Configuring Citrix MetaFrame Services

WebVPN users can use a connection to the security appliance to access Citrix MetaFrame services. The following sections introduce this function, list the prerequisites, and describe how to use ASDM to configure the security appliance to support this function:

Note As you follow the instructions in this chapter, click **Help** for more information about the attributes shown in the ASDM windows.

Introduction

The security appliance lets Citrix Independent Computing Architecture (ICA) clients access corporate enterprise applications running on a Citrix Presentation Server over a WebVPN connection. You can redirect the WebVPN home page to the Citrix web server, add a link to the server on the WebVPN home page, or instruct users to enter the URL of the server to access Citrix MetaFrame services. When a WebVPN user connects to the Citrix web server, the Citrix Web Interface authenticates the user and lets the user access corporate resources.

Note Within this configuration, the security appliance functions as the Citrix secure gateway.

Complete the instructions in the following sections to configure security appliance support for Citrix MetaFrame services running on one or more Citrix Presentation Servers.

Before You Begin

Before following the instructions in this chapter, configure the Citrix Web Interface software to operate in a mode that does not use the Citrix secure gateway.

Note All browsers connecting to the Citrix server must support 128-bit encryption.

Adding a Trustpoint

These instructions describe how to add a trustpoint to the security appliance appliance configuration to satisfy a Citrix connection requirement.

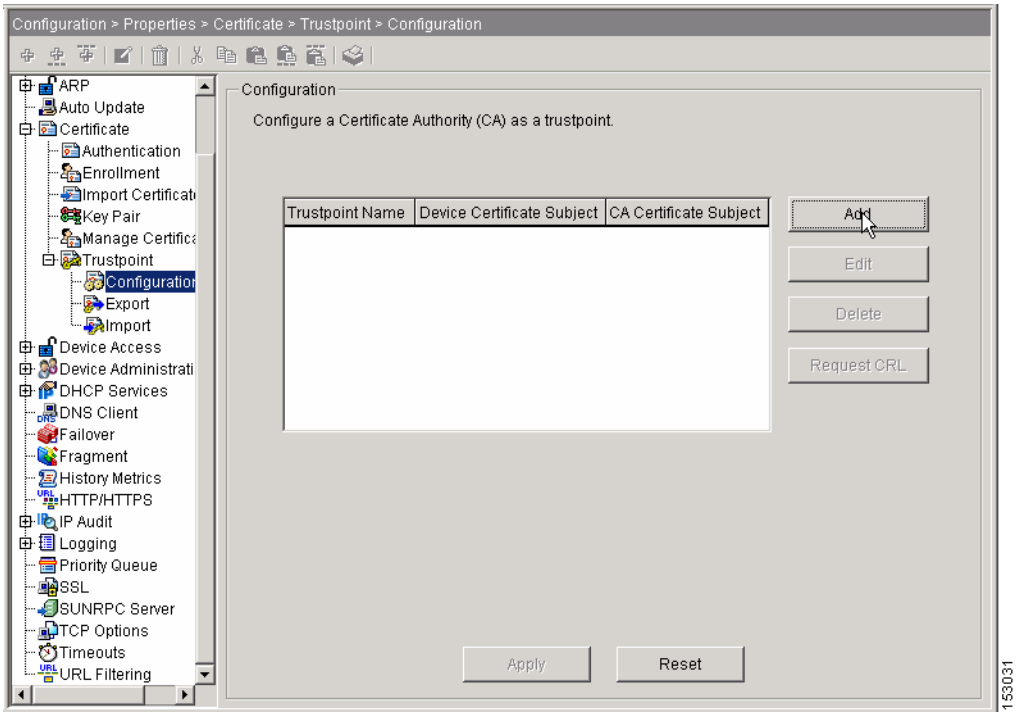
A trustpoint contains the identity of a certificate authority, CA-specific configuration parameters, and an association with one enrolled identity certificate. You need one trustpoint to connect with the Citrix server. You can configure up to two trustpoints, each to be assigned to a different interface on the security appliance; however, you can assign a single trustpoint to two interfaces.

Add a trustpoint to the security appliance configuration as follows:

Step 1 Choose Configuration > Properties > Certificate > Trustpoint > Configuration.

The Trustpoint Configuration window opens (Figure 2-1).

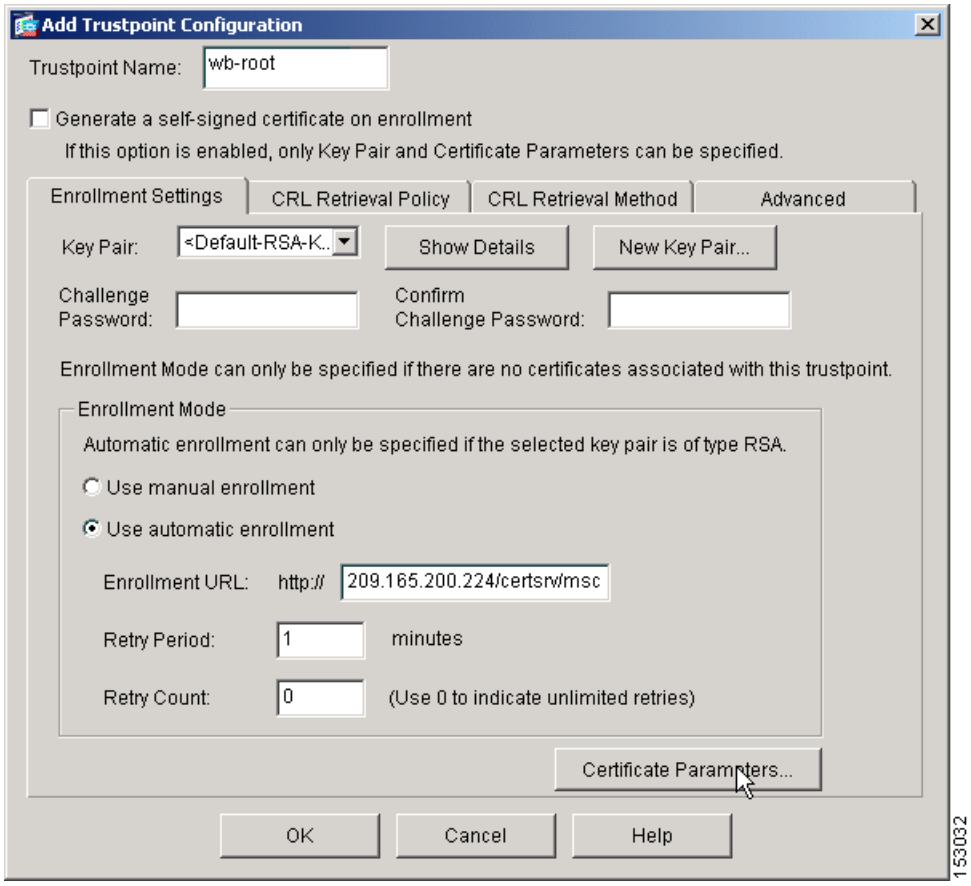
Figure 2-1 Trustpoint Configuration



Step 2 Click **Add**.

The Add Trustpoint Configuration window opens (Figure 2-2).

Figure 2-2 Add Trustpoint Configuration



Step 3 Enter a value, such as the name of the certificate, in the **Trustpoint Name** field to uniquely identify this trustpoint and provide a visual association to the certificate.

Step 4 Click either of the following attributes:

- **Use manual enrollment**

  This option specifies the intention to generate a PKCS10 certification request. The CA issues a certificate to the security appliance based on the request, and the certificate is installed on the security appliance by importing the new certificate.

- **Use automatic enrollment**

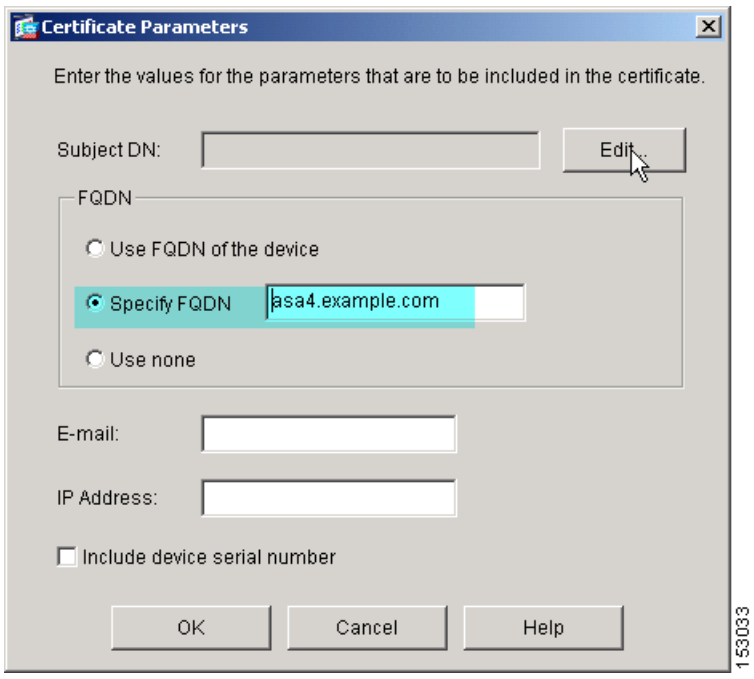
  If you choose this option, Enter the URL for automatic enrollment in the **Enrollment URL** field.

  The automatic enrollment option specifies the intention to use SCEP mode. When the trustpoint is configured for SCEP enrollment, the security appliance downloads the certificate using the SCEP protocol.

