Access Manager Appliance
Applications Configuration Guide

October 2016

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.netiq.com/company/legal/.

Copyright © 2016 NetIQ Corporation, a Micro Focus company. All Rights Reserved.

Contents

About this Book and the Library **5**
About NetIQ Corporation **7**

1 Overview of Access Manager Appliance Applications **9**

1.1 Understanding Basic Single Sign-On . . . 9
1.2 Understanding Federated Single Sign-On with SAML 2.0 . . . 11
1.3 Understanding SAML 2.0 . . . 13

2 Using the Application Connector Catalog **15**

2.1 Accessing Connectors through Administration Console . . . 15
2.2 Accessing and Using the Application Connector Catalog through the Website . . . 15

3 Configuring Applications for Basic Single Sign-On **17**

3.1 Requirements for Using Basic SSO Connectors . . . 17
3.2 Configuring a Connector for Basic SSO . . . 18
3.3 Understanding the Configuration Options for the Connectors for Basic SSO . . . 19
3.4 Managing Icons . . . 20
3.5 Troubleshooting Basic Single Sign-On . . . 20

4 Managing SAML 2.0 Applications **21**

4.1 Global Requirements for SAML 2.0 Connectors . . . 21
4.2 Converting SAML 2.0 Service Providers in the Applications Page . . . 21

5 Configuring the Application for Google Apps **23**

5.1 Requirements for the connector for Google Apps . . . 23
5.2 Configuring the Connector for Google Apps . . . 23
5.3 Understanding the Configuration Options for the Connector for Google Apps . . . 24

6 Configuring the Application for Salesforce **27**

6.1 Requirements for the Connector for Salesforce . . . 27
6.2 Configuring the Connector for Salesforce . . . 28
6.3 Understanding the Configuration Options for the Connector for Salesforce . . . 28
6.4 Provisioning Users to Salesforce . . . 30

About this Book and the Library

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

Intended Audience

This guide provides information for Access Manager Appliance administrators who are responsible for configuring and managing the single sign-on to Access Manager Appliance. 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

The library provides the following information resources:

Installation and Upgrade Guide

Provides an introduction to Access Manager Appliance and describes the installation and upgrade procedures.

Help

Provides context-sensitive information and step-by-step guidance for common tasks, as well as definitions for each field on each window.

Developer Documentation

Provides a collection of developer tools and examples to design a flexible and expandable access management system to enable your applications to interact with the Identity Management capabilities of Access Manager Appliance, including federation, provisioning, and the secure delivery of identity information to client-based applications.

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

About NetIQ Corporation

We are a global, enterprise software company, with a focus on the three persistent challenges in your environment: Change, complexity and risk—and how we can help you control them.

Our Viewpoint

Adapting to change and managing complexity and risk are nothing new

In fact, of all the challenges you face, these are perhaps the most prominent variables that deny you the control you need to securely measure, monitor, and manage your physical, virtual, and cloud computing environments.

Enabling critical business services, better and faster

We believe that providing as much control as possible to IT organizations is the only way to enable timelier and cost effective delivery of services. Persistent pressures like change and complexity will only continue to increase as organizations continue to change and the technologies needed to manage them become inherently more complex.

Our Philosophy

Selling intelligent solutions, not just software

In order to provide reliable control, we first make sure we understand the real-world scenarios in which IT organizations like yours operate — day in and day out. That's the only way we can develop practical, intelligent IT solutions that successfully yield proven, measurable results. And that's so much more rewarding than simply selling software.

Driving your success is our passion

We place your success at the heart of how we do business. From product inception to deployment, we understand that you need IT solutions that work well and integrate seamlessly with your existing investments; you need ongoing support and training post-deployment; and you need someone that is truly easy to work with — for a change. Ultimately, when you succeed, we all succeed.

Our Solutions

- Identity & Access Governance
- Access Management
- Security Management
- Systems & Application Management
- Workload Management
- Service Management

Contacting Sales Support

For questions about products, pricing, and capabilities, contact your local partner. If you cannot contact your partner, contact our Sales Support team.

Worldwide:	www.netiq.com/about_netiq/officelocations.asp
United States and Canada:	1-888-323-6768
Email:	info@netiq.com
Website:	www.netiq.com

Contacting Technical Support

For specific product issues, contact our Technical Support team.

Worldwide:	www.netiq.com/support/contactinfo.asp
North and South America:	1-713-418-5555
Europe, Middle East, and Africa:	+353 (0) 91-782 677
Email:	support@netiq.com
Website:	www.netiq.com/support

Contacting Documentation Support

Our goal is to provide documentation that meets your needs. The documentation for this product is available on the NetIQ website in HTML and PDF formats on a page that does not require you to log in. If you have suggestions for documentation improvements, click **comment on this topic** at the bottom of any page in the HTML version of the documentation posted at www.netiq.com/documentation. You can also email Documentation-Feedback@netiq.com. We value your input and look forward to hearing from you.

