NetIQ® SocialAccess

SAML 2.0 Connector 1.7 for ADFS Guide

May 2013

Legal Notice

Contents

About this Book and the Library

The *NetIQ® SocialAccess SAML 2.0 Connector for Active Directory Federation Service (ADFS) Guide* provides installation and configuration information for the SAML 2.0 Connector for ADFS.

Intended Audience

This guide provides information for SocialAccess administrators who are responsible for configuring and managing the SAML 2.0 Connector for ADFS.

Other Information in the Library

The library provides the following information resources:

Installation and Configuration Guide

Provides installation and configuration instructions for SocialAccess.

Help

Provides context-sensitive information and step-by-step guidance for common tasks.

About NetIQ Corporation

We are a global, enterprise software company, with a focus on the three persistent challenges in your environment: Change, complexity and risk—and how we can help you control them.

Our Viewpoint

Adapting to change and managing complexity and risk are nothing new

In fact, of all the challenges you face, these are perhaps the most prominent variables that deny you the control you need to securely measure, monitor, and manage your physical, virtual, and cloud computing environments.

Enabling critical business services, better and faster

We believe that providing as much control as possible to IT organizations is the only way to enable timelier and cost effective delivery of services. Persistent pressures like change and complexity will only continue to increase as organizations continue to change and the technologies needed to manage them become inherently more complex.

Our Philosophy

Selling intelligent solutions, not just software

In order to provide reliable control, we first make sure we understand the real-world scenarios in which IT organizations like yours operate — day in and day out. That's the only way we can develop practical, intelligent IT solutions that successfully yield proven, measurable results. And that's so much more rewarding than simply selling software.

Driving your success is our passion

We place your success at the heart of how we do business. From product inception to deployment, we understand that you need IT solutions that work well and integrate seamlessly with your existing investments; you need ongoing support and training post-deployment; and you need someone that is truly easy to work with — for a change. Ultimately, when you succeed, we all succeed.

Our Solutions

- Identity & Access Governance
- Access Management
- Security Management
- Systems & Application Management
- Workload Management
- Service Management

Contacting Sales Support

For questions about products, pricing, and capabilities, contact your local partner. If you cannot contact your partner, contact our Sales Support team.

Worldwide:	www.netiq.com/about_netiq/officelocations.asp
United States and Canada:	1-888-323-6768
Email:	info@netiq.com
Web Site:	www.netiq.com

Contacting Technical Support

For specific product issues, contact our Technical Support team.

Worldwide:	www.netiq.com/support/contactinfo.asp
North and South America:	1-713-418-5555
Europe, Middle East, and Africa:	+353 (0) 91-782 677
Email:	support@netiq.com
Web Site:	www.netiq.com/support

Contacting Documentation Support

Our goal is to provide documentation that meets your needs. If you have suggestions for improvements, click **Add Comment** at the bottom of any page in the HTML versions of the documentation posted at www.netiq.com/documentation. You can also email Documentation-Feedback@netiq.com. We value your input and look forward to hearing from you.

Contacting the Online User Community

Qmunity, the NetIQ online community, is a collaborative network connecting you to your peers and NetIQ experts. By providing more immediate information, useful links to helpful resources, and access to NetIQ experts, Qmunity helps ensure you are mastering the knowledge you need to realize the full potential of IT investments upon which you rely. For more information, visit http://community.netiq.com.

1 Configuring the SAML 2.0 Connector for ADFS

The SAML 2.0 Connector for ADFS provides single sign-on capabilities to Active Directory Federation Services (ADFS) through SocialAccess. The SAML 2.0 Connector for ADFS allows customers to access resources in ADFS while authentication and access is controlled through their local identity store.

1.1 Requirements

Verify that you meet the following requirements before you start configuring the connector:

- ❒ An ADFS 2.0 system installed and configured
- ❒ The metadata file from the ADFS 2.0 system.

