intercede

MyID 5.0 federation with Microsoft 365

MyID MFA

Product Version: 5.0

Publication date: March 2024

Call us on: +44 (0)1455 558 111 (UK & EMEA)
+1 408 706 2866 (US)

Email us: info@intercede.com

Intercede Ltd, Lutterworth Hall, St. Mary's Road, Lutterworth, Leicestershire, LE17 4PS, United Kingdom
UK Tel: +44 (0)1455 558 111 US Tel: +1 888 646 6943 email: info@intercede.com web: www.intercede.com

Table of Contents

Introduction 3

Prerequisites 3

- Powershell 3
- Verify the current federation configuration 4
- Removing an existing federation configuration 4
- Verify the Entra (Azure AD) default domain 4
- Switching from WS-Fed vs SAML2 5
- DNS and SSL 5

Adding the Microsoft 365 Application 6

Enabling Federation 8

- Configuring the PowerShell Script 8
- Verify the configuration 10
- Testing Federation 11

Troubleshooting 13

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 support federated access to 365 recoures via SAML 2.0 and WS-Fed federation protocols. This document will detail the steps required to configure MyID MFA 5.0 federation with Microsoft 365 using SAML 2.0.

MyID FMA natively supports SAML 2.0 and does not require ADFS for integration.

Prerequisites

This document does not detail how to setup a hybrid environment with Microsoft 365, this must already be in place. Specifically, the following must already be in place:

- Microsoft 365 tenant in "Managed" state (e.g. not currently federated)
- MSOnline PowerShell Module
- Directory synchronization (e.g. Azure AD Connect)
- Entra ID logon (e.g. via on-prem password sync)
- MyID MFA Server deployed
    - MFA users configured and tested (e.g. using Self Service Portal)
    - Public DNS entry for the IdP
    - Public SSL certificate configured on MFA Server matching DNS entry
    - Inbound SSL access to MFA server from the Internet

Powershell

The MSOnine PowerShell module is required for steps in this document. The module can be installed by running the following command at an administrator PowerShell prompt.

```
PS C:\Users\administrator\Desktop> Install-Module MSOnline -Force
```

Verify the current federation configuration

Ensure that the Office tenant is not already setup to use another federation server. Connect to MS Online and check the domain status is “verified” and “managed” by running the following commands:

```
PS C:\Users\administrator\Desktop> Connect-MsolService
Get-MsolDomain

Name                                Status   Authentication
----                                ------   --------------
federationdemo.onmicrosoft.com      Verified Managed
federationdemo.com                  Verified Managed
federationdemo.mail.onmicrosoft.com Verified Managed
```

Removing an existing federation configuration

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

```
PS C:\Users\administrator\Desktop> Connect-MsolService
Set-MsolDomainAuthentication -DomainName federationdemo.com -Authentication Managed
```

> **Note**
> This may take up to two hours to fully take effect in Entra (Azure AD), even if the PowerShell commands show that the configuration has been changed..

Verify the Entra (Azure AD) default domain

Microsoft Entra (Azure AD) does not allow the default domain to be federated. If you want to setup the domain federationdemo.com. To verify that the domain you want to federate with is not the default domain run the following command:

```
PS C:\Users\administrator\Desktop> Connect-MsolService
Get-AzureADDomain | select Name, AuthenticationType, IsDefault

Name                                AuthenticationType IsDefault
----                                ------------------ ---------
federationdemo.onmicrosoft.com      Managed                True
federationdemo.com                  Managed               False
federationdemo.mail.onmicrosoft.com Managed               False
```

If the domain you want to federate with is the default domain you can set the onmicrosoft.com (or another) domain as the default by running the following command:

```
PS C:\Users\administrator\Desktop> Connect-MsolService
Set-AzureADDomain -Name federationdemo.onmicrosoft.com -IsDefault $true
```

Switching from WS-Fed vs SAML2

Microsoft 365 supports both SAML2 and WS-Fed federation protocols. The only Microsoft PowerShell command that allows the setting of the protocol to SAML2 is *Set-MsolDomainAuthentication*. While *Set-MsolDomainFederationSettings* can set many federation properties it cannot set the protocol to SAML2.

Furthermore, this command will only work for a domain that is not already federated, thus to change from WS-Fed to SAML2 you must first disable federation for the domain by making it "Managed". See the *Removing an existing federation configuration* section above.

