Azure AD Integration Reference Guide

AZURE AD

eScribe Software Ltd.
IMPLEMENTATION | REFERENCE GUIDE – VERSION 1.4

Contents

1.0 OVERVIEW:

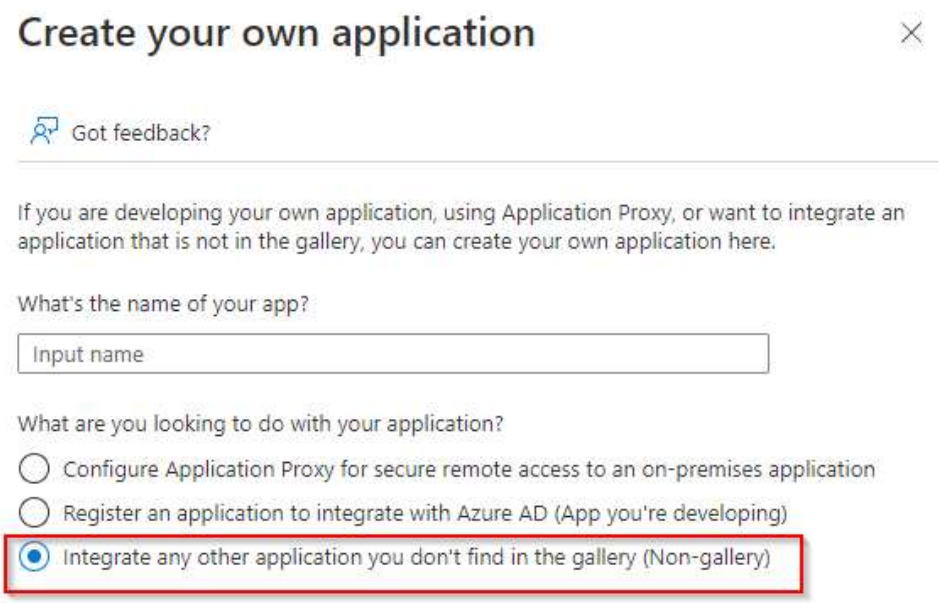
This document is meant to serve only as a reference for generating the information that is required by eScribe for your Azure integration. After completing this guide, you should be able to fill the requirements in the tables set by eScribe throughout this document.

2.0 PREREQUISITES:

1. Portal access to your Azure Tennant
2. One user account with the ability to create a new enterprise application
    - P1 or P2 License must be assigned to this user account

3.0 CREATING A NEW ENTERPRISE APPLICATION:

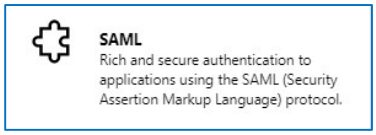
1. Open an internet browser, and sign into your tenant at https://portal.azure.com
2. Select "**Enterprise Applications**" from the list of categories
3. Select "**New Application**"
4. Select "**Create your own application**" (Without a premium P1/P2 License, this feature will be locked)



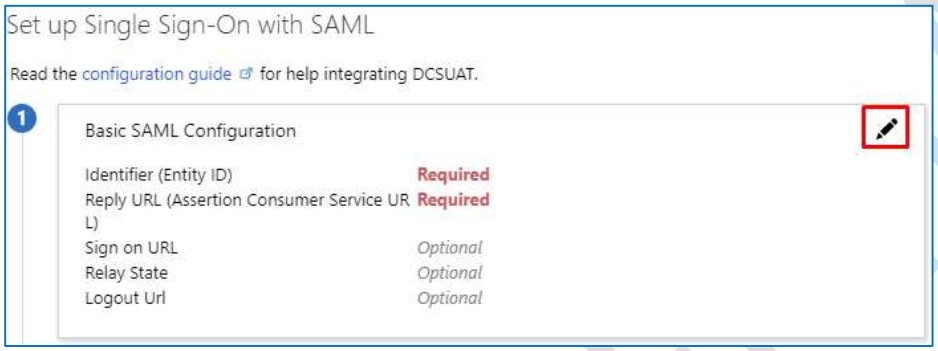
5. **Name** the enterprise application (We suggest prepending the app name with *eScribe* for easy identification)
6. Select **"Integrate any other application you don't find in the gallery (Non-gallery)"**
7. Select **"Create"** to create the application. The enterprise application menu will now appear on the next screen.

