ManageEngine ADSelfService Plus

How to secure

Microsoft Outlook Desktop Applications using MFA



Table of Contents

How to secure Microsoft Outlook using MFA	— 1
Process flow	— 1
Prerequisites	_ 2
Configuration Steps	- 2
AD FS configuration for modern authentication	— 3
Configuring the on-premises Exchange Server	— 11
Configuring the Outlook client on users' Windows machines	— 13
Enabling modern authentication on Outlook	— 14
Adding the AD FS domain as a trusted domain	— 14
Configuring MFA for Outlook using ADSelfService Plus	— 16
Prerequisite	— 16
Set up ADSelfService Plus to authenticate Outlook users	— 17
Configure the AD FS server to delegate authentication to ADSelfService Plus	— 19
Step 1: Adding a new claims provider trust	— 19
Step 2: Adding claims rules	— 22
Step 3: Executing Windows PowerShell commands	— 27
Reference Documentation	— 31

How to secure Microsoft Outlook using MFA

Modern authentication enables users to authenticate to Exchange using AD FS. When enabled, the Outlook client redirects users to AD FS, which authenticates their identity and generates access tokens that are subsequently validated by Exchange Server to grant users access to their mailboxes.

AD FS uses basic Active Directory authentication to verify users. This document details how to secure this authentication process by incorporating an extra layer of MFA from ManageEngine ADSelfService Plus.

Process flow

Instead of AD FS using Active Directory to authenticate the user, you can configure AD FS to utilize ADSelfService Plus for user authentication. By doing so, you can leverage ADSelfService Plus' suite of modern MFA factors to enhance the overall security of the authentication process. This is achieved by configuring ADSelfService Plus as the identity provider (IdP) for AD FS.

This diagram illustrates the process:



- 1. A user provides their email address to their Outlook client.
- 2. Outlook connects to Exchange Server.
- 3. Exchange Server requests modern (OAuth) authentication from AD FS.
- 4. AD FS now redirects the authentication request to ADSelfService Plus via SAML.
- 5. ADSelfService Plus performs the actual authentication by presenting the user with MFA.
- 6. Upon successful MFA, ADSelfService Plus returns a SAML assertion response to AD FS. After validating the SAML response from ADSelfService Plus, AD FS issues an access token to Outlook.
- 7. Outlook tries accessing Exchange Server with the access token from AD FS.
- 8. If the access token is valid, Exchange Server now allows Outlook access to the user's mailbox.

Prerequisites

- Exchange Server 2019 CU13 or later (Exchange Server 2016 supported with 2019 CU13 as the front-end server)
- AD FS for Windows Server 2019 or later
- Outlook 2021 (version 2304 or later) from the Microsoft 365 suite on machines running Windows 11 22H2 or later (ensure that update KB5023706 for version 22H2 is installed).

Note:

- The latest version of Outlook for Windows (version 1.2024.605.100) in the Microsoft Store does not support on-premises Exchange Server. Microsoft might add on-premises Exchange Server support for these versions later.
- Modern authentication to an on-premises Exchange server for clients such as Outlook for Mac, Outlook for iOS and Android, and the Apple Mail app for iOS, is yet to be added by Microsoft.

Detailed prerequisites for setting up modern authentication for Exchange Server, AD FS, the Outlook client, and Windows can be viewed <u>here</u>.

Configuration Steps

You will need to configure the following for modern authentication:

- <u>AD FS</u>
- On-premises Exchange Server
- The Outlook client on the user's Windows machine

Once these have been configured, you will need to configure

MFA for Outlook using ADSelfService Plus

AD FS configuration for modern authentication

1. Ensure that AD FS is functioning properly by accessing your metadata URL from a browser bar.



You can find the steps to access your metadata URL <u>here</u>. It should be in this format: <u>https://<ADFS_Server_FQDN>/federationmetadata/2007-06/federationmetadata.xml</u>. If AD FS is functioning properly, your federation metadata will be downloaded as an XML file.

 Open Server Manager on your Windows server and navigate to Tools > AD FS Management.
 In the AD FS console that opens, click on Edit Federation Service Properties to open the Federation Service Properties pop-up.

Image: AD FS Image: File Action View Window Help Image: Action		- 0 × - @ x
AD FS	AD FS	Actions
Service Access Control Policies	2 martine	AD FS
Relying Party Trusts	Overview	Add Relying Party Trust
Claims Provider Trusts	Active Directory Federation Services provides single-sign-on (SSO) access for client computers.	Add Claims Provider Trust
Application Groups	Learn More About AD FS	Add Attribute Store
	What's new in AD FS?	Add Application Group
	AD FS Deployment Guide	Edit Federation Service Properties
	AD FS Operations Guide	Edit Published Claims
	Integrate Azure Multi Factor Authentication with AD ES	Revoke All Proxies
	Monitor AD InSistence using Azure Active Directory Connect Health	View 🕨
	Learn More About Azure Active Directory	New Window from Here
	Azure Active Directory, a seperate online service, can provide simplified identity and access management, security reporting and single sign-on to cloud and on-premises web apps.	G Refresh
	What is Azure Active Directory?	Help
	Extend your directory to Azure Active Directory	
	Identity and Access Management	

3. Choose an appropriate **web SSO lifetime** to determine the number of minutes after which the user has to re-authenticate. Click **Apply** and then **OK** to close the pop-up.

	Organization Events	
Feder	ation Service display name:	
SSP	ADFS	
Exam	ple: Fabrikam Federation Service	
Feder	ration Service name:	
adfs.a	adssp.com	
Exam	ple: fs.fabrikam.com	
Feder	ration Service identifier:	
http:/	/adfs adsen com/adfs/senvices/tnust	
Evan	ale: http://fa.fahil.am.com/adfa/consisce.fn.ut	
Exam		
Web	SSO lifetime (minutes): 10 😴	
□ Er	nable delegation for service administration	
D	elegate name:	
_		Cda
	ow Local System account for service administration	
	ow Local System account for service administration	
AI N	low Local System account for service administration ow Local Administrators group for service administration	
AI	low Local System account for service administration ow Local Administrators group for service administration	
AI	low Local System account for service administration	
AI	low Local System account for service administration low Local Administrators group for service administration	

4. In the LHS pane, navigate to ADFS > Service > Device Registration. Verify that device registration is configured and device authentication is enabled. This step is recommended to reduce the number of authentication prompts for users and can help enforce Access Control Policies in AD FS.

on View Window Help		
	Device Registration	Actions
ibute Stores	Device Designation Councilous	Device Registration
hentication Methods	Device Registration Overview	Edit Access Control Policy
ificates	Now users to register devices with Active Likectory.	Properties
m Descriptions ice Registration	Satus	View
points	Device registration is configured and device authentication is enabled.	New Window from Here
pe Descriptions		@ Refresh
Control Policies	Disable device authentication	👔 Help
Party Trusts Provider Trusts tion Groups	Supported Account Formats Device registration is configured for the following user account formats. To allow additional account formats, see "Configuring Device Registration", someone@edutp.com	
	Learn More Reming for Device Registration Configure Device Registration an E Fue	

- 5. Configure an application group for modern authentication in Outlook on Windows:
 - a. Right-click on Application Groups and click Add Application Group.

🧌 AD FS			-	- 0 ×
🗌 File Action View Window Help				- 8 ×
🗢 🔿 🙍 🖬				
AD FS	Application Groups		Actions	
✓ Service	Name	Description	Application Groups	
Attribute Stores	Outlook		Add Application Group	
Certificates			View	
Claim Descriptions			VIEW	,
Device Registration			New Window from Here	
Endpoints			G Refresh	
Scope Descriptions			🛛 Help	
Web Application Proxy				
Relying Party Trusts				
Claims Provider Trusts				
Application Grouns				
Add Application Group	o			
View	>			
New Window from Her	re			
Refresh				
Help				

b. The Add Application Group wizard will open. Under Template, select Native Application accessing a web API and type an appropriate name for the application, such as *Outlook*. Click Next.

