

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

When enabling access control transactions to a trusted access management system, the Secure Access device and trusted access management system exchanges information.

To configure a SAML access control 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 access control resource policy.
2. Click the **Configuration** tab. Select **Users > Resource Policies > Web > SAML ACL**.
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 Access Control Resource Policy Details**

| <b>SAML ACL &gt; General tab or Detailed Rule tab</b> |   |   |
|---|---|---|
| Name  | Specifies the name of the policy.                     | Enter the name.   |
| Description   | Describes the policy.                                 | Enter the policy.   |
| New Resources   | Specifies the resources to which this policy applies. | Enter the resources.  |
| 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"> <li>■ <b>Policy applies to ALL roles</b>—Applies this policy to all users.</li> <li>■ <b>Policy applies to SELECTED roles</b>—Applies this policy only to users who are mapped to roles in the selected roles list.</li> <li>■ <b>Policy applies to all roles OTHER THAN those selected below</b>—Applies this policy to all users except for those who map to the roles in the selected roles list.</li> </ul> |

**Table 1: Configuring SAML Access Control Resource Policy Details (continued)**

|                         |  |  |
|-------------------------|--|--|
| Action                  | Allows or denies the Secure Access device to perform an access control check.  | Select one of the following options from the drop-down list: <ul style="list-style-type: none"> <li>■ <b>Use SAML</b>—Secure Access device performs an access control check to the specified URL.</li> <li>■ <b>Do not use SAML</b>—Secure Access device does not perform an access control check.</li> <li>■ <b>Use Detailed Rules</b>—Specifies one or more detailed rules for this policy.</li> </ul>                   |
| SAML Web Service URL    | Specifies the URL of the access management system's SAML server.   | Enter the URL, using the format:https://hostname/ws.   |
| SAML Web Service Issuer | Specifies the hostname of the issuer, which in most cases is the hostname of the access management system.   | Enter a unique string.   |
| Authentication Type     | Specifies the authentication method that the SAML Web service should use to authenticate the Secure Access device.   | Select one of the following options from the drop-down list: <ul style="list-style-type: none"> <li>■ <b>None</b>—Does not authenticate the Secure Access device.</li> <li>■ <b>Username/Password</b>—Authenticates the Secure Access device using a username and password.</li> <li>■ <b>Certificate</b>—Authenticates the Secure Access device using a certificate signed by a trusted certificate authority.</li> </ul> |
| Username                | Specifies the username that the Secure Access device must send the Web service.<br><br><b>NOTE:</b> The username and password fields are displayed only when you select the <b>Username/Password</b> option from the Authentication Type drop-down list. | Enter the username.  |
| Password                | Specifies the password that the Secure Access device must send the Web service.  | Enter the password   |
| Certificate             | Specifies the certificate installed on the Secure Access device to send to the Web service.<br><br><b>NOTE:</b> This box is displayed only when you select <b>Certificate</b> option from the Authentication Type drop-down list.                        | Select the certificate installed on the Secure Access device from the drop-down list.  |

**Table 1: Configuring SAML Access Control Resource Policy Details** (continued)

|   |   |  |
|---|---|--|
| Subject Name Type                       | Specifies which method the Secure Access device and SAML Web service should use to identify the user.   | Select one of the following options from the drop-down list: <ul style="list-style-type: none"> <li>■ <b>Other</b>—Sends the username in another format agreed upon by the Secure Access device and the SAML Web service.</li> <li>■ <b>DN</b>—Sends the username in the format of a DN (distinguished name) attribute.</li> <li>■ <b>Email Address</b>—Sends the username in the format of an e-mail address.</li> <li>■ <b>Windows</b>—Sends the username in the format of a Windows domain qualified username.</li> </ul> |
| Subject Name                            | Specifies the username that the Secure Access device should pass to the SAML Web service.   | Enter the username.  |
| Device Issuer                           | Specifies the hostname of the issuer, which in most cases is the hostname of the access management system.  | Enter the hostname.  |
| Maximum Cache Time (seconds)            | Specifies the amount of time the Secure Access device should cache the responses (in seconds).  | Enter the time.  |
| Ignore Query data                       | Specifies that the Secure Access device should remove the query string from the URL before requesting authorization or caching the authorization response.  | Select the <b>Ignore Query data</b> check box to enable this feature.  |
| <b>SAML ACL &gt; Role</b>               |   |  |
| Role                                    | Maps roles to access control policy resources.<br><br><b>NOTE:</b> The Role tab is enabled only when you select <b>Policy applies to SELECTED roles</b> or <b>Policy applies to all roles OTHER THAN those selected below</b> from the Action drop-down list. | Select a role and click <b>Add</b> to add roles from the Non-members to the Members list.  |
| <b>SAML ACL &gt; Detailed Rules tab</b> |   |  |
| Conditions                              | Specifies one or more expressions to evaluate to perform the action.  | Specify one of the following options: <ul style="list-style-type: none"> <li>■ Boolean expressions: Using system variables, write one or more Boolean expressions using the NOT, OR, or AND operators.</li> <li>■ Custom expressions: Using the custom expression syntax, write one or more custom expressions.</li> </ul>   |

**Related Topics**

- [Configuring SAML SSO Artifact Profile Resource Policy \(NSM Procedure\)](#)

- Setting Up Secure Access Device Host Checker Options (NSM Procedure)