

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



No parts of this publication may be reproduced in any form or by any means or used to make any derivative such as translation, transformation, or adaptation without the permission from Add-On Products.



Table of contents

Table of contents	2
Foreword	3
System Requirements	4
Affected areas	5
Authentication Details for OAuth2/Open ID Connect Part A. Register application in Azure AD Part B. Retrieve details for OAuth2/Open ID Connect Authentication Protocol Reply URL Tenant (Tenant ID) Client ID Client secret Auto-Login Networks	6 6 6 8 8 9 9
Authentication Details for OAuth2 with ADFS	10
Part A. Configure Active Directory Federation Services (ADFS)	.10
Part B. Retrieve details for OAuth2 with ADFS Authentication Protocol	.17
Reply URL	.17
Client Id	.17
Client Secret	.18
Authorization URL, Token URL and Logout URL	.18
Auto-Login Networks	.18
Authentication Details for OpenID Connect with ADFS	20
Part A. Configure Active Directory Federation Services (ADFS)	. 20
Part B. Retrieve details for OpenID Connect with AD FS Authentication Protocol	. 24
Reply URL	. 24
Client Id	. 24
Client Secret	. 25
Authorization URL, Token URL and Logout URL	. 25
Auto-Login Networks	. 25
Authentication Details for SAML2	26
Part A. Register application in Azure AD	.26
Part B. Retrieve details for SAML2 Authentication Protocol	.26
Identifier (Entity ID)	.26
Login URL, Logout URL and Azure AD Identifier	.27
Return URL	.28
Certificate (.pfx) and PFX Password	.28
Auto-Login Networks	.28
Authentication Details for SAML2 with ADFS	29
Part A1. Configure Active Directory Federation Services (ADFS)	.29
Part A2. Create Claim Rules	.32
Part A3. Adjust the trust settings	.37
Part B. Retrieve details for SAML2 with ADFS Authentication Protocol	.39
Identifier (Entity ID)	.39
Login URL	.40
Logout URL	.40
Return URL	.40
Azure AD Identifier	.41
Certificate (.pfx) and PFX Password	.42
Auto-Login Networks	. 42



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

Resource Central	External Authentication
V DAILY TASKS	SAVE
V REPORTS	External Authentication
V DESIGNER	
✓ LOCATION	
V SECURITY	
 SYSTEM 	Nemove form based login option
Parameters	
Manifest Files	Authenticated system areas
SMS Configuration	My Meetings
Calendar	
Mail Log	
SQL	My Meeting stand-alone page Specific users All authenticated users
Database Cleaner	Order Forms opened from emails
License	Specific users All authenticated users
External Authentication	* Authentication Protocol
GDPR Information	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:

2	Users All users Add-On Products & Add-On Development	t - Azure Active [Directory		
_	~	+ New use	r 🕂 New guest user 🗋 Bulk	activities 🗸 💍 Refresh 🔑 Reset passv	vord 🗹 Multi-
4	All users				
*	Deleted users	Search use	ers	+ Add filters	
•	Password reset	Name		User name	User type
©	User settings		Add-On Products	info@add-on-support.com	Member
×	Diagnose and solve problems		Add-On Products - Customer Sen	customerservice@add-on.com	Member
Act	tivity		Add-On Products Support	support@add-on-support.com	Member
Э	Sign-ins		admin no MFA	admin-no-MFA@add-on.com	Member
	Audit logs		David Herbert Garbo	dhg@aod.vn	Guest
	Bulk operation results		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 <i>My Meetings stand-alone</i> page	Use any account (that exists in the domain, no need to exist in RC/Persons) to access <i>My</i> <i>Meetings stand-alone page</i> 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 \rightarrow Azure Active Directory \rightarrow App registrations \rightarrow 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)
O Accounts in any organizational directory (Any Azure AD directory - Multitenant)
O 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 \rightarrow Azure Active Directory \rightarrow App registrations. Click [View all applications] then select the app that you registered in Part A to see its details.



