



# File Access Manager Installation with SAML and SSO

Version: 8.4

Revised: March 27, 2023

---

## Copyright and Trademark Notices

### Copyright © 2023 SailPoint Technologies, Inc. All Rights Reserved.

All logos, text, content, including underlying HTML code, designs, and graphics used and/or depicted on these written materials or in this Internet website are protected under United States and international copyright and trademark laws and treaties, and may not be used or reproduced without the prior express written permission of SailPoint Technologies, Inc.

"SailPoint," "SailPoint & Design," "SailPoint Technologies & Design," "Identity Cube," "Identity IQ," "IdentityAI," "IdentityNow," "SailPoint Predictive Identity" and "SecurityIQ" are registered trademarks of SailPoint Technologies, Inc. None of the foregoing marks may be used without the prior express written permission of SailPoint Technologies, Inc. All other trademarks shown herein are owned by the respective companies or persons indicated.

SailPoint Technologies, Inc. makes no warranty of any kind with regard to this manual or the information included therein, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. SailPoint Technologies shall not be liable for errors contained herein or direct, indirect, special, incidental or consequential damages in connection with the furnishing, performance, or use of this material.

Patents Notice. <https://www.sailpoint.com/patents>

Restricted Rights Legend. All rights are reserved. No part of this document may be published, distributed, reproduced, publicly displayed, used to create derivative works, or translated to another language, without the prior written consent of SailPoint Technologies. The information contained in this document is subject to change without notice.

Use, duplication or disclosure by the U.S. Government is subject to restrictions as set forth in subparagraph (c) (1) (ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 for DOD agencies, and subparagraphs (c)(1) and (c)(2) of the Commercial Computer Software Restricted Rights clause at FAR 52.227-19 for other agencies.

Regulatory/Export Compliance. The export and re-export of this software is controlled for export purposes by the U.S. Government. By accepting this software and/or documentation, licensee agrees to comply with all U.S. and foreign export laws and regulations as they relate to software and related documentation. Licensee will not export or re-export outside the United States software or documentation, whether directly or indirectly, to any Prohibited Party and will not cause, approve or otherwise intentionally facilitate others in so doing. A Prohibited Party includes: a party in a U.S. embargoed country or country the United States has named as a supporter of international terrorism; a party involved in proliferation; a party identified by the U.S. Government as a Denied Party; a party named on the U.S. Department of Commerce's Entity List in Supplement No. 4 to 15 C.F.R. § 744; a party prohibited from participation in export or re-export transactions by a U.S. Government General Order; a party listed by the U.S. Government's Office of Foreign Assets Control as ineligible to participate in transactions subject to U.S. jurisdiction; or any party that licensee knows or has reason to know has violated or plans to violate U.S. or foreign export laws or regulations. Licensee shall ensure that each of its software users complies with U.S. and foreign export laws and regulations as they relate to software and related documentation.

---

# Contents

---

- Configuring to use SAML Authentication ..... 4**
  - Creating an Okta Application ..... 5
  - Creating an ADFS Application ..... 14
  - Creating an Azure Application ..... 18
  - Switching from SAML to Windows Authentication Mode ..... 23
- System Settings Required to Support SSO .....28**
  - System Settings to Support SSO - Okta .....29
  - System Settings to Support SSO - ADFS ..... 34
  - System Settings to Support SSO - Azure ..... 35

## Configuring to use SAML Authentication

The File Access Manager login process can be integrated with any SAML 2.0 identity provider.

This guide details integration steps for the following providers:

- Azure
- Okta
- ADFS

You can later switch between SAML login and Windows login (See [Switching from SAML to Windows Authentication Mode](#))

### *To support SAML login*

1. Create a dedicated application within the identity provider for the File Access Manager authentication

Follow the installation for your identity provider:

- a. [Creating an Azure Application](#)
- b. [Creating an Okta Application](#)
- c. [Creating an ADFS Application](#)

2. Follow the File Access Manager installation instructions in this guide, with the following points
  - On the **Website authentication mode** screen, select SAML 2.0 (See [Website Authentication Mode](#))
  - Do not create an identity store
3. After installation set up the authentication on the File Access Manager servers and database to accept the SSO login.

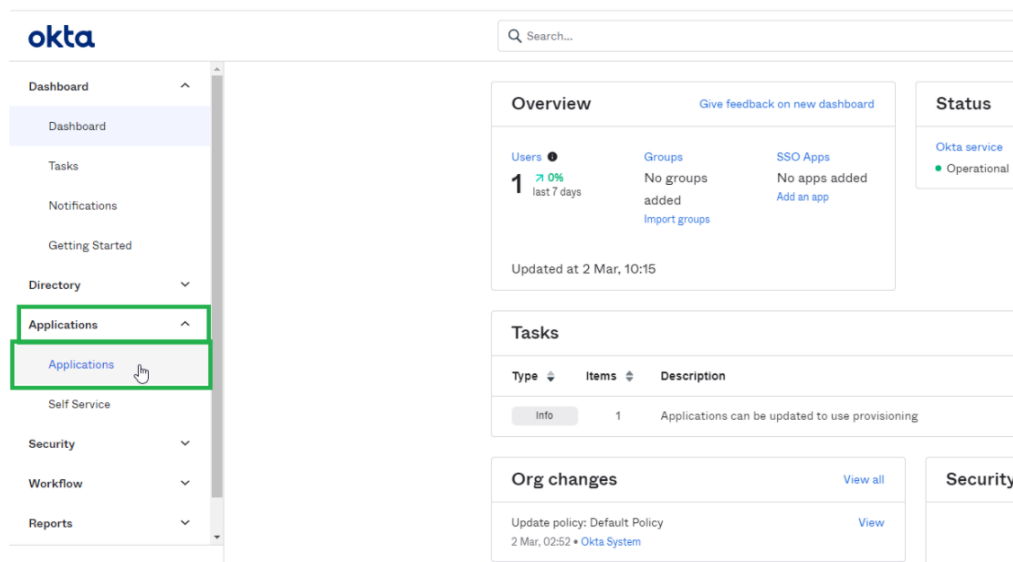
See [System Settings Required to Support SSO](#).

**Important: If you are using a load balancer:** Note that when configuring a system to use SAML authentication, if you are using a load balancer, it should be configured to use a sticky session.

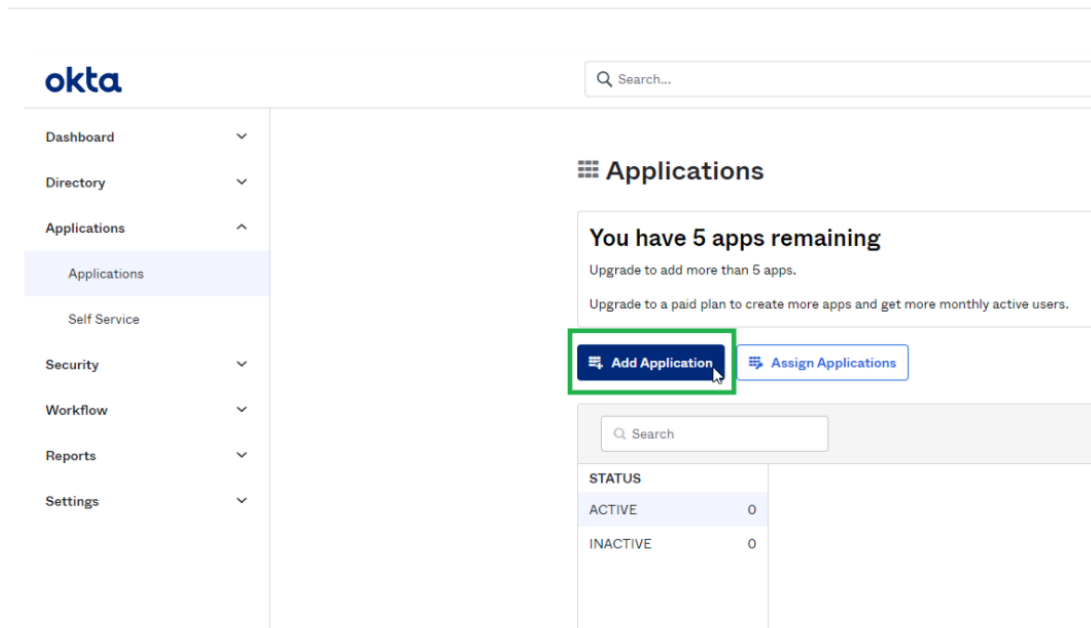
## Creating an Okta Application

If you are using SAML login connected to Okta for authentication, you have to first create a dedicated application in Okta.

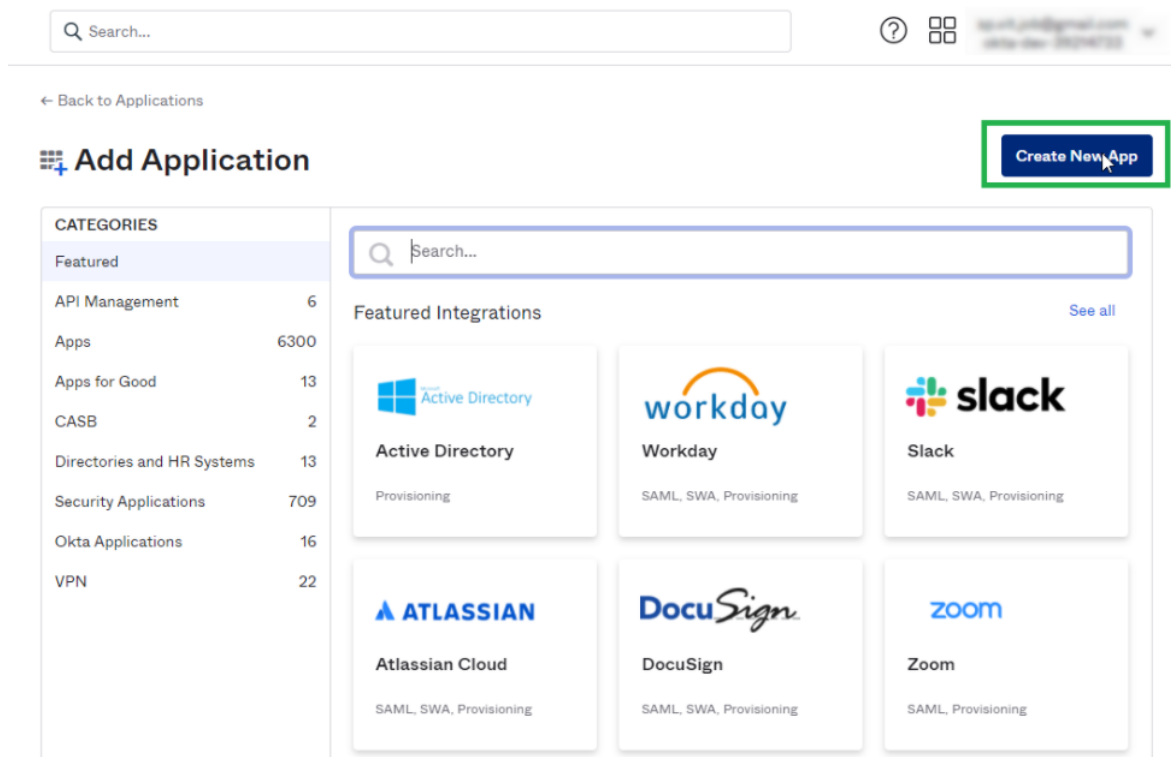
1. Open the **Create a new Application dialog**.
  - a. Log into Okta.
  - b. Select **Applications** to open the Applications screen.



- c. Select **Add Application**.



d. Select **Create New App**.



e. In the Platform select **Web** and in the Sign on method select **SAML 2.0**.

×

### Create a New Application Integration

Platform

Sign on method

- Secure Web Authentication (SWA)  
Uses credentials to sign in. This integration works with most apps.
- SAML 2.0  
Uses the SAML protocol to log users into the app. This is a better option than SWA, if the app supports it.
- OpenID Connect  
Uses the OpenID Connect protocol to log users into an app you've built.

f. Select **Create**.

2. Fill in the configuration fields.

a. General Settings

#### ***App name***

Enter any name for your Application

Click **Next**.

b. Configure SAML.

#### ***Single sign on URL***

-http://[SERVER\_NAME]/siqapi/login/AssertionConsumerService

Where SERVER\_NAME is the VM in which the Website is installed

#### ***Audience URI (SP Entity ID)***

Enter the name of the application.

This will be used later during the installation of the File Access Manager using the SAML option.

