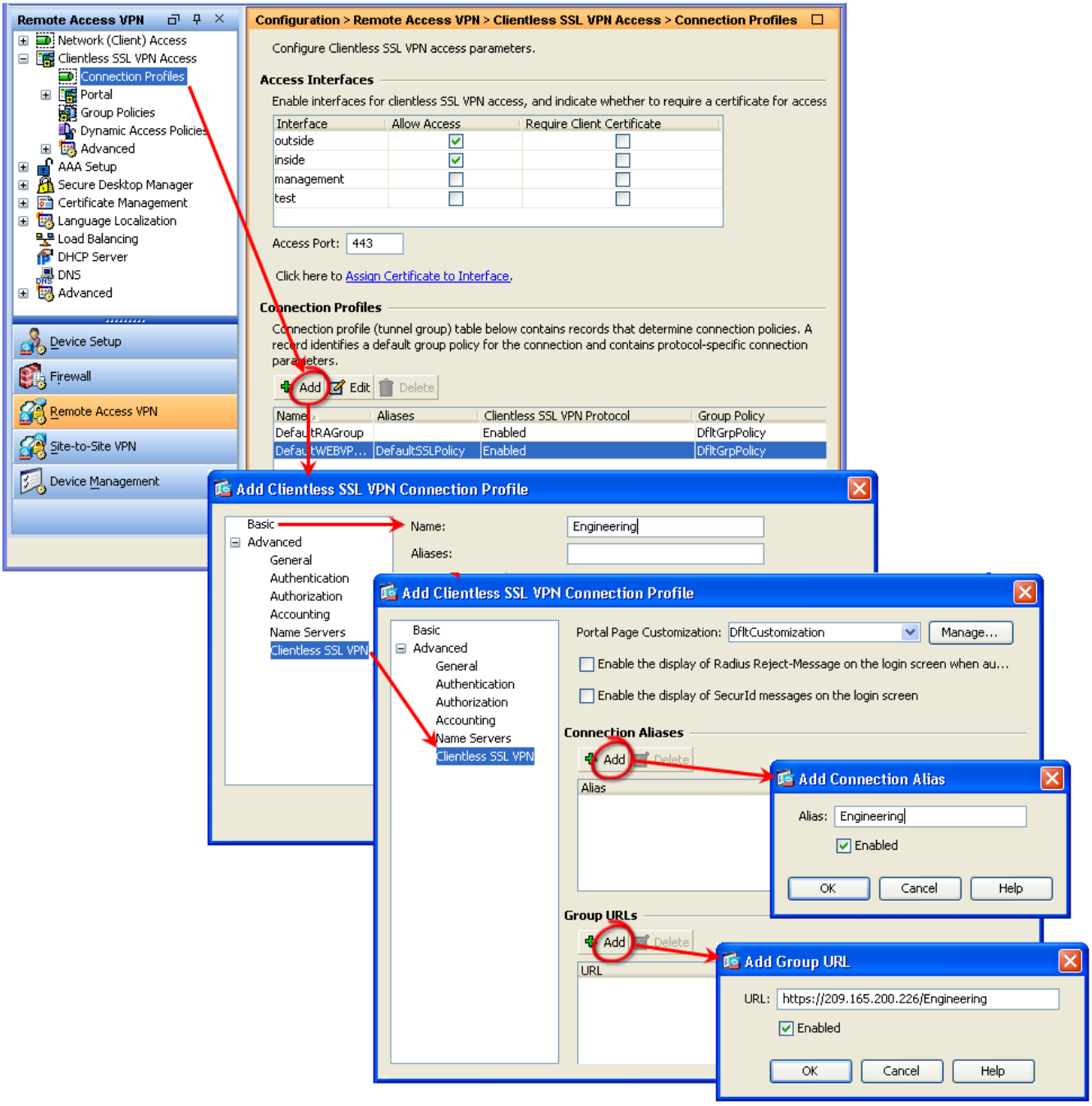
Step 6 On the left side of the screen select **Advanced** and select **Clientless SSL VPN**.

Step 7 In the Group URLs section, click **Add**. The Add Group URL screen opens.

Step 8 Enter the Group URL https://ip_address/Engineering.

Step 9 Click **OK** in the Add Group URL screen and **OK** in the Edit Clientless SSL VPN Connection Profile screen**,** and click **Apply** to apply the changes.

Step 10 Perform the same steps for the Sales connection profile using *Sales* as the alias and Group URL.



Configuring Engineering and Sales Group Policies

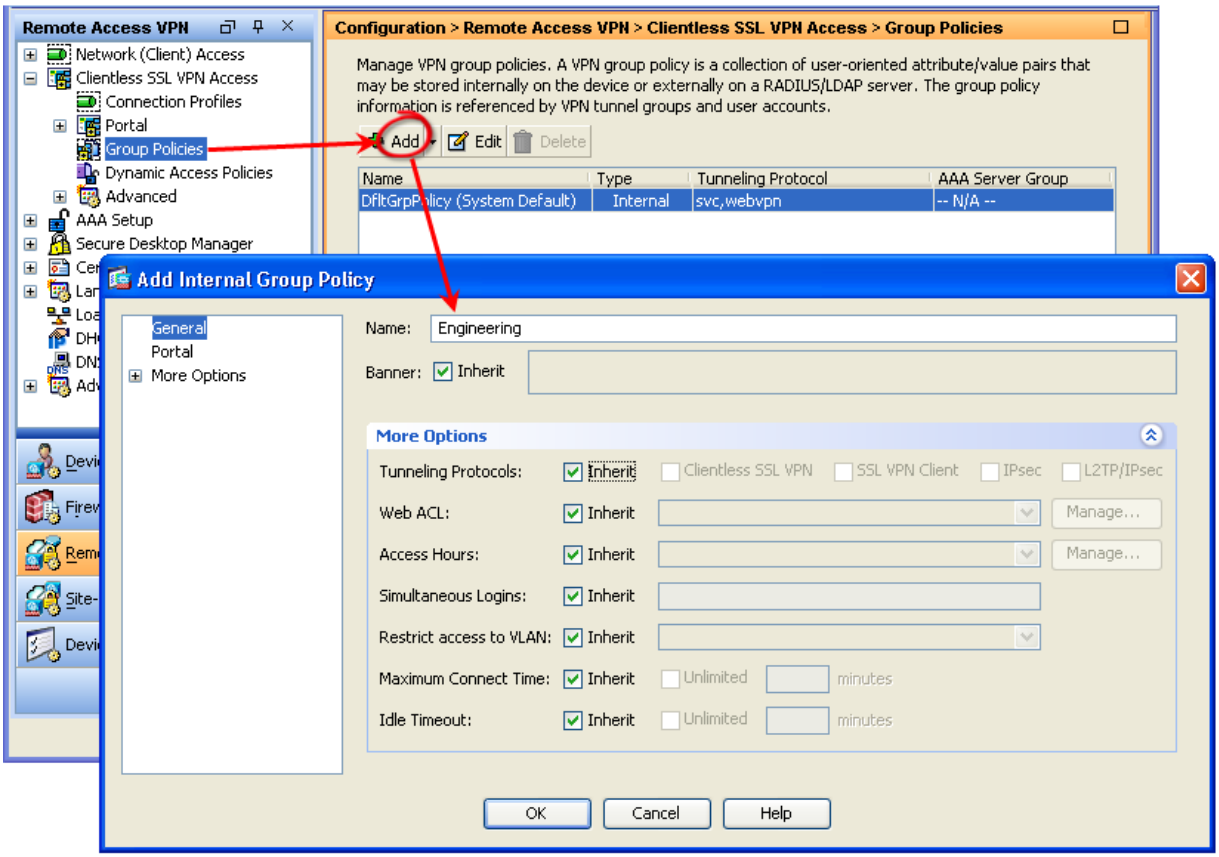
To configure a group policies for Engineering and Sales, perform the following steps.

Step 1 Navigate to Clientless SSL VPN Access > Group Policies. Click **Add**. The Add Internal Group Policy window displays.

Step 2 Enter *Engineering* as the Name.

Step 3 Click **OK** and **Apply** the changes.

Step 4 Repeat the procedure to create the *Sales* group policy.



Associating Group Policies Engineering and Sales to Connection Profiles

To associate the new group-policies Engineering and Sales to the Engineering and Sales Connection Profiles, perform the following steps.

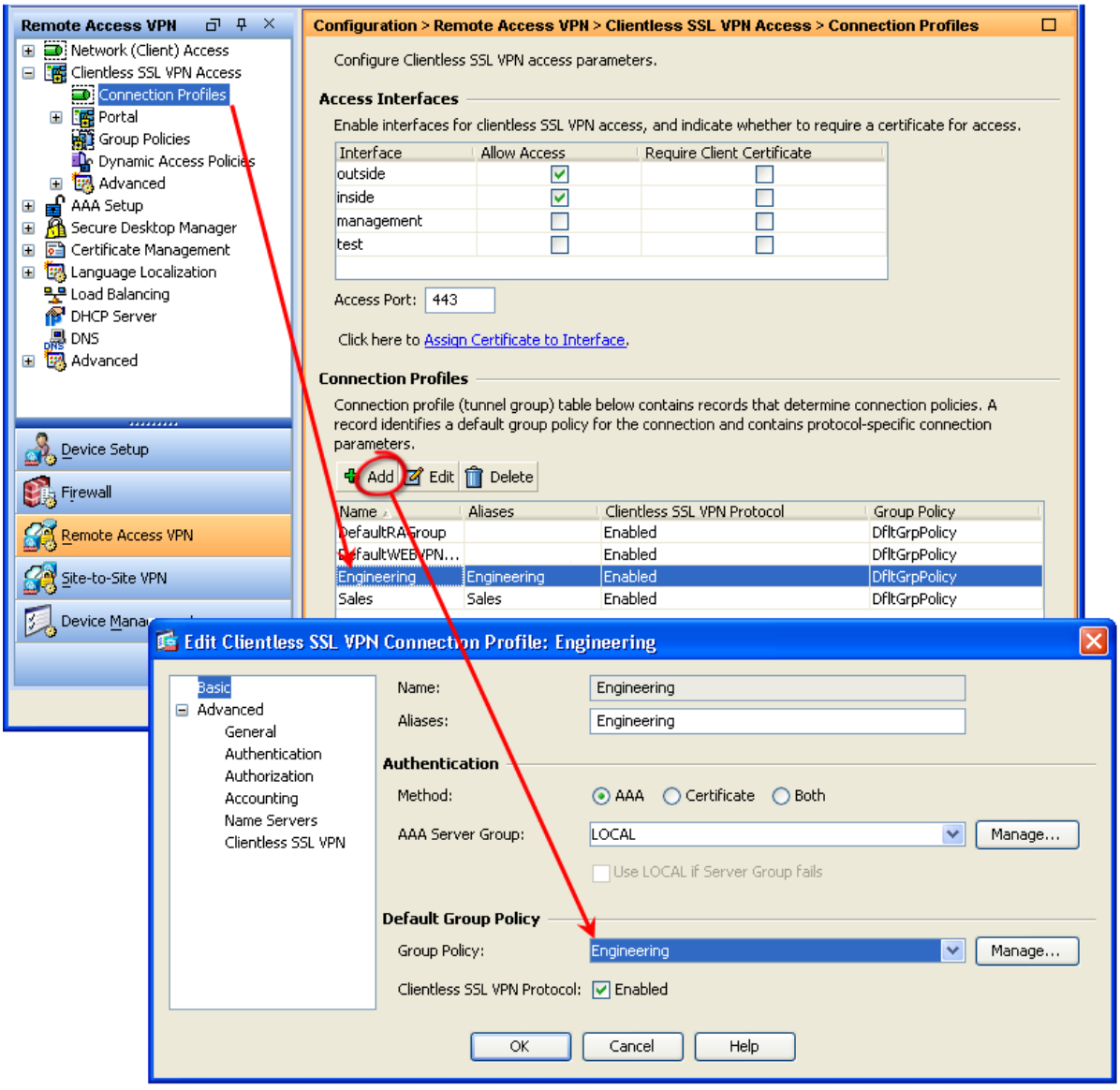
Step 1 Navigate to Clientless SSL VPN Access > Connection Profiles.

Step 2 In the Connection Profiles area, select the **Engineering** connection profile and click **Edit**. The Edit Clientless VPN Connection Profile displays.

Step 3 In the Default Group Policy drop-down menu, select the **Engineering** policy.

Step 4 Click **OK** and **Apply** the changes.

Step 5 Perform the same steps for the Sales Connection Profile using Sales as the default group policy.



Creating Bookmark Lists for the Engineering and Sales Group Policies

To create a bookmark list, and apply it to a group policy, perform the following steps. You can specify access through the SSL portal to your corporate resources such as OWA, Sharepoint, and Citrix with these bookmarks.

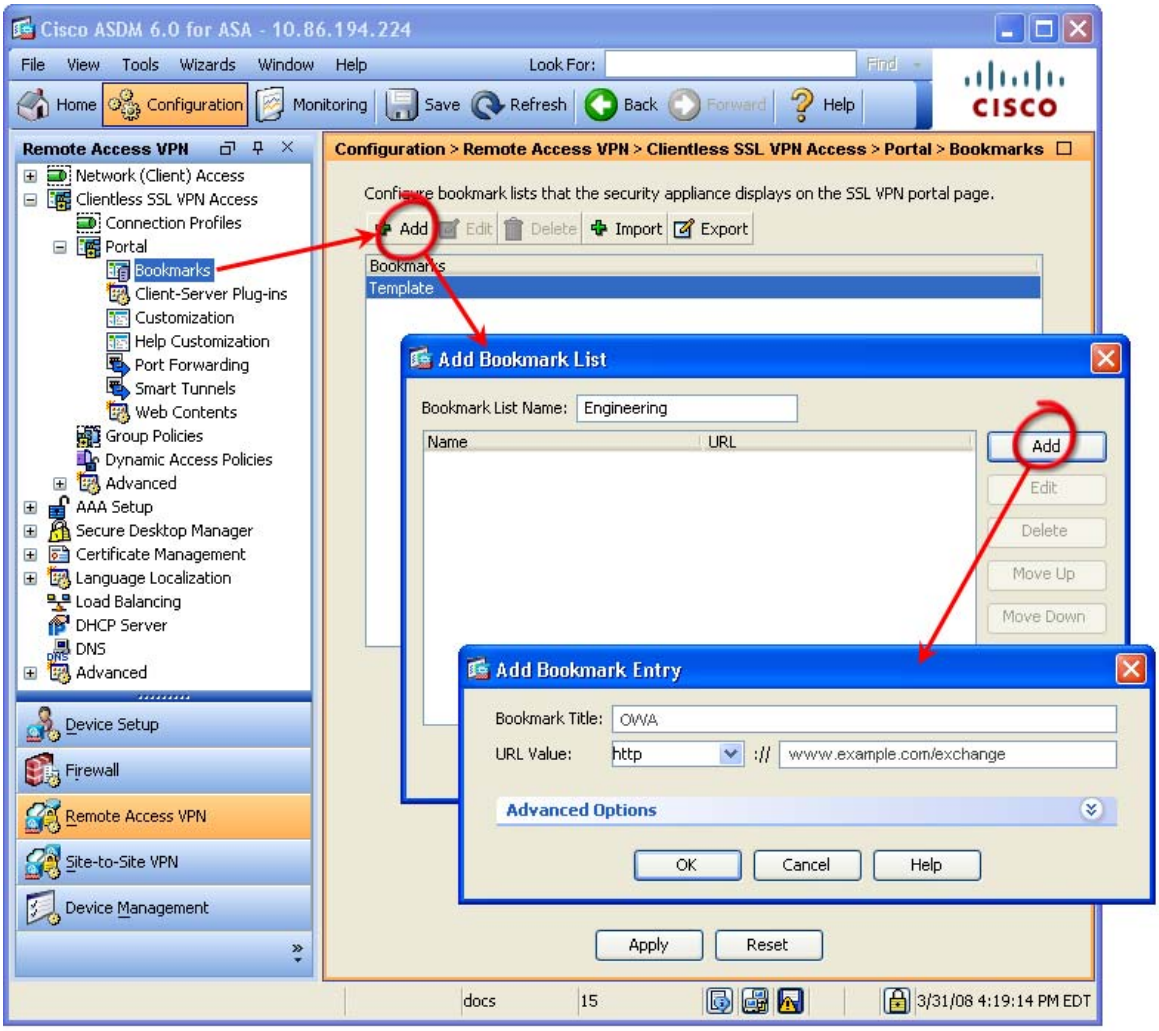
Step 1 Navigate to Clientless SSL VPN Access > Portal > Bookmarks. Click **Add**.

Step 2 Enter *Engineering* as the bookmark list name.

Step 3 Click **Add** and specify several URL entries.

Step 4 Perform the same steps for Sales, creating a *Sales* bookmark list with a different subset of URL entries and/or applications.

Step 5 Click **OK** and click **Apply** to apply the bookmark lists.



Applying the Bookmark Lists to Group Policies

Now you need to associate the bookmark lists to a specific group policy. Perform the following steps:

Step 1 Navigate to Clientless SSL VPN Access > Group Policies.

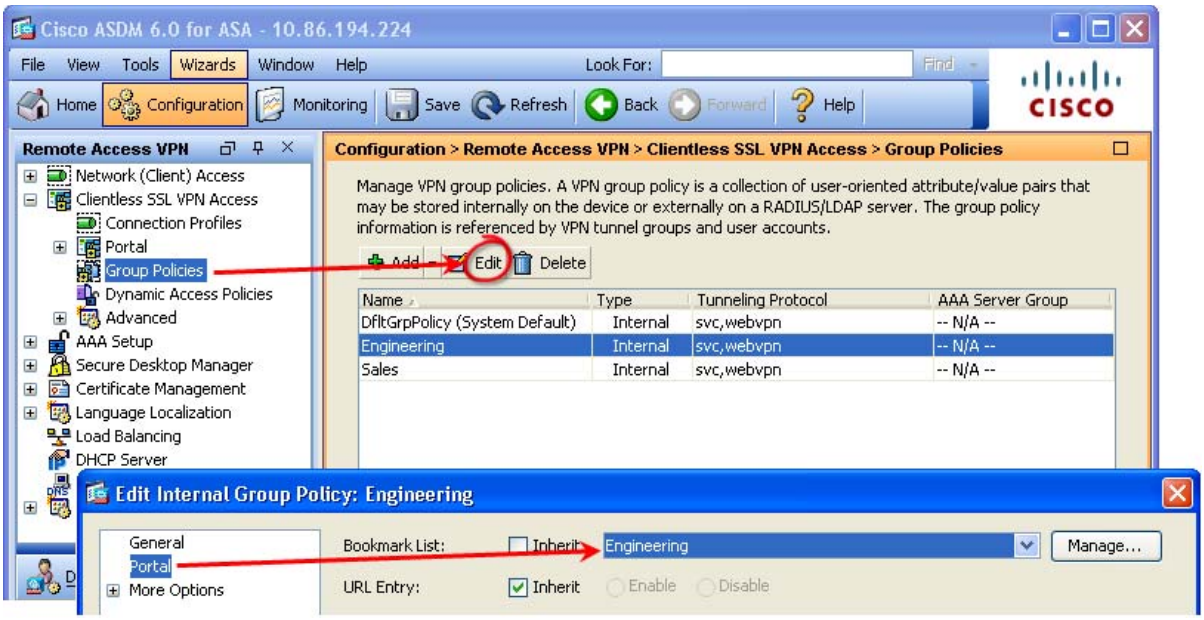
Step 2 Select the **Engineering** policy and click **Edit**. The Edit Internal Group Policy window displays.

Step 3 Select **Portal** in the left navigation pane.

Step 4 In the Bookmark list section, select **Engineering**.

Step 5 Select **Ok** and click **Apply** to apply the changes.

Step 6 Perform the same steps to apply the Sales URL list to the Sales group policy.

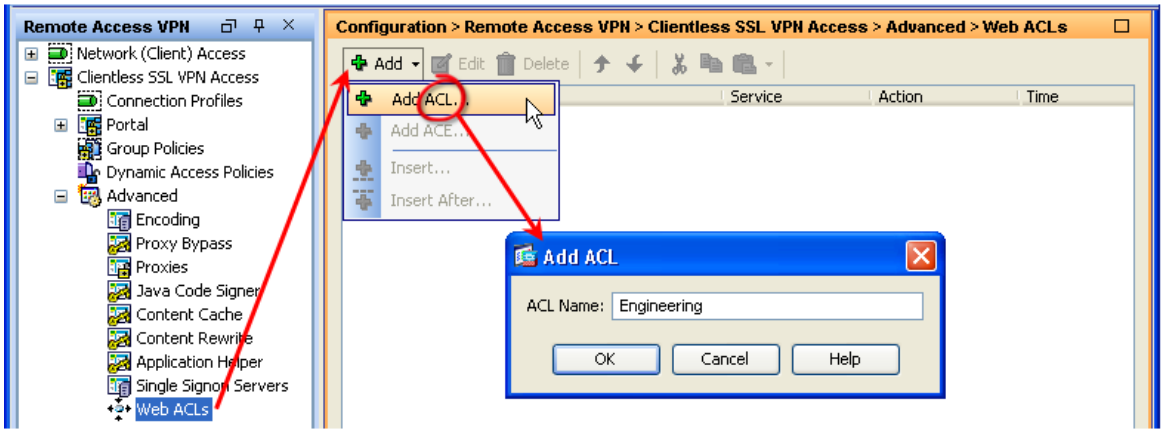


Creating WebType ACLs

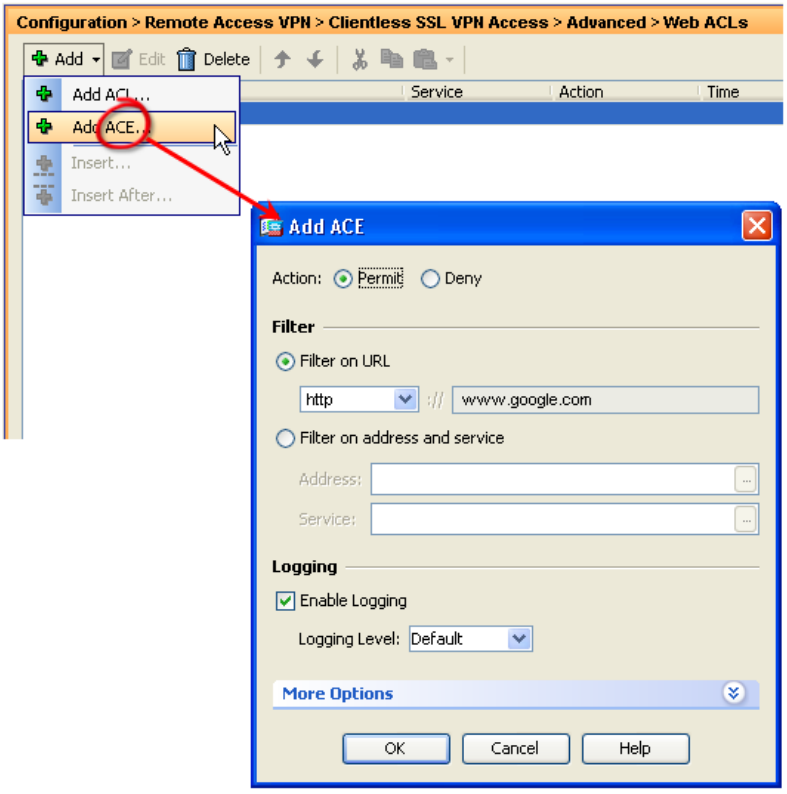
Web Access control lists (ACLs) filter internet traffic for clientless users. The ACLs table displays the filters configured on the security appliance and the access control entries (ACEs) for each ACL. Each ACL permits or denies access to specific networks, subnets, hosts, and web servers; the ACE specifies one rule for the ACL. To create an ACL, follow these steps:

Step 1 Navigate to Clientless SSL VPN Access > Advanced > Web ACLs**.**

Step 2 Click **Add** and enter *Engineering* as the ACL name.



Step 3 Click **Add** and select **Add ACE** .

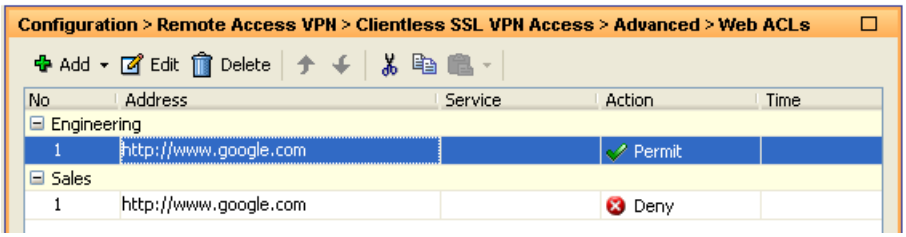


Step 4 For Action, select **Permit**.

Step 5 To demonstrate filtering, enter a URL such as http://www.google.com.

Step 6 Click **OK** to apply the changes

Step 7 Perform the same steps to create an ACL for Sales. Set the Sales ACL action to **Deny** to create an example whose actions are opposite the Engineering ACL.



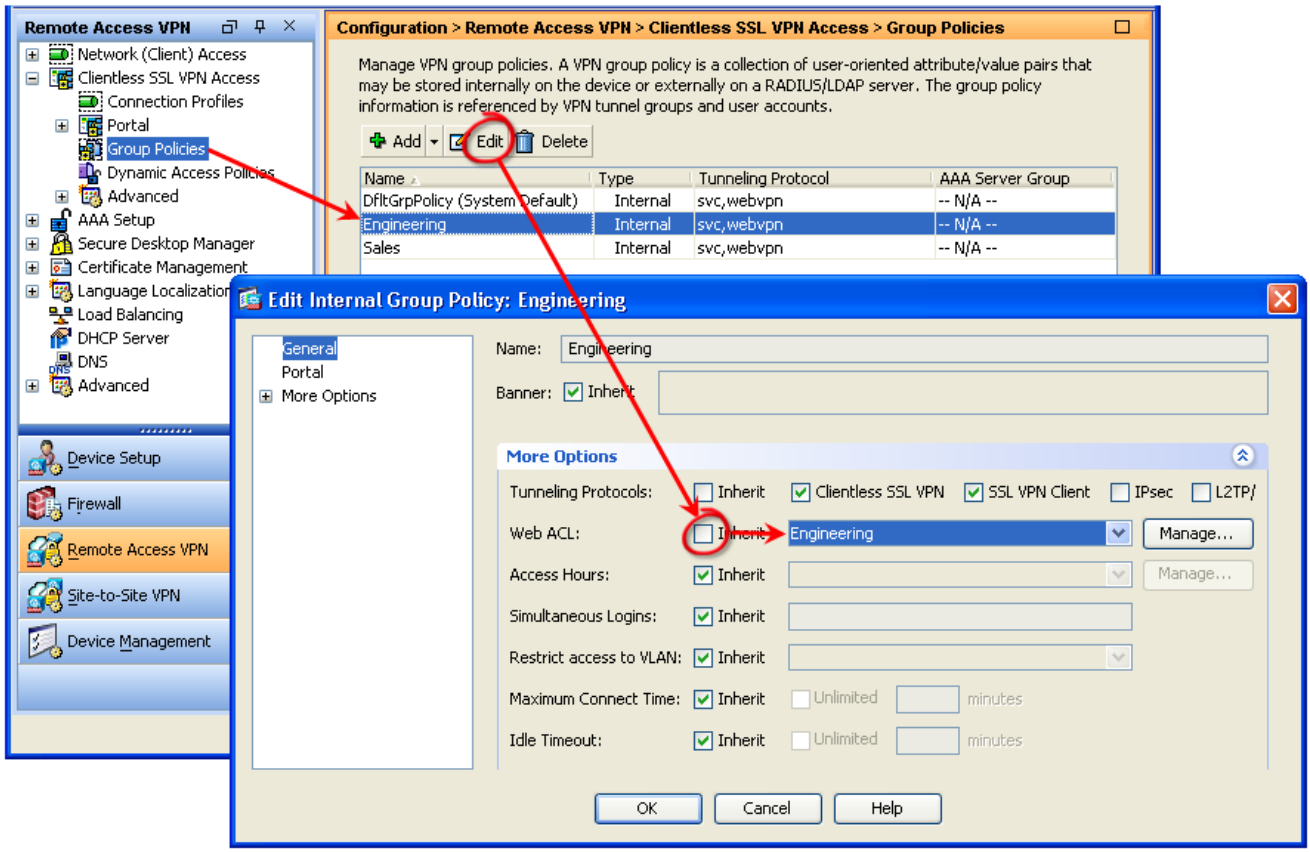
Step 8 In the main screen, click **Apply**.