OAuth2 app - Authentica	ation		
	🕞 Save 🗙 Discard 🛛 🖕 Try out the new experience 📔 💙 Got feedback?		
 Werview Quickstart Manage 	Redirect URIs The URIs that we will accept as destinations when returning authentication responses (token Learn more about adding support for web, mobile and desktop clients 🖄	s) after successfully authenticating users. Also referred to as reply URLs.	
i Branding	ТҮРЕ	REDIRECT URI	
Authentication	Web ~	https://aodtest2.southeastasia.cloudapp.azure.com/ResourceCentral/ExAuth/OAuthAuthentication/CallbackHandler	✓ 🛍
Certificates & secrets	Web	e.g. https://myapp.com/auth	
 API permissions 			
Expose an API	Suggested Redirect URIs for public clients (mobile, desktop)		
 Owners Roles and administrators (Previ 	If you are using the Microsoft Authentication Library (MSAL) or the Active Directory Authenti desktop or mobile devices, you may select from the suggested Redirect URIs below or enter information, refer to the library documentation.	ication Library (ADAL) to build applications for a custom redirect URI above. For more	
Manifest	msalf2602100-bc97-4e5f-845c-20858bad9b88://auth (MSAL only)		
Support + Troubleshooting	https://login.microsoftonline.com/common/oauth2/nativeclient		
X Troubleshooting			
New support request	Advanced settings		
	Implicit grant Allows an application to request a token directly from the authorization endpoint. Recomme architecture (SPA), has no backend components, or invokes a Web API via JavaScript.	nded only if the application has a single page	

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 <u>https://resourcecentral.com/resourcecentral</u>, so the URL you can fill in is: <u>https://resourcecentral.com/resourcecentral/ExAuth/OAuthAuthentication/CallbackHandler</u>

Click [Save] to finish.

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

Advanced	ettings
Logout URL 👩	e.g. https://myapp.com/logout
Implicit grant Allows an appli architecture (SI	cation to request a token directly from the authorization endpoint. Recommended only if the application has a single page A), has no backend components, or invokes a Web API via JavaScript.
To enable the i	nplicit grant flow, select the tokens you would like to be issued by the authorization endpoint:
To enable the i	nplicit grant flow, select the tokens you would like to be issued by the authorization endpoint:



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:



Figure 5. Tenant ID

Client ID

Go to Azure portal \rightarrow Azure Active Directory \rightarrow App registrations. Click [View all applications] then select the app that you registered in Part A to see its details.

🔟 Delete 🌐 Endpoints	
Welcome to the new and improved App registrations. Looking to learner	rn 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 \rightarrow Azure Active Directory \rightarrow App registrations. Click [View all applications] then select the app that you registered in Part A to see its details.

Click [Certificates & secrets] \rightarrow [New client secret].

Add a client secr	et	
Description		
Expires In 1 year In 2 years Never		
Add Ca	ncel	

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 + New client secret	s to prove its identity when requesting a toke	en. 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	
L	153.177.122.10 192.168.1.1/24	
L		

