ManageEngine
ADSelfService Plus

How to secure **Microsoft Outlook** Desktop Applications using MFA

Table of Contents

How to secure Microsoft Outlook using MFA

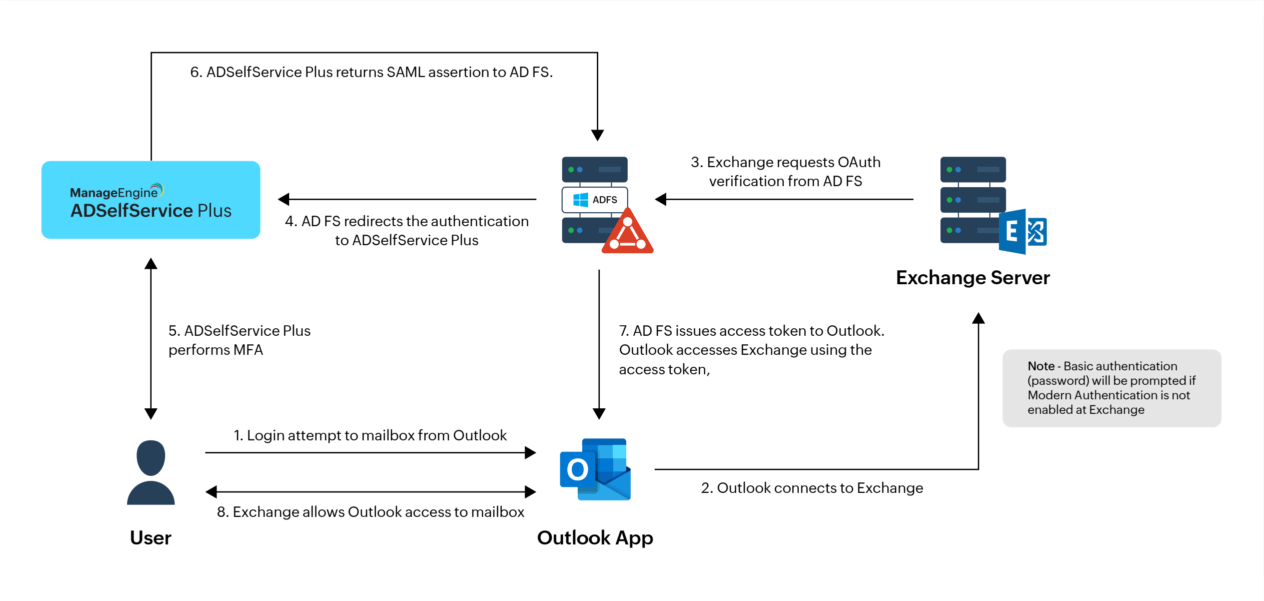
Modern authentication enables users to authenticate to Exchange using AD FS. When enabled, the Outlook client redirects users to AD FS, which authenticates their identity and generates access tokens that are subsequently validated by Exchange Server to grant users access to their mailboxes.

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:


6. ADSelfService Plus returns SAML assertion to AD FS.
ManageEngine ADSelfService Plus
4. AD FS redirects the authentication to ADSelfService Plus
ADFS
3. Exchange requests OAuth verification from AD FS
Exchange Server
5. ADSelfService Plus performs MFA
7. AD FS issues access token to Outlook. Outlook accesses Exchange using the access token,
Note - Basic authentication (password) will be prompted if Modern Authentication is not enabled at Exchange
1. Login attempt to mailbox from Outlook
8. Exchange allows Outlook access to mailbox
2. Outlook connects to Exchange
User
Outlook App

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 here.

Configuration Steps

You will need to configure the following for modern authentication:

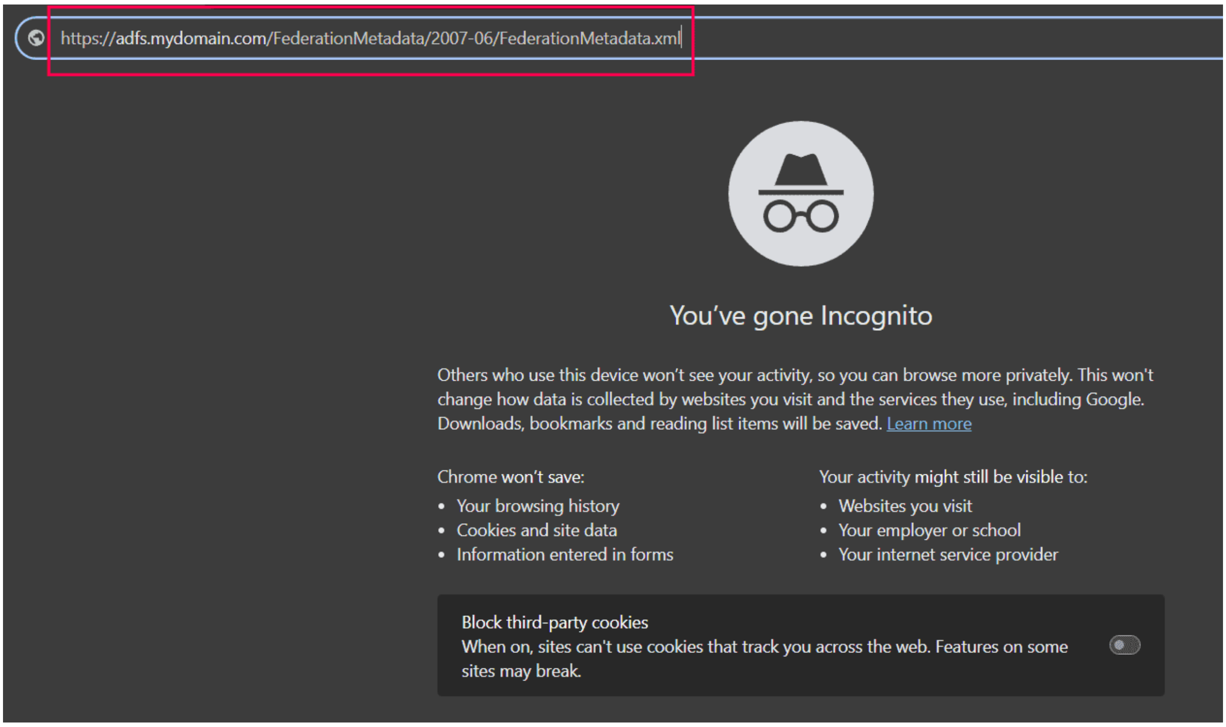
- AD FS
- On-premises Exchange Server
- The Outlook client on the user's Windows machine

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.



https://adfs.mydomain.com/FederationMetadata/2007-06/FederationMetadata.xml

You've gone Incognito

Others who use this device won't see your activity, so you can browse more privately. This won't change how data is collected by websites you visit and the services they use, including Google. Downloads, bookmarks and reading list items will be saved. Learn more

Chrome won't save:

- Your browsing history
- Cookies and site data
- Information entered in forms

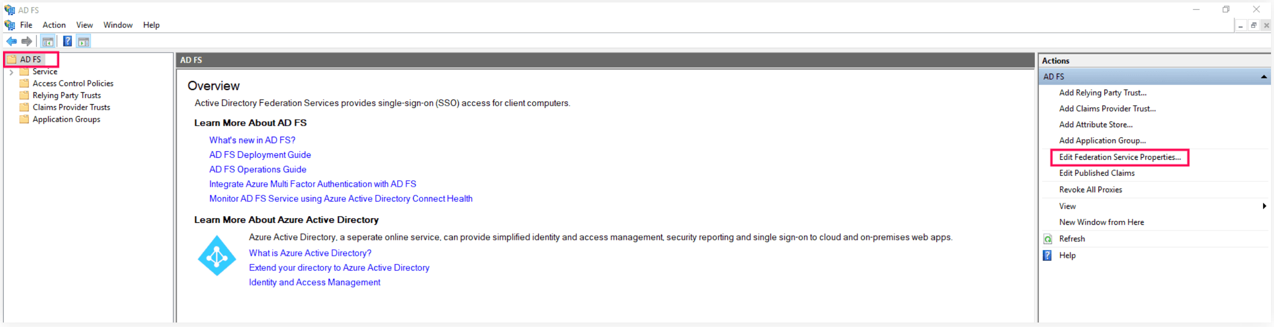
Your activity might still be visible to:

- Websites you visit
- Your employer or school
- Your internet service provider

Block third-party cookies
When on, sites can't use cookies that track you across the web. Features on some sites may break.

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

2. 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.



Overview

Active Directory Federation Services provides single-sign-on (SSO) access for client computers.

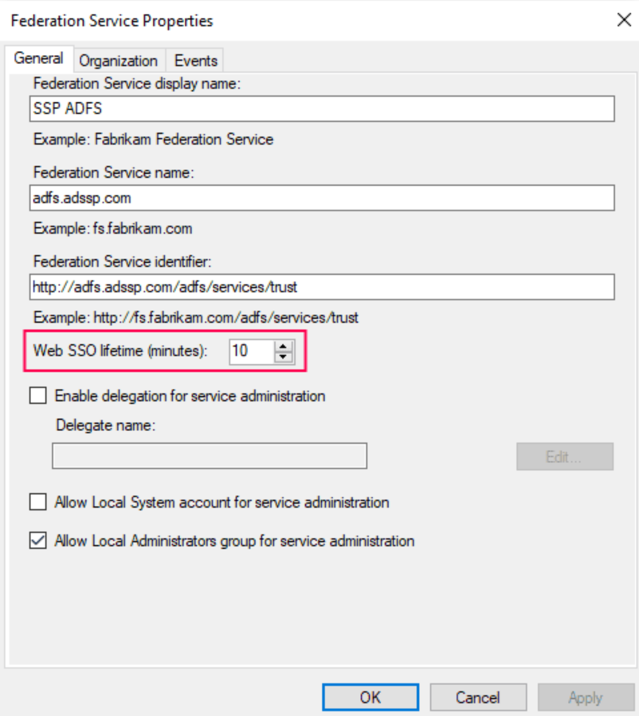
Learn More About AD FS

What's new in AD FS?
AD FS Deployment Guide
AD FS Operations Guide
Integrate Azure Multi Factor Authentication with AD FS
Monitor AD FS Service using Azure Active Directory Connect Health

Learn More About Azure Active Directory

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.
What is Azure Active Directory?
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.



Federation Service Properties

Federation Service display name: SSP ADFS

Example: Fabrikam Federation Service

Federation Service name: adfs.adssp.com

Example: fs.fabrikam.com

Federation Service identifier: http://adfs.adssp.com/adfs/services/trust

Example: http://fs.fabrikam.com/adfs/services/trust

Web SSO lifetime (minutes): 10

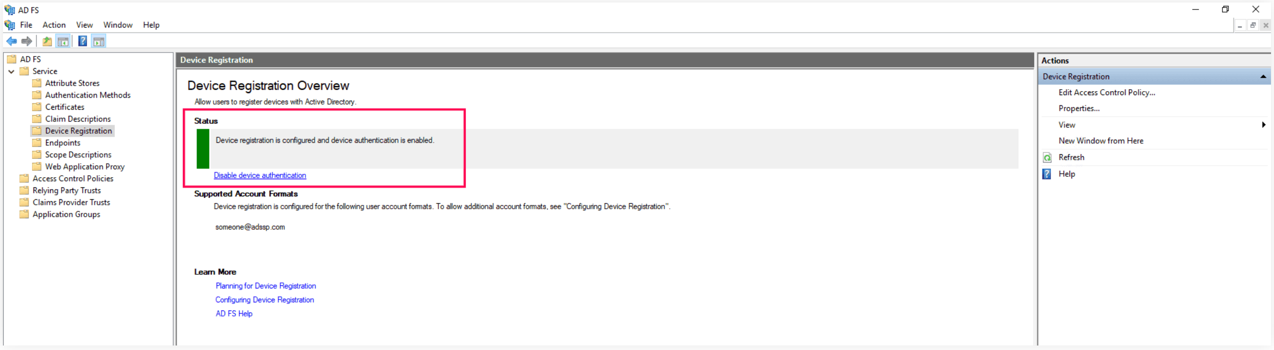
☐ Enable delegation for service administration

Delegate name:

☐ Allow Local System account for service administration

☑ Allow 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.



Device Registration Overview

Allow users to register devices with Active Directory.

Status

Device registration is configured and device authentication is enabled.

Disable device authentication

Supported Account Formats

Device registration is configured for the following user account formats. To allow additional account formats, see "Configuring Device Registration".

someone@adssp.com

Learn More

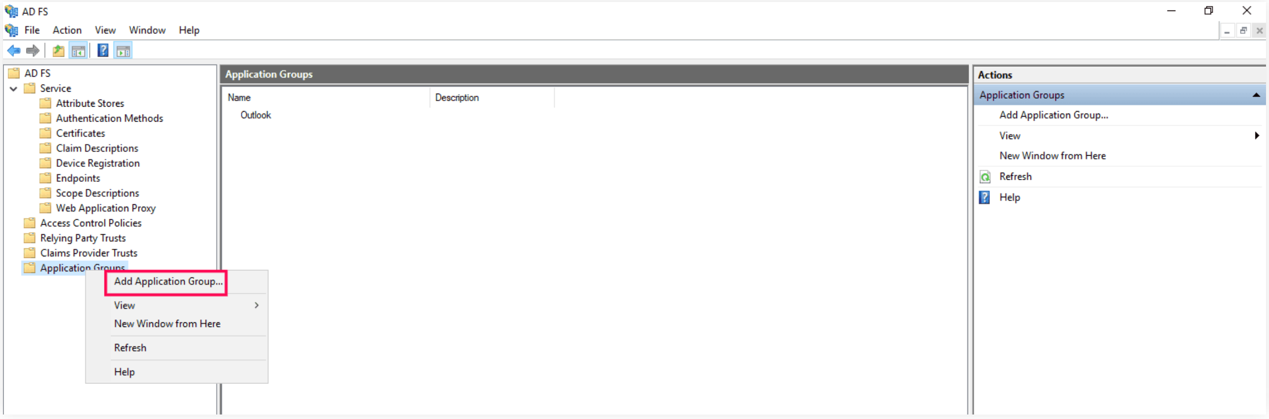
Planning for Device Registration

Configuring Device Registration

AD FS Help

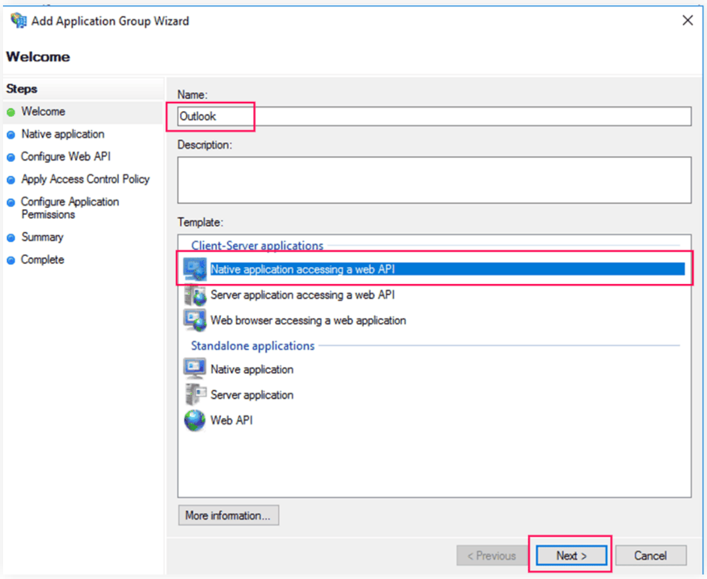
5. Configure an application group for modern authentication in Outlook on Windows:

a. Right-click on **Application Groups** and click **Add Application Group.**



Name	Description
Outlook	

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.**



Add Application Group Wizard

Welcome

Name: Outlook

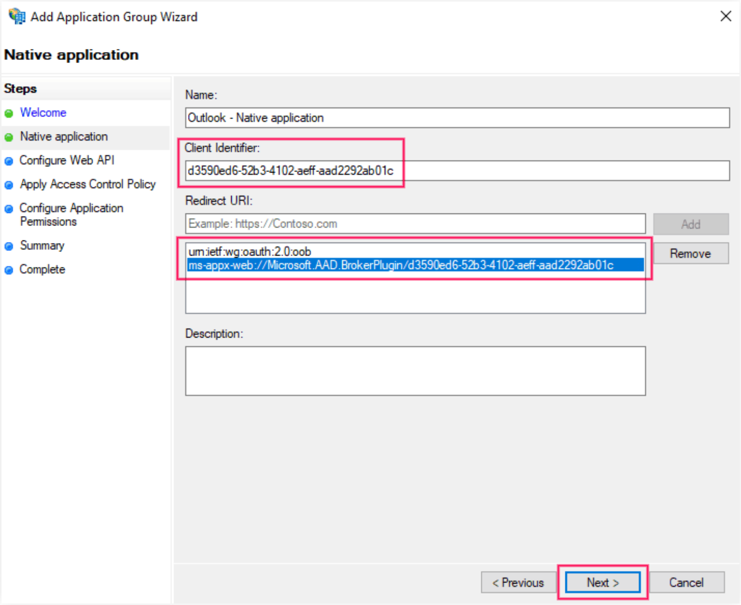
Description:

