

ADFS Integration Reference Guide

ADFS 3.0 | 4.0

eScribe Software Ltd.

IMPLEMENTATION | REFERENCE GUIDE – VERSION 1.1

Contents

ADFS Integration Reference Guide.....	0
1.0 OVERVIEW:	2
2.0 PREREQUISITES:.....	2
3.0 Generate eScribe Relying Party Trust:.....	2
4.0 ADFS Credential Table for eScribe:	10
4.1 How to get the Relying Party Trust URL and URN:.....	10
4.2 How to get your ADFS Token Signing Certificate:.....	10
5.0 Create ADFS Users for eScribe:	12
6.0 ADFS Timeout Configuration	12
6.1 Check the Current Timeout Value:.....	12
6.2 Update the Current Timeout Value:.....	13
7.0 eScribe Meetings Standard (STD) App and Professional (PRO) App – ADFS Configuration..	13
7.1 App registration for ADFS 3.0	14
7.2 Add registration for ADFS 4.0.....	15

1.0 OVERVIEW:

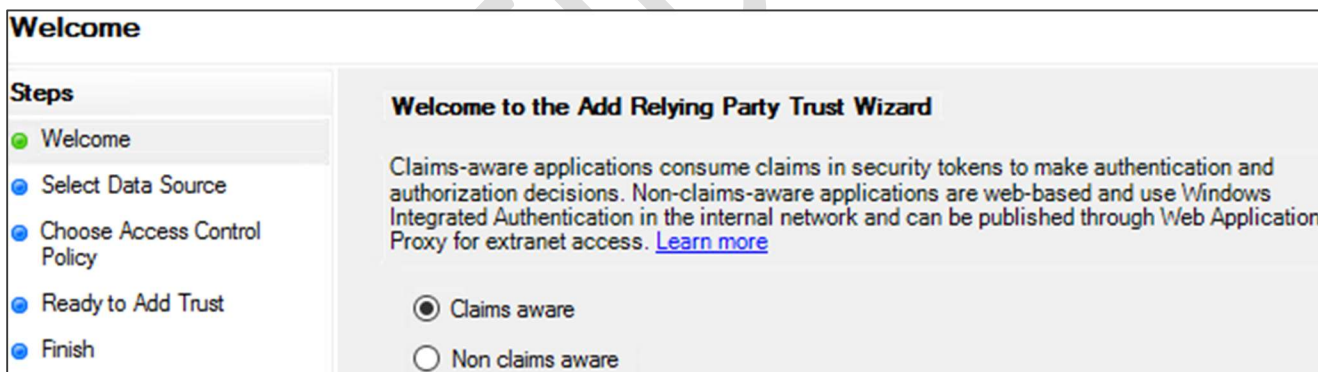
This document is meant to serve only as a reference for generating the information that is required by eScribe for your ADFS integration. After completing this guide, you should be able to fill the requirements in the table set by eScribe located at the end of the document.

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”**

Select Data Source

Steps

- Welcome
- Select Data Source
- Specify Display Name
- Configure Certificate
- Configure URL
- Configure Identifiers
- Choose Access Control Policy
- Ready to Add Trust
- Finish

Select an option that this wizard will use to obtain data about this relying party:

☐ Import data about the relying party published online or on a local network

Use this option to import the necessary data and certificates from a relying party organization that publishes its federation metadata online or on a local network.

Federation metadata address (host name or URL):

Example: fs.contoso.com or https://www.contoso.com/app

☐ Import data about the relying party from a file

Use this option to import the necessary data and certificates from a relying party organization that has exported its federation metadata to a file. Ensure that this file is from a trusted source. This wizard will not validate the source of the file.

Federation metadata file location:

☒ Enter data about the relying party manually

Use this option to manually input the necessary data about this relying party organization.

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

Specify Display Name

Steps

- Welcome
- Select Data Source
- Specify Display Name
- Configure Certificate
- Configure URL
- Configure Identifiers
- Choose Access Control Policy
- Ready to Add Trust
- Finish

Enter the display name and any optional notes for this relying party.