Step 5 Click **Certificate Parameters**.

The Certificate Parameters window opens (Figure 2-3).

Figure 2-3 Certificate Parameters



Step 6 Click **Specify FQDN**.

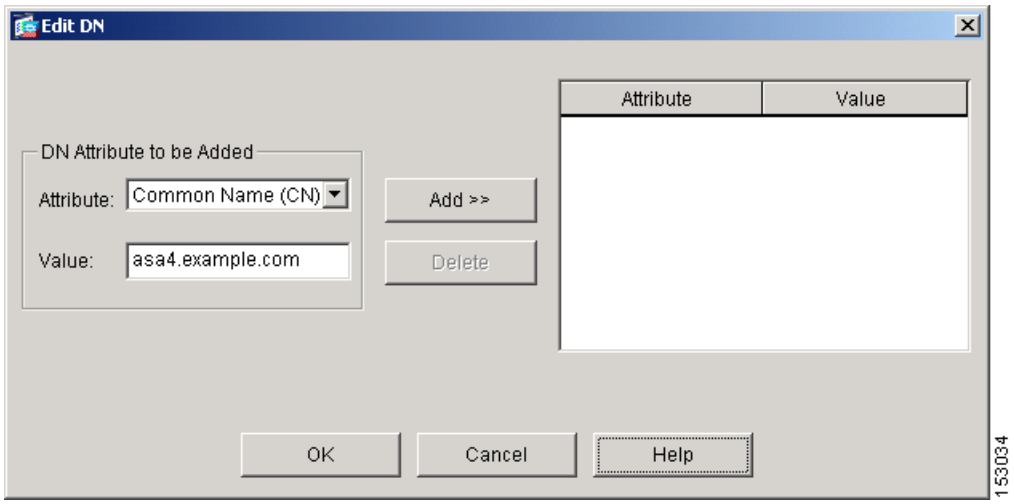
Step 7 Enter the fully qualified domain name used in the Subject Alternative Name extension of the certificate into the **Specify FQDN** field.

The FQDN addresses the server program to which to send requests.

Step 8 Click **Edit**.

The Edit DN window opens (Figure 2-4).

Figure 2-4 Edit DN



Step 9 Select **Common Name** from the drop-down list next to the **Attribute** field.

Step 10 Enter the FQDN you entered in Step 6 into the **Value** field and click **Add**.

The Citrix ICA connection application requires a fully qualified domain name (FQDN) in the common name (CN) field of the SSL certificate.

Caution Do not specify an IP address as the CN.

ASDM inserts the new entry into the table on the right.

Step 11 Click **OK** three times.

ASDM inserts the new trustpoint into the Trustpoint Configuration table (Figure 2-1).

Step 12 Click **Apply** to save the trustpoint to the Flash device.

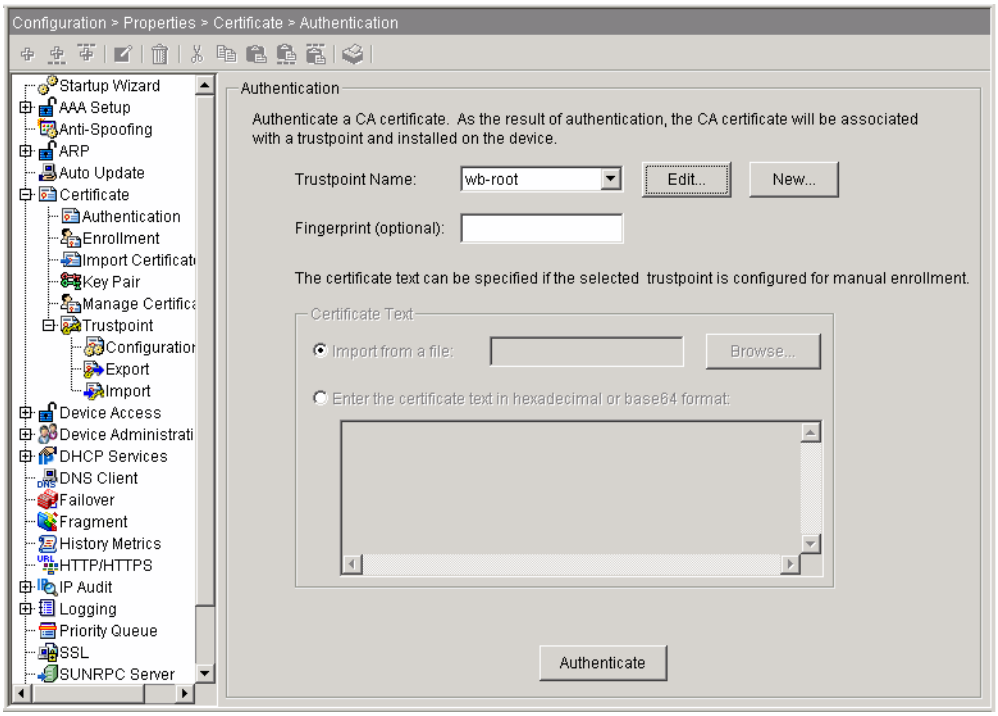
Authenticating the Certificate Authority

Now that you have a trustpoint, you need to authenticate the certificate authority, as follows:

Step 1 Choose Configuration > Properties > Certificate > Authentication.

The Authentication window opens (Figure 2-5).

Figure 2-5 Authentication



Step 2 Select the trustpoint you created in the previous section from the drop-down list next to the **Trustpoint Name** attribute.

Step 3 Click **Authenticate**.

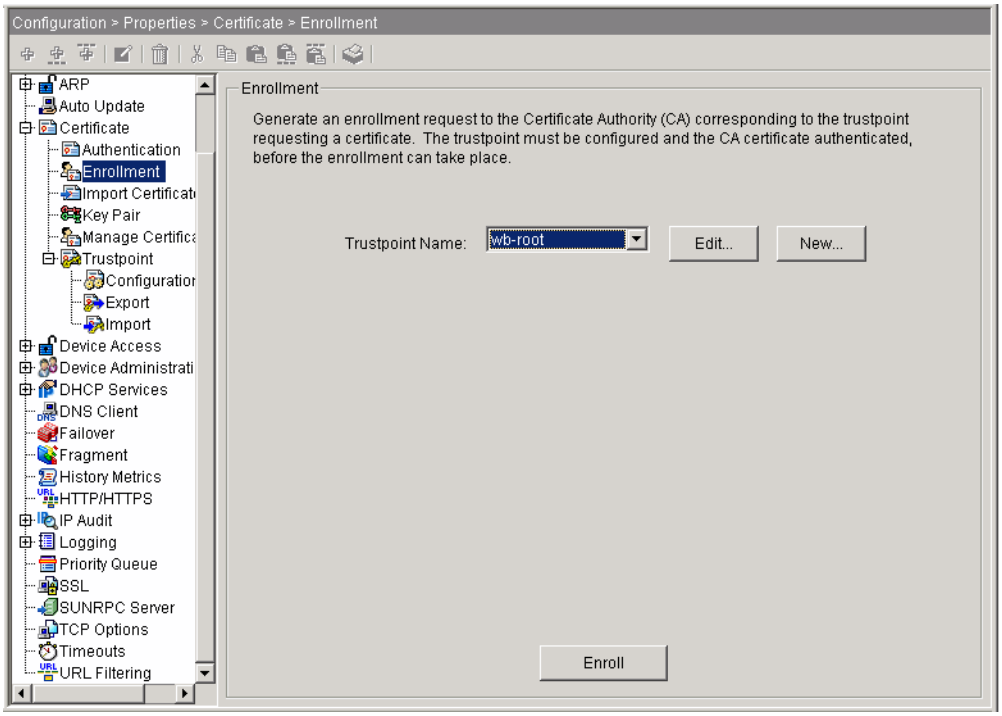
Enrolling the Certificate

When you enroll the certificate, you identify the certificate to be associated with the trustpoint. Enroll the certificate to be used for Citrix connections, as follows:

Step 1 Choose Configuration > Properties > Certificate > Enrollment.

The Enrollment window opens (Figure 2-6).

Figure 2-6 Enrollment



Step 2 Select the trustpoint you created in the previous section from the drop-down list next to the **Trustpoint Name** attribute.

Step 3 Click **Enroll**.

