NetIQ® CloudAccess

Connectors Guide

July 2013

Legal Notice

Contents

About this Book and the Library

The *NetIQ® CloudAccess Connectors Guide* provides installation and configuration information for the connectors that you use with CloudAccess.

Intended Audience

This guide provides information for CloudAccess administrators who are responsible for configuring and managing the connectors used with CloudAccess.

Other Information in the Library

The library provides the following information resources:

Installation and Configuration Guide

Provides installation and configuration instructions for CloudAccess.

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 Downloading and Importing Connectors

The CloudAccess connectors provide single sign-on (SSO) access to various Web services. The connectors enable users to access Web resources through CloudAccess while authentication and access are controlled locally through their enterprise LDAP server.

The connectors that support provisioning are embedded in the appliance. However, you must download the SSO-only connectors from the Access Connectors HQ Web site at https://www.netiq.com/products/accessconnectorhq/index.html (https://www.netiq.com/products/accessconnectorhq/index.html).

After downloading a 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/Admin.html` as an appliance administrator.
2. Click the **Tools** icon on the toolbar, then click **Import Connector Definition**.
3. Click **Browse,** then browse to and select the connector `.zip` file.
4. Click **Import**.

   The Applications palette displays the connector that you imported.
5. Proceed to the configuration instructions for the desired connector.

2 Configuring the Connector for Accellion

The connector for Accellion provides single sign-on access to Accellion through CloudAccess, but does not support provisioning. After importing the connector, you must configure the connector in CloudAccess and you must also configure Accellion to work with the connector.

2.1 Requirements

Verify that you meet the following requirements before you start configuring 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).

- ❒ 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.

2.2 Configuring the Connector

To 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**.

2.3 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 Chapter 12, “Logging into the Web Service,” on page 41.

3 Configuring the Connector for Access Manager

The connector for Access Manager provides single sign-on access to Access Manager through CloudAccess, but does not support provisioning. After importing the connector, you must configure the connector in CloudAccess and you must also configure Access Manager to work with the connector.

3.1 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.

3.2 Configuring the Connector

To configure the connector for Access Manager:

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 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 Access Manager metadata file is case sensitive. You must enter the information exactly as it appears in the metadata file (`https://nam_server:8443/nidp/saml2/metadata`).

   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: 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.

Signing certificate: Browse to and select an SSL certificate to secure communication to Access Manager.

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

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

3.3 Configuring Access Manager

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

1 In CloudAccess, 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 appliance in 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 Chapter 12, "Logging into the Web Service," on page 41.

4 Configuring the SAML 2.0 Connector for ADFS

The SAML 2.0 connector for ADFS provides single sign-on access through CloudAccess, but does not support provisioning. After importing the connector, you must configure the connector in CloudAccess and you must also configure ADFS to work with the connector.

4.1 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`

4.2 Configuring the Connector

To configure the SAML 2.0 connector for ADFS:

1. Log in to the Admin page at `https://dns_of_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**.

4.3 Configuring ADFS

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

To configure single sign-on for ADFS:

1 In CloudAccess, 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**.

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
```

If you do not want to connect to SharePoint, proceed to Chapter 12, “Logging into the Web Service,” on page 41.

4.4 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.

4.4.1 Requirements

Verify that you meet the following requirements:

- ❒ Two roles in the CloudAccess 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.

4.4.2 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 4.4.3, "Importing the Modified Connector," on page 20.

4.4.3 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 4.4.4, "Configuring the Modified Connector," on page 20.

4.4.4 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 4.2, "Configuring the Connector," on page 17.

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 4.4.5, "Modifying Claim Rules in the ADFS System," on page 20.

4.4.5 Modifying Claim Rules in the ADFS System

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

To modify the claim rules:

1 Log in to your ADFS system.

2 Access the **Claims Provider Trusts** for CloudAccess.

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 4.4.6, "Configuring ADFS to Send SharePoint the Claim Rules," on page 21

4.4.6 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 4.4.7, "Configuring People Picker to Specify the Roles," on page 22

4.4.7 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 4.4.2, "Modifying the SAML 2.0 Connector for ADFS Definition," on page 19.
4. Select the role SharePoint returns, then assign the role to the group within SharePoint.

4.4.8 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).

5 Configuring the Connector for Box

The connector for Box provides single sign-on access to Box through CloudAccess, but does not support provisioning. After importing the connector, you must configure the connector in CloudAccess and you must also configure Box to work with the connector.

5.1 Requirements

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

- ❒ An enterprise level Box account. Obtaining an enterprise Box account requires you to provide configuration details for your organization so Box can help set up the SSO connection.
- ❒ A Box user account for each user who wants access to the single sign-on service. The connector for Box does not provision user accounts.

5.2 Configuring the Connector Settings

After importing the connector, you must configure the connector settings in CloudAccess.

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 Box to the bar, then click **Configure**.
3. Use the following information to configure the new connector for Box:

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

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

   Assertion Attribute Mappings: In the **Email** field, select Email from the list for the user's email address. Optionally, also specify the user's first and last name. The First Name and Last Name attributes are used by Box to enable just-in-time provisioning, if it is enabled on the Box side.
4. Click **OK**, then click **Apply**.

5.3 Configuring the Box Connector for Single Sign-On

Once you have configured the connector in CloudAccess single sign-on (SSO) SAML 2.0 federation must be set up between Box and the Federation Service that serves your organization. Establishing this federation involves supplying data to Box that is specific to your Federation Service.

To configure Box for single sign-on:

1. In CloudAccess, obtain the required information:
   - **1a** On the Admin page, click the connector for Box.
   - **1b** Click **Configure**.
   - **1c** Expand the Federation Instructions, then copy and paste the signing certificate into a text file to use during the Box configuration. Ensure that you use a text editor that does not introduce hard returns or additional white space. For example, use Notepad instead of Wordpad.
2. Contact your Box account representative and provide the following information found in the Federation Instruction:

   Entity ID: `https://appliance_dns/osp/a/t1/auth/saml2/metadata`

   Assertion Consumer Service URL: `https://appliance_dns/osp/a/t1/auth/saml2/sso`

   Single Logout URL: `https://appliance_dns/osp/a/t1/auth/app/logout`

   The Profile that this connector will use is SAML 2.0 HTTP-POST. The following attributes will be sent in the assertion (case-sensitive):

   - email
   - first_name (optional)
   - last_name (optional)

   The first_name and last_name attributes are used by Box to enable just-in-time provisioning, if it is enabled on the Box side.
3. Proceed to Chapter 12, “Logging into the Web Service,” on page 41.

6 Configuring the Connector for Google Apps

The following documentation is only for the single sign-on connector for Google Apps. This is a different connector from the connector for Google Apps that is embedded in the CloudAccess appliance. Use this connector when you only need single sign-on capabilities. If you need provisioning, account management, and single sign-on capabilities, use the embedded connector.

6.1 Requirements

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

- ❒ A premier Google Apps account with the provisioning APIs enabled on the Google account. To set up a free sample account that expires after 14 days, see Google Apps (http://www.google.com/a/cpanel/sample/new).
- ❒ User accounts in Google Apps for each user who wants access to Google Apps.
- ❒ The Google Apps email addresses stored as an attribute on the users in their identity source. This can be the LDAP mail attribute, or another attribute of your choice.

6.2 Configuring the Connector

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

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