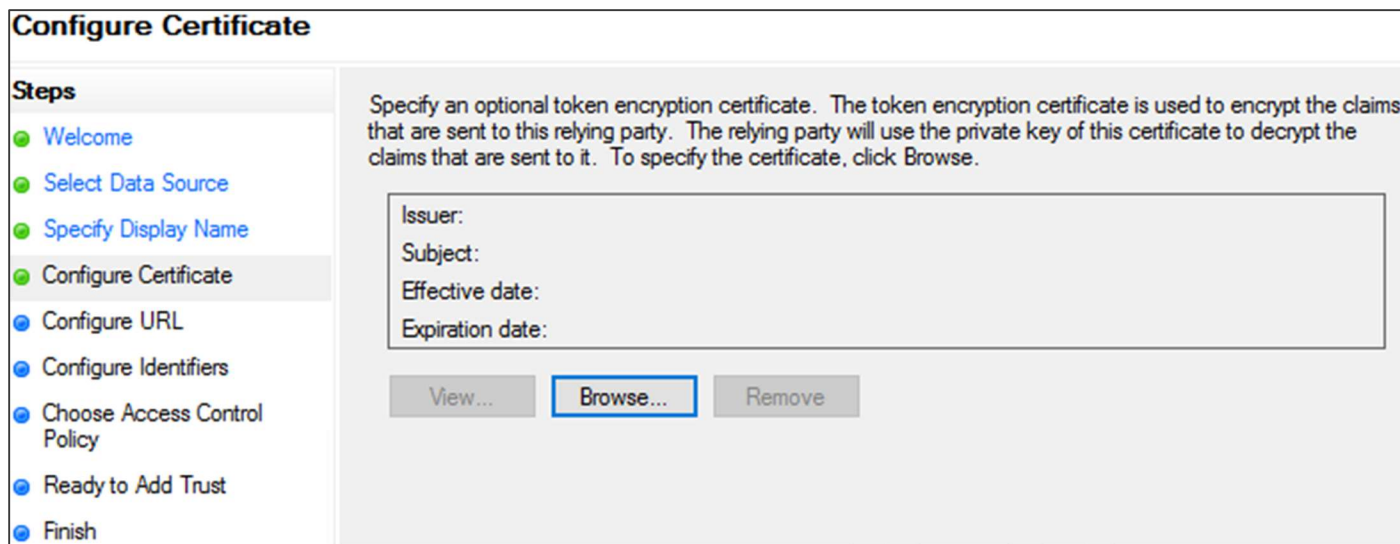
Display name:

Notes:

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**”.

Configure URL

Steps

- Welcome
- Select Data Source
- Specify Display Name
- Configure Certificate
- Configure URL**
- Configure Identifiers
- Choose Access Control Policy
- Ready to Add Trust
- Finish

AD FS supports the WS-Trust, WS-Federation and SAML 2.0 WebSSO protocols for relying parties. If WS-Federation, SAML, or both are used by the relying party, select the check boxes for them and specify the URLs to use. Support for the WS-Trust protocol is always enabled for a relying party.

☒ Enable support for the WS-Federation Passive protocol

The WS-Federation Passive protocol URL supports Web-browser-based claims providers using the WS-Federation Passive protocol.

Relying party WS-Federation Passive protocol URL:

Example: https://fs.contoso.com/adfs/ls/

☐ Enable support for the SAML 2.0 WebSSO protocol

The SAML 2.0 single-sign-on (SSO) service URL supports Web-browser-based claims providers using the SAML 2.0 WebSSO protocol.

Relying party SAML 2.0 SSO service URL:

Example: https://www.contoso.com/adfs/ls/

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.

Configure Identifiers

Steps

- Welcome
- Select Data Source
- Specify Display Name
- Configure Certificate
- Configure URL
- Configure Identifiers
- Choose Access Control Policy
- Ready to Add Trust
- Finish

Relying parties may be identified by one or more unique identifier strings. Specify the identifiers for this relying party trust.

