



Access Manager 4.5 Applications Configuration Guide

April 2019

Legal Notice

For information about legal notices, trademarks, disclaimers, warranties, export and other use restrictions, U.S. Government rights, patent policy, and FIPS compliance, see <https://www.microfocus.com/about/legal/>.

© Copyright 2019 Micro Focus or one of its affiliates.

Contents

About this Book and the Library	5
1 Introduction to Application Connectors	7
2 Application Connector Catalog	9
2.1 Accessing Connectors through Administration Console	9
2.2 Accessing the Application Connector Catalog through the Website	10
3 Single Sign-On Assistant Connectors	11
3.1 Understanding SSO Assistant	11
3.2 Requirements for Using SSO Assistant Connectors	13
3.3 Configuring a Connector for SSO Assistant	14
3.4 Managing Icons	15
3.5 Troubleshooting Single Sign-On Assistant	16
4 Custom Connectors	17
4.1 Navigating the Connector Studio Page	18
4.2 Creating an SSO Assistant Connector	18
4.2.1 SSO Assistant Connector Requirements	19
4.2.2 Planning for an SSO Assistant Connector	19
4.2.3 Creating an SSO Assistant Connector	19
4.3 Creating a SAML 2.0 Connector	21
4.3.1 SAML 2.0 Connector Requirements	21
4.3.2 Planning for a SAML 2.0 Connector	21
4.3.3 Creating a SAML 2.0 Connector	21
4.4 Downloading a Connector to a File	28
4.5 Importing a Connector from a File	28
4.6 Importing a Connector from the Global Catalog	28
4.7 Managing a Connector	29
4.8 Publishing a Connector to the Local Catalog	29
4.9 Importing a Connector into the Applications Page	30
4.10 Example: Using an Existing SAML Connector to Configure an Application	30
4.10.1 Importing a SAML 2.0 Connector from the Global Catalog	30
4.10.2 Modifying a SAML Connector	30
4.10.3 Importing the SAML Connector into the Applications Page	33
5 SAML Connectors	35
5.1 Understanding Federated SSO with SAML 2.0	35
5.1.1 Understanding SAML 2.0	35
5.1.2 Understanding SAML 2.0 Federated SSO Processes with Access Manager	36
5.2 Global Requirements for SAML 2.0 Connectors	38
5.3 Configuring a Connector for a SAML Application	38

5.4	Managing SAML 2.0 Applications	39
5.4.1	Disabling and Enabling a SAML Application	39
5.4.2	Deleting a SAML Application	39
5.4.3	Downloading a SAML Application	39
5.5	Converting SAML 2.0 Service Providers in to a SAML 2.0 Application.	40
5.6	Unique ID	41
6	SAML/Account Management Connectors	43
7	Configuring the Application for Access Manager on the Public Cloud	45
7.1	Requirements for the Access Manager Connector	45
7.2	Importing and Configuring the Connector.	46
7.3	Example Scenarios.	47
7.3.1	Scenario 1: Cloud-based IDP and On-Premises SP with a Protected Resource	48
7.3.2	Scenario 2: On-Premises IDP and Cloud-based SP with a Protected Resource	48
7.3.3	Scenario 3: On-Premises IDP and Cloud-based SP with Third-party SP	49
7.3.4	Scenario 4: On-Premises IDP, Cloud-based SP with Third-party SP, and Third-party SP Is Accessible from On-Premises User Portal	51
8	Configuring the Applications for Office 365 Using WS Federation and WS-Trust	53
8.1	Prerequisites for Configuring the Connector.	53
8.2	Configuring an Office 365 Domain to Federate with Access Manager	53
8.2.1	Prerequisites for Configuring an Office 365 Domain	54
8.2.2	Enabling Federation Settings in the Office 365 Domain	54
8.2.3	Verifying Single Sign-On Access	55
8.3	Configuring the Connector	56

About this Book and the Library

The *Access Manager Applications Configuration Guide* provides information about importing, configuring, and managing the connectors you use with Access Manager.

Intended Audience

This guide provides information for Access Manager administrators who are responsible for configuring and managing the single sign-on to Access Manager. Administrators must know and understand the following concepts:

- ◆ Secure Assertion Markup Language (SAML)
- ◆ Extensible Markup Language (XML)
- ◆ Public Key Infrastructure (PKI) digital signature concepts and Internet security
- ◆ Secure Socket Layer/Transport Layer Security (SSL/TLS)
- ◆ Hypertext Transfer Protocol (HTTP and HTTPS)
- ◆ Uniform Resource Identifiers (URLs)
- ◆ Domain Name System (DNS)
- ◆ Firewalls
- ◆ Public and private networks
- ◆ Connected applications

Other Information in the Library

You can access other information resources in the library at the following locations:

- ◆ [Access Manager Product Documentation \(https://www.netiq.com/documentation/access-manager/index.html\)](https://www.netiq.com/documentation/access-manager/index.html)
- ◆ [Access Manager Developer Resources \(https://www.netiq.com/documentation/access-manager-45-developer-documentation/\)](https://www.netiq.com/documentation/access-manager-45-developer-documentation/)

NOTE: Contact namsdk@microfocus.com for any query related to Access Manager SDK.

1 Introduction to Application Connectors

As an administrator, you have many users in your user stores that require access to many different web applications. The identity federation enables you to provide single sign-on (SSO) to your users. For more information about federation, see [“Federated Authentication”](#) in the *Access Manager 4.5 Administration Guide*.

Access Manager provides a simplified way using connectors to give users a secure SSO access to different web applications. Access Manager uses connectors to establish the connection between Access Manager and applications. An application connector contains pre-integrated configurations for a specific SaaS application.

An application connector helps you achieve the following objectives:

- ♦ Reduce the complexity in setting up SSO and account management to SaaS applications.
- ♦ Deploy integrations quickly without doing any application or protocol-specific configuration.

Access Manager supports the following types of application connectors:

- ♦ **Single Sign-On Assistants Connectors:** These connectors work with SSO Assistant extensions for browsers to securely collect, store, retrieve, and replay the users’ authentication information for the application you select.

For more information, see [Chapter 3, “Single Sign-On Assistant Connectors,”](#) on page 11.

- ♦ **Federation Connectors:** (SAML 2.0 and WS-Fed) These connectors simplify the configuration process of establishing a federated connection between applications or web services and Access Manager.

For more information, see [Chapter 5, “SAML Connectors,”](#) on page 35

- ♦ **Federation and Account Management Connectors:** (SAML 2.0) In addition to simplifying Access Manager configuration, these connectors can also configure SaaS Account Manager (SAM) in Access Manager to automatically provision user accounts at the corresponding SaaS providers.

To provision SAML accounts by using SAM, you must first purchase and deploy the SAM appliance and configure the appropriate SAM connector for the SAML application. For more information, see [Chapter 6, “SAML/Account Management Connectors,”](#) on page 43.

You can customize application connectors based on your requirements. See [Chapter 4, “Custom Connectors,”](#) on page 17.

When you configure a connector for an application, the system automatically creates an appmark for this application and adds it on the User Portal page. For more information about appmarks, see [“Appmarks”](#) in the *Access Manager 4.5 Administration Guide*.

2 Application Connector Catalog

Access Manager provides an [Application Connector Catalog \(https://catalog.netiq.com/ncarest/displayCatalog\)](https://catalog.netiq.com/ncarest/displayCatalog). The Application Connector Catalog displays all available connectors and the browsers which are compatible with the connectors.

The catalog can display the connectors by name or by connector type. The available connector types are SSO Assistant, SAML, SAML/Account Management, and WSFED.

You can access the catalog in the following ways:

- ◆ [Section 2.1, “Accessing Connectors through Administration Console,” on page 9](#)
- ◆ [Section 2.2, “Accessing the Application Connector Catalog through the Website,” on page 10](#)

2.1 Accessing Connectors through Administration Console

You require to import the connector from the Application Connector Catalog into Administration Console to configure the connector and create an appmark.

To access a connector through Administration Console:

- 1 Log in to Administration Console, then click **Administration Tasks > Applications > +** (plus sign).
- 2 Click **Add Application from Catalog** to import the predefined connector of a specific applications
Or,
Click **Add Application from Local Catalog**. Local catalog contains connectors that have been placed there by importing a connector from the public catalog or from a file, or by using the Publish option from connector studio.
- 3 Browse or search through the catalog, then select the appropriate connector.
- 4 Configure the connector.
 - ◆ For information about Single Sign-On Assistant connectors, see [Chapter 3, “Single Sign-On Assistant Connectors,” on page 11](#).
 - ◆ For information about SAML 2.0 connectors, see [Chapter 5, “SAML Connectors,” on page 35](#).
 - ◆ For information about SAML/Account Management connectors, see [“SAML/Account Management Connectors” on page 43](#).
 - ◆ For information about WS Federation Connectors, see [Chapter 8, “Configuring the Applications for Office 365 Using WS Federation and WS-Trust,” on page 53](#).
 - ◆ For information about custom connector, see [“Custom Connectors” on page 17](#).

2.2 Accessing the Application Connector Catalog through the Website

Depending on your firewall configuration, you might not be able to access the Application Connector Catalog through Administration Console. In this situation, you can download connectors from another computer and then copy those files to a computer that Administration Console can access.

Perform the following steps to access the catalog through the website:

- 1 Access [Application Connector Catalog \(https://catalog.netiq.com\)](https://catalog.netiq.com).
- 2 Browse through the Application Connector Catalog, then select the appropriate connector.
- 3 Select the desired application connector and save it.
- 4 Copy the application connector to a computer that Administration Console can access.
- 5 Log in to Administration Console, then click **Applications**.
- 6 Click + (plus sign) > **Import from File**.
- 7 Configure the connector.

For information about the Single Sign-On Assistant applications, see [Chapter 3, “Single Sign-On Assistant Connectors,” on page 11](#). For information about the other connector types, see the application-specific section in this guide.

3 Single Sign-On Assistant Connectors

Access Manager provides users a way to perform secure single sign-on to applications. Access Manager provides Single Sign-On (SSO) Assistant connectors that are customized for each application to meet the interactive and content requirements for logging in to the application. The SSO Assistant connectors work with SSO Assistant extensions for browsers to securely collect, store, retrieve, and replay the users' authentication information for the application you select. See [Section 3.1, "Understanding SSO Assistant," on page 11](#).

Access Manager provides many connectors for SSO Assistant that you can import from the Application Connector Catalog. You can access the Application Connector Catalog through Administration Console, but Administration Console must have access to the Internet for the Application Connector Catalog to work. Ensure that you have port 80 open on your firewall for communication to the Application Connector Catalog for the latest connectors. You can also access the Application Connector Catalog without Administration Console. You can see the list of current connectors in [Application Connector Catalog \(http://catalog.netiq.com/\)](http://catalog.netiq.com/). For more information, see [Section 2.2, "Accessing the Application Connector Catalog through the Website," on page 10](#).

You can also create custom connector definitions for SSO Assistant. See [Section 4.2, "Creating an SSO Assistant Connector," on page 18](#).

IMPORTANT: Contact [NetIQ Technical Support \(https://www.netiq.com/support/\)](https://www.netiq.com/support/) if a connector for SSO Assistant is not yet available for the application that your users access. This helps us to define requirements and set priorities for future connectors for SSO Assistant.

Use the information in the following sections to configure a connector for SSO Assistant.

- ♦ [Section 3.1, "Understanding SSO Assistant," on page 11](#)
- ♦ [Section 3.2, "Requirements for Using SSO Assistant Connectors," on page 13](#)
- ♦ [Section 3.3, "Configuring a Connector for SSO Assistant," on page 14](#)
- ♦ [Section 3.4, "Managing Icons," on page 15](#)
- ♦ [Section 3.5, "Troubleshooting Single Sign-On Assistant," on page 16](#)

3.1 Understanding SSO Assistant

SSO Assistant enables users to securely store their credentials for existing accounts of online applications and provides an SSO experience.

