Resource Central

External Authentication Configuration Guide

Version: 1.4

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

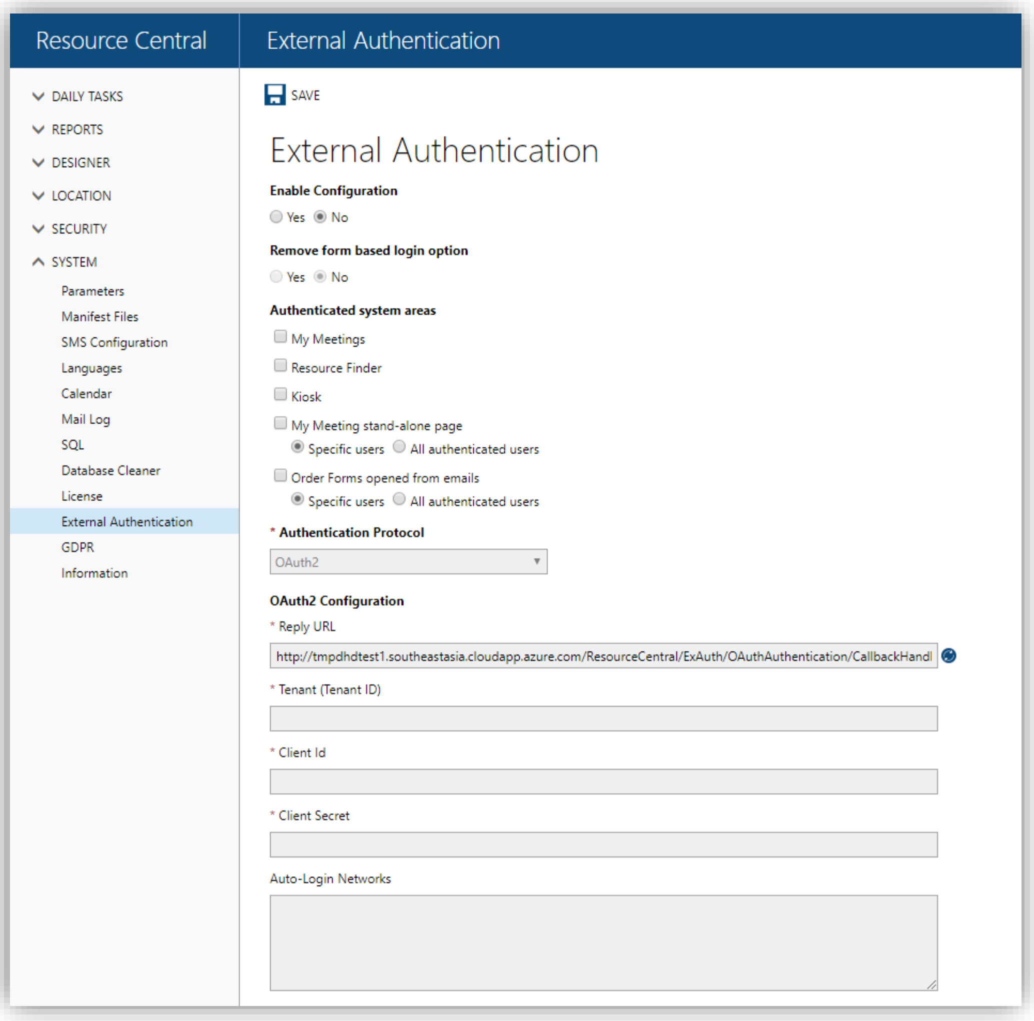
Table of contents

Foreword

External authentication is a new function in Resource Central (RC) that allows you to make configuration for supporting login using a third-party account. Currently, only signing in with Microsoft is supported and this requires some fields to be filled up with specific data in Resource Central backend.

External authentication currently covers the following Resource Central features

- Outlook COM Add-in: 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

□ 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

http://tmpdhdtest1.southeastasia.cloudapp.azure.com/ResourceCentral/ExAuth/OAuthAuthentication/CallbackHandl

* Tenant (Tenant ID)

* Client Id

* Client Secret

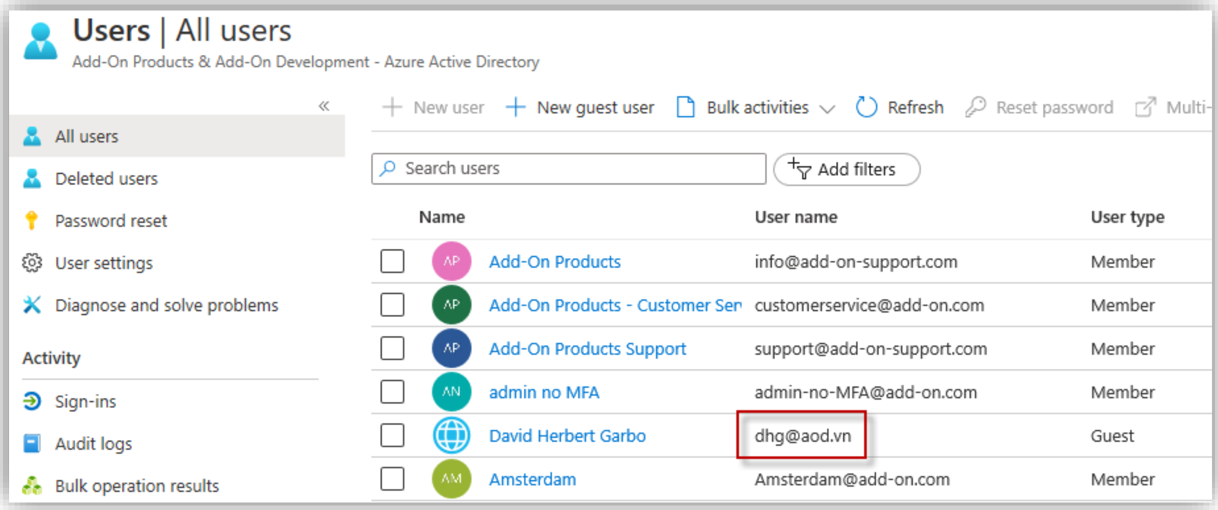
Auto-Login Networks

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.

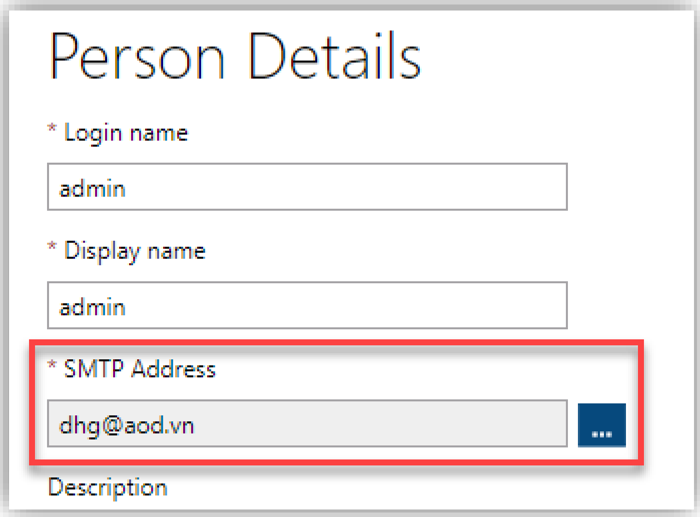
Each Authentication Protocol requires specific data fields to be filled in. This document is designed to give you detailed instructions to retrieve those details.

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



Name	User name	User type
Add-On Products	info@add-on-support.com	Member
Add-On Products - Customer Ser	customerservice@add-on.com	Member
Add-On Products Support	support@add-on-support.com	Member
admin no MFA	admin-no-MFA@add-on.com	Member
David Herbert Garbo	dhg@aod.vn	Guest
Amsterdam	Amsterdam@add-on.com	Member

Figure 2. All users in Azure



Person Details

* Login name

admin

* Display name

admin

* SMTP Address

dhg@aod.vn

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

Affected areas

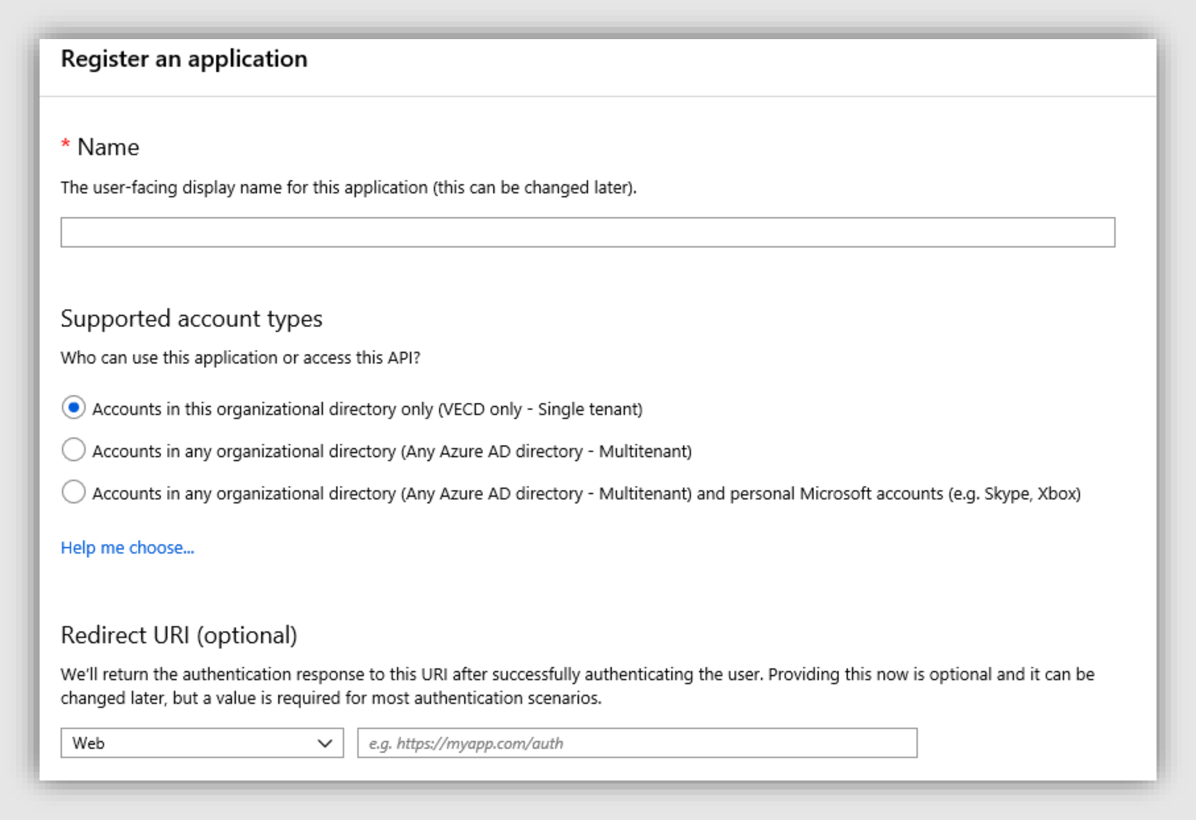
Look at the following table for further explanation:

	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 → New registration**.
2. Fill in application details:
   a. **Name**: enter application name
   b. **Supported account types**: select “Accounts in this organizational directory only (VECD only - Single tenant)”
   c. **Redirect URI**: enter **Reply URL** in RC backend/External Authentication/OAuth2



Register an application

* Name

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

Supported account types

Who can use this application or access this API?

● Accounts in this organizational directory only (VECD 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)

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.

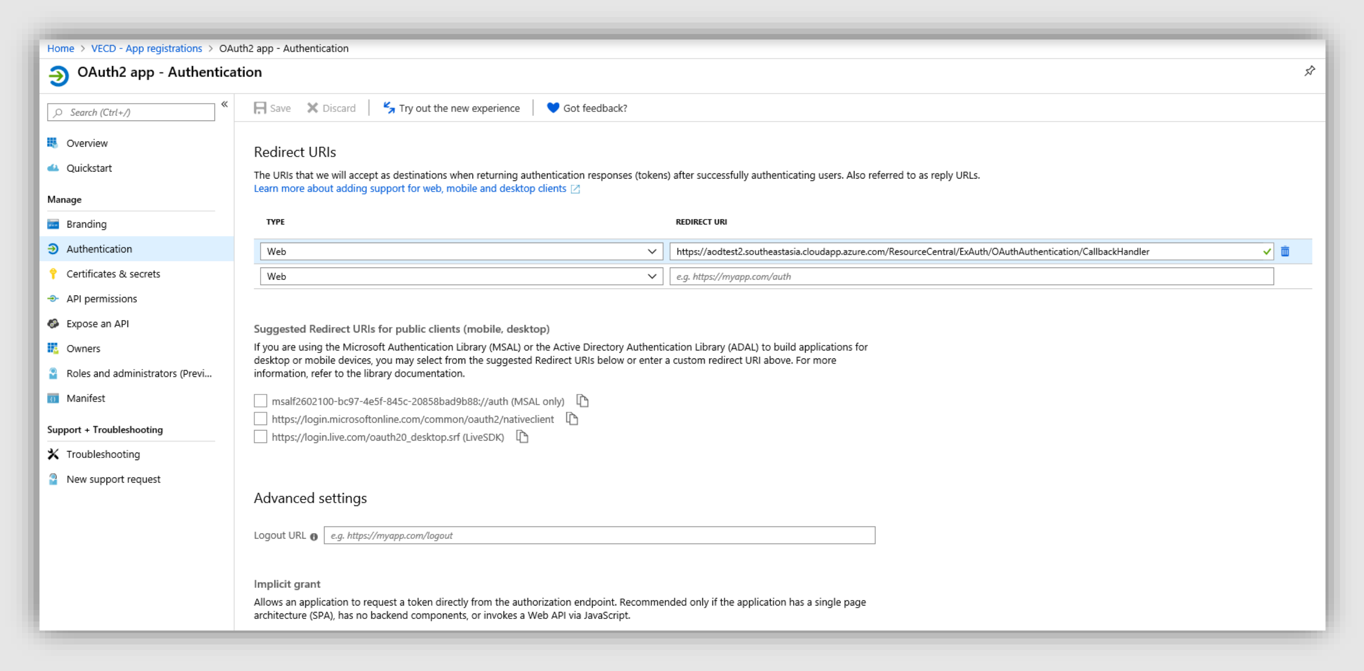
Web | e.g. https://myapp.com/auth

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

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

Reply URL

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.



Redirect URIs

The URIs that we will accept as destinations when returning authentication responses (tokens) after successfully authenticating users. Also referred to as reply URLs.
Learn more about adding support for web, mobile and desktop clients

TYPE	REDIRECT URI
Web	https://aodtest2.southeastasia.cloudapp.azure.com/ResourceCentral/ExAuth/OAuthAuthentication/CallbackHandler
Web	e.g. https://myapp.com/auth

Suggested Redirect URIs for public clients (mobile, desktop)

If you are using the Microsoft Authentication Library (MSAL) or the Active Directory Authentication Library (ADAL) to build applications for desktop or mobile devices, you may select from the suggested Redirect URIs below or enter a custom redirect URI above. For more information, refer to the library documentation.

□ msalf2602100-bc97-4e5f-845c-20858bad9b88://auth (MSAL only)
□ https://login.microsoftonline.com/common/oauth2/nativeclient
□ https://login.live.com/oauth20_desktop.srf (LiveSDK)

Advanced settings

Logout URL: e.g. https://myapp.com/logout

Implicit grant

Allows an application to request a token directly from the authorization endpoint. Recommended only if the application has a single page architecture (SPA), has no backend components, or invokes a Web API via JavaScript.

Figure 4. Registered app

Click [**Authentication**] as in the above figure, the **Redirect URI** panel is displayed on the right side of the screen.

Type the URI in the highlighted textbox with the following format:

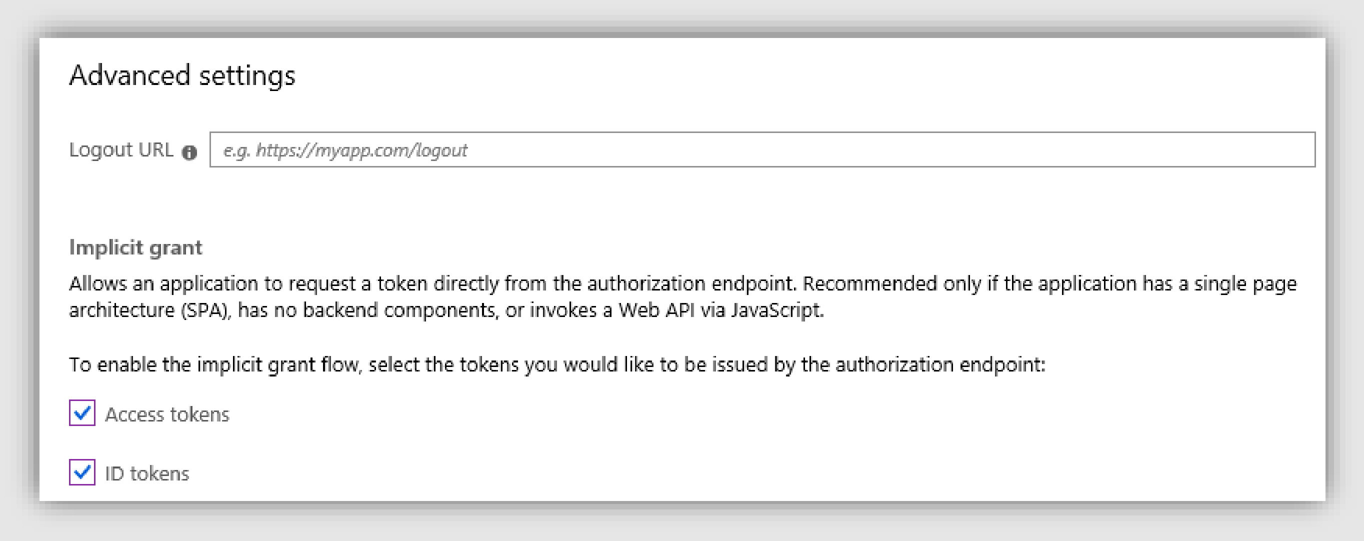
```
[Home page or Sign-on URL]/ExAuth/OAuthAuthentication/CallbackHandler
```

NOTE: OAuth2 and Open ID Connect authentication protocols require HTTPS.

In the above example, the Home page or Sign-on URL is https://resourcecentral.com/resourcecentral, so the URL you can fill in is:
https://resourcecentral.com/resourcecentral/ExAuth/OAuthAuthentication/CallbackHandler

Click [**Save**] to finish.

NOTE: For Open ID Connect authentication protocol, you need to check on 2 options in **Implicit grant**:



Advanced settings

Logout URL: e.g. https://myapp.com/logout

Implicit grant

Allows an application to request a token directly from the authorization endpoint. Recommended only if the application has a single page architecture (SPA), has no backend components, or invokes a Web API via JavaScript.