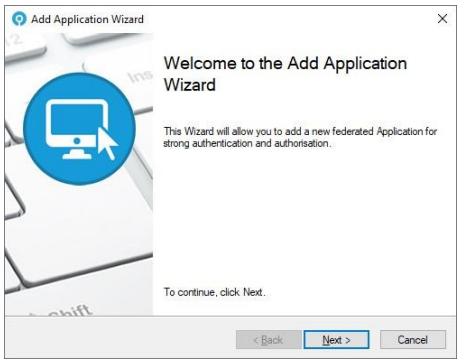
DNS and SSL

The MyID MFA server will require a publicly trusted SSL certificate. The DNS name in the certificate must resolve to the MyID MFA server on the Internet. Network firewalls must allow TCP port 443 from the Internet to the MyID MFA server.

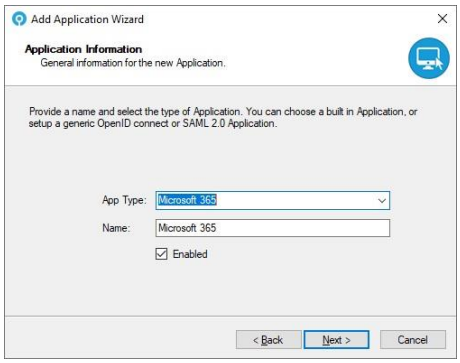
Adding the Microsoft 365 Application

Open the MyID MMC to add an Application.

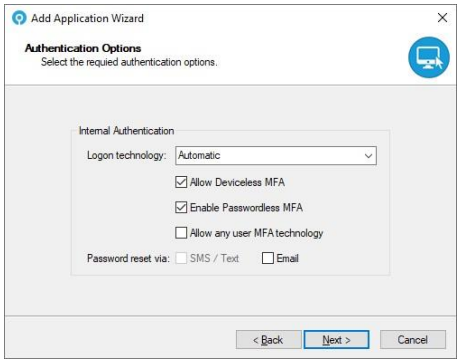
1. Start the Add Application Wizard.



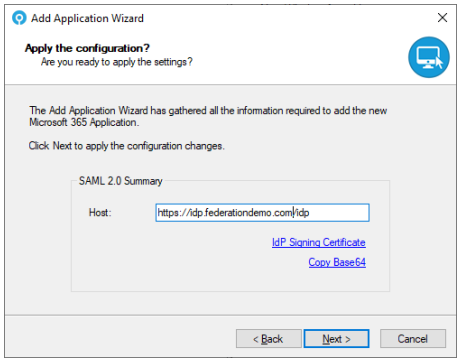
2. Click *Next*.



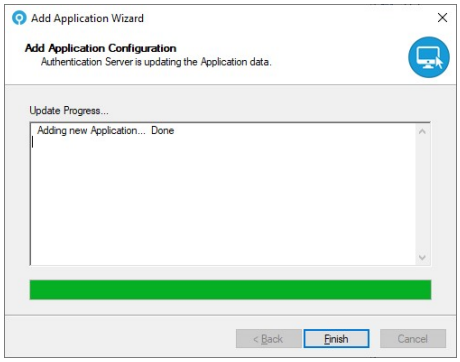
3. Select Microsoft 365 from the list and enter a custom name if required. Click *Next*.



4. Select the required logon technology and authentication options. Click *Next*.



5. Confirm the Host configuration information.
   Click Copy Base64 to copy the base64 signing certificate information to the clipboard.
   Click *Next*.



6. Click Finish.

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

Enabling Federation

The Microsoft 365 side of the configuration is done using PowerShell commands. To simplify the process a custom PowerShell script will be configured with the settings for your environment. When the PowerShell script is run it will configure Microsoft 365 to use the MyID MFA Server for federated authentication.

Configuring the PowerShell Script

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

- **$dom** = The DNS domain to federate which must already be setup in Microsoft 365.
- **$brand** = The friendly shown to users when signing in to Microsoft 365. We recommend that customers use something that is familiar to them, like their company name.
- **$name** = The SAML 2.0 IdP name from the Applications properties tab in the MMC. "`https://IdentityProvider`" is the default value and can be used.
- **$url** = The SMAL 2.0 IdP signon page URL. The path is fixed, however the DNS name must match the public DNS name of the IdP.
- **$logouturl** = The SMAL 2.0 IdP logout page URL. The path is fixed, however the DNS name must match the public DNS name of the IdP.
- **$cert** = The base64 representation of the IdP signing certificate. This value can be obtained by clicking the Copy64 link on the Application Properties tab or at the end of the Add Application Wizard.