Template: Native application accessing a web API

Steps
Welcome
Native application
Configure Web API
Apply Access Control Policy
Configure Application Permissions
Summary
Complete
Client-Server applications
Native application accessing a web API
Server application accessing a web API
Web browser accessing a web application
Standalone applications
Native application
Server application
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 Wizard

Native application

Name: Outlook - Native application

Client Identifier: d3590ed6-52b3-4102-aeff-aad2292ab01c

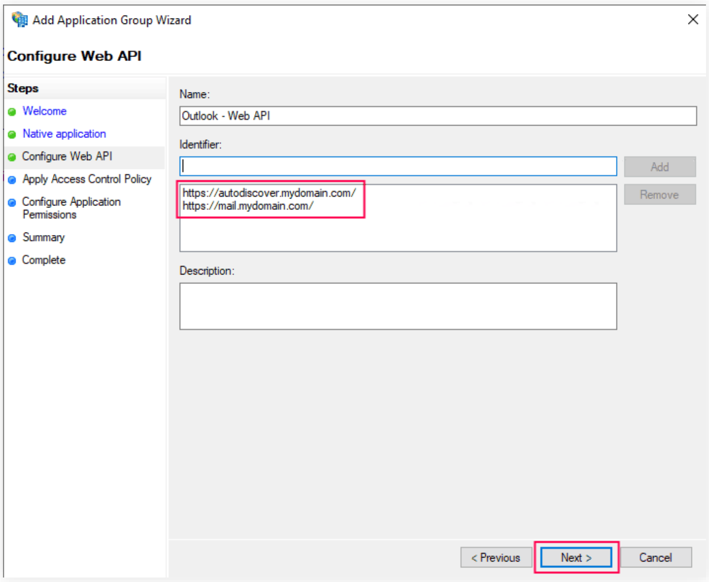
Redirect URI: Example: https://Contoso.com

urn:ietf:wg:oauth:2.0:oob
ms-appx-web://Microsoft.AAD.BrokerPlugin/d3590ed6-52b3-4102-aeff-aad2292ab01c

Description:

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/



Configure Web API

Name: Outlook - Web API

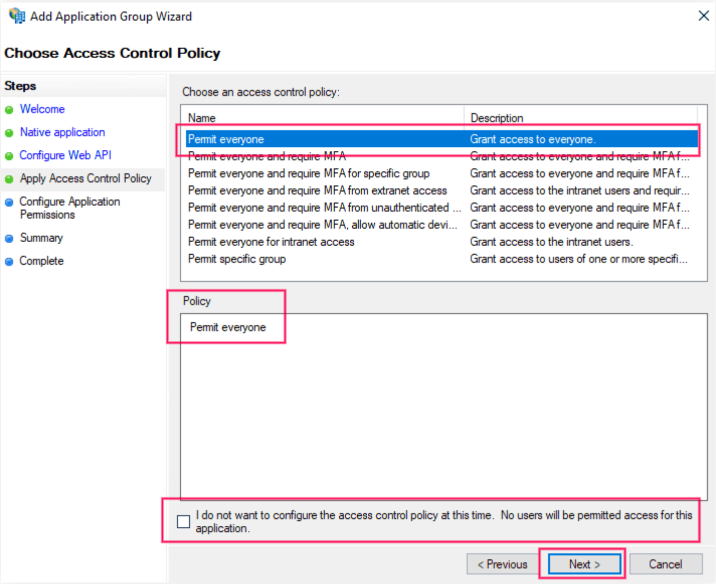
Identifier:

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

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.**



Add Application Group Wizard
Steps
Welcome
Native application
Configure Web API
Apply Access Control Policy
Configure Application Permissions
Summary
Complete
< Previous
Next >
Cancel

Choose Access Control Policy

Choose an access control policy:

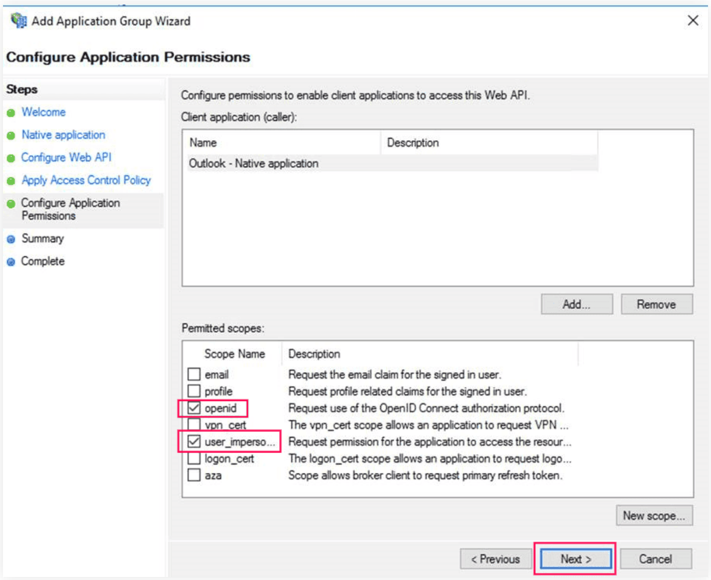
Name	Description
Permit everyone	Grant access to everyone.
Permit everyone and require MFA	Grant access to everyone and require MFA f...
Permit everyone and require MFA for specific group	Grant access to everyone and require MFA f...
Permit everyone and require MFA from extranet access	Grant access to the intranet users and requir...
Permit everyone and require MFA from unauthenticated ...	Grant access to everyone and require MFA f...
Permit everyone and require MFA, allow automatic devi...	Grant access to everyone and require MFA f...
Permit everyone for intranet access	Grant access to the intranet users.
Permit specific group	Grant access to users of one or more specifi...

Policy

Permit everyone

☐ I do not want to configure the access control policy at this time. No users will be permitted access for this application.

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.



Add Application Group Wizard

Configure Application Permissions

Steps
- Welcome
- Native application
- Configure Web API
- Apply Access Control Policy
- Configure Application Permissions
- Summary
- Complete

Configure permissions to enable client applications to access this Web API.

Client application (caller):

Name	Description
Outlook - Native application	

Add... Remove

Permitted scopes:

	Scope Name	Description
□	email	Request the email claim for the signed in user.
□	profile	Request profile related claims for the signed in user.
☑	openid	Request use of the OpenID Connect authorization protocol.
□	vpn_cert	The vpn_cert scope allows an application to request VPN ...
☑	user_imperso...	Request permission for the application to access the resour...
□	logon_cert	The logon_cert scope allows an application to request logo...
□	aza	Scope allows broker client to request primary refresh token.

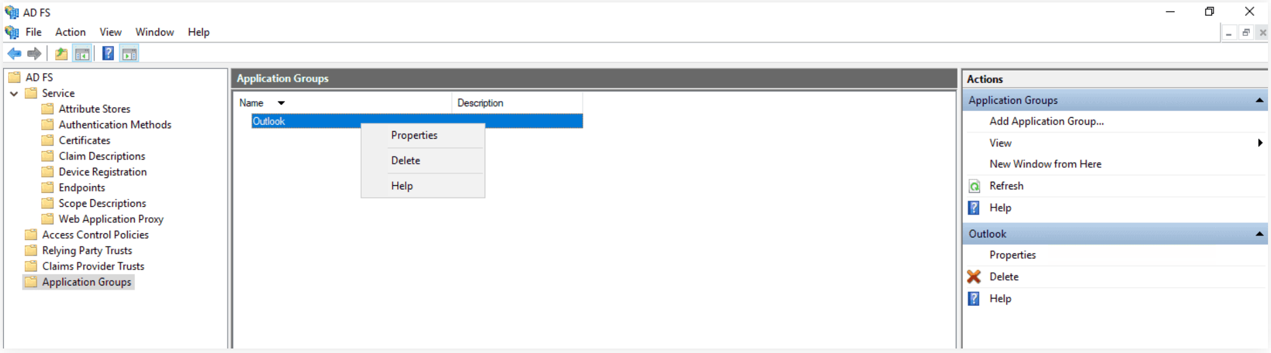
New scope...

< Previous Next > Cancel

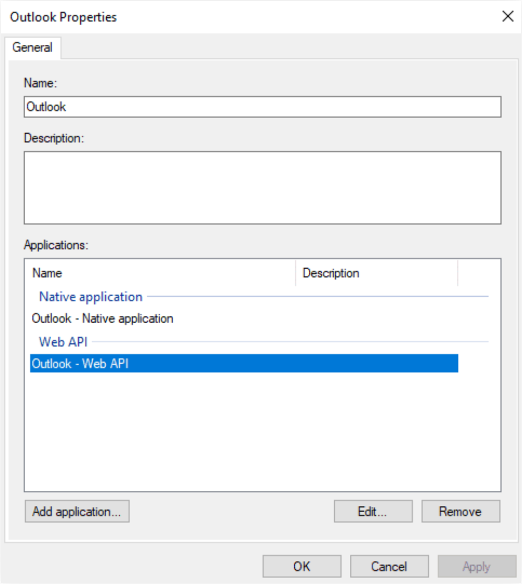
g. Click **Next** and complete the setup to create the application group.

6. Add **Issuance Transform Rules** to the newly created application group:

   a. Right-click on the Outlook application group and select **Properties.**



   b. Click **Edit** under **Web API** settings.



Outlook Properties

General

Name: Outlook

Description:

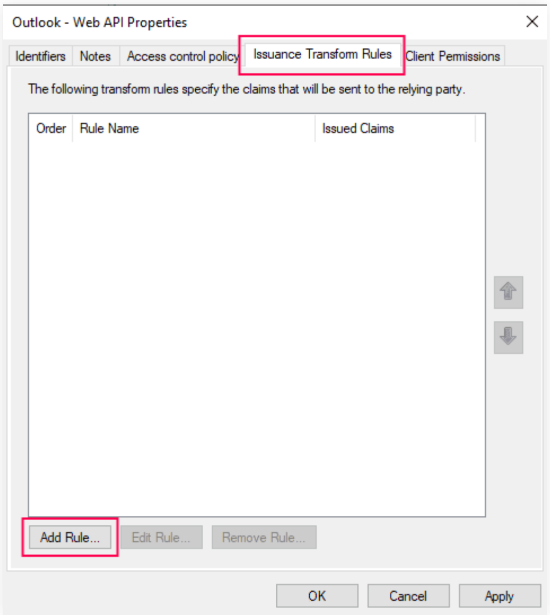
Applications:

Name	Description
Native application	
Outlook - Native application	
Web API	
Outlook - Web API	

Add application... Edit... Remove

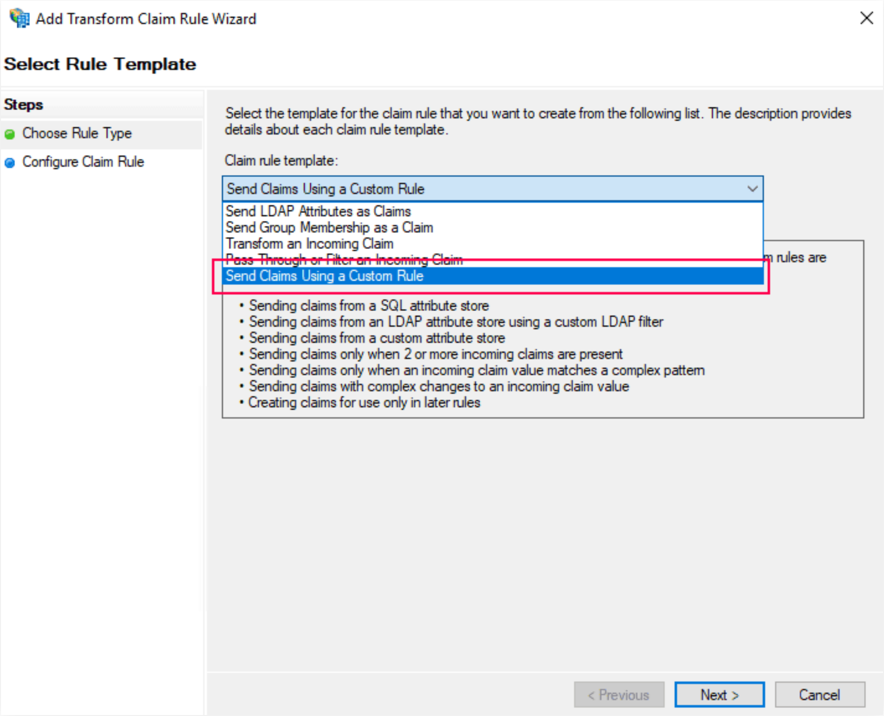
OK Cancel Apply

c. Under **Issuance Transform Rules**, click **Add Rule.**



The following transform rules specify the claims that will be sent to the relying party.

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


Add Transform Claim Rule Wizard
Select Rule Template
Steps
Choose Rule Type
Configure Claim Rule
Send LDAP Attributes as Claims
Send Group Membership as a Claim
Transform an Incoming Claim
Pass Through or Filter an Incoming Claim
Send Claims Using a Custom Rule
< Previous
Next >
Cancel

Select the template for the claim rule that you want to create from the following list. The description provides details about each claim rule template.

Claim rule template: Send Claims Using a Custom Rule

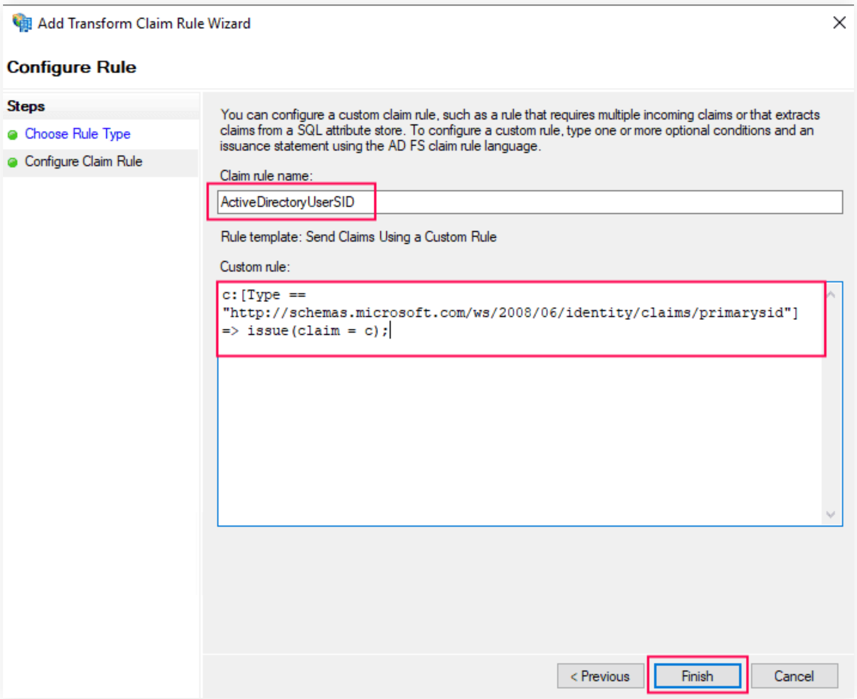
n rules are

- Sending claims from a SQL attribute store
- Sending claims from an LDAP attribute store using a custom LDAP filter
- Sending claims from a custom attribute store
- Sending claims only when 2 or more incoming claims 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.