Contacting the Online User Community

NetIQ Communities, the NetIQ online community, is a collaborative network connecting you to your peers and NetIQ experts. By providing more immediate information, useful links to helpful resources, and access to NetIQ experts, NetIQ Communities helps ensure you are mastering the knowledge you need to realize the full potential of IT investments upon which you rely. For more information, visit http://community.netiq.com.

1 Overview of Access Manager Appliance Applications

As an administrator, you have many users in your user stores that require access to many different web applications. In the past, you had to perform complex steps to configure identity federation between Access Manager Appliance and different web applications, depending on the authentication protocol. The identity federation allowed you to provide single sign-on (SSO) to your users. For more information, see "Federated Authentication" in the *NetIQ Access Manager Appliance 4.3 Administration Guide*.

Access Manager Appliance now provides a simplified way to give the users secure, single sign-on (SSO) access to different web applications. Access Manager Appliance contains the **Applications** page, under **Administration Tasks** in the Administration Console that allows you to configure basic single sign-on and SAML 2.0 applications.

Access Manager Appliance uses connectors to establish the connection between Access Manager Appliance and the applications. The User Portal page displays the applications as appmarks that the system automatically creates when you configure the connector for the application. For more information about appmarks, see "Configuring Appmarks" in the *NetIQ Access Manager Appliance 4.3 Administration Guide*.

There are different types of connectors that allow you to connect the applications.

- Section 1.1, "Understanding Basic Single Sign-On," on page 9
- Section 1.2, "Understanding Federated Single Sign-On with SAML 2.0," on page 11
- Section 1.3, "Understanding SAML 2.0," on page 13

1.1 Understanding Basic Single Sign-On

The purpose of Basic Single Sign-on (SSO) is to allow users to securely store their credentials for existing accounts of on-line applications while providing a single sign-on experience for users. For example, a user Maria has an account for Evernote. Maria uses Evernote to take notes for her job in marketing. Instead of logging into Evernote with separate credentials each time she wants to use it, she would log into Evernote once and Basic SSO will save and replay her saved credential every time she accesses Evernote.

Basic SSO and Form Fill policies both automatically populate HTML forms. Form Fill policies scan each login page, accelerated through the Access Gateway, to see if the Form Fill policy can populate the credential information. For more information, see "Form Fill Policies" in the *NetIQ Access Manager Appliance 4.3 Administration Guide*. Basic SSO does not go through the Access Gateway. Basic SSO provides connectors for the different applications. You configure the connector for the specific site. Basic SSO captures the users' credentials through a browser plugin or extension. It securely stores the users' credentials on the Identity Server, never using the Access Gateway.

Access Manager Appliance protects the users' credentials through an SSL connection and AES-256 encryption on Access Manager Appliance. The following graphic depicts how Access Manager Appliance securely stores the credentials.

Figure 1-1 How Access Manager Securely Stores Credentials

For the users to experience Basic SSO to an application, they must install the appropriate Basic SSO extension or plugin for their browser or install the MobileAccess app. The following occurs the first time a user logs in to access a Basic SSO application:

1. The user logs in to the User Portal page using their Access Manager Appliance credentials.
2. The user sees the appmarks for the available applications and clicks the appropriate appmark.
3. If the Basic SSO extension or plugin for the browser is not installed on the computer, Access Manager Appliance prompts the user to install it.
4. After installing the extension or plugin, the user must go back to the User Portal and click on the application a second time.
5. The extension or plugin opens a new tab where the user must enter their user name and password for the application.

   The user must enter the user name and password for the application once.
6. The extension or plugin captures the user's credentials for the application, then the extension or plugin sends the user's credentials to the Access Manager Appliance over an SSL connection.
7. The Access Manager Appliance 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 Access Manager Appliance.

   Access Manager Appliance encrypts the user's credentials with an encryption key that is unique per user account in Access Manager Appliance.
8. Access Manager Appliance then redirects the user to the application over an SSL connection.

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

The user must install the Basic SSO browser extension on each device where the user wants to access the application. Access Manager Appliance 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 Appliance 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 Appliance 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 if they are expired or stolen through the **Clear Single Sign-on Credentials** option.

If the user changes the user name or password to the account for the application, or if the user cancels the account, the user's stored credentials are no longer valid. 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. Access Manager Appliance removes the old credentials and stores the user's new credentials for subsequent logins to the application.

1.2 Understanding Federated Single Sign-On with SAML 2.0

Federated single sign-on relies on a trust relationship between an identity provider and a service provider to give users access to web services or applications. Access Manager Appliance uses SAML 2.0 (Security Assertion Markup Language) to create federated connections to web services and applications. The web services and applications are services providers and Access Manager Appliance is the identity provider.

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 Appliance and the web services or applications (service providers). For more information about SAML 2.0, see Section 1.3, "Understanding SAML 2.0," on page 13.