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

	anager • Dashboard					Anti- Director Administration Control
						Active Directory Administrative Center Active Directory Domains and Trusts
ishboard	WELCOME TO SERVER MANAGER					Active Directory Module for Windows PowerShell
cal Server						Active Directory Sites and Services
Servers		Course that a local second				Active Directory Users and Computers
DS	Con	igure this local server				AD FS Management
FS	QUICK START					ADSI Edit
-	2 Ac	dd roles and features				Component Services
and Storage Services D						Computer Management
	3 Ac	Id other servers to manage				Disk Cleanup
	WHAT'S NEW 4 Cr	reate a server group				DNS
	4 6	outo a sorror group				Event Viewer
	5 Co	onnect this server to cloud service	ces			Group Policy Management
						Internet Information Services (IIS) Manager
	LEARN MORE					iSCSI Initiator
						Local Security Policy
	ROLES AND SERVER GROUPS					Microsoft Azure Services
	ROLES AND SERVER GROUPS Roles: 5 Server groups: 1 Servers tota	<i>k</i> 1				Microsoft Azure Services ODBC Data Sources (32-bit) ODBC Data Sources (64-bit)
	ROLES AND SERVER GROUPS Roles: 5 Server groups: 1 Servers tota	*1		File and Storage		Microsoft Azure Services ODBC Data Sources (32-bit) ODBC Data Sources (64-bit) Performance Monitor
	Roles AND SERVER GROUPS Roles 5 Server groups: 1 Servers tota	# 1	A DNS 1	File and Storage Services	1 to IIS	Microsoft Azure Services ODBC Data Sources (32-bit) ODBC Data Sources (64-bit) Performance Monitor Print Management
	ROLES AND SERVER GROUPS Roles: 5 Server groups: 1 Servers tota Image: 0 AD DS 1 Image: 0 AD DS 1	a≟ 1	DNS 1	File and Storage Services	1 🐼 IIS	Microsoft Azure Services ODBC Data Sources (32-bit) ODBC Data Sources (64-bit) Performance Monitor Pinit Management Resource Monitor
	ROLES AND SERVER GROUPS Roles 5 Server groups 1 Servers tota AD DS 1 Manageability Events	# 1 AD FS 1 Manageability Events	DNS 1 Manageability Events	File and Storage Services Manageability Events	1 () IIS () Mana Even	Microsoft Aure Services ODBC Data Sources (22-bit) ODBC Data Sources (64-bit) Performance Monitor Print Management Resource Monitor Services
	ROLES AND SERVER GROUPS Roles: 5 Server groups: 1 Servers tota Manageability Events Senvices	# 1 AD FS 1 () Manageability Events Services	DNS 1 Manageability Events Services	File and Storage Services Manageability Events Sannices	1 iiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiiii	Microsoft Azure Services ODBC Das Sources (22-bit) ODBC Das Sources (42-bit) Performance Monitor Print Management Resource Monitor Services System Configuration
	ROLES AND SERVER GROUPS Reles: 5 Server groups: 1 Servers tota	AD FS 1 (*) Manageability Events Services Deformance	DNS 1 Manageability Events Services Deducements	File and Storage Services Manageability Events Services	1 C IIS Man Even 1 Servi	Microsoft Azure Services ODBC Das Sources (22-bit) ODBC Das Sources (42-bit) ODBC Data Sources (46-bit) Performance Monitor Print Management Resource Monitor Services System Cenfiguration System Information
	ROLES AND SERVER GROUPS Roles: 5 Server groups: 1 Servers tota Manageability Events Services Performance	il: 1 AD FS 1 Manageability Events Services Performance	DNS 1 One content of the second sec	File and Storage Services Manageability Events Services Performance	1 I S Mana Even Servi Perfc	Microsoft Aure Services ODBC Data Sources (32-bit) ODBC Data Sources (42-bit) Performance Monitor Print Management Resource Monitor Services System Configuration System Information Task Scheduler
	ROLES AND SERVER GROUPS Roles 5 server groups: 1 servers tota	No. 1 (************************************	DNS 1 Manageability Events Services Performance BPA results	File and Storage Services Manageability Events Services Performance BPA results	1 I S Manu Even 1 Servi Perfo BPA u	Microsoft Azure Services ODBC Das Sources (22-bit) ODBC Das Sources (42-bit) ODBC Das Sources (46-bit) Performance Monitor Periot Management Resource Monitor Services System Configuration System Information Task Scheduler Windows Firewall with Advanced Security Windows Firewall with Advanced Security
	ROLES AND SERVER GROUPS Roles 5 Server groups: 1 Servers tota	Alt 1 AD FS 1 AD FS 1 Additional of the second s	DNS 1 Manageability Events Services Performance BPA results	File and Storage Services Manageability Events Services Performance BPA results	1 To His Man: Even 1 Servi Perfc BPA	Microsoft Azure Services ODBC Das Sources (22-bit) ODBC Das Sources (42-bit) ODBC Das Sources (46-bit) Performance Monitor Resource Monitor Services System Configuration System Information Task Scheduler Windows Firewall with Advanced Security Windows Memory Diagnostic
	RoLES AND SERVER GROUPS Reles 5 Server groups: 1 Servers tota AD DS 1 Manageability Events Services Performance BPA results	AL 1 AD FS 1 AD FS 1 Add FS 1 Add FS 1 Add FS 5 Ad	DNS 1 Manageability Events Services Performance BPA results	File and Storage Services Manageability Events Services Performance BPA results	1 C IIS Mani Even 1 Servi Perfc BPA	Microsoft Auro Services ODBC Data Sources (32-bit) ODBC Data Sources (42-bit) ODBC Data Sources (46-bit) Performance Monitor Bervices System Configuration System Information Task Scheduler Windows Firewall with Advanced Security Windows ForwerShell Windows PowerShell
