NetIQ Access Connector Toolkit

Creating a Custom Connector

January 2013

This document provides information about implementing and using the NetIQ® Access Connector Toolkit.

This document is intended for NetIQ partners and people who know and understand SAML 2.0.

Contents

Overview

The Access Connector Toolkit allows you to create custom connectors for NetIQ CloudAccess. You must configure a connector for each Web service that uses CloudAccess as a trusted identity provider. A connector's most fundamental function is to aid in establishing federation, for single sign-on and logout, between CloudAccess and the Web service.

The custom connectors you create in the Access Connector Toolkit work in CloudAccess without any modifications to the connector.

Product Requirements

The Access Connector Toolkit is a stand alone Web application. The only requirement is that it only runs in a Windows environment.

Implementation Overview

The following table provides an overview of tasks to use the Access Connector Toolkit.

Steps	For more information, see…
Download the Access Connector Toolkit	“Downloading the Access Connector Toolkit” on page 3
Launch the Access Connector Toolkit	“Launching the Access Connector Toolkit” on page 3
Meet the Web service or application requirements	“Meeting the Web Service or Application Requirements” on page 3
Create a custom SAML connector definition	“Creating a Custom SAML Connector Definition” on page 4
Export the connector definition	“Exporting the Connector Definition” on page 7
Import and configure the connector	“Importing and Configuring the Connector” on page 7

Downloading the Access Connector Toolkit

The Access Connector Toolkit is a stand alone Web application. You download the Access Connector Toolkit from the Customer Center (http://www.novell.com/center).

Launching the Access Connector Toolkit

The Access Connector Toolkit is a self-contained Web application. To launch the Access Connector Toolkit:

1. After you download the Access Connector Toolkit, unzip the file to a local directory.
2. Run `actoolkit/bin/acKit.bat` to launch the application.

Meeting the Web Service or Application Requirements

The Access Connector Toolkit allows you to create custom connectors for SAML 2.0.

In order to create a custom SAML 2.0 connector, the application or the Web service that connects to CloudAccess must meet the following requirements:

- ❒ The Web service supports SAML 2.0 identity federation.

  For more information about SAML, see the OASIS Web site (http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security).

- ❒ The Web service supports a SAML Web browser single sign-on profile, specifically with Redirect/POST bindings for service-provider-initiated SSO, and POST binding for identity-provider-initiated SSO.
- ❒ The Web service must provide a way for the customer to configure the federation; this usually means providing a facility in the application's administration console that allows the customer to enable and configure SAML SSO.
- ❒ The Web service or application must have technical documents that describe what it requires for the following:
  - ❒ **SAML Assertions:** The document needs to describe the attributes that are required for authentication, such as the user's name or email address. It can include the attributes that are required to assign roles. If possible, obtain a SAML assertion from the application.
  - ❒ **Federation Requirements:** The document needs to describe what is required for federation. It should require an Identity Broker certificate, which allows the application to set the trusted relationship with the Identity Broker. The document should also include URLs for logging in and logging out.
  - ❒ **SAML Metadata:** The application sends SAML metadata to the Identity Broker in order to establish communication. This usually includes a login URL or a customer-specific domain name. Applications that support SAML should publish a SAML metadata document that describes their service. This document is often available from a public URL. If possible, get this document.

Ask the Web service or application vendors the following types of questions to gather the required information:

- What does your SAML assertion look like?
- Do you have a SAML metadata document? What fields, if any, are customer-specific?
- Does your service support the SAML single logout protocol?
- What configuration steps are required in your application to set up federation?
- What is the information that they provide to customers when they are setting up federation with their LDAP server?

Creating a Custom SAML Connector Definition

A SAML connector definition consists of multiple components. The Access Connector Toolkit allows you to create the components in one place.

To create a custom SAML connector definition:

1. Verify that you have gathered the Web service or application requirements listed in "Meeting the Web Service or Application Requirements" on page 3.
2. Launch the Access Connector Toolkit. For more information, see "Launching the Access Connector Toolkit" on page 3.
3. Click **New** > **SAML2**.
4. Create the connector definition. For detailed information, see "Creating the Connector Definition" on page 5.
5. Create the metadata. For detailed information, see "Creating the Metadata" on page 5.
6. Create the assertions. For detailed information, see "Creating the Assertion" on page 6.
7. (Optional) Create the provisioning definitions. For detailed information, see "Creating the Provisioning Definition" on page 7.

8 Click **Save** to save the new connector definition.

9 Proceed to "Exporting the Connector Definition" on page 7 to complete the creation of the new connector.

Creating the Connector Definition

You must import a connector definition into CloudAccess for the connector to work. The Access Connector Toolkit helps you create a connector definition.

