

## MyID MFA and PSM Version 5.0.7

# **Federation with Microsoft 365**

Lutterworth Hall, St Mary's Road, Lutterworth, Leicestershire, LE17 4PS, UK www.intercede.com | info@intercede.com | @intercedemyid | +44 (0)1455 558111



## Copyright

© 2001–2024 Intercede Limited. All rights reserved.

Information in this document is subject to change without notice. The software described in this document is furnished exclusively under a restricted license or non disclosure agreement. Copies of software supplied by Intercede Limited may not be used resold or disclosed to third parties or used for any commercial purpose without written authorization from Intercede Limited and will perpetually remain the property of Intercede Limited. They may not be transferred to any computer without both a service contract for the use of the software on that computer being in existence and written authorization from Intercede Limited.

The software or web site referred to in this manual may utilize or contain material that is © 1994-2000 DUNDAS SOFTWARE LTD., all rights reserved.

No part of this publication may be reproduced, stored in a retrieval system or transmitted in any form or any means electronic or mechanical, including photocopying and recording for any purpose other than the purchaser's personal use without the written permission of Intercede Limited.

Whilst Intercede Limited has made every effort in the preparation of this manual to ensure the accuracy of the information, the information contained in this manual is delivered without warranty, either express or implied. Intercede Limited will not be held liable for any damages caused, or alleged to be caused, either directly or indirectly by this manual.

#### Licenses and Trademarks

The Intercede<sup>®</sup> and MyID<sup>®</sup> word marks and the MyID<sup>®</sup> logo are registered trademarks of Intercede in the UK, US and other countries.

Microsoft and Windows are registered trademarks of Microsoft Corporation. Other brands and their products are trademarks or registered trademarks of their respective holders and should be noted as such. All other trademarks acknowledged.



### Conventions

- Lists:
  - Numbered lists are used to show the steps involved in completing a task when the order is important.
  - Bulleted lists are used when the order is unimportant or to show alternatives.
- **Bold** is used for menu items and for labels.

For example:

- "Record a valid email address in 'From' email address"
- Select Save from the File menu.
- *Italic* is used for emphasis and to indicate references to other sections within the current document:

For example:

- "Copy the file *before* starting the installation"
- "See Issuing a Card for further information"
- Bold and Italic are used to identify the titles of other documents.

For example: "See the *Release Notes* for further information."

Unless otherwise explicitly stated, all referenced documentation is available on the product media.

- A fixed width font is used where the identification of spaces is important, including filenames, example SQL queries and any entries made directly into configuration files or the database.
- **Notes** are used to provide further information, including any prerequisites or configuration additional to the standard specifications.

For example:

Note: This issue only occurs if updating from a previous version.

• Warnings are used to indicate where failure to follow a particular instruction may result in either loss of data or the need to manually configure elements of the system.

For example:

Warning: You must take a backup of your database before making any changes to it.



## Contents

1	Introd	Introduction		
	1.1	Change history	5	
2	Prere	Prerequisites		
	2.1	PowerShell	6	
	2.2	Verify the current federation configuration	8	
	2.3	Removing an existing federation configuration	8	
	2.4	Verify the Entra default domain		
	2.5	Switching from WS-Fed to SAML2		
	2.6	DNS and SSL	9	
3	Addin	ng the Microsoft 365 application	10	
4	Config	guring federation	12	
	4.1	Enable single domain federation using PowerShell	12	
	4.2	Verify the configuration		
	4.3	Testing the federation setup	15	
5	Multi-domain configuration			
	5.1	Adding additional domain names	17	
	5.2	IssuerUri format impact		
	5.3	Enable multi-domain federation using PowerShell		
	5.4	Changing from a single to multi-domain configuration	19	
6	Feder	ation without directory synchronization	21	
	6.1	Checking the Entra ID values for a user		
	6.1.1	Using PowerShell	21	
	6.1.2	Using the Microsoft Entra admin center		
	6.2	Creating an Immutable ID value in Entra		
	6.3	Adding the Immutable ID value to the MFA user account		
	6.3.1	Active Directory user		
	6.3.2	External / Realm user		
7	Troub	leshooting	24	
	7.1	Browser redirect loop between Microsoft 365 and the IdP		
	7.2	Unique IssuerUri values	24	
	7.3	Signing certificate error		



### 1 Introduction

**Note:** MyID MFA and MyID PSM were previously known as Authlogics products. Authlogics is now an Intercede Group company and the products have been rebranded accordingly. The term 'Authlogics' may still appear in certain areas of the product.

Microsoft supports federated access to Microsoft 365 resources through SAML 2.0 and WS-Fed federation protocols. This document details the steps required to configure MyID MFA 5.0 federation with Microsoft 365 using SAML 2.0.

MyID MFA natively supports multi-domain SAML 2.0, and does not require ADFS for integration.

### 1.1 Change history

Version	Description
INT2058-01	Reformatted and released with MyID MFA and PSM version 5.0.7. Updated to reflect MS Graph PowerShell and multi-domain configurations.



### 2 **Prerequisites**

This document does not detail how to set up a hybrid environment with Microsoft 365 or Entra ID; this must already be in place. Specifically, you must have already set up the following:

- A Microsoft 365 tenant in "Managed" state (that is, not currently federated).
- The Microsoft.Graph PowerShell module.
- Directory synchronization with Microsoft Entra Connect (Azure ID Connect), or other management method for the Entra Immutable ID.

See section 6, Federation without directory synchronization.

- Entra ID admin logon.
- A deployed MyID MFA Server, with:
  - MFA users configured and tested (for example, using the Self Service Portal).
  - Public DNS entry for the IdP.
  - Public SSL certificate configured on the MFA server matching the DNS entry.
  - Inbound SSL access to the MyID MFA server from the Internet.