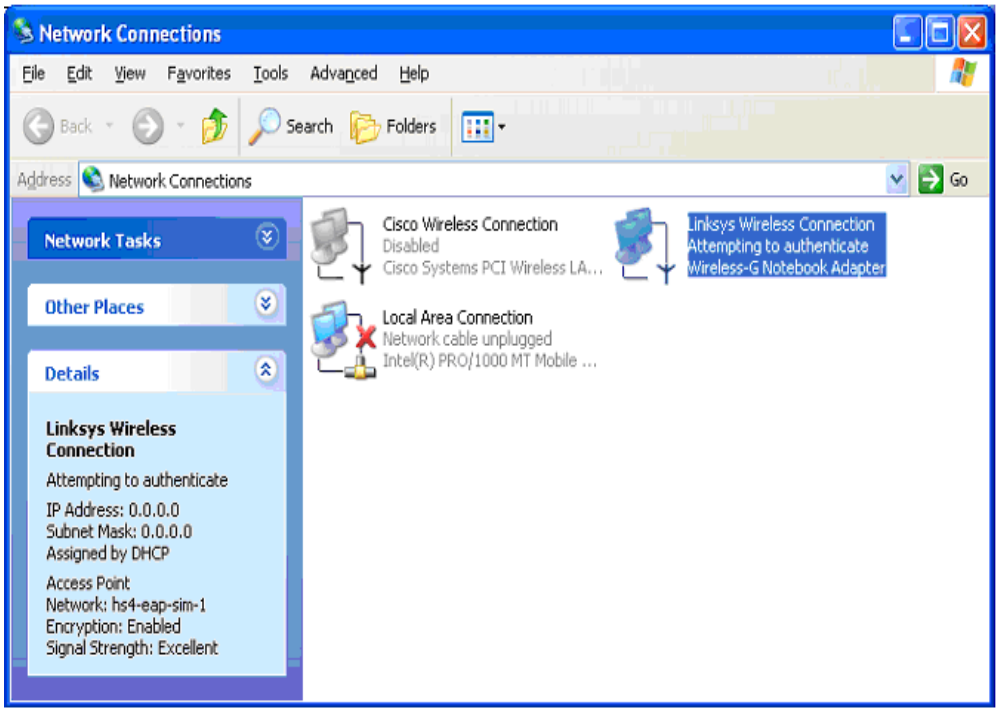
Applying the Trustpoint to an Interface

These instructions describe how to apply the trustpoint to the security appliance interface to be used to terminate WebVPN sessions to the Citrix server. You can, but are not required, to use this interface exclusively for Citrix connections. Apply the trustpoint to the interface as follows:

Step 1 Choose Configuration > Properties > SSL.

The SSL window opens (Figure 2-7).

Figure 2-7 SSL



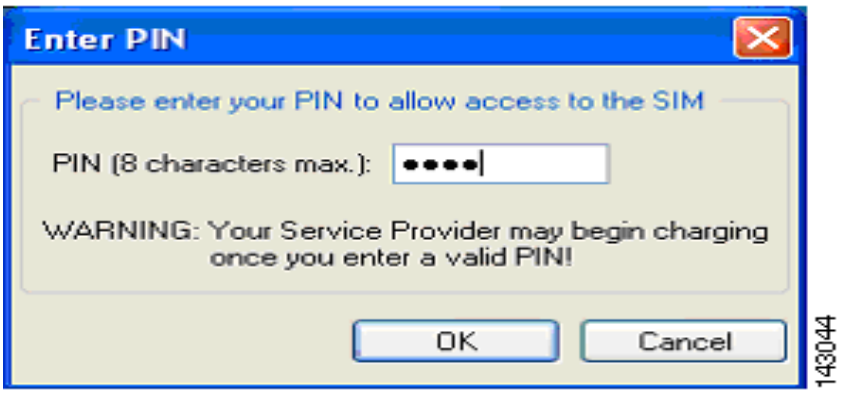
Step 2 Do either of the following:

- Select the trustpoint next to the **Fallback Trustpoint** attribute if you want any interface to use the trustpoint if it doesn't have a specific trustpoint assigned, then click **Apply** to save the configuration change to the Flash device. This step completes the assignment of the trustpoint to the interface.
- Double-click the interface to be used to terminate WebVPN sessions to the Citrix server, to make an explicit assignment of the trustpoint to the interface.

  Typically, the interface used to terminate these sessions is the outside interface.

  The Edit SSL Trustpoint window opens (Figure 2-8).

Figure 2-8 Edit SSL Trustpoint



Select the trustpoint next to the **Primary Enrolled Trustpoint** attribute and click **OK**, then click **Apply** to save the configuration change to the Flash device.

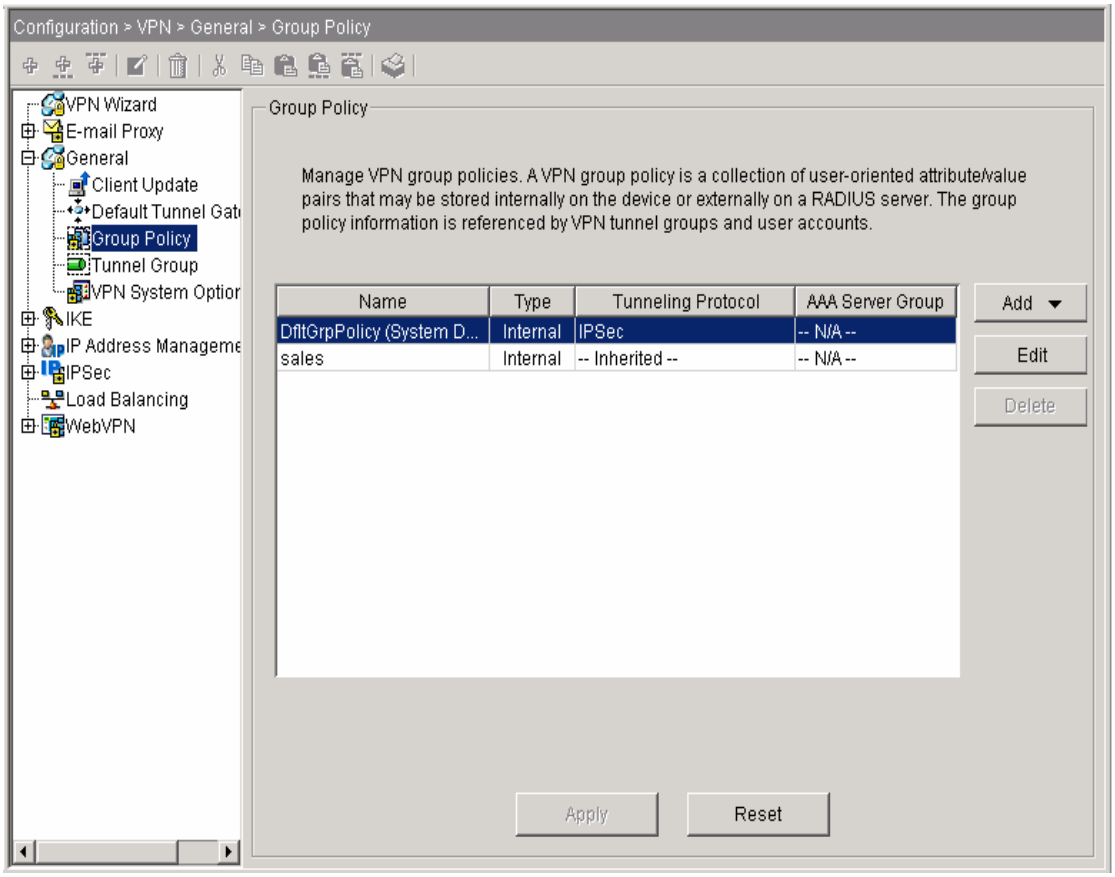
Enabling WebVPN

Remote access to Citrix MetaFrame services requires WebVPN tunneling to be enabled. Enable WebVPN on the group policy applied to the users for whom you want to provide these services as follows:

Step 1 Choose Configuration > VPN > General > Group Policy.

The Group Policy window opens (Figure 2-9).

Figure 2-9 Group Policy



Step 2 Use one of the following strategies:

- Set the default group policy to enable WebVPN tunneling.

  By default, group policies and users inherit the settings of the default group policy.

  Double-click the DfltGrpPolicy entry in the Group Policy table, verify the General tab is open, check **WebVPN** next to Tunneling Protocols, and click **OK**.

- Limit WebVPN to alternative group policies for which you want to provide Citrix MetaFrame services.

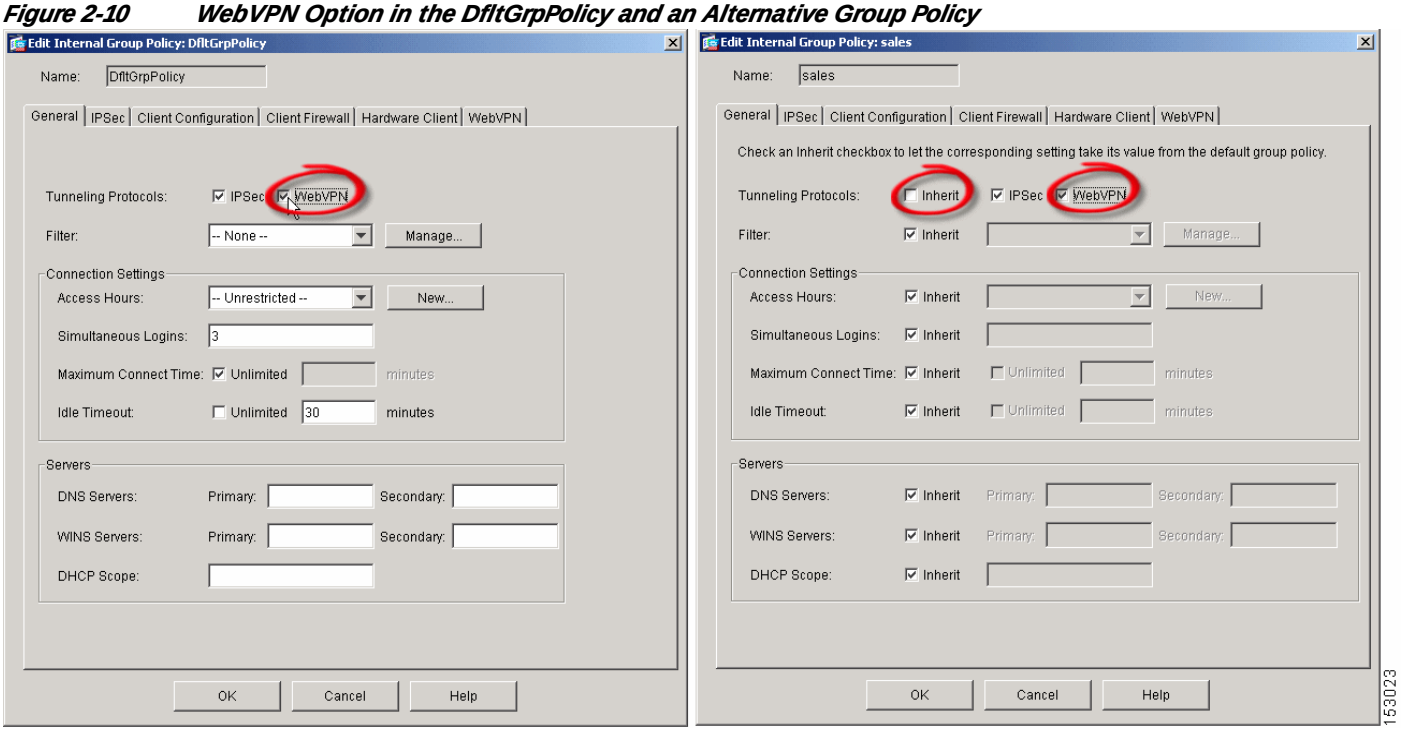
  By default, users inherit the tunneling protocols from their assigned group policies.