4.0 CONFIGURING THE ENTERPRISE APPLICATION:

8. On the Enterprise application screen (getting started), select "**Single sign-on**"
9. Select the option for "**SAML**".

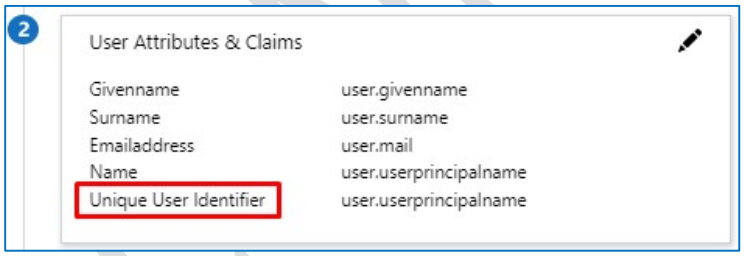


10. ***Edit*** "Basic SAML Configuration", and **supply** values below., Update your Azure settings (reference screenshot).

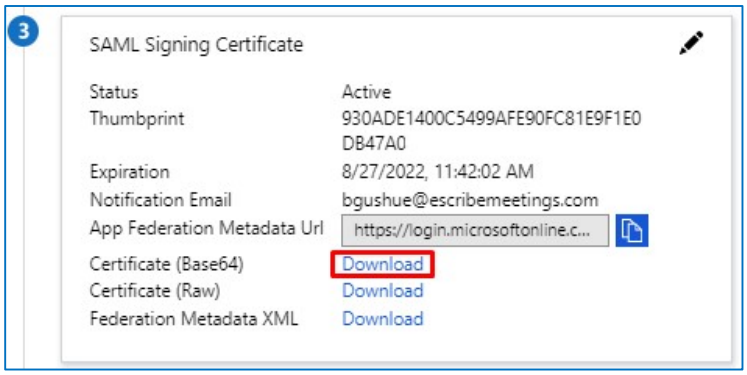


Property	**Values [Replace the yellow highlights with YOUR values]**
Identifier (Entity ID)	urn:eScribe:<subdomain>.eScribemeetings.com
Reply URL	https://<subdomain>.eScribemeetings.com/_trust/default.aspx
Sign on URL	https://<subdomain>.eScribemeetings.com/_trust/default.aspx

11. ***Review*** properties for "User Attributes & Claims". Ensure *Unique User Identifier* is set to **user.userprinciplename**

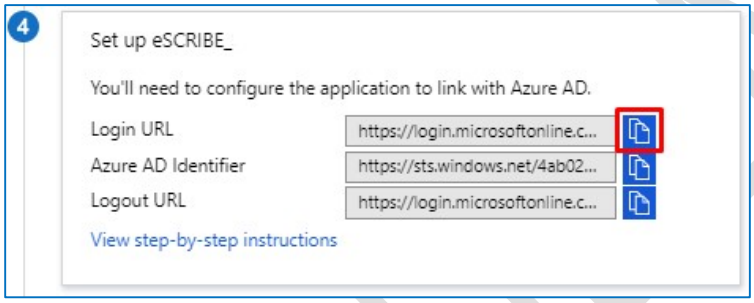


12. ***Download and Attach*** your SAML Signing Certificate from the "SAML Signing Certificate" section



SAML Signing Certificate	Attach your SAML Signing Certificate HERE

13. ***Provide*** your Login URL from the "Set Up" section



Login URL	Copy and Paste your Login URL HERE

14. Navigate to the **Properties** section of your Enterprise Application underneath the *Manage* category. Provide the values of your Application ID and Object ID.