Important: Additional settings can be found under the Show Advanced Settings link – these settings shouldn't be changed, but if they were changed they should also be changed in the File Access Manager installation with the SAML option.

c. Feedback

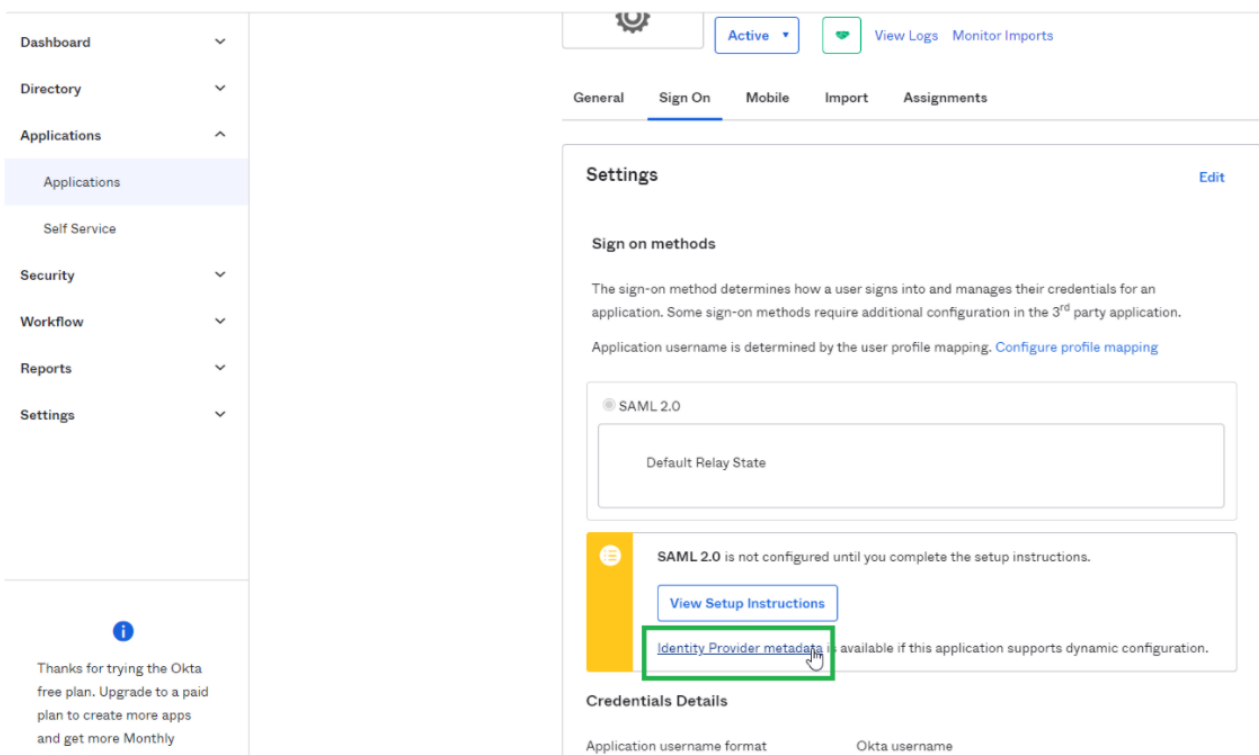
***Are you a customer or partner?***

I'm an Okta customer adding an internal app

Select **Finish**.

3. The application was successfully created.

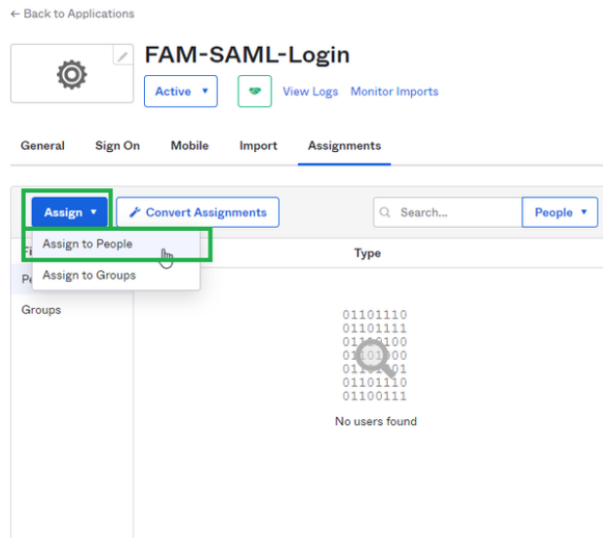
4. Click on the **Identity Provider metadata**.



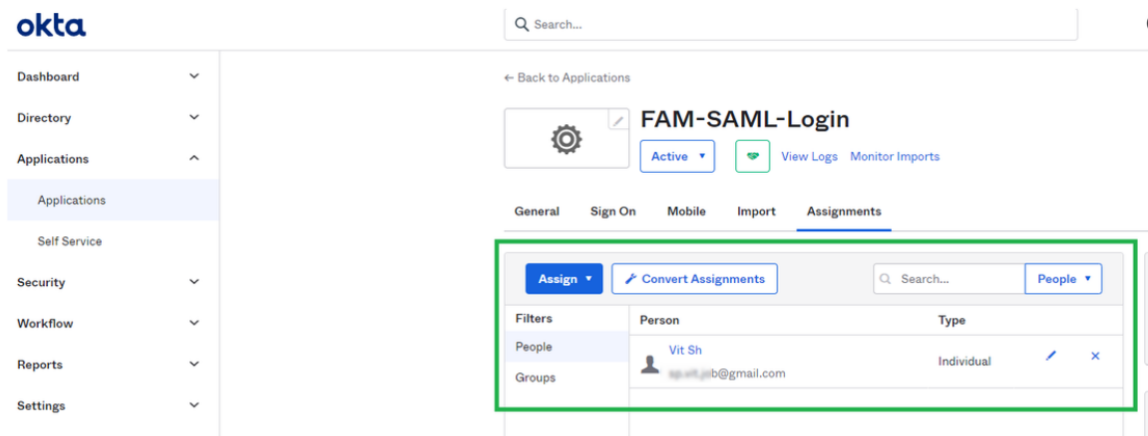
5. Copy the URL of the opened page. This will be used later during the installation of the File Access Manager using the SAML option.





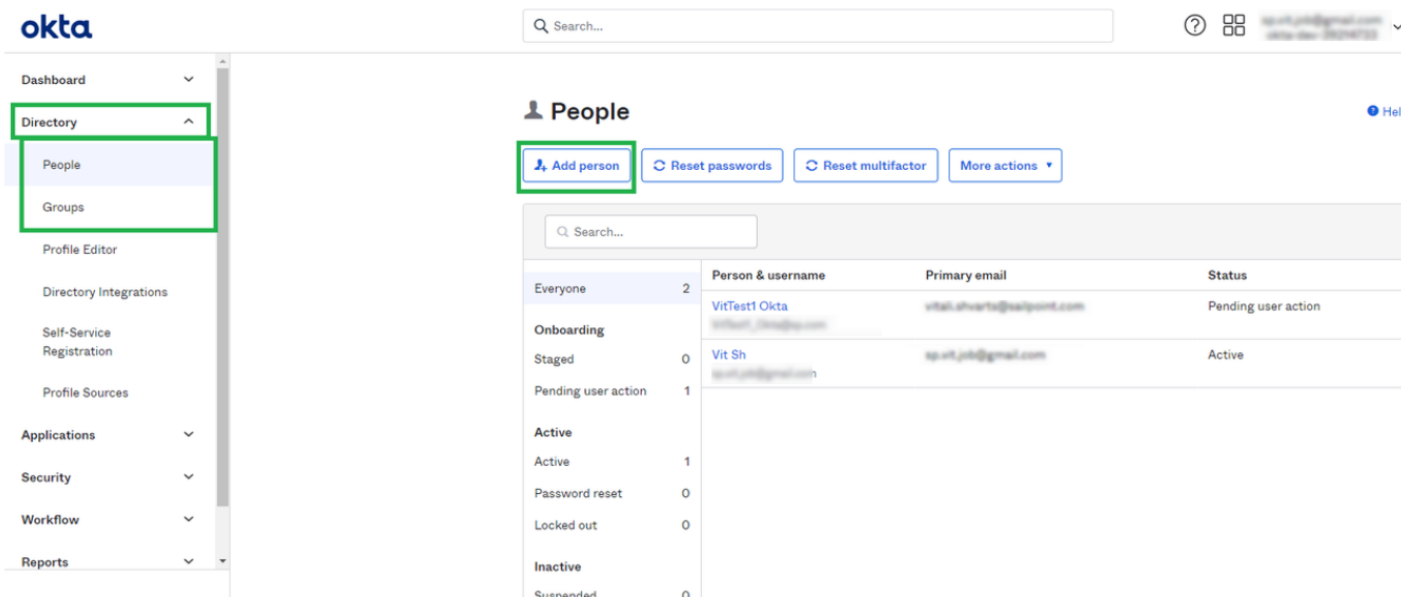


- c. Select **Assign** next to the displayed user.
- d. Select **Save to go Back** button.  
The user is now selected as **Assigned**.
- e. Select **Done**.
- f. User is displayed in the Application list.



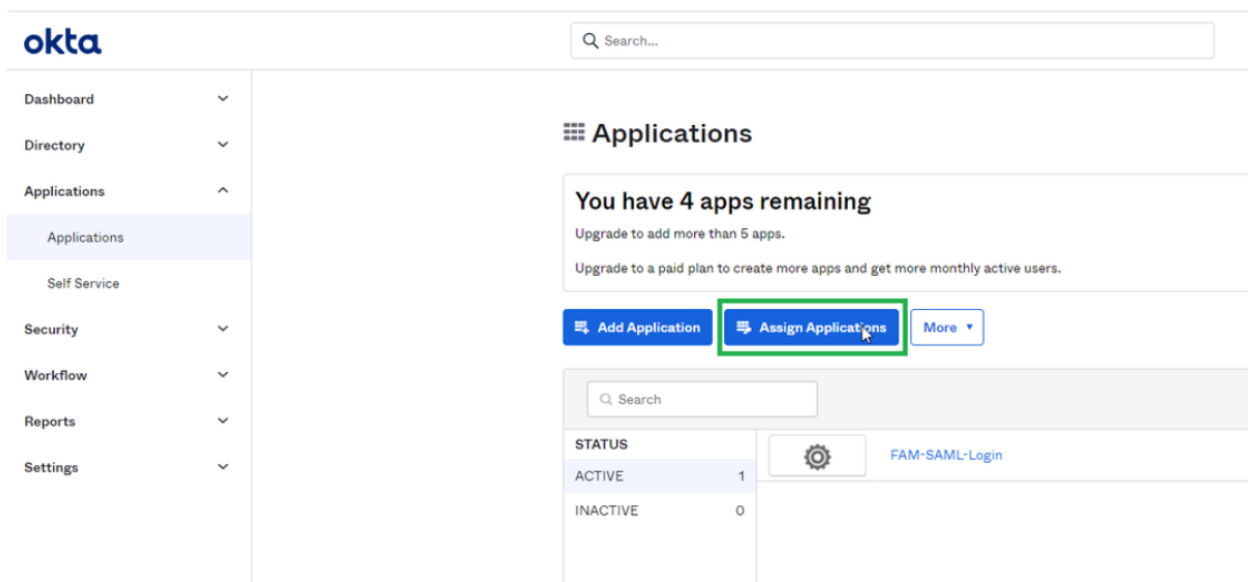
7. Additional users or groups can be added in  
**Directory > People > Add Person** or **Directory > Groups > Add Group**.

Important: The user email entered should be an actual email, because it is used as part of the account activation process.

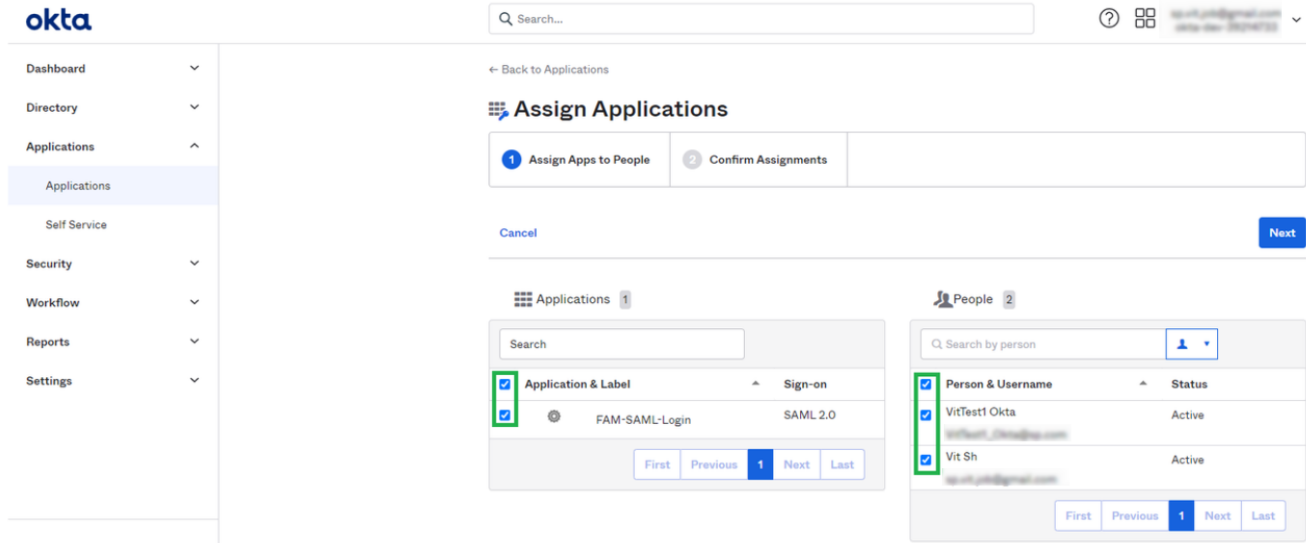


8. You can now assign the application for recently created users:

- a. Navigate to **Applications > Applications** and select **Assign Applications**.