Using a SAML 2.0 connection, the service provider (web services and applications) trusts the identity provider (Access Manager Appliance) 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.

For example, Figure 1-2 shows you how a SAML single sign-on authentication works with Access Manager Appliance.

Figure 1-2 *Access Manager Appliance Single Sign-On with SAML 2.0*

1. The user Steve Smith authenticates to the corporate identity server (Access Manager Appliance) with his corporate user name and password.
2. Access Manager Appliance authenticates Steve against the user name steve s. and associated password in the user store.
3. Access Manager Appliance presents the User Portal page to Steve with an appmark to the 401k application that he is entitled to use.
4. When Steve clicks the 401k appmark on the User Portal page, Access Manager Appliance produces an authentication assertion or token for the 401k application (service provider) that contains the identity attributes needed for authentication.
5. The 401k application (service provider) consumes the assertion or token to establish a security context for the user with Access Manager Appliance (identity provider).
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 (service provider) establishes a session with Steve.

   Through this process, Steve entered his user name and password once for the corporate identity server.

In the past, Access Manager Appliance allowed you to configure federated authentication using SAML 2.0 to internal and external identity providers, service providers, and embedded service providers (ESPs). Access Manager Appliance now provides a simpler means of creating the SAML 2.0 federation for single sign-on by providing connectors for specific applications. When you use the connectors, Access Manager Appliance 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 configure 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 Appliance allows you to migrate the existing SAML 2.0 service providers to applications that you can manage from the **Applications** page. The main benefit of migration is to add the ability to configure access control to the application using roles.For more information, see Section 4.2, “Converting SAML 2.0 Service Providers in the Applications Page,” on page 21.

Access Manager Appliance provides a set of connector for SAML 2.0 applications that you can import through the Applications Connector Catalog or you can import from a file you save from the Applications Connector Catalog. You must import and configure the connector for the appropriate applications in your environment. Use the appropriate connector-specific chapters to configure the SAML 2.0 connector. For more information, see:

- Chapter 5, “Configuring the Application for Google Apps,” on page 23
- Chapter 6, “Configuring the Application for Salesforce,” on page 27

1.3 Understanding SAML 2.0

To understand and use the SAML 2.0 connectors Access Manager Appliance provides, you must have a very good understanding of SAML 2.0. SAML, developed by the Security Services Technical Committed of the Organization for the Advancement of Structured Information Standards (OASIS), 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.

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 have to recreate the configuration for every vendor you want to share information.

To use the SAML 2.0 connectors provided for Access Manager Appliance, you must understand the basic concepts and components of SAML 2.0. SAML 2.0 defines each of the components using XML schema. You must be able to read and format documents in XML to use the connectors for SAML 2.0.

XML: SAML 2.0 is an XML-based framework. This means you must understand the XML format, structure, elements, and how it defines rules for encoding documents. For more information, see Introduction to XML on the 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 Appliance and the federation applications.

Attributes: LDAP attributes passed between two entities. In this cases, it is LDAP attributes passed between Access Manager Appliance 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 Appliance metadata information with the federated application. You must also be to access and share the federated application metadata with Access Manager Appliance.

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 Appliance and the federated applications. To establish the secure HTTPS connection, you must obtain the certificate from the metadata from Access Manager Appliance and the application. Each side then uses the other side’s certificate to create the secure connection.

2 Using the Application Connector Catalog

Access Manager Appliance provides an Application Connector Catalog for you to see all of the available application connectors that Access Manager Appliance supports for single sign-on. We updates the Application Connector Catalog as soon as there is a new application connector available.

There are two ways to access Application Connector Catalog:

- Section 2.1, “Accessing Connectors through Administration Console,” on page 15
- Section 2.2, “Accessing and Using the Application Connector Catalog through the Website,” on page 15

2.1 Accessing Connectors through Administration Console

Importing and configuring a connector is part of the process of creating appmarks for the applications. You must import the connector from the Application Connector Catalog into Administration Console before you can configure the connector and create an appmark.

The Application Connector Catalog displays all available connectors. The catalog can display the connectors by name or by connector type. The two currently available connector

To accessing the Application Connector Catalog through Administration Console:

1. Log in to Administration Console Dashboard, then click **Administration Tasks** > **Applications**.
2. Click **+** (plus sign), then click **Add Application from Catalog**.
3. Browse or search through the catalog, then select the appropriate connector.
4. Configure the connector.

   For information about the Basic Single Sign-On applications, see Chapter 3, “Configuring Applications for Basic Single Sign-On,” on page 17. For information about the other connector types, see the application-specific chapter in this guide.

2.2 Accessing and Using the Application Connector Catalog through the Website

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

Accessing and using the website for the Application Connector Catalog:

1. Access the website for the Application Connector Catalog at https://catalog.netiq.com.
2. Browse through the catalog, then select the appropriate connector.

3 Click the desired application connector, then save the application connector.

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), then click **Import from File**.