Madd Application Group W	fizard X
Welcome	
Steps	Name:
Welcome	Outlook
 Native application 	Description:
Configure Web API	
 Apply Access Control Policy 	
 Configure Application Permissions 	Template:
Summary	Client-Server applications
 Complete 	Native application accessing a web API
	Server application accessing a web API
	Web browser accessing a web application
	Standalone applications
	2 Native application
	Server application
	See Web API
	More information
	< Previous Next > Cancel

- c. In the Native application section, add the following client identifier and Redirect URI and click Next:
- Client Identifier: d3590ed6-52b3-4102-aeff-aad2292ab01c
- Redirect URI (add both of these URIs):
 - urn:ietf:wg:oauth:2.0:oob
 - ms-appx-web://Microsoft.AAD.BrokerPlugin/d3590ed6-52b3-4102-aeff-aad2292ab01c

🍿 Add Application Group W	fizard	×
Native application		
Steps	Name:	
Welcome	Outlook - Native application	
Native application	Client Identifier	
Configure Web API	d2500cdC 52b2 /102 coff cod2202cb01c	
 Apply Access Control Policy 	03550600520541024611480225280010	
 Configure Application 	Redirect URI:	
Permissions	Example: https://Contoso.com	Add
Summary	um.ietf.wg:oauth:2.0:oob	Remove
 Complete 	ms-appx-web://Microsoft.4AD.BrokerPlugin/d3590ed6-52b3-4102-aeft-aad2292ab01c	
	D	
	Description:	
	< Previous Next >	Cancel

d. In the **Configure Web API** section, add all the FQDNs used by your Exchange environment,

including auto-discover, load balancing, and server FQDNs. For example:

- https://autodiscover.mydomain.com/
- https://mail.mydomain.com/

onfigure Web API		
teps	Name:	
Welcome	Outlook - Web API	
Native application	dentifier:	
Configure Web API		Add
Apply Access Control Policy		700
Configure Application Permissions	https://autodiscover.mydomain.com/ https://mail.mydomain.com/	Remove
Summary		
Complete		
	Description:	

Note:

Include all the client-facing URLs for the setup to work properly. Ensure that the URLs start with **https://** and contain a trailing forward slash (/).

e. In the **Apply Access Control Policy** section, select **Permit everyone**. You can change this later if needed. **Leave the checkbox** at the bottom of the page unchecked. Click **Next.**

teps	Choose an access control policy:	
Welcome	Name	Description
Native application	Pomit oververe	Grant appears to even app
Configure Web API	Permit everyone and require MFA	Grant access to everyone and remain MEAf
Apply Access Control Policy Configure Application	Permit everyone and require MFA for specific group Permit everyone and require MFA from extranet access Permit everyone and require MFA from unauthenticated	Grant access to everyone and require MFA f Grant access to the intranet users and requir Grant access to everyone and require MFA f
Permissions	Permit everyone and require MFA, allow automatic devi	Grant access to everyone and require MFA f
Summary	Permit everyone for intranet access	Grant access to the intranet users.
	Policy Permit everyone	

f. In the **Configure Application Permissions** section, choose **Native application**. Under Permitted scopes, select **user_impersonation** in addition to **openid**, which is selected by default.

Steps	Configure permission	s to enable client applications to access this Web API		
Welcome	Client application (cal	ller):		
 Native application Configure Web API Apply Access Control Policy 	Name Outlook - Native ap	Description		
Configure Application Permissions				
Summary Complete				
			Add	Remove
	Permitted scopes:			

- g. Click **Next** and complete the setup to create the application group.
- 6. Add Issuance Transform Rules to the newly created application group:
 - a. Right-click on the Outlook application group and select **Properties.**

Image: Window Help Image: Help <th></th> <th></th> <th>- 0 × - 0 ×</th>			- 0 × - 0 ×
ad FS	Application Groups		Actions
Service Attribute Starser	Name 👻	Description	Application Groups
Authorite stores	Outlook		Add Application Group
Certificates		Properties	View 🕨
Claim Descriptions		Delete	New Window from Here
Endpoints		Help	C Refresh
Scope Descriptions			👔 Help
Access Control Policies			Outlook 🔺
Relying Party Trusts			Properties
Application Groups			🗙 Delete
			👔 Help

b. Click Edit under Web API settings.

Outlook Properties	
Name:	
Outlook	
Description:	
Applications:	,
Name	Description
Native application	
Outlook - Native application	
Web API	
Outlook - Web API	
Add application	Edit Remove

c. Under Issuance Transform Rules, click Add Rule.

outiook		linopenies		1	
Identifiers	Notes	Access control policy	Issuance Transform Rules	Client Permissior	ns
The follo	wing trar	nsform rules specify the	claims that will be sent to the r	elying party.	
Order	Rule Na	ame	Issued Claims		
					~
Add R	ule	Edit Rule Ren	nove Rule		
			01/		

d. In the **Choose Rule Type** section, select **Send Claims Using a Custom Rule** from the *Claim rule template* drop-down.

Steps	Select the template for the claim rule that you want to create from the following list. The description provides
Choose Rule Type	details about each claim rule template.
 Configure Claim Rule 	Claim rule template: Send Claims Using a Custom Rule Send Claims Using a Custom Rule Send Group Membership as a Claim Transform an Incoming Claim Pass-Through or Fitter on Incoming Claim Pass Through or Fitter on Incoming Claim Send Claims Using a Custom Rule • Sending claims from a SQL attribute store using a custom LDAP filter • Sending claims from a LDAP attribute store using a custom LDAP filter • Sending claims from a custom attribute store • Sending claims only when 2 or more incoming claim are present • Sending claims only when an incoming claim value matches a complex pattern • Sending claims with complex changes to an incoming claim value • Creating claims for use only in later rules

e. Click Next to proceed to the Configure Claim Rule section using the information in the table below.

Claim Rule Name	Custom Rule
ActiveDirectoryUserSID	c:[Type == "http://schemas.microsoft.com/ws/2008/06/ identity/claims/primarysid"] => issue(claim = c);
ActiveDirectoryUPN	c:[Type == "http://schemas.xmlsoap.org/ws/2005/05/ identity/claims/upn"] => issue(claim = c);
AppIDACR	=> issue(Type = "appidacr", Value = "2");
SCP	=> issue(Type = "http://schemas.microsoft.com/identity/ claims/scope", Value ="user_impersonation");

You will need to configure each claim rule individually, as shown in the screenshot below. Click **Finish** to add each claim rule.

🏟 Add Transform Claim	Rule Wizard
Configure Rule	
Steps Configure Rule Type Configure Claim Rule	You can configure a custom claim rule, such as a rule that requires multiple incoming claims or that extracts claims from a SQL attribute store. To configure a custom rule, type one or more optional conditions and an issuance statement using the AD FS claim rule language. Claim rule name: ActiveDirectoryUserSID Rule template: Send Claims Using a Custom Rule Custom rule: C: [Type == "http://schemas.microsoft.com/ws/2008/06/identity/claims/primarysid"] > issue (claim = c);

After adding the rules, the **Issuance Transform Rules** tab should look similar to the following screenshot:

lentifiers	Notes	Access control policy	Issuance T	ransform Rules	Client Perm	issions
The follo	wing tran	sform rules specify the	claims that wi	I be sent to the	relying party.	
Order	Rule Na	ame		Issued Claims		
1	ActiveD	lirectoryUserSID		<see claim="" rule<="" td=""><td>e></td><td></td></see>	e>	
2	ActiveD	lirectoryUPN		<see claim="" rule<="" td=""><td>e></td><td></td></see>	e>	
3	AppIDA	CR		<see claim="" rul<="" td=""><td>e></td><td></td></see>	e>	
4	SCP			<see claim="" rul<="" td=""><td>e></td><td></td></see>	e>	
						4
						ᠿ
						•
						☆
						↑
						•
						\$ \$
Add F	Rule	Edit Rule Ren	nove Rule			•

f. Click **Apply** and then **OK** to save your configuration. AD FS has now been configured for modern authentication.

Configuring the on-premises Exchange Server

By default, the on-premises Exchange server utilizes basic authentication. To enable MFA instead of basic authentication, we must configure the on-premises Exchange server to employ modern authentication (OAuth) via AD FS, for users accessing Exchange through Outlook.

This involves four steps:

- 1. Verifying that the virtual directories on your Exchange server are configured to use OAuth.
- 2. Registering your AD FS server as the authentication server.
- 3. <u>Setting the AD FS server as the default authorization endpoint.</u>
- 4. Enabling modern authentication at the organizational level.

You will need to use the Exchange Management Shell on your Exchange server to configure these settings. You can find information on using the Exchange Management Shell <u>here</u>.

1. Verify that the virtual directories in your Exchange server are configured to use OAuth.

On your Exchange server, open the Exchange Management Shell and run the following commands:

Get-MapiVirtualDirectory -Server <ExchangeServerName> | Format-List *auth* Get-WebServicesVirtualDirectory -Server <ExchangeServerName> | Format-List *auth* Get-OabVirtualDirectory -Server <ExchangeServerName> | Format-List *auth* Get-AutodiscoverVirtualDirectory -Server <ExchangeServerName> | Format-List *auth*

Note: Replace < ExchangeServerName> with your the name of your Exchange server.

Each command retrieves the authentication settings for the specified virtual directory type on the given Exchange server. Verify that **OAuth** is an authentication method for each virtual directory type.