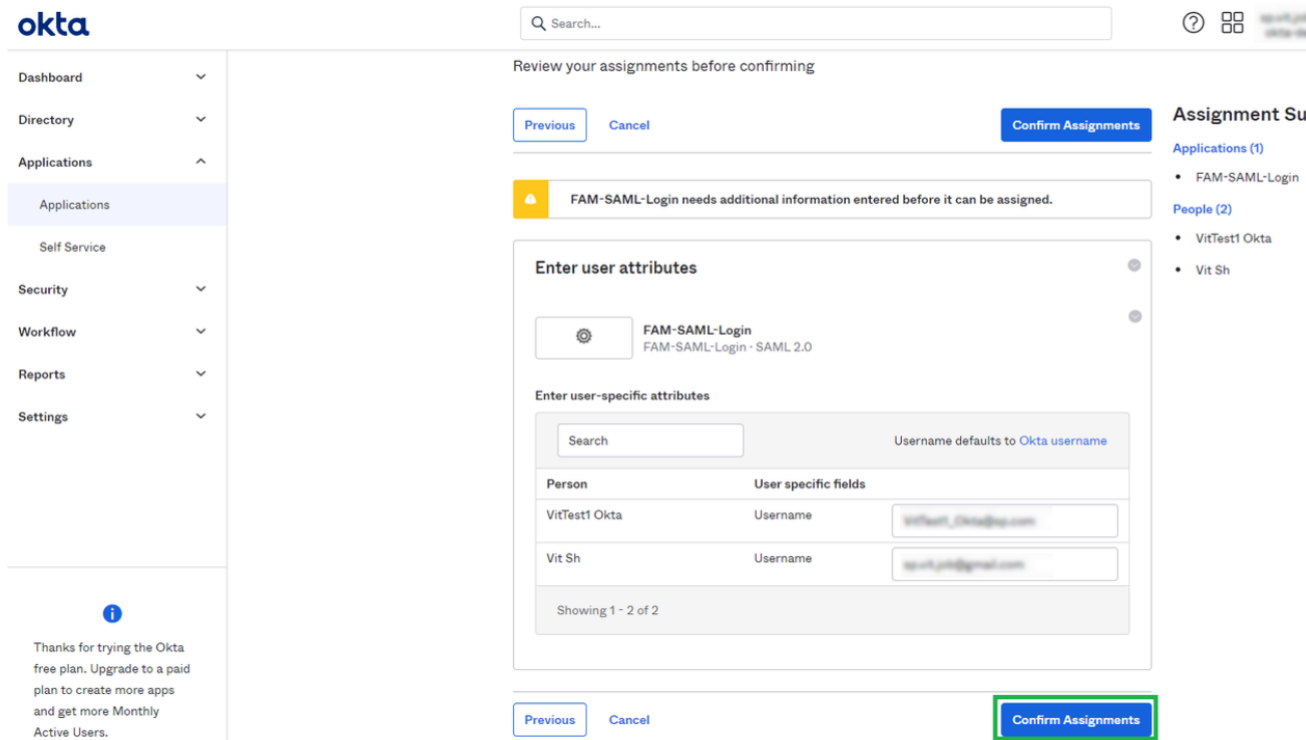


- b. Select the applications and the users which you want to assign.



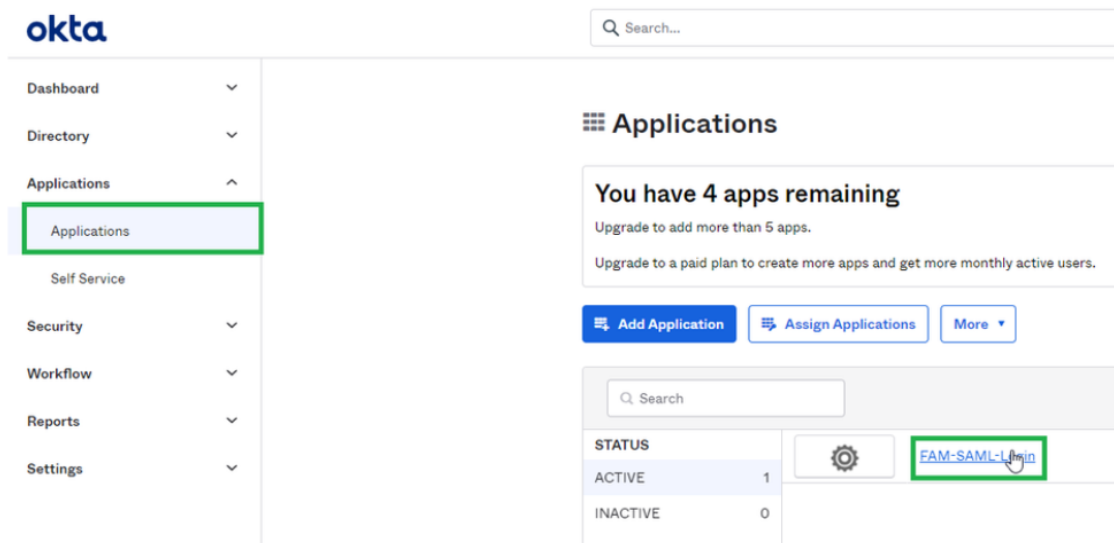
c. Click **Next**.

d. Click **Confirm Assignment**.

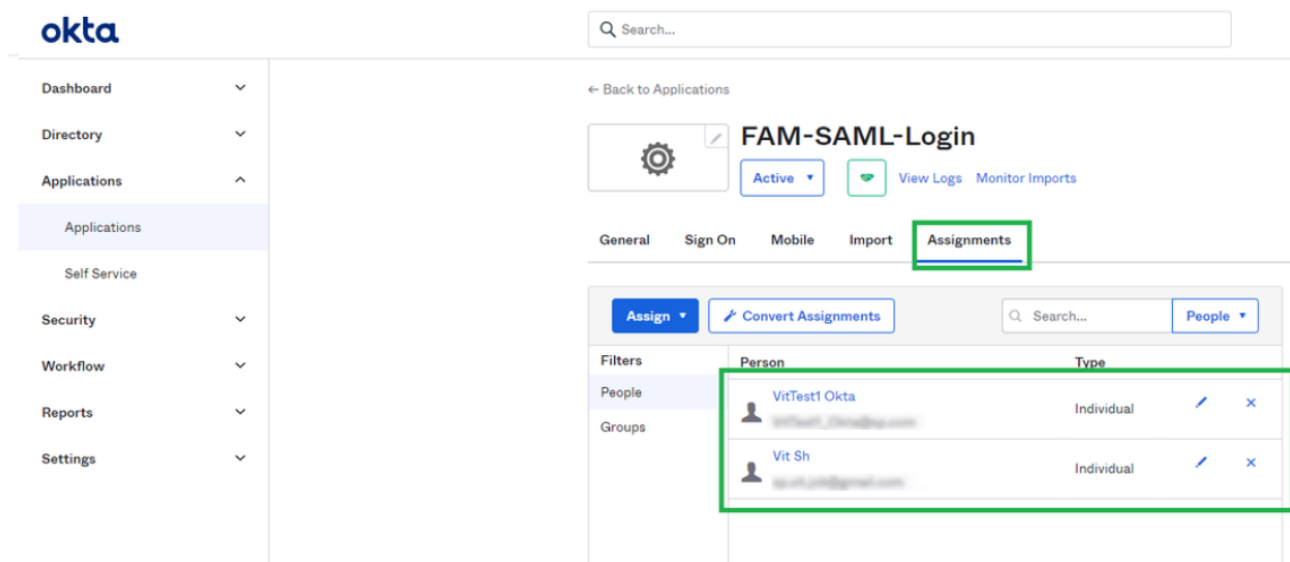


e. Navigate to **Applications > Applications**.

f. Select the Existing Application.



g. The Assignments tab is selected, verify that all the assigned users are displayed in the grid.



The Okta application is now set and the following data will be needed during the installation of the File Access Manager with the SAML 2.0 version.

- The name of the created Okta application. In this example “FAM\_SAML\_LogIn” Note that this string is case sensitive in the installation process in File Access Manager.
- The URL to the Metadata mentioned above.

When installing File Access Manager, make sure to follow the sections pertaining to SAML login installation.

## Creating an ADFS Application

In order to connect ADFS as an identity provider for File Access Manager, you must first create a dedicated application in ADFS.

1. Log into ADFS and navigate to **Trust Relationships > Relying Party Trusts**.
2. Click on **Add Relying Party Trust....**

In the opened wizard enter the following values in the following steps:

### **Welcome step**

Start

### **Select Data Source**

Enter data about the relying party manually (The last option)

3. Select **Next**.
4. Specify Display Name: Enter any name, this name will later be used during the installation of File Access Manager with SAML 2.0 option.  
Select **Next**.
5. Choose Profile: Select the first option **ADFS profile**.  
Select **Next**.
6. Configure Certificate  
Select **Next**.
7. Configure URL  
Select **Next**.
8. Relying party trust identifier.  
Enter the name entered in the step **Specify Display Name** above.  
Select **Add**.  
Select **Next**.
9. Configure multi-factor authentication settings...:  
Select **I do not want to configure multi-factor authentication...** option.

Select **Next**.

10. Choose Issuance...:

Select the first option **Permit all users to access the relying party**.

Select **Next**.

11. Ready to Add Trust

Select **Next**.

12. Finish.

“Open the Edit Claim Rules dialogue...” is checked.

Select **Close**.

13. In the opened Edit Claim Rules for [app name] window.

Select **Add Rule**.

14. In the opened wizard select and enter the following data:

a. Select Rule Template

***Claim Rule Template***

Select **Send LDAP Attributes as Claims**

Select **Next**.

b. Configure Claim Rule

***Claim rule name***

UserInfo

***Attribute store***

Active Directory

Mapping of LDAP attributes to outgoing claim types

LDAP Attribute (Select or type to add mote)	Outgoing Claim Type (Select or type to add more)
User-Principal-Name	Username
User-Principal-Name	Name

15. Select **Finish**.

16. Select the **Add Rule** button.
17. In the opened wizard select and enter the following data:
  - a. Choose Rule Type: input the fields as specified below

***Claim rule name***

Free text

***Claim rule template***

Transform an Incoming Claim

***Incoming claim type***

Username

***Outgoing claim type***

Name ID

***Outgoing name ID format***

Unspecified

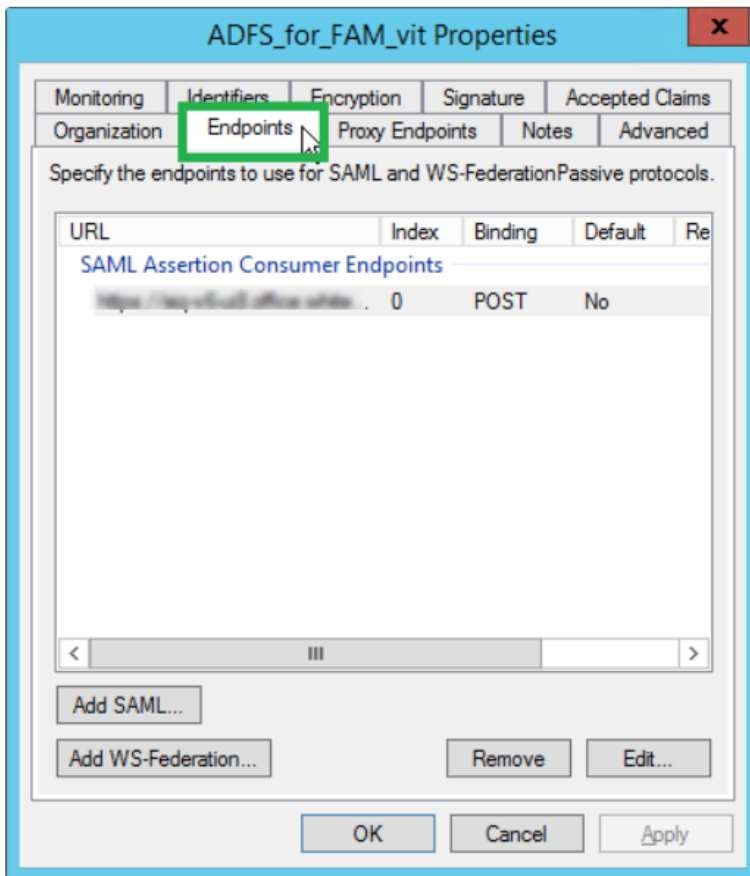
***Pass through all claim values***

Select this option

- b. Select **Finish**.

18. Select **OK**.
19. Right click on the recently created ***Relying Party Trust > Properties***.
20. Select the **EndPoints** tab.





21. Select **Add SAML**.

22. Fill the following values in all fields:

**Endpoint type**

SAML Assertion Consumer

**Binding**

POST

**Index**

0

### Trusted URL

Enter the following link. This the ADFS where to redirect the user logging in (A link to the File Access Manager system) `https://[SERVER_NAME]/siqapi/login/AssertionConsumerService`

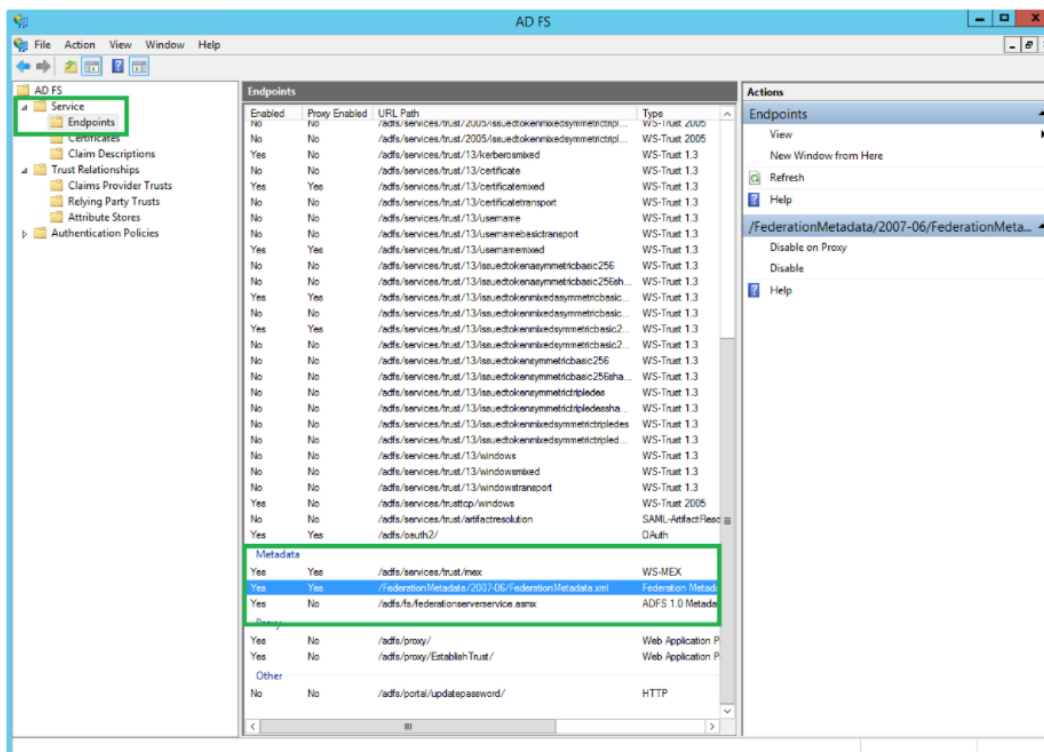
SERVER\_NAME is the server in which the website is installed

23. Select **OK**, and then **OK** on the next screen.

The ADFS application is now set and the following data will be needed during the installation of the FAM with the SAML 2.0 version.