7 Configure the connector.

For information about the Basic Single Sign-On applications, see Chapter 3, “Configuring Applications for Basic Single Sign-On,” on page 17. For information about the other connector types, see the application-specific section in this guide.

3 Configuring Applications for Basic Single Sign-On

Access Manager Appliance provides a way to securely provide single sign-on to applications for the users. Access Manager Appliance provides Basic Single Sign-On (SSO) connectors that are customized for each application to meet the interactive and content requirements for logging in to the application. The Basic SSO connectors work with Basic SSO extensions for browsers to securely collect, store, retrieve, and replay the users' authentication information for the application you select. For more information, see Section 1.1, "Understanding Basic Single Sign-On," on page 9.

Access Manager Appliance provides many connectors for Basic SSO 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. To see the list of current connectors, access this website (http://catalog.netiq.com/). For more information, see Section 2.2, "Accessing and Using the Application Connector Catalog through the Website," on page 15.

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

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

- Section 3.1, "Requirements for Using Basic SSO Connectors," on page 17
- Section 3.2, "Configuring a Connector for Basic SSO," on page 18
- Section 3.3, "Understanding the Configuration Options for the Connectors for Basic SSO," on page 19
- Section 3.4, "Managing Icons," on page 20
- Section 3.5, "Troubleshooting Basic Single Sign-On," on page 20

3.1 Requirements for Using Basic SSO Connectors

To use the connectors for Basic SSO, you must ensure that you meet the following requirements:

- ❒ Connectors for Basic SSO 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 the user.
  - ❒ The application requires the user's password to be sent for logging in to the application.
  - ❒ The application does not support using SAML 2.0 or WS-Federation protocols for federated trust relationships instead of sending passwords.
- ❒ The login page scheme must HTTPS not HTTP.

- The connectors for Basic SSO support user access to the application only through Chrome, Internet Explorer, and Firefox web browsers running on a desktop or laptop computer. The browsers work with the Basic SSO extension to securely collect, store, retrieve, and replay users' credentials for the applications.

  The connectors for Basic SSO support the following browser versions:

  - Chrome
  - Firefox 34 or later
  - Internet Explorer 11

  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 only the following versions:

  - iOS 9.*x*
  - Android Kit Kat 4.4 or Lollipop 5.*x*

- A user must install the Basic SSO extension in a supported browser one time on each desktop or laptop they use to access the Basic SSO 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 Appliance, Access Manager Appliance 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. The Firefox extension behaves the same way the Chrome extension behaves.

  For Internet Explorer, Access Manager Appliance prompts the user to install the Basic SSO extension, when the user accesses the application through Access Manager Appliance.

- Basic SSO is not supported in a mixed Access Manager Appliance environment. All nodes in the Access Manager Appliance cluster must be at 4.3 or later for Basic SSO to work.

3.2 Configuring a Connector for Basic SSO

The Application Connector Catalog contains all of the available Basic SSO connectors. You can import and configure as many of the connectors for Basic SSO as you need in Access Manager Appliance.

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

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

To configure a connector for Basic SSO:

1. Log in to Administration Console.
2. Click **Applications**.

3 Import a connector for Basic SSO from the Application Connector Catalog.

For more information, see Chapter 2, “Using the Application Connector Catalog,” on page 15.

4 Configure the connector for Basic SSO using the prompts.

For more information, see Section 3.3, “Understanding the Configuration Options for the Connectors for Basic SSO,” on page 19.

5 Click **Save**.

The **Applications** page displays the new connector for Basic SSO. The creation process of the connector for Basic SSO creates an appmark for the connector so that users can access it through the User Portal page. You must ensure that you have configured MobileAccess for the users to access and use the connectors you have added. For more information, see “Enabling Mobile and Web Access” in the *NetIQ Access Manager Appliance 4.3 Administration Guide*.

3.3 Understanding the Configuration Options for the Connectors for Basic SSO

You configure the connectors for Basic SSO in Administration Console under **Applications**. On each connector you import and configure, there is a menu on the upper right corner that allows to you to delete the connector. Clicking the plus sign (+) at the top of the page, allows you to import and configure a new connector. When you import a connector for Basic SSO the following options are available.

Table 3-1 *Connectors for Basic SSO Options*

Options	Description
Name	Specify a unique name for the connector for Basic SSO. Access Manager does not allow you to have two connectors with the same name.
Description	(Optional) Specify a description on the connector for Basic SSO. You can import and configure multiple connectors for the same application. You could have two connectors for Google 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 the users. Each connector for Basic SSO 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.
Roles	(Optional) Select the appropriate role from the list to determine which users see the appmarks for the connectors for Basic SSO on the User Portal page. If you do not assign a role, all users will see the appmark for the application on the User Portal page. All appmarks for the connectors for Basic SSO have a public endpoint to Identity Server (IdP). This means that even if a user is not a member of a role, and logs in to the User Portal page, plus they know the exact URL that is part of the appmark, the Basic SSO process starts. For more information about the Basic SSO process, see Section 1.1, “Understanding Basic Single Sign-On,” on page 9.
URL	Specify the URL that the users access when they click the appmark for the applications on the login page.