#### 2.1 PowerShell

You require the Microsoft Graph PowerShell module for steps in this document.

To check if you already have this module installed, run the following command at an administrator PowerShell prompt.

PS C:\> Get-Module -Name Microsoft.Graph -ListAvailable

If you do not have the module installed, to install the module, run the following commands at an administrator PowerShell prompt.

PS C:\> Install-Module Microsoft.Graph -Scope AllUsers -Repository PSGallery -Force

PS C: <> Import-Module Microsoft.Graph.Identity.DirectoryManagement



To execute a Microsoft Graph PowerShell command, you must authenticate with Entra. You are recommended to use an Entra ID administrator account, not a hybrid account, while configuring federation settings.

#### Run the following command:

```
PS C:\> Connect-MgGraph -Scopes
'User.ReadWrite.All,Group.ReadWrite.All,Directory.ReadWrite.All,Director
y.AccessAsUSer.All'
```

You are prompted to authenticate using the appropriate method configured on the Entra account:



Select the Consent on behalf of your organization option:

Sign in to your account	×
Hicrosoft	
admin@federationdemo.onmicrosoft.com	
Permissions requested	
Microsoft Graph Command Line Tools Microsoft Corporation 🐲	
This app would like to:	
Read and write all users' full profiles	
Read and write all groups	
Read and write directory data	
$\checkmark$ Access directory as the signed in user	
$\checkmark$ Maintain access to data you have given it access to	
Consent on behalf of your organization	
If you accept, this app will get access to the specified resources for all users in your organization. No one else will be prompted to review these permissions.	
Accepting these permissions means that you allow this app to use your data as specified in their terms of service and privacy statement. You can change these permissions at https://myapps.microsoft.com.Show details	
Does this app look suspicious? Report it here	
Cancel Accept	
Terms of use Privacy & cookies	



### 2.2 Verify the current federation configuration

Ensure that the Office tenant is not already set up to use another federation server. Connect to MS Online and check the domain status is <code>Verified</code> and <code>Managed</code> by running the following commands:

PS C:\> Get-MgDomain   select Id, Is	sVerified, AuthenticationType
Id	IsVerified AuthenticationType
federationdemo.onmicrosoft.com	True Managed
federationdemo.com	True Federated
federationdemo.mail.onmicrosoft.com	True Managed

### 2.3 Removing an existing federation configuration

To remove an existing federation configuration and set the authentication in Entra back to Managed, run the following command:

PS C:\> Update-MgDomain -DomainId 'federationdemo.com' AuthenticationType 'Managed'

**Note:** This may take up to two hours to take effect fully in Entra ID, even if the PowerShell commands show that the configuration has been changed.

### 2.4 Verify the Entra default domain

Microsoft Entra does not allow the default domain to be federated. To verify that the domain you want to federate with is *not* the default domain, run the following command:

If the domain with which you want to federate has the IsDefault value of True, you can set the xxx.onmicrosoft.com (or another) domain as the default by running the following command:

PS C:\> Update-MgDomain -DomainId 'federationdemo.onmicrosoft.com' - IsDefault

### 2.5 Switching from WS-Fed to SAML2

Microsoft 365 supports both SAML2 and WS-Fed federation protocols. To change from WS-Fed to SAML2 you must first disable federation for the domain by making it "Managed" (see section 2.3, *Removing an existing federation configuration*) and then create a new SAML2 configuration following the instructions in this guide.



### 2.6 DNS and SSL

The MyID MFA server requires a publicly trusted SSL certificate. The DNS name in the SSL certificate must match the MyID MFA-configured IdP Host and Domain configuration; for example:

idp.federationdemo.com

Applications Propert	ies	>
Identity Provider SA	ML 2.0	
Server Settings		
IdP Host:	idp	
IdP Domain:	federationdemo.com	
TCP Port:	443 🗘	
OpenID Connect I Authority URI:	Information	
Multiple DIVS Dom	lains	
Enabled	federationdemo.com acme.inc otherdomain.net	^
		~
	OK Cancel A	pply

The DNS A or CNAME record must resolve to the MyID MFA server through any firewalls or load balancers. Firewalls must allow TCP port 443 from the Internet to the MyID MFA server.

3



### Adding the Microsoft 365 application

Open the MyID MMC to add an Application.

1. Start the Add Application Wizard.

Add Application Wizard		×
Ins	Welcome to the Add Application Wizard	
	This Witzard will allow you to add a new federated Application for strong authentication and authorisation.	
	To continue, click Next.	
chift	< Back Next > Cancel	

2. Click Next.

oplication Information	a new Application	
General information for th	e new Application.	
Provide a name and select t setup a generic OpenID cor	he type of Application. You ca mect or SAML 2.0 Application	an choose a built in Application 1.
App Type:	Microsoft 365	~
Name:	Microsoft 365	

- 3. Select Microsoft 365 from the list and enter a custom name if required.
- 4. Click Next.

Select the requied auther	ntication options.
Internal Authenti	cation
Logon technol	ogy: Automatic V
	Allow Deviceless MFA
	Enable Passwordless MFA
	Allow any user MFA technology
Password rese	t via: SMS / Text Email

5. Select the required logon technology and authentication options.





6. Click Next.

Add Ap	plication Wiza	Ird	>
Apply the configuration? Are you ready to apply the settings?			<b>F</b>
The Add Microsoft Click Net	Application Wiz t 365 Application	card has gathered all the information required to add the new n. configuration changes	
CICK HE		o ingulatori o nangoz.	
	SAML 2.0 SL	ummary	
	Host:	https://idp.federationdemo.com/idp	
		IdP Signing Certificate	
		IdP Signing Certificate Copy Base64	
		<u>IdP Signing Certificate</u> <u>Copy Base64</u>	
		<u>IdP Staning Certificate</u> <u>Coov Base64</u>	

- 7. Confirm the Host configuration information.
- 8. Click **Copy Base64** to copy the Base64 signing certificate information to the clipboard.
- 9. Click Next.

