

Configuring SAML SSO Artifact Profile Resource Policy (NSM Procedure)

Configure SAML SSO Artifact profile resource policy to communicate using the artifact profile (also called Browser/Artifact profile) the trusted access management server “pulls” authentication information from the Secure Access device.

To configure SAML SSO artifact profile 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 SAML Artifact Profile resource policy.
2. Click the **Configuration** tab. Select **Users > Resource Policies > Web > SAML SSO**.
3. Add or modify settings as specified in Table 1 on page 1.
4. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 1: Configuring SAML SSO Artifact Profile Resource Policy Details

Option	Function	Your Action
SAML SSO > General tab or Detailed Role tab		
Name	Specifies the name of the policy.	Enter the name.
Description	Describes the policy.	Enter the description.
New Resources	Specifies the resources to which this policy applies.	Enter the path
Role application	Specifies the roles to which this policy applies.	Select one of the following options from the drop-down list: <ul style="list-style-type: none"> ■ Policy applies to ALL roles—Applies the policy to all users. ■ Policy applies to SELECTED roles—Applies the policy only to users who are mapped to roles in the Role Selection section. ■ Policy applies to all roles OTHER THAN those selected below—Applies the policy to all users except for those who mapped to the roles in the Role Selection section.

Table 1: Configuring SAML SSO Artifact Profile Resource Policy Details (continued)

Option	Function	Your Action
Action	Specifies that the Secure Access device performs a single-sign on (SSO) request to the specified URL.	<p>Select one of the following options from the drop-down list:</p> <ul style="list-style-type: none"> ■ Use SAML SSO—Secure Access device performs a single-sign on (SSO) request to the specified URL using the data specified in the SAML SSO details section. ■ Do not use SAML SSO—Secure Access device does not perform an SSO request. ■ Use Detailed Rules—Specifies one or more detailed rules for this policy.
SAML Assertion Consumer service URL	Specifies the URL that the Secure Access device must contact the assertion consumer service during SSO transactions.	Enter the URL.
Profile	Specifies the type of the profile.	Select Artifact or POST from the drop-down list.
Source ID	Specifies the source ID for the Secure Access device.	<p>Enter the source ID. If you enter a:</p> <ul style="list-style-type: none"> ■ Plain text string—The Secure Access device converts, pads, or truncates it to a 20-byte string. ■ Base-64 encoded string—The Secure Access device decodes it and ensures that it is 20 bytes.
Issuer	Specifies the string that the Secure Access device can use to identify itself when it generates assertions.	Enter the string.

Table 1: Configuring SAML SSO Artifact Profile Resource Policy Details (continued)

Option	Function	Your Action
Subject Name Type	Specifies which method the Secure Access device and assertion consumer service should use to identify the user.	<p>Select one of the following options from the drop-down list:</p> <ul style="list-style-type: none"> ■ Other—Sends the username in another format ■ DN—Sends the username in the format of a DN (distinguished name) attribute. ■ Emal Address—Sends the username in the format of an e-mail address. ■ Windows—Sends the username in the format of a Windows domain qualified username.
Subject Name	Specifies the username that the Secure Access device should pass to the assertion consumer service.	Enter a variable. Or, enter static text.
New Cookie Domain(s)	Specifies the list of domains to which the SSO cookies are associated.	Enter a comma-separated list of domains.
Authentication Type	Specifies the authentication method that the Secure Access device should use to authenticate the assertion consumer service.	<p>Select one of the following options from the drop-down list:</p> <ul style="list-style-type: none"> ■ None—Does not authenticate the assertion consumer service. ■ Username/Password—Authenticates the assertion consumer service using a username and password. ■ Certificate—Authenticates the assertion consumer service using certificate attributes.
Username	<p>Specifies the username that the assertion consumer service must send the Secure Access device.</p> <p>NOTE: The username and password boxes are displayed only when you select the Username/Password option from the Authentication Type drop-down list.</p>	Enter the username.

Table 1: Configuring SAML SSO Artifact Profile Resource Policy Details (continued)

Option	Function	Your Action
Password	Specifies the password that the Secure Access device must send the Secure Access device.	Enter the password.
Certificate		
Attribute Name	Specifies the attributes that the assertion consumer service must send the Secure Access device. (one attribute per line). NOTE: The certificates-attributes box is displayed only when you select Certificate option from the Authentication Type drop-down list.	Enter the attribute name. For example, enter cn = sales.
Attribute Value	Specifies the attribute values that match the values contained in the assertion consumer service's certificate.	Enter the attribute value.
SAML SSO > Role		
Role	Maps roles to the resource control policy. NOTE: The Role tab is enabled only when you select the Policy applies to SELECTED roles or the Policy applies to all roles OTHER THAN those selected below option from the Applies to role drop-down list.	Select a role and click Add to add roles from the Non-members to Members list.
SAML SSO > Detailed Role		
Conditions	Specifies one or more expressions to evaluate to perform the action.	Specify one of the following options: <ul style="list-style-type: none"> ■ Boolean expressions: Using system variables, write one or more Boolean expressions using the NOT, OR, or AND operators. ■ Custom expressions: Using the custom expression syntax, write one or more custom expressions.

Related Topics ■ Setting Up Secure Access Device Host Checker Options (NSM Procedure)

- Configuring a SAML Access Control Resource Policy (NSM Procedure)