- The name of the created Relying Party Trusts, in this example: "ADFS\_for\_FAM\_vit"
- The URL to the Metadata which is constant per a VM where the ADFS is set

The URL can be found in the ADFS Configuration: *Service > Endpoints > Metadata* section

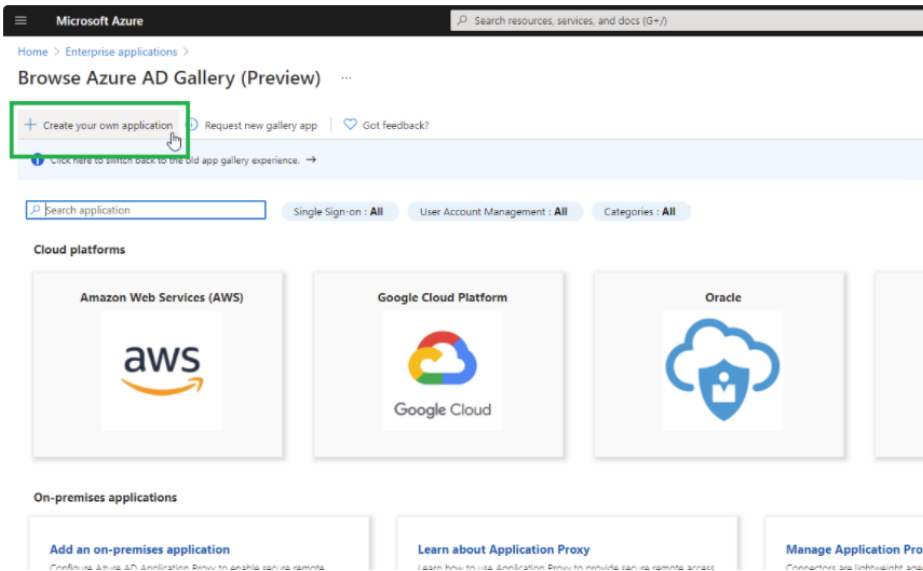


When installing File Access Manager, make sure to follow the sections pertaining to SAML login installation.

## Creating an Azure Application

In order to connect an Azure as an identity provider for File Access Manager, you must first create a dedicated application in Azure.

1. In Microsoft Azure, navigate to the **Portal**.
2. Go to “Enterprise applications” (You can search for it on the searchbar, and click on it).
3. Select **+ Create your own application**.



4. Fill the following fields:

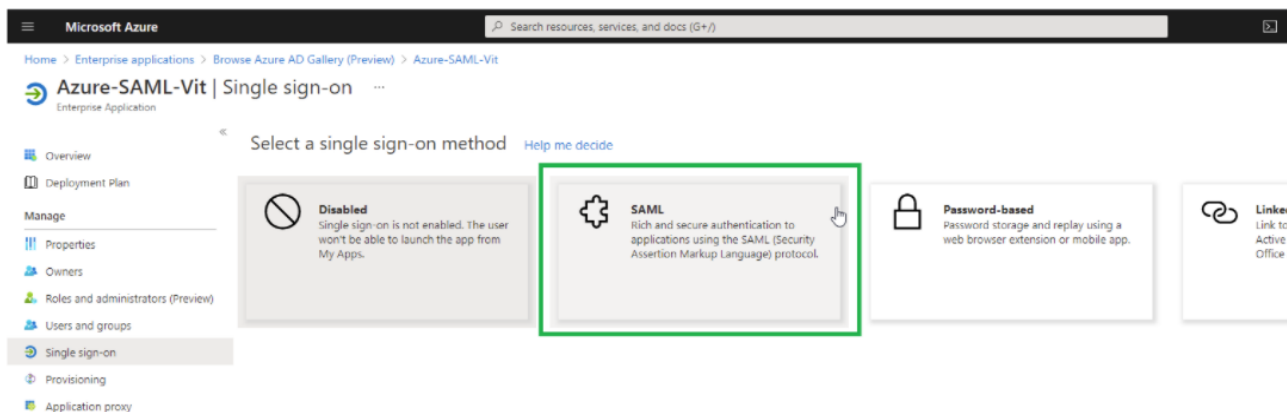
***What's the name of your app?***

Free text

***What are you looking to do with your application?***

Integrate any other application you don't find in the gallery

5. Select **Create**.
6. Select the **Single sign-on** option in the navigation menu located on the left side of the screen.
7. Select **SAML**.



8. In the Basic SAML Configuration panel, click **Edit**.
9. Fill the following fields with the following data:

### ***Identifier (Entity ID)***

This should be entered with `https://` and can be the address of the VM - this data will be used in the Server Installer during installation of the SAML option.

Delete the default value identifier.

Select the created identifier as default by checking the checkbox.

### ***Reply URL (Assertion Consumer Service URL)***

`https://[SERVER_NAME]/siqapi/login/AssertionConsumerService`

Where `SERVER_NAME` is the VM where the File Access Manager website is installed



Select **Save**.

10. In the User Attributes & Claims, select **Edit**.
  - a. Within Required Claim, click on the **Claim name** on the top.
  - b. Click on the **Choose name identifier format** dropdown list, and select **Unspecified**.
  - c. Look at the selected value within the Source Attribute dropdown.

Verify that the selected value is "user.userprincipalname".

[Home](#) > [Azure-SAML-Vit](#) > [SAML-based Sign-on](#) > [User Attributes & Claims](#) >

## Manage claim ⋮

 Save  Discard changes

Name

Namespace

^ Choose name identifier format

Source \*  Attribute  Transformation

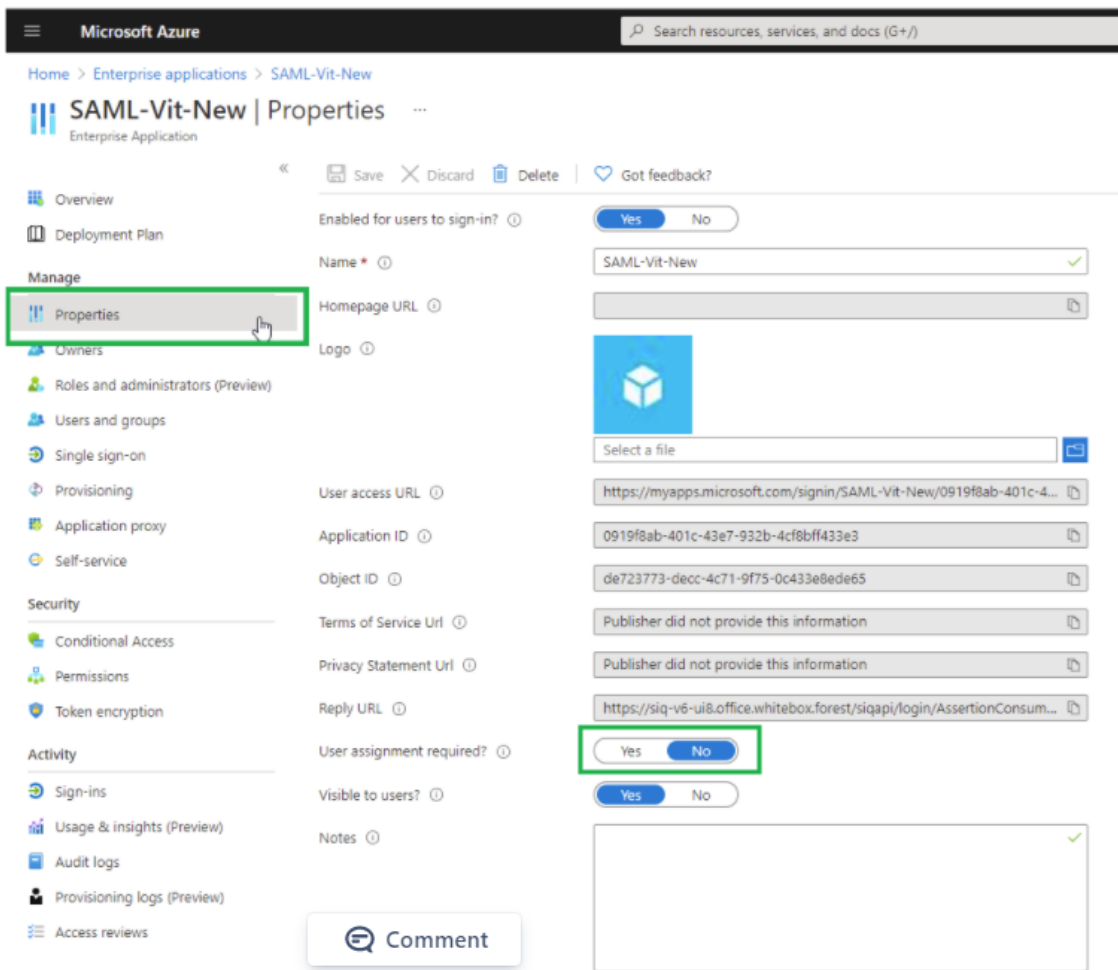
Source attribute \*

∨ Claim conditions

d. Select **Save**.

11. Close the currently displayed window (click on the **X**).

12. Select **Properties**.



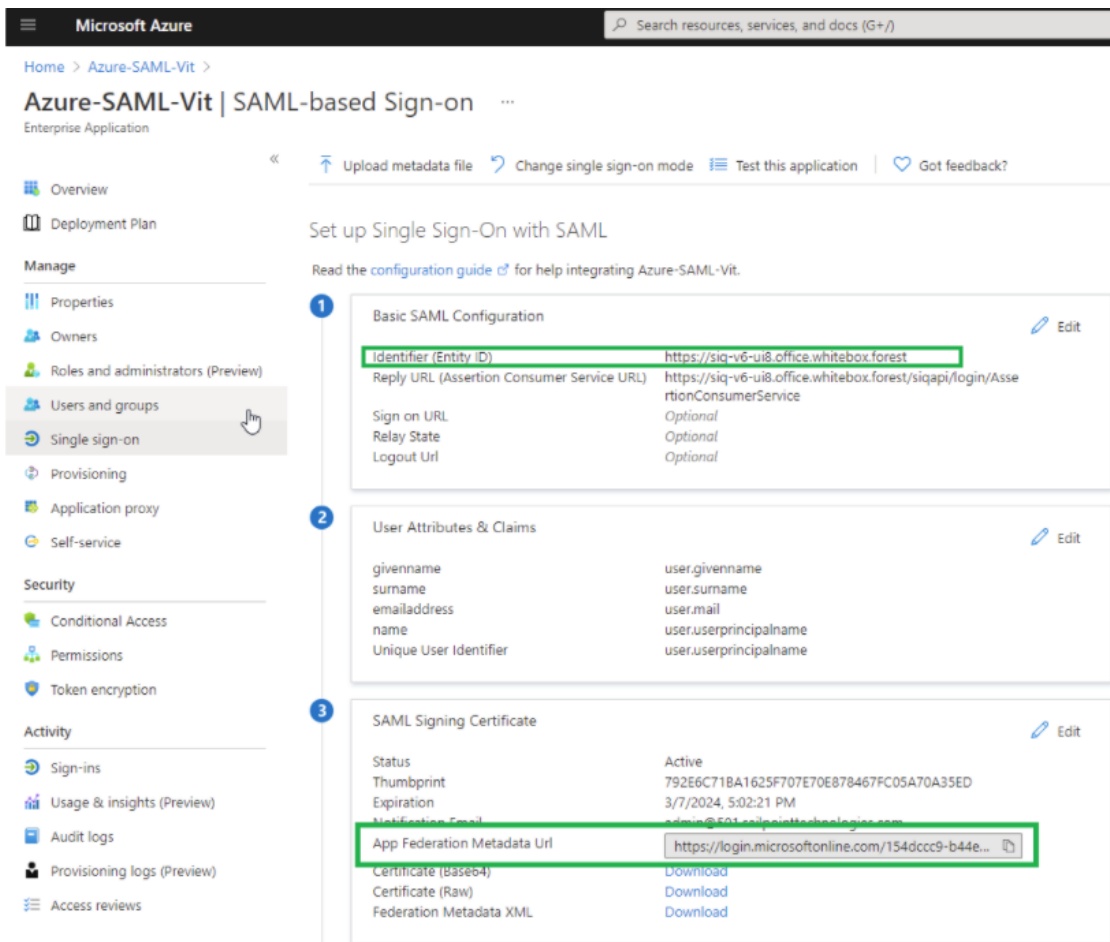
13. Verify that “User assignment required?” is set to **No**.

14. Select **Single sign-on > Test this application**.

The Azure application is now set and the following data will be needed during the installation of the FAM with the SAML 2.0 version.