Applying the ACLs to Group Policies

You must associate the ACLs created in the previous section, with group policies. To associate an ACL to a specific group policy, perform the following steps:

Step 1 Navigate to Configuration > Remote Access VPN > Clientless SSL VPN Access > Group Policies.

Step 2 Select the Engineering policy and click **Edit**. The Edit Group Policy Engineering pane displays:



Step 3 Select **General** in the left pane.

Step 4 Select the **More Options** drop down.

Step 5 Uncheck the Inherit checkbox and select *Engineering* in the drop down list.

Step 6 Select **Ok** and **Apply** the changes

Step 7 Perform the same steps for the Sales WebType ACL.

Creating Customization Objects for Engineering and Sales

The security appliance uses customization objects to customize the screens displayed during a clientless SSL VPN connection and to customize the AnyConnect client user interface.

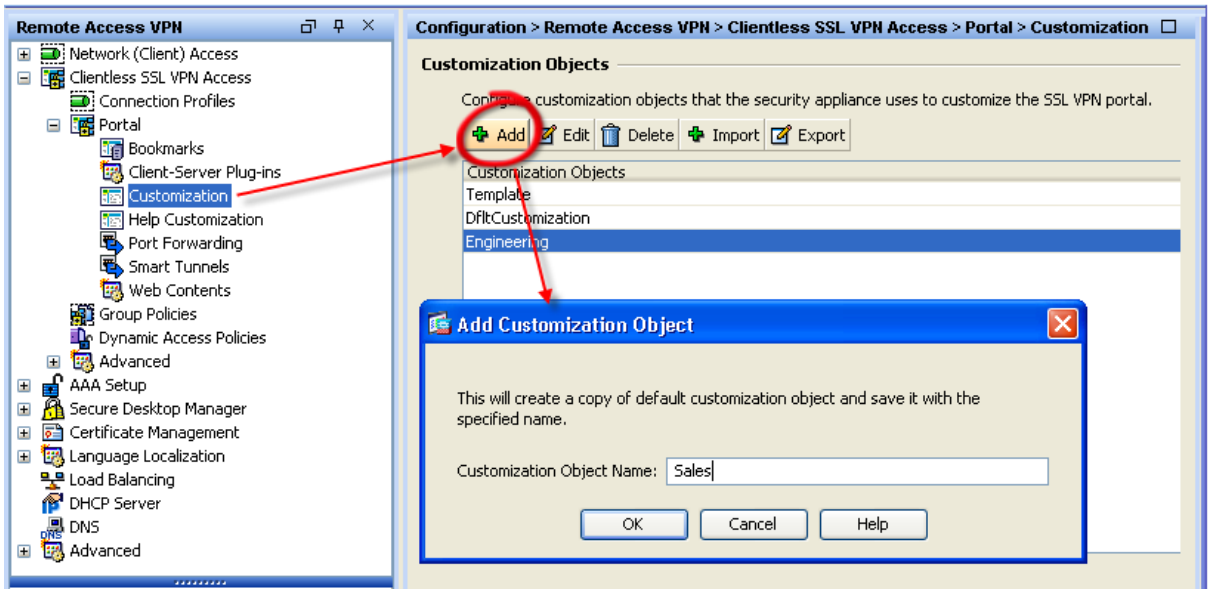
To create a customization object, perform the following steps:

Step 1 Create the new customization objects. Navigate to Clientless SSL VPN Access > Portal > Customization.

Step 2 Click **Add** and enter *Engineering* as the Customization Object Name. Click **OK**.

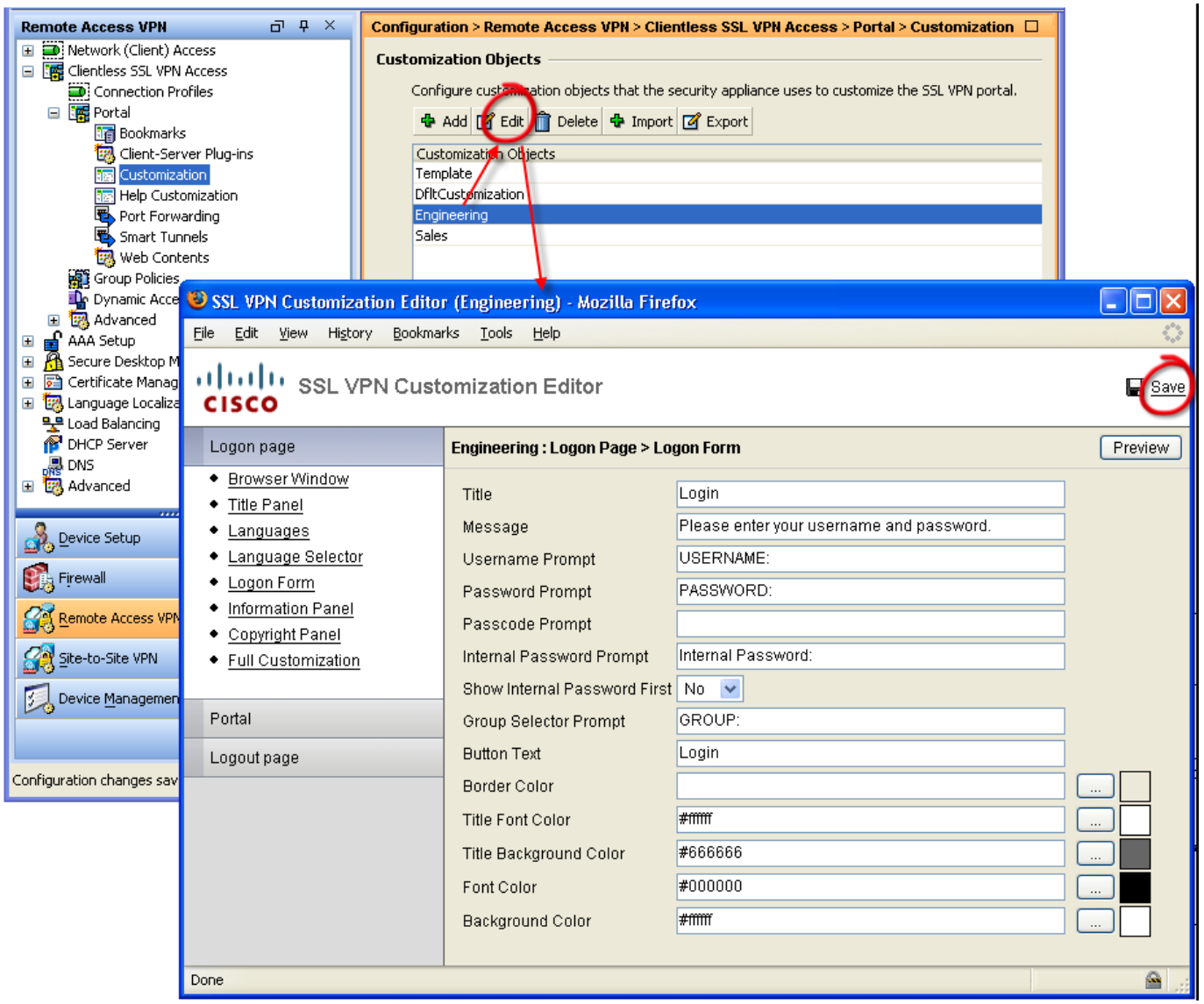
Step 3 Click **Add** again and enter *Sales* to create the Sales customization object. Click **OK**.

Step 4 Click **Apply** to add the new objects to the security appliance configuration:



Step 5 Edit the customization objects. Select each of the new customization objects in the table and click **Edit**. The Customization Editor launches in a browser window.

Step 6 Select the items to customize and make your changes. When you are done, click **Save**:



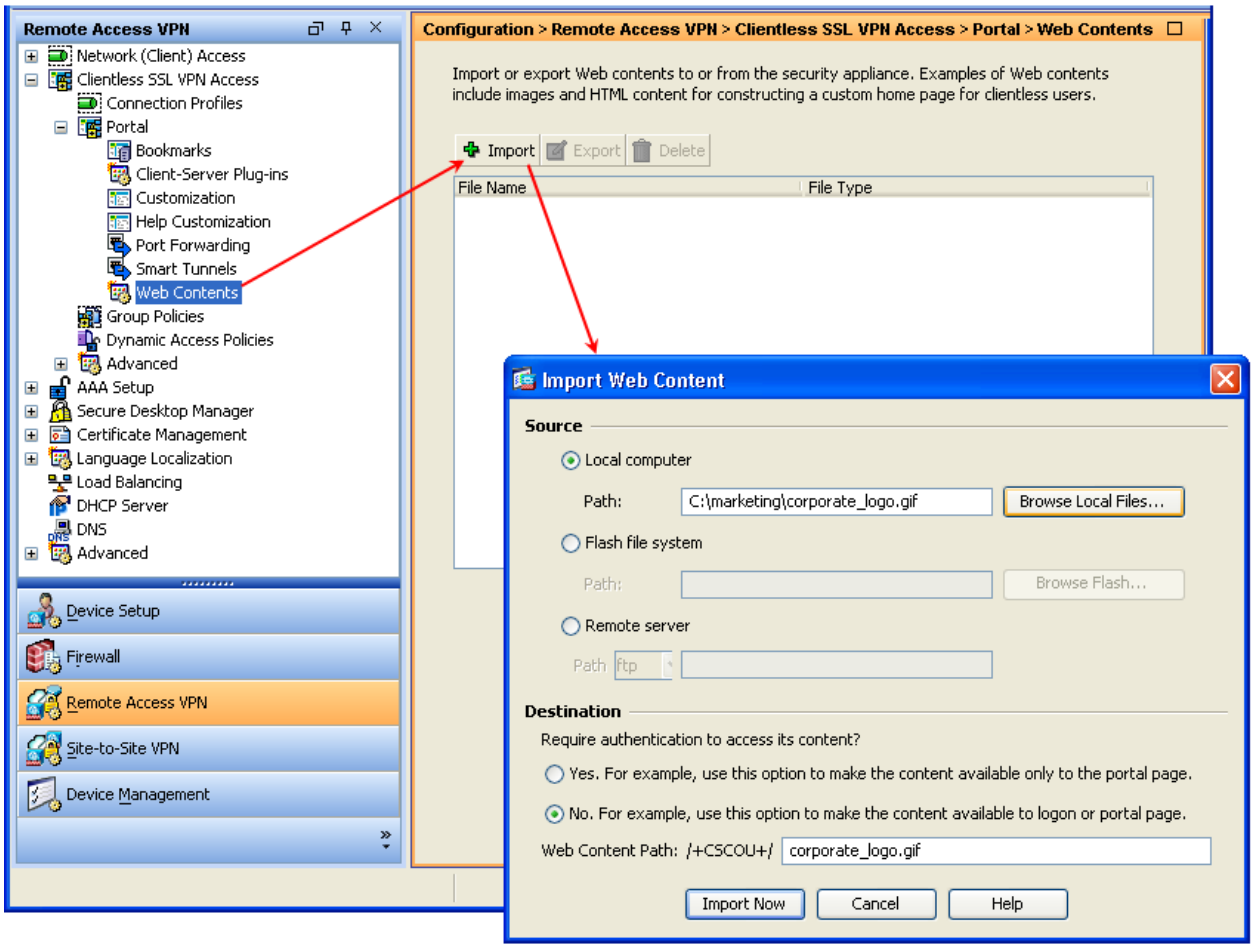
Importing Web Content for use with Logos

You can change the logo that appears on the portal screen with your own custom logo. Follow these steps to import your own logo and enable the security appliance to display it:

Step 1 Import your logo as web content. Navigate to Clientless SSL VPN Access > Portal > Web Contents.

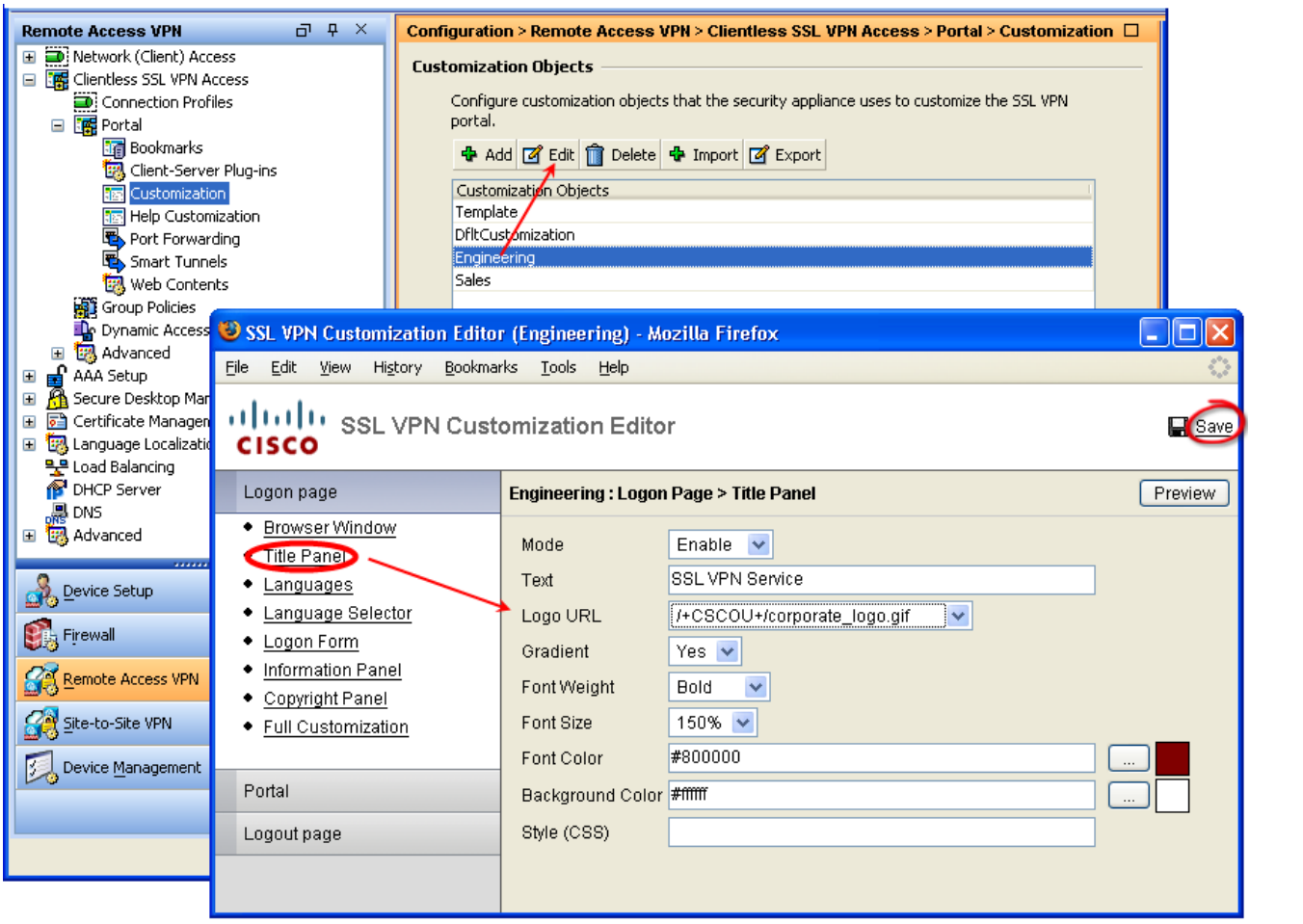
Step 2 Click **Import**. Specify a source file. *Destination* determines whether the logo appears to remote users before authentication or after.

Step 3 Click **Import Now**. Click **Apply** on the Web Contents pane.



Step 4 Specify the logo in a customization object. Navigate to Clientless SSL VPN Access > Portal > Customization.

Step 5 Edit the customization objects and specify the logo. Click **Save**.



Setting the Customization in the Connection Profile

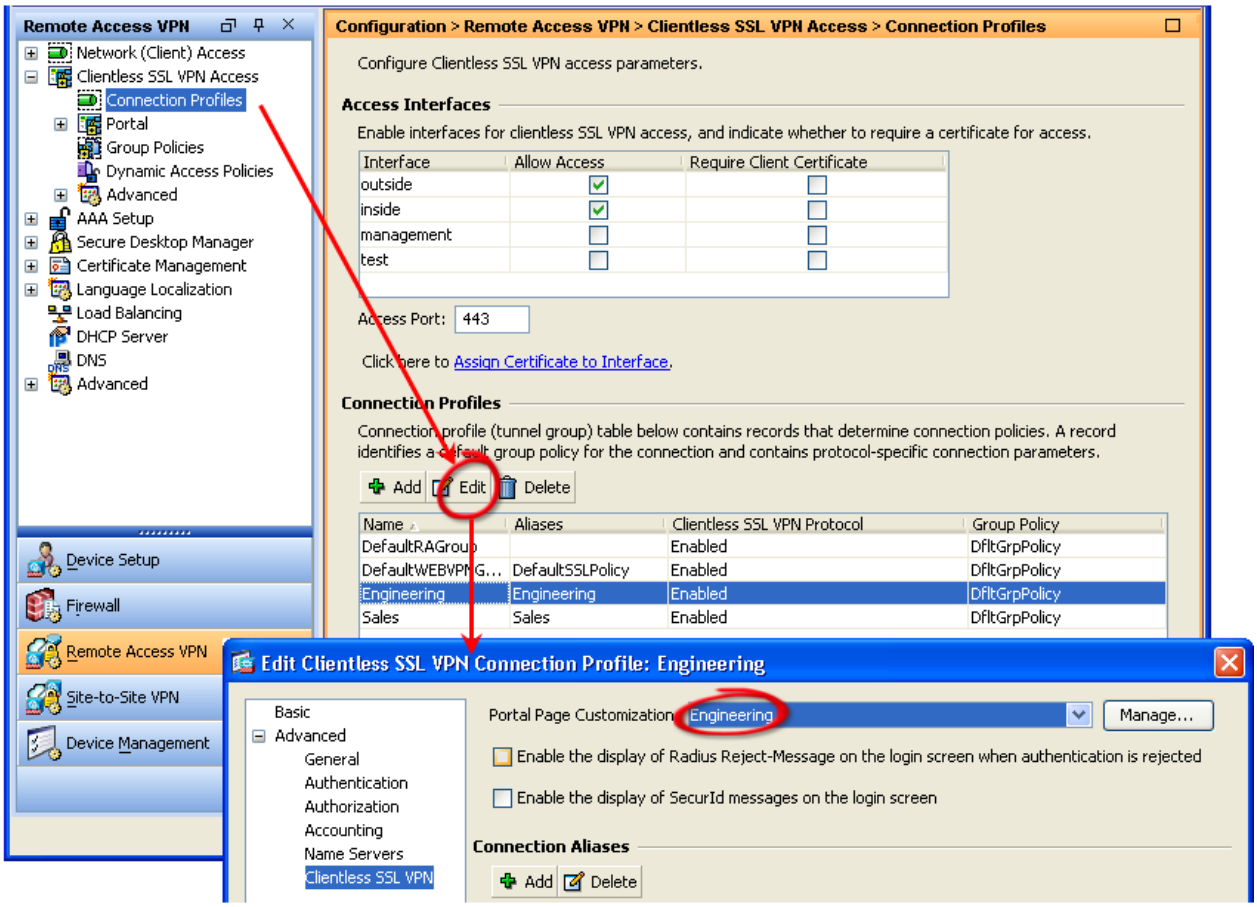
You must specify the customization objects for the connection profiles for Engineering and Sales. This ensures the portal is customized for different users connecting over different connection profiles. Follow these steps:

Step 1 Navigate to Configuration > Remote Access VPN > Clientless SSL VPN Access > Connection Profiles.

Step 2 Select **Engineering** connection profile and click **Edit**.

Step 3 In the left pane, select **Advanced > Clientless SSL VPN**.

Step 4 Verify that your customization is selected in the Portal Page Customization drop-down.



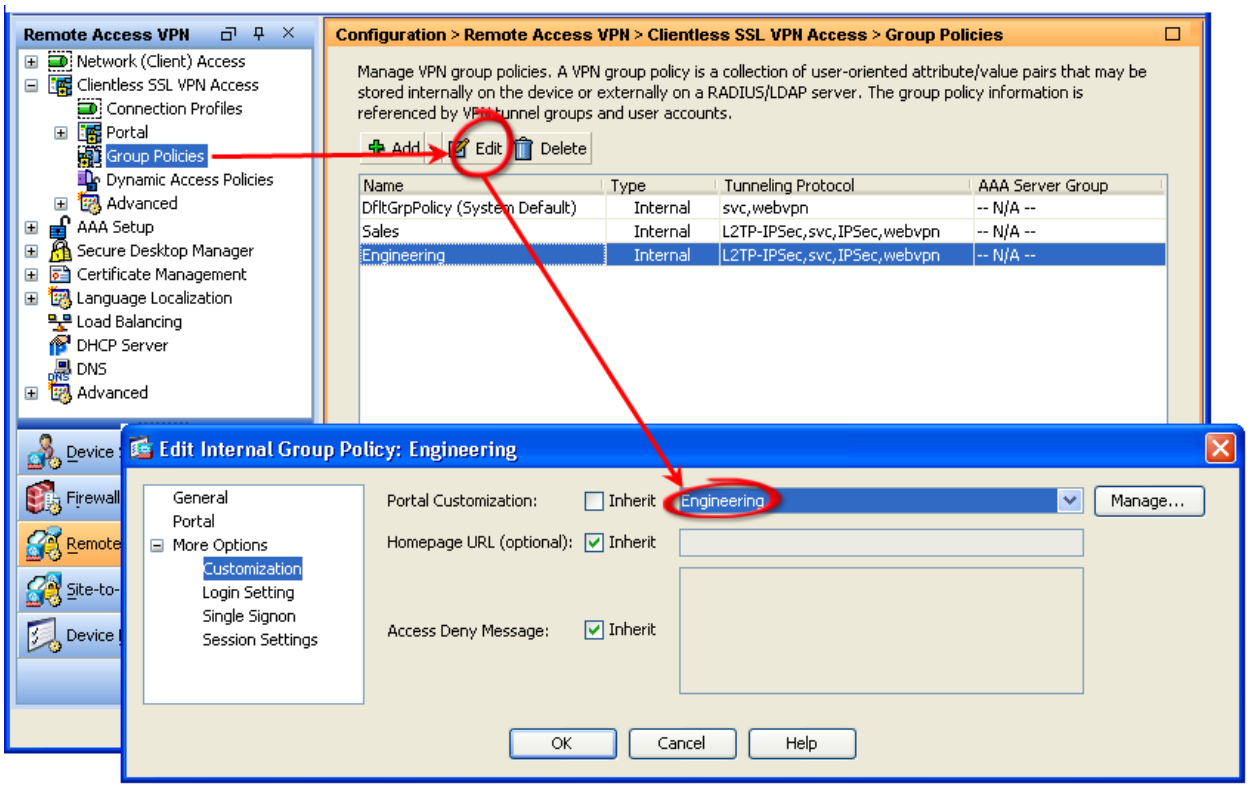
Setting the Customization in the Group Policy

Step 1 Navigate to Configuration > Remote Access VPN > Clientless SSL VPN Access > Group Policies.

Step 2 Select the **Engineering** group policy and click **Edit**.

Step 3 Select **More Options> Customization** in the left pane.

Step 4 Select the **Engineering** Customization object you created previously.



Step 5 Click **OK** and **Apply** the changes

Step 6 Perform the same steps for the Sales group policy**.**

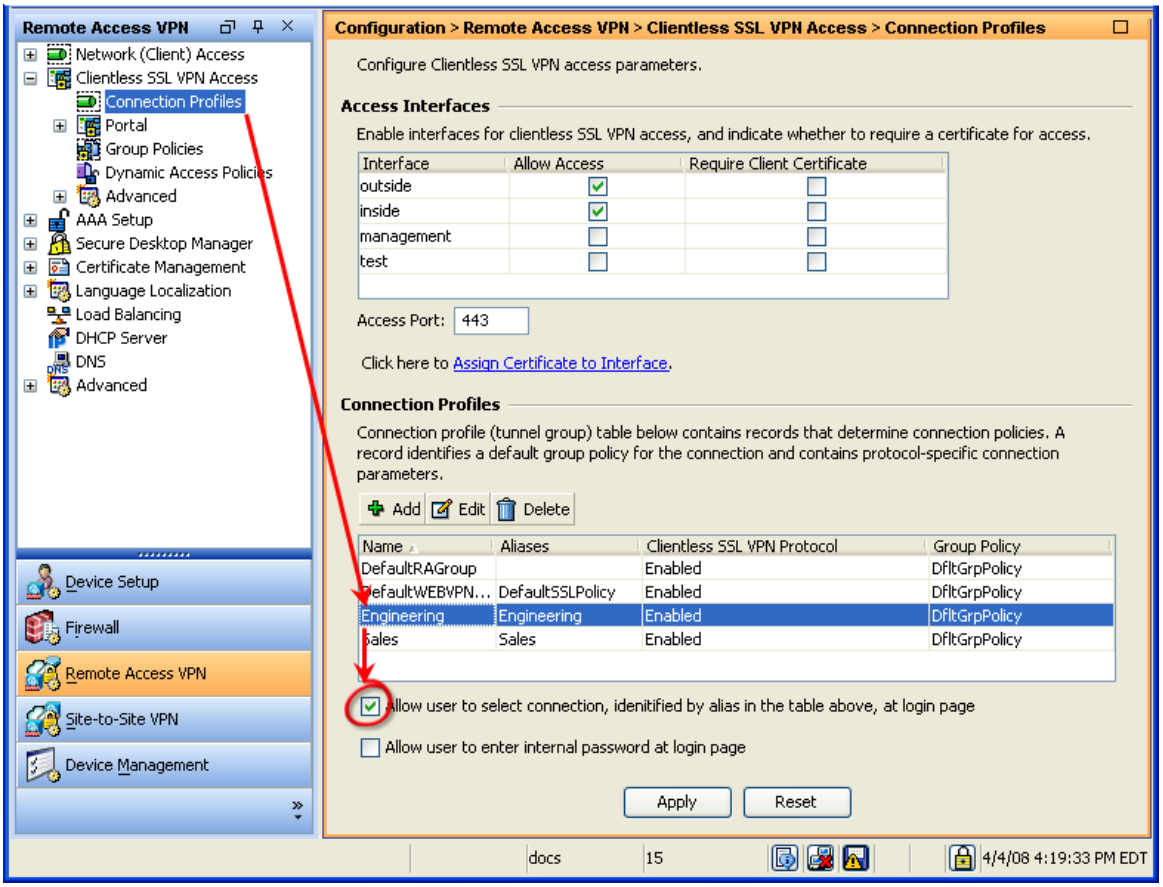
Establishing a Clientless Session Using the Drop-Down Menu

This section shows how to use the previously defined Engineering and Sales group-aliases to present aa drop-down menu to users that lets them select the appropriate connection profile.