Object ID	Copy and Paste your Object ID HERE

5.0 MANAGING USERS AND GROUPS:

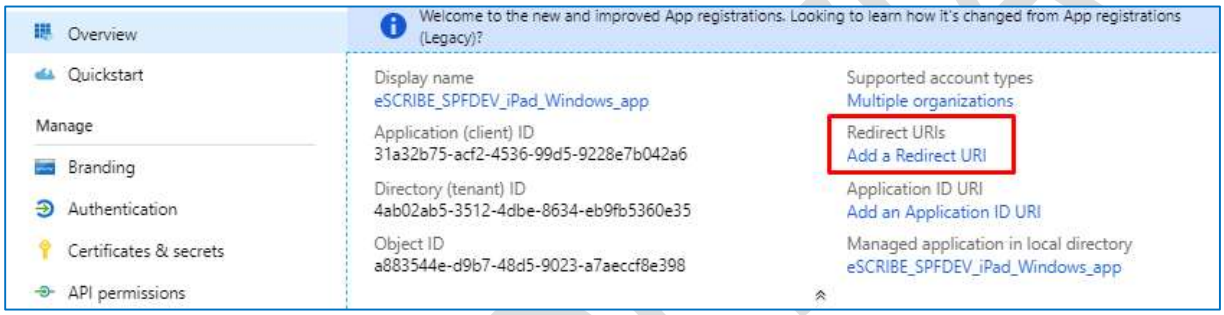
15. Navigate to the **Users and Groups** section of your Enterprise Application underneath the *Manage* category. Add three user accounts for eScribe Support:

eScribeAdministrator@yourdomain.com	Please insert account credential HERE
eScribeContributor@yourdomain.com	Please insert account credential HERE
eScribeParticipant@yourdomain.com	Please insert account credential HERE

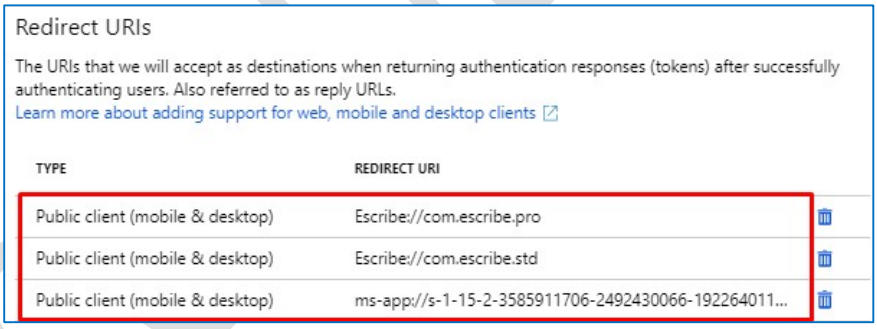
16. In addition to the support accounts above, other users in your organization will need access to this application so they can sign in. Add all other users who need access to eScribe.