  For each internal or external group policy for which you want to provide access to Citrix MetaFrame services, double-click the policy in the Group Policy table, verify the General tab is open, clear the **Inherit** check box next to Tunneling Protocols, check **WebVPN**, and click **OK**.

Note You can also create a new group policy to enable WebVPN services, but if you do, you also need to assign the group policy to the users to whom you want to grant this access right. For more information about configuring group policies, see Chapter 4, "Configuring Group Policies"

Figure 2-10 compares the General tab in the DfltGrpPolicy to that of alternative policies.

Figure 2-10 WebVPN Option in the DfltGrpPolicy and an Alternative Group Policy



Note If you check the Inherit check box in an alternative group policy, the policy uses the WebVPN setting of the default group policy. Clearing the Inherit check box allows you to customize an alternative group policy's WebVPN setting, making it independent from the default group policy's WebVPN setting.

Step 3 Click **Apply** to save the modified group policies to the Flash device.

Enabling Citrix

You can enable Citrix MetaFrame services in the default group policy, alternative group policies, or individual user accounts. Refer to the section that names the strategy you prefer to use.

- Enabling Citrix on a Group Policy, page 2-11
- Enabling Citrix on a User Account, page 2-12

Enabling Citrix on a Group Policy

Enable Citrix MetaFrame services on one or more group policies, as follows:

Step 1 Choose Configuration > VPN > General > Group Policy.

The Group Policy window opens.

Step 2 Use one of the following strategies to enable Citrix MetaFrame services:

- Set the default group policy to enable Citrix.

  By default, alternative group policies and users inherit the settings of the default group policy.

  Double-click the DfltGrpPolicy entry in the Group Policy table, open the **WebVPN** > **Functions** tab, check **Enable Citrix MetaFrame**, and click **OK**.

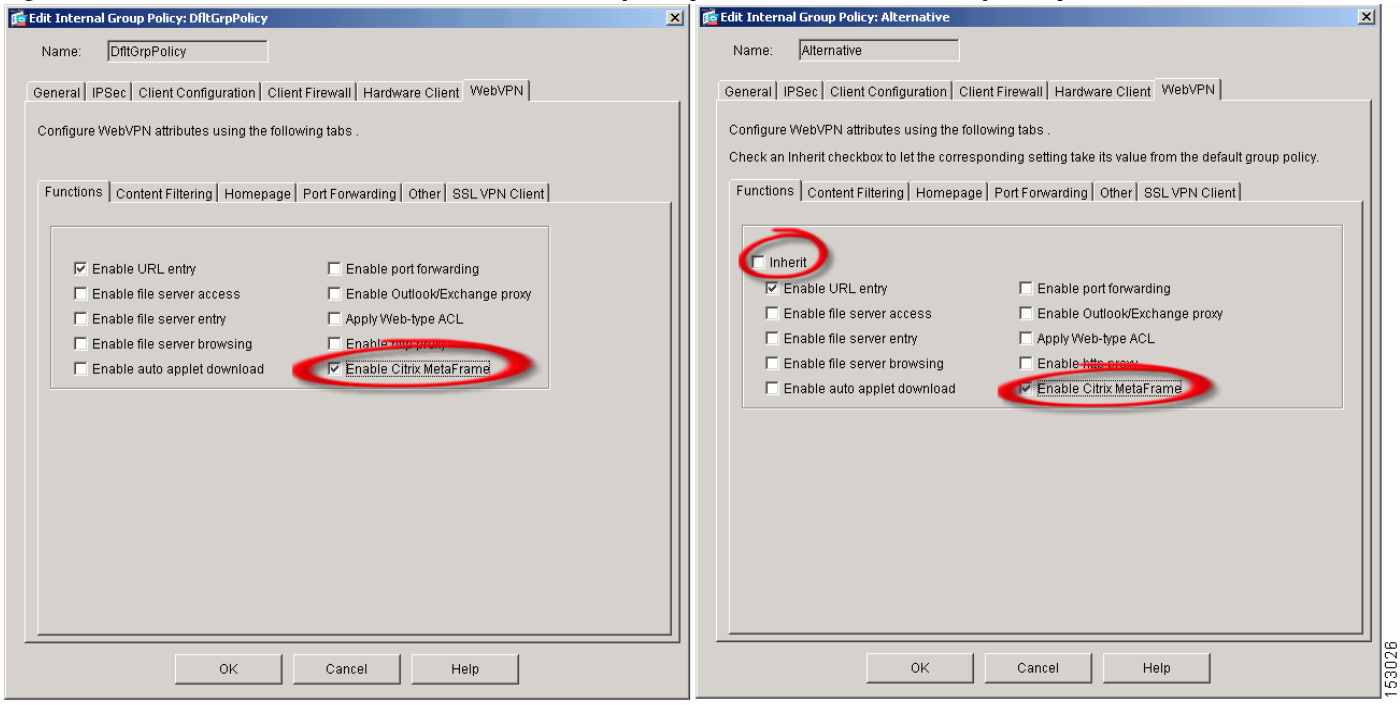
- Set the alternative group policies for which you want to configure support for Citrix to enable WebVPN tunneling.

  By default, users inherit the Functions settings from their respective assigned group policies.

  For each internal or external group policy for which you want to enable Citrix access, double-click the policy in the Group Policy table, open the **WebVPN** > **Functions** tab, clear **Inherit**, check **Enable Citrix MetaFrame**, and click **OK**.

Figure 2-11 compares the WebVPN > Functions tab in the DfltGrpPolicy to that of alternative policies.

Figure 2-11 Enable Citrix MetaFrame in the DfltGrpPolicy and an Alternative Group Policy



If you check the Inherit check box in an alternative group policy, the policy uses the Enable Citrix MetaFrame of the default group policy. Clearing the Inherit check box allows you to customize an alternative group policy's Functions settings, making them independent from the default group policy's WebVPN setting.

Tip The URL Enable entry attribute shown in Figure 2-11, if checked, lets remote users type the URL of the Citrix server in the WebVPN home page or floating toolbar. Redirecting the home page to the Citrix server or creating a link to the home page and floating toolbar are other ways you can let users connect to the Citrix server. By default, the URL Enable entry attribute is checked in the default group policy. ASDM automatically inserts a check mark to enable this attribute if you clear Inherit in an alternative group policy. Use the default setting (checked) if you want to let users enter URLs, including the URL of the Citrix server. Otherwise, clear this attribute. The section, Configuring a Citrix Access Method, page 2-15, provides more information about the options available to provide WebVPN access to a Citrix server.