7. Copy the text from the sample below to a new text document and save it as a .ps1 file.
8. Configure the yellow highlighted variables in the following sample script with the values of your domain and MyID MFA server
9. Run the script at a PowerShell command prompt to apply the configuration.

```
$dom = "federationdemo.com"
$brand = "Federation Demo"
$name = "https://FederationDemo"
$url= "https://idp.federationdemo.com/idp/SAML/SingleSignOnService"
$logouturl=
"https://idp.federationdemo.com/idp/SAML/SingleLogoutService"
$cert=
"MIIDGDCCAgCgAwIBAgIQFaTIA1mLiLtJ+wsZt9M2ejANBgkqhkiG9w0BAQsFADAf
MR0wGwYDVQQDDBQqLmZlZGVyYXRpb25kZW1vLmNvbTAeFw0yNDAzMDUxNDI0NTZa
Fw0zNDAzMDUxNDM0NTVaMB8xHTAbBgNVBAMMFCouZmVkZXJhdGlvbmRlbW8uY29t
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAnyjM01KPv3y4DUiKYpTH
DT9Gi4c/EGOU6bs8jh0Mke8TjTVWuHGiD98Mj4qLbb/yhk4LHemt58gtjxdj9+pj
gG38OU3dF0n7RMXES6EwK4KlsO16nrXEG6YtP6EelJPkCNXzzSeoeHPCTSMxp1gF
mY/z8fOyI//x/8AmRI2JfGr43exXCbMjYx4sgr85HOCVdw27uHEK9w0hAPPHt2vq
```

```
7BMDAfYj2IisbpVekasJDmXtyhvRFptESJ80qvmmyTLD85iHmO7aME1/7vYnl1RQ
CqbZbhtrWYl4VBAiy/ySnqJdcaJT3KCOVJZOKZxurjXXNJbTHe8i3sQZ0dP2poJZ
tQIDAQABo1AwTjAOBgNVHQ8BAf8EBAMCBaAwHQYDVR0lBBYwFAYIKwYBBQUHAwEG
CCsGAQUFBwMCMB0GA1UdDgQWBBR2d84eaCTxgzIeXnY41uMia8DkJDANBgkqhkiG
9w0BAQsFAAOCAQEACOEinC4t1V80Kgs9MXu843e0UqLseOkoClNZbhxM4n3Y9cTP
b9QYQLQ69g8Q2d6tG+DzTCAnJeTdM2A9QWpePNuGceSWlFHHXHv/ZuzixA2SS2mn
AVvs9GgP1W/l1anMD1mhd4p9F+U0E/KMnn8yo2pYGI/wlwYm0yW3uaDdAQ1WS+fZ
ev2n5WcDbQ6WGklOL5jOJPvkiXcXmzhPc1ogsCvsWCL9OGhFxy3buLTp1N3Rk4dj
Z2hWyoeU8WjYax2436rfQx2qYJvgtAD4MDAzl95N28kzGBWr+eOO460NzDJ2OGc0
rrIZUyo19Uqjje3lNPPyVAzGp+cyrqeRQWpMjg==”
Connect-MsolService
Set-MsolDomainAuthentication -DomainName $dom -Authentication Federated
-SupportsMfa 1 -FederationBrandName $brand -PassiveLogOnUri $url -
SigningCertificate $cert -IssuerUri $name –LogOffUri $logouturl -
PreferredAuthenticationProtocol Samlp
```

Further information relating to the Set-MsolDomainAuthentication PowerShell command can be found here: https://learn.microsoft.com/en-us/powershell/module/msonline/set-msoldomainauthentication?view=azureadps-1.0