- Entered Identifier, from the Basic SAML Configuration panel
- The link to the Federation metadata document – copy the value within “App Federation Metadata Url“ in the

third frame

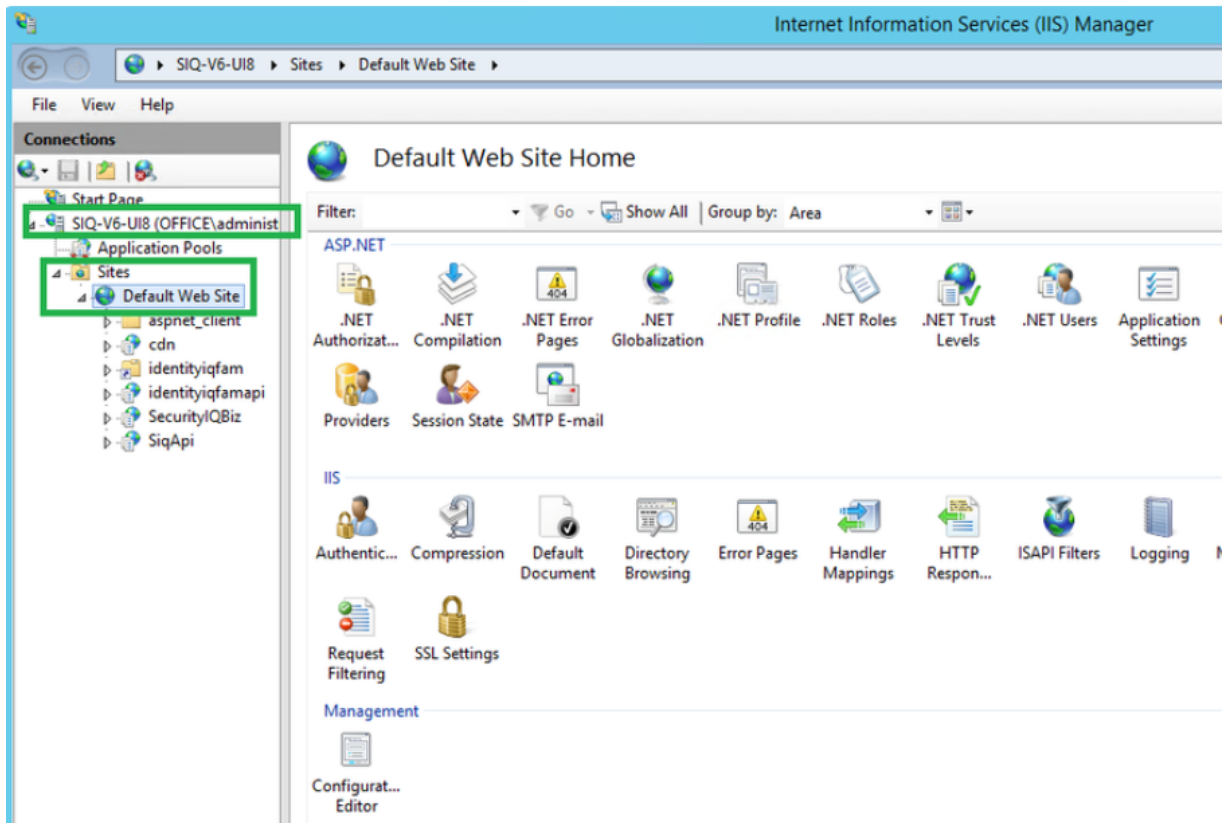


## Switching from SAML to Windows Authentication Mode

You can switch the File Access Manager authentication mode from SAML, using a local identity provider, to Windows username and password method, by changing the setup in the File Access Manager installer.

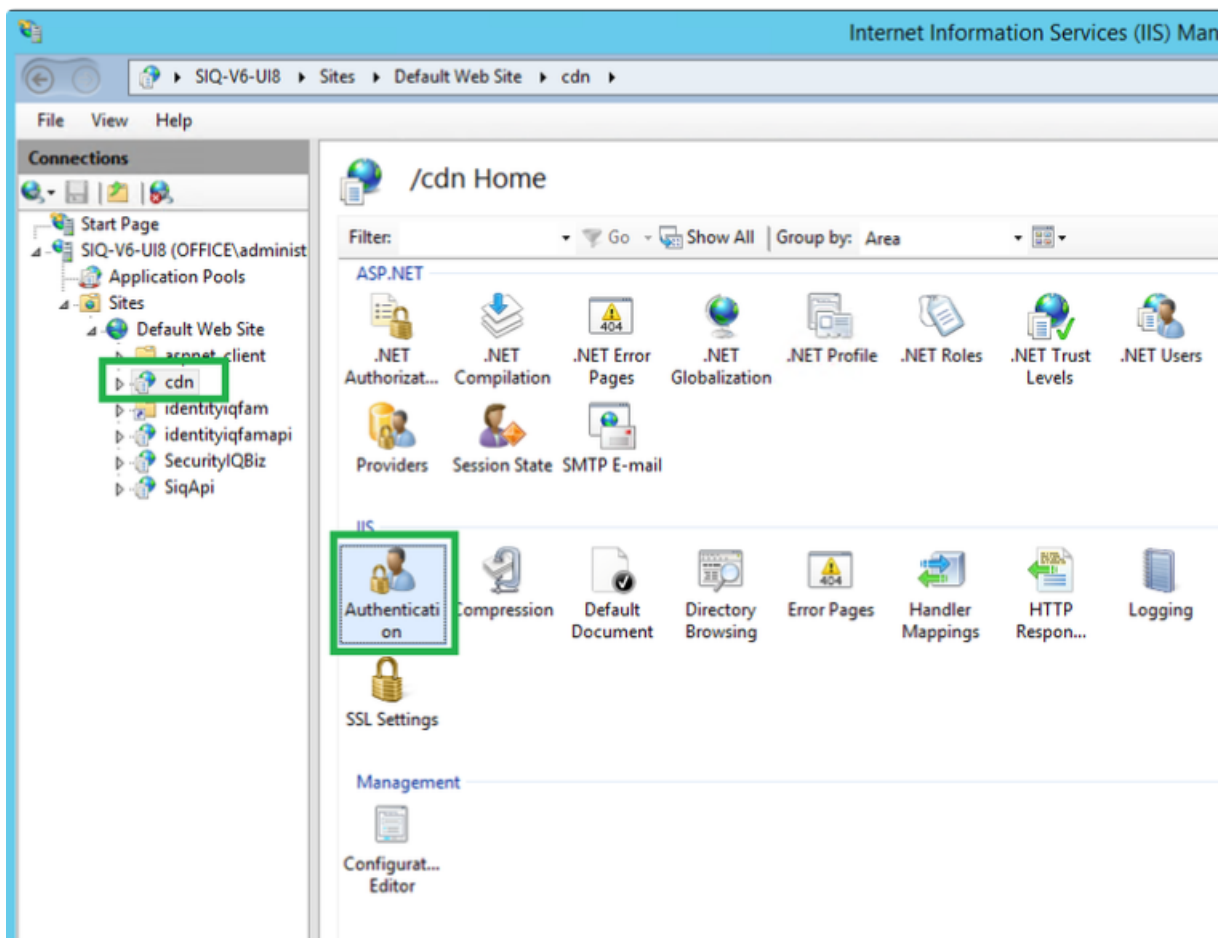
1. Set the authentication mode on the File Access Manager installer.
  - a. Open the File Access Manager installer on the sever the Web Client and the IIS are installed.
  - b. Navigate to the **Select web authentication mode** step and switch the option from SAML to Windows.
  - c. Click **Next** to the end of the installation wizard and click **Finish**.
2. Change the IIS authentication method.

- a. Open the IIS Manager
- b. In the tree on the left-hand side navigate to **Current Server > Sites > Default Web Site**.

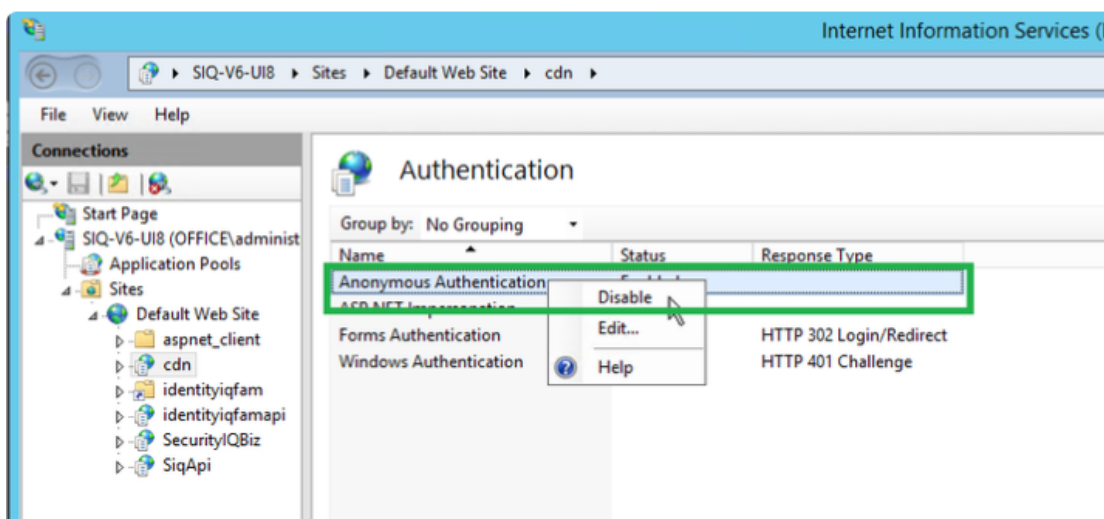


- c. Click on **cdn**, then in the IIS section click **Authentication**.

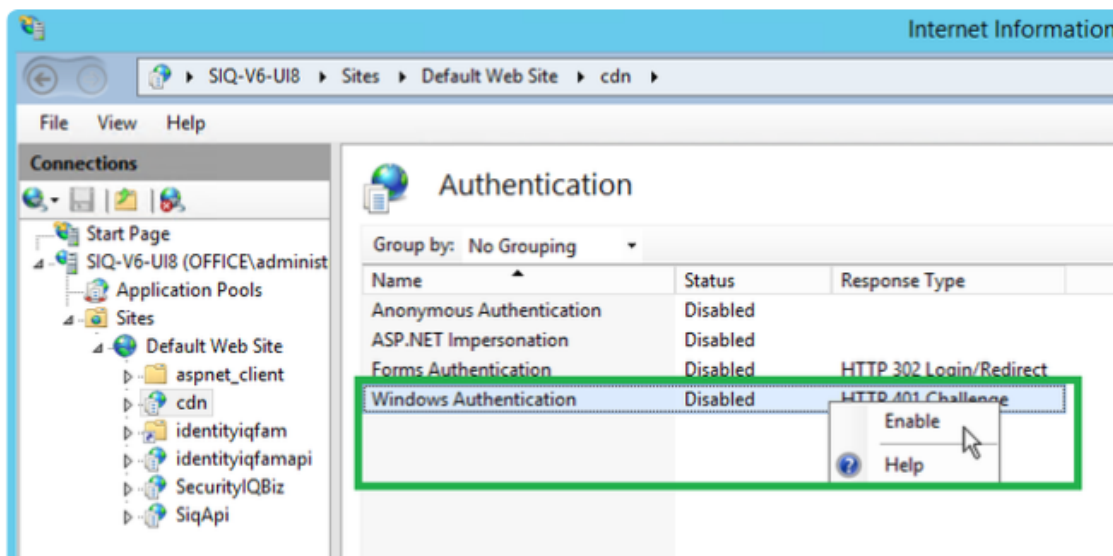




- d. Disable the Anonymous Authentication (right-click and select **Anonymous Authentication > Disable**).



- e. Enable the Windows Authentication (right-click and select **Windows Authentication > Enable**).



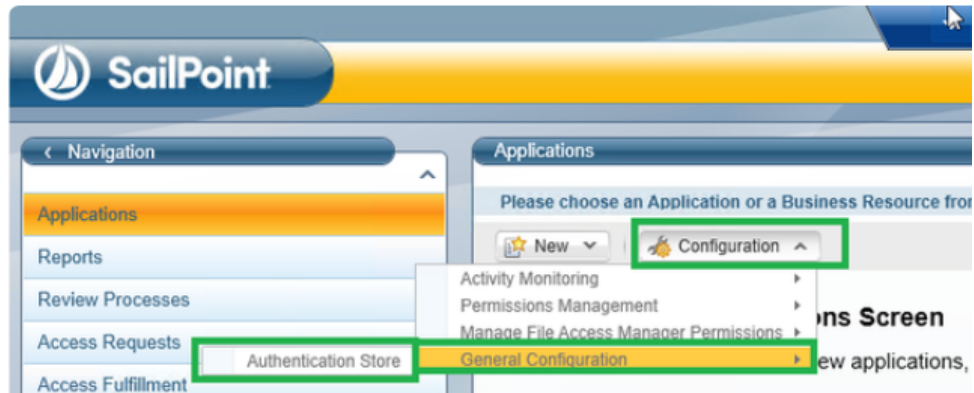
- f. Repeat the steps above also for the following folders \ locations:

- Identityiqfam > v1
- Identityiqfam > v2
- SecurityIQBiz
- SiqApi

- g. Restart IIS

3. Create an Active Directory identity collector, and make it the authentication store.

- a. In the Admin Client create an AD identity collector under **Application > Configuration > Permission Collection > Identity Collectors**. Set a schedule for this identity collector.
- b. Navigate to **Applications > Configuration > General Configuration > Authentication Store**, and select the identity collector you created above from the drop down list. You now have an Active Directory authentication store.



- c. Run the scheduled task of the authentication store created above.