6.0 IPAD AND WINDOWS APPLICATION SETTINGS:

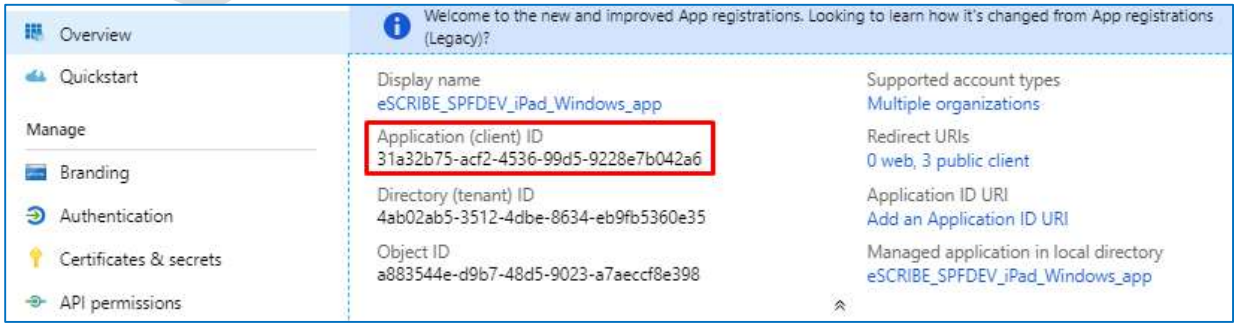
17. Select "**Azure Active Directory**" from the list of categories, and then select "**App Registrations**"
18. Select "**New Application**"
19. Select "**New Registration**", and then provide a name such as: eScribe_iPad_Windows_app
20. Select an option under "**Supported account types"** (Single or Multitenant)
21. **Register** (The application page will now open)
22. Select "**Redirect URIs**", and add 3 *Public Client* entries



   a. **EScribe://com.eScribe.pro**
   b. **EScribe://com.eScribe.std**
   c. **ms-app://s-1-15-2-3585911706-2492430066-1922640115-3814228788-4263615920-112324596-2256370002/**

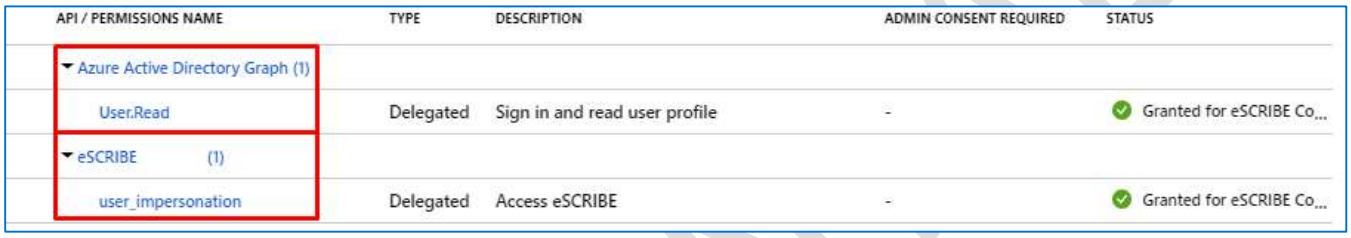


23. ***Provide*** your Application (client ID) from your App Registration page.

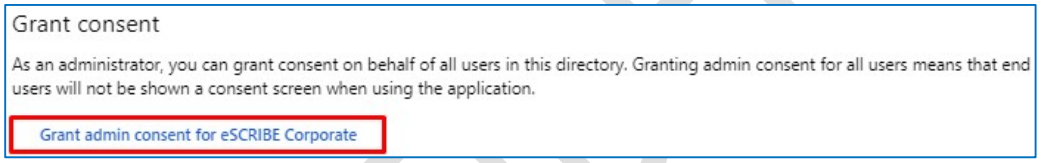


Application (Client) ID	Copy and Paste your Application (client) ID HERE

24. Select "**API Permissions**", and then ***remove*** the default User.Read permission under "*Microsoft Graph*"
25. Add two new permissions:
    a. *Add permission* > APIs my organization uses > search for your eScribe enterprise application created in section 3.0 > Delegated Permissions > Select *user_impersonation* permission > Add permissions
    b. *Add Permission* > Microsoft APIs > Azure Active Directory Graph > Delegated Permissions > expand user > select *User.read* permission > Add permissions



26. Grant admin consent



7.0 TENANT CONFIGURATION [PowerShell]:

27. Please follow below steps prior step #27

Set strong cryptography on 64 bit .Net Framework (PowerShell version 5.1 and above).
`Set-ItemProperty -Path 'HKLM:\SOFTWARE\Wow6432Node\Microsoft\.NetFramework\v4.0.30319' -Name 'SchUseStrongCrypto' -Value '1' -Type DWord`