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.

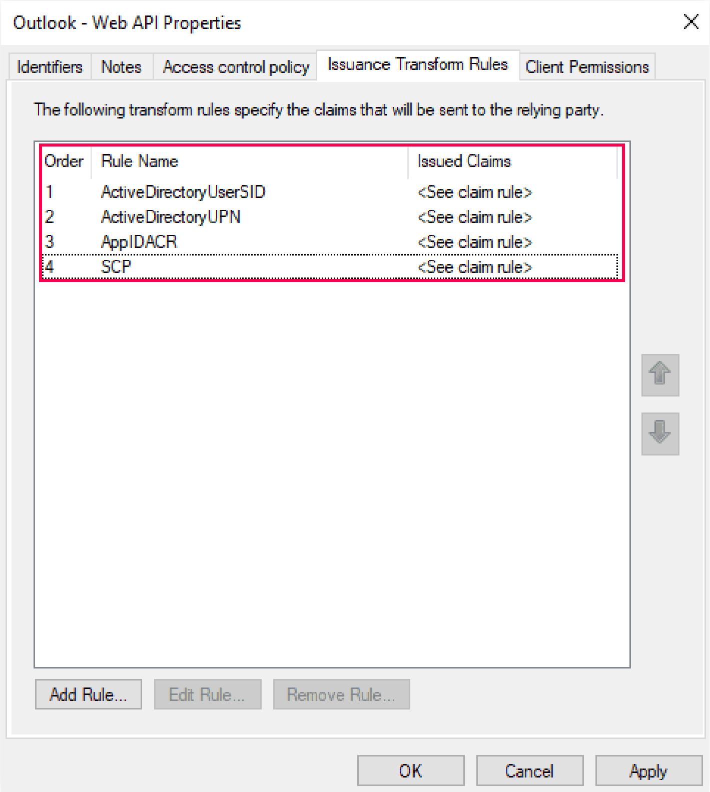
Claim rule name: ActiveDirectoryUserSID

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:



Outlook - Web API Properties

The following transform rules specify the claims that will be sent to the relying party.

Order	Rule Name	Issued Claims
1	ActiveDirectoryUserSID	<See claim rule>
2	ActiveDirectoryUPN	<See claim rule>
3	AppIDACR	<See claim rule>
4	SCP	<See claim 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. Setting the AD FS server as the default authorization endpoint.
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 here.

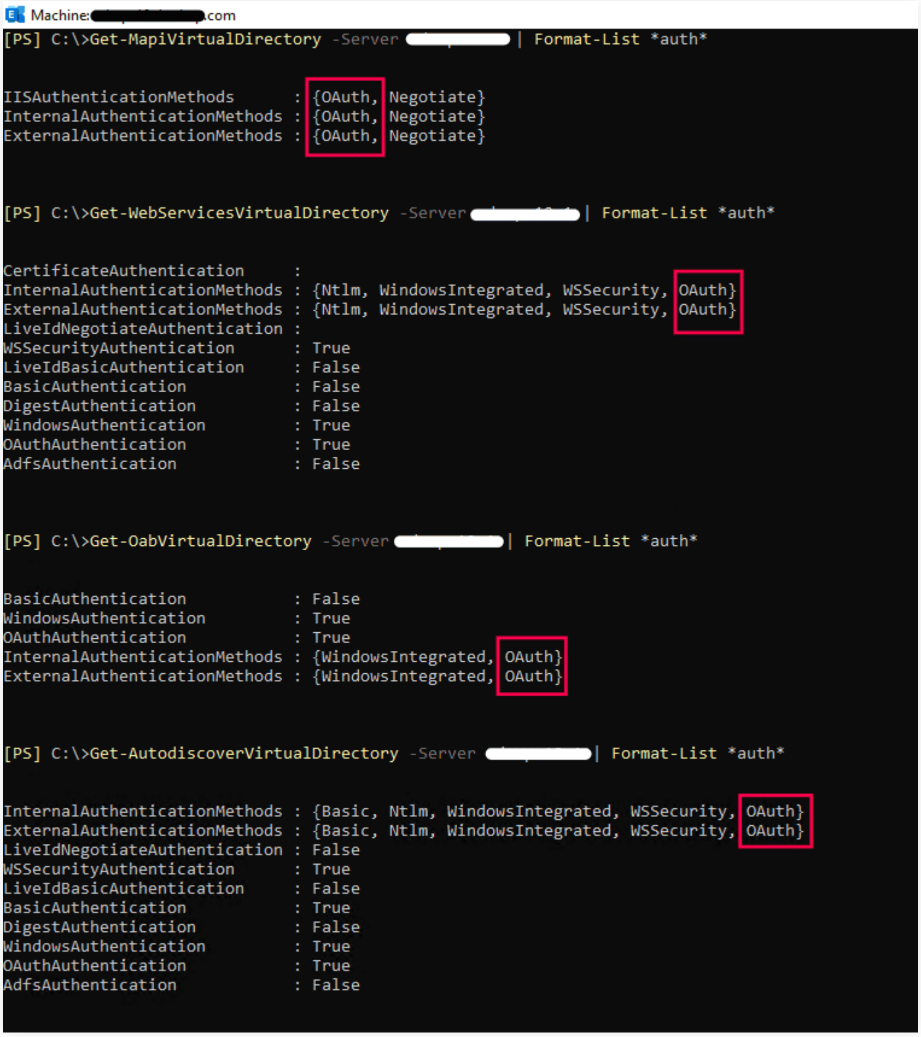
1. Verify that the virtual directories in your Exchange server are configured to use OAuth.

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.



Machine:[redacted].com

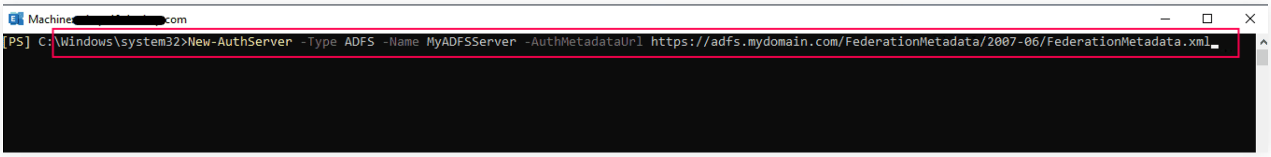
```
[PS] C:\>Get-MapiVirtualDirectory -Server [redacted] | Format-List *auth*

IISAuthenticationMethods      : {OAuth, Negotiate}
InternalAuthenticationMethods : {OAuth, Negotiate}
ExternalAuthenticationMethods : {OAuth, Negotiate}


[PS] C:\>Get-WebServicesVirtualDirectory -Server [redacted] | Format-List *auth*

CertificateAuthentication     :
InternalAuthenticationMethods : {Ntlm, WindowsIntegrated, WSSecurity, OAuth}
ExternalAuthenticationMethods : {Ntlm, WindowsIntegrated, WSSecurity, OAuth}
LiveIdNegotiateAuthentication :
WSSecurityAuthentication      : True
LiveIdBasicAuthentication     : False
BasicAuthentication           : False
DigestAuthentication          : False
WindowsAuthentication         : True
OAuthAuthentication           : True
AdfsAuthentication            : False


[PS] C:\>Get-OabVirtualDirectory -Server [redacted] | Format-List *auth*

BasicAuthentication           : False
WindowsAuthentication         : True
OAuthAuthentication           : True
InternalAuthenticationMethods : {WindowsIntegrated, OAuth}
ExternalAuthenticationMethods : {WindowsIntegrated, OAuth}


[PS] C:\>Get-AutodiscoverVirtualDirectory -Server [redacted] | Format-List *auth*

InternalAuthenticationMethods : {Basic, Ntlm, WindowsIntegrated, WSSecurity, OAuth}
ExternalAuthenticationMethods : {Basic, Ntlm, WindowsIntegrated, WSSecurity, OAuth}
LiveIdNegotiateAuthentication : False
WSSecurityAuthentication      : True
LiveIdBasicAuthentication     : False
BasicAuthentication           : True
DigestAuthentication          : False
WindowsAuthentication         : True
OAuthAuthentication           : True
AdfsAuthentication            : False
```

2. Register your AD FS server as the authentication server

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.



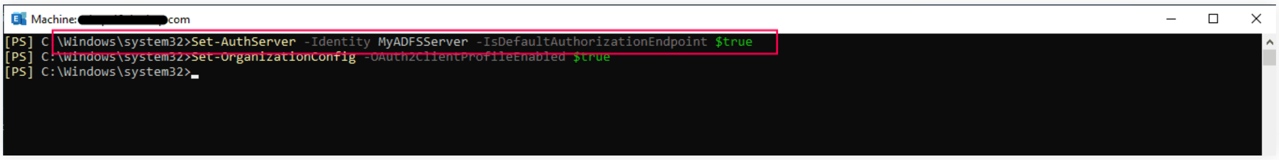
Machine[redacted]com

```
[PS] C:\Windows\system32>New-AuthServer -Type ADFS -Name MyADFSServer -AuthMetadataUrl https://adfs.mydomain.com/FederationMetadata/2007-06/FederationMetadata.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:

```
Set-AuthServer -Identity <MyADFSServer> -IsDefaultAuthorizationEndpoint $true
```



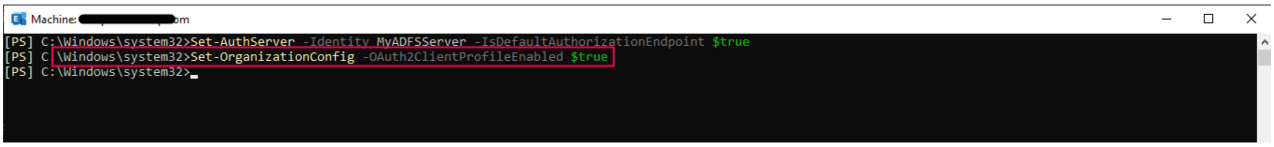
Machine: [redacted]com

```
[PS] C:\Windows\system32>Set-AuthServer -Identity MyADFSServer -IsDefaultAuthorizationEndpoint $true
[PS] C:\Windows\system32>Set-OrganizationConfig -OAuth2ClientProfileEnabled $true
[PS] C:\Windows\system32>_
```

4. Enable modern authentication at the organizational level

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

```
Set-OrganizationConfig -OAuth2ClientProfileEnabled $true
```



Machine: [redacted]om

```
[PS] C:\Windows\system32>Set-AuthServer -Identity MyADFSServer -IsDefaultAuthorizationEndpoint $true
[PS] C:\Windows\system32>Set-OrganizationConfig -OAuth2ClientProfileEnabled $true
[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:

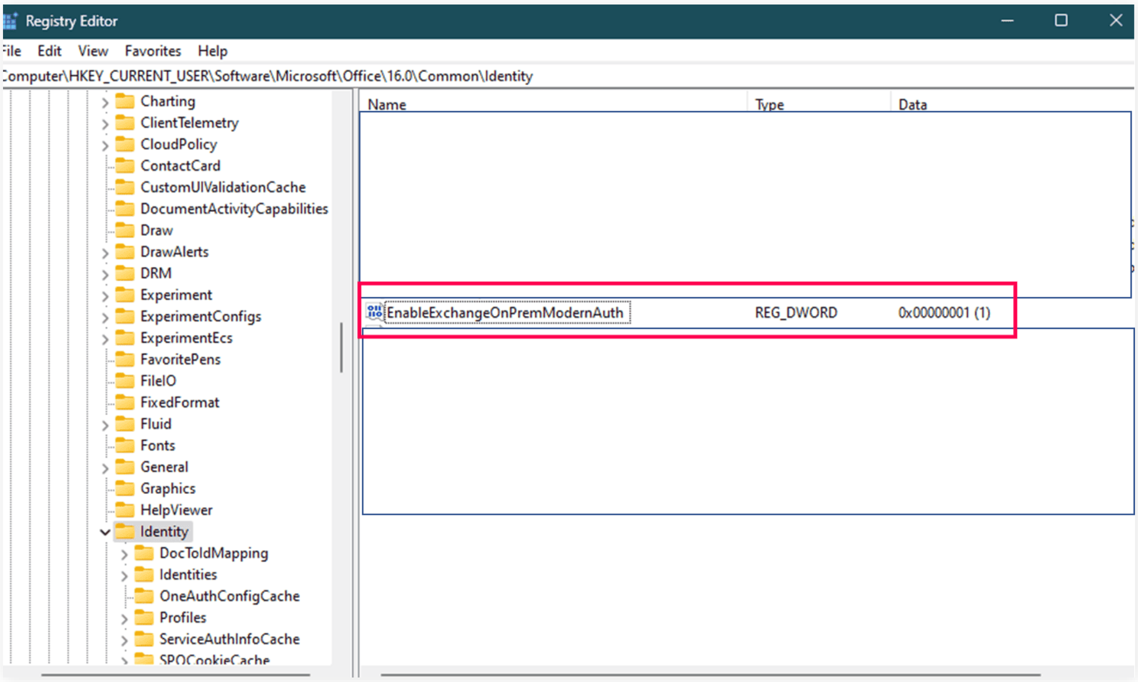
- Enable modern authentication via AD FS for Outlook
- Add AD FS as a trusted domain

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



Computer\HKEY_CURRENT_USER\Software\Microsoft\Office\16.0\Common\Identity

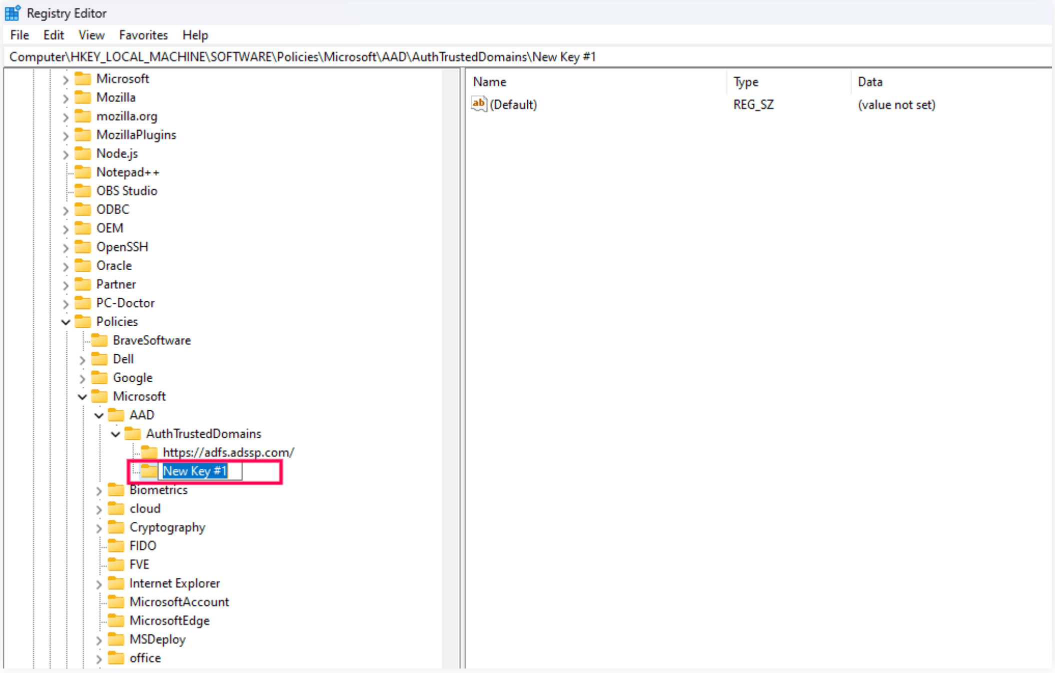
Name	Type	Data
EnableExchangeOnPremModernAuth	REG_DWORD	0x00000001 (1)

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:

1. 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.



