ADFS Integration Reference Guide

ADFS 3.0 | 4.0

eScribe Software Ltd.
IMPLEMENTATION | REFERENCE GUIDE – VERSION 1.1

Contents

1.0 OVERVIEW:

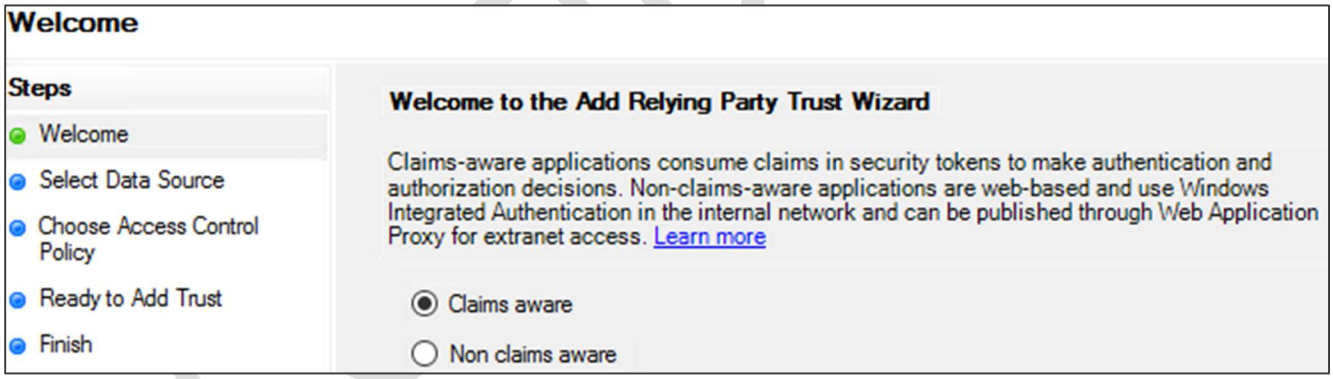
This document is meant to serve only as a reference for generating the information that is required by eScribe for your ADFS integration. After completing this guide, you should be able to fill the requirements in the table set by eScribe located at the end of the document.

2.0 PREREQUISITES:

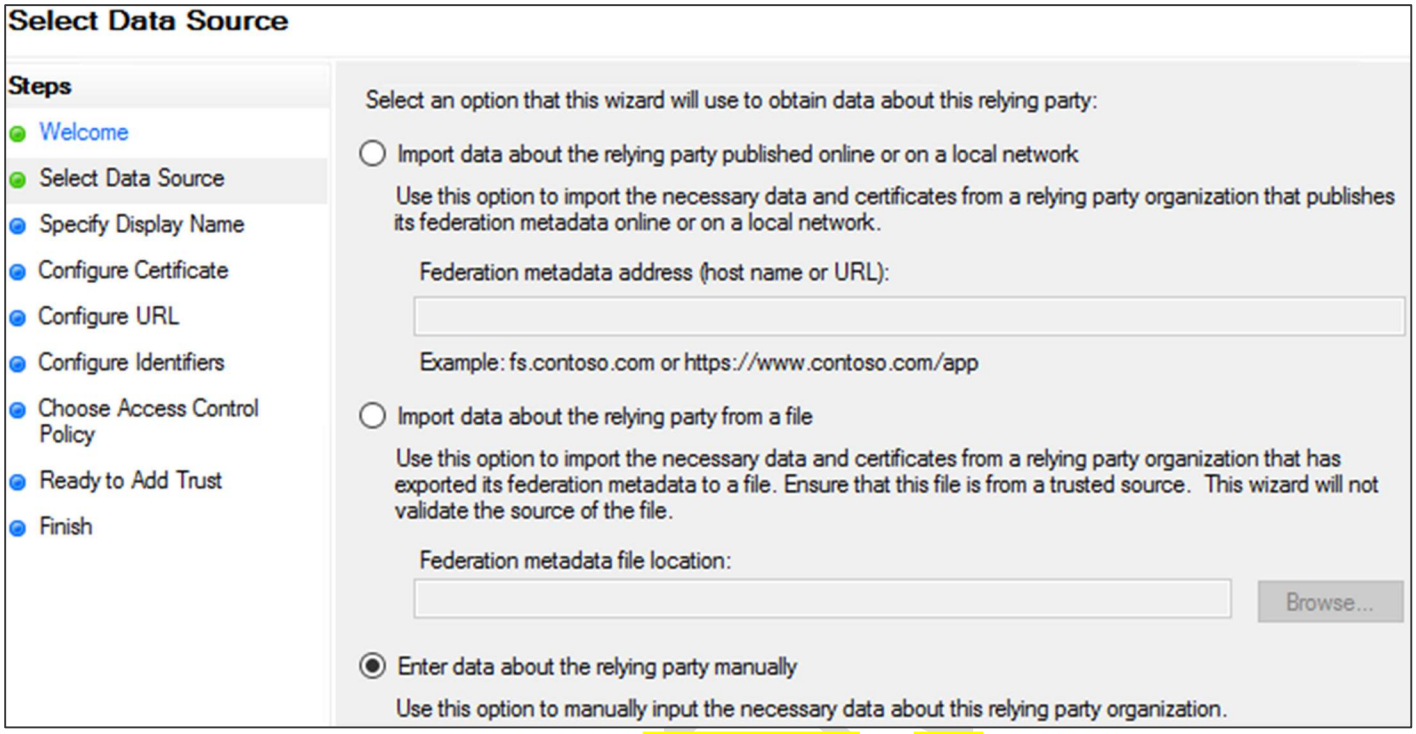
1. You are hosting your ADFS server on one of the following Operating Systems:
   ADFS 3.0 – *Windows Server 2012 R2* | **ADFS 4.0** – *Windows Server 2016*
2. Your ADFS infrastructure is functional and accessible from an external network before proceeding.
3. You have identified your Signin URL:
   https://<yoursubdomain>/adfs/ls/idpinitiatedsignon.htm