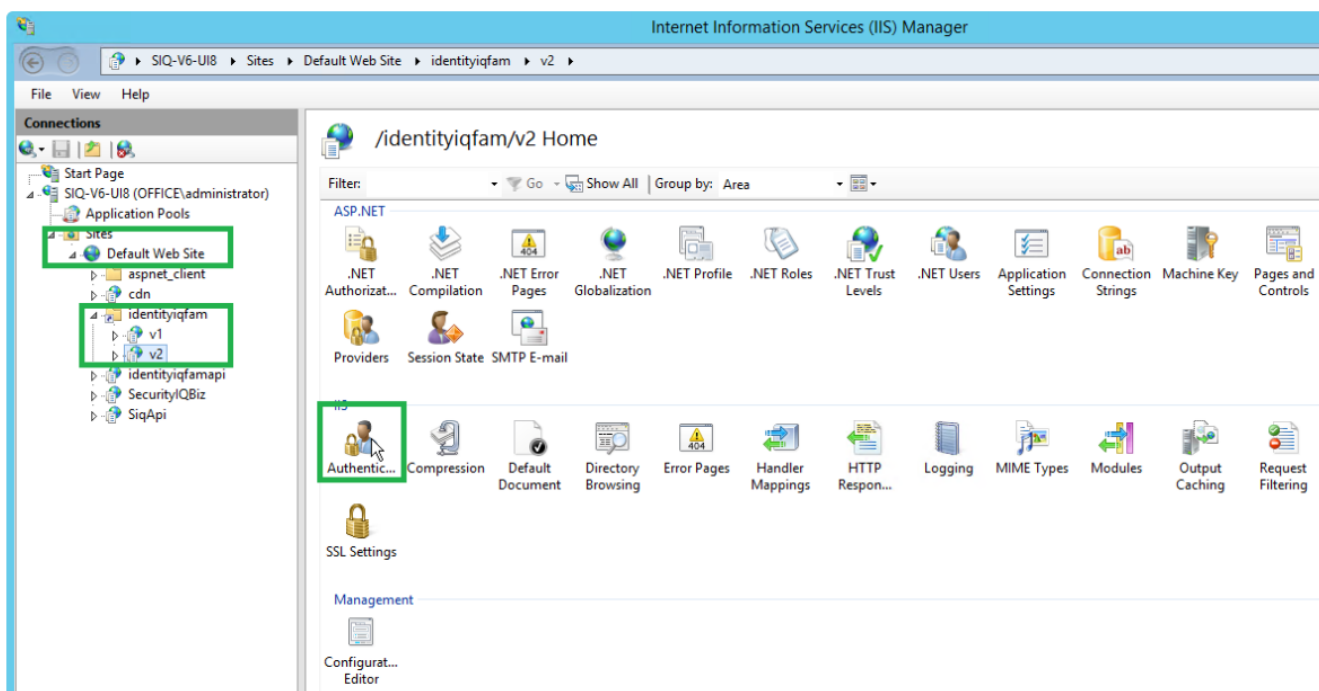
Important: Clear the cache of the previous sessions of your browser.

4. Open the Website and sign in with any user from the authentication store. The SAML Login option and the Logout button will no longer appear in this system.

## System Settings Required to Support SSO

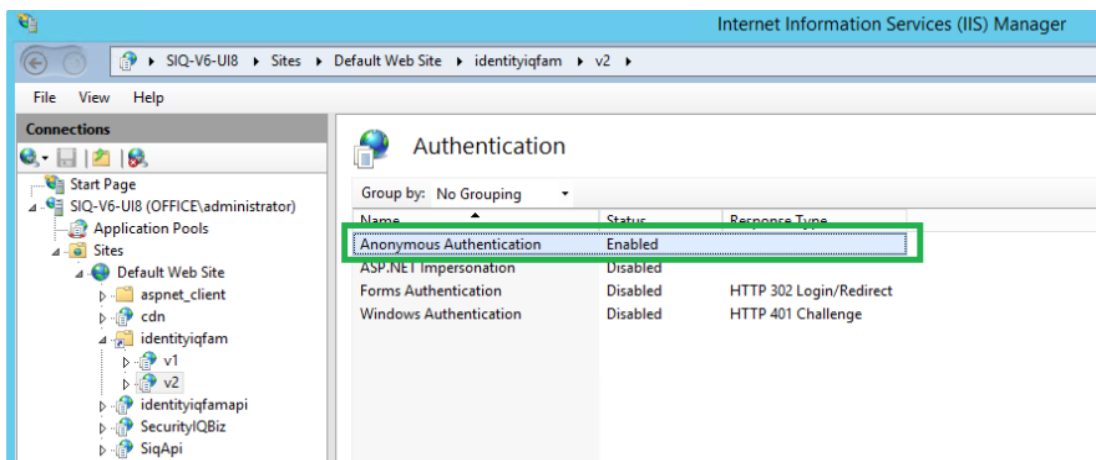
After completing the File Access Manager admin client and website, you have to configure the application to accept SSO login.

1. Connect to the server where the IIS (Website) is installed
  - a. Open the IIS Manager.
  - b. Navigate to one of the following server sites:
    - The server > Sites > Default Web Sites > identityiqfam > v1/v2 > Authentication
    - Server > Sites > Default Web Sites > identityiqfam > cdn > Authentication
    - Server > Sites > Default Web Sites > identityiqfam > SecurityIQBiz > Authentication
    - Server > Sites > Default Web Sites > identityiqfam > SiqApi > Authentication



- c. Verify that Windows Authentication is disabled and the only enabled option is “Anonymous Authentic-

ation.“



2. Continue the configuration setting according to the SSO provider

- [System Settings to Support SSO - Okta](#)
- [System Settings to Support SSO - ADFS](#)
- [System Settings to Support SSO - Azure](#)

## System Settings to Support SSO - Okta

The task checklist below is followed by a detailed description of each step:

1. Website: Log in using the wbxadmin credentials, and create a data source for SSO users.
2. Admin client: Create an identity collector based on this data source.
3. Admin client: Select this identity store as the authentication store.
4. Website: Run the Identity collector task which was recently selected as authentication store.  
This step will load the Okta users into the database.
5. Website: Click on the **SAML login** button and sign in to the relevant SSO Provider.
6. You should now be logged into File Access Manager the SSO provider user.

## Detailed Settings

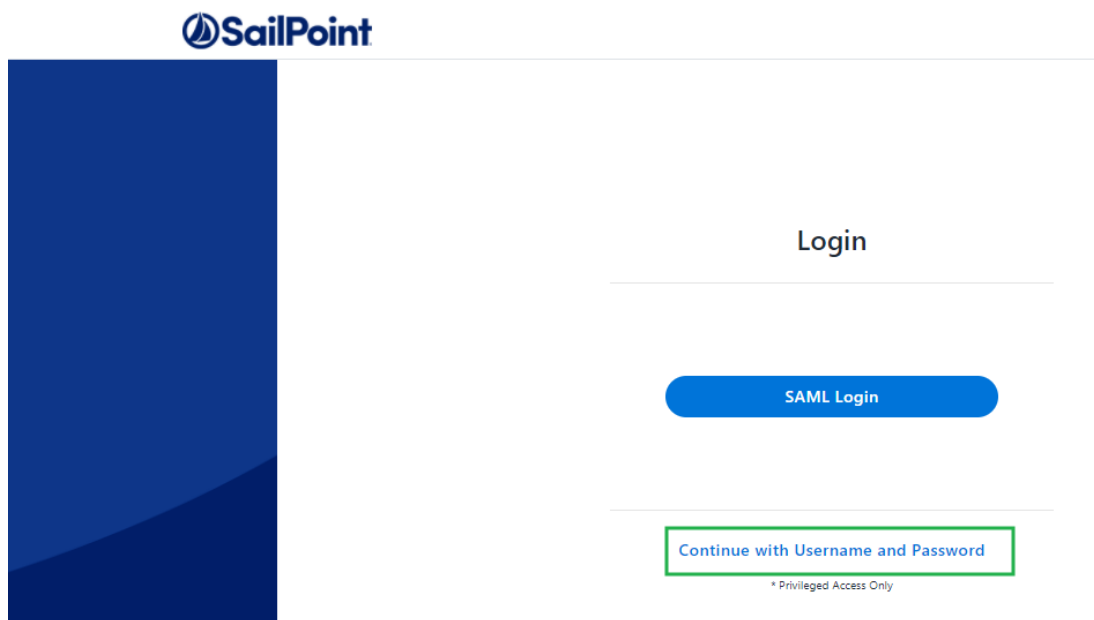
1. Website: Create a data source for SSO users.

(First time login to File Access Manager using wbxadmin credentials)

- a. Open the website and click on **Continue with username and password**

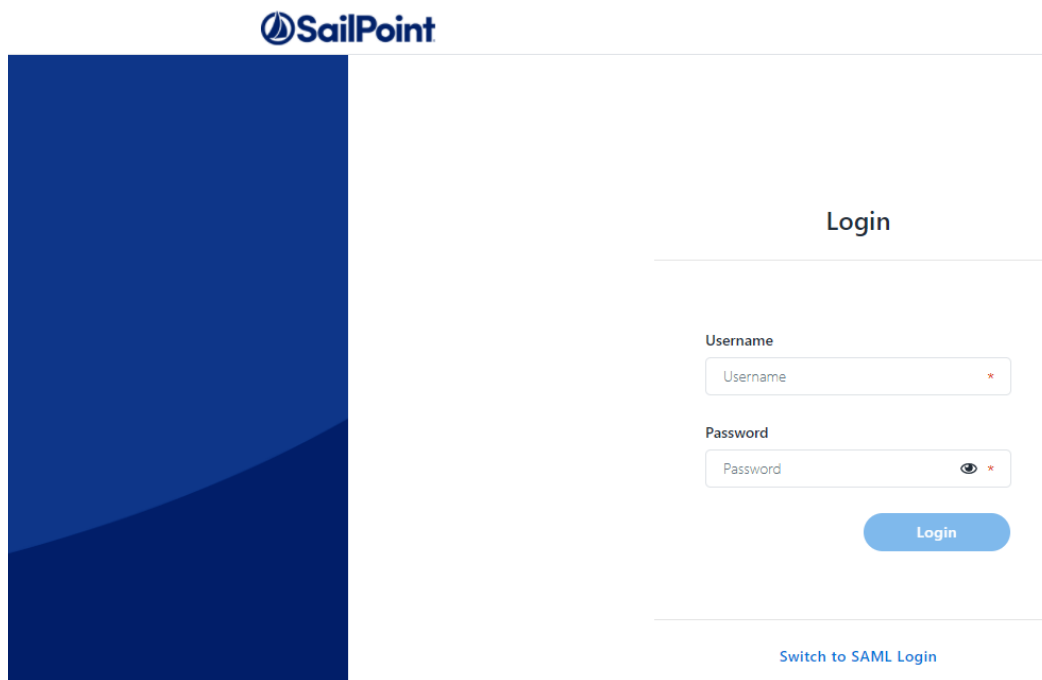
Warning: Make sure to use the correct URL. The URL used to log in should match the Redirect URL entered in the OKTA application when creating the application. E.g., If you use HTTPS connection, the Login link and redirect URL in Okta should both be HTTPS.

Warning: If you use an IP address instead of server name, the login link and Redirect URL in Okta should be written with an IP address as well.



- b. Log in to the system with the wbxadmin user and use the password entered during the installation of the system.

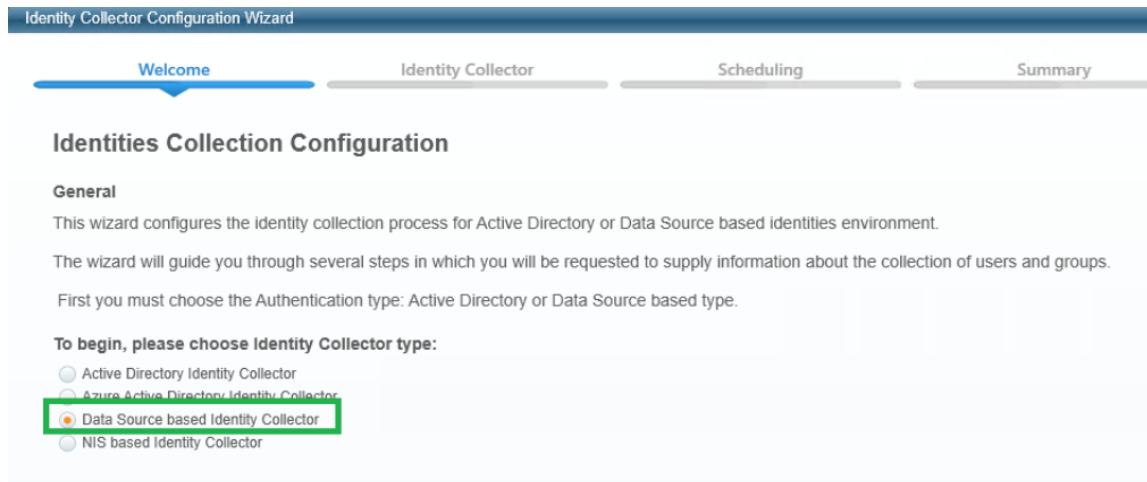
Select **Login**.



- c. Within the website navigate to **Admin > Data Sources > Add New Data Source**.
- d. Create a new data source that contains a list of Okta Users you want to access File Access Manager.
  - This could be any type of data source on your system such as a query on a table in your database, a local Excel file, or a static table stored in the File Access Manager system.  
See the chapter on data sources in the File Access Manager Admin Guide for further details.
  - The data source should contain a single column of the user login.
  - This data source will be read by the File Access Manager identity collector process when it is scheduled to run, or it could be triggered manually.
  - These users also have to be assigned to the File Access Manager application in Okta.

For this example, we'll call the data source "OktaUsers" and the column of users "User Principal Name."

2. Admin client: Create an identity collector based on this data source.
  - a. Navigate to **Configuration > Permissions Management > Identity Collectors**.
  - b. Click **new** and select the **Data Source based Identity Collector**.



c. Enter any name and uncheck **This application uses Groups**.

Select **Next**.

