



File Access Manager Installation Guide

Version: 8.3 Revised: March 30, 2022

This document and the information contained herein is SailPoint Confidential Information

Copyright and Trademark Notices.

Copyright © 2022 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

Contents	iii
Planning Your Installation	1
File Access Manager Architecture	1
Disaster Recovery	1
High Availability	1
High Security Deployment	1
File Access Manager Connector Services	1
Sizing Considerations	1
Authentication Method	2
Support Matrix	3
File Access Manager Server Support Information	3
Endpoint Support Information	3
Database Configuration	4
Dedicated Instance	4
Required Features	4
Required Settings	4
Hyper-Threading	4
Storage	4
Backup & Recovery	4
Temp Database	4
Recommended Performance	5
Preparing for Installation	6
Pre-Installation Checklist	6
Communication Requirements	6
.NET	6
Verifying .NET Core Settings	7
Inter-service Communication	8
Ensuring HTTP/2 Support	9

Connection Errors	9
Configuring File Access Manager to use SAML Authentication	10
Creating an Okta Application	10
Creating an ADFS Application	19
Creating an Azure Application	23
Switching from SAML to Windows Authentication Mode	27
File Access Manager Installation	32
Installation Log File	32
Server Installer	32
Creating a Database Using the Installer	33
Creating the Configuration	34
Adding a Server	34
Disaster Recovery Configuration	36
Service Configuration	36
Configuring High Availability Services	39
Website Configuration	41
IIS Settings	42
Website Authentication Mode	42
Service Configuration Summary	43
Storing the Configuration	43
Performing the Installation	43
Installation Using the Server Installer	44
Unattended Installation	44
Installation Command Script	44
Service Migration	46
Source Server – Database Connection	46
Source Server – Configuration Modification	46
Source Server – Configuration Summary	47
Source Server – Uninstallation Process	47

Target Server – Database Connection	47
Target Server – Install Migrating Service(s)	47
Administrative Client Installation	48
File Access Manager Website SSL	49
Recommended Secured Deployment	51
Required Environment	51
Installation Considerations and Constraints	51
Post Installation Configuration	51
Configuring the Process Exploit Mitigation for File Access Manager Services	52
Configuring the Program Settings Using FAM.Exploit.protection.Settings.xml Script	52
Configuring the Program Settings Using the Windows Defender Settings Tool	52
Enabling New Version Notifications	53
Removing Unnecessary Banner Information on Web Responses	54
System Settings Required to Support SSO	55
System Settings to Support SSO - Okta	56
Detailed Settings	56
System Settings to Support SSO - ADFS	60
Detailed Settings	60
Creating or Editing an Active Directory Identity Collector	61
System Settings to Support SSO - Azure	66
Detailed Settings	67
Creating or Editing an Azure Identity Collector	67
Azure AD Connector Full OAuth 2.0 Support	67
Configuring File Access Manager to Use Local Certificates	76
Changing Certificates for Elasticsearch	76
High Level Steps	76
Detailed Steps	76
Changing Certificates for RabbitMQ	78
Changing the Certificates for Core Services	78

Changing the Certificates for Collectors	79
Installing Collectors on a Server Without Core Services	79
Uninstalling File Access Manager	80
Uninstalling the File Access Manager Administrative Client	80
Uninstalling the Collectors	80
Uninstalling the File Access Manager Services	81
Uninstalling Elasticsearch	81
Uninstall all the Remaining Services	83
Cleanup After Uninstalling File Access Manager	83
Troubleshooting	85
Users Cannot Log into the Website After First Installation	85
3rd Party SSO Login Users Cannot Access the Website	85
Further Information	85

Planning Your Installation

File Access Manager Architecture

File Access Manager architecture usually requires a central installation with some remote gateways. Most File Access Manager connectors do not require any footprint on the monitored/analyzed system and therefore are installed on File Access Manager servers.

In some cases, due to 3rd party vendors (mostly NAS vendors), it is imperative to have a local server at the same physical site where the monitored system is located.

For more information on File Access Manager architecture see “Capabilities and Architecture” in the File Access Manager Administrator Guide.

Disaster Recovery

File Access Manager supports disaster recovery, based on building a parallel backup system as described below. This setup will lower any downtime incurred by physical servers going down.

The fail-over between systems is a combination of automatic and manual processes and procedures.

For a full description of the disaster recovery procedure, see the “Disaster Recovery Plan” document.

High Availability

File Access Manager supports a high availability configuration. The solution involves configuring duplicate services on additional servers, and having a customer deploy a load balancer to manage the services traffic. When a production service, or entire server stops for any reason, the load balancer will route the traffic to another service on a different server.

The services configuration is performed in the installation phase, as described in this guide.

High Security Deployment

If you require a higher security deployment, refer to the chapter [Recommended Secured Deployment](#).

File Access Manager Connector Services

Each type of connector has its own pre-requisites and its own configuration. See the relevant Connector Installation guide for more information about the connector.

Sizing Considerations

File Access Manager is a scalable solution that enables the distribution of its services and also works in an all-in-one mode. The Administrator Guide has a complete description of the File Access Manager architecture configuration.

One of the critical sizing considerations is the amount of disk space required to store activities over time. The table below describes the guidelines

Service	CPU	Memory	Disk
Elasticsearch	Minimum of 4 cores, Recommended 8	Minimum of 8Gb, Recommended 16Gb	0.5kb per event

Service	CPU	Memory	Disk
SQL Database			3.5kb per event

Additional factors that affect the required hardware are:

- Disaster recovery environment
- High Availability solution

It is highly recommended to consult with your SailPoint File Access Manager representative to obtain the correct configuration to support your requirements.

Authentication Method

The File Access Manager login process can use Active Directory, or be integrated with any identity provider (IdP) supporting SAML 2.0-based authentication.

Detailed integration steps are available for the following providers:

- Azure
- Okta
- ADFS

Support Matrix

File Access Manager Server Support Information

System	Supported Versions
File Access Manager Servers	Windows 2012R2 / 2016 / 2019 / 2022
Workstation	Windows 7 and above
Browser	IE11, Edge, Safari, Chrome, Firefox
Database	MS SQL Server 2012 / 2014 / 2016 / 2017 / 2019

Endpoint Support Information

[See the File Access Manager Connectors support document in Compass.](#)

Each connector has a separate Installation guide, with more information on supported versions and prerequisites.

Database Configuration

Dedicated Instance

We recommend installing File Access Manager on a dedicated instance. This configuration enables independence of configuration and assures resource allocation for the instance.

We realize, however that a dedicated instance is a costly solution and therefore might be chosen at a later stage.

Some of the File Access Manager requirements can be defined at the instance level and can work in such a way that avoids the definition of specific requirements for shared databases.

This decision should be part of the sizing process led by your SailPoint File Access Manager representative.

Required Features

File Access Manager uses MS SQL Standard Edition that utilizes the database engine only. No other feature is required. File Access Manager thus enables the use of MS SQL native features for high availability and encryption without any interruption.

Required Settings

The following settings must be chosen for the installation instance.

- FILESTREAM using "Full Access Enabled"
- CLR enabled (Running .NET code in the database in Safe mode)
- SQL Mixed Authentication

Hyper-Threading

It is recommended that hyper-threading on physical servers be disabled.

Storage

For a database server running as a virtual machine (of any kind), verify that the drives connected for the database storage are REAL disks (dedicated for the virtual machine).

- The drives must be separated for Data and Logs.
- Format the drives with a 64K allocation unit.

Backup & Recovery

It is recommended that you use a Simple database recovery plan.

Choosing any other recovery plan requires scheduled log backups to prevent the log file from overflowing. Data performance may be affected during log backups since File Access Manager is very write I/O intensive.

Temp Database

Depending on your database configuration, you might require additional storage allocate for a temp database. Please discuss this with your DBA.

Ensure that the database is:

- defined on a separate drive
- real and formatted to a 64K allocation unit
- allocated a Temp database file for each real core on the system
- one that limits the Temp database files (and logs) so they do not overgrow the size of the disk

Recommended Performance

Metric	Requirement
Disk I/O Throughput (IOPS)	12K IOPS
Disk I/O Throughput Rate	10500 Mb/s
Throughput in Transactions/sec	6000 TPS
Disk I/O latencies for Read	< 8 ms
Disk I/O latencies for Write	< 1 ms

Preparing for Installation

Before starting the installation, prepare a checklist of the required data, open the required ports, and set up the servers, as described below.

Pre-Installation Checklist

Database server

Verify connectivity to the DB server.

Database instance

Database name for File Access Manager

Static/Dynamic ports

Static port – port number

Dynamic port – use 0

(Optional) SysAdmin (SA) user + password

SA user (or equivalent).

Data files location

Full path for database data files.

FileStream files location

Full path for database FileStream files.

Log files location

Full path for database log files.

Servers names

Verify connectivity and name resolution (NetBIOS name and DNS name).

Services distribution

The location of the various server services to be used in the installation.

Communication Requirements

File Access Manager is a service-oriented solution and as such enables the distribution of its services on multiple servers. The model is flexible, and services can be shifted between servers to boost performance.

.NET

File Access Manager requires the latest ASP.NET Core 3.1.x Hosting Bundle. This bundle consists of .NET Runtime and ASP .NET Core Runtime.

You can download the latest 3.1.x Hosting Bundle version from [here](#)

Download .NET Core 3.1

Not sure what to download? [See recommended downloads for the latest version of .NET.](#)

Release information	Build apps - SDK	Run apps - Runtime																												
<p>v3.1.16</p> <p>Security patch</p> <p>Release notes</p> <p>Released June 08, 2021</p>	<p>This release contains multiple SDKs. If you're using Visual Studio, look for the SDK that supports the version you're using. If you're not using Visual Studio, install the first SDK listed.</p> <p>SDK 3.1.410</p> <p>Visual Studio support Visual Studio 2019 (v16.7) Visual Studio 2019 for Mac (v8.10)</p> <p>Included in Visual Studio 16.4.23, 16.7.16, 16.9.7</p> <p>Included runtimes .NET Runtime 3.1.16 ASP.NET Core Runtime 3.1.16 .NET Desktop Runtime 3.1.16</p> <p>Language support C# 8.0 F# 4.7 Visual Basic 15.9</p> <table border="1"> <thead> <tr> <th>OS</th> <th>Installers</th> <th>Binaries</th> </tr> </thead> <tbody> <tr> <td>Linux</td> <td>Package manager instructions</td> <td>Arm32 Arm64 Alpine</td> </tr> <tr> <td>macOS</td> <td></td> <td>x64</td> </tr> <tr> <td>Windows</td> <td>Hosting Bundle x64 x86</td> <td>Arm32 x64</td> </tr> </tbody> </table>	OS	Installers	Binaries	Linux	Package manager instructions	Arm32 Arm64 Alpine	macOS		x64	Windows	Hosting Bundle x64 x86	Arm32 x64	<p>ASP.NET Core Runtime 3.1.16</p> <p>The ASP.NET Core Runtime enables you to run external applications. On Windows, we recommend installing the ASP.NET Core Runtime, which includes the .NET Runtime and IIS support.</p> <p>IIS runtime support (ASP.NET Core Module v2) 13.1.21133.16</p> <table border="1"> <thead> <tr> <th>OS</th> <th>Installers</th> <th>Binaries</th> </tr> </thead> <tbody> <tr> <td>Linux</td> <td>Package manager instructions</td> <td>Arm32 Arm64 Alpine</td> </tr> <tr> <td>macOS</td> <td></td> <td>x64</td> </tr> <tr> <td>Windows</td> <td>Hosting Bundle x64 x86</td> <td>Arm32 x64</td> </tr> </tbody> </table> <p>.NET Desktop Runtime 3.1.16</p> <p>The .NET Desktop Runtime enables you to run external applications. This release includes the .NET Runtime, which you must install it separately.</p> <table border="1"> <thead> <tr> <th>OS</th> <th>Installers</th> </tr> </thead> <tbody> <tr> <td>Windows</td> <td>Hosting Bundle x64 x86</td> </tr> </tbody> </table>	OS	Installers	Binaries	Linux	Package manager instructions	Arm32 Arm64 Alpine	macOS		x64	Windows	Hosting Bundle x64 x86	Arm32 x64	OS	Installers	Windows	Hosting Bundle x64 x86
OS	Installers	Binaries																												
Linux	Package manager instructions	Arm32 Arm64 Alpine																												
macOS		x64																												
Windows	Hosting Bundle x64 x86	Arm32 x64																												
OS	Installers	Binaries																												
Linux	Package manager instructions	Arm32 Arm64 Alpine																												
macOS		x64																												
Windows	Hosting Bundle x64 x86	Arm32 x64																												
OS	Installers																													
Windows	Hosting Bundle x64 x86																													

Without completing this step, the upgrade will fail.

- All servers hosting File Access Manager services, including all Activity Monitors must, have .NET Core 3.1.x installed as a prerequisite for the upgrade.
- The administrative client computer must contain .NET Framework 4.7.2
- The User Interface service server must contain .NET Framework 4.7.2

.NET Core and .NET Framework 4.7.2 can be installed on the same server

Verifying .NET Core Settings

Complete the following steps to verify the version of .NET Core:

- Open a CMD window.
- Execute the following command:
 - dotnet --list-runtimes

The output should consist of at least these two:

- Microsoft.AspNetCore.App 3.1.x
- Microsoft.NETCore.App 3.1.x

If the command did not execute or the two runtimes mentioned above are not in the output list, reinstall or repair the hosting bundle.

Inter-service Communication

File Access Manager uses SSL communications for all its deployed services.

SSL communications use Server and Client Certificates which, by default, are self-signed and created when each service is installed. While the operating system may “not trust” these certificates, File Access Manager components do “trust” them.

The table below lists the relationships among the services and clients.

Service	Clients	Default Port
Agent Configuration Manager	Activity Monitor Event Manager Central Data Classification Central Permissions Collector Data Classification Collector Permissions Collector Collector Installation Manager	8000
Event Manager	Activity Monitor User Interface Central Data Classification Scheduled Task Handler Central Permissions Collection Web Server	8001
Reporting Service	User Interface	8006
User Interface	File Access Manager Administrative Client	8005
Workflow	User Interface	8008
Elasticsearch	Event Manager Reporting Service Scheduled Task Handler User Interface Web Server	9200
RabbitMQ	Central Permissions Collector Central Data Classification Permissions Collector Data Classification Collector	5671

Service	Clients	Default Port
RabbitMQ	Schedule Task Handler	15671
Activity Analytics	None	8010

It is a best practice for all components to be in a safe, secure network, behind firewalls, even though SSL secured communication is enabled.

Ensuring HTTP/2 Support

Services will only accept http/2 connections (version 8.2 uses gRPC as the communication protocol, the requires http2).

Once fully upgraded File Access Manager services should work seamlessly with http2. In some cases, some communication middleware components (such as load balancers, e.g.) may not be configured to support http/2, which may cause for communication failure and cause the upgrade to halt. As a pre-upgrade step ensure all servers and communication middleware components are configured to support http/2.

Connection Errors

Following a successful upgrade to version 8.2, services will only accept http2 connections (version 8.2 uses gRPC as the communication protocol, the requires http2).

Once fully upgraded, File Access Manager services should work seamlessly with http2. In instances where the customer upgrade halts after a successful Agent Configuration upgrade, one potential cause could be that the communication middleware (such as a load balancer) is not configured to work with http2.

The following error will be shown in the log of services trying to connect to the Agent Configuration manager:

```
Unable to connect to test.domain.com with user_name Grpc.Core.RpcException: Status(StatusCode=Internal, Detail="Bad gRPC response. Response protocol downgraded to HTTP/1.0.")at Grpc.Net.Client.Internal.HttpClientCallInvoker.BlockingUnaryCall[TRequest,TResponse](Method`2 method, String host, CallOptions options, TRequest request)at Grpc.Core.Interceptors.InterceptingCallInvoker.<BlockingUnaryCall>b__3_0[TRequest,TResponse](TRequest req, ClientInterceptorContext`2 ctx)at Grpc.Core.ClientBase.ClientBaseConfiguration.ClientBaseConfigurationInterceptor.BlockingUnaryCall[TRequest,TResponse](TRequest request, ClientInterceptorContext`2 context, BlockingUnaryCallContinuation`2 continuation)at Grpc.Core.Interceptors.InterceptingCallInvoker.BlockingUnaryCall[TRequest,TResponse](Method`2 method, String host, CallOptions options, TRequest request)
```

If such errors appear in the log files, make sure all communication middleware components are configured to work over http/2, and the connection is not downgraded to http/1.

In case the error appears in a service that is still in version 8.1, the errors may be safely ignored. Once the service is fully upgraded the errors will stop showing in the log.

Configuring File Access Manager 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.

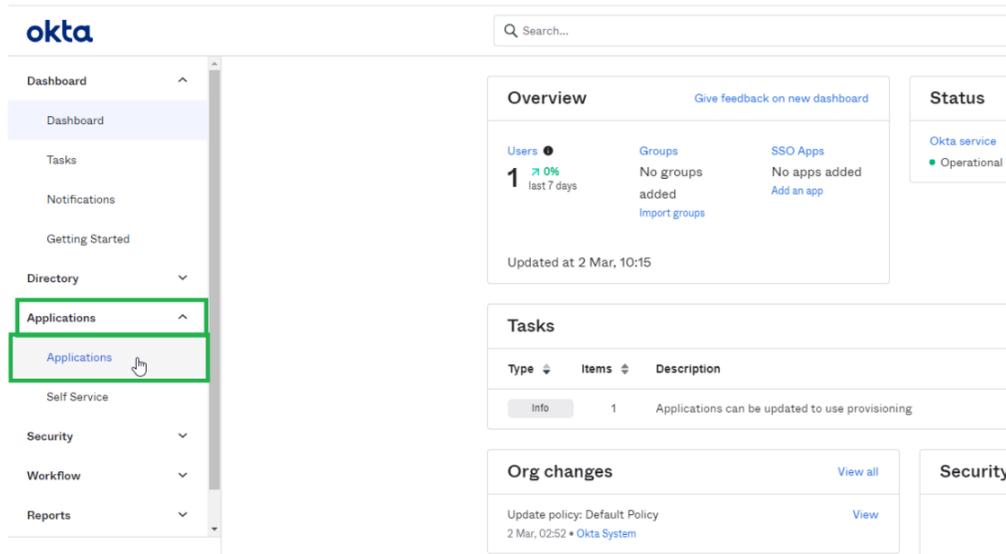
See [System Settings Required to Support SSO](#).

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.