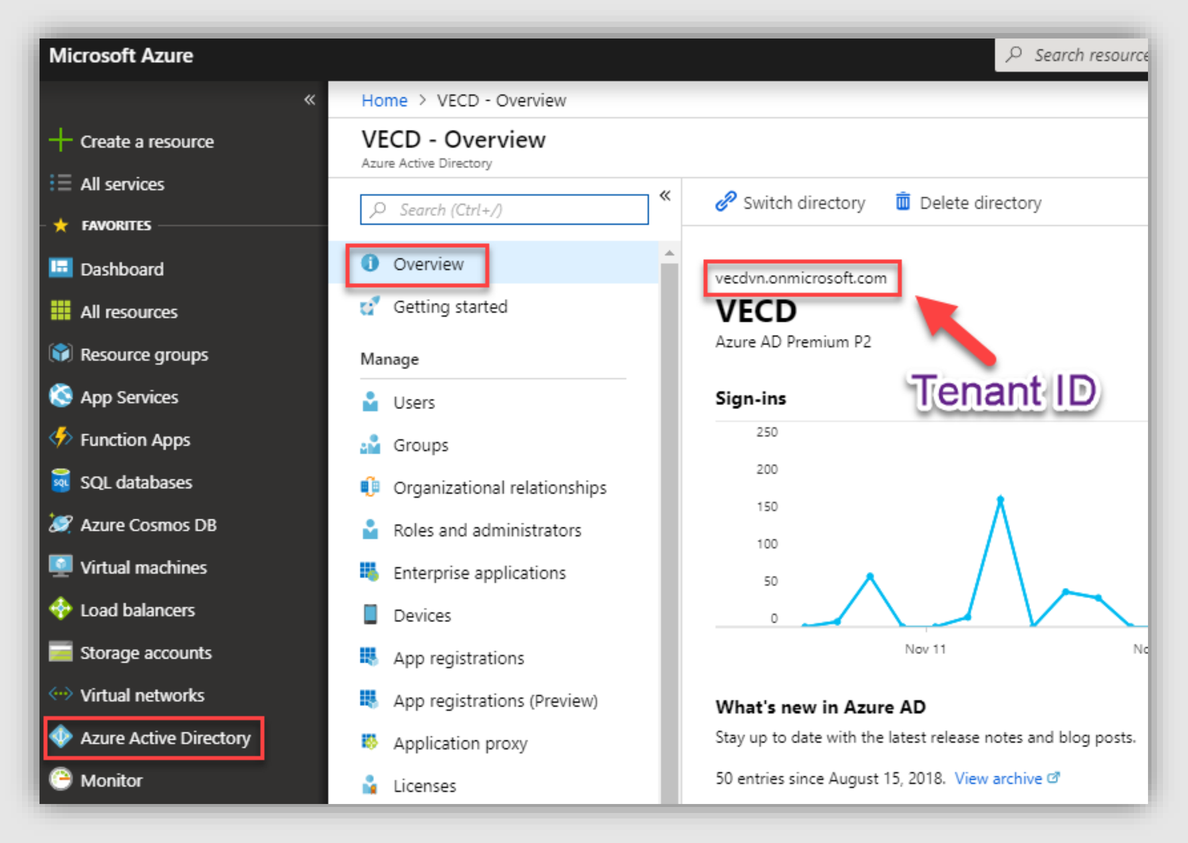
To enable the implicit grant flow, select the tokens you would like to be issued by the authorization endpoint:

☑ Access tokens

☑ ID tokens

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:



vecdvn.onmicrosoft.com

VECD

Azure AD Premium P2

What's new in Azure AD

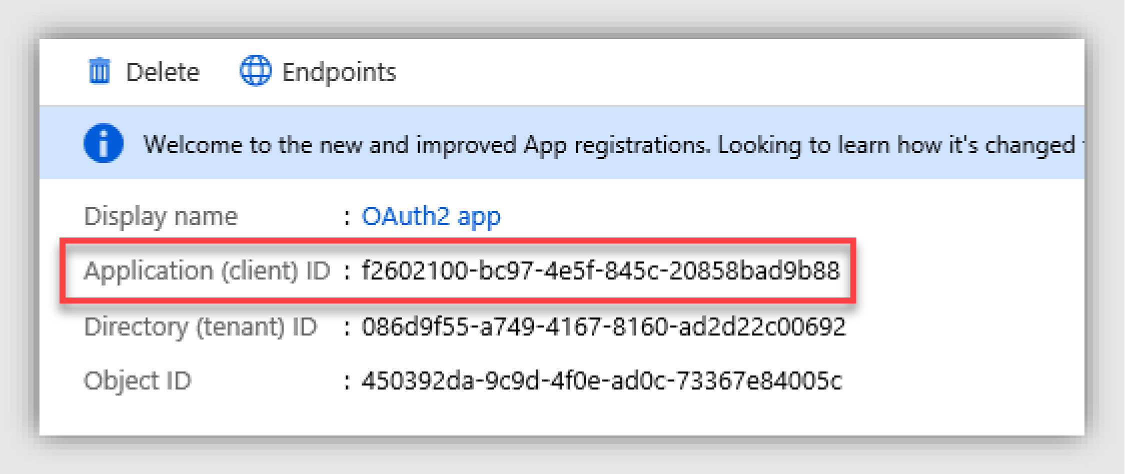
Stay up to date with the latest release notes and blog posts.

50 entries since August 15, 2018. View archive

Figure 5. Tenant ID

Client ID

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.



Welcome to the new and improved App registrations. Looking to learn how it's changed

Display name : OAuth2 app

Application (client) ID : f2602100-bc97-4e5f-845c-20858bad9b88

Directory (tenant) ID : 086d9f55-a749-4167-8160-ad2d22c00692

Object ID : 450392da-9c9d-4f0e-ad0c-73367e84005c

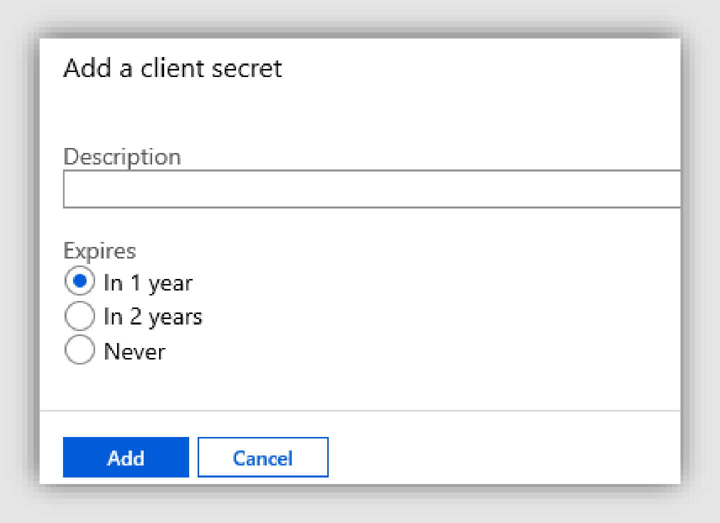
Figure 6. Client ID

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

Client secret

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.

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



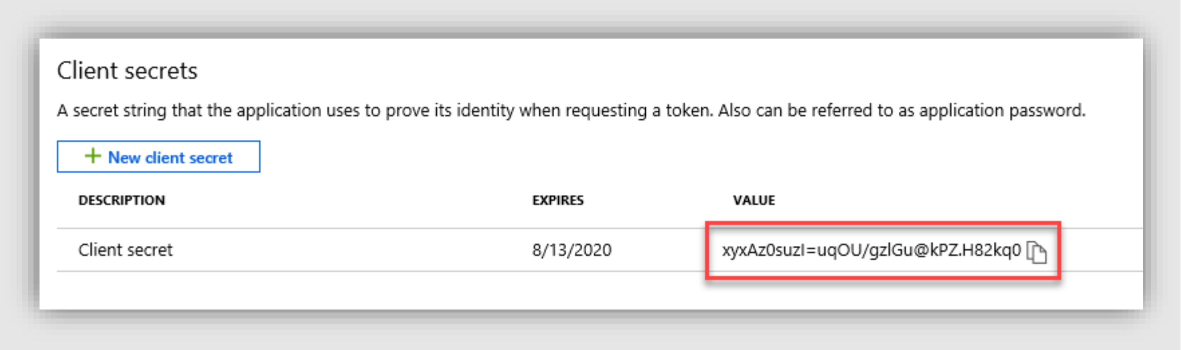
Add a client secret

Description

Expires
● In 1 year
○ In 2 years
○ Never

Figure 7. Client secret

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



Client secrets

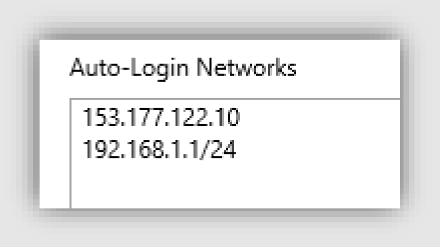
A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

DESCRIPTION	EXPIRES	VALUE
Client secret	8/13/2020	xyxAz0suzI=uqOU/gzlGu@kPZ.H82kq0

Please remember to copy this client secret value 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 8. Auto-Login Networks

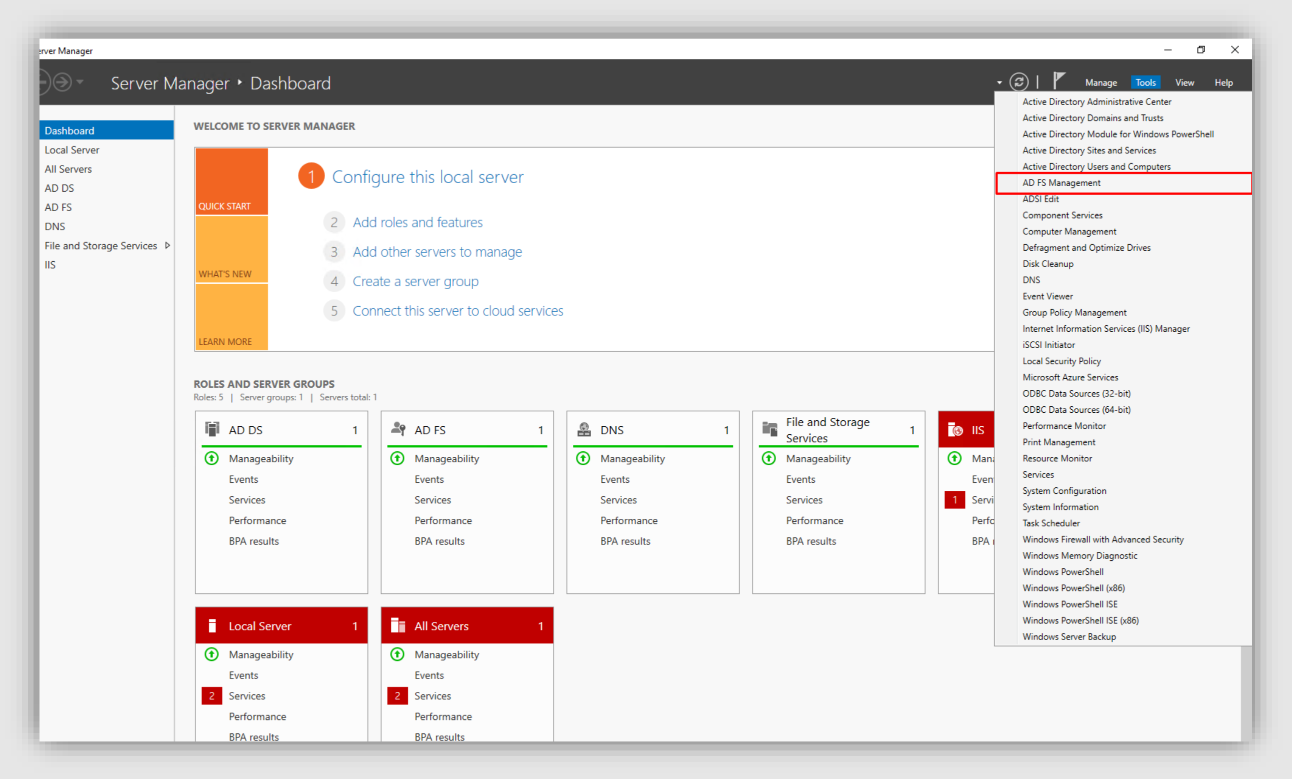
With this value filled in, client machines with the filled in IP address will be automatically logged in and use Single Sign-On function.

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

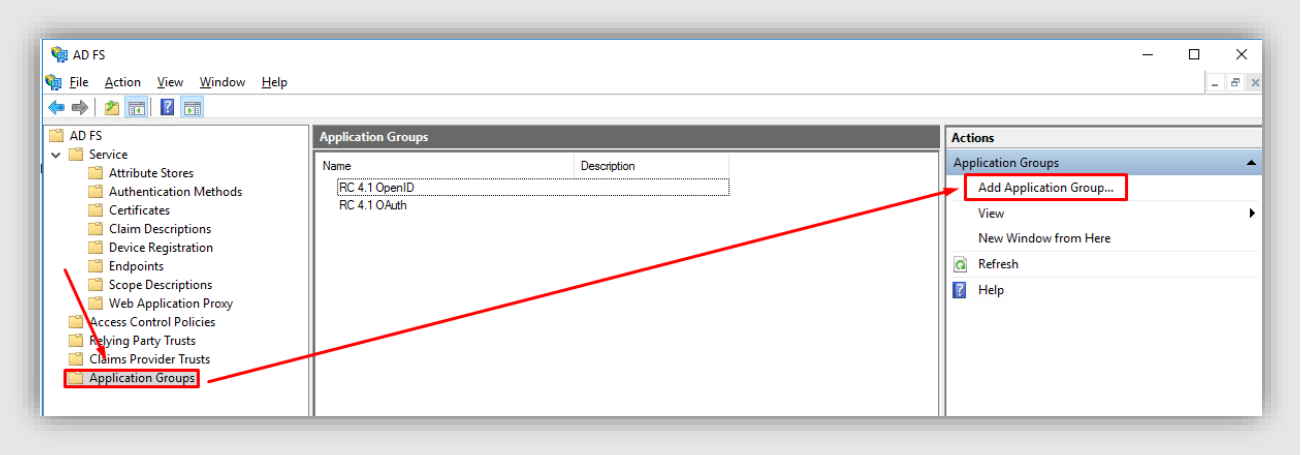
Authentication Details for OAuth2 with ADFS

Part A. Configure Active Directory Federation Services (ADFS)

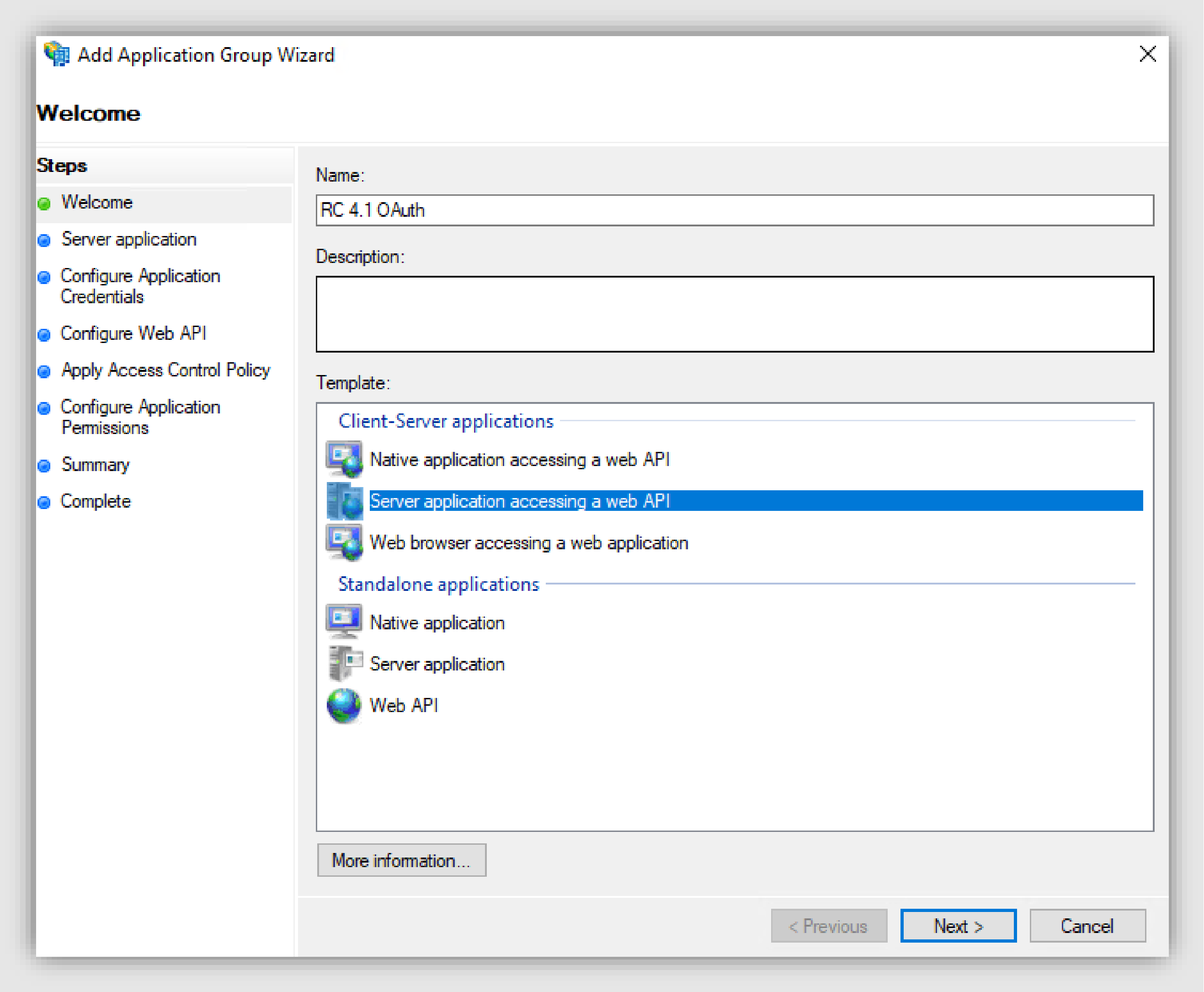
1. Go to **web server** where your Exchange server is installed, click **Start → Server Manager → Tools → AD FS Management**


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
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

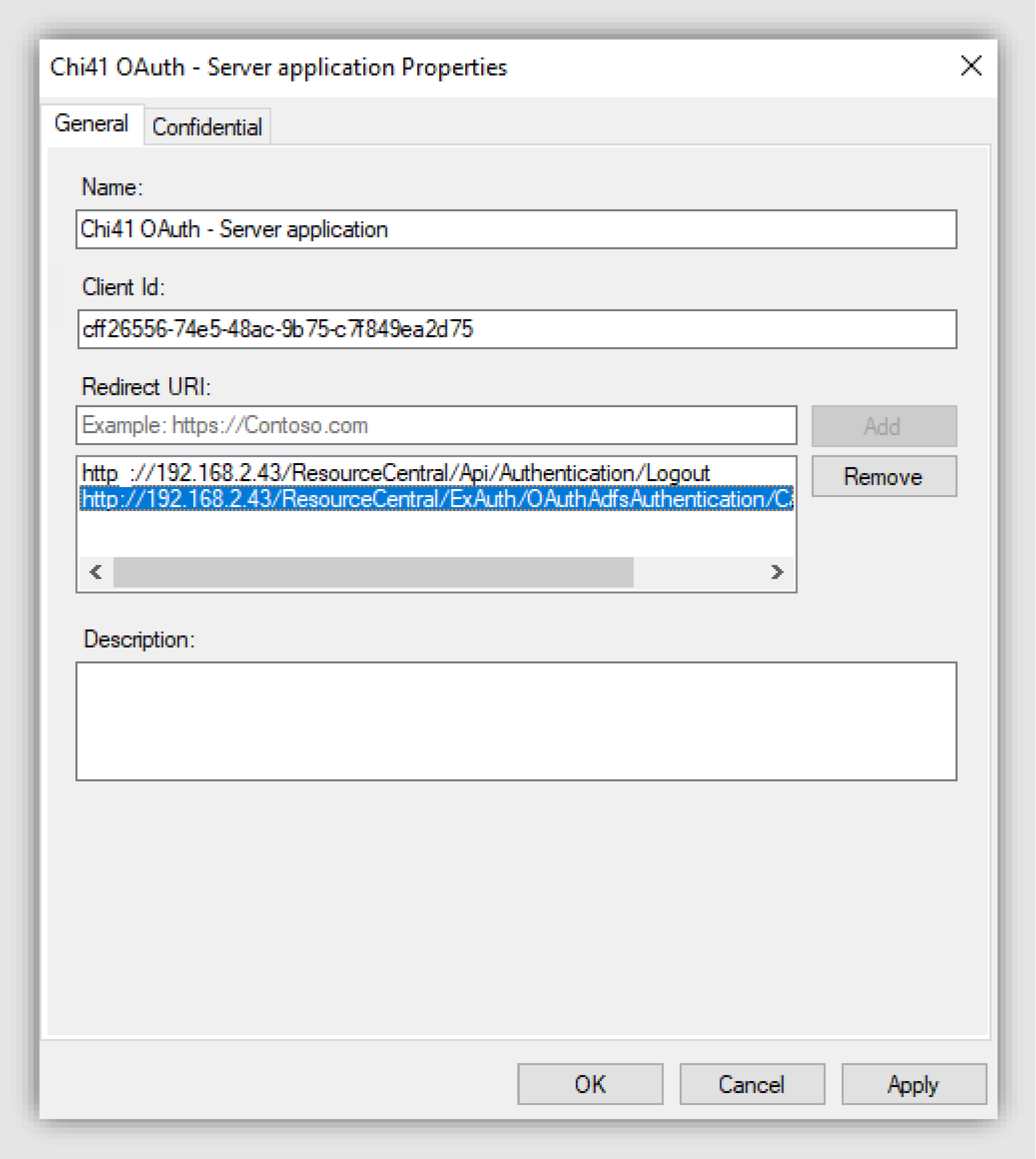
Name: RC 4.1 OAuth

Description:

Template: Server application accessing a web API

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

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

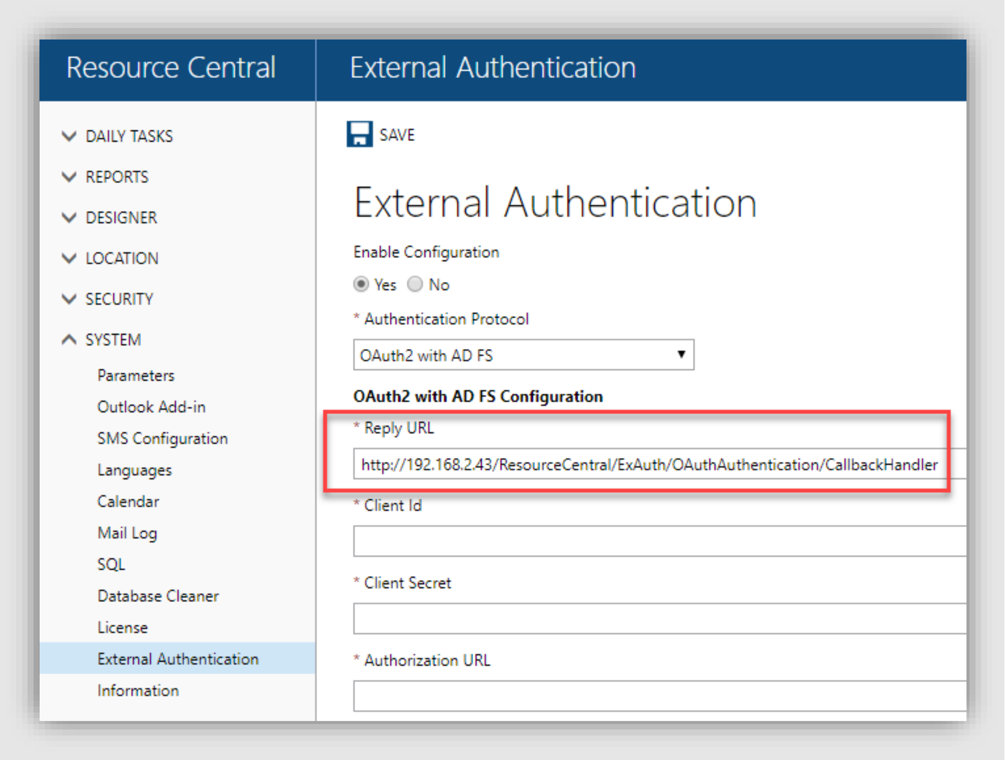
Client Id: cff26556-74e5-48ac-9b75-c7f849ea2d75

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

* Authentication Protocol: OAuth2 with AD FS

OAuth2 with AD FS Configuration

* Reply URL: http://192.168.2.43/ResourceCentral/ExAuth/OAuthAuthentication/CallbackHandler