Step 1 Navigate to Configuration > Remote Access VPN > Clientless SSL VPN Access > Connection Profiles > Edit Clientless SSL VPN Connection Profile.

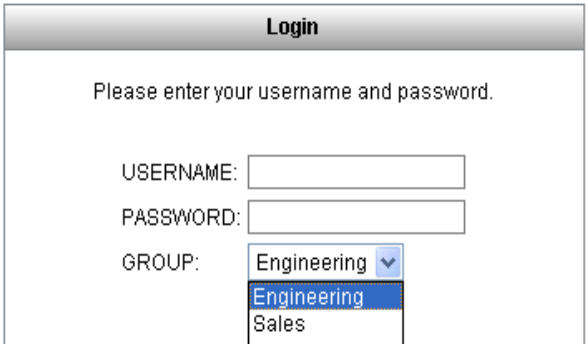
Step 2 Check **Allow user to select connection, identified by alias in the table above, at login page.**

Step 3 Click **Apply**.



Step 4 Establish a VPN session i.e. https://ip_address

The login page now displays a drop down menu that includes the Engineering group and the Sales group.



Step 5 Select the Engineering group and examine the portal. As a result of the configuration you have created, you should see:

- Customization for the Engineering group.
- A list of specific URLs.
- Access to www.google.com only, a result of creating your ACL.

Step 6 Establish a new connection and select the group Sales, and observe its portal.

Establishing an SSL VPN Session Using a Group URL

In *Configuring an Engineering and a Sales Connection Profile*, you configured a group URL for the Engineering and Sales connection profiles. Group URLs have the following advantages:

- The path part of the URL can be any text that is logical.
- You can configure multiple, unique group URL strings in a single connection profile.
- Group URLs do not expose group names, as group aliases do.
- If you not using a Group URL, using https://<IP | FWDN.com> [path] causes the security appliance to use the system default settings in the DefaultWEBVPNGroup connection profile and its associated group-policy, DfltGrpPolicy.

To demonstrate group URLs, follow these steps:

Step 1 Establish a VPN session to https://<*ip_address*>/Engineering

Step 2 As a result of the configuration you have created, you should see:

- Customization for the Engineering group.
- A list of specific URLs.
- Access to www.google.com only, a result of creating your Webtype ACL.

Step 3 Connect into the Sales Group and observe its portal and attributes: https://ip_address/Sales

Single Sign-on & Macros

This section explains how to configure Single Sign-on (SSO) with Macros.

Introduction into the Macros:

Your configuration will most likely require personalized resources that contain the username and password, for example, in URL lists or in group URLs. Macro substitutions let you enter a username and password just once per session to access all configured features. SSL VPN supports the following macro substitutions:

CSCO_WEBVPN_USERNAME – User login name

CSCO_WEBVPN_PASSWORD – User login password

CSCO_WEBVPN_INTERNAL_PASSWORD – User internal password that provides another field to specify a value along with the username and password.

CSCO_WEBVPN_CONNECTION_PROFILE –User login group drop-down (tunnel group alias)

CSCO_WEBVPN_MACRO1– Set via Radius or LDAP vendor specific attribute

CSCO_WEBVPN_MACRO2– Set via Radius or LDAP vendor specific attribute

Each time the security appliance recognizes one of these strings in an end-user request, it replaces the string with the user-specific value before passing the request to a remote server.

For example, a URL list that contains the link:
http://someserver/homepage/CSCO_WEBVPN_USERNAME.html

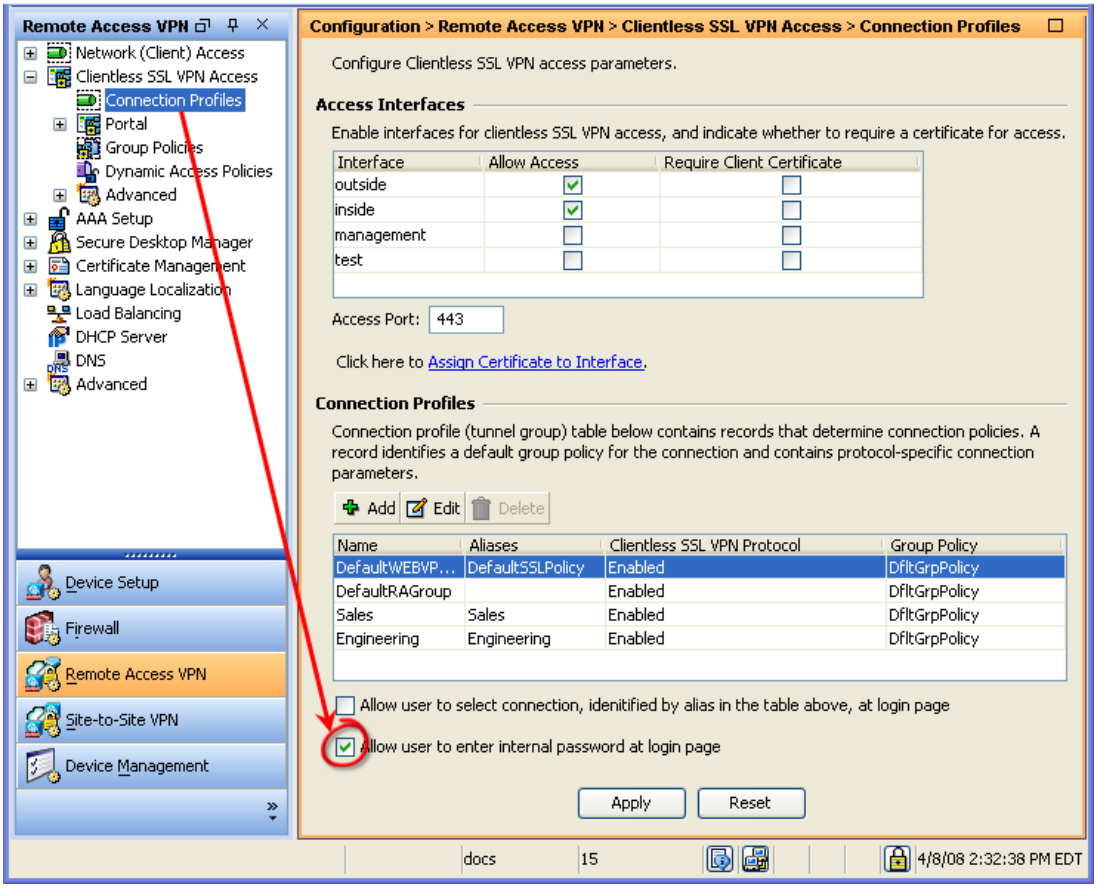
is translated by the security appliance to the following links for SSL VPN USER1 and USER2:

http://someserver/homepage/USER1.html

http://someserver/homepage/USER2.html

Note You can obtain the http-post parameters for any application by performing an HTTP Sniffer trace in the clear (without the security appliance involved). Here is a link to a free browser capture tool, also called an HTTP Analyzer: http://www.ieinspector.com/httpanalyzer/downloadV2/IEHttpAnalyzerV2.exe.

To enable the internal password feature, navigate to Clientless SSL VPN Access > Connection Profiles, then check **Allow user to enter internal password at login page**:



Configuring Post Parameters for SSO with Outlook Web Access

If the Exchange server uses forms-based authentication, the procedure for configuring SSO depends on the specifics of the Outlook Web Access (OWA) implementation. You can obtain the necessary information by analyzing a direct browser capture.

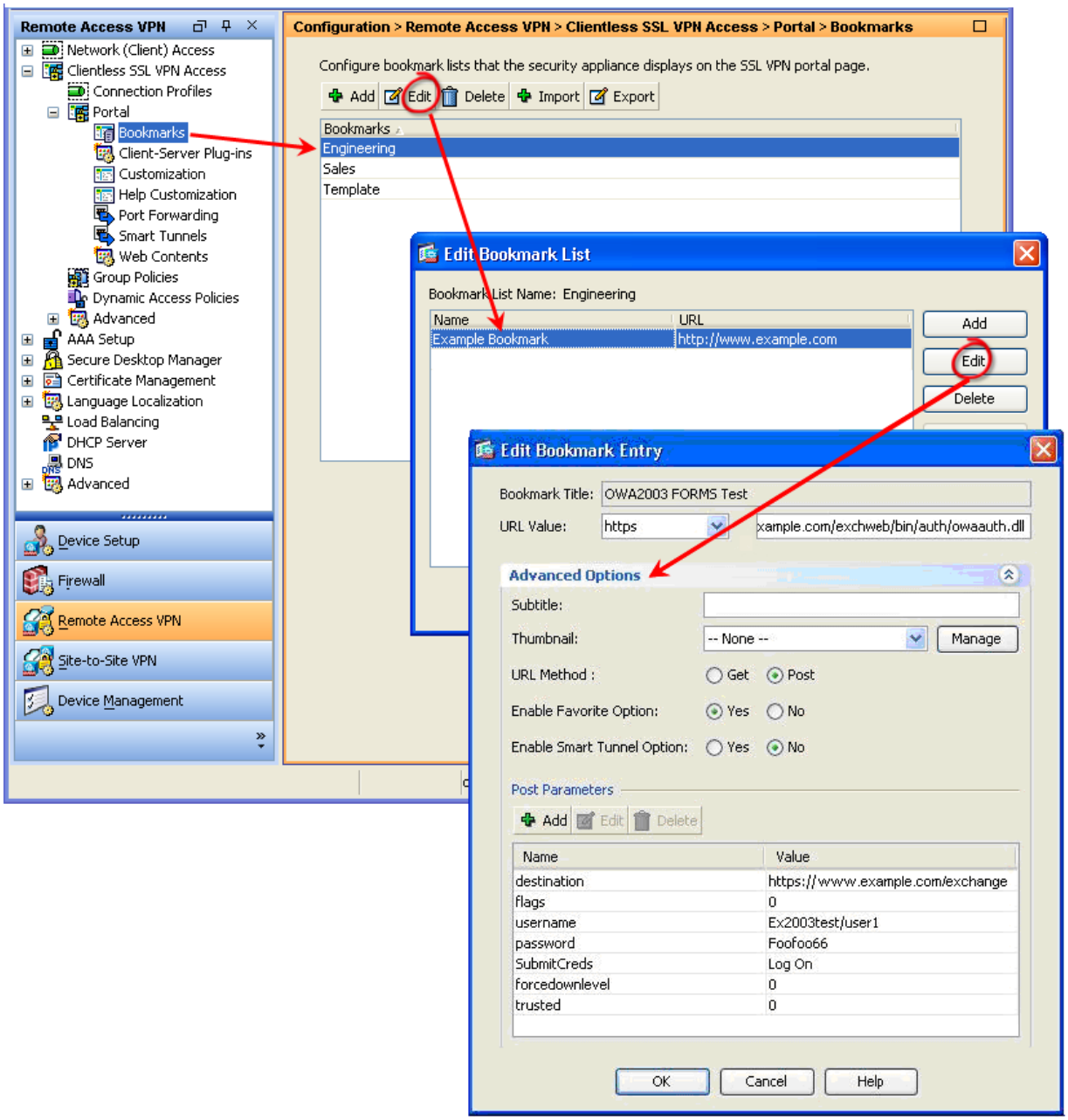
Exchange 2003 and later versions support forms-based authentication, but Exchange 2000 does not. Example configurations of the SSL VPN OWA bookmark follow:

Step 1 Navigate to Configuration-> Remote Access VPN-> Clientless-> Portal-> Bookmarks.

Step 2 Select and edit the bookmark list that contains a corporate OWA Server. You configured such lists for Engineering and for Sales in a previous exercise.

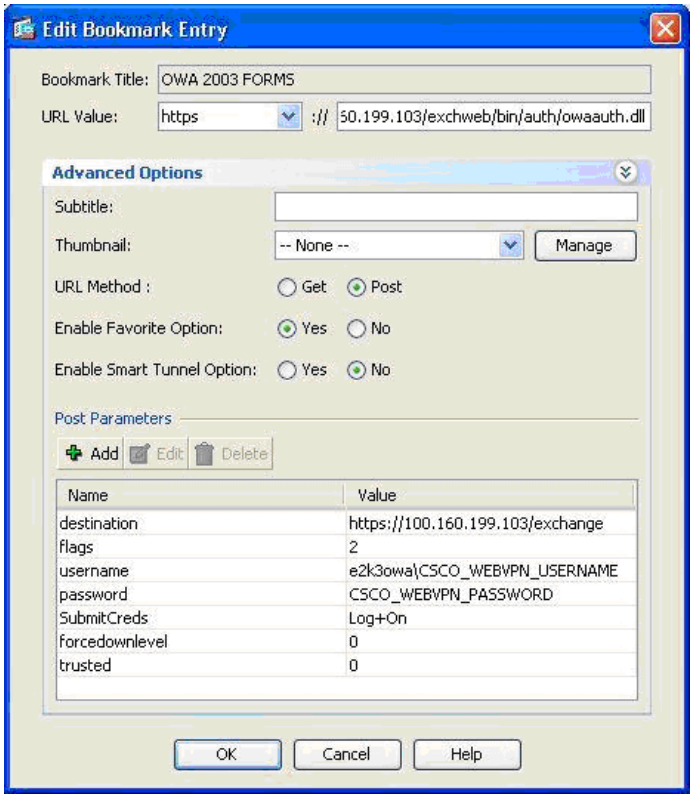
Step 3 Select **Advanced Options** and then select **Add** in the Post Parameters section.

Step 4 Review direct browser captures to be able to define the following post parameters as well as the username & password.



The next example includes the use of Macros to automatically enter the username & password. The security appliance substitutes login credentials supplied at initial SSL VPN login as seen below.

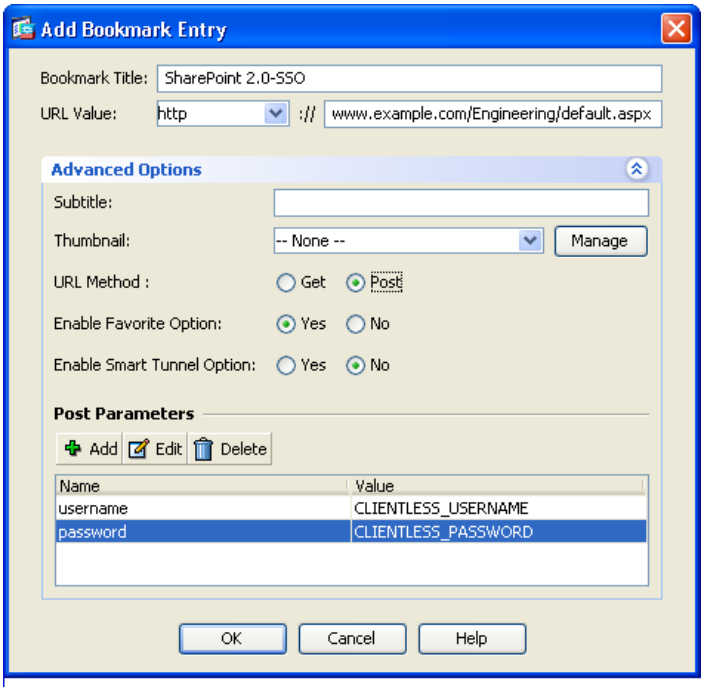
Note The Macro in the username works with or without defining the domain.



Step 5 Verify that you can connect to the portal page and launch the bookmark without OWA prompting for credentials.

Using Macros to Access SharePoint

This example shows how to use Macros to access SharePoint:



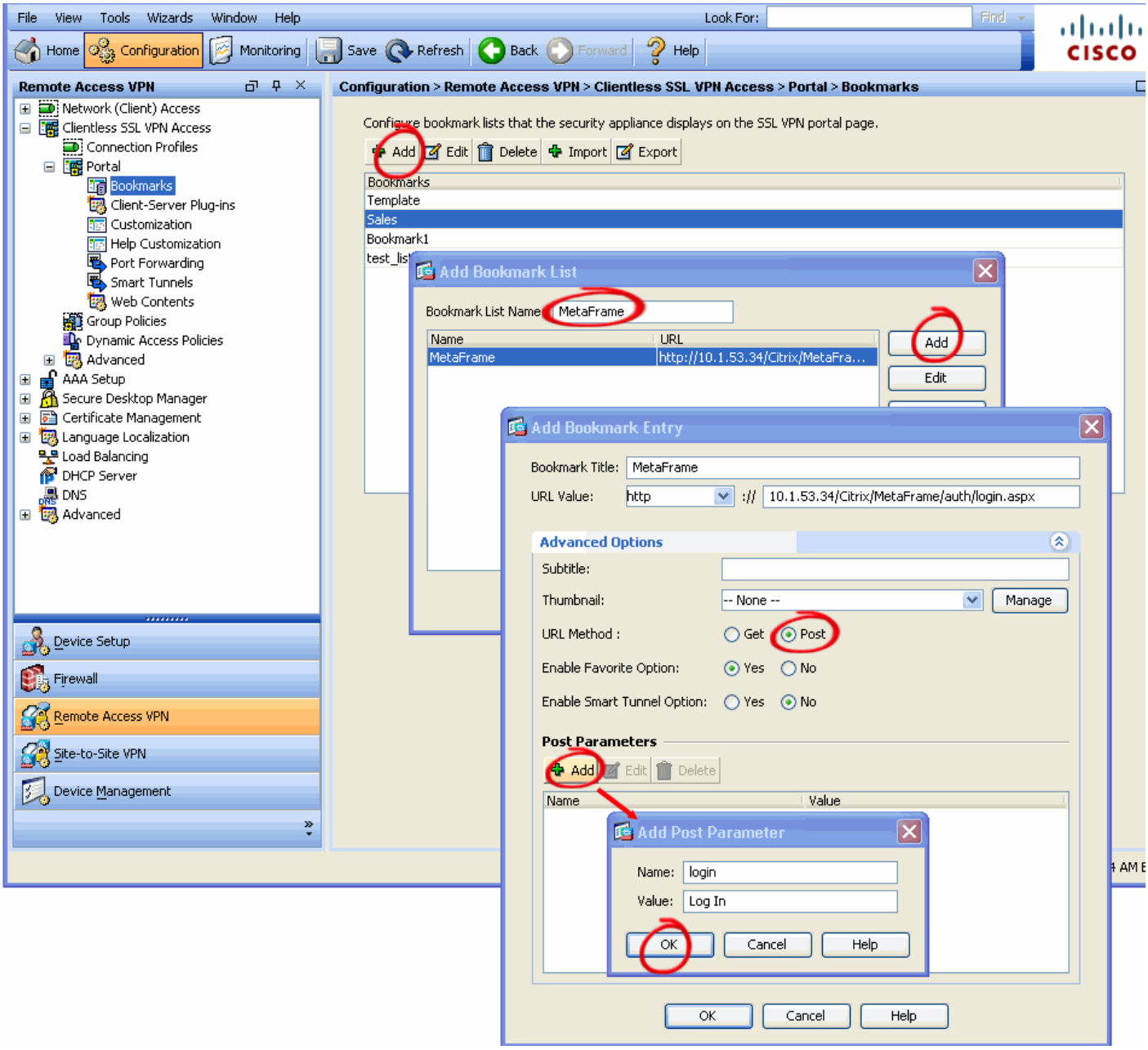
Configuring Post Parameters for Single Sign-on with Citrix

The following procedure uses Post parameters to create a new bookmark entry for Citrix with SSO.

Note Before following the procedure, use a browser capture tool such as http-watch to learn which parameters and values to specify.

Step 1 Navigate to Clientless SSL VPN Access > Portal > Bookmarks.

Step 2 Select a bookmark list, and click **Edit**. The Edit Bookmark List window opens.



Step 3 Click **Add** to create a new bookmark for Citrix. The Add Bookmark List window opens.

Step 4 Type a name, such as **MetaFrame**, in the text box next to Bookmark List Name.

Step 5 Click **Add** to create an entry to insert into the list. The Add Bookmark Entry window opens.

Step 6 Enter **MetaFrame** into the Bookmark Title text box.

The bookmark title and list have the same name because this list will have only one entry. The list name is for administrator use on ASDM; the bookmark title appears in the user's browser window.

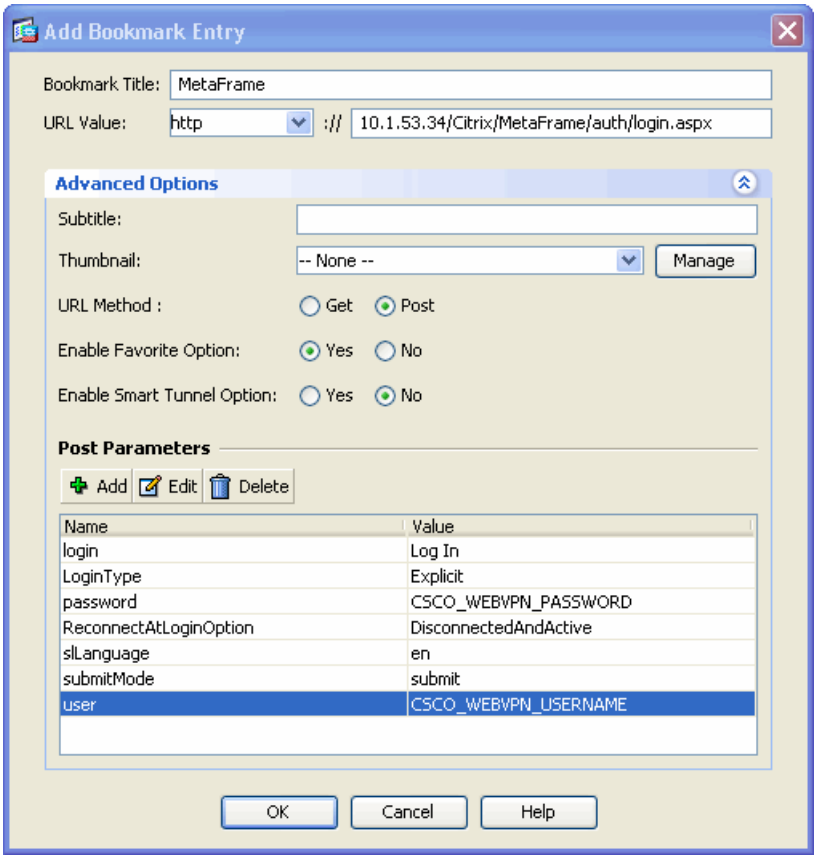
Step 7 Select **http** in the drop-down list next to "URL Value" and enter the Citrix login URL into the adjacent text box.

Step 8 Click **Post** next to URL Method.

Step 9 Click **Add**. The Add Post Parameter window opens.

Step 10 For each post parameter, enter the Name and Value text as follows, click **OK**, and reopen the Add Post Parameter window.

Note For the password attribute, use CSCO_WEBVPN_INTERNAL_PASSWORD rather than CSCO_WEBVPN_PASSWORD if you want to substitute the internal password of the security appliance for the user password.



Step 11 Click **OK** in each window. ASDM adds the newly created bookmark list to the Bookmarks window.

Step 12 Assign the bookmark list to each DAP and group policy for which you want to provide Citrix access, as follows:

- DAP—Choose **Configuration > Remote Access VPN > Clientless SSL VPN Access > Dynamic Access Policies,** double-click the DAP, click the **URL Lists** tab in the Access Policy Attributes area, check Enable URL Lists, select the name of the bookmark list below, and click **OK**.
- Group Policy—Choose **Configuration > Remote Access VPN > Clientless SSL VPN Access > Group Policies,** double-click the group policy, click **Edit > Portal**, uncheck Inherit next to Bookmark List, select the name of the bookmark list from the adjacent drop-down list, and click **OK**.

Step 13 Click **Apply** to save the changes to the running configuration.

Step 14 Verify that you are able to successfully connect into the Cisco Clientless SSL VPN page and use the bookmark without Citrix prompting for credentials.

SSO Substitution via Active Directory Attribute Mapping

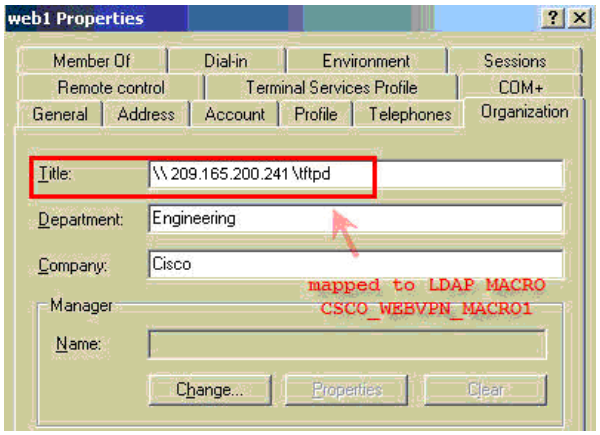
You can use values from a Radius or LDAP server for macro substitutions, using the CSCO_WEBVPN_MACRO1 and CSCO_WEBVPN_MACRO2 macros.

This example shows how to use macro substitution with values from an Active Directory/LDAP server during authentication/authorization of the SSL VPN clientless session. You accomplish this substitution by using a field in the LDAP/AD server to represent a URL. You then map the URL to a bookmark on the portal.