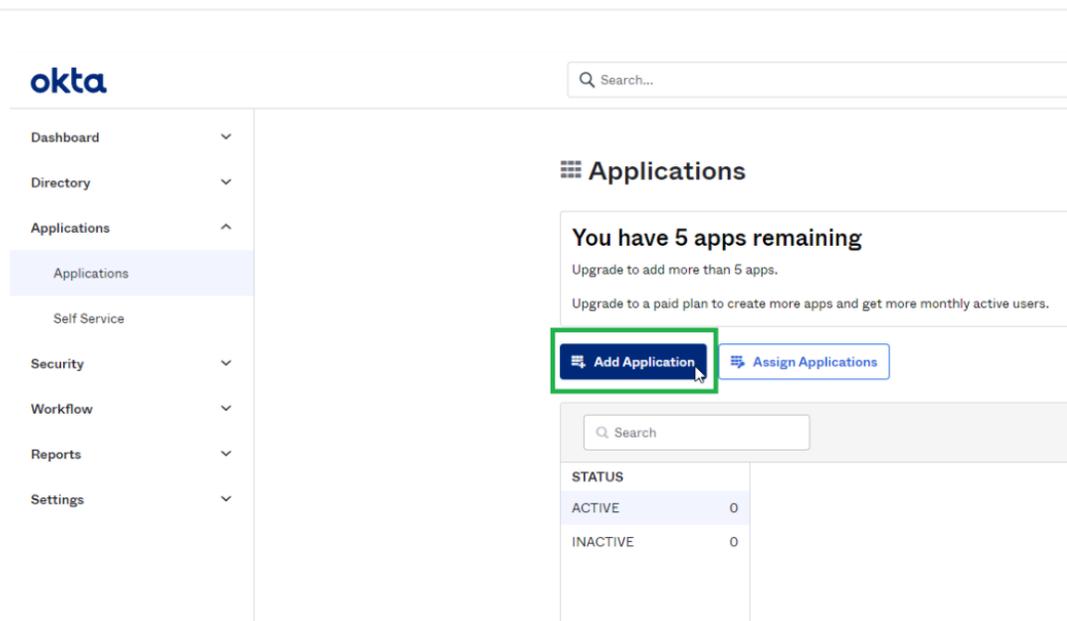
Creating an Okta Application

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

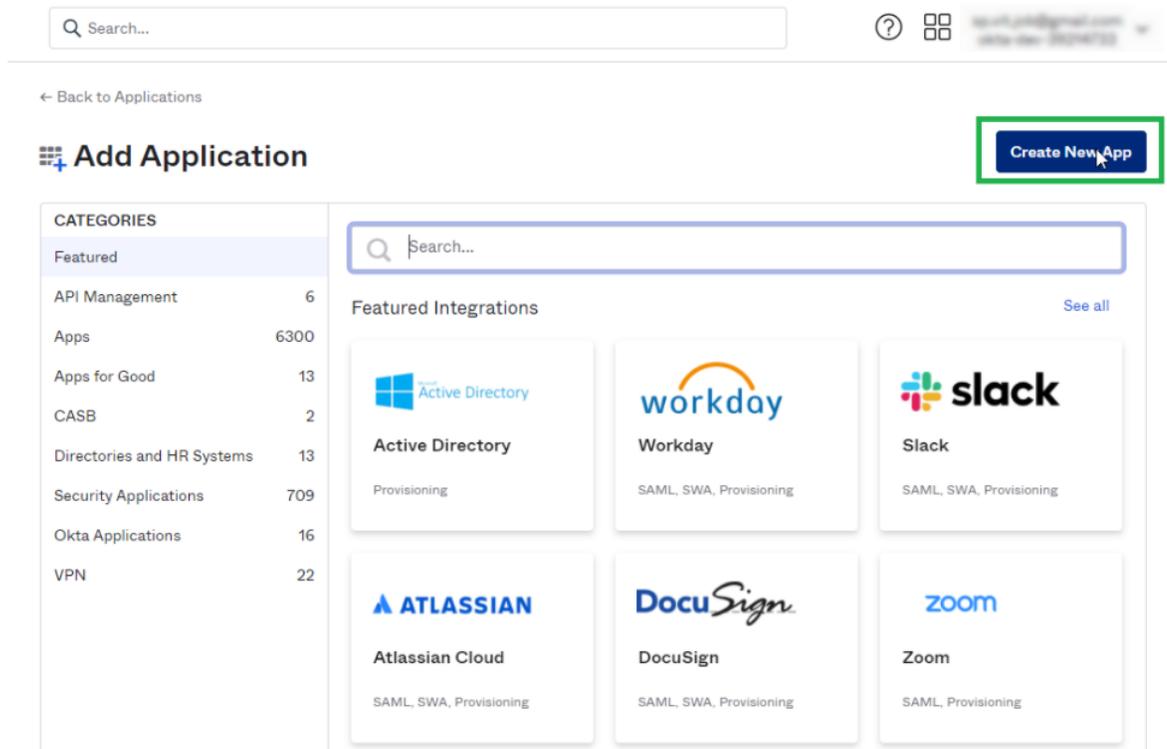
1. Open the **Create a new Application dialog**
 - a. Log into Okta
 - b. Click **Applications** to open the Applications screen



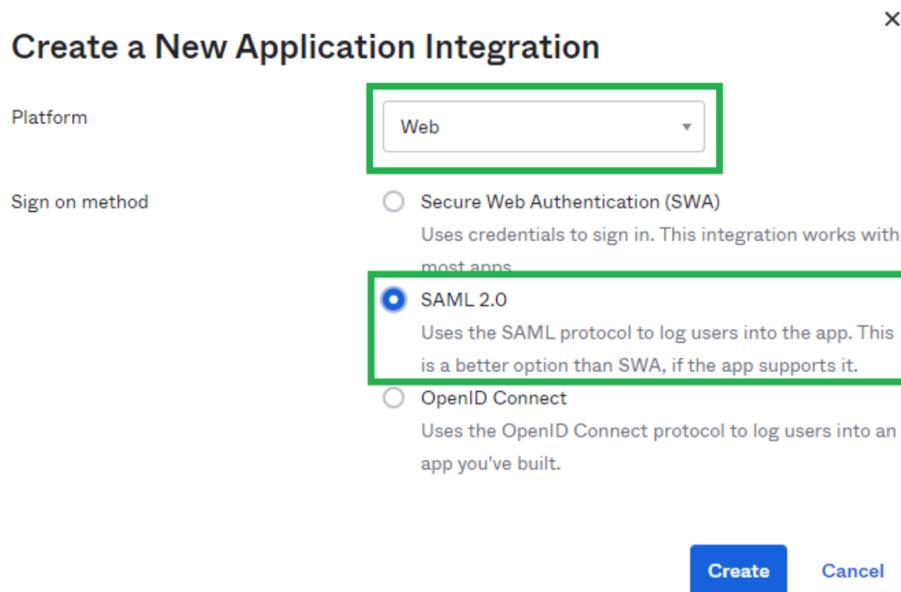
c. Click **Add Application**



d. Click **Create New App**



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



- f. Click **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

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?

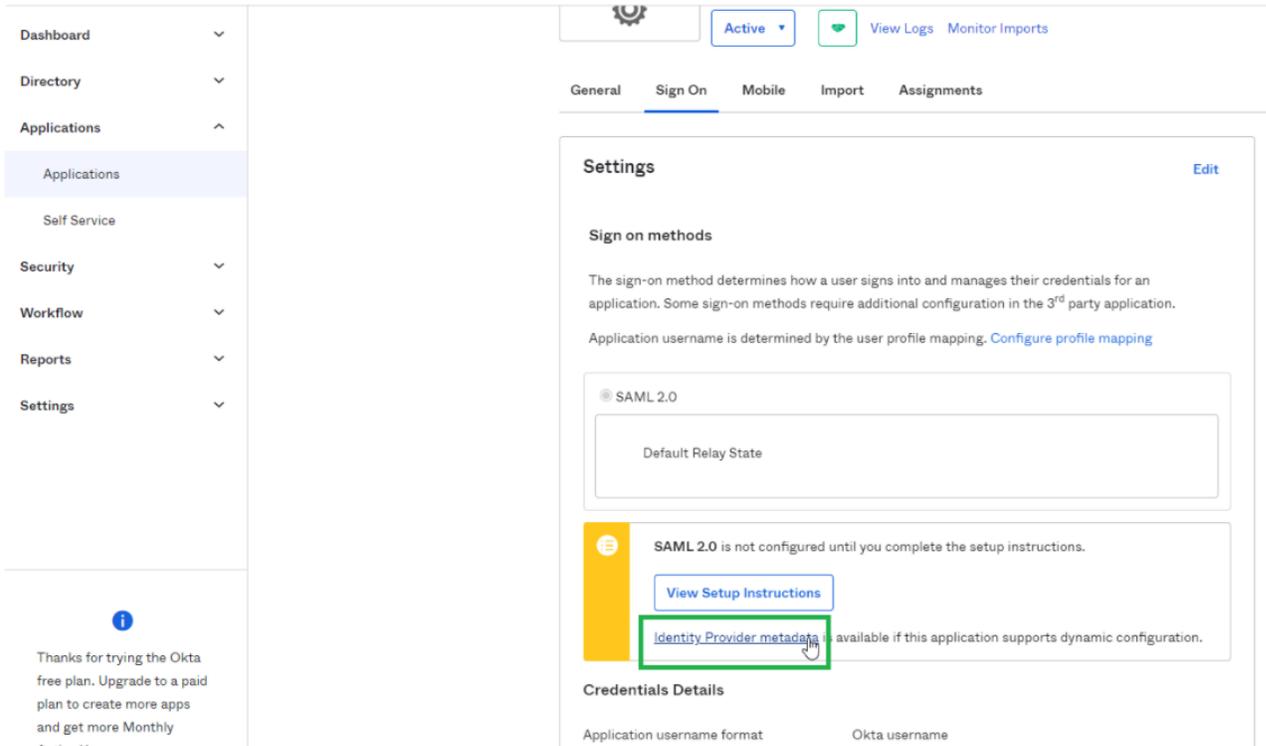
I'm an Okta customer adding an internal app

Click **Finish**

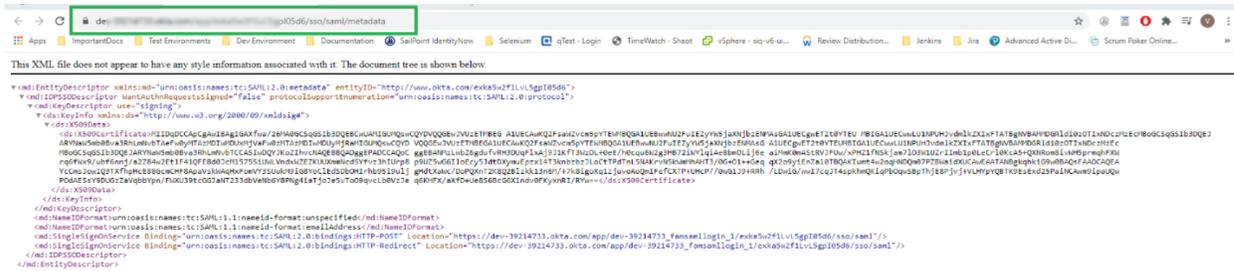
3. The application was successfully created

4. Click on the “Identity Provider metadata“

Configuring File Access Manager to use SAML Authentication

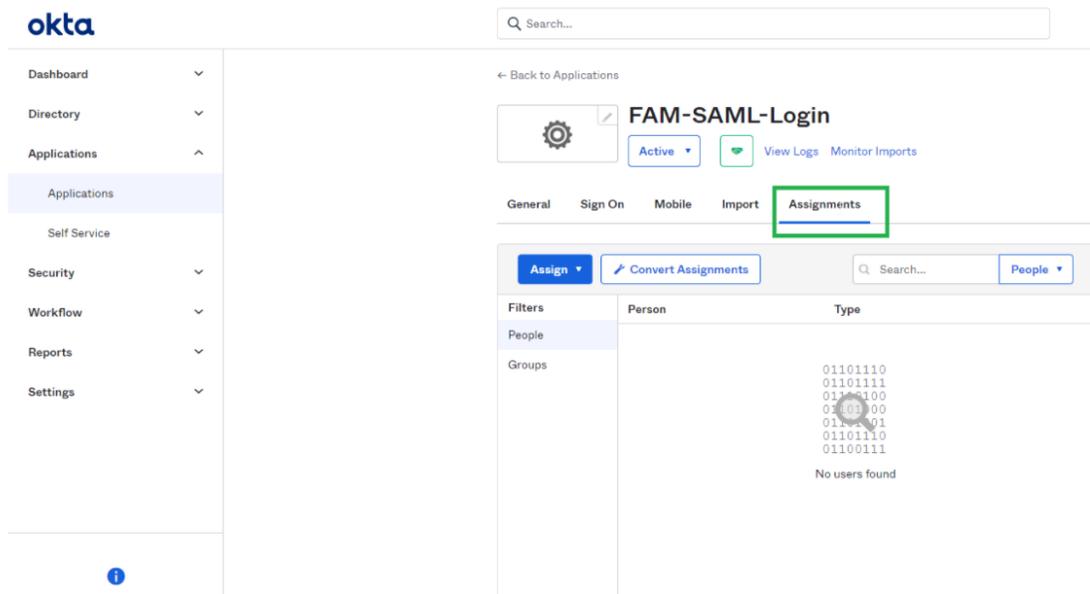


- 5. Copy the URL of the opened page. This will be used later during the installation of the File Access Manager using the SAML option

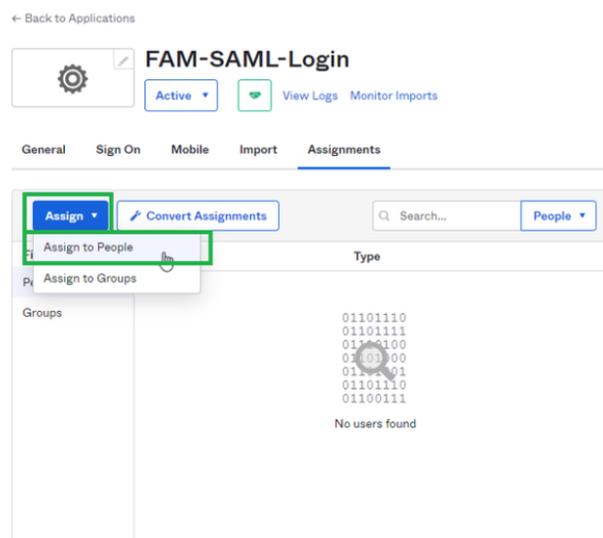


- 6. Add users who can see the application

- a. Click on the **Assignments** tab

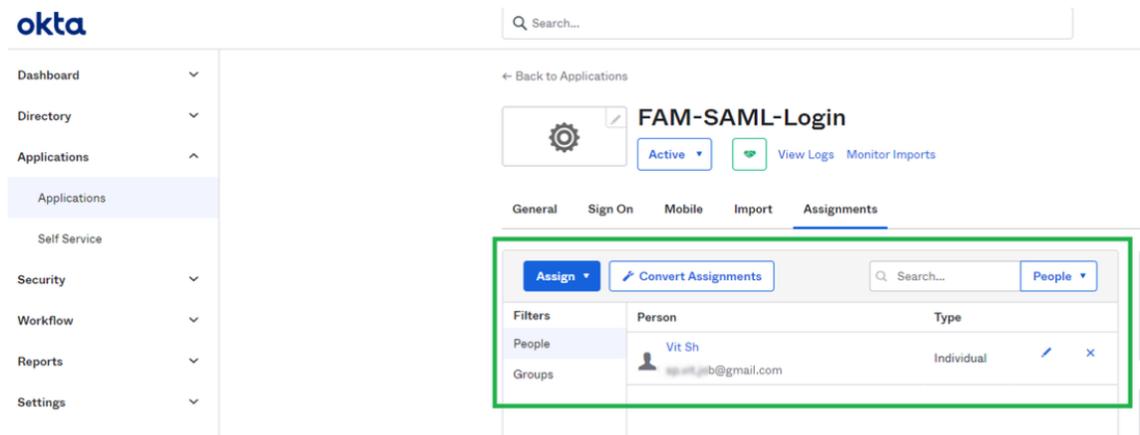


- b. Click **Assign** > **Assign to People**



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

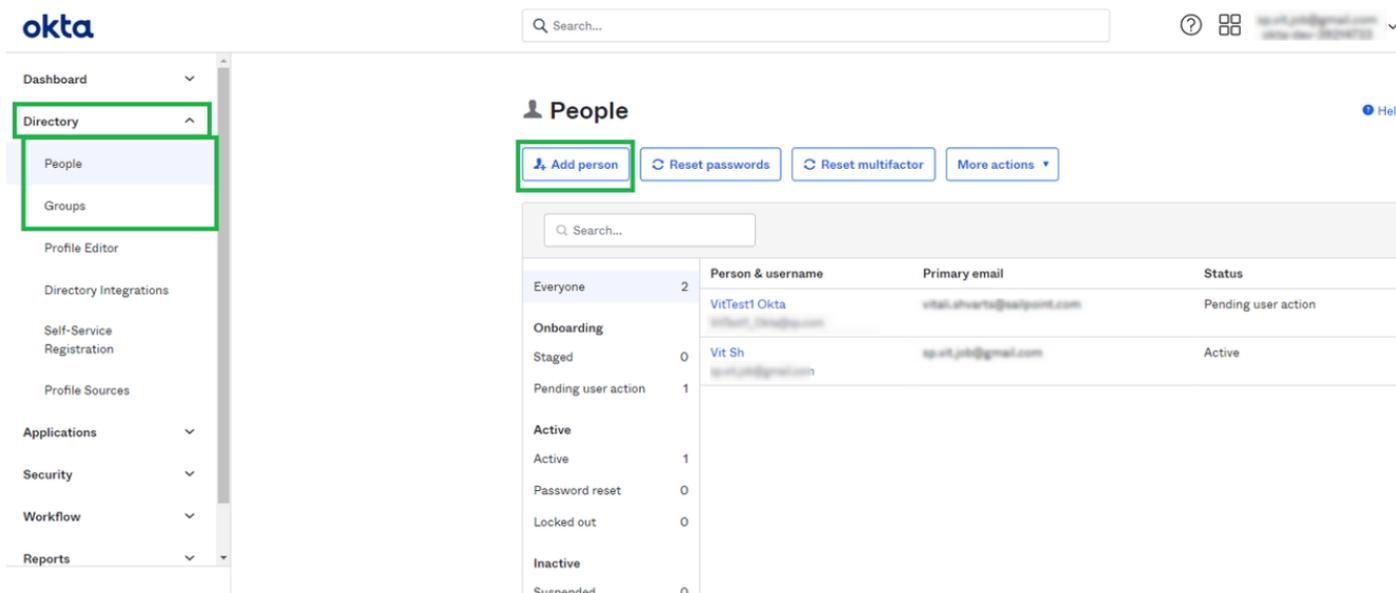
Configuring File Access Manager to use SAML Authentication



7. Additional users or groups can be added in

Directory > People > Add Person or Directory > Groups > Add Group

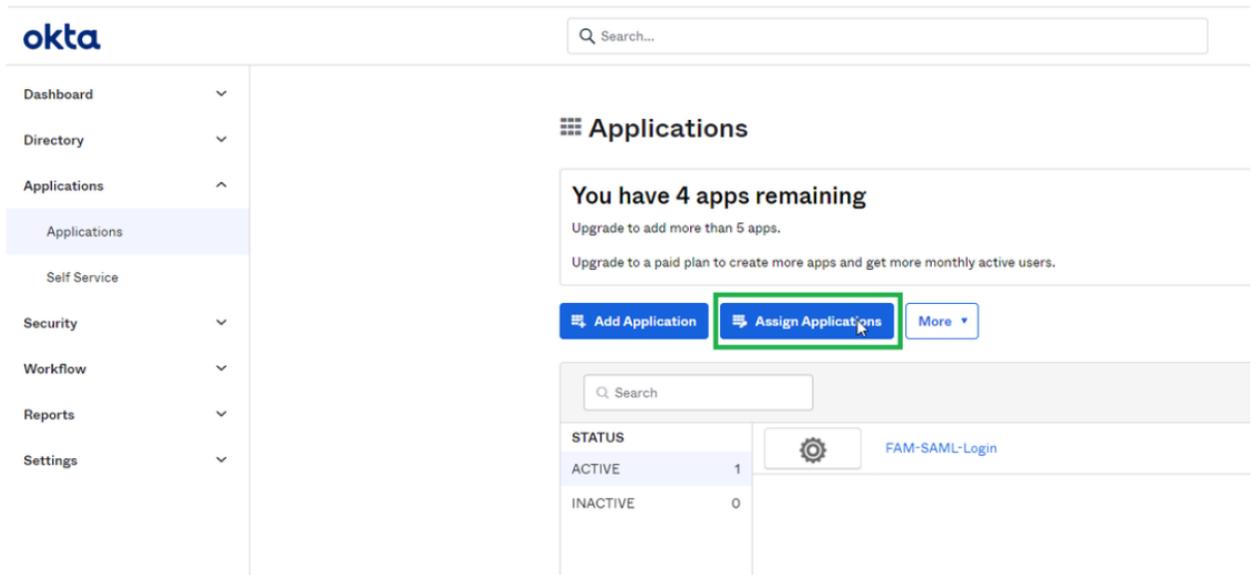
The user email entered should be an actual email, because it is used as part of the account activation process.



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

Configuring File Access Manager to use SAML Authentication

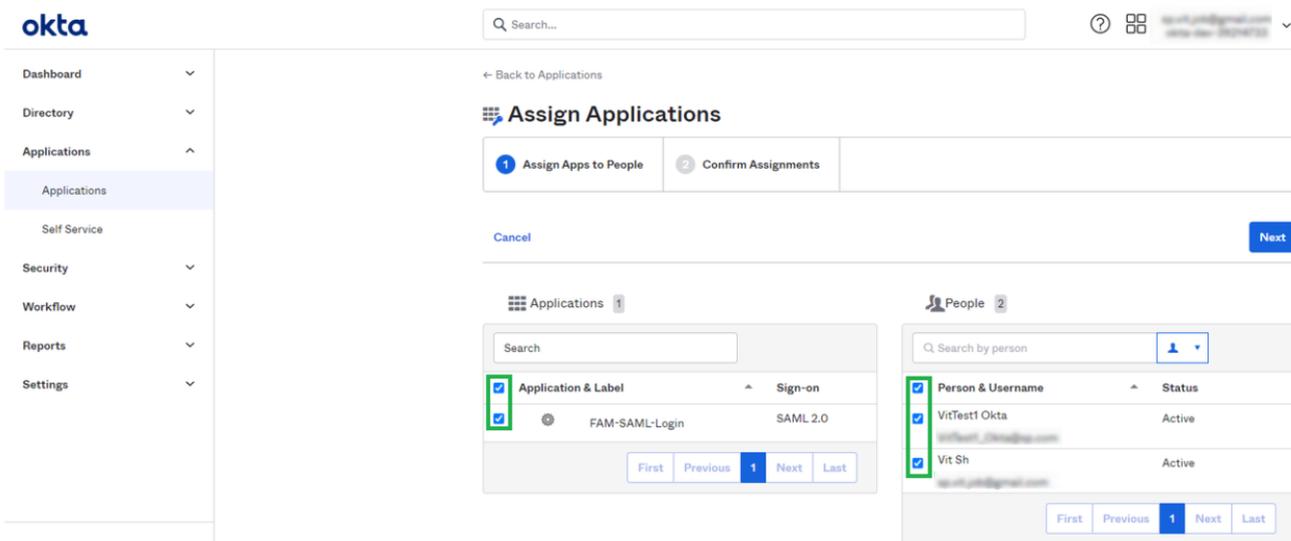
- Navigate to *Applications* > *Applications* and click the **Assign Applications** button.