  `https://adfsserver/FederationMetadata/2007-06/FederationMetadata.xml`
- ❒ A SocialAccess 1.0 or later system installed and configured

1.2 Configuring the Connector

You must configure the connector to work with your ADFS system.

To configure the SAML 2.0 Connector for ADFS:

1. Log in to the Admin page at `https://dns_appliance/appliance/index.html`.
2. Drag and drop the SAML 2.0 Connector for ADFS to the bar.
3. Click the SAML 2.0 Connector for ADFS, then click **Configure**.
4. Use the following information to configure the new SAML 2.0 Connector for ADFS:

   Display name: Specify a unique name for the SAML 2.0 Connector for ADFS so you can identify this connector on the Admin page.

   Assertion Consumer Service URL: In the ADFS metadata file, find the value in the **AssertionConsumerService** field with the HTTP-POST binding and copy the value into this field.

EntityID: In the ADFS metadata file, find the value in the **entityID** field and copy the value into this field.

Logout URL: In the ADFS metadata file, find the value in the **SingleLogoutService Location** field with the HTTP-POST binding and copy the value into this field.

Signing Certificate: (Optional) Browse to and select an SSL certificate if you want secure communication to ADFS.

Assertion Attribute Mappings: Select **NameID** from the list for the LDAP attribute which contains the users name identifier in the ADFS system.

5 Click **OK**, then click **Apply**.

6 Proceed to Section 1.3, "Configuring ADFS," on page 10.

1.3 Configuring ADFS

After configuring the connector, you must configure single sign-on SAML 2.0 federation with ADFS and SocialAccess.

To configure single sign-on for ADFS:

1 In SocialAccess, obtain the required information to configure ADFS:

- **1a** On the Admin page, click the SAML 2.0 Connector for ADFS.
- **1b** Click **Configure**.
- **1c** Expand the Federation Instructions, then copy and paste the instructions into a text file to use during the ADFS configuration.

2 Configure the SAML 2.0 settings in ADFS 2.0:

- **2a** Start the ADFS 2.0 Management Console.
- **2b** In the left pane, click **ADFS 2.0** > **Trust Relationships** > **Claims Provider Trusts**.
- **2c** Right-click and select **Add Claims Provider Trust**.
- **2d** Click **Start** on the Welcome page.
- **2e** Select **Enter claims provider trust data manually**, then click **Next**.
- **2f** Specify a display name for the claims provider, then click **Next**.
- **2g** Select **ADFS 2.0 Profile**, then click **Next**.
- **2h** Select **Enable support for the SAML 2.0 WebSSO protocol**.
- **2i** Copy and paste the Single Sign-on URL value from the Federation Instructions into the **Claims provider SAML 2.0 SSO service URL** field, then click **Next**.
- **2j** Copy and past the Entity ID value from the Federation Instructions into the **Claims provider trust identifier** field, then click **Next**.
- **2k** Add the certificate file you created from the instructions, then click **Next**.
- **2l** In the Ready to Add Trust step, click **Next**.
- **2m** Click **Close** to finish the process.
- **2n** Right-click on the newly created trust, then select **Properties**.
- **2o** Click the **Advanced** tab, then change the **Secure hash algorithm** to **SHA-1**.
- **2p** Click the **Endpoints** tab, select the SAML Single Sign-on Endpoint, then click **Edit.**

2q Change the **Binding** to POST.

2r Add the **SAML Logout** endpoint with a Binding of POST and the URL found in the Federation Instructions then click **OK**.

3 Proceed to Section 1.4, "Logging into ADFS," on page 11.

If certificate chain errors occur when using a self-signed certificate, run the following PowerShell command:

```
Set-ADFSClaimsProviderTrust -TargetName Display Name from above -
SigningCertificateRevocationCheck None
```

1.4 Logging into ADFS

Use the following information to create links for the end users to use when logging into ADFS while also authenticating to the identity source.

1.4.1 Configuring Service Provider-Initiated Logins

A service provider (SP) initiated login allows users to start the login process at the service provider or in this case, at ADFS.

