

Configuring Custom Web Applications Resource Profile (NSM Procedure)

A custom Web application resource profile is a resource profile that controls access to a Web application, Web server, or HTML page.

To configure a custom Web application resource profile:

1. In the NSM 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 the Web application resource profile.
2. Click the **Configuration** tab, and select **Users > Resource Profiles > Web** to create a custom Web resource profile.
4. Click the **New** button, the New dialog box appears.
5. Add or modify settings as specified in Table 1 on page 1.
6. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 1: Configuring Custom Web Applications Resource Profile Details

Option	Function	Your Action
Settings tab		
Name	Specifies a unique name for the resource profile.	Enter the name.
Description	Specifies a description for the resource profile.	Enter the description.
Type	Specifies the type of resource profile.	Select Custom from the Type drop-down list.
Base URL		
Base URL	Specifies the URL of the Web application or page for which you want to control access.	Enter the URL using the format: [protocol://]host[:port][/path]
Autopolicy: Web Access Control > Rules tab		
Name	Specifies the name for the policy that allows or denies users access to the resource specified in the Base URL box.	Enter the name.
Action	Allows or denies user access to the resource.	Select Allow or Deny from the Action drop-down list.
Resources	Specifies the resource for which this policy applies.	Enter the resource name.
Autopolicy: Basic Authentication and NTLM Single Sign-On		

Table 1: Configuring Custom Web Applications Resource Profile Details (continued)

Option	Function	Your Action
Resource	Specifies the resource for which this policy applies.	Specify the resource.
Authentication Type	Specifies the authentication type.	Select the authentication type.
Autopolicy: From POST Single Sign-On		
Resource	Specifies the application's sign-in page.	Enter the path, such as: http://my.domain.com/public/login.cgi . NOTE: Do not enter wildcard characters in this box.
POST URL	Specifies the absolute URL where the application posts the user's credentials.	Enter the URL, such as: http://yourcompany.com/login.cgi .
Deny direct login for this resource	Prevents users from manually entering their credentials in a sign-in page. (Users may see a sign-in page if the form POST fails.)	Select the Deny direct login for this resource check box to enable this option.
Allow multiple POSTs to this resource	Allows the Secure Access device to send POST and cookie values to the resource multiple times if required. If you do not select this option, the Secure Access device does not attempt single sign-on when a user requests the same resource more than once during the same session.	Select the Deny direct login for this resource check box to enable this option.
POST Variables		
Label	Specifies the label that appears on a user's preferences page in the Secure Access device. This field is required if you either enable or require users to modify data to post to back-end applications.	Enter the label name.
Name	Identifies the data in the Value box.	Enter the name.
Value	Specifies a value to post to the form.	Enter the value. You can enter static data or a system variable.

Table 1: Configuring Custom Web Applications Resource Profile Details (continued)

Option	Function	Your Action
User Modifiable?	Allows or denies user to change the information in the Value box.	Select any one of the following option: <ul style="list-style-type: none"> ■ Not Modifiable— User is not able to change the information in the Value box. ■ User Can Modify—User can specify data for a back-end application. ■ User Must Modify—User must enter additional data to access a back-end application.
Autopolicy: Cookies and Headers Single Sign-On		
Resource	Specifies the resources to which this policy applies to post header data to the specified URL when a user makes a request to a resource.	Specify the resource.
Header name	Specifies the text for the Secure ccess device to send as header data.	Enter the name.
Header Value	Specifies the value for the specified header.	Enter the value.
Autopolicy: Caching		
Name	Specifies the policy name.	Enter a name.

Table 1: Configuring Custom Web Applications Resource Profile Details (continued)

Option	Function	Your Action
Action	Specifies the action to perform by the cache cleaner on the resource.	Select one of the following option: <ul style="list-style-type: none"> <li data-bbox="1130 436 1421 751">■ Smart Caching (send headers appropriate for content and browser)—Allows the Secure Access device to send a cache-control:no-store header or a cache-control:no-cache header based on the user's Web browser and content type. <li data-bbox="1130 764 1421 1052">■ Don't Cache (send "Cache Control: No Store")—Delivers attachments to Internet Explorer without saving them to the disk. (The browser temporarily writes files to the disk, but immediately removes them once it has opened the file in the browser.) <li data-bbox="1130 1064 1421 1192">■ Don't Cache (send "Pragma: No Cache")—Prevents the user's browser from caching files to the disk. <li data-bbox="1130 1205 1421 1360">■ Unchanged (do not add/modify caching headers)—Secure Access device forwards the origin server's caching headers as is. <li data-bbox="1130 1373 1421 1528">■ Remove Cache-Control: No-Cache/No-Store—Removes the Cache Control:No Cache and Pragma:no-cache headers.
Resource	Specifies the resources to which this policy applies.	Enter the resource name.
Autopolicy: Java Applet Access Control		
Name	Specifies the name of the policy.	Enter the policy name.
Server Resource	Specifies the server resources to which this policy applies.	Enter the path using the format: host:[ports] .