The screenshot shows the Okta Applications page. The left sidebar contains navigation options: Dashboard, Directory, Applications (expanded), Self Service, Security, Workflow, Reports, and Settings. The main content area is titled 'Applications' and displays a message: 'You have 4 apps remaining. Upgrade to add more than 5 apps. Upgrade to a paid plan to create more apps and get more monthly active users.' Below this message are three buttons: 'Add Application', 'Assign Applications' (highlighted with a green box), and 'More'. A search bar is present above a table with the following data:

STATUS		
ACTIVE	1	 FAM-SAML-Login
INACTIVE	0	

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



The screenshot shows the 'Assign Applications' page in Okta. The page is divided into two main sections: 'Applications' and 'People'. The 'Applications' section has a search bar and a table with the following data:

Application & Label	Sign-on
<input checked="" type="checkbox"/> FAM-SAML-Login	SAML 2.0

The 'People' section has a search bar and a table with the following data:

Person & Username	Status
<input checked="" type="checkbox"/> VitTest1 Okta vittest1_@vit.com	Active
<input checked="" type="checkbox"/> Vit Sh vitsh@vit.com	Active

Both tables have pagination controls at the bottom, with the current page being 1 of 1. The 'Next' button is visible in the top right corner.

- Click **Next**
- Click **Confirm Assignment**

Configuring File Access Manager to use SAML Authentication

The screenshot shows the Okta Assignments page. The left sidebar has 'Applications' selected. The main content area is titled 'Review your assignments before confirming' and contains a confirmation dialog for the 'FAM-SAML-Login' application. The dialog includes a search bar and a table of user-specific attributes.

Person	User specific fields
VitTest1 Okta	Username: vittest1_1234@okta.com
Vit Sh	Username: vitsh.okta@gmail.com

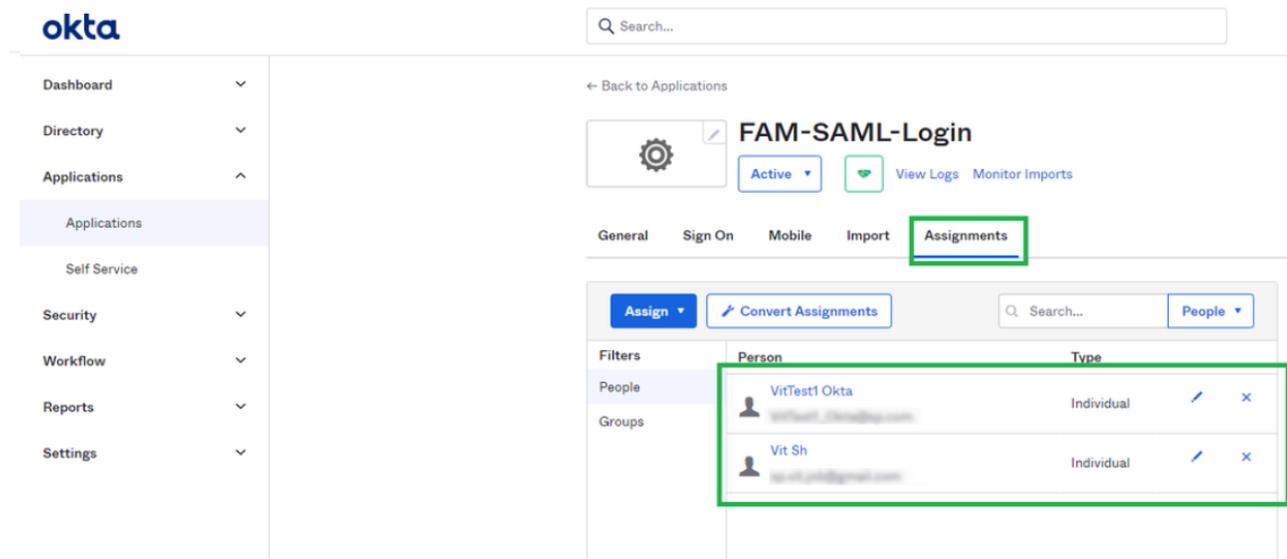
Showing 1 - 2 of 2

- e. Navigate to *Applications > Applications*
- f. Click on the Existing Application

The screenshot shows the Okta Applications page. The left sidebar has 'Applications' selected. The main content area is titled 'Applications' and shows a message: 'You have 4 apps remaining. Upgrade to add more than 5 apps. Upgrade to a paid plan to create more apps and get more monthly active users.' Below this is a table of applications.

STATUS		
ACTIVE	1	FAM-SAML-Login
INACTIVE	0	

- 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...**
3. 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)

Click **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

Click **Next**

5. Choose Profile: Select the first option **ADFS profile**

Click **Next**

6. Configure Certificate:

Click **Next**

7. Configure URL:

Click **Next**

8. Relying party trust identifier

Enter the name entered in the step **Specify Display Name** above.

Click **Add**

Click **Next**

9. Configure multi-factor authentication settings...:

Select "I do not want to configure multi-factor authentication..." option

Click **Next**

10. Choose Issuance...:

Select the first option "Permit all users to access the relying party"

Click **Next**

11. Ready to Add Trust

Click **Next**

12. Finish

"Open the Edit Claim Rules dialogue..." is checked

Click **Close**

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

Click **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"

Click **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. Click **Finish**
16. Click 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

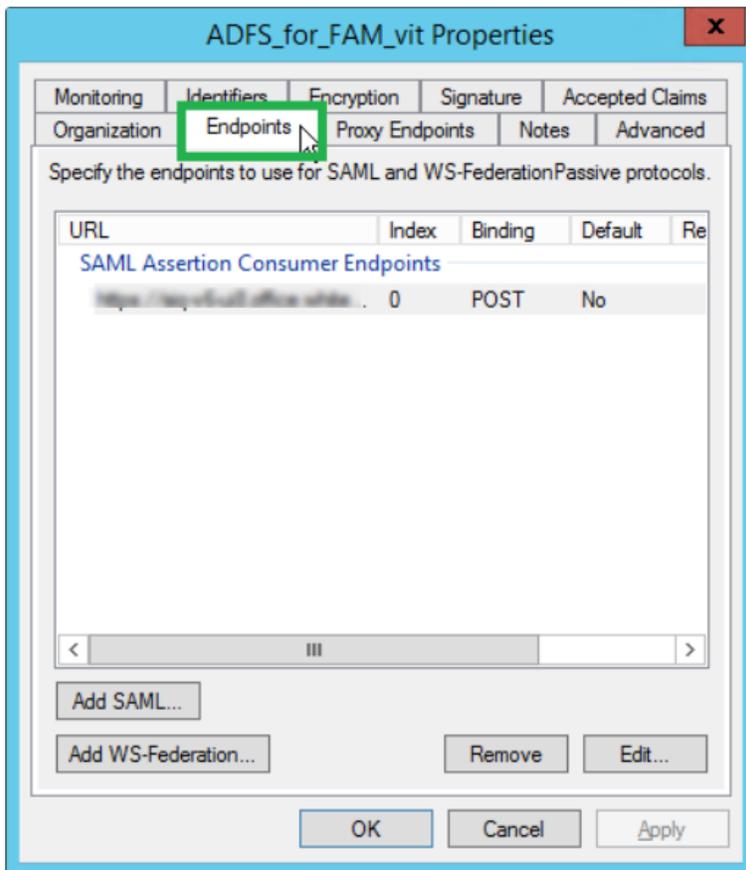
Unspecified

Pass through all claim values

Select this option

- b. Click **Finish**

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



21. Click Add SAML
22. Fill the following values in all fields:

Endpoint type

SAML Assertion Consumer

Binding

POST

Index

0

Trusted URL

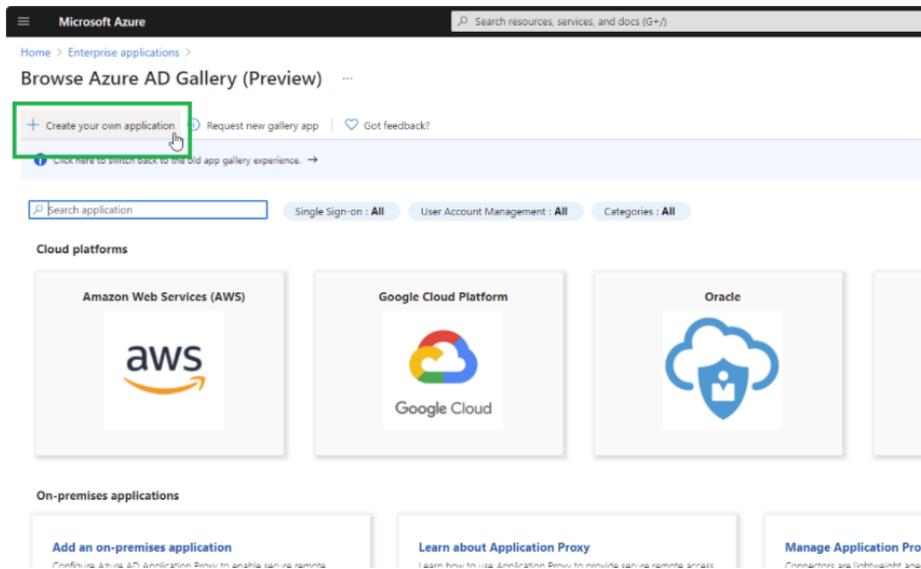
Enter the following link. This the ADFS where to redirect the user logging in (A link to the File Access Manager system) [https://\[SERVER_NAME\]/siqapi/login/AssertionConsumerService](https://[SERVER_NAME]/siqapi/login/AssertionConsumerService)

SERVER_NAME is the server in which the website is installed

23. Click **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

Configuring File Access Manager to use SAML Authentication



4. Fill the following fields:

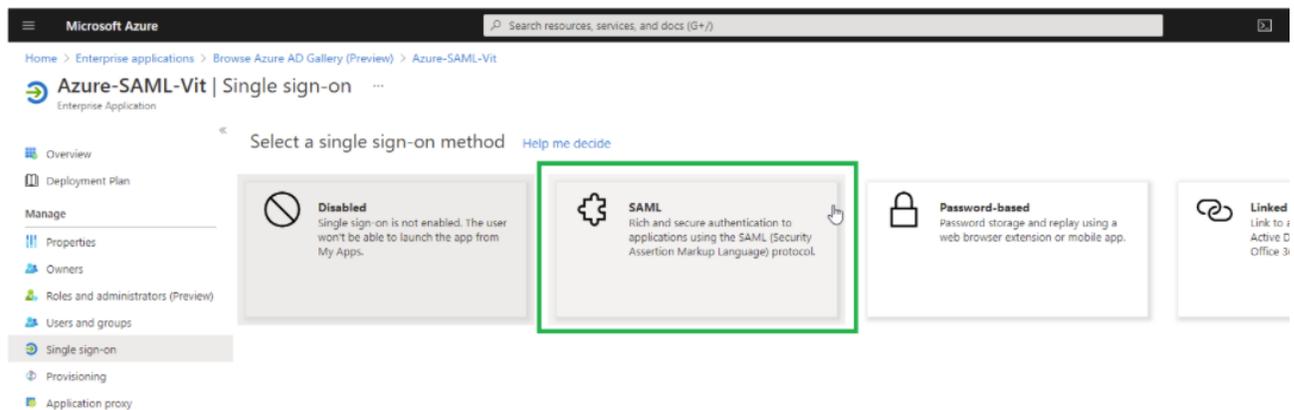
What's the name of your app?

Free text

What are you looking to do with your application?

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

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

Click **Save**.

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

Verify that the selected value is "user.userprincipalname"

Home > Azure-SAML-Vit > SAML-based Sign-on > User Attributes & Claims >

Manage claim ...

Name: nameidentifier

Namespace: http://schemas.xmlsoap.org/ws/2005/05/identity/claims

Choose name identifier format

Unspecified

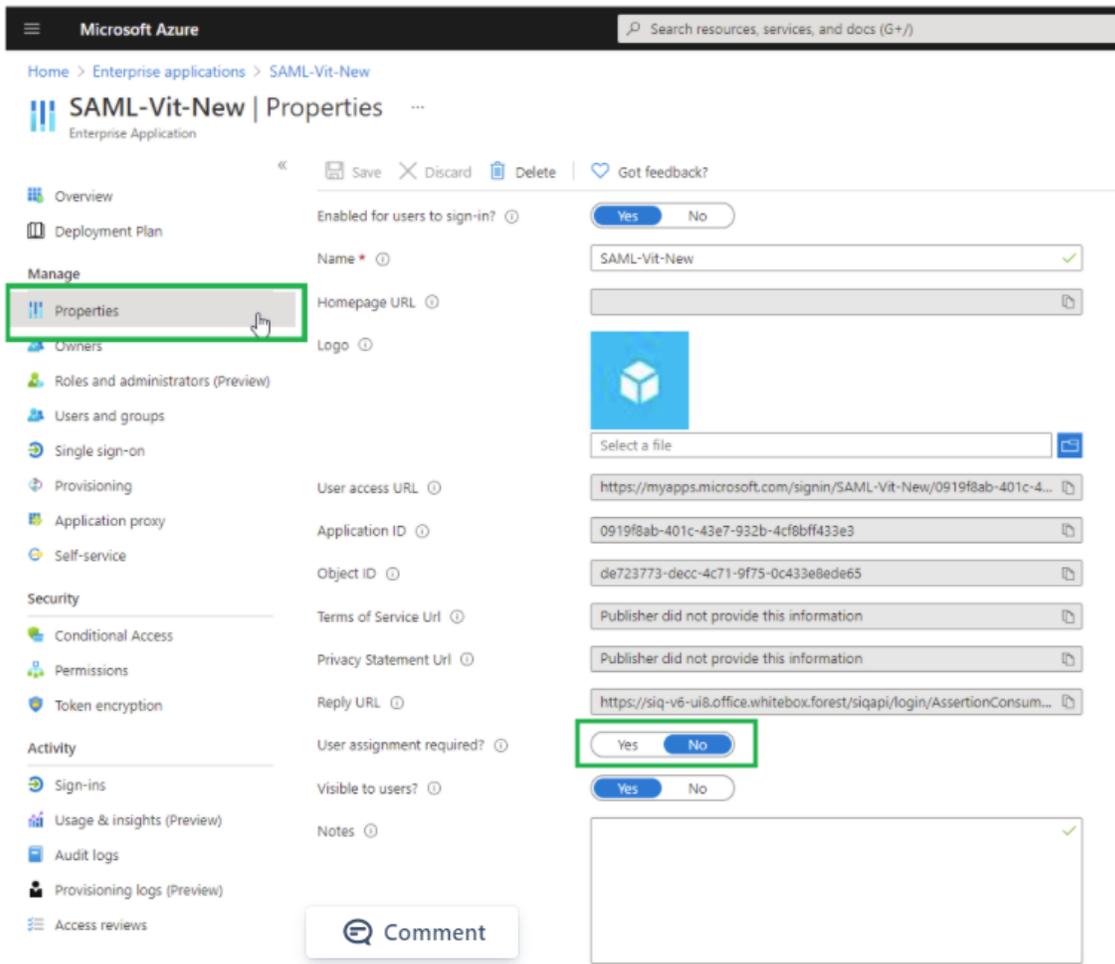
Source * Attribute Transformation

Source attribute * user.userprincipalname

Claim conditions

- d. Click **Save**.

11. Close the currently displayed window (Click on the X)
12. Click **Properties**



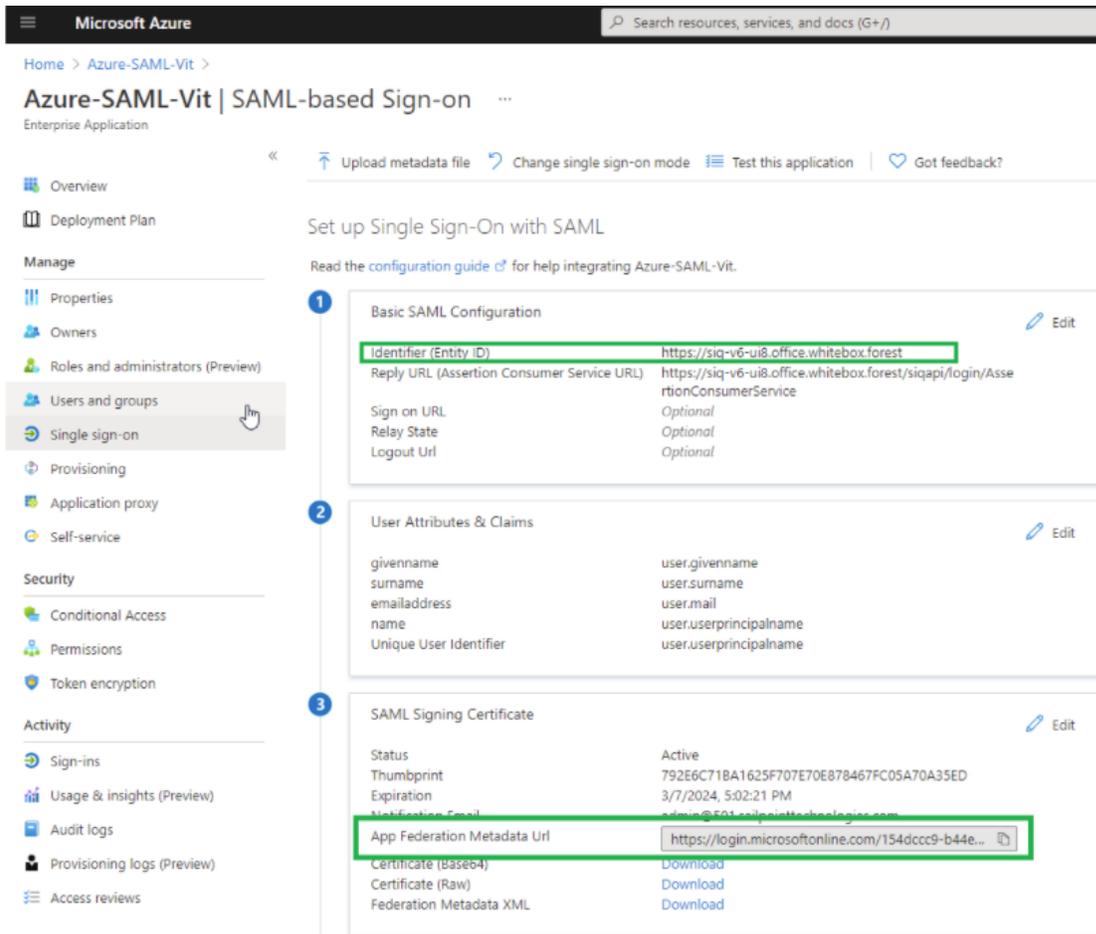
13. Verify that in the “User assignment required?” is set to **No**.