I Machine:	
[PS] C:\>Get-MapiVirtualDirect	cory -Server
IISAuthenticationMethods	: {OAuth, Negotiate}
InternalAuthenticationMethods	: {OAuth, Negotiate}
ExternalAuthenticationMethods	: {OAuth, Negotiate}
	Johnstein Course - to to I Course Link South®
[PS] C:\>Get-webServicesvirtua	IDIrectory -Server
CentificateAuthentication	
InternalAuthenticationMethods	·{Ntlm_WindowsIntegrated_WSSecurity_ΩΔuth}
ExternalAuthenticationMethods	: {Nt]m, WindowsIntegrated, WSSecurity, OAuth}
LiveIdNegotiateAuthentication	:
WSSecurityAuthentication	: True
LiveIdBasicAuthentication	: False
BasicAuthentication	: False
DigestAuthentication	: False
WindowsAuthentication	: True
OAuthAuthentication	: True
AdfsAuthentication	: False
	Land Converting to the south state of the south sta
[PS] C:\>Get-OabvirtualDirecto	pry -Server Format-List *auth*
BasicAuthentication	: False
WindowsAuthentication	: True
OAuthAuthentication	: True
InternalAuthenticationMethods	: {WindowsIntegrated, OAuth}
ExternalAuthenticationMethods	: {WindowsIntegrated, OAuth}
[PS] C:\>Get-AutodiscoverVirtu	alDirectory -Server
Tatana 1 Authoritication Matheda	(Design Mtlm, MindeusTatespation, MCCosumity, DAuth)
InternalAuthenticationMethods	: {Basic, Ntim, WindowsIntegrated, WSSecurity, OAuth}
LiveIdNegetisteAuthentication	: {basic, wiim, windowsintegrated, wssecurity, OAuth}
WSSecurityAuthentication	
LiveIdBasicAuthentication	: False
BasicAuthentication	: True
DigestAuthentication	: False
WindowsAuthentication	: True
OAuthAuthentication	: True
AdfsAuthentication	: False

2. Register your AD FS server as the authentication server

Machines

Windows\system32>N

Exchange accepts OAuth tokens only from authentication servers (AD FS servers). Register your AD FS server as the authentication server for Exchange using the following command:

New-AuthServer -Type ADFS -Name <MyADFSServer> -AuthMetadataUrl https://<adfs server FQDN>/FederationMetadata/2007-06/FederationMetadata.xml

Note: Replace *<MyADFSServer>* and *<ADFS* server FQDN> with the name of your AD FS server (this will serve as an identifier for Exchange Server) and the FDQN of your AD FS server, respectively.

adata.xml_

3. Set your AD FS server as the default authorization endpoint

When an Outlook client requests modern authentication from Exchange, Exchange responds with the authorization URL of the DefaultAuthorizationEndpoint. Set the AD FS server you created as the DefaultAuthorizationEndpoint:



4. Enable modern authentication at the organizational level

Finally, enable modern authentication for your organization with the following command:

Set-OrganizationConfig -OAuth2ClientProfileEnabled \$true

Machine
 Machine
 PS
 C:\Windows\system32>Set-AuthServer -Identity MyADESServer -IsDefaultAuthorizationEndpoint \$true
 [PS] C:\Windows\system32>
 [PS] C:\Windows\system32>

After completing the steps above, users logging into the on-premises Exchange server from their Outlook mail client on Windows will be prompted with modern authentication via AD FS.

Configuring the Outlook client on users' Windows machines

By default, Outlook for Windows and the Outlook app in the Microsoft 365 suite use the Windows Credential Prompt for authentication. Since modern authentication via AD FS is disabled for Outlook by default, we need to enable modern authentication and delegate authentication to AD FS. To do this, we will:

- Enable modern authentication via AD FS for Outlook
- Add AD FS as a trusted domain

Enabling modern authentication on Outlook

By enabling modern authentication on Outlook, we will enable authentication via a browser instead of the default Windows Credential Prompt. This step involves modifying the registry on client machines.

1. To enable modern authentication via AD FS for Outlook on Windows, add the following **REG_DWORD** hex value to **HKCU\SOFTWARE\Microsoft\Office\16.0\Common\Identity**

Name	Value
EnableExchangeOnPremModernAuth	1

📑 Regist	try Editor				-	D	×
File Edit	View	Favorites Help					
Computer	\HKEY_C	URRENT_USER\Software\Microsoft\0	Office\16.0\Common\Identity				
	· · · · · · · · · · · · · · · · · · ·	Charting ClientTelemetry CloudPolicy ContactCard CustomUIValidationCache DocumentActivityCapabilities Draw	Name	Туре	Data		
		DrawAlerts DRM Experiment ExperimentConfigs ExperimentEcs FavoritePens FileIO FikedFormat Fluid Fonts General Graphics HelpViewer	2000 EnableExchangeOnPremModernAuth	REG_DWORD	0x0000001 (1)		
		Identity DocToldMapping DocToldMapping Identities OneAuthConfigCache Profiles ServiceAuthInfoCache SPOConkieCache				_	

Adding the AD FS domain as a trusted domain

By adding AD FS as a trusted domain, we enable Outlook to delegate modern authentication to AD FS. This is disabled by default; please follow the steps below to enable it:

- Open the Windows Registry Editor on the end-user machine. Navigate to HKEY_LOCAL_MACHINE\ SOFTWARE\Policies\Microsoft\. Create a folder called AAD and under it, a subfolder called AuthTrustedDomains.
- 2. Right-click **AuthTrustedDomains** and click on **New > Key**. A subfolder named *New Key #1* will be created.



- 3. Rename *New Key #1* as your AD FS domain URL. Create another key and rename it to your AD FS domain URL, and append a forward-slash (/) to it.
 - i.e., these changes must be in the following format:

i. HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\AAD\AuthTrustedDomains\

- <ADFS domain URL>
- ii. HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\AAD\AuthTrustedDomains\
 - <ADFS domain URL>/

Replace <ADFS domain URL> with your AD FS domain URL.



Note: For ease of deployment, these registry changes can be configured on end-user machines using a Group Policy.

Configuring MFA for Outlook using ADSelfService Plus

Now, you should configure AD FS to delegate user authentication to ADSelfService Plus, thus integrating an additional layer of MFA.

- Set up ADSelfService Plus to authenticate Outlook users
- <u>Configure the AD FS server to delegate authentication to ADSelfService Plus</u>

Prerequisite

Download and save the AD FS server federation metadata by using the following URL in a browser:

https://<adfs_fqdn>/FederationMetadata/2007-06/FederationMetadata.xml

Note: Replace <ADFS server FQDN> with the FDQN of your AD FS server.

۲	https:// adfs.mydomain.com /FederationMetadata/20	07-06/FederationMetadata.xml		
	O d D	You thers who use this device won't set hange how data is collected by wet lownloads, bookmarks and reading	Ve gone Incognito e your activity, so you can browse more privately. This won't posites you visit and the services they use, including Google. list items will be saved. <u>Learn more</u>	
	ci • •	hrome won't save: Your browsing histony Cookies and site data Information entered in forms	Your activity might still be visible to: • Websites you visit • Your employer or school • Your internet service provider	
		Block third-party cookies When on, sites can't use cookies sites may break.	that track you across the web. Features on some 🛛 💽	

Set up ADSelfService Plus to authenticate Outlook users

- 1. Log in to ADSelfService Plus as an administrator.
- 2. Now, navigate to Configuration > Self-Service > Password Sync/Single Sign On > Add Application > Custom Application.
- 3. Enter the Application Name, Description, and Domain Name in the respective fields.
- 4. Choose the policy containing the users you wish to provide SSO access to AD FS from the **Assign Policies** drop-down.
- 5. Select the checkbox Enable SSO using SAML.
- 6. Set Support SSO flow to SP initiated.
- 7. In the Upload Metadata field, upload the file downloaded previously in the prerequisite step.
- 8. Under **Provider Settings**, enter the following information:
 - a. Select **RSA-SHA256** from the **RSA SHA Algorithm** drop-down.
 - b. Set the SAML Response value to Signed.
 - c. Select the option **Exclusive Canonicalization** from the **Canonicalization Method** drop-down.
 - d. Click Advanced in the top-left corner.

Search	Q	Create Custom Application ⑦		C Back
All Applications (125)	×	* Application 1	ame ADFS Description	dP Details
All		* Domain P	ame demo.com	
Productivity	48	* Assign Bo	All Policies Selected	
IT Management	31	Assign Po		
Customer Support	5	Small	Icon Browse Logo Browse	
CRM	7		Program Lines Press	
Analytical Tools	6	Large	JPG, JPEG, GIF or PNG; Max Dimension: 125 x 40, Size 250KB.	
Education Site Management	8	SAML OAuth/OpenID Connec		
Messaging Apps	6			
HR Management	7	Enable SSO Using SAML		
		Support SSO Flow	SP Initiated v	
 Custom Application 	,	* Upload Metadata	FederationMetadata.xml Browse	
			OR	
		* SAML Redirect URL	https://selfservice.com/adfs/ls/	
		ACS URL	https://selfservice.com/adfs/ls/	
			Provider Settings -	
		RSA SHA Algorithm	RSA-SHA236 V 🕐	
		SAML Response	SIGNED 🗸 🕐	
		Canonicalization Method	Exclusive Canonicalization 🗸 🕐	
			Create Custom Application Cancel	

- 9. Under the SAML Assertion Attributes Configuration section, create an attribute and enter the following values:
 - a. Enter an attribute name as "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn" and choose **userPrincipalName** for the **Value** drop-down.
 - b. Add another attribute name as "http://schemas.microsoft.com/ws/2008/06/identity/claims/ primarysid" and choose **objectSid** from the **Value** drop-down.

Note: You will need to create a custom attribute called **objectSid** to do this:

- Navigate to Configuration > Self-Service > Directory Self-Service.
 Click on Manage Custom Attributes at the top-right corner and create a custom attribute called objectSid.
- Link it to the *objectSid* AD attribute by entering *objectSid* in the LDAP field. Choose **Unicode String** as the datatype. Click **Add**.

Display Name	objectSid	?	
LDAP Name	objectSid	?	
Data Type	Unicode String	•	
	Update Cancel		

c. Add yet another attribute name as "http://schemas.microsoft.com/ws/2008/06/identity/claims/ windowsaccountname" and choose **sAMAccountName** from the **Value** drop-down.