* Client Id

* Client Secret

* Authorization URL

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

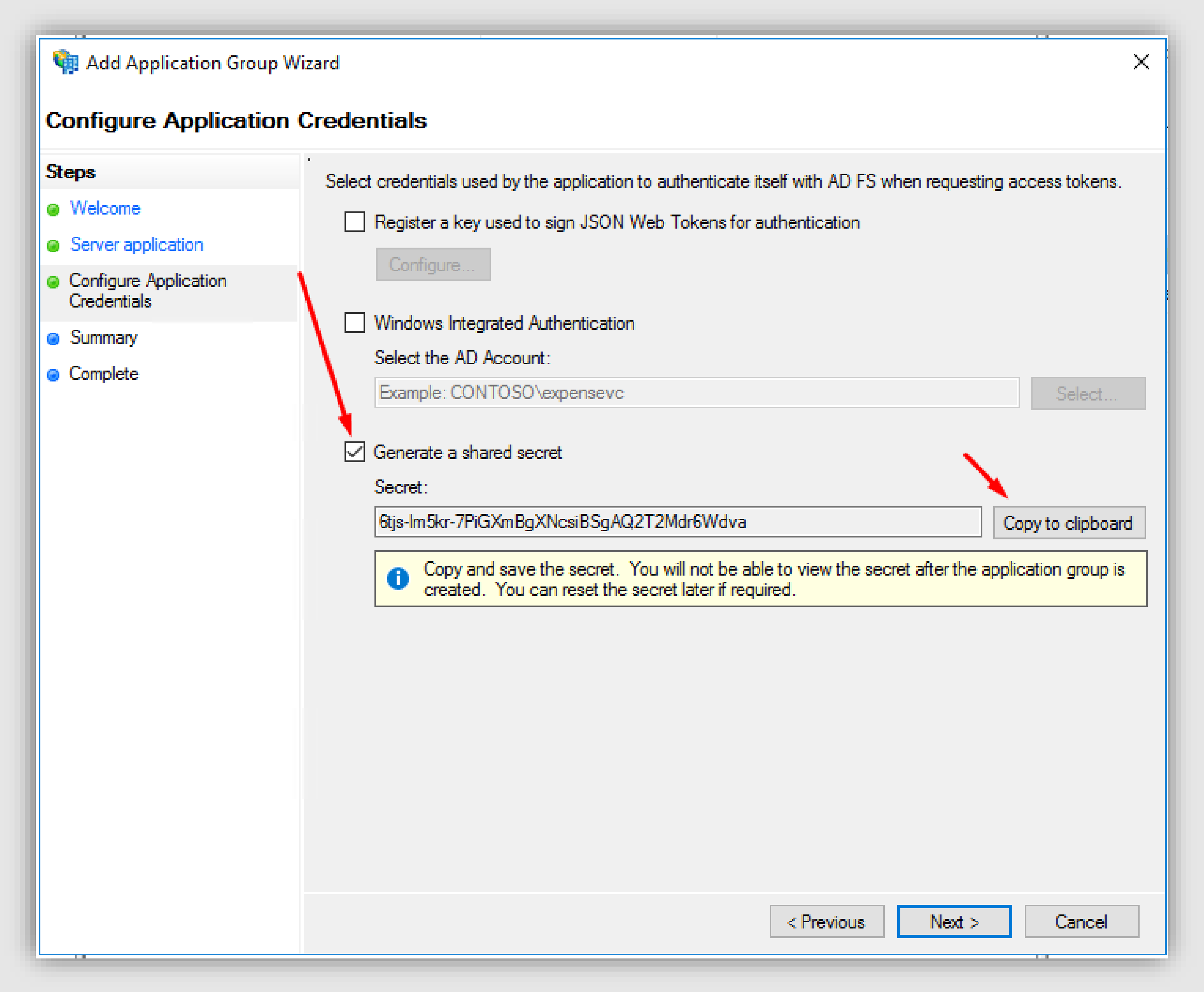
The URL for receiving logout details from ADFS must have the following format:

```
[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

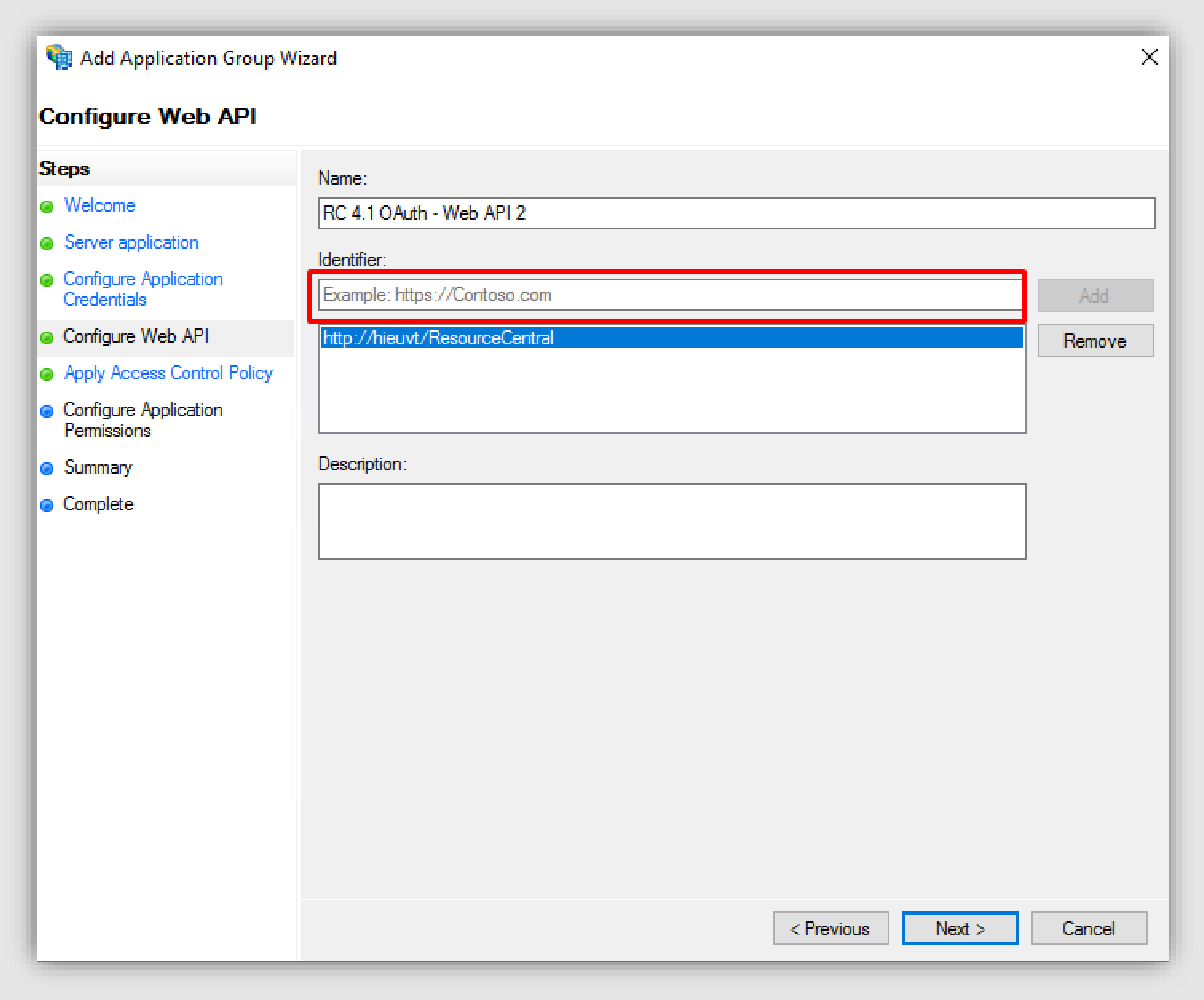
Select the AD Account: Example: CONTOSO\expensevc

☑ 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 URL to RC backend) and click [**Add**] button.


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: RC 4.1 OAuth - Web API 2

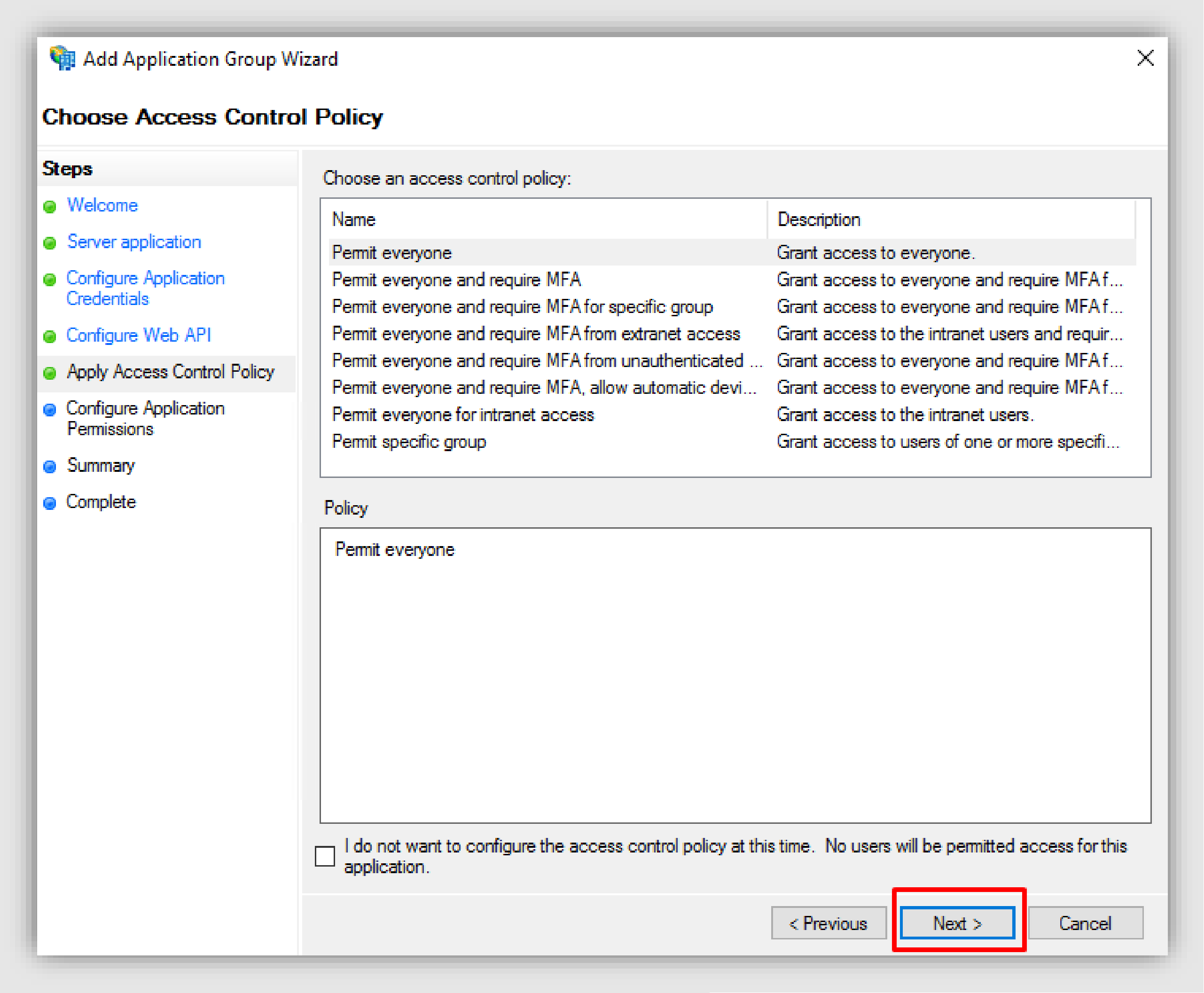
Identifier: Example: https://Contoso.com

http://hieuvt/ResourceCentral

Description:

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

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


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

Choose Access Control Policy

Choose an access control policy:

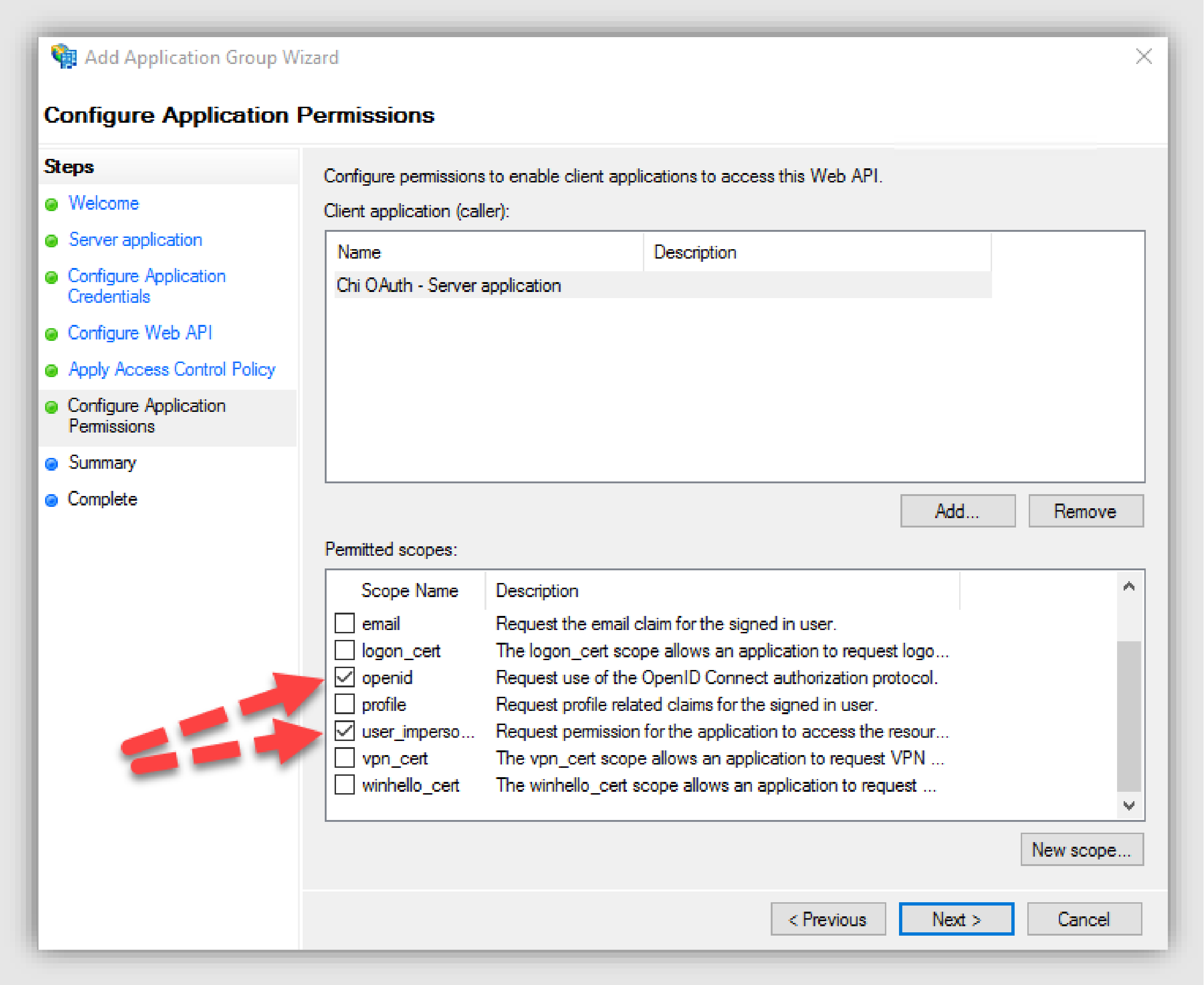
Name	Description
Permit everyone	Grant access to everyone.
Permit everyone and require MFA	Grant access to everyone and require MFA f...
Permit everyone and require MFA for specific group	Grant access to everyone and require MFA f...
Permit everyone and require MFA from extranet access	Grant access to 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.

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



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.

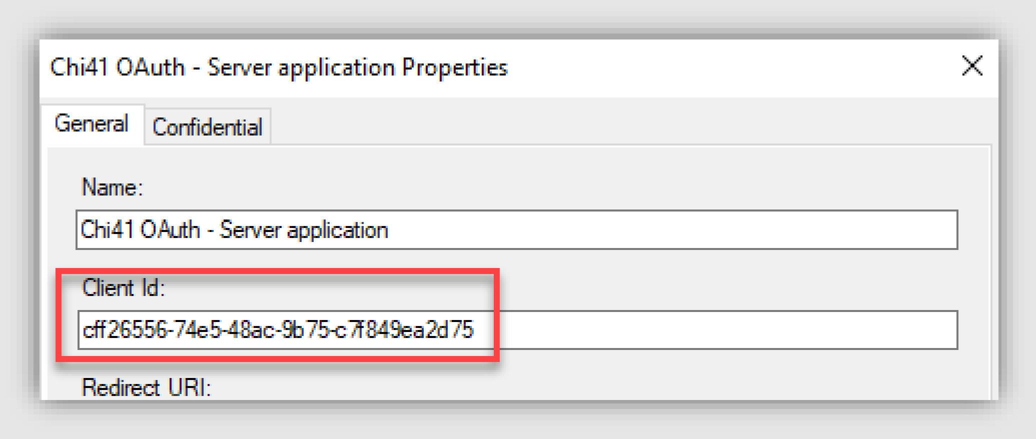
Part B. Retrieve details for OAuth2 with ADFS Authentication Protocol

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

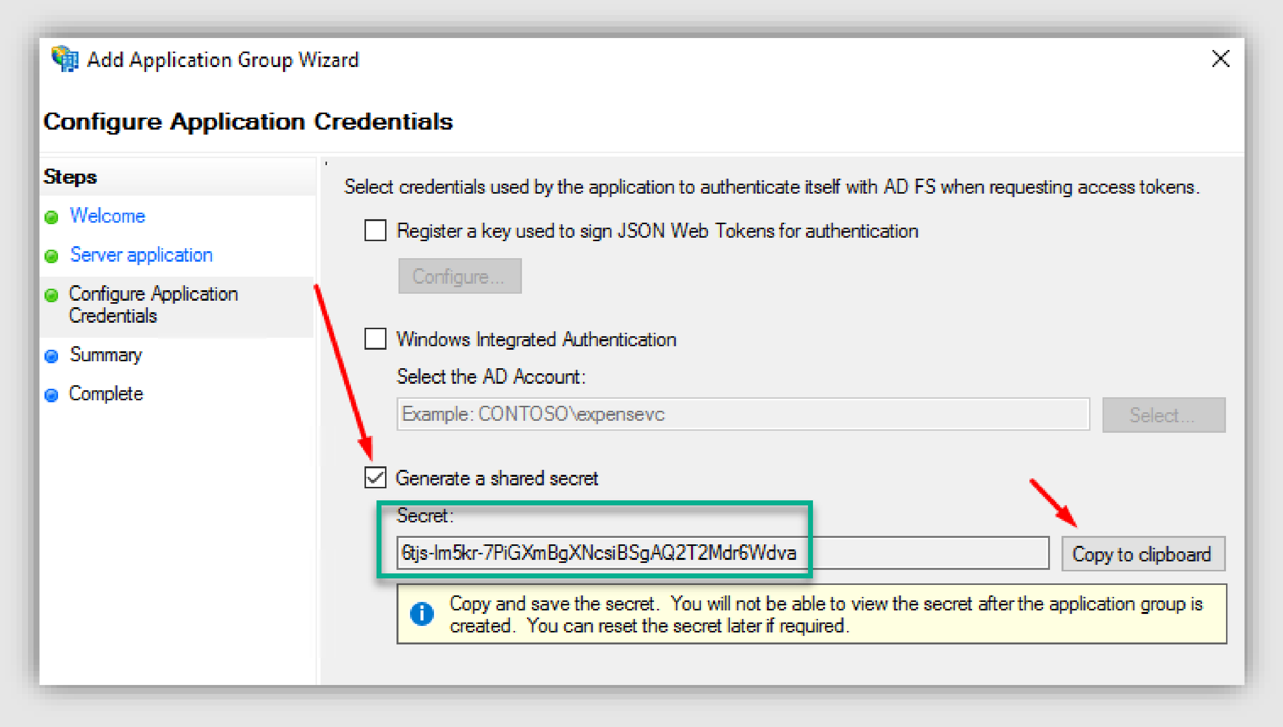
Name: Chi41 OAuth - Server application

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.

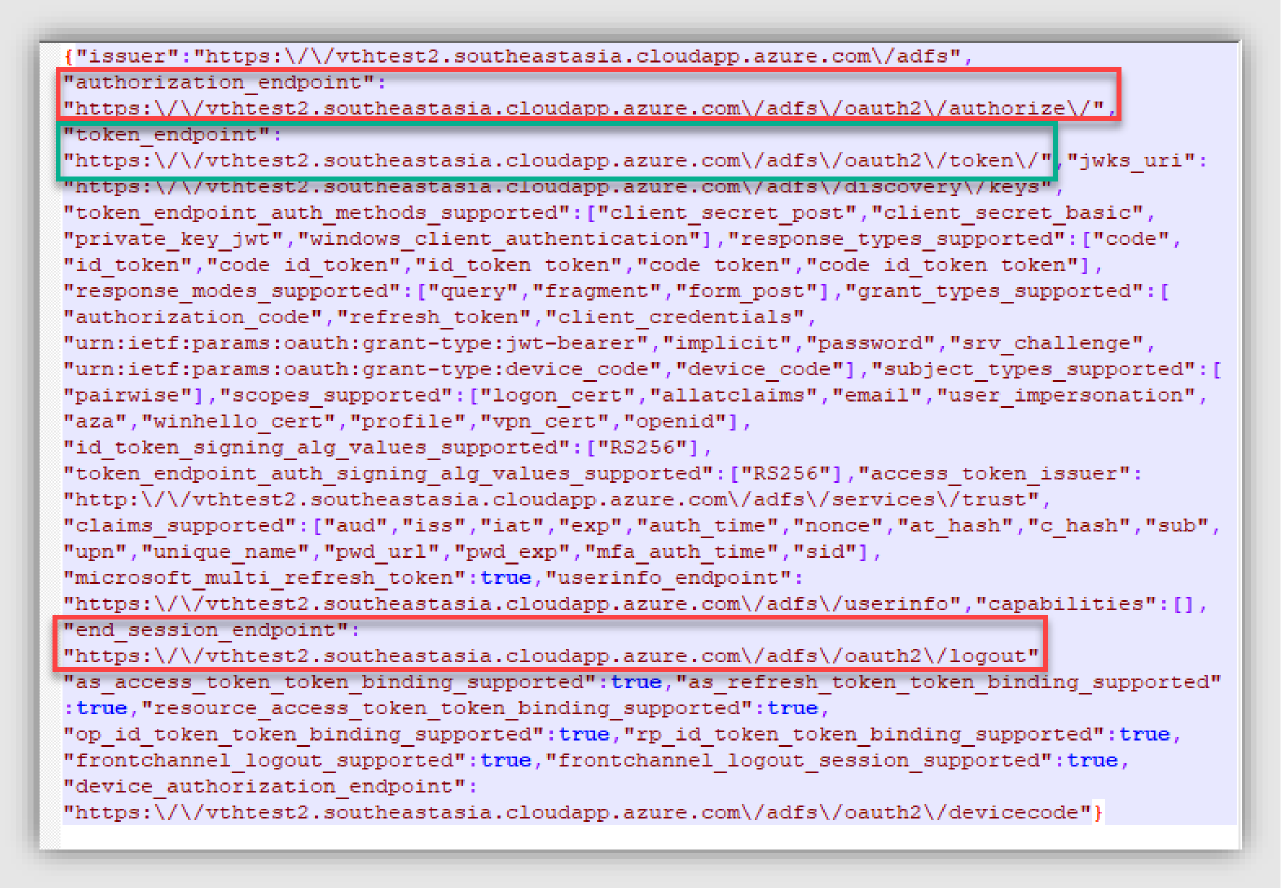
Authorization URL, Token URL and Logout URL

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.

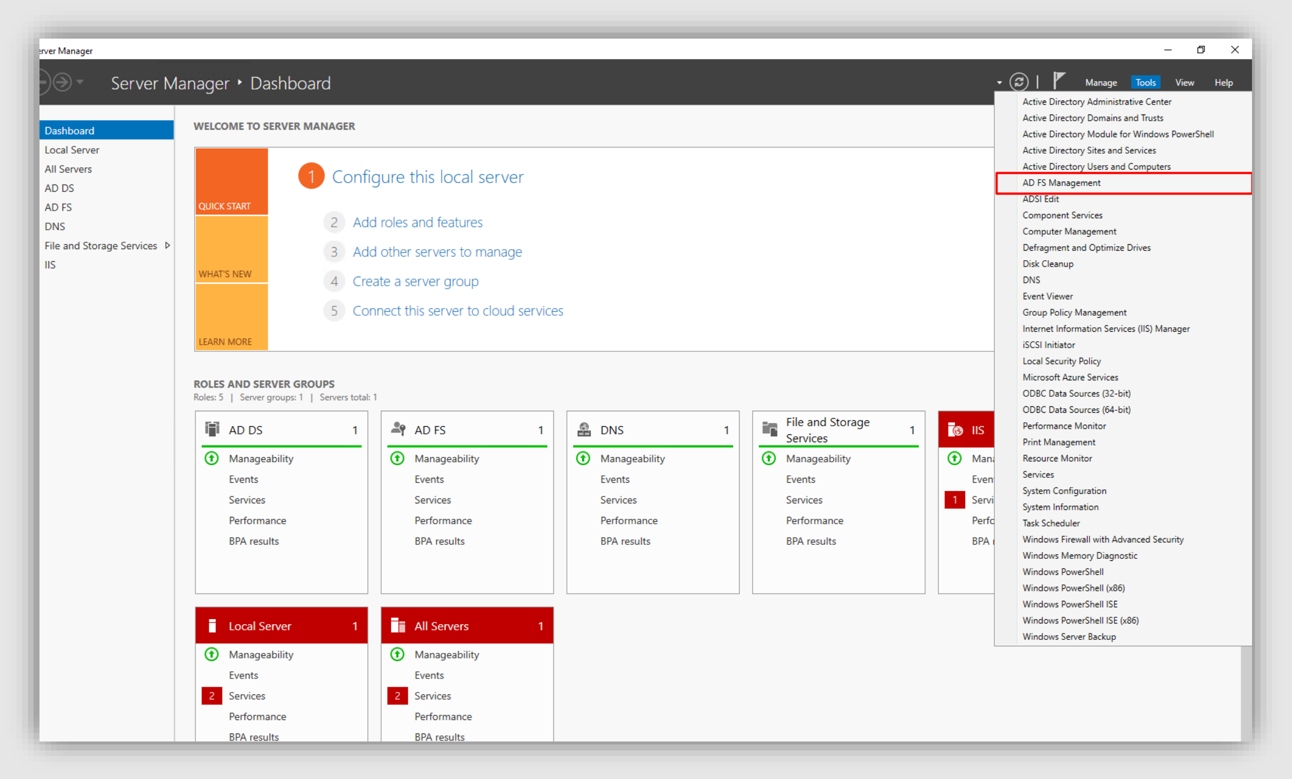
Auto-Login Networks

Refer to this section for more details.

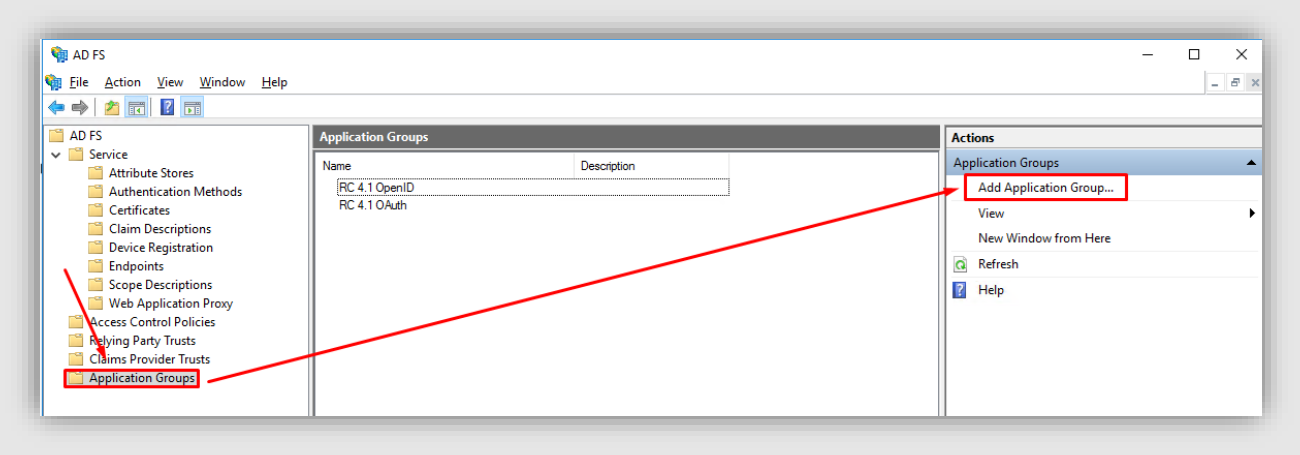
Authentication Details for OpenID Connect with ADFS

Part A. Configure Active Directory Federation Services (ADFS)

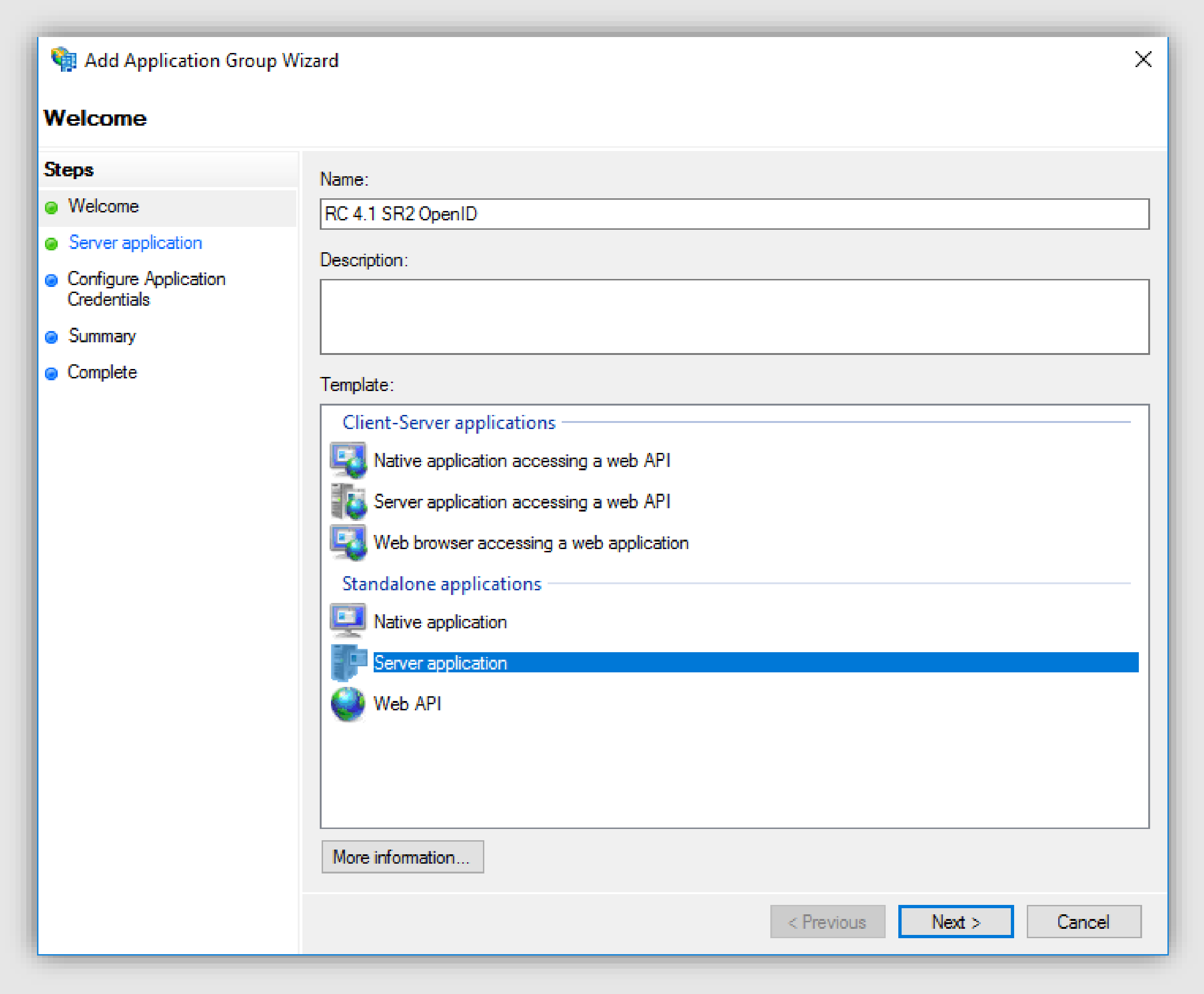
1. Go to **web server** where your Exchange server is installed, click **Start → Server Manager → Tools → AD FS Management**


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.



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
- Summary
- Complete

Name: RC 4.1 SR2 OpenID

Description:

Template:

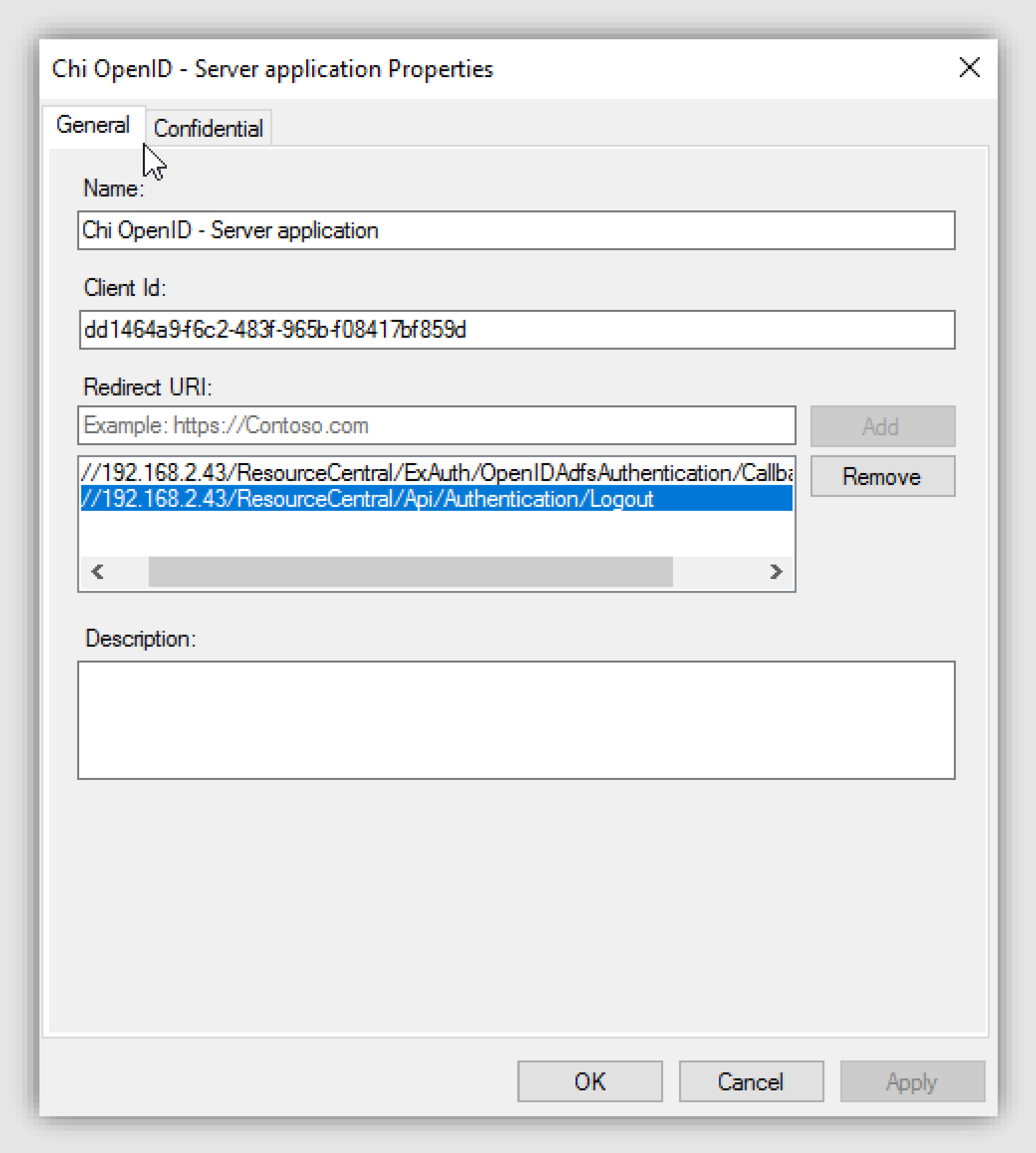
Client-Server applications

- 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



Chi OpenID - Server application Properties

Name:
Chi OpenID - Server application

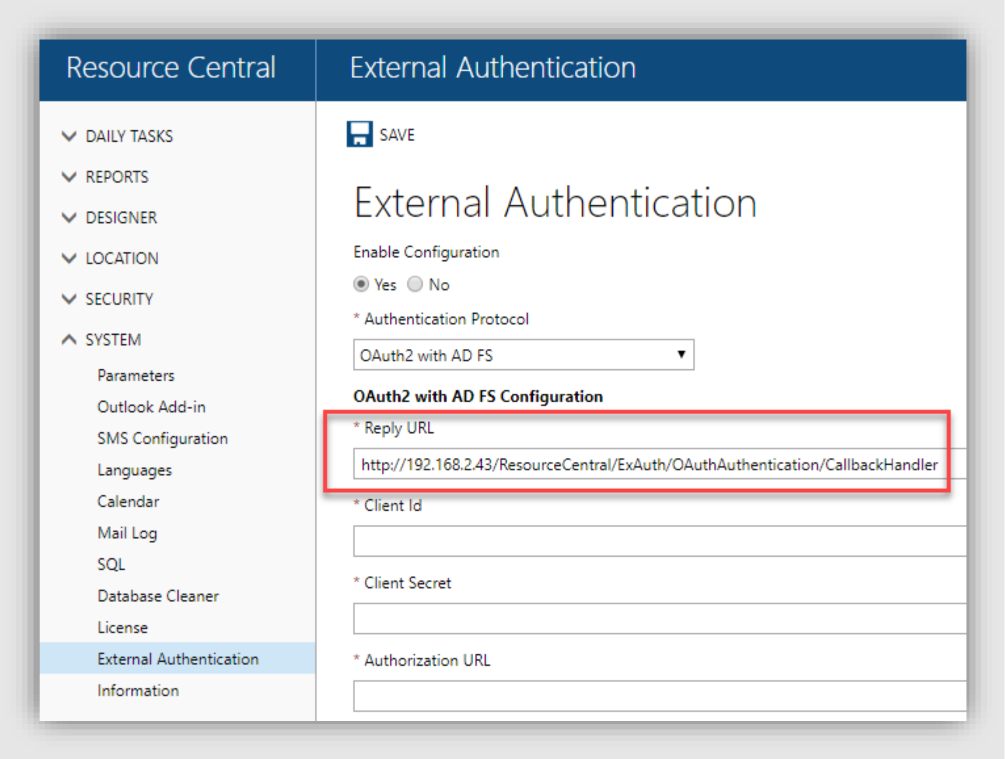
Client Id:
dd1464a9f6c2-483f-965b-f08417bf859d

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

//192.168.2.43/ResourceCentral/ExAuth/OpenIDAdfsAuthentication/Callba
//192.168.2.43/ResourceCentral/Api/Authentication/Logout

Description:

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



External Authentication

Enable Configuration

● Yes ○ No

* Authentication Protocol: OAuth2 with AD FS

OAuth2 with AD FS Configuration

* Reply URL: http://192.168.2.43/ResourceCentral/ExAuth/OAuthAuthentication/CallbackHandler

* Client Id

* Client Secret

* Authorization URL

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

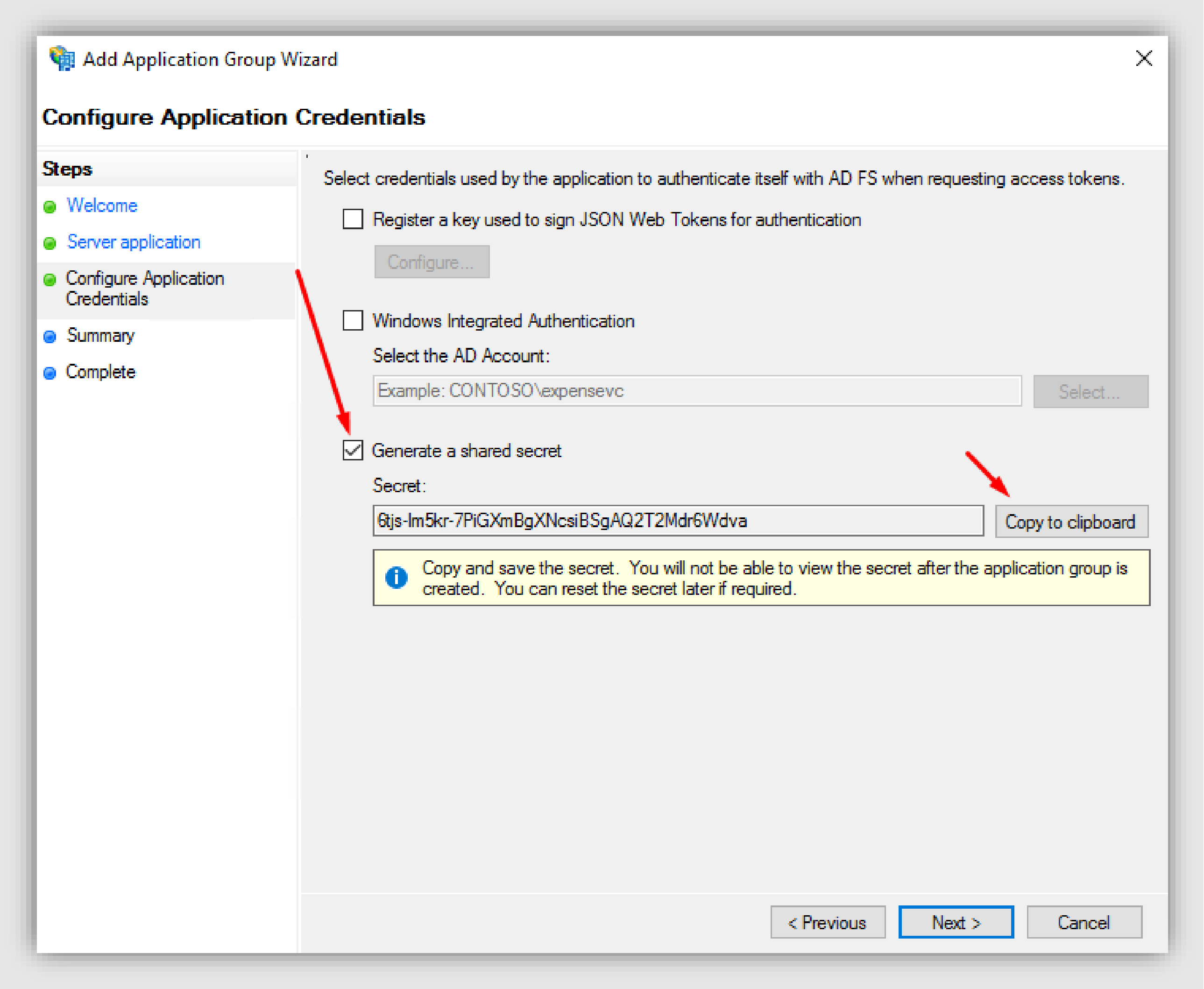
The URL for receiving logout details from ADFS must have the following format:

```
[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
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-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.

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

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

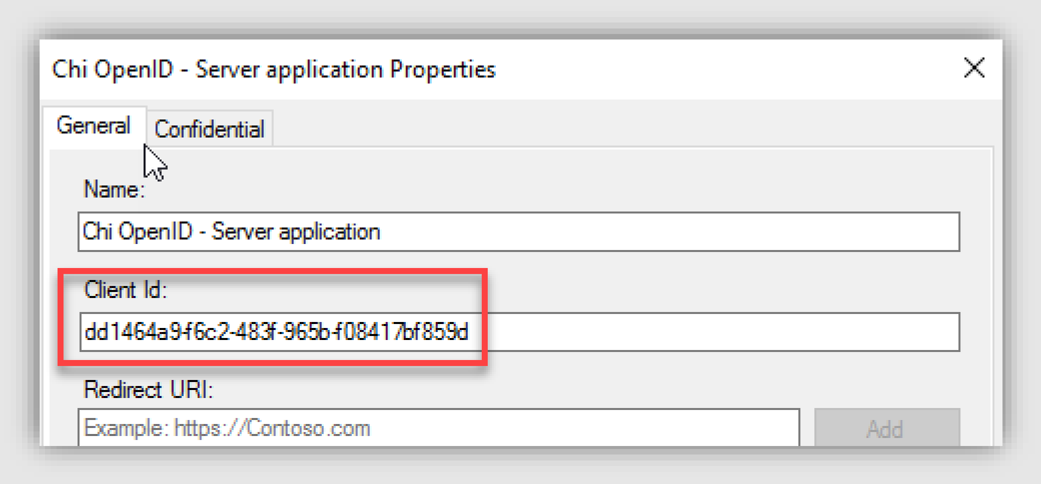
Part B. Retrieve details for OpenID Connect with AD FS Authentication Protocol

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.



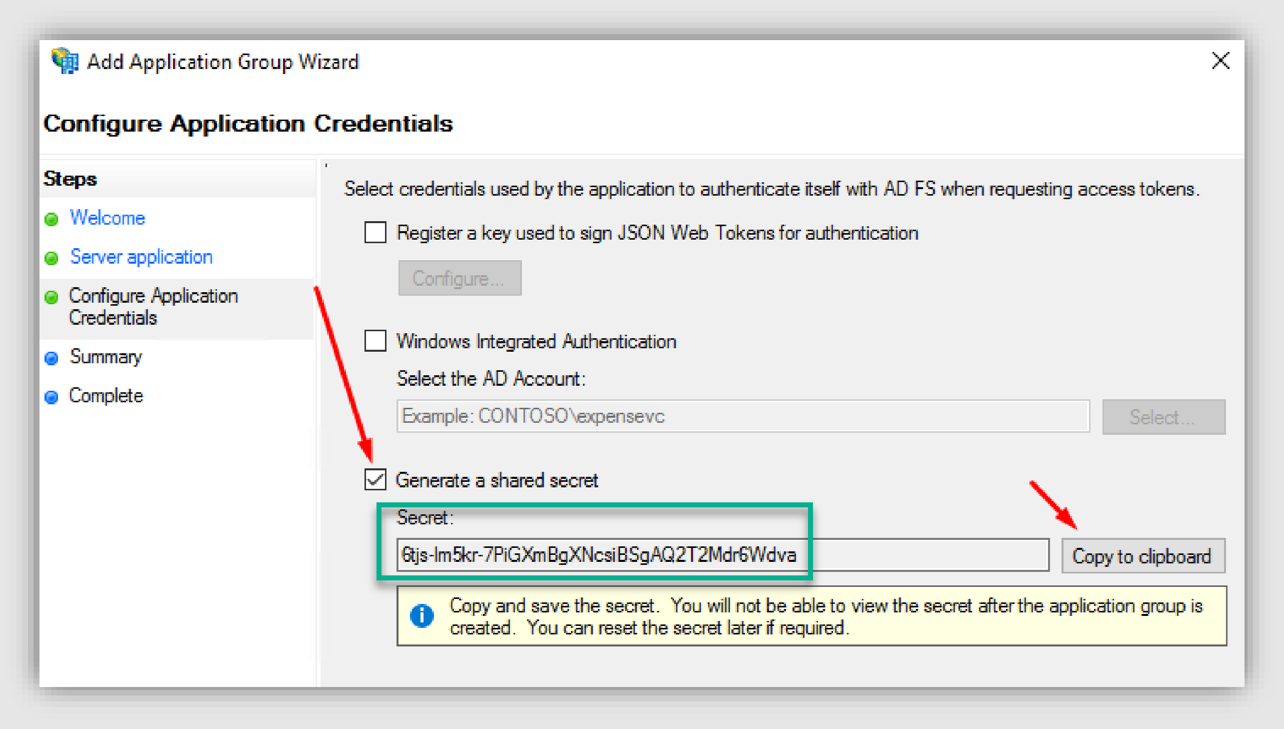
Name: Chi OpenID - Server application

Client Id: dd1464a9f6c2-483f-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).



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.

Authorization URL, Token URL and Logout URL

Refer to this section for more details.

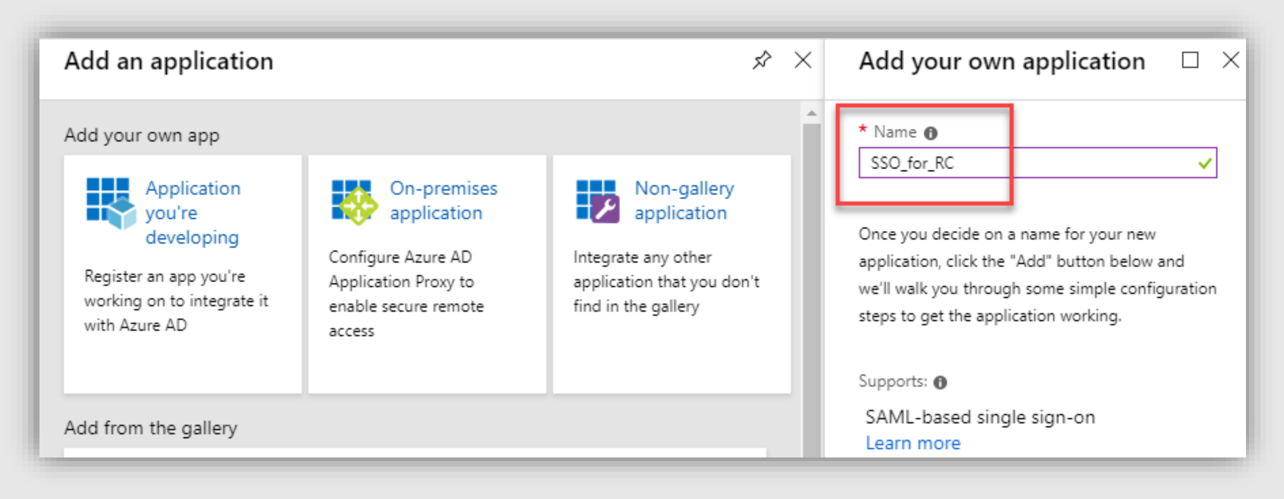
Auto-Login Networks

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**], select Non-gallery application and enter the name for the application:



Add an application

Add your own app

Application you're developing

Register an app you're working on to integrate it with Azure AD

On-premises application

Configure Azure AD Application Proxy to enable secure remote access

Non-gallery application

Integrate any other application that you don't find in the gallery

Add from the gallery

Add your own application

* Name: SSO_for_RC

Once you decide on a name for your new application, click the "Add" button below and we'll walk you through some simple configuration steps to get the application working.

Supports:

SAML-based single sign-on

Learn more

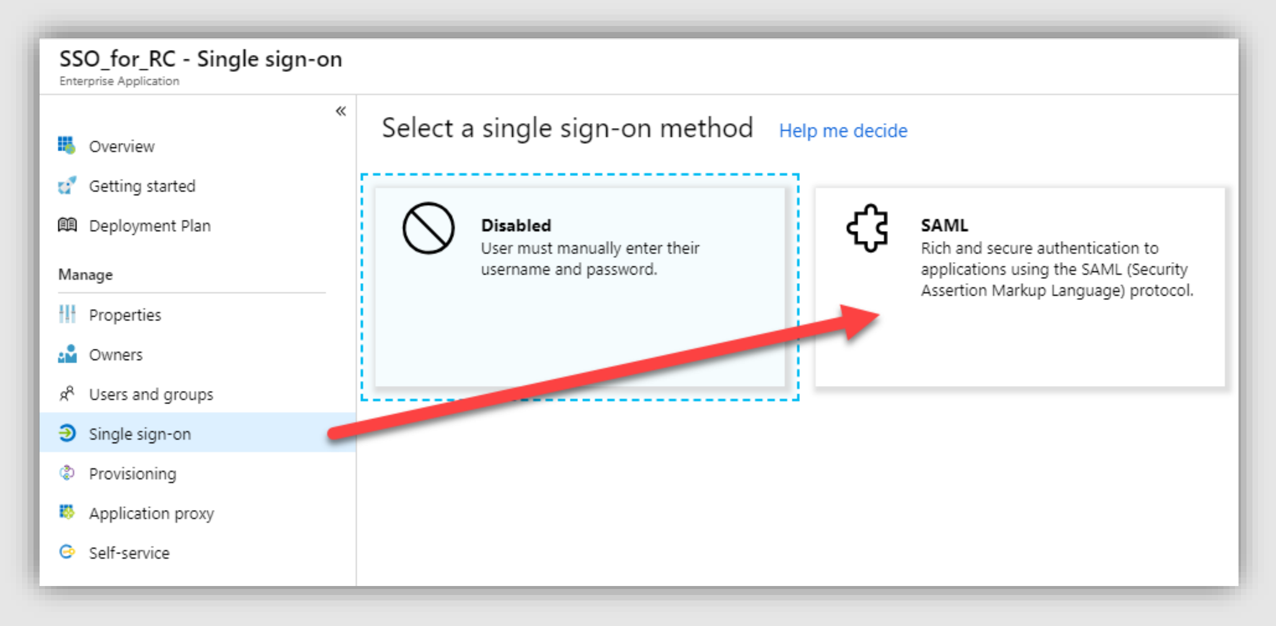
Figure 9. Add non-gallery application

Click [**Add**] 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

Select a single sign-on method

Help me decide

Disabled

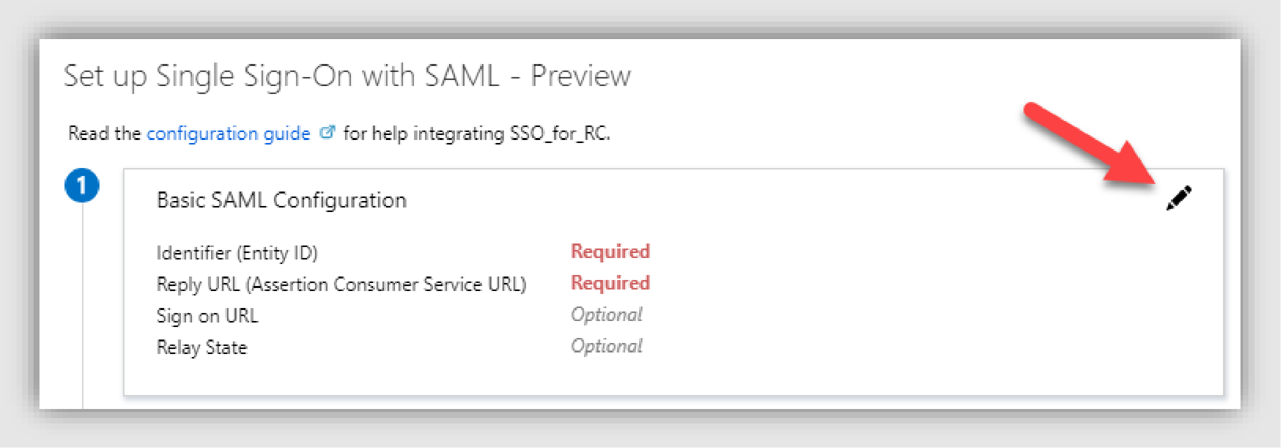
User must manually enter their username and password.

SAML

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

Figure 10. Select SSO method

A new panel is opened.



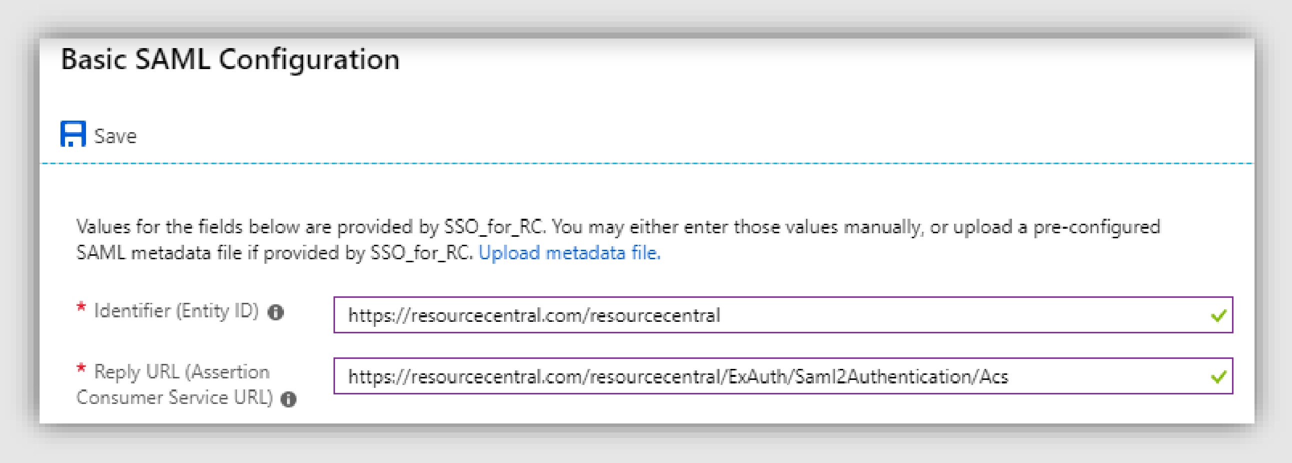
Set up Single Sign-On with SAML - Preview

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

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

Values for the fields below are provided by SSO_for_RC. You may either enter those values manually, or upload a pre-configured SAML metadata file if provided by SSO_for_RC. Upload metadata file.