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

   Customer domain: Specify the domain name that you used when creating your Google Apps account.

   Destination URL: Specify the URL to which users go after initial login. If you are using IdP-initiated logins, this field is required.

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

Assertion Attribute Mappings: Select the LDAP attribute that stores the user's Google Apps email address. This value can also be the LDAP **mail** attribute.

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

6.3 Configuring Google Apps for Single Sign-On

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

To configure Google Apps for single sign-on:

1 In CloudAccess, obtain the required information to configure Google Apps in the Federation Instructions:

1a On the Admin page, click the connector for Google Apps.

1b Click **Configure**.

1c Expand the Federation Instructions, then copy and paste the instructions into a text file to use during the Google Apps 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 Google Apps account, then log in as the administrator.

4 In the **Dashboard**, click **Advanced Tools** > **Set up single sign-on (SSO)**.

5 Configure the following options:

Enable Single Sign-on: Select this option.

Sign-in page URL: Paste the Single Sign-on URL from the Federation Instructions.

Sign-out page URL: Paste the Single Logout URL from the Federation Instructions.

Change password URL: Specify a value, because Google requires it. CloudAccess does not support this option.

Verification certificate: Browse to and select the certificate you created from the Federation Instructions, then upload the certificate.

Use a domain specific issuer: Do not select this option.

Network masks: Leave this field blank.

6 Click **Save Changes**.

7 Proceed to Chapter 12, "Logging into the Web Service," on page 41.

7 Configuring the Connector for Jive

The connector for Jive provides single sign-on access to Jive through CloudAccess, but does not support provisioning. After importing the connector, you must configure the connector in CloudAccess and you must also configure Jive to work with the connector.

7.1 Requirements

Verify that you meet the following requirements before you configure the connector:

- ❒ A Jive account

  NOTE: There are three types of Jive accounts: Cloud, Hosted, or On Prem. If you have a Hosted or On Prem account, you have access to the federation settings required to configure the connector for Jive. If you have a Cloud account, you must contact Jive technical support to configure the SAML 2.0 federation between Jive and CloudAccess.

- ❒ A CloudAccess 1.1.1 or later system

7.2 Configuring the Connector

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

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 Jive to the bar, then click **Configure**.
3. Use the following information to configure the new connector for Jive:

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

   Base metadata URL: Specify the Base Metadata URL that is displayed on the federation pages on Jive. Or, if you are using a Jive Cloud account, specify the Instance name.

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

   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**.

7.3 Configuring Jive for Single Sign-On

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

To configure Jive for single sign-on:

1. In CloudAccess, obtain the required information to configure Jive as follows:
   - **1a** On the Admin page, click the connector for Jive.
   - **1b** Click **Configure**.
   - **1c** Expand the Federation Instructions, then copy and paste the information into a text file to use during the Jive configuration.

     NOTE: If you have a Jive Cloud account, you must send a copy of this information to Jive technical support. Jive technical support uses this information to create a federation between CloudAccess and Jive.

     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 Jive administration console with your Jive system administrator credentials.
3. Click **Single Sign-on** > **SAML**.
4. Change the setting to **Enabled**.
5. On the Metadata page, provide the following information:

   Load metadata from URL: Specify the URL `https://`*`DNS_of_appliance`*`/osp/a/t1/auth/saml2/metadata`

   Username Identity: Ensure that you select this option.

   SAML > User Attribute Mapping: Select **Federated**, then make the following mappings:

   - Email to mail
   - First Name to givenName
   - Last Name to sn

   SAML > Advanced: Ensure that the Base metadata URL matches the value you entered in the **Base metadata URL** setting in CloudAccess for this connector.
6. Click **Save ALL SAML Settings**.
7. Proceed to Chapter 12, “Logging into the Web Service,” on page 41.

8 Configuring the Connector for Salesforce

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.

8.1 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.

8.2 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: The connector for Salesforce contains the default signing certificate for Salesforce. You have the option of changing the certificate as needed for your environment.

If you want to change the certificate, you must obtain the new 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**.

8.3 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 the Federation ID from the User object**.

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 Proceed to Chapter 12, "Logging into the Web Service," on page 41.

9 Configuring the Connector for ServiceNow

