

Configuring Web Rewriting Resource Policies (NSM Procedure)

Web access resource policies control which Web resources users can access in order to connect to the Internet, intranet, or extranet. You can deny or allow access to Web resources by URL or IP address range. For URLs, you can use the “*” and “?” wildcards to efficiently specify multiple hostnames and paths. For resources that you specify by hostname, you can also choose either HTTP, HTTPS, or both protocols.

To configure Web rewriting resource policy:

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 a Web rewriting resource policy.
2. Click the **Configuration** tab. Select **Users > Resource Policies > Web**.
3. Select a policy that you want to configure, and then enter the name, the description, and the resources for the policy.
4. In the Applies to roles list, select one:
 - **All**—Applies the policy to all users.
 - **Selected**—Applies the policy only to users who are mapped to roles in the Role Selection section.
 - **Except those selected**—Applies this policy to all users except for those who map to the roles in the role selection section.
5. In the Action or the Authentication Type list, select any option from the drop-down list for the policy.
6. Select the role, and click **Add** to move the roles from the Non-members to Members list.



NOTE: The Role Selections tab is enabled only when you select the **Selected** or the **Except those selected** option from the Applies to roles drop-down list.

7. Enter the name, and specify the resources for the detailed rules.



NOTE: The Detailed Rules tab is enabled only when you select the **Detailed Rules** option from the Action drop-down list.



NOTE: To apply detailed rules to the roles, see Step 4.

8. Specify one or more expressions in the Conditions box to evaluate to perform the action.
9. Add or modify more settings as specified in Table 1 on page 2.
10. Click one:

- **OK**—Saves the changes.
- **Cancel**—Cancels the modifications.

Table 1: Configuring Web Rewriting Resource Policy Details

Option	Function	Your Action
SSO From POST > General tab		
POST URL	Specifies the absolute URL where the application posts the user's credentials. such as: http://yourcompany.com/login.cgi.	Enter the URL, for example: http://yourcompany.com/login.cgi. NOTE: The Secure Access device does not accept wildcard characters in this field.
Deny direct login for this resource	Allows users to not access the URL directly.	Select the Deny direct login for this resource to enable this feature.
Allow multiple POSTs to this resource	Allows Secure Access device to send POST and cookie values to the resource multiple times if required.	Select the Allow multiple POSTs to this resource to enable this feature.
POST Variables > Label		
Label	Specifies the label that appears on a user's preferences page in the Secure Access device.	Enter the label name. NOTE: This field is required if you either enable or require users to modify data to post to back-end applications.
Name	Specifies the name to identify the data of the value box.	Enter the name. NOTE: The back-end application should expect this name.
Value	Specifies the value to post to the form for the specified name.	Enter the value. NOTE: You can enter static data, a system variable or Secure Access device session variables containing username and password values.
User Modifiable	Allows you to enable user to change the information in the value box.	Select any of the values from the drop-down list.
SSO Cookies/Headers > General tab		
Headers and Values > Header name	Specifies the text for the Secure Access device to send as header data.	Enter the text.
Headers and Values > Value	Specifies the value for the specified header.	Enter the value.
Caching > Options tab		

Table 1: Configuring Web Rewriting Resource Policy Details (continued)

Option	Function	Your Action
Client should cache all images less than (in KB):	Specifies the size of the image. Images are cached if it is less than the specified size.	Enter the size in KB.
Selective Rewriting > General tab		
Rewrite As	Allows Secure Access device to rewrite the content as if it were the file type.	Select any one value from the drop-down list.
Passthrough Proxy.		
Application	Specifies the application name.	Enter the name.
Description	Describes the application.	Enter the description.
URL	Specifies the application server hostname and the port used to access the application internally.	Enter the server hostname and the port. NOTE: Note that you cannot enter a path in this field.
Use virtual hostname	Allows you to specify a host name alias for the application server.	Enter the hostname name alias.
Use IVE port	Allows Secure Access device to listen for client requests to the application server on the specified Secure Access device port.	Specify a unique Secure Access device port in the range 11000-11099.
Rewrite XML	Allows Secure Access device to rewrite URLs contained within XML content.	Select the Rewrite XML to enable this feature.
Rewrite external links	Allows Secure Access device to rewrite all URLs.	Select the Rewrite external links to enable this feature.
Block cookies from being sent to the browser	Allows Secure Access device to block cookies destined for the client's browser.	Select the Block cookies from being sent to the browse to enable this feature.
Host-Header forwarding	Allows Secure Access device to pass the hostname as part of the host header instead of the actual host identifier.	Select the Host-Header forwarding check box to enable this feature.
ActiveX Parameters		
Class Id	Specifies class ID of the ActiveX control that you want to control with the policy.	Enter the class ID.
Description	Describes the policy.	Enter the description.
Parameters > Parameter	Specifies the ActiveX parameters that you want to control with the policy.	Enter the parameters.

Table 1: Configuring Web Rewriting Resource Policy Details (continued)

Option	Function	Your Action
Rewriting Filter		
Bug	Specifies the bug created for the device.	Enter the bug information.
Description	Describes about the bug.	Enter the description for the bug.
Enabled	Specifies if the bug needs to be filtered.	Select Enabled to enable this feature.
Web Proxy > Web Proxy Servers tab		
Name	Specifies the name or IP address of the Web proxy server and the port number at which the proxy server listens.	Enter the name or IP address.
Host	Specifies the hostname of the Web proxy server.	Enter the hostname.
Port	Specifies the port number at which the proxy server listens.	Enter the port.
Web Proxy > Web Proxy Policies > General tab		
Server	Specify a Web proxy server that you have defined. NOTE: This field is enabled only when you select Access web resources through web proxy from the Action drop-down list.	Enter or select a Web proxy server from the drop down list.
Options		
IP based matching for Hostname based policy resources	Allows Secure Access device to look up corresponding to each host name specified in a Web resource policy.	Select the IP based matching for Hostname based policy resources to enable this feature.
Case sensitive matching for the Path and Query string components in Web Resources	Allows you to require users to enter a case-sensitive URL to a resource.	Select the Case sensitive matching for the Path and Query string components in Web Resources to enable this feature.

- Related Topics**
- Configuring a Secure Access ACE Server Instance (NSM Procedure)
 - Configuring a File Rewriting Resource Policy (NSM Procedure)