

File Access Manager Installation with SAML and SSO

Version: 8.4

Revised: March 27, 2023

This document and the information contained herein is SailPoint Confidential Information

Copyright and Trademark Notices

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

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

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

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

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

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

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

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

Contents

Configuring	to use SAML Authentication	. 4
Creatir	ng an Okta Application	. 5
Creatir	ng an ADFS Application	. 14
Creatir	ng an Azure Application	. 18
Switch	ing from SAML to Windows Authentication Mode	. 23
System Set	tings Required to Support SSO	.28
System	n Settings to Support SSO - Okta	.29
System	n Settings to Support SSO - ADFS	.34
System	n Settings to Support SSO - Azure	. 35

Configuring to use SAML Authentication

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

This guide details integration steps for the following providers:

- Azure
- Okta
- ADFS

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

To support SAML login

- Create a dedicated application within the identity provider for the File Access Manager authentication Follow the installation for your identity provider:
 - a. Creating an Azure Application
 - b. Creating an Okta Application
 - c. Creating an ADFS Application
- 2. Follow the File Access Manager installation instructions in this guide, with the following points
 - On the Website authentication mode screen, select SAML 2.0 (See Website Authentication Mode)
 - Do not create an identity store
- 3. After installation set up the authentication on the File Access Manager servers and database to accept the SSO login.

See System Settings Required to Support SSO.

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

Creating an Okta Application

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

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

ta		Q	Search		
ď	^	0	verview	Give feed	lback on new dashboard
hboard	_				
		Us 1	ers 0 7 0%	Groups No groups	SSO Apps No apps added
ons	- 1		last / days	added Import groups	Add an app
i	- 1				
	~	Up	odated at 2 Mar, 1	0:15	
	^	Ta	asks		
Ŀ		ту	pe ≑ ltems ≑	Description	
			Info 1	Applications can	n be updated to use provision
	~				
	~	0	rg changes		View all
	~ .	Up	date policy: Default	Policy	View

c. Select Add Application.

Dashboard		
Dasmodru	~	
Directory	~	Applications
Applications	^	You have 5 apps remaining
Applications		Upgrade to add more than 5 apps.
Self Service		Upgrade to a paid plan to create more apps and get more monthly active of
Security	~	Add Application
Workflow	~	
Reports	~	Q Search
Settings	~	STATUS

d. Select Create New App.

Q Search				? ==
← Back to Applications	ion			Create New App
CATEGORIES				
Featured		Q Search		
API Management	6	Featured Integrations		See all
Apps	6300			
Apps for Good	13	Active Directory		: slack
CASB	2		workday	
Directories and HR Systems	13	Active Directory	Workday	Slack
Security Applications	709	Provisioning	SAML, SWA, Provisioning	SAML, SWA, Provisioning
Okta Applications	16			
VPN	22	ATLASSIAN	Docu Sign	zoom
		Atlassian Cloud	DocuSign	Zoom
		SAML, SWA, Provisioning	SAML, SWA, Provisioning	SAML, Provisioning

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

Create a No	ew Appl	ication lı	ntegration
-------------	---------	------------	------------

Platform	N	/eb 🔻
Sign on method	0	Secure Web Authentication (SWA) Uses credentials to sign in. This integration works with most apps
	0	SAML 2.0 Uses the SAML protocol to log users into the app. This is a better option than SWA, if the app supports it.
	0	OpenID Connect Uses the OpenID Connect protocol to log users into an app you've built.

×

Create

Cancel

f. Select Create.

2. Fill in the configuration fields.

a. General Settings

App name

Enter any name for your Application

Click Next.

b. Configure SAML.

Single sign on URL

-http://[SERVER_NAME]/siqapi/login/AssertionConsumerService

Where SERVER_NAME is the VM in which the Website is installed

Audience URI (SP Entity ID)

Enter the name of the application.

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

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

c. Feedback

Are you a customer or partner?

I'm an Okta customer adding an internal app

Select Finish.

