Add-On Products

Resource Central

External Authentication Configuration Guide

Version: 1.9

Add-On Products
Roms Hule 8 – 7100 Vejle – Denmark
Phone: +45 7944 7000 Fax: +45 7944 7001

Mail: info@add-on.com
Internet: www.add-on.com

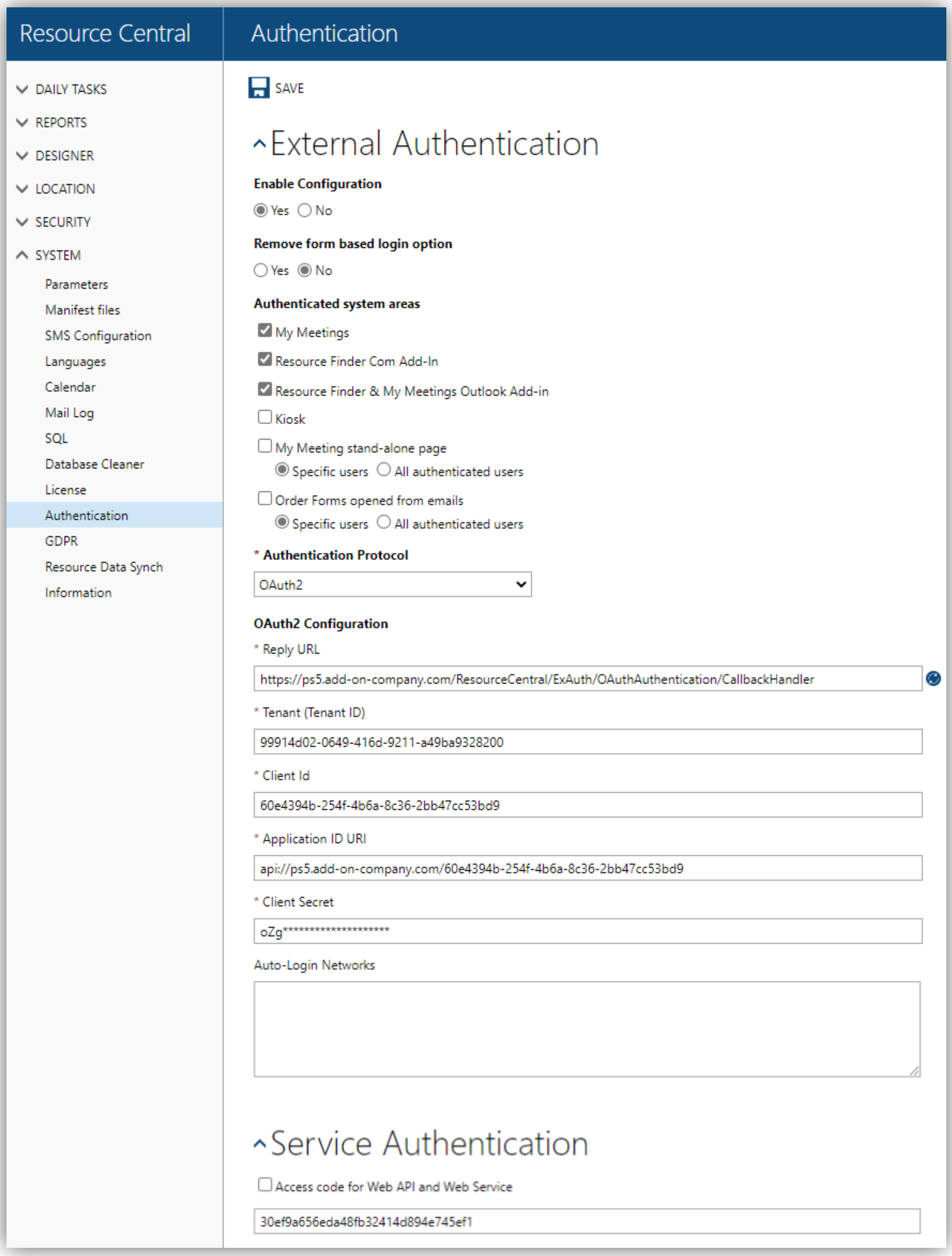
Table of contents

Foreword

External authentication is a new function in Resource Central (RC) that allows you to make configuration for supporting login using Microsoft account. This requires some fields to be filled up with specific data in Resource Central backend.

External authentication currently covers the following Resource Central features

- ResourceFinder and MyMeetings
- Resource Central Notification E-mails
- Resource Central Backend
- Kiosk screens
- MyMeeting stand-alone page



External Authentication

Enable Configuration

● Yes ○ No

Remove form based login option

○ Yes ● No

Authenticated system areas

☑ My Meetings

☑ Resource Finder Com Add-In

☑ Resource Finder & My Meetings Outlook Add-in

☐ Kiosk

☐ My Meeting stand-alone page

● Specific users ○ All authenticated users

☐ Order Forms opened from emails

● Specific users ○ All authenticated users

* **Authentication Protocol**

OAuth2

OAuth2 Configuration

* Reply URL

https://ps5.add-on-company.com/ResourceCentral/ExAuth/OAuthAuthentication/CallbackHandler

* Tenant (Tenant ID)

99914d02-0649-416d-9211-a49ba9328200

* Client Id

60e4394b-254f-4b6a-8c36-2bb47cc53bd9

* Application ID URI

api://ps5.add-on-company.com/60e4394b-254f-4b6a-8c36-2bb47cc53bd9

* Client Secret

oZg********************

Auto-Login Networks

Service Authentication

☐ Access code for Web API and Web Service

30ef9a656eda48fb32414d894e745ef1

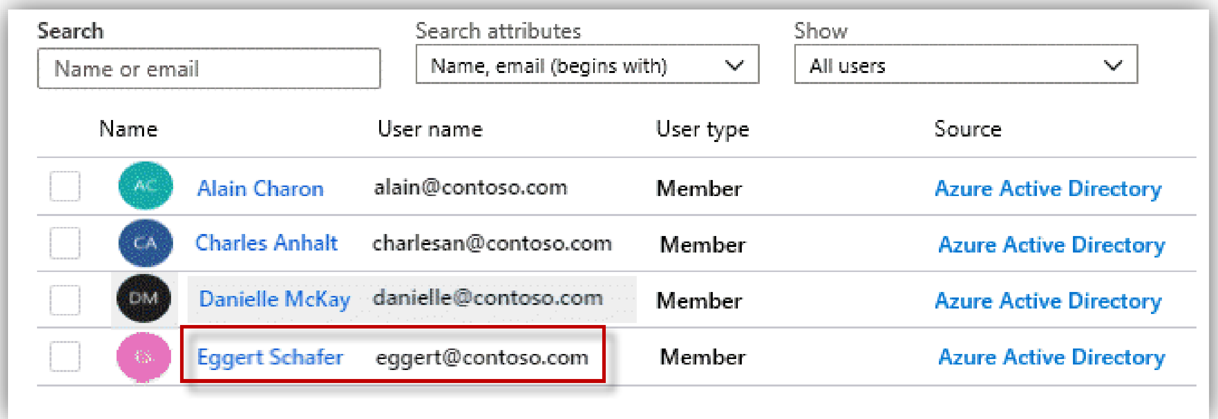
Figure 1. External Authentication in Resource Central

Option	Description

Enable Configuration	Select **Yes** to allow other fields to be configured. Select No will make other fields unavailable.
Remove form based login option	Select **Yes** to allow logging in using Single Sign-On only. NOTE: Selecting **No** for this option while SSO is not fully configured will leave the application inaccessible. It is important that the applied SSO is validated before this option is enabled.

Each Authentication Protocol requires specific data fields to be filled in. This document is designed to give you detailed instructions to retrieve those details.

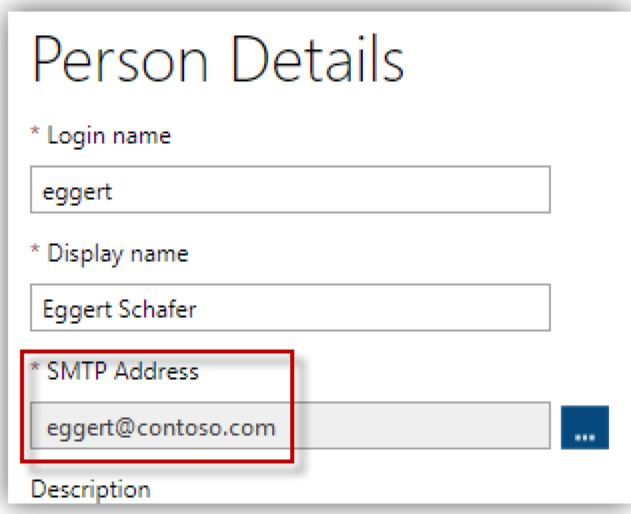
NOTE: The account used in Azure must be associated with a person in RC system via SMTP address:



Search: Name or email
Search attributes: Name, email (begins with)
Show: All users

Name	User name	User type	Source
Alain Charon	alain@contoso.com	Member	Azure Active Directory
Charles Anhalt	charlesan@contoso.com	Member	Azure Active Directory
Danielle McKay	danielle@contoso.com	Member	Azure Active Directory
Eggert Schafer	eggert@contoso.com	Member	Azure Active Directory

Figure 2. All users in Azure



Person Details

* Login name: eggert

* Display name: Eggert Schafer

* SMTP Address: eggert@contoso.com

Description

Figure 3. Person details in RC

System Requirements

Look at the following table for supported Windows Server versions and ADFS versions supported on these servers:

Supported Windows Server	Supported ADFS

Windows Server 2016	ADFS 4.0
Windows Server 2019	ADFS 5.0

NOTE: For the Outlook Add-in to run with Single Sign On it is from Resource Central Hotfix 8 needed to use the latest manifest version 1.10.0.

Affected areas

Look at the following table for further explanation:

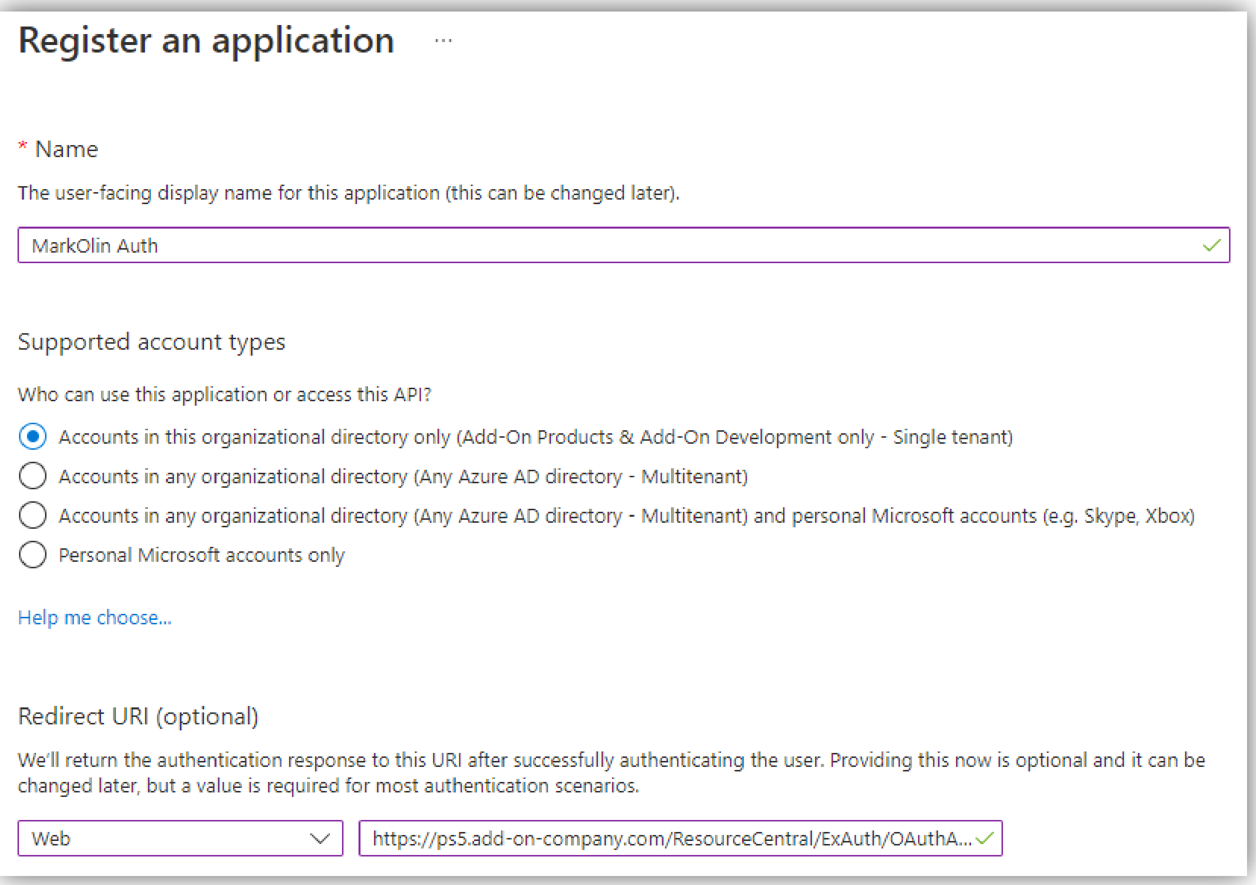
	Specific users	**All authenticated users**
My Meetings stand-alone page	Only organizer can log into their own *My Meetings stand-alone page*	Use any account (that exists in the domain, no need to exist in RC/Persons) to access *My Meetings stand-alone page* of any organizer
Order forms opened from emails	Only service provider / SDA can log into their own Order Form	Use any account (that exists in the domain, no need to exist in RC/Persons) to access Order Form of any user.

Authentication Details for OAuth2/Open ID Connect

Part A. Register application in Azure AD

1. Go to **Azure portal ➔ Azure Active Directory ➔ App registrations**, and click [**New registration**].

2. Fill in application details:
   a. **Name**: enter application name.
   b. **Supported account types**: select *'Accounts in this organizational directory only (… only – Single tenant'*.
   c. **Redirect URI (optional)**: select **Web** platform, then enter **Reply URL** generated in **RC backend ➔ System ➔ Authentication**. (This Reply URL is automatically created when you select an 'Authentication Protocol')



Register an application ···

* Name

The user-facing display name for this application (this can be changed later).

MarkOlin Auth ✓

Supported account types

Who can use this application or access this API?

● Accounts in this organizational directory only (Add-On Products & Add-On Development only - Single tenant)
○ Accounts in any organizational directory (Any Azure AD directory - Multitenant)
○ Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)
○ Personal Microsoft accounts only

Help me choose...

Redirect URI (optional)

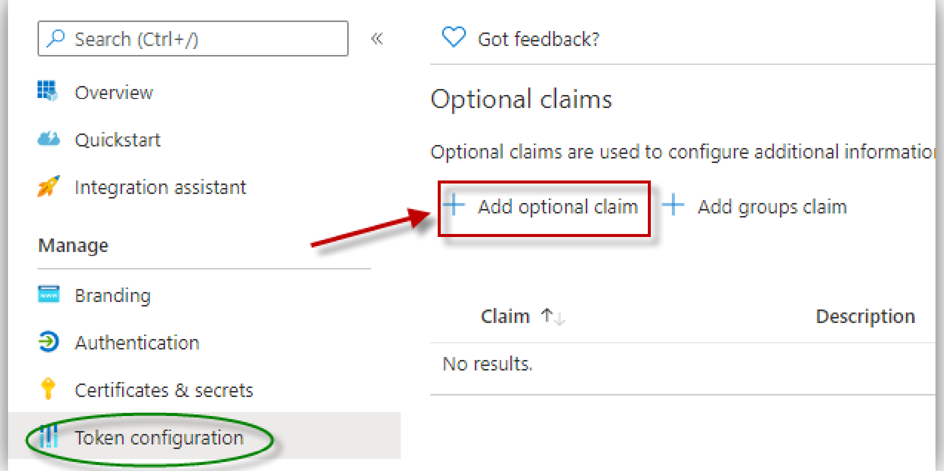
We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Web | https://ps5.add-on-company.com/ResourceCentral/ExAuth/OAuthA... ✓

3. Click [**Register**] button at the bottom of the screen.

NOTE: For **Open ID Connect** Authentication protocol, these additional steps below need to be implemented:

4. On the created app’s screen, open **Token configuration** and click [**Add optional claim**] button:

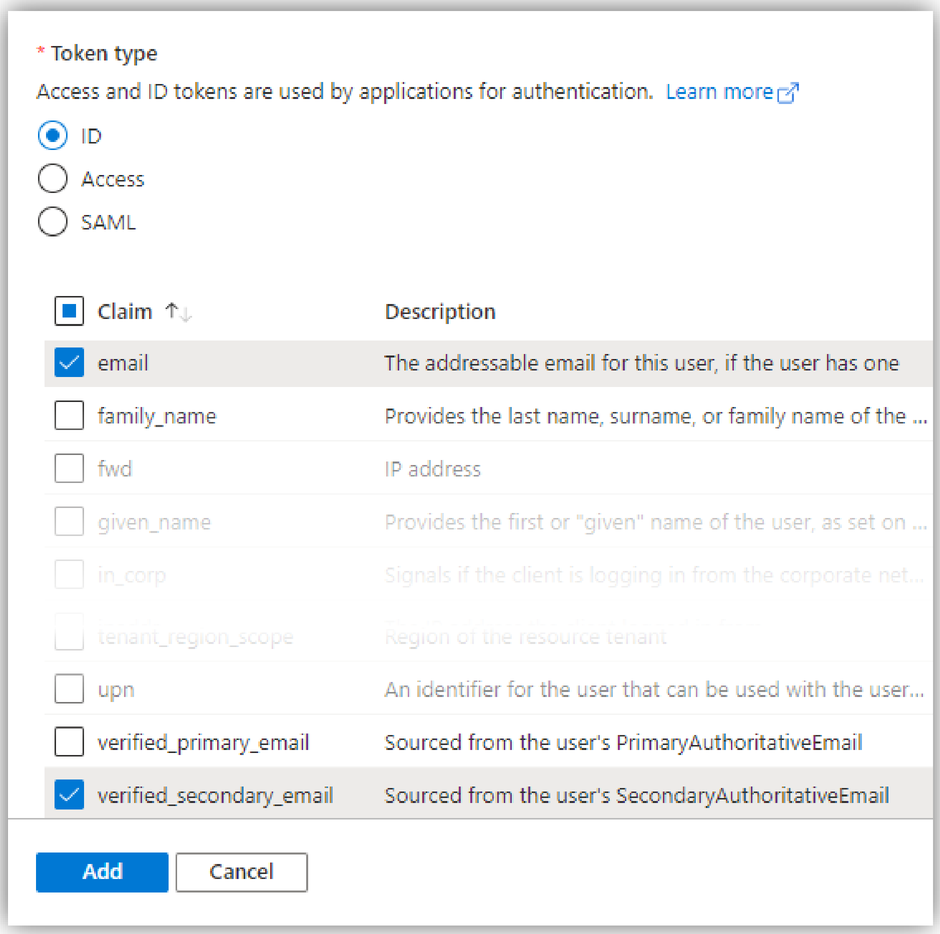


Optional claims

Optional claims are used to configure additional informatio

Claim ↑↓	Description
No results.	

5. Select **ID** for **Token type**, then check on **email** and **verified_secondary_email** as shown in the following figure:



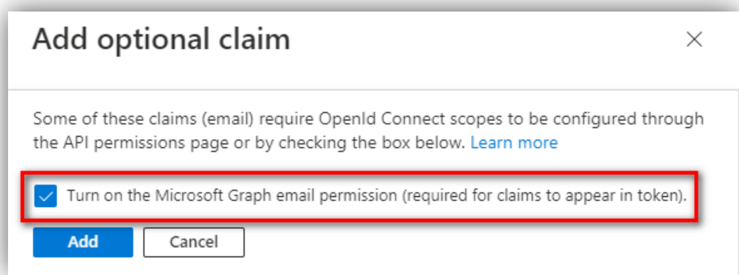
* Token type

Access and ID tokens are used by applications for authentication. Learn more

● ID
○ Access
○ SAML

■ Claim ↑↓	Description
☑ email	The addressable email for this user, if the user has one
□ family_name	Provides the last name, surname, or family name of the ...
□ fwd	IP address
□ given_name	Provides the first or "given" name of the user, as set on ...
□ in_corp	Signals if the client is logging in from the corporate net...
□ tenant_region_scope	Region of the resource tenant
□ upn	An identifier for the user that can be used with the user...
□ verified_primary_email	Sourced from the user's PrimaryAuthoritativeEmail
☑ verified_secondary_email	Sourced from the user's SecondaryAuthoritativeEmail

6. Click [**Add**] and the following message shows up.



Add optional claim

Some of these claims (email) require OpenId Connect scopes to be configured through the API permissions page or by checking the box below. Learn more

☑ Turn on the Microsoft Graph email permission (required for claims to appear in token).

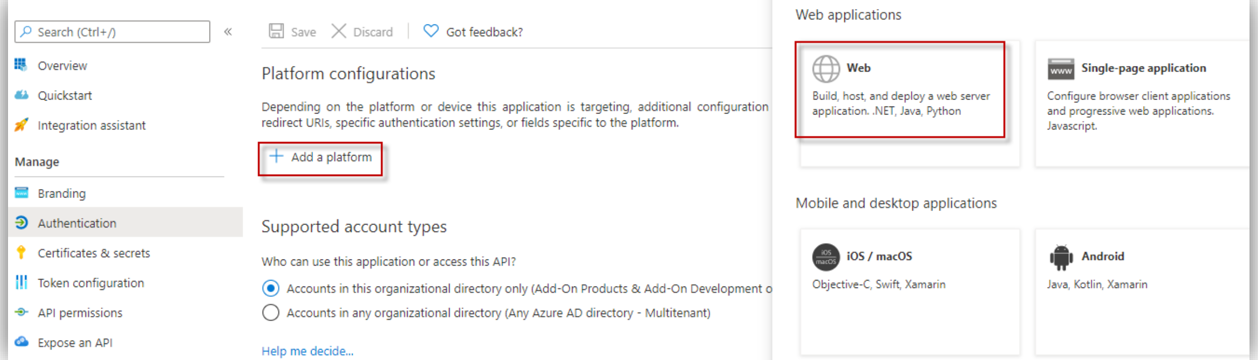
7. Check on the tick box *'Turn on the Microsoft Graph email permission'*, then click [**Add**] button to finish.

Part B. Retrieve details for OAuth2/Open ID Connect Authentication Protocol

Reply URL

NOTE: You can skip this step if you have already set **Redirect URI** back in step 2 of Part A. Register application in Azure AD.

Go to **Azure portal ➔ Azure Active Directory ➔ App registrations.** Click [**All applications**] then select the app that you registered in Part A to see its details.



Platform configurations

Depending on the platform or device this application is targeting, additional configuration redirect URIs, specific authentication settings, or fields specific to the platform.

Supported account types

Who can use this application or access this API?

● Accounts in this organizational directory only (Add-On Products & Add-On Development o

○ Accounts in any organizational directory (Any Azure AD directory - Multitenant)

Web applications

Web Build, host, and deploy a web server application. .NET, Java, Python

Single-page application Configure browser client applications and progressive web applications. Javascript.

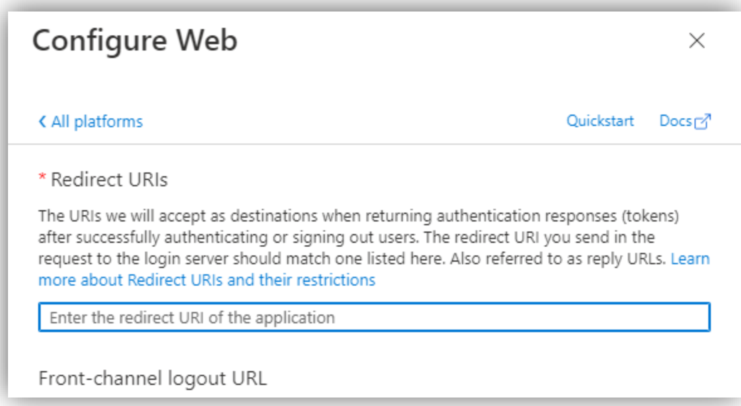
Mobile and desktop applications

iOS / macOS Objective-C, Swift, Xamarin

Android Java, Kotlin, Xamarin

Figure 4. Registered app

Click [**Authentication**] as in the above figure, click [**Add a platform**], select [**Web**] on the right panel of the screen. The following dialog shows up:



Configure Web

* Redirect URIs

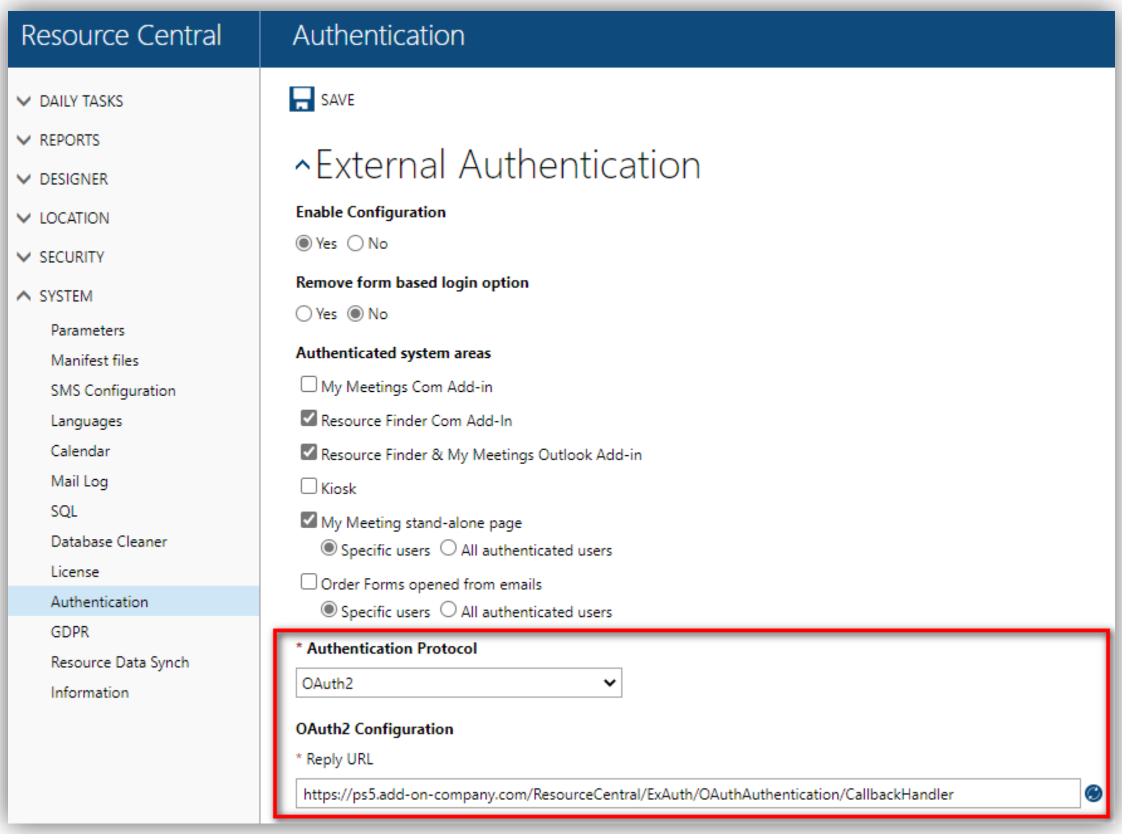
The URIs we will accept as destinations when returning authentication responses (tokens) after successfully authenticating or signing out users. The redirect URI you send in the request to the login server should match one listed here. Also referred to as reply URLs. Learn more about Redirect URIs and their restrictions

Enter the redirect URI of the application

Front-channel logout URL

Figure 5. Configure Web

Type the Reply URL generated in the **RC backend ➔ System ➔ Authentication**. This Reply URL is automatically created when you select an **Authentication Protocol**.



External Authentication

Enable Configuration
● Yes ○ No

Remove form based login option
○ Yes ● No

Authenticated system areas
☐ My Meetings Com Add-in
☑ Resource Finder Com Add-In
☑ Resource Finder & My Meetings Outlook Add-in
☐ Kiosk
☑ My Meeting stand-alone page
● Specific users ○ All authenticated users
☐ Order Forms opened from emails
● Specific users ○ All authenticated users

* Authentication Protocol
OAuth2

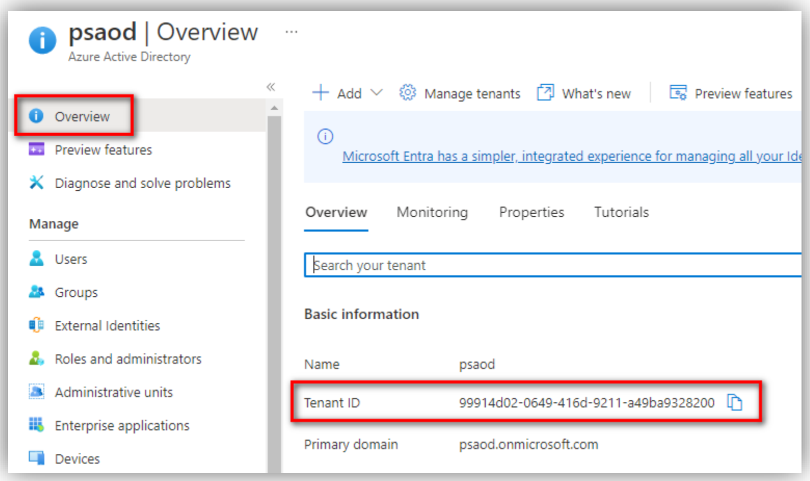
OAuth2 Configuration
* Reply URL
https://ps5.add-on-company.com/ResourceCentral/ExAuth/OAuthAuthentication/CallbackHandler

Figure 6. Reply URL generated in RC backend ➔ System ➔ Authentication.

Click [**Save**] to finish.

Tenant (Tenant ID)

Go to **Azure portal ➔ Azure Active Directory**, click [**Overview**] and you can see the **tenant ID** as shown in the following figure:



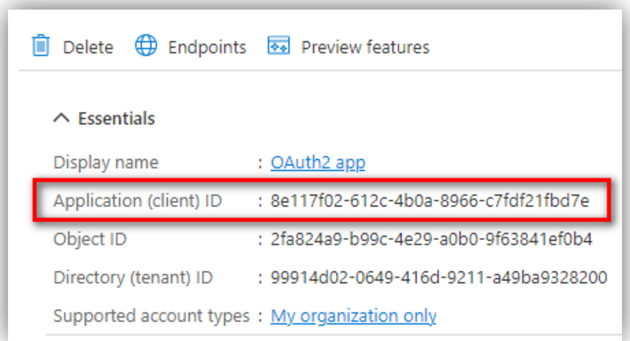
Basic information

Name psaod
Tenant ID 99914d02-0649-416d-9211-a49ba9328200
Primary domain psaod.onmicrosoft.com

Figure 7. Tenant ID

Client ID

Go to **Azure portal → Azure Active Directory → App registrations.** Click [**All applications**] then select the app that you registered in Part A to see its details.



