

Configuring a Secure Access SAML Server Instance (NSM Procedure)

The Secure Access device accepts authentication assertions generated by an SAML authority using either an artifact profile or a POST profile. This feature allows a user to sign in to a source site or portal without going through the Secure Access device first, and then to access the Secure Access device with single sign-on (SSO) through the SAML consumer service.

To configure a new SAML server instance:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the Secure Access device for which you want to configure an SAML server instance.
3. Click the **Configuration** tab and select **Authentication > Auth Servers**. The corresponding workspace appears.



NOTE: If you want to update an existing server instance, click the appropriate link in the Auth Server Name box, and perform the Steps 5 through 8.

4. Click the **New** button. The New dialog box appears.
5. In the Auth Server Name list, specify a name to identify the server instance.
6. Select **SAML Server** from the Auth Server Type list.
7. Configure the server using the settings described in Table 1.
8. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 1: SAML Server Instance Configuration Details

Option	Function	Your Action
SAML Settings > Basic Settings tab		
Source Site Inter-Site Transfer Service URL	Specifies the source site inter-site transfer service URL.	Enter the URL.
Issuer Value for Source Site	Specifies the issuer value for the source site.	Enter the URL or hostname of the issuer of the assertion.
User Name Template	Specifies the user name template, which is a mapping string from the SAML assertion to a Secure Access user realm.	Enter the string.

Table 1: SAML Server Instance Configuration Details (continued)

Option	Function	Your Action
Allow Clock Skew (minutes)	Determines the maximum allowed difference in time between the Secure Access device clock and the source site clock.	Enter the allowed clock skew value.
SAML Settings > Artifact SSO tab		
Source ID	Specifies the 20- byte identifier that the Secure Access device uses to recognize an assertion from a given source site.	Enter the Source ID.
Source SOAP Responder Service URL	Specifies the source SOAP responder service URL.	Enter a URL. NOTE: You should specify this URL in the form of an HTTPS: protocol.
SOAP Client Authentication	Specifies the SOAP client authentication.	Select either HTTP Basic or SSL Client Certificate .
Username	Specifies the username for SOAP client authentication.	Enter the username.
Password	Specifies password for SOAP client authentication.	Enter the password.
Device Certificate	Specifies the device certificate.	Select a device certificate the drop-down list.
SAML Settings > POST SSO tab		
Response Signing Certificate	Specifies the response signing certificate for the SAML response signature verification. This is the PEM-formatted signing certificate, which is loaded for the SAML response signature verification. The certificate you select should be the same certificate used for signing the SAML response at the source site. The source site may send this certificate along with the SAML response, depending on the source site configuration. By default, the system performs signature verification of the SAML response first on the locally configured certificate. If a certificate is not configured locally in the SAML authentication server, then the system performs the signature verification on the certificate included in the SAML response from the source site.	Enter the name or browse to locate the response signing certificate.
Issued To	Displays name and attributes of the entity to whom the certificate is issued.	Issued To details is displayed.
Issued By	Displays name and attributes of the entity that issued the certificate.	Issued By details is displayed.
Valid	Displays the time range that the certificate is valid.	Certificate valid time range is displayed.

Table 1: SAML Server Instance Configuration Details (continued)

Option	Function	Your Action
Enable Signing Certificate status checking	Allows the Secure Access device to check the validity of the signing certificate configured in the SAML authentication server POST profile.	Select SAML Settings > POST SSO > Enable Signing Certificate status checking to enable this feature.
Server Catalog > Expressions tab		
Name	Specifies a name for the user expression in the Certificate server user directory.	Enter the name.
Value	Specifies a value for the user expression in the Certificate server user directory.	Enter the value.

- Related Topics**
- Configuring a Secure Access Active Directory or NT Domain Instance (NSM Procedure)
 - Configuring a Secure Access NIS Server Instance (NSM Procedure)
 - Configuring a Secure Access Certificate Server Instance (NSM Procedure)

Published: 2009-08-20