14. Click on *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 the “App Federation Metadata Url” in

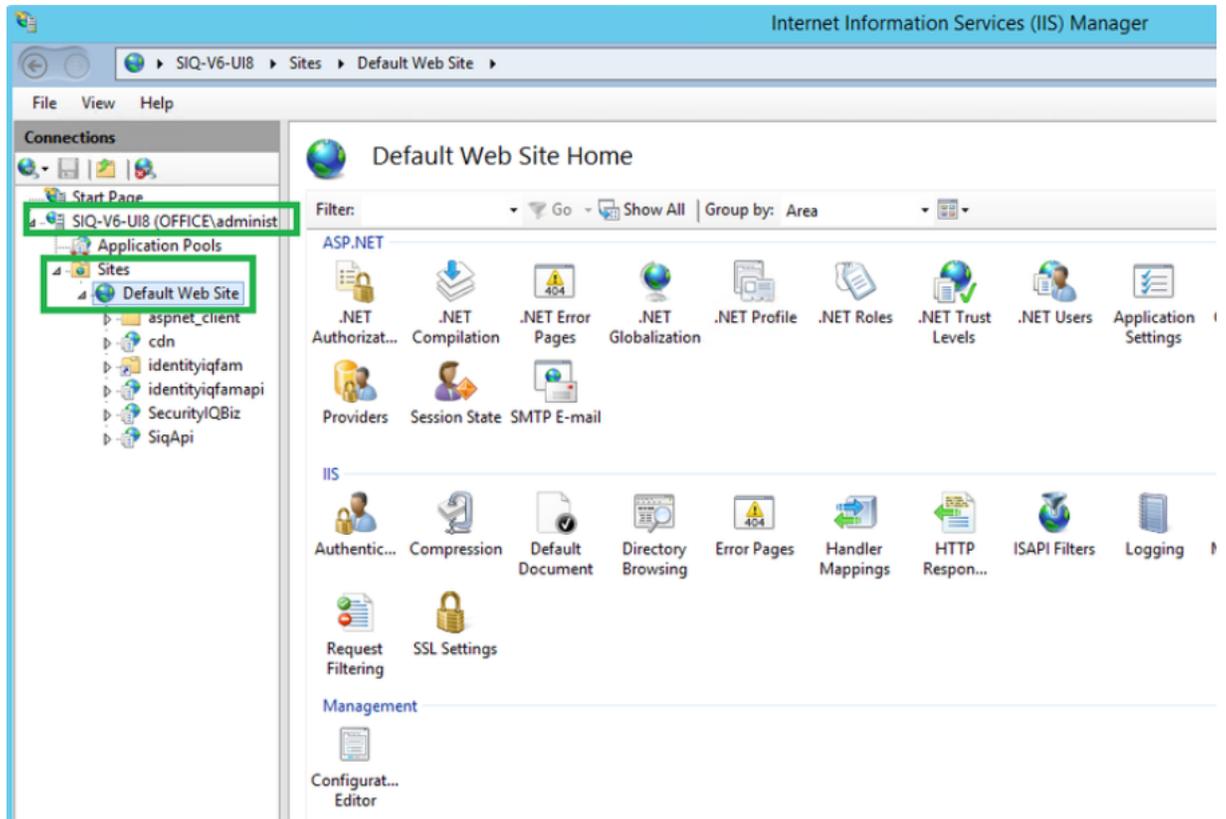
the third frame



Switching from SAML to Windows Authentication Mode

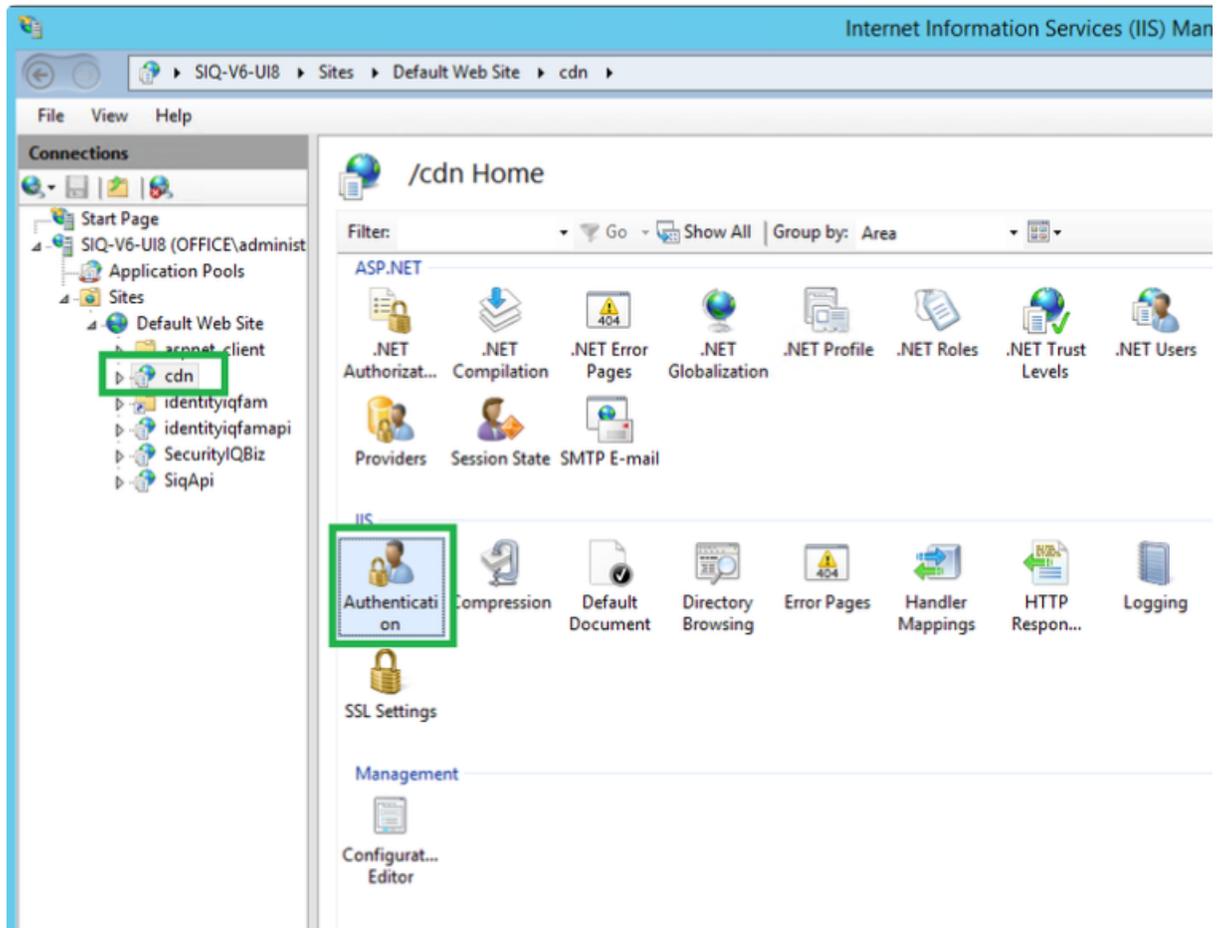
You can switch the File Access Manager authentication mode from SAML, using a local identity provider, to Windows username and password method, by changing the setup in the File Access Manager installer.

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*.

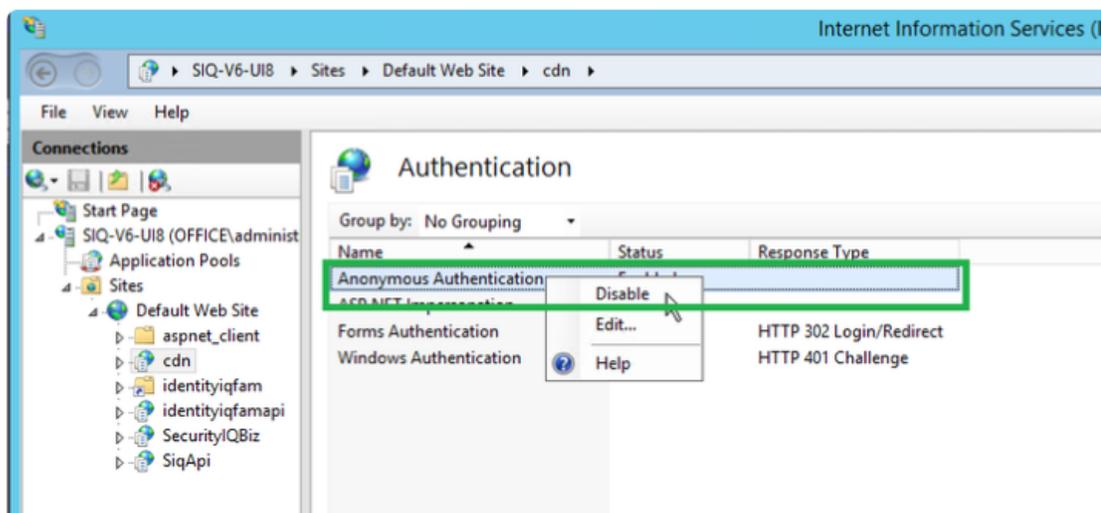


c. Click on **cdn** , then in the IIS section click **Authentication**.

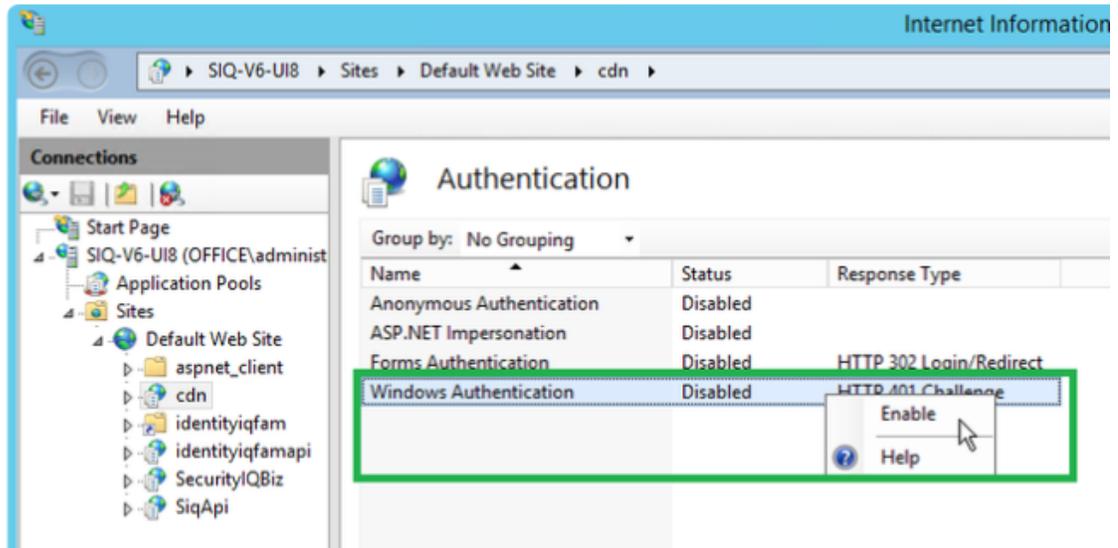
Configuring File Access Manager to use SAML Authentication



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



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



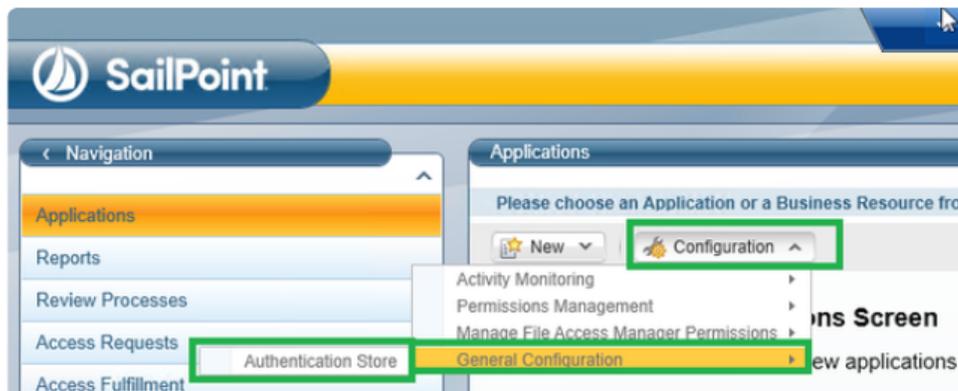
f. Repeat the steps above also for the following folders \ locations:

- 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
 - d.  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.

File Access Manager Installation

The File Access Manager installation consists of the following phases:

1. File Access Manager [Server Installer](#) installation
2. [Database creation](#)
3. [Configuration creation](#)
4. Service installation on each File Access Manager Server

Installation Log File

The installation process is logged to the installation logs. Any errors in the installation process, and references to the logs in error messages, refer to the logs in this folder (according to the installation directory):

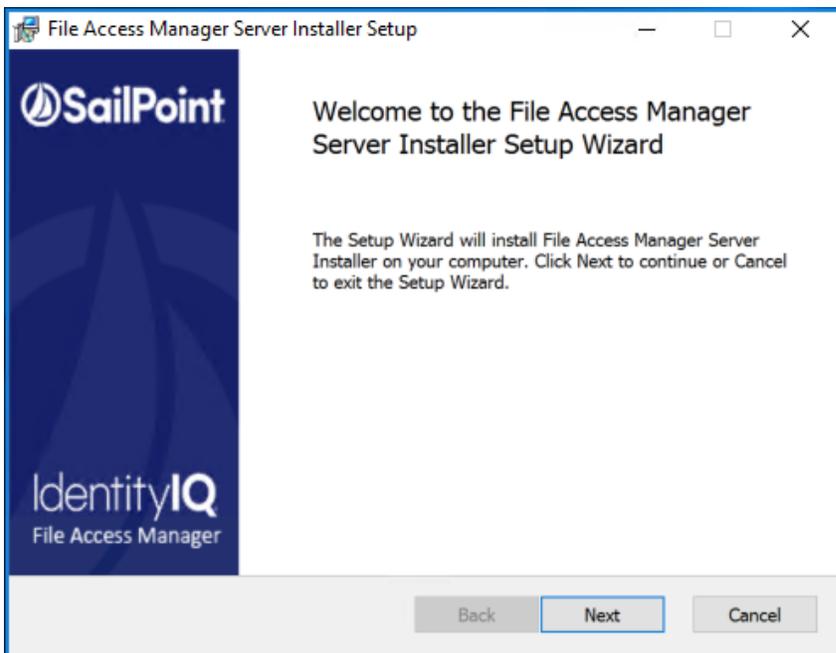
C:\Program Files\SailPoint\FileAccessManager\Server Installer\Server\Logs

Server Installer

The Server Installer manages the configuration of the File Access Manager central servers, and the installation process.

To start the Server installer:

1. Run the ServerInstaller.msi file.
The “Welcome to File Access Manager Server Installer Setup Wizard” window displays.



2. Click **Next**.
3. Select the destination folder and click **Next**.

4. Click **Install** to start the installation, or **Back** to change the installation folder.
5. After the installation processes are complete, the “Completed the File Access Manager Server Installer Setup Wizard” window displays.
6. Check the **Launch the File Access Manager server installer** check box, which launches the Install Wizard of the Server Services.

Opting for manual database creation requires the creation to be done before launching the installer.

7. Click **Finish**.
The File Access Manager Installation window displays.
8. Click **Next**

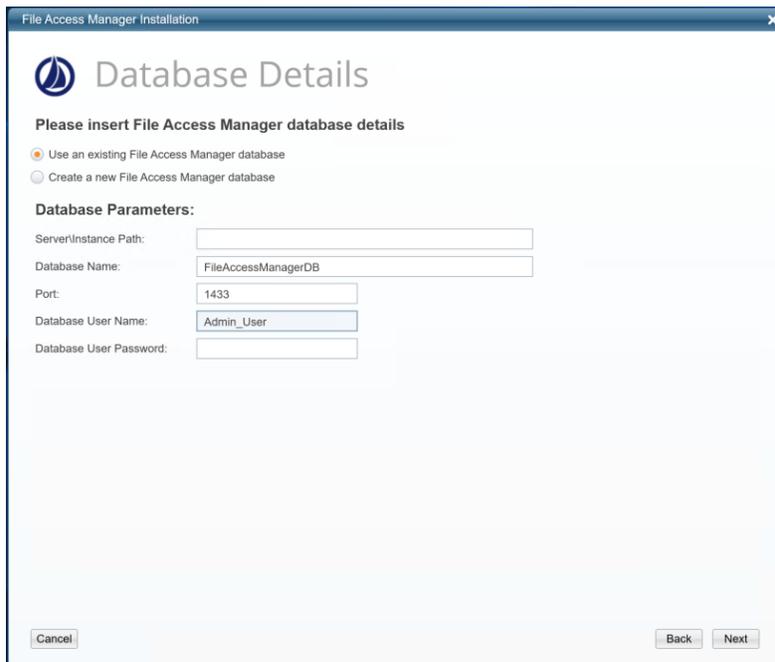
Creating a Database Using the Installer

To create the database, perform the following steps:

1. Start the installer by opening the `SailPoint\Server Installer` shortcut.

Run in Administrator mode.

2. Click **Next**.
The End User License Agreement (EULA) window displays.
3. When you have read and accepted the End User License Agreement, select the **I have read and accepted the agreement** option and click **Next**.
The Database Details window displays.



The screenshot shows the 'Database Details' window of the File Access Manager Installation wizard. The window title is 'File Access Manager Installation'. It features the SailPoint logo and the text 'Database Details'. Below this, it says 'Please insert File Access Manager database details'. There are two radio button options: 'Use an existing File Access Manager database' (which is selected) and 'Create a new File Access Manager database'. Under the heading 'Database Parameters:', there are five input fields: 'Server\Instance Path:' (empty), 'Database Name:' (containing 'FileAccessManagerDB'), 'Port:' (containing '1433'), 'Database User Name:' (containing 'Admin_User'), and 'Database User Password:' (empty). At the bottom of the window, there are three buttons: 'Cancel', 'Back', and 'Next'.

4. If you are installing File Access Manager for the first time:
 - a. Select **Create a New File Access Manager Database**.
 - b. Enter the server\instance path, database name and port number required in order to connect the database. (Write 0 for dynamic ports.)
 - c. Enter the database username and password to create.
 - d. **Import Assemblies Certificate** checkbox: Check this option if the CLR Strict Security Mode is enabled in the database. Using this option will import a certificate into the Master database. This option is relevant only for SQL Server 2017 and above.
 - e. Enter the database files path. This folder must exist on the database server
 - f. Enter the file stream files path
 - g. Enter the log files path. This folder must already exist on the database server.
 - h. Enter a password for the administrative client user and repeat the password
 - i. Select the **Authentication Type** from the SQL Server or Windows options. This is the authentication used to log in to the database for the creation of the File Access Manager database.
 - For **SQL**, type in the SA User Field and password for the system administrator.
 - For **Windows**, the Server Installer will use the logged-in user to connect to the database.
5. If you are installing additional services to an existing File Access Manager installation, select **Use an existing File Access Manager Database**.
6. Click **Next**.
The Action Select window displays.
7. Select **Create / Edit Installation Configuration** and click **Next**.

Creating the Configuration

The create / edit installation configuration will be the only option available if this is the first time running the Server Installer. After the first configuration is set, the rest of the options will be available for editing the configuration or uninstalling services.

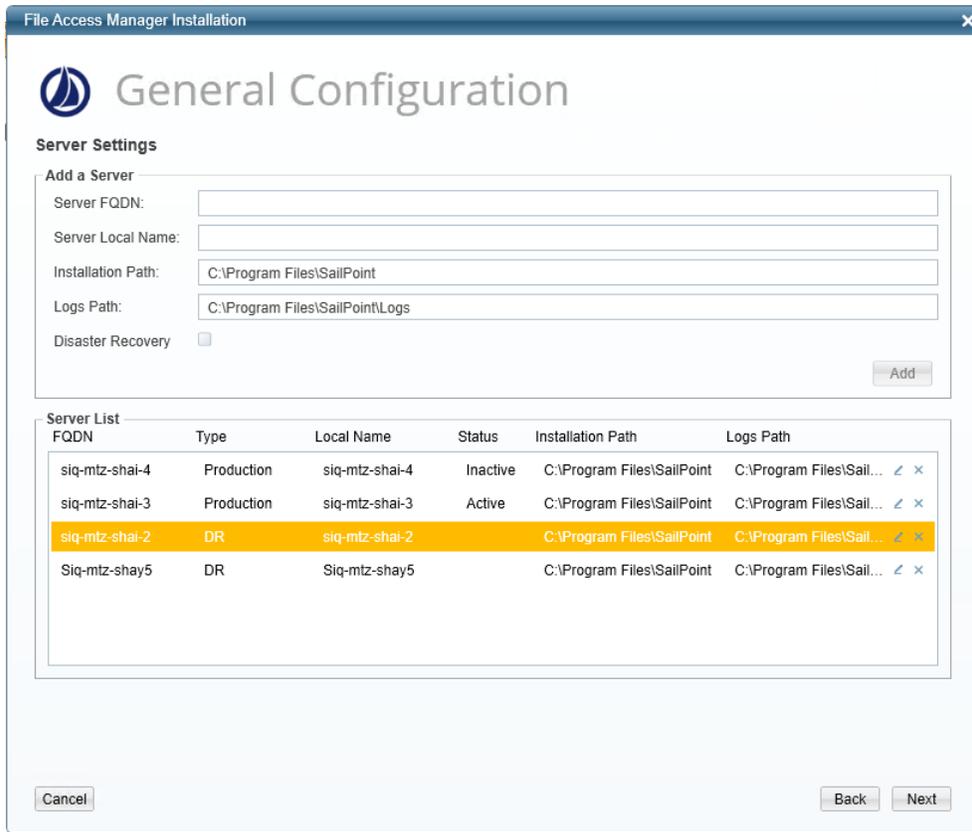
The configuration steps are:

1. Defining the servers as Production (default) or Disaster Recovery
2. Assigning File Access Manager services to Production servers
3. Assigning File Access Manager services to Disaster Recovery servers
4. Storing the installation configuration and installation commands file
5. Installing in one of two methods:
 - a. Installing on the current server using the installation GUI
 - b. Installing using the preconfigured command file

Adding a Server

To create the configuration for a new server:

1. In the General Configuration window, define all the servers on which the File Access Manager services will be installed and whether the installed server is a production server (Prod), or a disaster recovery server (DR). These servers should include DR servers, and High Availability duplicate servers, if required. This does not include the Windows file server activity monitors



2. For each server:
 - a. In the **Server FQDN** field, enter the server's Fully Qualified Domain Name (FQDN).
 - b. In the **Server Local Name** field, enter the server's short name (NetBIOS host name).
 - c. In the **Installation Path** field, enter the installation path. This becomes the SAILPOINT_HOME environment variable on the installation server. This is the path in which the **File Access Manager** services will be installed.
 - d. In the **Logs Path** field, enter the logs path. This becomes the SAILPOINT_HOME_LOGS environment variable on the installation server. This is the central folder, in which all **File Access Manager** logs will be written.
 - e. If this server is designated as a disaster recovery server, select the **Disaster Recovery** checkbox.
3. Click **Add**. The server configuration that you specified copies to the Server List.

File Access Manager services use SSL communication.

4. Click **Next**.

Disaster Recovery Configuration

You can set the servers to be inactive in the Server Installer. If a Production server is set to Inactive, the corresponding Disaster Recovery Server will be set to Active, and vice versa.

The user can set an active server to inactive from any machine.

To switch a server to Inactive:



1. Open the Server Installer and connect to an existing DB.
2. Select the server which will be inactivated, and click the **Edit** button to open the server detail panel.

File Access Manager Installation

General Configuration

Server Settings

Add a Server

Server FQDN:

Server Local Name:

Installation Path:

Logs Path:

Disaster Recovery

3. Click **Deactivate** to change the server state.
4. Click **Save**

Service Configuration

There are two Service Configuration screens: one for the Production environment, and one for the Disaster Recovery environment.

The services distribution should be planned before installation. SailPoint installation experts are available to discuss these options with you.

For each environment, this screen is used for associating services with the relevant servers defined in the “Services Configuration” window.

To configure services, perform the following steps:

1. In the **Action Select** window, select the **Create / Edit** configuration installation option.
2. Click **Next** to display the Service Configuration window.
Use the scroll bar to see all the configuration input fields.