3.0 Generate eScribe Relying Party Trust:

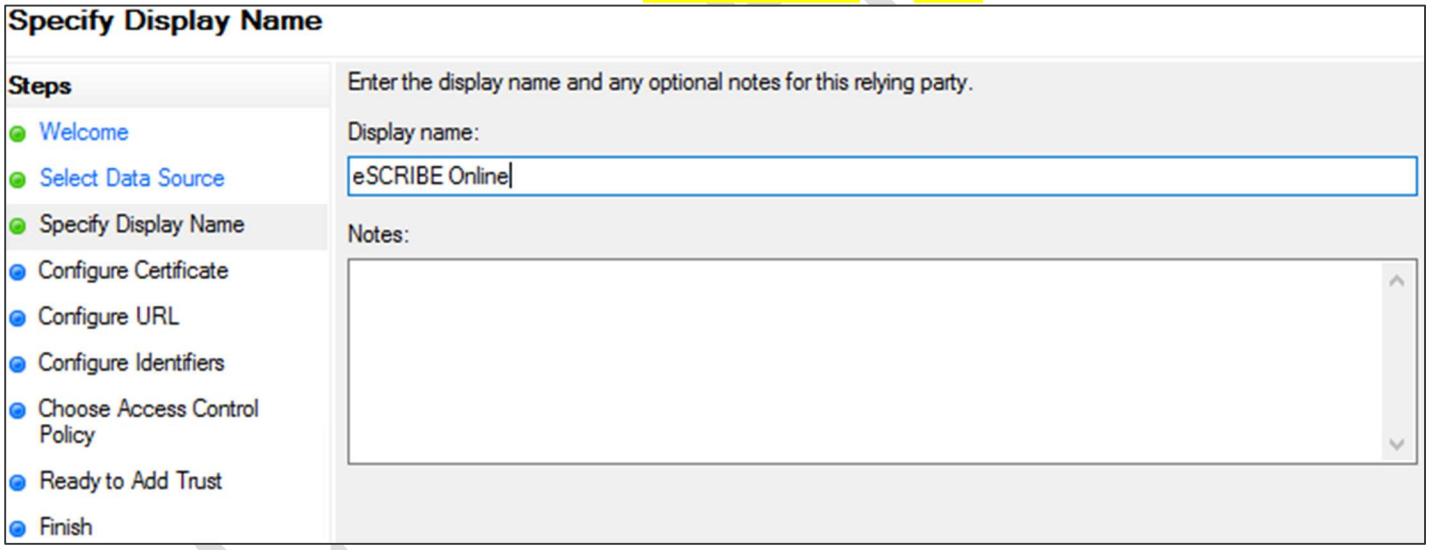
1. Open the "AD FS" Management Console in Server Manager.
2. Expand all categories if necessary and ***Right Click*** "**Relying Party Trusts**" > Then "**Add Relying Party Trust**".
3. The Trust Wizard opens… Select "**Claims aware**". If you are using Windows Server 2012 R2, no selection is required > **Start**



4. On the "Select Data Source" window, select "**Enter data about relying party trust manually**" > "**Next**"

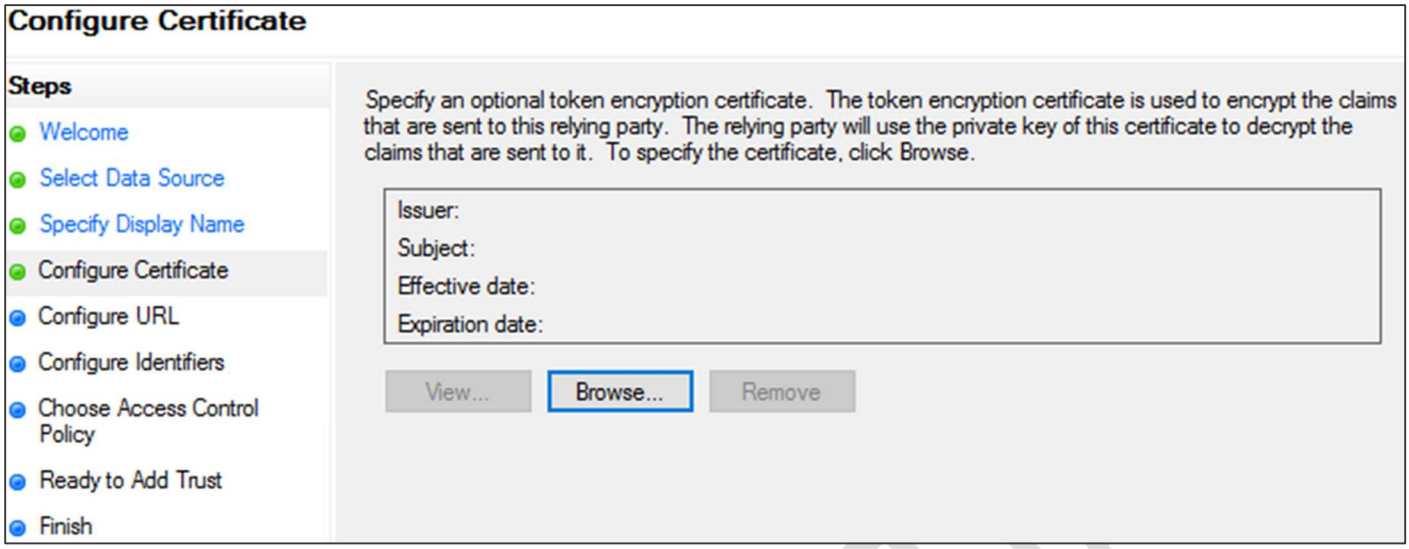


5. Now specify the Display Name to be "**eScribe Online**" > "**Next**"



6. **Choose a Profile** - (2012 R2 OS). This step is not required if you are running Server 2016 as the host.
   a. **If** you are using Windows Server 2012 R2 > Select "**AD FS profile**" > Next

