NetIQ® SocialAccess

Connector 1.6 for NetIQ Access Manager™ Guide

January 2013

Legal Notice

Contents

About this Book and the Library

The *NetIQ® SocialAccess Connector for NetIQ Access Manager™ Guide* provides installation and configuration information for the Connector for NetIQ Access Manager.

Intended Audience

This guide provides information for SocialAccess administrators who are responsible for configuring and managing the Connector for NetIQ Access Manager.

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

NetIQ, an Attachmate business, is a global leader in systems and security management. With more than 12,000 customers in over 60 countries, NetIQ solutions maximize technology investments and enable IT process improvements to achieve measurable cost savings. The company's portfolio includes award-winning management products for IT Process Automation, Systems Management, Security Management, Configuration Audit and Control, Enterprise Administration, and Unified Communications Management. For more information, please visit www.netiq.com.

Contacting Sales Support

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

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

Contacting Technical Support

For specific product issues, please 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, please visit http://community.netiq.com.

1 Configuring the Connector for Access Manager

The Connector for Access Manager provides single sign-on capabilities to Access Manager through SocialAccess. The Connector for Access Manager allows customers to access resources through Access Manager while authentication and access are controlled locally through their enterprise LDAP servers.

1.1 Requirements

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

- ❒ An Access Manager system installed and configured.
- ❒ The metadata file from your Access Manager system.

`https://<nam_server>/nidp/saml2/metadata`

- ❒ Access Manager user accounts for each user that wants the single sign-on service.
- ❒ A SocialAccess 1.0 system installed and configured.

1.2 Configuring the Connector

You must configure the connector to work with your Access Manager system.

To configure the Connector for Access Manager:

1. Log in to the Admin page at `https://dns_name/appliance/Admin.html`.
2. Drag and drop the Connector for Access Manager to the bar, then click **Configure**.
3. Use the following information to configure the new Connector for Access Manager:

   NOTE: The information from the metadata file is case sensitive. You must enter the information exactly as it appears in the metadata file.

   Display name: Specify a display name for the connector. This name should be unique so you can identify this connector in the Admin page.

   Assertion Consumer Service URL: Specify the value in the **AssertionConsumerService** field with the HTTP-POST bindings in the Access Manager metadata file.

Destination URL: (Optional) Specify the URL where users go after initial login.

Entity ID: Specify the value in the **entityID** field in the Access Manager metadata file.

Logout Response URL: Specify the value in the **SingleLogoutService ResponseLocation** field with the HTTP-POST binding in the Access Manager metadata file.

Logout URL: Specify the value in the **SingleLogoutService Location** field with the HTTP-POST binding in the Access Manager metadata file.

Assertion Attribute Mappings: Select **Email** from the list for the Subject/NameID attribute.

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

5 Proceed to Section 1.3, "Configuring Access Manager," on page 10.

1.3 Configuring Access Manager

After configuring the connector, you must configure single sign-on SAML 2.0 federation between Access Manager and SocialAccess.

1 In SocialAccess, obtain the required information to configure Access Manager:

1a On the Admin page, click the Connector for Access Manager.

1b Click **Configure**.

1c Expand the Federation Instructions, then copy and paste the instructions into a text file to use during the Access Manager configuration.

NOTE: You must use a text editor that does not introduce hard returns or additional white space. For example, use Notepad instead of Wordpad.

---

2 Create a new Identity Provider for the appliancein Access Manager:

2a Log in to the Access Manager Administration Console.

2b Click **Devices** > **Identity Servers** > **ClusterName** > **SAML 2.0**.

2c Click **New**, then select **Identity Provider**.

2d Use the following information to configure the Identity Provider:

Name: Specify the name of your appliance .

Source: Select **Metadata Text** in the list as the source, then open the Identity Broker metadata file in a browser. The URL is `https://appliance:443/osp/a/t1/auth/saml2/metadata`. Copy and paste the entry in the metadata file for Access Manager into the **Metadata Text** field.

or

Select **Metadata URL** in the list as the source, then copy the metadata URL. The URL is `https://appliance:443/osp/a/t1/auth/saml2/metadata`.

2e Click **Next**, then view the signing certificate of the Identity Broker.

2f Click **Finish** to save the configuration.

3 Configure the new Identity Provider you just created:

3a Click the new Identity Provider, then click the **Authentication Card** > **Authentication Request**.

3b Use the following information to configure the Identity Provider:

Name Identifier Format: Select **Transient**.

Options > Response protocol binders: Select **Post** from the list.

3c Click **OK** to save the changes.

4 Make any additional changes you require.

5 Import the certificate from the Connector for Access Manager:

5a Click **Security** > **Trusted Roots**, then click **Import**.

5b Use the following information to import the certificate:

Name: Specify the name as *appliance_name*_signing_cert.

Certificate data file: Copy and paste the certificate information from the text file you created in the first step of this procedure.

NOTE: You must use a text editor that does not introduce hard returns or additional white space. For example, use Notepad instead of Wordpad.

5c Click **OK** to import the certificate.

6 Add the certificate to the trust store:

6a Click **Add Trusted Roots to Trust Store**.

6b In the **Trust stores** field, click **Edit**.

6c Select **Trust Store for NIDP** and **OSCP Trust Store**.

6d Click **OK** twice to save the changes.

7 Update the Identity Provider:

7a Click **Devices**, then click your Identity Provider.

7b Click **Update All**, then click **OK**.

7c Wait for Access Manager to process the new configuration.

8 Log out of Access Manager.

9 Proceed to Section 1.4, “Logging in to Access Manager,” on page 11.

1.4 Logging in to Access Manager

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

1.4.1 Configuring Service Provider-Initiated Logins

A login initiated by the service provider (SP) allows users to start the login process at the service provider or, in this case, at Access Manager. The user must have an account in the identity source and in Access Manager for single sign-on to work.

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

   `https://Access_Manager_DNS_Name:8443/nidp`

2. SocialAccess redirects the login back to the appliance.
3. At the login screen, the user logs in using the user account and password from the identity source.

4. SocialAccess redirects the login back to Access Manager.
5. The user is authenticated to both the identity source and Access Manager at this point.

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

`https://Access_Manager_DNS_Name:8443/nidp`

1.4.2 Configuring Identity Provider-Initiated Logins

A login initiated by the identity provider (IdP) 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 login 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 Access Manager, then logs in using the user account and password from the identity source.
4. SocialAccess redirects the login back to Access Manager.
5. The user is authenticated to both the identity source and Access Manager at this point.

You must provide a link to the IdP-initiated login URL for 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 the user.