Add Application Configuration Authentication Server is updating the Application data.	
Update Progress	
Adding new Application Done	1
	N

10. Click Finish.

The MyID side of the Microsoft 365 configuration is now complete.



### 4 Configuring federation

You perform the Microsoft 365 side of the configuration using PowerShell commands. To simplify the process, configure a custom PowerShell script with the settings for your environment. When you run the PowerShell script, it configures Microsoft 365 to use the MyID MFA Server for federated authentication.

### 4.1 Enable single domain federation using PowerShell

Configure the yellow highlighted variables in the following sample script with the values of your domain and MyID MFA server.

- \$domain The DNS domain to federate, which must already be set up in Microsoft 365.
- \$display The friendly name shown to users when signing in to Microsoft 365. You are recommended to use something that is familiar, like your company name.
- \$issuerUri The Issuer URI from the SAML 2.0 tab in the Applications
  Properties dialog. The default value will be a derivative of your IdP host and
  domain name; for example:

'urn:uri:ipdfederationdemocom'

- \$signinUrl The SAML 2.0 IdP sign-on page URL. The path is fixed; however, the DNS name must match the public DNS name of the IdP.
- \$signoutUrl The SAML 2.0 IdP logout page URL. The path is fixed; however, the DNS name must match the public DNS name of the IdP.
- \$certificate The Base64 representation of the IdP signing certificate. You can
  obtain this value by clicking the Copy Base64 link on the Applications Properties
  tab or at the end of the Add Application Wizard.
- 1. Copy the text from the sample below to a new plain text document and save it as a .ps1 file.
- 2. Configure the yellow highlighted variables in the following sample script with the values of your domain and MyID MFA server.
- 3. Run the script at a PowerShell command prompt to apply the configuration.

```
$domain = 'federationdemo.com'
$display = 'Federation Demo'
$issuerUri = 'urn:uri:idpfederationdemocom'
$signinUrl =
'https://idp.federationdemo.com/idp/SAML/SingleSignOnService'
$signoutUrl =
'https://idp.federationdemo.com/idp/SAML/SingleLogoutService'
$certificate =
'MIIDGDCCAgCgAwIBAgIQFaTIA1mLiLtJ+wsZt9M2ejANBgkqhkiG9w0BAQsFADAf
MR0wGwYDVQQDDBQqLmZ1ZGVyYXRpb25kZW1vLmNvbTAeFw0yNDAzMDUxNDI0NTZa
Fw0zNDAzMDUxNDM0NTVaMB8xHTAbBqNVBAMMFCouZmVkZXJhdGlvbmRlbW8uY29t
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAnyjM01KPv3y4DUiKYpTH
DT9Gi4c/EGOU6bs8jh0Mke8TjTVWuHGiD98Mj4qLbb/yhk4LHemt58gtjxdj9+pj
gG38OU3dF0n7RMXES6EwK4KlsO16nrXEG6YtP6EelJPkCNXzzSeoeHPCTSMxp1gF
mY/z8f0yI//x/8AmRI2JfGr43exXCbMjYx4sgr85H0CVdw27uHEK9w0hAPPHt2vq
7BMDAfYj2IisbpVekasJDmXtyhvRFptESJ80qvmmyTLD85iHm07aME1/7vYnl1RQ
CqbZbhtrWY14VBAiy/ySnqJdcaJT3KCOVJZOKZxurjXXNJbTHe8i3sQZ0dP2poJZ
```



tQIDAQABo1AwTjAOBgNVHQ8BAf8EBAMCBaAwHQYDVR01BBYwFAYIKwYBBQUHAwEG CCsGAQUFBwMCMB0GA1UdDqQWBBR2d84eaCTxqzIeXnY41uMia8DkJDANBqkqhkiG 9w0BAQsFAAOCAQEACOEinC4t1V80Kgs9MXu843e0UqLseOkoClNZbhxM4n3Y9cTP b9QYQLQ69g8Q2d6tG+DzTCAnJeTdM2A9QWpePNuGceSWlFHHXHv/ZuzixA2SS2mn AVvs9GgP1W/l1anMD1mhd4p9F+U0E/KMnn8yo2pYGI/wlwYm0yW3uaDdAQ1WS+fZ ev2n5WcDbQ6WGkl0L5j0JPvkiXcXmzhPc1ogsCvsWCL90GhFxy3buLTp1N3Rk4dj Z2hWyoeU8WjYax2436rfQx2qYJvgtAD4MDAz195N28kzGBWr+eOO460NzDJ2OGc0 rrIZUyo19Uqjje3lNPPyVAzGp+cyrqeRQWpMjg=='

New-MgDomainFederationConfiguration -DomainId \$domain -DisplayName \$display -IssuerUri \$issuerUri -PassiveSignInUri \$signinUrl -SignOutUri \$signoutUrl -SigningCertificate \$certificate -PreferredAuthenticationProtocol saml -federatedIdpMfaBehavior enforceMfaByFederatedIdp | Format-List