Options	Description
Enable	Select the user platforms where the appmark will be visible. The platforms are Desktop, iOS, and Android.
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 the connectors, it populates these fields for you.

3.4 Managing Icons

Access Manager provides a set of default images you can use when 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 Basic Single Sign-On

Use the following information to help troubleshoot issues with Basic SSO.

- ❒ Basic SSO can only work with one instance of Access Manager. If you have two instances of Access Manager and the user has an account for both system, when they try to log in to Basic SSO applications, they will have issues. Basic SSO uses sessions for save and replaying the users' credentials. Have multiple sessions open in the same browser will cause problems.
- ❒ The Basic SSO plugin for Internet Explorer 11 does not detect if you have a prior version of the plugin installed. Ensure that you do not have the Basic SSO plugin installed before installing the plugin. The name that appears in the control panel is the Single Sign-on Assistant. Currently, there is no upgrade path.
- ❒ The Basic SSO plugin for Internet Explorer 11 does not support authentication to multiple instances of the browser. An cookie mismatch error occurs followed by a forced logout.

4 Managing SAML 2.0 Applications

Access Manager Appliance provides a number of SAML 2.0 connectors for you to use to create secure, federated connections to applications. You manage these connectors through the Applications page in the Administration Console Dashboard under Administration Tasks.

4.1 Global Requirements for SAML 2.0 Connectors

All of the 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 Appliance environment. All nodes in the Access Manager Appliance cluster must be at 4.3 or later for the SAML 2.0 connectors to work.
- ❒

4.2 Converting SAML 2.0 Service Providers in the Applications Page

In the past, Access Manager Appliance allowed you to configure federated authentication using SAML 2.0 to internal and external identity providers, service providers, and embedded service providers (ESPs). For more information, about the prior configuration for service providers, see "Configuring SAML 2.0" in the *NetIQ Access Manager Appliance 4.3 Administration Guide*. This release of Access Manager Appliance provides a way for you to convert the previously configured SAML 2.0 service providers to become an application managed through the **Applications** page.

Converting the service providers gives you the following benefits:

- Adds the ability to configure access control to the application using roles
- Automatically walks you through creating an appmark for the application

After you have upgraded to Access Manager Appliance 4.3 the new **Applications** page displays any service providers you have created in the past. Access Manager Appliance does not convert the service provider until you click on it.

To convert a service provider to an application:

1. Log in to Administration Console as an administrator.
2. In Administration Console Dashboard, click **Administration Tasks** > **Applications**.
3. Find the service provider you want to convert in the list of applications on the left.
4. Click the appropriate service provider.
5.

5 Configuring the Application for Google Apps

Access Manager Appliance provides a connector for Google Apps that allows you to create a federated connection between Access Manager Appliance and Google Apps. The federated connection uses SAML 2.0 to help you create a single sign-on experience for your users.

The connector for Google Apps simplifies the configuration process to establish a federated connection between Google Apps and Access Manager Appliance. When you import and configuration the connector, Access Manager Appliance automatically creates an appmark for the users to use in MobileAccess.

5.1 Requirements for the connector for Google Apps

To use the connector for Google Apps, you must meet the following requirements:

- ❒ An understanding of identity federation using the SAML 2.0 protocol. For more information, see Section 1.3, “Understanding SAML 2.0,” on page 13.
- ❒ A premier Google Apps account with the provisioning APIs enabled on the Google account.
- ❒ Read through and understand the single sign-on documentation from Google. For more information, see SAML-based Federated SSO.
- ❒ The metadata file from Google Apps including a signing certificate from Google Apps.
- ❒ Login URL from Google Apps.
- ❒ User accounts for each user in Google Apps who wants access to the single sign-on service for Google Apps.

To configure a federated connection between Access Manager Appliance and Google Apps, you must use the federation instructions you obtain when you configure the connector. The federation instructions contain metadata specific to Access Manager Appliance, certificates, and any other information you need to properly configure the federated connection.

5.2 Configuring the Connector for Google Apps

The connector for Google Apps uses a SAML 2.0 connection between Access Manager Appliance and Google Apps. The connector helps you create a federated connection between Access Manager Appliance and Google Apps so when your users log in to the User Portal page, they only have to authenticate once. For more information, see Section 1.2, “Understanding Federated Single Sign-On with SAML 2.0,” on page 11.

To configure the connector for Google Apps:

1. Log in to Administration Console as an administrator.
2. In the **Dashboard**, under **Administrative Tasks**, click **Applications**.
3. (Conditional) Select the appropriate IDP cluster to use application. If you only have one IDP cluster, there is nothing to select.