7. Configure Certificate Window – Leave everything as default> "**Next**"



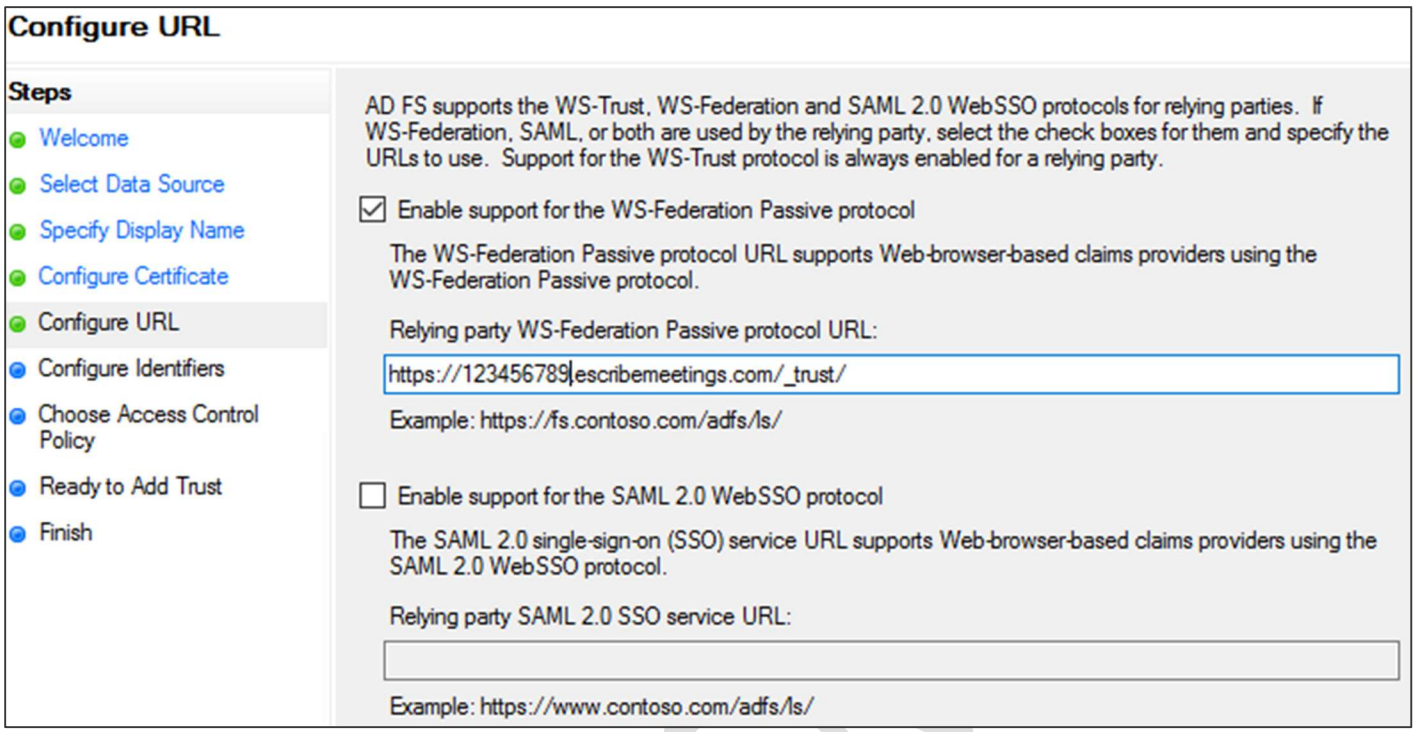
8. Configure URL – Select the box for "**Enable support for the WS-Federation Passive Protocol**". Now, you must enter the "Relying Party WS-Federation Passive Protocol URL" for our domain "eScribemeetings.com".

   Use the below for the Relying Party WS-Federation Passive Protocol URL:
   Replace the numbers in red with your assigned sub domain. This should have been sent by eScribe.
   https://123456789.eScribemeetings.com/_trust/

   If required, please reference the email sent by implementation team to which this document is attached.

   Examples:
   https://northcounty.eScribemeetings.com/_trust/
   https://bluemountain.eScribemeetings.com/_trust/

   After the URL has been created successfully > "**Next**".



9. Configure Identifiers – **Add an addition URL** with the following format:

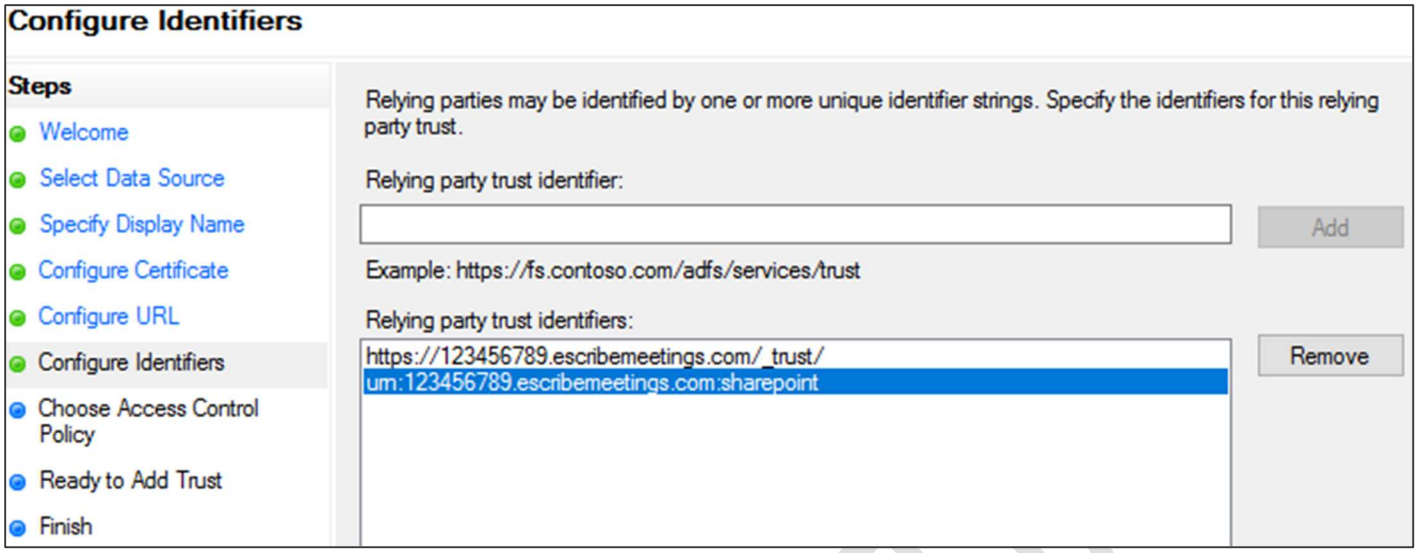
   Replace the numbers in red with your assigned sub domain. This should have been sent by eScribe.
   urn:123456789.eScribemeetings.com:sharepoint

   If required, please reference the email sent by implementation team to which this documents is attached.