Set strong cryptography on 32 bit .Net Framework (PowerShell version 5.1 and above).
`Set-ItemProperty -Path 'HKLM:\SOFTWARE\Microsoft\.NetFramework\v4.0.30319' -Name 'SchUseStrongCrypto' -Value '1' -Type DWord`

Restart Powershell and check for supported security protocols.
`[Net.ServicePointManager]::SecurityProtocol`

Returning results: Tls, Tls11, Tls12

Run the command Install-Module PowershellGet -Force and press Y to install NuGet provider, follow with Enter.

```
Install-Module PowershellGet -Force
```

28. Download and import the attached module [MSGraphTokenLifetimePolicy.psm1].
    The commands in this section can be executed on any workstation or server running the latest version of PowerShell and after step #27 completed

SAMLConfigPolicies.zip

Cd <the path where the zip file was extracted>

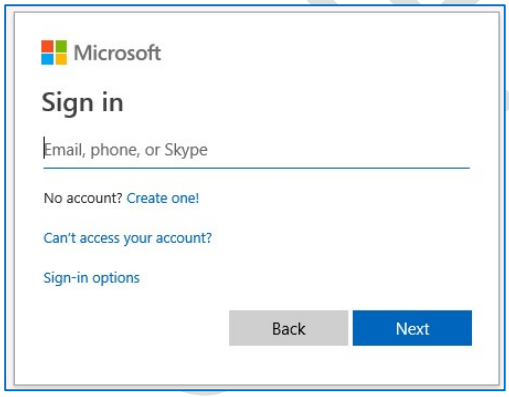
PS C:\SAMLConfigPolicies> Import-Module C:\SAMLConfigPolicies\Initialize.ps1

```
PS C:\WINDOWS\system32> cd C:\SAMLConfigPolicies
PS C:\SAMLConfigPolicies> Import-Module C:\SAMLConfigPolicies\Initialize.ps1
Importing Module: .\MSGraphTokenLifetimePolicy.psm1
Loading ADAL Assemblies ...
True
PS C:\SAMLConfigPolicies>
```

29. Issue a new SAML 1.1 Claim Rule using the below command

    Add-TokenIssuancePolicy -DisplayName eScribe_SharePointSAML1.1 -SigningAlgorithm "http://www.w3.org/2001/04/xmldsig-more#rsa-sha256" -TokenResponseSigningPolicy TokenOnly -SamlTokenVersion "1.1"

    Sign into your AzureAD Tenant using an account with Global Admin rights.



Example Output: Take note of your new Token Issuance policy **Object ID** for future commands.

```
odata.metadata      : https://graph.windows.net/myorganization/$metadata#directoryObjects/@Element
odata.type          : Microsoft.DirectoryServices.Policy
objectType          : Policy
objectId            : 89e4614f-8fac-4577-9fe7-77cc7b6ae45f
deletionTimestamp   :
displayName         : eSCRIBE_SharePointSAML1.1
keyCredentials      : {}
policyType          : 17
policyDetail        : {{"TokenIssuancePolicy":{"TokenResponseSigningPolicy":"TokenOnly","SamlTokenVersion":"1.1","Signi
                      ngAlgorithm":"http://www.w3.org/2001/04/xmldsig-more#rsa-sha256","Version":1}}}
policyIdentifier    :
tenantDefaultPolicy :
```

30. Obtain the default policy assigned to your Enterprise Application.

    Get-PoliciesAssignedToServicePrincipal -servicePrincipalId <OBJECT ID Value from Step 14>

```
PS C:\eInstall\SAMLConfigPolicies> Get-PoliciesAssignedToServicePrincipal -servicePrincipalId cc82b1b2-7696-4bb2-b173-4c
486cb1ab9f
GetPoliciesAssignedToEntityUrl: Using graph endpoint: https://graph.windows.net entity: servicePrincipals entityId: cc82
b1b2-7696-4bb2-b173-4c486cb1ab9f
HTTP GET https://graph.windows.net/myorganization/servicePrincipals/cc82b1b2-7696-4bb2-b173-4c486cb1ab9f/defaultPolicy?a
pi-version=1.61-internal


odata.type          : Microsoft.DirectoryServices.Policy
objectType          : Policy
objectId            : ec81099a-ed17-4831-9015-ff7f41f7d029
deletionTimestamp   :
displayName         : ClaimIssuancePolicy
keyCredentials      : {}
policyType          : 2
policyDetail        : {{
                        "AuthenticationPolicies": {
```