For example, a user Maria has an account on ChatWork. Maria uses ChatWork to communicate with her team members. Instead of logging in to ChatWork with separate credentials each time, she can log in to ChatWork once. SSO Assistant will save and replay her saved credential every time she accesses ChatWork.

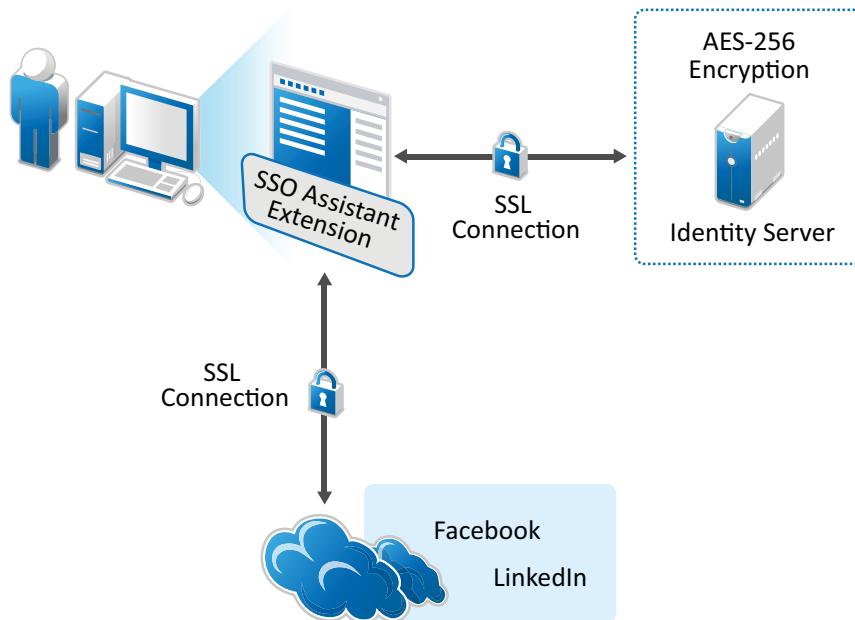
SSO Assistant and Form Fill policies both automatically populate HTML forms. Form Fill policies scan each login page accelerated through Access Gateway to populate the credential information. For more information, see ["Form Fill Policies"](#) in the [Access Manager 4.5 Administration Guide](#).

SSO Assistant does not go through Access Gateway. SSO Assistant provides connectors for the different applications. You can configure a connector for a specific site. SSO Assistant captures users' credentials through a browser plug-in or extension. It securely stores users' credentials on Identity Server.

Access Manager protects users' credentials through an SSL connection and AES-256 encryption on Access Manager.

The following graphic depicts how Access Manager securely stores the credentials:

Figure 3-1 How Access Manager Securely Stores Credentials



Users must install the appropriate SSO Assistant extension or plug-in for their browser or install the MobileAccess app to experience SSO Assistant to an application. The following is the flow of actions a user logs in to first time to access an SSO Assistant application:

1. A user logs in to User Portal by using Access Manager credentials.
2. The user sees the appmarks for the available applications and clicks the appropriate appmark.
3. If the SSO Assistant extension or plug-in for the browser is not installed on the computer, Access Manager prompts the user to install it.
4. After installing the extension or plug-in, the user goes to User Portal and click the application again.
5. The extension or plug-in opens a new tab where the user enters the user name and password for the application.
The user must enter the user name and password for the application once.
6. The extension or plug-in captures the user's credentials for the application. The extension or plug-in sends the user's credentials to Access Manager over an SSL connection.
7. Access Manager encrypts the user's credentials with AES-256 encryption, and then stores the user name and password in the credential store that is part of Identity Server.

Identity Server encrypts the user's credentials with an encryption key that is unique per user account in Access Manager.

8. Access Manager then redirects the user to the application over an SSL connection.

In subsequent Access Manager sessions, the user can log in with Access Manager credentials and access the destination application without providing the additional credentials for the application. Identity Server securely retrieves and submits the user's credentials for an automatic login on behalf of the user. This provides the user with an SSO experience.

The user must install the SSO Assistant browser extension on each device where the user wants to access the application. Access Manager automatically prompts the user to install the extension the first time that the user accesses the application's appmark from a different device, even if the user's credentials for the application are available in the user store. The extension then retrieves and submits the user's credentials for the selected application from Access Manager for an automatic login.

Typically, users have a different login user name and password for their individual accounts for each application. A user can have only one account per application. Access Manager stores the user's current credentials, but users still have the responsibility to maintain the credentials. The User Portal page, on the menu on the user's name, provides a way for users to modify their credentials through the **Clear Single Sign-on Credentials** option if they are expired or stolen.

If the user changes the user name or password or cancels the account, stored credentials become invalid. The automatic login fails and the browser extension takes the user to the application's login page where the user can log in with new credentials. You will need to remove the old credentials from the store on the portal page. For subsequent logins, the new credentials will be saved if the previous ones are removed.

3.2 Requirements for Using SSO Assistant Connectors

Ensure that the following requirements are fulfilled:

- Connectors for SSO Assistant work with applications that require forms-based authentication for login. Typically, they have the following login requirements:
 - The application's login page uses HTML forms as the main point of interaction with a user.
 - The application requires the user's password to be sent for logging in to an application.
 - The application does not support SAML 2.0 or WS-Federation protocols for federated trust relationships instead of sending passwords.
- The login page scheme must be HTTPS not HTTP.
- The connectors for SSO Assistant support the following browser versions:
 - ◆ Edge
 - ◆ Chrome
 - ◆ Firefox 34 or later

The MobileAccess app supports the secure retrieval and replay of previously stored credentials for applications that users access through the User Portal page on supported mobile devices.

For user access to the applications on supported mobile devices, the MobileAccess app supports the following versions:

- ◆ iOS 9.x
 - ◆ Android Kit Kat 4.4 or Lollipop 5.x
- ❑ A user must install the SSO Assistant extension in a supported browser one time on each desktop or laptop they use to access the SSO Assistant applications.

For Chrome, the extension is available for free from the Google Play Store. If it is not installed when the user accesses the application through Access Manager, Access Manager prompts the user to go to the Google Play Store and install it. The installation adds the extension to the Chrome Extensions list with the following permissions:

- ◆ Access your data on all websites
- ◆ Access your tabs and browsing activity

For Firefox, the extension is available through [Add-ons \(https://addons.mozilla.org/en-US/firefox/\)](https://addons.mozilla.org/en-US/firefox/). The Firefox extension behaves the same way the Chrome extension behaves.

- ❑ SSO Assistant is not supported in a mixed Access Manager environment. All components of Access Manager (Identity Server clusters, Access Gateway clusters, and Administration Console) must be of the same version.

3.3 Configuring a Connector for SSO Assistant

You can import and configure as many of the connectors for SSO Assistant as you need. However, users can store only up to 20 saved credentials. For example, you might import and configure 75 connectors for SSO Assistant. A user could only use and save credentials for 20 of the 75 connectors for SSO Assistant.

The steps to configure the connectors for SSO Assistant are the same for each connector provided in the Application Connector Catalog.

To configure a connector for SSO Assistant:

- 1 Log in to Administration Console.
- 2 Click **Applications**.
- 3 Import a connector for SSO Assistant from Application Connector Catalog or Local Application Catalog.

For more information, see [Chapter 2, “Application Connector Catalog,” on page 9](#).

4 Specify the following details:

Options	Description
Name	Specify a unique name for the connector.
Description	(Optional) Specify a description of the connector. You can import and configure multiple connectors for the same application. You can have more than one connectors for any application. So, ensure to use a unique name and a description to help determine the differences between the connectors.
Change Image	(Optional) Change the default image that the User Portal page displays to users.
Roles	(Optional) Select the appropriate role from the list to determine who can see the appmark for this connector on the User Portal page. If you do not assign a role, all users can see the appmark. Appmarks for SSO Assistant have a public endpoint to Identity Server. Even if users, who are not a member of a role, log in to User Portal and they know the exact URL that is part of the appmark, the SSO Assistant process starts. For more information about the SSO Assistant process, see Section 3.1, "Understanding SSO Assistant," on page 11.
URL	Specify the URL that users access when they click the appmark for an application.
Enable	Select the user platforms where the appmark will be visible.
Optional Configuration Values	Specify a different image and URL for the desktop browsers, iOS devices, and Android devices.
Login Form Data	Verify that the information displayed is correct for the application. When you import a connector, these fields are populated.

5 Click **Save**.

The Applications page displays the new connector for SSO Assistant. An appmark for this connector is created so that users can access it through User Portal. Ensure that you have configured MobileAccess for the users to access and use the connectors you have added. For more information, see ["Enabling Mobile Access"](#) in the [Access Manager 4.5 Administration Guide](#).

3.4 Managing Icons

Access Manager provides a set of default images you can use while creating an appmark. You can also upload your own images. The maximum image size is 200 x 200 pixels and the ideal image size is 100 x 100 pixels.

You can delete and edit any images you upload. You are not allowed to delete or edit any of the images that come with Access Manager. You edit or delete the images when you are creating or editing appmarks.

3.5 Troubleshooting Single Sign-On Assistant

Use the following information to help troubleshoot issues with SSO Assistant:

SSO Assistant can only work with one instance of Access Manager. If you have two instances of Access Manager and users have an account for both systems, when they try to log in to SSO Assistant applications, they might have issues.

SSO Assistant uses sessions for saving and replaying users' credentials. Opening multiple sessions in the same browser causes issues.

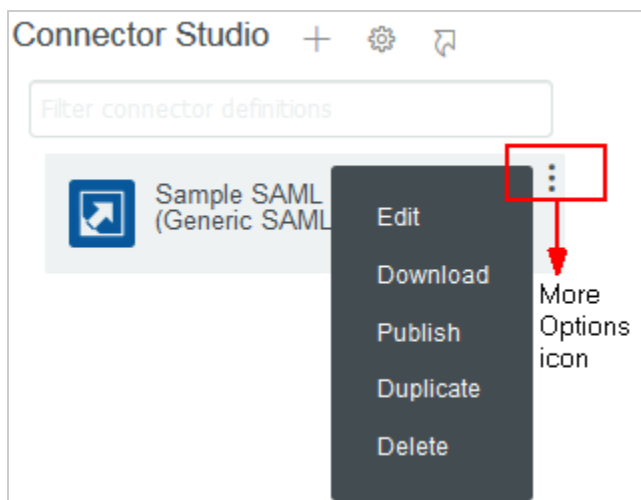
4 Custom Connectors

Access Manager provides *Connector Studio* and the *Applications* page to manage connectors and applications. Connector Studio enables you to create and edit Single Sign-On (SSO) Assistant and SAML 2.0 type connectors without coding or scripting. You can then import a connector into the Applications page for creating an SSO Assistant or SAML 2.0 type application based on the connector.

You can create a custom connector to integrate an application or a web service that has no predefined connector and that uses the following SSO authentication methods.

- ◆ SSO Assistant (Form-based)
- ◆ SAML 2.0

After you create a connector, you can save it to a file (connector > **More Options** icon > **Download**) or publish it to Access Manager's Local Catalog (connector > **More Options** icon > **Publish**).



This section includes the following topics:

- ◆ Section 4.1, "Navigating the Connector Studio Page," on page 18
- ◆ Section 4.2, "Creating an SSO Assistant Connector," on page 18
- ◆ Section 4.3, "Creating a SAML 2.0 Connector," on page 21
- ◆ Section 4.4, "Downloading a Connector to a File," on page 28
- ◆ Section 4.5, "Importing a Connector from a File," on page 28
- ◆ Section 4.6, "Importing a Connector from the Global Catalog," on page 28
- ◆ Section 4.7, "Managing a Connector," on page 29
- ◆ Section 4.8, "Publishing a Connector to the Local Catalog," on page 29
- ◆ Section 4.9, "Importing a Connector into the Applications Page," on page 30
- ◆ Section 4.10, "Example: Using an Existing SAML Connector to Configure an Application," on page 30

4.1 Navigating the Connector Studio Page

The Connector Studio page provides options for changing view size, switching to the Applications page, and redirecting to Dashboard.