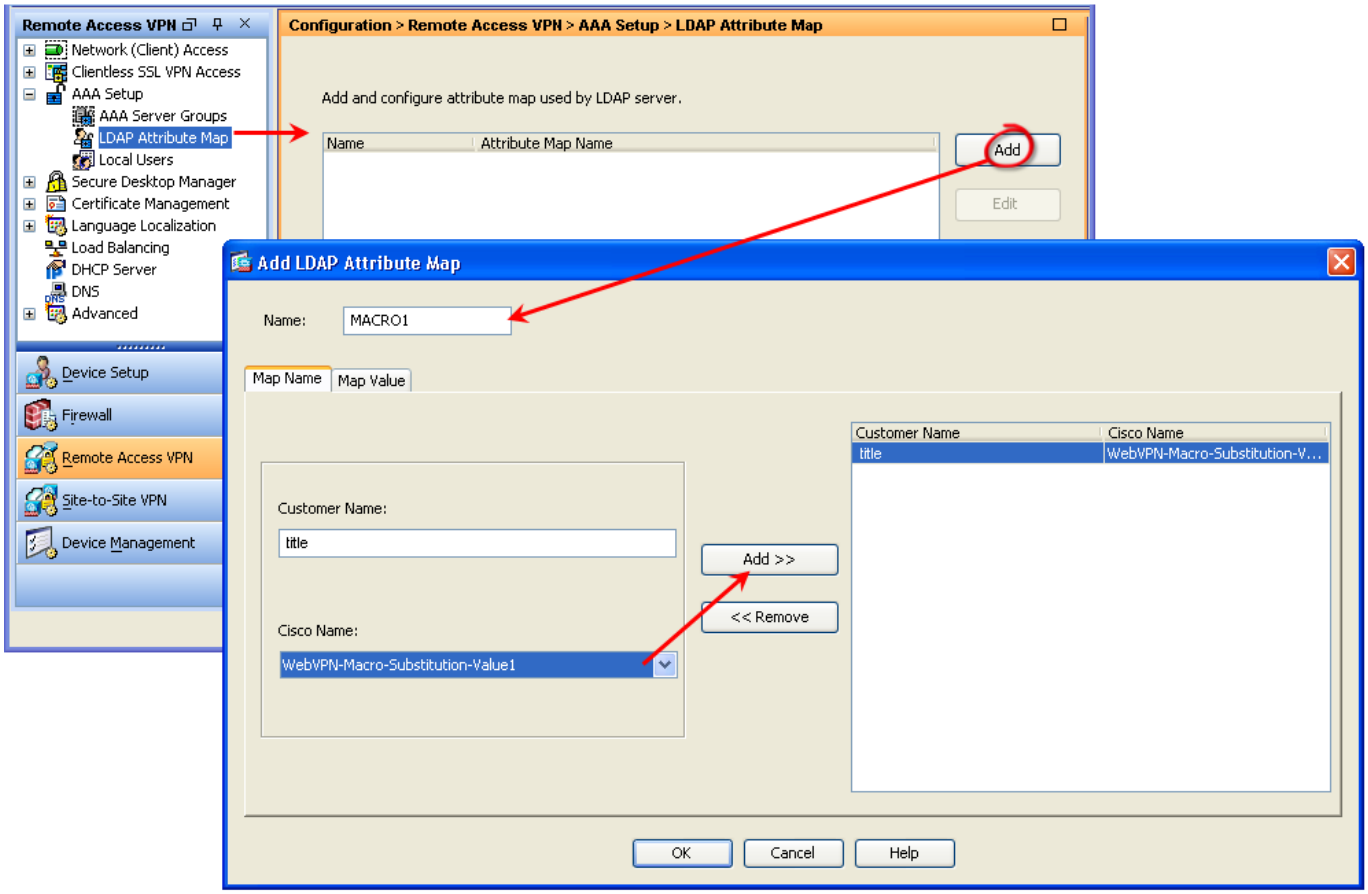
In this example, the AD user Title parameter having a value of \\209.165.200.241 maps to cifs://209.165.200.241/tftpd bookmark.

Note You can perform LDAP attribute mapping with any LDAP server.

Step 1 On the LDAP server, populate the user attribute Title with the URL \\209.165.200.241\tftpd.



Step 2 In ASDM, navigate to AAA Setup > LDAP Attributes Map. Click **Add**. The Add LDAP Attribute Map windows displays:

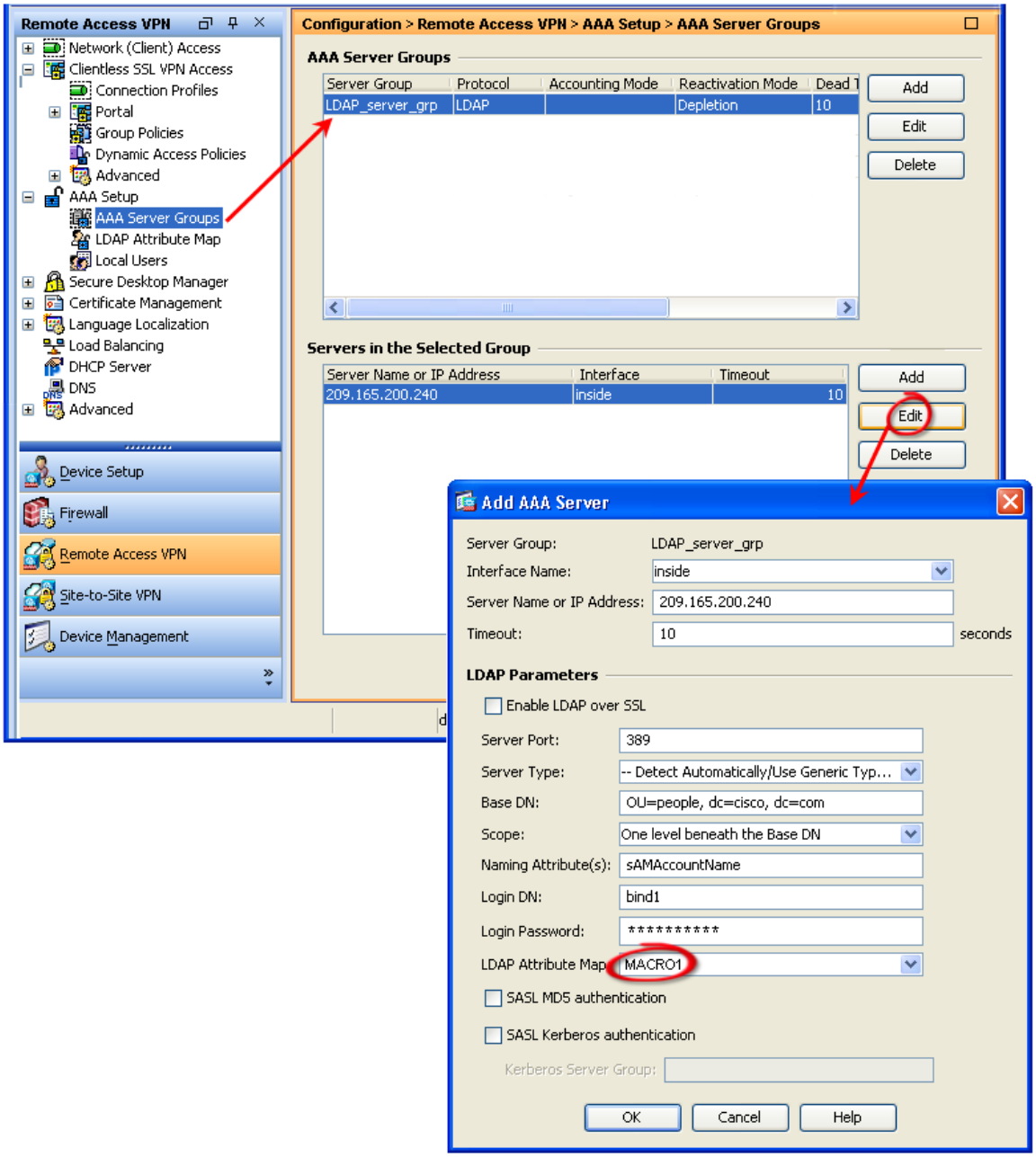


Step 3 Enter a name for the macro and click the Map Name tab.

Step 4 Enter a customer name, select the name of the Cisco attribute and click **Add**.

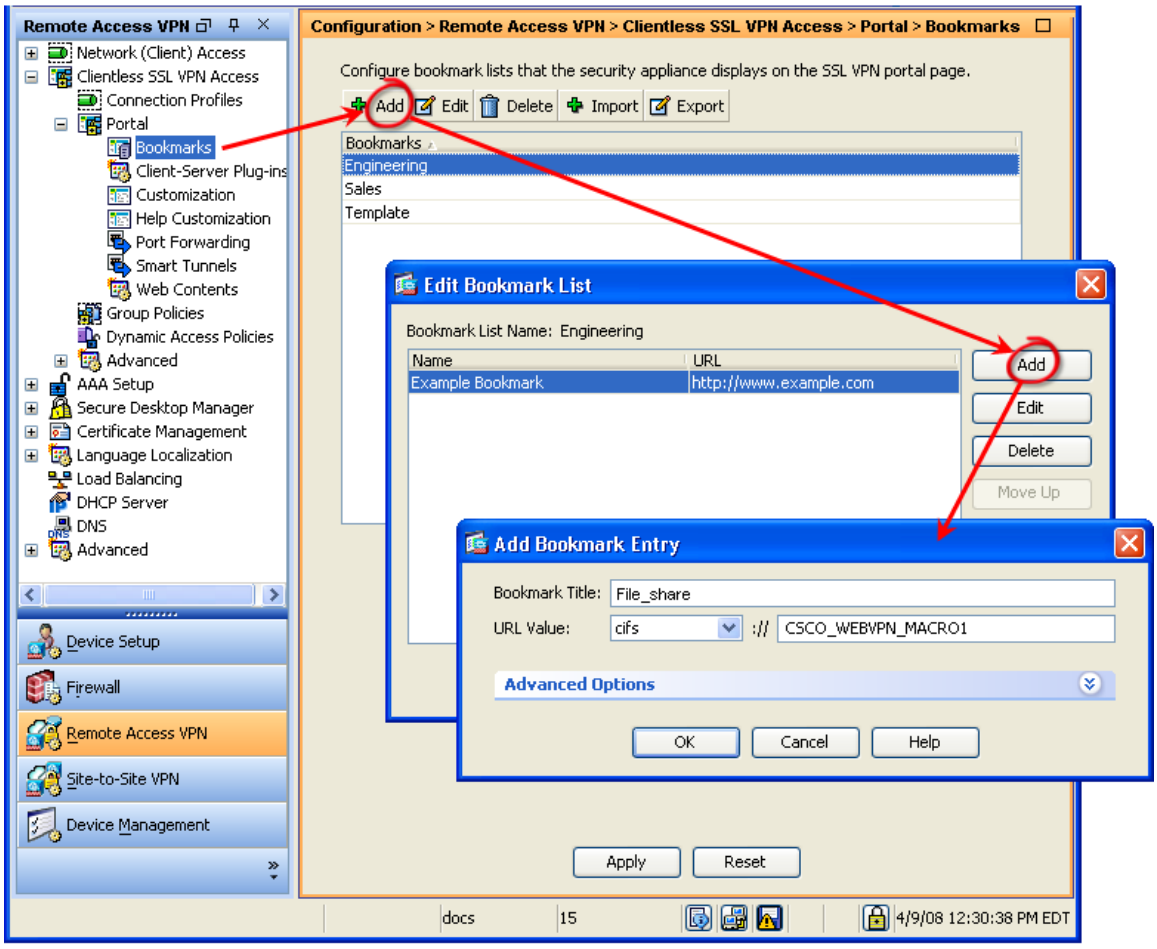
Step 5 Navigate to Configuration > Remote Access VPN > AAA Setup > AAA Server Groups > Edit AAA Server.

Step 6 Apply the LDAP attribute map to the LDAP AD server:



Step 7 Navigate to the Clientless SSL VPN Access > Portal > Bookmarks. Select a bookmark list and **Edit**. The Edit Bookmark List displays.

Step 8 Click Add. The Add Bookmark list displays. Enter the bookmark information:



Step 9 Establish a clientless SSL VPN session and observe that the portal has the bookmark. Click the bookmark to see that it takes you to address you specified, cifs://<*IP address*>/tftpd. The example screen below shows the new link:

Accessing Applications using Smart Tunnels and Plug-ins over Clientless Connections

This section describes how to configure the security appliance to allow application access using plug-ins or Smart Tunnels over clientless SSL VPN connections. Use the Table 1 to help you choose which access method to use.

Table 1 Clientless, Plug-in, and Smart Tunnel Usage Guidelines

Topic	Clientless SSL VPN (Using Content Rewriting)	Smart Tunnel (Bypassing Content Rewriter)	Plug-in
Recommendations	Use for all web applications unless the user experience is unsatisfactory. Most administrators choose this method for most web applications, including Citrix Presentation Server, OWA, or SharePoint	Enable Smart Tunnels if a specific application and/or a URL is experiencing problems over a clientless connection or if you want to use the native client application on the PC, such as Microsoft RDP. **Note:** If you enable a URL for Smart Tunnels, a client application is *not* required	Import a plug-in to allow a browser to perform a dedicated function, such as connect a client to a server within the browser window. Available plug-ins include SSH, RDP, VNC, and Citrix. Use a plug-in whenever the clientless connection or Smart Tunnel is not an option.
Client application required?	✗	✓	✗
Guest user access rights OK	✓	✓	✓
Stateful failover	✓ Not for IPv6 or Citrix authentication	✗	✗
Relative Performance	Lower	Between clientless and plug-ins	Higher
Session support for proxy server	✓	✗	✗
Macro_Substitutions variables	✓	✓	✗
32-bit Microsoft Windows operating systems (Vista, XP, and 2000)	✓	✓	✓
Mac OS 10.4 and 10.5	✓	✗	✓
Tested 32-bit Linux	✓	✗	✓

Plug-ins

The security appliance supports Java plug-ins for clientless SSL VPN connections. Plug-ins are Java programs that operate in a browser. These plug-ins include SSH/Telnet, RDP, VNC, and Citrix.

Per the GNU General Public License (GPL), Cisco redistributes plug-ins without making any changes to them. Per the GPL, Cisco cannot directly enhance these plug-ins.

To use plug-ins you must install Java Runtime Environment (JRE) 1.4.2.x or greater. You must also use a compatible browser specified here:
http://www.cisco.com/en/US/docs/security/asa/compatibility/asa-vpn-compatibility.html

Plug-in Requirements and Restrictions

Note Each SSH/Telnet, RDP, and VNC plug-in is an open source client redistributed without any changes, per the GNU General Public License. The origin of this client is http://javassh.org/.

Clientless SSL VPN must be enabled on the security appliance to provide remote access to the plug-ins.

The plug-ins do not work if the security appliance configures the clientless session to use a proxy server.

The minimum access rights required for remote use belong to the guest privilege mode. The plug-ins automatically install or update the Java version required on the remote computer.

A stateful failover does not retain sessions established using plug-ins. Users must reconnect following a failover.

Install an SSL certificate onto the security appliance interface to which remote users use a fully-qualified domain name (FQDN) to connect.

Note Do not specify an IP address as the common name (CN) for the SSL certificate. The remote user attempts to use the FQDN to communicate with the security appliance. The remote PC must be able to use DNS or an entry in the System32\drivers\etc\hosts file to resolve the FQDN.

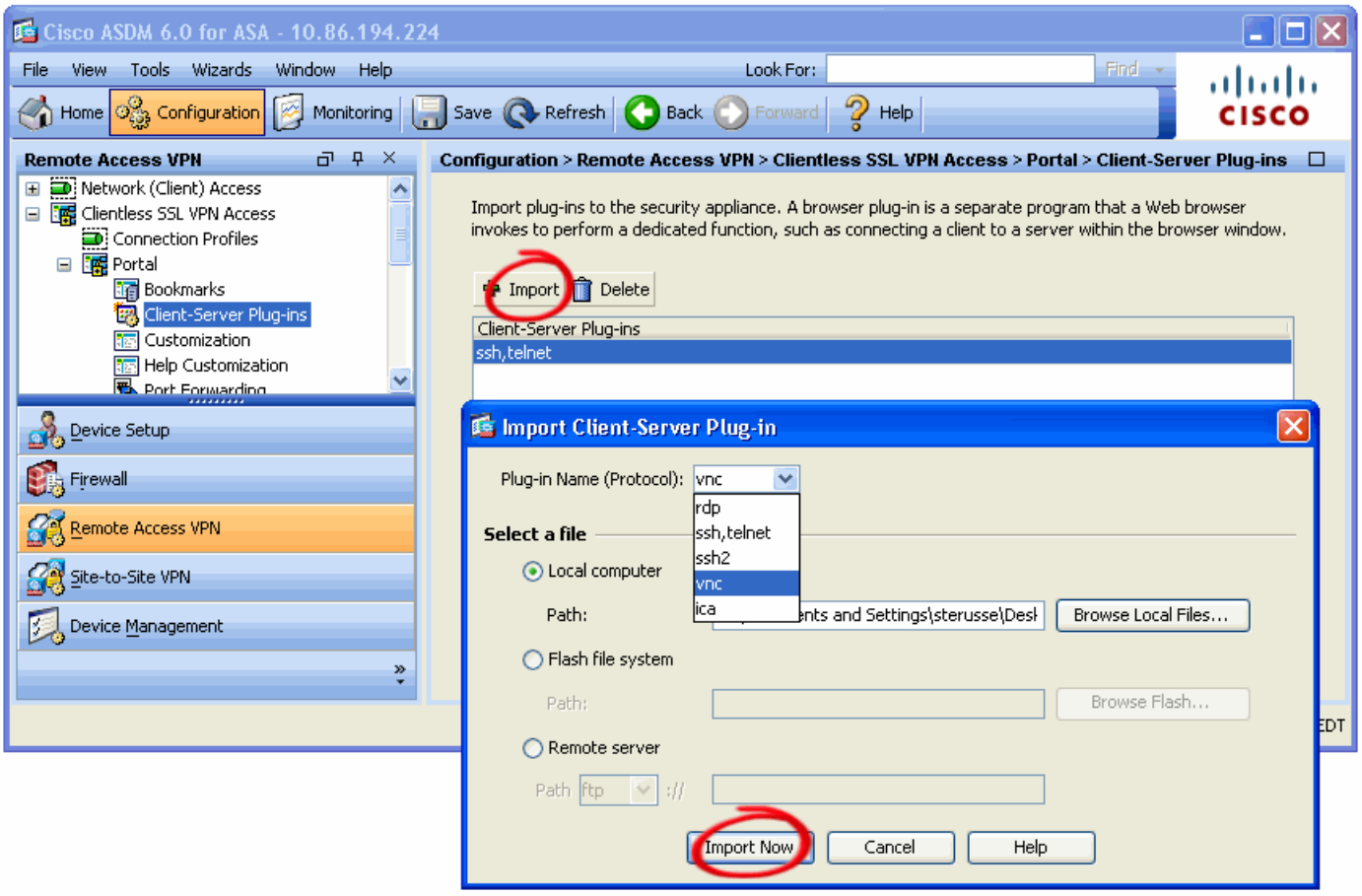
Importing Plug-ins

Plug-ins are not pre-installed on the ASA. Before you can use a plug-in, you must import it to the security appliance.

To import plug-ins, perform the following steps.

Step 1 Download the latest Cisco-published plug-ins from http://www.cisco.com/cgi-bin/tablebuild.pl/asa.

Step 2 To import the plug-ins, choose **Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Client-Server Plug-ins**.



Step 3 Click **Import**.

Step 4 Select the plug-in protocol from the **Plug-in Name** drop-down list.

Step 5 Click **Browser Local Files**, select the plug-in you downloaded, and click **Select**.

Step 6 Click **Import**.

Step 7 Click **OK** when the Information window opens.

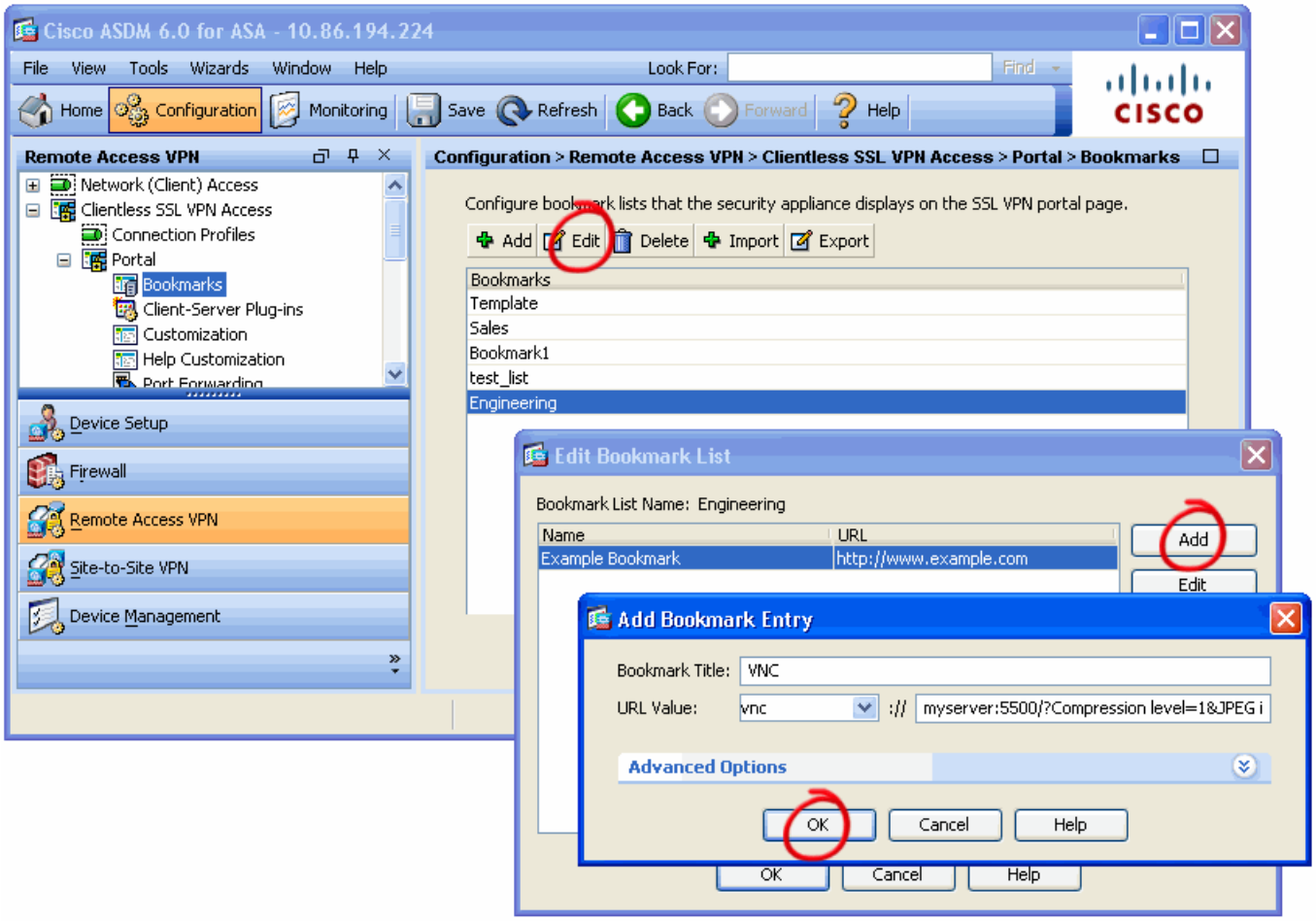
Configuring a Plug-in to Appear As a Bookmark

To predefine a bookmark for the plug-in and assign the bookmark to the group policy or DAP, perform the following steps:

Note As an alternative to this procedure, you can follow the instructions in one of the Using the Plug-in" sections that follows to enter the URL into the Address field of the Cisco Clientless SSL VPN page; however, if you want to use single sign-on (SSO), you must use this procedure because the user cannot enter the SSO-enabled URL on the Cisco Clientless SSL VPN page.

Step 1 Choose **Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Bookmarks**.

Step 2 Select a bookmark list already assigned to the group policy or DAP to be tested and click **Edit**, or click **Add** to create a new bookmark list if one is not already assigned.



Step 3 Name the bookmark list if this is a new one.

Step 4 Click **Add** to add an entry identifying the server to be accessed by the plug-in.

Step 5 Assign values to the following parameters:

Bookmark Title—Enter the name of the bookmark to appear in the Cisco Clientless SSL VPN browser window.

URL Value (drop-down list)—Select http, https, cifs, ftp, ssh, telnet or vnc to specify the protocol to be used to access the server.

URL Value (text box)—Enter the URL of the server, along with any parameters you want to specify.

Note To view the parameters for a plug-in, establish a clientless SSL VPN session with the security appliance, click the menu option associated with the plug-in protocol, and view the help on the right side of the page. (You do not need a bookmark configured to view the help, but the plug-in must be added to the running configuration for the help to appear.) The instructions in the "Using the Plug-in" sections that follow also provide basic syntax guidelines.

Refer to the following list of URLs if you want to add one without consulting the help. Substitute the text indicated in italics with the name of the server on your network:

- RDP without SSO—*terminal-server*/?geometry=1024X800&FullScreen=true
- SSH—*ssh-server*
- VNC—*vnc-server*:5500/?Compression level=1&JPEG image quality=9

All plug-ins support single sign-on (SSO). Enter the parameter csco_sso=1 if you want the bookmark to support it. For example, the following RDP URL supports SSO:

terminal-server/?geometry=1024X800&FullScreen=true&csco_sso=1

Note Plug-ins do not support the Macro_Substitutions variables.

Step 6 Click **OK** to add the entry to the bookmark list, then **OK** again.

Step 7 Assign the bookmark list to each DAP and group policy for which you want to provide bookmark access:

- DAP—Choose **Configuration > Remote Access VPN > Clientless SSL VPN Access > Dynamic Access Policies,** double-click the DAP, click the **URL Lists** tab in the Access Policy Attributes area, check Enable URL Lists, select the name of the bookmark list below, and click **OK**.
- Group Policy—Choose **Configuration > Remote Access VPN > Clientless SSL VPN Access > Group Policies,** double-click the group policy, click **Edit > Portal**, uncheck **Inherit next to Bookmark List**, select the name of the bookmark list from the drop-down list, and click **OK**.

Step 8 Click **Apply** to save the changes to the running configuration.

Using the SSH Plug-in

To use the SSH plug-in, perform the following steps.

Step 1 Clear your Java Runtime (JRE) cache.

Step 2 Start the clientless SSL VPN session.

Step 3 Click the SSH link and confirm that the plug-in starts, or manually enter the URL into the Address field. For entering the URL manually, the basic SSH URL is ssh://*server.* and the basic SSH URL is telnet://*server.* You can ask someone, that has physical access to the computer, for the full computer name. In Windows, this name is found in:

Start > (Settings >) Control Panel > Performance and Maintenance > System > Computer Name tab.

You can also add the following additional parameters beyond the basic URL in the format **server:port/?parameters** :

port (optional)—The virtual address of the host computer to which you want to connect.

parameters (optional)—a query string of parameter-value pairs in this format:

```
server:port/?Parameter1=value&Parameter2=value&Parameter3=value
```

Note For help with the URL syntax, click **Telnet/SSH Servers** on the left menu.

For each additional SSH session you want to establish, click “Click here if you want to open another window with the Cisco Clientless SSL VPN page”, then click the SSH link again.

Using the RDP Plug-in

To use the RDP plug-in, perform the following steps.

Step 1 Clear your Java Runtime (JRE) cache.

Step 2 Open the clientless SSL VPN session.

Step 3 Click on the RDP link and confirm that the plug-in starts, or manually enter the URL into the Address field.

The basic URL can be rdp://terminal-server/?geometry=1024X800&FullScreen=true

Note Help for this plug-in and all associated parameters displays on the right-pane after you open a clientless SSL VPN session and click the Terminal Servers icon on the left menu.

The parameters available for the ActiveX client used by Microsoft Internet Explorer include:

- RedirectDrives—Set to true to map remote drives locally.
- RedirectPrinters—Set to true to map remote printers locally.
- FullScreen— Set to true to start in FullScreen mode.
- force_java—Set to yes to force the Java client.

An intermediate window opens, then a client popup window. Please don't close the intermediate window, or return to the main page until your work is finished, otherwise the popup window closes.

Step 4 Enter the user credentials if they are required, and ensure the plug-in connects to the terminal server.

The plug-in supports both Microsoft ActiveX control and Java modes. The security appliance first tries to start the plug-in using ActiveX, used by Microsoft Internet Explorer. If ActiveX fails, Java, used by Mozilla Firefox, starts the plug-in.