Relying party trust identifier:

Example: https://fs.contoso.com/adfs/services/trust

Relying party trust identifiers:

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

Choose Access Control Policy

Steps

- Welcome
- Select Data Source
- Specify Display Name
- Configure Certificate
- Configure URL
- Configure Identifiers
- Choose Access Control Policy
- Ready to Add Trust
- Finish

Choose an access control policy:

Name	Description
Permit everyone	Grant access to everyone.
Permit everyone and require MFA	Grant access to everyone and require MFA.
Permit everyone and require MFA for specific group	Grant access to everyone and require MFA for specific group.
Permit everyone and require MFA from extranet access	Grant access to the intranet users and require MFA from extranet access.
Permit everyone and require MFA from unauthenticated devices	Grant access to everyone and require MFA from unauthenticated devices.
Permit everyone and require MFA, allow automatic device registration	Grant access to everyone and require MFA, allow automatic device registration.
Permit everyone for intranet access	Grant access to the intranet users.
Permit specific group	Grant access to users of one or more groups.

Policy

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

Ready to Add Trust

Steps

- Welcome
- Select Data Source
- Specify Display Name
- Configure Certificate
- Configure URL
- Configure Identifiers
- Choose Access Control Policy
- Ready to Add Trust**
- Finish

The relying party trust has been configured. Review the following settings, and then click Next to add the relying party trust to the AD FS configuration database.

Monitoring Identifiers Encryption Signature Accepted Claims Organization Endpoints Notes

Specify the monitoring settings for this relying party trust.

Relying party's federation metadata URL:

☐ Monitor relying party

☐ Automatically update relying party

This relying party's federation metadata data was last checked on:

< never >

This relying party was last updated from federation metadata on:

< never >

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

Finish

Steps

- Welcome
- Select Data Source

The relying party trust was successfully added.

☒ Configure claims issuance policy for this application

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

Edit Claim Issuance Policy for eSCRIBE Online

Issuance Transform Rules

The following transform rules specify the claims that will be sent to the relying party.

Order	Rule Name	Issued Claims
-------	-----------	---------------

15. Select "Transform an Incoming Claim", click **Next**

Select Rule Template

Steps

- Choose Rule Type
- Configure Claim Rule**

Select the template for the claim rule that you want to create from the following list. The description provides details about each claim rule template.

Claim rule template:

Transform an Incoming Claim

Send LDAP Attributes as Claims
Send Group Membership as a Claim
Transform an Incoming Claim
Pass Through or Filter an Incoming Claim
Send Claims Using a Custom Rule

that will send a role claim with the same claim value of an incoming group claim. You can also use this rule to send a group claim with a claim value of "Purchasers" when there is an incoming group claim with a value of "Admins". Multiple claims with the same claim type may be emitted from this rule. Sources of incoming claims vary based on the rules being edited.

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)

Configure Rule

Steps

- Choose Rule Type
- Configure Claim Rule

You can configure this rule to map an incoming claim type to an outgoing claim type. As an option, you can also map an incoming claim value to an outgoing claim value. Specify the incoming claim type to map to the outgoing claim type and whether the claim value should be mapped to a new claim value.

Claim rule name:

Rule template: Transform an Incoming Claim

Incoming claim type:

Incoming name ID format:

Outgoing claim type:

Outgoing name ID format:

☒ Pass through all claim values

☐ Replace an incoming claim value with a different outgoing claim value

Incoming claim value:

Outgoing claim value:

☐ Replace incoming e-mail suffix claims with a new e-mail suffix

New e-mail suffix:

Example: fabrikam.com

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

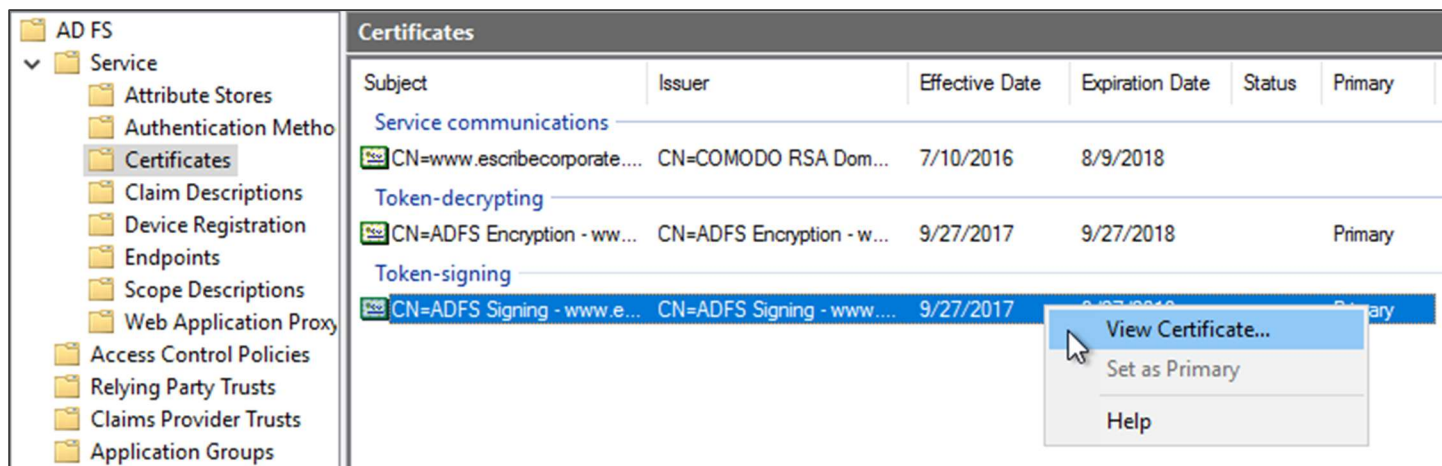
How to get this information? See Below:

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 "Identifier 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.

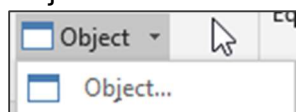
4.2 How to get your ADFS Token Signing Certificate:

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



Subject	Issuer	Effective Date	Expiration Date	Status	Primary
Service communications					
CN=www.escribecorporate....	CN=COMODO RSA Dom...	7/10/2016	8/9/2018		
Token-decrypting					
CN=ADFS Encryption - ww...	CN=ADFS Encryption - w...	9/27/2017	9/27/2018		Primary
Token-signing					
CN=ADFS Signing - www.e...	CN=ADFS Signing - www....	9/27/2017	9/27/2018		Primary

- 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
- Attach the exported certificate 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
	<i>eScribeAdministrator</i>		
	<i>eScribeContributor</i>		
	<i>eScribeParticipant</i>		

6.0 ADFS Timeout Configuration

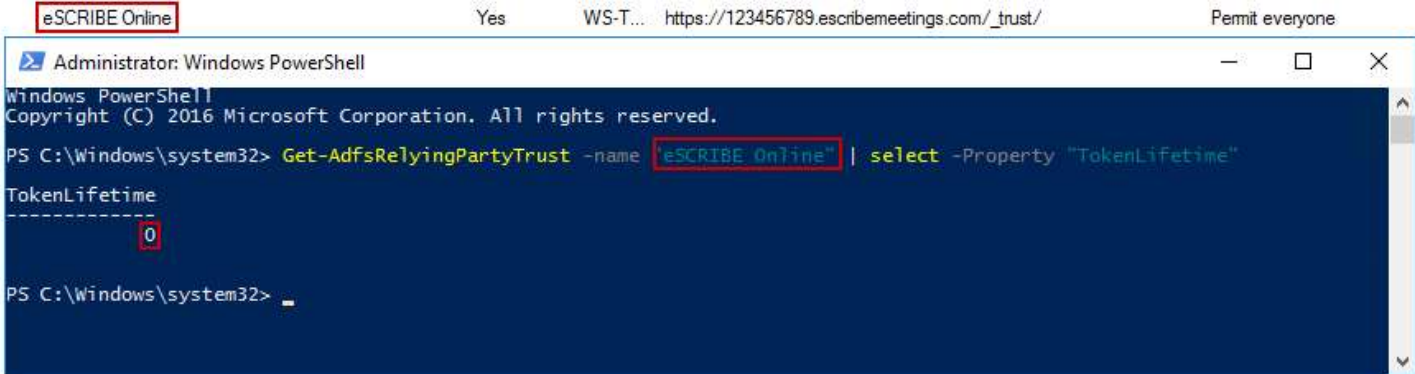
This command is part of the AD FS cmdlets and must be run on the AD FS server.