* Identifier (Entity ID): https://resourcecentral.com/resourcecentral ✓

* Reply URL (Assertion Consumer Service URL): 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:

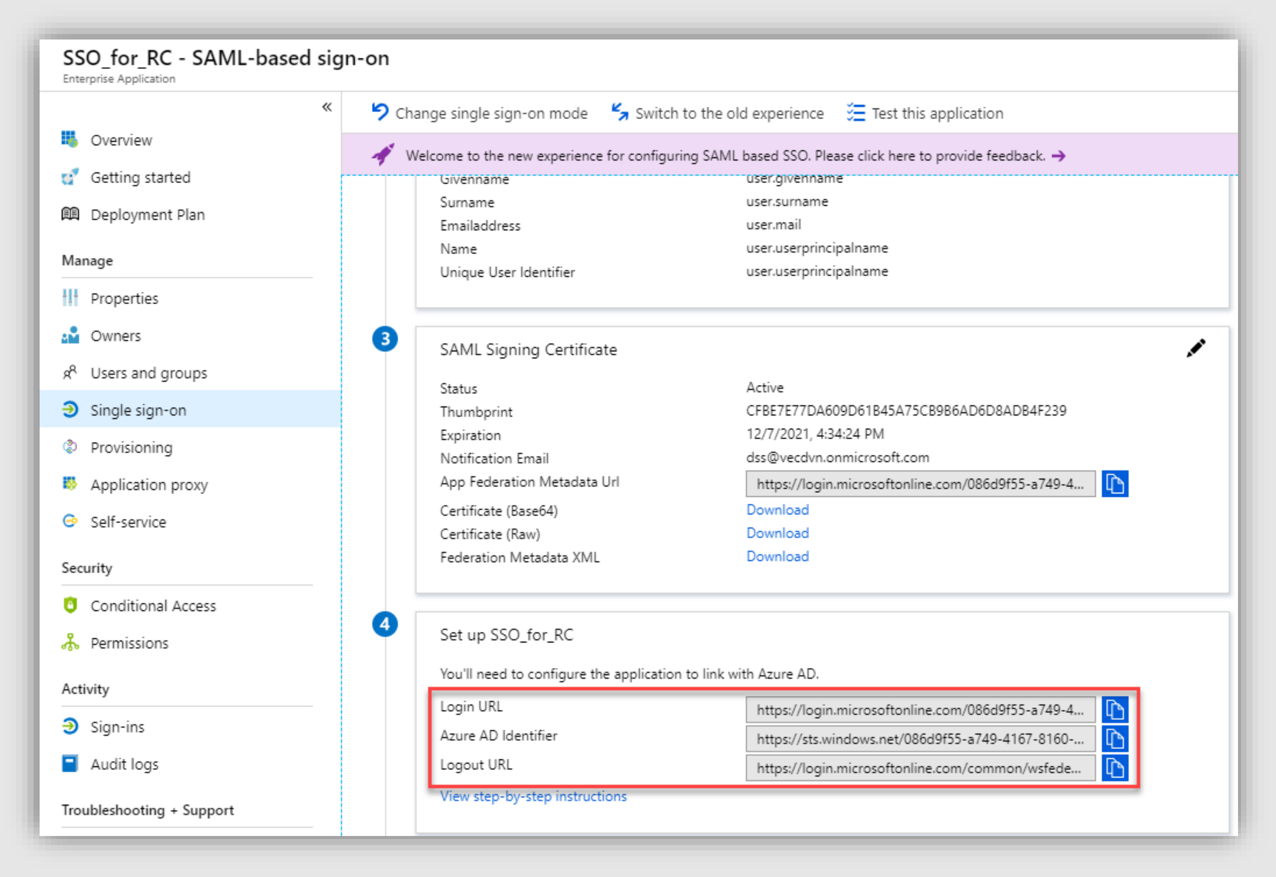
```
[RC Backend URL]/ExAuth/Saml2Authentication/Acs
```

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.** Click [**View 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 SSO_for_RC' section (SSO_for_RC is the application name):


SSO_for_RC - SAML-based sign-on
Enterprise Application
«
Overview
Getting started
Deployment Plan
Manage
Properties
Owners
Users and groups
Single sign-on
Provisioning
Application proxy
Self-service
Security
Conditional Access
Permissions
Activity
Sign-ins
Audit logs
Troubleshooting + Support
Change single sign-on mode
Switch to the old experience
Test this application
Welcome to the new experience for configuring SAML based SSO. Please click here to provide feedback. →
3
4
View step-by-step instructions

Givenname	user.givenname
Surname	user.surname
Emailaddress	user.mail
Name	user.userprincipalname
Unique User Identifier	user.userprincipalname

SAML Signing Certificate

Status	Active
Thumbprint	CFBE7E77DA609D61B45A75CB9B6AD6D8ADB4F239
Expiration	12/7/2021, 4:34:24 PM
Notification Email	dss@vecdvn.onmicrosoft.com
App Federation Metadata Url	https://login.microsoftonline.com/086d9f55-a749-4...
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/086d9f55-a749-4...
Azure AD Identifier	https://sts.windows.net/086d9f55-a749-4167-8160-...
Logout URL	https://login.microsoftonline.com/common/wsfede...

Figure 11. 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

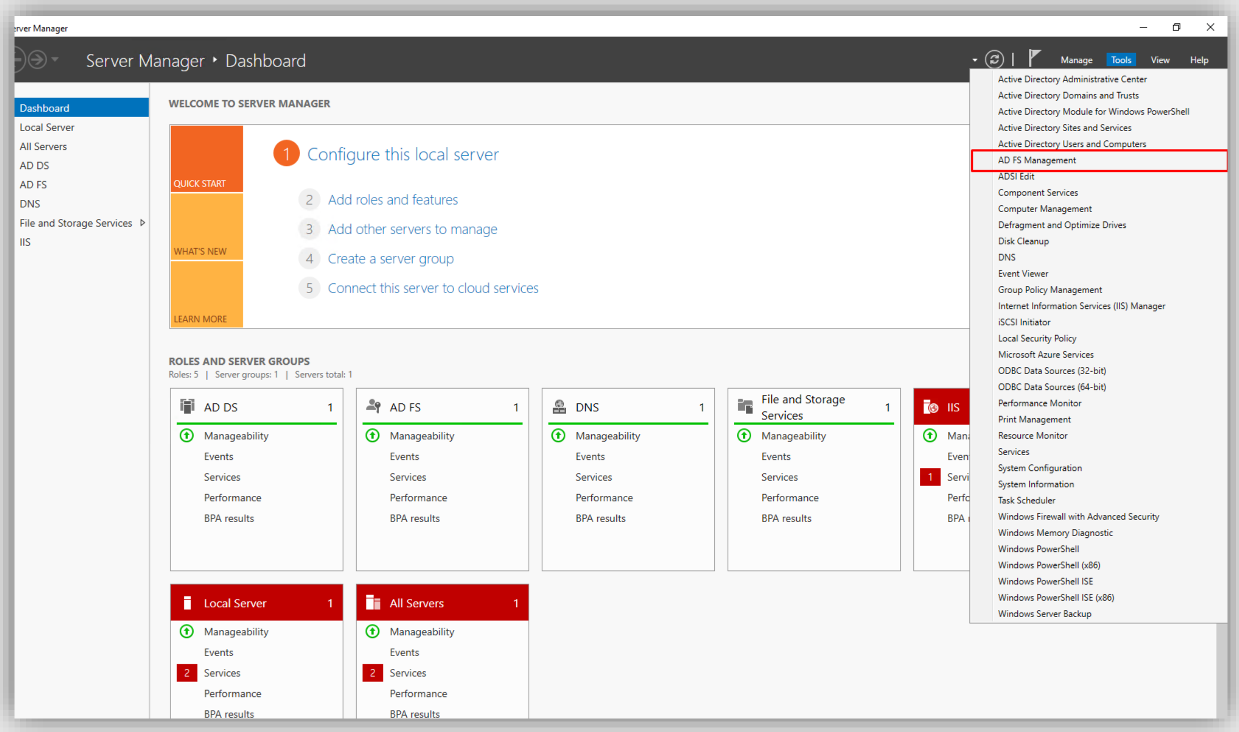
Refer to this section for more details.

Authentication Details for SAML2 with ADFS

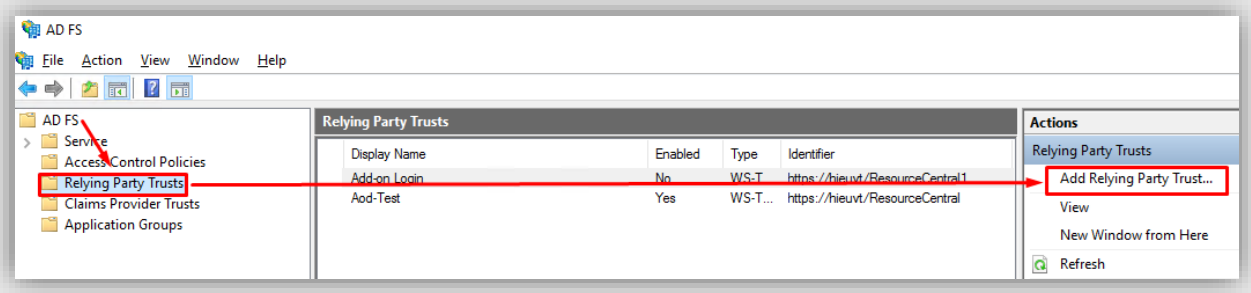
The SAML2 with AD FS protocol has the same code flow as that of SAML2. Therefore, authentication details for SAML2 with AD FS can be input to the data fields of SAML2 protocol.

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

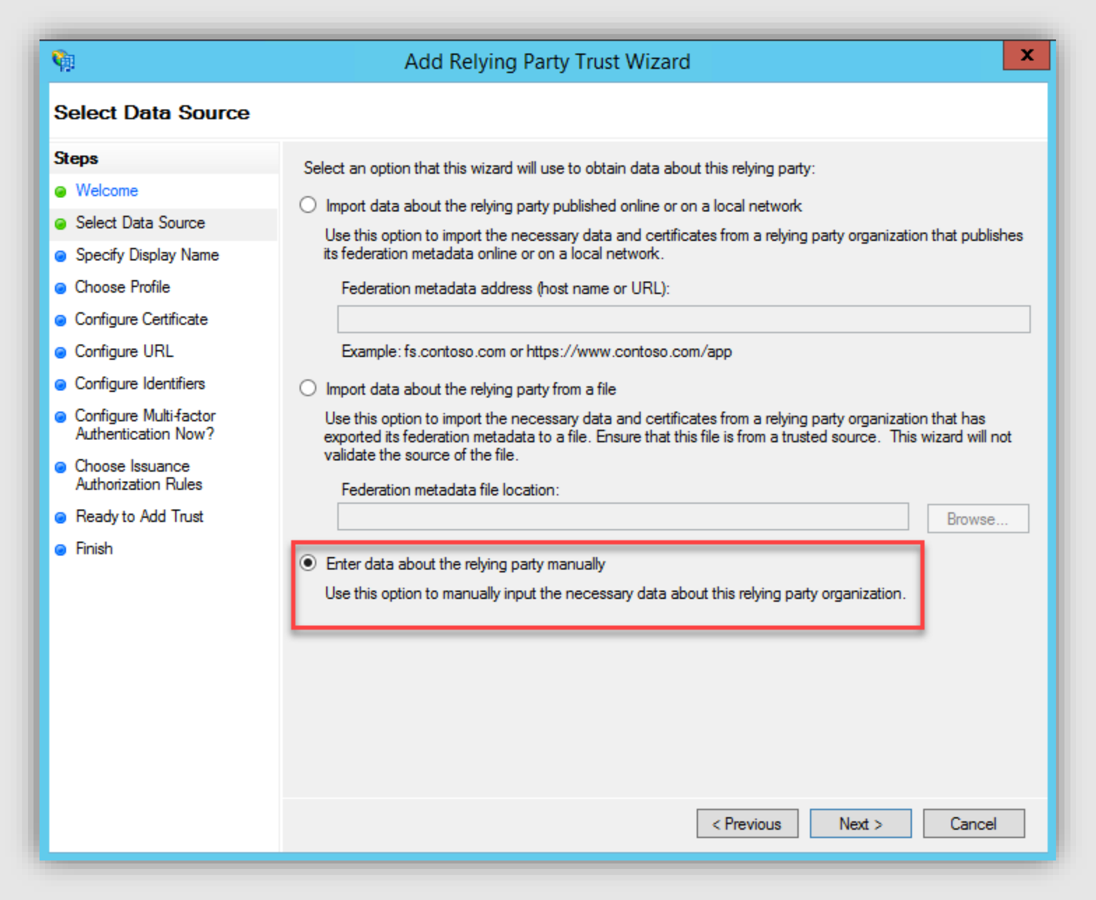
2. In the opened window, select **Replying Party Trusts** and [**Add Replying Party Trust...**] from the **Actions** sidebar. This starts the configuration wizard for a new **Replying Party Trust**.



Relying Party Trusts

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.

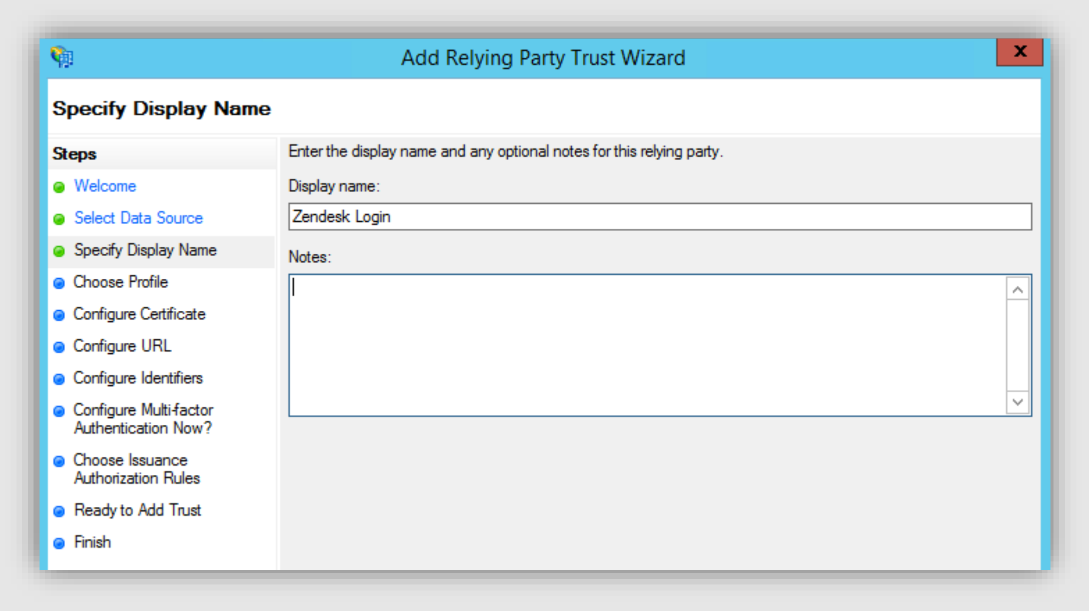
Federation metadata file location:

● 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

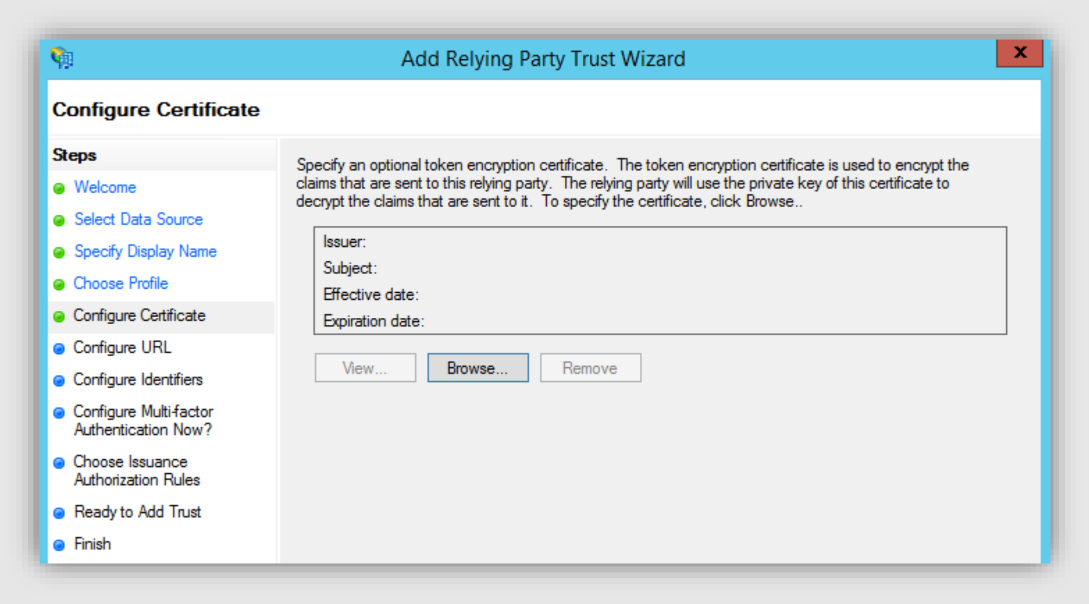
Steps
- Welcome
- Select Data Source
- Specify Display Name
- Choose Profile
- Configure Certificate
- Configure URL
- Configure Identifiers
- Configure Multi-factor Authentication Now?
- Choose Issuance Authorization Rules
- Ready to Add Trust
- Finish

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.

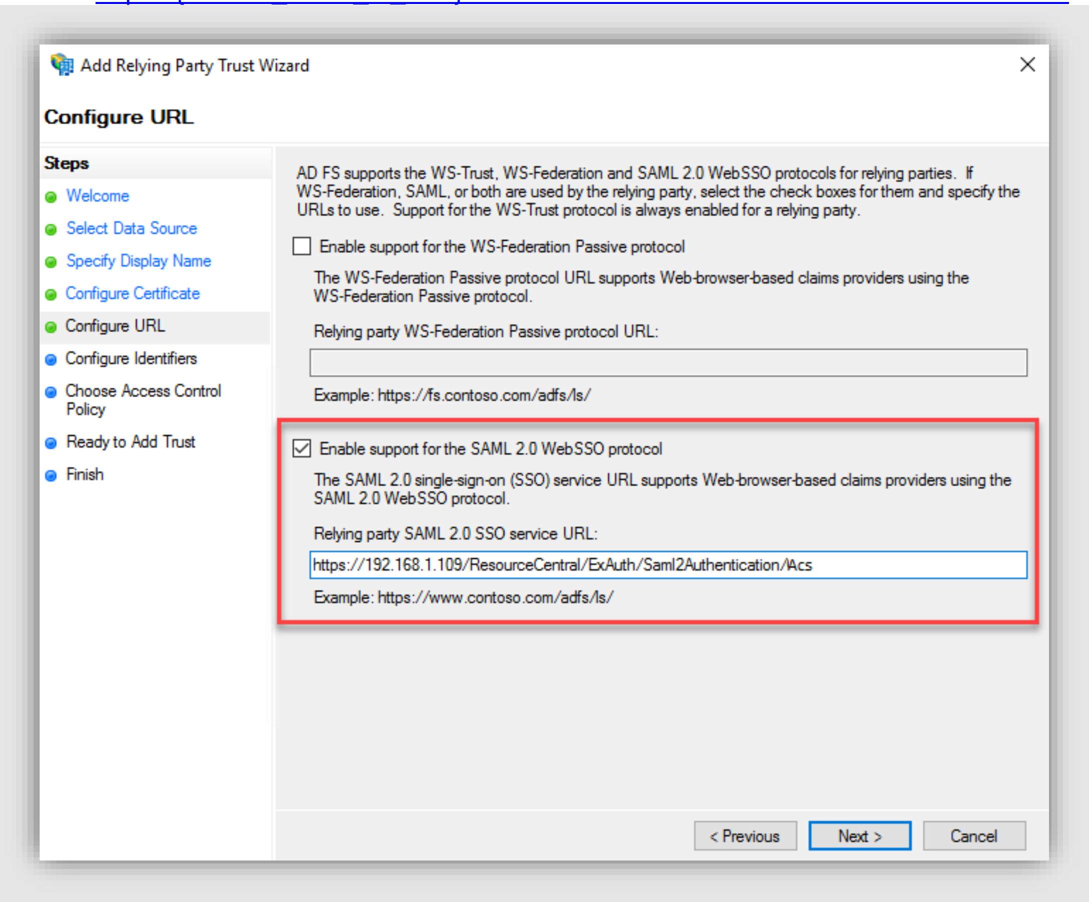


Configure Certificate

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: https://{domain_name_rc_web}/ResourceCentral/ExAuth/Saml2Authentication/Acs



Configure URL

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.

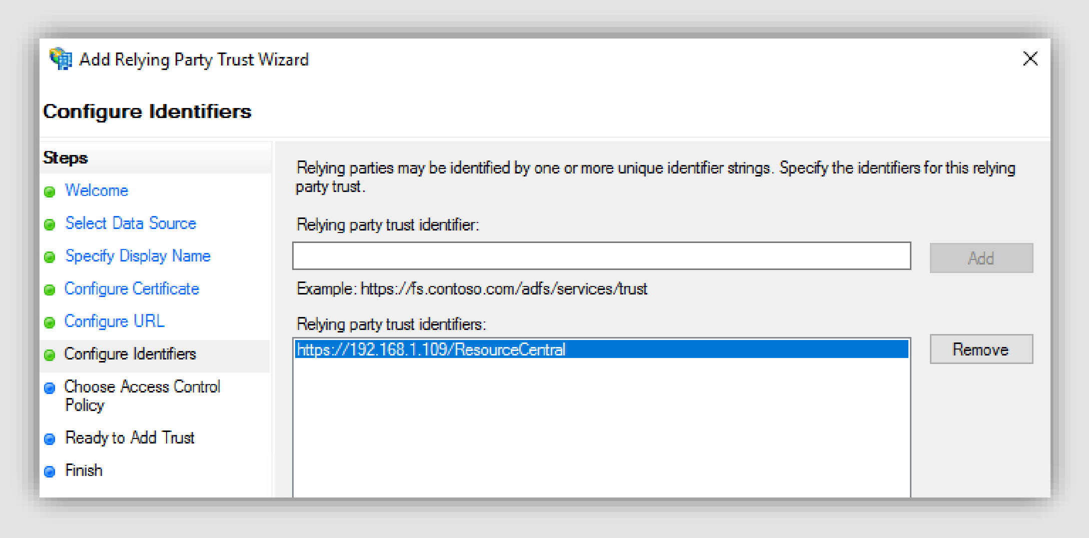
Relying party SAML 2.0 SSO service URL:

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: https://{domain_name_rc_web}/ResourceCentral



Configure Identifiers

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

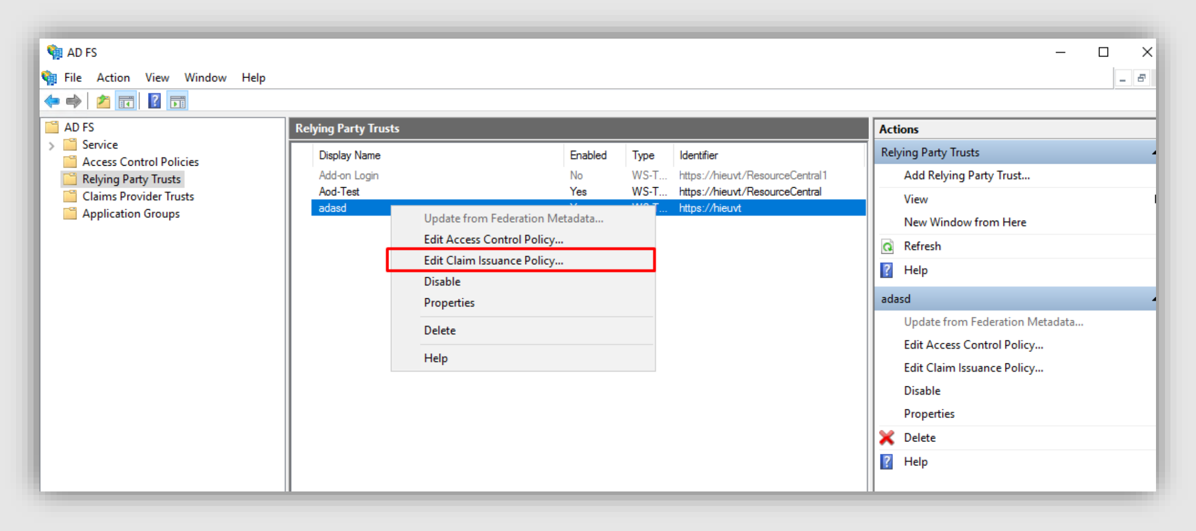
Then click [**Next**] to proceed.