4 Click the plus sign + to import the SAML 2.0 connector for Google Apps.

4a Click **Add Application from Catalog**, then search for the SAML 2.0 connector for Google Apps.

For more information, see Chapter 2, "Using the Application Connector Catalog," on page 15.

or

4b Click **Import Application from File**, then browse to and select the file.

5 Configure the connector for Google Apps following the prompts.

For more information, see Section 3.3, "Understanding the Configuration Options for the Connectors for Basic SSO," on page 19.

6 Click **Save**.

5.3 Understanding the Configuration Options for the Connector for Google Apps

You configure the connectors for Google Apps in Administration Console Dashboard, under **Administration Tasks > Applications**. On each connector you import and configure, there is a menu on the upper right corner that allows to you to delete the connector. Clicking the plus sign (+) at the top of the page allows you to import and configure a new connector. When you import a connector for Google Apps the following options are available.

The **Applications** page populates a number of fields for you. It is able to use information in your environment to help populate the metadata and other fields. The information in the Federation Instructions is specific to your environment.

Table 5-1 *Connector for Google Apps Configuration Options*

Options	Description
Name	Specify a name for the connector for Google Apps.
Description	(Optional) Specify a description on the connector for Google Apps. You could have two connectors for Google Apps 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 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.
Application Connector Setup	This section displays the metadata information Access Manager Appliance requires from Google Apps to create the federated connection. **NOTE:** The **Advanced Setup** does not appear until you save the connector.
Application Connector Setup > **Login URL**	Specify the **Google Apps Assertion Consumer Service URL** assigned to a particular client.In the Google Apps administration tool, this is the value identified as the **Google Apps.com Login URL** on the Single Sign-On Settings page.

Options	Description
Application Connector Setup > **Metadata**	Displays the metadata for the connector. You can view or download the metadata. If you have not saved the connector, the system creates the SAML 2.0 metadata using the values provided and other values from the connector.
Application Connector Setup > **Signing Certificate**	Uploads a signing certificate file to secure communication between Access Manager Appliance and Google Apps. Or it displays the content of the signing certificate if you have saved the connector. The system automatically adds this new certificate to the trust store for Administration Console. However, this new certificate is not automatically added to the trust store for the IDP cluster. **IMPORTANT:** You must manually add this signing certificate to the IDP Cluster trust store or the health of the IDP cluster turns yellow and users do not see this new appmark when they log in to the User Portal page. For more information, see "Managing Certificates and Keystores" in the *NetIQ Access Manager Appliance 4.3 Administration Guide*.
Attributes	Allows you to see and manage the attributes that are part of the SAML 2.0 assertion. **NOTE:** The **Advanced Setup** does not appear until you save the connector.
Attributes > **Subject/NameID**	Select the appropriate attribute from Google Apps for the ID of the users. Typically, the user's email address is the user ID for Google Apps.
Attributes > **Additional mappings**	(Conditional) If you have configured Just-in-Time provisioning, you must add an additional attribute map. For more information, see Section 6.4, "Provisioning Users to Salesforce," on page 30.
Access and Roles	Allows you to control who has access to the application. **NOTE:** The **Advanced Setup** does not appear until you save the connector.
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.
Contracts	Select the contracts presented to users when they click the appmark. The users see these contract unless the contract is satisfied during login or through the authentication levels.
System Setup	Displays the metadata information from Access Manager Appliance to use in Google Apps to create the federated connection.
System Setup > **Metadata**	You can view or download the metadata information from Access Manager Appliance to create the federated connection.
System Setup > **Signing Certificate**	You can view or download the signing certificate from Access Manager Appliance to create the federated connection.
System Setup > **Federation Instructions**	Contains the federation instructions on what you must change or modify in Google Apps to create the federated connection. Follow the federated instructions.

6 Configuring the Application for Salesforce

Access Manager Appliance provides a connector for Salesforce that allows you to create a federated connection between Access Manager Appliance and Salesforce. The federated connection uses SAML 2.0 to help you create a single sign-on experience for your users.

In prior releases of Access Manager Appliance, there were many detailed steps required to configure this type of connection to Salesforce. For more information, see "Integrating Salesforce With Access Manager By Using SAML 2.0" in the *NetIQ Access Manager Appliance 4.3 Administration Guide*.

The new connector for Salesforce simplifies the configuration process to establish a federated connection between Salesforce and Access Manager Appliance. When you import and configure the connector, Access Manager Appliance automatically creates an appmark for the users that by default appears in the User Portal page and in the MobileAccess app. We recommend that you use the new connector for Salesforce to configure a SAML 2.0 federated connection between Salesforce and Access Manager Appliance.

Use the following information to help you configure a SAML 2.0 federated connection between Salesforce and Access Manager Appliance.

