

Clientless SSL VPN Login Screen Advanced Customization

The ASA5500 Series Adaptive Security Appliance presents a login screen to remote users establishing Clientless SSL VPN connections. The software image includes a template for the login screen. You can change the appearance of the screen by editing the template with the Customization Editor launched from ASDM, or by exporting, editing, and re-importing the file manually.

If you prefer to use your own, custom login screen, rather than changing specific screen elements of the login screen we provide, you can perform this advanced customization using the *Full Customization* feature.

With Full Customization, you provide the HTML for your own login screen, and you insert Cisco HTML code that calls functions on the security appliance that create the Login form and the Language Selector drop-down list.

This document describes the modifications you need to make to your HTML code and the tasks required to configure the security appliance to use your code.

[Figure 1](#) shows the standard Cisco login screen that displays to Clientless SSL VPN users. The Login form is displayed by a special Cisco function called by the HTML code.

Figure 1 **Standard Cisco Login Page**

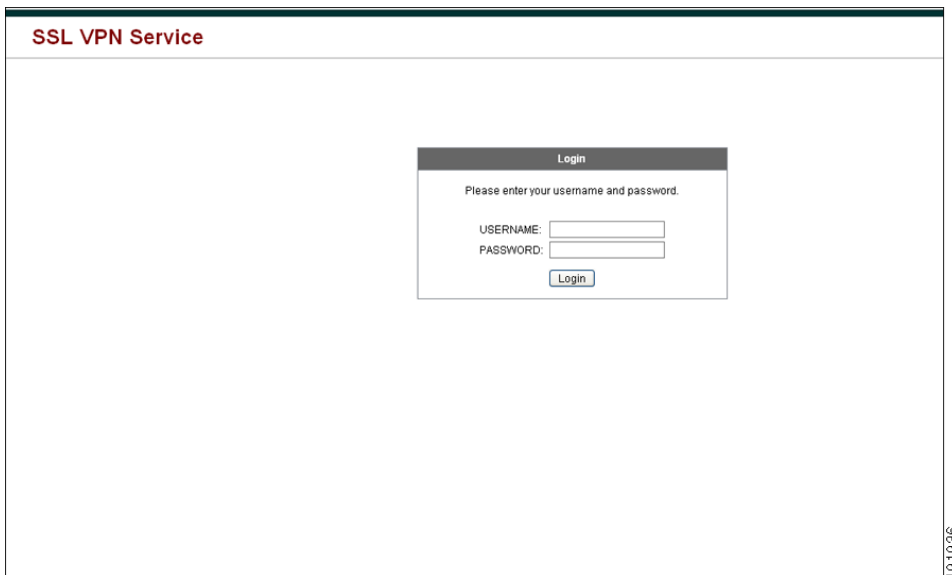


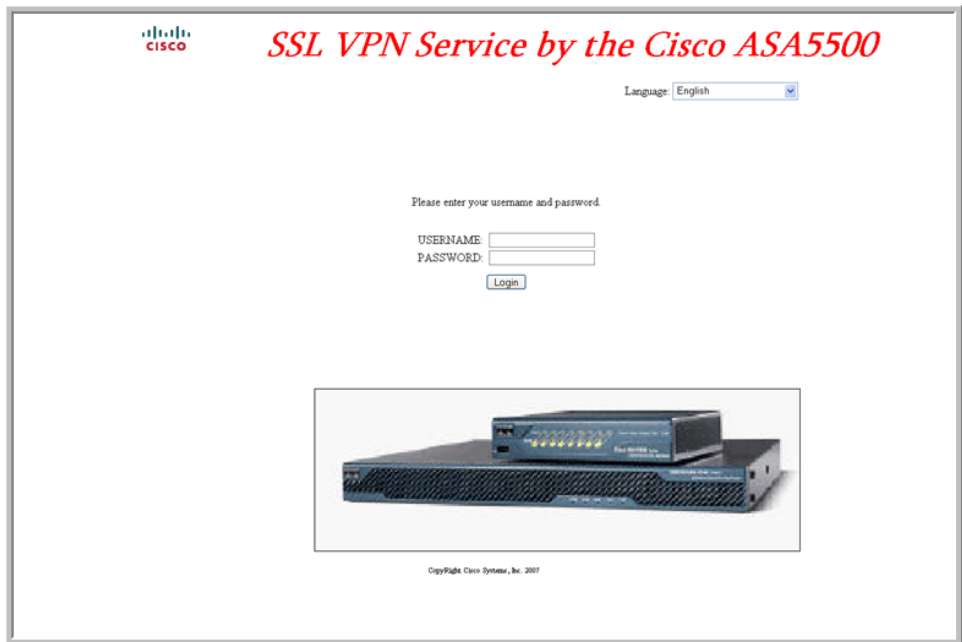
Figure 2 shows the Language Selector drop-down list. This feature is an option for Clientless SSL VPN users, and is also called by a special Cisco function in the HTML code of the login screen.