- 3. The application was successfully created.
- 4. Click on the Identity Provider metadata.

board	~	Active View Logs Monitor Imports
	~	General Sign On Mobile Import Assignments
	^	
		Settings
		Sign on methods
	~	The sign-on method determines how a user signs into and manages their credentials for an
~		application. Some sign-on methods require additional configuration in the 3 rd party applicat
~		Application username is determined by the user profile mapping. Configure profile mapping
~		@ SAML 2.0
		Default Relay State
		SAML 2.0 is not configured until you complete the setup instructions.
		View Setup Instructions
e Okta		terning - rome inteledant a available in this application supports dynamic coming
o a paid apps		Credentials Details
nly		Application username format Okta username

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

← → C	d6/sso/saml/metadata			☆ @ 🛛 🔿 🗯 🗊 🕲 🗄
🔛 Apps 🧧 ImportantDocs 🧧 Test Environments 🧧 Dev Environment	📙 Documentation 🚇 SailPoint IdentityNow 📒 Selenium 💽] qTest - Login 😵 TimeWatch - Shaot 🔂 vSphere - siq-v6-ui	😡 Review Distribution 📙 Jenkins 📃 Jira 🔞 Advanced Ac	tive Di 🛞 Scrum Poker Online »
This XML file does not appear to have any style information associat	ed with it. The document tree is shown below.			
<pre>radiintiyyaacriyabe wahanad "waxaadiaanaa tic SULLI waxaa radiintiyyaacriyabe wahanada" waxaadia waxaa ti Sullia "diintiyyaacriyabe wahanada "waxaadiaana" yaxaa "diintiyyaacriyabe wahanada "yaxaadiaana" "diintiyyaacriyabe saka wahanada wahana waxaa yaxaa "diintiyyaacriyabe saka wahanada wahana waxaa yaxaa "diintiyyaacriyabe saka wahana wahayaa yaxaa waxaa "diintiyyaacriyabe yaxaa waxaa yaxaa yaxaa yaxaa "diintiyyaacriyabe yaxaa waxaa yaxaa yaxaa yaxaa "diintiyyaacriyabe yaxaa waxaa yaxaa yaxaa yaxaa "diintiyyaacriyabe yaxaa yaxaa yaxaa yaxaa yaxaa "diintiyyaacriyabe yaxaa yaxaa yaxaa yaxaa yaxaa yaxaa "diintiyyaacriyaa yaxaa yaxaa yaxaa yaxaa yaxaa yaxaa "diintiyyaacriyaa yaxaa yaxaa yaxaa yaxaa yaxaa yaxaa yaxaa adiishaa yaxaa yaxaa yaxaa yaxaa yaxaa yaxaa yaxaa yaxaa yaxaa yaxaa adiishaa yaxaa yaxa</pre>	eadma" ently/D="http://www.okta.com/edu/si/fil/iSprit clooper/thumeration" writesiinameritesiin ** Kisesibeogesiaware.com yeepi-writesiines aluecame horizolagesigaagesaccomy egetaware.com/edu/oktaware horizolagesigaagesaccomy egetaware.com/edu/oktaware horizolagesigaagesaccomy egetaware.com/edu/oktaware horizolagesigaagesaccomy egetaware.com/edu/oktaware horizolagesigaagesaccomy egetaware.com/edu/oktaware horizolagesigaagesaccomy egetaware.com/edu/oktaware horizolagesigaagesaccomy egetaware.com/edu/oktaware gitawijosishirooSgoccomy egetaware.com/edu/oktaware timesigaagesaccomy egetaware.com/edu/oktaware timesigaadesaccom/edu/oktaware/ closeliadesac/mileesiDformat> 2.0000militario/fileesiDformat>	DBGS") Practic vectory TEXPROSALIES.net/DJPLIEJYNS (BAT(ble DMAGBAL) Practic vectory TEXPROSALIES.net/J27/LETY/NGS/DAT(ble LATAGA DIAT/SILACK-MET/ACQUARGEMPT2101G1a-detworl) (Bate Diat/SILACK-MET/ACQUARGEMPT2101G1a-detworl) (Bate Diates Diata (Diata) Diata (Diata) Diat	RCgeHIICPYTEV (MISAURCH-LUIMPHY-Vall2ZIS-TATEgMEWPD pHI22PYTEWBIALURCH-LUIMPHY-Vall2ZIS-TATEgMEWPD018 MaSSRY/WWJ.SHZITRES/amJOINULFIEMJeHE-CIERCAS-MQWAI Marta JUTMOLTHA-JangGooghTSHIILBUC-JanzarJagekel Janz Lagolangel.getOogadg/hjter/y/WonryrQHI02L2Hd2 Sgg185dd/sso/aml'/> 1Uv3.gp185dd/sso/aml'/>	NOLLIBOOTISMO-LITE-OFMONSAGESIBIOQEJ IBOOTISMOCINET MELANDERANDA MELANDERANDA NUBACHMOLIGACA NUBACHMOLIGACA