-					(
AML Assertion Attributes	s Configuration				(
Assertion Attribute	Attributes Value				
	http://schemas.xmlsoap.org/ws/	userPrincipalName	~	+ 🗙	
	http://schemas.microsoft.com/w	objectSid	~	+ ×	
	http://schemas.microsoft.com/w	sAMAccountName	~	+ 🗙	
Note • When a SAM the user is a Use the abo provider, to	AL assertion is sent to the service prov authenticated. ve setting to add certain attributes, th the SAML assertion, that will override	ider, the identity provider asserts th at are required by the service the default attributes (first name, la	ast		

Click Save to go back to the Create Custom Application page.

10. Click **IdP details** at the top-right corner and select **Download IdP Metadata**, which will download the metadata file required for later.

dP Details
SSO (SAML)
A Please configure the application with IdP details given below to complete the setup. Help
Entity ID https://adselfserviceplus.com/iamapps/ssologin/custom_saml_a
Login URL https://adselfserviceplus.com/iamapps/ssologin/custom_saml_a
Logout URL https://adselfserviceplus.com/iamapps/ssologout/custom_saml_
SHA1 FingerPrint b9:42:5f:5d:df:8b:05:31:a3:7a:90:9d:dd:65:f0:c6:92:23:27:c
Download X.509 Certificate Download IdP Metadata
Close

Configure the AD FS server to delegate authentication to ADSelfService Plus

Configuring the AD FS server to delegate authentication to ADSelfService Plus involves the following steps:

- Adding a new claims provider trust
- Adding claim rules
- <u>Executing Windows PowerShell commands</u>
- Enabling MFA for cloud apps in ADSelfService Plus

Step 1: Adding a new claims provider trust

Open Server Manager on your Windows server and navigate to Tools > AD FS Management.
 In the AD FS console that opens, navigate to AD FS > Claims Provider Trusts.

🎕 AD FS 🎕 File Action View Window Help			- 0 ×
A PS Constraint of the service Access Control Policies Access Control Policies Access Control Policies Cham Provider Trusts Application Groups	Claims Provider Trusts Doplay Name Active Dectory ADSSP IdP	Enabled Yes Yes	Actions Claims Provider Trusts Add Claims Provider Trust View New Window from Here Refresh
			Help Active Directory Update from Federation Metadata Edit Claim Rules Disable Properties Help

2. Click Add Claims Provider Trust in the Actions pane. This will open the Add Claims Provider

Trust Wizard. Click Start.

Image: AD FS Image: File Action View Window Help Image: File Action View Window Help			- 0 ×
 File Action View Window Help File Action View Window Help File Action Policies Service Duplay Name Relying Party Trutts Claims Provider Trutts Application Groups 	Trusts ory Add Claims Provider In Welcome Seps • Welcome • Select Data Source • Reedy to Add Trust • Prish	Enabled Yes Yes at Wicard	Actions Claims Provider Trust. Add Claims Provider Trust View New Window from Here Refeah Help Active Directory Active Directory Disable Properties B Help

 In the Select Data Source section, choose Import data about the claims provider from a file and upload the metadata file downloaded in <u>Step 11</u> of the ADSelfService Plus configuration steps. Click Next.

TT 2 FT			
C	laims Provider Trusts		Actions
Control Policies	Display Name	Enabled	Claims Provider Trusts
g Party Trusts	Active Directory	Yes	Add Claims Provider Trust
Provider Trusts	ADSSP IdP	Yes	View
ation Groups			New Window from Here
			Q Refresh
	Madd Claims Provider 1	Frust Wizard X	👔 Help
	Select Data Source		Active Directory
	Steps	Select an option that this wizard will use to obtain data about this claims provider:	Update from Federation Metadata
	Welcome		Edit Claim Rules
	Select Data Source	Use this option to import the percessary data and certificates from a claims provider organization that	Disable
	 Ready to Add Trust 	publishes its federation metadata online or on a local network.	Properties
	Final	Federation metadata address frost name or UFLU: Example: fs fabrikam com or https://fs fabrikam.com/ Texter blance in the second of the sec	Ka Help
		< Previous Next > Cancel	