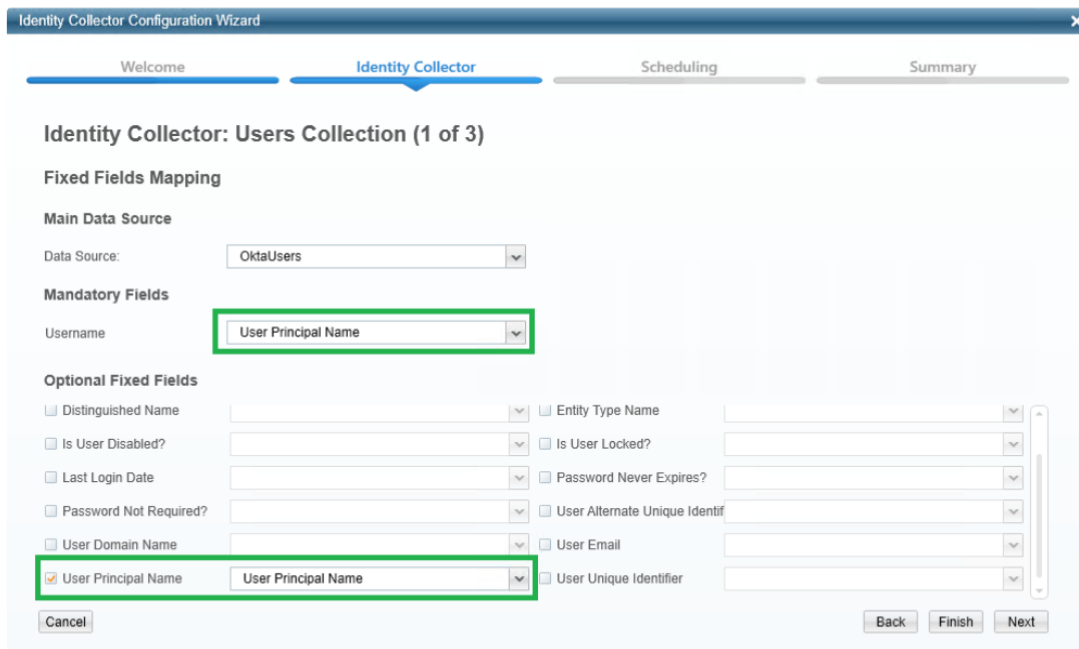
d. Make the following selections:

- Select the Data Source created in the website
- Map the only existing field (User Principal Name) to the following fields:

User Principal Name

Username





Select **Next**.

- e. In the Identity Collector Users Collections (3 of 3) uncheck all the checkboxes (Users Tree, Unique User Accounts Mapping).

Click **Next**.

- f. Create a scheduler. This will determine the update frequency in which new users read from the Okta data source will be read.

Click **Finish**.

- g. Wait until the task is finished, and close the Identity Collector Configuration window.

- 3. Admin client: Select this identity store as the authentication store.

- a. Navigate to **Configuration > General Configuration > Authentication Store**.

- b. Select the identity collector created above as the current authentication store.

### Authentication Store Wizard

#### Authentication Store Change Wizard

This wizard enables you to choose an Identity Collector as the new Authentication Store

Please notice that proceeding with this wizard, will STOP the review processes of running Access Certification Campaigns and Access Requests.

Changing the Authentication Store, will have no effect on completed Access Certification Campaigns and Access Requests.

After having completed the change process, please make sure of the following:

- The defined review processes are still relevant.
- The local File Access Manager users are associated with the right Authentication Store users.

Authentication Store:

- c. Click **Finish**.
4. Website: Run the Identity collector task which was recently selected as authentication store.
  - a. Navigate to **Settings > Tasks Management > Scheduled Tasks**.
  - b. Run the Identities Synchronization task which was recently selected as authentication store.
5. Website: Click on the **SAML login** button and sign in to the relevant SSO Provider.  
Click on **Send anyway** if needed, sign in for the first time if needed.
6. You should now be logged into File Access Manager the SSO provider user.

## System Settings to Support SSO - ADFS

The task checklist below is followed by a detailed description of each step:

1. Admin client: Create an Active Directory identity collector.
2. Admin client: Select this identity store as the authentication store.
3. Website: Log in using the wbxadmin credentials, and run the Identity collector task which was recently selected as authentication store.  
This step will load the ADFS users into the database.
4. Website: Click on the **SAML login** button and sign in to the relevant SSO Provider.
5. You should now be logged into File Access Manager as the SSO provider user.

## Detailed Settings

1. Admin client: Create an Azure AD identity collector.

Note: Instead of creating a new store, you can use the authentication store created during the initial launch of the admin client, and skip the next step.

See [Creating or Editing an Active Directory Identity Collector](#).

2. Admin client: Select this identity store as the authentication store.
  - a. Navigate to **Configuration > General Configuration > Authentication Store**.
  - b. Select the identity collector created above as the current authentication store.
  - c. Click **Finish**.
3. Website: Log in using the wbxadmin credentials, and run the Identity collector task which was recently selected as authentication store.
  - a. Open the website and click on **Continue with username and password**.
  - b. Log in to the system with the wbxadmin user and use the password entered during the installation of the system.  
Click **Login**.
  - c. Navigate to **Settings > Tasks Management > Scheduled Tasks**.
  - d. Run the identity collector task created above as authentication store.

This step will load the ADFS users into the database.

4. Website: Click on the **SAML login** button to sign in using your credentials.
5. You should now be logged into File Access Manager as the SSO provider user.

## System Settings to Support SSO - Azure

The task checklist below is followed by a detailed description of each step:

1. Admin client: Create an Azure identity collector.
2. Admin client: Select this identity store as the authentication store.

3. Website: Log in using the wbxadmin credentials, and run the Identity collector task which was recently selected as authentication store.

This step will load the Azure users into the database.

4. Website: Click on the **SAML login** button and sign in to the relevant SSO Provider.
5. You should now be logged into File Access Manager as the SSO provider user.

## Detailed Settings

1. Admin client: Create an Azure identity collector.

See [Creating or Editing an Azure Identity Collector](#)

2. Admin client: Select this identity store as the authentication store.
  - a. Navigate to **Configuration > General Configuration > Authentication Store**.
  - b. Select the identity collector created above as the current authentication store.
  - c. Click **Finish**.
3. Website: Log in using the wbxadmin credentials, and run the Identity collector task which was recently selected as authentication store.
  - a. Open the website and click on **Continue with username and password**.
  - b. Log in to the system with the wbxadmin user and use the password entered during the installation of the system  
Click **Login**.
  - c. Navigate to **Settings > Tasks Management > Scheduled Tasks**.
  - d. Run the identity collector task created above as authentication store.

This step will load the Azure users into the database.

4. Website: Click on the **SAML login** button to sign in using your credentials.
5. You should now be logged into File Access Manager as the SSO provider user.

## Creating or Editing an Azure Identity Collector

### *Azure AD Connector Full OAuth 2.0 Support*

File Access Manager now offers full support of standard OAuth 2.0 Authentication for the Azure AD connector.

The new authorization sequence will direct the user through a standard Microsoft O365 consent flow, to grant the File Access Manager Azure AD Connector app the privilege to acquire and refresh access tokens.

The new authentication method replaces the previous Basic Authentication flow, that required admins to provide user and password credentials.

This enhancement brings full OAuth support to the Azure AD Identity Collector, instead of the legacy user and password approach.

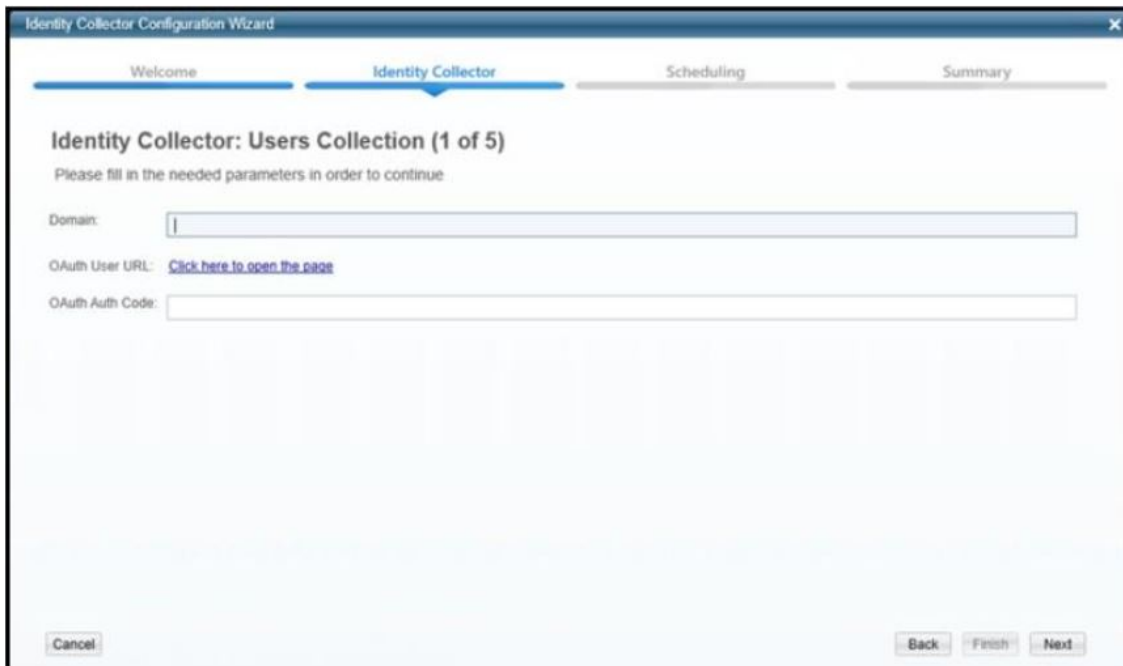
This means the configuration will resemble other connectors for cloud applications such as OneDrive.

- Configuring the Identity Collector, instead of providing a username and a password, you will click on a link that sends you to a Microsoft login page.
- Enter the relevant user credentials and give your consent for the File Access Manager Azure AD O365 Application to access your directory data.
- You will then copy the resulting Authorization Code to the appropriate field, which will then be used to generate the first access token.
- The access token will be used in all requests to the tenant's Azure AD and will be automatically refreshed when needed.

### Configuration

Complete the following steps:

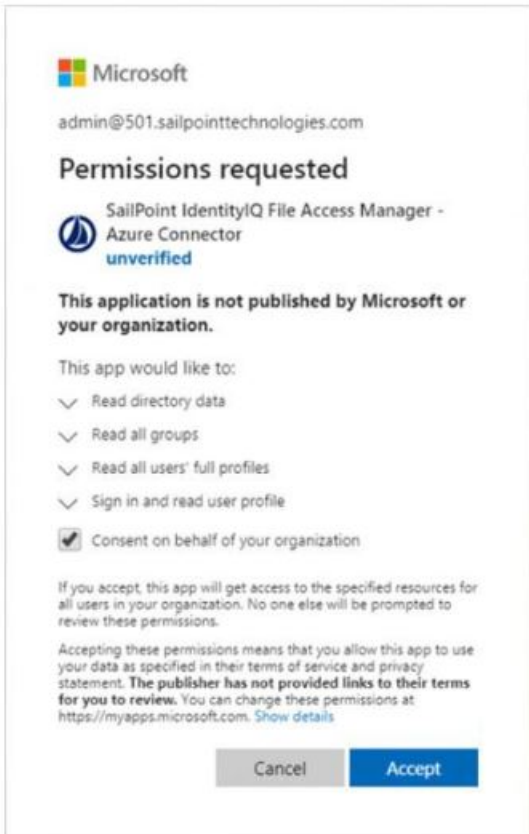
1. In the Identity Collector Configuration Wizard enter your O365 Domain name, then click on the **OAuth User URL** link to generate an Authorization Code.



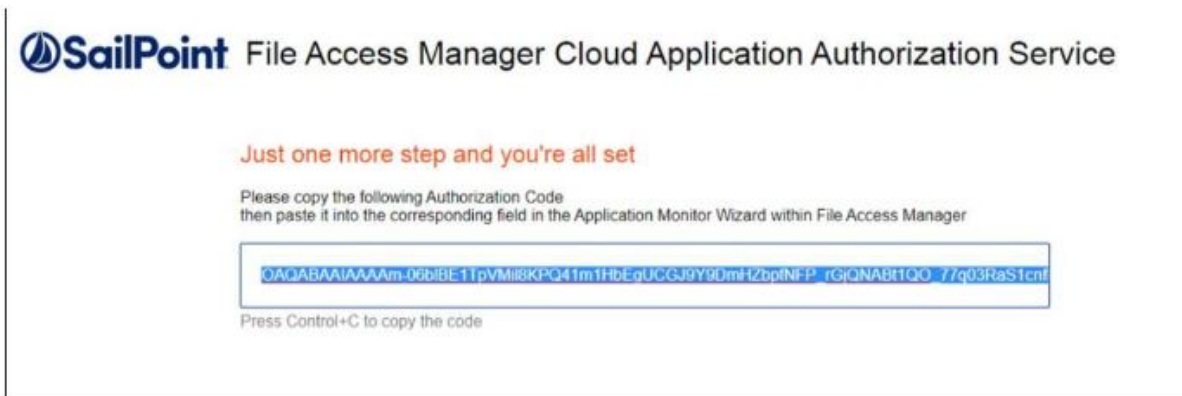
2. You will then be redirected to the Microsoft O365 Login Screen Login with the user that should be used by the Identity Collector.



3. You will then be prompted to consent to granting access to the File Access Manager Azure Connector Accept to receive an Authorization Code and continue with generating the Access Token.



- A final redirect will lead you to the File Access Manager Cloud Application Authorization Service, and will present the received Authorization Code.



- Copy that code and past it in the Auth Code field in the Identity Collector Configuration Wizard screen.
- Click **Next** and complete the Identity Collector configuration flow.

## Permissions

The File Access Manager Azure AD Connector requires the following permissions:

- Directory.Read.All – this Permission grants read only access to AAD contents (by default, all domain users can read all AAD data).

## Azure Active Directory Connectivity Requirements

File Access Manager uses the AzureAD graph API – which works exclusively in HTTPS.