Display name	: OAuth2 app
Application (client) ID	: 8e117f02-612c-4b0a-8966-c7fdf21fbd7e
Object ID	: 2fa824a9-b99c-4e29-a0b0-9f63841ef0b4
Directory (tenant) ID	: 99914d02-0649-416d-9211-a49ba9328200
Supported account types	: My organization only

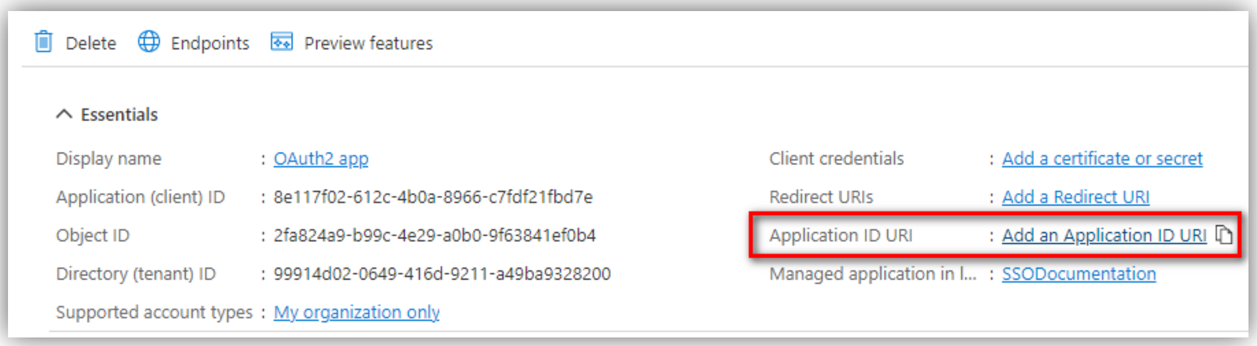
Figure 8. Client ID

The **Client ID** is the **Application (client) ID** as you can see in the above figure.

Application ID URI

To retrieve Application ID Url, follow these steps below:

1. Go to **Azure portal → Azure Active Directory → App registrations.** Click [**View all applications**] then select the app that you registered in Part A to see its details. Then click [**Add an Application ID URI**].



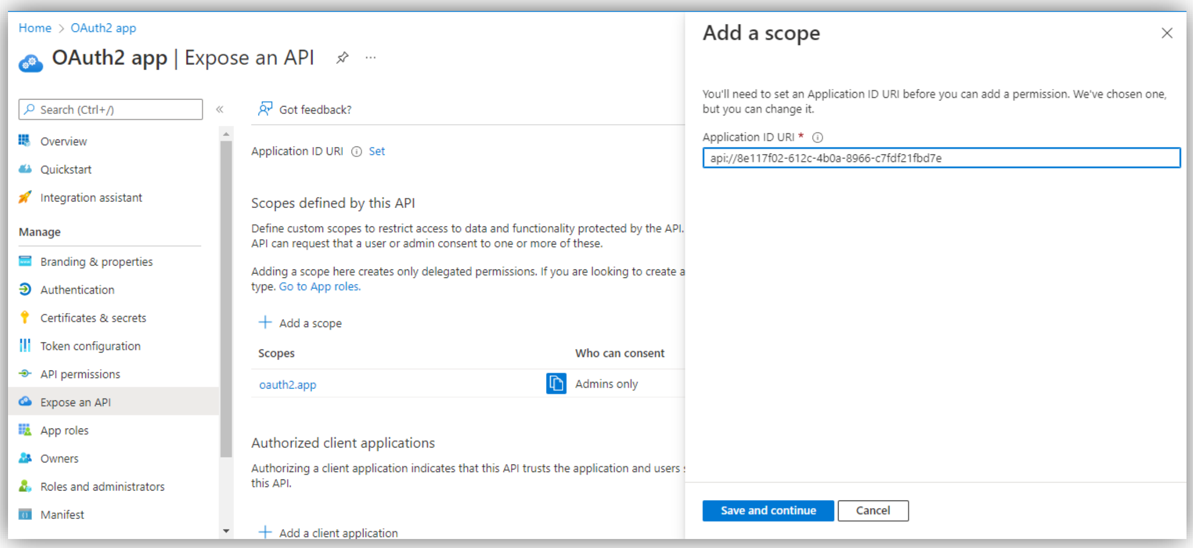
Display name	: OAuth2 app	Client credentials	: Add a certificate or secret
Application (client) ID	: 8e117f02-612c-4b0a-8966-c7fdf21fbd7e	Redirect URIs	: Add a Redirect URI
Object ID	: 2fa824a9-b99c-4e29-a0b0-9f63841ef0b4	Application ID URI	: Add an Application ID URI
Directory (tenant) ID	: 99914d02-0649-416d-9211-a49ba9328200	Managed application in l...	: SSODocumentation
Supported account types	: My organization only		

Figure 9. Add an Application ID URI

2. Look for ‘Scopes defined by this API’ section, then click [**Add a scope**] which opens a screen on the right side. The ‘Application ID URI’ field is shown with the following format:

```
api://[ Application (client) ID of this app]
```

For example: *api://8e117f02-612c-4b0a-8966-c7fdf21fbd7e*



Define custom scopes to restrict access to data and functionality protected by the API. API can request that a user or admin consent to one or more of these.

Adding a scope here creates only delegated permissions. If you are looking to create a type. Go to App roles.

Authorizing a client application indicates that this API trusts the application and users this API.

You'll need to set an Application ID URI before you can add a permission. We've chosen one, but you can change it.

Application ID URI *: api://8e117f02-612c-4b0a-8966-c7fdf21fbd7e

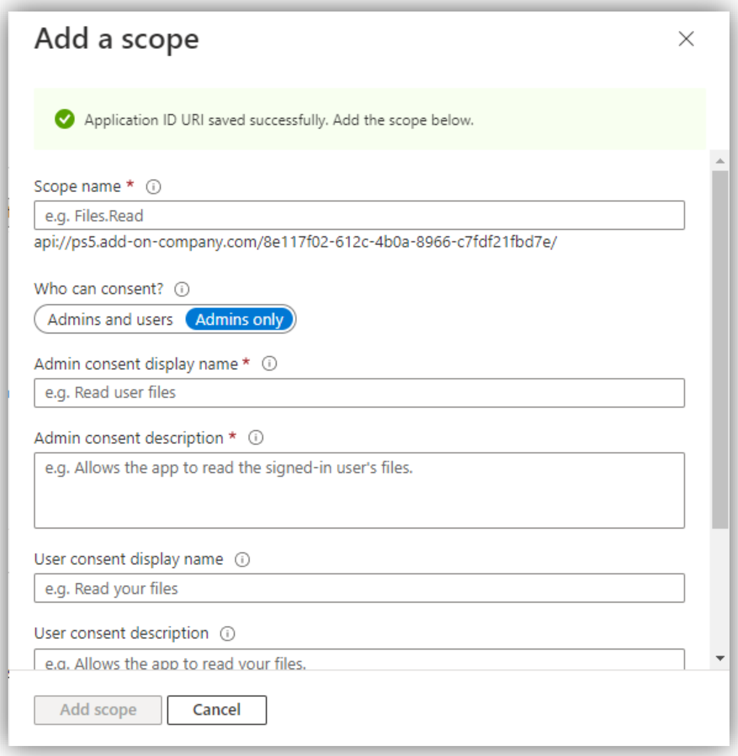
Now, change the value of this field by adding the RC backend URL to this value as follows:

```
api://[RC backend URL]/[Application (client) ID of this app]
```

For example: *api://**ps5.add-on-company.com**/8e117f02-612c-4b0a-8966-c7fdf21fbd7e*

After that, click [**Save and continue**] to proceed to the next step.

3. On ‘Add a scope’ screen (figure below), enter necessary information for the 3 mandatory fields: **Scope name**, **Admin consent display name**, and **Admin consent description**.
Once you are done, click [**Add scope**].

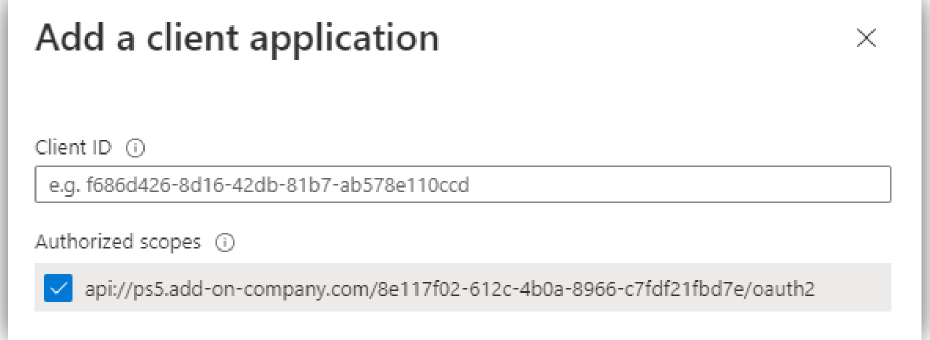

Add a scope
Scope name *
e.g. Files.Read
Who can consent?
Admins and users
Admins only
Admin consent display name *
e.g. Read user files
Admin consent description *
e.g. Allows the app to read the signed-in user's files.
User consent display name
e.g. Read your files
User consent description
e.g. Allows the app to read your files.
Add scope
Cancel

Application ID URI saved successfully. Add the scope below.

api://ps5.add-on-company.com/8e117f02-612c-4b0a-8966-c7fdf21fbd7e/

Figure 10. Add a scope

4. Look for ‘Authorized client applications’ section, then click [**Add a client application**] which opens the following screen:



Add a client application

Client ID ⓘ

e.g. f686d426-8d16-42db-81b7-ab578e110ccd

Authorized scopes ⓘ

☑ api://ps5.add-on-company.com/8e117f02-612c-4b0a-8966-c7fdf21fbd7e/oauth2

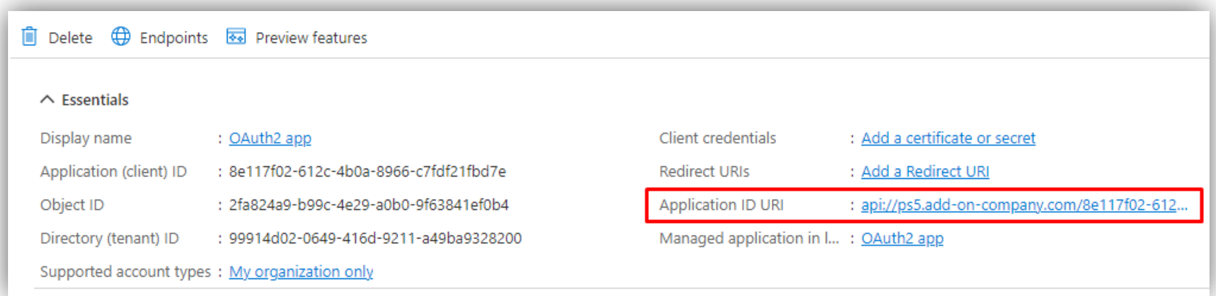
Figure 11. Add a client application

Here, select the scope(s) that you have added from step 2, then enter the ‘Client ID’ which will allow Office to access to this app.
There are 4 Client IDs that you can choose, each allows specified Office app to have access:

- For all Microsoft Office application endpoints: `ea5a67f6-b6f3-4338-b240-c655ddc3cc8e` (highly recommended)
- For for Microsoft Office (desktop app): `d3590ed6-52b3-4102-aeff-aad2292ab01c`
- For Office on the web: `93d53678-613d-4013-afc1-62e9e444a0a5`
- For Outlook on the web: `bc59ab01-8403-45c6-8796-ac3ef710b3e3`

After entering a Client ID, click [**Add application**].

5. To get **Application ID URI**, click [**Overview**] to see the app’s details. You can now copy the new value in ‘Application ID URI’ field:



Essentials

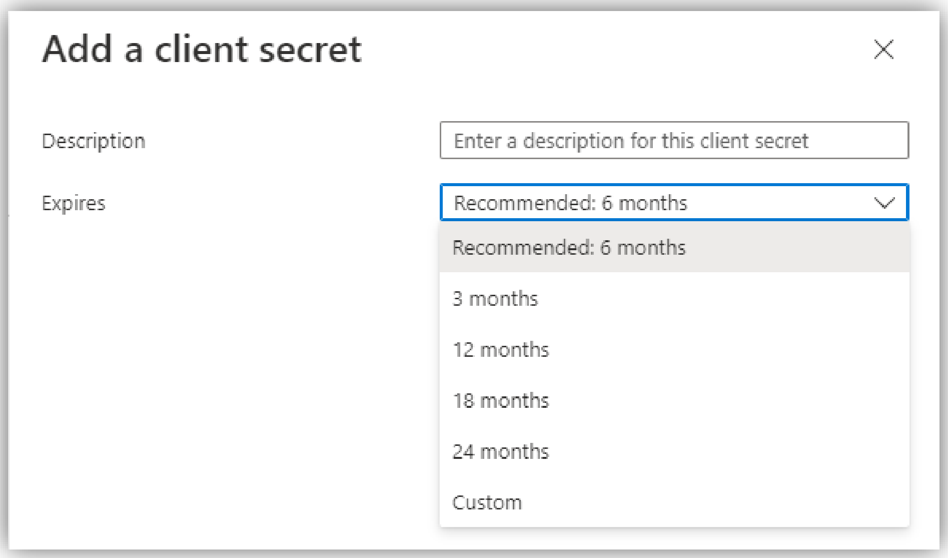
Display name	: OAuth2 app	Client credentials	: Add a certificate or secret
Application (client) ID	: 8e117f02-612c-4b0a-8966-c7fdf21fbd7e	Redirect URIs	: Add a Redirect URI
Object ID	: 2fa824a9-b99c-4e29-a0b0-9f63841ef0b4	Application ID URI	: api://ps5.add-on-company.com/8e117f02-612...
Directory (tenant) ID	: 99914d02-0649-416d-9211-a49ba9328200	Managed application in l...	: OAuth2 app
Supported account types	: My organization only		

Figure 12. Get Application ID URI

Client secret

Go to **Azure portal → Azure Active Directory → App registrations.** Click [**All applications**] then select the app that you registered in Part A to see its details.

Click [**Certificates & secrets**] → [**New client secret**].

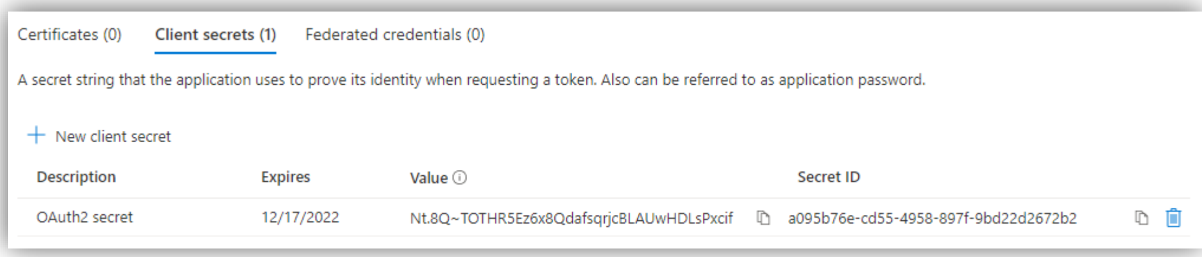


Add a client secret

Description	Enter a description for this client secret
Expires	Recommended: 6 months

Figure 13. Client secret

Enter **Description**, select **Expires** time, then click [**Add**] button. The **Value** and **Secret ID** column will be populated with **Client secret** and an ID:



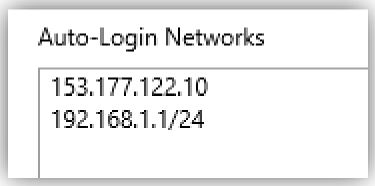
A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

Description	Expires	Value ⓘ	Secret ID
OAuth2 secret	12/17/2022	Nt.8Q~TOTHR5Ez6x8QdafsqrjcBLAUwHDLsPxcif	a095b76e-cd55-4958-897f-9bd22d2672b2

Please remember to copy client secret value & secret ID because you will not be able to retrieve it after leaving this panel.

Auto-Login Networks

For this section in RC backend, you can fill in IP addresses or IP address ranges, each value in a line.



Auto-Login Networks

153.177.122.10
192.168.1.1/24

Figure 14. Auto-Login Networks

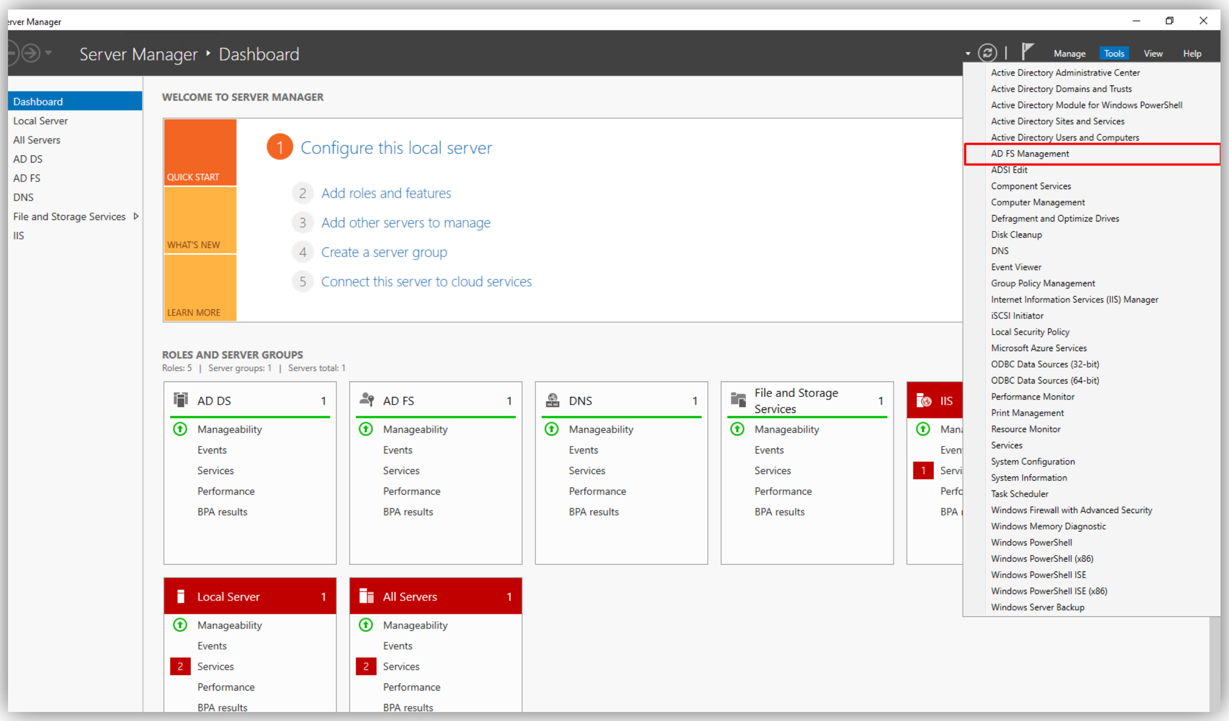
With this value filled in, client machines with the filled in IP address will be automatically logged in and use Single Sign-On function.

Apart from this, refer to this article to enable seamless SSO to work with RC Auto-Login Networks.

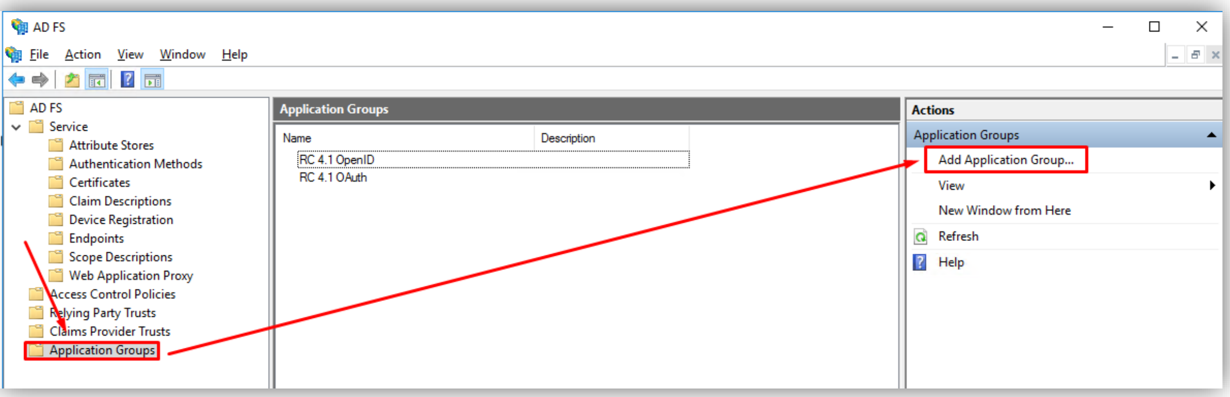
Authentication Details for OAuth2 with ADFS

Part A. Configure Active Directory Federation Services (ADFS)

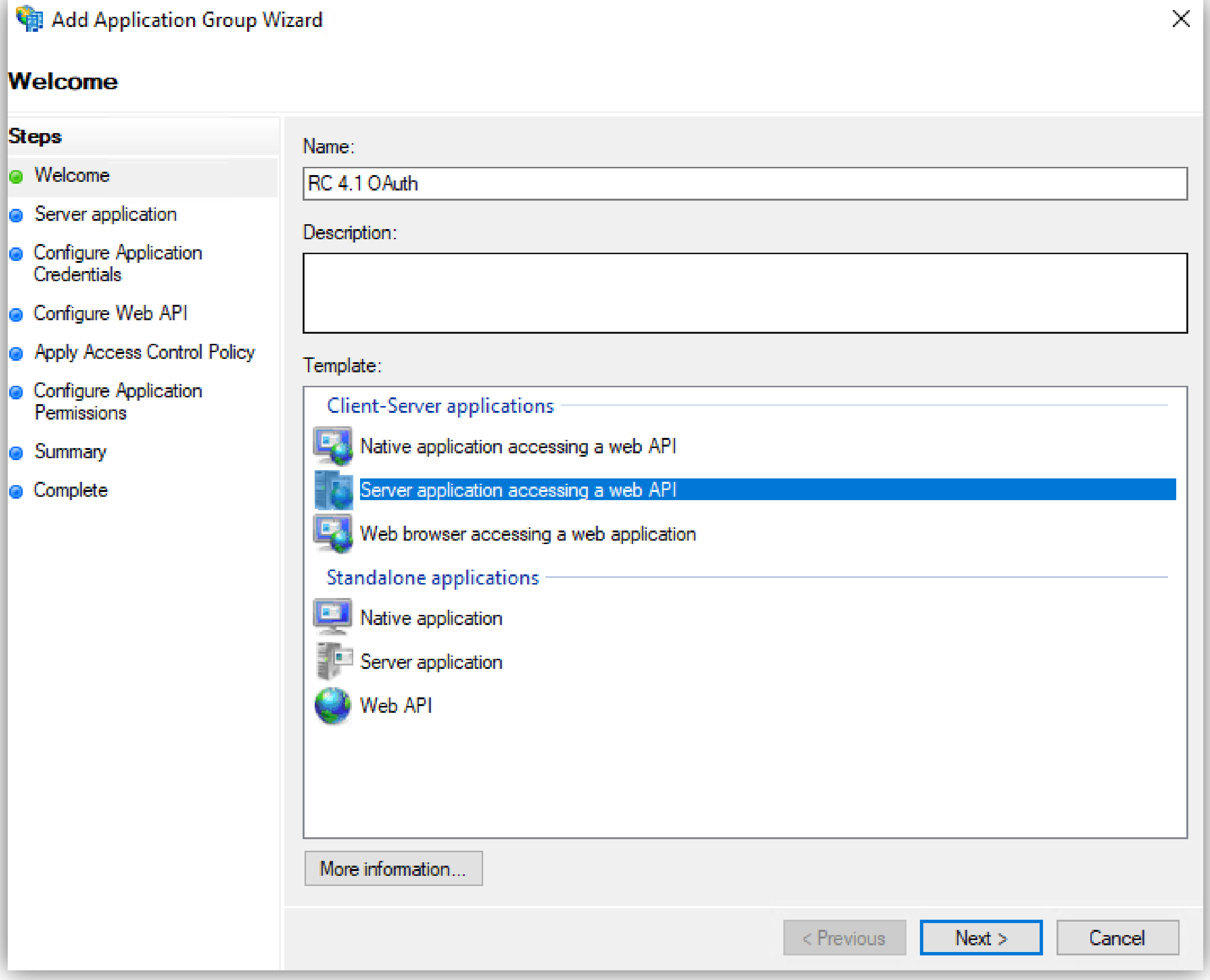
1. Go to **web server** where your Exchange server is installed, click **Start → Server Manager → Tools → AD FS Management**


Server Manager
Server Manager ‣ Dashboard
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
AD DS
AD FS
DNS
File and Storage Services
IIS
WELCOME TO SERVER MANAGER
QUICK START
WHAT'S NEW
LEARN MORE
1 Configure this local server
2 Add roles and features
3 Add other servers to manage
4 Create a server group
5 Connect this server to cloud services
ROLES AND SERVER GROUPS
Roles: 5 | Server groups: 1 | Servers total: 1
AD DS 1
AD FS 1
DNS 1
File and Storage Services 1
IIS
Manageability
Events
Services
Performance
BPA results
Local Server 1
All Servers 1
2
Active Directory Administrative Center
Active Directory Domains and Trusts
Active Directory Module for Windows PowerShell
Active Directory Sites and Services
Active Directory Users and Computers
AD FS Management
ADSI Edit
Component Services
Computer Management
Defragment and Optimize Drives
Disk Cleanup
DNS
Event Viewer
Group Policy Management
Internet Information Services (IIS) Manager
iSCSI Initiator
Local Security Policy
Microsoft Azure Services
ODBC Data Sources (32-bit)
ODBC Data Sources (64-bit)
Performance Monitor
Print Management
Resource Monitor
Services
System Configuration
System Information
Task Scheduler
Windows Firewall with Advanced Security
Windows Memory Diagnostic
Windows PowerShell
Windows PowerShell (x86)
Windows PowerShell ISE
Windows PowerShell ISE (x86)
Windows Server Backup

2. In the opened window, select **Application Groups** and [**Add a new Application Group**] from the **Actions** sidebar. This starts the configuration wizard for a new Group.



3. On the ‘Add Application Group wizard’ → Welcome screen, fill in Name and select “**Server application accessing a web API**” in Template and Click “**Next**”



Add Application Group Wizard

Welcome

Steps
- Welcome
- Server application
- Configure Application Credentials
- Configure Web API
- Apply Access Control Policy
- Configure Application Permissions
- Summary
- Complete

Name: RC 4.1 OAuth

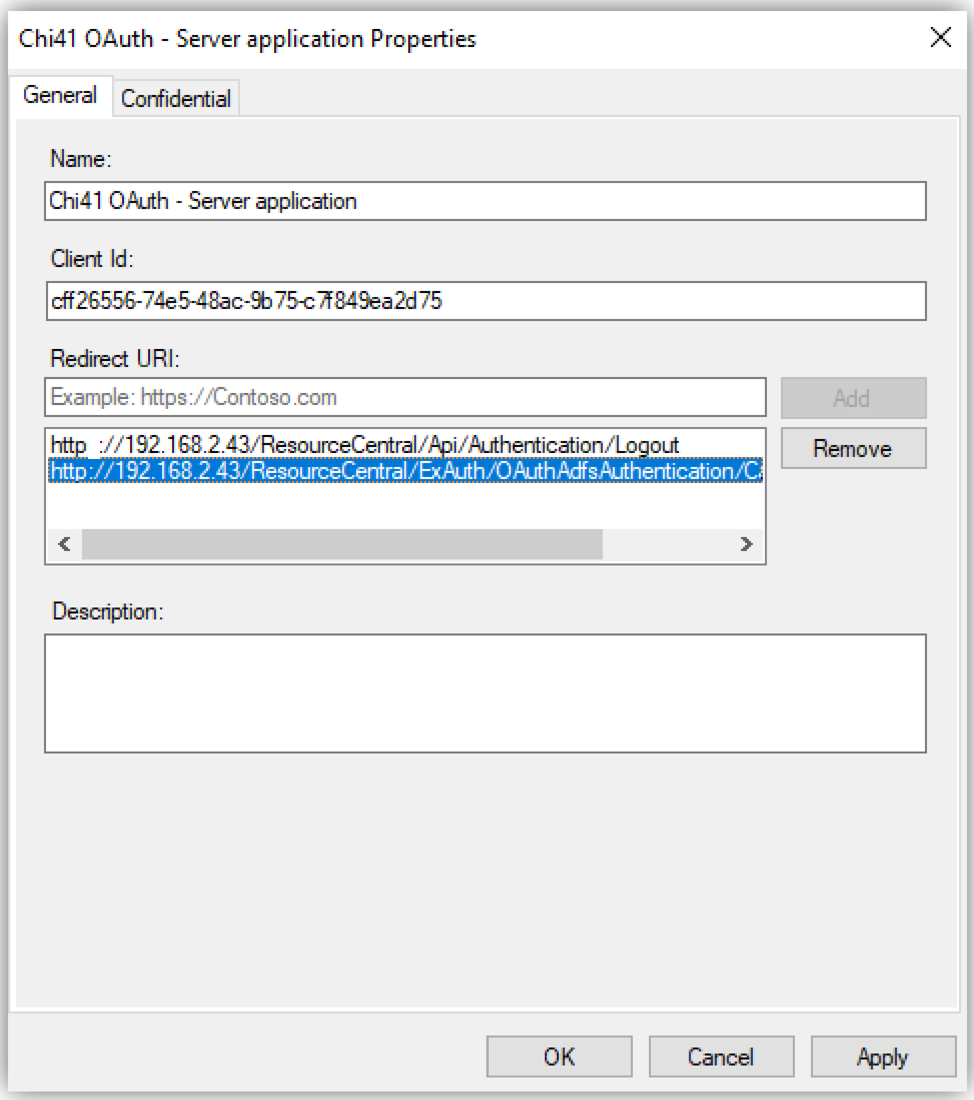
Description:

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

4. On the next screen (Server application), fill in Redirect URI and Click "**Add**" then Click "**Next**". You will have to provide 2 URLs: one for receiving login details from ADFS, one for receiving logout information from ADFS



Chi41 OAuth - Server application Properties

Name:
Chi41 OAuth - Server application

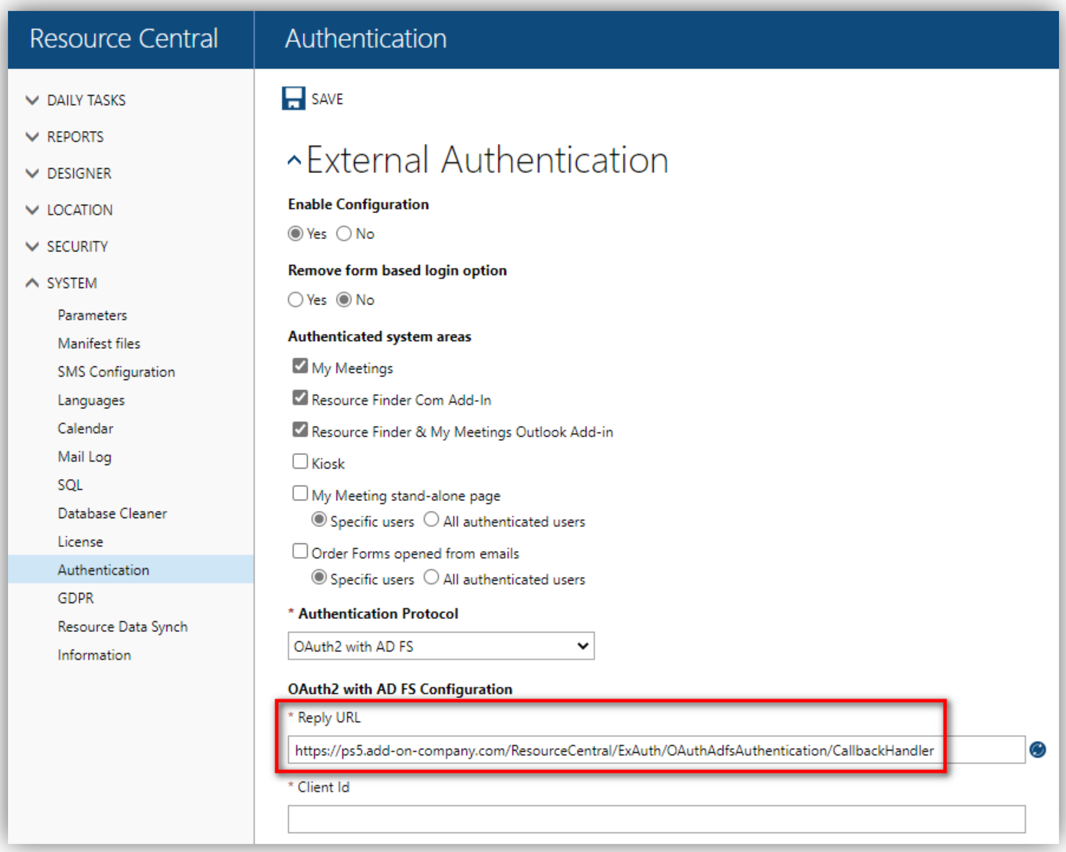
Client Id:
cff26556-74e5-48ac-9b75-c7f849ea2d75

Redirect URI:
Example: https://Contoso.com

http ://192.168.2.43/ResourceCentral/Api/Authentication/Logout
http://192.168.2.43/ResourceCentral/ExAuth/OAuthAdfsAuthentication/C

Description:

The URL for receiving login details from ADFS is the Reply URL in **RC backend → External Authentication**



External Authentication

Enable Configuration
● Yes ○ No

Remove form based login option
○ Yes ● No

Authenticated system areas
☑ My Meetings
☑ Resource Finder Com Add-In
☑ Resource Finder & My Meetings Outlook Add-in
□ Kiosk
□ My Meeting stand-alone page
● Specific users ○ All authenticated users
□ Order Forms opened from emails
● Specific users ○ All authenticated users

* **Authentication Protocol**
OAuth2 with AD FS

OAuth2 with AD FS Configuration
* Reply URL
https://ps5.add-on-company.com/ResourceCentral/ExAuth/OAuthAdfsAuthentication/CallbackHandler
* Client Id

To retrieve this information, refer to this section for more details.