31. Remove the default policy from your Enterprise Application.

    Remove-PolicyFromServicePrincipal -policyId <OBJECT ID Value from Step 30> -servicePrincipalId <OBJECT ID Value from Step 14>

```
PS C:\eInstall\SAMLConfigPolicies> Remove-PolicyFromServicePrincipal -policyId ec81099a-ed17-4831-9015-ff7f41f7d029 -ser
vicePrincipalId cc82b1b2-7696-4bb2-b173-4c486cb1ab9f
AssignPolicyToEntity: Using graph endpoint: https://graph.windows.net entity: servicePrincipals entityId: cc82b1b2-7696-
4bb2-b173-4c486cb1ab9f
HTTP DELETE https://graph.windows.net/myorganization/servicePrincipals/cc82b1b2-7696-4bb2-b173-4c486cb1ab9f/$links/defau
ltPolicy/ec81099a-ed17-4831-9015-ff7f41f7d029?api-version=1.61-internal
```

32. Verify that the policy was successfully removed. Run the same command from step 29, and the output should appear similar to below:

```
PS C:\eInstall\SAMLConfigPolicies> Get-PoliciesAssignedToServicePrincipal -servicePrincipalId cc82b1b2-7696-4bb2-b173-4c
486cb1ab9f
GetPoliciesAssignedToEntityUrl: Using graph endpoint: https://graph.windows.net entity: servicePrincipals entityId: cc82
b1b2-7696-4bb2-b173-4c486cb1ab9f
HTTP GET https://graph.windows.net/myorganization/servicePrincipals/cc82b1b2-7696-4bb2-b173-4c486cb1ab9f/defaultPolicy?a
pi-version=1.61-internal
```

33. Add the new Token Issuance Policy [created in step 29] to your Enterprise Application.

    Set-PolicyToServicePrincipal -policyId <OBJECT ID Value from Step 29> -servicePrincipalId <OBJECT ID Value from Step 14>

```
PS C:\eInstall\SAMLConfigPolicies> Set-PolicyToServicePrincipal -policyId 32ae49e6-814c-4981-8c6f-07b0d417e262 -serviceP
rincipalId cc82b1b2-7696-4bb2-b173-4c486cb1ab9f
AssignPolicyToEntity: Using graph endpoint: https://graph.windows.net entity: servicePrincipals entityId: cc82b1b2-7696-
4bb2-b173-4c486cb1ab9f
GetEntityUrl: Using graph endpoint: https://graph.windows.net entity: policies entityId: 32ae49e6-814c-4981-8c6f-07b0d41
7e262
HTTP POST https://graph.windows.net/myorganization/servicePrincipals/cc82b1b2-7696-4bb2-b173-4c486cb1ab9f/$links/default
Policy?api-version=1.61-internal
{"url":"https://graph.windows.net/myorganization/policies/32ae49e6-814c-4981-8c6f-07b0d417e262?api-version=1.61-internal
"}
```

8.0 INCREASING TOKEN LIFE TIME:

34. Download and Install the latest **AzureAD Model Public Release** for PowerShell. Latest PowerShell version is recommended for compatability.
    https://www.powershellgallery.com/packages/AzureADPreview/
    Install-Module AzureADPreview -AllowClobber

    Note: If there is an error from Step 35, Uninstall the AzureAD Module using UnInstall-Module AzureAD