Smart Tunnels

The smart tunnel feature allows only winsock2 TCP applications to use the security appliance as a proxy gateway to the private side of a network. Examples of applications that work through smart tunnels include Telnet, Passive FTP, Outlook Express, Sametime, SSH, RDP, and VNC.

Note We recommend that you enable CSD cache-cleaner whenever you are using smart tunnels. The cache-cleaner removes any sensitive content in the cache of the browser and logs out the user after the user closes all browser windows.

Requirements for Smart Tunnels

To use smart tunnels, you must have the following:

- A browser with either ActiveX or Java *and* JavaScript.
- 32-bit operating system only (you cannot use 32-bit applications on a 64-bit OS).
- Microsoft Windows XP, 2000, or Vista. For Vista, if you are starting smart tunnels from Internet Explorer protected mode, the security appliance must be in the trusted zone.
- If you need a proxy to reach the security appliance, only basic authentication is supported. Also, the remote end (the private side, not the security appliance) must be in the excluded list (or you must configure the application to reach the remote end by its normal address rather than the proxy address).

Note Smart tunnels do not support MAPI with Microsoft Exchange.

The smart tunnel feature intercepts all connections and redirects them to the security appliance, except connections to the following:

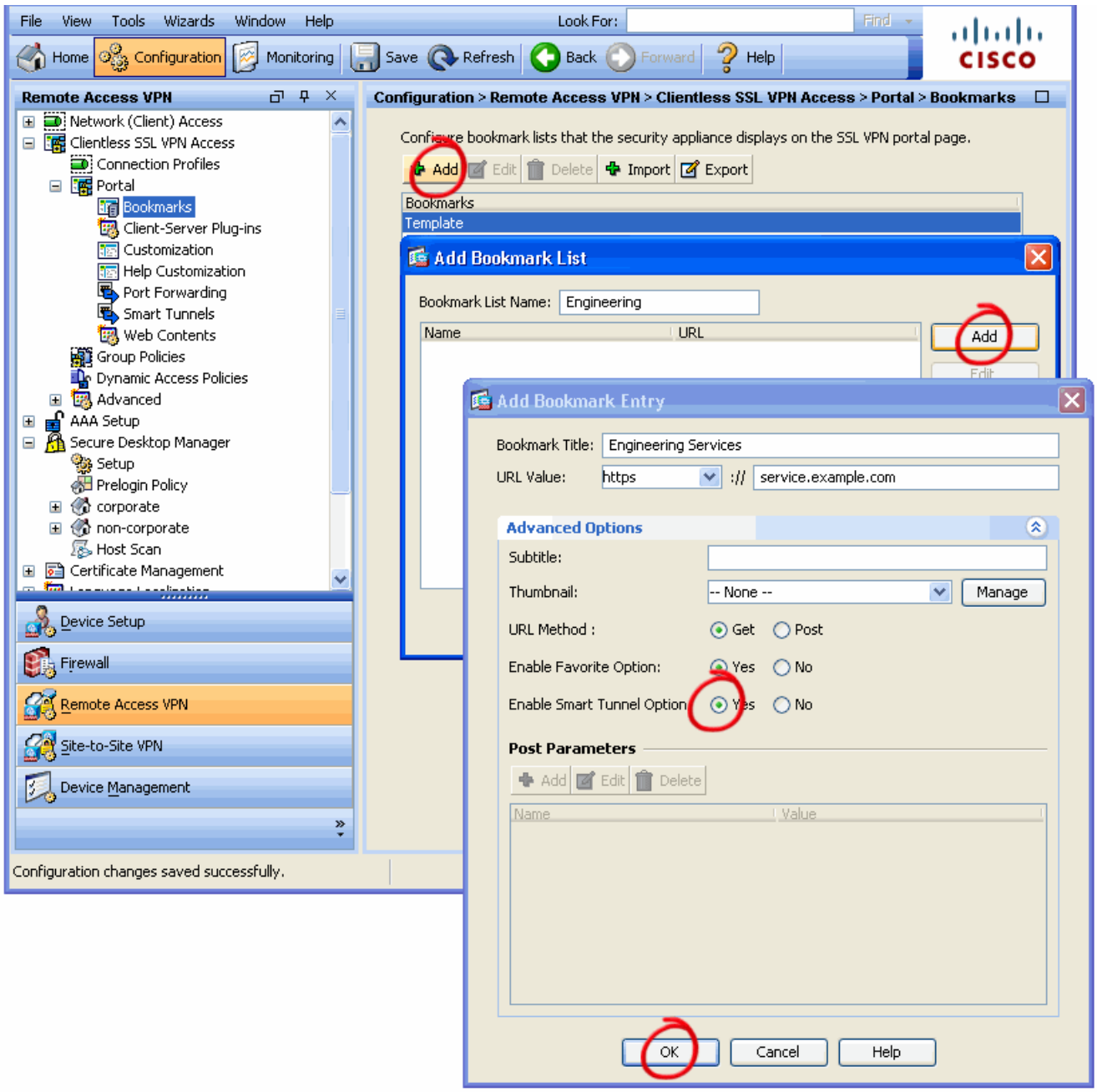
- The security appliance (no point to redirect).
- The proxy (because the endpoint might not be able to reach the security appliance without going through the proxy; the alternative would be to implement a proxy within the smart tunnel, which bloats its size prohibitively).
- The local host.

Connections to proxies are not redirected. For a smart tunnel to intercept and redirect a connection to an application, the application must call connect to the target address, not the proxy address. If an application is connecting to a proxy, it is probably aware of the proxy settings, so it probably knows about the Internet Explorer proxy exception list as well. Therefore, we recommend that you insert the target addresses into the Internet Explorer proxy exception list.

Using Smart Tunnels for Web Applications

If an application does not render well through the clientless rewriter, you can modify a bookmark for the application to enable the Smart Tunnels for that bookmark. This does not require additional CLI commands. It is just a convenient way to open a bookmark within a new window, using the smart tunnel feature to pass the traffic for that application, avoiding rewrite issues.

Step 1 Choose **Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Bookmarks**.



Step 2 Click **Add** to create a bookmark list, and name it *Engineering* or *Sales*.

Step 3 Click **Add** to open the Add Bookmark Entry pane.

Step 4 Configure the bookmark entry, then click **Advanced Options**.

Step 5 Click **Enable Smart Tunnel Option.**

Step 6 Click **OK** twice, then click **Apply** to save the changes to the running configuration.

Step 7 Establish a clientless SSL session and click the smart tunnel-enabled bookmark.

The application opens in a new browser window.

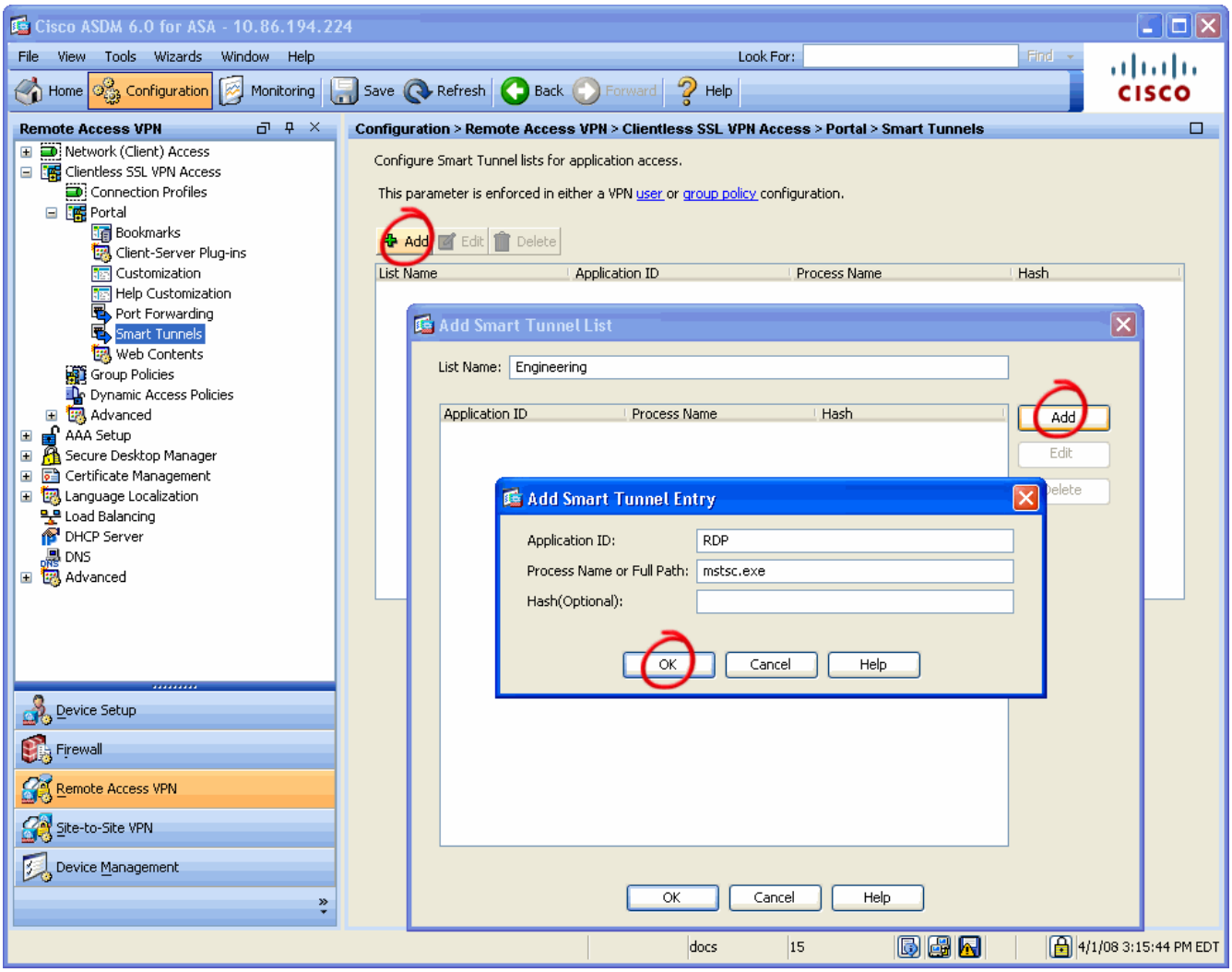
Configuring Smart Tunneling for Nonbrowser-based Applications

Configuring the smart tunnel feature to support an application requires that you know which processes the application executes. For example, because RDP uses the process mstsc.exe, you must specify that process name when creating a smart tunnel entry for RDP.

Note Complicated applications can require multiple processes. Some processes have parent processes, which an application also requires. Applications started from the Windows Command window, such as Telnet, require Telnet access to the cmd.exe process. We recommend that you use a utility to identify the processes of the application you want the Smart Tunnel feature to start before proceeding, if you choose an application other than the one used in the example.

The following example configures the Smart Tunnel feature to support RDP.

Step 1 Choose **Configuration > Remote Access VPN > Clientless SSL VPN Access > Portal > Smart Tunnels.**



Step 2 Click **Add**. The Add Smart Tunnel List window opens.

Step 3 Enter a list name such as **Engineering** into the List Name text box and click **Add**. The Add Smart Tunnel Entry window opens.

Step 4 In the Application ID text box, enter **RDP**.

Step 5 In the Process Name or Full Path text box, enter **mstsc.exe**.

Step 6 Click **OK** to insert the entry into the list.

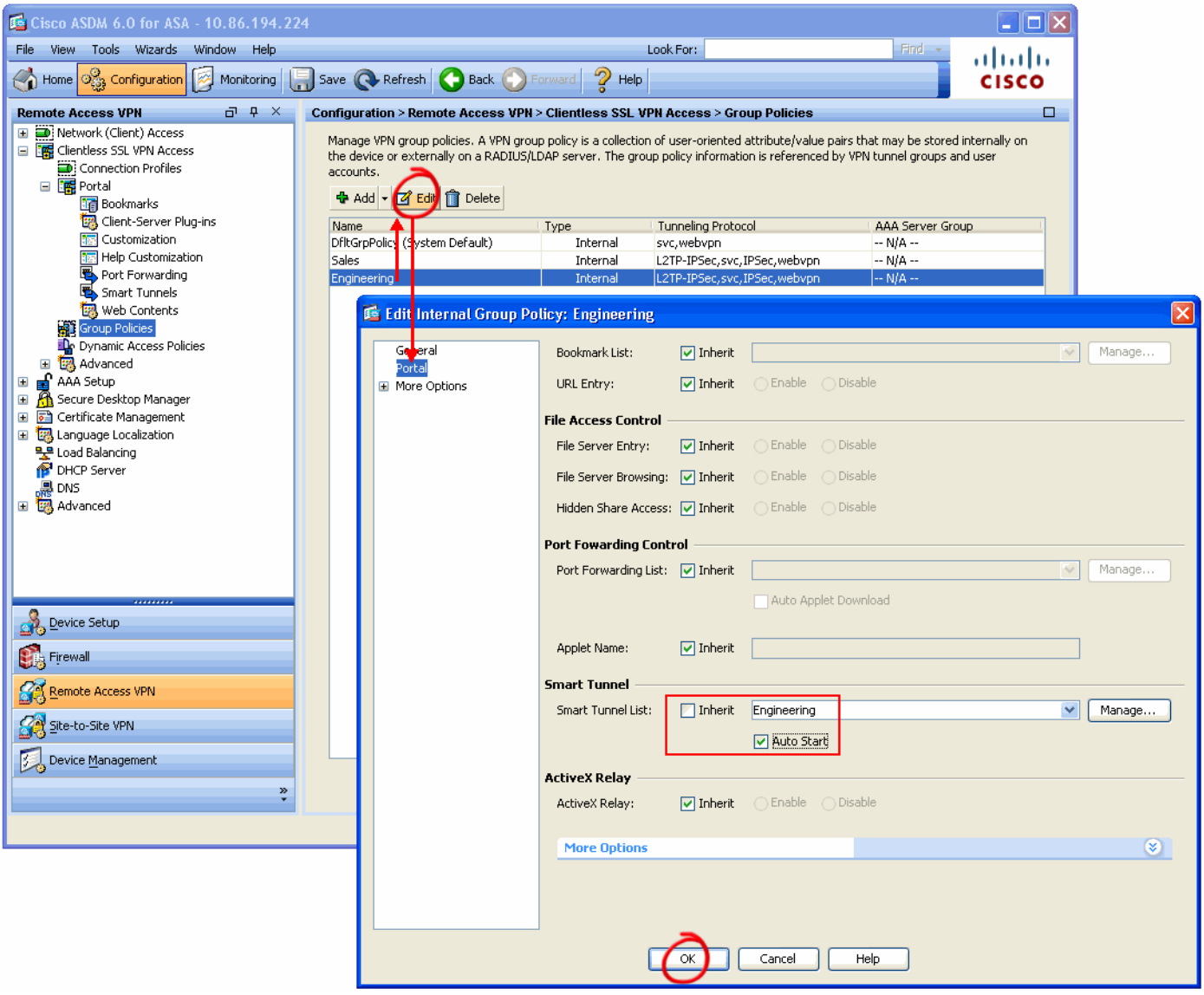
Step 7 Add more entries for each additional process the application requires, using the same value for the Application ID.

Step 8 Click **OK** to insert the list, then click **Apply** to save it to the running configuration.

Assigning a Smart Tunnel List to a Group Policy

If a group policy specifies a smart tunnel list and the security appliance assigns the policy to a clientless session, the applications specified in the list become available to the session. Therefore, to complete the configuration of the smart tunnel feature, you must assign a smart tunnel list to any group policies to be applied to the users for whom you want to provide smart tunnel access, as follows:

Step 1 Choose **Configuration > Remote Access VPN > Clientless SSL VPN Access > Group Policies**.



Step 2 Select the policy for which you want to provide smart tunnel access and click **Edit**. The Edit Internal Group Policy window opens.

Step 3 Click the **Portal** option in the left menu.

Step 4 Uncheck **Inherit** next to Smart Tunnel List.

Step 5 Select the smart tunnel list you created earlier from the adjacent drop-down menu.

Step 6 Check **Auto Start** if you want to start smart tunnel access automatically upon user login, or leave it unchecked to require the user to click **Application Access > Start Smart Tunnels** on the Cisco Clientless SSL VPN page for the smart tunnel feature to work.

Step 7 Click **OK**, then click **Apply** to save the changes to the running configuration.

Using Smart Tunnels

To use the smart tunnel feature if the Auto Start option is checked, establish a clientless SSL session, then start the application from outside of the browser. For example, to initiate an RDP session through the clientless SSL connection, start Remote Desktop Connection natively on the client PC.

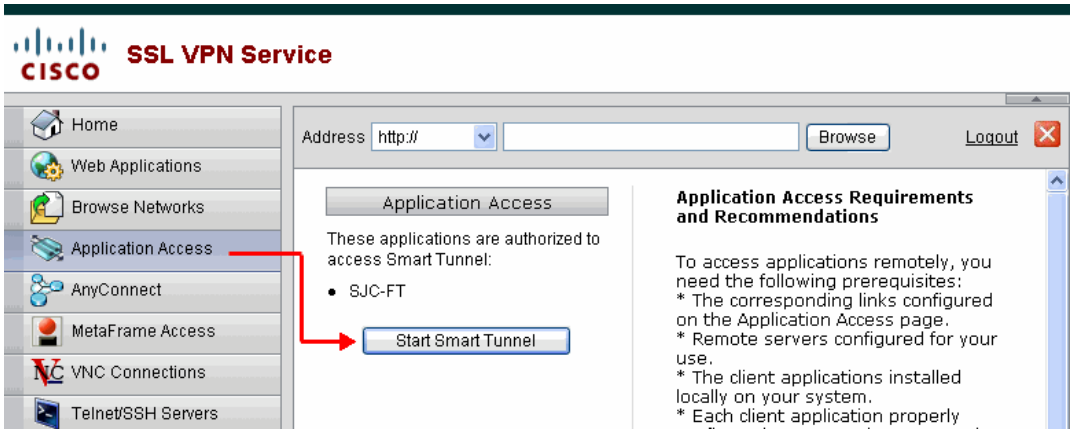
To use the smart tunnel feature if the Auto Start option is unchecked, perform the following steps:

Step 1 Establish a clientless SSL session, as follows:

- Enter the fully-qualified domain name (FQDN) into the address field of the browser (e.g., http://*fqdn*), then enter login credentials associated with the group policy for which you assigned the smart tunnel list.
- Enter the FQDN, followed by "Admins" ("Admins" is case-sensitive, e.g., http://*fqdn*/Admins), then enter the administrator's login credentials to receive an aggregation of the policies configured on the security appliance.

Step 2 Click **Application Access**.

Step 3 Click **Start Smart Tunnel**.



Step 4 Click **Yes** in response to the confirmation prompts.

The Start Smart Tunnel button changes to the text "Smart Tunnel has been started," and a list shows the eligible applications that can connect to the private side of the network.

Step 5 Start the application from outside of the browser. For example, to initiate an RDP session through the tunnel to the server, start Remote Desktop Connection natively on the client PC.

Dynamic Access Policies (DAP)

Using DAPs for VPN Policies (no Cisco Secure Desktop)

In this section we configure and test basic Dynamic Access Policies (DAP). The security appliance combines or aggregates DAP access attributes, for example, ACLs and URL lists, from multiple DAP records and then applies them to user sessions.

In 8.0.x not all VPN authorization/enforcement attributes can be set in DAP, therefore the security appliance enforces the complete VPN policy as the aggregation of the DAP record(s) and the group-policy attributes.

The current VPN policy enforcement/authorization criteria is defined at http://www.cisco.com/en/US/partner/docs/security/asa/asa80/configuration/guide/extsvr.html, "Understanding Policy Enforcement of Permission and Attributes"section, as summarized below:

The security appliance applies attributes in the following order:

1. Dynamic Access Policy attributes—Take precedence over all others.
2. User attributes—The AAA server returns these after successful user authentication or authorization.
3. Group policy attributes —These attributes come from the group policy associated with the user. You identify the user group policy name in the local database by the vpn-group-policy attribute or from a RADIUS/LDAP server by the value of the RADIUS CLASS attribute (25) in the OU=GroupName. The group policy provides any attributes that are missing from the DAP or user attributes.
4. Connection profile (tunnel group) default-group-policy attributes —These attributes come from the default group policy associated with the connection profile. This group policy provides any attributes that are missing from the DAP, user or group policy.
5. System default attributes—System default attributes provide any values that are missing from the DAP, user, group policy, or connection profile.
6. If the security appliance receives attributes from multiple sources, the attributes are aggregated and applied to the user policy. If there are conflicts between attributes coming from the external AAA server and from a group policy, those attributes obtained from the DAP always take precedence.

Advantages of Using DAP instead of Group Policies

DAP provides:

- Flexible VPN policy selection criteria based on AAA or endpoint access attributes.
- Tighter integration with Active Directory attributes (for example, memberOf).
- Aggregation of multiple DAP policies.

Creating a DAP for Engineering

To create a DAP for Engineering users, perform the following steps:

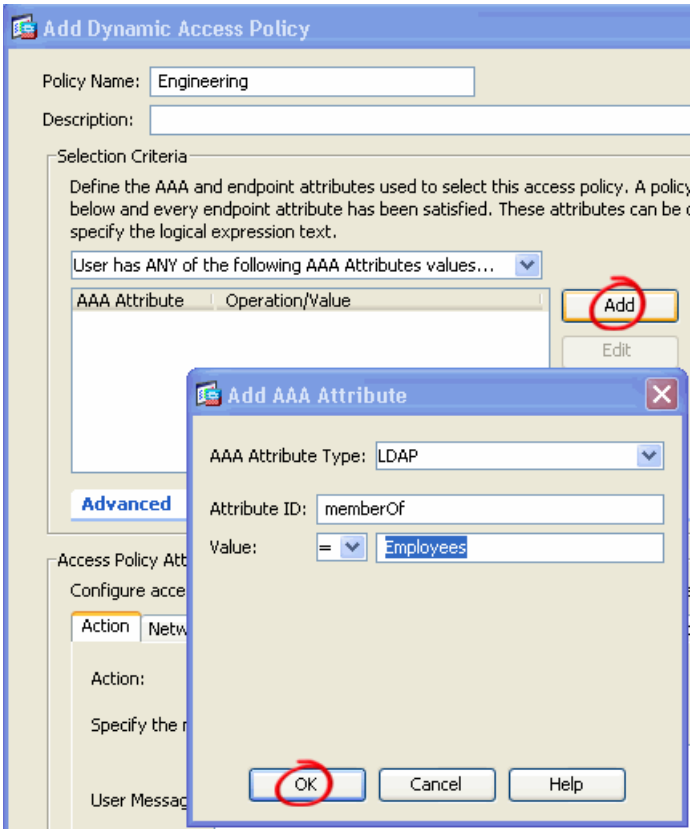
Step 1 Remove the bookmark list assignment from each group policy and URL list assignment from each DAP that you previously configured.

Note You can configure local AAA service to run on this security appliance for testing.

Step 2 Configure the Engineering connection profile for LDAP authentication and authorization, using the Active Directory server configured earlier.

Step 3 Choose **Configuration > Remote Access VPN > Clientless SSL VPN Access > Dynamic Access Policies**.

Step 4 Click **Add**.



Step 5 Enter **Engineering** next into the Policy Name text box.

The next steps show how to assign the users for whom this DAP applies to two Active Directory groups (Employees and Engineering).

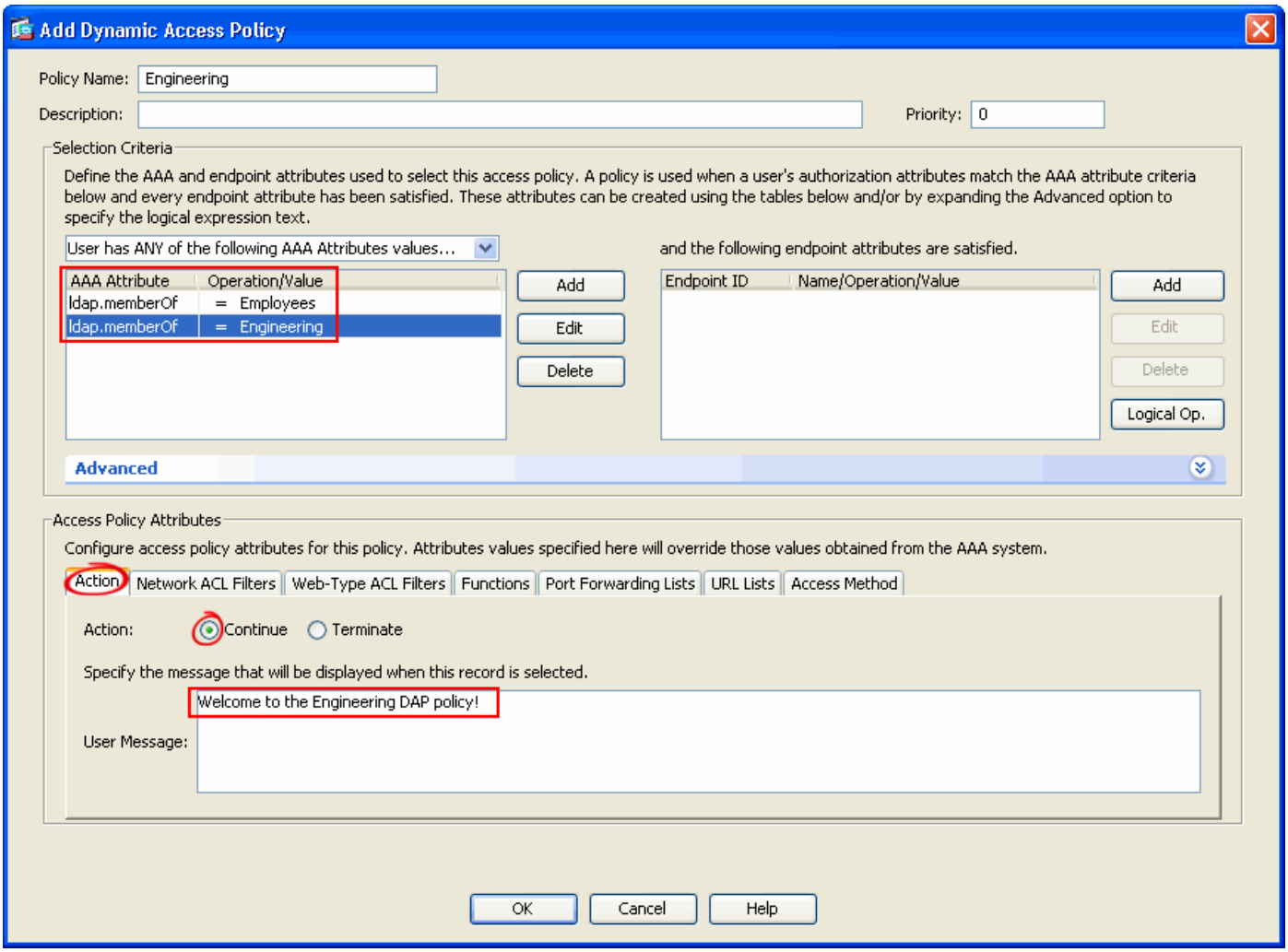
Step 6 In the AAA section on the left side of the window, click **Add**, and set the following parameters:

- AAA Attribute Type—LDAP
- Attribute ID—memberOf
- Value (drop-down list) — =
- Value (text box)—Employees

Note These steps assume you are using remote authentication. If you are using local authentication (that is, authentication configured on this security appliance), select **Cisco** next to AAA Attribute Type and enter the values to match those in the security appliance configuration. Then go to Step 9.