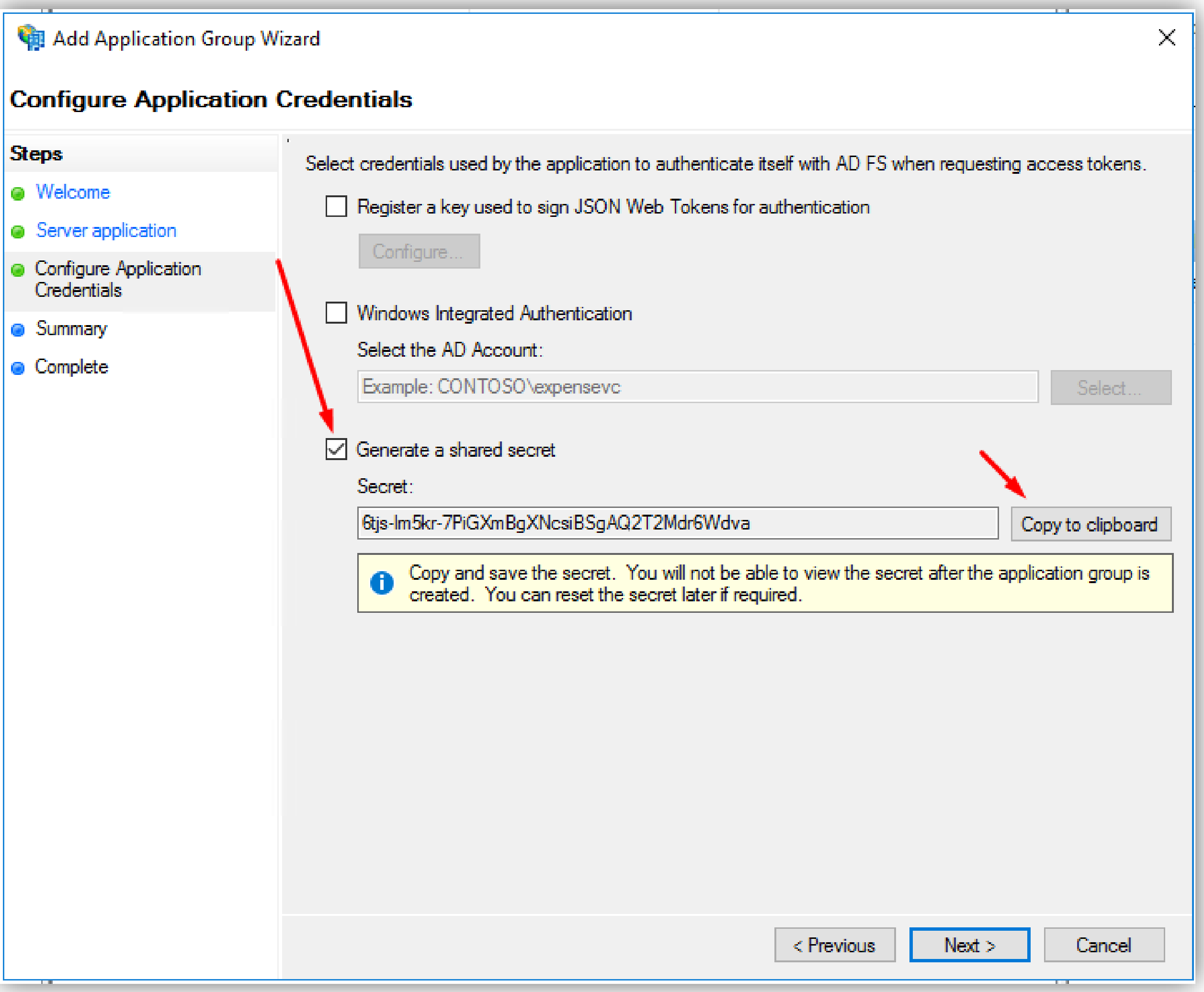
The URL for receiving logout details from ADFS must have the following format:

```
[RC backend URL]/Api/Authentication/Logout
```

e.g. http://ResourceCentral.com/Api/Authentication/Logout

Then click [**OK**] to proceed.

5. On the next screen (*Configure Application Credentials*), check on “**Generate a shared secret**” and click “**Copy to clipboard**” save the client secret then click “**Next**”.



Add Application Group Wizard

Configure Application Credentials

Select credentials used by the application to authenticate itself with AD FS when requesting access tokens.

□ Register a key used to sign JSON Web Tokens for authentication

□ Windows Integrated Authentication

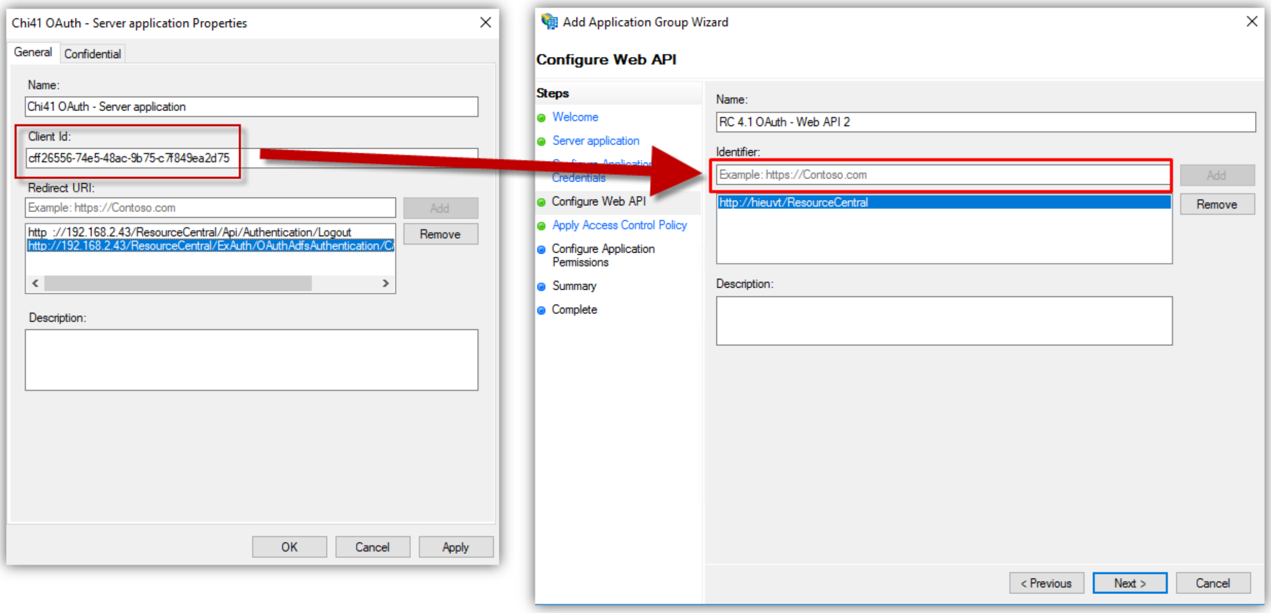
Select the AD Account: Example: CONTOSO\expensevc

☑ Generate a shared secret

Secret: 6tjs-Im5kr-7PiGXmBgXNcsiBSgAQ2T2Mdr6Wdva

Copy and save the secret. You will not be able to view the secret after the application group is created. You can reset the secret later if required.

6. On *Configure Web API* screen, fill in “**Identifier**” (which is Client Id in Step 4 of this section) and click [**Add**] button.



Chi41 OAuth - Server application Properties

Name: Chi41 OAuth - Server application

Client Id: cff26556-74e5-48ac-9b75-c7f849ea2d75

Redirect URI: Example: https://Contoso.com

http ://192.168.2.43/ResourceCentral/Api/Authentication/Logout
http://192.168.2.43/ResourceCentral/ExAuth/OAuthAdfsAuthentication/C

Description:

Add Application Group Wizard

Configure Web API

Name: RC 4.1 OAuth - Web API 2

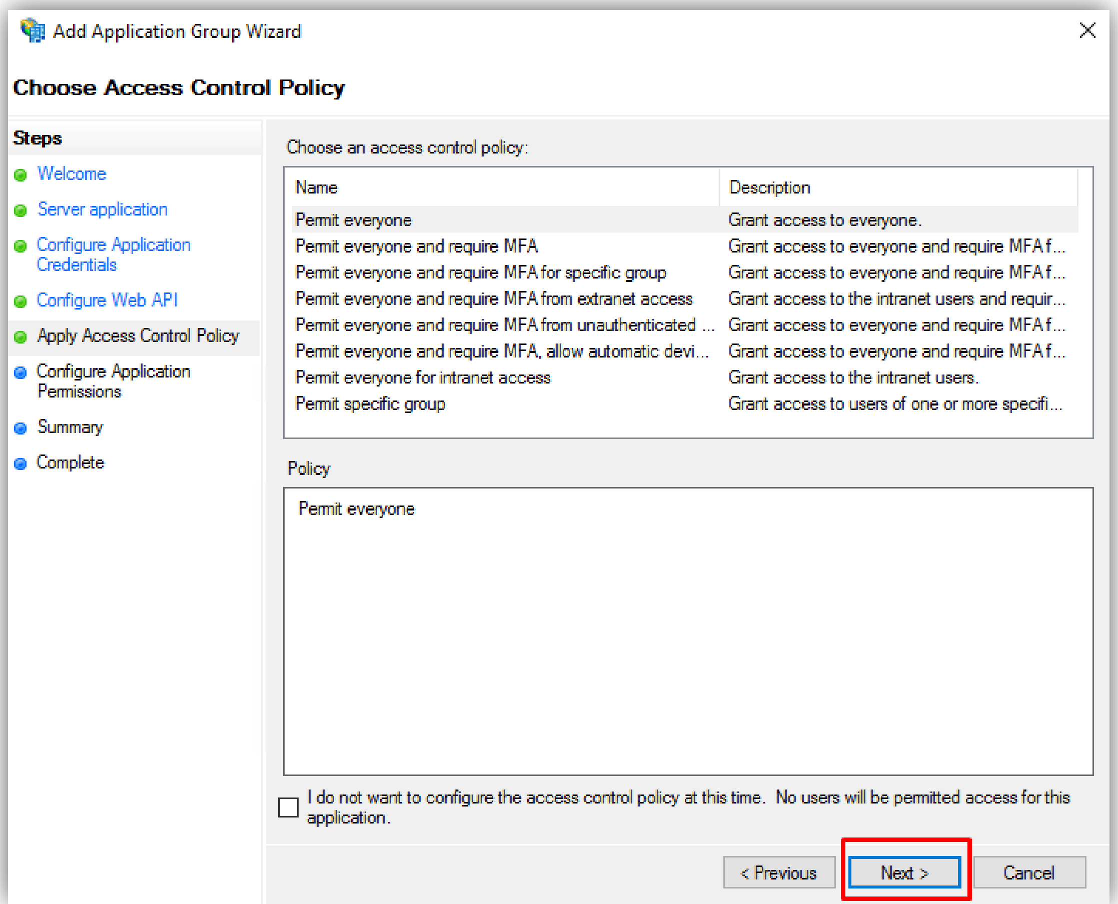
Identifier: Example: https://Contoso.com

http://hieuvt/ResourceCentral

Description:

Then click [**Next]** to proceed.

7. Click [**Next**] on **Choose Access Control Policy** screen.



Add Application Group Wizard

Choose Access Control Policy

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 f...
Permit everyone and require MFA for specific group	Grant access to everyone and require MFA f...
Permit everyone and require MFA from extranet access	Grant access to the intranet users and requir...
Permit everyone and require MFA from unauthenticated ...	Grant access to everyone and require MFA f...
Permit everyone and require MFA, allow automatic devi...	Grant access to everyone and require MFA f...
Permit everyone for intranet access	Grant access to the intranet users.
Permit specific group	Grant access to users of one or more specifi...

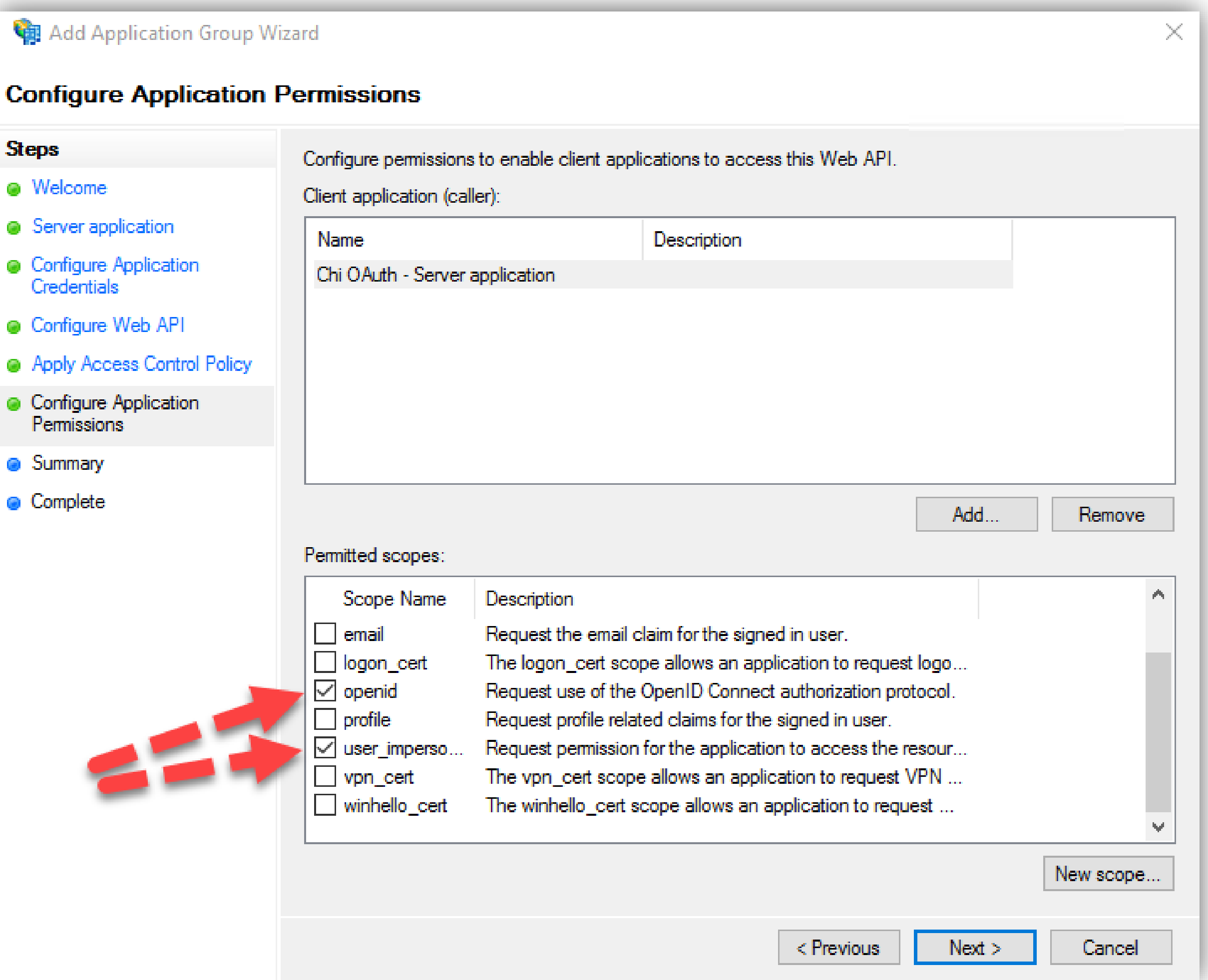
Policy

Permit everyone

☐ I do not want to configure the access control policy at this time. No users will be permitted access for this application.

Steps
Welcome
Server application
Configure Application Credentials
Configure Web API
Apply Access Control Policy
Configure Application Permissions
Summary
Complete
< Previous
Next >
Cancel

8. On *Configure Application Permissions* screen, check on **openid** and **user_impersonate** checkboxes.



Add Application Group Wizard

Configure Application Permissions

Steps
Welcome
Server application
Configure Application Credentials
Configure Web API
Apply Access Control Policy
Configure Application Permissions
Summary
Complete

Configure permissions to enable client applications to access this Web API.

Client application (caller):

Name	Description
Chi OAuth - Server application	

Permitted scopes:

	Scope Name	Description
□	email	Request the email claim for the signed in user.
□	logon_cert	The logon_cert scope allows an application to request logo...
☑	openid	Request use of the OpenID Connect authorization protocol.
□	profile	Request profile related claims for the signed in user.
☑	user_imperso...	Request permission for the application to access the resour...
□	vpn_cert	The vpn_cert scope allows an application to request VPN ...
□	winhello_cert	The winhello_cert scope allows an application to request ...

Click [**Next**] proceed.

9. Click [**Next**] on **Summary** screen and click [**Close**] on **Complete** screen to finish.

NOTE: If, in the system, there are users who have User Principal Name different from SMTP address, we need to add claim to retrieve all email addresses. Please refer to this appendix for more details.

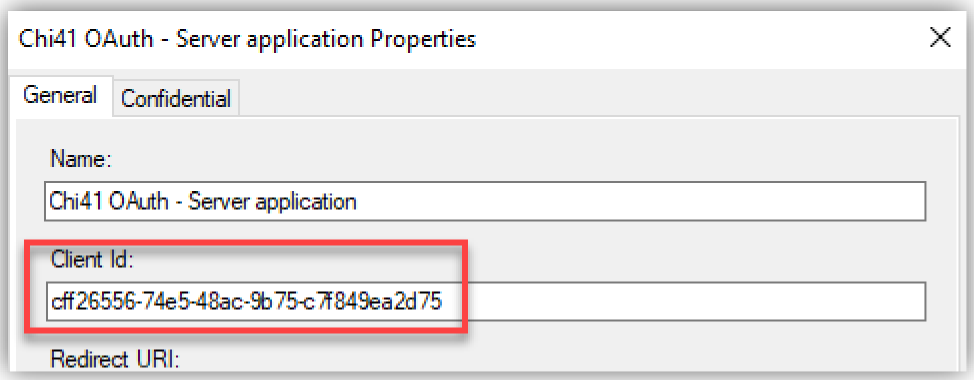
Part B. Retrieve details for OAuth2 with ADFS Authentication Protocol

Reply URL

Refer to this section for more details.

Client Id

The **Client Id** can be retrieved from **Step 4** in Part A of this protocol.



Chi41 OAuth - Server application Properties

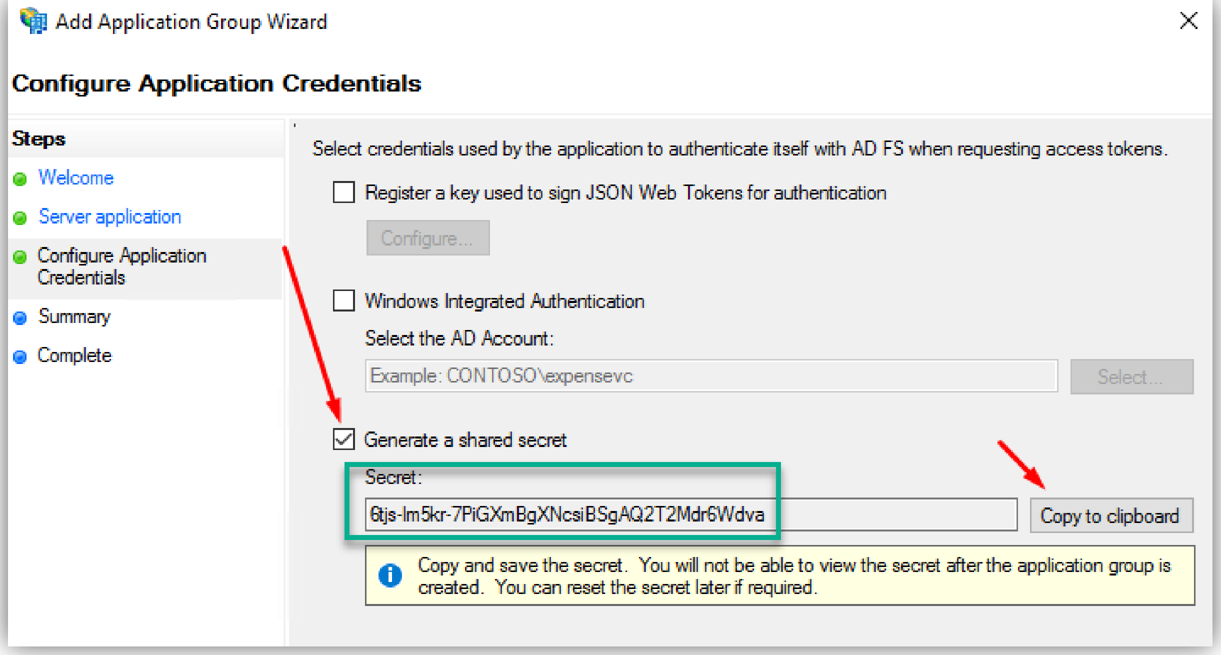
Name:
Chi41 OAuth - Server application

Client Id:
cff26556-74e5-48ac-9b75-c7f849ea2d75

Redirect URI:

Client Secret

The **Client Secret** can be retrieved from **Step 5** in Part A of this protocol (highlighted in Green).



Add Application Group Wizard

Configure Application Credentials

Select credentials used by the application to authenticate itself with AD FS when requesting access tokens.

☐ Register a key used to sign JSON Web Tokens for authentication

☐ Windows Integrated Authentication

Select the AD Account:
Example: CONTOSO\expensevc

☑ Generate a shared secret

Secret:
6tjs-lm5kr-7PiGXmBgXNcsiBSgAQ2T2Mdr6Wdva

Copy and save the secret. You will not be able to view the secret after the application group is created. You can reset the secret later if required.

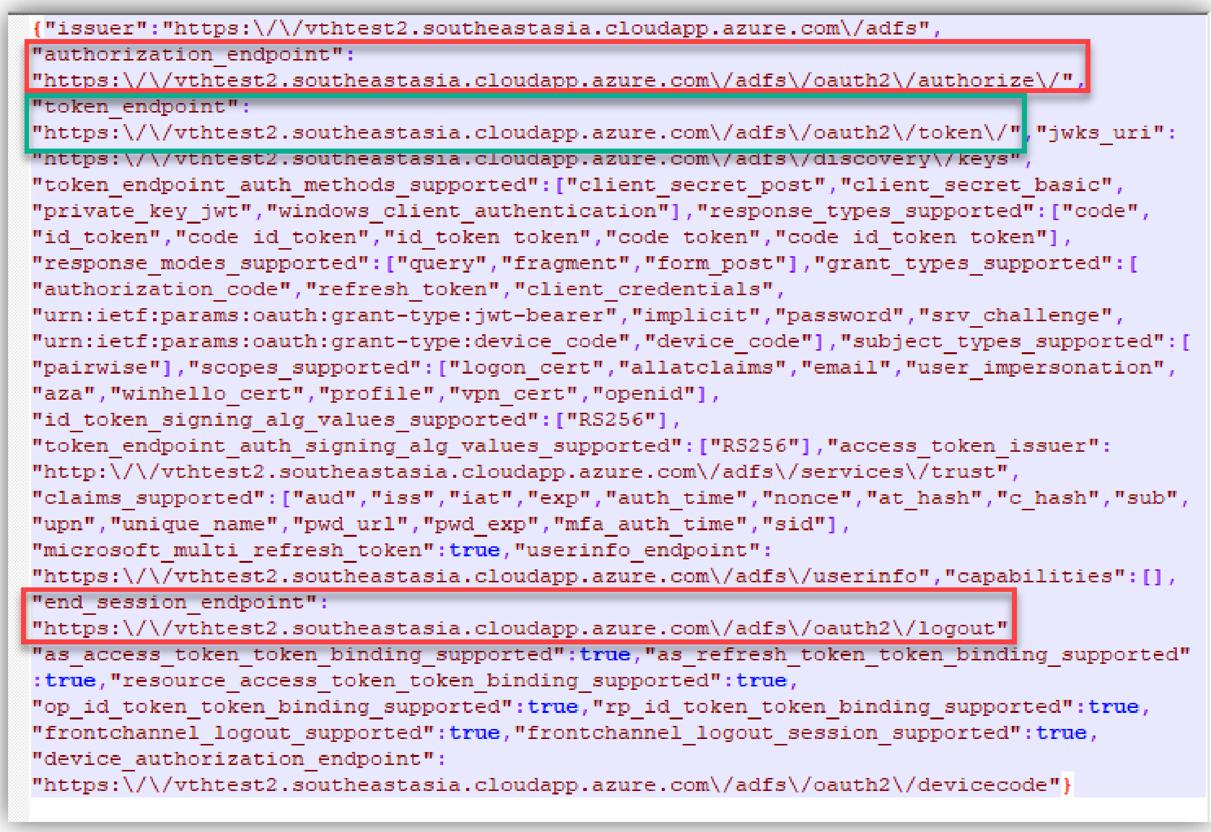
Authorization URL, Token URL and Logout URL

Go to the following link:

```
https://<server of ADFS>/adfs/.well-known/openid-configuration
```

And a json file (***openid-configuration.json***) will be available for you to download/view. If you download it, open this file with Notepad or Notepad++, look for the necessary information as described in the following table:

URL	**Keywords to look for in the json file**
Authorization URL	authorization_endpoint
Token URL	token_endpoint
Logout URL	end_session_endpoint



```
{"issuer":"https:\/\/vthtest2.southeastasia.cloudapp.azure.com\/adfs",
"authorization_endpoint":
"https:\/\/vthtest2.southeastasia.cloudapp.azure.com\/adfs\/oauth2\/authorize\/",
"token_endpoint":
"https:\/\/vthtest2.southeastasia.cloudapp.azure.com\/adfs\/oauth2\/token\/","jwks_uri":
"https:\/\/vthtest2.southeastasia.cloudapp.azure.com\/adfs\/discovery\/keys",
"token_endpoint_auth_methods_supported":["client_secret_post","client_secret_basic",
"private_key_jwt","windows_client_authentication"],"response_types_supported":["code",
"id_token","code id_token","id_token token","code token","code id_token token"],
"response_modes_supported":["query","fragment","form_post"],"grant_types_supported":[
"authorization_code","refresh_token","client_credentials",
"urn:ietf:params:oauth:grant-type:jwt-bearer","implicit","password","srv_challenge",
"urn:ietf:params:oauth:grant-type:device_code","device_code"],"subject_types_supported":[
"pairwise"],"scopes_supported":["logon_cert","allatclaims","email","user_impersonation",
"aza","winhello_cert","profile","vpn_cert","openid"],
"id_token_signing_alg_values_supported":["RS256"],
"token_endpoint_auth_signing_alg_values_supported":["RS256"],"access_token_issuer":
"http:\/\/vthtest2.southeastasia.cloudapp.azure.com\/adfs\/services\/trust",
"claims_supported":["aud","iss","iat","exp","auth_time","nonce","at_hash","c_hash","sub",
"upn","unique_name","pwd_url","pwd_exp","mfa_auth_time","sid"],
"microsoft_multi_refresh_token":true,"userinfo_endpoint":
"https:\/\/vthtest2.southeastasia.cloudapp.azure.com\/adfs\/userinfo","capabilities":[],
"end_session_endpoint":
"https:\/\/vthtest2.southeastasia.cloudapp.azure.com\/adfs\/oauth2\/logout"
"as_access_token_token_binding_supported":true,"as_refresh_token_token_binding_supported"
:true,"resource_access_token_token_binding_supported":true,
"op_id_token_token_binding_supported":true,"rp_id_token_token_binding_supported":true,
"frontchannel_logout_supported":true,"frontchannel_logout_session_supported":true,
"device_authorization_endpoint":
"https:\/\/vthtest2.southeastasia.cloudapp.azure.com\/adfs\/oauth2\/devicecode"}
```

Copy the URL, remove the character “\” in each URL and paste into the relevant fields in RC backend.

