Microsoft Viva

Set up federation of Google with AAD

Google Federation Pre-Step:

If you are currently using a Microsoft product or have a user already present in AAD, the **on-premises immutable id** will need to be set manually, as Google is not able to map an immutable id to the present user in AAD. The on-premises immutable id can be updated by following the commands run in PowerShell ISE:

- Connect-AzureAD
- $user = Get-AzureADUser -UserPrincipleName <User principal name>
- $immutableId = '<UPN>'
- $user | Set-AzureADUser -ImmutableId $immutableId

After running these commands, try signing in to AAD. Once you sign in successfully, you'll need to bulk update for all users by running the code below as shown in the image. In the CSV file, you will need to have one attribute as UPN and the other attributes as immutable id. In this case, UPN and immutable id should be the same.

```
# Connect to AzureAD
Connect-AzureAD

# Get CSV content
$CSVrecords = Import-Csv C:\Temp\Test.csv -Delimiter ";"

# Create arrays for skipped and failed users
$SkippedUsers = @()
$FailedUsers = @()

# Loop trough CSV records
foreach ($CSVrecord in $CSVrecords) {
    $upn = $CSVrecord.UserPrincipalName
    $user = Get-AzureADUser -Filter "userPrincipalName eq '$upn'"
    if ($user) {
        try{
        $user | Set-AzureADUser -immutableId $CSVrecord.immutableId
        } catch {
        $FailedUsers += $upn
        Write-Warning "$upn user found, but FAILED to update."
        }
    }
    else {
        Write-Warning "$upn not found, skipped"
        $SkippedUsers += $upn
    }
}

# Array skipped users
# $SkippedUsers

# Array failed users
# $FailedUsers
```

1. **Create a SAML app in Google:**
    a. Go to Apps >> Web and Mobile Apps
    b. Click on add apps and search for Microsoft
    c. In the list shown, please select Microsoft Office 365 SAML application
    d. Check on Signed Response
    e. In the Attributes section, select Primary Email to map to IDPEmail*. AAD will use this email as UPN (or user principal name)
    f. Turn on the user access for everyone or specific groups so that users can see this SAML app. Please note that it takes up to few minutes for users to start seeing this app.

2. **Add the domain that needs to be federated from Google workspace to AAD.**
    a. Go to admin.microsoft.com > Settings > Domains on the left panel
    b. Click on add domain
    c. Enter your domain which you want to federate from Google workspace to AAD. For example, if you want to federate users with @contoso.com in Google workspace, you need to specify contoso.com as your domain.
    d. If it's a GoDaddy domain or a Google workspace domain, you will be asked sign into GoDaddy or google workspace to verify the domain.
        i. AAD might also ask you to add some custom TXT records in your domain settings
        ii. Selecting using exchange is optional. Its recommended not to select it if the domain is Google managed as DNS records addition might cause some issues.
        iii. Once the addition is successful, you should be able to see the newly added domain.
        iv. If the newly added domain is a default domain, please set some other domain as the default domain.
        v. 3P federated domains ideally should not be default domains.
        vi. Please wait for few minutes so that the domain information is propagated. It takes up to 3-10 minutes for it to propagate.

3. **Configure auto provisioning in Google**
    a. Go back to the Google Workspace SAML app created in step 1. Click on configure auto provisioning.
    b. Authorize using the google workspace admin email.

c. If the authorization returns Oauth2 error, please try the following - Sign into the AAD account created in 1. in the same browser session. If it still doesn't work, reach out to Microsoft support.
d. Go to attribute mapping step and configure the following:
    i. onPremisesImmutableId* should be set to Email > Value
    ii. UserPrincipalName* should be set to Email > Value
    iii. mailNickname* should be set to Additional Details > Alias name
e. Specify group(s) from which the users should be provisioned. If you don't specify one, then everyone who has access to this SAML application will be provisioned
f. Select Deprovisioning settings
    i. Select the option of Hard deleting a user from O365 if the user is deleted from Google workspace. This will save effort to manage user deletion in both the IDPs.
    ii. Rest of the option could be selected by you based on convenience.
    iii. Turn on user provisioning
    iv. It takes 15-20 minutes for user provisioning to kick in and is controlled by Google workspace
    v. Any updates to users should also be triggered in a similar amount of time.
g. Download the SAML metadata and store it somewhere locally in your machine

4. In order to setup federated authentication via AAD, please run the following commands in PowerShell from a windows device as an administrator

a. Install-Module MSOnline
b. Import-Module MSOnline
c. Connect-MsolService
d. $domainName = "<your domain>"
e. [xml]$idp = **Get-Content** <metadata-xml-file-path>
f. $activeLogonUri = "https://login.microsoftonline.com/login.srf"
g. $signingCertificate = ($idp.EntityDescriptor.IDPSSODescriptor.KeyDescriptor.KeyInfo.X509Data.X509Certificate | **Out-String**).Trim()
h. $issuerUri = $idp.EntityDescriptor.entityID
i. $logOffUri = $idp.EntityDescriptor.IDPSSODescriptor.SingleSignOnService.Location[0]
j. $passiveLogOnUri = $idp.EntityDescriptor.IDPSSODescriptor.SingleSignOnService.Location[0]
k. Set-MsolDomainAuthentication -DomainName $domainName -FederationBrandName $domainName -Authentication Federated -PassiveLogOnUri $passiveLogOnUri -ActiveLogOnUri $activeLogonUri -SigningCertificate $signingcertificate -IssuerUri $issuerUri -LogOffUri $logOffUri -PreferredAuthenticationProtocol "SAMLP"

5. You can test if the setup is working fine or not by hitting goals.microsoft.com and using your google workspace email to authenticate. You will be redirected to the tenant not allowed page but that's fine. The next step will ensure that you have access to the Viva Goals application.