The following diagram demonstrates Connector Studio options:

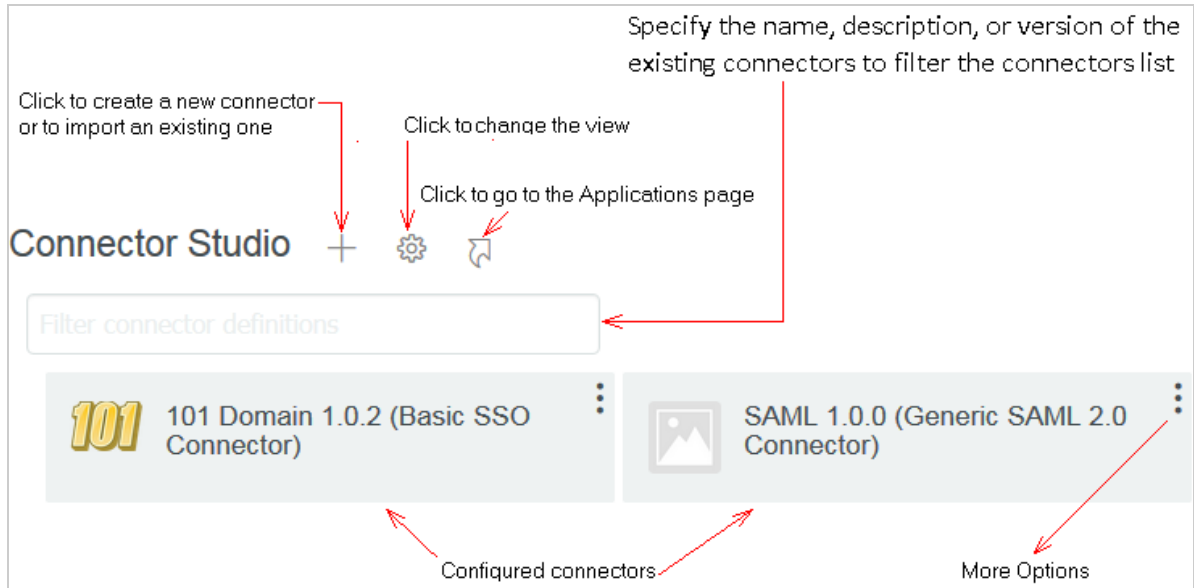






Table 4-1 Icons on the Connector Studio Page

Icon/Option	Description
	Provides options to create a new connector or import an existing connector from a file or from the Global Catalog.
	Provides options to change the view size.
	Redirects to the Applications page.
	Provides more options to edit, download, publish, duplicate, and delete a connector.
Filter Connector Definition	Filters the list of displayed connectors. This option is useful when you have configured many connectors and want to list only those that match the filter condition.

4.2 Creating an SSO Assistant Connector

An SSO assistant connector uses HTML forms to populate the authentication information. To create an SSO assistant connector, you must define the HTML form for the application.

- ◆ [Section 4.2.1, “SSO Assistant Connector Requirements,” on page 19](#)
- ◆ [Section 4.2.2, “Planning for an SSO Assistant Connector,” on page 19](#)
- ◆ [Section 4.2.3, “Creating an SSO Assistant Connector,” on page 19](#)

4.2.1 SSO Assistant Connector Requirements

- ❑ The application or web service must support HTML forms.

For more information, see [www.w3.org \(http://www.w3.org/TR/html401/interact/forms.html\)](http://www.w3.org/TR/html401/interact/forms.html).

- ❑ The connector supports user access to destination websites through web browsers running on a desktop or a laptop.

The MobileAccess app supports the secure retrieval and replay of stored credentials for websites that users access through the landing page on supported mobile devices.

- ❑ Determine whether the application uses different HTML forms for desktop and mobile.

4.2.2 Planning for an SSO Assistant Connector

Collect the following information before creating an SSO assistant connector:

- ◆ Domain name of the web service or application
- ◆ Login URL of the web service or application
- ◆ ID or name of the form that contains user name
- ◆ ID or name of the form that contains user password
- ◆ Input type used for the form
- ◆ Criterion for a successful login or a failed login

4.2.3 Creating an SSO Assistant Connector

- 1 Log in to Administration Console as an administrator.
- 2 In **Dashboard**, click **Administrative Tasks > Connector Studio > + > Create SSO Assistant connector**.

The type and the type name of the connector are set when you select the type of connector to create.

- 3 Under **General**, specify the following details:

Target Name: Specify a unique name for the connector.

Description: Specify the purpose of the connector.

Version: Specify a three-digit version number for the connector.

Icon: Browse to and select a graphic that you want as the icon for the new connector.

- 4 Under **Settings**, create a new setting for the connector. This setting provides a way for administrators to input data while creating the connector.

Field	Description
Name	Specify a name for the setting. This name is used to reference or track the setting internally.
Display Name	Specify a display name for the setting. This name appears on the Applications page under Setting Name and Value while configuring an application using this connector.
Data Owner	Access Manager does not use this option for an SSO assistant connector.

Field	Description
Type	Select String as the data type of the value that you specify in Setting Name and Value on the Applications page while configuring an application.
Min	Access Manager does not use this option for an SSO assistant connector.
Max	Access Manager does not use this option for an SSO assistant connector.
Description	Specify the description of this setting. This value appears when you mouse over the help icon for this setting under Setting Name and Value in the Applications page while configuring an application.
Default Value	Specify a default value. This value appears by default for the corresponding Setting Name and Value in the Applications page while configuring an application.
Required	Ensure to select this option. After selecting, the end user must enter a value for the setting.
Concealed	Access Manager does not use this option for an SSO assistant connector.

- 5 Define the HTML form for the appropriate application and platform under **Desktop**, **iOS**, and **Android**.

You can use the same fields for all three platforms or define a unique form for each platform. The HTML forms for some applications are different for the desktop application and the mobile application. When the HTML forms are different, you must create multiple forms for the application.

Field	Description
Login URL	Specify the login URL of the application.
Import	Use this option if you want to populate the values in Form ID , Input Field Definitions , and Submit ID by using Login URL that you have specified. When you use this option, you do not need to specify details in the other fields on this page manually.
Input Field Definitions	Click + to add more input fields if required. Only the <code>String</code> type is supported.
Submit ID	Specify the ID or name on the element that submits the login form.

- 6 Click **OK**.
- 7 Proceed to [Section 4.8, “Publishing a Connector to the Local Catalog,” on page 29](#).

4.3 Creating a SAML 2.0 Connector

Connector Studio and the Applications page help you set up basic configuration settings for a SAML 2.0 application. After you create a SAML 2.0 application by using a connector, the Applications page displays **Advanced Setup** links in each configuration section. You can use these links to go to the SAML 2.0 configuration pages and configure additional settings.

- ◆ [Section 4.3.1, “SAML 2.0 Connector Requirements,” on page 21](#)
- ◆ [Section 4.3.2, “Planning for a SAML 2.0 Connector,” on page 21](#)
- ◆ [Section 4.3.3, “Creating a SAML 2.0 Connector,” on page 21](#)

4.3.1 SAML 2.0 Connector Requirements

To create a SAML 2.0 connector, ensure that the service provider meets the following protocol-specific requirements:

- Supports identity federation by using the SAML 2.0 protocol.

For more information about SAML, see the [OASIS website \(https://wiki.oasis-open.org/security/FrontPage\)](https://wiki.oasis-open.org/security/FrontPage).
- Supports the SAML web browser single sign-on profile, with the Redirect and POST bindings for service-provider-initiated SSO, and the POST binding for identity-provider-initiated SSO.
- Provides technical documents that describe the application’s SAML federation requirements, metadata, and assertions.

4.3.2 Planning for a SAML 2.0 Connector

You must collect information about the destination web service or application before creating a SAML 2.0 connector.

Ask the application service provider the following 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 are the required configuration steps in your application to set up federation?
- ◆ What information do you provide to customers when they set up federation with their identity source?

4.3.3 Creating a SAML 2.0 Connector

You must configure the fields shown in red before saving a connector. Other fields are optional, but may require configuration based on requirements of the service provider.

Perform the following steps to create a SAML 2.0 connector:

- 1 Log in to Administration Console as an administrator.
- 2 In **Dashboard**, click **Administrative Tasks** > **Connector Studio** > + > **Create SAML 2.0 connector**.

3 Under **General**, specify the following details:

Field	Description
Target Name	Specify a unique name for the connector file. This name is used as the filename when downloading the connector to a file or publishing to the Local Application Catalog.
Version	Specify a three-digit version number for the connector. This value is used in the filename when downloading the connector to a file or publishing to the Local Application Catalog. It is displayed in the Applications page while configuring an application based on this connector.
Description for Provider	Access Manager does not use this option.
Description for Tenant	Specify the description of the connector. This value is displayed in the Description field on the Applications page while configuring an application based on this connector.
Certificate required for provider	Select if the service provider requires a signing certificate. If selected, the Applications page displays the signing certificate field as required. If this option is selected, the Applications page considers the certificate field as mandatory and displays a red asterisk. A certificate from the service provider must be imported to save the application. You can also import a default certificate from the service provider while creating the connector by using the Metadata page. See Step 5 on page 23 .
Change Image	Add a custom graphic to use for the icon that represents the connector in Connector Studio and the Applications page.

4 Select **Settings**.

You can use the Settings page to create settings based on requirements of a service provider. These settings are used to create SAML metadata while creating an application based on this connector.

You can use these settings to gather and display configuration information from the administrator while configuring a connector in Connector Studio and while configuring an application on the Applications page.

In Connector Studio, these settings are available for selection on other configuration pages within Connector Studio (Metadata, Assertion, and Federation Instructions pages) and in the Applications page under the **Application Connector Setup** section. Settings, also referred to as `replaceable` values, are used as configuration data placeholders. An administrator can specify actual values while configuring an application based on this connector. In the XML definition file of a connector created in Connector Studio, `replaceable` values use the `${nameOfSetting}` format.

In the Applications page, while creating an application based on a connector with one or more settings, the **Display Name** of the setting is displayed in the **Application Connector Setup** section. The values specified for those settings while configuring the application are then used to create metadata for the application.

The Settings page provides the following options to create a new setting or edit an existing one:

Field	Description
Name	Specify a name for the setting. This name is used to reference or track the setting internally.
Display Name	Specify a display name for the setting. This name is used on the Metadata, Assertion, and Federation Instructions pages in Connector Studio and also in the Applications page under the Application Connector Setup section.
Data Owner	Select Tenant . Access Manager does not support other options in the list.
Type	Select the type of the data. Access Manager supports only <code>String</code> and <code>URL</code> data types.
Min	Specify the minimum acceptable limit of the data. This value depends on the type you select under Type . For example, if you select String , specify the minimum length of the value. If you leave this field blank, then no minimum value is enforced.
Max	Specify the maximum acceptable limit of the data. This value depends on the type you select under Type . For example, if you select String , specify the maximum length of the value. If you leave this field blank, then no maximum value is enforced.
Description	Specify the description of this setting. This value is displayed when you mouse over the help icon associated with this setting in the Application Connector Setup section on the Applications page.
Default Value	Specify a default value.
Required	Select if you want to make this field mandatory. When selected, the field is marked as required (a red asterisk) on the Applications page. If not selected, you can skip specifying a value while creating or editing an application.
Concealed	If you select this option, the value for this setting is masked with asterisks (*) when you create an application based on this connector on the Applications page.

5 Select Metadata.

Access Manager uses the service provider's metadata for communications with the service provider. You can use the Metadata page to determine how the metadata representing the service provider is created and configured.

Some service providers allow you to download their metadata from a URL. If not, you can manually generate the metadata based on the settings defined here.