Computer\HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\AAD\AuthTrustedDomains\New Key #1

Name	Type	Data
(Default)	REG_SZ	(value not set)

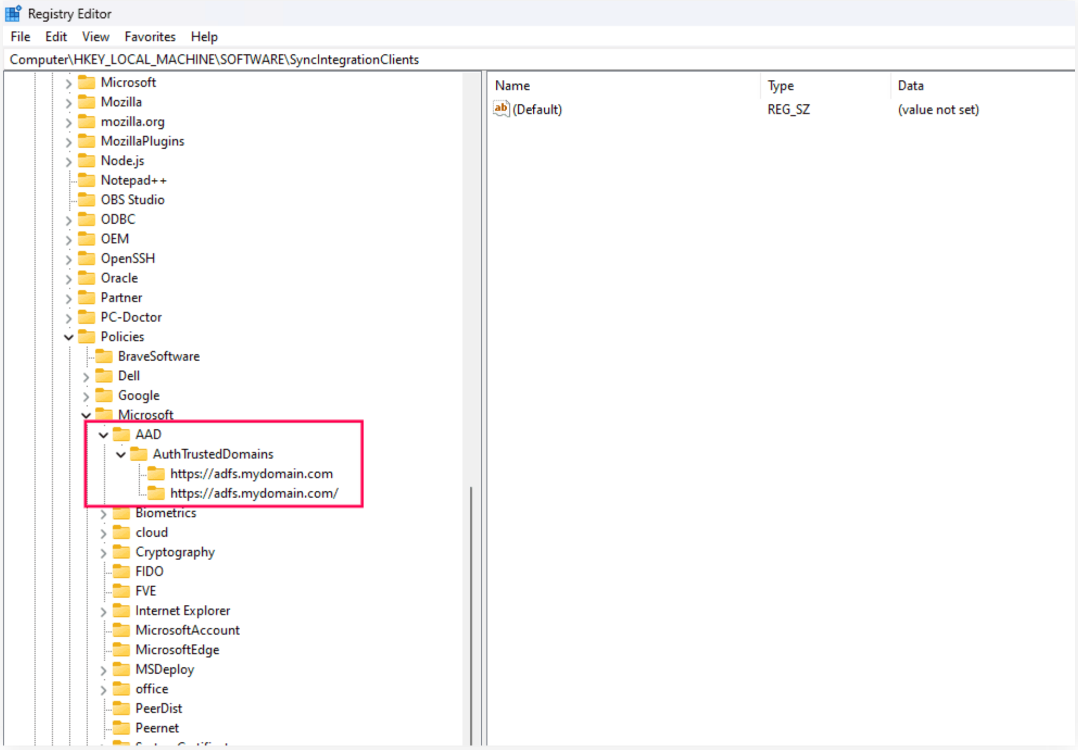
3. Rename *New Key #1* as your AD FS domain URL. Create another key and rename it to your AD FS domain URL, and append a forward-slash (/) to it.

   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.



Computer\HKEY_LOCAL_MACHINE\SOFTWARE\SyncIntegrationClients

Name	Type	Data
(Default)	REG_SZ	(value not set)

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.

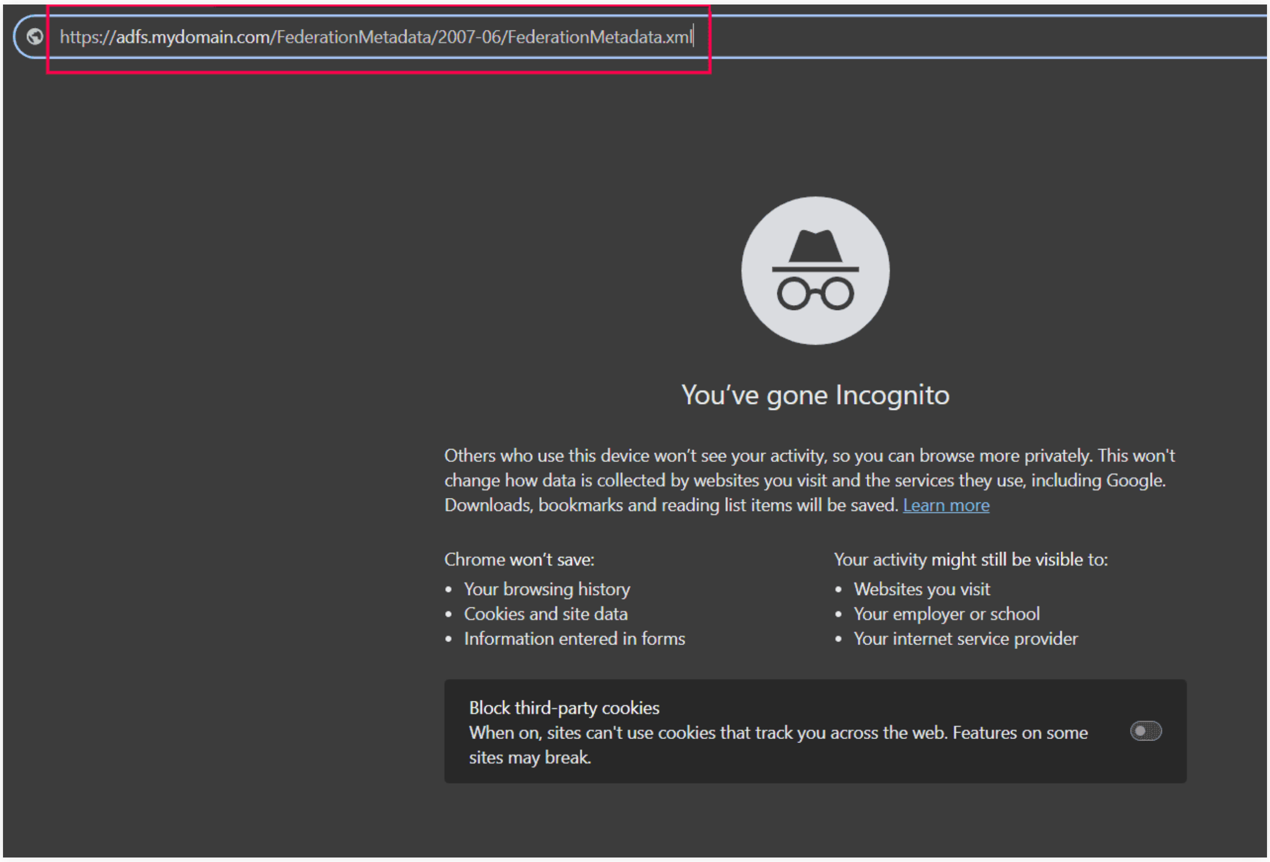
- Set up ADSelfService Plus to authenticate Outlook users
- Configure the AD FS server to delegate authentication to ADSelfService Plus

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.



https://adfs.mydomain.com/FederationMetadata/2007-06/FederationMetadata.xml

You've gone Incognito

Others who use this device won't see your activity, so you can browse more privately. This won't change how data is collected by websites you visit and the services they use, including Google. Downloads, bookmarks and reading list items will be saved. Learn more

Chrome won't save:

- Your browsing history
- Cookies and site data
- Information entered in forms

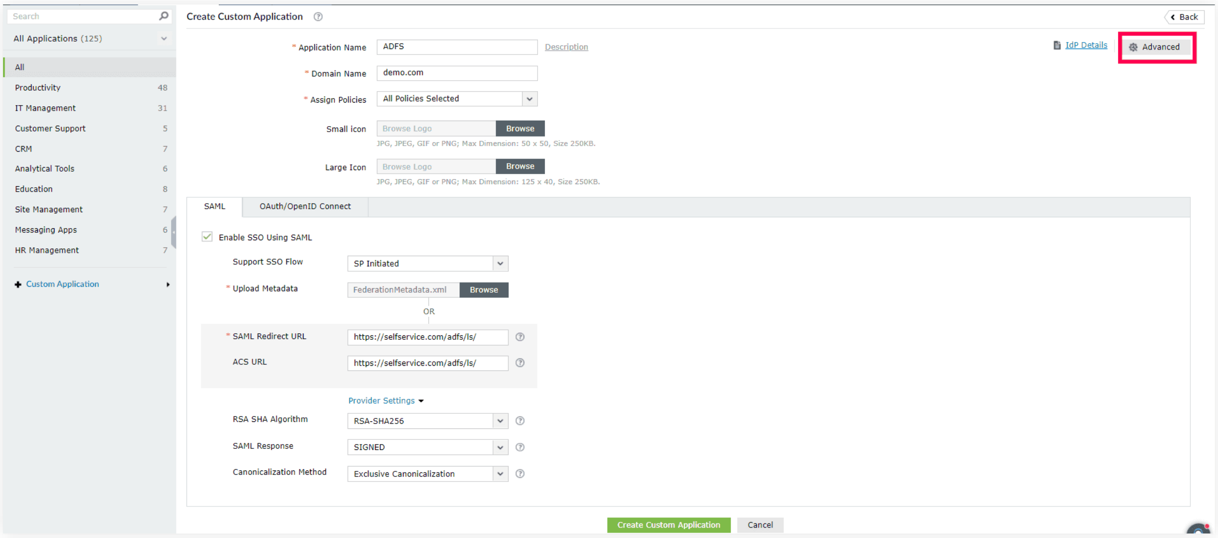
Your activity might still be visible to:

- Websites you visit
- Your employer or school
- Your internet service provider

Block third-party cookies
When on, sites can't use cookies that track you across the web. Features on some sites may break.

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.



Create Custom Application

* Application Name: ADFS

* Domain Name: demo.com

* Assign Policies: All Policies Selected

Small icon: Browse Logo
JPG, JPEG, GIF or PNG; Max Dimension: 50 x 50, Size 250KB.

Large Icon: Browse Logo
JPG, JPEG, GIF or PNG; Max Dimension: 125 x 40, Size 250KB.

☑ Enable SSO Using SAML

Support SSO Flow: SP Initiated

* Upload Metadata: FederationMetadata.xml

* SAML Redirect URL: https://selfservice.com/adfs/ls/

ACS URL: https://selfservice.com/adfs/ls/

RSA SHA Algorithm: RSA-SHA256

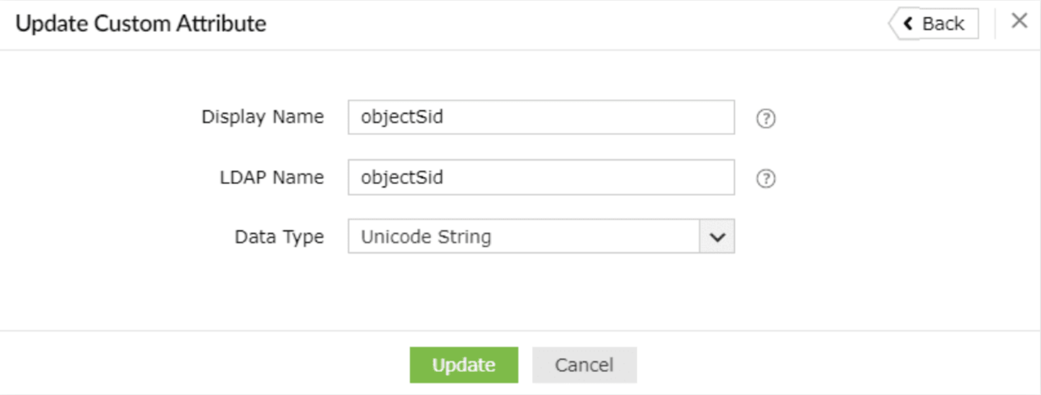
SAML Response: SIGNED

Canonicalization Method: Exclusive Canonicalization

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.**

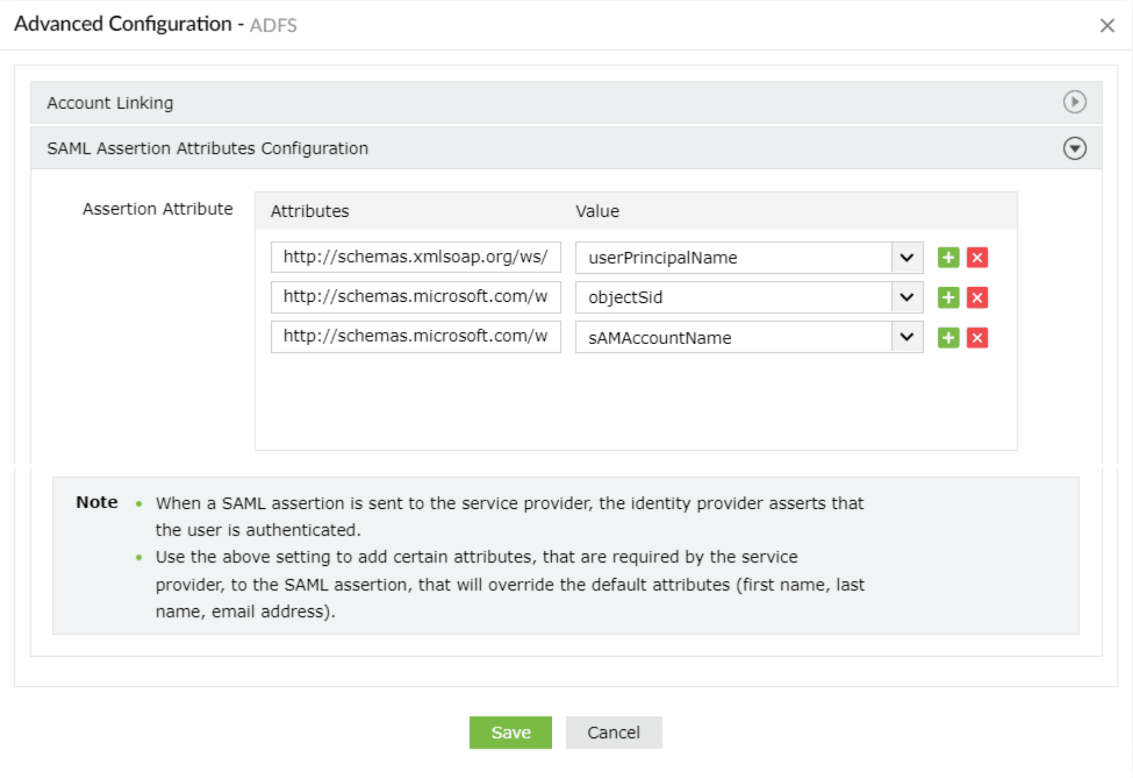

Update Custom Attribute

Display Name: objectSid

LDAP Name: objectSid

Data Type: Unicode String

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.


Advanced Configuration - ADFS

Account Linking

SAML Assertion Attributes Configuration

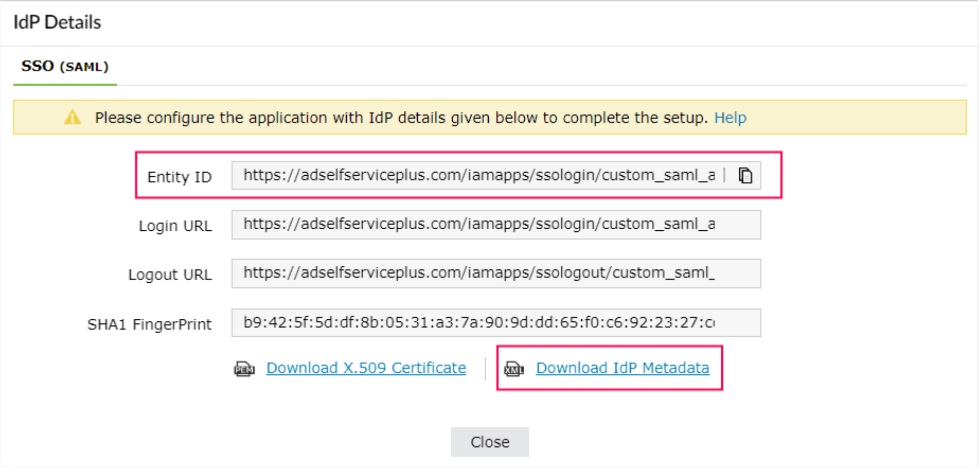
Assertion Attribute

Attributes	Value
http://schemas.xmlsoap.org/ws/	userPrincipalName
http://schemas.microsoft.com/w	objectSid
http://schemas.microsoft.com/w	sAMAccountName

Note
- When a SAML assertion is sent to the service provider, the identity provider asserts that the user is authenticated.
- Use the above setting to add certain attributes, that are required by the service provider, to the SAML assertion, that will override the default attributes (first name, last name, email address).