- 6. Add users who can see the application.
 - a. Select on the Assignments tab.

okta		Q Search		
shboard	~	← Back to Application	3	
ctory	~		FAM-SAML	-Login
cations	^	Ω,	Active 🔻 🖙	View Logs Monitor Imports
plications		General Sign C	n Mobile Import	Assignments
Self Service				
ity	~	Assign 🔻	Convert Assignments	Q Search
,	~	Filters	Person	Туре
	~	People		
3	~	Groups		01101110 01101111 012000 01000 0110101 0110110 01100111 No users found
6				

b. Navigate to **Assign > Assign to People**.

Active • V	iew Logs Monitor Imports	
Assign • Convert Assignments Assign to People	Q. Search	People •
p, Assign to Groups Groups	01101110 01101111 01:00 01:01 01:010 01:0110 01:0111 No users found	

- c. Select **Assign** next to the displayed user.
- d. Select Save to go Back button.

The user is now selected as **Assigned**.

- e. Select Done.
- f. User is displayed in the Application list.

kta	
shboard	~
ectory	~
cations	^
pplications	
Service	
Service y	~
If Service ity flow	× ×
lf Service ty Iow Is	* * *

7. Additional users or groups can be added in

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

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

okta	Q Search	Q Search				
Dashboard 🗸						
Directory ^	L People				• Hel	
People	J₊ Add person ◯ ◯	Reset pas	swords C Reset mu	Iltifactor More actions 🔻		
Groups						
Profile Editor	Q Search					
Diractory Integrations	Everyone	2 Per	rson & username	Primary email	Status	
Self-Service	Onboarding	Vit	Test1 Okta	vital.shvarts@salpoint.com	Pending user action	
Registration	Staged	0 Vit	Sh	spuitjob@gmail.com	Active	
Profile Sources	Pending user action	1				
Applications ~	Active					
Security	Active	1				
occurry	Password reset	0				
Workflow ~	Locked out	0				
Reports 🗸 🗸	Inactive					
	Suspended	0				

- 8. You can now assign the application for recently created users:
 - a. Navigate to *Applications* > *Applications* and select Assign Applications.

okta	
Dashboard	~
Directory	~
Applications	^
Applications	
Self Service	
Security	~
Workflow	~
Reports	~
Settings	~

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

okta		Q Search 🕐 🗄 🗸
Dashboard	~	← Back to Applications
Directory	~	🗰 Assign Applications
Applications	^	Assign Apps to People O Confirm Assignments
Applications		
Self Service		Cancel
Security	~	
Workflow	~	Applications 1
Reports	~	Search Q. Search by person
Settings	~	Z Application & Label ^ Sign-on Z Person & Username ^ Status
		FAM-SAML-Login SAML 2.0
		First Previous 1 Next Last Vit Sh Active
		First Previous 1 Next Last

- c. Click Next.
- d. Click Confirm Assignment.

okta		Q Search				
board	~	Review your as	signments before	confirming		
rectory	~	Previous C	Cancel		Confirm Assignmen	nts
Applications	^					
Applications		A FAM-SA	AML-Login needs ad	ditional information en	tered before it can be assigned.	
Self Service		Enterna	attributes			0
ecurity	~	Enter user	attributes			Ŭ
Vorkflow	~	۵	FAM-SAML-Log FAM-SAML-Log	gin in • SAML 2.0		0
ports	~	Enter user-sp	ecific attributes			
ettings	~	Enter user-sp	ecine attributes			
		Search			Username defaults to Okta username	
		VitTest1 Okt	a	User specific fields		
		Vit Sh		Username	terhait, Ortaglig.com	
		vic on		ooomano	drog top (dates) course	
0		Showing 1	- 2 of 2			
Thanks for trying th free plan. Upgrade	he Okta to a paid					
plan to create more	apps					
and get more Mont Active Users.	niy	Previous C	Cancel		Confirm Assignmen	nts

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

okta	
Dashboard	~
Directory	~
Applications	^
Applications	
Self Service	
urity	~
rkflow	~
rts	~
igs	~

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

okta		Q Search	Q Search						
Dashboard	~	← Back to Applicati	ons						
Directory Applications	~	Ø	FAM-SAML-Log	n s Monitor Imports					
Applications Self Service		General Sig	n On Mobile Import Assi	gnments					
Security	~	Assign •	✓ Convert Assignments	Q Search	People				
Workflow	~	Filters	Person	Түре					
Reports	~	Groups	VitTest1 Okta	Individual	1				
Settings	~		Vit Sh	Individual	1				

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

- The name of the created Okta application. In this example "FAM_SAML_LogIn" Note that this string is case sensitive in the installation process in File Access Manager.
- The URL to the Metadata mentioned above.