- Section 6.1, "Requirements for the Connector for Salesforce," on page 27
- Section 6.2, "Configuring the Connector for Salesforce," on page 28
- Section 6.3, "Understanding the Configuration Options for the Connector for Salesforce," on page 28
- Section 6.4, "Provisioning Users to Salesforce," on page 30

6.1 Requirements for the Connector for Salesforce

To use the connector for Salesforce, you must meet the following requirements:

- ❒ An understanding of identity federation using the SAML 2.0 protocol. For more information, see Section 1.3, "Understanding SAML 2.0," on page 13.
- ❒ A full or developer type Salesforce account.
- ❒ Read through and understand the single sign-on documentation from Salesforce. For more information, see Configuring SAML Settings for Single Sign-On.
- ❒ The metadata file downloaded from Salesforce. If you will use service provider (SP) initiated single sign-on, you must extract the signing certificate from this metadata file and save the certificate file in `.pem` format.
- ❒ The login URL from Salesforce.com. It is available in the downloaded metadata file as the Location value for `AssertionConsumerService`.
- ❒ The connector for Salesforce does not provision user accounts. You must either manually create user accounts at Salesforce or use the Salesforce Just-In-Time provisioning feature. The Salesforce Just-in-Time provisioning feature requires additional configuration steps. For more information, see Section 6.4, "Provisioning Users to Salesforce," on page 30.

IMPORTANT: If you do not configure Salesforce for Just-in-Time provisioning, user accounts that match accounts in the Identity Server must already exist in Salesforce for single sign-on to function.

To configure the required **Single Sign-On** settings at Salesforce, use the **Federation Instructions** available in the **System Setup** section when you configure or edit the connector for Salesforce. These **Federation Instructions** contain metadata specific to Access Manager Appliance including URLs, certificates, and other information you need to properly configure the **Single Sign-On** settings in Salesforce.

6.2 Configuring the Connector for Salesforce

Ensure that you have meet all of the requirements before configuring the connector for Salesforce. For more information, see Section 6.1, "Requirements for the Connector for Salesforce," on page 27.

To configure the connector for Salesforce:

1. Log in to Administration Console as an administrator.
2. In the **Dashboard**, under **Administrative Tasks**, click **Applications**.
3. (Conditional) Select the appropriate IDP cluster to use application. If you only have one IDP cluster, there is nothing to select.
4. Click the plus sign **+** to import the SAML 2.0 connector for Salesforce.
   - **4a** Click **Add Application from Catalog**, then search for the SAML 2.0 connector for Salesforce.

     For more information, see Chapter 2, "Using the Application Connector Catalog," on page 15.

     or
   - **4b** Click **Import Application from File**, then browse to and select the file.
5. Configure the connector for Salesforce following the prompts.

   For more information, see Section 6.3, "Understanding the Configuration Options for the Connector for Salesforce," on page 28.
6. Click **Save**.
7. Click the **Configuration Panel**, then perform an **Update All** to have the changes take effect.

6.3 Understanding the Configuration Options for the Connector for Salesforce

You configure the connectors for Salesforce in Administration Console Dashboard, under **Administration Tasks** > **Applications**. On each connector you import and configure, there is a menu on the upper right corner that allows to you to delete the connector. Clicking the plus sign (**+**) at the top of the page allows you to import and configure a new connector. When you import a connector for Salesforce the following options are available.

The **Applications** page populates a number of fields for you. It is able to use information in your environment to help populate the metadata and other fields. The information in the Federation Instructions is specific to your environment.

Table 6-1 Connector for Salesforce Configuration Options

Options	Description
Name	Specify a name for the connector for Salesforce.
Description	(Optional) Specify a description on the connector for Salesforce. You could have two connectors for Salesforce 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 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.
Application Connector Setup	This section displays the metadata information Access Manager Appliance requires from Salesforce to create the federated connection. **NOTE:** The **Advanced Setup** does not appear until you save the connector.
Application Connector Setup > **Login URL**	Specify the **Salesforce Assertion Consumer Service URL** assigned to a particular client.In the Salesforce administration tool, this is the value identified as the **Salesforce.com Login URL** on the Single Sign-On Settings page.
Application Connector Setup > **Metadata**	Displays the metadata for the connector. You can view or download the metadata. If you have not saved the connector, the system creates the SAML 2.0 metadata using the values provided and other values from the connector.
Application Connector Setup > **Signing Certificate**	Uploads a signing certificate file to secure communication between Access Manager Appliance and Salesforce. Or it displays the content of the signing certificate if you have saved the connector. The system automatically adds this new certificate to the trust store for Administration Console. However, this new certificate is not automatically added to the trust store for the IDP cluster. **IMPORTANT:** You must manually add this signing certificate to the IDP Cluster trust store or the health of the IDP cluster turns yellow and users do not see this new appmark when they log in to the User Portal page. For more information, see "Managing Certificates and Keystores" in the *NetIQ Access Manager Appliance 4.3 Administration Guide*.
Attributes	Allows you to see and manage the attributes that are part of the SAML 2.0 assertion. **NOTE:** The **Advanced Setup** does not appear until you save the connector.
Attributes > **Subject/NameID**	Select the appropriate attribute from Salesforce for the ID of the users. Typically, the user's email address is the user ID for Salesforce.
Attributes > **Additional mappings**	(Conditional) If you have configured Just-in-Time provisioning, you must add an additional attribute map. For more information, see Section 6.4, "Provisioning Users to Salesforce," on page 30.
Access and Roles	Allows you to control who has access to the application. **NOTE:** The **Advanced Setup** does not appear until you save the connector.