Step 7 Click **OK**.

Step 8 Add another AAA attribute record to the DAP using the same values, except enter Engineering in the Value text box.



Step 9 Use the following table to enter values into the Access Policy Attributes area of the window.

Table 2 Access Policy Attribute Settings for Engineering DAP Policy

Tab	Attribute	Value
Action	Action	Continue
Action	User Message	Welcome to the Engineering DAP policy!
Web-Type ACL Filters	Web-Type ACL	Engineering (select, then click **Add**)

Table 2 Access Policy Attribute Settings for Engineering DAP Policy

Tab	Attribute	Value
Functions	Entry	Disable
Lists	Enable lists (check box)	Check
Lists	Enable lists drop-down list	Engineering (select, then click **Add**)
Access Method	Access Method	AnyConnect Client

Step 10 Click **OK**, then click **Apply** to save the changes to the running configuration.

Verifying the DAP for Engineering

To verify the DAP for Engineering, perform the following steps:

Step 1 Establish the Clientless SSL VPN session to https://IP_FQDN/Engineering.

Step 2 Verify the following:

- Only the links configured as bookmarks are present on the Cisco Clientless SSL VPN page for Engineering.
- The Address Bar is not available to enter a URL. Only the links appear.

Creating a DAP for Sales

To create a DAP for Sales users, perform the following steps:

Step 1 Remove the bookmark list assignment from each group policy and URL list assignment from each DAP that you previously configured.

Step 2 Configure the Sales connection profile for LDAP authentication and authorization, using the Active Directory server configured earlier.

Note You can configure local AAA service to run on this security appliance for testing.

Step 3 Choose **Configuration > Remote Access VPN > Clientless SSL VPN Access > Dynamic Access Policies**.

Step 4 Click **Add**.

Step 5 Enter **Sales** into the Policy Name text box.

The next steps show how to assign the users for whom this DAP applies to two Active Directory groups (Sales and Employees).

Step 6 In the AAA section on the left side of the window, click **Add**, and set the following parameters:

- AAA Attribute Type—LDAP
- Attribute ID—memberOf
- Value (drop-down list) — =
- Value (text box)—Sales

Note These steps assume you are using remote authentication. If you are using local authentication (that is, authentication configured on this security appliance), select **Cisco** next to AAA Attribute Type and enter the values to match those in the security appliance configuration. Then go to Step 9.

Step 7 Click **OK**.

Step 8 Add another AAA attribute record to the DAP using the same values, except enter Employees in the Value text box.

Step 9 Use the following table to enter values into the Access Policy Attributes area of the window.

Table 3 Access Policy Attribute Settings for Sales DAP Policy

Tab	Attribute	Value
Action	Action	Continue
Action	User Message	Welcome to the Sales DAP policy!
Web-Type ACL Filters	Web-Type ACL	Sales (select, then click **Add**)
Functions	File Browsing	Disable
Lists	Enable lists (check box)	Check
Lists	Enable lists drop-down list	Sales (select, then click **Add**)
Access Method	Access Method	Web-Portal

Step 10 Click **OK**, then click **Apply** to save the changes to the running configuration.

Verifying the DAP for Sales

To verify the DAP for Sales users, perform the following steps:

Step 1 Establish the Clientless SSL VPN session to https://IP_FQDN/Sales.

Step 2 Verify the following in the Sales portal that opens.

- The Address bar lets you enter a URL.
- Attempting to browse to a file share (i.e., CIFS://<file-share>) fails (because file-browsing is disabled for this policy).
- Attempting to browse to Engineering fails (because the Web-type ACL denies access).

Creating a DAP for Administrators: An Example of Multiple DAP Aggregation

This section shows how to configure a DAP for a user who belongs to the Administrators, Engineering, Sales, and Employees Active Directory groups. The resulting DAP is an aggregation of the Administrators, Engineering, and Sales DAP polices, including the lists, ACLs, and other attributes.

To create a DAP for administrators, perform the following steps:

Step 1 Remove the bookmark list assignment from each group policy and URL list assignment from each DAP that you previously configured.

Step 2 Configure an Administrators connection profile for LDAP authentication and authorization, using the Active Directory server configured earlier.

Note You can configure local AAA service to run on this security appliance for testing.

Step 3 Choose **Configuration > Remote Access VPN > Clientless SSL VPN Access > Dynamic Access Policies**.

Step 4 Click **Add**.

Step 5 Enter **Administrators** into the Policy Name text box.

The next steps show how to assign the users for whom this DAP applies to three Active Directory groups (Administrators, Sales and Employees).

Step 6 Add a AAA attribute record consisting of AAA Attribute Type **LDAP** and Attribute ID **memberOf** with the Value Administrators, another for Engineering, another for Sales, and the last for Employees.

Note This step assumes you are using remote authentication. If you are using local authentication (that is, authentication configured on this security appliance), select **Cisco** next to AAA Attribute Type and enter the values to match those in the security appliance configuration instead.

Step 7 Click **OK**, then click **Apply** to save the changes to the running configuration.

Verifying the Multiple DAP Aggregation

To verify the DAP for administrators, perform the following steps:

Step 1 Establish the Clientless SSL VPN session to https://IP_FQDN/Admins.

The Administrators portal opens.

Step 2 Verify that the lists are an aggregation of the Engineering, Sales, and Administrators DAPs.

Integrating Cisco Secure Desktop with DAPs

This section provides information on how to use Cisco Secure Desktop with DAPs.

Installing and Enabling Cisco Secure Desktop

Cisco Secure Desktop Release 3.2.1 requires ASA Release 8.0(3). You do not need to restart the security appliance after you install or upgrade Cisco Secure Desktop. However, you must exit and restart your ASDM connection to access Secure Desktop Manager.

To install and enable Cisco Secure Desktop, perform the following steps.

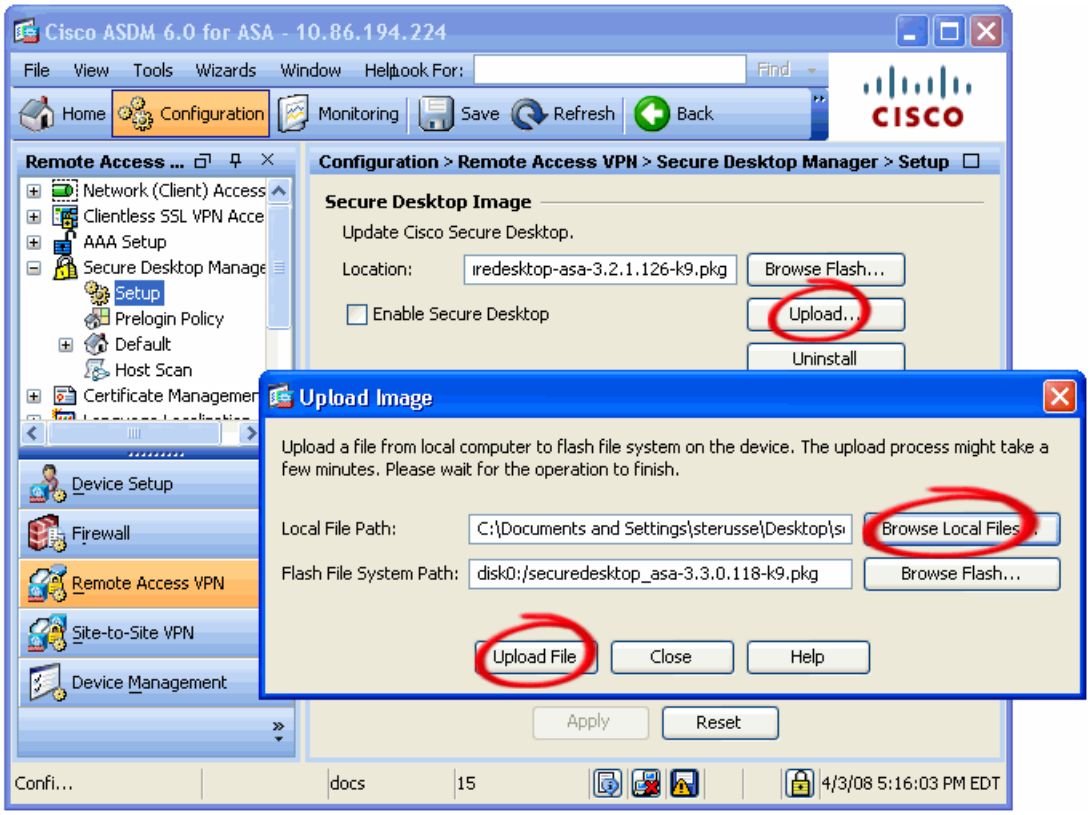
Note Be sure to install the Advanced Endpoint Assessment license.

Step 1 Use a browser to download the securedesktop.pkg from the following URL to "My Documents" on your PC:

http://www.cisco.com/cgi-bin/tablebuild.pl/securedesktop.

Step 2 Establish an ASDM session with the security appliance.

Step 3 Choose **Configuration > Remote Access VPN > Secure Desktop Manager > Setup**.



Step 4 Click **Upload** to prepare to transfer a copy of the Cisco Secure Desktop software from your local PC to the security appliance.

Step 5 Click **Browse Local Files** to select the file on your local PC.

Step 6 Choose the securedesktop.pkg you downloaded in and click **Select**.

Step 7 Click **Browse Flash** and enter the name of the securedesktop.pkg file you are uploading in the File Name field, then click **OK**.

Step 8 Click **Upload File**.

Step 9 Click **OK**.

The Use Uploaded Image dialog box displays the following message:

Use disk0:/securedesktop.pkg as your new current image?

Step 10 Click **OK**.

Step 11 Check **Enable Secure Desktop**.

Step 12 Click **Apply**.

An ASDM Restart Confirmation window displays the following message:

The Secure Desktop image is successfully updated. The new features can be accessed after ASDM is restarted.

Step 13 Choose **File > Save Running Configuration to Flash**.

Step 14 Close the ASDM session and restart before continuing.

Cisco Secure Desktop Prelogin Policy Checks

The prelogin policy feature lets you specify checks to be performed between the time the user establishes a connection with the security appliance and the time the user enters the login credentials. These checks determine whether to assign a prelogin policy or whether to display a Login Denied message for the remote user. The settings of the matched prelogin policy determine whether Secure Desktop, Cache Cleaner or only Host Scan loads. The application of a prelogin policy to a dynamic access policy (DAP) determines the access rights and restrictions placed on the connection.

When a remote PC attempts to establish a remote VPN connection, Cisco Secure Desktop automatically checks for the conditions you configure, and assigns the attribute settings of the prelogin policy associated with the result of the checks to the connection, or issues a login denied message.

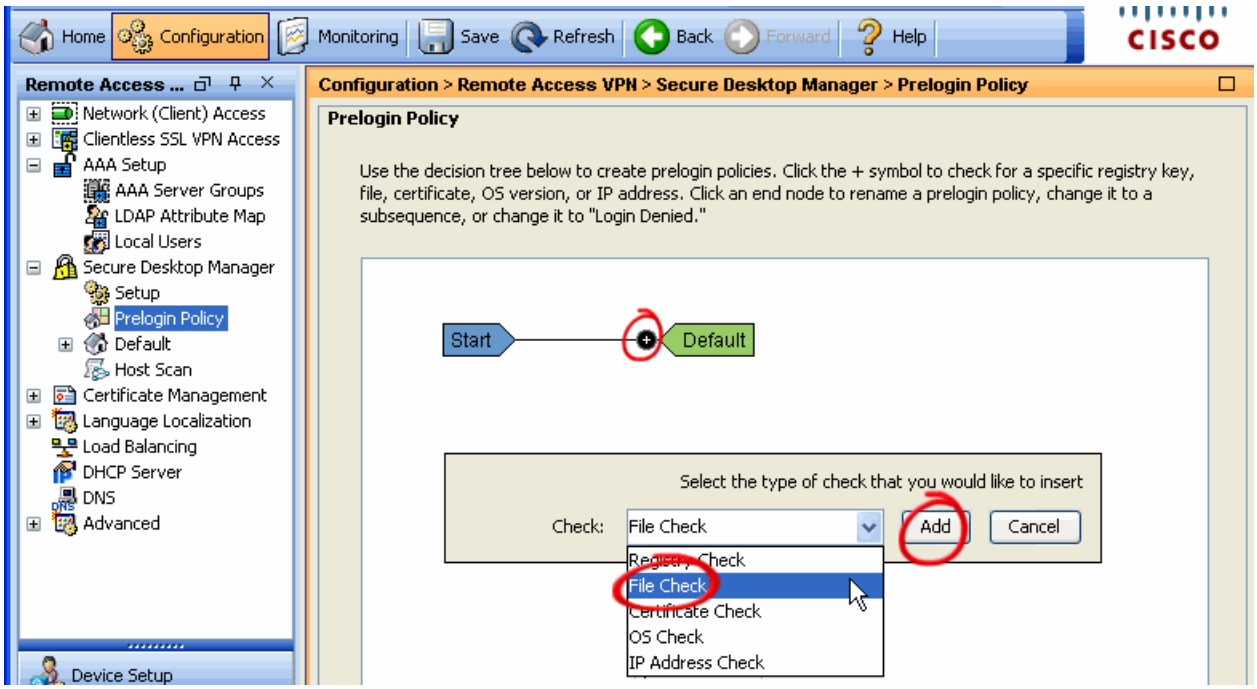
The following checks are available:

- Checking for a Registry Key
- Checking for a File
- Checking for a Certificate
- Checking for the OS Version
- Checking for an IP Address

The following example initiates a check based upon the existence of a file. The outcome of the prelogin check determines if the connection loads Secure Vault (non-corporate asset) or runs only Host Scan (corporate asset).

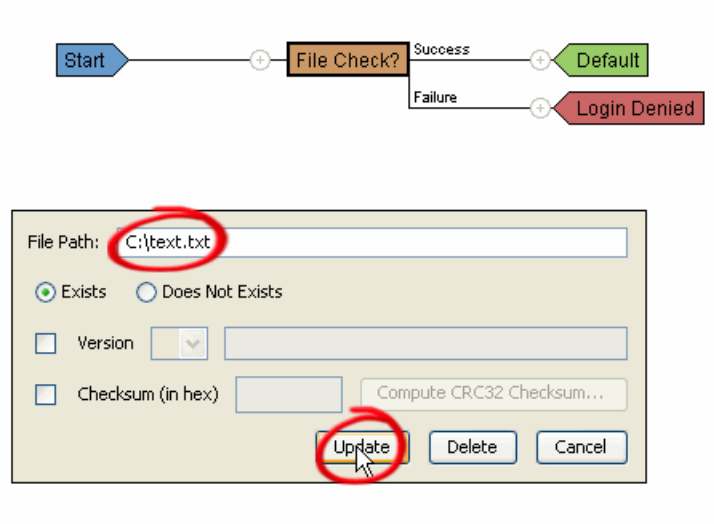
Note In the C:\ directory of the PC, create a file, `test.txt`.

Step 1 To view the prelogin assessments present in the configuration, choose **Secure Desktop Manager > Prelogin Policy**.



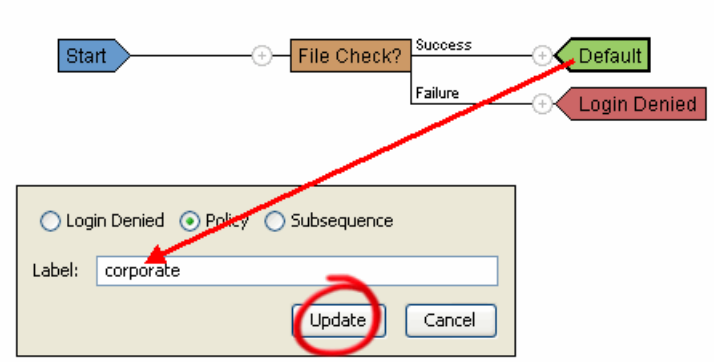
Step 2 Click the "+" icon.

Step 3 In the Check drop down menu select **File Check** and click **Add**.



Step 4 In the File Path field enter **C:\test.txt** and click **Update**.

Step 5 Rename the Default location to "corporate" by clicking on the Default icon and entering **corporate** in the Label text box. This prelogin policy is to identify corporate assets.

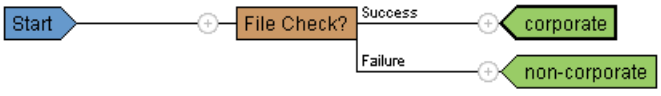


Step 6 Click **Update**.

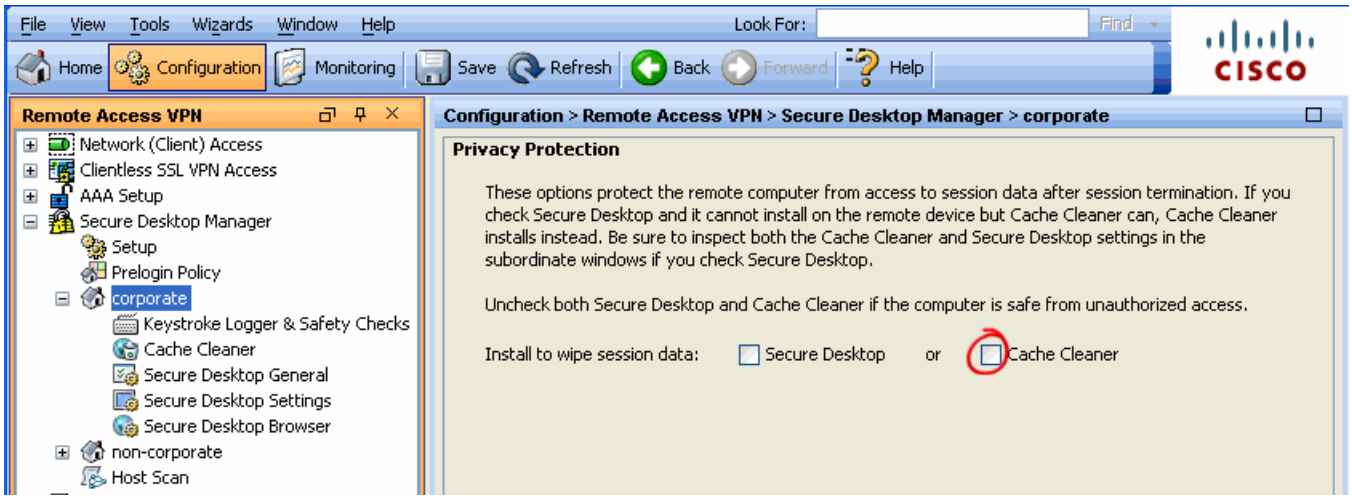
Step 7 Click **Login denied** to open a dialog box for that end node.

Step 8 Click **Policy** and enter **non-corporate** in the Label text box.

Step 9 Click **Update**.



In the left menu under Prelogin Policy, click the **corporate** icon.



Step 10 Uncheck Cache Cleaner and confirm that Secure Desktop is also unchecked. Doing so runs only Host Scan on corporate assets.

Step 11 Click the **non-corporate** icon and check **Secure Desktop** to run Secure Desktop on non-corporate assets.

Step 12 Click **Apply All**.

Step 13 Create a test.txt file on the **C:** drive on a PC and test the prelogin policy for corporate computers.

Only Host Scan runs on the PC when you connect.

Step 14 Delete the test.txt file, then try again, this time to test the prelogin policy for non-corporate computers.

Secure Desktop runs on the PC when you connect.

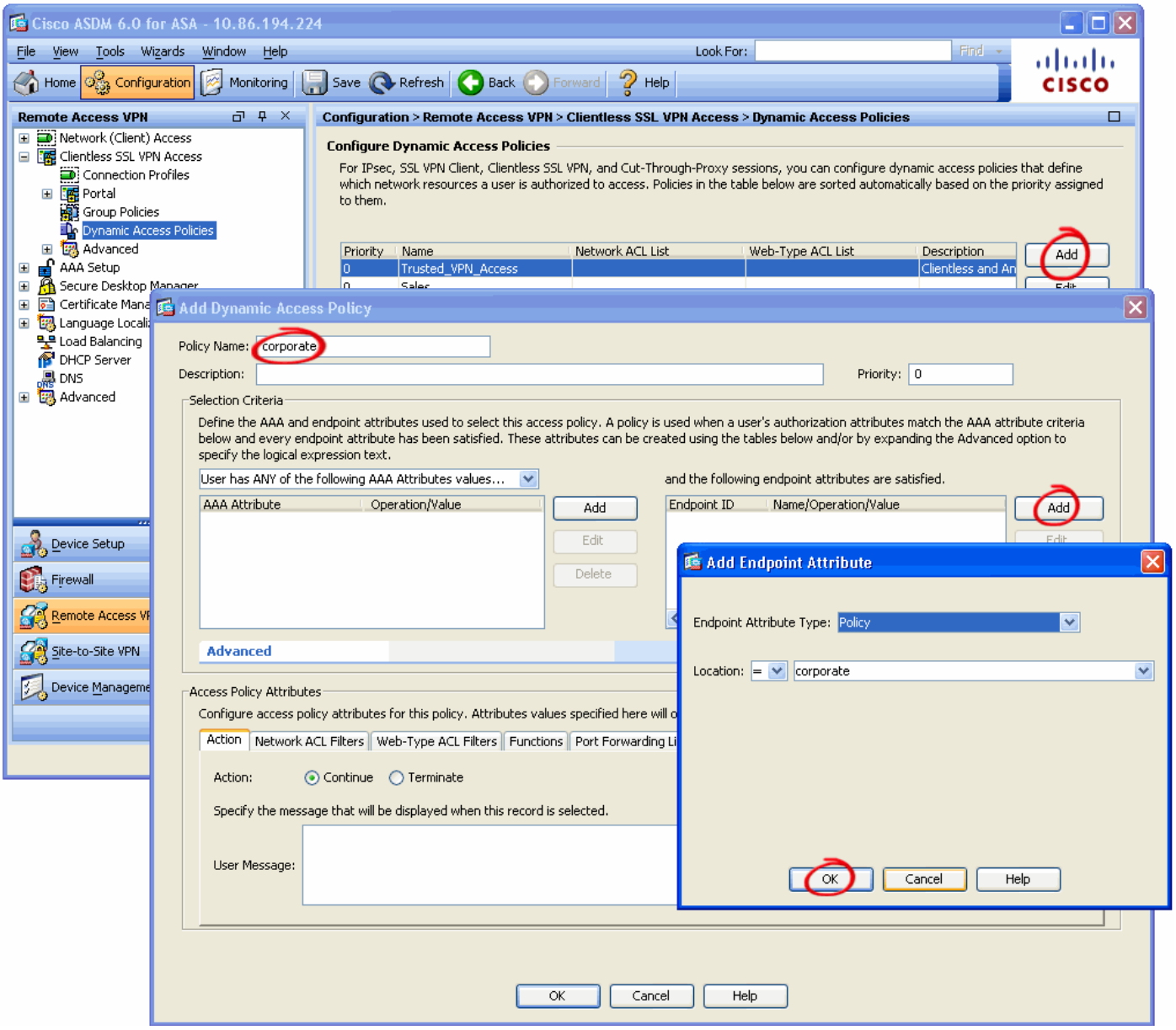
Configuring DAPs for AnyConnect and Clientless SSL VPN Access

You can configure one DAP to support AnyConnect access for corporate computers, and another DAP to support only clientless SSL VPN access for non-corporate computers.

This section assumes you have already used Cisco Secure Desktop to create different prelogin policies for corporate and non-corporate computers, as described in the previous section. To configure the DAPs for corporate and non-corporate computers, perform the following steps:

Note Install AnyConnect before beginning these instructions.

Step 1 Choose **Configuration > Remote Access VPN > Clientless SSL VPN Access > Dynamic Access Policies**.



Step 2 Click **Add**.

Step 3 Enter **corporate** next into the Policy Name text box.

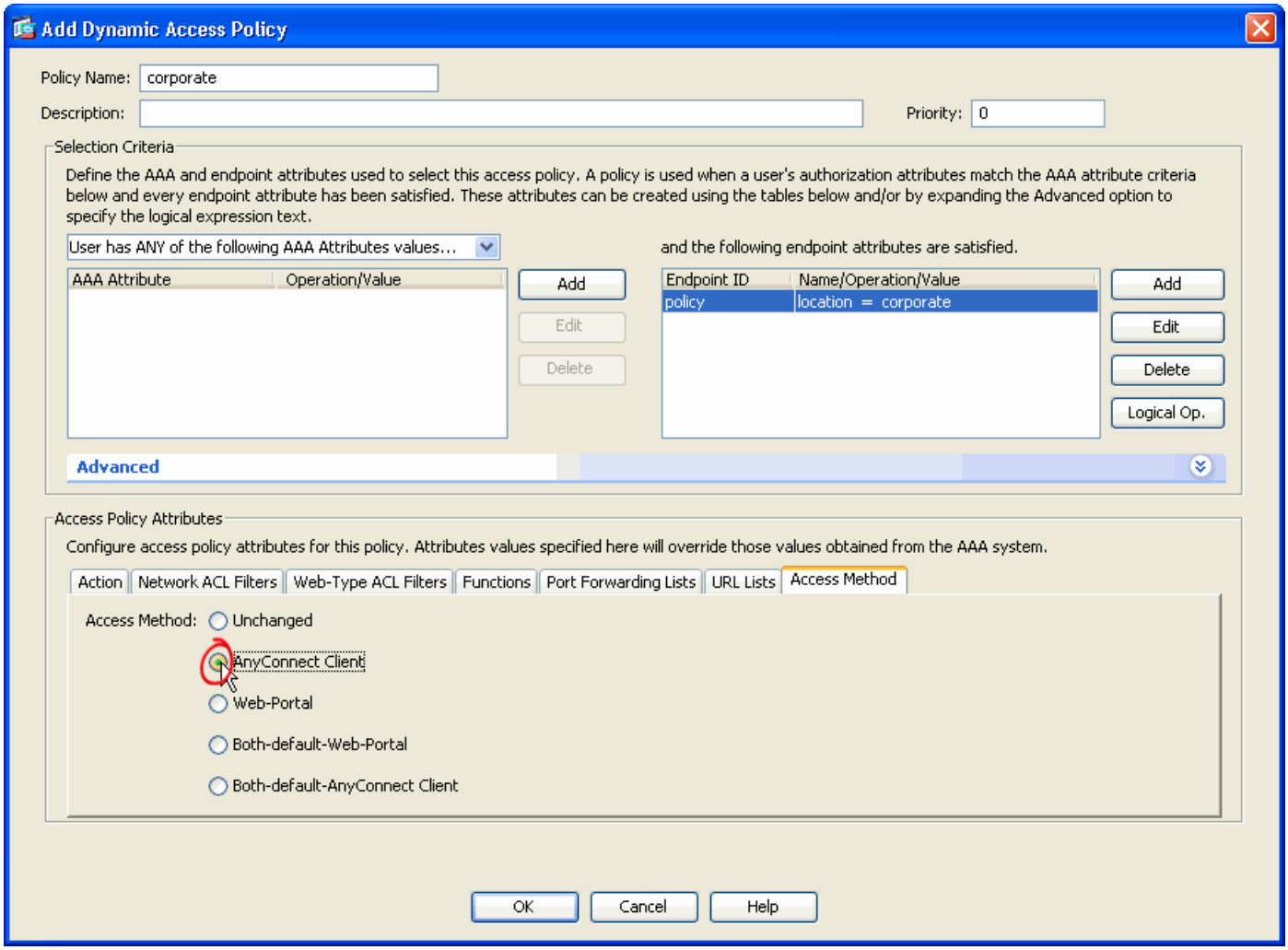
Step 4 In the endpoint attributes section on the right side of the window, click **Add**.

