Setting-up Azure Entra with Classlink

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 ImmutableI
  - 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-Module MSOnline
```

- 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
    - Google Drive

Azure AD PowerShell Code

```
<#
.SYNOPSIS
    Federate Microsoft Entra ID (Azure AD/Microsoft Online Services) to ClassLink for IdP Services.

    Change the <GUID> in the $idpMetadataUrl to be the GUID from your SAML console App.
    Change $DomainName to match your domain name that is going to be Federated
    Change the script extension to ".ps1"

    *NOTE: you may need to set the PowerShell Execution Policy to remote signed or bypass temporarily.

#>

Install-Module -Name MSOnline
Import-Module MSOnline

$idpMetadataUrl = "https://idp.classlink.com/sso/metadata/<GUID>"

$DomainName = "<your domain name>"
```

```
$metadataxml = [Xml](Invoke-WebRequest -Uri $idpMetadataUrl -ContentType
"application/xml").content

$cert = -join
$metadataxml.EntityDescriptor.IDPSSODescriptor.KeyDescriptor.KeyInfo.X509Data.X509Certific
ate.Split()
$issuerUri = $metadataxml.EntityDescriptor.entityID
$logOnUri = $metadataxml.EntityDescriptor.IDPSSODescriptor.SingleSignOnService | ? {
$_.Binding.Contains('Redirect') } | % { $_.Location }
$LogOffUri = $metadataxml.EntityDescriptor.IDPSSODescriptor.SingleLogoutService | ? {
$_.Binding.Contains('Redirect') } | % { $_.Location }
$brand = "ClassLink Identity"
Connect-MsolService
$DomainAuthParams = @{
    DomainName = $DomainName
    Authentication = "Federated"
    IssuerUri = $issuerUri
    FederationBrandName = $brand
    ActiveLogOnUri = $logOnUri
    PassiveLogOnUri = $logOnUri
    LogOffUri = $LogOffUri
    SigningCertificate = $cert
    PreferredAuthenticationProtocol = "SAMLP"
}

Set-MsolDomainAuthentication @DomainAuthParams
```

If you receive an error regarding scripts being disabled Open an elevated PowerShell prompt
Type the following:
`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

Open PowerShell

1. Run the command
2. Connect-MsolService

After authenticating to your Entra ID (Azure AD) Tenant

Run the command:

```
  Set-MsolDomainAuthentication -authentication managed -domainName
<domainname>
```

> Replace `<domainname>` with your domain you wish to remove federation

Revision #7
Created 15 May 2024 11:31:13 by joliveira
Updated 15 May 2024 12:06:14 by joliveira