Select one of the following methods to create the metadata:

- ◆ **Request:** Specify **Source URL** to retrieve the metadata from the service provider. You can specify **Source URL** by using replaceable values configured on the Settings page if required.
- ◆ **Generate:** Specify the following details to manually generate the metadata for the service provider based on the information provided by the service provider. You can use **Import from URL** or **Import from File** if the metadata is available in that form instead of specifying the following values:

Field	Description
EntityID	<p>The value required for EntityID is available in the service provider’s metadata or in the help information that may be available in federation instructions from the provider.</p> <p>Specify the entityID of the metadata that uniquely identifies the particular service provider, such as <code>sp_domain_name</code>.</p> <p>For example, <code>google.com</code>.</p> <p>You can also specify a previously configured setting (replaceable value) by clicking the Select icon.</p>
Signing Certificate	<p>If you have selected Certificate required for provider under General and do not upload a certificate here, the administrator will be required to add a certificate while configuring an application based on this connector by using the Applications page.</p>
Assertion Consumer Service URL	<p>Specify the URL where the assertion is posted by the browser. For example, <code>https://www.google.com/a/\${customer-domain}/acs</code>.</p> <p>You can also specify a previously configured setting (replaceable value) by clicking the Select icon.</p>
Logout URL	<p>Specify a logout URL.</p> <p>The logout URL corresponds to the field <code>SingleLogoutService</code> from the service provider’s metadata.</p> <p>You can also specify a previously configured setting (replaceable value) by clicking the Select icon.</p>
Logout URL Binding	<p>Specify the logout URL Binding (HTTP Post or Redirect).</p> <p>For SAML 2.0, the only supported binding method is POST.</p>
Logout Response URL	<p>Specify the URL a logout request be sent to.</p> <p>The logout response URL is required when the <code>SingleLogoutService</code> field has <code>ResponseLocation</code> specified in the metadata.</p> <p>You can also specify a previously configured setting (replaceable value) by clicking the Select icon.</p>
Import from File	<p>If you selected Method > Generate and you have downloaded the service provider’s metadata to a file, use this option to populate the values in Metadata page configuration fields using that file.</p>

Field	Description
Import from URL	If you selected Method > Generate and the service provider's metadata is available at a specified URL, use this option to populate the values in Metadata page configuration fields.

6 Select **Attributes**.

You can use the Attributes page to define mappings between the remote attribute names required by the service provider and the user attributes available in the local Access Manager user stores. The mapped attributes are included in the SAML response and are used by the service provider to identify the user.

Attribute mappings configured here are displayed in the Attributes section while creating an application based on this connector (using the Applications page). When the application is created, an `Attribute Set` object is automatically created that contains these attribute mappings. You can view or edit the attribute set in the Shared Settings page of Access Manager.

Using the Attributes page, you can either create new attributes or import existing attributes from attribute sets already configured on the local Access Manager system.

To import existing attributes:

1. Click **Import Attribute Set**.

All attribute sets from the local Access Manger system are displayed.

2. Select one or more attribute sets from the list.

The mappings from the selected sets are displayed.

3. (Optional) Click the **More Options** icon associated with each attribute and click **Edit** to modify the details if needed. You can use the attributes as it is also.

Any change that you make in attribute mappings here does not impact the source attribute set that was used as a template. These changes are applicable only for this connector. After you save the connector, the attribute mappings are saved in the connector. When you download or publish the connector, these attribute mappings are included in the connector definition.

4. Click **OK**.

To create new attributes:

1. Click **New Attribute**.
2. Specify the following details:

Field	Description
Display Name	Specify a display name. The value of Display Name is used in the Assertion page when the Select icons are clicked for Audience Restriction and Name ID .
Remote Attribute Name	Specify a name. This name is used to identify the attribute in the SAML response sent to the service provider. It is displayed on the Applications page under Attributes > Remote Attribute while configuring an application based on this connector.

Field	Description
Description	Specify the description of this attribute. This text is displayed when you mouse over the help icon associated with this attribute in the Attributes section on the Applications page while configuring an application.
Remote Namespace	Specify the namespace defined for the attribute by the remote system.
Remote Format	Select one of the following formats: <ul style="list-style-type: none"> ◆ Unspecified: Indicates that the interpretation of the content is implementation-specific. ◆ URI: Indicates that the interpretation of the content is application-specific. ◆ Basic: Indicates that the content conforms to the <code>xs:Name</code> format as defined for attribute profiles.
Type	Select the type of the attribute. Available options are LDAP Attribute, String, and Token.
Encoding	Select None . Access Manager does not support attribute encoding while publishing connectors to the Local Application Catalog or while importing connectors into the Applications page. Selecting encoding types other than None is allowed in Connector Studio for compatibility when creating connectors to be exported and used with other system types.
Local Attribute	(Optional) You can specify a default value for the Type you have selected. If a default value is specified, you can view or edit it in the Mapped to System Attribute column on the Applications page for this attribute. In the Applications page, the Attributes section displays the mappings defined here.
Required	If you select this option, a red asterisk is displayed with the attribute in the Applications page and the attribute mapping must be completed to save the application.

7 Select Assertion.

You can use the Assertion page to configure values for specific elements included in the SAML assertion sent to the service provider.

Specify the following details:

Field	Description
Audience Restriction	Access Manager does not support this option.
Name ID	Select an attribute that uniquely identifies the user at the service provider. If an attribute has not yet been created (using the Attributes page), click the select icon > New Attribute to create a new attribute.
Format	Select the NameID formats to match the requirements of the service provider by inspecting the provider's metadata or federation instructions.
Destination URL	Specify the URL of the destination application. The default appmark created for an application that is configured based on this connector contains the target override field populated with the value specified here. The user's browser is redirected to this URL after a successful single sign-on when clicking the appmark.

8 Select **Federation Instructions**.

You can use the Federation Instructions page to create the help information that is displayed in the Applications page while configuring an application based on this connector. This information is available under the **System Setup** section in the Applications page. Specify the detailed instructions here for configuring the service provider to trust Access Manager as an identity provider.

Federation instructions can use the following system-provided replaceable values. When configuring an application in the Applications page, these placeholders are replaced with values appropriate for the Access Manager Identity Server cluster where the application is being configured.

Field	Description
`\${entityID}`	Represents the value of Identity Server cluster's Entity ID.
`\${ssoURL}`	Represents the value of the Identity Server cluster's single sign-on URL.
`\${sloURL}`	Represents the value of the Identity Server cluster's single logout URL.
`\${sloReturnURL}`	Represents the value of the Identity Server cluster's logout return URL.
`\${signingCert}`	Represents the value of the Identity Server cluster's default signing certificate.

9 Click **OK** to save the connector.

10 Proceed to [Section 4.8, "Publishing a Connector to the Local Catalog,"](#) on page 29 to finish creating the new connector.

4.4 Downloading a Connector to a File

Access Manager enables you to save the connector to the local drive as a ZIP file that contains the XML definition for the connector. You can import this ZIP file on other Access Manager setups and use to configure applications.

Perform the following steps to download a connector:

- 1 In **Dashboard**, click **Administrative Tasks > Connector Studio**.
The Connector Studio page lists all connectors.
- 2 Click the **More Options** icon in the upper right corner of the connector that you want to download and click **Download**.
- 3 Save the ZIP file.

4.5 Importing a Connector from a File

You can import a connector as a file that you have downloaded from the same or a different Access Manager setup. The file must be in the ZIP format and contain a valid XML.

Perform the following steps to import a connector:

- 1 In **Dashboard**, click **Administrative Tasks > Connector Studio > + > Import Connector from file**.
- 2 Browse to and select the ZIP file.
The connector gets listed on the Connector Studio page.
- 3 Edit the details as required.
- 4 Publish the connector. See [Section 4.8, “Publishing a Connector to the Local Catalog,” on page 29](#).

4.6 Importing a Connector from the Global Catalog

The Global Catalog is a public website at <https://catalog.netiq.com> and contains existing SSO Assistant and SAML 2.0 connectors. If your Access Manager configuration does not have Internet connectivity, you can access the catalog from a different machine and download connectors to a file.

Perform the following steps to import a connector from the Global Catalog:

- 1 Click **Administrative Tasks > Connector Studio > + > Import Connector from Global Catalog**.
- 2 Select the required connector from the catalog.
The connector gets listed on the Connector Studio page.
- 3 Edit the details as required.
- 4 Publish the connector. See [Section 4.8, “Publishing a Connector to the Local Catalog,” on page 29](#).

4.7 Managing a Connector

Perform the following steps to edit, duplicate, and delete SSO Assistant and SAML connectors:

- 1 In **Dashboard**, click **Administrative Tasks > Connector Studio**.
- 2 Click the **More Options** icon in the upper right corner of the connector. Select any of the following commands based on your requirement:

Command	Description
Edit	Opens the Edit Connector page. For Access Manager to consider the modifications, you must publish the connector again. You must change the version or name of the connector before re-publishing it. Or, you can delete the published connector before publishing the changes.
Download	Saves the connector to a ZIP file that you can use on the local system or import to other Access Manager systems. For more information, see Section 4.4, “Downloading a Connector to a File,” on page 28 .
Publish	Publishes the connector to the Local Catalog. For more information, see Section 4.8, “Publishing a Connector to the Local Catalog,” on page 29 .
Duplicate	Creates an identical copy of the connector. You can modify the details to differentiate between two connectors.
Delete	Deletes the connector.

4.8 Publishing a Connector to the Local Catalog

After creating a connector, you can publish it to Access Manager’s Local Application Catalog. You can then select this connector to configure an application by using the Applications page (**Applications > + > Import Application from File** or **Add Application from Local Catalog**).

IMPORTANT: Connector Studio allows you to create connectors with configurations that can be used with other products apart from Access Manager. However, such connectors may not be compatible with Access Manager. If you attempt to publish a connector that contains settings that are not compatible with Access Manager, an error message is displayed.

Perform the following steps to publish a connector to the Local Application Catalog:

- 1 In **Dashboard**, click **Administrative Tasks > Connector Studio**.
The Connector Studio page lists all available connector.
- 2 Click the **More Options** icon in the upper right corner of the connector and click **Publish**.
- 3 Confirm that you want to publish the connector you created and click **Publish**.
- 4 Click **Yes** in the confirmation box.

4.9 Importing a Connector into the Applications Page

- 1 In **Dashboard**, click **Administrative Tasks > Applications > +** (plus).
Options to import connectors from the global catalog, file, and local catalog are available.
- 2 Select **Add Application from Local Catalog**.
- 3 Select the connector that you want to import into the Applications page.
- 4 Make changes based on your requirements.
- 5 Click **Save**.
- 6 Update Identity Server.

4.10 Example: Using an Existing SAML Connector to Configure an Application

This example describes how to import an existing SAML connector from the Global Catalog into Connector Studio, create a SAML connector, and configure an application based on this connector in the Applications page. Let us use an existing SAML type connector for Salesforce for understanding these tasks.

- ♦ [Section 4.10.1, “Importing a SAML 2.0 Connector from the Global Catalog,” on page 30](#)
- ♦ [Section 4.10.2, “Modifying a SAML Connector,” on page 30](#)
- ♦ [Section 4.10.3, “Importing the SAML Connector into the Applications Page,” on page 33](#)

4.10.1 Importing a SAML 2.0 Connector from the Global Catalog

- 1 In **Dashboard**, click **Administrative Tasks > Connector Studio > + > Import connector from Global Catalog**.
- 2 In the Connector Catalog window, specify `salesforce` to see existing connectors that have been created for Salesforce, then select the Salesforce SAML connector to import into Connector Studio.

4.10.2 Modifying a SAML Connector

- 1 In Connector Studio, click the **More Options** icon on the Salesforce connector that you have imported in the [“Importing a SAML 2.0 Connector from the Global Catalog” on page 30](#) section.
- 2 Click **Edit**.

Configuration options on each page are as follows. The default configuration values for the Salesforce connector are shown in italics.