Step 5 In the drop down menu for Endpoint Attribute Type, select **Policy**.

Step 6 Be sure the Location is equal to the corporate location previously created in Cisco Secure Desktop.

Step 7 Click **OK**.

Step 8 In the Access Methods tab of the Access Policy Attributes section in the Edit Dynamic Access Policy pane, click **AnyConnect Client**.



Step 9 Click **OK**.

Step 10 Repeat these steps to create another DAP for non-corporate computers.

Note Set the Location attribute in the Add Endpoint Attribute window to **non-corporate**.

Step 11 Set the Access Method to **Web-Portal**.

Step 12 Click **OK**, then click **Apply** to save the changes to the running configuration.

Step 13 Create a test.txt file on the **C:** drive on a PC and test the DAP for corporate computers. Start AnyConnect or establish a clientless SSL VPN session, click the **AnyConnect** menu option, then click **Start AnyConnect**.

Step 14 Delete the test.txt file, then try again, this time to test the DAP for non-corporate computers.

Even though the connection profile is set to allow all VPN tunneling protocols (AnyConnect and clientless SSL), DAP values prevail. Non-corporate assets have only clientless access while Corporate assets have AnyConnect (full tunneling) access.

Remediation via Advanced Endpoint Assessment

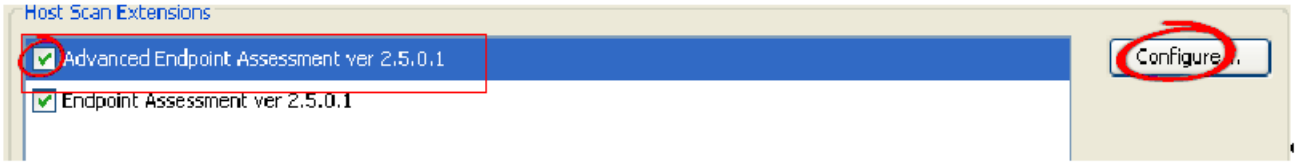
Advanced Endpoint Assessment attempts automatic remediation of specific antivirus, antispyware, and firewall applications, based on selection criteria. The remediation process supported by Advanced Endpoint Assessment is independent and in addition to the basic host scan and endpoint assessment Cisco Secure Desktop performs. Therefore, use DAPs to ensure posture enforcement in case a remediation fails or a user cancels the remediation.

Advanced Endpoint Assessment provides the following features for antivirus, antispyware, and firewalls:

- Turns on active scans if that function is not enabled.
- Verifies the active scan function is running, and if it is not, turns it on.
- Forces the antivirus, antispyware, and firewall applications to auto update the .dat file if it has not been updated in the time period you specify.
- Pushes firewall rules.

To configure automatic remediation for antivirus, antispyware and firewall software programs, remediation, perform the following steps.

Step 1 Choose **Cisco Desktop Manager > Host Scan** and check **Advanced Endpoint Assessment**.

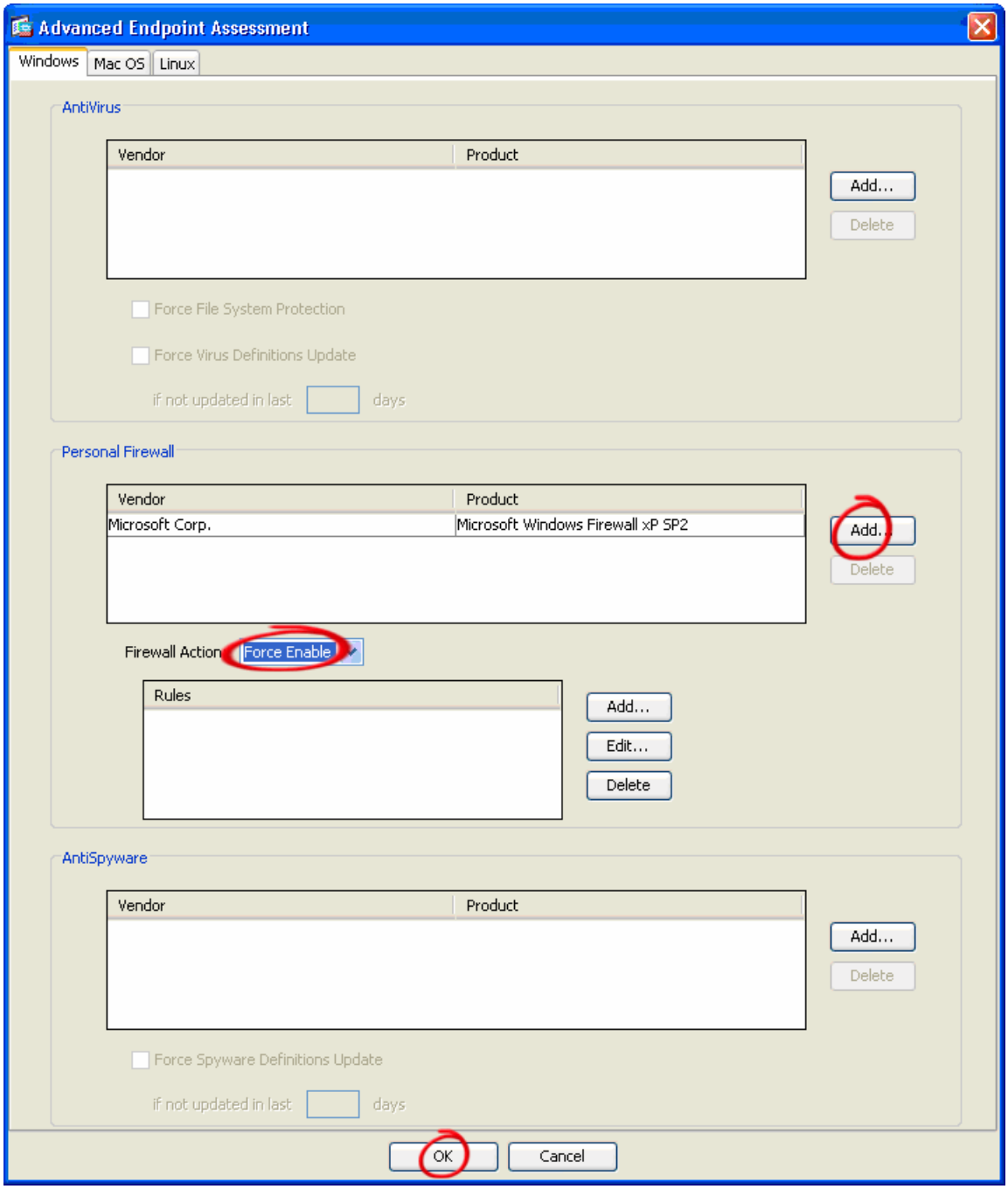


Step 2 Check **Advanced Endpoint Assessment**.

Note The **Configure** button activates only if the configuration includes a key for an Advanced Endpoint Assessment license. To enter a key after acquiring it from Cisco, choose **Device Management > System Image/Configuration > Activation Key**, enter the key in the New Activation Key field, and click **Update Activation Key**.

When you check **Advanced Endpoint Assessment**, Secure Desktop Manager inserts a check mark next to both options.

Step 3 Click **Configure**.



Step 4 In the Personal Firewall section, click **Add** and select **Microsoft Windows Firewall XP SP2**.

Step 5 In the Firewall Action drop-down drop-down list, select **Force Enable**.

Step 6 Click **OK**, then click **Apply** to save the changes to the running configuration.

Step 7 On the PC you are using for testing, disable the Microsoft Firewall.

The Windows XP Firewall is disabled by default. To check or change its status, choose **Start > Control Panel > Network Connections > Local Area Connection**, click **Properties**, click the **Advanced** tab, and click **Settings** in the Windows Firewall area.

Step 8 Establish a VPN connection with the security appliance.

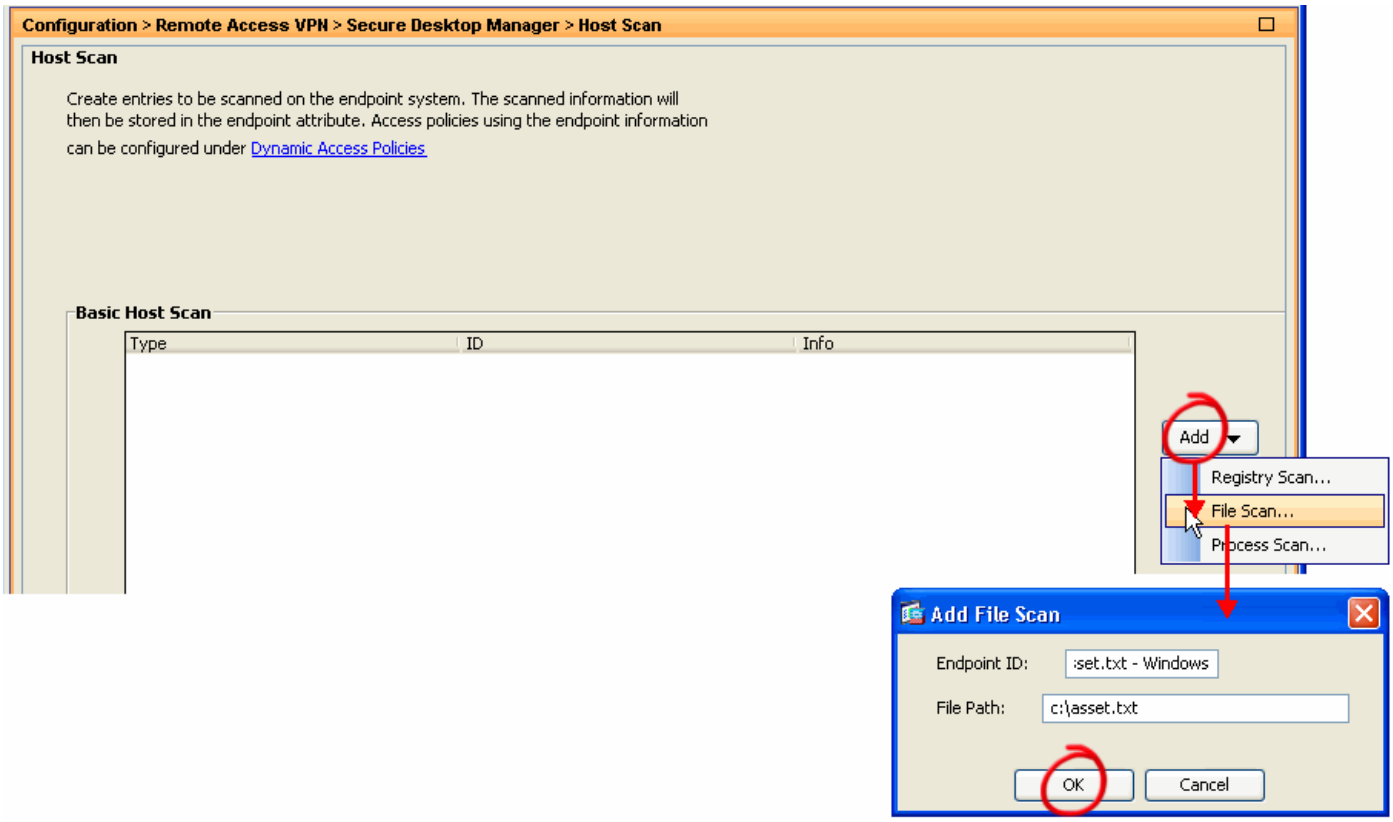
Cisco Secure Desktop automatically enables the Microsoft Firewall, despite the fact that it was disabled.

Using a DAP to Enforce Access Based on Attributes Returned from Host Scan

This section shows how to use Host Scan to scan both Windows and Mac computers for a file named *asset.txt*, and how to configure a DAP to grant access to the corporate network for computers that satisfy this criterion.

To configure the Host Scan check and create the associated DAP, perform the following steps.

Step 1 Choose **Configuration > Remote Access VPN > Secure Desktop Manager > Host Scan**.



The next steps describe how to configure different checks for Windows and Macs. The path structure is different, so you must create two unique entries.

Step 2 Click **Add** and select **File Scan** from the drop-down list, then enter the following values to specify the path of the asset.txt file on computers running Microsoft Windows:

- Endpoint ID—Enter **asset.txt - Windows**.
- File Path—Enter c:\asset.txt

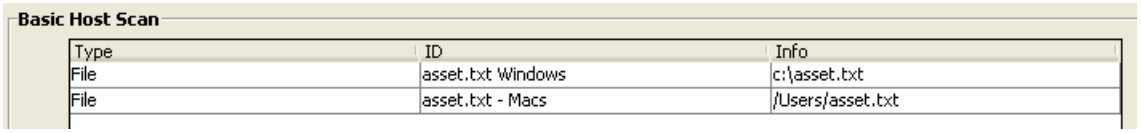
The value of the Endpoint ID attribute serves only as a unique index to the Basic Host Scan entry.

Step 3 Click **OK**.

Step 4 Click **Add** and select **File Scan** again, then enter the following values to specify the path of the asset.txt file on Macs:

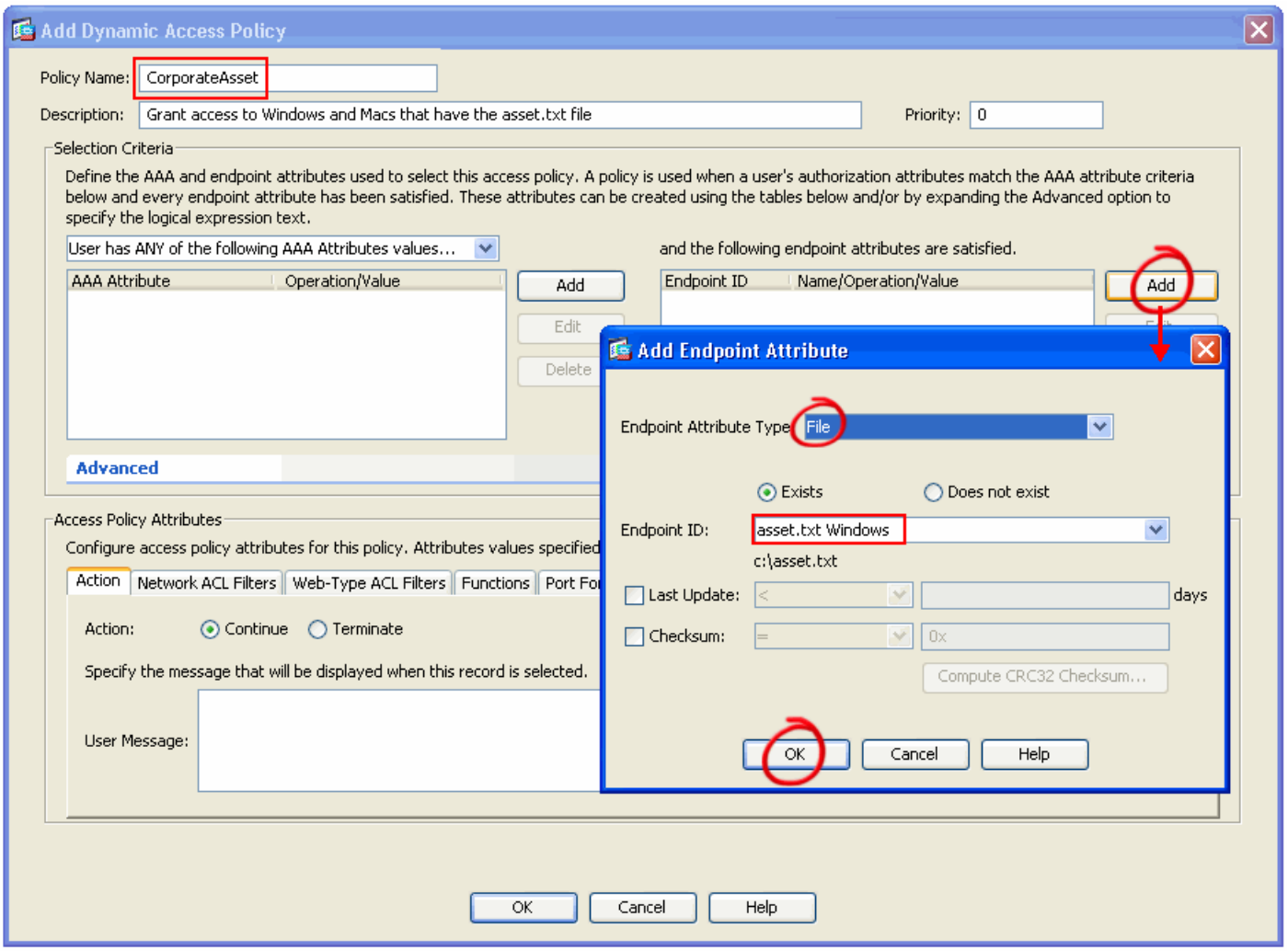
- Endpoint ID—Enter **asset.txt - Macs**.
- File Path—Enter **/Users/asset.txt**

Step 5 Click **OK**.



Step 6 Click **Apply All** to save the changes to the running configuration.

Step 7 Choose **Configuration > Remote Access VPN > Clientless SSL VPN Access > Dynamic Access Policies** and click **Add**.



Step 8 Enter a string into the **Policy Name** text box to serve as an index to this DAP.

Note ASDM does not accept the DAP if the policy name contains a space.

Step 9 Click **Add** on the right side of the window.

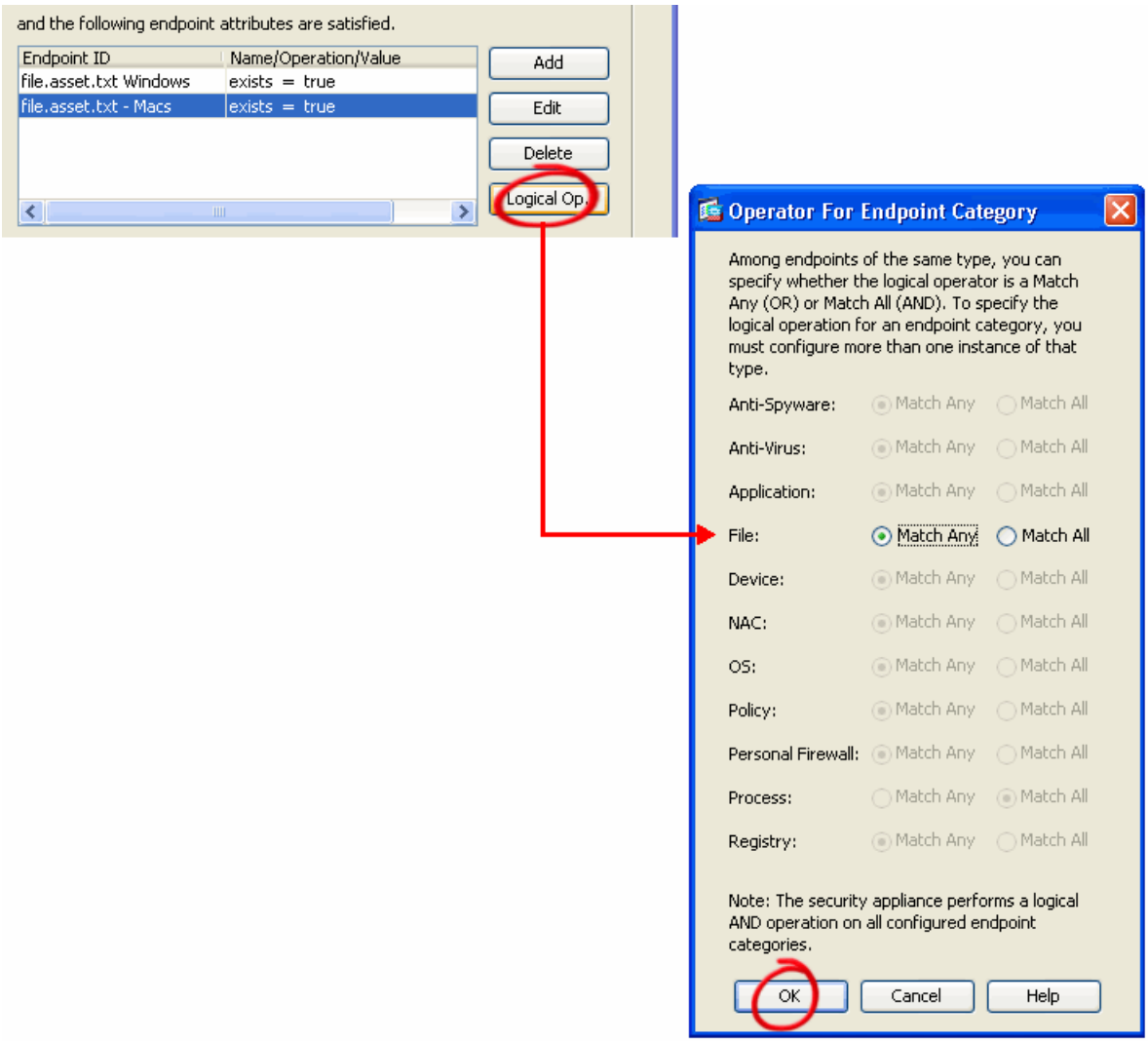
Step 10 In the Endpoint attribute pane, select **File** next to Endpoint Attribute Type.

Step 11 Select **asset.txt Windows** next to Endpoint ID.

Step 12 Click **OK**.

Step 13 Add another endpoint attribute of type **File**, but this time select **asset.txt - Macs** next to Endpoint ID.

ASDM displays the Windows and Macs entries in the endpoint attributes table.

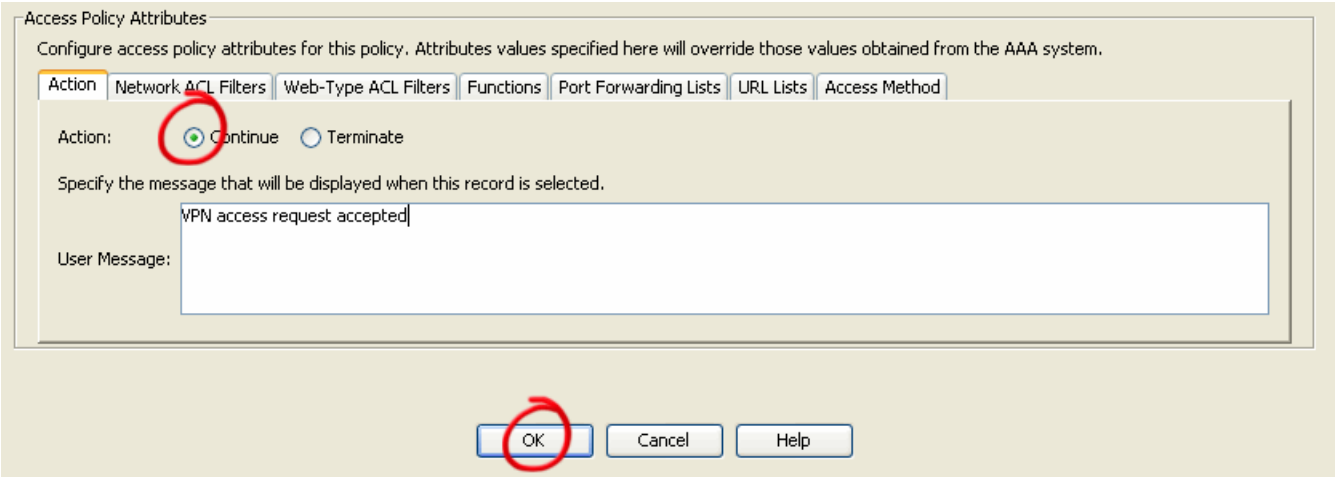


Step 14 Click **Logical Op**.

Step 15 Check **Match Any** next to File to indicate that either endpoint attribute satisfies the criterion for assigning the DAP.

Step 16 Click **OK**.

Step 17 In the Access Policy Attributes area, set the Action of the new DAP to **Continue**.



Step 18 (Optional)—Enter a message to display to users for whom this DAP applies into the User Message text box.

Step 19 Click **OK**.

Step 20 Be sure that the Action for the Default DAP policy is set to **Terminate**.

Step 21 Click **Apply** to save the changes to the running configuration.

To test the file scan and DAP configuration, perform the following steps:

Step 1 Add a c:\asset.txt file to a PC running Microsoft Windows and establish a VPN connection.

The security appliance grants access.

Step 2 Disconnect. Remove the c:\asset.txt file and try again.

The security appliance denies access.

Step 3 Add a /Users/asset.txt file to a Mac and establish a VPN connection.

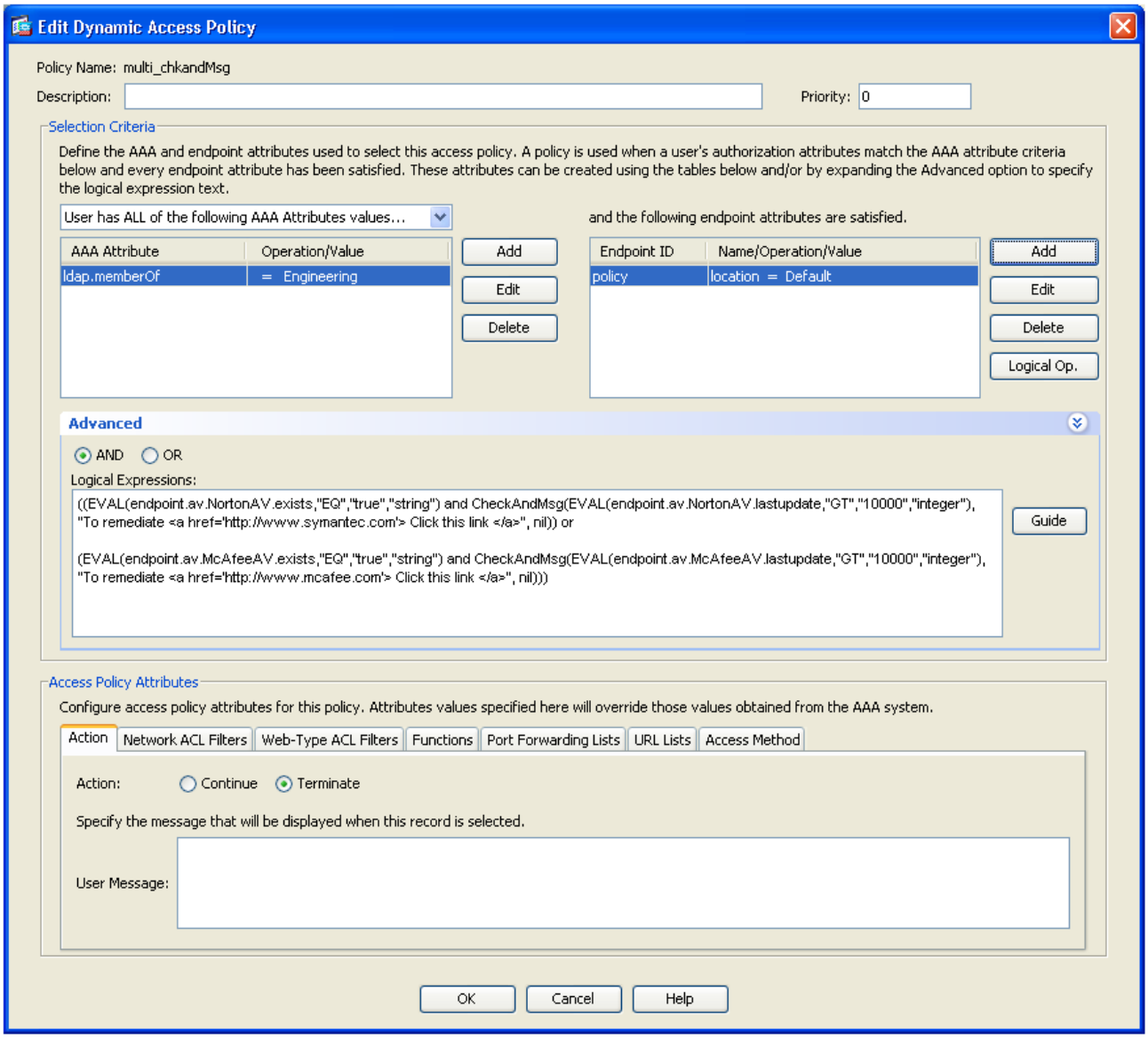
The security appliance grants access.