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.



```

eSCRIBE Online Yes WS-T... https://123456789.escribemeetings.com/_trust/ Permit everyone
Administrator: Windows PowerShell
Windows PowerShell
Copyright (C) 2016 Microsoft Corporation. All rights reserved.

PS C:\Windows\system32> Get-AdfsRelyingPartyTrust -name "eSCRIBE Online" | select -Property "TokenLifetime"

TokenLifetime
-----
0

PS C:\Windows\system32>

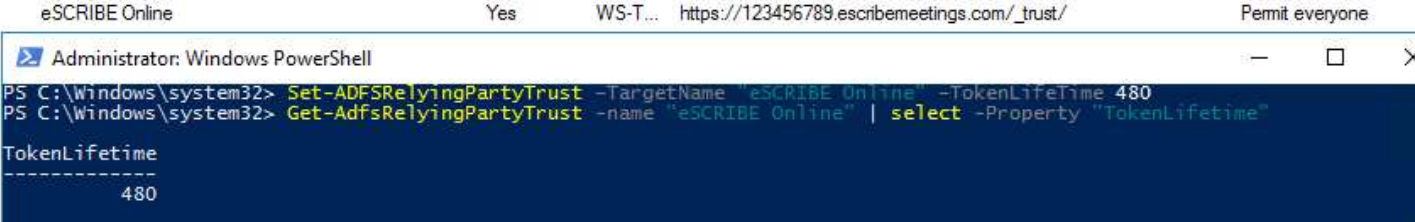
```

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^



```

eSCRIBE Online Yes WS-T... https://123456789.escribemeetings.com/_trust/ Permit everyone
Administrator: Windows PowerShell
PS C:\Windows\system32> Set-ADFSRelyingPartyTrust -TargetName "eSCRIBE Online" -TokenLifeTime 480
PS C:\Windows\system32> Get-AdfsRelyingPartyTrust -name "eSCRIBE Online" | select -Property "TokenLifetime"

TokenLifetime
-----
480

```

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](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:

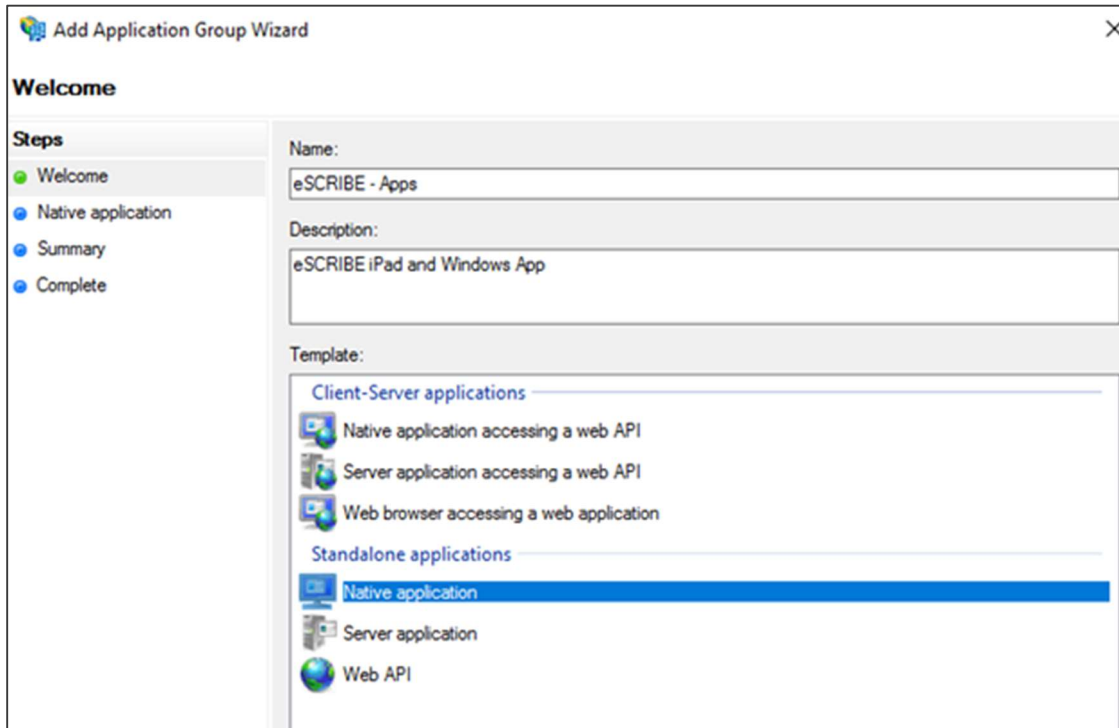
```
Add-ADFSClient -Name "eScribe_App" -ClientId "519F8D12-84CF-41d0-A7BD-4A1560679BBD" -  
RedirectUri "ms-app://s-4-16-5-40634344-5435167187-8586191251-4007792947-1579001535-  
3277149805-580866876/"
```