The API base path is : `https://graph.windows.net/{tenant_domain_name}` where the tenant domain name is the customer assigned domain name on Microsoft cloud. It is usually in the format of `domain_name.on-microsoft.com`, but might be changed in your configuration.

***A list of resources that are accessed by File Access Manager using the REST graph API include:***

`https://graph.windows.net/{tenant_domain_name}/tenantDetails`

`https://graph.windows.net/{tenant_domain_name}/users`

`https://graph.windows.net/{tenant_domain_name}/users/{user_id}`

`https://graph.windows.net/{tenant_domain_name}/groups/{group_id}`

`https://graph.windows.net/{tenant_domain_name}/directoryRoles`

`https://graph.windows.net/{tenant_domain_name}/directoryRoles/{role_id}`

## Administrator's Consent Requirements

To grant a third-party application (ISV) with the Directory.Read.All permission requires an administrator consent, which can be given by users with one of the following roles:

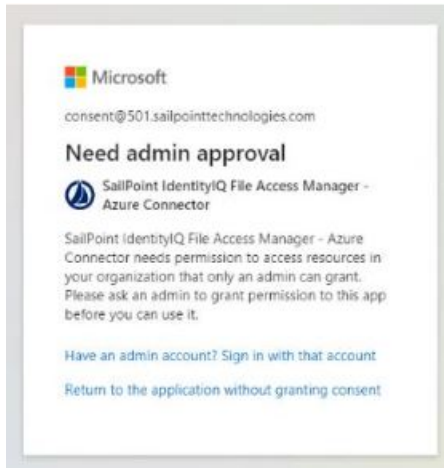
- Global Administrator (Company Administrator)
- Cloud Application Administrator
- Application Administrator

Hence, during the initial configuration phase (while generating the token for the first time), the service account dedicated to the File Access Manager Azure AD Connector must have one of the above-mentioned roles. Once consent is given, the role can be removed from the user.

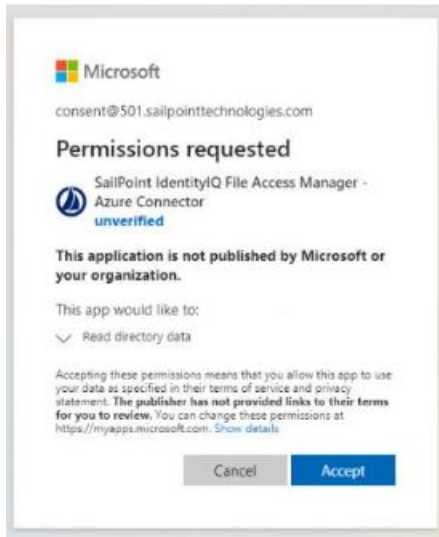
The Consent flow will appear different for users with different roles.

Non-admin user trying to access the consent screen will be presented with the following screen:

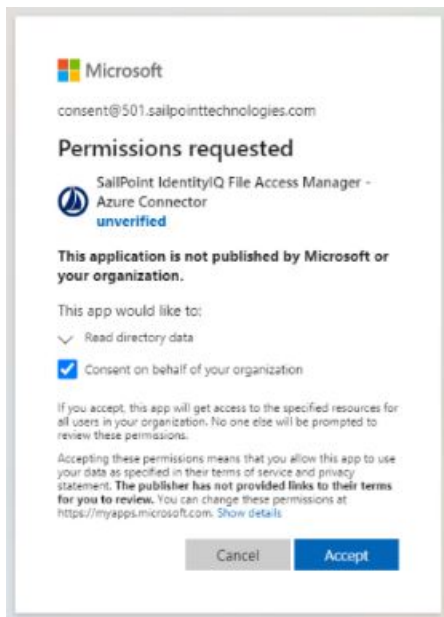




Application Administrators trying to access the consent screen, will be presented with a request to consent and grant the File Access Manager Application the Read Directory Data permissions:



Users with the Global Administrator role trying to give consent to an application will be presented with a screen containing an additional checkbox (consent on behalf of your organization):



This extra checkbox consents to give permissions to the application on behalf of all other users in the organization, thereby ensuring no other user would have to explicitly give consent to the app to run on its behalf. File Access Manager does not require this checkbox to be checked, as our application only needs to run on behalf of the consenting user.

Checking this option is optional, and not mandatory.

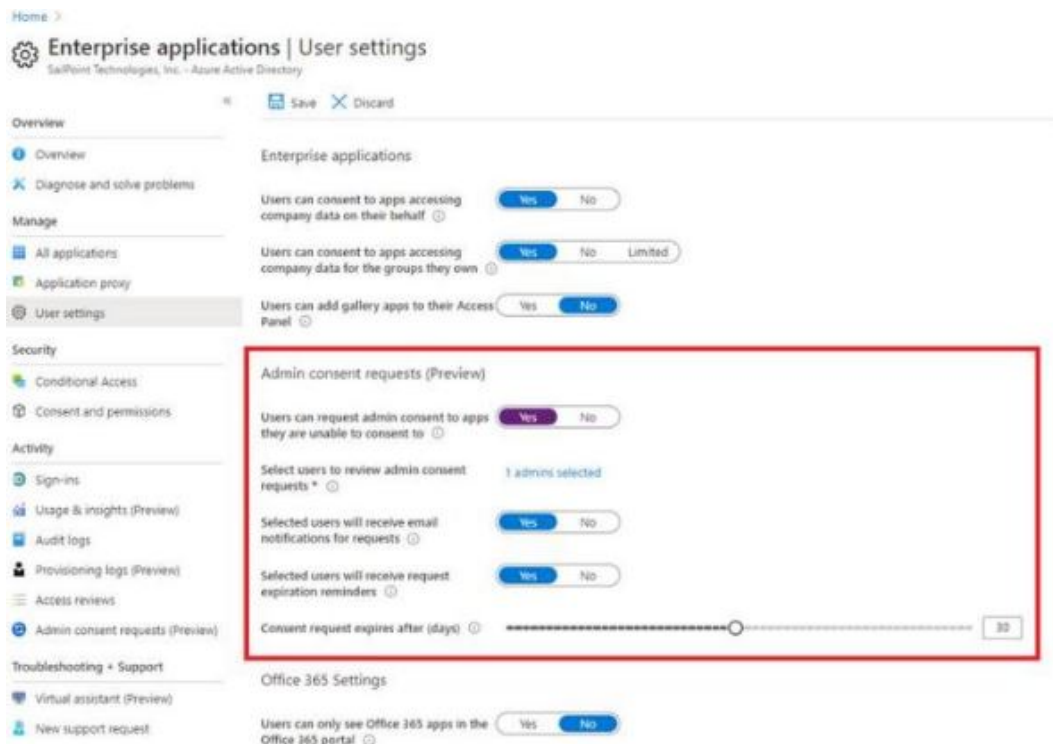
### Avoiding the Administrative Roles Grant

To avoid granting an administrative role to the service account, even if only for the duration of the consent sequence, you may use Azure's AdminConsentRequests.

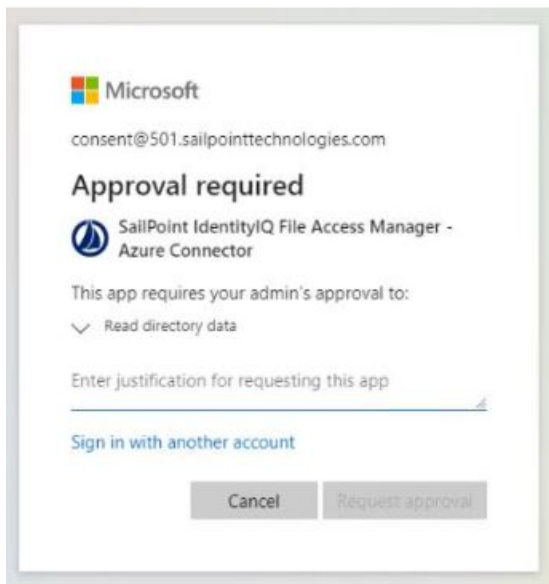
This relatively new feature lets non-admin users indirectly give consent to applications that require admin consent by requesting an admin's authorization.

This feature can be enabled on the tenant's level, and allows setting one of the three above-mentioned administrator roles as are viewer:

## System Settings Required to Support SSO

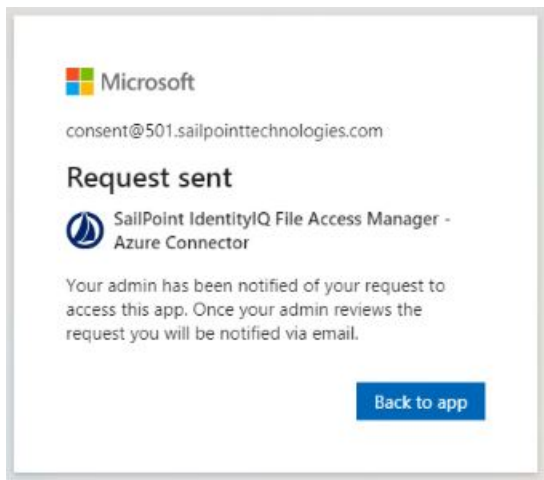


When users without one of these administrative roles go through the normal consent flow, they will be presented with the screen:



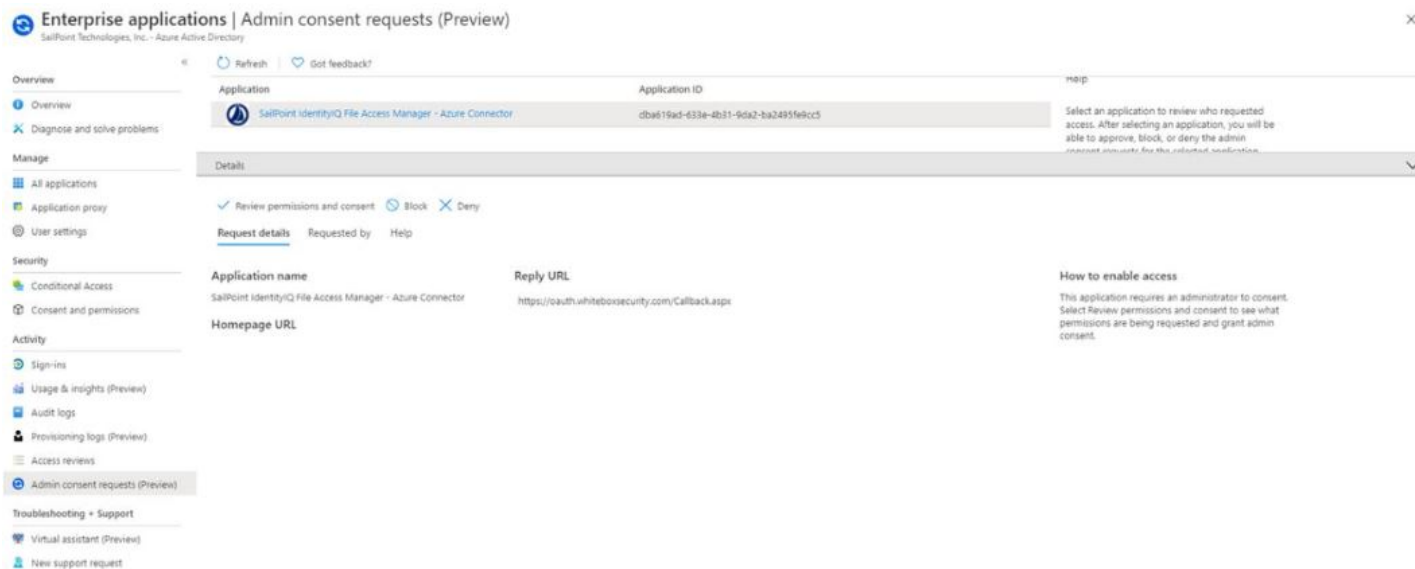
The requested is required to provide a justification for granting consent to the application and a request is sent to the administrator listed in the configuration as reviewers.

When clicking on **Request approval** to continue, the following screen appears:

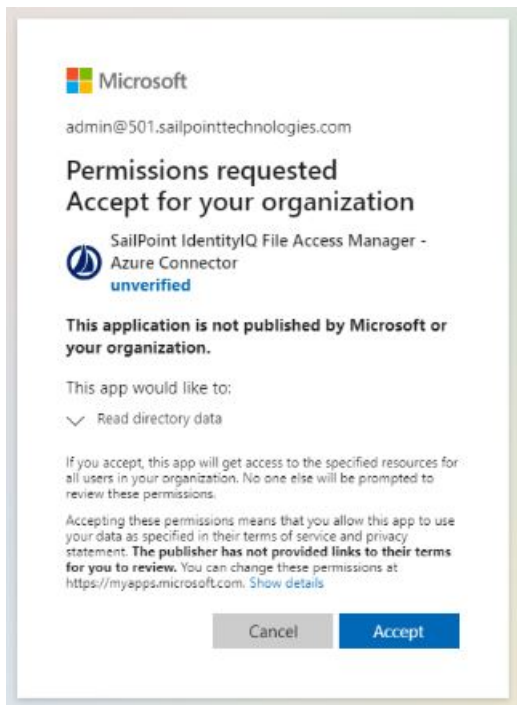


Clicking on **Back to app** would just return an access denied error as access was not yet granted. This screen can be safely closed while waiting for admin consent.

The reviewing administrator will either receive an email notifying them of the request, or have to go to the Admin Consent Requests screen and check for new requests:



To approve a request, the administrator will go through the Review permissions and consent flow, where they will be presented with the familiar consent screen:



After an administrator Accepts, non-administrator users will have to go through token generation sequence again. However, this time the consent screen will be skipped entirely, and the flow will lead directly to the Authorization code.

Note: This method gives consent to the app on behalf of the entire organization, similar to when a Global Administrator ticks the checkbox to enable the Consent on behalf of your organization, as described above.