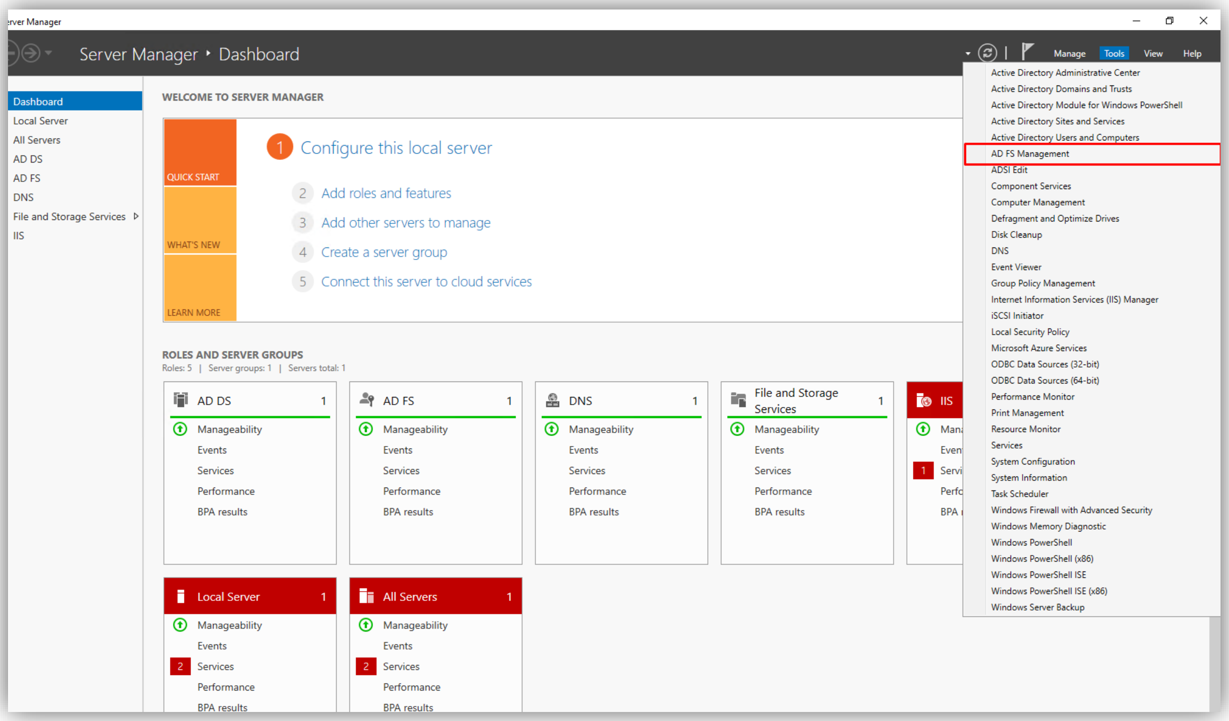
Auto-Login Networks

Refer to this section for more details.

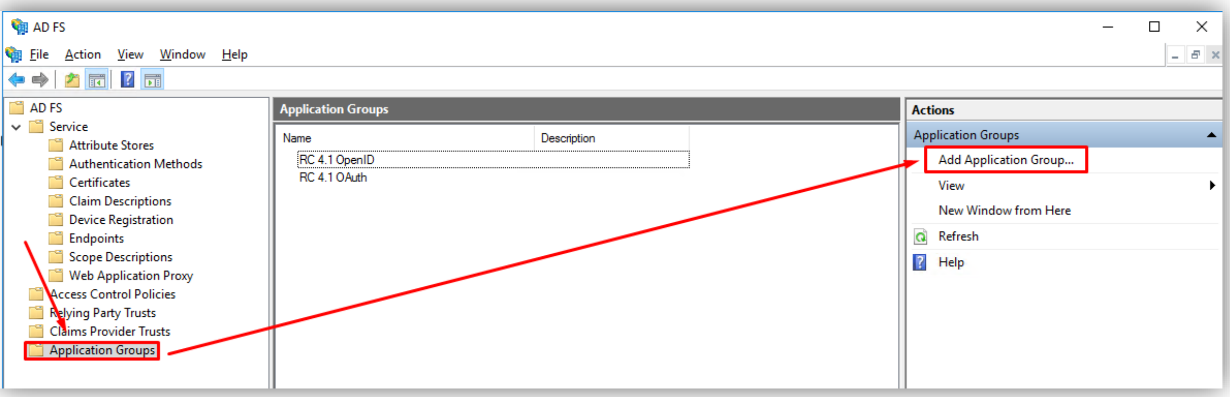
Authentication Details for OpenID Connect with ADFS

Part A. Configure Active Directory Federation Services (ADFS)

1. Go to **web server** where your Exchange server is installed, click **Start → Server Manager → Tools → AD FS Management**


Server Manager
Server Manager ‣ Dashboard
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
AD DS
AD FS
DNS
File and Storage Services
IIS
WELCOME TO SERVER MANAGER
QUICK START
WHAT'S NEW
LEARN MORE
1 Configure this local server
2 Add roles and features
3 Add other servers to manage
4 Create a server group
5 Connect this server to cloud services
ROLES AND SERVER GROUPS
Roles: 5 | Server groups: 1 | Servers total: 1
AD DS 1
AD FS 1
DNS 1
File and Storage Services 1
IIS
Manageability
Events
Services
Performance
BPA results
Local Server 1
All Servers 1
Active Directory Administrative Center
Active Directory Domains and Trusts
Active Directory Module for Windows PowerShell
Active Directory Sites and Services
Active Directory Users and Computers
AD FS Management
ADSI Edit
Component Services
Computer Management
Defragment and Optimize Drives
Disk Cleanup
DNS
Event Viewer
Group Policy Management
Internet Information Services (IIS) Manager
iSCSI Initiator
Local Security Policy
Microsoft Azure Services
ODBC Data Sources (32-bit)
ODBC Data Sources (64-bit)
Performance Monitor
Print Management
Resource Monitor
Services
System Configuration
System Information
Task Scheduler
Windows Firewall with Advanced Security
Windows Memory Diagnostic
Windows PowerShell
Windows PowerShell (x86)
Windows PowerShell ISE
Windows PowerShell ISE (x86)
Windows Server Backup

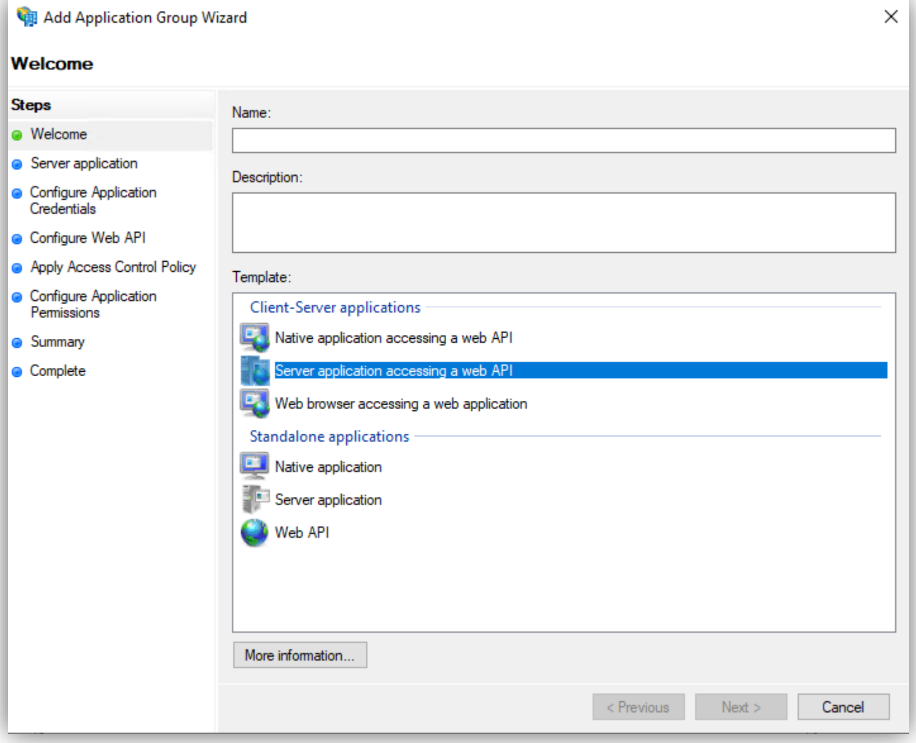
2. In the opened window, select **Application Groups** and [**Add a new Application Group**] from the **Actions** sidebar. This starts the configuration wizard for a new Group.



Application Groups

Name	Description
RC 4.1 OpenID	
RC 4.1 OAuth	

3. On the ‘Add Application Group wizard’ → Welcome screen, fill in Name and select “**Server application**” in Template and Click [**Next].**



Add Application Group Wizard

Welcome

Steps
- Welcome
- Server application
- Configure Application Credentials
- Configure Web API
- Apply Access Control Policy
- Configure Application Permissions
- Summary
- Complete

Name:

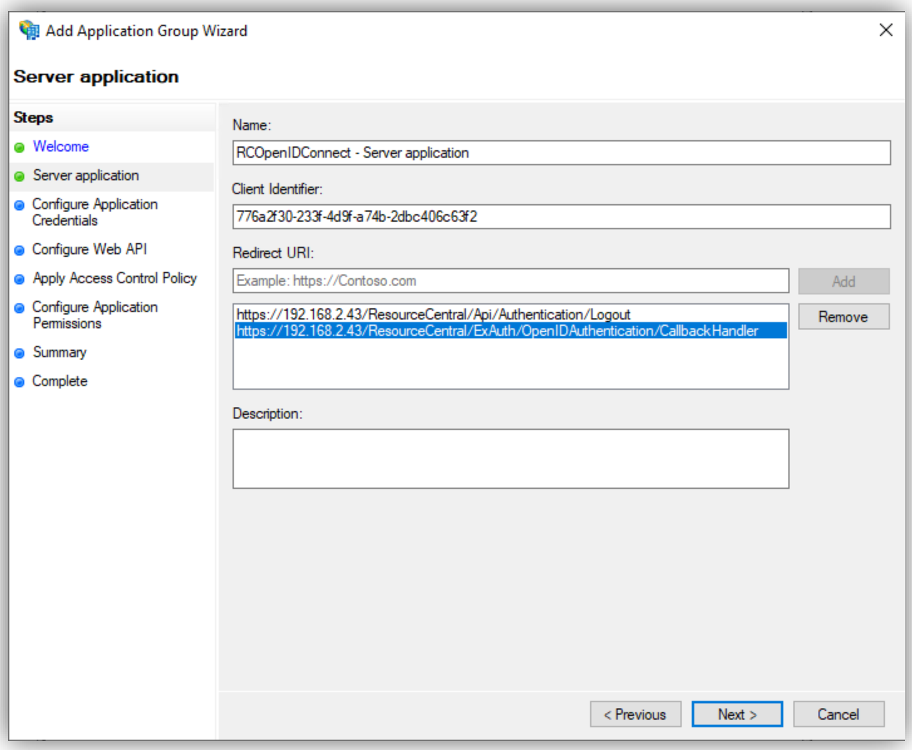
Description:

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

4. On the next screen, fill in ‘**Redirect URL**’ and click [**Add**]. You will have to provide 2 URLs: one for receiving login details from ADFS, one for receiving logout information from ADFS



Add Application Group Wizard

Server application

Steps
- Welcome
- Server application
- Configure Application Credentials
- Configure Web API
- Apply Access Control Policy
- Configure Application Permissions
- Summary
- Complete

Name: RCOpenIDConnect - Server application

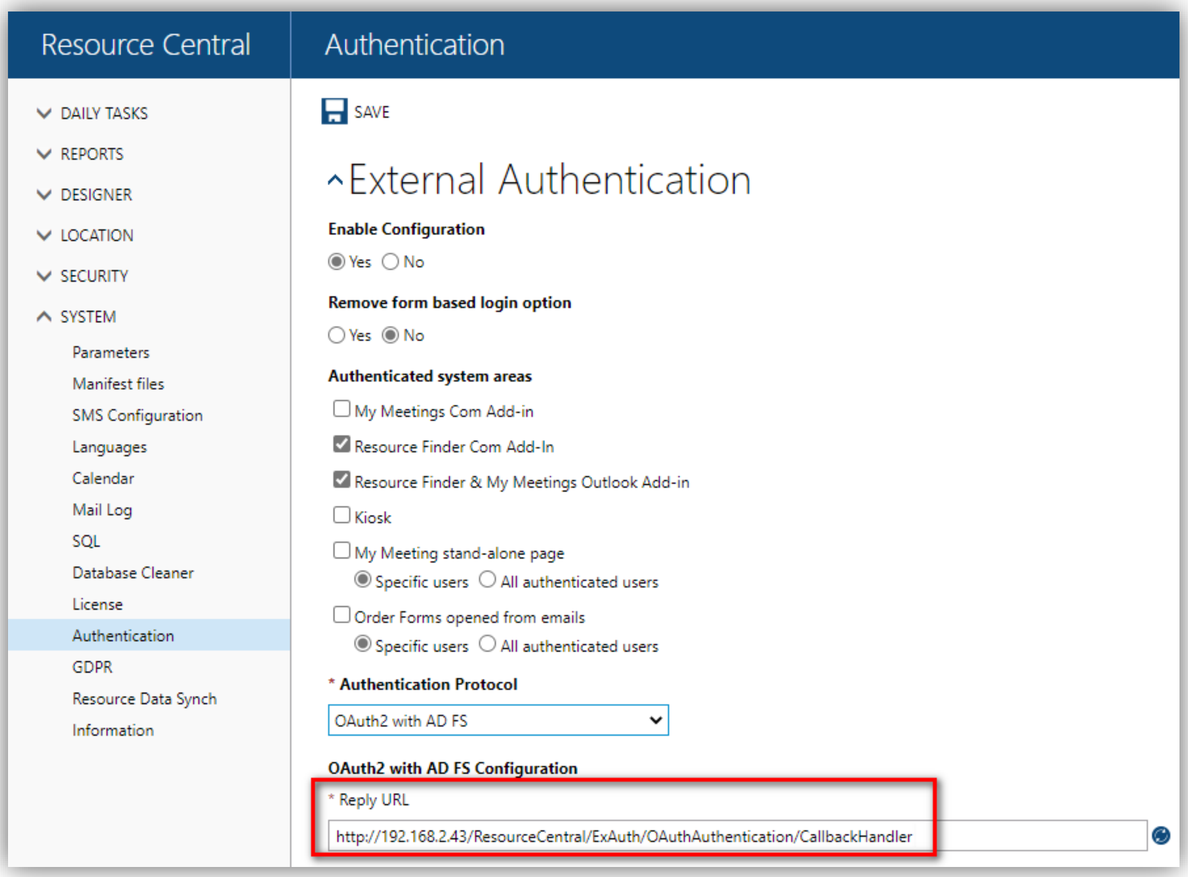
Client Identifier: 776a2f30-233f-4d9f-a74b-2dbc406c63f2

Redirect URI: Example: https://Contoso.com

https://192.168.2.43/ResourceCentral/Api/Authentication/Logout
https://192.168.2.43/ResourceCentral/ExAuth/OpenIDAuthentication/CallbackHandler

Description:

The URL for receiving login details from ADFS is the Reply URL in **RC backend → Authentication → External Authentication**.



External Authentication

Enable Configuration

● Yes ○ No

Remove form based login option

○ Yes ● No

Authenticated system areas

□ My Meetings Com Add-in

☑ Resource Finder Com Add-In

☑ Resource Finder & My Meetings Outlook Add-in

□ Kiosk

□ My Meeting stand-alone page

● Specific users ○ All authenticated users

□ Order Forms opened from emails

● Specific users ○ All authenticated users

* **Authentication Protocol**

OAuth2 with AD FS

OAuth2 with AD FS Configuration

* Reply URL

http://192.168.2.43/ResourceCentral/ExAuth/OAuthAuthentication/CallbackHandler

To retrieve this information, refer to this section for more details.

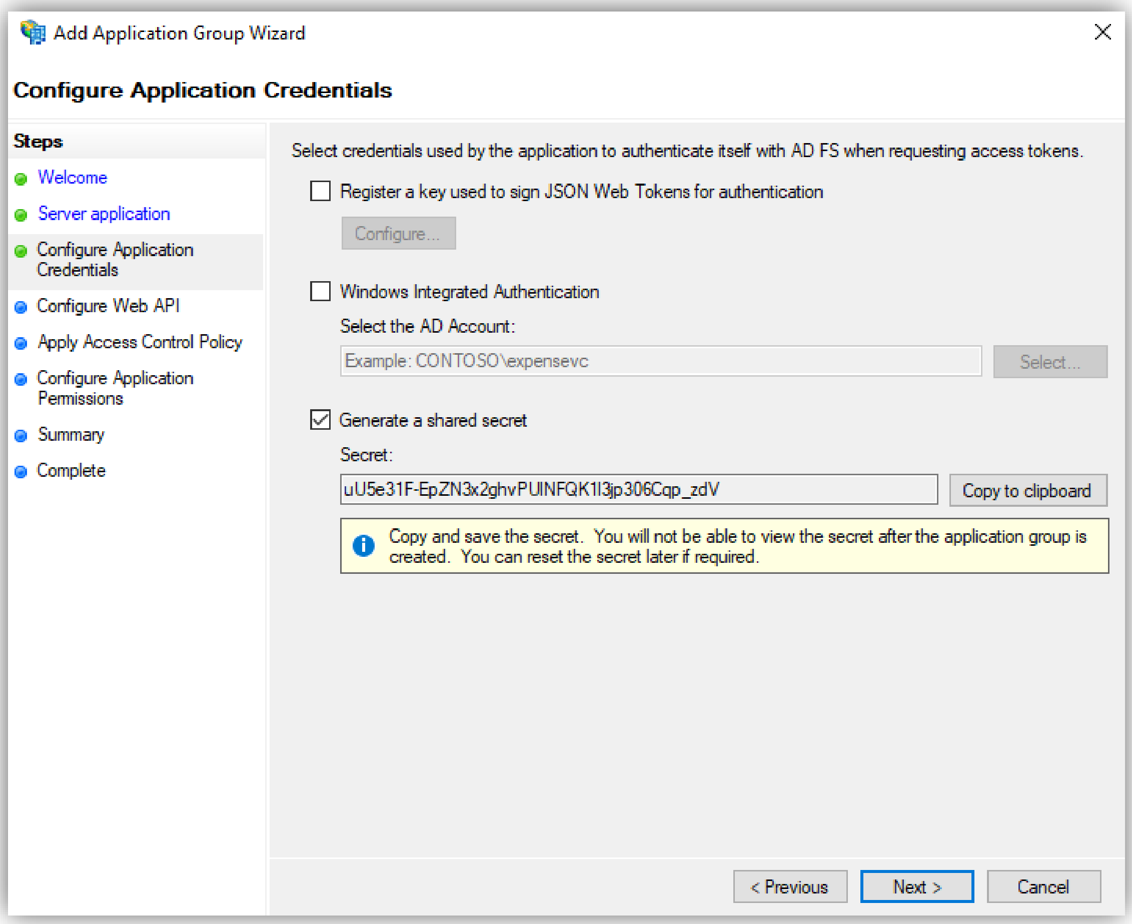
The URL for receiving logout details from ADFS must have the following format:

```
[RC backend URL]/Api/Authentication/Logout
```

e.g. http://ResourceCentral.com/Api/Authentication/Logout

then click [**OK**] to proceed.

5. On the next screen (*Configure Application Credentials*), check on “**Generate a shared secret**” and click “**Copy to clipboard**” save the *client secret*.



Add Application Group Wizard

Configure Application Credentials

Select credentials used by the application to authenticate itself with AD FS when requesting access tokens.

□ Register a key used to sign JSON Web Tokens for authentication

□ Windows Integrated Authentication

Select the AD Account: Example: CONTOSO\expensevc

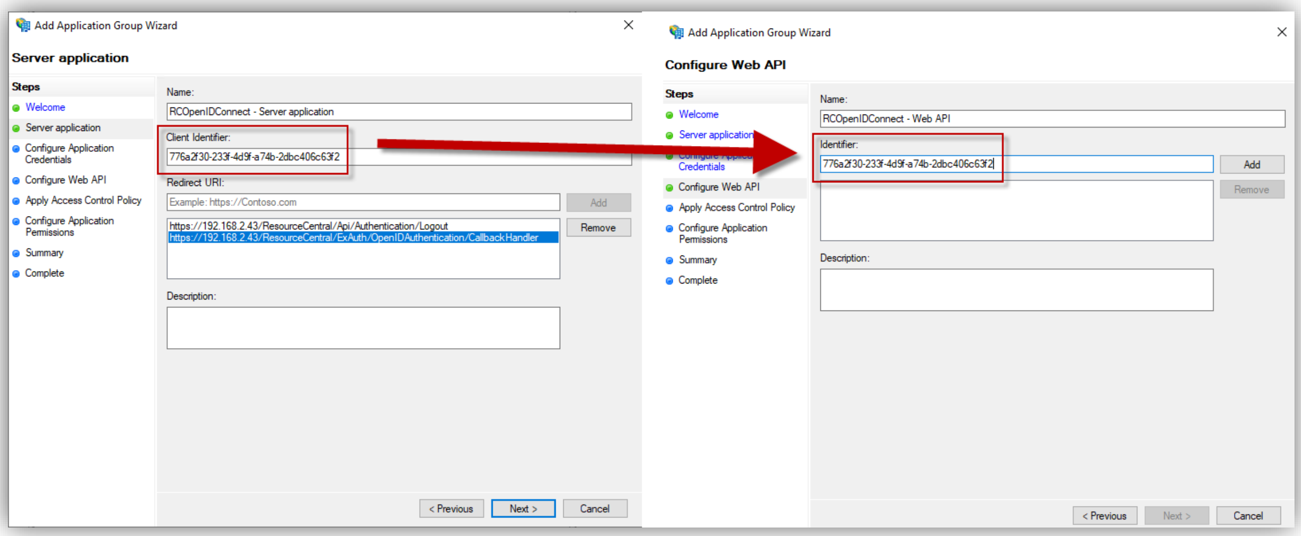
☑ Generate a shared secret

Secret: uU5e31F-EpZN3x2ghvPUINFQK1l3jp306Cqp_zdV

Copy and save the secret. You will not be able to view the secret after the application group is created. You can reset the secret later if required.

Then click [**Next**] to proceed.

6. On *Configure Web API* screen, fill in “**Identifier**” (which is Client Id in Step 4 of this section) and click [**Add**] button.


Add Application Group Wizard
Server application
Steps
Welcome
Server application
Configure Application Credentials
Configure Web API
Apply Access Control Policy
Configure Application Permissions
Summary
Complete
Add
Remove
< Previous
Next >
Cancel
Add Application Group Wizard
Configure Web API
Steps
Welcome
Server application
Configure Application Credentials
Configure Web API
Apply Access Control Policy
Configure Application Permissions
Summary
Complete
Add
Remove
< Previous
Next >
Cancel

Name: RCOpenIDConnect - Server application

Client Identifier: 776a2f30-233f-4d9f-a74b-2dbc406c63f2

Redirect URI: Example: https://Contoso.com

https://192.168.2.43/ResourceCentral/Api/Authentication/Logout
https://192.168.2.43/ResourceCentral/ExAuth/OpenIDAuthentication/CallbackHandler

Description:

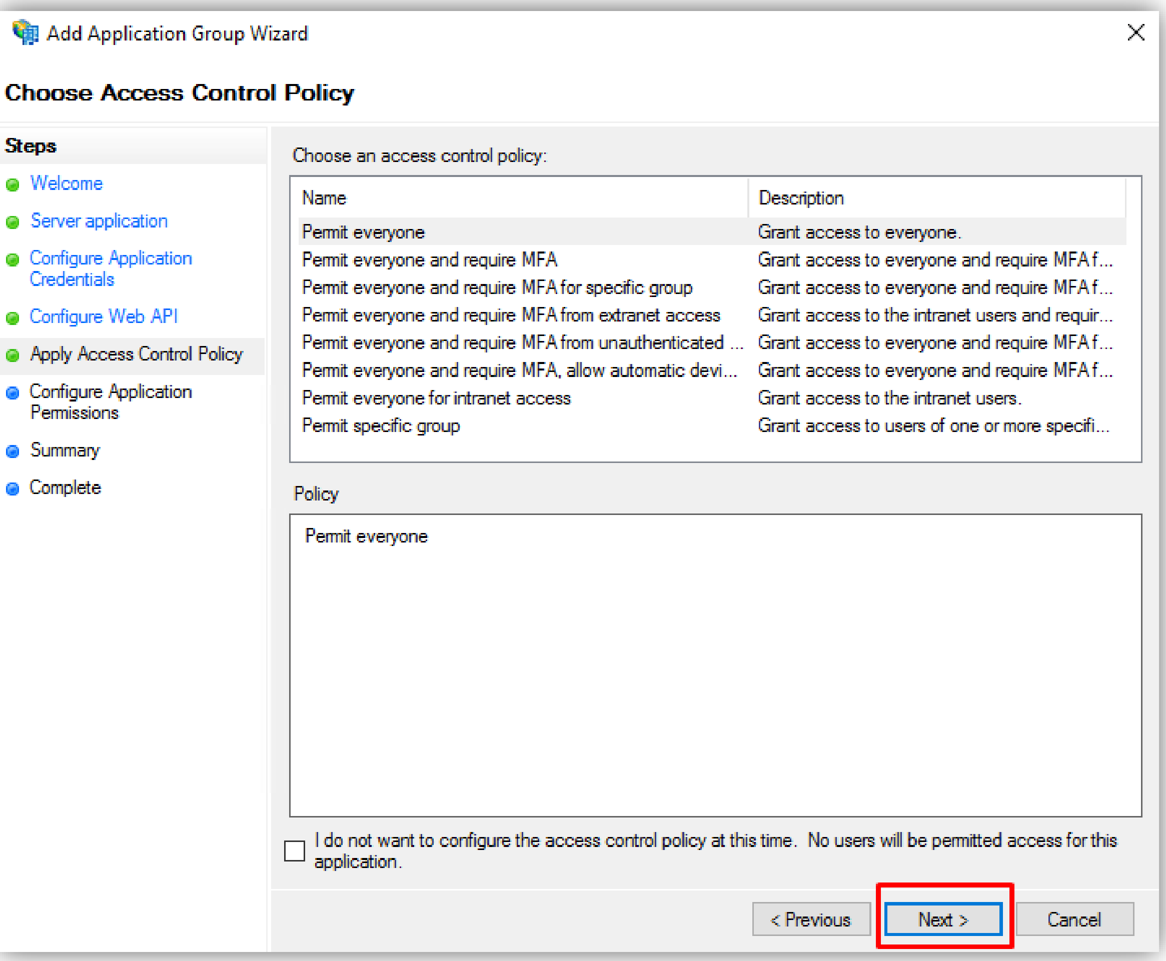
Name: RCOpenIDConnect - Web API

Identifier: 776a2f30-233f-4d9f-a74b-2dbc406c63f2

Description:

Then click [**Next]** to proceed.

7. Click [**Next**] on **Choose Access Control Policy** screen.


Add Application Group Wizard
Choose Access Control Policy
Steps
Welcome
Server application
Configure Application Credentials
Configure Web API
Apply Access Control Policy
Configure Application Permissions
Summary
Complete
< Previous
Next >
Cancel

Choose an access control policy:

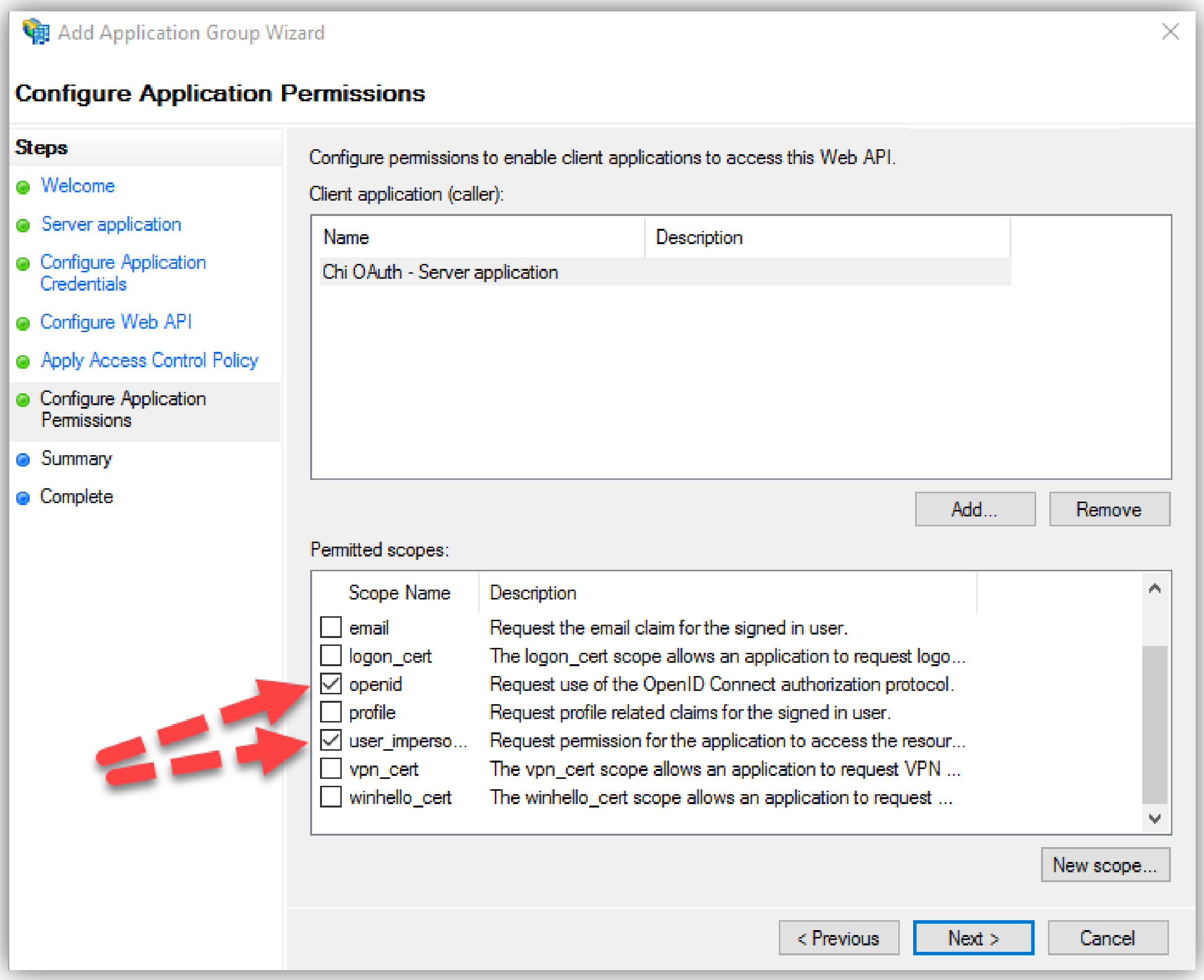
Name	Description
Permit everyone	Grant access to everyone.
Permit everyone and require MFA	Grant access to everyone and require MFA f...
Permit everyone and require MFA for specific group	Grant access to everyone and require MFA f...
Permit everyone and require MFA from extranet access	Grant access to the intranet users and requir...
Permit everyone and require MFA from unauthenticated ...	Grant access to everyone and require MFA f...
Permit everyone and require MFA, allow automatic devi...	Grant access to everyone and require MFA f...
Permit everyone for intranet access	Grant access to the intranet users.
Permit specific group	Grant access to users of one or more specifi...

Policy

Permit everyone

☐ I do not want to configure the access control policy at this time. No users will be permitted access for this application.

8. On *Configure Application Permissions* screen, check on **openid** and **user_impersonate** checkboxes.



Add Application Group Wizard

Configure Application Permissions

Steps
Welcome
Server application
Configure Application Credentials
Configure Web API
Apply Access Control Policy
Configure Application Permissions
Summary
Complete

Configure permissions to enable client applications to access this Web API.

Client application (caller):

Name	Description
Chi OAuth - Server application	

Permitted scopes:

	Scope Name	Description
□	email	Request the email claim for the signed in user.
□	logon_cert	The logon_cert scope allows an application to request logo...
☑	openid	Request use of the OpenID Connect authorization protocol.
□	profile	Request profile related claims for the signed in user.
☑	user_imperso...	Request permission for the application to access the resour...
□	vpn_cert	The vpn_cert scope allows an application to request VPN ...
□	winhello_cert	The winhello_cert scope allows an application to request ...