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.



IdP Details

SSO (SAML)

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

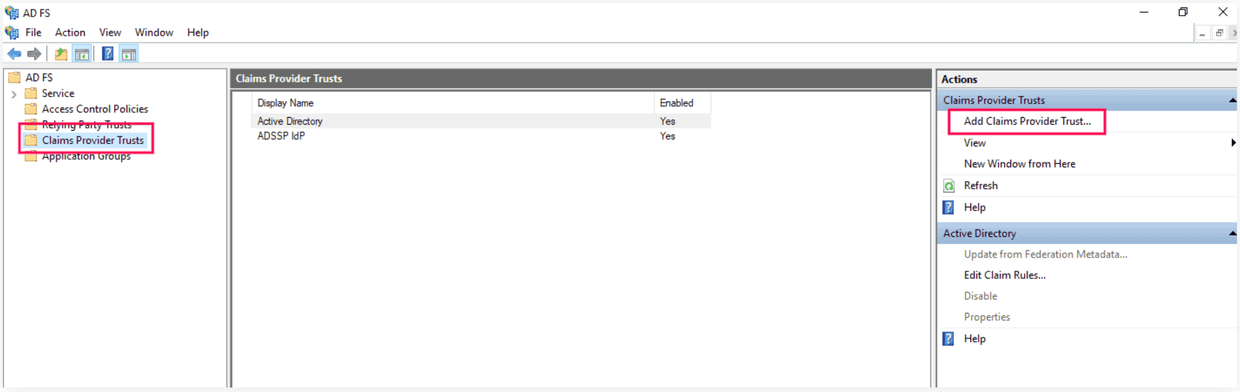
Configure the AD FS server to delegate authentication to ADSelfService Plus

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

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

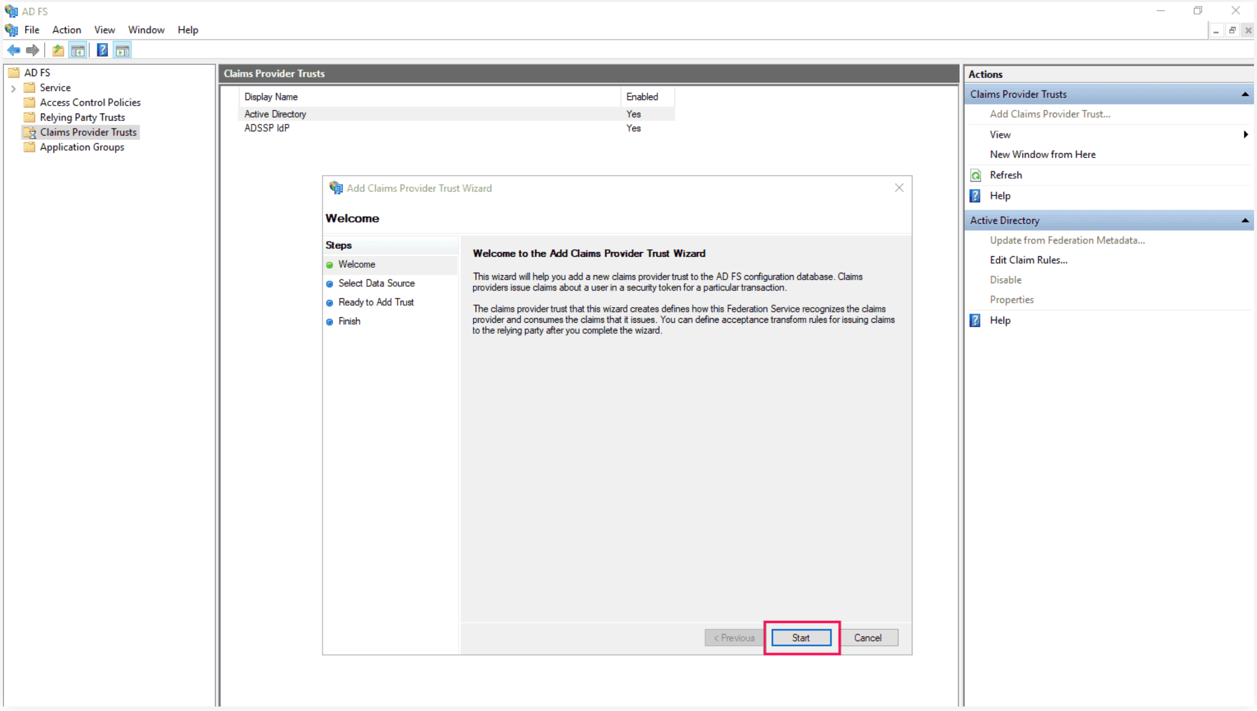
Step 1: Adding a new claims provider trust

1. 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.**



Display Name	Enabled
Active Directory	Yes
ADSSP IdP	Yes

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



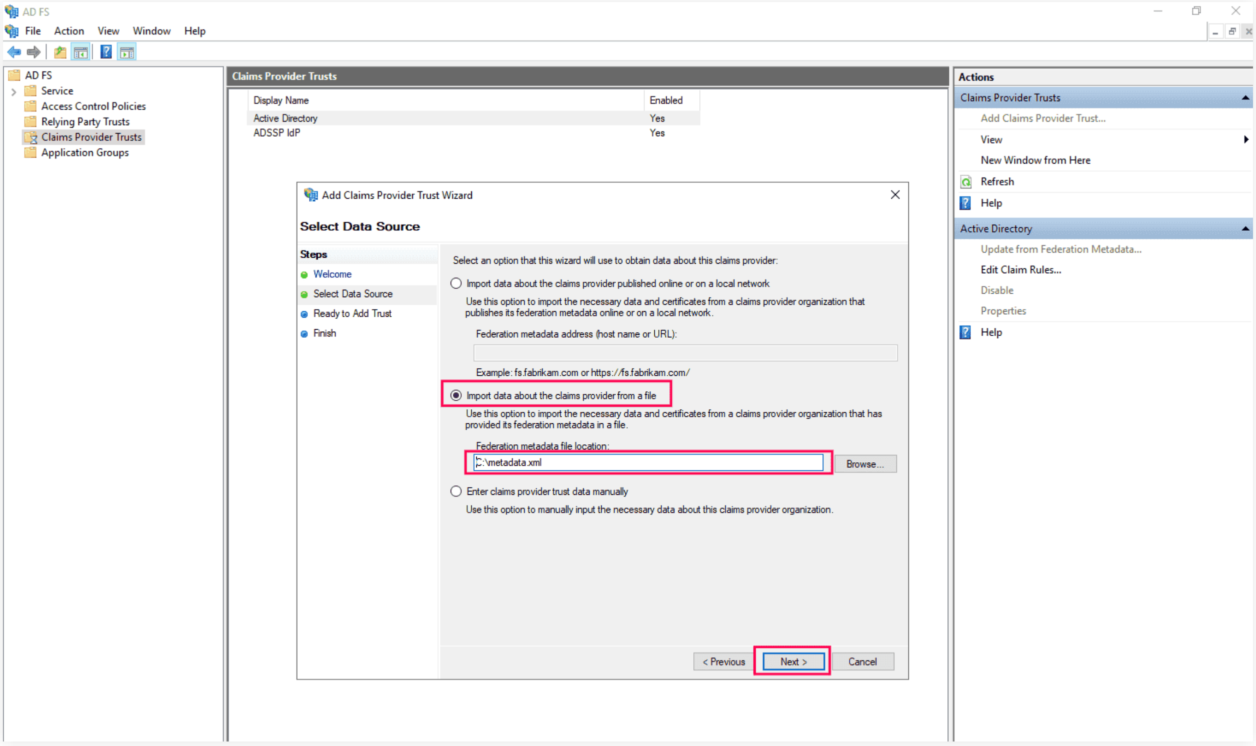
Display Name	Enabled
Active Directory	Yes
ADSSP IdP	Yes

Welcome to the Add Claims Provider Trust Wizard

This wizard will help you add a new claims provider trust to the AD FS configuration database. Claims providers issue claims about a user in a security token for a particular transaction.

The claims provider trust that this wizard creates defines how this Federation Service recognizes the claims provider and consumes the claims that it issues. You can define acceptance transform rules for issuing claims to the relying party after you complete the wizard.

3. In the *Select Data Source* section, choose **Import data about the claims provider from a file** and upload the metadata file downloaded in [Step 11]() of the ADSelfService Plus configuration steps. Click **Next.**



Display Name	Enabled
Active Directory	Yes
ADSSP IdP	Yes

Select an option that this wizard will use to obtain data about this claims provider:

○ Import data about the claims provider published online or on a local network

Use this option to import the necessary data and certificates from a claims provider organization that publishes its federation metadata online or on a local network.

Federation metadata address (host name or URL):

Example: fs.fabrikam.com or https://fs.fabrikam.com/

● Import data about the claims provider from a file

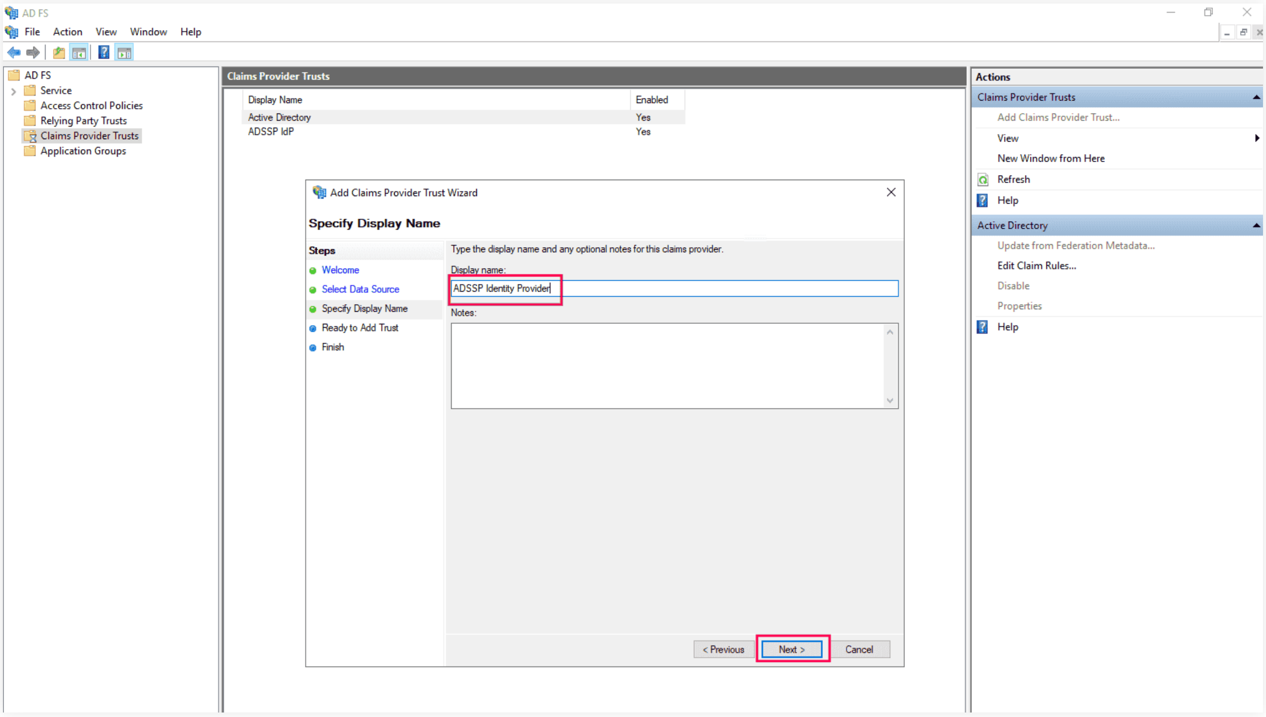
Use this option to import the necessary data and certificates from a claims provider organization that has provided its federation metadata in a file.

Federation metadata file location: C:\metadata.xml

○ Enter claims provider trust data manually

Use this option to manually input the necessary data about this claims provider organization.

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



Claims Provider Trusts

Display Name	Enabled
Active Directory	Yes
ADSSP IdP	Yes

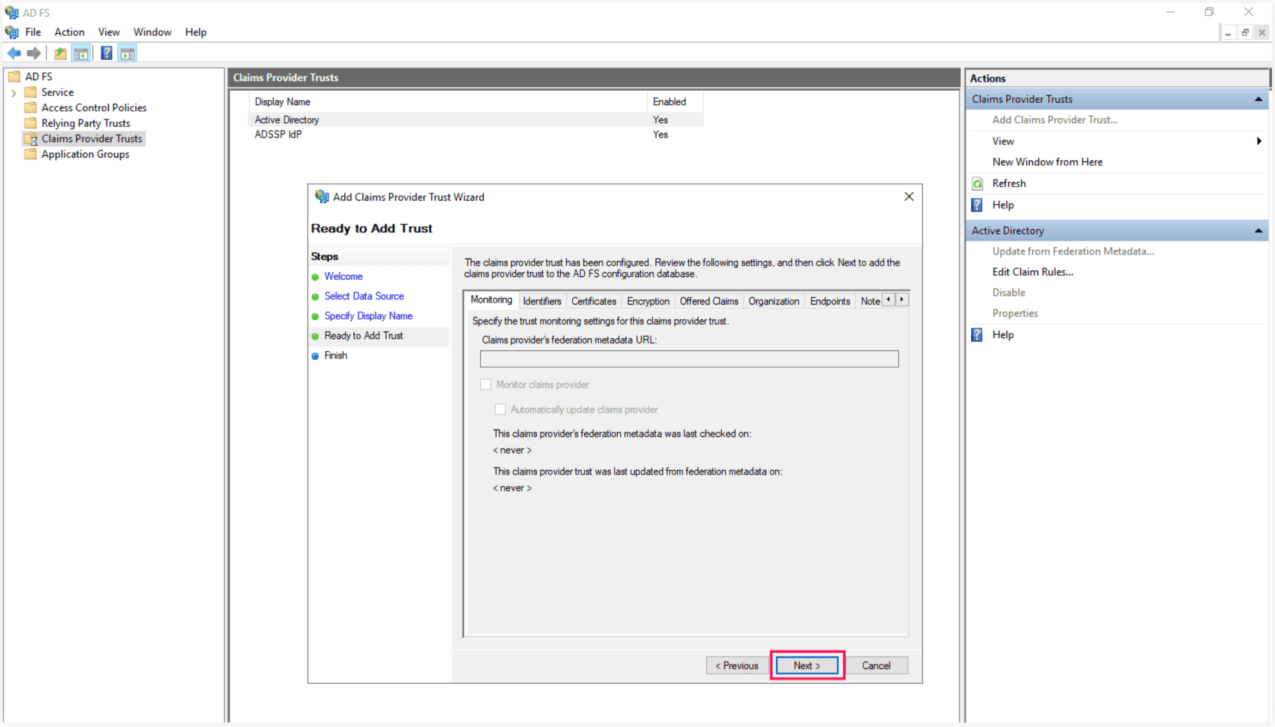
Add Claims Provider Trust Wizard

Specify Display Name

Type the display name and any optional notes for this claims provider.

Display name: ADSSP Identity Provider

Notes:



Claims Provider Trusts

Display Name	Enabled
Active Directory	Yes
ADSSP IdP	Yes

Add Claims Provider Trust Wizard

Ready to Add Trust

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.