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

Creating an ADFS Application

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

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

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

Welcome step

Start

Select Data Source

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

- 3. Select Next.
- 4. Specify Display Name: Enter any name, this name will later be used during the installation of File Access Manager with SAML 2.0 option.

Select Next.

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

Select Next.

6. Configure Certificate

Select Next.

7. Configure URL

Select Next.

8. Relying party trust identifier.

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

Select Add.

Select Next.

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

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

Select Next.

10. Choose Issuance...:

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

Select Next.

11. Ready to Add Trust

Select Next.

12. Finish.

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

Select Close.

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

Select Add Rule.

- 14. In the opened wizard select and enter the following data:
 - a. Select Rule Template

Claim Rule Template

Select Send LDAP Attributes as Claims

Select Next.

b. Configure Claim Rule

Claim rule name

UserInfo

Attribute store

Active Directory

Mapping of LDAP attributes to outgoing claim types

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

15. Select Finish.

16. Select the Add Rule button.

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

Claim rule name

Free text

Claim rule template

Transform an Incoming Claim

Incoming claim type

Username

Outgoing claim type

Name ID

Outgoing name ID format

Unspecified

Pass through all claim values

Select this option

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

ADFS_for	_FAM_vit	Properti	es	x
Monitoring Identifiers E Organization Endpoints Specify the endpoints to use for	ncryption Proxy End SAML and	Signature points N WS-Federati	Accepted lotes Adv onPassive pro	Claims anced btocols.
URL	Inde	x Binding	Default	Re
SAML Assertion Consum	er Endpoin	ts		
Heat / Nov-Full office of	. 0	POST	No	
<	1			>
Add SAML				
Add WS-Federation		Remov	e Edi	t
	ОК	Cano	el	pply

21. Select Add SAML.

22. Fill the following values in all fields:

Endpoint type

SAML Assertion Consumer

Binding

POST

Index

0

Trusted URL

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

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

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

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

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

\$			AD FS		_ _ X
😪 File Action View Window Help					- 6
AD FS	Endpoints				Actions
⊿ 🧮 Service	Enabled	Prov Enabled	URI Path	Type	Endpoints
Endpoints	NO	NO	/adts/services/trust/2005/issuedtokenmixedsymmetrictipl	WS-Irust 2005	
Certificates	No	No	/adfs/services/trust/2005/issuedtokenmixedsymmetrictripl	WS-Trust 2005	View
Claim Descriptions	Yes	No	/adfs/services/trust/13/kerberosmixed	WS-Trust 1.3	New Window from Here
Trust Relationships	No	No	/adfs/services/trust/13/certificate	WS-Trust 1.3	G Refresh
Claims Provider Trusts	Yes	Yes	/adfs/services/trust/13/certificatemixed	WS-Trust 1.3	
Relying Party Trusts	No	No	/adfs/services/trust/13/certificatetransport	WS-Trust 1.3	I Help
Attribute Stores	No	No	/adfs/services/trust/13/usemame	WS-Trust 1.3	/FederationMetadata/2007-06/FederationMeta •
Authentication Policies	No	No	/adfs/services/trust/13/usemamebasictransport	WS-Irust 1.3	Dirable on Brown
	Yes	Tes	/adfs/services/trust/13/usemamemored	WS-Irust 1.3	Disable on Proxy
	No	No	/adfs/services/trust/13/issuedtokenasymmetricbasic256	WS-Iruet 1.3	Disable
	No	No	/adfs/services/trust/13/issuedtokenasymmetricbasic256sh	WS-Irust 1.3	Help
	Tes	Tes	/adfs/services/trust/13/issuedtokenmixedasymmetricbasic	WS-Irust 1.3	
	No	No	/adis/services/trust/13/issuedtokenmixedasymmetricbasic	WS-Irust 1.3	
	Tes No.	Tes No.	/adis/services/trust/13/issuedtokenmixedsymmetricbasic2	WS-Irust 1.3	
	No	No	/adts/services/trust/13/issuedtokenmixedsymmetricbasic2	WS-Inust 1.3	
	No	No	/adis/services/trust/13/issuedtokensymmetricbasic256	WS-Trust 1.3	
	No	No	/adis/services/dust/13/issuedtokensymmetricbasic236sha	WS-Trust 1.3	
	No	No	/adis/services/irusi/13/issued.okensymmetrictipledes	WS-Teat 1.3	
	No	No	/adis/services/irusi/13/issueduckensymmetricingledessrid	WS-Teat 13	
	No	No	/adis/services/irusi/13/issued/okeninkeusyinneircripteues /adis/services/irusi/13/issued/okeninkeusyinneircripteues	WS-Teat 13	
	No	No	/adis/services/irds/13/issoed/okerinkeusynneuroupied /adis/services/irds/13/windows	WS-Trust 13	
	No	No	/affe/ean/cae/hiet/13/windowentvad	WS-Truet 1.3	
	No	No	/adfe/services/trust/13/windowstranenort	WS-Truet 1.3	
	Yes	No	/adfs/services/trusticp/windows	WS-Trust 2005	
	No	No	/adfs/services/trust/adfactresolution	SAML-Artifact Besc =	
	Yes	Yes	/adfs/pauth2/	OAuth	
	Metadat	1			
	Yes	Yes	/artis/services/trust/max	WSMEX	
	Yes	Yes	/Federation Metadata /2007-06/Federation Metadata xml	Federation Metada	
	Yes	No	/adfs/fs/federationserverservice asmx	ADFS 1.0 Metada	
	0				
	Yes	No	/adfs/proxy/	Web Application P	
	Yes	No	/adfs/proxy/EstablishTrust/	Web Application P	
	Other				
	No	No	/adfs/portal/updatepassword/	HTTP	
	<			>	