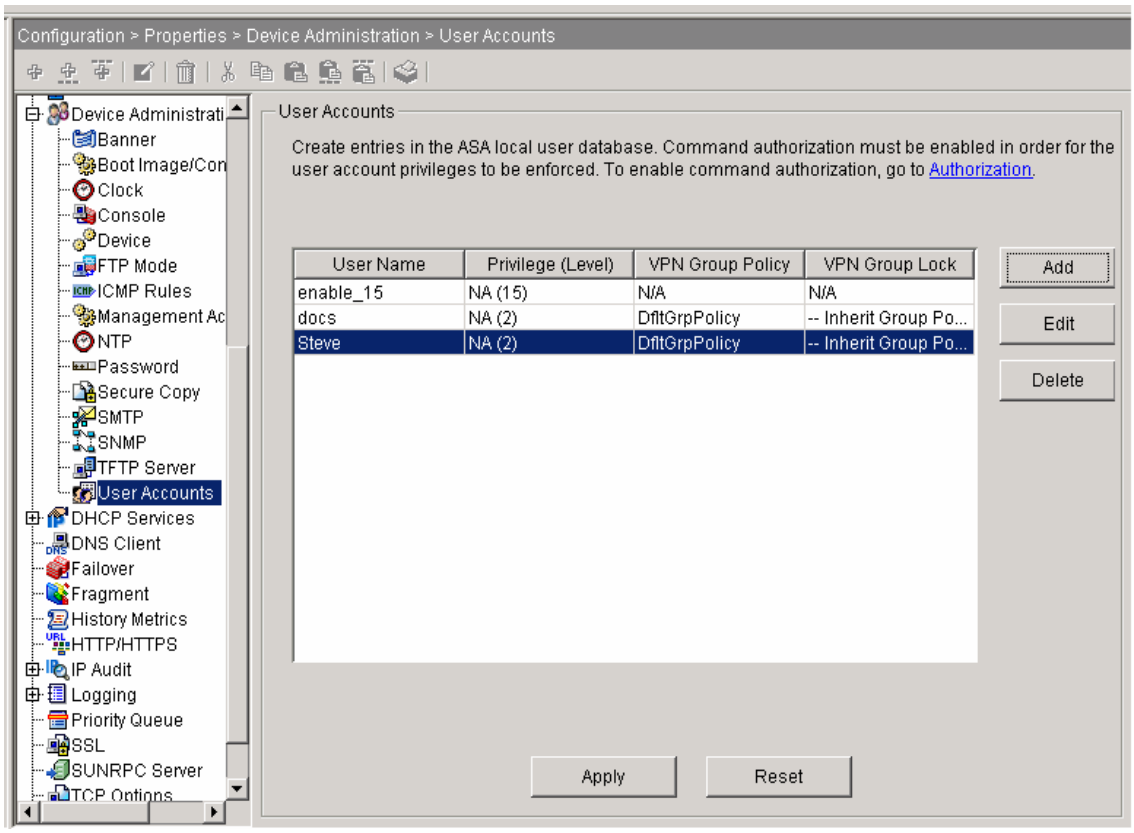
Enabling Citrix on a User Account

As an alternative to enabling Citrix services on group policies applied to users, you can modify user accounts to support Citrix MetaFrame Services. Follow this procedure once for each user account you want to modify.

Step 1 Choose Configuration > Properties > Device Administration > User Accounts.

The User Accounts window opens (Figure 2-12).

Figure 2-12 User Accounts

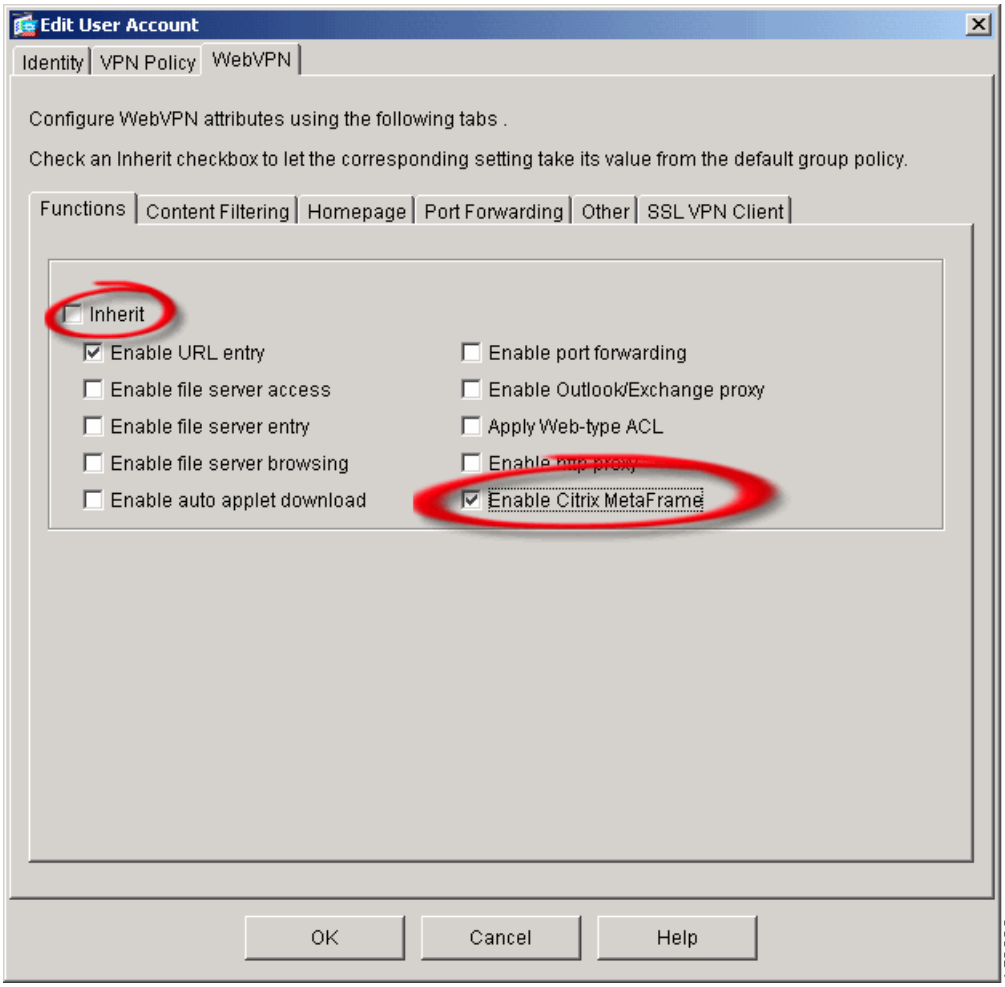


Step 2 Double-click the user name.

Step 3 Open the WebVPN > Functions tab.

The WebVPN Functions window opens (Figure 2-13).

Figure 2-13 Edit User Account — WebVPN Functions



Step 4 Clear the **Inherit check box** and check **Enable Citrix MetaFrame**.

If you check the Inherit check box, the user account uses all of its Functions settings from the assigned group policy. Clearing the Inherit check box lets you customize the Functions settings for that user.

Step 5 Make sure that the other Functions settings are appropriate for the user.

Tip The URL Enable entry attribute shown in Figure 2-13, if checked, lets the user type the URL of the Citrix server in the WebVPN home page or floating toolbar. Redirecting the home page to the Citrix server or creating a link to the home page and floating toolbar are other ways you can let users connect to the Citrix server. By default, the URL Enable entry attribute is checked in the default group policy. ASDM automatically inserts a check mark to enable this attribute if you clear the Inherit check box in the user account. Use the default setting (checked) if you want to let the user enter URLs, including the URL of the Citrix server. Otherwise, clear this attribute. The section, Configuring a Citrix Access Method, page 2-15, provides more information about the options available to provide WebVPN access to a Citrix server.

Step 6 Click **OK**.

Step 7 Click **Apply** to save the modified user accounts to the Flash device.

Note Now that you have cleared the Inherit check box for the Functions settings , the user may lose access to features that were enabled. To view the previously inherited Functions settings, open the **VPN Policy** tab and note the Group Policy setting. Choose Configuration > VPN > General > Group Policy, double-click the group policy name that matches the Group Policy setting you previously viewed, and view the settings in the group policy's **WebVPN** > **Functions** tab.

Configuring a Citrix Access Method

To let users connect to a Citrix MetaFrame server, they need a facility for doing so on the WebVPN home page or toolbar. To provide a means to connect to the Citrix server, refer to the section that names the method you want to use.

- Redirecting the WebVPN User Home Page to the Citrix Server, page 2-15
- Adding a Link on the WebVPN Home Page to the Citrix Server, page 2-17
- Enabling URL Entry on the WebVPN Home Page, page 2-25

Redirecting the WebVPN User Home Page to the Citrix Server

To let WebVPN users access a Citrix server, you can specify its URL as the remote user's WebVPN home page. Use at least one of the following sections to change the URL of the home page:

- Redirecting the Home Page on a Group Policy, page 2-15
- Redirecting the Home Page on a User Account, page 2-16

Redirecting the Home Page on a Group Policy

Redirect the WebVPN home page to the URL of a Citrix MetaFrame server in one or more group policies, as follows:

Step 1 Choose Configuration > VPN > General > Group Policy.

The Group Policy window opens.

Step 2 Use one of the following strategies to redirect the WebVPN home page:

- Set the default group policy to redirect the WebVPN home page.

  By default, alternative group policies and users inherit the Custom Homepage setting of the default group policy.

  Double-click the DfltGrpPolicy entry in the Group Policy table, open the **WebVPN** > **Homepage** tab, click **Specify URL**, select **http** from the drop-down menu, enter the URL of the Citrix server in the field to the right, and click **OK**.