   Type the URN in the "**Relying part trust identifier**" box > **ADD**

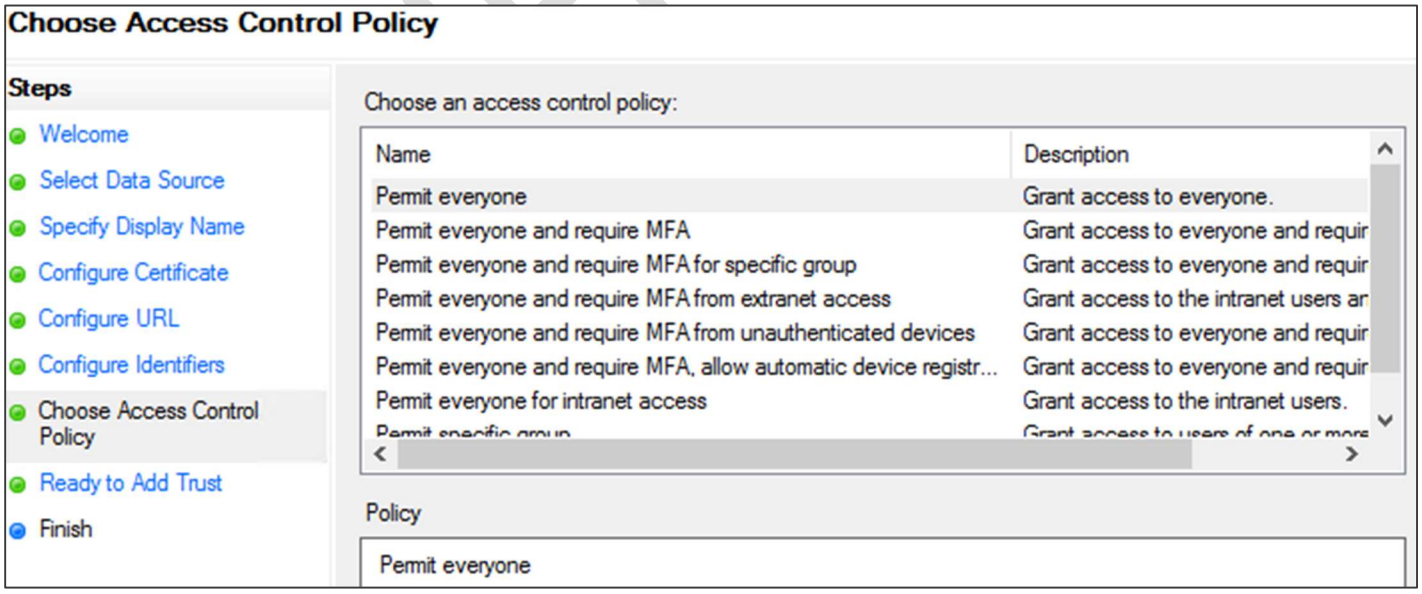
   Examples:
   urn:northcounty.eScribemeetings.com:sharepoint
   urn:bluemountain.eScribemeetings.com:sharepoint

   After the URL has been created successfully > "**Next**".
   The next step may vary based on your Operating System and version of AD FS.

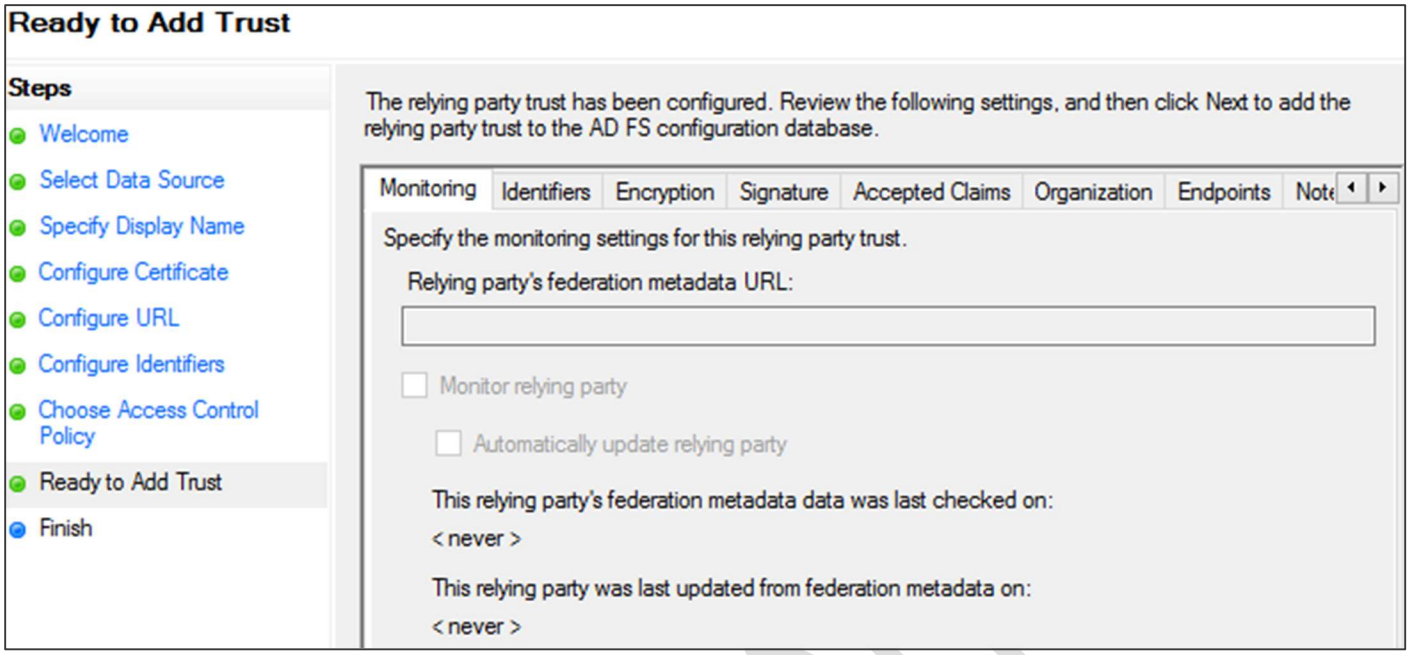


10. If you are using **Server 2012 R2**, you will see a screen to "Configure Multi-factor Authentication Now?". Select "**I do not want to configure Multi-factor authentication settings for this relying party trust at this time**". **Next**

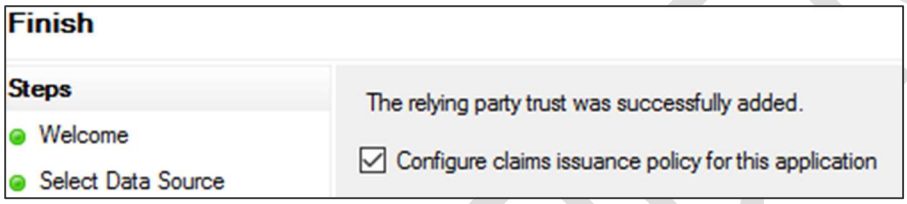
11. "**Choose Access Control Policy**" on 2016 **OR** "**Insuance Authorization Rules**" on Server 2012 R2.
    [2012 R2] - Choose Insuance Authorization Rules: Select "**Permit all users to access this relying party**." **Next**.
    [2016] - **Click Next**.