#### Sample output:

ActiveSignInUri	:
DisplayName	: Federation Demo
FederatedIdpMfaBehavior	: enforceMfaByFederatedIdp
Id 853fdee26510	: 523dd120-113b-480a-af4d-
${\tt IsSignedAuthenticationRequestRequired}$	:
IssuerUri	: urn:uri:idpfederationdemocom
MetadataExchangeUri	:
NextSigningCertificate	:
PassiveSignInUri https://idp.federationdemo.com/idp/SAM	: L/SingleSignOnService
PreferredAuthenticationProtocol	: saml
PromptLoginBehavior	:
SignOutUri https://idp.federationdemo.com/idp/SAM	: IL/SingleLogoutService
SigningCertificate MIIDGDCCAgCgAwIBAgIQFaTIA1mLiLtJ+wsZt9 VQQDDBQqLmZ1ZGVyYXRpb25kZW1vLmNvbTAeFw NTVaMB8xHTAbBgNVBAMMFCouZmVkZXJhdGlvbm AAOCAQ8AMIIBCgKCAQEAnyjM01KPv3y4DUiKYp D98Mj4qLbb/yhk4LHemt58gtjxdj9+pjgG380U 1JPkCNXzzSeoeHPCTSMxp1gFmY/z8fOyI//x/8 uHEK9w0hAPPHt2vq7BMDAfYj2IisbpVekasJDm 7vYn11RQCqbZbhtrWY14VBAiy/ySnqJdcaJT3F tQIDAQABo1AwTjAOBgNVHQ8BAf8EBAMCBaAwHQ	: M2ejANBgkqhkiG9w0BAQsFADAfMR0wGwYD 0yNDAzMDUxNDI0NTZaFw0zNDAzMDUxNDM0 R1bW8uY29tMIIBIjANBgkqhkiG9w0BAQEF oTHDT9Gi4c/EGOU6bs8jh0Mke8TjTVWuHGi V3dF0n7RMXES6EwK4Kls016nrXEG6YtP6Ee AmR12JfGr43exXCbMjYx4sgr85H0CVdw27 XtyhvRFptESJ80qvmmyTLD85iHm07aME1/ COVJZ0KZxurjXXNJbTHe8i3sQZ0dP2poJZ YDVR01BBYwFAYIKwYBBQUHAwEGCCsGAQUF

QUF BwMCMB0GA1UdDqQWBBR2d84eaCTxqzIeXnY41uMia8DkJDANBqkqhkiG9w0BAQsFAAOCAQEA COEinC4t1V80Kgs9MXu843e0UqLseOkoC1NZbhxM4n3Y9cTPb9QYQLQ69g8Q2d6tG+DzTCAn JeTdM2A9QWpePNuGceSWlFHHXHv/ZuzixA2SS2mnAVvs9GgP1W/l1anMD1mhd4p9F+U0E/KM nn8yo2pYGI/wlwYm0yW3uaDdAQ1WS+fZev2n5WcDbQ6WGklOL5j0JPvkiXcXmzhPclogsCvs WCL90GhFxy3buLTp1N3Rk4djZ2hWyoeU8WjYax2436rfQx2qYJvgtAD4MDAz195N28kzGBWr +e00460NzDJ2OGc0rrIZUyo19Uqjje31NPPyVAzGp+cyrqeRQWpMjg==

SigningCertificateUpdateStatus Microsoft.Graph.PowerShell.Models.MicrosoftGraphSigningCertificateUpdate Status



```
AdditionalProperties : {[@odata.context,
https://graph.microsoft.com/v1.0/$metadata#domains('federationdemo.com')
/federationConfiguration/$entity]}
```

For further information relating to the New-MgDomainFederationConfiguration PowerShell command, see:

<u>https://learn.microsoft.com/en-</u> us/powershell/module/microsoft.graph.identity.directorymanagement/newmgdomainfederationconfiguration

#### 4.2 Verify the configuration

To verify the configuration, run the following command.

PS C:\> Get-MgDomainFederationConfiguration -DomainId
'federationdemo.com' | Format-List

ActiveSignInUri	:
DisplayName	: Federation Demo
FederatedIdpMfaBehavior	:
Id 5985564224ff	: dbb35c60-4dc7-4396-86df-
${\tt IsSignedAuthenticationRequestRequired}$	:
IssuerUri	: urn:uri:msp:federationdemocom
MetadataExchangeUri	:
NextSigningCertificate	:
PassiveSignInUri https://idp.federationdemo.com/idp/SAM mocom	: ML/SingleSignOnService/federationde
PreferredAuthenticationProtocol	: saml
PromptLoginBehavior	:
SignOutUri https://idp.federationdemo.com/idp/SAN mocom	: ML/SingleLogoutService/federationde
SigningCertificate MIIDATCCAemgAwIBAgIQdPDr/iI1jbhDMTj5VY VQQDEwt3d3cuaWRwLmNvbTAeFw0xMzExMjIw01 BgNVBAMTC3d3dy5pZHAuY29tMIIBIjANBgkqhl RLDrcbSyqUd8XG4BgxObQMYLAkEN1mJOSAEp13 QUUE0WtVUh5JPMsukolf9q1jbJkCkvHXH304Ue gU/NamjiqwHI4fI8kFJKwKBJchRPUQdC41jRRr OWuchIK+1vAKKBUh9nDEXfr80+xW680w5TqHyI 36Ck9H5Pw+1PPu6NzBFSz5ZkC8KzrS6vuZXc/3 QDA+gBD4dY4MCPEmG4sxZrcni8vtoRgwFjEUMH NY24QzE4+VWMmvkwDQYJKoZIhvcNAQELBQADgg 211i0WhD4/xe7Ry5haC6TeXIp8Q4cC3MzsrDa3 pe16+ssTL4upS1cGydigqwUzsdpGck4wI1moJ9 VRdbQIH5GsKUeAjOdRQmy+X1MX6KyRoaCwWGYw h/75aN0cFQfDEdJ7C5NE0vonidE0QtIFvsoWt2 q31yh3gr3kSN62H8iVKLQLA=	: (Ya+TANBgkqhkiG9w0BAQsFADAWMRQwEgYD DIwNTJaFw000TEyMzExNDAwMDBaMBYxFDAS ciG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAi0XJ LxMabUiq1X4v0Fc8ZaCpUE3fFGENMEWgBjn en7vA2oNQWt4bK96SpXADpZKFvpk4D7btKO nGIrSnpY+t25/d3KGXwbe9Z2MGGy2hyA0tg DcqbWvQsXXhH0yZLfINKNS6/IojHPsBy7tf ImYrnheMQsqQIDAQABo0swSTBHBgNVHQEE BIGA1UEAxMLd3d3LmlkcC5jb22CEHTw6/4i gEBABhak2aR84MCdyX04AKOQvZybsCMdhRq L74xHI714BW01oafpHAsXfd9EvkKTVaJ+1Z 04770+46If2gF27u9Cdk7Onxe/5dwLIxWmk vxi5Sa+r+3AtDvD4BX0EJGKFZeeM3J/yMpY ZUtur2fiW7yBxse38TPQsi2r6A6c/TZsZ5b
SigningCertificateUpdateStatus Microsoft.Graph.PowerShell.Models.Mic Status	: rosoftGraphSigningCertificateUpdate
AdditionalProperties	: {}