1. The user accesses the SP-initiated URL you provide:

   `https://ADFS_DNS/adfs/ls/IDPInitiatedSignon.aspx`
2. SocialAccess redirects the login back to the appliance.
3. At the login screen, the user logs in using the user name and password from the identity source.
4. SocialAccess redirects the login back to ADFS.
5. The user is authenticated to both the identity source and ADFS at this point.

You must provide a link to the SP-initiated login URL for users to access:

`https://ADFS_DNS/adfs/ls/IDPInitiatedSignon.aspx`

You can also copy the auto-generated URL on each icon to provide as a link for users.

1.4.2 Configuring Identity Provider-Initiated Logins

An identity provider (IdP) initiated login allows users to start the login process at the identity provider or in this case, at the appliance.

1. The user accesses the IdP-initiated URL you provide:

   `https://appliance_DNS/osp/a/t1/auth/app/login`
2. The login page displays different authentication cards for each application configured to work with the appliance.
3. The user clicks the card for ADFS, then logs in using the user name and password from the identity source.
4. SocialAccess redirects the login to ADFS.
5. The user is authenticated to both the identity source and ADFS at this point.

You must provide a link to the IdP-initiated login URL for the end users to access:

`https://appliance_DNS/osp/a/t1/auth/app/login`

You can also copy the auto-generated URL on each icon to provide as a link for users.

1.5 Connecting to SharePoint

With additional configuration, the SAML 2.0 Connector for ADFS allows users log in to SharePoint as well as ADFS using single sign-on.

1.5.1 Requirements

Verify that you meet the following requirements:

- ❒ Two roles in the of USER and ADMIN.
- ❒ One server with the following components installed:
  - ❒ Windows Server 2008 with the latest updates.
  - ❒ Active Directory with the latest updates.
  - ❒ ADFS 2.0 with the latest updates.
  - ❒ The SharePoint 2010 server connected to the ADFS server. Follow these instructions to connect the servers: How to Configure ADFS v 2.0 in SharePoint Server 2010 (http://technet.microsoft.com/en-us/library/hh305235%28v=office.14%29.aspx).
- ❒ Roles enabled within the SharePoint system using PowerShell scripts.
- ❒ A SocialAccess 1.0 system installed and configured.

1.5.2 Modifying the SAML 2.0 Connector for ADFS Definition

You must modify the SAML 2.0 Connector for ADFS definition file.

1. Obtain a copy of the SAML 2.0 Connector for ADFS.
2. Import the connector file into the Access Connector Toolkit.
3. Click the **Assertions** tab, then on the left side of the screen, click the **Attributes** tab.
4. Click **New,** then use the following information to populate the form:

   Name: Specify `http://schemas.microsoft.com/ws/2008/06/identity/claims/role`.

   Display Name: Specify `Role`.

Data Owner: Leave this field blank.

Required: Select **false** to make this attribute optional.

Description: Specify `A role assigned to the user account.`

Role Attribute: Select **true**, then use the following information to create the role attributes:

4a Click **New**.

4b In the **Name** field, specify `ADMIN,` then in the **Description** field, specify `Administrator Role`.

4c Click **Save**.

4d Click New again.

4e In the **Name** filed specify `USER`, then in the **Description** field specify `User Role`.

4f Click **Save**.

4g Add or customize any additional roles that you need for the SharePoint environment.

4h Click **Save**.

5 Click **Save** twice.

6 On the toolbar of the **Connector Definitions** panel, click **Export**.

7 Proceed to Section 1.5.3, "Importing the Modified Connector," on page 13.

1.5.3 Importing the Modified Connector

After modifying the SAML 2.0 Connector for ADFS, you must import and configure the connector.

1 Log in to the Admin page at `https://`*`dns_of_appliance`*`/appliance/index.html` as an appliance administrator.

2 Click the **Admin** icon on the toolbar.

3 Click the **Tools** icon on the toolbar, then click **Import Connector Definition**.

4 Click **Browse,** then browse to and select the SAML 2.0 Connector for ADFS ZIP file that you exported.

5 Click **Import**.

The Applications palette displays the SAML 2.0 Connector for ADFS.