File Access Manager Installation

Service Configuration

Select services to install, and associate them with servers

* Agent Configuration Manager	siq-mtz-shai-4	Listening Port: 8000
* Activity Analytics	siq-mtz-shai-4	Listening Port: 8010
* API	siq-mtz-shai-4	
* Business Asset Control	siq-mtz-shai-4	
* Business Website	siq-mtz-shai-4	
* Collector Synchronizer	siq-mtz-shai-4	
* Crowd Analyzer	siq-mtz-shai-4	
* Elasticsearch	siq-mtz-shai-4	<input type="checkbox"/> Define manual credentials ?
Database Path: c:\es		
* Event Manager	siq-mtz-shai-4	Listening Port: 8001 +
* Reporting Service	siq-mtz-shai-4	Listening Port: 8006
* Scheduled Task Handler	siq-mtz-shai-4	
* User Interface	siq-mtz-shai-4	Listening Port: 8005
* Workflow	siq-mtz-shai-4	Listening Port: 8008
<input checked="" type="checkbox"/> Central Data Classification	siq-mtz-shai-4	Service Name: dc +

Cancel Back Next

3. Select the server to use in the Production environment for each service. The dropdown list of available servers only includes Production servers.

When allocating services to servers, make sure any servers dedicated to high availability are not used for the first instance of any services.

Service Ports

Enter the relevant port information. Make sure to adjust firewall rules, if required.

Agent Configuration Manager

The Agent Configuration Manager service is a prerequisite for installing all other services, therefore the server configured for the Agent Configuration Manager must be installed first.

Elasticsearch

If this is the first time you are installing File Access Manager, specify the name of the server on which to install the Elasticsearch database, as well as the full database path.

An account is required to handle internal processes between the service and File Access Manager server. Credentials can be created automatically or inserted manually.

You must use this Installation wizard if you want to move the Elasticsearch database from one server to another. Contact the File Access Manager Support Center if the Elasticsearch database must be moved after installation.

RabbitMQ

File Access Manager uses an open source message broker, RabbitMQ, to distribute operations across multiple services. The File Access Manager Administrator Guide has more information on horizontal scaling in this service.

The connection between the message broker and File Access Manager services is secured with SSL.

An account is required to handle internal processes between the message broker and File Access Manager server. Credentials can be created automatically or inserted manually.

When installed in a High-availability environment, RabbitMQ is used to synchronize data between IIS servers, making sure all users see up to date data in our web site. If your installation uses more than one IIS you should make sure you install RabbitMQ.

When installing RabbitMQ, the user completing the installation must have a valid %homepath% variable. During the installation the erlang.cookie will be copied over using this variable, which will cause the failure of the installation if not set.

Event Manager

The Event Manager Service can be duplicated and installed on multiple servers.

Click the + next to the port and select the correct destination server for the newly created service.

Central Data Classification

File Access Manager allows multiple instances of installed Central Data Classification services. The Architecture section of the File Access Manager Administrator Guide has additional information on installation planning.

- Click the + next to the port to add instances.
- Click the x to remove instances.

Central Permissions Collection

File Access Manager allows multiple instances of installed Central Permissions Collection services. The Architecture section of the File Access Manager Administrator Guide has additional information on installation planning.

- Provide a unique name for each service. This name will be displayed during the Application configuration wizard when defining a new Application in the File Access Manager Administrative Client.
- Click **Next** to repeat this configuration for the Disaster Recovery environment. The list of servers in the next panel will be servers defined previously as Disaster Recovery servers.

File Access Manager supports installing a non-dedicated Permissions Collector service to handle multiple Applications on the same service. You can also install a dedicated Permissions Collector service for an Application. The Collector Installation guide has additional information.

Removing a Central Permission Collector may orphan associated collectors. Any orphaned collectors should be uninstalled through the Collector Installation Manager.

Business Website

The Business Website installs IIS if it is not yet installed.

Configuring High Availability Services

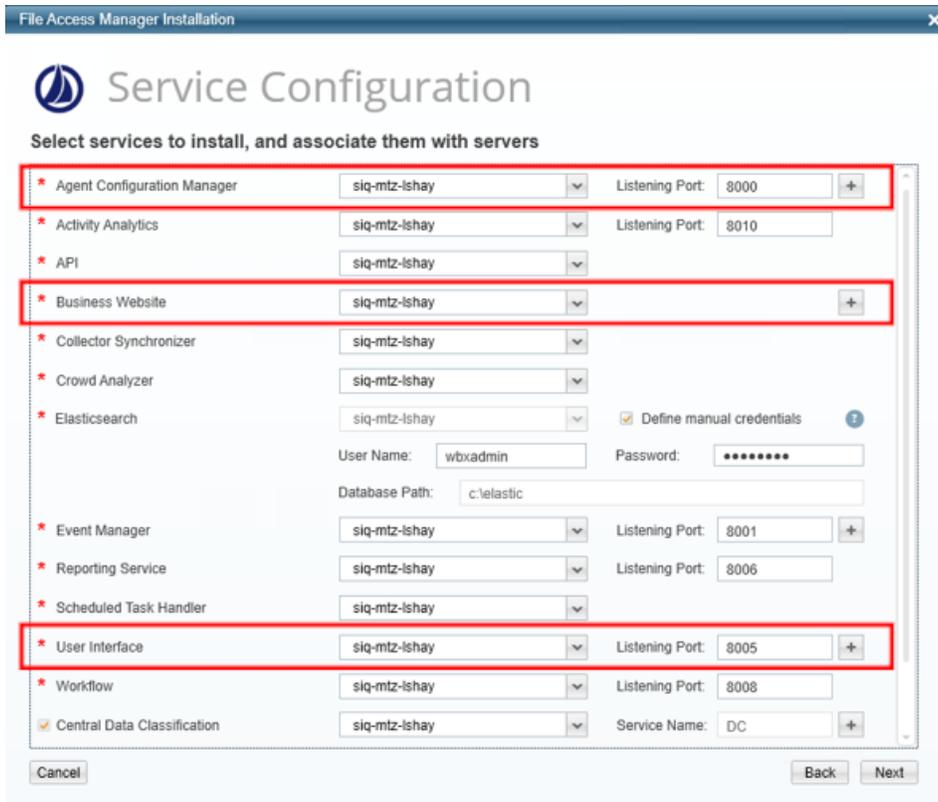
To configure High availability services:

- Add an additional instance of the service, by clicking the + icon next to the service on the configuration panel.
- Configure the installer to install the service on a parallel server allocated for high availability.
- Run your load balancer on the second server (or servers).
- Configure your load balancer to select between these instances.

The load balancer should be configured for SSL passthrough. It should not terminate the client TLS connection and create a new one between the load balancer and the server. This will cause an authentication error since each client has its own client certificate.

Duplicated Services to Allocate to a Parallel Server

Service	Listening port
Agent Configuration Manager	8000
Business Website	80 / 443
Event Manager	8001
User Interface	8005



After the Service Configuration screen, click **Next** to open the Load Balancer Configuration screen.

This screen will only be displayed if there is at least one service with multiple instances.

The Load Balancer Configuration screen lists all the services that support high availability. Services that have not been defined with multiple instances in the previous stage will be grayed out.

- Server Address: The server address of the high availability server allocated for this service.
- Port: The port should be unique

Service Group	Load Balancer Address	Port
* File Access Manager Agent Configuration Manager	siq-mtz-lshay2	7000
* File Access Manager Business Website	siq-mtz-lshay2	8080
* File Access Manager User Interface	siq-mtz-lshay2	8002
File Access Manager Event Manager	siq-mtz-lshay2	7001

Website Configuration

After configuring the services, the Web configuration screen will display.

Configure IIS settings

Use this setting to configure the File Access Manager Site's IIS name, Root Directory location and Listening Port. These are system-wide settings and will apply to all deployed instances of the File Access Manager Business Website and the SCIM API. You can edit these settings as long as no instances are installed. To edit these settings once components are already installed, please uninstall all Business Website and SCIM API instances.

Site Name: Listening Port:

Root directory path:

Select web authentication mode

Windows

Saml 2.0

IIS Settings

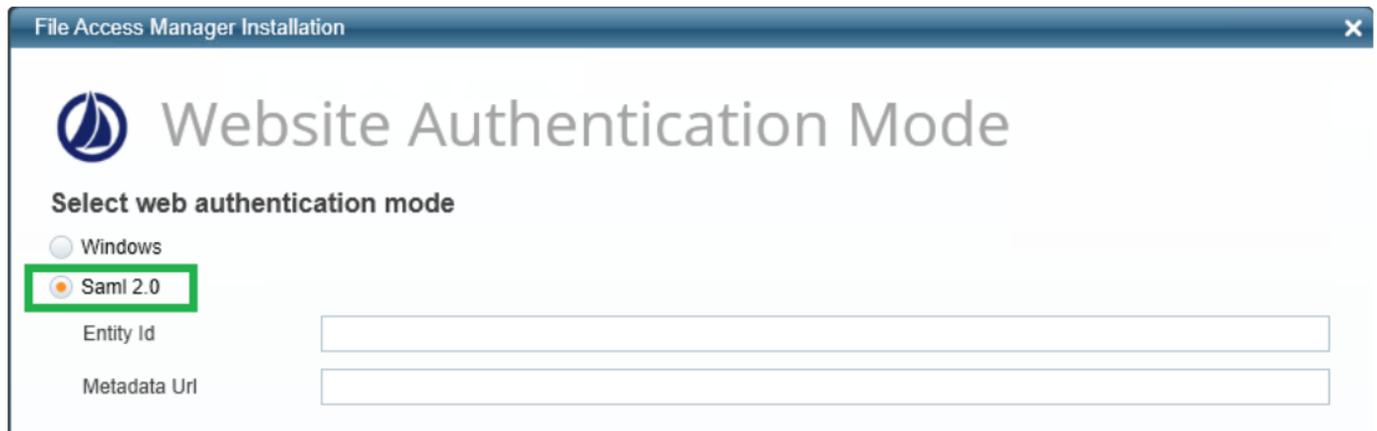
These settings allow for a non default IIS installation.

Change the site name and physical path. File Access Manager will install its websites on the specified location.

Both site name and directory path must be changed for a non-default install.

Website Authentication Mode

Now you can decide the type of authentication mode.



The screenshot shows a window titled "File Access Manager Installation" with a close button in the top right corner. The main heading is "Website Authentication Mode" next to a logo. Below this is the instruction "Select web authentication mode". There are two radio button options: "Windows" (unselected) and "Saml 2.0" (selected and highlighted with a green box). Underneath, there are two text input fields: "Entity Id" and "Metadata Url".

Windows

Using an Active Directory identity store

SAML 2.0

Using a 3rd party authentication store, such as Okta, ADFS or Azure.

See [SAML Authentication](#)

Selecting SAML 2.0 on the Website Authentication Mode opens the SSO provider identification fields

- **Entity ID**

The application name of the relevant SSO provider

- **Metadata URL**

the URL to the relevant SSO provider

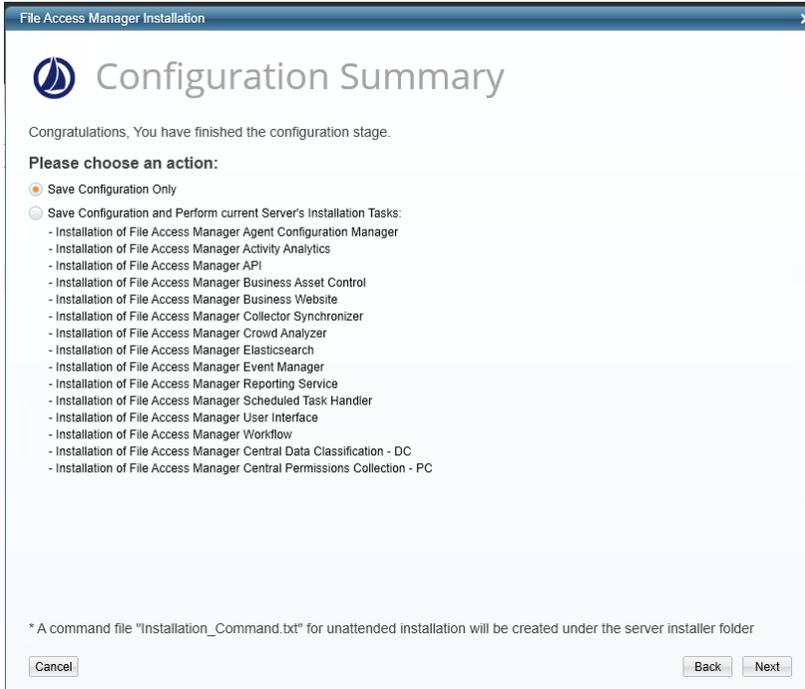
These fields are defined when creating an application in the relevant SSO provider. If you haven't created them yet, see the relevant section below

- [Creating an ADFS Application](#)
- [Creating an Azure Application](#)
- [Creating an Okta Application](#)

Continue with the installation , without creating an authentication store.

Service Configuration Summary

1. In the **Action Select** window, select the **Configuration Summary** option.
2. Click **Next**.
The Configuration Summary window displays.



Storing the Configuration

The installation process using the server installer creates a text file containing the commands for installation of the services on any server defined in the configuration.

The configuration itself is stored in the database.

Depending on the method of installation, select the next action. (See [Performing the Installation](#)

- Select **Save Configuration Only** to save the configuration without installing on this server
- Select **Save Configuration and Perform current Server's Installation Tasks** option to start the installation of the services on the current server.

Click **Next** to install the services on the current server.

If the services installed require a system restart, the installer will open a popup message requesting a restart. Following the restart, run the installer again to continue the installation process.

Performing the Installation

You can install using either the Server Installer or unattended installation, mostly for a installing a system with many servers.

Installation Using the Server Installer

Some notes to consider when installing:

- The installation process runs service installers in groups.
 - When a service starts the installation process, it is listed on the installation window.
 - When a service is installed correctly, the application adds a checkmark next to the service name, and a comment "Action succeeded".
 - If an installation of a service fails, the application adds a warning symbol on the installation line. Check the log file for further details and analysis.
1. Open the Server Installer if it is not already open.
 2. If you changed the configuration with the Server Installer, select **Save Configuration and Perform current Server's Installation Tasks** to start the installation.
 3. If you are using an existing configuration, select **Perform Current Server's Installation tasks** to start the configured installation tasks for this server.
 4. When the progress bar shows "Finished", click **Next**.
The Installation Summary window displays.
 5. Check the **Open Installation Log** check box and click Finish.
The Installation log displays.
 6. Verify that no errors occurred during the install progress by searching the log for the word ERROR (note the capital letters).

Unattended Installation

The installation configuration process stores the configuration in the database, and creates a file with the commands for installation of the services in the required servers.

These commands can be configured to fit the installation on multiple servers using a distribution tool.

The script is described below.

- File name: `Installation_Command.txt`
- File path: Server installer folder (C:\Program Files\SailPoint\FileAccessManager\Server Installer\Server)

Installation Command Script

The installation command file contains three commands:

- Install the server installer
- Install the services required for the current server
- Return the last error code

Install the Server Installer

This is an msi installation file that installs the server installer on this server.

Command:

File Access Manager Installation

```
start /wait msixec /i "[INSTALLER_PATH]\ServerInstaller.msi" /l*v "C:\FAMIn-  
staller.log" /quiet /norestart TARGETDIR="[TARGETDIR]"
```

Parameters:

INSTALLER_PATH: The path of the msi file

TARGETDIR: Target directory of the application. E.g. : c:\Program Files\SailPoint\

Run the Unattended Installer with Database Connection Parameters

The script is created without the password. You will have to add it in to the command when you copy it across.

Command:

```
start /wait /d "[TARGETDIR]\FileAccessManager\Server Installer\Server" Unat-  
tendedInstaller.exe --server "database server name" --database "Database name" --  
port "1433" --user "database user" --password "[PASSWORD]"
```

Parameters:

TARGETDIR: This should be identical to the targetdir of the previous command
server - database server name

port: database server port number

database: database name

user: database user name

password: database password

Return the last resulting error code

0 – successful installation

For further details, check the installation log in C:\Program Files\SailPoint\FileAccessManager\Server Installer-
\Server\Logs

File Access Manager identifies which installation tasks are meant for this server, according to the con-
figuration.

Error codes:

Code	Description
0	Success
1	Unknown error
2	Unable to perform prerequisites
3	Error in verifying the installation
4	Some services failed to install
5	There is a pending reboot on this machine. Please

Code	Description
	reboot and re-run the File Access Manager Server Installer
6	Bad arguments were passed to executable
7	Database version not compatible with server installer version
8	Database connection failed
9	Server address resolution failed

Service Migration

This section relates to moving installed services from their original server and installing them on another server.

To migrate services, follow the instructions for each service on the server where the service to be migrated is installed:

You cannot use the Installation Wizard to move the Elasticsearch database from one server to another. For help with moving the Elasticsearch database, contact the File Access Manager Support Center.

Source Server – Database Connection

To connect to an existing database:

1. Start the installer in `C:\Program Files\SailPoint\FileAccessManager\Server Installer-\Server\ServerInstaller`
 - Run in Administrator mode.
2. Click **Next**.
The End User License Agreement (EULA) window displays.
3. When you have read and accepted the End User License Agreement, select the **I have read and accepted the agreement** option and click **Next**.
The Database Details window displays with the database connection details and the Database User Password filled out.
4. In the *Database User Password* field, enter the database user password.
5. Click **Next**.

Source Server – Configuration Modification

A service migration requires configuring another server to migrate to.

To modify the configuration:

1. In the Action Select window, select the **Create/Edit installation configuration** option.
2. Click **Next**.
The General Configuration window displays.
3. Add new servers if necessary, as described in the section [Adding a Server](#).
4. The General Configuration window displays.
5. Click **Next**
6. Change the server of each of the services to be migrated as described in [Service Configuration](#).
The Service Configuration window displays.
7. Click **Next** to open the Configuration Summary window

Source Server – Configuration Summary

1. Select the “**Save Configuration and Perform current Server’s Installation Tasks**” option.
2. Click **Next** to uninstall the services to begin migration from the current server.

Source Server – Uninstallation Process

- The uninstallation process uninstalls services on this server in groups.
 - When a service starts the uninstall process, it is listed on the uninstall window.
 - When a service is uninstalled, the application adds a checkmark next to the service name, and a comment "Action succeeded".
1. When the progress bar shows **Finished**, click **Next**.
The Installation Summary window displays.
 2. Check the **Open Installation Log** check box and click **Finish**.
The Installation log displays automatically.
 3. Verify that no errors occurred during the uninstall progress by searching the log for the word `ERROR` (note the capital letters).

Target Server – Database Connection

1. Connect to the database on the server that will host the migrating service(s) and run the Server Installer.
2. Follow the instructions in [Source Server – Database Connection](#).
3. Click **Next**

Target Server – Install Migrating Service(s)

To modify the configuration, perform the following steps:

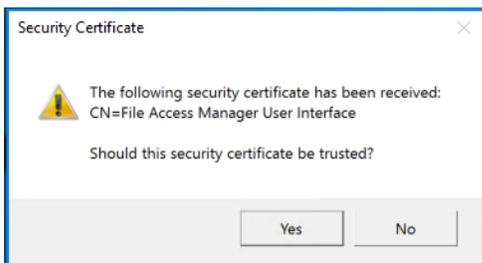
1. In the “Action Select” window, select the Perform current server’s installation tasks configuration option.
2. Click **Next**.
The “Configuration Summary” window displays, listing the services to be installed.
3. Proceed with the installation by following the instructions at [Preparing for Installation](#).

Administrative Client Installation

The administrative Client can be installed locally on one of the File Access Manager servers, or on any remote station with access to the User Interface service.

To run the Administrative Client installation, perform the following steps:

1. Open the Administrative Client Installation folder. This is in the File Access Manager distribution package
2. Run ClientInstaller_x64.msi.
The Welcome to the File Access Manager administrative client Setup Wizard screen displays.
3. Click **Next** to open the “Connection Properties” window
4. In the *UI Server* field, enter the FQDN of the server that hosts the User Interface service.
5. In the *Service Port* field, enter the relevant port.
The default port is 8005.
6. Click **Next** to open the “Destination Folder” window.
7. Enter the destination folder where you want to install the Administrative Client binaries.
8. Click **Next** to open the “Ready to install File Access Manager administrative client” window.
9. Click **Install to start the installation process.**
10. **Once the installation completes, a confirmation message will appear on the screen.**
11. Check the “Launch File Access Manager Client” check box to open the Administrative Client.
12. The first time you open the File Access Manager administrative client, you will see the following notification to confirm that the SSL certificate has been applied.



13. Click **Yes** if the certificate should be trusted.
The File Access Manager Administrator Guide has additional information on changing the File Access Manager security certificate.
14. Click **Finish**.
15. The SailPoint File Access Manager logon window displays.
16. When logging into the File Access Manager administrative client for the first time, use the following database user and the password entered in for the administrative client:
User: wbxadmin
17. After you have logged in successfully, follow the instructions to change the admin password.
The File Access Manager Administrator Guide has additional information on managing users.

File Access Manager Website SSL

The File Access Manager website is not affected by general SSL settings.

Setting the File Access Manager website to use SSL is not required, but is recommended.