### 4.3 Testing the federation setup

1. To test the federation setup, go to the following URL and sign in: <u>https://portal.office.com</u>

Sign in to your account × +					- 0	
← → C iii login.microsoftonline.com/common/oauth2/	v2.0/authorize?client_id=4765445b-32c6-49b0-83e6-1d93765276ca&redirect_uri=http •	H 63	*		🛞 Incognit	• :
Google Chrome isn't your default browser     Set as default	m common/cadd/2//2 4/ard/torosoft dent.gld-d7554490-32x6-4980-43146-1933755276x38/rederet; yen http://					
	Microsoft					
	Sign in					
	stevenh@federationdemo.com					
	No account? Create one!					
	Can't access your account?					
	Back Next					
	Sign-in options					
		Ter	ms of use	e Pr	ivacy & cooki	es

2. Enter your Account name.

← → C 🔒 login.microsoftonline.com/common/oauth		6	\$	🔒 Incogni	to f
Google Chrome isn't your default browser					*
	Microsoft Taking you to your organisation's sign-in page				

3. Wait while Microsoft redirects you to the MyID MFA logon page.

MyID Authentication Server IdP × +						
→ C iii idp.federationdemo.com/id	p/Account/Login?ReturnUrl=%2Fidp%2FSaml%2FSingleSignOnServiceComp	letion%3Fcontext%3DCfDJ8IPkC	04 ·	* •	🔒 Incognit	•
	Login					
	209					
	Username					
	stevenn@rederationdemo.com					
	Sign In					
	View user guide					





4. Confirm your account name.



5. Enter your MFA details based on the configuration.

This example uses Passwordless & Deviceless Grid authentication.



Once validated, you are redirected back to Microsoft 365 and are signed in.



### 5 Multi-domain configuration

Microsoft Entra (Azure AD) requires a unique SAML IssuerUri for each DNS domain across all Azure tenants. The IssuerUri is a federation server value, and not a Microsoft 365 application specific value.

Note: If you only have one DNS domain to federate, this configuration is not required.

#### 5.1 Adding additional domain names

To support multiple domains, the actual domain names to be federated must be specified. You must add, remove, and view the names through the MMC or through the Rest API.

To specify the names through the MMC, in the **Multiple DNS Domains** section, set the **Enabled** option, then list the domains in the text box.

Applications Propert	ies	×
Identity Provider SA	ML 2.0	
Server Settings		
IdP Host:	idp	
IdP Domain:	federationdemo.com	
TCP Port:	443 🗘	
OpenID Connect	Information	
Authority URI:	https://idp.federationdemo.com/idp	
Multiple DNS Dom	ains	
🗹 Enabled	federationdemo.com acme.inc otherdomain.net	
	OK Cancel Apply	

To specify the names through the API, use the following calls:

- AddIdpDnsName
- RemoveIdpDnsName
- GetIdpDnsNames

When calling AddIdpDnsName or RemoveIdpDnsName you must:

- Specify the full DNS name of the domain; for example: acme.com
- Run <code>iisreset</code> for the IdP to read the new configuration.

Note: These API calls require administrator rights.



### 5.2 IssuerUri format impact

The default IssuerUri format for the MyID Authentication Server is:

urn:uri:{idp-fqdn-without-dots}

#### For example:

urn:uri:idpfederationdemocom

dentity Provider 3	AML 2.0
Identity Provider	(ldP)
Description:	MyID Identity Provider
Issuer Uri:	um:uri:idpfederationdemocom
Issuer URI:	
um:uri:idpfede	erationdemocom federationdemocom 🗸 🗸
Login URI: https://idp.fec Logout URI:	derationdemo.com/idp/SAML/SingleSignOnService/fr
https://idp.fed	derationdemo.com/idp/SAML/SingleLogoutService/fe
Artifact URI:	
	derationdemo.com/idp/SAML/ArtifactResolutionServic
https://idp.fed	ate.
https://idp.feo	
https://idp.fec Signing Certific <u>Properties</u>	Copy Base64

This ensures that each MyID MFA deployment has a unique IssuerUri for each MyID MFA customer. However, when multiple domains are required to be federated, multiple unique IssuerUri values are also required.