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

Creating an Azure Application

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

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



4. Fill the following fields:

What's the name of your app?

Free text

What are you looking to do with your application?

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

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



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

Identifier (Entity ID)

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

Delete the default value identifier.

Select the created identifier as default by checking the checkbox.

Reply URL (Assertion Consumer Service URL)

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

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

Select Save.

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

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

Home > Azure-SAML-Vit > SAML-based Sign-on > User Attributes & Claims >								
Manage claim ····								
🔚 Save 🗙 Discard changes								
Name	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. Select Save.

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

12. Select Properties.

		$\mathcal P$ $$ Search resources, services, and docs (G+/) $$	
Home > Enterprise applications > SAML	-Vit-New		
SAML-Vit-New Pro	perties		
«	🗟 Save 🗙 Discard 📋 Delete	♡ Got feedback?	
Overview Deployment Blan	Enabled for users to sign-in? 🕕	Ves No	
	Name * 🕕	SAML-Vit-New	~
Manage	Homepage URL 🕕		\square
Owners	Logo ①		
8 Roles and administrators (Preview)	-		
Users and groups			
Single sign-on		Select a file	6
Provisioning	User access URL ①	https://myapps.microsoft.com/signin/SAML-Vit-New/0919f8ab-401c-4	\mathbb{D}
Application proxy	Application ID ①	0919f8ab-401c-43e7-932b-4cf8bff433e3	\mathbb{D}
Generation Self-service	Object ID (j)	de723773-decc-4c71-9f75-0c433e8ede65	
Security	Terms of Service Url ①	Publisher did not provide this information	D
Conditional Access	Drivery: Statement Liel (1)	Dublisher did not provide this information	10
Permissions	Privacy statement on ()	Publisher did not provide this information	43
Token encryption	Reply URL ①	https://siq-v6-ui8.office.whitebox.forest/siqapi/login/AssertionConsum	0
Activity	User assignment required? 🛈	Yes No	
➔ Sign-ins	Visible to users? ①	Yes No	
🕍 Usage & insights (Preview)	Notes ①		~
Audit logs			
Provisioning logs (Preview)			
E Access reviews	Comment		