Specify the trust monitoring settings for this claims provider trust.

Claims provider's federation metadata URL:

□ Monitor claims provider

□ Automatically update claims provider

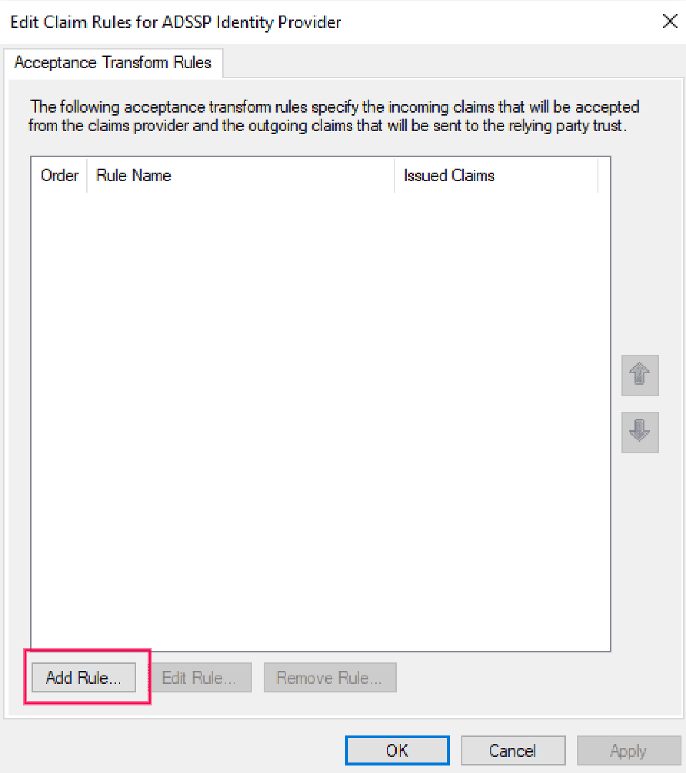
This claims provider's federation metadata was last checked on:
< never >

This claims provider trust was last updated from federation metadata on:
< never >

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

Step 2: Adding claims rules

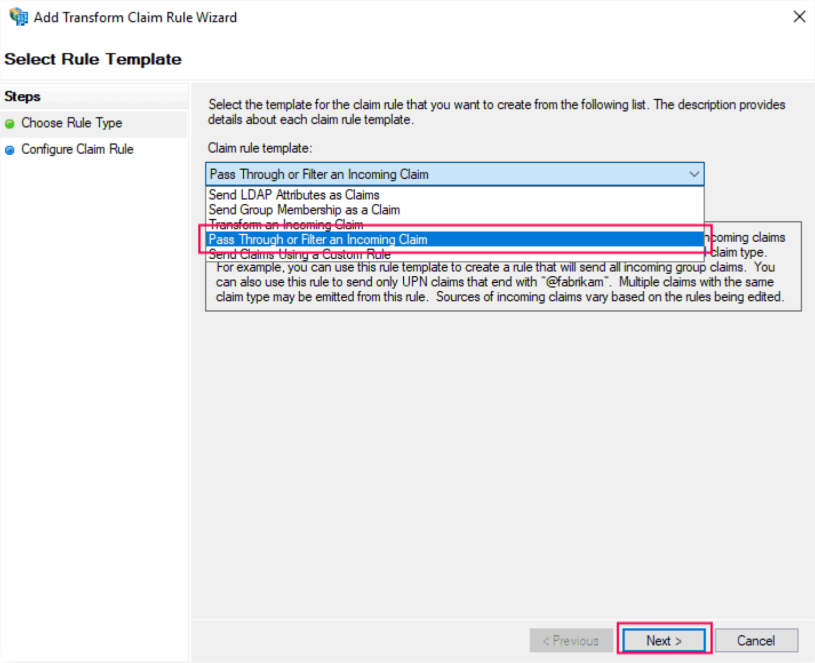
1. Once the claims provider trust configuration is complete, the *Edit Claims Rule for ADSSP Identity Provider* editor window opens. Click **Add Rule.**



Edit Claim Rules for ADSSP Identity Provider

The following acceptance transform rules specify the incoming claims that will be accepted from the claims provider and the outgoing claims that will be sent to the relying party trust.

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



Add Transform Claim Rule Wizard

Select Rule Template

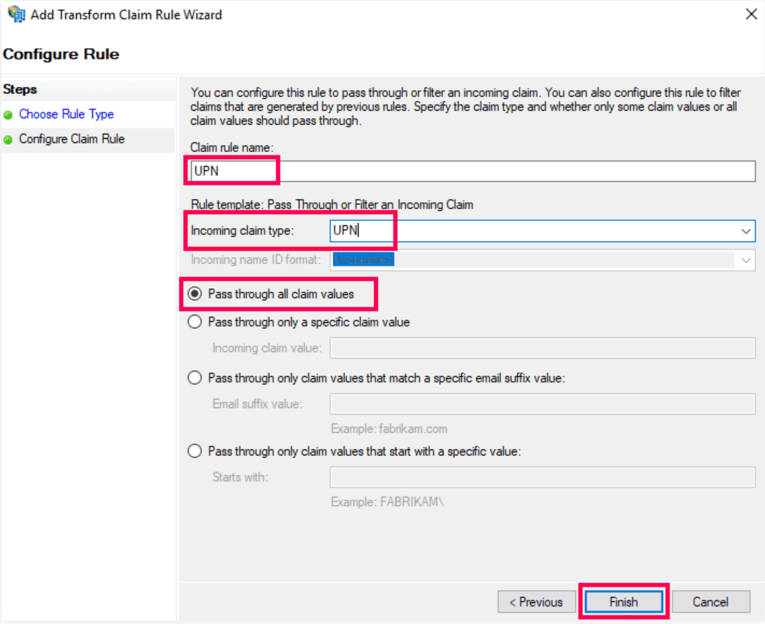
Select the template for the claim rule that you want to create from the following list. The description provides details about each claim rule template.

Claim rule template: Pass Through or Filter an Incoming Claim

ncoming claims 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 vary based on the rules being edited.

Steps
Choose Rule Type
Configure Claim Rule
Send LDAP Attributes as Claims
Send Group Membership as a Claim
Transform an Incoming Claim
Pass Through or Filter an Incoming Claim
Send Claims Using a Custom Rule
< Previous
Next >
Cancel

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.



Configure Rule

You can configure this rule to pass through or filter an incoming claim. You can also configure this rule to filter claims that are generated by previous rules. Specify the claim type and whether only some claim values or all claim values should pass through.

Claim rule name: UPN

Rule template: Pass Through or Filter an Incoming Claim

Incoming claim type: UPN

Incoming name ID format: Unspecified

● Pass through all claim values

○ Pass through only a specific claim value

Incoming claim value:

○ Pass through only claim values that match a specific email suffix value:

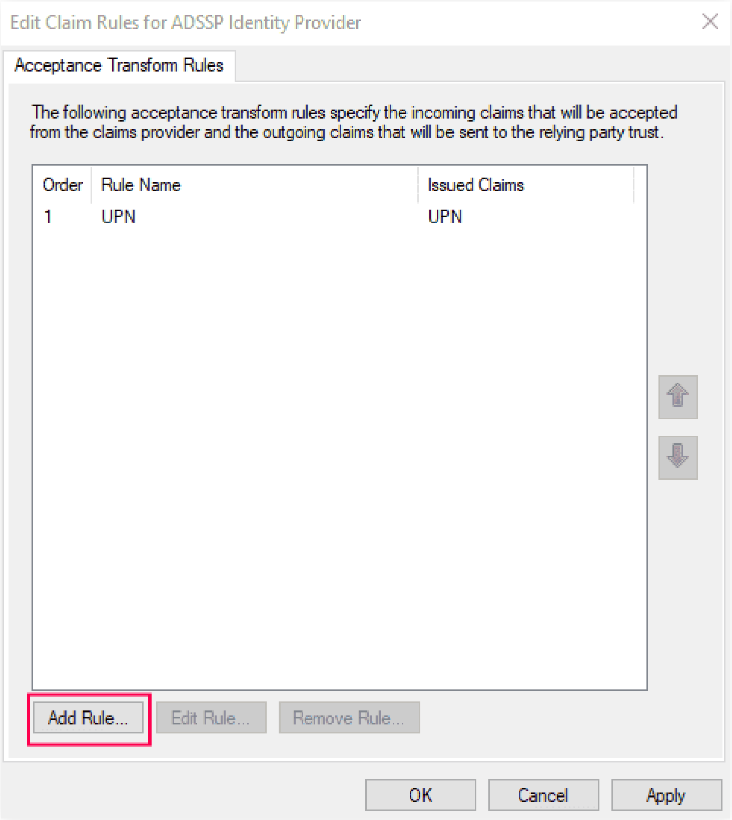
Email suffix value:

Example: fabrikam.com

○ Pass through only claim values that start with a specific value:

Starts with:

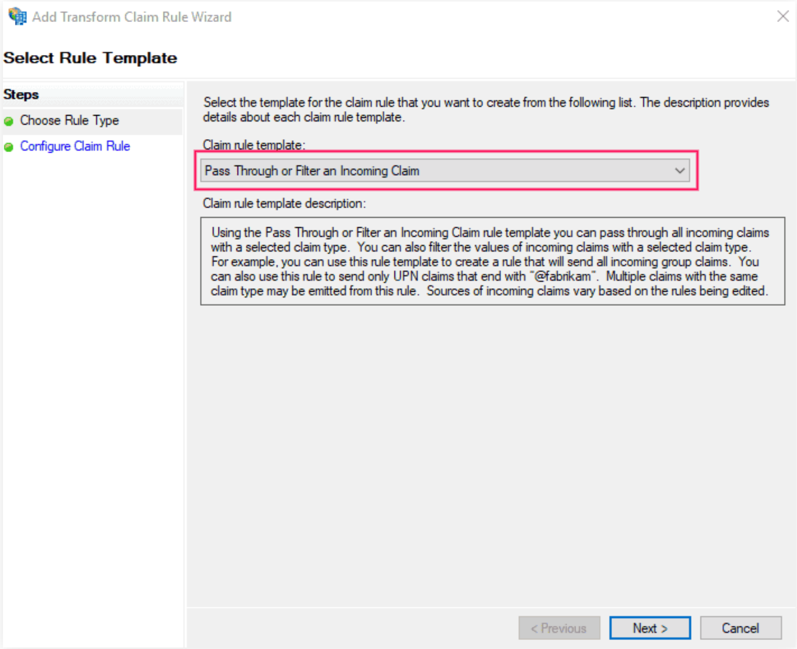
Example: FABRIKAM\


Edit Claim Rules for ADSSP Identity Provider
Acceptance Transform Rules
Add Rule...
Edit Rule...
Remove Rule...
OK
Cancel
Apply

The following acceptance transform rules specify the incoming claims that will be accepted from the claims provider and the outgoing claims that will be sent to the relying party trust.

Order	Rule Name	Issued Claims
1	UPN	UPN

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 Rule Template

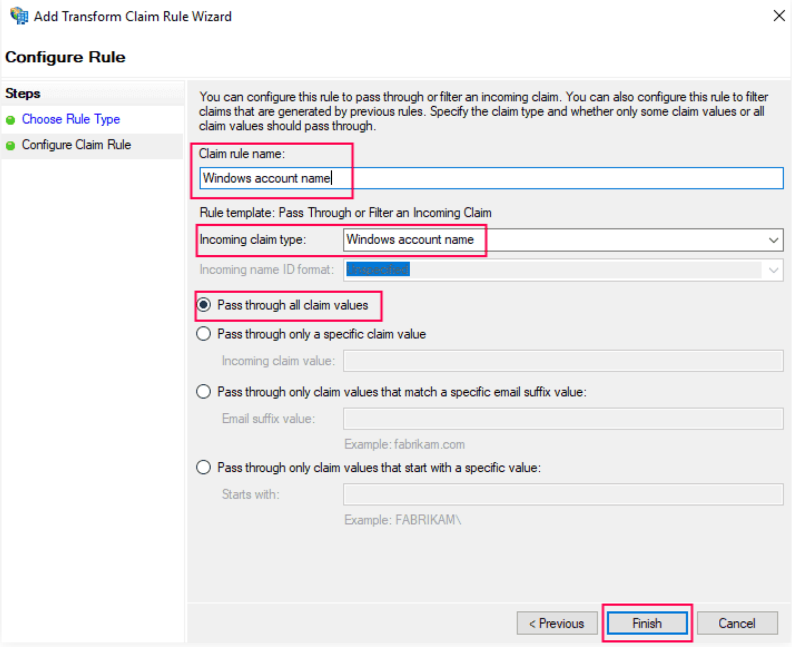
Select the template for the claim rule that you want to create from the following list. The description provides details about each claim rule template.

Claim rule template: Pass Through or Filter an Incoming Claim

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 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.**



Configure Rule

You can configure this rule to pass through or filter an incoming claim. You can also configure this rule to filter claims that are generated by previous rules. Specify the claim type and whether only some claim values or all claim values should pass through.

Claim rule name: Windows account name

Rule template: Pass Through or Filter an Incoming Claim

Incoming claim type: Windows account name

Incoming name ID format:

● Pass through all claim values

○ Pass through only a specific claim value

Incoming claim value:

○ Pass through only claim values that match a specific email suffix value:

Email suffix value:

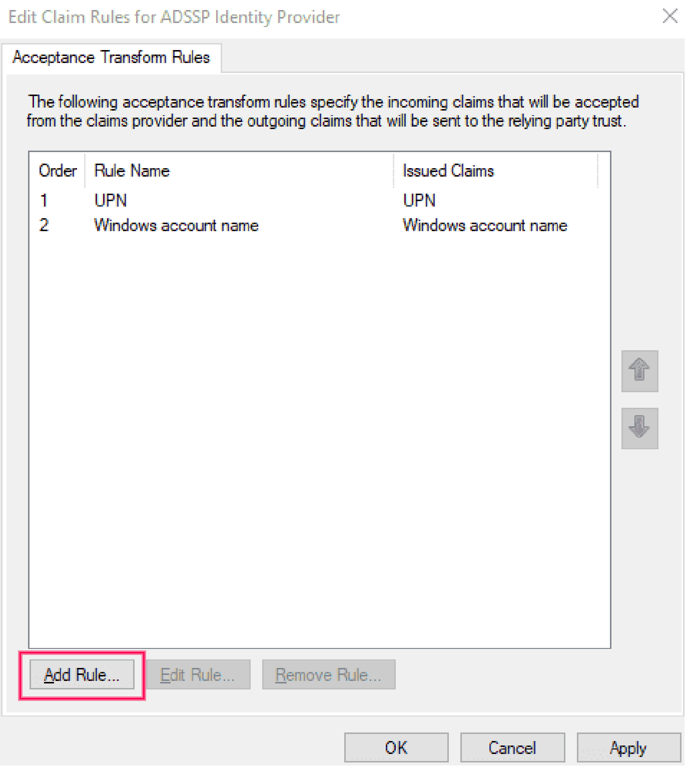
Example: fabrikam.com

○ Pass through only claim values that start with a specific value:

Starts with:

Example: FABRIKAM\

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.