Click [**Next**] proceed.

9. Click [**Next**] on **Summary** screen and click [**Close**] on **Complete** screen to finish.

NOTE: If, in the system, there are users who have User Principal Name different from SMTP address, we need to add claim to retrieve all email addresses. Please refer to this appendix for more details.

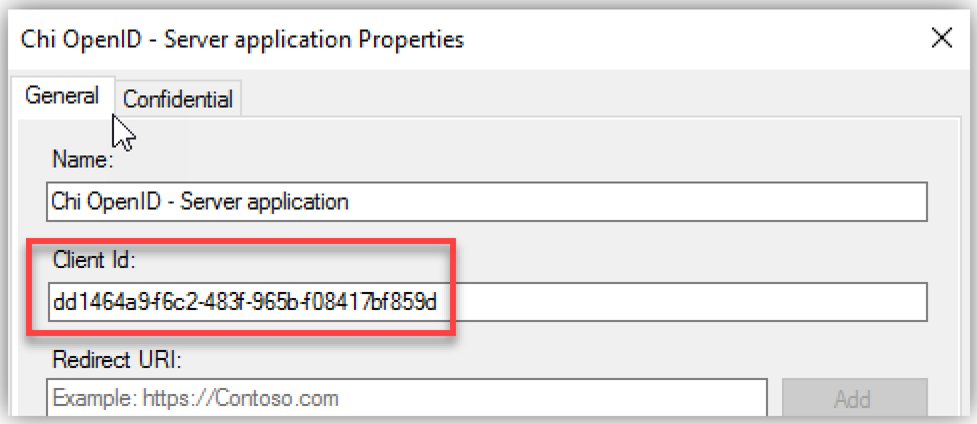
Part B. Retrieve details for OpenID Connect with AD FS Authentication Protocol

Reply URL

Refer to this section for more details.

Client Id

The **Client Id** can be retrieved from **Step 4** in Part A of this protocol.



Chi OpenID - Server application Properties

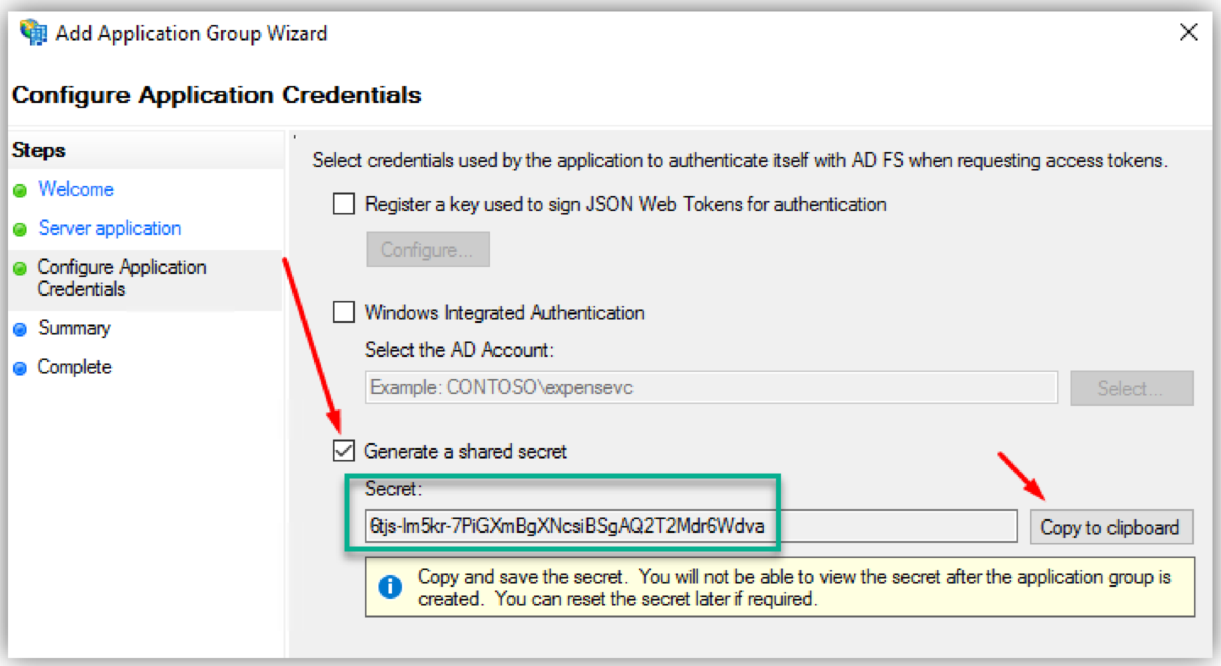
Name: Chi OpenID - Server application

Client Id: dd1464a9-f6c2-483f-965b-f08417bf859d

Redirect URI: Example: https://Contoso.com

Client Secret

The **Client Secret** can be retrieved from **Step 5** in Part A of this protocol (highlighted in Green).



Add Application Group Wizard

Configure Application Credentials

Steps
- Welcome
- Server application
- Configure Application Credentials
- Summary
- Complete

Select credentials used by the application to authenticate itself with AD FS when requesting access tokens.

☐ Register a key used to sign JSON Web Tokens for authentication

☐ Windows Integrated Authentication

Select the AD Account: Example: CONTOSO\expensevc

☑ Generate a shared secret

Secret: 6tjs-lm5kr-7PiGXmBgXNcsiBSgAQ2T2Mdr6Wdva

Copy and save the secret. You will not be able to view the secret after the application group is created. You can reset the secret later if required.

Authorization URL, Token URL and Logout URL

Refer to this section for more details.

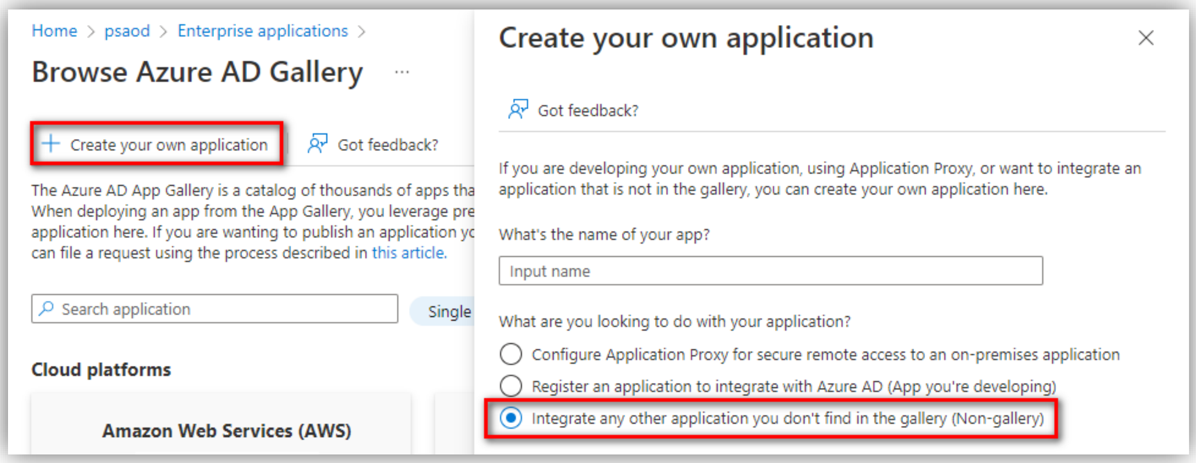
Auto-Login Networks

Refer to this section for more details.

Authentication Details for SAML2

Part A. Register application in Azure AD

Go to **Azure portal → Azure Active Directory → Enterprise applications →** Click [**New application**] which opens 'Browse Azure AD Gallery' screen. Then click [**Create your own application**]



Home > psaod > Enterprise applications >

Browse Azure AD Gallery ...

+ Create your own application | Got feedback?

The Azure AD App Gallery is a catalog of thousands of apps tha When deploying an app from the App Gallery, you leverage pre application here. If you are wanting to publish an application yc can file a request using the process described in this article.

Search application | Single

Cloud platforms

Amazon Web Services (AWS)

Create your own application ×

Got feedback?

If you are developing your own application, using Application Proxy, or want to integrate an application that is not in the gallery, you can create your own application here.

What's the name of your app?

Input name

What are you looking to do with your application?

○ Configure Application Proxy for secure remote access to an on-premises application
○ Register an application to integrate with Azure AD (App you're developing)
● Integrate any other application you don't find in the gallery (Non-gallery)

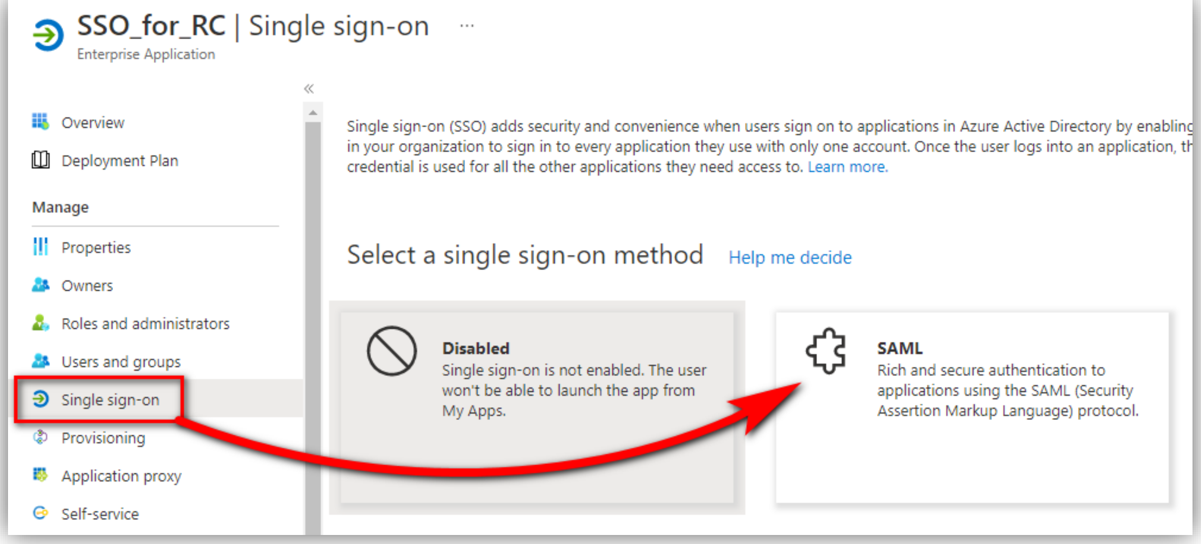
Figure 15. Add non-gallery application

Enter the name of your app, select the 3rd option - '*Intergrate any other application you don't find in the gallery*'. Then click [**Create**] button at the bottom of the screen.

Part B. Retrieve details for SAML2 Authentication Protocol

Identifier (Entity ID)

Go to **Azure portal → Azure Active Directory → Enterprise applications.** Click [**View all applications**] then select the app that you registered in Part A to see its details. Click [**Single sign-on**] → SAML



SSO_for_RC | Single sign-on ...
Enterprise Application

Overview
Deployment Plan
Manage
Properties
Owners
Roles and administrators
Users and groups
Single sign-on
Provisioning
Application proxy
Self-service

Single sign-on (SSO) adds security and convenience when users sign on to applications in Azure Active Directory by enabling in your organization to sign in to every application they use with only one account. Once the user logs into an application, th credential is used for all the other applications they need access to. Learn more.

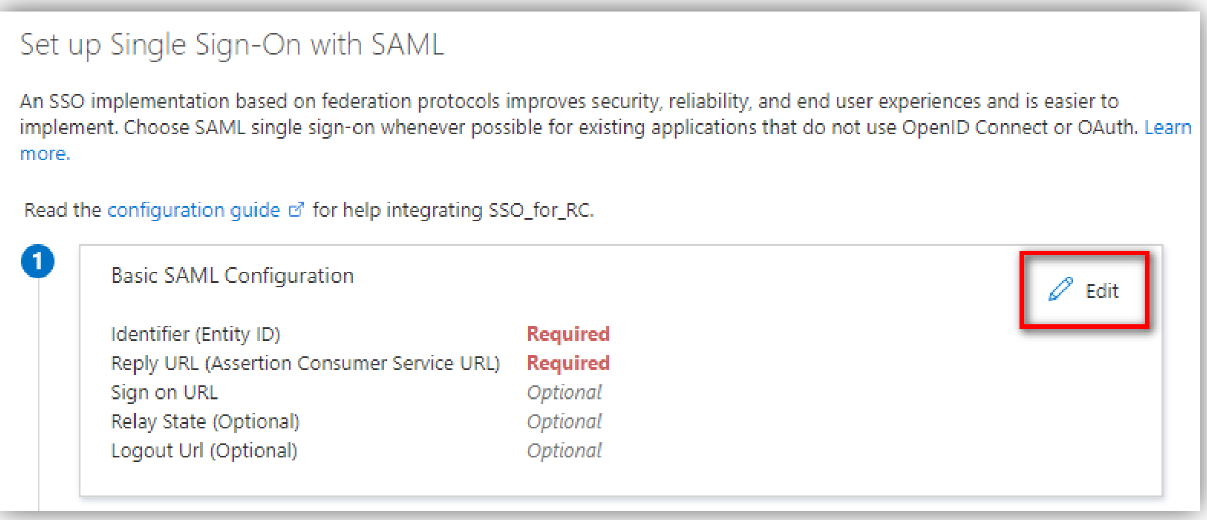
Select a single sign-on method Help me decide

Disabled
Single sign-on is not enabled. The user won't be able to launch the app from My Apps.

SAML
Rich and secure authentication to applications using the SAML (Security Assertion Markup Language) protocol.

Figure 16. Select SSO method

A new panel is opened.



Set up Single Sign-On with SAML

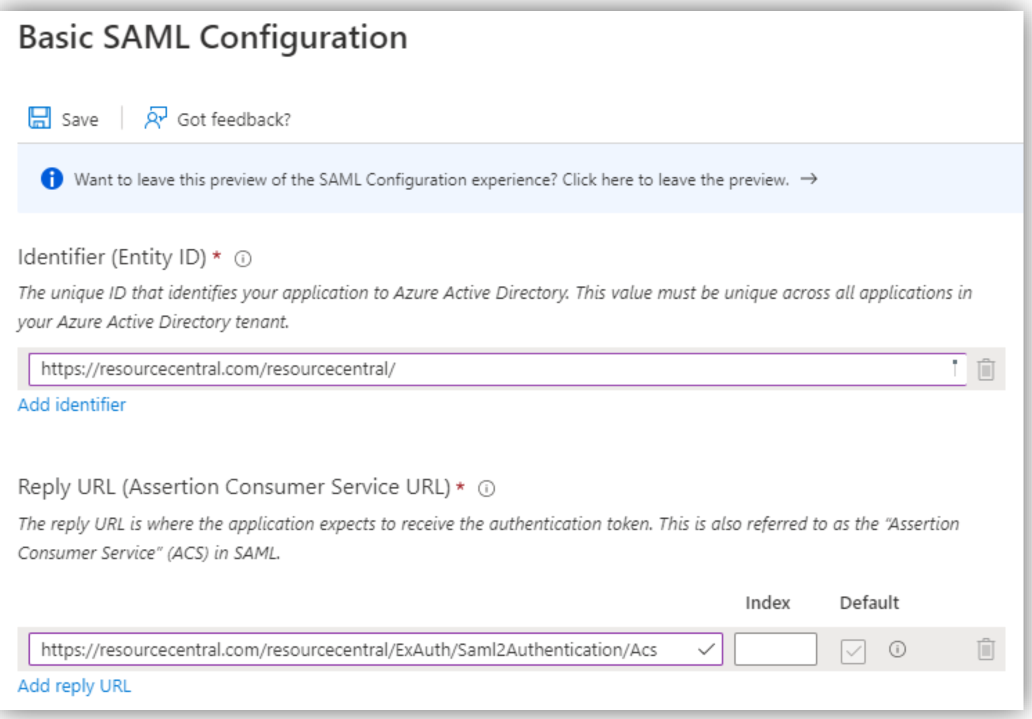
An SSO implementation based on federation protocols improves security, reliability, and end user experiences and is easier to implement. Choose SAML single sign-on whenever possible for existing applications that do not use OpenID Connect or OAuth. Learn more.

Read the configuration guide for help integrating SSO_for_RC.

1 Basic SAML Configuration

Identifier (Entity ID)	Required
Reply URL (Assertion Consumer Service URL)	Required
Sign on URL	Optional
Relay State (Optional)	Optional
Logout Url (Optional)	Optional

Now click the [**Edit**] button on the **Basic SAML Configuration** section. A new panel shows up on the right side of the screen:



Basic SAML Configuration

Want to leave this preview of the SAML Configuration experience? Click here to leave the preview. →

Identifier (Entity ID) *

The unique ID that identifies your application to Azure Active Directory. This value must be unique across all applications in your Azure Active Directory tenant.

https://resourcecentral.com/resourcecentral/

Reply URL (Assertion Consumer Service URL) *

The reply URL is where the application expects to receive the authentication token. This is also referred to as the "Assertion Consumer Service" (ACS) in SAML.

	Index	Default
https://resourcecentral.com/resourcecentral/ExAuth/Saml2Authentication/Acs		☑

For **Identifier (Entity ID)**, enter the URL of RC backend.

For **Reply URL**, it can be composed with the following format:

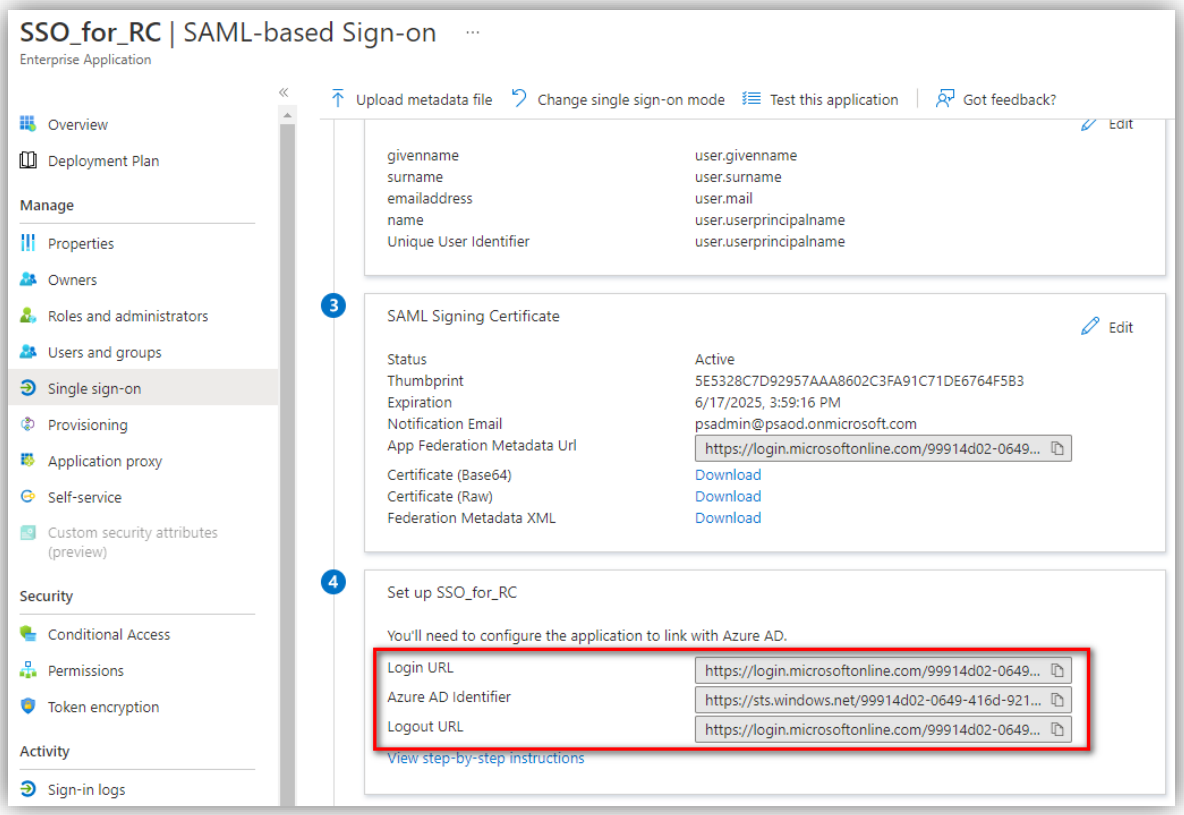
```
[RC Backend URL]/ExAuth/Saml2Authentication/Acs
```

In the above example, the RC Backend URL is https://resourcecentral.com/resourcecentral, so the Reply URL you can fill in is: https://resourcecentral.com/resourcecentral/ExAuth/Saml2Authentication/Acs

Click [**Save**] to finish.

Login URL, Logout URL and Azure AD Identifier

Go to **Azure portal → Azure Active Directory → Enterprise applications → All applications**. Then select the app that you registered in Part A to see its details.
Click [**Single sign-on**] and scroll down to the **Set up [App name]** section (i.e., 'Set up SSO_for_RC'):



SSO_for_RC | SAML-based Sign-on ...
Enterprise Application

givenname user.givenname
surname user.surname
emailaddress user.mail
name user.userprincipalname
Unique User Identifier user.userprincipalname

SAML Signing Certificate

Status Active
Thumbprint 5E5328C7D92957AAA8602C3FA91C71DE6764F5B3
Expiration 6/17/2025, 3:59:16 PM
Notification Email psadmin@psaod.onmicrosoft.com
App Federation Metadata Url https://login.microsoftonline.com/99914d02-0649...
Certificate (Base64) Download
Certificate (Raw) Download
Federation Metadata XML Download

Set up SSO_for_RC

You'll need to configure the application to link with Azure AD.

Login URL https://login.microsoftonline.com/99914d02-0649...
Azure AD Identifier https://sts.windows.net/99914d02-0649-416d-921...
Logout URL https://login.microsoftonline.com/99914d02-0649...

View step-by-step instructions

Figure 17. Set up application

You can see the details for **Login URL**, **Logout URL**, and **Azure AD Identifier** highlighted in the above figure.

Return URL

You can compose the **Return URL** with the following format:

```
[RC Backend URL]/ExAuth/Saml2Authentication/CallbackHandler
```

In the above example, the RC Backend URL is https://resourcecentral.com/resourcecentral, so the Reply URL you can fill in is:
https://resourcecentral.com/resourcecentral/ExAuth/Saml2Authentication/CallbackHandler

Certificate (.pfx) and PFX Password

Usually you have been provided with the .pfx file and the attached password after you buy the certificate (with key). This certificate must be created with the parameter provider = **Microsoft Enhanced RSA and AES Cryptographic Provider.**

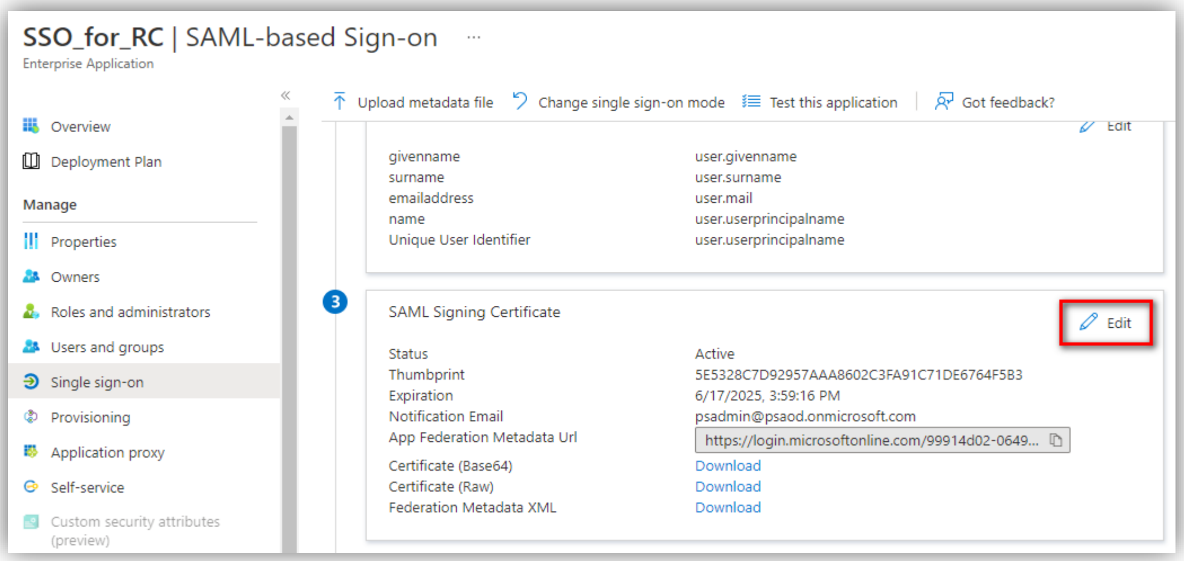
Auto-Login Networks

Refer to this section for more details.

Part C. Configure SAML Signing Certificate

Go to **Azure portal → Azure Active Directory → Enterprise applications → All applications** then select the app that you registered in Part A to see its details.

Click [**Single sign-on**] and scroll down to the '**SAML Signing Certificate**' then click [**Edit**]:



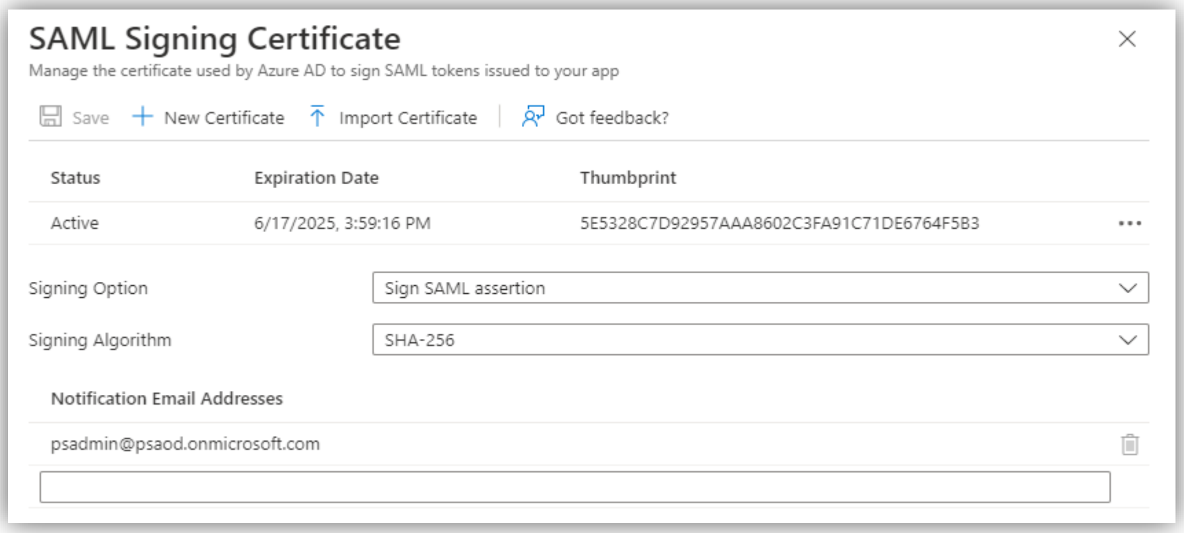
SSO_for_RC | SAML-based Sign-on
Enterprise Application

givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.userprincipalname
Unique User Identifier	user.userprincipalname

SAML Signing Certificate

Status	Active
Thumbprint	5E5328C7D92957AAA8602C3FA91C71DE6764F5B3
Expiration	6/17/2025, 3:59:16 PM
Notification Email	psadmin@psaod.onmicrosoft.com
App Federation Metadata Url	https://login.microsoftonline.com/99914d02-0649...
Certificate (Base64)	Download
Certificate (Raw)	Download
Federation Metadata XML	Download

A new panel is opened.



SAML Signing Certificate
Manage the certificate used by Azure AD to sign SAML tokens issued to your app

Status	Expiration Date	Thumbprint
Active	6/17/2025, 3:59:16 PM	5E5328C7D92957AAA8602C3FA91C71DE6764F5B3

Signing Option: Sign SAML assertion

Signing Algorithm: SHA-256

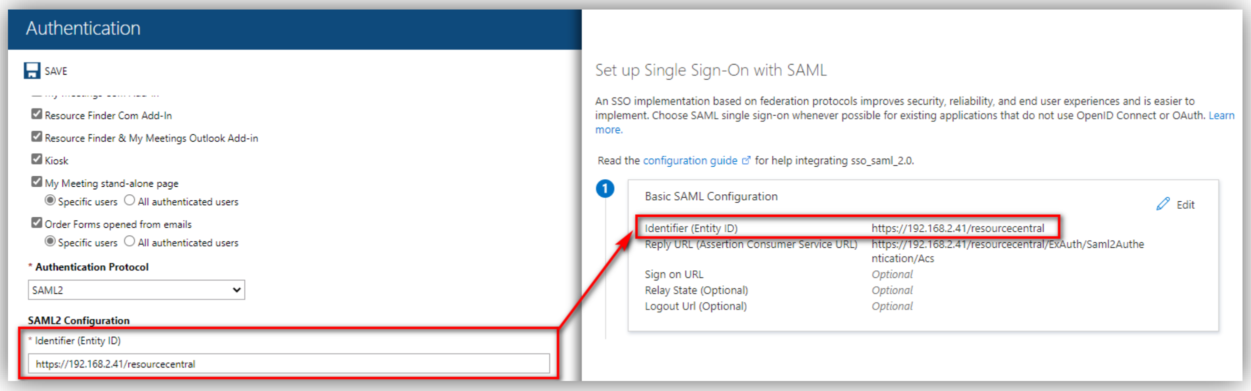
Notification Email Addresses

psadmin@psaod.onmicrosoft.com

Click **[Import certificate]** to upload your PFX file.

Part D. Configure External Authentication in the RC backend

Log in to **RC backend**, and click **[Authentication]** on the left menu. On ‘External Authentication’ section, select **SAML2** for ‘Authentication Protocol’ then configure as shown in the following figures:



Authentication

SAVE

☑ Resource Finder Com Add-In
☑ Resource Finder & My Meetings Outlook Add-in
☑ Kiosk
☑ My Meeting stand-alone page
● Specific users ○ All authenticated users
☑ Order Forms opened from emails
● Specific users ○ All authenticated users

* **Authentication Protocol**
SAML2

SAML2 Configuration
* Identifier (Entity ID)
https://192.168.2.41/resourcecentral

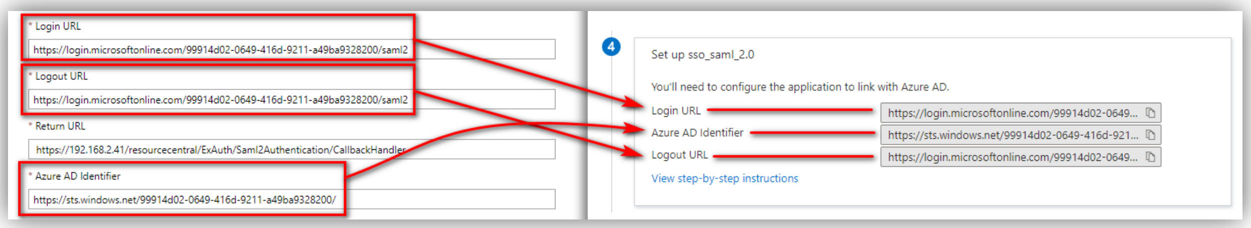
Set up Single Sign-On with SAML

An SSO implementation based on federation protocols improves security, reliability, and end user experiences and is easier to implement. Choose SAML single sign-on whenever possible for existing applications that do not use OpenID Connect or OAuth. Learn more.