The connector for ServiceNow provides single sign-on access to ServiceNow through CloudAccess, but does not support provisioning. After importing the connector, you must configure the connector in CloudAccess and you must also configure ServiceNow to work with the connector.

9.1 Requirements

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

- ❒ A management ServiceNow account created with the SAML 2.0 Update 1 plugin.
- ❒ The ServiceNow instance name. For example, `http://you_instance.service-now.com/`.
- ❒ A ServiceNow user account for each user who wants access to the single sign-on service. The connector for ServiceNow does not provision user accounts.

9.2 Configuring the Connector

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

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

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

   Instance name: Specify the instance name that ServiceNow sent to you when you set up the ServiceNow enterprise account.

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

   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**.

9.3 Configuring ServiceNow for Single Sign-On

After configuring the connector, you must configure single sign-on SAML 2.0 federation between ServiceNow and CloudAccess.

To configure ServiceNow for single sign-on:

1. In CloudAccess, obtain the required information to configure ServiceNow:
   - **1a** On the Admin page, click the connector for ServiceNow.
   - **1b** Click **Configure**.
   - **1c** Expand the Federation Instructions, then copy and paste the instructions into a text file to use during the ServiceNow configuration.
2. Log in to your ServiceNow account with your system administrator credentials.
3. Scroll through the items on the left side of the screen, then click **SAML 2 Single Sign-on > Properties**.
4. In the **Properties** window, provide the following information:

   Enable external authentication: Select **Yes.**

   The Identity Provider URL which will issue the SAML2 security token with user info: Copy and paste the Entity ID from the Federation Instructions. For example, `https://appliance_dns/osp/a/t1/auth/saml2/metadata`

   The base URL to the Identity Provider's AuthenRequest service: The AuthenRequest will be posted to the following URL as the SAMLRequest parameter:

   `https://appliance_dns/osp/a/t1/auth/app/its/connectors_NCSSSAML2:eRu6J_ycNWw`

   The base URL to the Identity Provider's SingleLogoutRequest service: Copy and paste the Single Logout URL from the Federation Instructions. For example, `https://appliance_dns/osp/a/t1/auth/app/logout`

   When SAML 2.0 single sign-on fails because the session is not authenticated, or this is the first login, redirect to this URL: Copy and paste the Entity ID from the Federation Instructions. For example, `https://appliance_dns/osp/a/t1/auth/saml2/metadata`
5. Click **Save** to save the changes.
6. Navigate to **SAML 2 Single Sign-on** > **Certificate**.
7. Edit the **SAML 2** entry, then replace the PEM certificate information with the certificate information from the Federation Instructions.
8. Click **Update** to save the certificate changes.
9. Proceed to Chapter 12, "Logging into the Web Service," on page 41.

10 Configuring the Connector for WebEx

The connector for WebEx provides single sign-on access to WebEx through CloudAccess, but does not support provisioning. After importing the connector, you must configure the connector in CloudAccess and you must also configure WebEx to work with the connector.

10.1 Requirements

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

- ❒ A WebEx account. Trial accounts do not support federation.
- ❒ WebEx user accounts for each user who wants access to the single sign-on service. The connector for WebEx does not provision user accounts.

10.2 Configuring the Connector

After importing the connector, you must configure the connector to work with your WebEx system. To configure the connector for WebEx:

1. Log on to the CloudAccess appliance and then access the Admin page at `https://dns_of_appliance/appliance/index.html`.
2. Drag and drop the connector for WebEx to the bar, then click **Configure**.
3. Use the following information to configure the new connector for WebEx:

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

   WebEx Domain: Specify your WebEx domain name.

   `https://custom-ID.webex.com`

   Signing Certificate: Browse to and select an SSL certificate if you want secure communication to WebEx.

   Assertion Attribute Mappings: Select **Email** from the list.
4. Copy the information in the Federation Instructions into a text file to use while configuring WebEx for single sign-on.
5. Click **OK**, then click **Apply**.

10.3 Configuring the WebEx Account for Single Sign-On

To configure the WebEx account:

1. In CloudAccess, obtain the required information to configure WebEx:
   - **1a** On the Admin page, click the connector for WebEx.
   - **1b** Click **Configure**.
   - **1c** Expand the Federation Instructions, then copy and paste the instructions into a text file to use during the WebEx 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 administration URL of the WebEx site (`https://`*`Domain Name`*`.webex.com/admin.php`).
4. Click **Host a Meeting**.
5. Select **My WebEx site** for the Account type, then log in as the administrator.
6. In the Menu bar, click **More Services > Site Administration**.
7. In the **Manage Site** list, click **SSO Configuration**.

   If this option does not appear, contact the WebEx account manager and have this option enabled.
8. Import the signing certificate as follows:
   - **8a** Click **Site Certificate Manager**.
   - **8b** Click **Browse.**
   - **8c** Browse to and select the certificate you created from the Federation Instructions.
   - **8d** Click **OK**, then click **Close**.