The Authentication Server automatically generates unique IssuerUri names using the configured IssuerUri name appended with the specified DNS domains you want to federate. The resulting format is as follows:

urn:uri:{idp-fqdn-without-dots}:{federated-domain-without-dots}

For example, if acme.com and contoso.com are federated domains with an Authentication Server having a configured IssuerUri of urn:uri:idpfederationdemocom, the resulting domain specific URIs are:

- urn:uri:idpfederationdemocom:acmecom
- urn:uri:idpfederationdemocom:contosocom

You must use these domain specific URIs during each Microsoft 365 configuration.

#### 5.3 Enable multi-domain federation using PowerShell

Configure the yellow highlighted variables in the following sample script with the values of your domain and MyID MFA server.

- \$domain The DNS domain to federate, which must already be set up in Microsoft 365.
- \$display The friendly name shown to users when signing in to Microsoft 365. You are recommended to use something that is familiar, like your company name.
- \$issuerUri The Issuer URI from the SAML 2.0 tab in the Applications Properties dialog. The default value will be a derivative of your IdP host and domain name. This is then appended with a colon and the federated domain name without dots; for example:

'urn:uri:ipdfederationdemocom:customdomaincom'

• \$signinUrl - The SMAL 2.0 IdP sign-on page URL. The path is fixed; however, the DNS name must match the public DNS name of the IdP.



- \$signoutUrl The SMAL 2.0 IdP logout page URL. The path is fixed; however, the DNS name must match the public DNS name of the IdP.
- \$certificate The Base64 representation of the IdP signing certificate. You can
  obtain this value by clicking the Copy Base64 link on the Applications Properties
  tab or at the end of the Add Application Wizard.
- 1. Copy the text from the sample below to a new plain text document and save it as a .ps1 file.
- 2. Configure the yellow highlighted variables in the following sample script with the values of your domain and MyID MFA server
- 3. Add the domain name to the MFA Server using the AddIdpDnsName API call.
- 4. Run the script at a PowerShell command prompt to apply the configuration.

```
$domain = 'federationdemo.com'
$display = 'Federation Demo'
$issueruri = 'urn:uri: idpfederationdemocom: federationdemocom'
$signinUrl =
'https://idp.federationdemo.com/idp/SAML/SingleSignOnService/federationd
emocom'
$signoutUrl =
'https://<mark>idp.federationdemo.com</mark>/idp/SAML/SingleLogoutService/<mark>federationd</mark>
emocom
$certificate =
'MIIDGDCCAgCgAwIBAgIQFaTIA1mLiLtJ+wsZt9M2ejANBgkqhkiG9w0BAQsFADAf
MR0wGwYDVQQDDBQqLmZ1ZGVyYXRpb25kZW1vLmNvbTAeFw0yNDAzMDUxNDI0NTZa
Fw0zNDAzMDUxNDM0NTVaMB8xHTAbBqNVBAMMFCouZmVkZXJhdGlvbmRlbW8uY29t
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAnyjM01KPv3y4DUiKYpTH
DT9Gi4c/EGOU6bs8jh0Mke8TjTVWuHGiD98Mj4qLbb/yhk4Lhemt58gtjxdj9+pj
gG38OU3dF0n7RMXES6EwK4KlsO16nrXEG6YtP6EelJPkCNXzzSeoeHPCTSMxp1gF
mY/z8f0yI//x/8AmRI2JfGr43exXCbMjYx4sqr85H0CVdw27uHEK9w0hAPPHt2vq
7BMDAfYj2IisbpVekasJDmXtyhvRFptESJ80qvmmyTLD85iHm07aME1/7vYnl1RQ
CqbZbhtrWY14VBAiy/ySnqJdcaJT3KCOVJZOKZxurjXXNJbTHe8i3sQZ0dP2poJZ
tQIDAQABo1AwTjAOBgNVHQ8Baf8EBAMCBaAwHQYDVR01BBYwFAYIKwYBBQUHAwEG
CCsGAQUFBwMCMB0GA1UdDgQWBBR2d84eaCTxgzIeXnY41uMia8DkJDANBgkqhkiG
9w0BAQsFAAOCAQEACOEinC4t1V80Kgs9Mxu843e0UqLse0koC1NZbhxM4n3Y9cTP
b9QYQLQ69g8Q2d6tG+DzTCAnJeTdM2A9QWpePNuGceSWlFHHXHv/ZuzixA2SS2mn
Avvs9GgP1W/l1anMD1mhd4p9F+U0E/KMnn8yo2pYGI/wlwYm0yW3uaDdAQ1WS+fZ
ev2n5WcDbQ6Wgkl0L5j0JPvkiXcXmzhPc1ogsCvsWCL90ghFxy3buLTp1N3Rk4dj
Z2hWyoeU8WjYax2436rfQx2qYJvqtAD4MDAz195N28kzGBWr+eOO460NzDJ2Oqc0
rrIZUyo19Uqjje3lNPPyVAzGp+cyrqeRQWpMjg=='
```

New-MgDomainFederationConfiguration -DomainId \$domain -DisplayName \$display -IssuerUri \$issuerUri -PassiveSignInUri \$signinUrl -SignOutUri \$signoutUrl -SigningCertificate \$certificate -PreferredAuthenticationProtocol saml -federatedIdpMfaBehavior enforceMfaByFederatedIdp | Format-List

#### 5.4 Changing from a single to multi-domain configuration

To change from a single domain to a multi-domain configuration:



- Remove the existing federated connection to Entra.
   See section 2.3, *Removing an existing federation configuration*.
- 2. Add the federated domain names to the MFA server. See section *5.1*, *Adding additional domain names*.
- Add the new multi-domain federation configuration.
   See section 5.3, Enable multi-domain federation using PowerShell.