Read the configuration guide for help integrating sso_saml_2.0.

1 Basic SAML Configuration — Edit

Identifier (Entity ID)	https://192.168.2.41/resourcecentral
Reply URL (Assertion Consumer Service URL)	https://192.168.2.41/resourcecentral/ExAuth/Saml2Authentication/Acs
Sign on URL	*Optional*
Relay State (Optional)	*Optional*
Logout Url (Optional)	*Optional*



* Login URL
https://login.microsoftonline.com/99914d02-0649-416d-9211-a49ba9328200/saml2

* Logout URL
https://login.microsoftonline.com/99914d02-0649-416d-9211-a49ba9328200/saml2

* Return URL
https://192.168.2.41/resourcecentral/ExAuth/Saml2Authentication/CallbackHandler

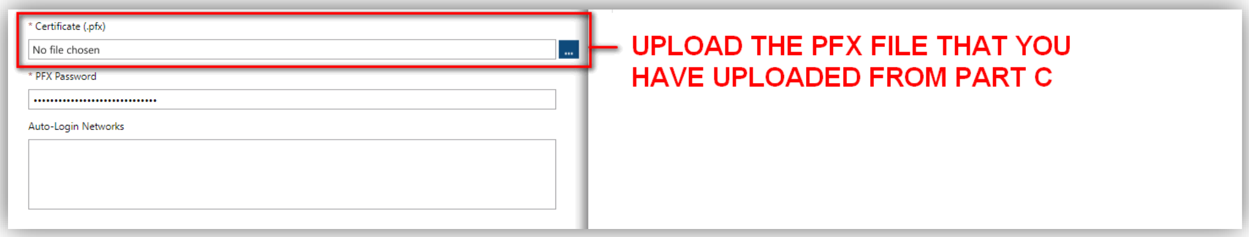
* Azure AD Identifier
https://sts.windows.net/99914d02-0649-416d-9211-a49ba9328200/

4 Set up sso_saml_2.0

You'll need to configure the application to link with Azure AD.

Login URL	https://login.microsoftonline.com/99914d02-0649...
Azure AD Identifier	https://sts.windows.net/99914d02-0649-416d-921...
Logout URL	https://login.microsoftonline.com/99914d02-0649...

View step-by-step instructions



* Certificate (.pfx)
No file chosen

* PFX Password
••••••••••••••••••••••••••••••••

Auto-Login Networks

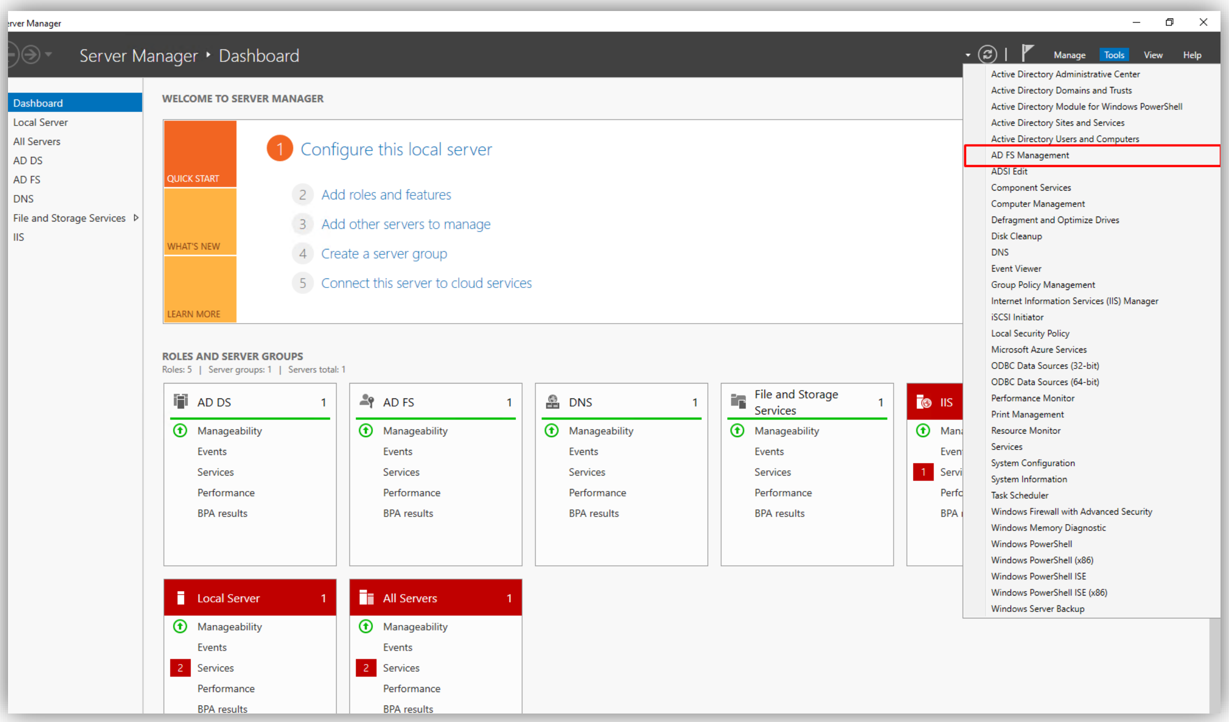
UPLOAD THE PFX FILE THAT YOU HAVE UPLOADED FROM PART C

Authentication Details for SAML2 with ADFS

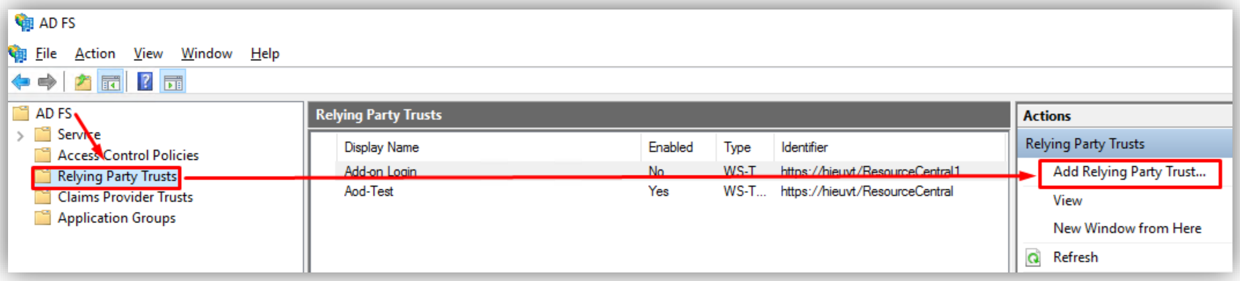
The SAML2 with AD FS protocol has the same code flow as that of SAML2. Therefore, authentication details for SAML2 with AD FS can be input to the data fields of SAML2 protocol.

Part A1. Configure Active Directory Federation Services (ADFS)

1. Go to **web server** where your Exchange server is installed, click **Start → Server Manager → Tools → AD FS Management**


Server Manager
Server Manager ‣ Dashboard
Manage
Tools
View
Help
Dashboard
Local Server
All Servers
AD DS
AD FS
DNS
File and Storage Services
IIS
WELCOME TO SERVER MANAGER
QUICK START
WHAT'S NEW
LEARN MORE
1 Configure this local server
2 Add roles and features
3 Add other servers to manage
4 Create a server group
5 Connect this server to cloud services
ROLES AND SERVER GROUPS
Roles: 5 | Server groups: 1 | Servers total: 1
AD DS 1
AD FS 1
DNS 1
File and Storage Services 1
IIS
Manageability
Events
Services
Performance
BPA results
Local Server 1
All Servers 1
Active Directory Administrative Center
Active Directory Domains and Trusts
Active Directory Module for Windows PowerShell
Active Directory Sites and Services
Active Directory Users and Computers
AD FS Management
ADSI Edit
Component Services
Computer Management
Defragment and Optimize Drives
Disk Cleanup
DNS
Event Viewer
Group Policy Management
Internet Information Services (IIS) Manager
iSCSI Initiator
Local Security Policy
Microsoft Azure Services
ODBC Data Sources (32-bit)
ODBC Data Sources (64-bit)
Performance Monitor
Print Management
Resource Monitor
Services
System Configuration
System Information
Task Scheduler
Windows Firewall with Advanced Security
Windows Memory Diagnostic
Windows PowerShell
Windows PowerShell (x86)
Windows PowerShell ISE
Windows PowerShell ISE (x86)
Windows Server Backup

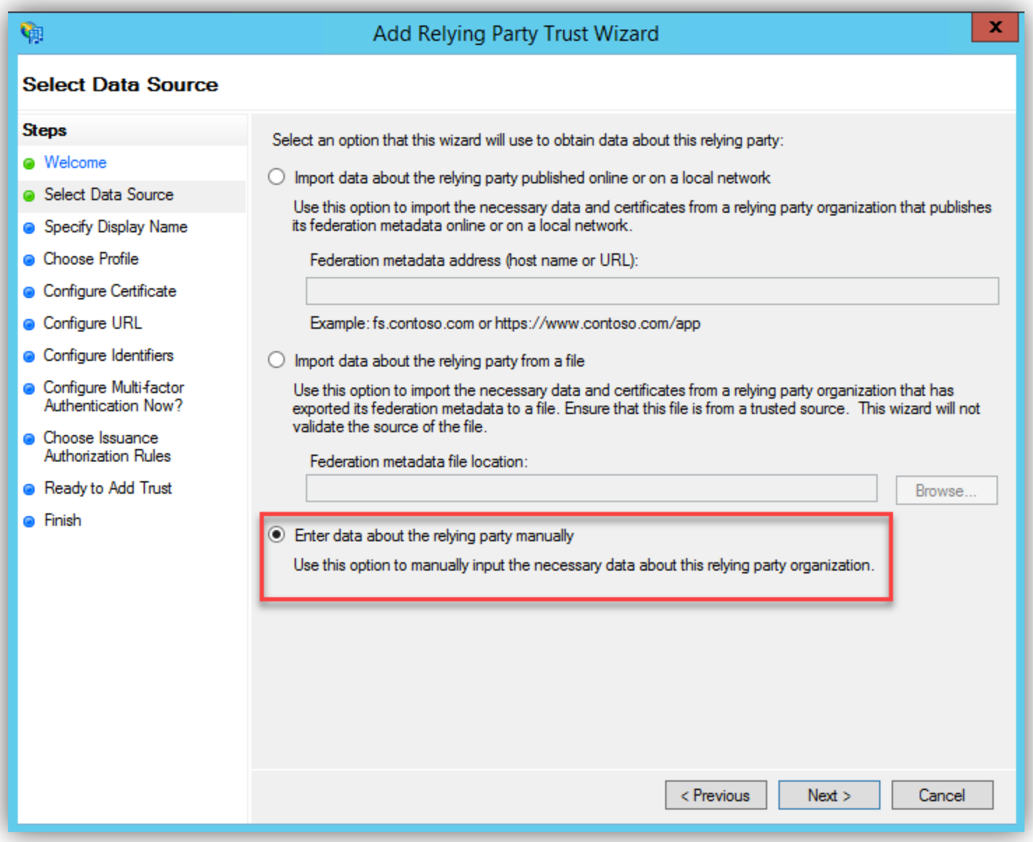
2. In the opened window, select **Replying Party Trusts** and [**Add Replying Party Trust...**] from the **Actions** sidebar. This starts the configuration wizard for a new **Replying Party Trust**.



Display Name	Enabled	Type	Identifier
Add-on Login	No	WS-T...	https://hieuvt/ResourceCentral1
Aod-Test	Yes	WS-T...	https://hieuvt/ResourceCentral

3. On the 'Add Replying Party Trust wizard' → **Welcome** screen, select Claims aware, then click [Start].

4. In the Select Data Source screen, select option **Enter Data About the Party Manually**.



Add Relying Party Trust Wizard

Select Data Source

Steps
- Welcome
- Select Data Source
- Specify Display Name
- Choose Profile
- Configure Certificate
- Configure URL
- Configure Identifiers
- Configure Multi-factor Authentication Now?
- Choose Issuance Authorization Rules
- 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.

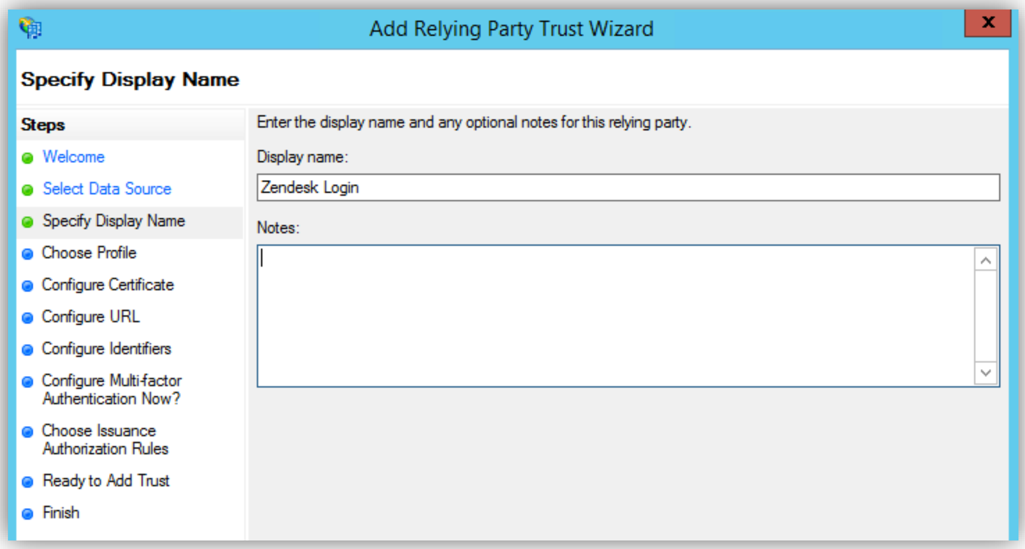
Federation metadata file location:

● Enter data about the relying party manually

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

Then click [**Next**] to proceed.

5. On the next screen, enter a **Display name** that you'll recognize in the future, and any notes you want to make. Then click [**Next**] to proceed.



Add Relying Party Trust Wizard

Specify Display Name

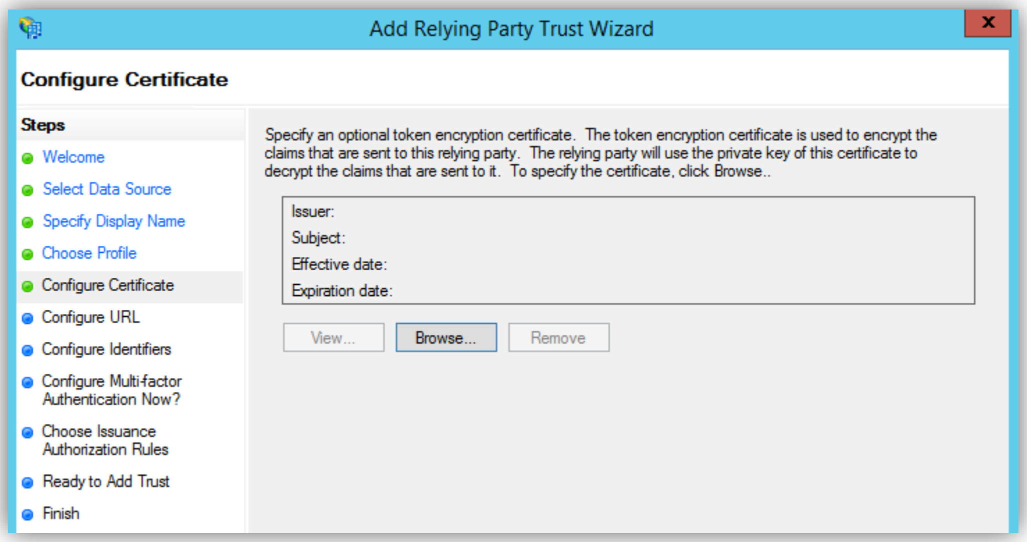
Steps
- Welcome
- Select Data Source
- Specify Display Name
- Choose Profile
- Configure Certificate
- Configure URL
- Configure Identifiers
- Configure Multi-factor Authentication Now?
- Choose Issuance Authorization Rules
- Ready to Add Trust
- Finish

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

Display name: Zendesk Login

Notes:

6. On the next screen, leave the certificate settings at their defaults. Then click [**Next**] to proceed.

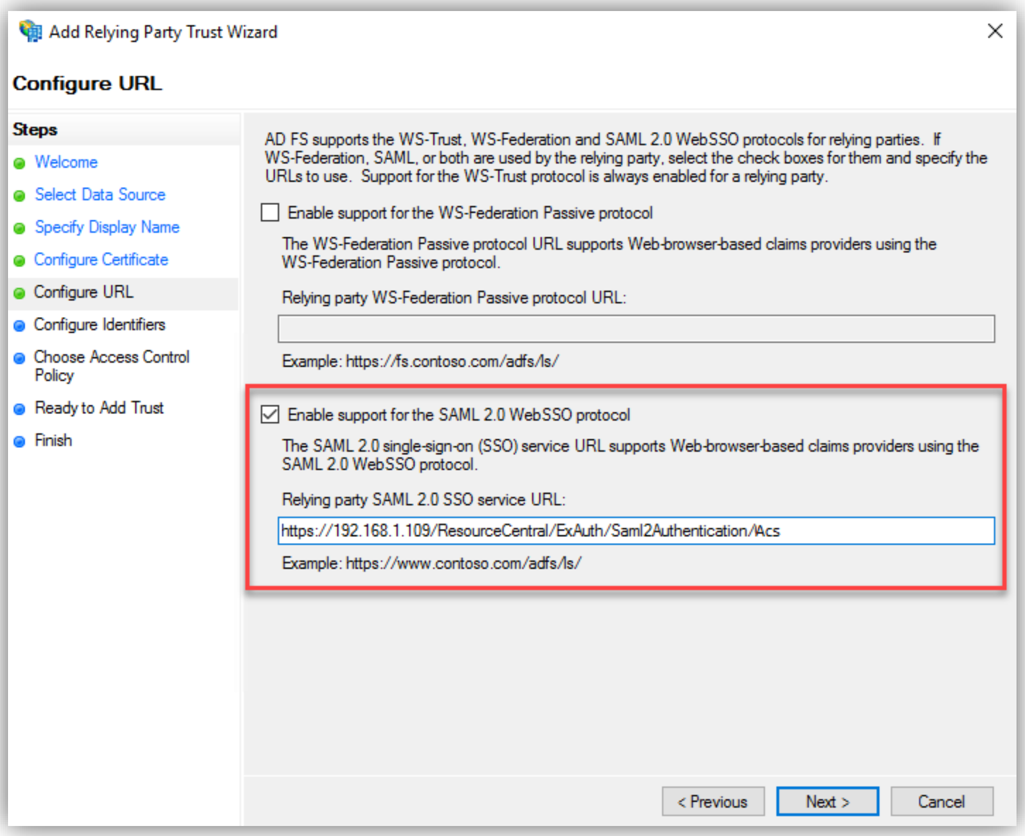


Specify an optional token encryption certificate. The token encryption certificate is used to encrypt the claims that are sent to this relying party. The relying party will use the private key of this certificate to decrypt the claims that are sent to it. To specify the certificate, click Browse..

Issuer:
Subject:
Effective date:
Expiration date:

7. On the next screen, check on **Enable Support for the SAML 2.0 WebSSO** protocol. The service URL will have the following format:

Error! Hyperlink reference not valid.



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.

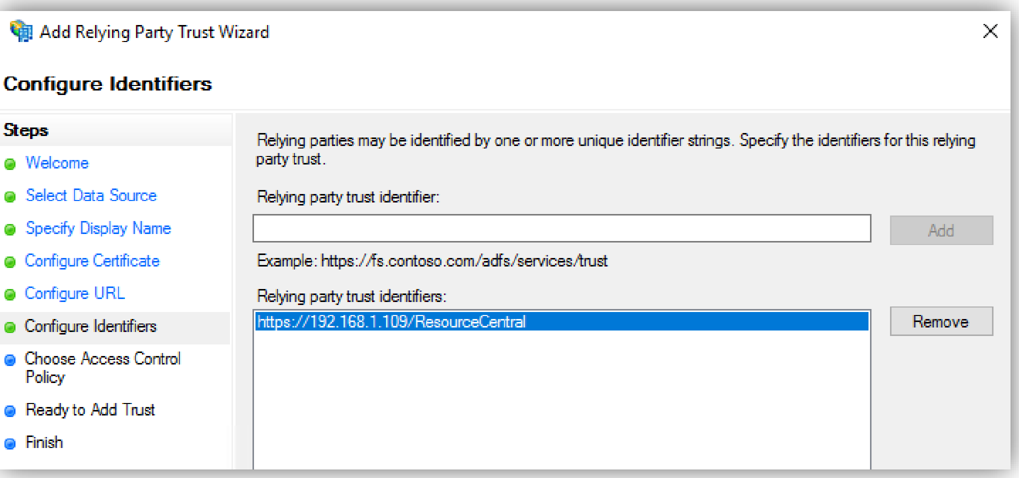
Relying party SAML 2.0 SSO service URL:

https://192.168.1.109/ResourceCentral/ExAuth/Saml2Authentication/Acs

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

Then click [**Next**] to proceed.

8. On the next screen, add a **Relying party trust identifier**, you can compose the link with the following format:
   Error! Hyperlink reference not valid.



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:

https://192.168.1.109/ResourceCentral

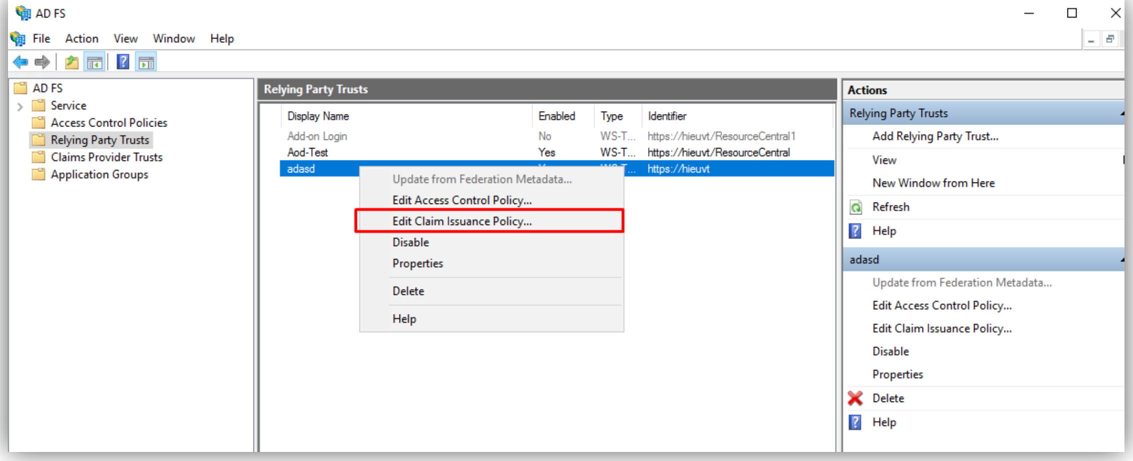
Then click [**Next**] to proceed.

9. On the **Choose Access Control Policy** screen, leave it as it is and click [**Next**].
10. On the **Ready to Add Trust** screen, leave it as it is and click [**Next**].
11. On the **Finish** screen, click [**Close**] to finish.

Part A2. Create Claim Rules

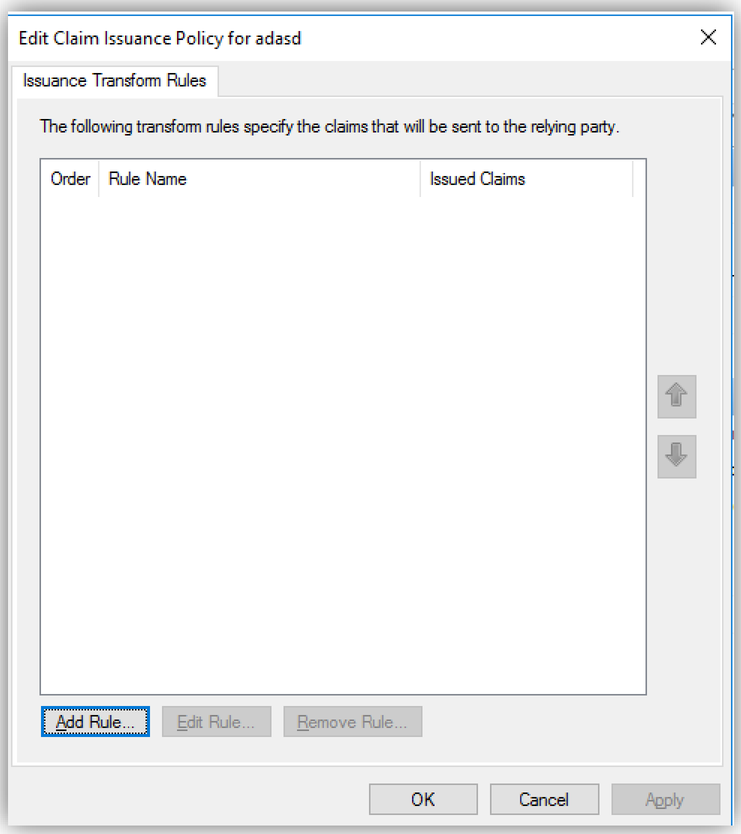
Once the relying party trust has been created, you can create the claim rules and update the RPT with minor changes that aren't set by the wizard. By default the claim rule editor opens once you created the trust. If you want to map additional values beyond authentication.

Select a newly created **Relying Party Trust**, right click and choose **Edit Claim Issuance Policy…** from the context menu (or Actions sidebar).



Display Name	Enabled	Type	Identifier
Add-on Login	No	WS-T...	https://hieuvt/ResourceCentral1
Aod-Test	Yes	WS-T...	https://hieuvt/ResourceCentral
adasd	Y	WS-T...	https://hieuvt

This starts the configuration wizard for a new claim.



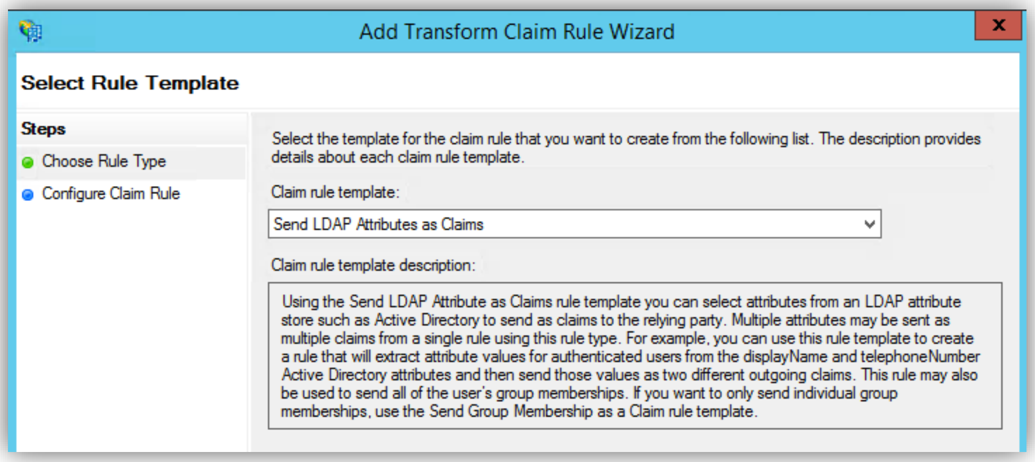
Edit Claim Issuance Policy for adasd

Issuance Transform Rules

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

Order	Rule Name	Issued Claims

1. To create a new rule, click on **Add Rule**. Create a **Send LDAP Attributes as Claims** rule.



Add Transform Claim Rule Wizard

Select Rule Template

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: Send LDAP Attributes as Claims

Claim rule template description:

Using the Send LDAP Attribute as Claims rule template you can select attributes from an LDAP attribute store such as Active Directory to send as claims to the relying party. Multiple attributes may be sent as multiple claims from a single rule using this rule type. For example, you can use this rule template to create a rule that will extract attribute values for authenticated users from the displayName and telephoneNumber Active Directory attributes and then send those values as two different outgoing claims. This rule may also be used to send all of the user's group memberships. If you want to only send individual group memberships, use the Send Group Membership as a Claim rule template.

2. On the next screen, using **Active Directory** as your attribute store, do the following:

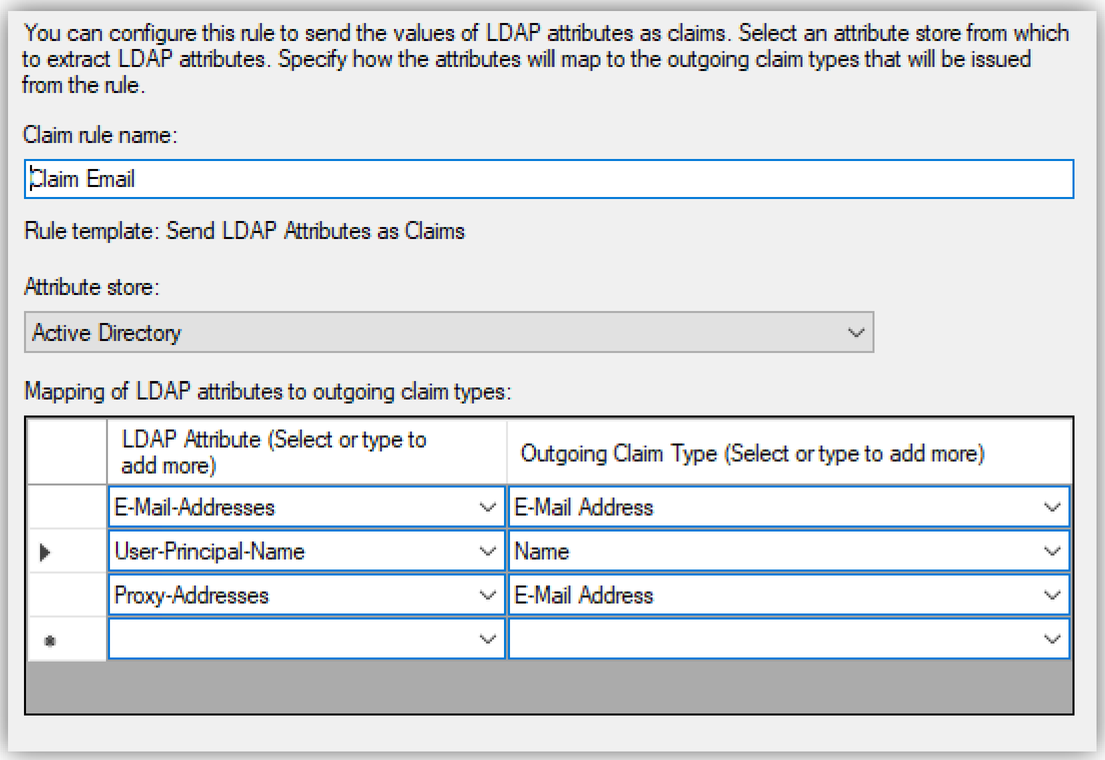
Line 1:
a. From the LDAP Attribute column, select **E-Mail-Addresses**.
b. From the Outgoing Claim Type, select **E-Mail Address**.