Options	Description
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.
Contracts	Select the contracts presented to users when they click the appmark. The users see these contract unless the contract is satisfied during login or through the authentication levels.
System Setup	Displays the metadata information from Access Manager Appliance to use in Salesforce to create the federated connection.
System Setup > **Metadata**	Allows you to view or download the metadata information from Access Manager Appliance to create the federated connection.
System Setup > **Signing Certificate**	Allows you to view or download the signing certificate from Access Manager Appliance to create the federated connection.
System Setup > **Federation Instructions**	Contains the federation instructions on what you must change or modify in Salesforce to create the federated connection. Follow the federated instructions.

6.4 Provisioning Users to Salesforce

To have single sign-on work, the users must have an account in Salesforce. This means you must manually create the users in Salesforce or configure the Just-In-Time provisioning feature in Salesforce.

Just-in-Time provisioning automatically creates an account for the user the first time they log in to Salesforce by using the SAML 2.0 assertion from Access Manager Appliance.

To use Just-in-Time provisioning, you must make configuration changes in both Salesforce and Access Manager Appliance. Ensure that you have read the documentation from Salesforce for Just-in-Time provisioning before proceeding. For more information, see About Just-in-Time Provisioning for SAML.

NOTE: User account names in Salesforce are in email form. Ensure that the value for the `User.Username` attribute in the SAML 2.0 assertion is in the form an email.

Configuring Just-in-Time provisioning:

1. In the Salesforce, configure the Single Sign-On (SSO) settings.
   - **1a** Configure the following fields:

     SAML Identity Type: Select **Assertion contains the Federation ID from the User object**.

     User Provisioning Enable: Select this option.

     User Provisioning Type: Select **Standard**.
   - **1b** Save your changes.
   - **1c** From Salesforce, download the metadata.
2. Configure the connector for Salesforce. For more information, see Section 6.2, “Configuring the Connector for Salesforce,” on page 28.

3 Create a new attribute set between Access Manager Appliance and Salesforce.

3a In the Administration Console, click **Devices** > **Identity Servers**.

3b Click **Shared Settings**.

3c Under **Attribute Sets**, click **New**.

3d Create an attribute set to map attributes between Access Manager Appliance and Salesforce.

3d1 Specify a name for the attribute set, then click **Next**.

3d2 Click **New**, then use the following information to create an attribute mapping:

Local attribute: Select **Ldap Attribute:mail**.

Remote attribute: Specify `User.Email`.

3d3 Leave all of the other fields to the default values, then click **OK**.

3d4 Click **New**, then use the following information to create an attribute mapping:

Local attribute: Select **Ldap Attribute:sn**.

Remote attribute: Specify `User.LastName`.

3d5 Leave all of the other fields to the default values, then click **OK**.

3d6 Click New, then use the following information to create an attribute mapping:

Local attribute: Select **Ldap Attribute:cn**.

Remote attribute: Specify `User.Username`.

3d7 Leave all of the other fields to the default values, then click **OK**.

3d8 Click **New**, then select **Constant**.

3d9 Use the following information to create a constant defining what type of Salesforce account the users have:

Constant: Specify the profile type for the users account. For example, `Chatter Free User`.

Remote attribute: Specify `User.ProfileId`.

3d10 Leave all of the other fields to the default values, then click **OK**.

3d11 Click **Finish**, then **Close**.

4 Add the attribute map created in Step 3 to the Service Provider for Salesforce.

4a In Administration Console, click **Devices** > **Identity Servers**, then select the Identity Server running the connector for Salesforce.

4b Click the **Trusted Providers** tab.

4c In the **Service Providers** list, click the Salesforce Service Provider.

4d Click the **Attributes**.

4e In the **Attributes set** field, select the attribute map you created in Step 3d1.

4f Select all of the four attributes in the **Available** panel, then click the left arrow to add the attribute to the **Send with authentication** panel.

4g Click **OK** twice.

4h In the Status field next to the Identity Server name, click **Update**.

With this configuration, the SAML 2.0 assertion sent by Access Manager Appliance contains all of the information required to create an account for a user in Salesforce. The first time a user logs in to the User Portal and clicks on the appmark for Salesforce, Salesforce creates an account and the user is authenticated.

IMPORTANT: Ensure that you have populated the local attributes specified in the attribute set in Step 3d in the Access Manager Appliance user store and that these attributes are in the format required by Salesforce.