#### 6

### Federation without directory synchronization

For federation to work with Entra ID (Microsoft 365 / Azure AD) there must be a specific mapping between the MFA user account and the Entra ID user account.

In a typical Microsoft hybrid configuration, the Microsoft Entra Connect (Azure ID Connect) synchronizes the required fields to link the accounts. If Entra Connect is not in place (for example, in a Managed Service Provider environment) you must map the account attributes manually.

The following user specific attributes must match in both MFA and Entra ID:

NameID

The Entra user's Immutable ID (OnPremisesImmutableId).

If Microsoft Entra Connect is deployed, the Entra Immutable ID property contains the Base64 equivalent value of the Active Directory <code>objectGUID</code> property.

**Important:** Once you have set the Immutable ID value, you cannot change it; that is the defining feature of *immutable* IDs.

If Microsoft Entra Connect has *not* been deployed, the Entra Immutable ID property is empty and *must* be populated before federation will work for the user.

IDPEmail

The User Principal Name (UPN) value in Entra; not the email address field (despite the attribute name being IDPEmail). The UPN is typically the same as the email address, although this may vary.

For further information, see:

https://learn.microsoft.com/en-us/entra/identity/hybrid/connect/how-to-connect-fed-samlidp

#### 6.1 Checking the Entra ID values for a user

You can check the Entra ID values for a user with PowerShell or using the Microsoft Entra admin center.

#### 6.1.1 Using PowerShell

To view the values stored in Entra for a user, run the following PowerShell script, replacing the highlighted values for \$tenantId and \$accountUpn:

\$tenantId = 'federationdemo.com'

\$accountUpn = 'johnd@federationdemo.com'

Connect-MgGraph -TenantId \$tenantId -Scopes 'User.ReadWrite.All' - NoWelcome

Get-MgUser -UserId \$accountUpn -Property UserPrincipalName, OnPremisesImmutableId | fl UserPrincipalName, OnPremisesImmutableId

#### The PowerShell script outputs the user details as follows:

UserPrincipalName : johnd@federationdemo.com

OnPremisesImmutableId : X1vAuhkd70KAAfnfxA6DyA==



#### 6.1.2 Using the Microsoft Entra admin center

To view the values stored in Entra for a user using a browser:

1. Open the Entra ID Users page:

https://entra.microsoft.com/#blade/Microsoft\_AAD\_UsersAndTenants/UserManage mentMenuBlade/menuId/

- 2. Select the user.
- 3. Select the **Properties** tab near the top.
- 4. Locate the User principal name value.
- 5. Locate the **On-premises immutable ID** value.

#### 6.2 Creating an Immutable ID value in Entra

If you have not deployed Microsoft Entra Connect, the user account does not have an Immutable ID value. If your intention is to configure a hybrid deployment, you must configure Microsoft Entra Connect to set the Immutable ID value. If you do *not* intend to configure a hybrid deployment (that is, you want to remain cloud-only) you must generate and configure an Immutable ID value in both MFA and Entra.

To generate a new Immutable ID value and view the results in Entra for a user, run the following PowerShell script, replacing the highlighted values for \$tenantId and \$accountUpn:

\$tenantId = 'federationdemo.com'
\$accountUpn = 'johnd@federationdemo.com'
\$newGuid = [system.guid]::newguid()
\$base64 =
[system.convert]::ToBase64String(([GUID]\$newGuid).ToByteArray())
Connect-MgGraph -TenantId \$tenantId -Scopes 'User.ReadWrite.All' NoWelcome
Update-MgUser -UserId \$accountUpn -OnPremisesImmutableId \$base64

Get-MgUser -UserId \$accountUpn -Property UserPrincipalName, OnPremisesImmutableId | fl UserPrincipalName, OnPremisesImmutableId

**Important:** Once you have set the Immutable ID value, you cannot change it; that is the defining feature of *immutable* IDs.

### 6.3 Adding the Immutable ID value to the MFA user account

Use the MFA Server Rest API to get and set the user account EntraID property.

You can specify the value as Base64 or a GUID formats when setting it. When reading the value, the Base64 version is always returned to allow you to match the value displayed in Entra.

Note: This API call requires administrator rights.

#### 6.3.1 Active Directory user

An MFA user created on an Active Directory user account automatically has an EntraID property, as this is derived from the <code>objectGUID</code> property and cannot be changed. You can only get the value using the MFA server Rest API; you cannot set it.

If you are using an Active Directory user account that is not synchronized with Entra, extract the value from the MFA server and configure it on the Entra user account. Do *not* generate a random GUID (as above) as the account will never match.





#### 6.3.2 External / Realm user

An MFA user created on an External / Realm based user account has an empty EntraID property by default. As it is not an actual Active Directory user account, the objectGUID value is not used. Instead, you can get and set the user's EntraID property using the MFA server Rest API, and you can change it if required.



### 7 Troubleshooting

This section contains troubleshooting information for situations that may occur when working with federated access.

### 7.1 Browser redirect loop between Microsoft 365 and the IdP

Microsoft Entra (Azure AD) and 365 are regularly adding features, changing settings, and updating security defaults. This may cause problems with federated connections from time to time.

The security defaults of Entra may interfere with third-party federated access, as Entra tries to apply Entra MFA security policies which are not being used. This may result in the inability to access the 365 website after a successful federated logon, including a browser redirect loop.