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).

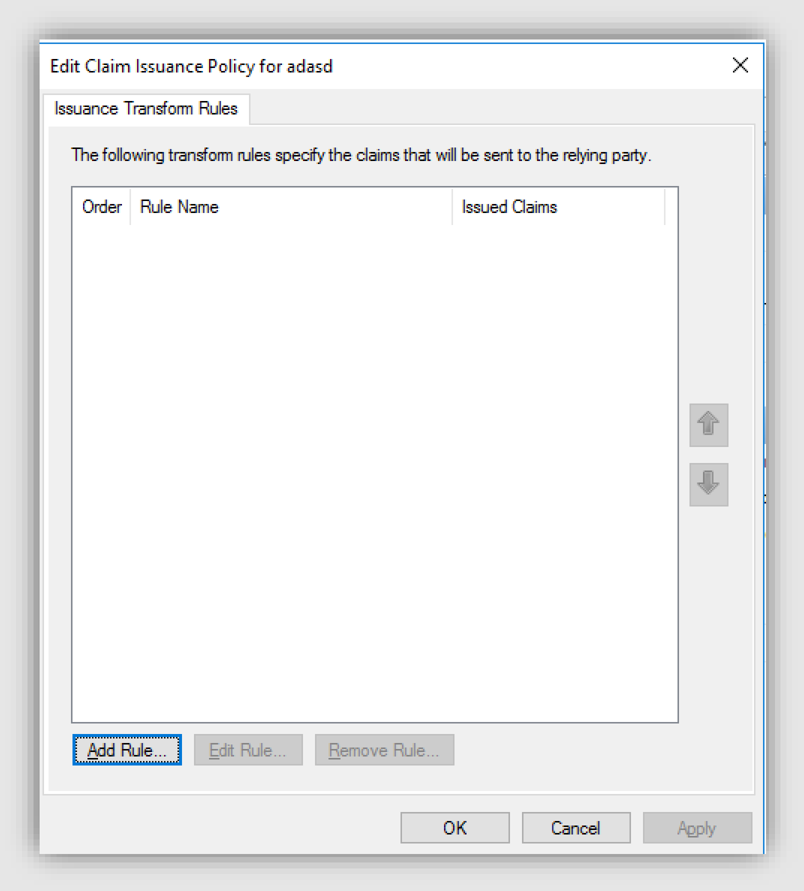


AD FS
File Action View Window Help
AD FS
Service
Access Control Policies
Relying Party Trusts
Claims Provider Trusts
Application Groups
Update from Federation Metadata...
Edit Access Control Policy...
Edit Claim Issuance Policy...
Disable
Properties
Delete
Help
Actions
Relying Party Trusts
Add Relying Party Trust...
View
New Window from Here
Refresh
Help
adasd
Update from Federation Metadata...
Edit Access Control Policy...
Edit Claim Issuance Policy...
Disable
Properties
Delete
Help

Relying Party Trusts

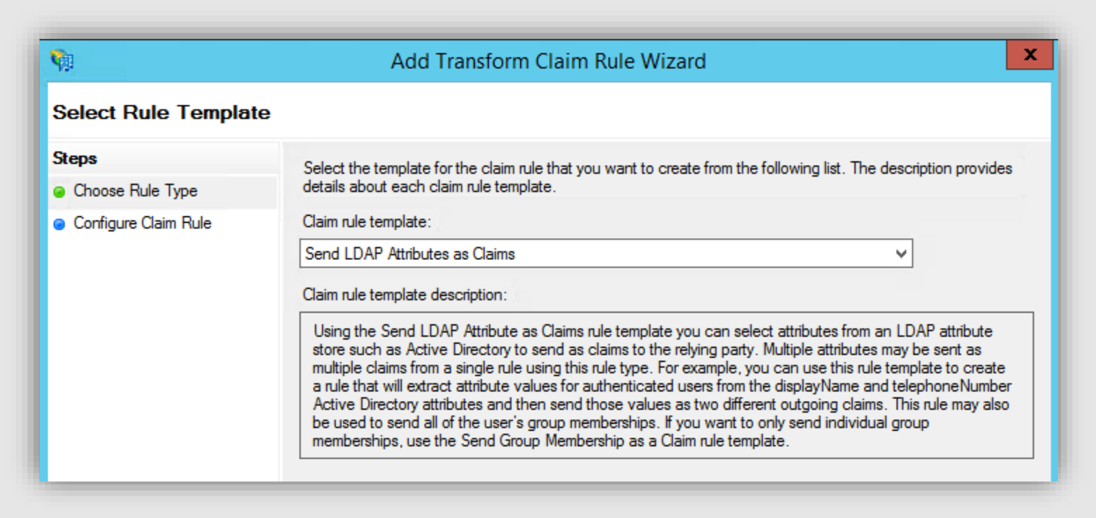
Display Name	Enabled	Type	Identifier
Add-on Login	No	WS-T...	https://hieuvt/ResourceCentral1
Aod-Test	Yes	WS-T...	https://hieuvt/ResourceCentral
adasd	Y...	WS-T...	https://hieuvt

This starts the configuration wizard for a new claim.



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

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



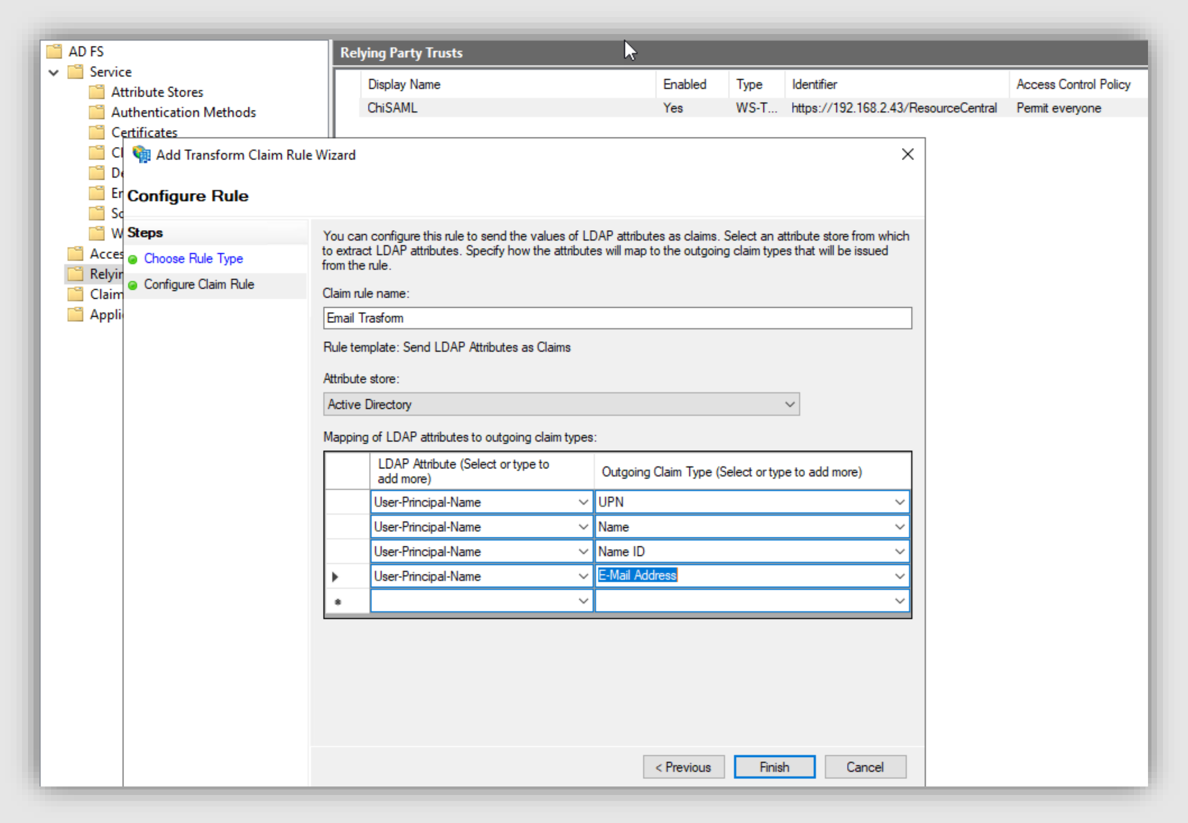
Select the template for the claim rule that you want to create from the following list. The description provides details about each claim rule template.

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.

2. On the next screen, using **Active Directory** as your attribute store, do the following:
   a. From the **LDAP Attribute** column, select **User-Principal-Name**.
   b. From the **Outgoing Claim Type**, select **UPN**.



Display Name	Enabled	Type	Identifier	Access Control Policy
ChiSAML	Yes	WS-T...	https://192.168.2.43/ResourceCentral	Permit everyone

Add Transform Claim Rule Wizard

Configure 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.

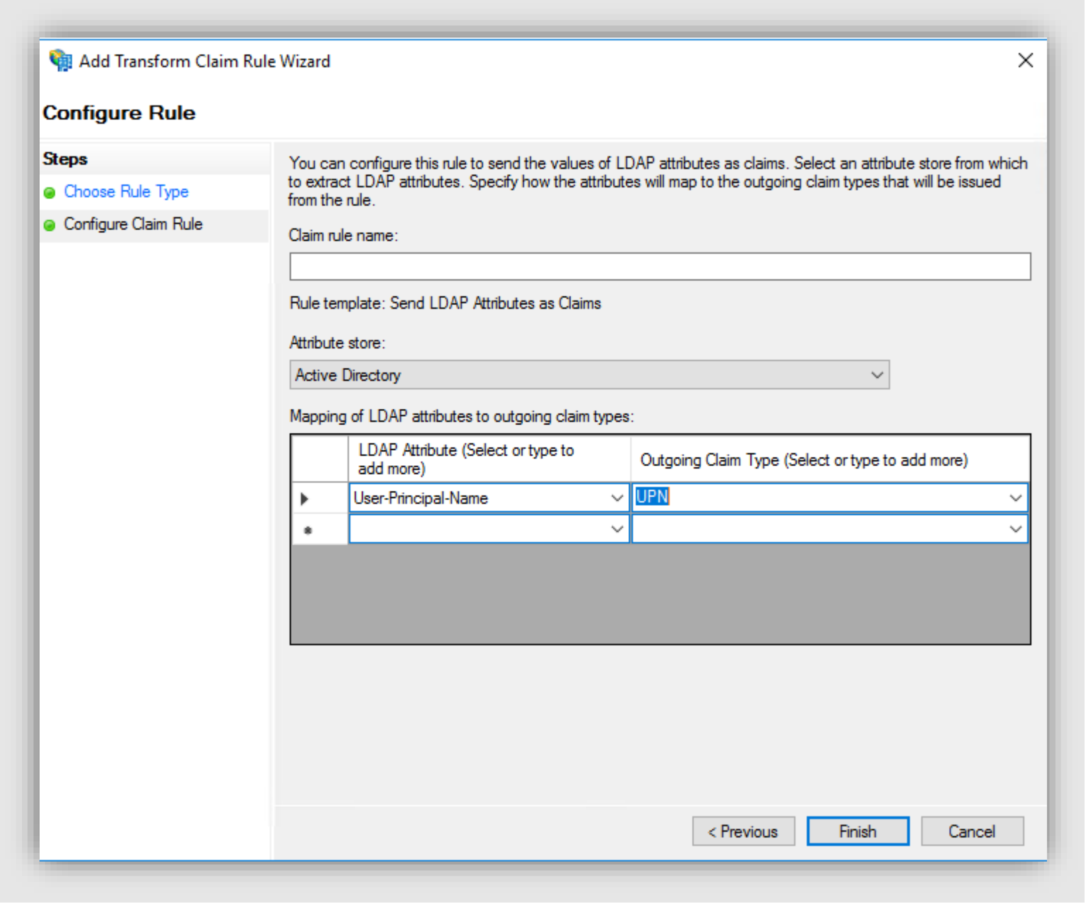
Claim rule name: Email Trasform

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)
User-Principal-Name	UPN
User-Principal-Name	Name
User-Principal-Name	Name ID
User-Principal-Name	E-Mail Address



Add Transform Claim Rule Wizard

Configure 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:

Rule template: Send LDAP Attributes as Claims

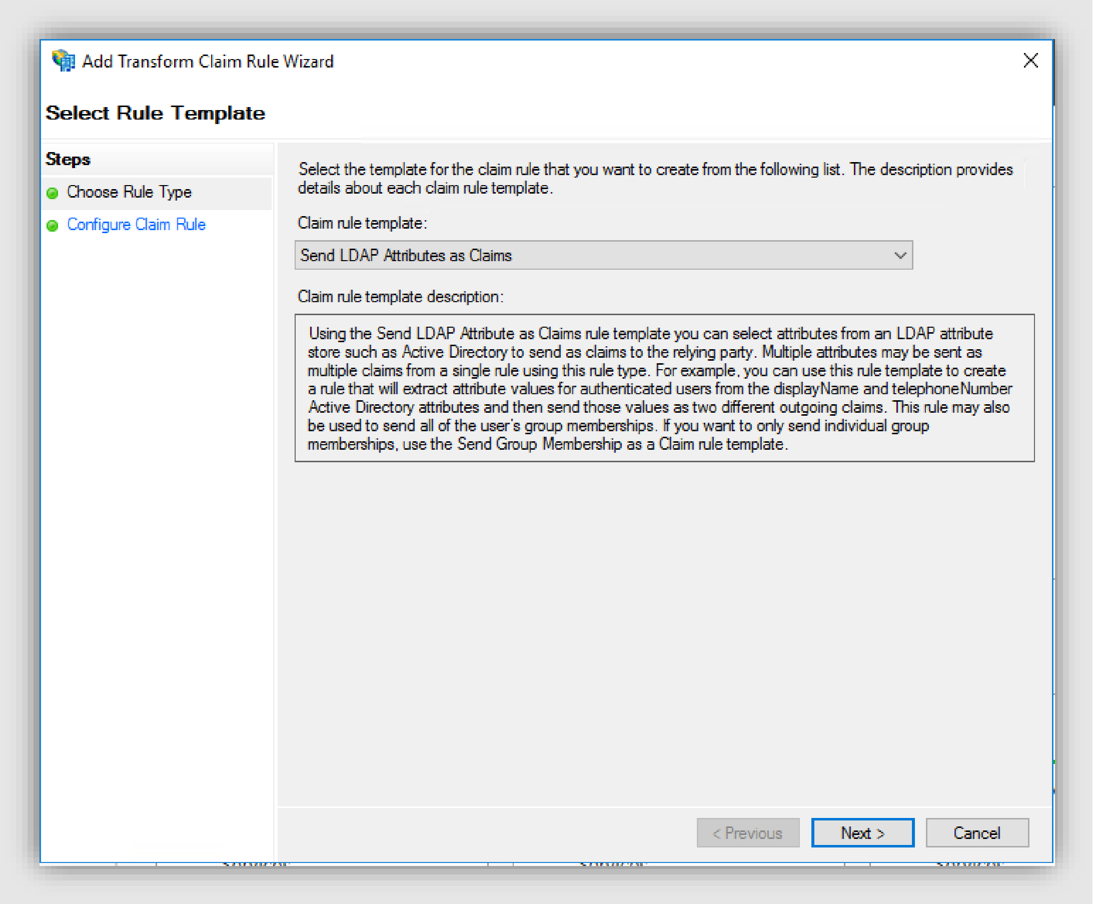
Attribute store: Active Directory

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)
User-Principal-Name	UPN

3. Click [OK] to save the new rule.

4. Create another new rule by clicking [**Add 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.

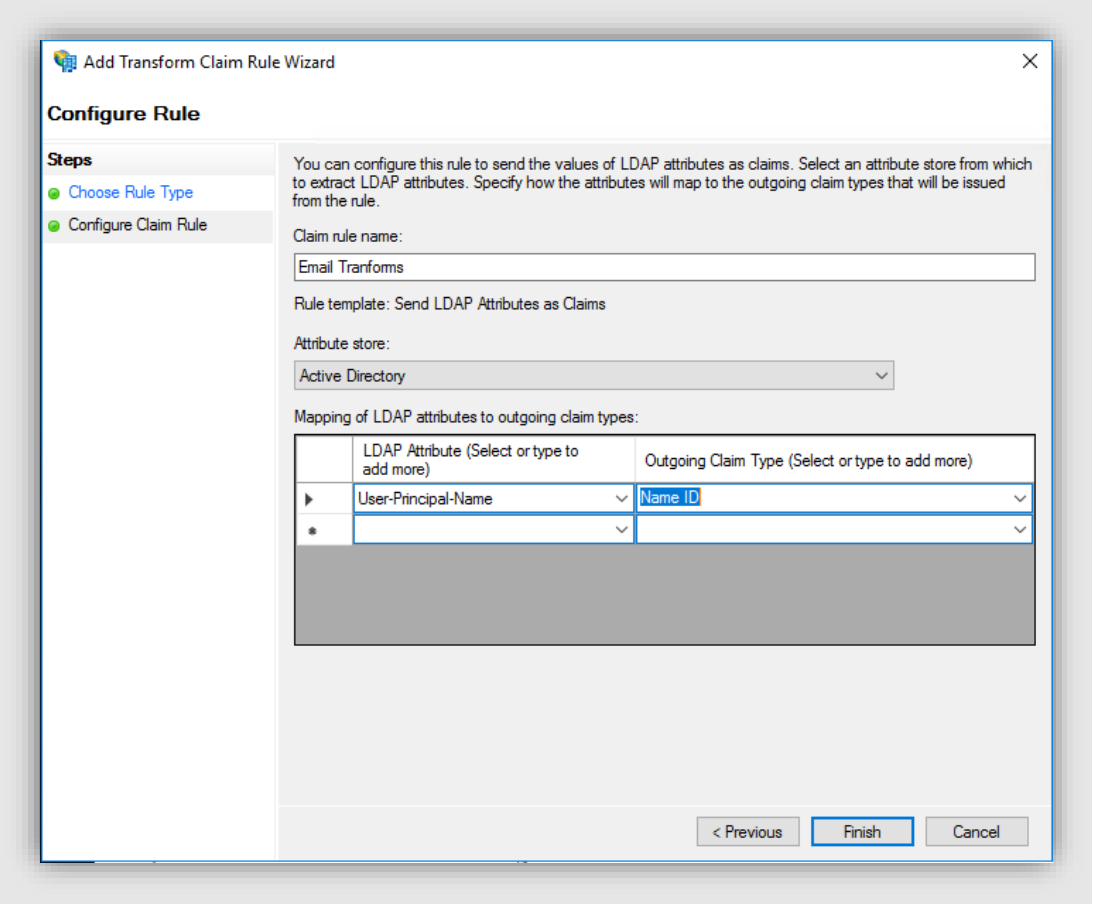
Claim rule template: Send LDAP Attributes as Claims

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.

5. On the next screen:
   a. Select **E-mail Address** or **User-Principal-Name** as the **Incoming claim type** (LDAP Attribute).
   b. For **Outgoing Claim Type**, select **Name ID**.
   c. For **Outgoing Name ID Format**, select **Email**.

   Leave the rule to the default of Pass through all claim values.