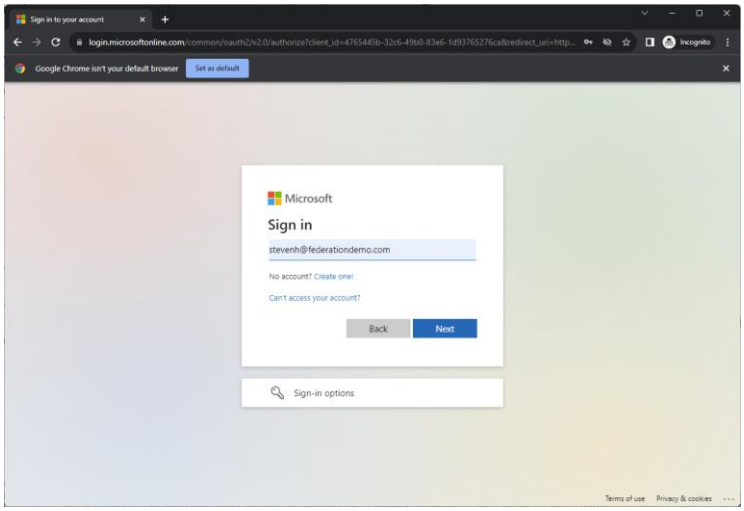
```
PS C:\Users\administrator\Desktop> Connect-MsolService
$dom = “federationdemo.com”
$name = “https://IdentityProvider”
$url= “https://idp.federationdemo.com/idp/SAML/SingleSignOnService”
$logouturl= “https://idp.federationdemo.com/idp/SAML/SingleLogoutService”
$cert=
“MIIDGDCCAgCgAwIBAgIQFaTIA1mLiLtJ+wsZt9M2ejANBgkqhkiG9w0BAQsFADAfMR0wGwYDVQQDDBQqLm
ZlZGVyYXRpb25kZW1vLmNvbTAeFw0yNDAzMDUxNDI0NTZaFw0zNDAzMDUxNDM0NTVaMB8xHTAbBgNVBAMMF
CouZmVkZXJhdGlvbmRlbW8uY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAnyjM01KPv3y4
DUiKYpTHDT9Gi4c/EGOU6bs8jh0Mke8TjTVWuHGiD98Mj4qLbb/yhk4LHemt58gtjxdj9+pjgG38OU3dF0n
7RMXES6EwK4KlsO16nrXEG6YtP6ElJPkCNXzzSeoeHPCTSMxp1gFmY/z8fOyI//x/8AmRI2JfGr43exXCb
MjYx4sgr85HOCVdw27uHEK9w0hAPPHt2vq7BMDAfYj2IisbpVekasJDmXtyhvRFptESJ8OqvmmyTLD85iHm
O7aME1/7vYnl1RQCqbZbhtrWYl4VBAiy/ySnqJdcaJT3KCOVJZOKZxurjXXNJbTHe8i3sQZ0dP2poJZtQID
AQABo1AwTjAOBgNVHQ8BAf8EBAMCBaAwHQYDVR0lBBYwFAYIKwYBBQUHAwEGCCsGAQUFBwMCMB0GA1UdDgQ
WBBR2d84eaCTxgzIeXnY41uMia8DkJDANBgkqhkiG9w0BAQsFAAOCAQEACOEinC4t1V80Kgs9MXu843e0Uq
LseOkoClNZbhxM4n3Y9cTPb9QYQLQ69g8Q2d6tG+DzTCAnJeTdM2A9QWpePNuGceSWlFHHXHv/ZuzixA2SS
2mnAVvs9GgP1W/l1anMD1mhd4p9F+U0E/KMnn8yo2pYGI/wlwYm0yW3uaDdAQ1WS+fZev2n5WcDbQ6WGklO
L5jOJPvkiXcXmzhPc1ogsCvsWCL9OGhFxy3buLTp1N3Rk4djZ2hWyoeU8WjYax2436rfQx2qYJvgtAD4MDA
zl95N28kzGBWr+eOO460NzDJ2OGc0rrIZUyo19Uqjje3lNPPyVAzGp+cyrqeRQWpMjg==”
Set-MsolDomainAuthentication -DomainName $dom -Authentication Federated -
SupportsMfa 1 -FederationBrandName $dom -PassiveLogOnUri $url -SigningCertificate
$cert -IssuerUri $name –LogOffUri $logouturl -PreferredAuthenticationProtocol Samlp
```