To use SSL for Website communications, perform the following steps:

1. Install a certificate on the same server as the File Access Manager page (preferably with the same certificate criteria described above).
2. Open Internet Information Services Manager (inetmgr).
3. Navigate to the Default Web Site, and click “Bindings” on the panel to the right.
4. Click **Add**
5. Select HTTPS on the Type dropdown menu.
6. Select **Select** on the SSL Certificate dropdown menu to use a trusted certificate, preferably one from your organization.
7. Click **OK**
8. Click **Close**
9. A manual update must be made in the DB to reflect the web site URL (Check for fields with the URL in it for the SQL below):

```
update [whiteops].[system_configuration_value] set [value] = replace
([value], 'http', 'https') where [name]='Web Site URL'
```

10. Set the "requireSSL" flag and SSL port in the configuration file.

File: C:\inetpub\wwwroot\siqApi\SiqApi.dll.config

```
<add key="requireSSL" value="true" />
```

true

require SSL

false

regular http protocol

```
<add key="sslPort" value="443" />
```

ssl port

Change this value if you want to change the default

11. When securing cookies, ensure the following is in each web.config file for v1, v2, and siqapi.

```
<httpCookies httpOnlyCookies="true" requireSSL="true" />
```

The web.config files are located at:

```
V1 - "{website root folder}\identityiqfam\v1\web.config"
V2 - "{website root folder}\identityiqfam\v2\web.config"
```

SiqApi - "{website root folder} \siqApi\web.config"

The default installation path for File Access Manager IIS application is "C:\inetpub\wwwroot"

To make browsing to the page using HTTPS mandatory, perform the following steps:

1. Double click on SSL Settings while on the Default Website.
2. Click **Require SSL**.
3. Leave "**Ignore**" on Client Certificates.
4. Click **Apply**.

Recommended Secured Deployment

File Access Manager uses self signed certificates, and SSL for internal communication.

If you require a higher security configuration, follow these configuration guidelines:

- [Required Environment](#)
- [Installation Considerations and Constraints](#)
- [Post Installation Configuration](#)
- [Configuring the Process Exploit Mitigation for File Access Manager Services](#)
- [Enabling New Version Notifications](#)

Required Environment

Windows operating system version:

File Access Manager must be installed on a Windows Server 2019 Datacenter edition, version 1809.

File Access Manager version:

For a secured deployment use File Access Manager version 8.1.0.1 or higher.

Installation Considerations and Constraints

- File Access Manager should be installed in the default directories (e.g. C:\Program Files\SailPoint). These include:
 - Server Installer
 - All Services (Core and Collectors)
 - Administrative Client
- The File Access Manager database should be created on an SQL Server that is setup with a certificate and enforces encryption.

Post Installation Configuration

Complete the following:

1. Replace all File Access Manager self-signed certificates with trusted certificates that you must provide. See section [Configuring File Access Manager to Use Local Certificates](#).
2. Setup the recommended Process Exploit Mitigation for File Access Manager services (Windows Defender settings). See [Configuring the Process Exploit Mitigation for File Access Manager Services](#)
3. Change the IIS (on which our web components are installed on) settings to require SSL. See [File Access Manager Website SSL](#)
4. Set all Active Directory connections to use LDAPS (Identity Collectors / Data Enrichment Connectors).
5. Enable the File Access Manager New Version Notifications feature (See section [Enabling New Version Noti-](#)

fications)

- For all these steps to take effect, restart all the services, or restart the server.

Configuring the Process Exploit Mitigation for File Access Manager Services

Part of the higher security settings involve configuring the Process Exploit Mitigation settings in Windows Defender for the File Access Manager Services, with the following settings enabled:

Component	Setting	Location
Control Flow Guard (CFG)	on (default)	System setting
DEP	on (default)	System setting
Randomize memory allocations (Bottom-Up ASLR)	on (default)	System setting
Export Address Filtering (EAF)	on (This requires manual configuration per service)	Program settings
Import Address Filtering (IAF)	on (This requires manual configuration per service)	Program settings

The *system settings* should be kept in the default values. Please verify that these settings above are in fact set in the Windows Exploit Protection Settings under the system tab.

The *program settings* can be updated using a script which is part of the File Access Manager deployment package, or manually in the Process Exploit Mitigation tool. Both methods are described below,

Configuring the Program Settings Using *FAM.Exploit.protection.Settings.xml* Script

You can enable the recommended security settings for File Access Manager using the file **FAM.Exploit.protection.Settings.xml** from in the installation folder.

To apply the settings, run the command below in an elevated PowerShell window:

```
Set-ProcessMitigation -PolicyFilePath "Full path to FAM.Exploit.protection.Settings.xml "
```

This script lists the File Access Manager to update, and configures the permissions per service.

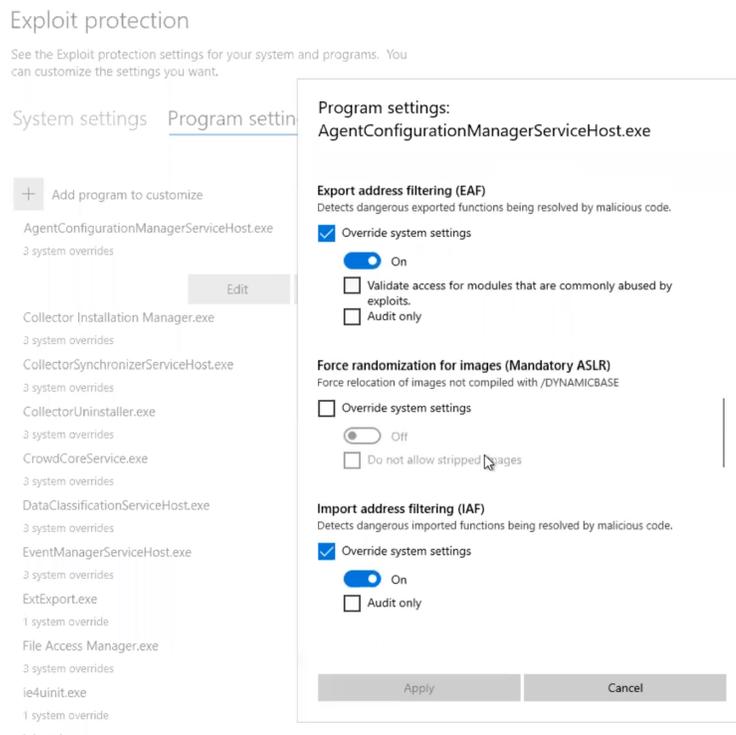
For these settings to take effect, the services have to be restarted.

Configuring the Program Settings Using the Windows Defender Settings Tool

If you can't run the script described above, or want to see what's happening under the hood - the recommended security settings for File Access Manager can be changed manually in the Windows Defender Settings tool, as described below:

- On the Windows server, open the *Windows Defender Settings*
- Click **App & Browser Control**
- Click **Exploit Protection Settings**
- Click **Program Settings** tab

5. For each of the File Access Manager services:
 - a. Click **+ Add program to customize** to open the parameters panel.
 - b. Set the **EAF** and **IAF** to *on*.



6. Click **Apply** to save the changes.
7. Restart all the services modified, or reboot the server.

Enabling New Version Notifications

SailPoint publishes updates to the File Access Manager from time to time, as new releases, minor releases, and software patches.

When updates are available, the application can send an email to the File Access Manager administrator to notify you of the update. This feature is disabled by default.

To enable this feature:

1. Update the database with the email address which the notification mail will be sent to, by running the following update statement:


```
update [whiteops].[system_configuration_value] set [value] = N'[ENTER DESIRED eMAIL HERE]' where [name] = N'New Version Message To'
```
2. From the *"Scheduled Task Handler"* service server, edit the file `%SAILPOINT_HOME%\FileAccessManager\ScheduledTaskHandler\ScheduledTaskHandlerServiceHost.exe.config`.

3. In the **appSettings** section, change the `newVersionCheckIntervalInMinutes`, from -1 (which means, do not check for new versions) to a desired check interval (in minutes). Save the file and close it.
4. Restart the "Scheduled Task Handler" service.

After the service restart, an email will be sent to this address when a newer version is available for download from on Compass.

Removing Unnecessary Banner Information on Web Responses

Microsoft's Internet Information Server (IIS) includes a header with every response that includes the originating server and webserver version.

To remove this information, you should configure the IIS to remove the 'Server' header. The method depends on the installed IIS version, as described below:

For IIS before version 10:

In Windows IIS Manager, you can use the URL Rewrite module to create a rule to rewrite all outgoing messages, replacing the server value in the header with an empty string. A detailed description can be found on MS IIS Support blog below, in the third method "**3. Using URLRewrite**":

<https://techcommunity.microsoft.com/t5/iis-support-blog/remove-unwanted-http-response-headers/ba-p/369710>

For IIS version above 10

Update the SiqWeb web.config file

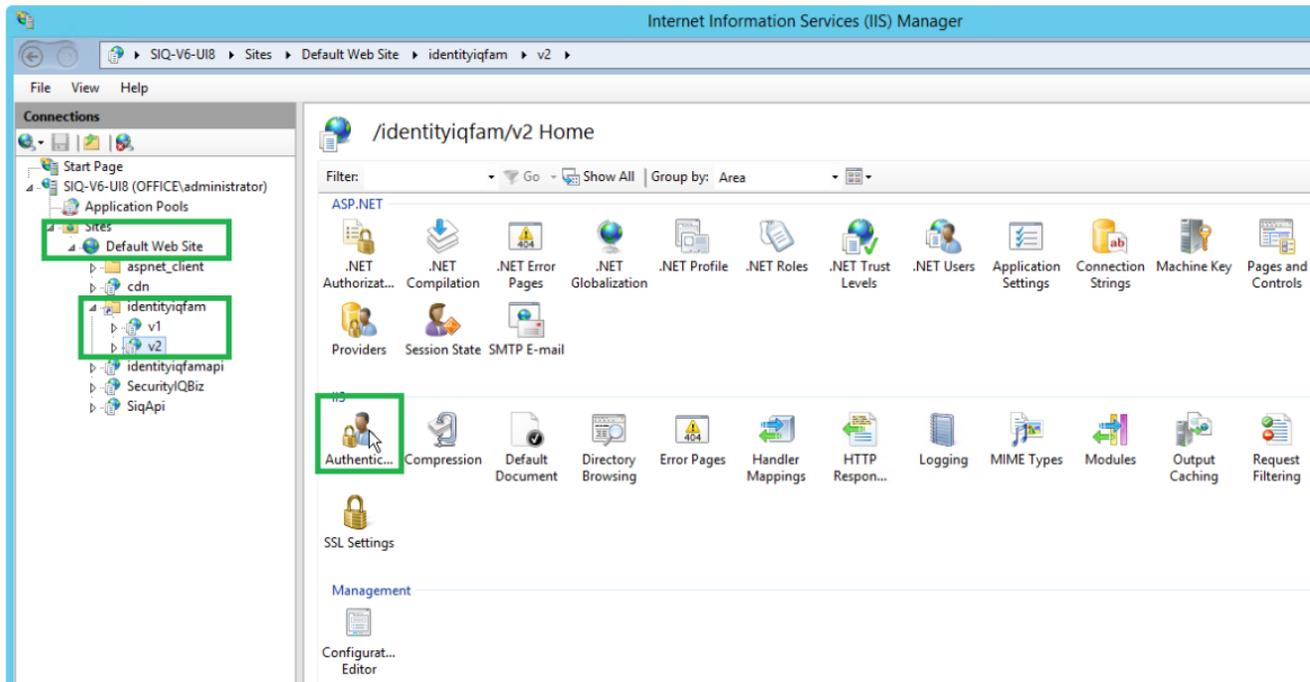
C:\inetpub\wwwroot\siqApi\web.config

```
<?xml version="1.0" encoding="UTF-8"?>
<configuration>
  <system.webServer>
    <security>
      <requestFiltering removeServerHeader="true" />
    </security>
  </system.webServer>
</configuration>
```

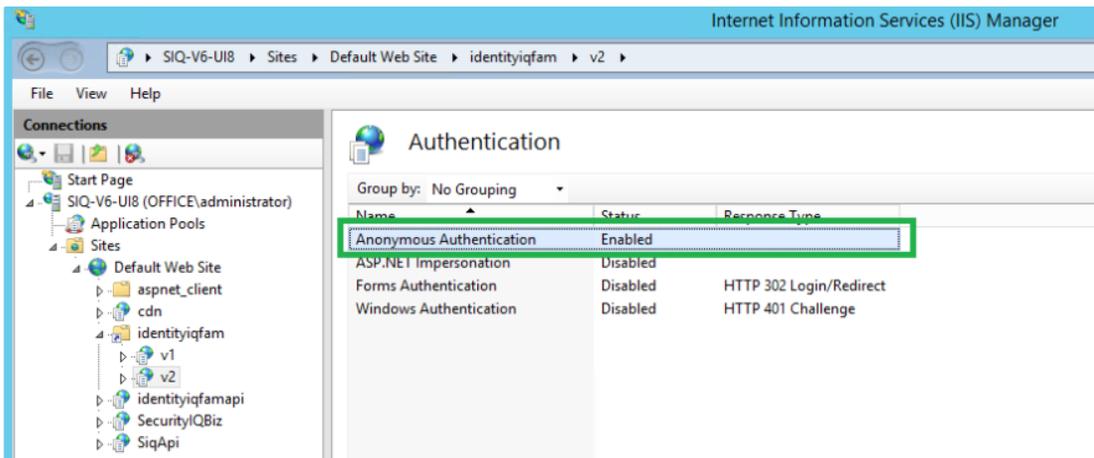
System Settings Required to Support SSO

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 *The server > Sites > Default Web Sites > identityiqfam > v1\v2 > Authentication*



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



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.

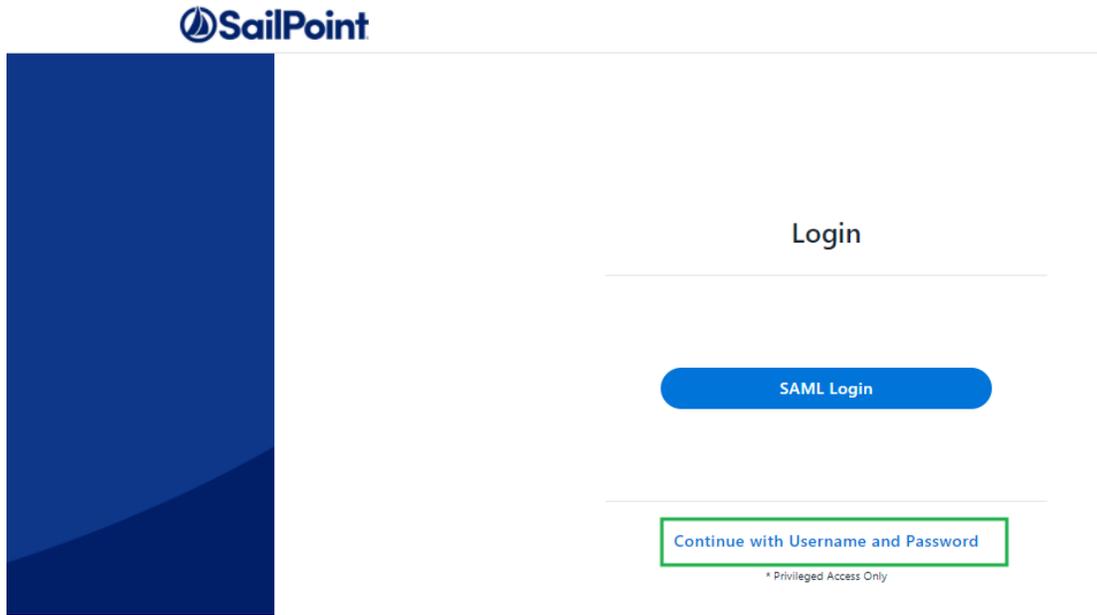
(First time login to File Access Manager using wbxadmin credentials)

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

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.

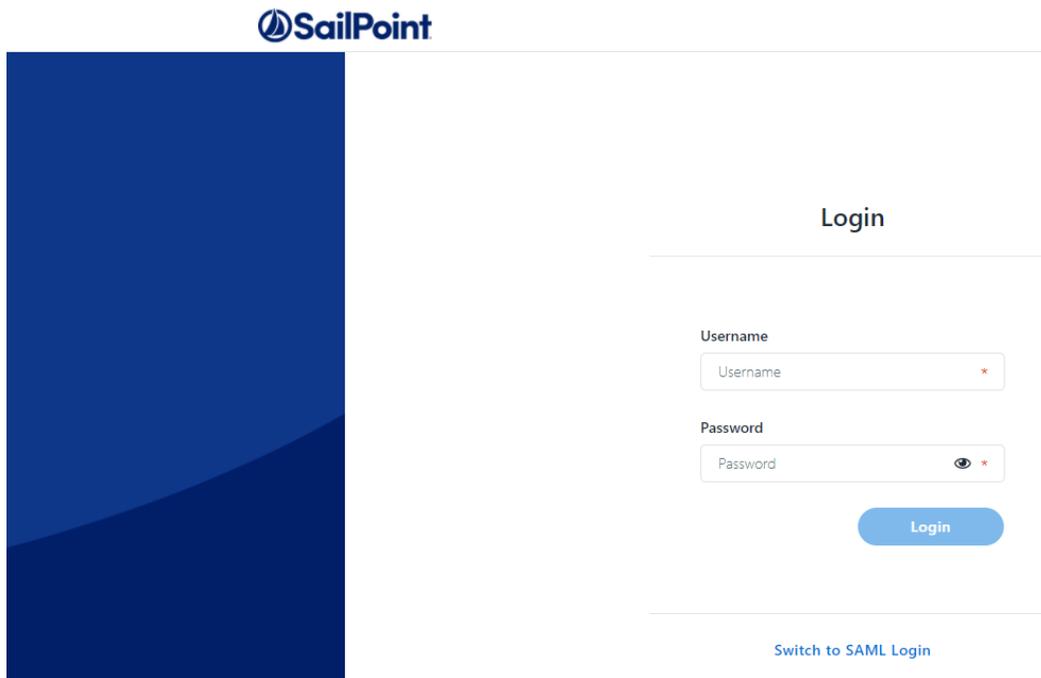
e.g.: If you use HTTPS connection, the Login link and redirect URL in Okta should both be HTTPS.

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

Click **Login**.

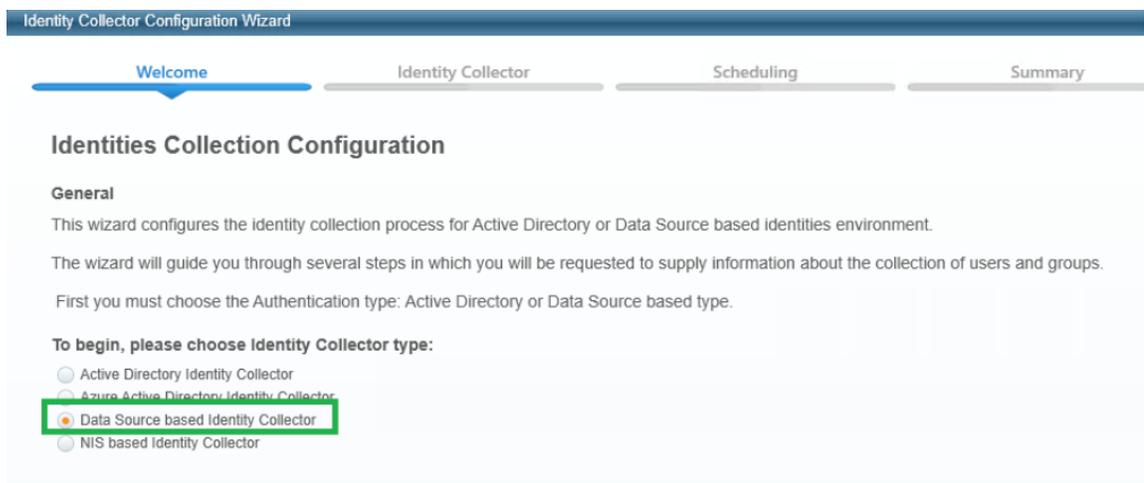


- c. Within the website navigate to *Admin > Data Sources > Add New Data Source*
- d. Create a new data source that contains a list of Okta Users you want to access File Access Manager.

- 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"

Click **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

The screenshot shows the 'Identity Collector Configuration Wizard' window, specifically the 'Identity Collector' step. The wizard has four tabs: 'Welcome', 'Identity Collector', 'Scheduling', and 'Summary'. The current step is 'Identity Collector: Users Collection (1 of 3)'. Under 'Fixed Fields Mapping', the 'Main Data Source' is set to 'OktaUsers'. In the 'Mandatory Fields' section, 'Username' is set to 'User Principal Name'. In the 'Optional Fixed Fields' section, 'User Principal Name' is checked and set to 'User Principal Name'. Other optional fields are unchecked. At the bottom, there are 'Cancel', 'Back', 'Finish', and 'Next' buttons.

Click **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.

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 the *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

Creating or Editing an Active Directory Identity Collector

To create or edit an Active Directory Identity Collector:

1. Open the Identity Collectors panel by navigating to **Applications > Configuration > Permissions Management > Identity Collectors**.
2. Click **New** to open the Identity Collector Configuration Wizard .

Identity Collector Configuration Welcome panel

1. Select an Identity Collector type from one of the following:
 - Active Directory Identity Collector
 - Azure Active Directory Identity Collector
 - Data Source-based Identity Collector
 - NIS-based Identity Collector
2. Click **Next**.

The Identities Collection window displays.

Identity Collector Configuration Identity Collector panel

The Identity Collector is responsible for collecting information about users and groups and the relationships between them. If required, you can map collected fields to data dictionary fields (for users and groups).