VIII ES			
The Action View Window Help			- U X
			000
AD FS	Claims Provider Trusts		Actions
> Service	Display Name	Enabled	Claims Provider Trusts
Access Control Policies Relving Party Trusts	Active Directory	Yes	Add Claims Provider Trust
🖳 Claims Provider Trusts	ADSSP IdP	Yes	View 🕨
Application Groups			New Window from Here
			Q Refresh
	🗌 Add Claims Provider Tr	ust Wizard X	Help
	Specify Display Nam	e	Active Directory
		Time the simpley name and any actional actor for this slatter any idea	Update from Federation Metadata
	Steps	Type the display name and any optional notes for this claims provider.	Edit Claim Rules
	Salast Data Sauma	ADSSP Identity Provided	Disable
	Snecify Display Name		Properties
	Ready to Add Trust	Notes:	Help
	Finish		
		· · ·	
		< Previous Next > Cancel	
1	1		
N AD FS			
🧌 File Action View Window Help			- 0 ×
			- 8 ×
🔶 🕪 🖄 📰 🔢 🖬			- 0 × - 0 ×
← ➡ 2 〒 2 〒	Claims Provider Trusts		- C ×
← ➡ 2	Claims Provider Trusts	Ender	Actions Chims Provider Trusts
AD FS Service Access Control Policies Access Control Policies	Claims Provider Trusts Display Name Active Directory	Enabled Yes	Actions Claims Provider Trusts Add Claims Provider Trust
	Claims Provider Trusts Display Name Active Directory ADSSP IdP	Enabled Yes Yes	Actions Claims Provider Trusts Add Claims Provider Trust
	Claims Provider Trusts Daplay Name Active Directory ADSSP IdP	Enabled Yes Yes	Actions Claims Provider Trusts Add Claims Provider Trust View New New Ne
AD FS Strvice AA Access Control Policies Relying Party Trusts Claims Provider Trusts Application Groups	Claims Provider Trusts Display Name Active Deectory ADSSP IdP	Enabled Yes Yes	Actions Claims Provider Trusts Add Claims Provider Trust View New Window from Here
Ap FS Service Access Control Policies Relying Party Trusts Claims Provider Trusts Application Groups	Claims Provider Trusts Daplay Name Active Directoy ADSSP IdP	Enabled Yes Yes	Actions Claims Provider Trusts Add Claims Provider Trust View New Window from Here Refresh Refresh
Application Groups	Claims Provider Trusts Display Name Active Directory ADSSP IdP	Enabled Yes Yes	Actions Claims Provider Trusts Add Claims Provider Trust View New Window from Here Refresh Help Help
AD FS Service Access Control Policies Reying Party Trusts Claims Provide Trusts Application Groups	Claims Provider Trusts Display Name Active Directory ADSSP IdP	Tust Wizard X	Actions Claims Provider Trusts Add Claims Provider Trust View New Window from Here Refereh Help Active Directory
Image: AD FS Image: Source Image: Access Control Policies Image: Reving Party Trusts Image: Application Groups	Claims Provider Trusts Display Name Active Directory ADSSP IdP Contemport Ready to Add Trust Steps	Tust Wizerd X	Actions Claims Provider Trust View New Window from Here Refresh Help Active Directory Update from Federation Metadata
AP 5 Service Access Control Policies Relying Party Trusts Claims Provider Trusts Claims Application Groups	Claims Provider Trusts Display Name Active Directoy ADSSP IdP Active Directoy ADSSP IdP	Enabled Yes Yes Trust Wizard X The clarms provider trust has been configured. Review the following settings, and then click. Next to add the clarms provider trust to the AD FS configuration database.	Actions Claims Provider Trusts Add Claims Provider Trust View New Window from Here Refresh Help Active Directory Update from Federation Metadata Edit Claim Rules
Acess Control Policies Access Control Policies Relying Party Trusts Claim Porder Trusts Application Groups	Claims Provider Trusts Display Name Active Disology ADSSP IdP	Enabled Yes Yes Trust Wizard X The dams provider trust has been configured. Review the following settings, and then click. Next to add the cleans provider trust to the AD FS configured. Review the following settings, and then click. Next to add the cleans provider trust to the AD FS configured. Review the following settings.	Actions Claims Provider Trusts Add Claims Provider Trust View New Window from Here Refresh Help Active Directory Update from Federation Metadata Edit Claim Rules Disable
Image: Service Image: AD FS Image: Service Image: Access Control Policies Image: Reving Party Trusts Image: Claims Provider Trusts Image: Application Groups	Claims Provider Trusts Display Name Active Directory ADSSP IdP Control Add Claims Provider T Ready to Add Trust Steps Welcome Steps Step	Enabled Yes Yes Trust Wizard X The clams provider trust has been configured. Review the following settings, and then click. Next to add the clams provider trust to the AD FS configuration database.	Actions Claims Provider Trusts Add Claims Provider Trust View New Window from Here Refresh Help Active Directory Update from Federation Metadata Edit Claim Rules Disable Properties
Image: Application Groups	Claims Provider Trusts Display Name Active Directoy ADSSP IdP	Enabled Yes Yes Tust Wizard X The clams provider trust has been configured. Review the following settings, and then click. Next to add the clams provider trust to the AD FS configuration database. Montoring Identifier Cestificates Encoption Offered Clams Organization Endpoints Note * X Specify the trust montoring settings for this claims provider trust. Open consider leader are set at 1810	Actions Claims Provider Trust Claims Provider Trust View New Window from Here Refresh Help Active Directory Update from Federation Metadata Edit Claim Rules Disable Properties Refresh Re
Image: Application Groups	Claims Provider Trusts Display Name Active Directoy ADSSP IdP	Enabled Yes Yes Trust Wizard X The clams provider trust has been configured. Review the following settings, and then click Next to add the clams provider trust to the AD FS configuration database. Monitoring identifies Centificates Encoption Offered Clams Organization Endpoints Note () Specify the trust monitoring atertings for this claims provider trust. Claims provider's federation metadata URL:	Actions Claims Provider Trust View Add Claims Provider Trust View Mindow from Here Refresh Help Active Directory Update from Federation Metadata Edit Claim Rules Disable Properties Help Help
Image: Service Image: AD FS Image: Service Image: Access Control Policies Image: Reving Party Trusts Image: Claims Provider Trusts Image: Application Groups	Claims Provider Trusts Display Name Active Directory ADSSP IdP	Enabled Yes Yes Trust Wizard X The claims provider trust has been configured. Review the following settings, and then click Next to add the claims provider trust to the AD FS configured. Review the following settings, and then click Next to add the claims provider trust to the AD FS configured. Review the following settings, and then click Next to add the claims provider trust to the AD FS configured. Review the following settings, and then click Next to add the claims provider trust to the AD FS configured. Review the following settings and then click Next to add the Cast of the AD FS configured. Review the following settings are trust of the AD FS configured trust. Claims provider's federation metadata URL:	Actions Claims Provider Trust View Add Claims Provider Trust View New Window from Here Refes.h Help Active Directory Update from Federation Metadata Edit Claim Rules Disable Properties Help Help Help
Image: AD FS Image: Source Image: Access Control Policies Image: Reving Party Trusts Image: Access Control Policies Ima	Claims Provider Trusts Display Name Active Directory ADSSP IdP Control ADSSP IdP Control Contr	Enabled Yes Yes rust Wizard X The claims provider trust has been configured. Review the following settings, and then click. Next to add the claims provider trust to the AD FS configuration database. Montoring identifien Cestificates Encoption Offered Claims Organization Endpoints Note** Speefy the trust montoring settings for this claims provider trust. Claims provider's federation metadata URL: Montor claims provider	Actions Claims Provider Trust Claims Provider Trust View New Window from Here Refresh Help Active Directory Update from Federation Metadata Edit Claim Rules Disable Properties Help Help
Image: Application Groups	Claims Provider Trusts Display Name Active Directoy ADSSP IdP	Enabled Yes Yes Tust Wizard X The clams provider that has been configured. Review the following settings, and then click. Next to add the clams provider that to the AD FS configuration diabase. Montoring identifies Certificates Encoption Offered Claims Organization Endpoints Note • Specify the that monitoring settings for this claims provider that. Claims provider's federation metadata URL: Monitor claims provider Monitor claims provider Monitor claims provider	Actions Claims Provider Trust View Add Claims Provider Trust View New Window from Here Refresh Help Active Directory Update from Federation Metadata Edit Claim Rules Disable Properties Help Help Help
Image: Service Image: AD FS Image: Service Image: Access Control Policies Image: Reving Party Trusts Image: Claims Provider Trusts Image: Application Groups	Claims Provider Trusts Daplay Name Active Directory ADSSP IdP Active Directory	Enabled Yes Yes Tust Wizard X The dams provider tust has been configured. Review the following settings, and then click Next to add the clams provider tust to the AD FS configuration database. Monitoring Identifiers Centificates Encorption Offered Clams Organization Endpoints Note • • Speedy the tust monitoring settings for this claims provider trust. Claims provider's federation metadata URL: Monitor claims provider Automatically update claims provider This claims provider This claims provider federation metadata was last checked on:	Actions Claims Provider Trust View Add Claims Provider Trust View New Window from Here Refresh Help Active Directory Update from Federation Metadata Edit Claim Rules Disable Properties Help Help Help
Image: AD FS Image: Service Image: Access Control Policies Image: Reving Party Trusts Image: Reving Pa	Chims Provider Trusts Display Name Active Directory ADSSP IdP Control Chimsen Provider T Ready to Add Trust Steps Welcome Sector Data Source Sector Data Source Prosh	Enabled Yes Yes Trust Wizard X The claims provider trust has been configured. Review the following settings, and then click. Next to add the claims provider trust to the AD FS configuration database. Monitoring identifiem Cestificates Encoption Offered Claims Organization Endpoints Note (*) Specify the trust monitoring settings for this claims provider trust. Claims provider's federation metadata URL: Monitor claims provider Monitor claims provider Monitor claims provider is defraction metadata uses as last checked on: 	Actions Claims Provider Trusts Add Claims Provider Trust View New Window from Here Refersh Help Active Directory Update from Federation Metadata Edit Claim Rules Disable Properties Help Help Help
 AD FS Service Access Control Policies Reying Party Trusts Claims Provider Trusts Application Groups 	Chims Provider Trusts Display Name Active Directory ADSSP IdP	Enabled Yes Yes Tust Wizard The claims provider truth has been configured. Review the following settings, and then click. Next to add the claims provider fructs to the AD FS configuration distabase. Montoring identifies Certificates Encopption Offered Claims Organization Endpoints Note ** Specify the trust monitoring satings for this claims provider trust. Claims provider's federation metadata URL: Montor claims provider is defined provider in the claims provider for this claims provider is defined provider in the claims provider is federation metadata use last checked on: c. new right is claims provider in the claims provider in the claims provider is claims provider in the claims provider is federation metadata was last checked on: c. new right is claims provider is last updated from federation metadata on:	Actions Claims Provider Trusts Add Claims Provider Trust View New Window from Here Refresh Help Active Directory Update from Federation Metadata Edit Claim Rules Disable Properties Help Help Help
 AD FS Service Access Control Policies Relying Party Trusts Claims Provider Trusts Application Groups 	Claims Provider Trusts Display Name Active Directoy ADSSP IdP Vigit Add Claims Provider T Reody to Add Trust Seps • Welcome • Select Data Source • Specify Display Name • Ready to Add Trust • Ready to Add Trust • Ready to Add Trust • Pready to Add Trust • Fresh	Enabled Yes Yes The clams provider trust has been configured. Review the following settings, and then click. Next to add the clams provider trust to the AD FS configuration distabase. Montoring leartifiem Centificates Encoption Offered Claims Organization Endpoints Note () Specify the trust nomkoring aetings for this claim provider trust. Claims provider's federation metadata URL: Claims provider's federation metadata URL: Claims provider's federation metadata was last checked on: < never > This claims provider trust was last updated from federation metadata on: < never >	Actions Claims Provider Trust View Add Claims Provider Trust View Refresh Refresh Help Active Directory Update from Federation Metadata Edit Claim Rules Disable Properties Help Help
Image: Service Image: AD FS Image: Service Image: Access Control Policies Image: Reving Party Trusts Image: Claims Provider Trusts Image: Application Groups	Claims Provider Trusts Display Name Active Directory ADSSP IdP	Enabled Yes Montor claims provider tout hab been corfigured. Review the following settings, and then click Next to add the claims provider tout. Game provider forderation metadata URL: Montor claims provider forderation metadata URL: Montor claims provider is federation metadata was last checked on: < newer > This claims provider tout was last updated from federation metadata on: < newer >	Actions Claims Provider Trust View Add Claims Provider Trust View New Window from Here Refresh Help Active Directory Update from Federation Metadata Edit Claim Rules Disable Properties Help Help Help
 AD FS Service Access Control Policies Reying Party Trusts Claims Provider Trusts Application Groups 	Chims Provider Trusts Display Name Active Directory ADSSP IdP Control ADSSP IdP Control Control		Actions Claims Provider Trusts Add Claims Provider Trust View New Window from Here Refersh Help Active Directory Update from Federation Metadata Edit Claim Rule Disable Properties Help Help Help
AD FS Sorvice Access Control Policies Relying Party Trusts Claims Provider Trusts Application Groups	Chims Provider Trusts Display Name Active Directoy ADSSP IdP	Enabled Yes Yes Yes Yes The claims provider trust has been configured. Review the following settings, and then click. Next to add the claims provider trust to the AD FS configuration disabase. Montoring identifies Certificates Encoption Offered Claims Organization Endpoints Nete * Specify the trust monitoring settings for this claims provider trust. Claims provider's federation metadata use last checked on:	Actions Claims Provider Trust View Add Claims Provider Trust View New Window from Here Refresh Help Active Directory Update from Federation Metadata Edit Claim Rules Disable Properties Help Help Help
AD FS Service A Access Control Policies Reying Party Trusts Claims Provider Trusts Application Groups	Claims Provider Trusts Display Name Active Directory ADSSP IdP	Enabled Yes Yes Yes Yes Yes Tutt Wizard X The dams provider tutt has been configured. Review the following settings, and then click Next to add the Montoring Identifiers Cetificates Encryption Offered Clams Organization Endpoints Note Specify the trust montoring settings for this claims provider trust. Claims provider's federation metadata URL: Immunor Calams provider Automatically update claims provider Inclaims provider trust was last checked on: <never> This claims provider trust was last updated from federation metadata on: <never></never></never>	Actions Claims Provider Trust View Add Claims Provider Trust View New Window from Here Refresh Help Active Directory Update from Federation Metadata Edd Claim Rufex Disable Properties Help Help Help
AD FS Service Access Control Policies Reying Party Trusts Claims Provider Trusts Application Groups	Chims Provider Trusts Display Name Active Directory ADSSP IdP Control Chimsen Provider T Ready to Add Trust Ready to Add Trust Prosh	Enabled Yes Yes rust Wizard Montoring identifies Deen configured. Review the following settings, and then click. Next to add the climits provider trust has been configured. Review the following settings, and then click. Next to add the climits provider trust to the AD FS configuration diadabase. Montoring identifies Cestificates Encorption Offered Clams Organization Endpoints Note* Genery the trust montoring settings for this clams provider trust. Clams provider's federation metadata URL: Montor clams provider Automatically update clams provider Its clams provider trust was last checked on: cnever >	Actions Claims Provider Trust. Claims Provider Trust View New Window from Here Refresh Help Active Directory Update from Federation Metadata Edit Claim Rules Disable Properties Help Help
AD FS Sorvice Access Control Policies Relying Party Trusts Claims Provider Trusts Application Groups	Chims Provider Trusts Display Name Active Directory ADSSP IdP	Enabled Yes Yes Instruct Wizard X The claims provider trust has been configured. Review the following settings, and then click Next to add the claims provider trust to the AD FS configuration disabase. Monotring identifies Certificates Encoption Offered Claims Organization Endpoints Nete Specify the trust monitoring settings for this claims provider trust. Claims provider's federation metadata URI: Monotring Gertifies provider: Automatically update claims provider Monotor claims provider funct was last checked on:	Actions Claims Provider Trust View Add Claims Provider Trust View Refresh Help Active Directory Update from Federation Metadata Edit Claim Rules Disable Properties Help Help
AD FS Service A Access Control Policies Reying Party Trusts Claims Provider Trusts Application Groups	Claims Provider Trusts Display Name Active Directory ADSSP IdP	Enabled Yes Yes Yes Yes Turk Wizard Xentering in derating provider trutt has been configured. Review the following settings, and then click Next to add the click for the AD PS configured on database. Montoring inderating in configured. Review the following settings, and then click Next to add the click for the AD PS configured on database. Montoring inderating in configured. Review the following settings, and then click Next to add the click for the AD PS configured on database. Montoring inderating in configured. Review the following settings, and then click Next to add the click for the AD PS configured on database. Montoring inderating in configured. Review the following settings, and then click Next to add the click is claims provider trut. Claims provider is following settings provider trut. Claims provider is following in detadata was last checked on: Claims provider trut was last updated from federation metadata on: Claims provider trut was last updated from federation metadata on: Claims provider trut was last updated from federation metadata on: Claims provider trut was last updated from federation metadata on: Claims provider trut was last updated from federation metadata on: Claims provider trut was last updated from federation metadata on: Claims provider trut was last updated from federation metadata on:	Actions Claims Provider Trust View Add Claims Provider Trust View New Window from Here Refresh Help Active Directory Update from Federation Metadata Edd Claim Rufez Disable Properties Help Help Help
AD FS Service A Access Control Policies Reying Party Trusts Claims Browder Trusts Application Groups	Chims Provider Trusts Display Name Active Directory ADSSP IdP Control Chimsen Provider T Ready to Add Trust Steps Welcome Select Data Source Select Data Source Ready to Add Trust Finah	Enabled Yes Yes rust Wizard Montoring identifies Cestificates Encryption Offered Claims Organization Endpoints Note Montoring identifies Cestificates Encryption Offered Claims Organization Endpoints Note Genery the trust montoring settings for this claims provider trust. Claims provider's federation metadata URL: Montor claims provider Automatically update claims provider This claims provider trust was last checked on: <never> This claims provider trust was last updated from federation metadate on: <never></never></never>	Actions Claims Provider Trust View Add Claims Provider Trust View New Window from Here Refersh Help Active Directory Update from Federation Metadata Edit Claim Rules Disable Properties Refersh Help Help
AD FS Svvice Access Control Policies Reving Party Trusts Application Groups	Chims Provider Trusts Display Name Active Directory ADSSP IdP	Enabled Yes Yes Instructions provider trutt has been configured. Review the following settings, and then click. Next to add the clasms provider trutt to the AD FS configuration diabase. Montoring identifies Certificates Encopption Offered Claims Organization Endpoints Nete** Specify the trutt monitoring settings for this claims provider trutt. Claims provider's federation metadata was last checked on: Claims provider's federation metadata was last checked on: Claims provider trutt was last updated from federation metadata on: Crewer >	Actions Claims Provider Trust View Mindow from Here Refresh Help Active Directory Update from Federation Metadata Edit Claim Rules Disable Properties Help Help
AD FS Service A Access Control Policies Reving Party Trusts Claims Browide Trusts Application Groups	Claims Provider Trusts Daplay Name Active Directory ADSSP IdP	Enabled Yes Yes Yes Yes Total component of the base on configured. Review the following settings, and then click. Next to add the class provider trust to the AD FS configuration distabase. Montaining identifies Cetificates Encorption Offered Claims Organization Endpoints Nete (*) Specify the trust monitoring settings for this claims provider trust. Claims provider's federation metadata URI: Montain of the densition metadata was last checked on: Cleimer > This claims provider federation metadata was last checked on: Crever > This claims provider trust was last updated from federation metadata on: Crever >	Actions Claims Provider Trust View Add Claims Provider Trust View Refresh Refresh Help Active Directory Update from Federation Metadata Edit Claim Rules Disable Properties Help Help
AD FS Service A Access Control Policies Beijing Party Trusts Claims Browide Trusts Application Groups	Claims Provider Trusts Display Name Active Directory ADSSP IdP	Enabled Yes Yes Yes Yes Turut Wizzd To claims provider turut has been configured. Review the following settings, and then click Next to add the Montoring Identifiers Configured. Review the following settings, and then click Next to add the Montoring Identifiers Configured. Review the following settings, and then click Next to add the Montoring Identifiers Configured. Review the following settings, and then click Next to add the Montoring Identifiers Configured. Review the following settings, and then click Next to add the Montoring Identifiers Configured. Review the following settings. Specify the turut montoring settings for this claims provider turut. Claims provider Specify the turut montoring settings for this claims provider Tis claims provider Automatically update claims provider Its claims provider turut was last updated from federation metadate on: enser > Tis claims provider turut was last updated from federation metadate on: enser > Its claims provider turut was last updated from federation metadate on: enser > Its claims provider enser > Its claims provider enser > Its	Actions Claims Provider Trust View Add Claims Provider Trust View New Window from Here Refresh Help Active Directory Update from Federation Metadata Edd Claim Rufex Disable Properties Help Help Help

