

Configuring Web Rewriting on a Secure Access Device User Role (NSM Procedure)

The Secure Access device Web rewriting feature enables you to intermediate Web URLs through the Content Intermediation Engine. You can intermediate URLs on the World Wide Web or on your corporate Intranet.

To configure Web rewriting on the user role:

1. In the navigation tree, select **Device Manager > Devices**. Click the **Device Tree** tab, and then double-click the Secure Access device for which you want to configure Web rewriting.
2. Click the **Configuration** tab. Select **Users > User Roles**.
3. Click the **New** button. The New dialog box appears.
4. Add or modify settings as specified in Table 1.
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 1: User Role Web Rewriting Configuration Details

Option	Function	Your Action
Web > Web Bookmarks tab		
Name	Specifies the name for the device home page bookmark.	Enter a name.
Description	Specifies the description for the device home page bookmark.	Enter a description.
Open New Window	Enables the Secure Access device to automatically open the web resource in a new browser window.	Select the Open New Window check box to enable this feature.
Do Not Display Address Bar	Allows Web traffic through the Secure Access device by precluding users in the specified role from typing a new URL in the address bar. This option is displayed only when you enable the Open New Window option.	Select the Do Not Display Address Bar check box to enable this feature.

Table 1: User Role Web Rewriting Configuration Details (continued)

Option	Function	Your Action
Do Not Display Tool Bar	<p>Allows all Web traffic through the Secure Access device by precluding users in the specified role from typing a new URL in the tool bar.</p> <p>This option is displayed only when you enable the Open New Window option.</p>	<p>Select the Do Not Display Tool Bar check box to enable this feature.</p>
Bookmark Type	<p>Allows you to create two types of bookmarks.</p>	<p>Select one of the following option:</p> <ul style="list-style-type: none"> ■ Standard—Links the user to Web URLs on the Internet or on your corporate intranet. When you create Web bookmarks, you can insert the user's Secure Access device username in the URL path to provide single sign-on access to back-end Web applications. ■ Applet—Links the user to Java applets that you upload to the Secure Access device through the NSM by selecting Users > Resource Profiles > Web > Hosted Java Applets.
URL	<p>Specifies the URL to bookmark.</p> <p>NOTE: This box is displayed only when you select Standard from the Bookmark Type drop-down list.</p>	<p>Enter the URL.</p>

Table 1: User Role Web Rewriting Configuration Details (continued)

Option	Function	Your Action
Applet HTML	<p>Specify an HTML page definition that includes references to your Java applets.</p> <p>NOTE: Enter a unique HTML page definition in this box. If you create two bookmarks with the same HTML code, the Secure Access device deletes one of the bookmarks in the end-user view. You can still see both bookmarks, however, in the administrator console.</p> <p>NOTE: The Applet HTML and Multi-Valued User Attributes fields are displayed only when you select Applet from the Bookmark Type drop-down list.</p>	Enter the unique HTML page definition.
Multi-Valued User Attributes	Allows you to specify multiple attributes if your HTML code contains attributes that may expand to multiple values (such as userAttr.hostname or userAttr.ports), .	Enter multiple attributes.
Web > Options tab		
User can type URLs in IVE browse bar	Enables users to enter URLs on the welcome page.	Select the User can type URLs in Secure Access device browse bar check box to enable this feature.
Users can add bookmarks	Enables users to create personal Web bookmarks on the Secure Access device welcome page.	Select the User can add bookmarks check box to enable this feature.
Mask hostnames while browsing	<p>Conceals the target resources in the URLs to which users browse.</p> <p>Users can mask IP addresses and hostnames in the user's:</p> <ul style="list-style-type: none"> ■ Web browser address bar (when the user navigates to a page.) ■ Web browser status bar (when the user hovers over a hyperlink.) ■ HTML source files (when the user chooses to view source.) 	Select the Mask hostnames while browsing check box to enable this feature.

Table 1: User Role Web Rewriting Configuration Details (continued)

Option	Function	Your Action
Allow Java applets	Enables users to: and allows user to <ul style="list-style-type: none"> ■ Browse to web pages containing client-side Java applets. ■ Run applications that are implemented as client-side Java applets. ■ Run application such as the Virtual Network Computing (VNC) Java client, Citrix NFuse Java client, WRQ Reflection Web client, and Lotus WebMail. 	Select the Allow Java applets check box to enable this feature.
Allow Flash content	Enables the Secure Access device to intermediate flash content through its Content Intermediation Engine.	Select the Allow Flash content check box to enable this feature. NOTE: Secure Access device provides limited support for ActionScript 2.0 Flash Remoting, and does not support XML Socket connections.
Persistent cookies	Enables users to customize their browsing experiences through persistent cookies.	Select the Persistent cookies to enable this feature. By default, the Secure Access device flushes Web cookies that are stored during a user session. A user can delete cookies through the Advanced Preferences if you enable this option.
Unrewritten pages open in new window	Allows configuration of Secure Access device to open content in a new browser window when a user accesses an unrewritten Web page.	Select the Unrewritten pages open in new window check box to enable this feature.

Table 1: User Role Web Rewriting Configuration Details (continued)

Option	Function	Your Action
Allow browsing untrusted SSL websites	Enables users to access untrusted Web sites through the Secure Access device.	<p>Select the Allow browsing untrusted SSL Web sites check box to enable this feature.</p> <p>NOTE: If a Web page has internal references to files within a SCRIPT tag and these files are hosted on different HTTPS servers that have SSL certificates not trusted by the Secure Access device, the Web page does not render correctly. In these cases, the Warn users about the certificate problems option must be disabled.</p>
Warn users about the certificate problems	Notifies the user with a warning message at the time of first access on an untrusted web site.	<p>Select the Warn users about the certificate problems check box to enable this feature.</p> <p>NOTE: If you select this option and the user accesses non-HTML content (such as images, js, and css) served from an SSL server that differs from the HTML page, the page containing the links may not display correctly. You can avoid this problem either by clearing this option or by uploading a valid production SSL certificate on the servers that serve the non- HTML content.</p>
Allow users to bypass warnings on a server-by-server basis	Allows users to suppress all further warnings for an untrusted Web site. The user never sees a warning for this site, provided the user accesses it from the current Secure Access device or cluster.	<p>Select Allow users to bypass warnings on a server-by-server basis to enable this feature.</p> <p>NOTE: If you allow users to access untrusted Web sites without seeing a warning, the Secure Access device still logs a message to the user access log whenever a user navigates to an untrusted site. Also note that if a user chooses to suppress warnings, he can clear the persistent settings of the untrusted Web sites.</p>

Table 1: User Role Web Rewriting Configuration Details (continued)

Option	Function	Your Action
Rewrite file:// URLs	Allows the configuration of a Secure Access device to rewrite file:// URLs so that they are routed through the Secure Access device's file browsing CGI.	Select the Rewrite file:// URLs check box to enable this feature.
Rewrite links in PDF files	Allows the configuration of a Secure Access device to rewrite hyperlinks in PDFs.	Select the Rewrite links in PDF files check box to enable this feature.
HTTP Connection Timeout	Allows users to accept the default value or set the duration to tell the Secure Access device how long to wait for a response from an HTTP server before timing out and closing the connection.	Select a timeout value from 30 to 1800 seconds.

- Related Topics**
- Configuring Telnet/SSH on a Secure Access Device User Role (NSM Procedure)
 - Configuring File Rewriting Resource Profiles (NSM Procedure)
 - Configuring Web Rewriting Resource Policies (NSM Procedure)

Published: 2009-08-20