To resolve this problem:

1. Go to the following URL:

https://entra.microsoft.com/#view/Microsoft\_AAD\_IAM/TenantOverview.ReactView ?Microsoft\_AAD\_IAM\_legacyAADRedirect=true

- 2. Select the Properties tab.
- 3. Scroll down to the bottom and click Manage security defaults.
- 4. Select Disabled (not recommended).
- 5. Save the settings.

	Security defaults - Microsoft Entri	< +	~ - c x
÷	→ C 🕯 entra.microso	t.com/#view/Microsoft_AAD_IAM/TenantOverview.ReactView?Microsoft_AAD_IAM_legacyAADRedirect=true	🍋 🖈 🔲 🍮 Incognito 🚦
м	icrosoft Entra admin center	,P Search resources, services, and docs (G+/)	다. 다. 🛞 🕜 🖓 stevenh@federationde 🥥
A	Home	Federation Demo	Security defaults ×
*	Favorites	→ + Add > ③ Manage tenants ⑦ What's new   중 Preview features   R Got feedback? >	Security defaults Disabled (not recommended)
٠	Identity	Azure Active Directory is now Microsoft Entra ID. Learn more (2)	
0	Overview	Overview Monitoring Properties Recommendations Tutorials	With security defaults disabled, your organization is vulnerable to common identity-related attacks.
8	Users	Vasa issassini Lo inisuel ciause compriani ualacentera	99.9% of account compromise could be stopped by using
24	Groups	V Notification language English V	multifactor authentication, which is a feature that security defaults provides.
-6	Devices	Tenant ID 160c0d14-6922-40df-af1c-773151918d17	Microsoft's security teams see a drop of 80% in compromise rate when security defaults are enabled
₿,	Applications	Yechnical contact admin@federationdemo.com	mich second de charcon
8	Protection	Global privacy contact	
۲	Identity governance	Privary statement (IR)	
ŋ	External Identities		
	Show more	Access management for Azure resources	
	Protection	Steven Hope (stevenh@federationdemo.com) can manage access to all Azure subscriptions and management groups in this tena	nt
		No No	
۲	Identity governance	Carucitu defaulte	
-	Verified ID	Security defaults a back identity security mechanisms recommended by Microsoft. When enabled, these recommendations will uses will be better protected from common identity-related attacks.	ь
۵	Permissions Management	Learn more 12	
		Your organization is not protected by security defaults.     Manage security defaults	
2	Learn & support	^	Save Cancel
		CC Save Discard	Cancer

#### 7.2 Unique IssuerUri values

Microsoft requires a unique IssuerUri for each DNS domain registered in Entra; this applies across all tenants, not just your own tenant. If you attempt to federate a domain in Entra using an IssuerUri that has previously been used, may see a PowerShell error similar to:

Unable to complete this action. Try again later.

If you wait and try again as stated, this has no effect. You must make sure your IssuerUri is unique, or make use of the MyID multi-domain configuration; see section *5*, *Multi-domain configuration*.



#### 7.3 Signing certificate error

If, after the MFA login as the browser is redirected back to Microsoft 365, an error occurs similar to the following:

```
Sorry, that didn't work.
Please go back to Office.com and try again.
Thanks.
```

This error is caused by the IdP signing certificate being incorrectly configured.



To resolve this issue:

1. On the Applications Properties dialog, select the **SAML 2.0** tab, then click **Copy Base64** to get the Base64 value of the IdP signing certificate.

y Provider S/	AML 2.0	
entity Provider (	ldP)	
Description:	MyID Identity Provider	
lssuer Uri:	um un idpfederation democom	
ssuer URI:		
um :uri :idpfeder	ationdemocom federationdemocom	
Login URI:		
https://idp.fede	erationdemo.com/idp/SAML/SingleSignOnService/fi	
Logout URI:		
https://idp.fede	$eration demo.com/idp/SAML/SingleLogoutService/f\epsilon$	
Artifact URI:		
https://idp.fede	erationdemo.com/idp/SAML/ArtifactResolutionServic	
Signing Certifica	ite:	
Properties	Copy Base64	
	antity Provider ( Description: ssuer UR: um uni idpfeder ungin URI: https://idp.fed thtps://idp.fed thtps://idp.fed thtps://idp.fed biggning Cettfic: ?opeties	serity Provider (IdP) Description: My/D Identity Provider  ssuer UR: um unidpfederationdemocom um unidpfederationdemocom um unidpfederationdemocom um unidpfederationdemo com/dp/SAML/SingleSignOnService.fs https://dp.federationdemo.com/dp/SAML/SingleSignOnService.fs /kfact URI: https://dp.federationdemo.com/dp/SAML/AtfactResolutionServic Signing Centificate: Signing Centificate: Copy: Base54

#### 2. Run the following PowerShell command:

PS C:\> Get-MgDomainFederationConfiguration -DomainId
'federationdemo.com' | select SigningCertificate

#### The PowerShell returns the signing certificate:

SigningCertificate

\_\_\_\_\_

MIIDGDCCAgCgAwIBAgIQFaTIA1mLiLtJ+wsZt9M2ejANBgkqhkiG9w0BAQsFADAfMR0w GwYDVQQDDBQqLmZ1ZGVyYXRpb25kZW1vLmNvbTAeFw0yNDAzMDUxNDI0NTZaFw0zNDAz MDUxNDM0NTVaMB8xHTAbBgNVBAMMFCouZmVkZXJhdG1vbmRlbW8uY29tMIIBIjANB...



3. Check that the result returned from the PowerShell script is the same as the Base64 you obtained from the Applications Properties dialog.

If the results are not the same, this means that Entra is configured to use a different certificate to the IdP. Ensure the IdP is using the correct signing certificate (not to be confused with the SSL certificate), then configure Entra to use the correct Base64 value.