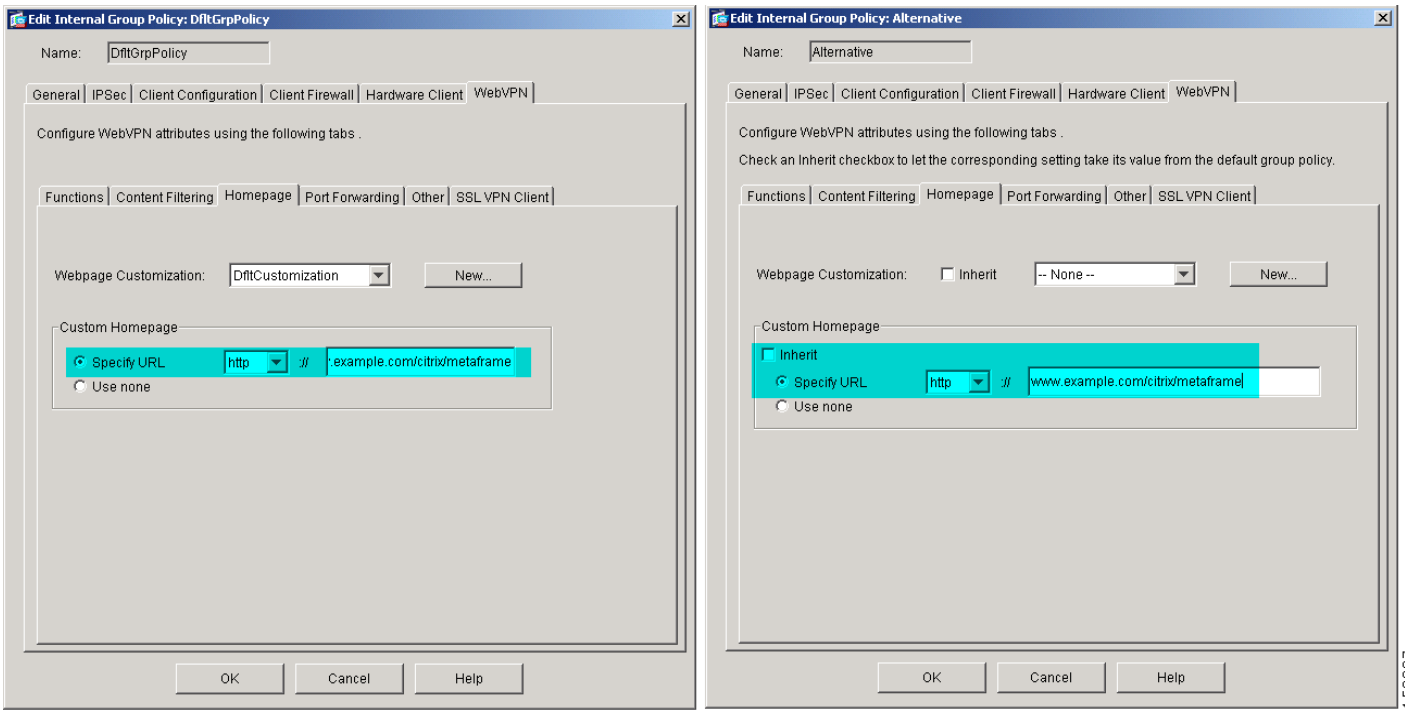
- Set the alternative group policies to redirect the WebVPN home page.

  By default, users inherit the Custom Homepage setting from their respective assigned group policies.

For each internal or external group policy for which you want to redirect the WebVPN home page, double-click the policy in the Group Policy table, open the **WebVPN** > **Homepage** tab, clear **Inherit** in the Custom Homepage area, click **Specify URL**, select **http** from the drop-down menu, enter the URL of the Citrix server in the field to the right, and click **OK**.

Figure 2-14 compares the WebVPN > Homepage tab in the DfltGrpPolicy to that of alternative policies.

Figure 2-14 Home Page Redirection in the DfltGrpPolicy and an Alternative Group Policy



Note If you check the Inherit check box in an alternative group policy, the policy uses the Custom Homepage area settings of the default group policy. Clearing the Inherit check box lets you customize the Custom Homepage area settings for an alternative group policy, making those settings independent from those of the default group policy.

Step 3 Click **Apply** to save the modified group policies to the Flash device.

Redirecting the Home Page on a User Account

As an alternative to redirecting the WebVPN home page on group policies, you can redirect it on user accounts. For each user account for which you want to redirect the home page, do the following steps:

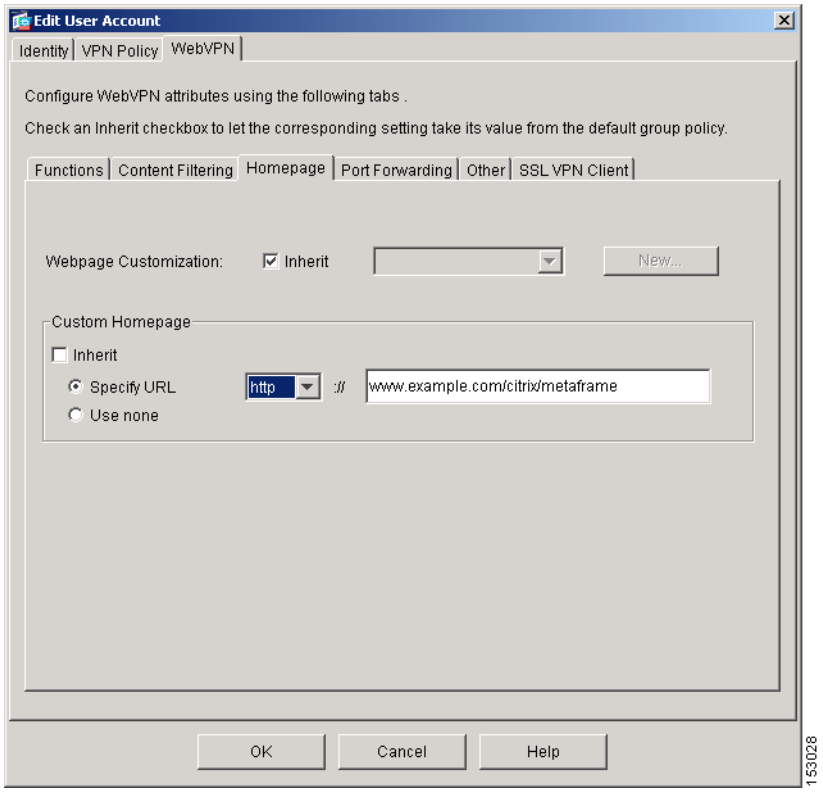
Step 1 Choose Configuration > Properties > Device Administration > User Accounts.

The User Accounts window opens.

Step 2 Double-click the user name and open the **WebVPN** > **Homepage** tab.

Figure 2-15 shows the Edit User Account WebVPN > Homepage tab.

Figure 2-15 Edit User Account WebVPN > Homepage Tab



Step 3 Clear the **Inherit** check box in the Custom Homepage area, click **Specify URL**, select **http** from the drop-down menu, enter the URL of the Citrix server in the field to the right, and click **OK**.

Note If you check the Inherit check box, the user account uses Custom Homepage settings from the assigned group policy. Clearing the Inherit check box lets you customize the settings for that user.

Step 4 Click **Apply** to save the modified user accounts to the Flash device.

Adding a Link on the WebVPN Home Page to the Citrix Server

To let WebVPN users access a Citrix server, you can display a link to the server on the WebVPN home page and floating toolbar (Figure 2-16).

Figure 2-16 WebVPN Home Page and Floating Toolbar

Users only need to click on the Citrix link in the Web Bookmarks menu or list to access the Citrix server.

Use the instructions in the following sections to prepare and configure the link to the Citrix server.

- Examining the URL List Mappings, page 2-18
- Configuring the Link to the Citrix Server, page 2-20

Examining the URL List Mappings

Inserting a URL onto the WebVPN home page requires modifying one or more existing lists of URLs or adding one or more new lists. (A “list” can consist of only one URL.)

To know which lists to modify or whether to add a new list, you need to know whether the group policies and user accounts for whom you want to create a Citrix link are using a list, and if so, which list. Examine the current group policy and user account configuration to determine how to proceed, as follows:

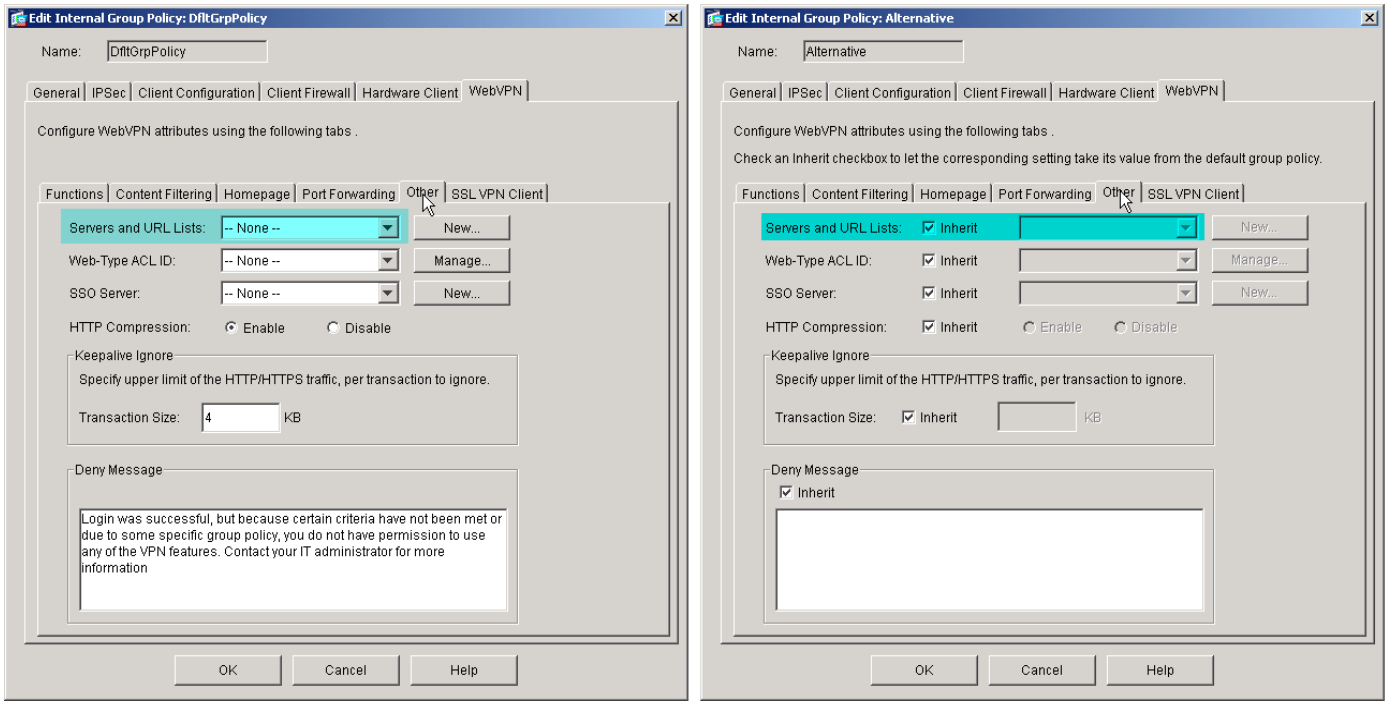
Step 1 Choose Configuration > VPN > General > Group Policy.