Line 2:
a. From the LDAP Attribute column, select **User-Principal-Name**.
b. From the Outgoing Claim Type, select Name.

Line 3:

a. From the LDAP Attribute column, select **Proxy-Addresses**.

b. From the Outgoing Claim Type, select **E-Mail Address**.



You can configure this rule to send the values of LDAP attributes as claims. Select an attribute store from which to extract LDAP attributes. Specify how the attributes will map to the outgoing claim types that will be issued from the rule.

Claim rule name:

Claim Email

Rule template: Send LDAP Attributes as Claims

Attribute store:

Active Directory

Mapping of LDAP attributes to outgoing claim types:

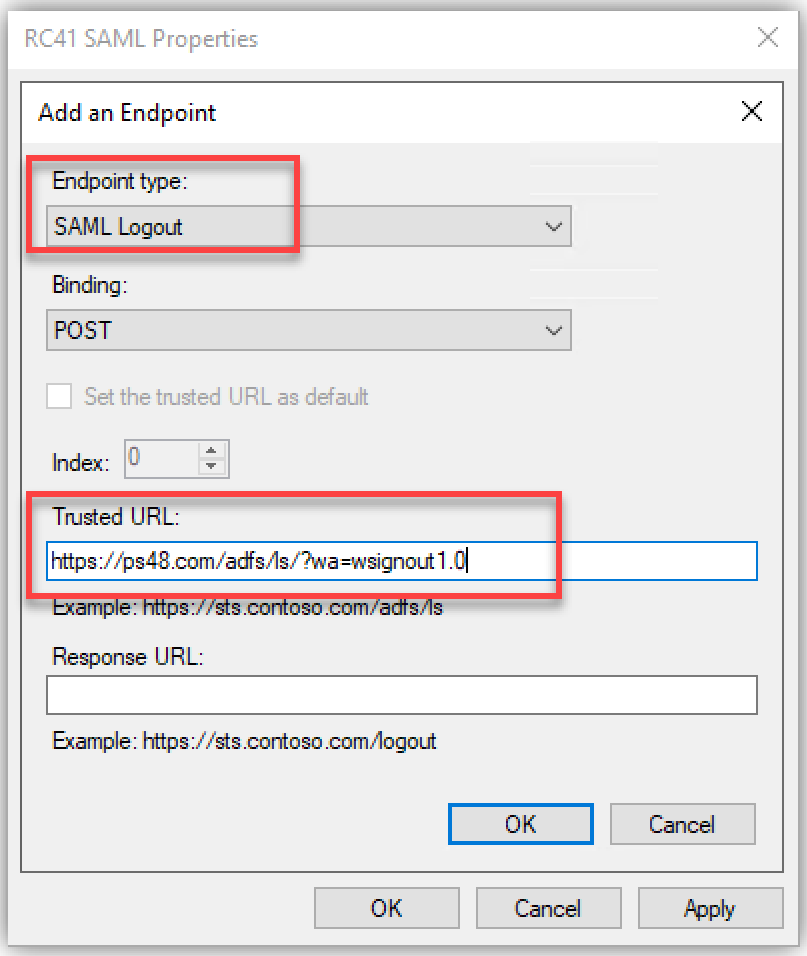
	LDAP Attribute (Select or type to add more)	Outgoing Claim Type (Select or type to add more)
	E-Mail-Addresses	E-Mail Address
▶	User-Principal-Name	Name
	Proxy-Addresses	E-Mail Address
*		

Click [OK] to finish.

Part A3. Adjust the trust settings

You still need to adjust a few settings on your relying party trust. To access these settings, select **Properties** from the **Actions** sidebar while you have the **Replying Party Trusts** (RPT) selected.

1. In the **Endpoints** tab, click on **add SAML** to add a new endpoint.



RC41 SAML Properties

Add an Endpoint

Endpoint type: SAML Logout

Binding: POST

□ Set the trusted URL as default

Index: 0

Trusted URL: https://ps48.com/adfs/ls/?wa=wsignout1.0

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

Response URL:

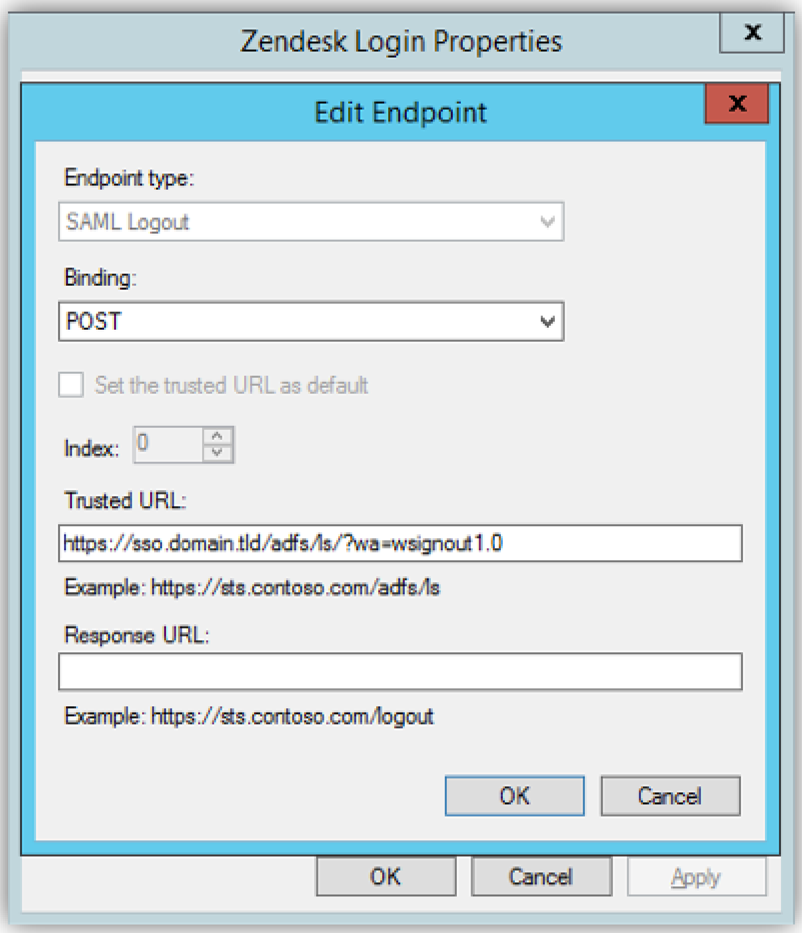
Example: https://sts.contoso.com/logout

For the **Endpoint type**, select **SAML Logout**.
For the **Binding**, select **POST**
For the **Trusted URL**, create URL using:

  a. The web address of your ADFS server
  b. The ADFS SAML endpoint you noted earlier
  c. The string '?wa=wsignout1.0'

The URL should look something like this: https://sso.yourdomain.tld/adfs/ls/?wa=wsignout1.0

2. Confirm you changes by clicking OK on the endpoint and the RPT properties. You should now have a working RPT for RC.



Endpoint type: SAML Logout

Binding: POST

□ Set the trusted URL as default

Index: 0

Trusted URL: https://sso.domain.tld/adfs/ls/?wa=wsignout1.0

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

Response URL:

Example: https://sts.contoso.com/logout

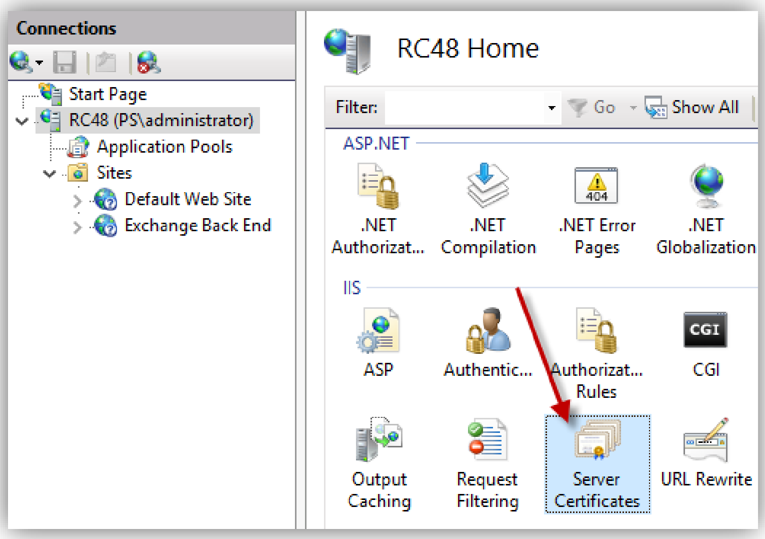
Part A4. Import Certificate on AD FS Server

Usually, you have been provided with the .pfx file and the attached password after you buy the certificate (with key). This certificate must be created with the parameter provider = **Microsoft Enhanced RSA and AES Cryptographic Provider.**

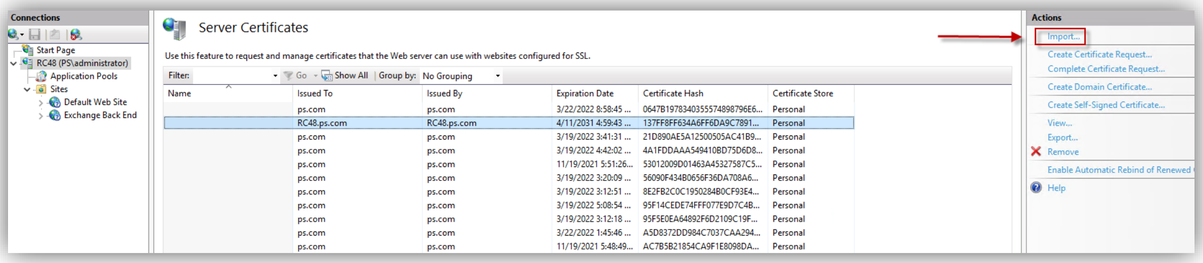
Now you need to import the certificate on IIS on AD DS Server. Follow these steps:

1. Copy PFX file into AD DS server machine.

2. Open IIS on AD DS server machine, double click [**Server Certificates**]:



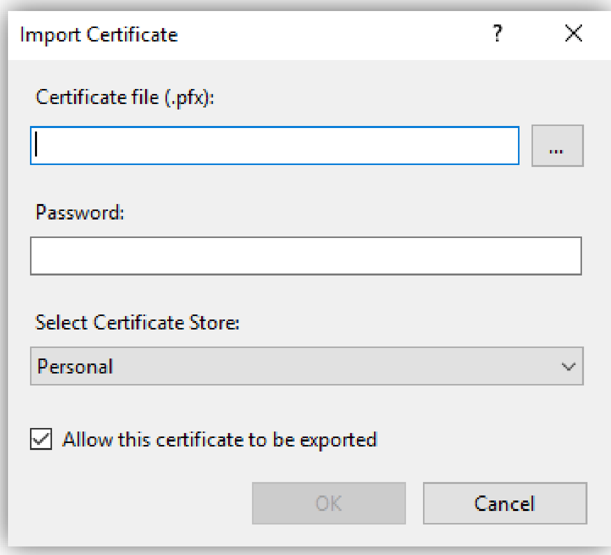
3. On the list of server certificates, click [Import] on the right panel of the screen:



Use this feature to request and manage certificates that the Web server can use with websites configured for SSL.

Name	Issued To	Issued By	Expiration Date	Certificate Hash	Certificate Store
	ps.com	ps.com	3/22/2022 8:58:45 ...	0647B19783403555748987 96E6...	Personal
	RC48.ps.com	RC48.ps.com	4/11/2031 4:59:43 ...	137FF8FF634A6FF6DA9C7891...	Personal
	ps.com	ps.com	3/19/2022 3:41:31 ...	21D890AE5A12500505AC41B9...	Personal
	ps.com	ps.com	3/19/2022 4:42:02 ...	4A1FDDAAA549410BD75D6D8...	Personal
	ps.com	ps.com	11/19/2021 5:51:26...	53012009D01463A45327587C5...	Personal
	ps.com	ps.com	3/19/2022 3:20:09 ...	56090F434B0656F36DA708A6...	Personal
	ps.com	ps.com	3/19/2022 3:12:51 ...	8E2FB2C0C1950284B0CF93E4...	Personal
	ps.com	ps.com	3/19/2022 5:08:54 ...	95F14CEDE74FFF077E9D7C4B...	Personal
	ps.com	ps.com	3/19/2022 3:12:18 ...	95F5E0EA64892F6D2109C19F...	Personal
	ps.com	ps.com	3/22/2022 1:45:46 ...	A5D8372DD984C7037CAA294...	Personal
	ps.com	ps.com	11/19/2021 5:48:49...	AC7B5B21854CA9F1E8098DA...	Personal

4. On the pop-up dialogue, browse to the Certificate file and input provided password:



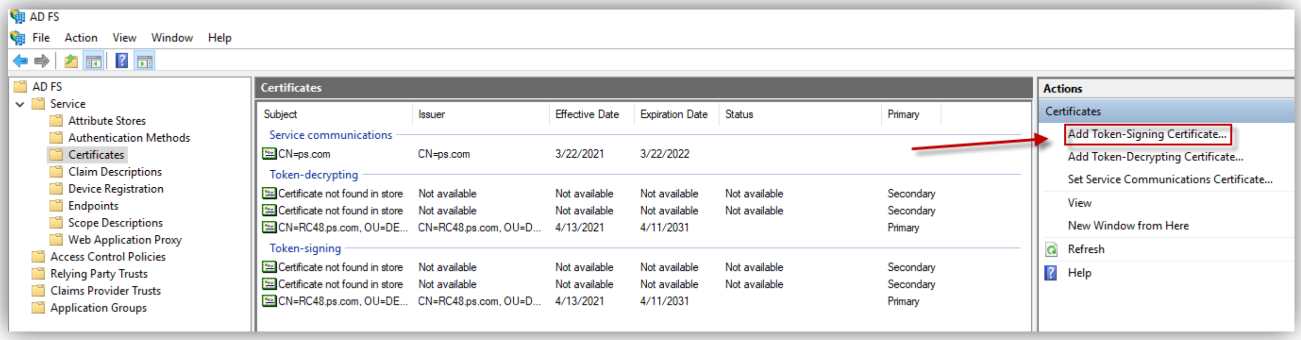
Certificate file (.pfx):

Password:

Select Certificate Store:
Personal

☑ Allow this certificate to be exported

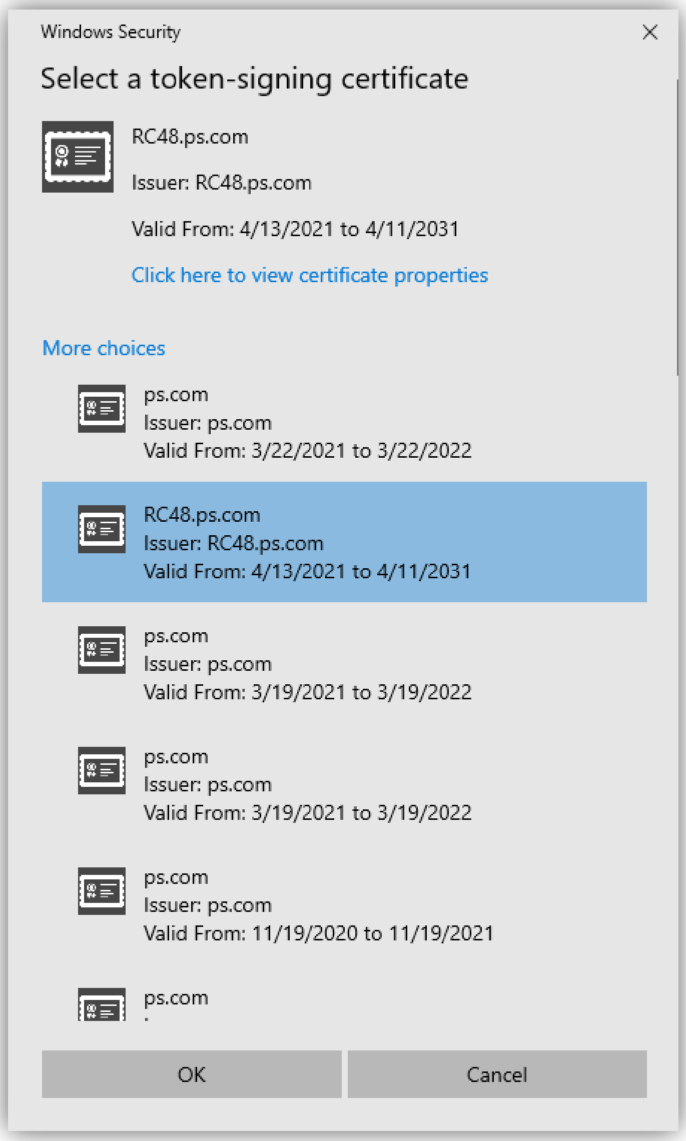
5. Open AD FS Management, select [Certificate] → Add Token Signing Certificate…



Certificates

Subject	Issuer	Effective Date	Expiration Date	Status	Primary
Service communications					
CN=ps.com	CN=ps.com	3/22/2021	3/22/2022		
Token-decrypting					
Certificate not found in store	Not available	Not available	Not available	Not available	Secondary
Certificate not found in store	Not available	Not available	Not available	Not available	Secondary
CN=RC48.ps.com, OU=DE...	CN=RC48.ps.com, OU=D...	4/13/2021	4/11/2031		Primary
Token-signing					
Certificate not found in store	Not available	Not available	Not available	Not available	Secondary
Certificate not found in store	Not available	Not available	Not available	Not available	Secondary
CN=RC48.ps.com, OU=DE...	CN=RC48.ps.com, OU=D...	4/13/2021	4/11/2031		Primary

6. A dialogue shows up as shown in the following figure:



Select a token-signing certificate

RC48.ps.com

Issuer: RC48.ps.com

Valid From: 4/13/2021 to 4/11/2031

Click here to view certificate properties

More choices

ps.com
Issuer: ps.com
Valid From: 3/22/2021 to 3/22/2022

RC48.ps.com
Issuer: RC48.ps.com
Valid From: 4/13/2021 to 4/11/2031

ps.com
Issuer: ps.com
Valid From: 3/19/2021 to 3/19/2022

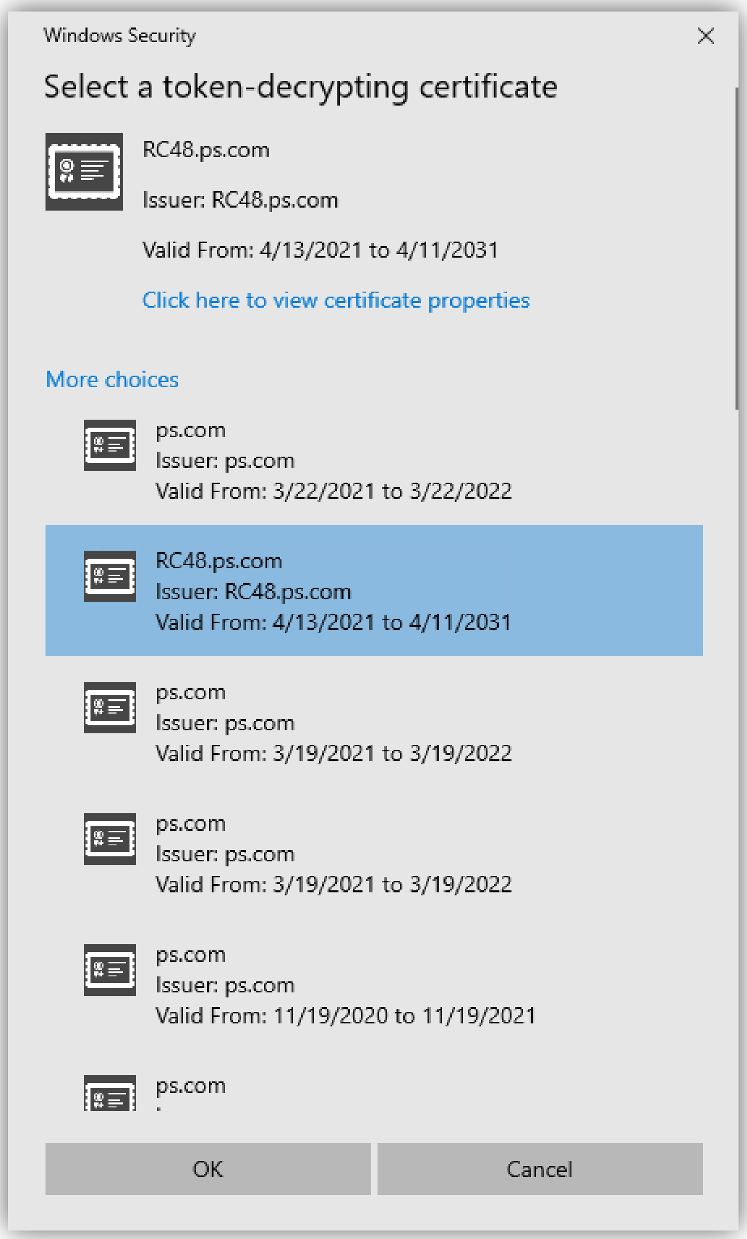
ps.com
Issuer: ps.com
Valid From: 3/19/2021 to 3/19/2022

ps.com
Issuer: ps.com
Valid From: 11/19/2020 to 11/19/2021

ps.com

Click **More choices** and select the certificate that you have imported in the previous step. Click [**OK**].

7. Going back to the main screen, select **Add Token-decrypting Certificate…** (under **Add Token Signing Certificate…** button).



Windows Security

Select a token-decrypting certificate

RC48.ps.com

Issuer: RC48.ps.com

Valid From: 4/13/2021 to 4/11/2031

Click here to view certificate properties

More choices

ps.com
Issuer: ps.com
Valid From: 3/22/2021 to 3/22/2022

RC48.ps.com
Issuer: RC48.ps.com
Valid From: 4/13/2021 to 4/11/2031

ps.com
Issuer: ps.com
Valid From: 3/19/2021 to 3/19/2022

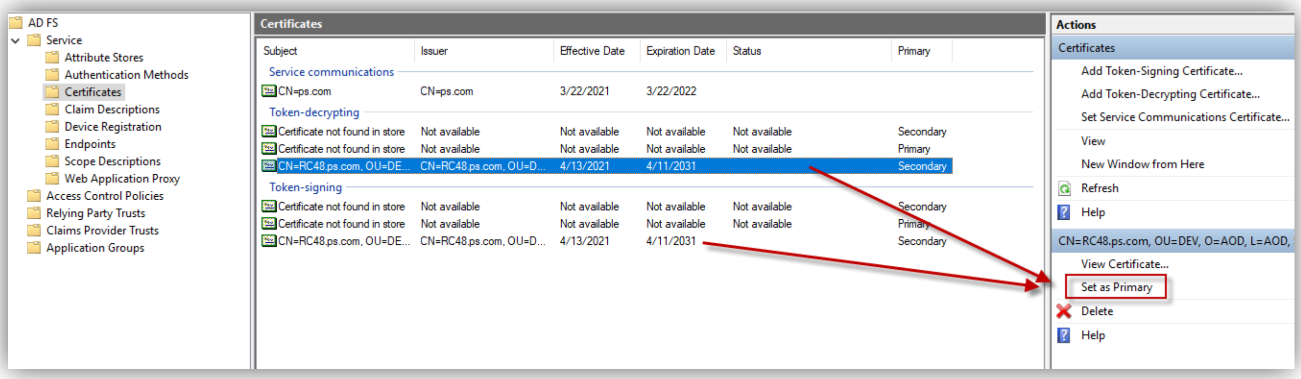
ps.com
Issuer: ps.com
Valid From: 3/19/2021 to 3/19/2022

ps.com
Issuer: ps.com
Valid From: 11/19/2020 to 11/19/2021

ps.com

Select the imported certificate and lick [**OK**] to finish.

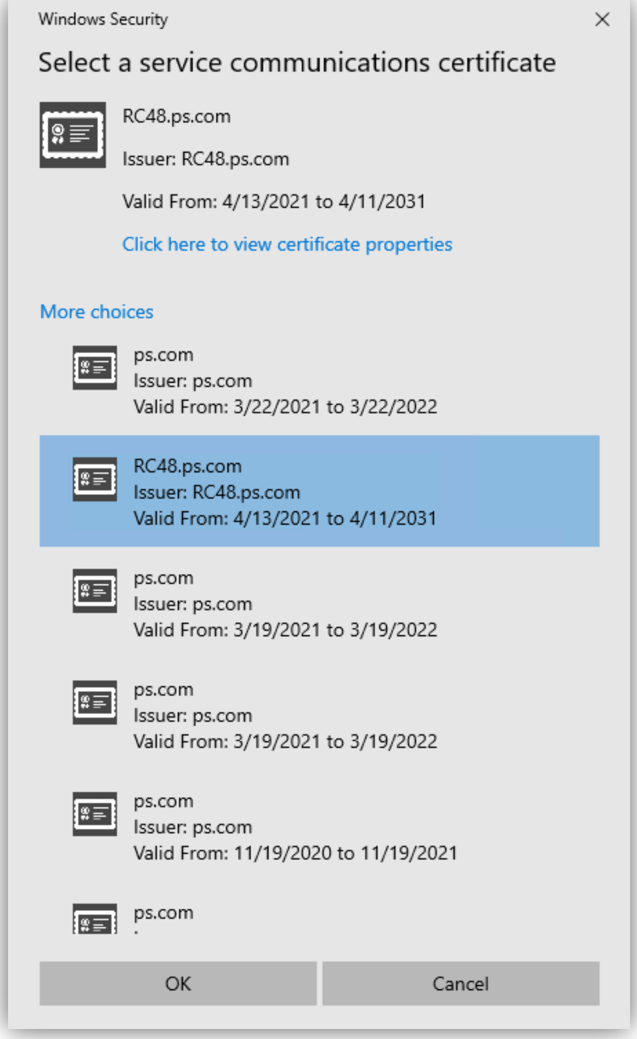
8. Click on the certificates in 2 sections (Token-decrypting and Token-signing) one after another and set it as Primary:



Certificates

Subject	Issuer	Effective Date	Expiration Date	Status	Primary
Service communications					
CN=ps.com	CN=ps.com	3/22/2021	3/22/2022		
Token-decrypting					
Certificate not found in store	Not available	Not available	Not available	Not available	Secondary
Certificate not found in store	Not available	Not available	Not available	Not available	Primary
CN=RC48.ps.com, OU=DE...	CN=RC48.ps.com, OU=D...	4/13/2021	4/11/2031		Secondary
Token-signing					
Certificate not found in store	Not available	Not available	Not available	Not available	Secondary
Certificate not found in store	Not available	Not available	Not available	Not available	Primary
CN=RC48.ps.com, OU=DE...	CN=RC48.ps.com, OU=D...	4/13/2021	4/11/2031		Secondary

9. On the main screen, select the primary certificate (that you have just set) in **Token-decrypting** section and click **Set Service Communications Certificate…,** a dialogue shows up:



Select a service communications certificate

RC48.ps.com
Issuer: RC48.ps.com
Valid From: 4/13/2021 to 4/11/2031

ps.com
Issuer: ps.com
Valid From: 3/22/2021 to 3/22/2022

RC48.ps.com
Issuer: RC48.ps.com
Valid From: 4/13/2021 to 4/11/2031

ps.com
Issuer: ps.com
Valid From: 3/19/2021 to 3/19/2022

ps.com
Issuer: ps.com
Valid From: 3/19/2021 to 3/19/2022

ps.com
Issuer: ps.com
Valid From: 11/19/2020 to 11/19/2021

ps.com

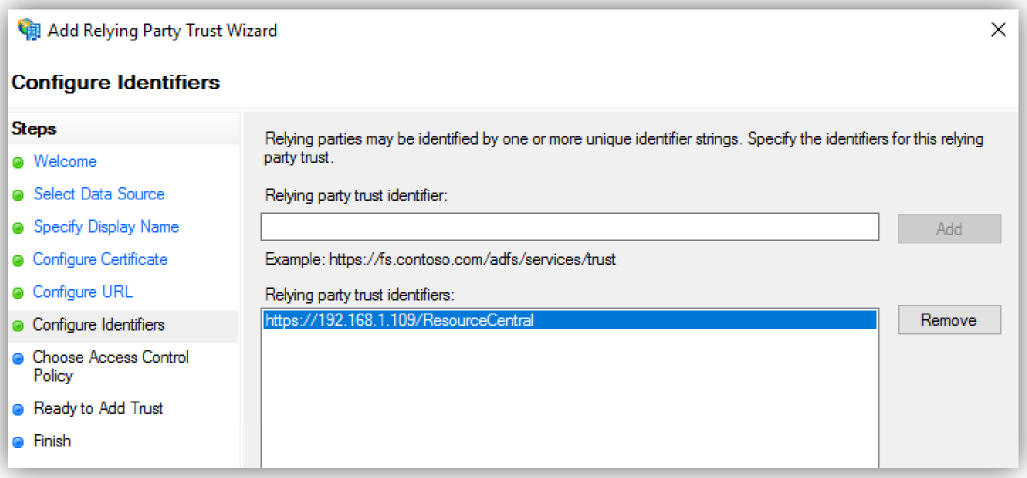
Click **More choices**, select the imported certificate and click [**OK**].

10. On the main screen, this time select the primary certificate (that you have just set) in **Token-signing** section and click **Set Service Communications Certificate…,** a dialogue shows up. Follow the procedure in step 9 to finish.

Part B. Retrieve details for SAML2 with ADFS Authentication Protocol

Identifier (Entity ID)

Identifier is the value of **Replying party trust identifier** in **Step 8**, Part A1 of this protocol.