General

Field	Value
Target Name	<i>Salesforce</i>
Version	1.10.1

Field	Value
Description for Provider	<i>SAML connector to Salesforce</i> Not used with Access Manager.
Description for Tenant	<i>SAML connector to Salesforce</i>
Certificate required for provider	Not selected This option is not selected in the default Salesforce connector because a signing certificate is not required when doing identity provider type single sign-on to Salesforce. For example, when the user clicks the Salesforce appmark in the Access Manager user portal page.
Change Image	An image is specified

Settings

Field	Value
Name	<i>ssoStartPage</i> Where <i>ssoStartPage</i> is a replaceable value represented as $\${ssoStartPage}$ in the connector XML and as shown in the configuration fields on Metadata and Assertion configuration pages when this setting is chosen from the list of settings.
Display Name	<i>Login URL</i> Where <i>Login URL</i> is the name used to represent this replaceable value in the selection lists shown on the Metadata and Assertion pages while configuring the connector in Connector Studio, and also under the Application Connector Setup section of the Applications page when configuring the application based on this connector. The value entered for Login URL in the Applications page becomes the AssertionConsumerService endpoint in the metadata that gets created for the application.
Data Owner	<i>Tenant</i>
Type	<i>URL</i>
Min	<i>1</i>
Max	<i>1024</i>
Description	<i>The Login URL is the value of the Salesforce Assertion Consumer Service URL assigned to a particular client. This is the value identified as the Salesforce.com Login URL on the Single Sign-on Settings page.</i>
Default Value	<i>https://login.salesforce.com</i>
Required	Selected
Concealed	Not selected

Metadata

Field	Value
Method	<i>Generate</i>
EntityID	<i>https://saml.salesforce.com</i>
Signing Certificate	Not populated
Assertion Consumer Service URL	<i>`\${ssoStartPage}`</i>
Logout URL	Not used by the Salesforce service provider.
Logout URL Binding	Not used by the Salesforce service provider.
Logout Response URL	Not used by the Salesforce service provider.
Import from File	Not used by the Salesforce service provider.
Import from URL	Not used by the Salesforce service provider.

Attributes

Field	Value
Name	<i>Subject/NameID</i> Where Subject/NameID is used to identify the attribute in the SAML assertion sent to the application.
Display Name	<i>Salesforce ID</i> Where Salesforce ID is the name used to represent this mapping in the Assertion page of Connector Studio and in the Attributes section of the Applications page.
Data Owner	<i>Tenant</i>
Encoding	<i>None</i>
Description	<i>Contains the user's Salesforce ID.</i>
Default Value	<i>mail</i>
Required	Selected
Role Attribute	Not selected

Assertion

Field	Value
Audience Restriction	<i>https://saml.salesforce.com</i>
Name ID	<i>Salesforce ID</i> Where Salesforce ID is the Display Name of the attribute mapping created on the Attributes page. The mapping results in the value of the user's local LDAP mail attribute being used to populate the value of the NameID element and the remote attribute "Subject/NameID" in the SAML assertion.
Format	<i>Email</i>
Destination URL	Not specified

Federation Instructions

Field	Description
<code>#{entityID}</code>	Represents the value of Identity Server cluster's Entity ID.
<code>#{ssoURL}</code>	Represents the value of the Identity Server cluster's single sign-on URL.
<code>#{sloURL}</code>	Represents the value of the Identity Server cluster's single logout URL.
<code>#{sloReturnURL}</code>	Represents the value of the Identity Server cluster's logout return URL.
<code>#{signingCert}</code>	Represents the value of the Identity Server cluster's default signing certificate.

- 3 Click **OK**.
- 4 Click the **More Options** icon on the connector > **Publish** to save the connector into the Local Application Catalog of Access Manager or click **More Options** > **Download** to save the connector to a ZIP file in the local file system.

4.10.3 Importing the SAML Connector into the Applications Page

- 1 In **Dashboard**, click **Administrative Tasks** > **Applications** > + > **Add Application from Local Catalog**.
- 2 Select the Salesforce connector that you published in "**Modifying a SAML Connector**" on [page 30](#).

The connector is imported into the Applications page and opened for editing.

The following table lists the mapping between fields and respective configuration in the Connector Studio page and the Applications page:

Connector Studio	Applications Page
General > Target Name	Name
General > Description for Tenant	Description
General > Version	Created from Connector with version [<i>Version</i>]

Connector Studio	Applications Page
General > Image	Default image
Settings	Application Connector Setup
Metadata	Application Connector Setup
Assertion	Application Connector Setup
Attributes	Attributes
Federation Instructions	System Setup

- 3 Edit the values based on your requirements.
- 4 Click **Save** to create a Salesforce application.
- 5 Update Identity Server.

The following are few important points:

- ♦ The **Settings** and **Attributes** sections contain help icons. When you mouse over the icon, help text is displayed that was specified in the **Description** fields of the connector.
- ♦ Clicking **Show** in the **System Setup** section displays the federation instructions that contain substituted actual values for the `${ssoURL}`, `${sloURL}`, `${entityID}`, and other replaceable values that were specified in the connector's federation instructions.
- ♦ Settings and attribute mappings that are configured as **Required** in the connector are flagged with a red asterisk. If you remove the default values, a warning symbol is displayed indicating that a required value is not available. If an application is saved without configuring required settings, the application is displayed under **Application needs more information** on the Applications page.
- ♦ Saving the application creates an associated appmark that, by default, is visible in the user portal page.
- ♦ A SAML 2.0 service provider is created. You can view or edit the details of this service provider by clicking **Advanced Settings**.

5 SAML Connectors

Access Manager provides a number of SAML 2.0 connectors to create secure and federated connections to applications. You can manage these connectors through the Applications page in Administration Console Dashboard under **Administration Tasks**.

SAML 2.0 connectors simplify the configuration process of establishing a federated connection between applications or web services and Access Manager.

When you import and configure a SAML 2.0 connector, Access Manager automatically creates an appmark for the connector. The role assignments that you specify while configuring a connector allow access to the applications and the role assignment on the appmarks determines whether users can see the appmark on the User Portal or in the MobileAccess app.

- ♦ [Section 5.1, “Understanding Federated SSO with SAML 2.0,” on page 35](#)
- ♦ [Section 5.2, “Global Requirements for SAML 2.0 Connectors,” on page 38](#)
- ♦ [Section 5.3, “Configuring a Connector for a SAML Application,” on page 38](#)
- ♦ [Section 5.4, “Managing SAML 2.0 Applications,” on page 39](#)
- ♦ [Section 5.5, “Converting SAML 2.0 Service Providers in to a SAML 2.0 Application,” on page 40](#)
- ♦ [Section 5.6, “Unique ID,” on page 41](#)

To see the list of all SAML connectors that Access Manager provides, refer to [Application Connector Catalog > SAML \(http://catalog.netiq.com/ncarest/displayCatalog?type=saml\)](#).

For information about SAML connectors that support account provisioning, see [Part 6, “SAML/Account Management Connectors,” on page 43](#).

5.1 Understanding Federated SSO with SAML 2.0

To understand the federated single sign-on process with Access Manager, you must understand SAML 2.0.

- ♦ [Section 5.1.1, “Understanding SAML 2.0,” on page 35](#)
- ♦ [Section 5.1.2, “Understanding SAML 2.0 Federated SSO Processes with Access Manager,” on page 36](#)

5.1.1 Understanding SAML 2.0

SAML is an XML-based framework for communicating user authentication, entitlement, and attribute information. For more information see, [Security Assertion Markup Language \(SAML\) V2.0 Technical Overview \(http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-tech-overview-2.0.html\)](#)

SAML 2.0 creates a two-way agreement between two vendors asserting that the information provided is valid. It provides a standard framework to share this information, so you do not need to recreate the configuration for every vendor you want to share information.

To use the SAML 2.0 connectors provided for Access Manager, you must understand the basic concepts and components of SAML 2.0.

SAML 2.0 defines each of the components using the XML schema. You must be able to read and format documents in XML to use SAML 2.0 connectors.

XML-based framework: You must understand the XML format, structure, elements, and how it defines rules for encoding documents. For more information, see [Introduction to XML \(http://www.w3schools.com/xml/xml_what.asp\)](http://www.w3schools.com/xml/xml_what.asp) on the [w3schools \(http://www.w3schools.com\)](http://www.w3schools.com) website.

Assertion: SAML assertions define the syntax for creating XML-encoded assertions to describe authentication, attribute, and authorization information for an entity. The SAML 2.0 connectors help create the assertions for Access Manager and the federation applications.

Attributes: LDAP attributes passed between two entities. In this case, it is LDAP attributes passed between Access Manager and connected federation applications.

Metadata: Metadata defines how SAML 2.0 shares configuration information between two communicating entities. You must be able to access and share the Access Manager metadata information with the federated application. You must also be to access and share the federated application metadata with Access Manager

Protocols: SAML 2.0 supports HTTP, HTTPS, and SOAP protocols. The SAML 2.0 connectors use HTTPS to establish a secure connection between Access Manager and the federated applications. To establish the secure HTTPS connection, you must obtain the certificate from the metadata of Access Manager and the application. Each side then uses the other side's certificate to create the secure connection.

5.1.2 Understanding SAML 2.0 Federated SSO Processes with Access Manager

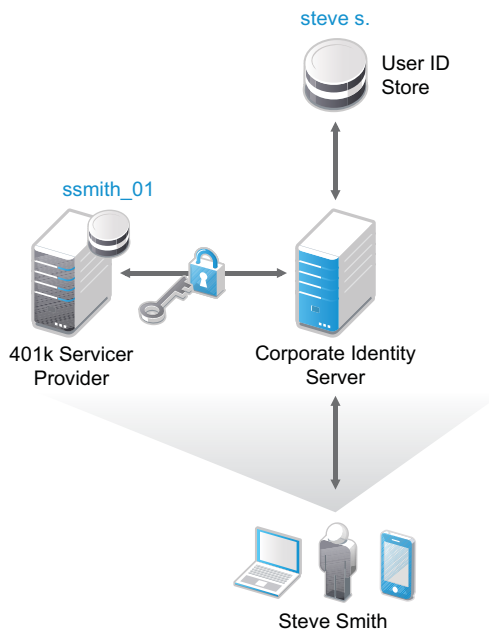
Federated SSO relies on a trust relationship between an identity provider and a service provider to give users access to web services or applications.

SAML 2.0 is an open standard for federation that provides a vendor-neutral means of exchanging user identity, authentication, attribute information, and authorization information. SAML 2.0 defines the structure and content of assertions and protocol messages used to transfer this information between Access Manager and the web services or applications (service providers). For more information about SAML 2.0, see [Section 5.1.1, "Understanding SAML 2.0," on page 35](#).

Using a SAML 2.0 connection, the service provider (web services or applications) trusts the identity provider (Access Manager) to validate the user's authentication credentials and to send identity information about the authenticated user. The service provider accepts the data and uses it to give the user access to the web service or application. This data exchange is transparent for the user. It allows the user to access the web service or application without providing additional credentials.

Figure 5-1 illustrates how a SAML SSO authentication works with Access Manager:

Figure 5-1 Access Manager SSO with SAML 2.0



1. The user Steve Smith authenticates to the corporate Identity Server (Access Manager) with his corporate user name and password.
2. Access Manager authenticates Steve against the user name steve s. and associated password in the user store.
3. Steve accesses User Portal with an appmark to the 401k application that he is entitled to use.
4. When Steve clicks the 401k appmark, Access Manager produces an authentication assertion or token for the 401k application (service provider) that contains the identity attributes needed for authentication.
5. The 401k application consumes the assertion or token to establish a security context for the user with Access Manager.
6. The 401k application uses the assertion or token to validate that steve s. is ssmith_01 and authorizes the authentication (resource request).
7. The 401k application establishes a session with Steve.

Access Manager now provides a simpler means of creating the SAML 2.0 federation for SSO by providing connectors for specific applications. When you use the connectors, Access Manager automatically creates an appmark for the web service or application and places the appmark on the User Portal page for users to access. You can limit access to the SAML 2.0 web service or application by using role assignments configured on the **Applications** page. You can limit visibility of the SAML 2.0 appmarks on the User Portal page by using role assignments configured on the appmarks.

Access Manager allows you to convert the existing SAML 2.0 service providers to applications that you can manage from the **Applications** page. The benefit of conversion is to add the ability to configure access control to the application using roles. For more information, see [Section 5.5, “Converting SAML 2.0 Service Providers in to a SAML 2.0 Application,”](#) on page 40.