The Group Policy window opens.

Step 2 For each group policy, double-click the policy name and open the **WebVPN** > **Other** tab.

Figure 2-17 compares the WebVPN > Other tab of the default group policy to that of the alternative policy.

Figure 2-17 Servers and URL Lists in the DfltGrpPolicy and an Alternative Group Policy



Step 3 Note the values of the Servers and URLs Lists attributes, then click **Cancel**.

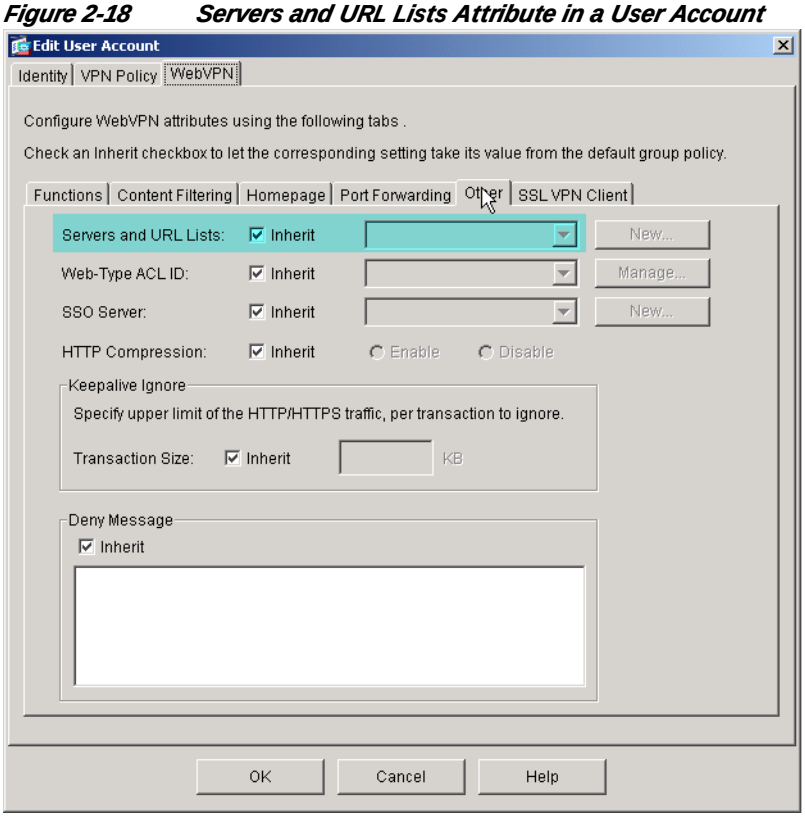
Step 4 Choose Configuration > Properties > Device Administration > User Accounts.

The User Accounts window opens.

Step 5 For each user account for which you are adding support for Citrix services, double-click the policy name and open the **WebVPN** > **Other** tab.

Figure 2-18 shows the Servers and URL Lists attributes on the WebVPN > Other tab of an example user account.

Figure 2-18 Servers and URL Lists Attribute in a User Account



Step 6 Note the values of the Servers and URLs Lists attributes, then click **Cancel**.

Configuring the Link to the Citrix Server

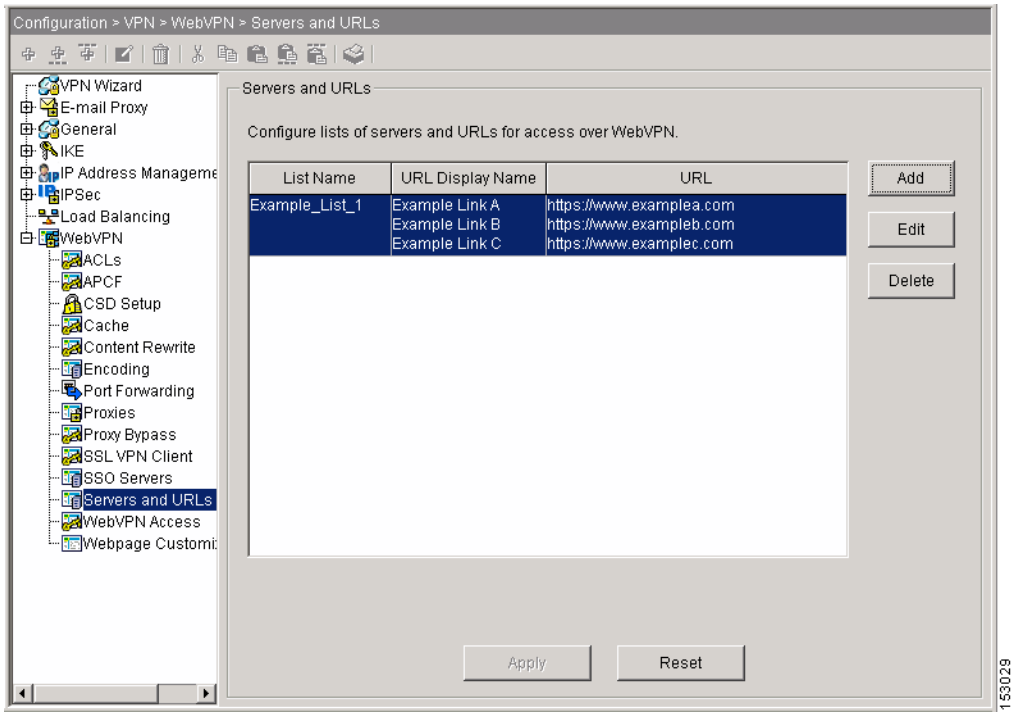
Now that you know whether the group policies and users for whom you want to provide Citrix MetaFrame services are using URL lists, and the names of any URL lists they are using, you are qualified to modify the security appliance configuration of servers and URLs to create the link to the Citrix server.

Create the link to the Citrix server and assign it to the group policies and users for whom you are configuring Citrix access, as follows:

Step 1 Choose Configuration > VPN > WebVPN > Servers and URLs.

The Servers and URLs window opens (Figure 2-19).

Figure 2-19 Servers and URLs



Each list displayed in this window consists of the link names (URL Display Names) and their associated URLs. Following the configuration of a new list, you assign it to at least one group policy or user account to display the list on the WebVPN home page and floating toolbar.

If you add a link to a list that is already assigned to a group policy or user account, the WebVPN home page and floating toolbar automatically add the link for each subsequent login.

Note The Servers and URLs lists have a one-to-one association with the default group policy, and a one-to-many relationship to alternative group policies and user accounts. You can assign one list to more than one group policy and user account, but you cannot assign more than one list to the same group policy or user account.

Step 2 Continue with the instructions in one of the following sections:

- See Adding a Servers and URLs List, page 2-22 if the group policies or user accounts for which you are configuring Citrix services do not have an assigned Servers and URLs list.
- See Adding a URL to a Servers and URLs List, page 2-23 if the group policies or user accounts for which you are configuring Citrix services already have an assigned Servers and URLs list.

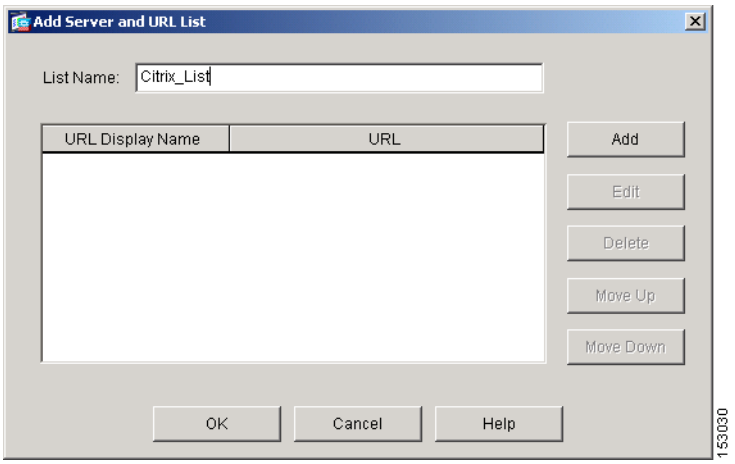
Adding a Servers and URLs List

Continue with the instructions from the previous section to add a Servers and URLs list if the group profiles or user accounts for which you are configuring access to Citrix MetaFrame services do not already have an assigned Servers and URLs list:

Step 1 Click Add in the Servers and URLs window shown in Figure 2-19.