Figure 2 Language Selector Drop-down List



Figure 3 shows a simple example of a custom login screen enabled by the Full Customization feature.

Figure 3 Example of Full Customization of Login Screen



The following sections describe the tasks to customize the login screen:

- [Create the Custom Login Screen File](#)
- [Import the File and Images](#)
- [Configure the Security Appliance to use the Custom Login Screen](#)

Create the Custom Login Screen File

The following HTML code is used as an example and is the code that displays the screen shown in Figure 3:

```

<head>
<meta http-equiv="Content-Type" content="text/html; charset=windows-1252">
<title>New Page 3</title>
<base target="_self">
</head>

<p align="center">
<font face="Snap
ITC" size="6" color="#FF00FF">
</font><font face="Snap ITC" color="#FF00FF" size="7">&nbsp;</font><i><b><font
color="#FF0000" size="7" face="Sylfaen"> SSL VPN Service by the Cisco
ASA5500</font></b></i></p>

<body onload="cscs_ShowLoginForm('lform');cscs_ShowLanguageSelector('selector')">

<table>

<tr><td colspan=3 height=20 align=right><div id="selector" style="width:
300px"></div></td></tr>
<tr><td></td><td></td><td></td></tr>
<tr>
<td height="379"></td>
<td height="379"></td>
<td align=middle valign=middle>
<div id=lform >
<p>&nbsp;</p>
<p>&nbsp;</p>
<p>&nbsp;</p>
<p>Loading...</p>
</div>
</td>
</tr>
<tr>
<td width="251"></td>
<td width="1"></td>
<td align=right valign=right width="800">

</td></tr>

</table>

```

The indented code injects the Login form and the Language Selector on the screen. The function **cscs_ShowLoginForm('lform')** injects the logon form. **cscs_ShowLanguageSelector('selector')** injects the Language Selector.

Follow these steps to modify your HTML file:

-
- Step 1** Name your file **logon.inc**. When you import the file, the security appliance recognizes this filename as the logon screen.
 - Step 2** Modify the paths of images used by the file to include **/+CSCOU+/.
Files that are displayed to remote users before authentication must reside in a specific area of the security appliance cache memory represented by the path **/+CSCOU+/. Therefore, the source for each image in the file must include this path. For example:****

```
src="/+CSCOU+/asa5520.gif"
```
 - Step 3** Insert the special HTML code below. This code contains the Cisco functions, described earlier, that inject the login form and language selector onto the screen.

```
<body onload="cscs_ShowLoginForm('lform');cscs_ShowLanguageSelector('selector')">
```

```
<table>

<tr><td colspan=3 height=20 align=right><div id="selector" style="width:
300px"></div></td></tr>
<tr><td></td><td></td><td></td></tr>
<tr>
<td height="379"></td>
<td height="379"></td>
<td align=middle valign=middle>
<div id=lform >
<p>&nbsp;</p>
<p>&nbsp;</p>
<p>&nbsp;</p>
<p>Loading...</p>
</div>
</td>
</tr>
<tr>
<td width="251"></td>
<td width="1"></td>
<td align=right valign=right width="800">

</td></tr>

</table>
```

Import the File and Images

Follow these steps to import your HTML file and any images to the security appliance:

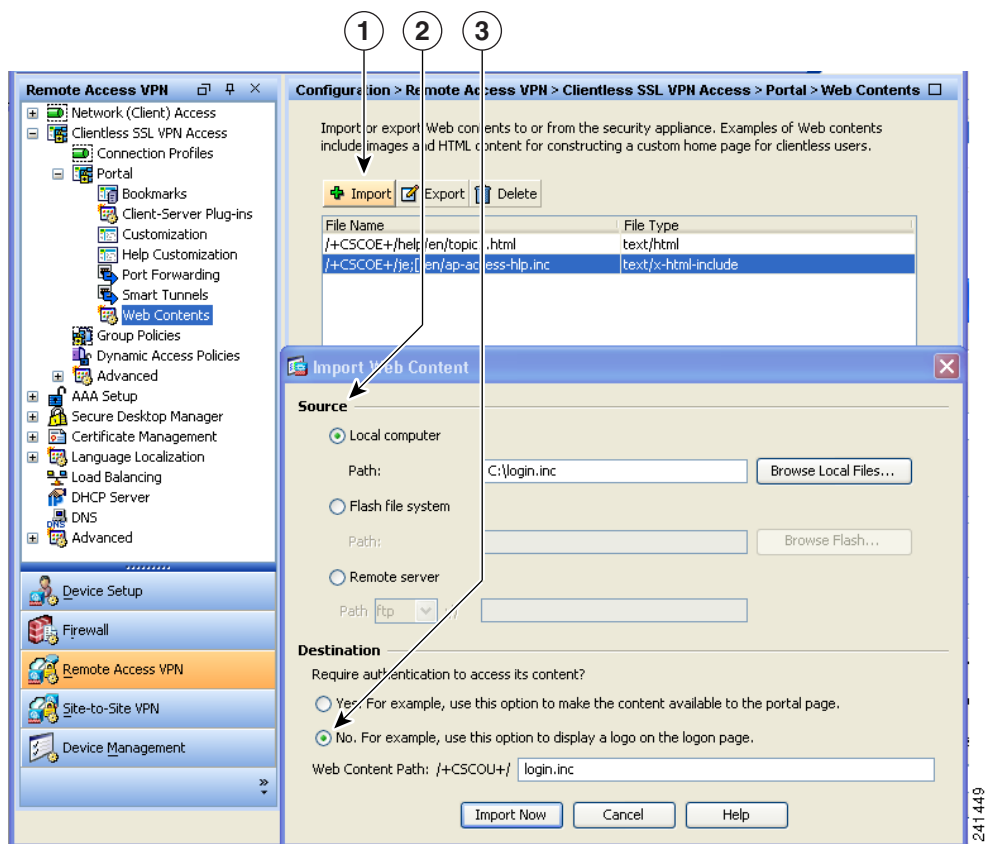
Step 1 Import the file and images as Web Content.

Go to **Clientless SSL VPN Access > Portal > Web Contents** (Figure 4).

Click Import (1). The Import Web Content window displays. Enter the Source information (2). In the Destination area, select **No** for *Require Authentication to access its content* (3). This ensures the files are stored in the area of flash memory accessible to users before authentication.

Step 2 Import any images used by the file as Web Content using the same window.

Figure 4 Import Web Content



Configure the Security Appliance to use the Custom Login Screen

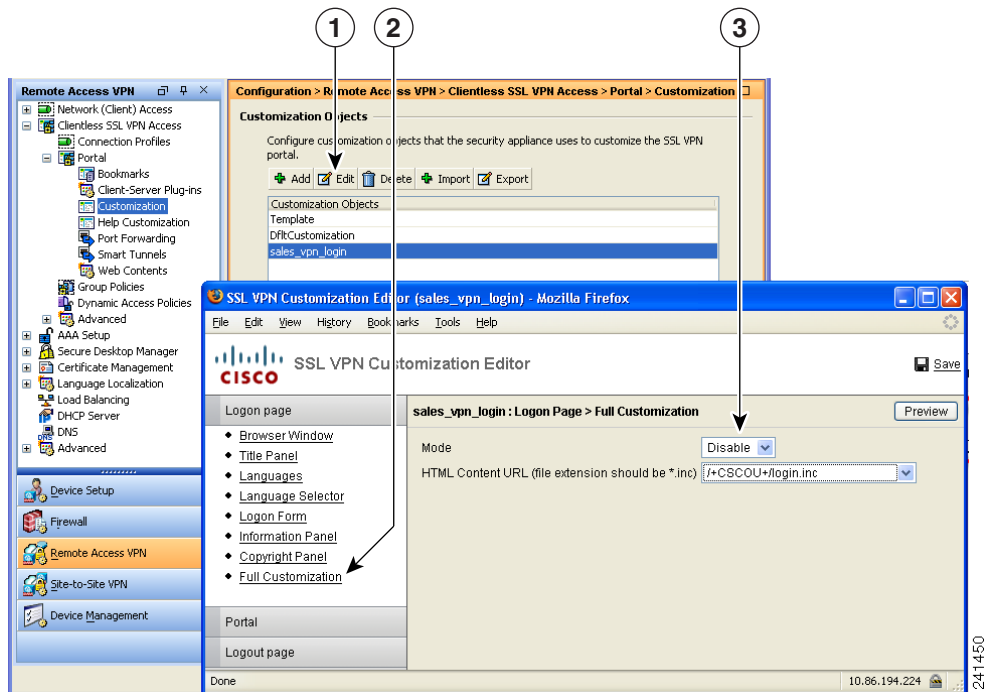
Follow these steps to enable the security appliance to use the new login screen in a customization object:

Step 1 Edit a customization object using the Customization Editor.