4. In the Specify Display Name section, enter the desired **Display name**. Click **Next.**

5. Complete the remaining steps in the wizard by retaining the default values for the rest of the fields.

Step 2: Adding claims rules

1. Once the claims provider trust configuration is complete, the *Edit Claims Rule for ADSSP Identity Provider* editor window opens. Click **Add Rule.**

Edit Claim	n Rules for ADSSP Identity Provider	×
Acceptant	ce Transform Rules	
The follo from the	owing acceptance transform rules specify the incoming claims that will be accepted e claims provider and the outgoing claims that will be sent to the relying party trust.	
Order	Rule Name Issued Claims	
	*	1
Add F	Rule Edit Rule Remove Rule	
	OK Cancel Apply	

2. From the *Claim rule template* drop-down, select **Pass Through or Filter an Incoming Claim** and click **Next.**

Steps	Select the template for the claim rule that you want to create from the following list. The description provides
Choose Rule Type	details about each claim rule template.
Configure Claim Rule	Claim rule template: Pass Through or Filter an Incoming Claim Send LDAP Attributes as Claims Send Group Membership as a Claim Transform on Incoming Claim Pass Through or filter an Incoming Claim Part Claims Wing of Culture The Incoming Claim State and Wing Section The Incoming Group claims. You can also use this rule to send only UPN claims that end with "@fabrikam". Multiple claims with the same claim type may be emitted from this rule. Sources of incoming claims vary based on the rules being edited.

3. In the next window, enter a **Claim rule name** and set **UPN** as the **Incoming claim type**. Choose the **Pass through all claim values** radio button. Click **Finish** to complete adding the claims rule.