1. Type the name of the Identity Collector in the Name field.
2. Click **Enable Access Fulfillment for this Identity Collector** to enable access fulfillment for this Identity Collector.

You can only enable access fulfillment for Active Directory identity collectors. If you enable access fulfillment, the system can add and remove users from groups in this identity collector.

3. Click **Next**.

The Active Directory Identity Collector Users Collection (1 of 5) window displays.

4. Click **DEC** to fill the Identity Collector with pre-configured data in DEC or click **By Properties** to select a property manually from a list of defined properties.
 - a. If you selected **DEC**, select the relevant DEC from the dropdown list, and click **Next**.

If you configured DEC to connect to Active Directory, you can re-use that configuration here.

5. If you click **By Properties**, type the following data in the relevant fields:

Domain NetBios

Domain NetBios name

Port

The port number must be 389, or 636 if SSL is enabled

6. Check the **SSL**, **Server Bind**, and **Base DN** check boxes, as required.
7. By default, File Access Manager retrieves several properties from Active Directory, such as Department, Email, and Display Name. Check the **Properties to Fetch** check box, and type the relevant properties to retrieve.

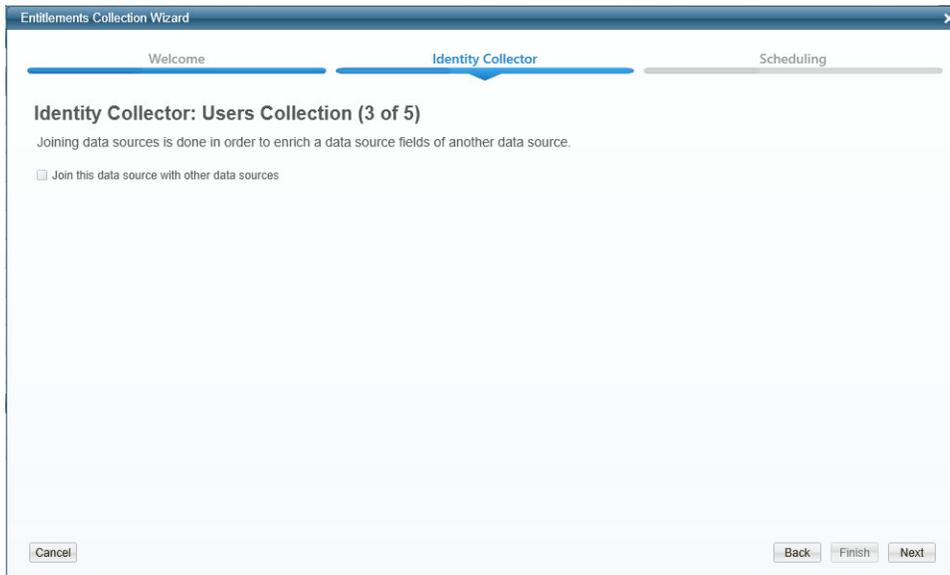
The properties you retrieve come from the Active Directory, and will be available later for mapping to the Data Dictionary fields.

8. Click **Next** to open the **Identity Collector: Users Collection (2 of 5)** window.
9. Verify that the system retrieved the requested information successfully.

Only the first ten results display.

10. Click **Next**.

The Identity Collector: Users Collection (3 of 5) window displays:



11. Data sources are created that contain user fields so that the Identity Collector can collect the Users.
12. Check the **Join this data source with other data sources** check box to join this data source to other data sources.
13. You can use one of the Identity Collector fields as the local key to gather additional user fields from other data sources by joining those data sources. Chapter contains additional information on joining data sources.
14. Type the relevant Data Source, Local Key, and Remote Key.

After you type the relevant data, click Test Data Sources to verify that the system has accepted the data.

15. Click **Next**.

The Identity Collector: Users Collection (4 of 5)/ Dynamic Fields window displays.

16. Type the Dynamic Fields Mapping data from the **Dictionary Field** and **Mapped Field** dropdown lists.

When integrating with AWS, ADDomain has to be selected for the first Dictionary Field.

Use the **X** / **+** buttons to remove / add fields, as required.

17. Click **Next**.

The Identity Collector: Users Collection (5 of 5)/Hierarchy and Authentication Users Mapping window displays:

The screenshot shows the 'Entitlements Collection Wizard' window, specifically the 'Identity Collector' step. The window has a title bar with a close button. Below the title bar is a progress indicator with three steps: 'Welcome', 'Identity Collector' (which is highlighted), and 'Scheduling'. The main content area is titled 'Identity Collector: Users Collection (5 of 5)'. Underneath, it says 'Hierarchy and Authentication Users Mapping'. There are two sections: 'Users Tree' and 'Unique User Accounts Mapping'. In the 'Users Tree' section, there is a checked checkbox 'Should the users tree be grouped?'. Below it are two radio buttons: 'Use the domain Organizational Units structure' (which is selected) and 'Group by a field'. A 'Field:' dropdown menu is present below the radio buttons. In the 'Unique User Accounts Mapping' section, there is a checked checkbox 'Use a field to map between accounts of the same user?'. Below it is a 'Field:' dropdown menu. At the bottom of the window, there are three buttons: 'Cancel', 'Back', and 'Next'.

18. Click **Should the users tree be grouped**, and select one of the following:

- a. Use the domain Organization Units structure
- b. Group by a field (then select the field from the dropdown list)

The Users Tree grouping is the same as that of the Users Tree in Advanced Forensics Control.

“Use the Domain Organizational Unit’s Structure” is only available for an Active Directory Identity Collector.

The Email Field Mapping section will only be displayed for the Active Director Identity Collector and if it is defined in the Authentication Store. In order to have fields in the dropdown, you must first define a field mapping.

19. Check the Use a field to map between accounts of the same user check box.

The Access Request wizard uses this mapping to match multiple accounts belonging to the same user so users can request permissions on those accounts.

20. Select a field from the dropdown list.

21. All of the accounts in various Identity Collectors with the same value in the selected field map to the same user. When the user logs into the web application to issue an Access Request, that user can request access to a specific account mapped to the logged in account.

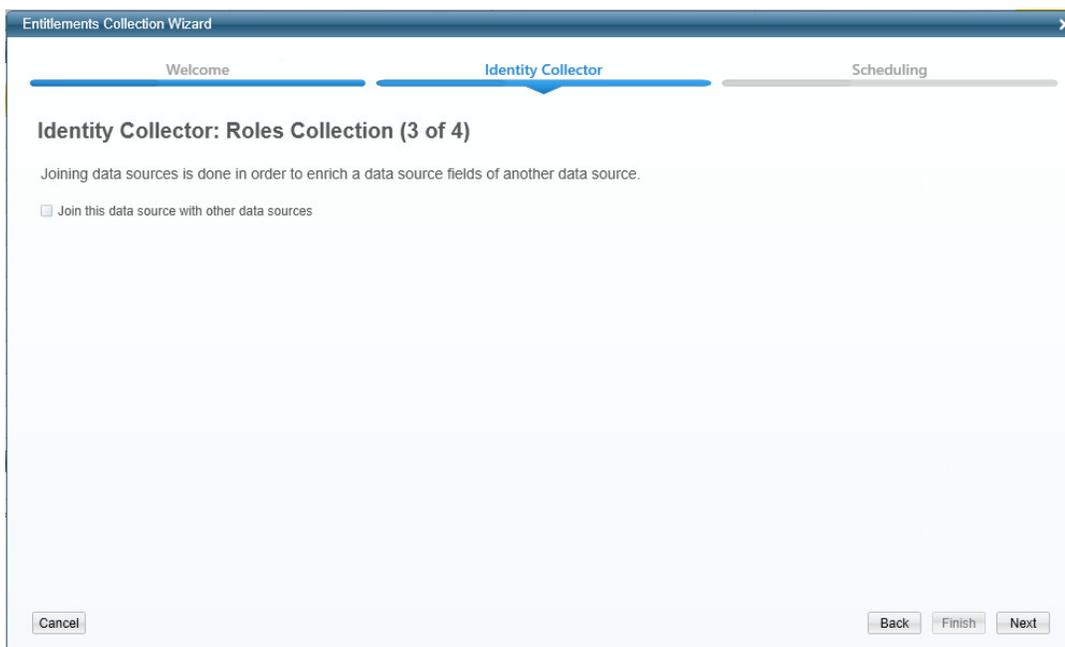
22. Click **Next**.

23. In addition to the standard properties that File Access Manager retrieves, you can retrieve additional properties for Active Directory groups.
24. Type additional properties to retrieve.
25. Click **Next**.
26. Verify that the system retrieved the requested information successfully.

Only the first ten results display.

27. Click **Next**.

The Identity Collector: Groups Collection (3 of 4) window displays:



28. File Access Manager creates data sources that contain user fields so that the Identity Collector can collect the Users.
29. Check the **Join this data source with other data sources** check box to join this data source to other data sources.
30. You can use one of the Identity Collector fields as the local key to gather additional user fields from other data sources by joining those data sources. Chapter has additional information on joining data sources.
31. Type the Data Source, the Local Key, and the Remote Key.

After you type the relevant data, select Test Data Sources to verify that the system has accepted the data.

32. Click **Next**.
33. Enter the Dynamic Fields Mapping data from the *Dictionary Field* and *Mapped Field* dropdown lists.

Use the **X** / **+** buttons to remove / add fields, as required.

34. Click **Next**.

The Identity Collector Scheduling window displays.

Identity Collector Configuration scheduling panel

The screenshot shows the 'Entitlements Collection Wizard' window, specifically the 'Scheduling' step. The window has three tabs: 'Welcome', 'Identity Collector', and 'Scheduling', with 'Scheduling' being the active tab. The title is 'Identity Collector Scheduling' and the subtitle is 'Set the schedule for identities collection'. There is a checkbox 'Create a Schedule?' which is checked. Below this are several input fields: 'Name' (Identity Collector), 'Schedule' (Daily), 'Start Date' (10/19/2015), 'At' (4:27 PM), 'Until' (1/10/2016), 'Interval of' (1 days), and 'Active?' (checked). At the bottom, there are 'Cancel', 'Back', 'Finish', and 'Next' buttons.

1. Enter the relevant scheduling values.
2. Click **Finish** to end the wizard or click **Next** to run an identity collection now.

If you are running the task now, you can view the task progress in the relevant service view in Health Center or in the File Access Manager website, **Settings > Task Management > Tasks screen**.

If you are running the task as part of the initial configuration, you will not have access to the File Access Manager web application until the task has completed. In this case, you can view the status of the identity collection task in the Health Center by navigating to **Health Center > Permission Collection > File Access Manager Collector Synchronizer > Tasks**.

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 the *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.

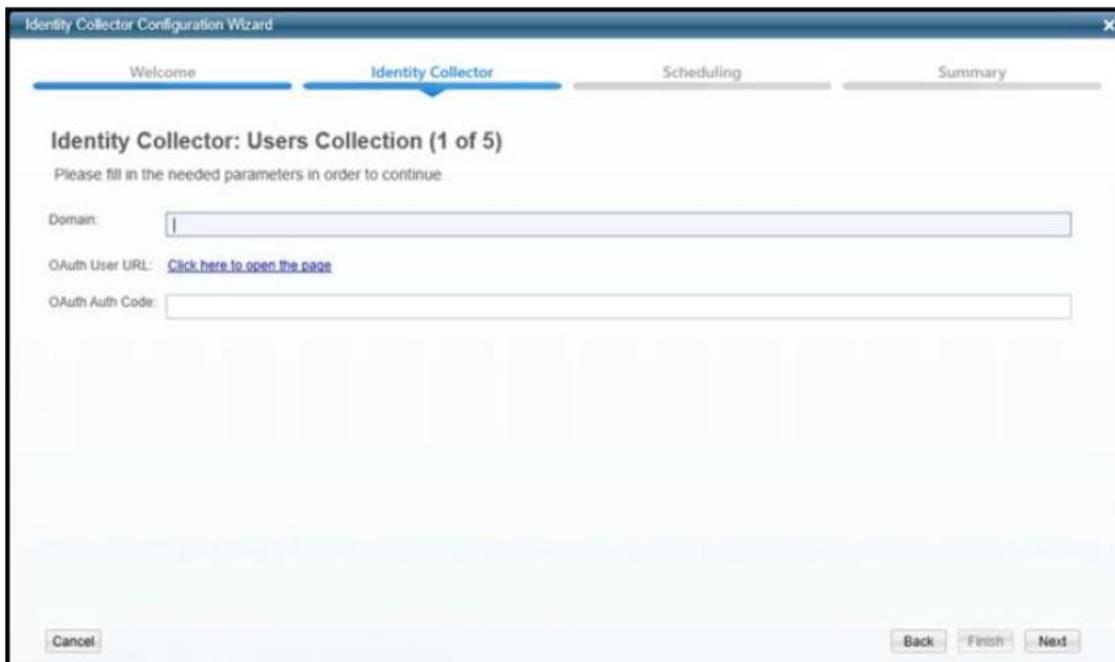
This means the configuration will resemble other connectors for cloud applications such as OneDrive.

- 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.

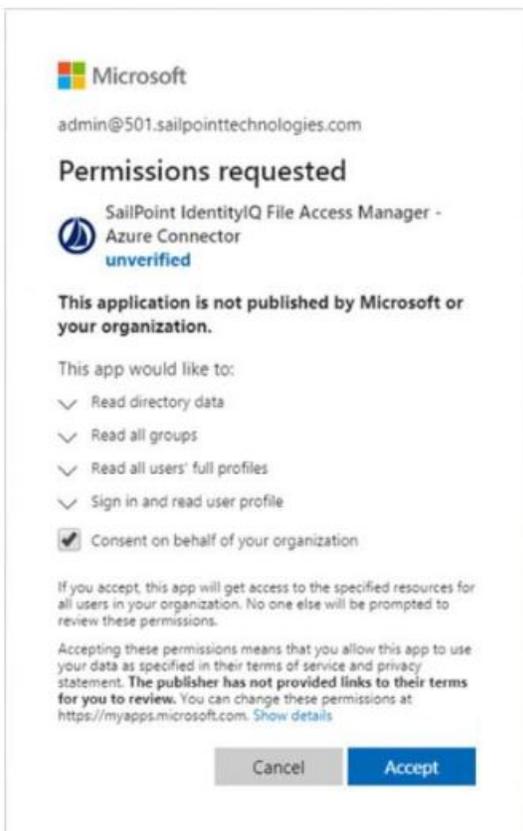


The screenshot shows the 'Identity Collector Configuration Wizard' window. The title bar reads 'Identity Collector Configuration Wizard'. The progress bar at the top indicates four steps: 'Welcome', 'Identity Collector' (which is the active step), 'Scheduling', and 'Summary'. Below the progress bar, the main heading is 'Identity Collector: Users Collection (1 of 5)'. Underneath this heading, it says 'Please fill in the needed parameters in order to continue'. There are three input fields: 'Domain' with a text box, 'OAuth User URL' with a blue hyperlink that says 'Click here to open the page', and 'OAuth Auth Code' with a text box. At the bottom of the window, there are four buttons: 'Cancel', 'Back', 'Finish', and 'Next'.

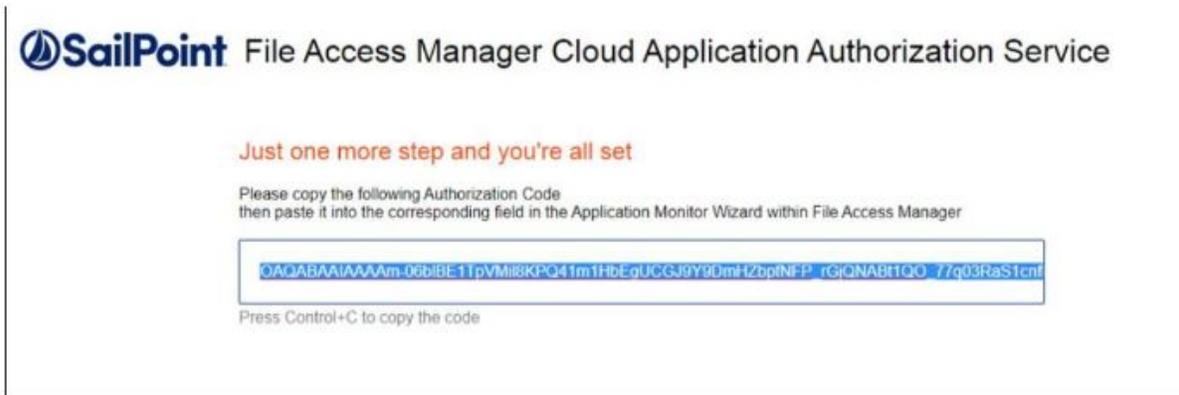
2. You will then be redirected to the Microsoft O365 Login Screen Login with the user that should be used by the Identity Collector.



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.



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



5. Copy that code and past it in the Auth Code field in the Identity Collector Configuration Wizard screen.
6. 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:

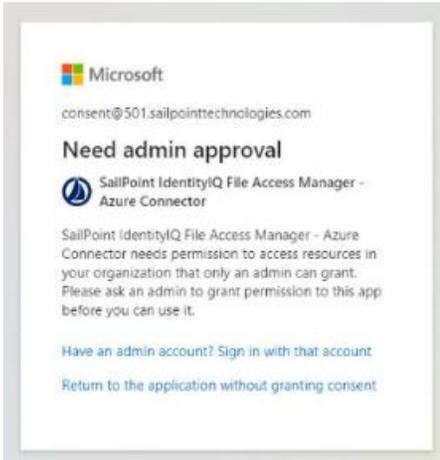
- Global Administrator (Company Administrator)
- Cloud Application Administrator
- Application Administrator

System Settings Required to Support SSO

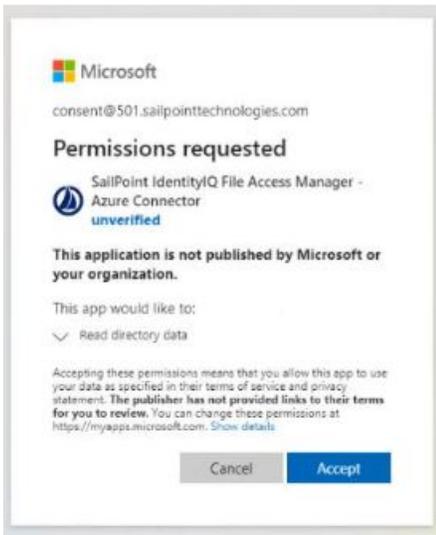
Hence, during the initial configuration phase (while generating the token for the first time), the service account dedicated to the File Access Manager Azure AD Connector must have one of the above-mentioned roles. Once consent is given, the role can be removed from the user.

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

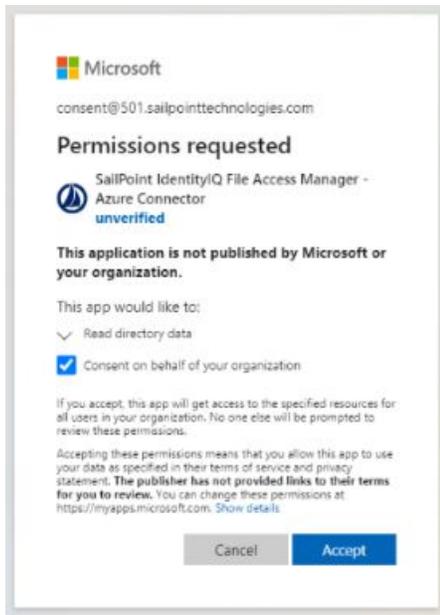
Non-admin user trying to access the consent screen will be presented with the following screen:



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.

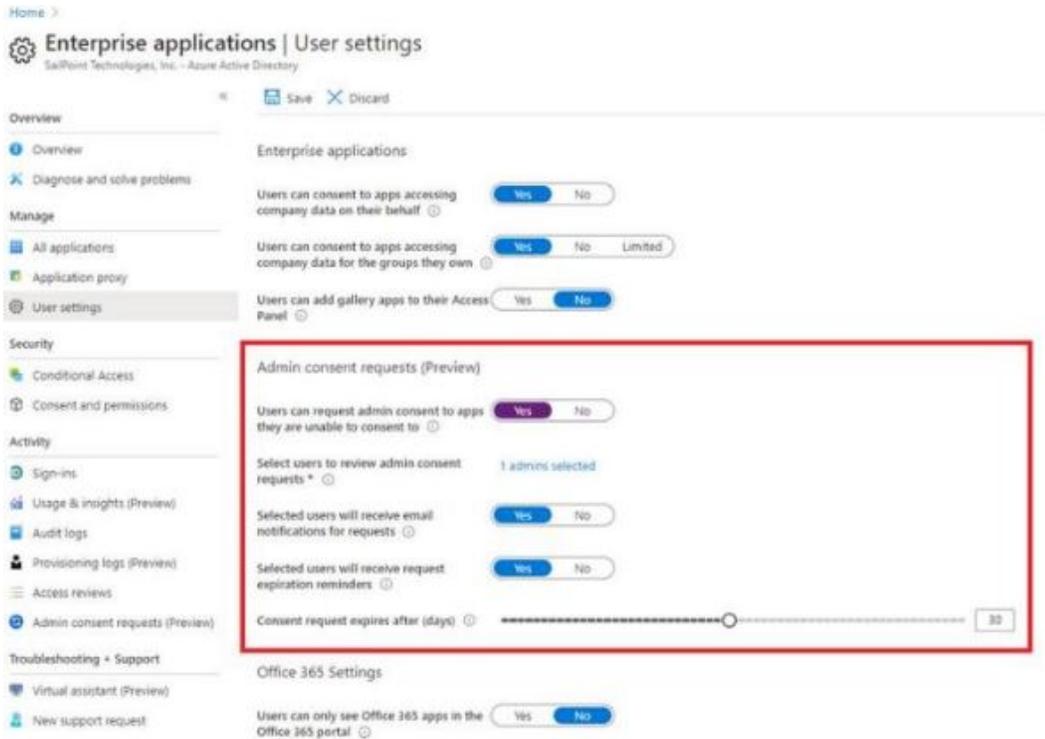
Avoiding the Administrative Roles Grant

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".