Verify the configuration

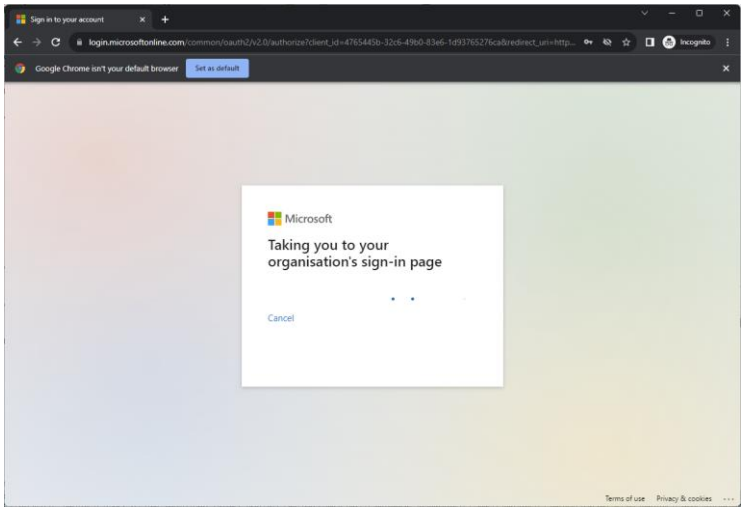
```
PS C:\Users\administrator\Desktop> Connect-MsolService
$dom = “federationdemo.com”
Get-MSolDomainFederationSettings -DomainName $dom | Format-List *



ExtensionData                             :
System.Runtime.Serialization.ExtensionDataObject
ActiveLogOnUri                            :
DefaultInteractiveAuthenticationMethod    :
FederationBrandName                       : federationdemo.com
IssuerUri                                 : https://IdentityProvider
LogOffUri                                 :
https://idp.federationdemo.com/idp/SAML/SingleLogoutService
MetadataExchangeUri                       :
NextSigningCertificate                    :
OpenIdConnectDiscoveryEndpoint            :
PassiveLogOnUri                           :
https://idp.federationdemo.com/idp/SAML/SingleSignOnService
PasswordChangeUri                         :
PasswordResetUri                          :
PreferredAuthenticationProtocol           : Samlp
PromptLoginBehavior                       :
SigningCertificate                        :
MIIDGDCCAgCgAwIBAgIQFaTIA1mLiLtJ+wsZt9M2ejANBgkqhkiG9w0BAQsFADAfMR0wGwYDVQQDDBQqLmZ
lZGVyYXRpb25kZW1vLmNvbTAeFw0yNDAzMDUxNDI0NTZaFw0zNDAzMDUxNDM0NTVaMB8xHTAbBgNVBAMMFC
ouZmVkZXJhdGlvbmRlbW8uY29tMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQ

EAnyjMO1KPv3y4DUiKYpTHDT9Gi4c/EGOU6bs8jhOMke8TjTVWuHGiD98Mj4qLbb/yhk4LHemt58gtjxdj9
+pjgG38OU3dFOn7RMXES6EwK4KlsO16nrXEG6YtP6ElJPkCNXzzSeoeHPCTSMxp1gFmY/z8fOyI//x/8Am
RI2JfGr43exXCbMjYx4sgr85HOCVdw27uHEK9w0hAPPHt2vq7BMDAfYj2IisbpVekasJ

DmXtyhvRFptESJ8OqvmmyTLD85iHmO7aME1/7vYnl1RQCqbZbhtrWYl4VBAiy/ySnqJdcaJT3KCOVJZOKZx
urjXXNJbTHe8i3sQZOdP2poJZtQIDAQABo1AwTjAOBgNVHQ8BAf8EBAMCBaAwHQYDVR0lBBYwFAYIKwYBBQ
UHAwEGCCsGAQUFBwMCMB0GA1UdDgQWBBR2d84eaCTxgzIeXnY41uMia8DkJDANBgkqhk

iG9w0BAQsFAAOCAQEACOEinC4t1V8OKgs9MXu843e0UqLseOkoClNZbhxM4n3Y9cTPb9QYQLQ69g8Q2d6tG
+DzTCAnJeTdM2A9QWpePNuGceSWlFHHXHv/ZuzixA2SS2mnAVvs9GgP1W/l1anMD1mhd4p9F+U0E/KMnn8y
o2pYGI/wlwYm0yW3uaDdAQ1WS+fZev2n5WcDbQ6WGklOL5jOJPvkiXcXmzhPc1ogsCvs

WCL9OGhFxy3buLTp1N3Rk4djZ2hWyoeU8WjYax2436rfQx2qYJvgtAD4MDAzl95N28kzGBWr+eOO46ONzDJ
2OGcOrrIZUyo19Uqjje3lNPPyVAzGp+cyrqeRQWpMjg==
SigningCertificateUpdateStatus            :
SupportsMfa                               : True
```