6 Proceed to Section 1.5.4, "Configuring the Modified Connector," on page 13.

1.5.4 Configuring the Modified Connector

After exporting and importing the modified connector, you must configure the connector. You configure the connector as if it is a regular connector by following the steps in Section 1.2, "Configuring the Connector," on page 9.

After you configure a SAML 2.0 Connector for ADFS that supports SharePoint roles, you must modify ADFS and SharePoint to accept these roles. Proceed to Section 1.5.5, "Modifying Claim Rules in the ADFS System," on page 14.

1.5.5 Modifying Claim Rules in the ADFS System

You must modify the ADFS claim rules between ADFS and SocialAccess.

To modify the claim rules:

1. Log in to your ADFS system.
2. Access the **Claims Provider Trusts** for SocialAccess.
3. Click **Edit Claim Rules**.
4. Add two rules using the following information:
   - Rule 1
     - **Claim rule template:** Select **Pass Through or Filter an Incoming Claim**.
     - **Claim rule name:** Specify `pass nameID`.
     - **Incoming claim type:** Specify `Name ID`.
     - **Incoming name ID format:** Specify `Email`.
     - **Pass through all claim values:** Select this option.
   - Rule 2
     - **Claim rule template:** Select **Pass Through or Filter an Incoming Claim**.
     - **Claim rule name:** Specify `pass Roles`.
     - **Incoming claim type:** Specify `Roles`.
     - **Pass through all claim values:** Select this option.
5. Exit the Rule editor.
6. Proceed to Section 1.5.6, "Configuring ADFS to Send SharePoint the Claim Rules," on page 14

1.5.6 Configuring ADFS to Send SharePoint the Claim Rules

The follow steps map Email Address to Login on the SharePoint system. You only have to perform these steps once.

1. Within the ADFS 2.0 console, select **Trust Relationships** > **Relying Party Trusts** > *Name of your SharePoint system*.
2. Right-click, then select **Edit Claim Rules**.
3. Create two rules with the following information:
   - Rule 1
     - **Claim rule template:** Select **Transform an Incoming Claim**.
     - **Claim rule name:** Specify `NameID to EmailAddress`.
     - **Incoming claim type:** Specify `Name ID`.
     - **Incoming name ID format:** Specify `Email`.
     - **Outgoing claim type:** Specify `E-mail Address`.
     - **Pass through all claim values:** Select this option.
   - Rule 2
     - **Claim rule template:** Select **Pass Through or Filter an Incoming Claim**.
     - **Claim rule name:** Specify `pass Roles`.
     - **Incoming claim type:** Specify `Roles`.

- **Pass through all claim values:** Select this option.

4 Exit the Rule editor.

5 Proceed to Section 1.5.7, “Configuring People Picker to Specify the Roles,” on page 15

1.5.7 Configuring People Picker to Specify the Roles

After completing the ADFS configuration, you must configure the SharePoint 2010 option of **People Picker**.

1 Where the SharePoint 2010 system grants access, select **People Picker**.

2 Under **ADFS**, select **Role**.

3 In the **Find** box, specify either `ADMIN` or `USER`.

This field must contain the name of the role you configure the connector to use in Section 1.5.2, “Modifying the SAML 2.0 Connector for ADFS Definition,” on page 12.

4 Select the role SharePoint returns, then assign the role to the group within SharePoint.

1.5.8 Troubleshooting

Use the following information if you encounter problems.

Issue: Error: The root of the certificate chain is not a trusted root authority.

Solution: You need to change the SharePoint server certificates. For detailed instructions, see Root Certificate Chain not Trusted (http://blogs.technet.com/b/speschka/archive/2010/02/13/root-of-certificate-chain-not-trusted-error-with-claims-authentication.aspx).