Table 1: Configuring Custom Web Applications Resource Profile Details (continued)

Option	Function	Your Action
Action	Allows or denies Java applets to connect to the servers	Select one of the following options: <ul style="list-style-type: none"> ■ Allow Socket Access—Allows Java applets to connect to the servers (and optionally ports) in the resource list. ■ Deny Socket Access—Prevents Java applets from connecting to the servers (and optionally ports) in the resource list.
Sign Java applets with uploaded code-signing certificate(s)	Resigns the specified resources using the uploaded certificate.	Select the Sign Java applets with uploaded code-signing certificate(s) check box to enable this option.
Autopolicy: Rewriting Options > Passthrough Proxy tab		
Use virtual hostname	Specifies the hostname alias for the application server. When the Secure Access device receives a client request for the application server hostname alias, it forwards the request to the specified application server port in the Base URL box.	Enter the hostname.
Use IVE port	Specifies a unique Secure Access device port in the range 11,000-11,099.	Enter the port in the range 11,000-11,099.
Rewrite XML	Allows Secure Access device to rewrite URLs contained within XML content. If this option is disabled, the Secure Access device passes the XML content “as is” to the server.	Select the Rewrite XML tab check box to enable this option.
Rewrite external links	Allows Secure Access device to rewrite all the URLs presented to the proxy. If this option is disabled, the Secure Access device rewrites only those URLs where the hostname is configured as part of the passthrough proxy policy.	Select the Rewrite external links check box to enable this option.

Table 1: Configuring Custom Web Applications Resource Profile Details (continued)

Option	Function	Your Action
Block cookies from being sent to the browser	Allows Secure Access device to block cookies destined for the client's browser. The Secure Access device stores the cookies locally and sends them to applications whenever they are requested.	Select the Block cookies from being sent to the browser check box to enable this option.
Host-Header forwarding	Allows Secure Access device to pass the hostname as part of the host header instead of the actual host identifier.	Select Host-Header forwarding to enable this option.
Autopolicy: Rewriting Options > No rewriting (use JSAM) > JSAM Parameters		
Server Hostname or IP	Specifies the DNS name of the application server or the server IP address.	Enter the DNS name of the application server or the server IP address.
Server Port	Specifies the port on which the remote server listens for client connections.	Enter the port.
Localhost IP	Specifies a static loopback address. If you do not provide a static IP loopback address, the Secure Access device assigns an IP loopback address dynamically.	Enter the IP address.
Client Port	Specifies the port on which JSAM should listen for client application connections.	Enter the port.
Launch JSAM	Automatically starts JSAM when the Secure Access device encounters the base URL.	Select the Launch JSAM check box to enable this option.
Autopolicy: Rewriting Options > No rewriting (use JSAM) > Allowed WSAM Servers		
Network Destination	Specifies resources for which WSAM secures client/server traffic between the client and the Secure Access device. By default, the Secure Access device extracts the correct server from the Web access control policy. You may choose to use this server as-is, modify it, and/or add new servers to the list.	Enter the hostname (the wild cards '*' or '?' are accepted) or an IP/netmask pair. Specify multiple ports for a host as separate entries.
Autopolicy: Rewriting Options > No rewriting tab		
No rewriting	Automatically creates a selective rewriting policy for the autopolicy's URL.	Select the No rewriting check box to enable this option.

Table 1: Configuring Custom Web Applications Resource Profile Details (continued)

Option	Function	Your Action
Autopolicy: Web Compression		
Name	Specifies the policy name.	Enter the policy.
Action	Allows the Secure Access device to compress the supported content type for the specified resource.	Select one of the following options: <ul style="list-style-type: none"> ■ Compress—Secure Access device compresses the supported content types from the specified resource. ■ Do not compress—Secure Access device does not compress the supported content types from the specified resource.
Resource	Specifies the resources to which this policy applies.	Enter the resource name.
Settings tab > Type > Custom > Bookmarks > General		
Name	Specifies the name of the bookmark.	Enter the name.
Description	Describes the bookmark.	Enter the description.
URL	Adds a suffix to the URL if you want to create links to subsections of the domain defined in the primary resource profile.	Enter a suffix to the URL.
Open New Window	Allows the enable Secure Access device to automatically open the Web resource in a new browser window.	Select the Open New Window check box to enable this option.
Do Not Display Address Bar	Removes the address bar from the browser.	Select the Do Not Display Address Bar check box to enable this feature.
Do Not Display Tool Bar	Removes the menu and toolbar from the browser. This feature removes all menus, browsing buttons, and bookmarks from the browser window so that the user browses only through the Secure Access device.	Select the Do Not Display Tool Bar check box to enable this feature.

Table 1: Configuring Custom Web Applications Resource Profile Details (continued)

Option	Function	Your Action
Applies to roles	Specifies the roles to which you want to display the bookmark.	Select any one of the following options: <ul style="list-style-type: none">■ All Web Profile roles—Displays the bookmark to all of the roles associated with the resource profile.■ Subset of Web Profile roles—Displays the bookmark to a subset of the roles associated with the resource profile. Then select roles from the ALL Selected Roles list and click Add to move them to the Subset of selected roles list.
Settings tab > Type > Custom > Bookmarks > Role Selections		
Role Selections	Specifies the roles to which the resource profile applies.	Select the role, and click Add .

- Related Topics**
- Configuring File Rewriting Resource Profiles (NSM Procedure)
 - Configuring Windows Terminal Services (NSM Procedure)
 - Configuring a Citrix Listed Application Resource Profile (NSM Procedure)