5.2 Global Requirements for SAML 2.0 Connectors

All SAML 2.0 connectors have unique requirements. However, some of the requirements are the same no matter which SAML 2.0 connector you use. Ensure that you meet the following global requirements before configuring a SAML 2.0 connector:

- ❑ SAML 2.0 connectors are not supported in a mixed Access Manager environment. All components of Access Manager (Identity Server clusters, Access Gateway clusters, and Administration Console) must be of the same version.
- ❑ An understanding of identity federation using the SAML 2.0 protocol. For more information, see [Section 5.1.2, “Understanding SAML 2.0 Federated SSO Processes with Access Manager,”](#) on page 36.

5.3 Configuring a Connector for a SAML Application

The following is the common procedure for configuring a SAML connector. For specific details, see the instructions embedded within the individual connectors.

1. Log in to Administration Console as an administrator.
2. In **Dashboard**, under **Administrative Tasks**, click **Applications**.
3. Select the appropriate Identity Server cluster to use the application.
4. Click the plus sign **+** and then perform any one of the following actions:
 - ◆ Click **Add Application from Catalog**, then search for the SAML 2.0 connector that you want to configure.
For more information, see [Chapter 2, “Application Connector Catalog,”](#) on page 9.
 - ◆ Click **Import Application from File**, then browse to and select the file.
5. (Optional) Review the name of the application, and specify additional appmarks if needed.
6. In **System Setup**, click **Show** to view the federation instruction.
7. Configure the SAML application as instructed in the federation instructions
8. At Access Manager, review and configure **Application Connector Setup**, **Attributes**, **Access and Roles**, and **System Setup**.
You can find the help associated with each field when you mouse over the help icon.
9. Click **Save**.
10. Click **Configuration Panel** and update all servers.

NOTE: If the federation is not setup successfully after configuring the connector, refer to the application’s latest metadata or contact the support team.

5.4 Managing SAML 2.0 Applications

Each connector that you import and configure contains the **More Options** (⋮) icon on the upper right corner. This icon enables you to disable, delete, and download the application to a connector.

You can save the configuration information at any stage and complete the SAML 2.0 connector configuration later. If you save any SAML 2.0 application without configuring all required details, the application appears at the top of the list of connectors on the left side of the Applications page under the heading **Application needs more information**. The **More Options** icon does not appear on this connector until you complete the configuration.

Any section of the SAML 2.0 connector that requires information contains a red warning symbol. Until the configuration is complete, Access Manager does not configure an appmark or a service provider for the application.

5.4.1 Disabling and Enabling a SAML Application

- 1 In **Dashboard**, click **Administrative Tasks > Applications**.
- 2 Click the **More Options** (⋮) icon in the upper right corner of the connector that you want to disable.
- 3 Click **Disable**.
- 4 Update Identity Server for it to take effect. The application gets disabled.
- 5 Click **More Options** icon of the disabled connector > **Enable** and then update Identity Server if you want to enable it.

5.4.2 Deleting a SAML Application

- 1 Click the **More Options** (⋮) icon in the upper right corner of the connector that you want to delete.
- 2 Click **Delete**.
- 3 Update Identity Server.

5.4.3 Downloading a SAML Application

You can download a SAML application as a connector and use it to create any number of applications in the same or different Access Manager setups. However, when you download an application, a few settings configured for this application in the Applications page or in the SAML 2.0 configuration pages for the associated service provider will not be exported to the downloaded file.

The downloaded connector includes the following details:

- ♦ Application's name, icon, and description.
- ♦ The settings configured in the **Application Connector Setup** section. These settings are used to generate Assertion Consumer Service URL, Binding, Entity ID, Name ID, and Signing Certificate in the metadata for the associated service provider. However, if the metadata of the associated service provider object contains elements other than the ones listed here, those elements will not be preserved.

- ◆ The settings configured in the **Attributes** section. The attribute mappings are preserved, but the **Send With** option is cleared for all mappings.
- ◆ The settings configured in the **System Setup** section. However, the **Show** button may display only partial federation instructions if this application was converted from a SAML service provider.

The downloaded connector does not include the following details:

- ◆ Any setting that you have configured in SAML 2.0 configuration pages
- ◆ Roles or contracts configured in the **Access and Roles** section on the Applications page
- ◆ Unique ID
- ◆ Additional certificate of the service provider
- ◆ Additional appmarks

Perform the following steps to download a SAML application:

- 1 Click the **More Options** icon in the upper right corner of the connector that you want to download.
- 2 Review the details and click **Download**.
- 3 Click **OK** to save the application as a zip file that contains the XML definition for the connector.

5.5 Converting SAML 2.0 Service Providers in to a SAML 2.0 Application

If you have configured federated authentication using SAML 2.0 to internal and external identity providers, service providers, and embedded service providers (ESP), you can convert the previously configured SAML 2.0 service providers to a SAML 2.0 application.

For more information about the prior configuration for service providers, see “[Configuring SAML 2.0](#)” in the *Access Manager 4.5 Administration Guide*.

Converting the service providers gives you the following benefits:

- ◆ Adds the ability to configure access control to the application by using roles.
- ◆ Automatically creates an appmark for the application.

No change takes place to the appmarks that you had created for SAML 2.0 service providers. The conversion process only adds a new appmark for the SAML 2.0 application, if you select to create a new appmark.

In an upgraded Access Manager setup, the Applications page displays any service providers you have created in the past. Access Manager does not convert the service provider until you click it and save the new configuration options.

If the service provider contains only one signing certificate, you cannot upload the additional certificate after conversion. However, if the service provider has been configured with multiple signing certificate, the application retains the configured certificates after conversion.

To convert a service provider to an application:

- 1 Log in to Administration Console as an administrator.

2 In Dashboard, click **Administration Tasks > Applications**.

3 Identify the service provider you want to convert and click it.

If the service provider is not converted, then there is no menu in the upper right corner of the tile and the image is a default SAML image for all SAML 2.0 service providers.

4 Review the available options to ensure that these are correct.

NOTE: If you have existing appmarks, Access Manager populates the **Roles** field with the roles assignments from the existing appmarks. The roles assignments here grant the users accessibility to applications. The role assignments on the appmark grants visibility to appmarks for the users.

5 Click **Save** to convert the SAML 2.0 service provider to be a SAML 2.0 application.

6 Click **Yes** to create a new appmark for this SAML 2.0 application.

7 Click the **Configuration Panel**, then perform an **Update All**.

After you convert a SAML 2.0 service provider to a SAML 2.0 application, the **Advanced Setup** links appear in each configuration section. You can use these links to view or edit additional settings.

5.6 Unique ID

While creating a SAML application, if the specified entity ID is already in use by another service provider, Access Manager prompts to specify a different entity ID or a unique ID. You must specify a different entity ID or a unique ID to create the application.

Consider the following points while specifying a unique ID:

- ♦ A unique ID can contain numbers, alphabets, special characters or combination of all.
- ♦ A unique ID must not contain spaces.
- ♦ A unique ID must not contain patterns `uniqueid` or `naminstance` (case-insensitive).
- ♦ A unique ID must be unique among all unique IDs available for different SAML 2.0 service providers in the Identity Server cluster.
- ♦ Adding a unique ID changes the Access Manager identity provider's metadata, such as single sign-on endpoint and entity ID, for that service provider. The service provider uses this new metadata for establishing federation with Access Manager.

Later, if you change the unique ID, you must re-import Access Manager identity provider's new metadata for that service provider.

For more information, see "[Configuring Different Instances of a SAML 2.0 Service Provider in an Identity Server Cluster](#)" in the *Access Manager 4.5 Administration Guide*.

6 SAML/Account Management Connectors

The Application Connector Catalog includes a specialized set of connectors called `Account Management Connectors`. In addition to simplifying Access Manager configuration, these connectors can also configure SaaS Account Manager (SAM) in Access Manager to automatically provision user accounts at the corresponding SaaS providers. SAM can provision user accounts, update, and deprovision accounts for connected applications based on changes made in your user store.

Each SAML/Account Management connector requires configuration at the SaaS provider. Detailed instructions are available when you configure the application in Access Manager Administration Console.

When you save your application configuration, SAM starts provisioning users from the specified LDAP user stores that are members of the filtered groups to the SaaS provider. Depending on the number of users and groups in your user stores, the operation time varies.

To see the list of all SAML/Account Management connectors that Access Manager provides, see [Application Connector Catalog > Account Management \(http://catalog.netiq.com/ncarest/displayCatalog?type=accmgmt\)](http://catalog.netiq.com/ncarest/displayCatalog?type=accmgmt).

NOTE: SAM supports only SAML 2.0 applications.

Prerequisite

To provision SAML accounts by using SAM, you must first deploy the SAM appliance and configure the appropriate SAML/Account Management connector for the SAML application.


For more information about deploying the SAM appliance and SAML/Account Management connectors, see the [NetIQ SaaS Account Management 1.0 'Installation Guide \(https://www.netiq.com/documentation/saas-account-management-10/sam-install/data/bookinfo.html\)](https://www.netiq.com/documentation/saas-account-management-10/sam-install/data/bookinfo.html) and [NetIQ SaaS Account Management 1.0 Connectors Guide \(https://www.netiq.com/documentation/saas-account-management-10/sam-connectors/data/bookinfo.html\)](https://www.netiq.com/documentation/saas-account-management-10/sam-connectors/data/bookinfo.html).

You do not need to perform any action in Access Manager. Installing and configuring SAM automatically configure the SAM-NAM integration.

Perform the following steps in Access Manager to configure a new SAML/Account Management connector:

1. On **Dashboard**, under **Administrative Tasks**, click **Applications**.
2. Select the appropriate Identity Server cluster to use the application.
3. Click the plus sign + and then perform any of the following actions:
 - ◆ Click **Add Application from Catalog**, click the filter icon, select **Account Management**, and then search for the connector that you want to configure.
For more information, see [Chapter 2, "Application Connector Catalog," on page 9](#).
 - ◆ Click **Import Application from File** and select the file.

4. (Optional) Review the name of the application and specify additional appmarks if needed.
5. Review and configure other sections: **Application Connector Setup**, **Attributes**, **Access and Roles**, and **System Setup**.
6. Expand the **Account Management** section and select **Enable Account Management**.
7. Click **Setup Instructions** and follow the help for configuring the service account and completing other steps at the SAML application site.
8. Provide the required information, such as credentials for the service account and other details, for the SaaS application. This information varies depending on the connector.
9. Under **LDAP User Store Configuration**, specify the user store information:

Field	Description
User Store	Select the user store that you want SAM to use for provisioning users to SaaS applications.
Polling Interval	Specify a duration for SAM to check your LDAP user store for changes
LDAP Groups and Authorizations	<p>Select the LDAP groups containing users that might be provisioned to SaaS applications.</p> <p>You can map authorizations returned by the SaaS application, such as licenses, service plans, roles, and groups to the local LDAP groups in the Access Manager user stores. While provisioning qualified users from the LDAP user stores to a SaaS application, SAM creates these users with the authorizations as mapped in the LDAP Groups and Authorizations page. Click the LDAP Groups and Authorizations  icon to perform the following actions:</p> <ul style="list-style-type: none"> ◆ Add, view, or remove the selected groups. ◆ Manage authorizations for the selected groups. <p>NOTE: The LDAP Groups and Authorizations page does not work in Microsoft Internet Explorer and Microsoft Edge 18 or earlier. Consider upgrading to the new Chromium-based Edge (which provides backward-compatibility with IE 11) or using another browser, such as Chrome or Firefox.</p>

(Conditional) If you want to add more than one user store, click the plus (+) icon next to the heading and provide the similar information for the additional user store. Repeat this step to add multiple user stores.

10. Click **Save**.

After you save your application configuration, SAM begins provisioning users from the specified LDAP user stores that are members of the filtered groups to the SaaS service provider.

7 Configuring the Application for Access Manager on the Public Cloud

Access Manager provides a connector that simplifies the procedure for creating a SAML 2.0 federated connection between an on-premises Access Manager setup and a cloud-based Access Manager setup.