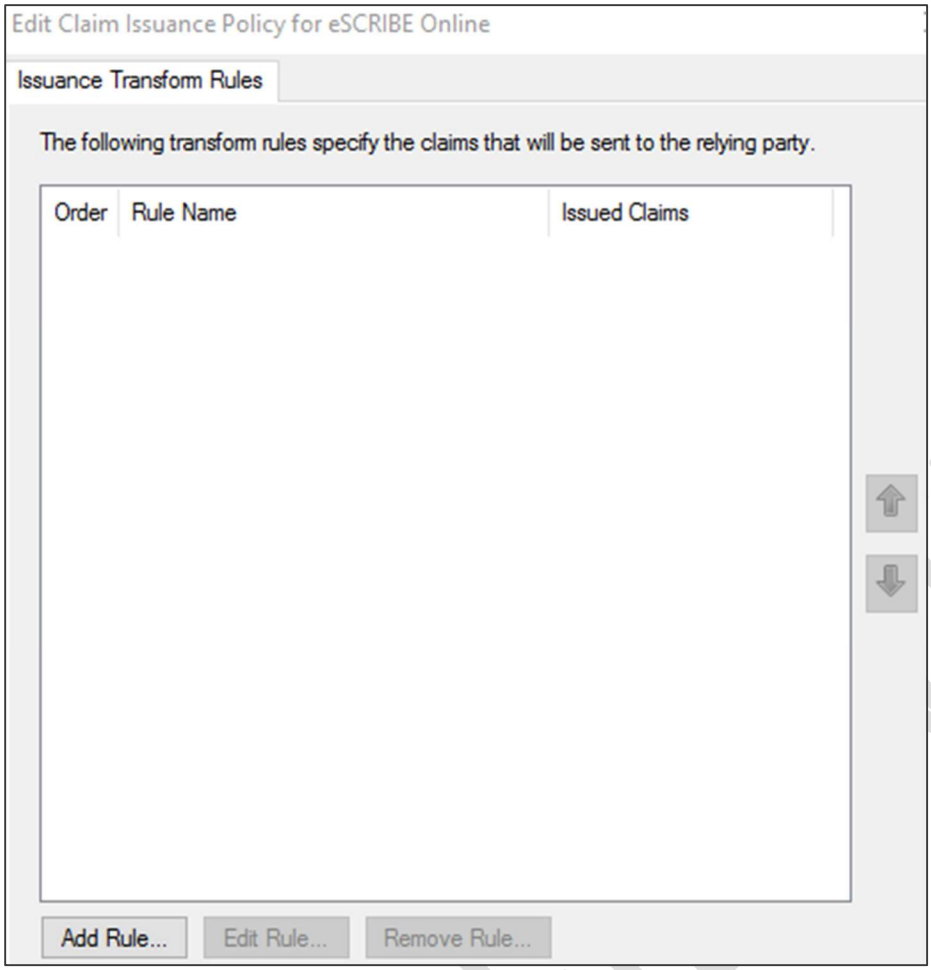
12. Ready to Add Trust – Accept the defaults and click **Next**.



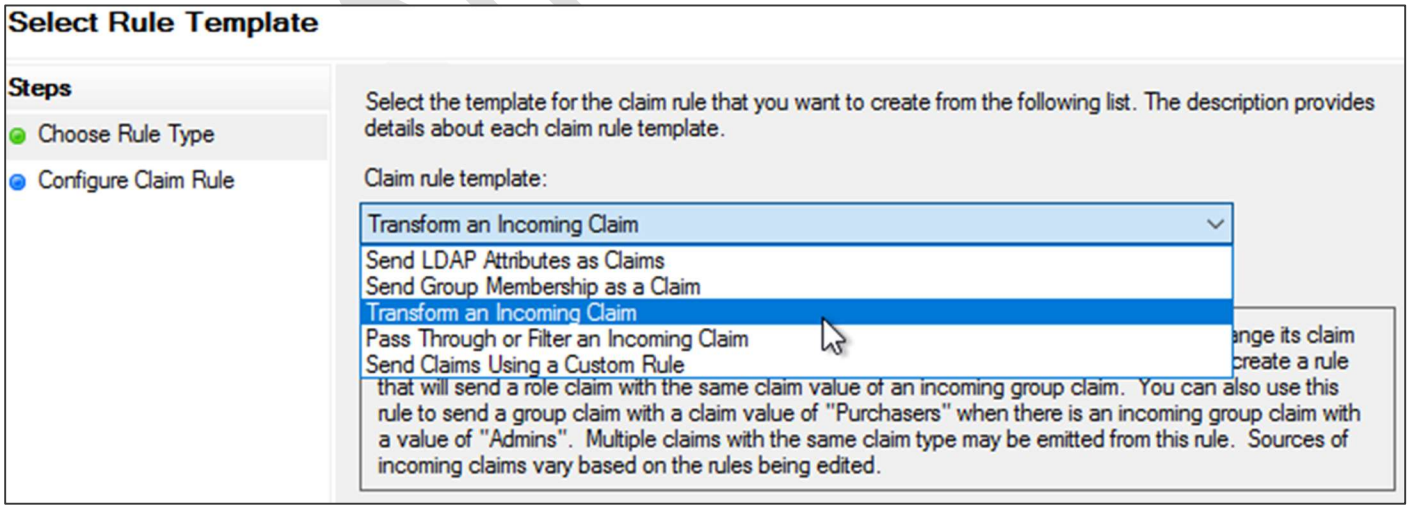
13. Finish – Select the check box and click Close.