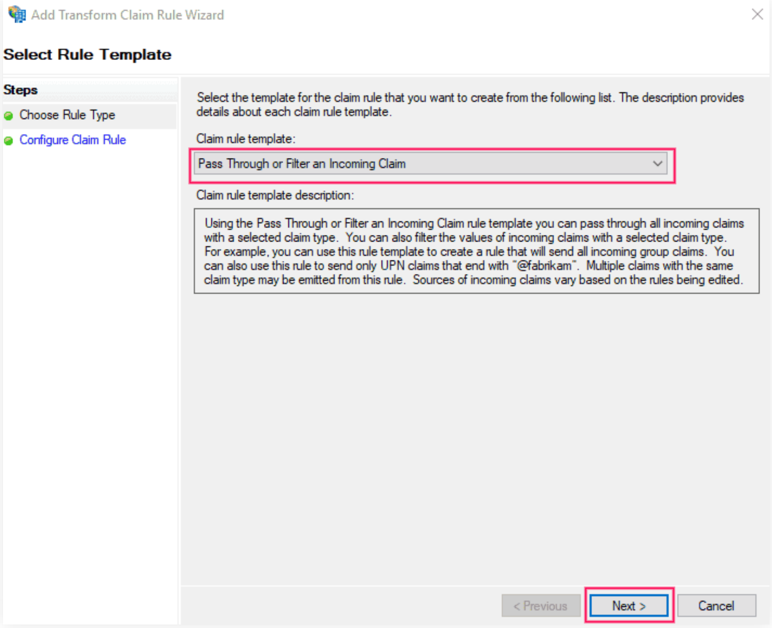
Edit Claim Rules for ADSSP Identity Provider

Acceptance Transform Rules

The following acceptance transform rules specify the incoming claims that will be accepted from the claims provider and the outgoing claims that will be sent to the relying party trust.

Order	Rule Name	Issued Claims
1	UPN	UPN
2	Windows account name	Windows account name

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



Add Transform Claim Rule Wizard

Select Rule Template

Steps
- Choose Rule Type
- Configure Claim Rule

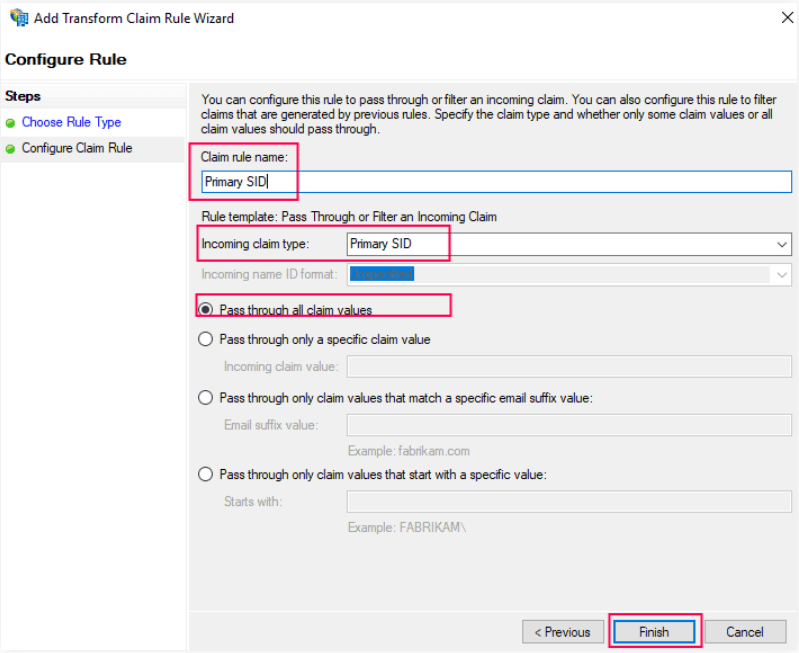
Select the template for the claim rule that you want to create from the following list. The description provides details about each claim rule template.

Claim rule template: Pass Through or Filter an Incoming Claim

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 vary 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.**



Add Transform Claim Rule Wizard

Configure Rule

Steps
- Choose Rule Type
- Configure Claim Rule

You can configure this rule to pass through or filter an incoming claim. You can also configure this rule to filter claims that are generated by previous rules. Specify the claim type and whether only some claim values or all claim values should pass through.

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

○ Pass through only a specific claim value

Incoming claim value:

○ Pass through only claim values that match a specific email suffix value:

Email suffix value:

Example: fabrikam.com

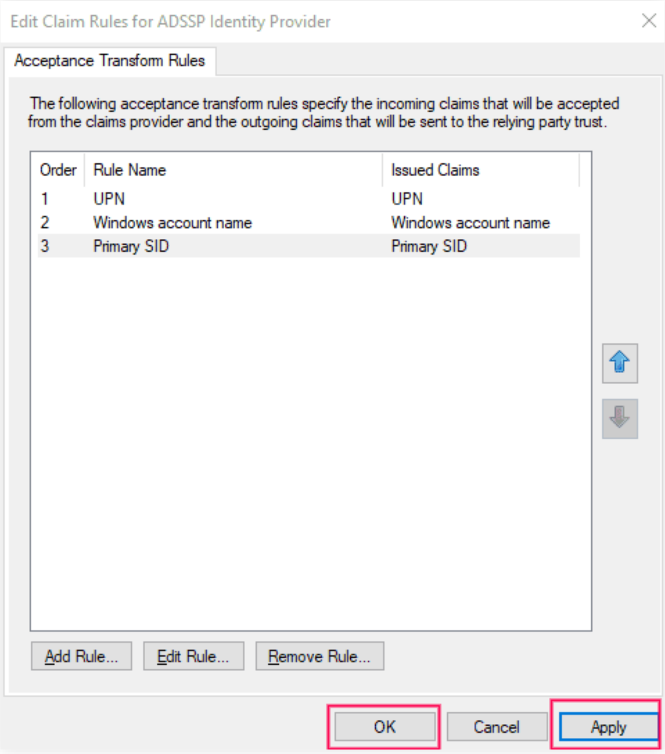
○ Pass through only claim values that start with a specific value:

Starts with:

Example: FABRIKAM\

9. 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 Transform Rules

The following acceptance transform rules specify the incoming claims that will be accepted from the claims provider and the outgoing claims that 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

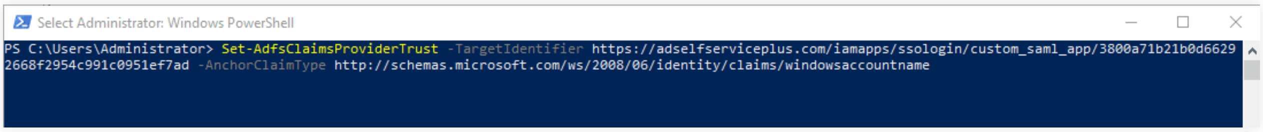
10. Click **Apply** and then **OK** to save the claim rules for ADSelfService Plus.

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
```

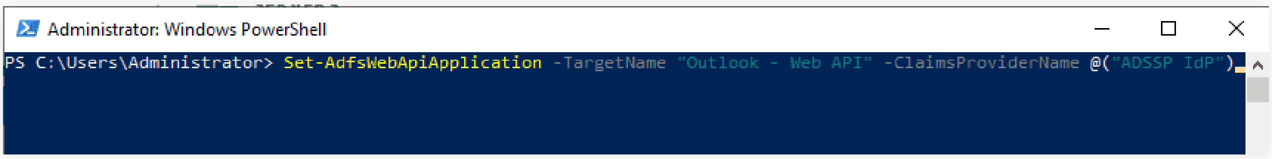


```
PS C:\Users\Administrator> Set-AdfsClaimsProviderTrust -TargetIdentifier https://adselfserviceplus.com/iamapps/ssologin/custom_saml_app/3800a71b21b0d6629
2668f2954c991c0951ef7ad -AnchorClaimType http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname
```

Note: The value of the *<ADSSP IdP Entity URL>* should be copied from the IdP metadata in Step 11 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>")
```



```
PS C:\Users\Administrator> Set-AdfsWebApiApplication -TargetName "Outlook - Web API" -ClaimsProviderName @("ADSSP IdP")
```

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

Note:

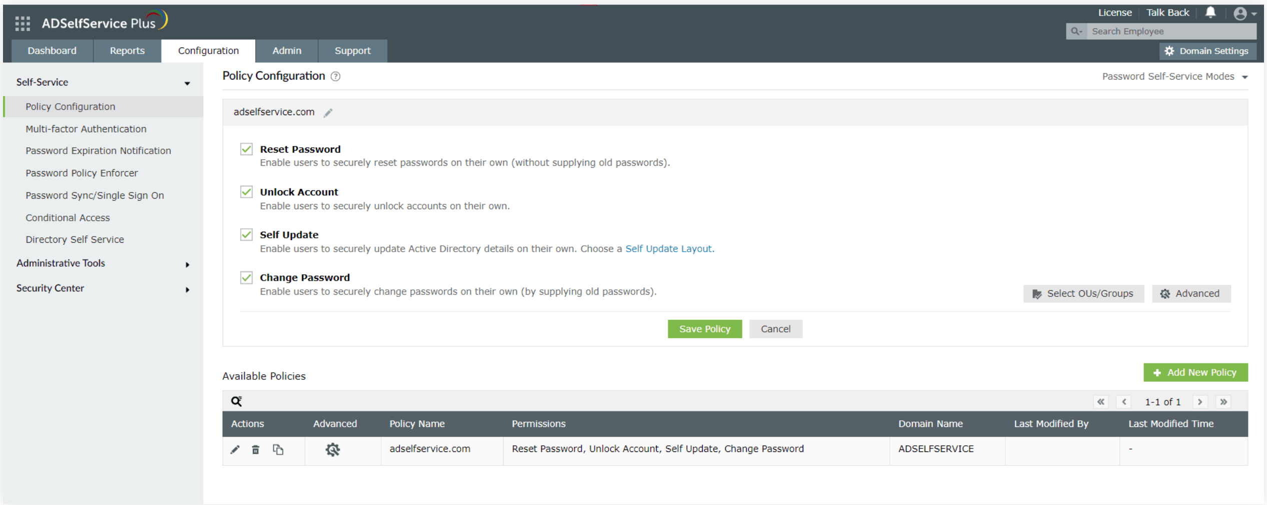
- Replace *<Display name of ADSSP claims provider name in ADFS>* with the claim name copied in Step 4 of the **Adding a new claims provider trust** section.
- Replace <Outlook> with the name for the native application group created in Step 6b of the **ADFS configuration for modern authentication** section.

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.**



adselfservice.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.

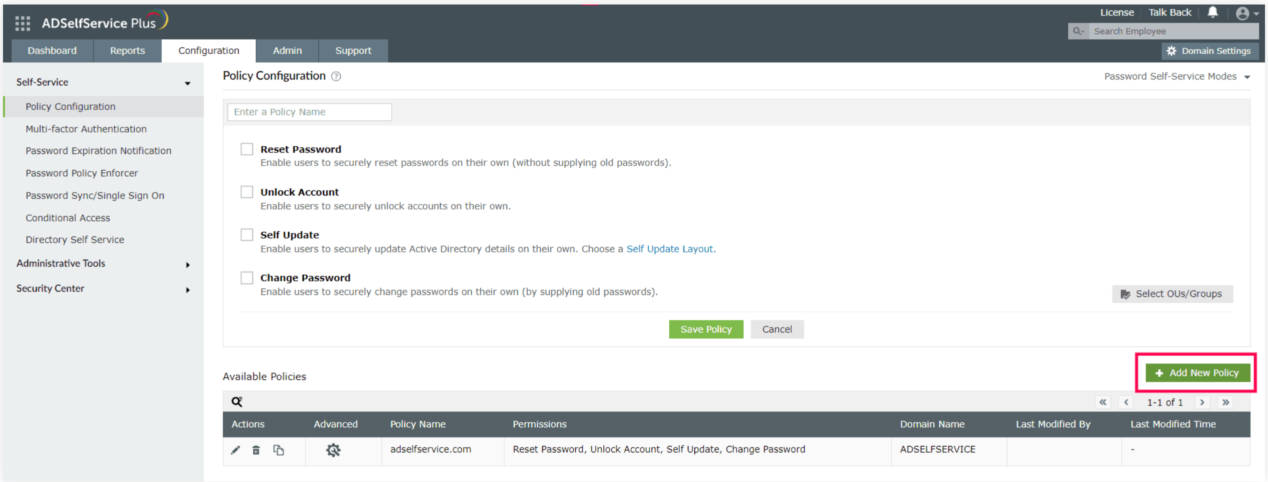
☑ **Self Update**
Enable users to securely update Active Directory details on their own. Choose a Self Update Layout.

☑ **Change Password**
Enable users to securely change passwords on their own (by supplying old passwords).

Available Policies

Actions	Advanced	Policy Name	Permissions	Domain Name	Last Modified By	Last Modified Time
		adselfservice.com	Reset Password, Unlock Account, Self Update, Change Password	ADSELFSERVICE		-

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



□ **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.

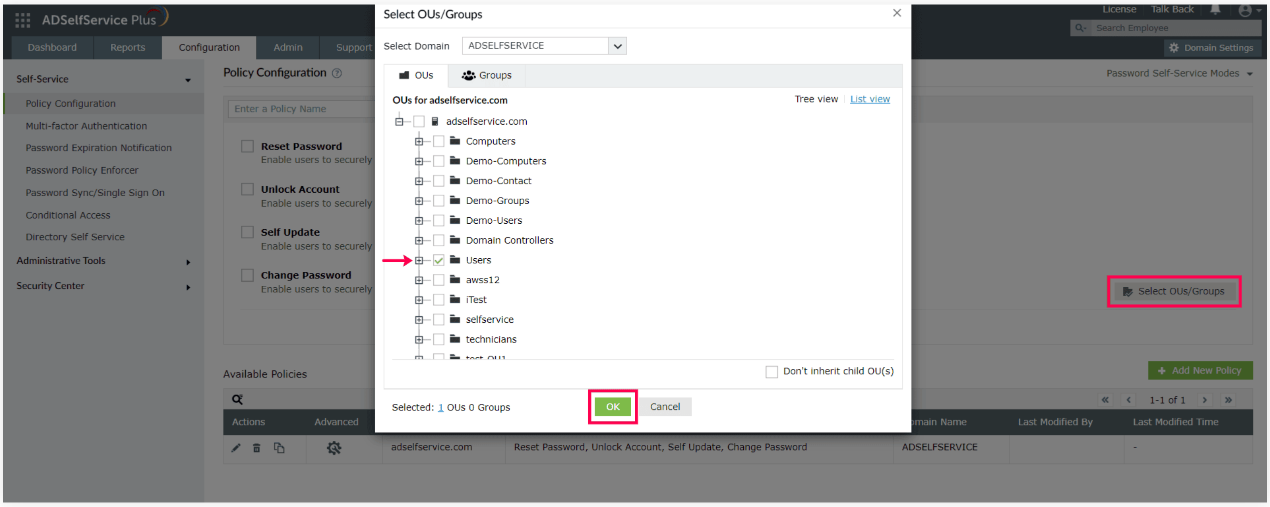
□ **Self Update**
Enable users to securely update Active Directory details on their own. Choose a Self Update Layout.

□ **Change Password**
Enable users to securely change passwords on their own (by supplying old passwords).