Add Transform Claim Rule Wizard

Configure 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: Email Tranforms

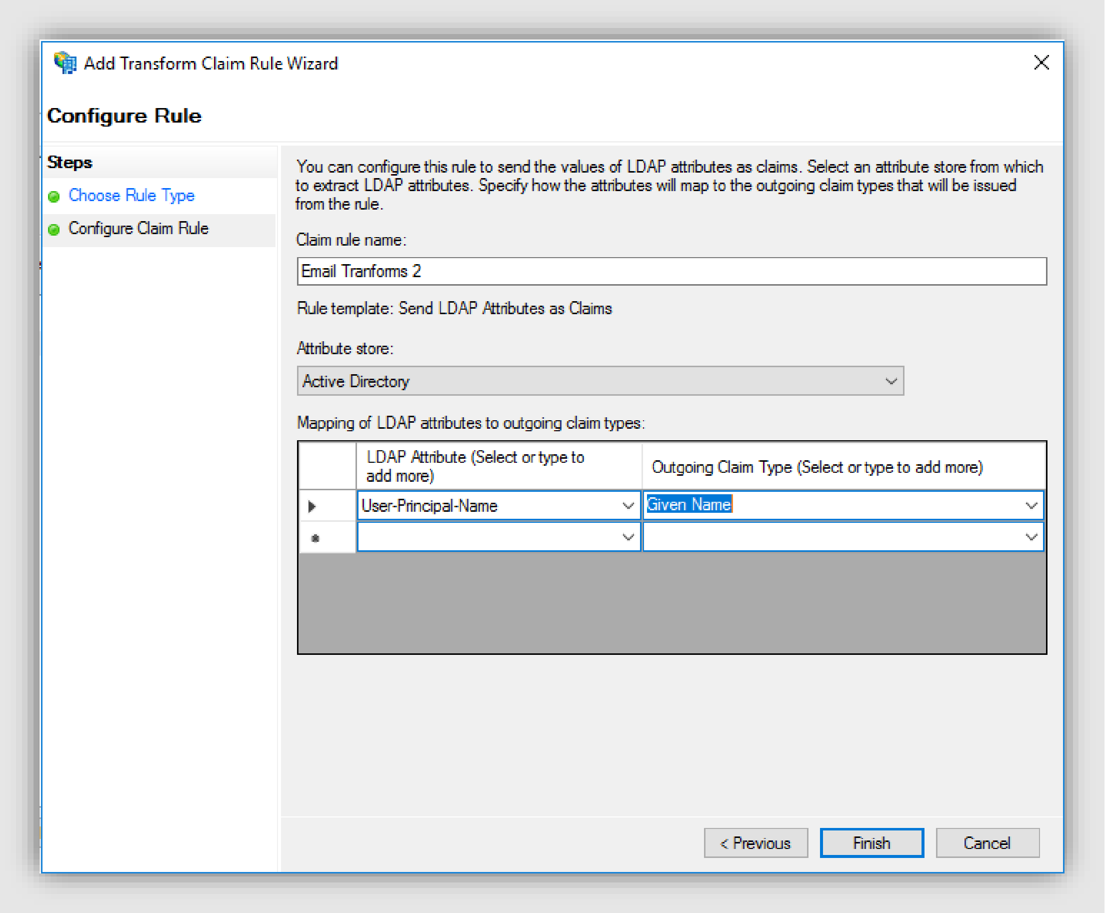
Rule template: Send LDAP Attributes as Claims

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)
User-Principal-Name	Name ID

6. Click [**OK**] to create the claim rule, and then [**OK**] again to finish creating rules.
7. After that, repeat Steps 4-6 to create another claim rule, but this time select **User-Principal-Name** for LDAP Attribute and **Given Name** for Out Going Type.



Configure 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: Email Tranforms 2

Rule template: Send LDAP Attributes as Claims

Attribute store: Active Directory

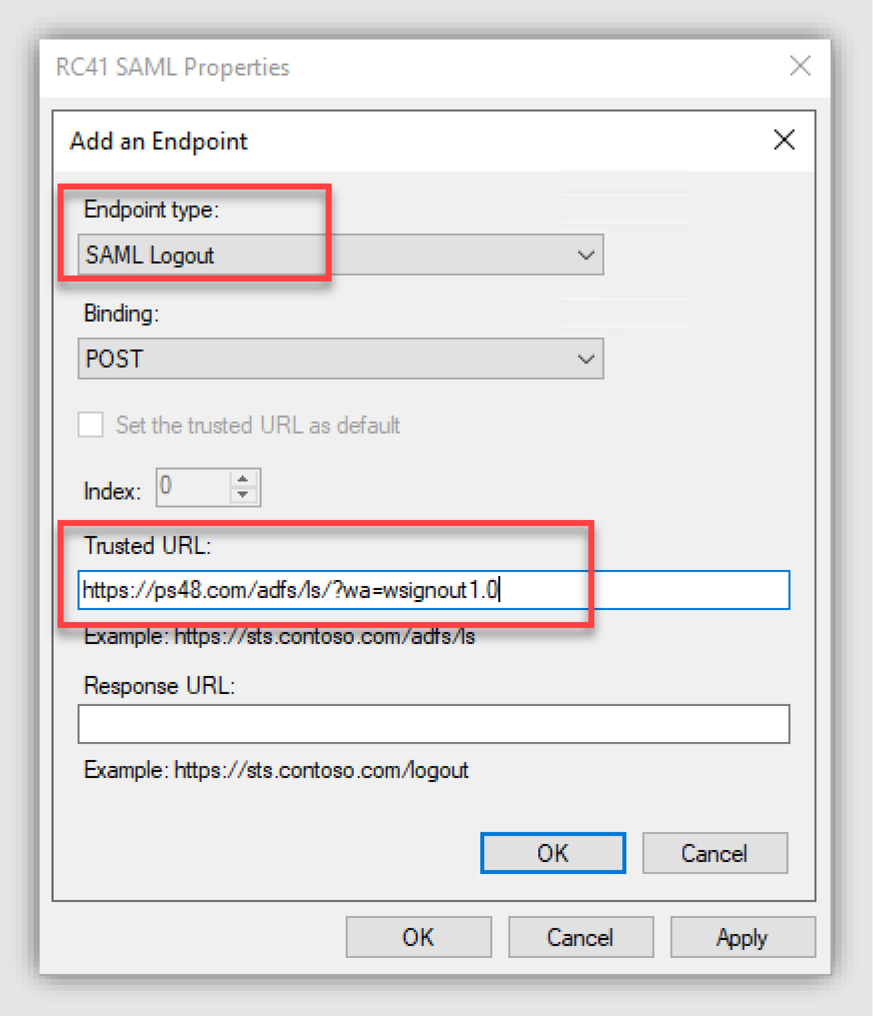
Mapping of LDAP attributes to outgoing claim types:

	LDAP Attribute (Select or type to add more)	Outgoing Claim Type (Select or type to add more)
▶	User-Principal-Name	Given Name
*		

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.



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:

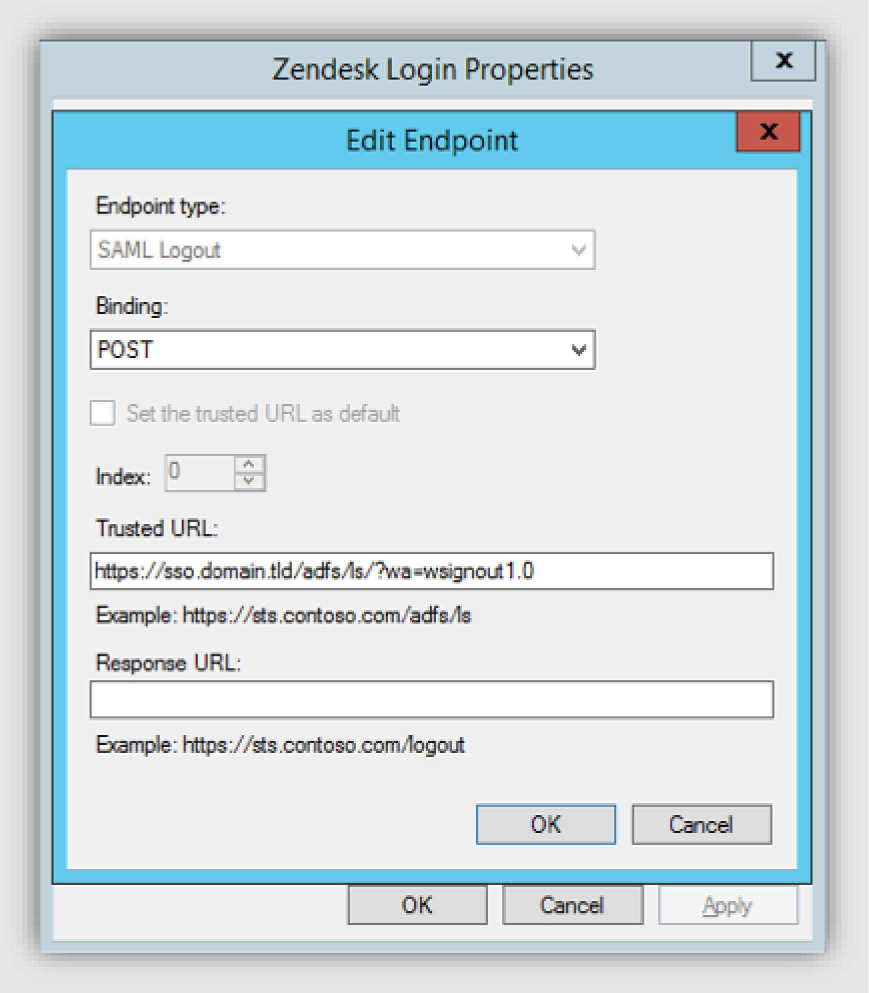
Example: https://sts.contoso.com/logout

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

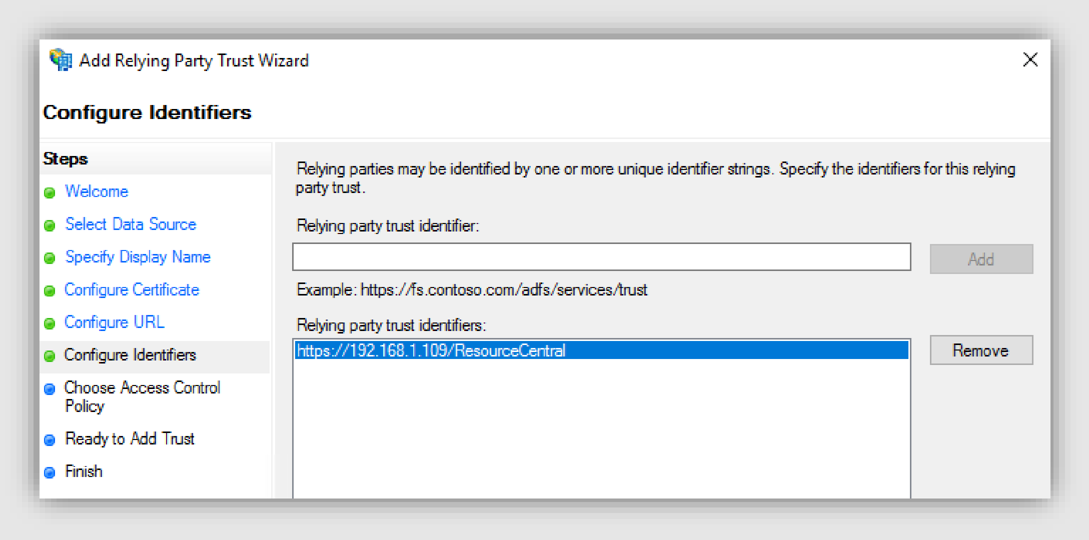
Response URL:

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

Part 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:

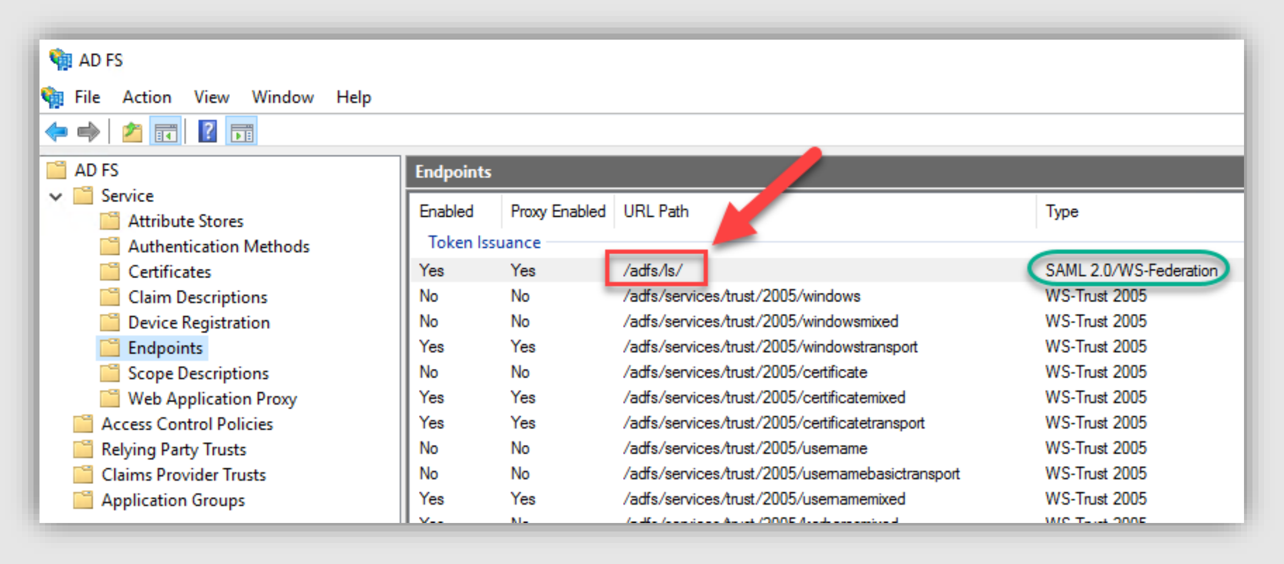
Example: https://fs.contoso.com/adfs/services/trust

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**



Endpoints

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

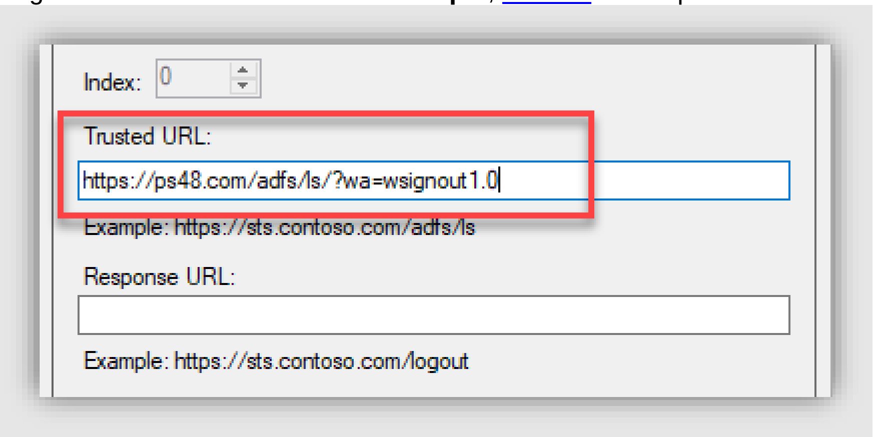
3. Compose the Login URL with the following format:

```
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

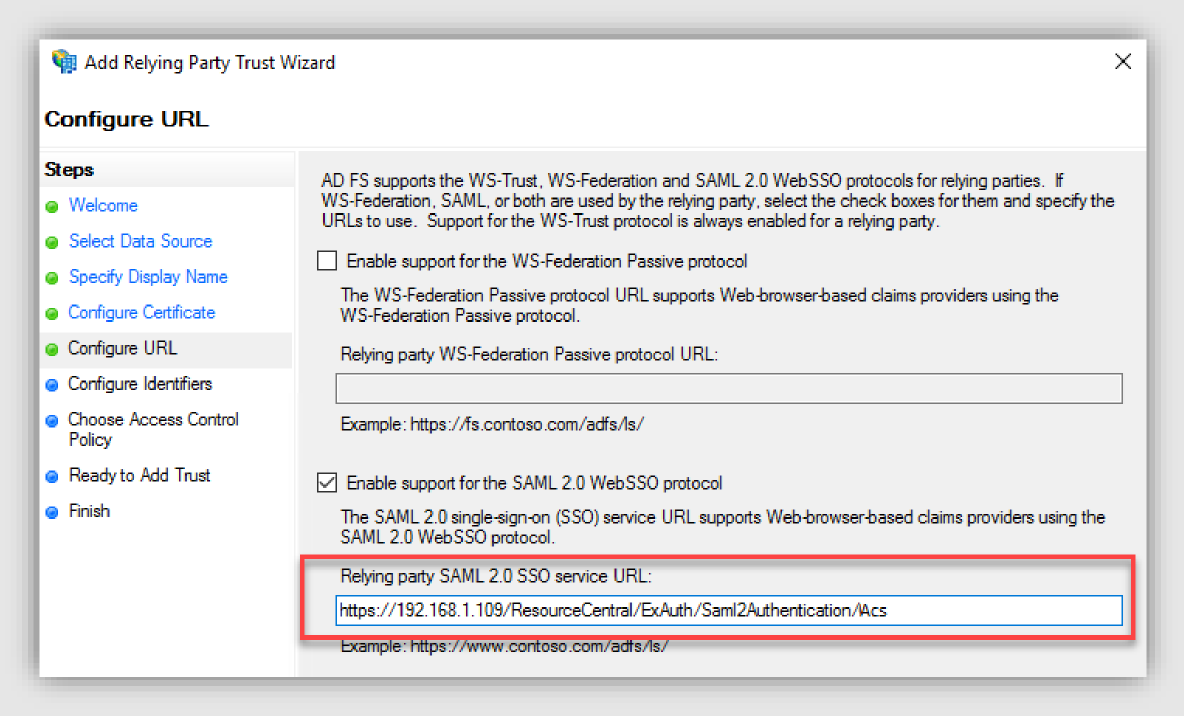
Example: https://sts.contoso.com/adfs/ls

Response URL:

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

Return URL

Return URL is the **Replying party SAML 2.0 SSO service URL** in **Step 7**, Part A1 of this protocol.



Add Relying Party Trust Wizard

Configure URL

Steps

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

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

☐ Enable support for the WS-Federation Passive protocol

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

Relying party WS-Federation Passive protocol URL:

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

☑ Enable support for the SAML 2.0 WebSSO protocol

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

Relying party SAML 2.0 SSO service URL:

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

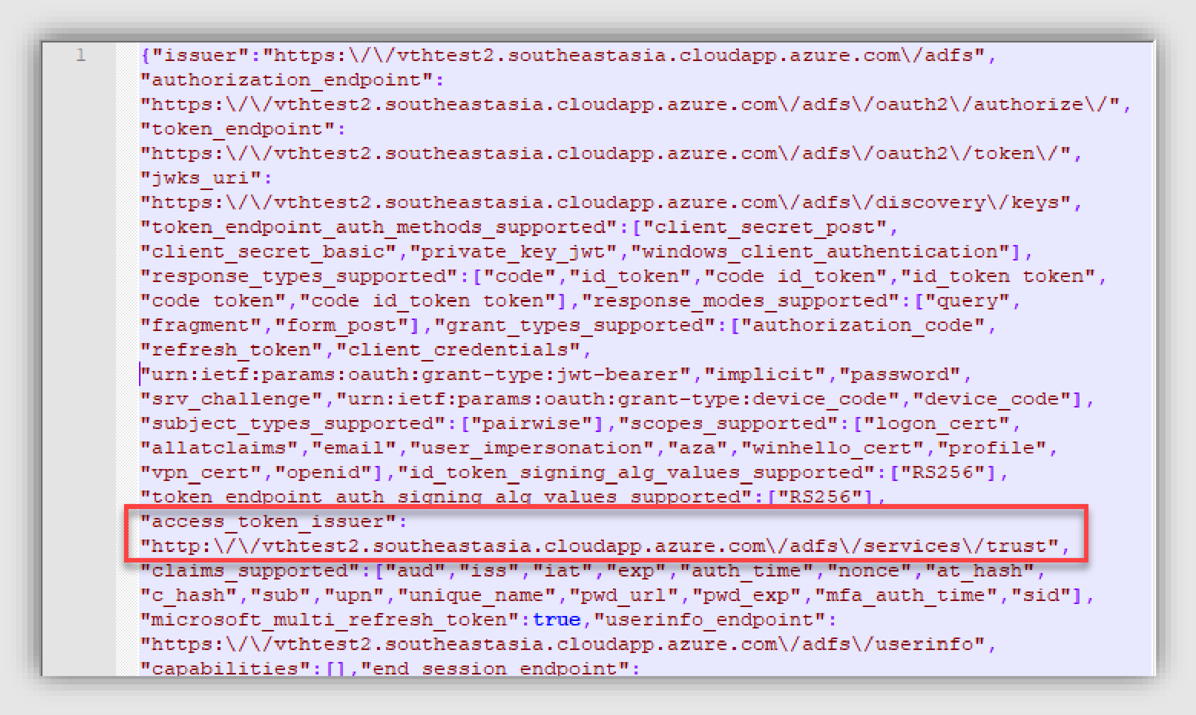
Example: https://www.contoso.com/adfs/ls/

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.