Testing Federation

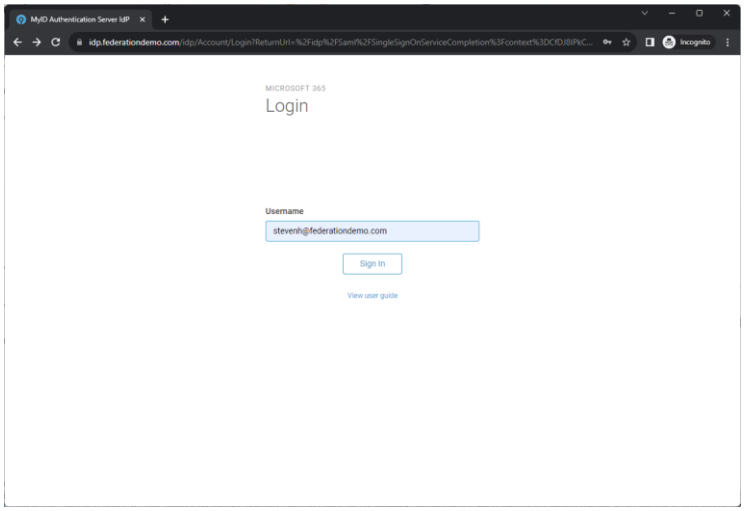
1. To test the federation setup go to https://portal.office.com and sign in.



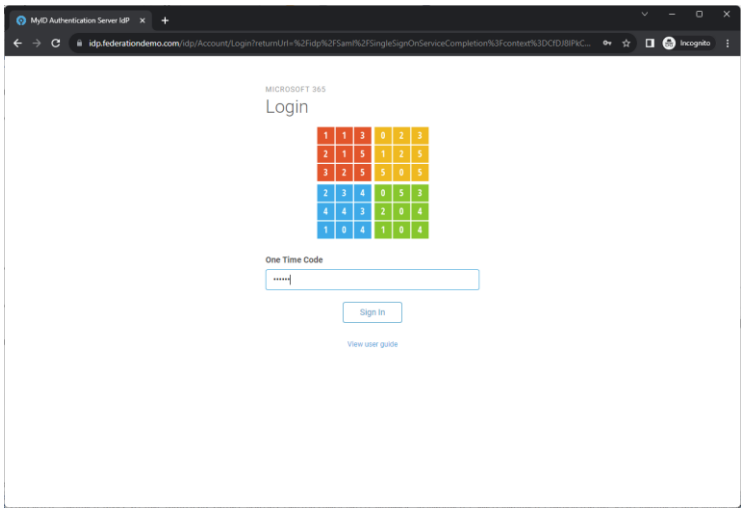
2. Enter your Account name.



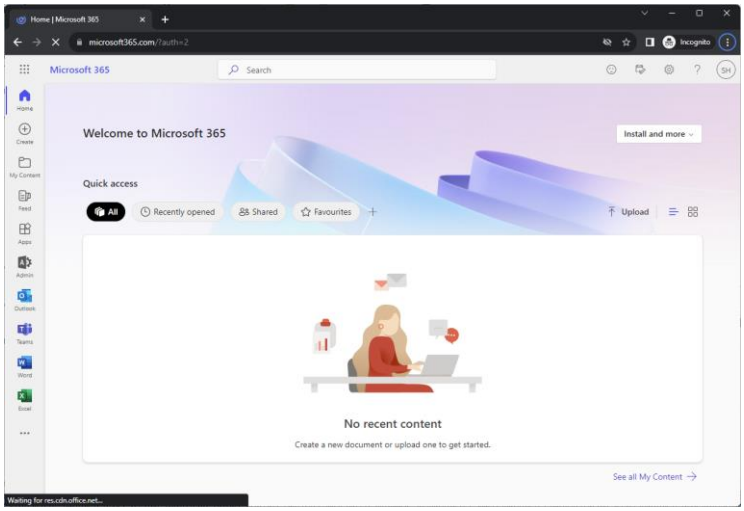
3. Wait while Microsoft redirects you to the MyID MFA logon page.