Available Policies

Actions	Advanced	Policy Name	Permissions	Domain Name	Last Modified By	Last Modified Time
		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.**



Select OUs/Groups

Select Domain: ADSELFSERVICE

OUs | Groups

OUs for adselfservice.com — Tree view | List view

- □ adselfservice.com
  - □ Computers
  - □ Demo-Computers
  - □ Demo-Contact
  - □ Demo-Groups
  - □ Demo-Users
  - □ Domain Controllers
  - ☑ Users
  - □ awss12
  - □ iTest
  - □ selfservice
  - □ technicians
  - □ test-OU1

□ Don't inherit child OU(s)

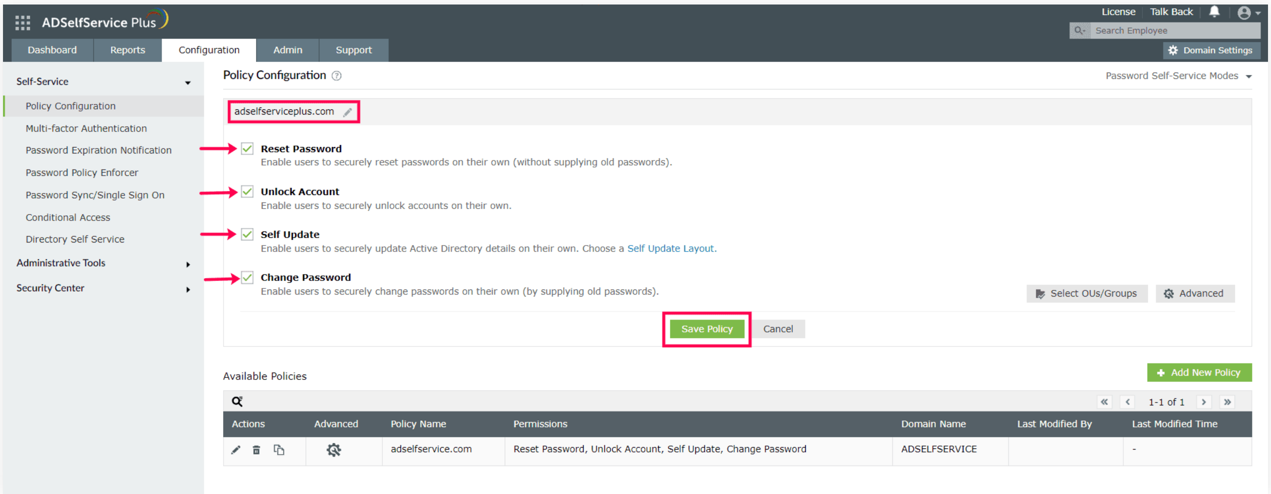
Selected: 1 OUs 0 Groups — OK | Cancel

Policy Configuration: Enter a Policy Name

□ Reset Password — Enable users to securely
□ Unlock Account — Enable users to securely
□ Self Update — Enable users to securely
□ Change Password — Enable users to securely

Actions	Advanced	Policy Name	Permissions	Domain Name	Last Modified By	Last Modified Time
		adselfservice.com	Reset Password, Unlock Account, Self Update, Change Password	ADSELFSERVICE		-

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.**



Policy Configuration

adselfserviceplus.com

☑ **Reset Password**
Enable users to securely reset passwords on their own (without supplying old passwords).

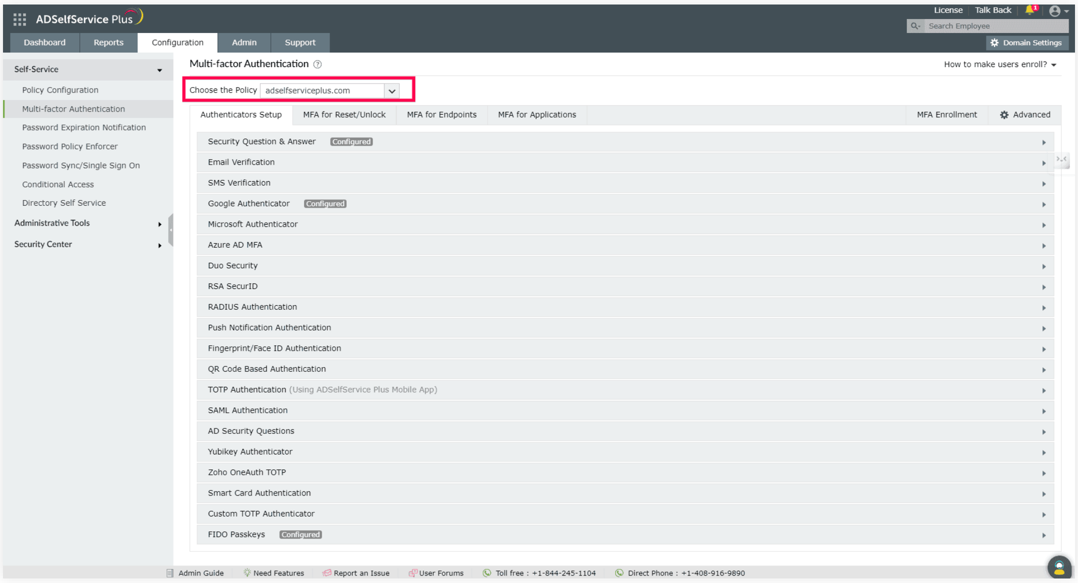
☑ **Unlock Account**
Enable users to securely unlock accounts on their own.

☑ **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).

Actions	Advanced	Policy Name	Permissions	Domain Name	Last Modified By	Last Modified Time
		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.



Multi-factor Authentication

Choose the Policy: adselfserviceplus.com

- Security Question & Answer — Configured
- Email Verification
- SMS Verification
- Google Authenticator — Configured
- Microsoft Authenticator
- Azure AD MFA
- Duo Security
- RSA SecurID
- 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

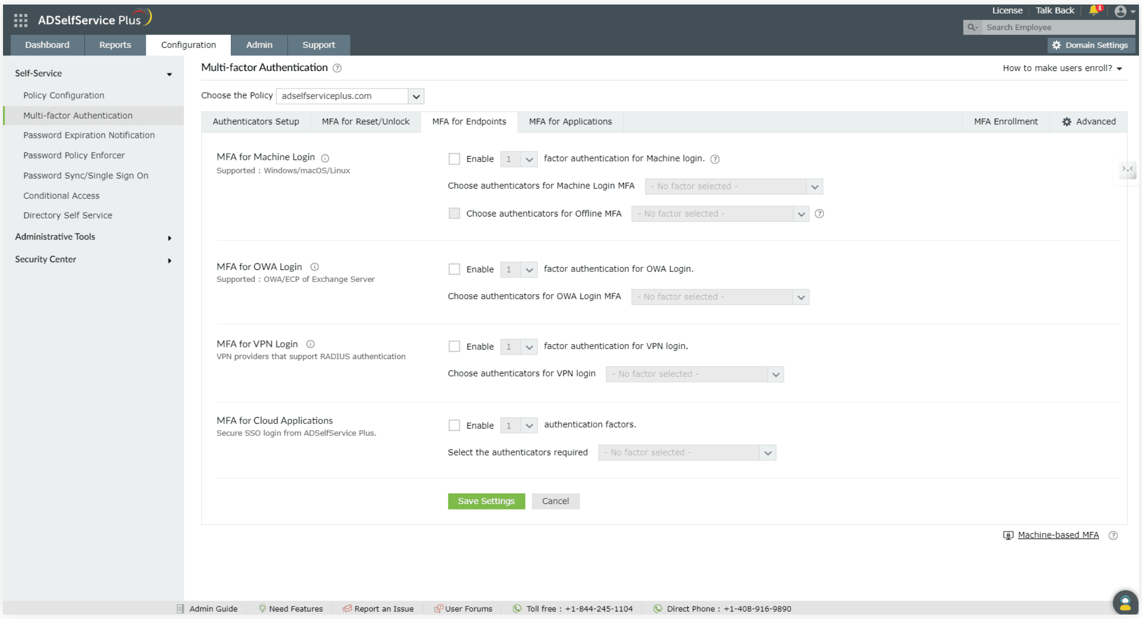
Toll free : +1-844-245-1104 | Direct Phone : +1-408-916-9890

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 this page.

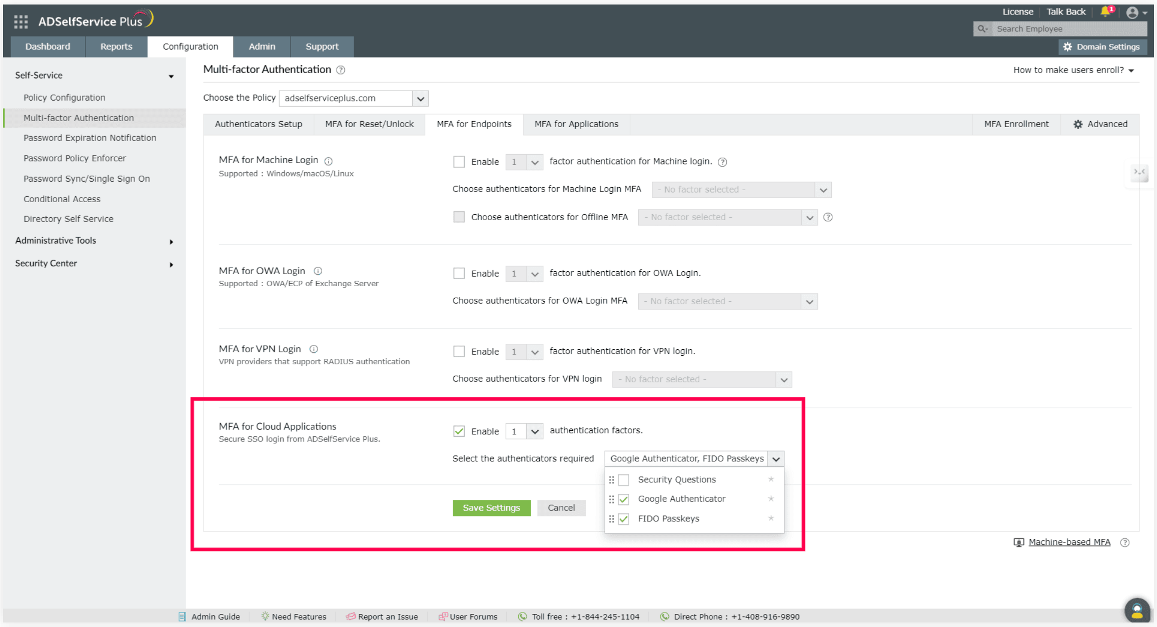
Step 2: Enable the required MFA factors

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.

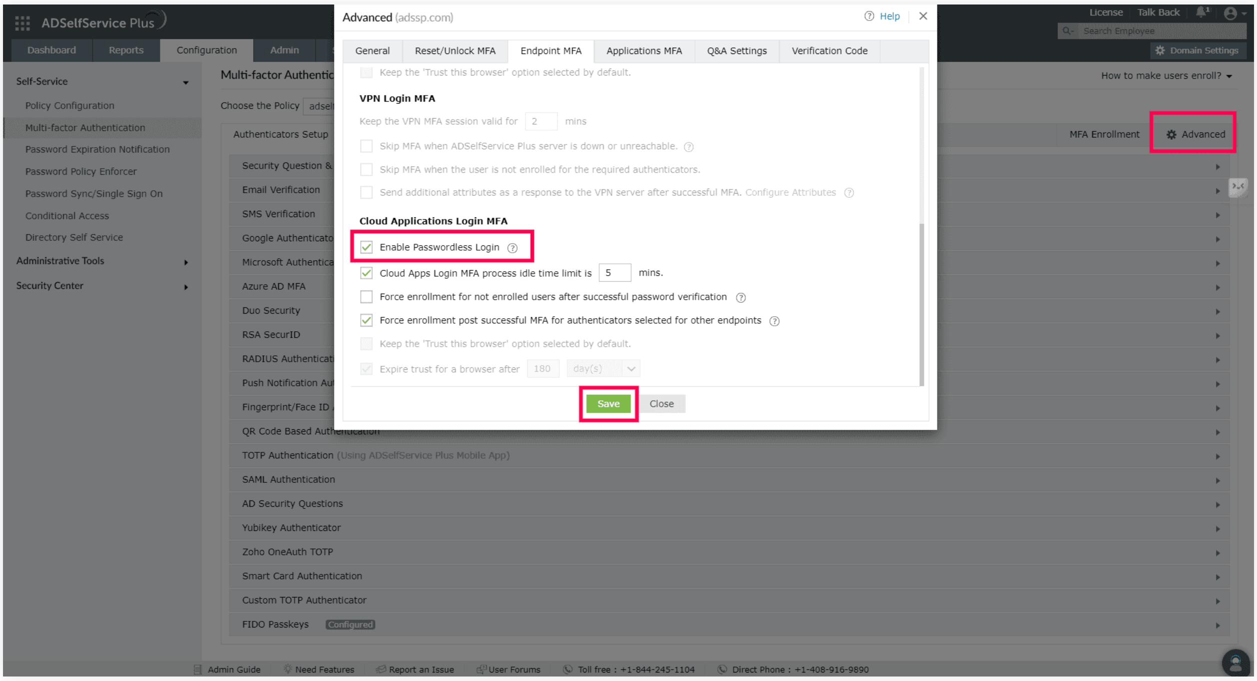
a. Log into ADSelfService Plus with admin credentials and navigate to **Configuration > Self-Service > Multi-Factor Authentication > MFA for Endpoints.**


ADSelfService Plus
License
Talk Back
Search Employee
Domain Settings
Dashboard
Reports
Configuration
Admin
Support
Self-Service
Policy Configuration
Multi-factor Authentication
Password Expiration Notification
Password Policy Enforcer
Password Sync/Single Sign On
Conditional Access
Directory Self Service
Administrative Tools
Security Center
Multi-factor Authentication
How to make users enroll?
Choose the Policy adselfserviceplus.com
Authenticators Setup
MFA for Reset/Unlock
MFA for Endpoints
MFA for Applications
MFA Enrollment
Advanced
MFA for Machine Login
Supported : Windows/macOS/Linux
□ Enable 1 factor authentication for Machine login.
Choose authenticators for Machine Login MFA - No factor selected -
□ Choose authenticators for Offline MFA - No factor selected -
MFA for OWA Login
Supported : OWA/ECP of Exchange Server
□ Enable 1 factor authentication for OWA Login.
Choose authenticators for OWA Login MFA - No factor selected -
MFA for VPN Login
VPN providers that support RADIUS authentication
□ Enable 1 factor authentication for VPN login.
Choose authenticators for VPN login - No factor selected -
MFA for Cloud Applications
Secure SSO login from ADSelfService Plus.
□ Enable 1 authentication factors.
Select the authenticators required - No factor selected -
Save Settings
Cancel
Machine-based MFA
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.**


ADSelfService Plus
License
Talk Back
Search Employee
Domain Settings
Dashboard
Reports
Configuration
Admin
Support
Self-Service
Policy Configuration
Multi-factor Authentication
Password Expiration Notification
Password Policy Enforcer
Password Sync/Single Sign On
Conditional Access
Directory Self Service
Administrative Tools
Security Center
Multi-factor Authentication
How to make users enroll?
Choose the Policy adselfserviceplus.com
Authenticators Setup
MFA for Reset/Unlock
MFA for Endpoints
MFA for Applications
MFA Enrollment
Advanced
MFA for Machine Login
Supported : Windows/macOS/Linux
□ Enable 1 factor authentication for Machine login.
Choose authenticators for Machine Login MFA - No factor selected -
□ Choose authenticators for Offline MFA - No factor selected -
MFA for OWA Login
Supported : OWA/ECP of Exchange Server
□ Enable 1 factor authentication for OWA Login.
Choose authenticators for OWA Login MFA - No factor selected -
MFA for VPN Login
VPN providers that support RADIUS authentication
□ Enable 1 factor authentication for VPN login.
Choose authenticators for VPN login - No factor selected -
MFA for Cloud Applications
Secure SSO login from ADSelfService Plus.
☑ Enable 1 authentication factors.
Select the authenticators required Google Authenticator, FIDO Passkeys
□ Security Questions
☑ Google Authenticator
☑ FIDO Passkeys
Save Settings
Cancel
Machine-based MFA
Admin Guide
Need Features
Report an Issue
User Forums
Toll free : +1-844-245-1104
Direct Phone : +1-408-916-9890

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.**



Advanced (adssp.com)

General | Reset/Unlock MFA | Endpoint MFA | Applications MFA | Q&A Settings | Verification Code

□ Keep the 'Trust this browser' option selected by default.

VPN Login MFA

Keep the VPN MFA session valid for 2 mins

□ Skip MFA when ADSelfService Plus server is down or unreachable.

□ Skip MFA when the user is not enrolled for the required authenticators.

□ Send additional attributes as a response to the VPN server after successful MFA. Configure Attributes

Cloud Applications Login MFA

☑ Enable Passwordless Login

☑ Cloud Apps Login MFA process idle time limit is 5 mins.

□ Force enrollment for not enrolled users after successful password verification

☑ Force enrollment post successful MFA for authenticators selected for other endpoints

□ Keep the 'Trust this browser' option selected by default.

☑ Expire trust for a browser after 180 day(s)

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 demo video.

Reference Documentation

- Microsoft Docs
- 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