35. Connect to your Azure AD Tenant
    Connect-AzureAD -Confirm

36. Create a new TokenLifeTime Policy. Set the access/ID token lifetime and the max single-factor session token age to three hours. You may adjust the command values as required.
    New-AzureADPolicy -Definition @('{"TokenLifetimePolicy":{"Version":1, "AccessTokenLifetime":"03:00:00"}}') -DisplayName "eScribe_Tokenlifetime_eScribe_Timeout" -IsOrganizationDefault $false -Type "TokenLifetimePolicy"

```
PS C:\WINDOWS\system32> New-AzureADPolicy -Definition @('{"TokenLifetimePolicy":{"Version":1,"AccessTokenLifetime":"03:0
0:00","MaxAgeSessionSingleFactor":"03:00:00"}}') -DisplayName "eSCRIBE_Tokenlifetime_eSCRIBE_Timeout" -IsOrganizationDef
ault $false -Type "TokenLifetimePolicy"

Id                                   DisplayName                          Type                IsOrganizationDefault
--                                   -----------                          ----                ---------------------
869e08c5-4375-4b8b-98d5-b9ecae2aa79f eSCRIBE_Tokenlifetime_eSCRIBE_Timeout TokenLifetimePolicy False
```

37. Verify that your policy has been created.
    Get-AzureADPolicy -id <OBJECT ID value from Step 36>

38. Add your new TokenLifeTime policy to the enterprise application.
    Add-AzureADServicePrincipalPolicy -Id <OBJECT ID Value from Step 14> -RefObjectId <OBJECT ID value from Step 36>

```
PS C:\WINDOWS\system32> Add-AzureADServicePrincipalPolicy -Id cc82b1b2-7696-4bb2-b173-4c486cb1ab9f -RefObjectId 104878dc
-af3c-4980-b242-19b23a95f427
```

39. Verify that the policy has been added to your Tenant policy. There should be two entries.

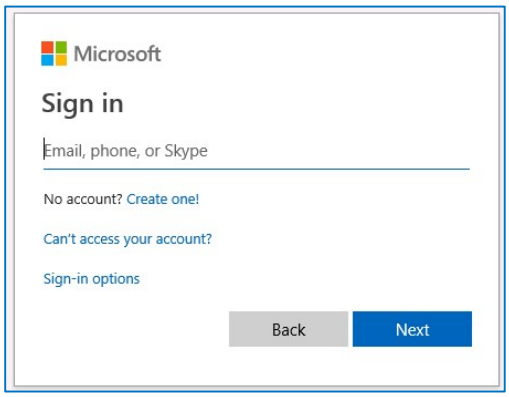
```
PS C:\WINDOWS\system32> Get-AzureADServicePrincipalPolicy -Id cc82b1b2-7696-4bb2-b173-4c486cb1ab9f

Id                                   DisplayName                          Type                IsOrganizationDefault
--                                   -----------                          ----                ---------------------
32ae49e6-814c-4981-8c6f-07b0d417e262 SPFDEV_SharePointSAML1.1             TokenIssuancePolicy False
869e08c5-4375-4b8b-98d5-b9ecae2aa79f eSCRIBE_Tokenlifetime_eSCRIBE_Timeout TokenLifetimePolicy False
```

40. Verify if the Token Life Time policy has been applied to the Enterprise application step #14

    Open a new powershell session, run the import module command, follow step #28

    Get policy assigned to service principal.
    Get-PoliciesAssignedToServicePrincipal -servicePrincipalId <OBJECT ID Value from Step 14>

    Sign into your AzureAD Tenant using an account with Global Admin rights.