This connector helps you configure single sign-on (SSO) to the on-premises applications and cloud-based applications of an organization and provides seamless login experience to users.

Using this connector, you can configure an Access Manager Identity Server as a SAML 2.0 identity provider (IDP) by importing the SAML 2.0 metadata of another Access Manager Identity Server that will act as a service provider (SP).

NOTE: By default, this connector establishes the transient federation between two Access Manager setups. If needed, you can later change the type of federation by using **Advanced Setup** under **Attributes** on the application page.

This section includes the following topics:

- ♦ [Section 7.1, “Requirements for the Access Manager Connector,” on page 45](#)
- ♦ [Section 7.2, “Importing and Configuring the Connector,” on page 46](#)
- ♦ [Section 7.3, “Example Scenarios,” on page 47](#)

7.1 Requirements for the Access Manager Connector

To use this connector, you must meet the following requirements:

- Ensure that you have met the global requirements for SAML 2.0 connectors. For more information, see [Section 5.2, “Global Requirements for SAML 2.0 Connectors,” on page 38](#).
- An administrator account for both Access Manager setups is available.
- Users must be able to access both Identity Servers. However, direct communication between Identity Servers is not required.
- The metadata URL of the Access Manager setup acting as an SP is reachable from the Administration Console of the IDP setup.
- The user store must be available in the Access Manager IDP setup.
- Both on-premises and cloud-based Access Manager Identity Server cluster instances are running, resolvable, and reachable during the connector administration process.

7.2 Importing and Configuring the Connector

You need to import and configure the connector on the Access Manager setup that will act as the IDP.

This section provides information about how to create the SAML relationship between the IDP setup, on which you are configuring the connector, and the Access Manager SP setup.

Perform the following steps to import and configure the connector:

- 1 Log in to Administration Console of the Access Manager system that will be the IDP.
- 2 In **Dashboard**, under **Administrative Tasks**, click **Applications**.
- 3 Select the desired Identity Server cluster.
- 4 Click **+** (plus sign) to import the connector.
- 5 Click **Add Application from Catalog**, and then search for the Access Manager connector.
For more information, see [Chapter 2, "Application Connector Catalog,"](#) on page 9.
- 6 Specify a name and description for the connector.
- 7 In **Application Connector Setup**, specify the following details:

Field	Description
Access Manager IDP Base URL	Specify the base URL of Access Manager Identity Server that will become the SP. For example, <code>https://spidp.com:8443/nidp</code>
Get Metadata	Click this to retrieve the metadata from the base URL specified in Access Manager IDP Base URL . This action populates the required values in Assertion consumer service URL , EntityID , Logout response URL , and Logout URL . In addition, it downloads the signing certificate of the SP.
Destination URL	(Optional) Specify the URL to which users are redirected after being authenticated to the SP via SAML. The specified URL will become the URL (Target override) value specified in the default appmark that is created when saving the application.

- 8 In **Attributes**, keep the default attribute mappings to map values from the local user store into attributes sent with the assertion. See the Help information associated with the options for modifying the default mappings if necessary.
- 9 (Optional) In **Access and Roles**, specify the following details:

Field	Description
Roles	Select the role assignments to determine the user accessibility of this application.
Contracts	Select the contract presented to users when they click the appmark. Users see the specified contract unless the contract is satisfied during login or through the authentication levels.

- 10 In **System Setup**, perform the following actions:

Field	Description
Metadata	(Optional) You can view or download the metadata information from Access Manager that can be used later to create the federated connection at the SP.
Signing Certificate	(Optional) You can view or download the signing certificate from Access Manager to create for later use when creating the federated connection at the SP setup.
Federation Instructions	Click Show to display the federation instructions. These instructions provide detailed steps that you must perform at the Access Manager setup that will be configured as the SP. If clicking Show returns an error and does not display the federation instructions, ensure that the machine (virtual or physical) where Administration Console is being accessed can connect directly to the base URL of the Identity Server cluster.

- 11 Click **Save**.

- 12 Click **Configuration Panel**, and then update the Identity Server.

If the Identity Server health status turns yellow after the update, it is likely due to an untrusted certificate. For more information, see [“Managing the Keys, Certificates, and Trust Stores”](#) in the *Access Manager 4.5 Administration Guide*.

An appmark is created automatically after saving the application. By default, all users can see this appmark on their user portal page. The appmark is configured with a target URL set to the value specified in the **Destination URL** field you configured in [Step 7 on page 46](#).

- 13 In the **System Setup** section, click **Show** to display the federation instructions. Follow these instructions at the Access Manager setup that will act as the SP.

7.3 Example Scenarios

- ◆ [Section 7.3.1, “Scenario 1: Cloud-based IDP and On-Premises SP with a Protected Resource,”](#) on page 48
- ◆ [Section 7.3.2, “Scenario 2: On-Premises IDP and Cloud-based SP with a Protected Resource,”](#) on page 48
- ◆ [Section 7.3.3, “Scenario 3: On-Premises IDP and Cloud-based SP with Third-party SP,”](#) on page 49
- ◆ [Section 7.3.4, “Scenario 4: On-Premises IDP, Cloud-based SP with Third-party SP, and Third-party SP Is Accessible from On-Premises User Portal,”](#) on page 51

7.3.1 Scenario 1: Cloud-based IDP and On-Premises SP with a Protected Resource

In this scenario, the cloud-based setup is configured as the IDP and the on-premises setup is configured as the SP. The SP setup has Access Gateway protected resources.

The protected resources need to be accessed from appmarks displayed in the user portal page of the cloud-based setup.

User Flow

1. A user browses to the URL of the cloud-based user portal page and specifies the credentials.

The user sees the expected appmarks including the appmark for the Access Gateway protected resource at the on-premises SP.
2. The user clicks the appmark for the protected resource. The user is authenticated to the on-premises SP using the SAML protocol.

After a successful SAML authentication, the user sees the expected content of the protected resource.

Configuration Details

1. Establish the federation between the two setups by importing and configuring the Access Manager SAML connector at the cloud-based setup to create the SAML application.
2. Follow the federation instructions provided by SAML application to complete the federation at the on-premises setup.

With this configuration, the cloud-based Access Manager setup acts as an IDP while the on-premises Access Manager setup acts as an SP.
3. At the on-premises setup, configure an Access Gateway protected resource with **Authentication Procedure** set to `Any Contract`.
4. At the cloud-based setup, use the Applications page to create an appmark for the Access Manager SAML application and configure **URL (Target override)** with the public URL of the Access Gateway protected resource at the on-premises setup.

7.3.2 Scenario 2: On-Premises IDP and Cloud-based SP with a Protected Resource

In this scenario, the on-premises setup is configured as the IDP and the cloud-based setup is configured as the SP. The SP setup has Access Gateway protected resources.

The protected resources need to be accessed from appmarks displayed in the user portal page of the on-premises setup.

User Flow

1. A user browses to the URL of the on-premises user portal page and specifies the credentials.

The user sees the expected appmarks including the appmark for the Access Gateway protected resource at the cloud-based SP.

2. The user clicks the appmark for the protected resource. The user is authenticated to the cloud-based SP the SAML protocol.

After a successful SAML authentication, the user sees the expected content of the protected resource.

Configuration Details

1. Establish the federation between the on-premises and cloud-based setups by importing and configuring the Access Manager SAML connector at the on-premises setup to create the SAML application
2. Follow the federation instructions provided by the SAML application to complete the federation at the cloud-based setup.

With this configuration, the on-premises Access Manager acts as an IDP and the cloud-based Access Manager acts as an SP.

3. At the cloud-based setup, configure an Access Gateway protected resource with **Authentication Procedure** set to *Any Contract*.
4. At the on-premises setup, use the Applications page to create an appmark for the Access Manager SAML application and configure **URL (Target override)** with the public URL of the Access Gateway protected resource at the cloud-based setup.

7.3.3 Scenario 3: On-Premises IDP and Cloud-based SP with Third-party SP

This scenario builds upon [Scenario 2: On-Premises IDP and Cloud-based SP with a Protected Resource](#) by adding additional configuration required for SSO to third-party SAML SPs, such as Salesforce, Google, and Office 365. These service providers are configured and trusted by the cloud-based Access Manager setup.

This scenario enables SSO to the cloud-based user portal page and third-party SPs when the users log in to the on-premises setup.

User Flow

1. A user browses to the URL of the on-premises Access Manager IDP user portal page and specifies credentials.

The user sees the expected appmarks including the new appmark for the user portal page at the cloud-based Access Manager setup.

2. The user clicks the appmark for the user portal page at the cloud-based setup.

The user is authenticated to the cloud-based SP using the SAML protocol.

After a successful SAML authentication, the user sees the user portal page of the cloud-based setup.

3. The user clicks the appmark for the third-party SP.

After a successful SAML authentication, the user sees the expected content of the SP.

Configuration Details

1. Establish the federation between the two Access Manager setups and verify as described in [Scenario 2: On-Premises IDP and Cloud-based SP with a Protected Resource](#).

2. Configure the on-premises setup as follows:

- a. In the Applications UI, modify the Access Manager application and add an additional appmark.
- b. In **URL (Target override)**, specify the URL of the user portal page of the cloud-based Access Manager setup.
- c. Modify the attribute set originally created and used by the Access Manager SAML application in **Administration Console > Shared Settings**.

By default, the mappings for sn and givenName are created. Add the additional attribute mappings as follows:

Local Attribute	Remote Attribute
Ldap Attribute: cn	cn
Ldap Attribute: GUID	GUID
Ldap Attribute: mail	mail

- d. In the Applications page for the Access Manager connector, select **Send with** for all attributes in the **Attributes** section.

3. Configure the cloud-based setup as follows:

- a. Verify that the SAML 2.0 federations have been configured with third-party SPs, such as Salesforce, Google, and Office 365. After logging in to the user portal page of the cloud-based setup, users see appmarks associated with each provider. Users are single signed-on to these providers when clicking the respective appmarks.
- b. Modify the attribute set originally created when following federation instructions to create the IDP object in **Administration Console > Shared Settings**.

By default, the mappings for sn and givenName are created. Add the additional attribute mappings as follows:

Local Attribute	Remote Attribute
Ldap Attribute: cn	cn
Ldap Attribute: objectGUID	GUID
Ldap Attribute: mail	mail

- c. Go to **Devices > Identity Server > Edit > SAML 2.0 > [IDP] > Configuration > Attributes**. Modify the IDP object and move all attributes to the **Obtain at authentication** field. All these attributes will be obtained during authentication.

If the Office 365 SAML application is configured at the cloud-based setup, ensure that the `SAML2_OFFICE365_NAMEID_ATTRIBUTE_NAME` property is configured for the Office 365 SP. Else, SSO may fail for users being federated from the on-premises setup.

Configuring SAML2_OFFICE365_NAMEID_ATTRIBUTE_NAME

- 1 In the cloud-based Administration Console, click **Devices > Identity Servers > cluster > Edit > SAML 2.0 > [Office 365 SP] > Configuration > Options**.

- 2 Click **New**.
- 3 Select **Other** from the list.
- 4 Specify the following values:
 - Property Name:** SAML2_OFFICE365_NAMEID_ATTRIBUTE_NAME
 - Property Value:** objectGUID
- 5 Click **OK**.
- 6 Update the Identity Server cluster.

7.3.4 Scenario 4: On-Premises IDP, Cloud-based SP with Third-party SP, and Third-party SP Is Accessible from On-Premises User Portal

This scenario builds upon [Scenario 3: On-Premises IDP and Cloud-based SP with Third-party SP](#) by adding appmarks for each third-party service provider (Salesforce, Google, and Office 365) on the user portal page of the on-premises setup. With this configuration, users can access these service providers without navigating to the user portal page of the cloud-based Access Manager setup.

In addition to the configurations made in the scenario 3, you need to add appmarks on the Access Manager SAML application at the on-premises setup.

