

Notes

This is an all or none type of configuration. Once enabled all users of the domain will be redirected to Launchpad for authentication in all Microsoft applications. Users previously Authenticated to Office 365/Entra ID (Azure AD) may need to reauthenticate their desktop applications. Office365 Administrator accounts will not be affected by this workflow.

Prerequisites

- Authenticate to LaunchPad with AD (technically could be Google as well but unlikely)
- District's Azure user profile **must** contain an ImmutableID
 - If the district uses Azure AD Connect, it's handled
 - If the district enters users manually, it's handled
 - If the district uses OneSync for Azure, it can be handled in the configuration
- Add Verified Domain to Entra ID (Azure AD)
 - Do not make it primary.
- Install MSOnline PowerShell module
- Install Azure Active Directory Connect and configure it – Do not federate via this method.
- Active Directory should be connected in launchpad under settings > domain gear icon
- Active Directory Groups should be imported into launchpad

Step 1

1. In the Classlink tenant SAML Console, Create a new SAML configuration by copying existing and selecting "A New SAML App (template)"
2. Configure the following options.
 - Metadata URL
 - <https://nexus.microsoftonline-p.com/federationmetadata/saml20/federationmetadata.xml>
 - Loginurl with custom login, e.g. <https://launchpad.classlink.com/<customurl>>
 - Attribute Mapping
 - Select "Custom Attribute"
 - Change name of the custom attribute to "IDPEmail"
 - Add {email} in the data field
 - MetaOverrides
 - Logout Service URL (POST)
 - <https://login.microsoftonline.com/common/oauth2/logout>
 - NamedID Format
 - Persistent
 - NameID Custom Value
 - {ldapguid:hexbase64}

- Save or Update

Step 2

- Copy the metadata URL and modify the PowerShell Script below
- Use this PowerShell Script, change the file extension to “.ps1” after downloading - You may need to unblock the file and change your execution policy on the server
 - https://drive.google.com/file/d/1RygKi9I7PmLio6yL1EWihQbn3jerS68X/view?usp=drive_link
- Hit enter key to run
 - If you receive an error regarding scripts being disabled.
 - Open an elevated PowerShell prompt
 - Type the following without Quotation Marks “set-executionpolicy remotesigned -force”
 - This will allow local PowerShell scripts to run
- If you use an account that is being federated (using the custom domain instead of an onmicrosoft.com domain) <https://portal.azure.com> should redirect you to <https://launchpad.classlink.com/<customurl>> for login from now on, along with any other Microsoft Service

Step 3:

- Make sure you have break-glass accounts within Microsoft in case something happens.
 - <https://learn.microsoft.com/en-us/azure/active-directory/roles/security-emergency-access>

Revert to Entra ID (Azure AD) Managed Authentication

1. Open PowerShell
 - a. Run the command
 - i. Connect-MsolService
 - b. After authenticating to your Entra ID (Azure AD) Tenant
 - c. Run the command
 - i. Set-MsolDomainAuthentication -authentication managed -domainName <domainname>
 - ii. Replace <domainname> with your domain you wish to remove federation