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

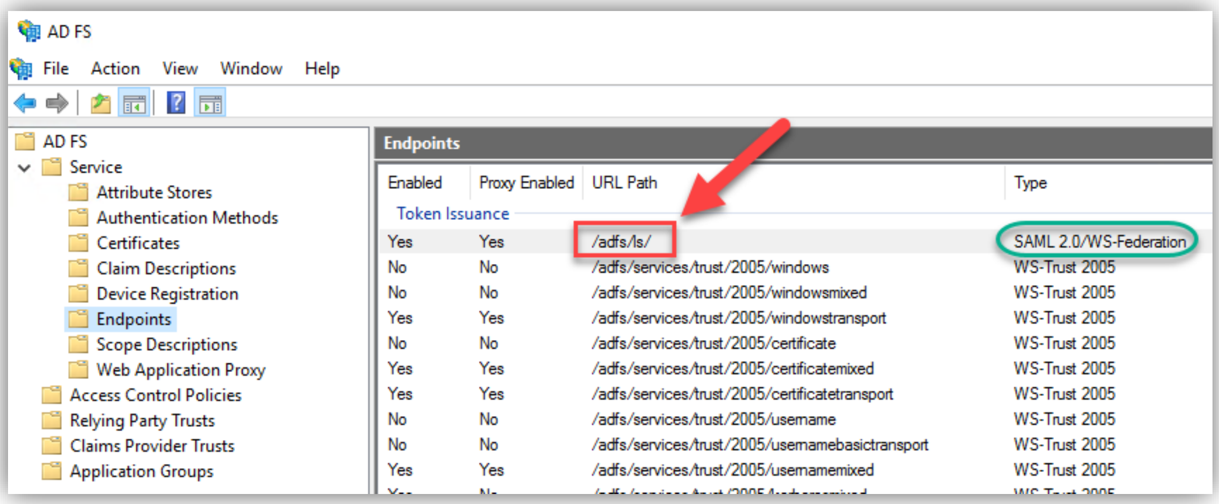
Relying party trust identifier:

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

Relying party trust identifiers:
https://192.168.1.109/ResourceCentral

Login URL

1. Go to **web server** where your Exchange server is installed, click **Start → Server Manager → Tools → AD FS Management.**
2. In the opened window, select **Service → Endpoints**. Copy the URL path for the endpoint with type **SAML 2.0**



Enabled	Proxy Enabled	URL Path	Type
Token Issuance			
Yes	Yes	/adfs/ls/	SAML 2.0/WS-Federation
No	No	/adfs/services/trust/2005/windows	WS-Trust 2005
No	No	/adfs/services/trust/2005/windowsmixed	WS-Trust 2005
Yes	Yes	/adfs/services/trust/2005/windowstransport	WS-Trust 2005
No	No	/adfs/services/trust/2005/certificate	WS-Trust 2005
Yes	Yes	/adfs/services/trust/2005/certificatemixed	WS-Trust 2005
Yes	Yes	/adfs/services/trust/2005/certificatetransport	WS-Trust 2005
No	No	/adfs/services/trust/2005/usemame	WS-Trust 2005
No	No	/adfs/services/trust/2005/usemamebasictransport	WS-Trust 2005
Yes	Yes	/adfs/services/trust/2005/usemamemixed	WS-Trust 2005

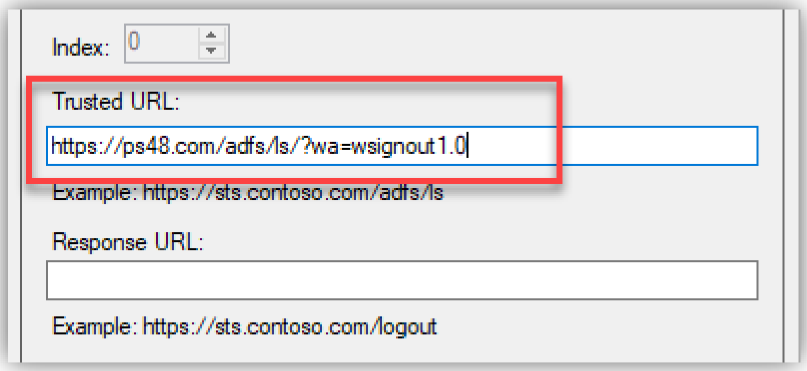
3. Compose the Login URL with the following format:

```
https:// <web_server_URL>/Endpoint_URL_path
```

For example: https://rc48.ps.com/adfs/ls

Logout URL

Logout URL is the Trusted URL in **Step 1**, Part A3 of this protocol.



Index: 0

Trusted URL:
https://ps48.com/adfs/ls/?wa=wsignout1.0
Example: https://sts.contoso.com/adfs/ls

Response URL:

Example: https://sts.contoso.com/logout

Return URL

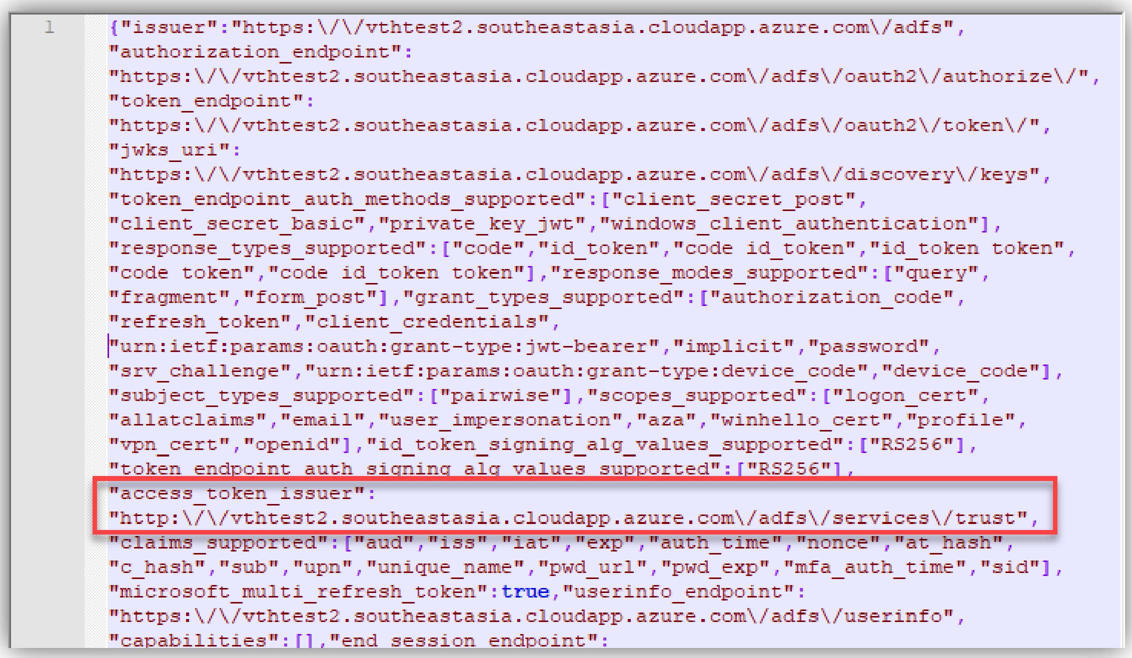
Refer to this section for more details.

Azure AD Identifier

Go to the following link:

```
https://<server of ADFS>/adfs/.well-known/openid-configuration
```

And a json file (***openid-configuration.json***) will be available for you to download/view. If you download it, open this file with Notepad or Notepad++, look for the keyword: access_token_issuer and you will find the link following it.



```
{"issuer":"https:\/\/vthtest2.southeastasia.cloudapp.azure.com\/adfs",
"authorization_endpoint":
"https:\/\/vthtest2.southeastasia.cloudapp.azure.com\/adfs\/oauth2\/authorize\/",
"token_endpoint":
"https:\/\/vthtest2.southeastasia.cloudapp.azure.com\/adfs\/oauth2\/token\/",
"jwks_uri":
"https:\/\/vthtest2.southeastasia.cloudapp.azure.com\/adfs\/discovery\/keys",
"token_endpoint_auth_methods_supported":["client_secret_post",
"client_secret_basic","private_key_jwt","windows_client_authentication"],
"response_types_supported":["code","id_token","code id_token","id_token token",
"code token","code id_token token"],"response_modes_supported":["query",
"fragment","form_post"],"grant_types_supported":["authorization_code",
"refresh_token","client_credentials",
"urn:ietf:params:oauth:grant-type:jwt-bearer","implicit","password",
"srv_challenge","urn:ietf:params:oauth:grant-type:device_code","device_code"],
"subject_types_supported":["pairwise"],"scopes_supported":["logon_cert",
"allatclaims","email","user_impersonation","aza","winhello_cert","profile",
"vpn_cert","openid"],"id_token_signing_alg_values_supported":["RS256"],
"token_endpoint_auth_signing_alg_values_supported":["RS256"],
"access_token_issuer":
"http:\/\/vthtest2.southeastasia.cloudapp.azure.com\/adfs\/services\/trust",
"claims_supported":["aud","iss","iat","exp","auth_time","nonce","at_hash",
"c_hash","sub","upn","unique_name","pwd_url","pwd_exp","mfa_auth_time","sid"],
"microsoft_multi_refresh_token":true,"userinfo_endpoint":
"https:\/\/vthtest2.southeastasia.cloudapp.azure.com\/adfs\/userinfo",
"capabilities":[],"end_session_endpoint":
```

Copy the URL, remove the character “\” in the URL and this is the Azure AD Identifier you are looking for.

Certificate (.pfx) and PFX Password

Usually you have been provided with the .pfx file and the attached password after you buy the certificate (with key). This certificate must be created with the parameter provider = **Microsoft Enhanced RSA and AES Cryptographic Provider.**

Auto-Login Networks

Refer to this section for more details.

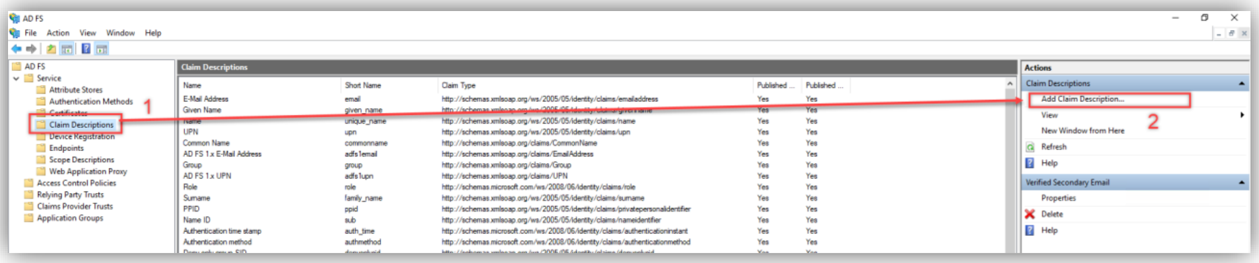
Appendix

Appendix A. Add claim to retrieve all email addresses for users who have UPN different from SMTP

If, in the system, there are users who have User Principal Name different from SMTP address, we need to add claim to retrieve all email addresses.

Option 1: Add claim as LDAP attributes

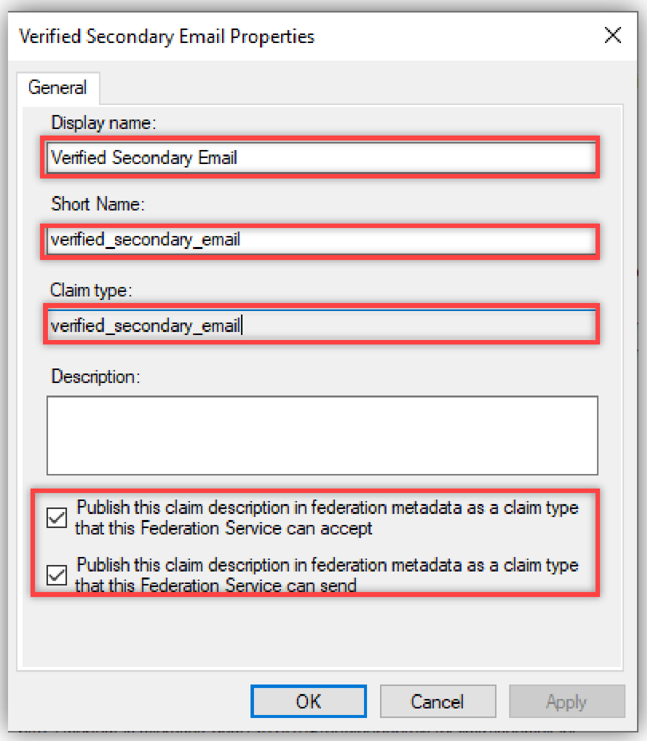
1. In AD FS manager, choose “**Claim Description”** then click “**Add Claim Description…”**:



Claim Descriptions

Name	Short Name	Claim Type	Published ...	Published ...
E-Mail Address	email	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress	Yes	Yes
Given Name	given_name	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/givenname	Yes	Yes
Name	unique_name	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/name	Yes	Yes
UPN	upn	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/upn	Yes	Yes
Common Name	commonname	http://schemas.xmlsoap.org/claims/CommonName	Yes	Yes
AD FS 1.x E-Mail Address	adfs1email	http://schemas.xmlsoap.org/claims/EmailAddress	Yes	Yes
Group	group	http://schemas.xmlsoap.org/claims/Group	Yes	Yes
AD FS 1.x UPN	adfs1upn	http://schemas.xmlsoap.org/claims/UPN	Yes	Yes
Role	role	http://schemas.microsoft.com/ws/2008/06/identity/claims/role	Yes	Yes
Surname	family_name	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/surname	Yes	Yes
PPID	ppid	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/privatepersonalidentifier	Yes	Yes
Name ID	sub	http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier	Yes	Yes
Authentication time stamp	auth_time	http://schemas.microsoft.com/ws/2008/06/identity/claims/authenticationinstant	Yes	Yes
Authentication method	authmethod	http://schemas.microsoft.com/ws/2008/06/identity/claims/authenticationmethod	Yes	Yes

2. In the pop-up window, enter Name and Claim Type for new Claim Descriptions



Display name:
Verified Secondary Email

Short Name:
verified_secondary_email

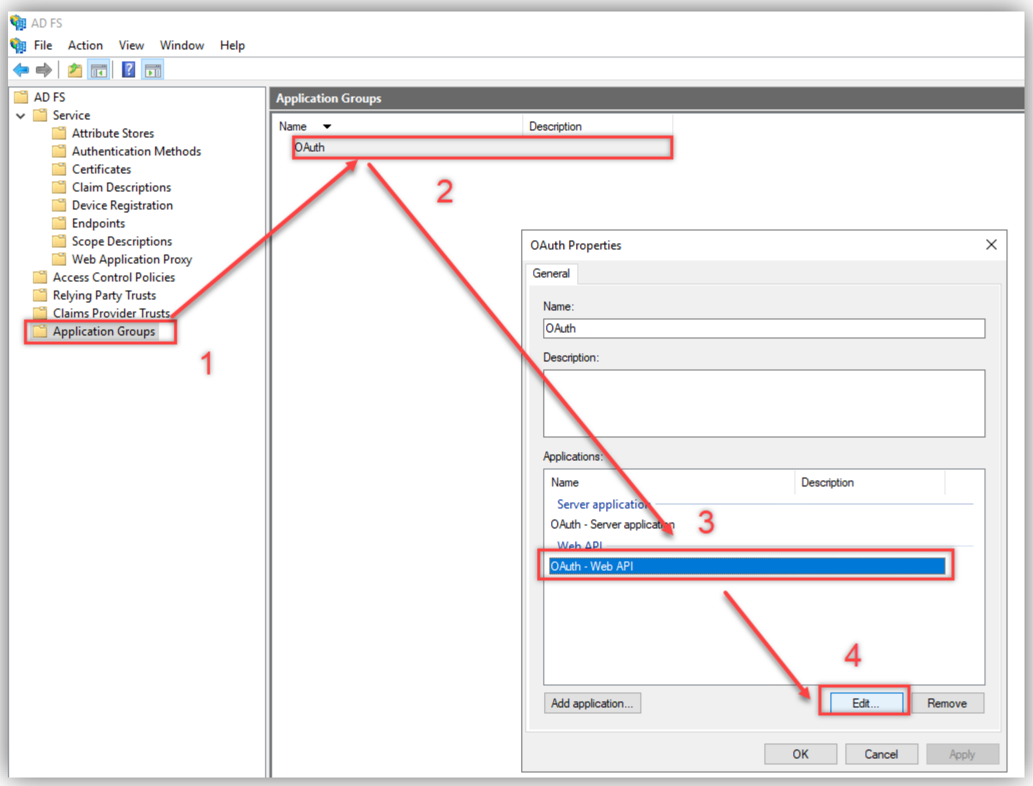
Claim type:
verified_secondary_email

Description:

☑ Publish this claim description in federation metadata as a claim type that this Federation Service can accept

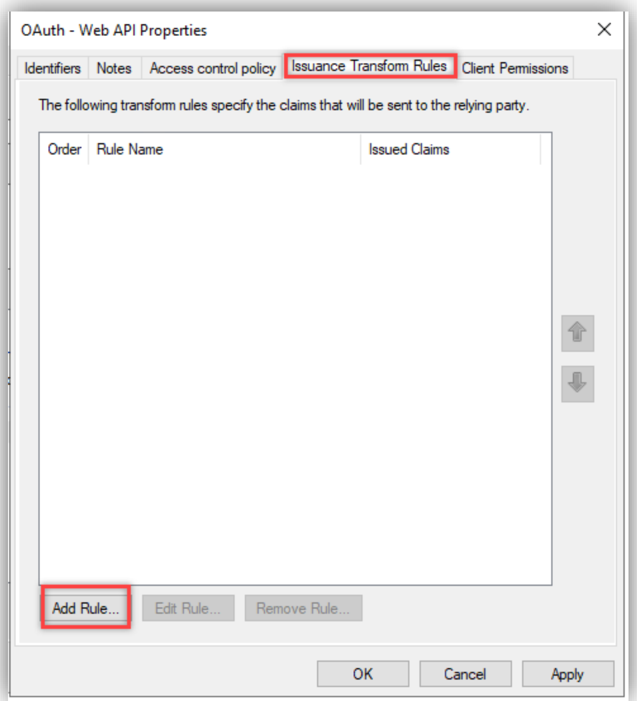
☑ Publish this claim description in federation metadata as a claim type that this Federation Service can send

3. Go back to **Application Groups** folder:

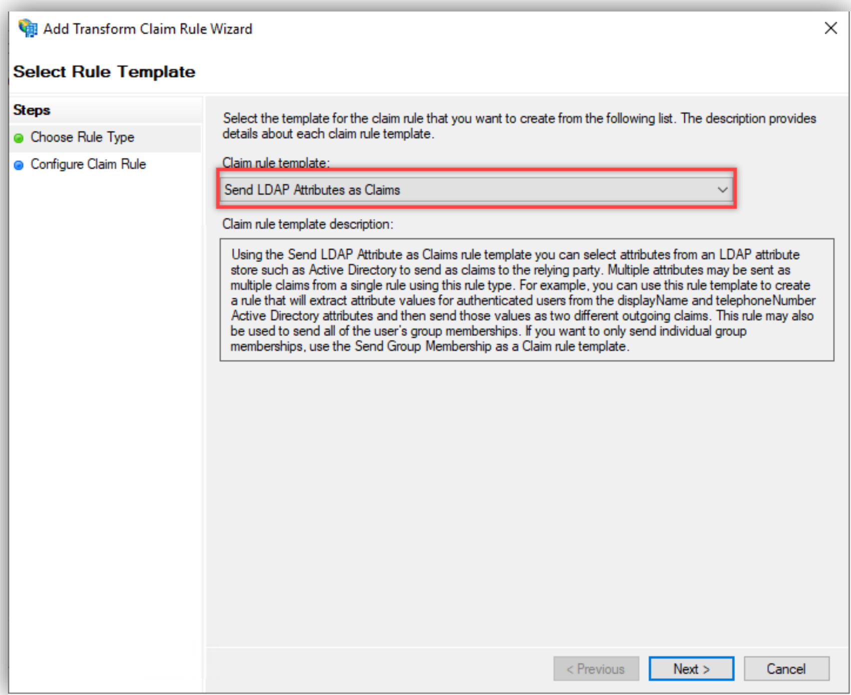


Right click on **Application Groups** we created, select "**Properties**". In properties window, click **"Web Api Application"**, then click [**Edit**].

4. In the next screen, select **"Issuance Transform Rules"** tab, then click **"Add Rule…"** button.



5. In the next screen, select **“Send LDAP Attribute as Claims”** then click [**Next**].



Add Transform Claim Rule Wizard

Select Rule Template

Steps
- Choose Rule Type
- Configure Claim Rule

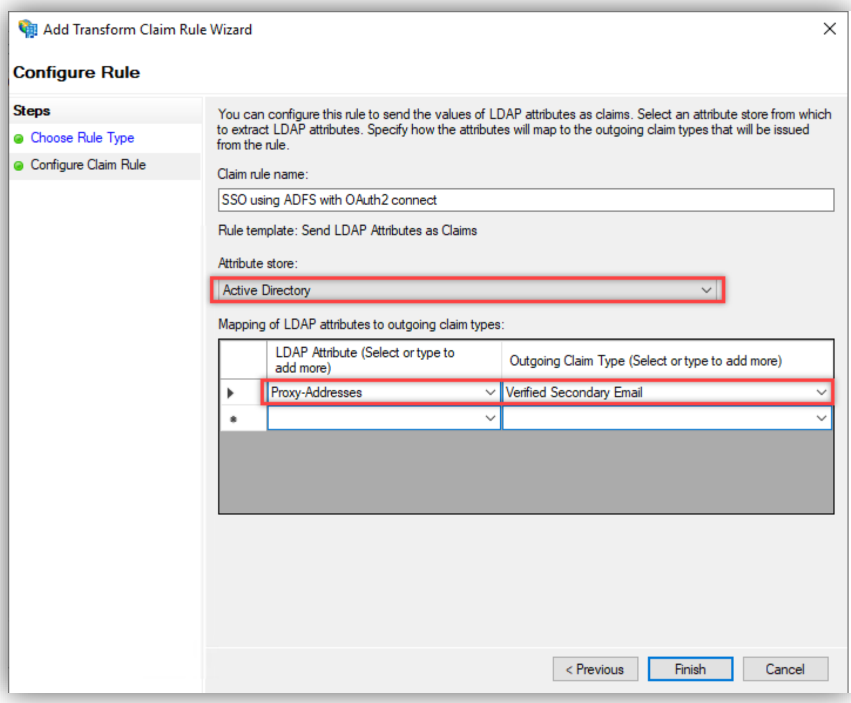
Select the template for the claim rule that you want to create from the following list. The description provides details about each claim rule template.

Claim rule template: Send LDAP Attributes as Claims

Claim rule template description:

Using the Send LDAP Attribute as Claims rule template you can select attributes from an LDAP attribute store such as Active Directory to send as claims to the relying party. Multiple attributes may be sent as multiple claims from a single rule using this rule type. For example, you can use this rule template to create a rule that will extract attribute values for authenticated users from the displayName and telephoneNumber Active Directory attributes and then send those values as two different outgoing claims. This rule may also be used to send all of the user's group memberships. If you want to only send individual group memberships, use the Send Group Membership as a Claim rule template.

6. In the next screen, set up Claim Rule as shown in the following figure:



Add Transform Claim Rule Wizard

Configure Rule

Steps
- Choose Rule Type
- Configure Claim Rule

You can configure this rule to send the values of LDAP attributes as claims. Select an attribute store from which to extract LDAP attributes. Specify how the attributes will map to the outgoing claim types that will be issued from the rule.

Claim rule name: SSO using ADFS with OAuth2 connect

Rule template: Send LDAP Attributes as Claims

Attribute store: Active Directory

Mapping of LDAP attributes to outgoing claim types:

LDAP Attribute (Select or type to add more)	Outgoing Claim Type (Select or type to add more)
Proxy-Addresses	Verified Secondary Email

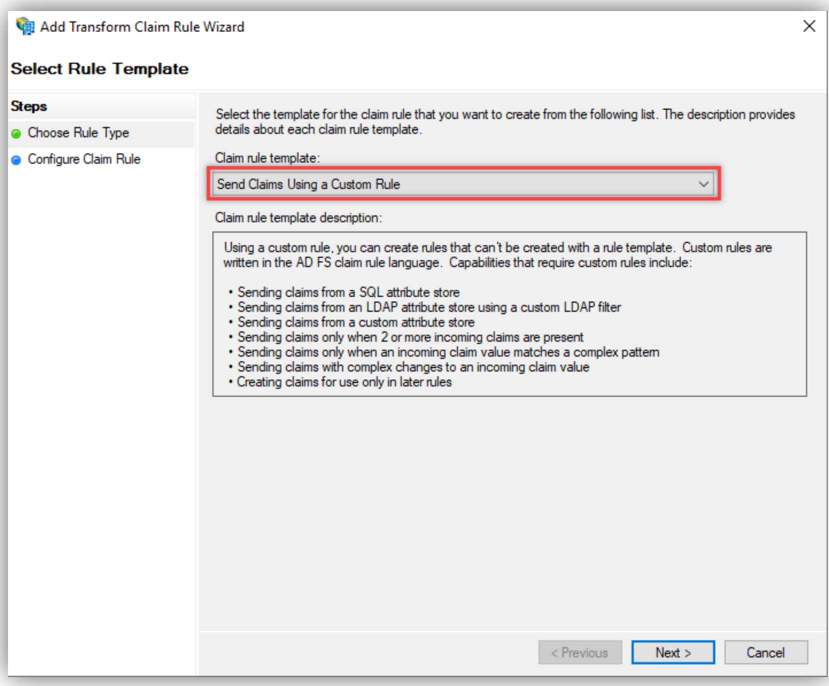
- In **“Attribute store”** field: select **“Active Directory”.**
- In “**LDAP Attributes**” column: add **Proxy-Addresses** attribute.
- In “**Outgoing Claim Type**” column: select the claim rule created in step 2.

Then click [**Finish**] and [**Save**] configuration.

Option 2: Add Claim by custom rule

NOTE: Step 1 to 4 of this option are similar to those of Option 1. Refer to the Option 1 and continue with step 5.

5. In the next screen, select **"Send Claim Using a Custom Rule"** then click [**Next**]:



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:

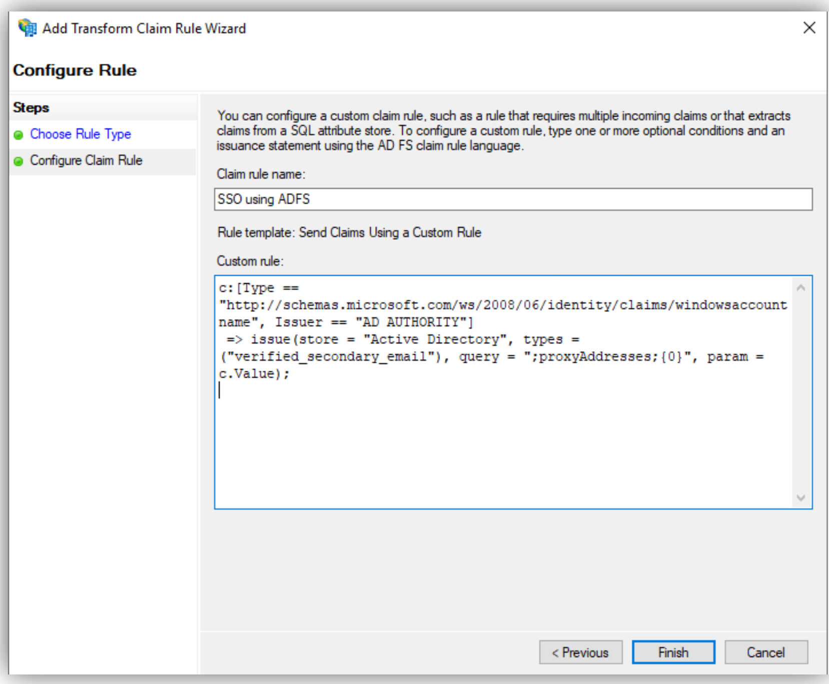
Send Claims Using a Custom Rule

Claim rule template description:

Using a custom rule, you can create rules that can't be created with a rule template. Custom rules are written in the AD FS claim rule language. Capabilities that require custom rules include:

- Sending claims from a SQL attribute store
- Sending claims from an LDAP attribute store using a custom LDAP filter
- Sending claims from a custom attribute store
- Sending claims only when 2 or more incoming claims are present
- Sending claims only when an incoming claim value matches a complex pattern
- Sending claims with complex changes to an incoming claim value
- Creating claims for use only in later rules

6. In the next screen, fill in Custom rule name and setting rule:



You can configure a custom claim rule, such as a rule that requires multiple incoming claims or that extracts claims from a SQL attribute store. To configure a custom rule, type one or more optional conditions and an issuance statement using the AD FS claim rule language.

Claim rule name:

SSO using ADFS

Rule template: Send Claims Using a Custom Rule

Custom rule:

```
c:[Type ==
"http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccount
name", Issuer == "AD AUTHORITY"]
 => issue(store = "Active Directory", types =
("verified_secondary_email"), query = ";proxyAddresses;{0}", param =
c.Value);
```

The custom rule should be entered with the following text:

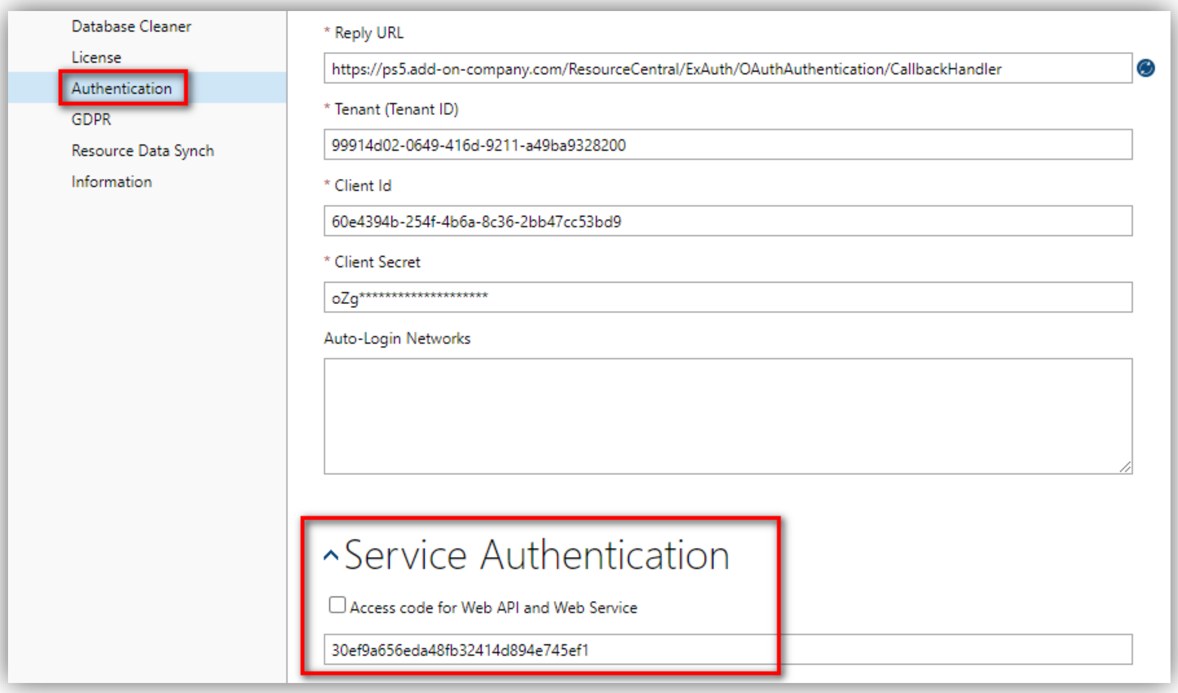
```
c:[Type ==
"http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname", Issuer ==
"AD AUTHORITY"]
 => issue(store = "Active Directory", types = ("verified_secondary_email"), query =
";proxyAddresses;{0}", param = c.Value);
```

Then click [**Finish]** and [**Save]**.

Appendix B. Configure access code for Web API and Web Service

From RC 4.2 Hot Fix 8 onwards, you can configure an access code for Web API and Web Service to authenticate the communication between and with different Resource Central services.

To do so, go to **RC backend → SYSTEM → Authentication**, then go to ‘Service Authentication’ section:



* Reply URL: https://ps5.add-on-company.com/ResourceCentral/ExAuth/OAuthAuthentication/CallbackHandler

* Tenant (Tenant ID): 99914d02-0649-416d-9211-a49ba9328200

* Client Id: 60e4394b-254f-4b6a-8c36-2bb47cc53bd9

* Client Secret: oZg*******************

Auto-Login Networks:

Service Authentication

□ Access code for Web API and Web Service

30ef9a656eda48fb32414d894e745ef1

Check on ‘Access code for Web API and Web Service’ option will generate a new code below.

NOTE:

- Authentication on Resource Finder Com Add-in combined with this Service Authentication requires a Com Add-in version of 4.1.X.
- If you uncheck ‘Access code for Web API and Web Service’ option, yet the code still exists, this function will actually be disabled.
- In order to generate new code, you need to delete the existing code. Then check on ‘Access code for Web API and Web Service’ option again.
- The access code can also be used to authenticate third party apps reading from ResourceInfo.asmx