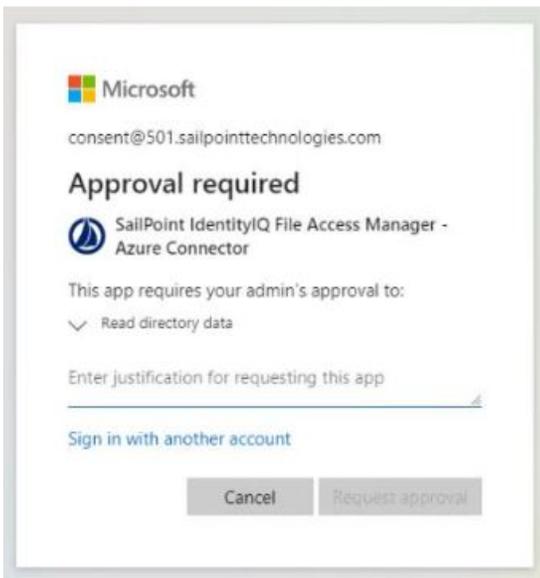
This relatively new feature lets non-admin users indirectly give consent to applications that require admin consent by requesting an admin's authorization.

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



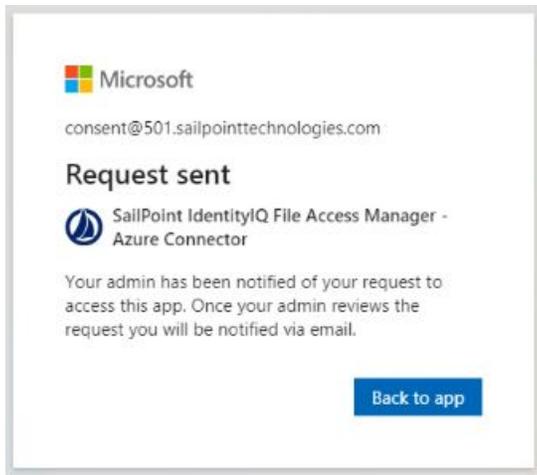
When users without one of these administrative roles go through the normal consent flow, they will be presented with the screen:



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.

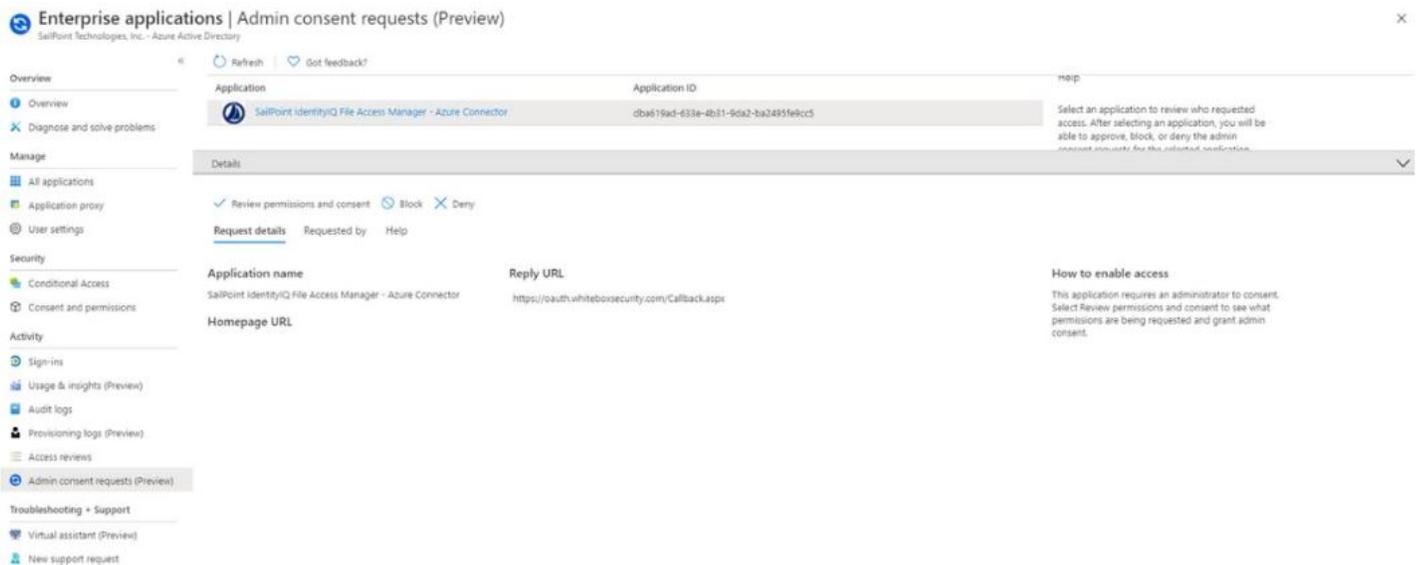
When clicking on "Request approval" to continue, the following screen appears:

System Settings Required to Support SSO

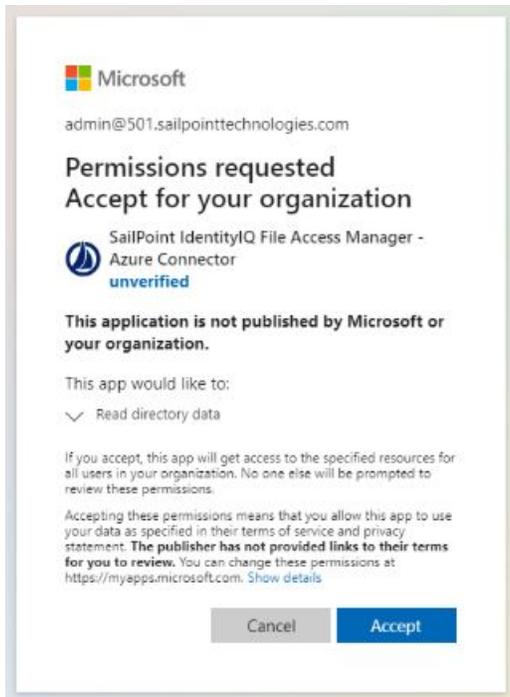


Clicking on “Back to app” would just return an “access denied” error as access was not yet granted. This screen can be safely closed while waiting for admin consent.

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 the token generation sequence again.

However, this time the consent screen will be skipped entirely, and the flow will lead directly to the Authorization code.

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

Configuring File Access Manager to Use Local Certificates

File Access Manager uses a self-signed certificate for each of the services.

You can configure the system to use your own trusted certificates, using the procedure described in this chapter. To be trusted, server certificates must conform to the following guidelines:

- Certificates are signed by a Certificate Authority (CA), trusted by all servers in the organization, whether the CA is commercial or in-house.
- Certificates are issued to each server hosting one of the WCF hosting services (as described below).
- Certificates include the server name as it is to be used by File Access Manager. This could be a short name or a Fully Qualified Domain Name (FQDN) in the Subject or in the Subject Alternative Names list.
- The certificate must have the following extensions defined:
 - Key Usage: Digital Signature, Key Encipherment.
 - Enhanced Key Usage: Server Authentication, Client Authentication.

The certificate may have other key usages, but must have at minimum those mentioned above.

Changing Certificates for Elasticsearch

The Elasticsearch certificate is stored in JKS - the Java keystore, which is Java's standard way of storing certificates and private keys. This is equivalent of the Windows' Store. We will have to make a private key for use with Elasticsearch, and supply the password.

ReadOnlyRest can support multiple certificates and choosing one in the configuration, but we assume that there is only one certificate in the JKS.

The scripts below are run in an elevated command line.

High Level Steps

1. Delete the current certificate from the JKS.
2. Provide a certificate with a private key, import the pfx file using the keytool, and change the certificate alias.
3. Edit the readonlyrest.yml file and change the 'key_pass' config key to the password of the .pfx file
4. Export certificate to a .cer file
5. Insert the certificate to the File Access Manager database, using the SailPoint FAMCertificateManager
6. Restart Elasticsearch

Detailed Steps

Delete the current certificate from the Java keystore (JKS):

1. Use the store password listed in the readonlyrest.yml file of the Elasticsearch.

```
Open the file readonlyrest.yml
```

Open the folder `%SAILPOINT_HOME%\elasticsearch-5.1.1\config\`

Copy the `keystore_pass` value

2. List the entries in the JKS, and store the certificate alias for later:

```
"%JAVA_HOME%\bin\keytool.exe" -list -v -storepass <store password> -keystore  
"%SAILPOINT_HOME%\elasticsearch-5.1.1\config\fileaccessmanager-elastic-cert-  
t.jks"
```

3. Delete the certificate

```
"%JAVA_HOME%\bin\keytool.exe" -delete -alias <certificate alias> -keystore  
"%SAILPOINT_HOME%\elasticsearch-5.1.1\config\fileaccessmanager-elastic-cert-  
t.jks" -storepass <store password>
```

Provide a .pfx file, which is a certificate with a private key:

- Generate a pfx file. The pfx file can be generated in different ways, from makecert to a CA issued certificate.
- If you have the pfx::

```
"%JAVA_HOME%\bin\keytool.exe" -importkeystore -srckeystore "<full path to pfx  
file>" -srcstoretype pkcs12 -destkeystore "%SAILPOINT_HOME%\elasticsearch-  
5.1.1\config\fileaccessmanager-elastic-cert.jks" -deststoretype JKS -dest-  
storepass <store password> -srcstorepass <pfx file password>
```

- Import will generate a new alias for the certificate. Change this alias back to the original alias, as read from step 1.b. above :

```
"%JAVA_HOME%\bin\keytool.exe" -changealias -alias <current alias> -destalias  
<new alias> -keystore "%SAILPOINT_HOME%\elasticsearch-5.1.1\config\fileaccessmanager-elastic-cert.jks" -storepass <store password> -keypass  
<pfx file password>
```

1. Edit the `%SAILPOINT_HOME%\elasticsearch-5.1.1\config\readonlyrest.yml` file and change the `'key_pass'` config key to the password of the .pfx file
2. Export certificate to a .cer file.

```
"%JAVA_HOME%\bin\keytool.exe" -export -alias <certificate alias> -storepass  
<store password> -file <full path to a cer file> -keystore "%SAILPOINT_  
HOME%\elasticsearch-5.1.1\config\fileaccessmanager-elastic-cert.jks"
```

3. Insert the certificate to the File Access Manager database, using the SailPoint FAMCertificateManager:
 - a. Open an elevated command line, and run the command:

```
"%SAILPOINT_HOME%\FileAccessManager\Server Installer-  
\Tools\FAMCertificateManager\FAMCertificateManager.exe" 20 -esCertFile=<full path to the cer  
file>
```

20 is the ID of Elasticsearch service.

4. Restart Elasticsearch.

If there are many services being updated, it might be simpler to reboot the server.

Changing Certificates for RabbitMQ

To replace the RabbitMQ certificates with your own trusted certificates:

1. Provide the following certificate files and keys:
 - a. The file containing the public key of the root Certificate Authorities that you wish to implicitly trust with the name: "ca.cer".
 - b. The file containing the client's own certificate public key with the name: "rabbitmq.cer".
 - c. The file containing the client's private key in PEM format: "key.pem".
2. To configure the RabbitMQ certificate files:
 - Replace the files located under "%SAILPOINT_HOME%\RabbitMQ\certificates" with the certificates and key mentioned above.
 - Open the file %SAILPOINT_HOME%\RabbitMQ\data\rabbitmq.config with a text editor, and replace the current files path with the path of your own trusted certificates and key. Then save the file.
3. Delete the SailPoint RabbitMQ certificate from the certificate computer store. The certificate name is - "File Access Manager RabbitMQ".
4. Restart the rabbitmq service, the Central Permission Collection Engine(s) and Collector(s) services and the Central Data Collection Engine(s) and Collector(s) services.

Changing the Certificates for Core Services

This process will replace the certificate for all the services except for Elasticsearch and RabbitMQ with your selected certificate.

All the SailPoint supplied certificates will be removed

To replace the certificates with your own:

1. Open an elevated command line

```
"%SAILPOINT_HOME%\FileAccessManager\Server Installer-  
\Tools\FAMCertificateManager\FAMCertificateManager.exe" -a -existingCertificate
```
2. Select your certificate from the dropdown list.
3. Restart the services, or reboot the server.

You can change the certificate for a single service, using the SailPoint tool FAMCertificateManager.exe, using the service_id of that service.

Changing the Certificates for Collectors

Changing the certificates of the collectors (Activity Monitor, Permission Collector, Data Classification) using the *Collector Installation Manager* replaces the SailPoint self-signed certificates with your appointed certificate, and deletes the corresponding SailPoint certificate from the certificate store.

To replace the certificates for collectors using the Collector Installation Manager:

1. Run the Collector Installation Manager

This will open a list of the collectors. You can update separate certificates per collector, or use the same certificate for all.

2. Click **Set Certificate for all Services**

If this server does not have a server installer, you will have to update the watchdog certificate manually. See [Installing Collectors on a Server Without Core Services](#) .

3. Select your certificate from the dropdown list to update the certificate list.
4. Restart all the services, or simply reboot the server.

Installing Collectors on a Server Without Core Services

If you are installing collectors on a server without installing the server installer, the **Collector Installation Manager** will not replace the watchdog certificate. This must be done manually, as described below:

Verify that you have to preform this step

Check the certificate store (local computer store), after running the Collector Installation Manager. If there is a certificate called "File Access Manager WatchDog [servername]", the watchdog certificate has not been replaced.

1. Copy the thumbprint of your trusted certificate
 - a. Find the certificate you want to use. This should be in the certificate store (local computer store).
 - b. Right click to read the certificate details, and copy the *thumbprint* value.
2. Update the thumbprint value in the watchdog configuration file
 - a. Locate the Watchdog configuration file
`%SAILPOINT_HOME%\%SAILPOINT_APP_NAME%\WBXWatchDogServiceHost.exe.config`
 - b. Open the configuration file with a text editor, and search for the "clientCertificateThumbprint"
 - c. Replace the value with the copied thumbprint from your trusted certificate in step 1
 - d. Save the file
3. Restart the watchdog service
4. Delete the SailPoint watchdog service certificate from the certificate list

Uninstalling File Access Manager

To uninstall the File Access Manager completely (High level):

Feature to Uninstall / Remove	Uninstall Method
File Access Manager Administrative Client	Windows Programs and Features
Collectors (Permission, Data Classification, Activity Monitor)	SailPoint Collector Installation Manager.
Elasticsearch	SailPoint script and manual steps
Java	Windows Programs and Features
Other File Access Manager Services (including the website)	SailPoint Server Installer
Folders of application and data created by the installation	File Explorer
Registry keys created by the installation	Regedit (or similar)

Uninstalling the File Access Manager Administrative Client

To completely remove the Administrative Client:

1. If the Administrative Client is running, close it.
2. Open the windows "Programs and Features" (Control Panel > Programs > Programs and Features)
3. Right click "File Access Manager Client" and choose uninstall.
4. Delete the folder %SECURITYIQ_HOME%\Client - This is the folder on which the administrative client was installed.
5. Delete the environment variables SECURITYIQ_HOME and SECURITYIQ_HOME_LOGS.

Uninstalling the Collectors

The collectors are services that collect information from the connected applications, for the File Access Manager to analyze. The collectors consist of the following:

- Permission collector
- Data Classification collector
- Activity Monitor collector

To uninstall the collectors:

- Open the Collector Installation Manager.
- Click uninstall for each of the collectors.

The collectors can be uninstalled in any order.

When the last collector has been uninstalled, if there are no other File Access Manager services running, the Connector Installation Manager will uninstall the Watchdog service.

Remove folders:

Delete the folder "*Collectors*" - This is an installation folder that you created when downloading the collector installation manager from the SailPoint source.

Remove registry keys:

Using a Windows registry editor, remove the folder **HKEY_LOCAL_MACHINE > Software > whiteboxsecurity > WhiteOPS > Components**.

If this server has no other services installed, you can remove the entire folder **whiteboxsecurity**.

Uninstalling the File Access Manager Services

To uninstall the File Access Manager services:

- Manually uninstall the Elasticsearch
- Uninstall all the remaining services
- Cleanup the remaining folders and registry keys

Uninstalling Elasticsearch

The ElasticSearch could be installed either on a dedicated server, or on the main File Access Manager server.

To uninstall the Elasticsearch:

1. Open an elevated command line in Windows and run the following commands. After running the commands, close the cmd windows:

- a. "%SAILPOINT_HOME%\elasticsearch-5.1.1\bin\elasticsearch-service.bat" remove
- b. setx JAVA_HOME "" -m

There is no need to stop the Elasticsearch service before removing it

In some instances the service will still be listed in the Windows services, even though it has actually been removed. A refresh, waiting a few minutes, or a reboot (in extreme cases) will update the services list. We can trust that it has indeed been deleted.

2. From windows "Programs and Features", uninstall the Java 8. This program was installed by the installer to support the Elasticsearch.
3. Delete the folder "%SAILPOINT_HOME%\elasticsearch-5.1.1". This folder stores the Elasticsearch program and configuration files, but not the actual stored data.
4. Execute the following update in the DB, to mark that the Elasticsearch database is uninstalled :

```
update service
```

```
set    server_id = null,  
       installed_server_id = null,  
       certificate_wbx_file_id = null,  
       status_enum_id = 5  
FROM    [whiteops].[installed_service] service  
        INNER JOIN [whiteops].[install_server] server ON service.installed_  
server_id = server.id  
WHERE   install_service_id = 20  
and     server.[name] = N'ELASTICSEARCH SERVER FQDN'
```

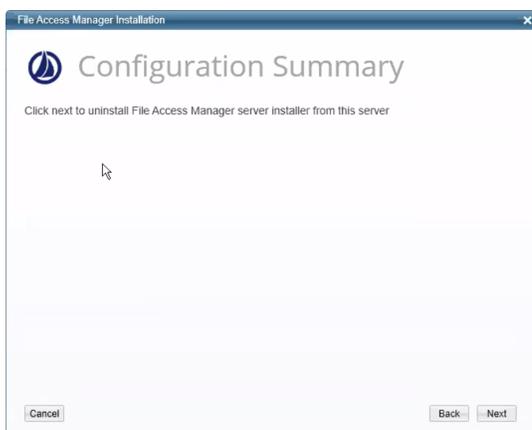
ELASTICSEARCH SERVER FQDN

This value must be replaced with the FQDN of the server from which we wish to uninstall the Elasticsearch.

5. Delete the Elasticsearch data folder. Deleting this folder will delete all the activities it stores, so make sure you want to delete it. If you wish to reinstall Elasticsearch at a later time and use these data, do not delete this folder.
6. If this instance of the Elasticsearch is on a dedicated server - Uninstall the Watchdog service from this server
 - a. Open the Server Installer
 - b. **Next** till the Action Select page
 - c. Click **Uninstall File Access Manager Features from the current server**

This procedure removes all services from this server, including the Server Installer itself.

This will open the configuration summary page. In this case, the list of services will be empty. This is normal, since no services besides the watchdog are to be uninstalled.



7. Click **Next** to start the uninstall process.

To reinstall Elasticsearch

1. Install Elasticsearch using the Server Installer.
2. Restart the Event Manager services.

Uninstalling File Access Manager

SAILPOINT_HOME_LOGS

SAILPOINT_APP_NAME

In some configurations these variables are removed by the uninstall process

Troubleshooting

Check the issues below for common problems and suggested ways of handling them.

Users Cannot Log into the Website After First Installation

When installing File Access Manager for the first time, the “Identity Sync” task has to complete its operation in order to get a list of users who can log into the web application. You can follow the progress of this task on the Health Center in the administrative client. (The task status is generally displayed in the web application which you cannot access before this task has completed.)

3rd Party SSO Login Users Cannot Access the Website

1. Verify that the correct connectivity values were stored in the database

Table: system_configuration_value

Record: WebSamlConfiguration

The JSON should be similar the sample below, depending on the SSO provider.

EntityId

The File Access Manager application created in the SSO provider

MetadataUrl

Generated in the process of creating the application above

```
{
  "EntityId": "FAM_SAML_LogIn",
  "MetadataUrl": "https://dev-39214733.okta.-
com/app/exka5w2f1LvL5gpI05d6/sso/saml/metadata",
  "SignatureAlgorithm": "http://www.w3.org/2001/04/xmldsig-more#rsa-sha256",
  "CertificateValidationMode": "0",
  "RevocationMode": "0"
}
```

2. Verify that all the users from the SSO provider were added correctly to the File Access Manager database.

The identity collector should upload the users listed in the data source into the following tables:

- whiteops.ra_user
- crowdSource.[user]

Further Information

For further configuration, and installation of the File Access Manager website, see chapter **File Access Manager Initial Configuration** in the File Access Manager Administrator Guide