

NetIQ[®] CloudAccess

Connector 1.0 for Accellion

January 2013



Legal Notice

THIS DOCUMENT AND THE SOFTWARE DESCRIBED IN THIS DOCUMENT ARE FURNISHED UNDER AND ARE SUBJECT TO THE TERMS OF A LICENSE AGREEMENT OR A NON-DISCLOSURE AGREEMENT. EXCEPT AS EXPRESSLY SET FORTH IN SUCH LICENSE AGREEMENT OR NON-DISCLOSURE AGREEMENT, NETIQ CORPORATION PROVIDES THIS DOCUMENT AND THE SOFTWARE DESCRIBED IN THIS DOCUMENT "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. SOME STATES DO NOT ALLOW DISCLAIMERS OF EXPRESS OR IMPLIED WARRANTIES IN CERTAIN TRANSACTIONS; THEREFORE, THIS STATEMENT MAY NOT APPLY TO YOU.

For purposes of clarity, any module, adapter or other similar material ("Module") is licensed under the terms and conditions of the End User License Agreement for the applicable version of the NetIQ product or software to which it relates or interoperates with, and by accessing, copying or using a Module you agree to be bound by such terms. If you do not agree to the terms of the End User License Agreement you are not authorized to use, access or copy a Module and you must destroy all copies of the Module and contact NetIQ for further instructions.

This document and the software described in this document may not be lent, sold, or given away without the prior written permission of NetIQ Corporation, except as otherwise permitted by law. Except as expressly set forth in such license agreement or non-disclosure agreement, no part of this document or the software described in this document may be reproduced, stored in a retrieval system, or transmitted in any form or by any means, electronic, mechanical, or otherwise, without the prior written consent of NetIQ Corporation. Some companies, names, and data in this document are used for illustration purposes and may not represent real companies, individuals, or data.

This document could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein. These changes may be incorporated in new editions of this document. NetIQ Corporation may make improvements in or changes to the software described in this document at any time.

U.S. Government Restricted Rights: If the software and documentation are being acquired by or on behalf of the U.S. Government or by a U.S. Government prime contractor or subcontractor (at any tier), in accordance with 48 C.F.R. 227.7202-4 (for Department of Defense (DOD) acquisitions) and 48 C.F.R. 2.101 and 12.212 (for non-DOD acquisitions), the government's rights in the software and documentation, including its rights to use, modify, reproduce, release, perform, display or disclose the software or documentation, will be subject in all respects to the commercial license rights and restrictions provided in the license agreement.

© 2013 NetIQ Corporation and its affiliates. All Rights Reserved.

For information about NetIQ trademarks, see <https://www.netiq.com/company/legal/>.

Contents

About this Book and the Library	5
About NetIQ Corporation	7
1 Installing and Configuring the Connector for Accellion	9
1.1 Requirements	9
1.2 Downloading the Connector	9
1.3 Importing the Connector	10
1.4 Configuring the Connector	10
1.5 Configuring Accellion for Single Sign-On	11
1.6 Logging in to Accellion	11
1.6.1 Configuring Service Provider-Initiated Logins	12
1.6.2 Configuring Identity Provider-Initiated Logins	12

About this Book and the Library

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

Intended Audience

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

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 Accellion

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

- ◆ [Section 1.1, “Requirements,” on page 9](#)
- ◆ [Section 1.2, “Downloading the Connector,” on page 9](#)
- ◆ [Section 1.3, “Importing the Connector,” on page 10](#)
- ◆ [Section 1.4, “Configuring the Connector,” on page 10](#)
- ◆ [Section 1.5, “Configuring Accellion for Single Sign-On,” on page 11](#)
- ◆ [Section 1.6, “Logging in to Accellion,” on page 11](#)

1.1 Requirements

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

- An enterprise Accellion account.
To set up a free trial account that expires after 45 days, see the [Accellion Web site \(https://www.accellion.com/pricing\)](https://www.accellion.com/pricing).
- The Accellion domain name and the application ID. The Accellion administrative URL contains both elements.
`http://domain_name.accellion.net/courier/application_id@/index.html`
- Accellion user accounts for each user who wants access to the single sign-on service. The Connector for Accellion does not provision user accounts.
- A CloudAccess 1.1 system installed and configured.

1.2 Downloading the Connector

You must download the Connector for Accellion 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 Accellion 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 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 Connector for Accellion ZIP file.
- 5 Click **Import**.

The Applications palette displays the Connector for Accellion.

- 6 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 Accellion.

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

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

Domain name: Specify the domain name that you received from Accellion when setting up an Accellion enterprise account.

NOTE: Use only the left-most element of the domain name. Do not include the “.accellion.net” portion of the DNS name.

Application ID: Specify the Application ID that you retrieved from the Accellion administrative URL or the API settings page in the Accellion administrative console.

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

Assertion Attribute Mappings: Select the LDAP attribute that stores the user NameID attribute. This value can also be the LDAP **mail** attribute. Also, select **email** from the list for the email attribute.

- 4 Click **OK**, then click **Apply**.
- 5 Proceed to [Section 1.5, “Configuring Accellion for Single Sign-On,” on page 11](#).

1.5 Configuring Accellion for Single Sign-On

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

To configure Accellion for single sign-on:

- 1 In CloudAccess, obtain the required information to configure Accellion:
 - 1a On the Admin page, click the Connector for Accellion.
 - 1b Click **Configure**.
 - 1c Expand the Federation Instructions, then copy and paste the instructions into a text file to use during the Accellion 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 Log in to your Accellion account.
- 3 Click **Administration** to access the SSO settings, then click **Edit**.
- 4 Use the following information to configure SSO for Accellion:

Protocol: Select **SAML 2.0**.

Redirection Criteria: Select this option, then select how you want the redirection to occur.

Show option to login via SSO to the user: Select this option, then select how you want this to happen.

E-Mail Attribute: Specify email for the value of this field.

Single Sign-On Service URL: Specify the following from the Federation Instructions:

`https://appliance/osp/a/t1/auth/saml2/metadata`

Single Logout Service URL: Specify the following from the Federation Instructions:

`https://appliance/osp/a/t1/auth/saml2/slo`

RSA Public Key Certificate: Copy and paste the certificate information from the text file you created in the first step of this procedure to create a certificate to upload.

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

Sign Logout Request: Select **OFF** for this field.

- 5 Click **Submit** to save the changes.
- 6 Proceed to [“Logging in to Accellion”](#) on page 11.

1.6 Logging in to Accellion

The following procedures allow the user to log in to Accellion while also authenticating to the identity source.

- ♦ [Section 1.6.1, “Configuring Service Provider-Initiated Logins,”](#) on page 12
- ♦ [Section 1.6.2, “Configuring Identity Provider-Initiated Logins,”](#) on page 12

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

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

```
https://domain_name.accellion.net/
```

Replace *domain_name* with the domain name of your Accellion account.

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 Accellion.
5. The user is authenticated to both the identity source and Accellion at this point.

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

```
https://domain_name.accellion.net/
```

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 Accellion, then logs in using the user account and password from the identity source.
4. CloudAccess redirects the login back to Accellion.
5. The user is authenticated to both the identity source and Accellion at this point.

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