13. Verify that "User assignment required?" is set to No.

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

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

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

third frame

■ Microsoft Azure	✓ Search resources, services, and docs (G+/)
Home > Azure-SAML-Vit >	
Azure-SAML-Vit SAML	-based Sign-on …
«	↑ Upload metadata file > Change single sign-on mode i Test this application Soft feedback?
Deployment Plan	Set up Single Sign-On with SAML
Manage	Read the configuration guide 🖒 for help integrating Azure-SAML-Vit.
Properties	1 Basic SAML Configuration
Owners	Cedit
🙇 Roles and administrators (Preview)	Reply URL (Assertion Consumer Service URL) https://siq=v6-ui8.office.whitebox.forest/siqapi/login/Asse
Users and groups	rtionConsumerService
Single sign-on	Relay State Optional
Provisioning	Logout Url Optional
Application proxy	8
Self-service	User Attributes & Claims 🖉 Edit
Security	givenname user.givenname
2. Contraction of the second sec	emailaddress user.mail
Conditional Access	name user.userprincipalname
🖧 Permissions	Unique User Identifier user.userprincipalname
Token encryption	
Activity	3 SAML Signing Certificate 2 Edit
Sign-ins	Status Active Toursenant Toursenant Active Tours
🕍 Usage & insights (Preview)	Expiration 3/7/2024, 5:02:21 PM
Audit logs	App Federation Metadata Url https://login.microsoftonline.com/154dccc9-b44e D
Provisioning logs (Preview)	Certificate (Baseb4) Download
3 Access reviews	Certificate (Raw) Download
	regeration metagata XML Download

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.

V j				Inte	rnet Inform	ation Servio	es (IIS) Mar
중 SIQ-V6-UI8 ►	Sites Default Web Site	▶ cdn ▶					
File View Help							
Connections Connections Start Page SIQ-V6-UI8 (OFFICE\administ Papelication Pools Application Pools Application Pools Connection	Filter: ASP.NET NET Authorizat Compilati	e Go Co MET Error Pages ate SMTP E-mai	Show All	Group by: An	ea .NET Roles	• III •	.NET Users
	Authenticati on SSL Settings	ion Default Document	Directory Browsing	A 404 Error Pages	Handler Mappings	HTTP Respon	Logging
	Management						

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



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

<i>6</i>]			Internet Information
	iites 🕨 Default Web Site 🕨 cdn	•	
File View Help			
Connections Image: C	Group by: No Grouping	Set 1	December 7 and
Application Pools	Name Anonymous Authentication ASP.NET Impersonation Forms Authentication	Status Disabled Disabled Disabled	HTTP 302 Login/Redirect
 ↓ Cdn <li< th=""><td>Windows Authentication</td><td>Disabled</td><td>HTTP://11.Challenge Enable Help</td></li<>	Windows Authentication	Disabled	HTTP://11.Challenge Enable Help

- 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.

🕖 SailP	Point				
< Navigation		~	Applications		
Applications			Please choose an Application or a	Bus	iness Resource from
Reports			🔅 New 👻 🔏 Configuration	^	
Davie Davies		1	Activity Monitoring	۲	
Review Processes		F	Permissions Management	•	ns Screen
Access Requests	Authoritication Store		Aanade File Access Manader Permissions		ow applications
Access Fulfillment	Authentication Store			,	ew applications,

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

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

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

System Settings Required to Support SSO

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

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



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

ation."

U _1		Internet Information Services (IIS) Manager
SIQ-V6-UI8 → Sites →	Default Web Site 🔸 identityiqfam 🔸 v2	•
File View Help		
Connections	Authentication	
Start Page	Group by: No Grouping -	
	Name A St	atus Response Type
∠ Application Pools	Anonymous Authentication Er	nabled
🖌 😜 Default Web Site	ASP.NET Impersonation Di	isabled
aspnet_client	Forms Authentication Di	isabled HTTP 302 Login/Redirect
⊳ 🔐 cdn	Windows Authentication Di	isabled HTTP 401 Challenge
4 🚝 identityiqfam		
Þ-⊕ v1 ⊳⊕ v2		
⊳ SiqApi		

- 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.
- Website: Run the Identity collector task which was recently selected as authentication store.
 This step will load the Okta users into the database.
- 5. Website: Click on the **SAML login** button and sign in to the relevant SSO Provider.
- 6. You should now be logged into File Access Manager the SSO provider user.

Detailed Settings

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

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

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

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

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



SailPoint
 SailPoint

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

Select Login.