9. In the **Federation SSO Configuration** section, specify the following values found in the Federation Instructions:.

   Federation Protocol: Specify `SAML 2.0`.

   SSO Profile: Select **SP Initiated** or **IdP Initiated**.

   Destination: Specify the Single Sign-on URL from the Federation Instructions.

   WebEx SAML Issuer (SP): Specify your WebEx site ID.

   Issuer for SAML (IdP ID): Specify the Entity ID (appliance) URL.

   Tenant SSO Service Login URL: Specify the Single Sign-on URL from the Federation Instructions.

   NameID Format: Select **Email address**.

AuthnContextClassRef: Specify `urn:oasis:names:tc:SAML:2.0:ac:classes:Password`

Default WebEx Target page URL: Leave this option blank.

Tenant SSO Error URL: Leave this option blank.

Single Logout: Enable this option, and for the **Tenant SSO Service Logout URL**, specify the Single Logout URL from the Federation Instructions.

Auto Account Creation: Select this option to automatically create accounts.

Auto Account Update: Select this option to automatically update accounts.

10 Scroll to the bottom of the page, and save the configuration.

11 Proceed to Chapter 12, "Logging into the Web Service," on page 41.

11 Configuring the Connector for Zoho

The connector for Zoho provides single sign-on access to Zoho through CloudAccess, but does not support provisioning. After importing the connector, you must configure the connector in CloudAccess and you must also configure Zoho to work with the connector.

11.1 Requirements

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

- ❒ A Zoho business account. For more information, see Zoho Mail (http://www.zoho.com/mail/zohomail-pricing.html).
- ❒ A valid public domain that you have registered with Zoho. Select the **Enable MailHosting** option after logging in to the Zoho account.
- ❒ A Zoho user account for each user who wants to access Zoho.

11.2 Configuring the Connector

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

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 Zoho to the bar, then click **Configure**.
3. Use the following information to configure the new connector for Zoho:

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

   Customer domain: Specify the domain name that you used when creating your Zoho App.

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

   Assertion Attribute Mappings: Select the LDAP attribute that stores the user's NameID attribute. This value can also be the LDAP **mail** attribute.
4. Click **OK**, then click **Apply**.

11.3 Configuring Zoho for Single Sign-On

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

To configure Zoho for single sign-on:

1. In CloudAccess, obtain the required information to configure Zoho:
   - **1a** On the Admin page, click the connector for Zoho.
   - **1b** Click **Configure**.
   - **1c** Expand the Federation Instructions, then copy and paste the instructions into a text file to use during the Zoho 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. Log in to your Zoho account as an administrator.
4. From the **Account** menu, select **Zoho Mail**.
5. Click the **Control Panel**.
6. In the left panel, click **SAML Authentication**.
7. Use the following information to configure SSO for Zoho:

   Login URL: Paste the `Sign-in page URL` that you obtained from the Federation Instructions.

   Logout URL: Paste the Sign-out page URL that you obtained from the Federation Instructions.

   Password URL: Paste the Sign-in page URL that you obtained from the Federation Instructions. The connector does not use this value, but it is required by Zoho.

   PublicKey: Click **Get key From File**, browse to the location of the certificate you saved from the Federation Instructions, then upload the certificate.

   Algorithm: Select **RSA**.
8. Click **Submit** to save the changes.
9. Proceed to Chapter 12, "Logging into the Web Service," on page 41.

12 Logging into the Web Service

You must complete some additional configuration steps to enable users to log in to the Web service while also authenticating to the identity source.

12.1 Configuring Service Provider-Initiated Logins

A login initiated by the service provider (SP) allows users to start the login process at the service provider. If you are not using an embedded connector, the user must have an account in the identity source and in the Web service for single sign-on to work.

1. The user accesses the SP-initiated login URL you provide.
2. The service provider 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 the Web service.
5. The user is authenticated to both the identity source and the Web service at this point.

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

Table 12-1 *Sample SP-Initiated Login URLs*

Web Service	URL
Accellion	`https://domain_name.accellion.net/`
Access Manager	`https://Access_Manager_DNS_Name:8443/nidp` **NOTE:** If you are using the one box Access Manager, do not use the port number.
ADFS	`https://ADFS_DNS/adfs/ls/IDPInitiatedSignon.aspx`
Box	`https://domain_name.box.com/` **NOTE:** Box currently supports only SP-initiated login and does not support single logout. Clicking the **Logout** link on the OSP welcome page does not log the user out of the Box session.
Google Apps	`http://mail.google.com/a/Google_Domain_Name`

Web Service	URL
Jive	`https://Instance_Name.jiveon.com` **NOTE:** There is no SAML logout supported by Jive. When users log out at the Jive site, they are still logged in to the appliance. This is normal and expected behavior.
Salesforce	`https://custom_name.my.salesforce.com`
ServiceNow	`https://Instance_Name.service-now.com`
WebEx	`https://custom-ID.webex.com`
Zoho	`https://Customer_Domain.business.zoho.com`

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