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



Add Application Group Wizard

Welcome

Steps

- Welcome
- Native application
- Summary
- Complete

Name:
eSCRIBE - Apps

Description:
eSCRIBE iPad and Windows App

Template:

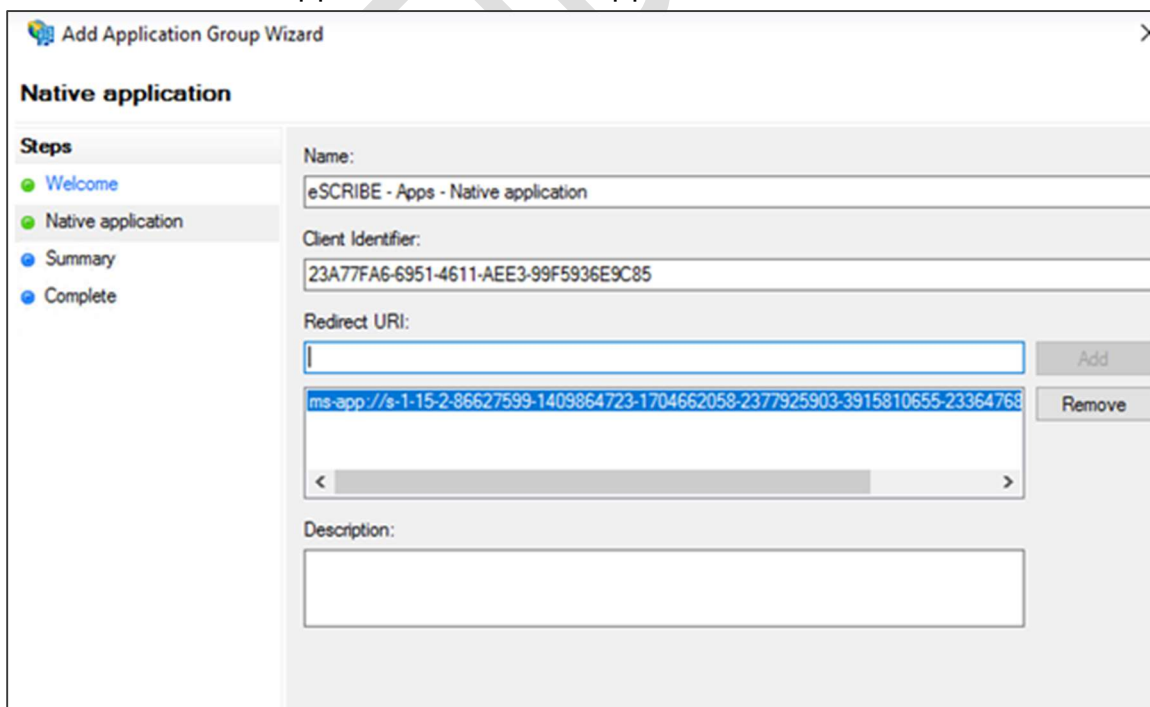
Client-Server applications

- Native application accessing a web API
- Server application accessing a web API
- Web browser accessing a web application

Standalone applications

- Native application**
- Server application
- Web API

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



Add Application Group Wizard

Native application

Steps

- Welcome
- Native application
- Summary
- Complete

Name:
eSCRIBE - Apps - Native application

Client Identifier:
23A77FA6-6951-4611-AEE3-99F5936E9C85

Redirect URI:

Description:

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:xxxxxxx.eScribemeetings.com:sharepoint