Conligure Rule			,
Steps	You can configure this	Ile to pass through or filter an incoming claim. You can also	configure this rule to filter
Choose Rule Type	claim values should pas	s through.	some claim values of all
Configure Claim Rule	Claim rule name:		
	UPN		
	Rule template: Pass Th	ough or Filter an Incoming Claim	
	Incoming claim type:	UPN	~
	Incoming name ID form	t: Unsectied	~
	Pass through all claim	n values	
	 Pass through only a 	pecific claim value	
	Incoming claim valu	ə:	
	 Pass through only c 	im values that match a specific email suffix value:	
	Email suffix value:		
		Example: fabrikam.com	
	 Pass through only c 	im values that start with a specific value:	
	Starts with:		
		Example: FABRIKAM\	
		< Previous	-inish Cancel
The following a from the claims	acceptance transform provider and the out	ules specify the incoming claims that will b oing claims that will be sent to the relying p	e accepted party trust.
Order Date	News	lanual Christe	
Order Rule	Name	Issued Claims	
1 UPN		UPN	
			1
			<u>ا</u>
			\$
			\$
			\$ \$
			\$ \$
			4
			A
			\$ \$
			\$ \$
Add Rule	Edit Rule	Remove Rule	\$
Add Rule	Edit Rule	Remove Rule	\$ \$
Add Rule	Edit Rule	Remove Rule	\$ \$

4. You need to add two more claim rules. So, click **Add Rule** from the *Edit Claims Rule for ADSSP Identity Provider* editor again.

	Select the template for the claim rule that you want to create from the following list. The description provider
Choose Rule Type	details about each claim rule template.
Configure Claim Rule	Claim rule template:
	Pass Through or Filter an Incoming Claim \checkmark
	Claim rule template description:
	Using the Pass I hrough or Filter an incoming Claim rule template you can pass through all incoming claim with a selected claim type. You can also filter the values of incoming claims with a selected claim type. For example, you can use this rule template to create a rule that will send all incoming group claims. You can also use this rule to send only UPN claims that and with "Graham". Multiple claims with the same claim type may be emitted from this rule. Sources of incoming claims vary based on the rules being edited

5. From the *Claim rule template* drop-down, select **Pass Through or Filter an Incoming Claim** and click **Next**.

Madd Transform Claim Rul	e Wizard			×
Steps	You can configure this rule	to pass through or filter an inc	oming claim. You can a	also configure this rule to filter
Choose Rule Type	claims that are generated l claim values should pass t	by previous rules. Specify the c hrough.	laim type and whether	only some claim values or all
Configure Claim Rule	Claim rule name:	7		
	Windows account name			
	Rule template: Pass Throu	igh or Filter an Incoming Claim		
	Incoming claim type:	Windows account name		~
	Incoming name ID format:	Inspecified		~
	Pass through all claim y	values		
	 Pass through only a sp 	ecific claim value		
	Incoming claim value:			
	O Pass through only claim	n values that match a specific e	email suffix value:	
	Email suffix value:			
		Example: fabrikam.com		
	Pass through only clain	n values that start with a specifi	ic value:	
	Starts with:	E L EADDIKANA		
		Example: FABRIKAM\		
			< Previous	Finish Cancel

6. In the next window, enter a **Claim rule name** and set **Windows account name** as the **Incoming claim type.** Choose the **Pass through all claim values** radio button. Click **Finish** to complete adding the claims rule.

t Claim	Rules for ADSSP Identity Provider		
ceptanc	e Transform Rules		
The follo from the	wing acceptance transform rules spec claims provider and the outgoing claim	ify the incoming claims that will be accep is that will be sent to the relying party true	oted st.
Order	Rule Name	Issued Claims	
1	UPN	UPN	
2	Windows account name	Windows account name	
			♣
Add R	ule Edit Rule Remove F	Rule	
		OK Canad	Annak.

7. You need to add one more claim rule, so click **Add Rule** again.

steps	Select the template for the claim rule that you want to create from the following list. The description provides
Choose Rule Type	details about each claim rule template.
Configure Claim Rule	Claim rule template:
	Pass Through or Filter an Incoming Claim $\qquad \lor$
	Claim rule template description:
	Using the Pass Through or Filter an Incoming Claim rule template you can pass through all incoming claims with a selected claim type. You can also filter the values of incoming claims with a selected claim type. For example, you can use this rule template to create a rule that will send all incoming group claims. You can also use this rule to send only UPN claims that end with "@fabrikam". Multiple claims with the same claim type may be emitted from this rule. Sources of incoming claims way based on the rules being edited.

8. From the *Claim rule template* drop-down, select **Pass Through or Filter an Incoming Claim** and click **Next.**

Steps	You can configure this rule to nase through or filter an incoming claim. You can also configure this rule to f	iter
Choose Rule Type	claims that are generated by previous rules. Specify the claim type and whether only some claim values or claim values should pass through.	all
Configure Claim Rule	Claim rule name:	
	Primary SID	
	Rule template: Pass Through or Filter an Incoming Claim	
	Incoming claim type: Primary SID	`
	Incoming name ID format:	
	Pass through all claim values	
	O Pass through only a specific claim value	
	Incoming claim value:	
	O Pass through only claim values that match a specific email suffix value:	
	Email suffix value:	
	Example: fabrikam.com	
	Pass through only claim values that start with a specific value:	
	Starts with:	
	Example: FABRIKAM\	

 In the next window, enter a Claim rule name and set Primary SID as the Incoming claim type. Choose the Pass through all claim values radio button. Click Finish to complete adding the claims rule.

Once all three claim rules are added, the **Edit Claim Rules for ADSSP Identity Provider** dialog box should look like this:

Edit Claim	Rules for ADSSP Identity Provider	×
Acceptance	e Transform Rules	
The follo from the	wing acceptance transform rules specify the claims provider and the outgoing claims that	incoming claims that will be accepted will be sent to the relying party trust.
Order	Rule Name	Issued Claims
1	UPN	UPN
2	Windows account name	Windows account name
3	Primary SID	Primary SID
Add F	lule <u>E</u> dit Rule <u>R</u> emove Rule	
		OK Cancel Apply

10. Click **Apply** and then **OK** to save the claim rules for ADSelfService Plus.

Step 3: Executing Windows PowerShell commands

Open Windows PowerShell on the AD FS server and execute the following commands:

• Set the ADSelfService Plus claims provider to use **sAMAccountName** as the anchor claim type:

Set-AdfsClaimsProviderTrust -TargetIdentifier <ADSSP IdP Entity URL> -AnchorClaimType http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname

Select Administrator: Windows PowerShell

Solution

Set-AdfsClaimsProviderTrust
-TargetIdentifier
https://adselfserviceplus.com/iamapps/ssologin/custom_saml_app/3800a71b21b0d6629

Solution

Solution

Note: The value of the <ADSSP IdP Entity IIRI > should be conjed from the IdP metadata in

Note: The value of the *<ADSSP IdP Entity URL>* should be copied from the IdP metadata in <u>Step 11</u> of the **Set up ADSelfService Plus to authenticate Outlook users** section.

• Configure AD FS to redirect to ADSelfService Plus for authentication when logging into the Outlook on Windows app:

Set-AdfsWebApiApplication -TargetName "<Outlook> - Web API" -ClaimsProviderName @("<Display name of ADSSP claims provider name in ADFS>")

27 Administrator: Windows PowerShell	_		×	:
PS C:\Users\Administrator> Set-AdfsWebApiApplication -TargetName "Outlook - Web API" -ClaimsProviderName	@("	ADSSP 1	IdP") <mark>-</mark>	^

Once configured, users will be presented with the ADSelfService Plus login prompt with MFA when connecting to Exchange Server via Outlook on Windows.

Note:

- Replace *<Display name of ADSSP claims provider name in ADFS>* with the claim name copied in <u>Step 4</u> of the **Adding a new claims provider trust** section.
- Replace <Outlook> with the name for the native application group created in <u>Step 6b</u> of the **ADFS configuration for modern authentication** section.

Step 4: Enabling MFA for cloud apps in ADSelfService Plus

ADSelfService Plus provides 20 MFA methods to secure your applications. Follow the steps below to configure the necessary authentication methods and enable MFA protection for Outlook.

Step 1: Create a policy for users requiring MFA

a. Log into ADSelfService Plus with admin credentials and navigate to **Configuration > Self-Service > Policy Configuration.**

		License Talk Back 📮 🕒 🗸
Dashboard Reports	Configuration Admin Support	🔅 Domain Settings
Self-Service	Policy Configuration (?)	Password Self-Service Modes 👻
Policy Configuration	adselfservice.com 🧪	
Multi-factor Authentication Password Expiration Notification Password Policy Enforcer Password Sync/Single Sign On Conditional Access Directory Self Service Administrative Tools Security Center	 Reset Password Enable users to securely reset passwords on their own (without supplying old passwords). Unlock Account Enable users to securely unlock accounts on their own. Self Update Enable users to securely update Active Directory details on their own. Choose a Self Update Layout. Change Password Enable users to securely change passwords on their own (by supplying old passwords). 	🎼 Select OUs/Groups 🔇 Advanced
	Save Policy Cancel Available Policies Advanced Policy Name Policy Name Domain Name Actions Advanced Policy Name Permissions Domain Name Image: Im	Add New Policy

b. If only the specific subset of users needing MFA for Outlook are already in a policy, skip to <u>Step e</u>.
 Otherwise, create a new policy by clicking the **Add New Policy** button.