Step 4 Disconnect. Remove the /Users/asset.txt file and try again.

The security appliance denies access.

Advanced DAP Settings

The Advanced section of the Add or Edit Dynamic Access Policy window supports logical expressions for AAA or endpoint attributes. These expressions are based on the Lua programming language. For more information about the expression syntax, contact Cisco Engineering or TAC. You can also learn more about Lua at www.lua.org.



In the Advanced text box you enter free-form Lua text that represents AAA and/or endpoint selection logical operations. ASDM does not validate text that you enter here; it just copies this text to the DAP file, and the security appliance processes it, discarding any expressions it cannot parse.

This option is useful for adding selection criteria other than what is possible in the AAA and endpoint attribute areas. For example, while you can configure the ASA to use AAA attributes that satisfy any, all, or none of the specified criteria, endpoint attributes are cumulative; all must be satisfied. To let the security appliance use one endpoint attribute or another, you need to create appropriate logical expressions in Lua and enter them here.

In the screen above, the Logical Expressions field contains an expression that checks for the presence of antivirus software (Norton & McAfee), and if the definitions are greater than 1.5 days (10,000 sec), the session is terminates with a message and link for remediation.

AnyConnect VPN Client

The Cisco AnyConnect VPN client is an SSL VPN client that connects a remote user's PC and provides a secure connection to a security appliance running version 8.0 or higher and ASDM 6.0 or higher. It does not connect with a PIX device nor with a VPN 3000 Series Concentrator. The AnyConnect client supports Windows Vista, Windows XP, and Windows 2000; Mac OSX (Version 10.4 or later) on either Intel or PowerPC platforms; and Red Hat Linux (Version 9 or later). See the Release Notes for the AnyConnect client for the full set of platform requirements and supported versions.

Installing and Configuring the AnyConnect Client

The AnyConnect client software is supported by ASA Release 8.0(1) and later and ASDM Release 6.0 and later.

You can configure the security appliance to download and install the client to remote PCs through Web deployment. Alternatively, you can install the client using corporate IT software deployment systems, such as Altiris, or you can manually install the client on individual PCs. This section provides instructions for Web deployment. For more information on IT deployment or manual installation, see the *AnyConnect SSL VPN Client Administrators Guide*.

How Web Deployment Works

Without a previously-installed client, remote users enter into their browser the IP address or DNS name of an interface configured to accept clientless SSL VPN connections. Unless the security appliance is configured to redirect http:// requests to https://, users must enter the URL in the form https://<*address*>.

After the user enters the URL, the browser connects to that interface and displays the login screen. If the user satisfies the login and authentication, and the security appliance identifies the user as requiring the client, it loads the client that matches the operating system of the remote computer. After loading, the client installs and configures itself, establishes a secure SSL connection and either remains or uninstalls itself (depending on the security appliance configuration) when the connection terminates.

In the case of a previously-installed client, when the user authenticates, the security appliance examines the revision of the client, and upgrades the client as necessary.

When the client negotiates an SSL VPN connection with the security appliance, it connects using Transport Layer Security (TLS). The client can also negotiate a simultaneous Datagram Transport Layer Security (DTLS) connection. DTLS avoids latency and bandwidth problems associated with some SSL connections and improves the performance of real-time applications that are sensitive to packet delays.

Before You Install the AnyConnect Client

The following sections contain recommendations to ensure successful AnyConnect client installation:

- Ensuring Automatic Installation of AnyConnect Clients, page 78
- Adding a Security Appliance to the List of Trusted Sites (IE), page 78

Ensuring Automatic Installation of AnyConnect Clients

The following recommendations and caveats apply to the automatic installation of AnyConnect client software on client PCs:

- To minimize user prompts during AnyConnect client setup, make sure certificate data on client PCs and on the security appliance match:
  - If you are using a Certificate Authority (CA) for certificates on the security appliance, choose one that is already configured as a trusted CA on client machines.
  - If you are using a self-signed certificate on the security appliance, be sure to install it as a trusted root certificate on clients.

    The procedure varies by browser. See the procedures that follow this section.
  - Make sure the Common Name (CN) in security appliance certificates matches the name clients use to connect to it. By default, the security appliance certificate CN field is its IP address. If clients use a DNS name, change the CN field on the security appliance certificate to that name.
- The Cisco Security Agent (CSA) might display warnings during the AnyConnect client installation.

Current shipping versions of CSA do not have a built-in rule that is compatible with the AnyConnect client. You can create the following rule using CSA version 5.0 or later by following these steps:

Step 1 In Rule Module: "Cisco Secure Tunneling Client Module", add a FACL:

```
Priority Allow, no Log, Description: "Cisco Secure Tunneling Browsers, read/write
vpnweb.ocx"
Applications in the following class: "Cisco Secure Tunneling Client - Controlled Web
Browsers"
Attempt: Read file, Write File
```

On any of these files: @SYSTEM\vpnweb.ocx

Step 2 Application Class: "Cisco Secure Tunneling Client - Installation Applications" add the following process names:

```
**\vpndownloader.exe
@program_files\**\Cisco\Cisco AnyConnect VPN Client\vpndownloader.exe
```

This rule will be built into a future version of CSA.

We recommend that Microsoft Internet Explorer (MSIE) users add the security appliance to the list of trusted sites, or install Java. Doing so enables the ActiveX control to install with minimal interaction from the user. This is particularly important for users of Windows XP SP2 with enhanced security. Windows Vista users *must* add the security appliance to the list of trusted sites in order to use the dynamic deployment feature. For information about adding a security appliance to the list of trusted sites, see the *Cisco AnyConnect VPN Client Administrator Guide*. For information about how to use Microsoft Active Directory to add the security appliance to the list of trusted sites for Internet Explorer, see Appendix B of *Cisco AnyConnect VPN Client Administrator Guide*.

Adding a Security Appliance to the List of Trusted Sites (IE)

To add a security appliance to the list of trusted sites, use Microsoft Internet Explorer and do the following steps.

Note This is required on Windows Vista to use WebLaunch.

Step 1 Go to Tools | Internet Options | Trusted Sites.

The Internet Options window opens.

Step 2 Click the Security tab.

Step 3 Click the Trusted Sites icon.

Step 4 Click Sites.

The Trusted Sites window opens.

Step 5 Type the host name or IP address of the security appliance. Use a wildcard such as https://*.yourcompany.com to allow all ASA 5500s within the yourcompany.com domain to be used to support multiple sites.

Step 6 Click Add.

Step 7 Click OK.

The Trusted Sites window closes.

Step 8 Click OK in the Internet Options window.

Installing Start Before Logon Components (Windows Only)

The Start Before Logon components must be installed *after* the core client has been installed. Additionally, the AnyConnect 2.2 Start Before Logon components require that version 2.2, or later, of the core AnyConnect client software be installed. If you are pre-deploying the AnyConnect client and the Start Before Logon components using the MSI files (for example, you are at a big company that has its own software deployment—Altiris or Active Directory or SMS.) then you must get the order right. The order of the installation is handled automatically when the administrator loads AnyConnect if it is web deployed and/or web updated.

Both the AnyConnect client and the Start Before Login components must be installed the same way, either both manually or both via WebLaunch. Therefore:

- If you pre-deploy AnyConnect, you must also pre-deploy the Start Before Logon components.
- If you web-update AnyConnect, you must web-update the Start Before Logon components.
- If you web-deploy AnyConnect, you must web-deploy the Start Before Logon components.
- You cannot pre-deploy AnyConnect, and then web-deploy the Start Before Logon components.

If you manually uninstall GINA or PLAP, you must manually reinstall it.

You can, for example, pre-deploy both of them... put a new version of both on the head end and web-update them both. The two are joined together in whatever action you perform.

For example, a customer sends out laptops with the software pre-installed. Six months later, Cisco ships a new version of the software and the network administrators want all their users to get the latest version. To do this, the network administrators can put the new software on the security appliance, and all users get the web update.

They could *not* pre-image with just core AnyConnect software and then decide to update via the security appliance both the client and the Start Before Logon software components, since they never pre-installed the Start Before Logon software to begin with.

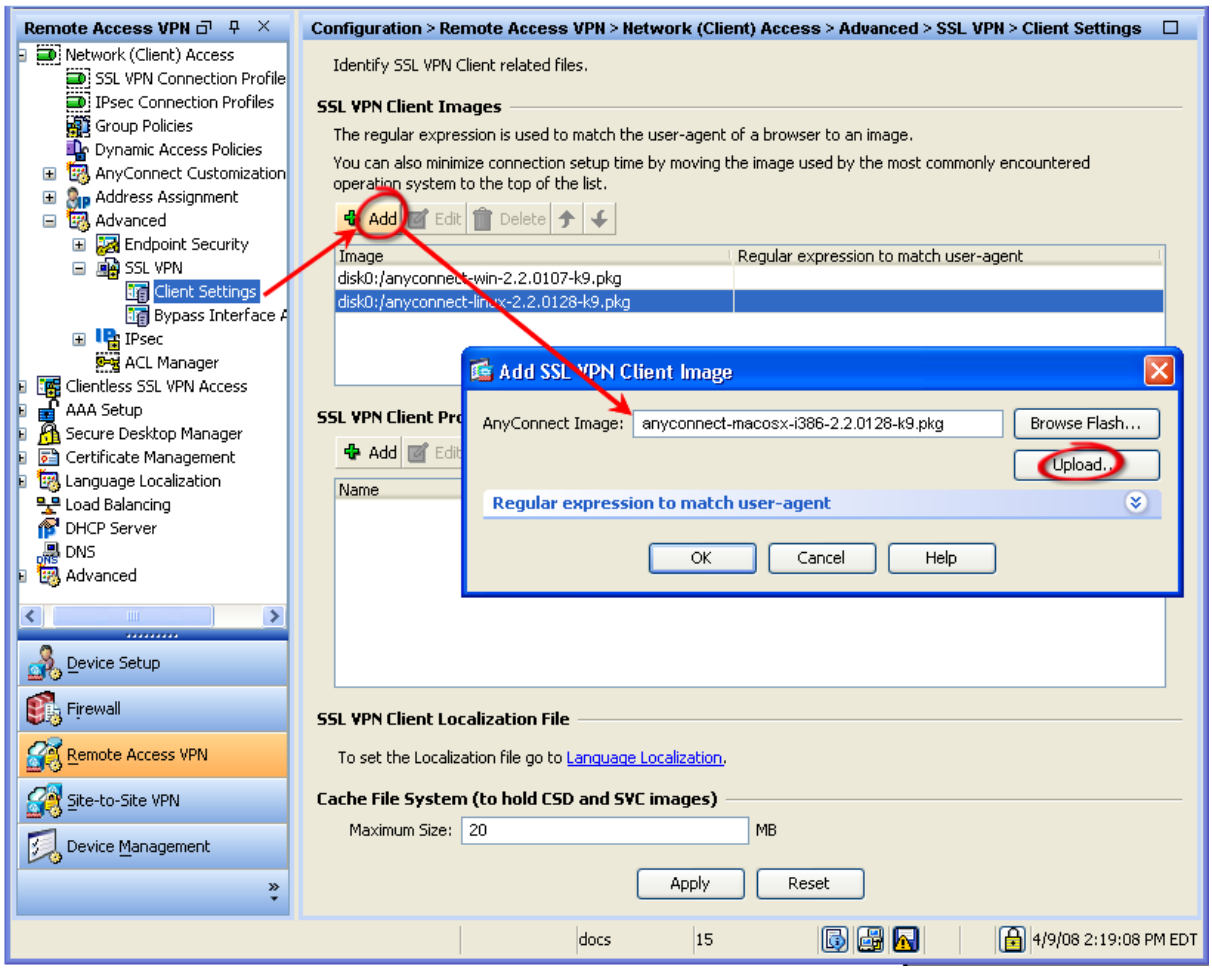
Installing the AnyConnect Client and Configuring the Security Appliance

Installing the client on the security appliance consists of copying a client image to the security appliance and identifying the file to the security appliance as a client image. With multiple clients, you must also assign the order in which the security appliance loads the clients to the remote PC.

Note All of the AnyConnect clients are located in the same place: http://www.cisco.com/cgi-bin/tablebuild.pl/anyconnect

Perform the following steps to install the client on the security appliance:

Step 1 Load the AnyConnect client images to the security appliance. In ASDM, navigate to **Configuration > Remote Access VPN > Network (Client) Access > Advanced > SSL VPN > Client Settings**. The SSL VPN Client Settings panel displays, as shown in the following figure.



This panel lists any AnyConnect client files that have been identified as AnyConnect client images. The order in which they appear in the table reflects the order in which they download to the remote computer. To add an AnyConnect client image, Click **Add** in the SSL VPN Client Images area. The Add SSL VPN Client Image dialog appears.

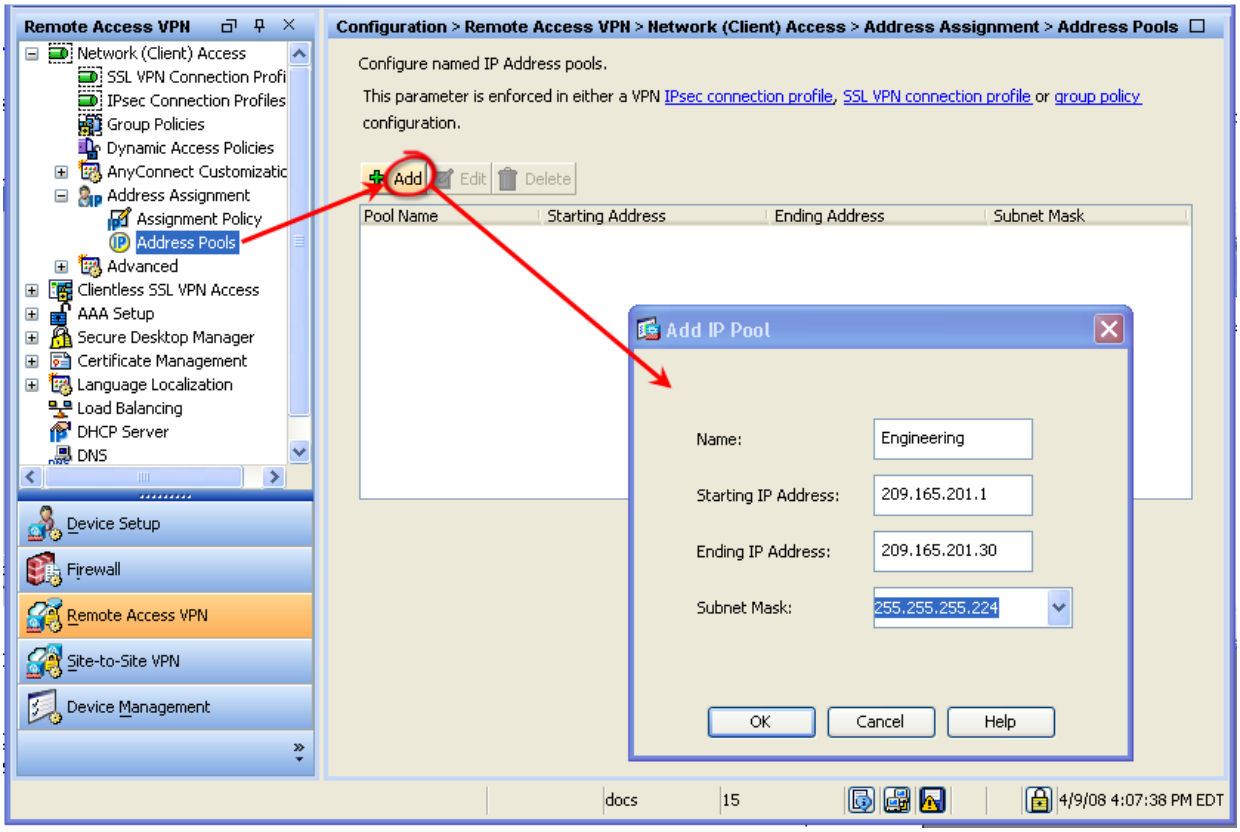
If you already have an image located in the flash memory of the security appliance, you can enter the name of the image in the Flash SVC Image field, and click **OK**. The SSL VPN Client Settings panel now shows the AnyConnect client images you identified.

Note The security appliance downloads portions of each client in the order you specify until it matches the operating system of the remote PC. Therefore, assign the topmost position to the image used by the most commonly-encountered operating system.

Step 2 Click on an image name, and use the **Move Up** or **Move Down** button to change the position of the image within the list. This establishes the order in which the security appliance loads them to the remote computer. The security appliance loads the AnyConnect client image at the top of the list of images first. Therefore, you should move the image used by the most commonly-encountered operating system to the top of the list.

Step 3 Configure a method of address assignment. You can use DHCP, and/or user-assigned addressing. You can also create a local IP address pool and assign the pool to a tunnel group.

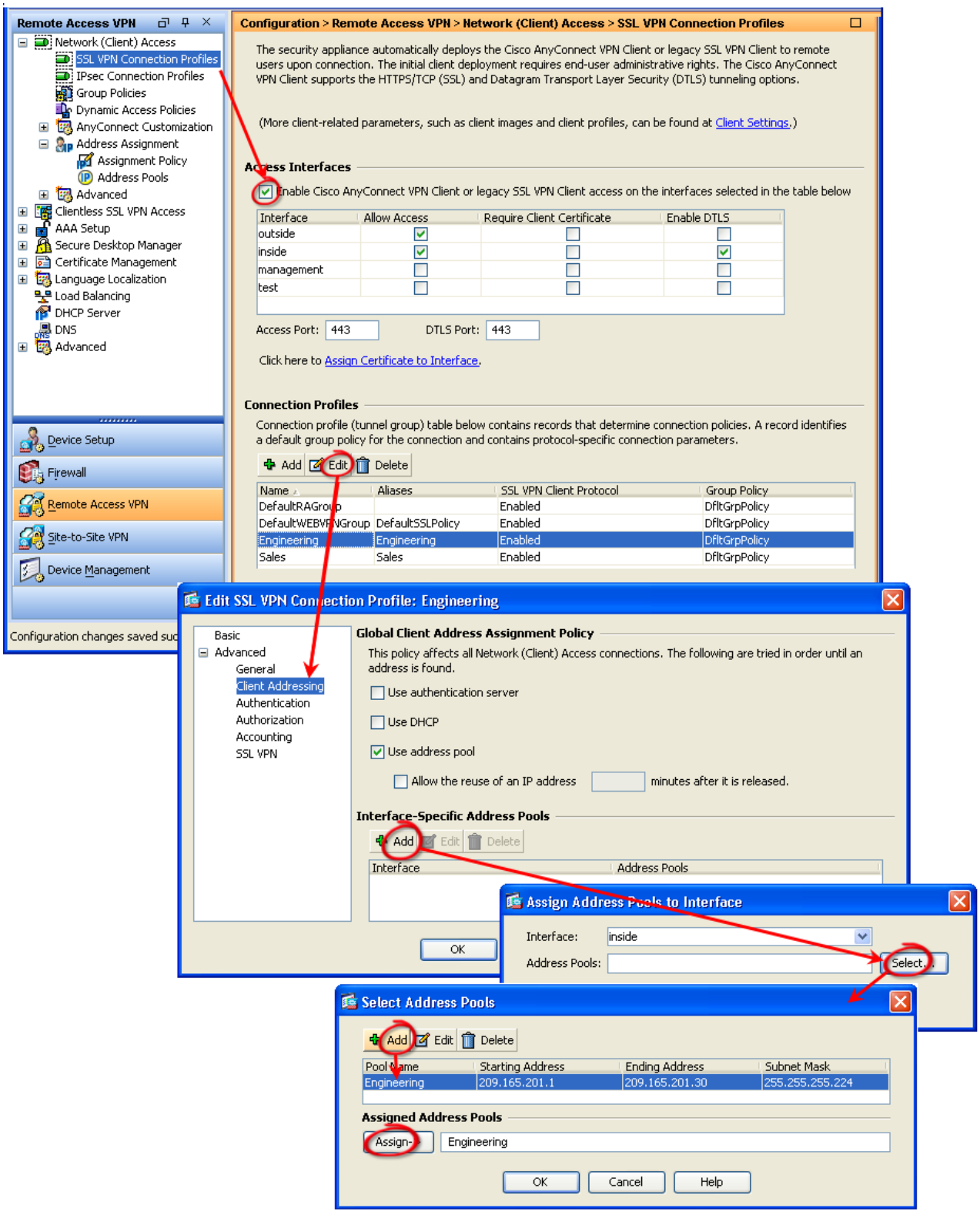
To create an IP address pool, choose **Network (Client) Access > Address Management > Address Pools**. Click **Add**. The Add IP Pool dialog appears:



Enter the name of the new IP address pool. Enter the starting and ending IP addresses, and enter the subnet mask and click **OK**.

Step 4 Enable the security appliance to download the AnyConnect client to remote users and assign the IP address pool. Go to **Network (Client) Access > Connection Profiles**:

Step 5 Select the Engineering group policy and click **Edit**. The Edit Internal Group Policy window displays:



Step 6 Check **Enable Cisco AnyConnect VPN Client**.

Step 7 Associate the address pool to the connection profile. In the Connection Profiles area, select the Engineering connection profile and click **Edit**. The Edit SSL VPN Connection Profile: Engineering window displays.

Step 8 In the navigation pane, select **Client Addressing**. In the Interface-specific Address Pools area, click Add. The Assign Address Pools to Interface window displays.

Step 9 Click **Select**. The Select Address Pools window displays.

Step 10 Select the Engineer address pool and click **Assign**. Click **Ok** and **Apply**.

Check the **SSL VPN Client** check box to include SSL VPN as a tunneling protocol.

CSA Interoperability with the AnyConnect Client and Cisco Secure Desktop

If your remote users have Cisco Security Agent (CSA) installed, you must import new CSA policies to the remote users to enable the AnyConnect VPN Client and Cisco Secure Desktop to interoperate with the security appliance.

To do this, follow these steps:

Step 1 Retrieve the CSA policies for the AnyConnect client and Cisco Secure Desktop. You can get the files from:

- The CD shipped with the security appliance.
- The software download page for the ASA 5500 Series Adaptive Security Appliance at http://www.cisco.com/cgi-bin/tablebuild.pl/asa.

The filenames are AnyConnect-CSA.zip and CSD-for-CSA-updates.zip

Step 2 Extract the .export files from the .zip package files.

Step 3 Choose the correct version of the .export file to import. The Version 5.2 export files work for CSA Versions 5.2 and higher. The 5.x export files are for CSA Versions 5.0 and 5.1.

Step 4 Import the file using the Maintenance > Export/Import tab on the CSA Management Center.

Step 5 Attach the new rule module to your VPN policy and generate rules.

For more information, see the CSA document *Using Management Center for Cisco Security Agents 5.2*. Specific information about exporting policies is located in the section *Exporting and Importing Configurations*.

Uninstalling the Cisco AnyConnect VPN Client

To manually uninstall the AnyConnect client from a Windows system, use the standard "Add or Remove Programs" Control Panel available from the Start menu.

The procedure for manually uninstalling the AnyConnect client from a Linux or Mac OS X system is the same for both systems. As root, run the following shell script:

```
/opt/cisco/vpn/bin/vpn_uninstall.sh
```

Typically, you would do this via sudo, as follows:

```
$ sudo /opt/cisco/vpn/bin/vpn_uninstall.sh
```

If you do not use sudo, use a root shell:

```
# /opt/cisco/vpn/bin/vpn_uninstall.sh
```

Sample Security Appliance Configuration for AnyConnect Client

This section presents an example of a security appliance configuration for AnyConnect:

```
f1> enable
Password:
f1# config terminal
f1(config)# interface gigabitEthernet 0/0
f1(config-if)# ip address 192.168.0.6
f1(config-if)# nameif public
f1(config-if)# security-level 0
f1(config-if)# no shutdown
f1(config-if)# exit
f1(config)# interface gigabitEthernet 0/1
f1(config-if)# ip address 10.86.194.193 255.255.254.0
f1(config-if)# nameif inside
f1(config-if)# security-level 10
f1(config-if)# no shutdown
f1(config-if)# exit
f1(config)# domain-name frqa.cisco.com
f1(config)# dns domain-lookup inside
f1(config)# dns name-server 10.86.195.22
f1(config)# route inside 10.86.195.0 255.255.254.0 10.86.194.1 1
f1(config)# username user2 password internal
f1(config)# username user2 attributes
f1(config-username)# vpn-tunnel-protocol WebVPN
f1(config-username)# WebVPN
f1(config-username-WebVPN)# functions url-entry file-access file-entry file-browsing
f1(config-username-WebVPN)# exit
f1(config-username)# exit
f1(config)# WebVPN
f1(config-WebVPN)# enable public
f1(config-WebVPN)# enable inside
f1(config-WebVPN)# exit
f1(config)# route inside 0 0 10.86.194.1
f1(config)# http server enable
```

Example Clientless SSL VPN Configuration

```
f1> enable
Password:
f1# config terminal
f1(config)# interface gigabitEthernet 0/0
f1(config-if)# ip address 192.168.0.6
f1(config-if)# nameif public
f1(config-if)# security-level 0
f1(config-if)# no shutdown
f1(config-if)# exit
f1(config)# interface gigabitEthernet 0/1
f1(config-if)# ip address 10.86.194.193 255.255.254.0
f1(config-if)# nameif inside
f1(config-if)# security-level 10
f1(config-if)# no shutdown
f1(config-if)# exit
f1(config)# domain-name frqa.cisco.com
f1(config)# dns domain-lookup inside
f1(config)# dns name-server 10.86.195.22
f1(config)# route inside 10.86.195.0 255.255.254.0 10.86.194.1 1
f1(config)# username user2 password internal
f1(config)# username user2 attributes
f1(config-username)# vpn-tunnel-protocol WebVPN
f1(config-username)# WebVPN
f1(config-username-WebVPN)# functions url-entry file-access file-entry
file-browsing
f1(config-username-WebVPN)# exit
f1(config-username)# exit
f1(config)# WebVPN
f1(config-WebVPN)# enable public
f1(config-WebVPN)# enable inside
f1(config-WebVPN)# exit
f1(config)# route inside 0 0 10.86.194.1
f1(config)# http server enable
```