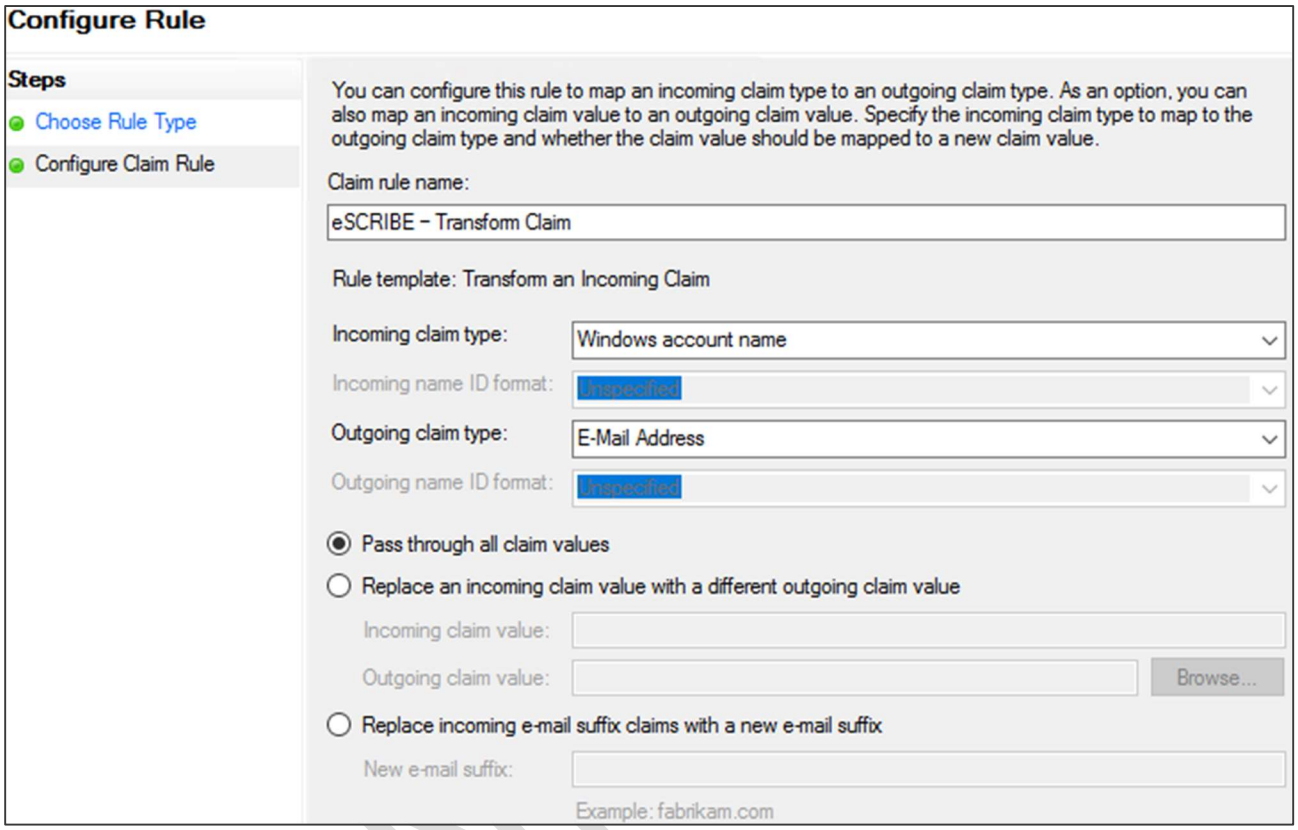
14. Edit Claim Inssuance Policy for eScribe Online > **Add Rule**



15. Select “Transform an Incoming Claim”, click “**Next**”



16. Populate the information as follows:
    Claim rule name: **eScribe – Transform Claim**
    Incoming claim type: **Windows account name**
    Outgoing claim type: **E-Mail Address**
    Pass through all claim values (default)



Finish. Apply Rule. Close.

4.0 ADFS Credential Table for eScribe:

Once the ADFS Relying party setup has been completed, please fill in following information for eScribe:

Please replace everything in red with the proper values.

1	Relying Party Trust URL	https://**123456789**.eScribemeetings.com/_trust/
2	Relying Party Trust URL (URN)	urn:**123456789**.eScribemeetings.com:sharepoint
3	ADFS Sign in URL	https://**Your ADFS Server URL**/adfs/ls/
4	ADFS Token Signing Certificate	ADFS Signing Certificate from your server. Please insert object **HERE**.
5	Exported List of Active ADFS users	Export a list of your ADFS users, including First Name, Last Name, Domain, Username and Email in an Excel spreadsheet. Insert object **HERE**. Example: eSCRIBE - User List Example.xlsx

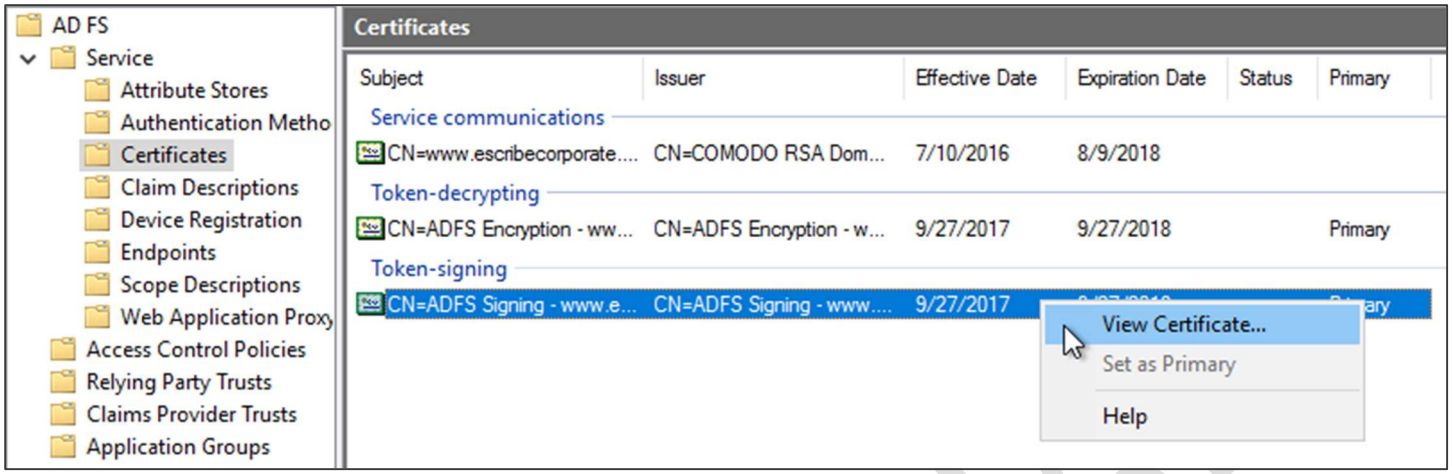
How to get this information? See Below:

4.1 How to get the Relying Party Trust URL and URN:

1. Open AD FS management console > Expand "Relying party trusts" > search for the trust that you have created for eScribe > Open the trust to see the details.
   a. Under the "Indentifier heading", you will find both URL trusts as created in the previous steps.
      i. Populate the first 2 rows of the table above with these values.

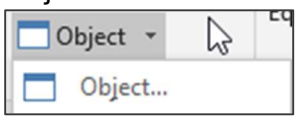
4.2 How to get your ADFS Token Signing Certificate:

1. Open AD FS management console > Expand "Service" > Open "Certificates" > Find the "Token-signing" certificate and right click on it > "View Certificate"



2. Go to Details > Copy to File > The certificate wizard opens > Next > Select the default format which is “DER encoded binary X.509 (.CER)” > Next > Specify a file name > Next > Finish

3. Attach the exported certitificate to row 4 in the above table. In Word, go to “Insert” Tab > Object > Create from file



5.0 Create ADFS Users for eScribe:

!IMPORTANT!
eScribe also requires the following accounts to be created in your AD, so we can test the ADFS integration. We will also use these accounts to perform configurations and testing.