Go to **Clientless SSL VPN Access > Portal > Customization** (Figure 5).

Select a customization object from the table and click Edit (1). The Customization Editor displays in a browser window. In the Editor navigation pane, click Full Customization (2). Change the Full Customization mode to Enable and specify the HTML Content URL as **login.inc** (3).

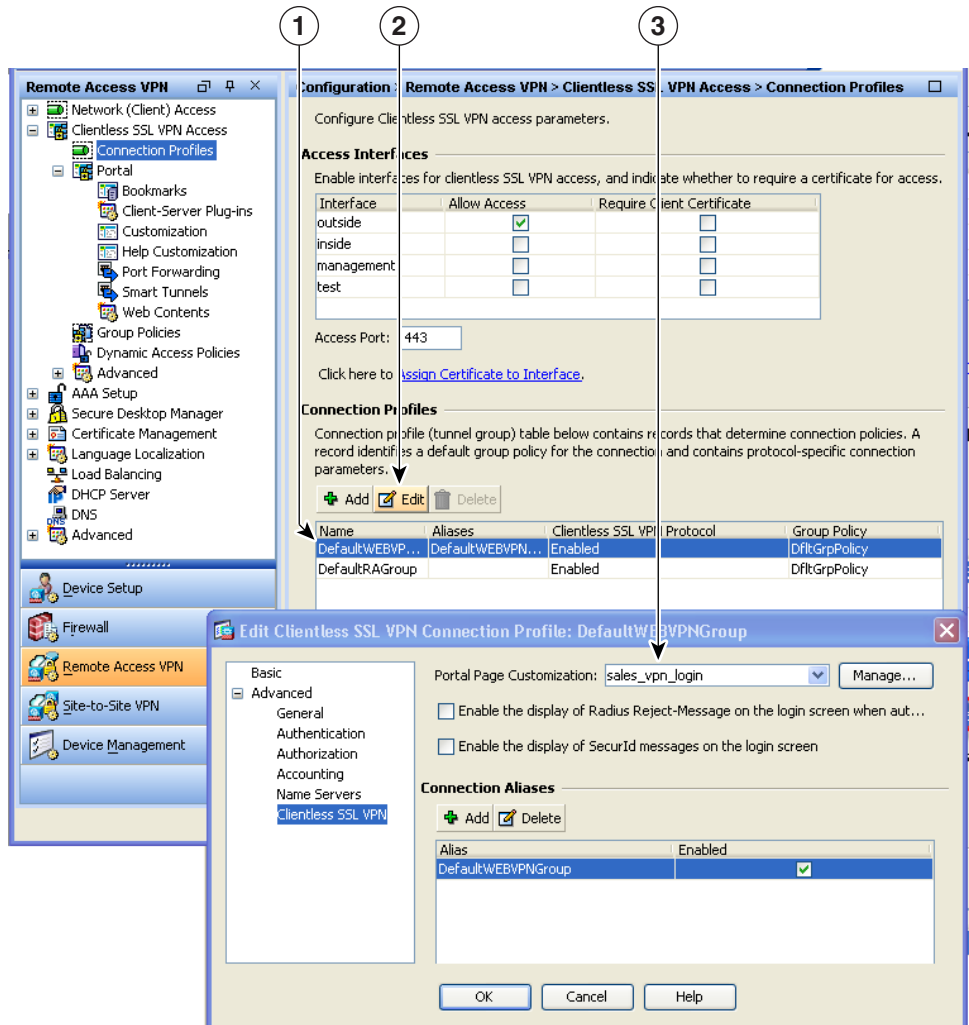
Figure 5 Customization Editor



Step 2 Apply the customization object to a Connection Profile (Figure 6).

Go to **Clientless SSL VPN Access > Connection Profiles**. Select a connection profile (1) and click Edit (2). Select a Portal Page Customization (3).

Figure 6 Applying Customization to Connection Profile



241451