4. Confirm your account name.



5. Enter your MFA details based on the configuration. This example uses Passwordless & Deviceless Grid authentication.



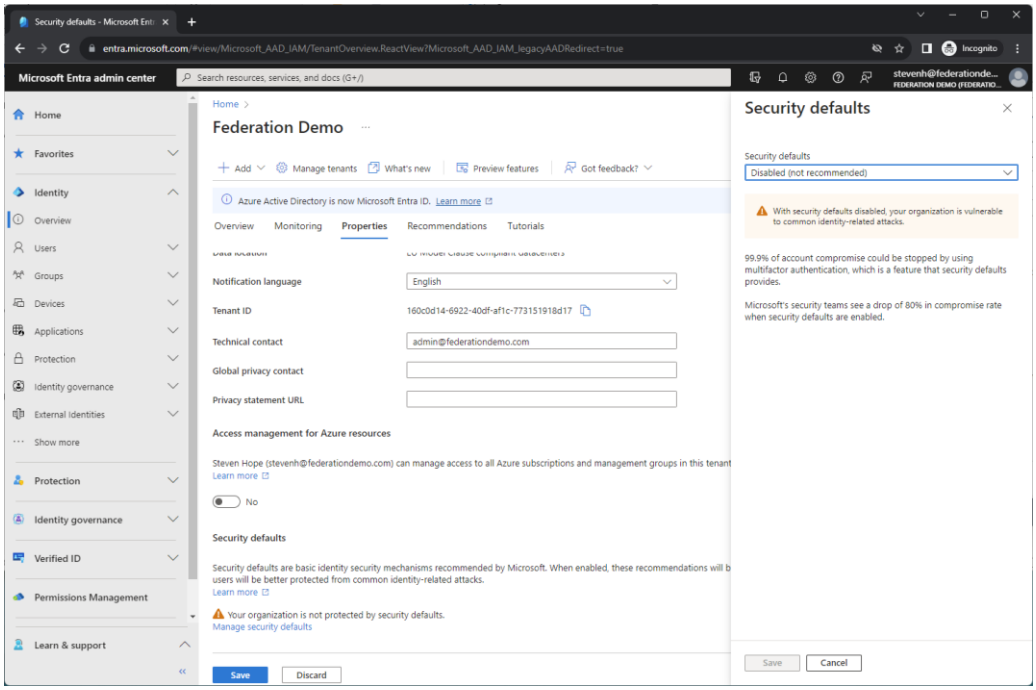
6. Once validated you are redirected back to Microsoft 365 and are signed in.

Troubleshooting

Microsoft Entra (Azure AD) / 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 3rd party federated access as it 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. https://entra.microsoft.com/#view/Microsoft_AAD_IAM/TenantOverview.ReactView?Microsoft_AAD_IAM_legacyAADRedirect=true
2. Select 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 Entra
entra.microsoft.com/#view/Microsoft_AAD_IAM/TenantOverview.ReactView?Microsoft_AAD_IAM_legacyAADRedirect=true
Incognito
Microsoft Entra admin center
Search resources, services, and docs (G+/)
stevenh@federationde...
FEDERATION DEMO (FEDERATIO...
Home
Favorites
Identity
Overview
Users
Groups
Devices
Applications
Protection
Identity governance
External Identities
Show more
Protection
Identity governance
Verified ID
Permissions Management
Learn & support
Home >
Federation Demo
Add
Manage tenants
What's new
Preview features
Got feedback?
Azure Active Directory is now Microsoft Entra ID. Learn more
Overview
Monitoring
Properties
Recommendations
Tutorials
Notification language
English
Tenant ID
160c0d14-6922-40df-af1c-773151918d17
Technical contact
admin@federationdemo.com
Global privacy contact
Privacy statement URL
Access management for Azure resources
Steven Hope (stevenh@federationdemo.com) can manage access to all Azure subscriptions and management groups in this tenant
Learn more
No
Security defaults
Security defaults are basic identity security mechanisms recommended by Microsoft. When enabled, these recommendations will b
users will be better protected from common identity-related attacks.
Learn more
Your organization is not protected by security defaults.
Manage security defaults
Save
Discard
Security defaults
Security defaults
Disabled (not recommended)
With security defaults disabled, your organization is vulnerable to common identity-related attacks.
99.9% of account compromise could be stopped by using multifactor authentication, which is a feature that security defaults provides.
Microsoft's security teams see a drop of 80% in compromise rate when security defaults are enabled.
Save
Cancel