Output:

```
PS C:\WINDOWS\system32> cd C:\SAMLConfigPolicies
PS C:\SAMLConfigPolicies> Import-Module C:\SAMLConfigPolicies\Initialize.ps1
Importing Module: .\MSGraphTokenLifetimePolicy.psm1
Loading ADAL Assemblies ...
True
PS C:\SAMLConfigPolicies> Get-PoliciesAssignedToServicePrincipal -servicePrincipalId cc82b1b2-7696-4bb2-b173-4c486cb1ab9f
GetPoliciesAssignedToEntityUrl: Using graph endpoint: https://graph.windows.net entity: servicePrincipals entityId: cc82b1b2-7696-4bb2-b173-4c486cb1ab9f
HTTP GET https://graph.windows.net/myorganization/servicePrincipals/cc82b1b2-7696-4bb2-b173-4c486cb1ab9f/defaultPolicy?api-version=1.61-internal


odata.type          : Microsoft.DirectoryServices.Policy
objectType          : Policy
objectId            : 32ae49e6-814c-4981-8c6f-07b0d417e262
deletionTimestamp   :
displayName         : SPFDEV_SharePointSAML1.1
keyCredentials      : {}
policyType          : 17
policyDetail        : {{"TokenIssuancePolicy":{"TokenResponseSigningPolicy":"TokenOnly","SamlTokenVersion":"1.1","Signi
                      ngAlgorithm":"http://www.w3.org/2001/04/xmldsig-more#rsa-sha256","Version":1}}}
policyIdentifier    :
tenantDefaultPolicy :

odata.type          : Microsoft.DirectoryServices.Policy
objectType          : Policy
objectId            : 104878dc-af3c-4980-b242-19b23a95f427
deletionTimestamp   :
displayName         : eSCRIBE_Tokenlifetime_SPFDEV_Timeout
keyCredentials      : {}
policyType          : 13
policyDetail        : {{"TokenLifetimePolicy":{"Version":1,"AccessTokenLifetime":"03:00:00","MaxAgeSessionSingleFactor"
                      :"03:00:00"}}}
policyIdentifier    :
tenantDefaultPolicy :


PS C:\SAMLConfigPolicies>
```

TokenLifeTime policy applied to Enterprise Application
Paste the screenshot here:

41. Setup is now complete. Please return back to eScribe.

--------- Below are optional setting to increase the tokenlifetime policy if it was set to 3hours from above command--------

9.0 UPDATE TIMEOUT FROM 3 HOURS TO 8 HOURS.

42. Open a new powershell session, run the import module command, follow step #28

    Get policy assigned to service principal.

    Get-PoliciesAssignedToServicePrincipal -servicePrincipalId <OBJECT ID Value from Step 14>

    Take note of the Object ID of the current TokenlifetimePolicy

43. Remove-PolicyFromServicePrincipal -policyId <ObjectID from above result (TokenlifetimePolicy)> -servicePrincipalId <OBJECT ID Value from Step 14>

    Verify if that the timeout policy is no longer assigned to the eScribe application.

    Get-PoliciesAssignedToServicePrincipal -servicePrincipalId <OBJECT ID Value from Step 14>

44. Create a new TokenLifeTime Policy. Set the access/ID token lifetime and the max single-factor session token age to three hours. Adust the command values to 08:00:00
    New-AzureADPolicy -Definition @('{"TokenLifetimePolicy":{"Version":1, "AccessTokenLifetime":"08:00:00"}}') -DisplayName "eScribe_Tokenlifetime_eScribe_Timeout" -IsOrganizationDefault $false -Type "TokenLifetimePolicy"

45. Add your new TokenLifeTime policy to the enterprise application.
    Add-AzureADServicePrincipalPolicy -Id <OBJECT ID Value from Step 14> -RefObjectId <OBJECT ID value from Step 44>

46. Follow step 42 to verify if the new policy has been applied.

10.0 REFERENCES LINK FROM MICROSOFT TO SUPPORT CONFIGURATION.

- https://docs.microsoft.com/en-us/azure/active-directory/saas-apps/samlssoconfluence-tutorial
- https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/non-gallery-apps
- https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/add-application-portal-setup-sso
- https://devblogs.microsoft.com/powershell/powershell-gallery-tls-support/