User Flow

1. A user browses to the URL of the on-premises Access Manager IDP user portal page and specifies credentials.

The user sees the expected appmarks including the new appmarks for each third-party SP configured in the cloud-based Access Manager setup.
2. The user clicks any of the appmarks for the third-party SP.

After a successful SAML authentication to the cloud-based Access Manager setup, the user is single signed-on to the third-party SP and redirected to the appropriate destination.

Configuration Details

1. Follow the steps for configuring [Scenario 3: On-Premises IDP and Cloud-based SP with Third-party SP](#). See “[Configuration Details](#)” on page 51.
2. Configure additional appmarks on the Access Manager SAML application at the on-premises setup (one for each third-party SAML SP configured in the cloud-based setup).

- a. In the Applications page of the on-premises setup, open the Access Manager SAML application for editing.
- b. In the Appmarks region, click + to add an additional appmark.
- c. Specify an appropriate value for Name and other settings as desired.
- d. In **URL (Target Override)**, specify the URL of the appmark at the cloud-based setup.

You can copy this URL from the appmark editor for the third-party application, under **URL used by Appmark on User Portal** at the cloud-based setup.

A typical configuration of a Google application contains an appmark with a URL that includes scheme, Identity Server Base URL, PID, and an optional Target.

The following are examples for Salesforce, Google, and Office 365 configuration:

Salesforce: `https://idp.baseurl.cloud:8443/nidp/saml2/idpsend?PID=TSP_3bdb77e5-9515-4f2d-9699-86c0a48fba2c`

Google: `https://idp.baseurl.cloud:8443/nidp/saml2/idpsend?PID=TSP_59d317d4-85cb-407a-9d39-431a88ad164a&target=https://mail.google.com/a/cloudtest13.info`

Office 365: `https://idp.baseurl.cloud:8443/nidp/saml2/idpsend?PID=TSP_975bf51a-91b8-4a35-ab48-5aad5cdc8510`

3. Repeat the step 2 for each third-party SAML application for which you want to create an appmark at the on-premises setup.

NOTE: If the Office 365 SAML application is configured at the cloud-based setup, ensure that the `SAML2_OFFICE365_NAMEID_ATTRIBUTE_NAME` property is configured for the Office 365 SP. Else, SSO may fail for users being federated from the on-premises setup.

For information about how to configure this property for the Office 365 SP, see [“Configuring SAML2_OFFICE365_NAMEID_ATTRIBUTE_NAME” on page 50](#).

8

Configuring the Applications for Office 365 Using WS Federation and WS-Trust

Access Manager provides a connector for Microsoft Office 365 that allows you to create a federated connection between Access Manager and Microsoft Office 365 by using WS Federation and WS-Trust protocols.

This connector simplifies the configuration process to establish a federated connection between Office 365 and Access Manager. This connector supports both passive mode applications, such as SharePoint, and active mode applications, such as Skype.

When you import and configure the connector, Access Manager automatically creates an appmark for the users.

- ◆ [Section 8.1, “Prerequisites for Configuring the Connector,” on page 53](#)
- ◆ [Section 8.2, “Configuring an Office 365 Domain to Federate with Access Manager,” on page 53](#)
- ◆ [Section 8.3, “Configuring the Connector,” on page 56](#)

8.1 Prerequisites for Configuring the Connector

- ❑ WS-Trust and WS Federation protocols are enabled in Access Manager.

Perform the following steps:

1. In Administration Console, click **Devices > Identity Servers > Edit**.
 2. In the **Enabled Protocols** section, ensure that **WS-Trust** and **WS Federation** are selected.
- ❑ An Office 365 administrative account is available. This administrative user must not belong to the Office 365 domain that your organization will manage.
 - ❑ Microsoft does not support sub-domains having different federated settings than their parent. To use a sub-domain for Office 365, ensure that either you do not use Office 365 with the parent domain, or both the parent domain and its sub-domain have the identical federation settings.
 - ❑ An Office 365 domain for your organization is available. See [Section 8.2, “Configuring an Office 365 Domain to Federate with Access Manager,” on page 53](#).

8.2 Configuring an Office 365 Domain to Federate with Access Manager

You must configure an Office 365 domain before using the Office 365 connector.

- ◆ [Section 8.2.1, “Prerequisites for Configuring an Office 365 Domain,” on page 54](#)
- ◆ [Section 8.2.2, “Enabling Federation Settings in the Office 365 Domain,” on page 54](#)
- ◆ [Section 8.2.3, “Verifying Single Sign-On Access,” on page 55](#)

8.2.1 Prerequisites for Configuring an Office 365 Domain

- ❑ Identity Server must be accessible from outside the firewall so that the Office 365 domain can communicate with Identity Server.
- ❑ Sign up for an Office 365 account.
- ❑ For enabling single-sign on to the Office 365 applications, ensure that you download the application from the Office 365 portal.
- ❑ Create a federated domain in Office 365 and prove ownership of it. This ensures that you add your company domain into the Office 365 domain.

For more information, see [Adding and Verifying a Domain for Office 365 \(https://docs.microsoft.com/en-us/microsoft-365/admin/setup/add-domain?view=o365-worldwide\)](https://docs.microsoft.com/en-us/microsoft-365/admin/setup/add-domain?view=o365-worldwide).

- ❑ Ensure that the Windows 7 or Windows 8 workstations do not have the Active Directory Federation Service 2.0 snap-in installed.
- ❑ Ensure that the SSL certificate is issued by a well-known external certification authority (CA).
- ❑ If you are using Microsoft Lync or Microsoft Outlook thick clients with WS-Trust, replace the default self-signed SSL server certificate included with Access Manager with one that is signed by a public CA. This enables Office 365 to establish a trusted SSL session with Access Manager. For more information, see “[Managing Trusted Roots and Trust Stores](#)” in the *Access Manager 4.5 Administration Guide*.

NOTE: If you are using Microsoft Lync, ensure that you enable federation. For more information, see [Lync External Access \(https://office.microsoft.com/en-in/support/let-lync-online-users-communicate-with-external-lync-or-skype-contacts-HA102817865.aspx?CTT=5&origin=HA102817356\)](https://office.microsoft.com/en-in/support/let-lync-online-users-communicate-with-external-lync-or-skype-contacts-HA102817865.aspx?CTT=5&origin=HA102817356).

- ❑ Install Microsoft Live Sign-in Module to help manage and establish a remote session with the Office 365 account that is created to manage the Office 365 domain. To download, go to [Microsoft Downloads Center \(http://www.microsoft.com/en-us/download/details.aspx?id=41950\)](http://www.microsoft.com/en-us/download/details.aspx?id=41950).
- ❑ Install Microsoft Azure Active Directory Module. To download, go to [Manage Azure AD using Windows PowerShell \(https://docs.microsoft.com/en-us/office365/enterprise/powershell/connect-to-office-365-powershell\)](https://docs.microsoft.com/en-us/office365/enterprise/powershell/connect-to-office-365-powershell).

8.2.2 Enabling Federation Settings in the Office 365 Domain

Modify the following commands with your domain name as per your setup and run these in PowerShell. The domain name in the example is `nametest.com`.

- 1 Launch Windows Azure Active Directory Module for Windows PowerShell.
- 2 Run `$cred=Get-Credential` and specify your cloud service administrator account credentials.
- 3 Ensure that the Identity Server certificate is in the `.cer` format. Access Manager does not support the `.ctr` format.
- 4 Run `Connect-MSolService -Credential $cred`.

For example, if the name of the domain is `nametest.com` and **Base URL** of Identity Server is `https://nametest.com/nidp/`, run the following commands in PowerShell:

IMPORTANT: In this example, the port is not specified with **Base URL** because it uses the default port 443. If you are using a different port, specify the port with **Base URL**.

```
$dom = "namtest.com"
$url = "https://namtest.com/nidp/wsfed/ep"
$secpUrl = "https://namtest.com/nidp/wstrust/sts/active12"
$url = "https://namtest.com/nidp/wsfed/"
$logourl = "https://namtest.com/nidp/jsp/o365wsfedlogout.jsp"
$mex = "https://namtest.com/nidp/wstrust/sts/mex"
$cert = New-Object
System.Security.Cryptography.X509Certificates.X509Certificate2 "<name
and path of the certificate>"
$certData = [system.convert]::tobase64string($cert.rawdata)
$brand = "NamTest Co Bangalore"
```

5 Use the following cmdlet to update the settings of the single sign-on domain:

```
Set-MSolDomainAuthentication -FederationBrandName $brand -DomainName
$dom -Authentication Federated -PassiveLogOnUri $url -
SigningCertificate $certData -IssuerUri $uri -ActiveLogOnUri $secpUrl -
LogOffUri $logourl -MetadataExchangeUri $mex
```

8.2.3 Verifying Single Sign-On Access

You need at least one Office 365 user to verify that single sign-on is set up. If you have an existing user, ensure that the Immutable ID matches the GUID of the Access Manager user.

For example, if your user store is eDirectory and you want to retrieve the GUID of an existing Access Manager user, run the following command on the eDirectory server terminal:

```
ldapsearch -D cn=<context> -w <password> -b <search base> cn=<fqdn of the
administrator> GUID | grep GUID
```

Where D is the bind credential, w is the password, and b is the search scope.

Create an Office 365 user with this GUID as the Immutable ID by running the following command in PowerShell:

```
new-msoluser -userprincipalname "user1@domain name" -immutableid "GUID of
user1" - lastname "lastname of user 1" -firstname "user1" -DisplayName
"user1 users" -BlockCredential $false -LicenseAssignment
"testdomain:ENTERPRISEPACK" -usageLocation "two letter country
code[example: US,IN,DE,BE,GB etc]" -Password "password of the user"
```

To verify that single sign-on is set up correctly, perform the following steps in a server that is not added to the domain:

- 1 Go to [Microsoft Online Services \(http://login.microsoftonline.com/\)](http://login.microsoftonline.com/).
- 2 Log in with your corporate credentials.

For example, *user1@digitalairlines.com*

If single sign-on is enabled, the password field is disabled and the following message is displayed:

You are now required to Sign in at <your company>.

- 3 Click the **Sign in at <your company>** link.

If you are able to sign in without errors, single sign-on is set up successfully.

8.3 Configuring the Connector

- 1 Log in to Administration Console as an administrator.
- 2 In Dashboard, click **Applications** under Administrative Tasks.
- 3 (Conditional) Select the appropriate Identity Server cluster in **Cluster**.
- 4 Click the plus sign (+) and perform any one of the following steps:
 - 4a Click **Add Application from Catalog**, then search for the WS Federation and WS-Trust connector for Office 365. For more information, see [Chapter 2, “Application Connector Catalog,”](#) on page 9.
 - 4b Click **Import Application from File**, then browse to and select the file.
 - 4c Click **Add Application from Catalog** to select a custom connector.
- 5 Specify the following details:

Field	Description
Name	Specify a unique name for the connector.
Description	Specify a description of the connector. You can configure multiple connectors for Office 365. Ensure that you use a unique name and a description to help determine differences between the connectors.
Change Image (Optional)	Change the default image that the User Portal page displays to the users. Each connector contains a default image. You can change that image to any image you want. The maximum image size is 200 x 200 pixels and the ideal image size is 100 x 100 pixels. You can use an image from the Image Gallery or upload your own image.
Attributes: This section enables you to view and manage the attributes that are part of the assertion.	
ImmutableID	By default, <i>Ldap Attribute:GUID [LDAP Attribute Profile]</i> is selected.
User Principal Name (UPN)	By default, <i>Ldap Attribute:mail [LDAP Attribute Profile]</i> is selected.
Roles and Federation Instructions: This section enables you to control who has access to the application and how to configure the federation.	
Roles	Select the role assignments to determine the user accessibility of this application. The Role assignments made in the Appmark editor determine the user visibility of the appmarks associated with this application, not the accessibility of the application.

Field	Description
Federation Instructions	Contains the federation instructions on what you must change or modify in Office 365 to create the federated connection. Follow these instructions.

NOTE: The **Advanced Setup** does not appear in any of these sections until you save the connector.

6 Click **Save**.