Table 1 *Connector Definition Fields*

Field	Description	Action
Type	Defines the type of connector for CloudAccess. You cannot change the value of this field. It is set when you select the type of connector to create. For example: SAML2	
Type Name	Defines the type name of the connector for CloudAccess. You cannot change the value of this field. It is set when you select the type of connector to create. For example Generic SAML2 Connector	
Target Name	The target name is the name of the connector definition file.	Specify a unique name for the connector definition file.
Icon	Allows you to uses a custom graphic for your new connector.	Browse to and select a graphic that you want as the icon for the new connector.
Description for Provider	CloudAccess does not use this field.	
Description for Customer	Provide enough information so that the CloudAccess administrator knows what the connector does.	Specify a description that CloudAccess displays in the Admin page.
Settings > Federation Instructions	CloudAccess displays the Federation Instructions in when the administrator configures the connector.	Edit the default federation instructions for your connector. You must add information that is specific to your CloudAccess appliance.
Settings > New Settings	A setting provides a way for the CloudAccess administrators to input data when creating the connector.	Create a setting for your connector. ◆ Customer specific sections of the Assertion Consumer Service URL. ◆ Connector specific setting; for example, a Customer Domain.

Creating the Metadata

The metadata is the configuration information the Web service or application uses to communicate to CloudAccess. Some Web services and applications allow you to export the required metadata in to an XML file or it is contained in a URL provided by the Web service or application. You can either import the XML file or enter the required information.

Table 2 *Metadata Fields*

Field	Description	Example
EntityID	Select whether the entity ID comes from the federation instructions or if it comes from the new setting you created when you created the connector definition. EntityID is a field from the metadata that uniquely identifies that particular service provider.	google.com
Assertion Consumer Service URL	Select whether the Assertion Consumer Service URL comes from the federation instructions or if it comes from the new setting you created when you created the connector definition. The Assertion Consumer Service URL is a field from the metadata where the Assertion is posted by the browser.	https://www.google.com/a/${customer-domain}/acs
Logout URL	(Optional) Specify a logout URL. The logout URL corresponds to the field SingleLogoutService from the metadata.	
Logout Response URL	(Optional) Specify a logout response URL. The logout response URL is required when the SingleLogoutService field has ResponseLocation specified in the metadata.	The Connector for Access Manager requires this field.
NameID Format	Specify the format of the NameID from the metadata. The NameID format field in the metadata tells CloudAccess what NameID formats the service provider supports.	
Signing Certificate	Browse to and select a certificate to provide secure communication between the service provider and CloudAccess.	
Import from a file	You can import the metadata from a file or from a URL.	
Import from URL	You can import the metadata from a file or from a URL.	

Creating the Assertion

The assertion is a package of information that supplies statements made by the identity source.

Table 3 *Assertion Fields*

Fields	Description	Example
Audience Restriction	(Optional) Audience Restriction is a field in the SAML Assertion that defines the recipient of the Assertion. Usually this is the same value as the EntityID, and if you leave the field blank the EntityID value is used for this field.	google.com
NameID	The NameID field in the SAML Assertion defines what the service provider receives.	
Format	The NameID format is an email address or it is unspecified. It depends on the requirements of the connected system as to which format you use.	
Destination URL	(Optional) The Destination URL is where the end user ends up after CloudAccess logs in with the URL provided on the connector configuration page.	
Protocol Binding	The only binding currently supported is POST.	

Creating the Provisioning Definition

Provisioning is only supported through connectors created by NetIQ. As this time, you cannot create a connector definition that supports provisioning user accounts to the connected system.

Exporting the Connector Definition

After you create the connector definition, you must export the connector definition. The first step, when creating a connector, is to import the connector definition. Exporting the connector definition creates a file you can use in CloudAccess.

To export the connector definition:

1. Launch the Access Connector Toolkit.
2. Highlight the connector definition you created, then click **Export**.
3. Save the ZIP file for use in CloudAccess.

Importing and Configuring the Connector

After you create the connector definition, you must import the connector in the Access Gateway products and configure the connector. The steps to configure the connector are determined by the information you added to the connector definition and by which Access Gateway product you use.

For more information about importing and configuring the connectors, see “Importing and Configuring Custom Connectors”in the *NetIQ CloudAccess Installation and Configuration Guide* (https://www.netiq.com/documentation/cloudaccess/install_config/data/bookinfo.html).

Known Issue

No Time out Feature: After you launch the Access Connector Toolkit, it does not time out your session. You must close your browser to end the session.

WS-Federation Not Supported: This release of the Access Connector Toolkit does not support the WS-Federation option when you create a custom connector.