NetIQ® CloudAccess

Connector 1.5 for Salesforce Guide

January 2013

Legal Notice

Contents

About this Book and the Library

The *NetIQ® CloudAccess Connector for Salesforce Guide* provides installation and configuration information for the Connector for Salesforce.

Intended Audience

This guide provides information intended for CloudAccess administrators who are responsible for configuring and managing the Connector for Salesforce.

Other Information in the Library

The library provides the following information resources:

Installation and Configuration Guide

Provides installation and configuration instructions for CloudAccess.

Connector Guides

Provide detailed installation and configuration information for each connector available with CloudAccess.

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 Installing and Configuring the Connector for Salesforce

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

The following documentation is only for the single sign-on Connector for Salesforce. This is a different connector from the Connector for Salesforce that is embedded in the CloudAccess appliance. Use the connector when you need only single sign-on capabilities. If you need provisioning, account management, and single sign-on capabilities, use the embedded connector. For more information about the embedded Connector for Salesforce, see the *NetIQ CloudAccess Installation and Configuration Guide* (https://www.netiq.com/documentation/cloudaccess/install_config/data/bookinfo.html).

1.1 Requirements

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

- ❒ A Salesforce account to enable the Connector for Salesforce. To set up a free developer account for a testing environment, see Developer Force (http://developer.force.com/), then click **Join Now.**
- ❒ A Salesforce account for each user who wants to access Salesforce.
- ❒ The Salesforce email address stored as an attribute on the users in the identity source. This can be the LDAP mail attribute, or another attribute of your choice.
- ❒ A CloudAccess 1.1 system installed and configured.

1.2 Downloading the Connector

You must download the Connector for Salesforce from the Access Connectors HQ Web site at https://www.netiq.com/products/accessconnectorhq/index.html (https://www.netiq.com/products/accessconnectorhq/index.html). The Connector for Salesforce is not included with CloudAccess.

After you have downloaded the connector, proceed to Section 1.3, "Importing the Connector," on page 10.

1.3 Importing the Connector

After downloading the connector, you must import the connector into CloudAccess in order to use the connector.

To import the connector:

1. Unzip the downloaded connector archive.
2. Log in to the Admin page at `https://dns_of_appliance/appliance/index.html` as an appliance administrator.
3. Click the **Admin** icon on the toolbar.
4. Click the **Tools** icon on the toolbar, then click **Import Connector Definition**.
5. Click **Browse,** then browse to and select the Connector for Salesforce ZIP file that was extracted above.
6. Click **Import**.

   The Applications palette displays the Connector for Salesforce.
7. Proceed to Section 1.4, "Configuring the Connector," on page 10.

1.4 Configuring the Connector

After importing the connector, you must configure the connector to work with Salesforce.

1. Log in to the CloudAccess appliance at `https://dns_of_appliance/appliance/index.html` as an appliance administrator, then access the Admin page.
2. Drag and drop the Connector for Salesforce to the bar, then click **Configure**.
3. Use the following information to configure the new Connector for Salesforce:

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

   Login URL: Specify the **Salesforce.com Login URL** obtained from the Single Sign-On Settings page in the Salesforce account.

   Signing certificate: Browse to and select the Salesforce signing certificate.

   You obtain the certificate by downloading the Salesforce metadata (on the Salesforce Single Sign-On Settings page click **Download Metadata**). The metadata contains the signing certificate. To import that certificate into the connector configuration, you must copy the certificate from the metadata, then manually format and save the certificate in `.pem` or similar format.

   Assertion Attribute Mappings: Select the attribute used to store the user's Salesforce ID in the identity source, which is usually the user's email attribute. This value also can be the LDAP **mail** attribute.

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

5 Proceed to Section 1.5, "Configuring Salesforce for Single Sign-On," on page 11.

1.5 Configuring Salesforce for Single Sign-On

After configuring the connector, you must configure single sign-on (SSO) SAML 2.0 federation between Salesforce and CloudAccess.

To configure Salesforce for single sign-on:

1 In CloudAccess, obtain the required information to configure Salesforce:

1a On the Admin page, click the Connector for Salesforce.

1b Click **Configure**.

1c Expand the Federation Instructions, then copy and paste the instructions into a text file to use during the Salesforce 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 From the Federation Instructions, use the following steps to create a signing certificate:

2a In the Federation Instructions, copy the text between the following tags:

```
-----BEGIN CERTIFICATE-----
-----END CERTIFICATE-----
```

Ensure that you copy the beginning and ending hyphens in the tags.

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

2b Paste the certificate information into a text file.

2c Save the file with a `.pem` extension.

3 Open a browser, enter the URL of the Salesforce account, then log in as the administrator.

4 In the menu bar, by your name, click **Setup**.

5 In the **Administration Setup** section, expand **Security Controls**.

6 Click **Single Sign-On Settings** > **Edit**.

7 Configure the SAML settings as follows:

SAML Enabled: Select this option.

SAML Version: Select **2.0**.

Issuer: Paste the Entity ID (Issuer) URL that you obtained from the Federation Instructions.

Identity Provider Certificate: Browse to the location of the certificate you created from the Federation Instructions and upload it.

Identity Provider Login URL: Paste the Single Sign-on URL that you obtained from the Federation Instructions.

Custom Error URL: Leave this option unconfigured.

SAML User ID Type: Select **Assertion contains User's salesforce.com username**.

SAML User ID Location: Select **User ID is in the NameIdentifier element of the Subject statement**.

Entity Id: Select **https://saml.salesforce.com/**.

Service Provider Initiated Request Binding: Select **HTTP POST**.

Identity Provider Logout URL: Paste the Single Logout URL that you obtained from the Federation Instructions.

8. Click **Save**.
9. To verify that the configuration is valid, continue with "Logging in to Salesforce" on page 12.

1.6 Logging in to Salesforce

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

1.6.1 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 Salesforce. You can find the Salesforce SP-initiated login URL on the Salesforce administration page under **Setup** > **Company Profile** > **My Domain**.

The user must have an account in the identity source and in Salesforce for single sign-on to work.

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

   `https://custom_name.my.salesforce.com`
2. CloudAccess 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. CloudAccess redirects the login back to Salesforce.
5. The user is authenticated to both the identity source and Salesforce at this point.

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

`https://custom_name.my.salesforce.com`

1.6.2 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 Salesforce, then logs in using the user account and password from the identity source.
4. CloudAccess redirects the login back to Salesforce.
5. The user is authenticated to both the identity source and Salesforce 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 users.