The Add Server and URL List window opens (Figure 2-20)

Figure 2-20 Add Server and URL List

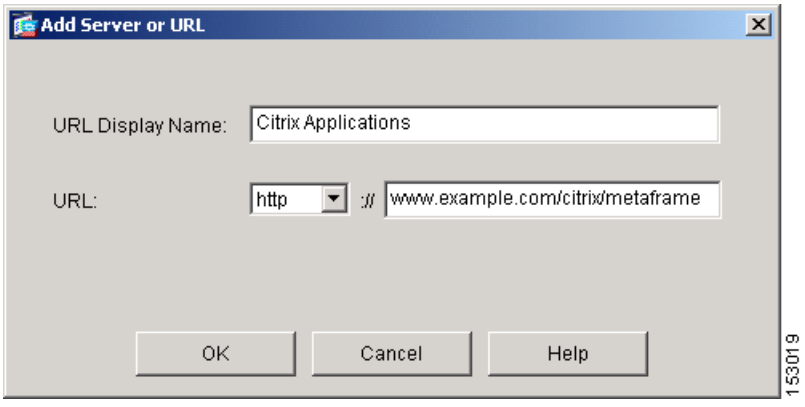


Step 2 Enter a name in the List Name field to differentiate this list from the others in the Servers and URLs configuration. We suggest a name that describes the intent of the group profiles and user accounts for which you want to use them.

Step 3 Click **Add** to create the Citrix link.

The Add Server or URL window opens (Figure 2-21).

Figure 2-21 Add Server or URL



Step 4 Select **http** from the drop-down menu, enter the URL of the Citrix server in the field to the right, and click **OK**.

ASDM inserts the URL entry into the Add Server and URL List table shown in Figure 2-20.

Step 5 Click **OK**.

ASDM inserts the list entry into the Servers and URLs window shown in Figure 2-19.

Step 6 Click **Apply** to save the modified Servers and URLs configuration to the Flash device.

Step 7 Choose Configuration > VPN > General > Group Policy.

The Group Policy window opens.

Step 8 For each group policy for which you want to provide a URL to the Citrix MetaFrame server, double-click the group policy, open the **WebVPN** > **Other** tab, clear the **Inherit** check box next to Servers and URL Lists if the group policy is an alternative to the default group policy, select the list you created in the drop-down menu to the right of the Servers and URL Lists attribute, and click **OK**.

Step 9 Click **Apply** to save the modified group policies to the Flash device.

Step 10 Choose Configuration > Properties > Device Administration > User Accounts.

The User Accounts window opens.

Step 11 For each custom user account for which you want to provide a URL to the Citrix MetaFrame server, double-click the user account, open the **WebVPN** > **Other** tab, clear the **Inherit** check box next to the Servers and URL Lists attribute, select the list you created in the drop-down menu to the right of Servers and URL Lists, and click **OK**.

Step 12 Click **Apply** to save the modified user accounts to the Flash device.

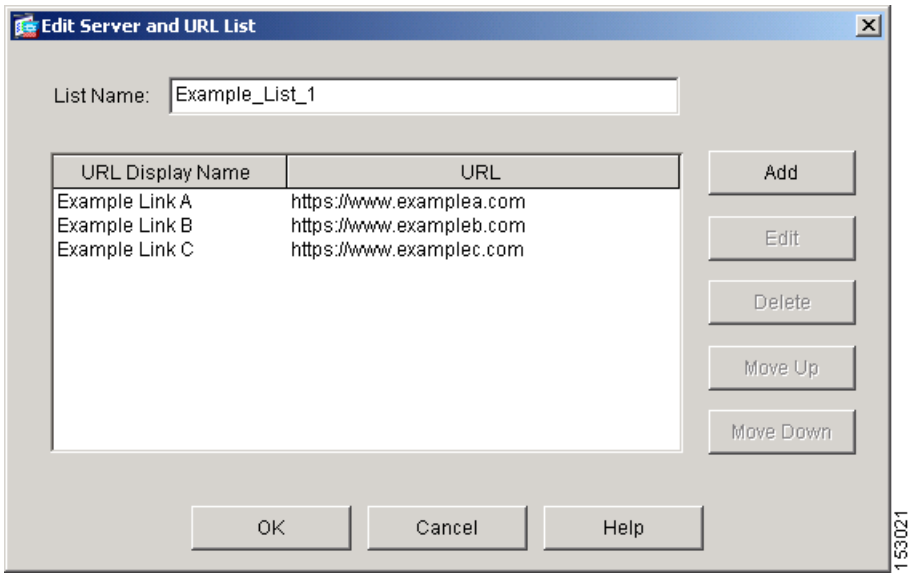
Adding a URL to a Servers and URLs List

Continue with the instructions to modify an entry in the Servers and URLs table displayed in Figure 2-19. Use these instructions only if the group policies or user accounts for which you want to add a URL to the Citrix server already have a Servers and URLs list assignment.

Step 1 Double-click the entry in the Servers and URLs window (Figure 2-19).

The Edit Server and URL List window opens (Figure 2-22)

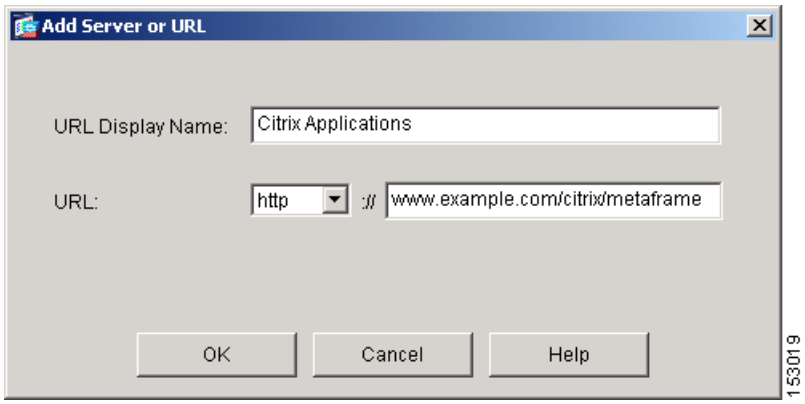
Figure 2-22 Edit Server and URL List



Step 2 Click **Add** to insert the Citrix link into this list.

The Add Server or URL window opens (Figure 2-23).

Figure 2-23 Add Server or URL



Step 3 Select **http** from the drop-down menu, enter the URL of the Citrix server in the field to the right, and click **OK**.

ASDM inserts the URL entry into the Edit Server and URL List table shown in Figure 2-22.

Step 4 Click **OK**.

ASDM inserts the list entry into the Servers and URLs window shown in Figure 2-19.

Step 5 Click **Apply** to save the modified list to the Flash device.

Note This step completes the configuration of the link to the Citrix server if the Servers and URLs list is already assigned to all of the group policies and user accounts for which you want to add a link to the Citrix server. If it is not, continue with the remaining instructions.

Step 6 Choose Configuration > VPN > General > Group Policy.

The Group Policy window opens.

Step 7 For each group policy for which you want to assign the list containing the newly added link to the Citrix server, double-click the group policy, open the **WebVPN** > **Other** tab, clear the **Inherit** check box next to Servers and URL Lists if the group policy is an alternative to the default group policy, select the list you created in the drop-down menu to the right of Servers and URL Lists, and click **OK**.

Step 8 Click **Apply** to save the modified group policies to the Flash device.

Step 9 Choose Configuration > Properties > Device Administration > User Accounts.

The User Accounts window opens.

Step 10 For each custom user account for which you want to assign the list containing the newly added link to the Citrix server, double-click the user account, open the **WebVPN** > **Other** tab, clear **Inherit** check box next to Servers and URL Lists, select the list you created in the drop-down menu to the right of Servers and URL Lists, and click **OK**.

Step 11 Click **Apply** to save the modified user accounts to the Flash device.

Enabling URL Entry on the WebVPN Home Page

To let WebVPN users access a Citrix server, you can enable URL entry and send them the URL to enter to access the server. Users enter the URL into the Enter Web Address field of the WebVPN home page or floating toolbar (Figure 2-16).

The default setting of the Enable URL Entry attribute in the default group policy is checked.

The Enable URL Entry attribute in the WebVPN > Functions tab of the group policy or user account, if checked, lets remote users type the URL of the Citrix server in the WebVPN home page or floating toolbar. By default, the Enable URL Entry attribute shown on the left side in Figure 2-11 is checked in the default group policy. ASDM automatically inserts a check mark to enable this parameter if you e Inherit in an alternative group policy or user account. Use the default setting (checked) if you want to let users enter URLs, including the URL of the Citrix server. Otherwise, clear this attribute.

Because the Enable URL Entry attribute is enabled by default, it is unlikely that you will need to do anything to display the Enter Web Address field on the WebVPN home page or floating toolbar. We do, however, recommend that you check the value of this attribute for each group policy and user account to be sure that users can use the Enter Web Address field. Make sure the Enable URL Entry attribute is either checked or inherited from each applicable group policy or user account, as follows:

Step 1 For each group policy for which you enabled Citrix MetaFrame services, choose Configuration > VPN > General > Group Policy, double-click the entry in the Group Policy table (beginning with the DfltGrpPolicy if you are using it for Citrix access), open the **WebVPN** > **Functions** tab, check **Inherit** or both **Enable URL Entry** and **Enable Citrix MetaFrame**, click **OK**, and click **Apply**.

Step 2 For each user account for which you enabled Citrix MetaFrame services, choose Configuration > Properties > Device Administration > User Accounts, double-click the entry in the User Accounts table, open the **WebVPN** > **Functions** tab, check **Inherit** or both **Enable URL Entry** and **Enable Citrix MetaFrame**, click **OK**, and click **Apply**.