Each account will require a unique email address, and we will need an email, username and password.

Please provide the usernames and passwords in the chart below:

If this chart does not comply with your internal security policy, please specify an alternative way to share this information.

Domain Name	Suggested Username	Password	Email
	eScribeAdministrator		
	eScribeContributor		
	eScribeParticipant		

6.0 ADFS Timeout Configuration

This command is part of the AD FS cmdlets and must be run on the AD FS server.

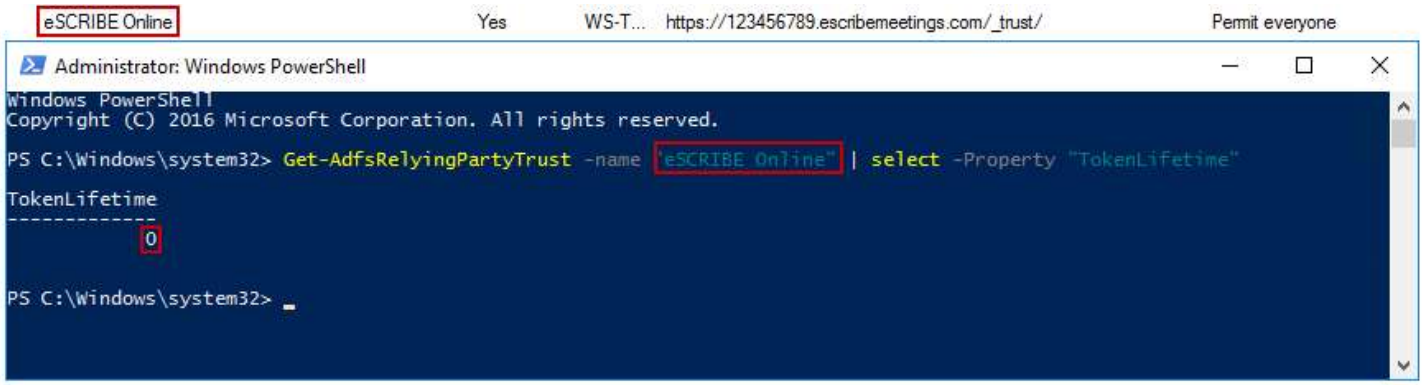
6.1 Check the Current Timeout Value:

Open PowerShell as Administrator and run the below command:

Get-ADFSRelyingPartyTrust -Name "eScribe Online" | Select -Property "TokenLifetime"

^Relying Trust Display Name^

If the value returned by the command is **0**, you will need to increase it. The recommended new value should be 480.

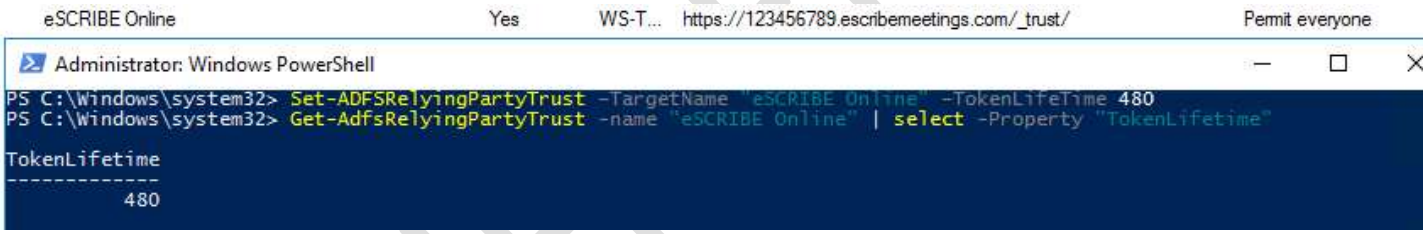


6.2 Update the Current Timeout Value:

Set the new timeout value to be 8 hours with the following command:

Set-ADFSRelyingPartyTrust –TargetName "eScribe Online" –TokenLifeTime 480

^Relying Trust Display Name^



Please review the above settings and align it with your internal security policy.

Reference: https://technet.microsoft.com/en-us/library/gg188586(v=crm.6).aspx

7.0 eScribe Meetings Standard (STD) App and Professional (PRO) App – ADFS Configuration

- STD / PRO applies only to iPad App.

In order for the eScribe Meetings Professional Applications (for Windows or iPad) to be connected with an organizations ADFS, the app must first be registered within the ADFS that will be used. Please complete the following steps, depending on the authentication in use with your eScribe site.

7.1 App registration for ADFS 3.0

For additional information from Microsoft on completing this step please see the following Microsoft link:
https://docs.microsoft.com/en-us/powershell/module/adfs/add-adfsclient?view=win10-ps

Run below command(s) on your ADFS server to Register App(s):

- This can be disabled or removed any time.

For use of iPad PRO app:

Add-ADFSClient -Name "eScribe_App" -ClientId "23A77FA6-6951-4611-AEE3-99F5936E9C85" -RedirectUri "ms-app://s-1-15-2-86627599-1409864723-1704662058-2377925903-3915810655-2336476812-747460542/"

For use of iPad STD app:

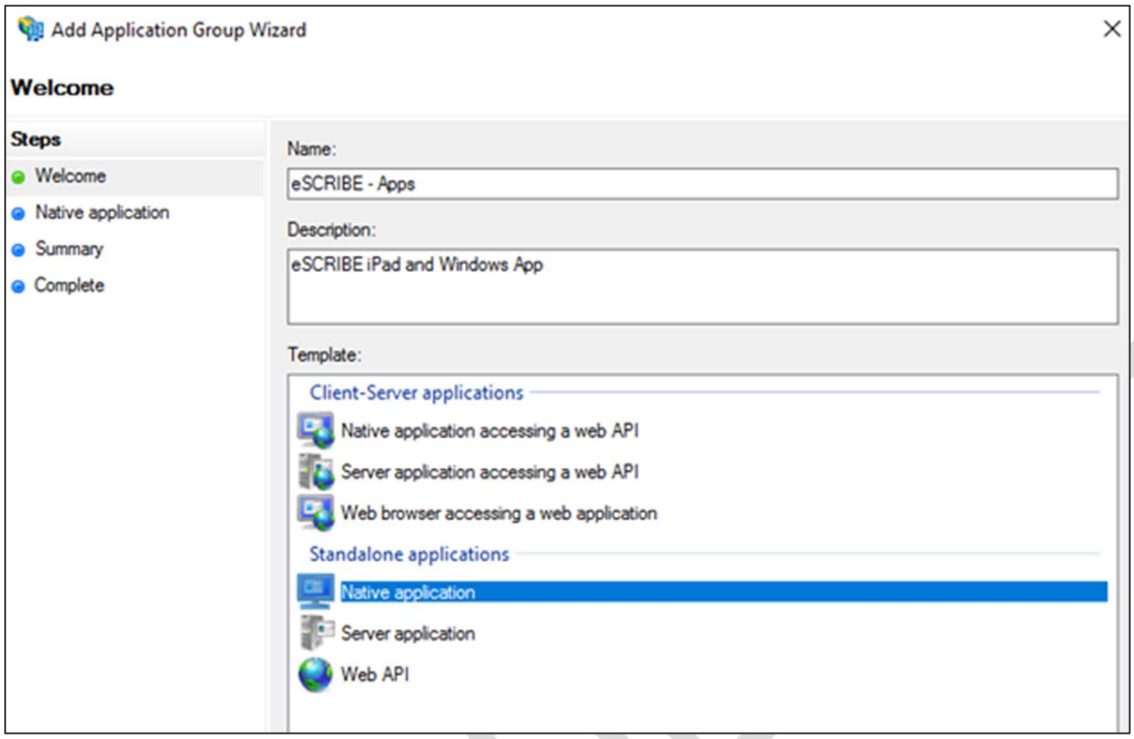
Add-ADFSClient -Name "eScribe_App" -ClientId "519F8D12-84CF-41d0-A7BD-4A1560679BBD" -RedirectUri "ms-app://s-4-16-5-40634344-5435167187-8586191251-4007792947-1579001535-3277149805-580866876/"

For use of Windows 10 app:

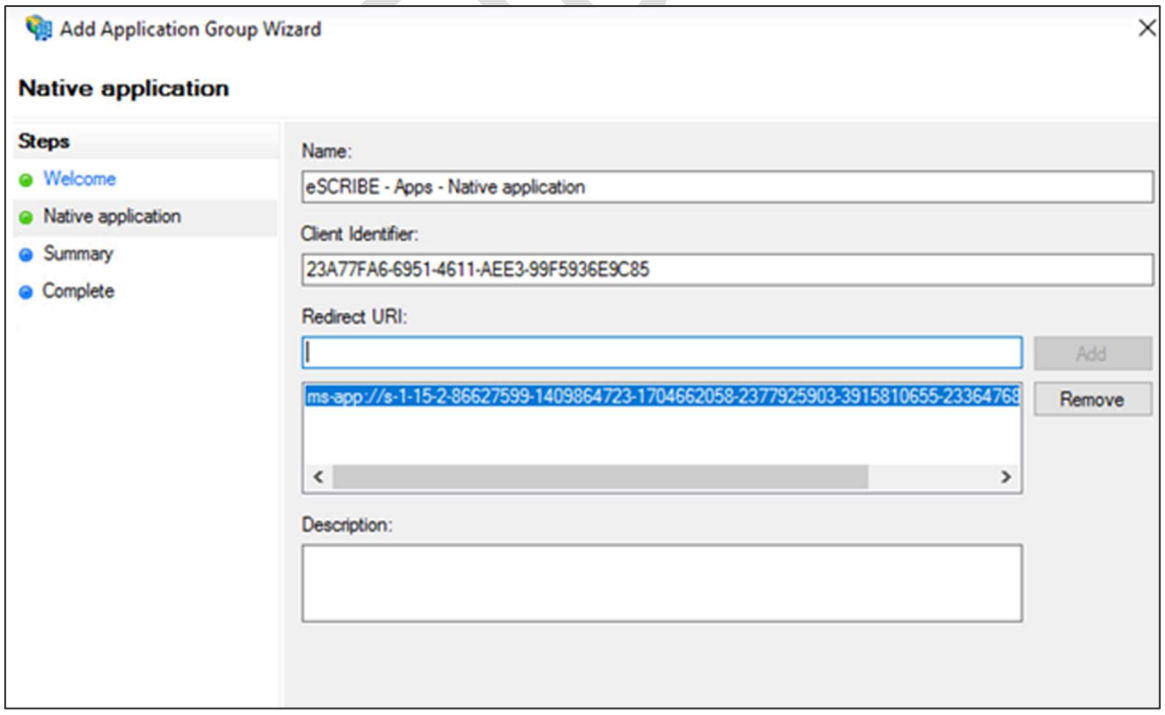
Add-ADFSClient -Name "eScribe_UWP_App" -ClientId "FF71EFF8-11F5-445e-9D31-C8706C48F69D" -RedirectUri "ms-app://S-1-15-2-3585911706-2492430066-1922640115-3814228788-4263615920-112324596-2256370002"

7.2 Add registration for ADFS 4.0

1. Application Groups > Add Application Group



2. Enter any Name and Description
3. Select Standalone applications > Native application > Next



4. Add identifiers for the apps for one or both depending on subscription:

For iPad PRO app:
Enter Client Identifier: 23A77FA6-6951-4611-AEE3-99F5936E9C85
Enter Redirect URI: ms-app://s-1-15-2-86627599-1409864723-1704662058-2377925903-3915810655-2336476812-747460542

For iPad STD app:
Enter Client Identifier: 519F8D12-84CF-41d0-A7BD-4A1560679BBD
Enter Redirect URI: ms-app://s-4-16-5-40634344-5435167187-8586191251-4007792947-1579001535-3277149805-580866876

For Windows 10 app:
Enter Client Identifier: FF71EFF8-11F5-445e-9D31-C8706C48F69D
Enter Redirect URI: ms-app://S-1-15-2-3585911706-2492430066-1922640115-3814228788-4263615920-112324596-2256370002

5. Click Next > Review/Next > Close

Now that the apps are registered, we need to grant the apps permission to use our Relying Party Trust (RPT). Run this command in your ADFS PowerShell:

For iPad PRO app:
Grant-AdfsApplicationPermission -ClientRoleIdentifier "23A77FA6-6951-4611-AEE3-99F5936E9C85" -ServerRoleIdentifier "<RPT identifier provided>"

For iPad STD app:
Grant-AdfsApplicationPermission -ClientRoleIdentifier "519F8D12-84CF-41d0-A7BD-4A1560679BBD" -ServerRoleIdentifier "<RPT identifier provided>"

For Windows 10 app:
Grant-AdfsApplicationPermission -ClientRoleIdentifier "FF71EFF8-11F5-445e-9D31-C8706C48F69D" -ServerRoleIdentifier "<RPT identifier provided>"

Your RPT identifier looks like this: urn:xxxxxxxx.eScribemeetings.com:sharepoint