(d) Sai	IPoint		
		Logi	n
		Username	
		Username	*
		Password	
		Password	۰ *
			Login
		Switch to SAN	IL 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.

dentity Collector Configuration Wizard			
Welcome	Identity Collector	Scheduling	Summary
Identities Collection Cor	nfiguration		
General			
This wizard configures the identity co	Ilection process for Active Directory or	Data Source based identities environme	ent.
The wizard will guide you through se	veral steps in which you will be request	ed to supply information about the colle	ction of users and groups.
First you must choose the Authentic	ation type: Active Directory or Data Sou	rce based type.	
To begin, please choose Identity C	ollector type:		
Active Directory Identity Collector			
Azure Active Directory Identity Collector			
 Data Source based Identity Collector 			
 NIS based Identity Collector 	_		

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

Select Next.

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

User Principal Name

Username

Welcome	Identity Collector	_	Scheduling	Summary
dentity Collector	: Users Collection (1 of 3)		
Fixed Fields Mapping				
Main Data Source				
Data Source:	OktaUsers	~		
Mandatory Fields				
Jsername	User Principal Name	*		
Optional Fixed Fields				
Distinguished Name		~ _ E	ntity Type Name	× (
		✓ □ b	User Locked?	~
Is User Disabled?		× •	assword Never Expires?	~
Is User Disabled?		-		
Is User Disabled? Last Login Date Password Not Required?		v 🗆 l	ser Alternate Unique Identif	~
Is User Disabled? Last Login Date Password Not Required? User Domain Name		~ I (lser Alternate Unique Identif	~

Select Next.

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

Click Next.

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

Click Finish.

- g. Wait until the task is finished, and close the Identity Collector Configuration window.
- 3. Admin client: Select this identity store as the authentication store.
 - a. Navigate to **Configuration > General Configuration > Authentication Store**.
 - b. Select the identity collector created above as the current authentication store.

Authentication Store Wizard
Authentication Store Change Wizard This wizard enables you to choose an Identity Collector as the new Authentication Store
Please notice that proceeding with this wizard, will STOP the review processes of running Access Certification Campaign 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: OktaUsers

- 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 Identies Synchronization task which was recently selected as authentication store.
- 5. Website: Click on the **SAML login** button and sign in to the relevant SSO Provider.

Click on **Send anyway** if needed, sign in for the first time if needed.

6. You should now be logged into File Access Manager the SSO provider user.

System Settings to Support SSO - ADFS

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

- 1. Admin client: Create an Active Directory identity collector.
- 2. Admin client: Select this identity store as the authentication store.
- 3. Website: Log in using the wbxadmin credentials, and run the Identity collector task which was recently selected as authentication store.

This step will load the ADFS users into the database.

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

Detailed Settings

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

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

See Creating or Editing an Active Directory Identity Collector.

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

Click Login.

- c. Navigate to Settings > Tasks Management > Scheduled Tasks.
- d. Run the identity collector task created above as authentication store.

This step will load the ADFS users into the database.

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

System Settings to Support SSO - Azure

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

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

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

This step will load the Azure users into the database.

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

Detailed Settings

- Admin client: Create an Azure identity collector.
 See Creating or Editing an Azure Identity Collector
- 2. Admin client: Select this identity store as the authentication store.
 - a. Navigate to Configuration > General Configuration > Authentication Store.
 - b. Select the identity collector created above as the current authentication store.
 - c. Click Finish.
- 3. Website: Log in using the wbxadmin credentials, and run the Identity collector task which was recently selected as authentication store.
 - a. Open the website and click on Continue with username and password.
 - b. Log in to the system with the wbxadmin user and use the password entered during the installation of the system

Click Login.

- c. Navigate to Settings > Tasks Management > Scheduled Tasks.
- d. Run the identity collector task created above as authentication store.

This step will load the Azure users into the database.

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

Creating or Editing an Azure Identity Collector

Azure AD Connector Full OAuth 2.0 Support

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

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

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

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

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

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

Configuration

Complete the following steps:

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

Web	come -	Identity Collector	Scheduling	Summary
dentity C	ollector: Users C	ollection (1 of 5)		
Please fill in the	e needed parameters in (order to continue		
Domain:	1			
OAuth User URL:	Click here to open the page	£		
OAuth Auth Code:				
Cancel				Back Finish 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.