ADSelfService Plus		License Talk Back 📮 😝 🗸
Dashboard Reports	onfiguration Admin Support	🕸 Domain Settings
Self-Service	Policy Configuration ()	Password Self-Service Modes \bullet
Policy Configuration	Enter a Policy Name	
Multi-factor Authentication		
Password Expiration Notification Password Policy Enforcer	Reset Password Enable users to securely reset passwords on their own (without supplying old passwords).	
Password Sync/Single Sign On	Unlock Account Enable users to securely unlock accounts on their own.	
Directory Self Service	Self Update Enable users to securely update Active Directory details on their own. Choose a Self Update Layout.	
Administrative Tools		
Security Center	Enable users to securely change passwords on their own (by supplying old passwords).	Select OUs/Groups
	Save Policy Cancel	
	Available Policies	+ Add New Policy
	α	<
	Actions Advanced Policy Name Permissions Domain Name Last Modifie	ed By Last Modified Time
	The the adselfservice.com Reset Password, Unlock Account, Self Update, Change Password ADSELFSERVICE	-

c. Click Select OUs/Groups at the bottom right of the page, select the users who need MFA, and click OK.

ADSelfService Plus	Select OUs/Groups	×	License Talk Back 🐥 🕙 🛩
Dashboard Reports Configuration Admin Support	Select Domain ADSELFSERVICE 🗸		🔅 Domain Settings
Self-Service Policy Configuration ③	🖬 OUs 🛛 🍪 Groups		Password Self-Service Modes 👻
Self-Service Policy Configuration Muth-Factor Authentication Password Expiration Notification Password Expiration Notification Password Spin/Single Sign On Conditional Access Directory Self Service Administrative Tools Security Center Authous Secure Sec	Image: State of the state	Tree view List view	Select OUX/Groups Add New Policy K C 1-1 of 1 > > Nume Last Modified By Last Modified Time SERVICE -

d. Choose the password self-service features you want to enable for these users (Reset Password, Unlock Account, Self Update, or Change Password), name the policy, and click **Save Policy**.

III ADSelfService Plus		License Talk Back 📮 😁 🗸 Q Search Employee
Dashboard Reports	Configuration Admin Support	🔅 Domain Settings
Self-Service	Policy Configuration ③	Password Self-Service Modes 👻
Policy Configuration Multi-factor Authentication Password Expiration Notification Password Policy Enforcer Password Sync/Single Sign On Conditional Access	adselfserviceptus.com Reset Password Enable users to securely reset passwords on their own (without supplying old passwords). Unlock Account Enable users to securely unlock accounts on their own. Enable users to securely unlock accounts on their own.	
Directory Self Service Administrative Tools Security Center	Ser Update Enable users to securely update Active Directory details on their own. Choose a Self Update Layout. Change Password Enable users to securely change passwords on their own (by supplying old passwords). Save Policy Cancel	Select OUs/Groups 🛱 Advanced
	Available Policies	+ Add New Policy
	Q	< 1-1 of 1 > >>
	Actions Advanced Policy Name Permissions Domain Name Last Mor	dified By Last Modified Time
	A g r b k adselfservice.com Reset Password, Unlock Account, Self Update, Change Password ADSELFSERVICE	•

e. Go to **Configuration > Self-Service > Multi-Factor Authentication > Authenticator Setup** and select the policy you just created from the drop-down menu.

ADSelfService Plus		License Talk Back 👫 😔 🗸
Dashboard Reports Co	nfiguration Admin Support	🔅 Domain Settings
Self-Service	Multi-factor Authentication ③	How to make users enroll? 👻
Policy Configuration	Choose the Policy adselfserviceplus.com	
Multi-factor Authentication	Authenticators Setue MFA for Reset/Linlock MFA for Endopints MFA for Applications	MFA Enrollment
Password Expiration Notification		
Password Policy Enforcer	Security Question & Answer Constitution	÷
Password Sync/Single Sign On	Email Venfication	► ²¹⁰
Conditional Access	SMS Verification	•
Directory Self Service	Google Authenticator Configured	
Administrative Tools	Microsoft Authenticator	÷
Security Center	Azure AD MFA	÷
	Duo Security	*
	RSA SecurID	<u>۶</u>
	RADIUS Authentication	÷
	Push Notification Authentication	÷
	Fingerprint/Face ID Authentication	•
	QR Code Based Authentication	÷
	TOTP Authentication (Using ADSelfService Plus Mobile App)	÷
	SAML Authentication	•
	AD Security Questions	
	Yubikey Authenticator	÷
	Zoho OneAuth TOTP	•
	Smart Card Authentication	•
	Custom TOTP Authenticator	÷
	FIDO Passkeys Configured	÷
		-
	🗧 Admin Guide 🔅 Need Features 🧀 Report an Issue 🔤 🖓 User Forums 🕠 Toll free : +1-844-245-1104 🕓 Direct Phone : +1-408-916-9890	E

f. Configure the desired authentication methods for the selected policy and click **Save**. You can learn how to configure each authentication method by clicking the links on <u>this page</u>.

Step 2: Enable the required MFA factors

Since ADSelfService Plus will be prompted by AD FS to act as an IdP via a browser, you need to enable **MFA for Cloud Applications** and select the required authenticators.

a. Log into ADSelfService Plus with admin credentials and navigate to **Configuration > Self-Service > Multi-Factor Authentication > MFA for Endpoints.**

ADSelfService Plus	Confinuation Admin Support	License Talk Back 199 G - Q Search Employee
Self-Service	Multi-factor Authentication ③	How to make users enroll? -
Policy Configuration	Choose the Policy adselfservicenius com	
Multi-factor Authentication		
Password Expiration Notification	Authenticators Setup MFA for Reset/Unlock MFA for Endpoints MFA for Applications	MFA Enrollment & Advanced
Password Policy Enforcer	MFA for Machine Login O Enable 1 🗸 factor authentication for Machine login. 🕜	
Password Sync/Single Sign On	Supported : Windows/macOs/Linux Choose authenticators for Machine Looin MFA - No factor selected -	745
Conditional Access		
Directory Self Service	Choose authenticators for Offline MFA - No factor selected - 🗸 🗸 🗇	
Administrative Tools		
Security Center	MFA for OWA Login Supported : OWA/ECP of Exchange Server Choose authenticators for OWA Login MFA - No factor selected -	
	MEA for VPN Login () VPN providers that support RADIUS authentication Choose authenticators for VPN login - No factor selected - V	
	MFA for Cloud Applications Secure SSO login from ADSelfService Plus. Select the authenticators required Violator selected - V	
	Save Settings Cancel	
		(a) Machine-based MFA ⑦
	🛿 Admin Guide 🔍 Need Features 🥩 Report an Issue 🥐 User Forums 🕓 Toll Free : +1-844-245-1104 🕓 Direct Phone : +1-408-916-9890	

b. Under *MFA for Cloud Applications,* select the checkbox to **Enable <number_of_factors> authentication factors** and choose the required authenticators from the drop-down menu. Click **Save Settings.**

	Multi-factor Authentication (?)		How to make users enrol
-Service +	Choose the Policy adreficencicanius com		
ulti-factor Authentication			
assword Expiration Notification	Authenticators Setup MFA for Reset/Unlock MFA	for Endpoints MFA for Applications	MFA Enrollment 🎄 Advanc
assword Policy Enforcer	MFA for Machine Login	Enable 1 v factor authentication for Machine Iogin ③	
assword Sync/Single Sign On	Supported : Windows/macOS/Linux		
onditional Access		Choose authenticators for Machine Login MFA - No factor selected -	
rectory Self Service		Choose authenticators for Offline MFA - No factor selected - 🗸 🧿	
inistrative Tools			
irity Center 🔸	MFA for OWA Login Supported : OWA/ECP of Exchange Server	Enable 1 v factor authentication for OWA Login. Choose authenticators for OWA Login MFA - No factor selected -	
	MFA for VPN Login ③ VPN providers that support RADIUS authentication	Enable 1 v factor authentication for VPN login. Choose authenticators for VPN login -No factor selected - v	
	MFA for Cloud Applications Secure SSO legin from ADSelfService Plus.	Enable 1 v authentication factors.	
		Select the authenticators required Google Authenticator, FIDO Passkeys 🗸	
		II Security Questions *	
		Save Settions Cancel	
		II 🗹 FIDO Passkeys *	
			Machine-based MFA

c. By default, ADSelfService Plus requires users to enter a password before initiating MFA.
 To enable Passwordless logins, click Advanced at the top-right corner, go to Endpoint MFA > Cloud
 Applications Login MFA, select Enable Passwordless logins, and click Save.



That's it! Users will now see the ADSelfService Plus login prompt with the configured MFA factors when connecting to Exchange Server via the Outlook client.

For a visual walkthrough of the user experience, refer to this <u>demo video</u>.

Reference Documentation

- <u>Microsoft Docs</u>
- ManageEngine ADSelfService Plus Documentation

Our Products

AD360 | Log360 | ADManager Plus | ADAudit Plus RecoveryManager Plus | M365 Manager Plus

ManageEngine) ADSelfService Plus

ADSelfService Plus is an identity security solution to ensure secure and seamless access to enterprise resources and establish a Zero Trust environment. With capabilities such as adaptive multi-factor authentication, single sign-on, self-service password management, a password policy enhancer, remote work enablement and workforce self-service, ADSelfService Plus provides your employees with secure, simple access to the resources they need. ADSelfService Plus helps keep identity-based threats out, fast-tracks application onboarding, improves password security, reduces help desk tickets and empowers remote workforces. For more information about ADSelfService Plus, visit www.manageengine.com/products/self-service-password.

\$ Get Quote

± Download