admin@501	sailpointtechnologies.co	om
Permiss	sions requested	1
SailPo Azure	oint IdentityIQ File Acces Connector rified	ss Manager -
This applic your organ	ation is not published b ization.	by Microsoft or
This app wo	ould like to:	
 Read dire 	ectory data	
Read all	groups	
Read all	users' full profiles	
 Sign in a 	nd read user profile	
 Consent 	on behalf of your organizati	on
If you accept, t all users in you review these p	his app will get access to the s ir organization. No one else wi ermissions.	pecified resources for I be prompted to
Accepting thes your data as sp statement. The for you to rev https://myapp	e permissions means that you becified in their terms of service publisher has not provided lew. You can change these per smicrosoft.com. Show details	allow this app to use e and privacy links to their terms missions at
		-

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

SailPoint SailPoint	File Access Manager Cloud Application Authorization Service
	Just one more step and you're all set Please copy the following Authorization Code then paste it into the corresponding field in the Application Monitor Wizard within File Access Manager
	OAQABAAIAAAAm-06bIBE1TpVMi8KPQ41m1HbEgUCGJ9Y9DmH2bptNFP_rGjQNA8t1QO_77q03RaS1cnf
	Press Control+C to copy the 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

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:

Interosoft		
consent@501.sailp	ointtechnologies.	com
Permission	s requested	1
SailPoint Id Azure Conn unverified	entityIQ File Acces ector	ss Manager -
This application i your organizatio	is not published t n.	ey Microsoft or
This app would lik	e to:	
Read directory is	iata	
Accepting these permi your data as specified statement. The publish for you to review. Yo https://myapps.micros	ssions means that you in their terms of servic her has not provided u can change these per officion. Show details	allow this app to use e and privacy links to their terms missions at

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 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 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:

Overview	Enterprise applications
Diagnose and solve problems	Users can consent to apps accessing No
All applications	Users can consent to apps accessing
Application proxy	company data for the groups they own
User settings	Users can add gallery apps to their Access Ves No
curity	
Conditional Access	Admin consent requests (Preview)
Consent and permissions	Users can request admin consent to apps Nos No
tivity	Select users to review admin consent to believe colored
Sign-ins	requests * 🔘
Usage & insights (Preview)	Selected users will receive email No
Audit logs	notifications for requests ③
Provisioning logs (Preview)	Selected users will receive request
Access reviews	
Admin consent requests (Preview	() Convent request expires after (days) () 30
subleshooting + Support	Office 365 Settinge
Virtual assistant (Preview)	Autor and actually

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

consent@501.sailpointtechn	ologies.com
Approval required	d
SailPoint IdentityIQ Fi Azure Connector	le Access Manager -
This app requires your admir	n's approval to:
Read directory data	
Enter justification for reques	ting this app
Sign in with another account	1

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

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



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

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

P.C. Manager and an other states of the stat					
Overview		O Refresh 🛛 🛇 Got feedback?		1600	
0 Austriau		Application	Application ID		
Disanate and take problem:		SeliPoint Identity/Q File Access Manager - Azure Connecto	dba619ad-633e-4b31-9da2-ba2495fe9cc5	Select an application to review who requested access. After selecting an application, you will be	
A pageos and sove provents				able to approve, block, or deny the admin	
Manage	- 1	Details			~
All applications					
Application proxy		Review permissions and consent Solock X Deny			
Ø User settings		Request details Requested by Help			
Security					
Conditional Access		Application name	Reply URL	How to enable access	
Consent and permissions		SalPoint Identity/Q File Access Manager - Azure Connector	https://oauth.whiteboxsecurity.com/Callback.aspx	This application requires an administrator to consent. Select Review permissions and consent to see what	
		Homepage URL		permissions are being requested and grant admin	
Activity					
3 Sign-ins					
sa Usage & insights (Preview)					
Audit logs					
Provisioning Togs (Preview)					
Access reviews					
 Admin consent requests (Preview 	n9				
Troubleshooting + Support					
🖤 Virtual assistant (Preview)					
Rev support request					

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:

admin@501.sailpoir	nttechnologies.com
Permissions Accept for y	requested our organization
SailPoint Iden Azure Connec unverified	ntityIQ File Access Manager - ctor
This application is your organization.	not published by Microsoft o
This app would like	to:
✓ Read directory dat	ta
If you accept, this app wi all users in your organiza review these permissions	Il get access to the specified resources tion. No one else will be prompted to
Accepting these permissi your data as specified in statement. The publishe for you to review. You o https://myapps.microsoft	ions means that you allow this app to u their terms of service and privacy r has not provided links to their term an change these permissions at tcom. Show details

After an administrator Accepts, non-administrator users will have to go the through token generation sequence again.

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

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