	RoLES AND SERVER GROUPS Roles 5 server groups: 1 servers tota D D D 1 Manageability Events Services Performance BPA results	al: 1 Image: AD FS 1 <td>Image: DNS 1 Image: DNS 1 <td>File and Storage Services Manageability Events Services Performance BPA results</td><td>1 To IIS To Man. Even 1 Servi Perfc BPA</td><td>Microsoft Azure Services ODBC Das Sources (22-bit) ODBC Das Sources (42-bit) ODBC Das Sources (46-bit) Performance Monitor Services Services System Configuration System Information Task Scheduler Windows Firewall with Advanced Security Windows NewerShell Windows PowerShell Windows PowerShell Windows PowerShell (55)</td></td>	Image: DNS 1 Image: DNS 1 <td>File and Storage Services Manageability Events Services Performance BPA results</td> <td>1 To IIS To Man. Even 1 Servi Perfc BPA</td> <td>Microsoft Azure Services ODBC Das Sources (22-bit) ODBC Das Sources (42-bit) ODBC Das Sources (46-bit) Performance Monitor Services Services System Configuration System Information Task Scheduler Windows Firewall with Advanced Security Windows NewerShell Windows PowerShell Windows PowerShell Windows PowerShell (55)</td>	File and Storage Services Manageability Events Services Performance BPA results	1 To IIS To Man. Even 1 Servi Perfc BPA	Microsoft Azure Services ODBC Das Sources (22-bit) ODBC Das Sources (42-bit) ODBC Das Sources (46-bit) Performance Monitor Services Services System Configuration System Information Task Scheduler Windows Firewall with Advanced Security Windows NewerShell Windows PowerShell Windows PowerShell Windows PowerShell (55)
	ROLES AND SERVER GROUPS Roles 5 server groups: 1 servers tota AD DS 1 Manageability Events Services Performance BPA results I coal Server 1	Al Servers 1	DNS 1 Manageability Events Services Performance BPA results	File and Storage Services Manageability Events Services Performance BPA results	1 To IIS To Man, Even 1 Servi Perfc BPA	Microsoft Azure Services ODBC Das Sources (22-bit) ODBC Das Sources (42-bit) ODBC Das Sources (46-bit) Performance Monitor Services System Configuration System Information Task Scheduler Windows Freiwall with Advanced Security Windows Memory Diagnostic Windows Memory Diagnostic Windows PowerShell Windows PowerShell Windows PowerShell SE
	ROLES AND SERVER GROUPS Reles 5 server groupe: 1 servers tota AD DS 1 Manageability Events Services Performance BPA results I Local Server 1	All Servers 1	DNS 1 Manageability Events Services Performance BPA results	File and Storage Services Manageability Events Services Performance BPA results	1 The second sec	Microsoft Aure Services ODBC Data Sources (22-bit) ODBC Data Sources (42-bit) ODBC Data Sources (46-bit) Performance Monitor Print Management Resource Monitor Services System Information Task Scheduler Windows Finerwall with Advanced Security Windows Finerwall with Advanced Security Windows Fore/Shell Windows PowerShell (56) Windows PowerShell (56) Windows PowerShell (56)
	Roles AND SERVER GROUPS Reles 5 [server groups 1] servers tota Image ability Image ability Events Services Performance BPA results Image ability Image ability	al: 1 Image ability 1 Image ability Events Services Performance BPA results 1 Image ability 1 Image ability 1 Image ability 1	DNS 1 Manageability Events Services Performance BPA results	File and Storage Services Manageability Events Services Performance BPA results	1 CO IIS C Man Even 1 Servi Perfo BPA	Microsoft Azure Services ODBC Das Sources (22-bit) ODBC Das Sources (42-bit) ODBC Das Sources (46-bit) Performance Monitor Services Services System Configuration System Information Task Scheduler Windows Firewall with Advanced Security Windows NeweShell Windows NeweShell Windows NeweShell Windows NeweShell (55) Windows NeweShell (55) Windows NeweShell (55)
	ROLES AND SERVER GROUPS Roles 5 server groups: 1 servers tota AD DS 1 Manageability Events Services Performance BPA results Local Server 1 Manageability Events	al: 1 Image ability Events Services Performance BPA results Image ability Image ability Image ability	DNS 1 Manageability Events Services Performance BPA results	File and Storage Services Manageability Events Services Performance BPA results	1 To IS To Man Even 1 Servi Perfc BPA	Microsoft Azure Services ODBC Das Sources (22-bit) ODBC Das Sources (32-bit) ODBC Das Sources (45-bit) Performance Monitor Resource Monitor Services System Configuration System Information Task Scheduler Windows Terwell with Advanced Security Windows Memory Diagnostic Windows PowerShell Windows PowerShell (566) Windows PowerShell ISE Windows Server Backup
	ROLES AND SERVER GROUPS Reles 5 server groupe: 1 servers tota AD DS 1 Manageability Events Services Performance BPA results I Local Server 1 Manageability Events Services Performance	al: 1 Image ability 1 Image ability Events Services Performance BPA results Image ability Image ability Events Image ability 1 Image ability 1 Image ability Events	DNS 1 Manageability Events Services Performance BPA results	File and Storage Services Manageability Events Services Performance BPA results	1 Constant	Microsoft Auro Exercises ODBC Data Sources (32-bit) ODBC Data Sources (32-bit) ODBC Data Sources (46-bit) Performance Monitor Print Management Resource Monitor Services System Cenfiguration System Information Task Scheduler Windows Mermory Diagnostic Windows Mermory Diagnostic Windows NewerShell (36) Windows PowerShell (36) Windows PowerShell (35) Windows PowerShell (35) Windows Sever 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.

Image: Section View Window Help Image: Section View Window Help Image: Section View View View View Help				×
AD FS Service Attribute Stores Attribute Stores Claim Descriptions Endpoints Scope Descriptions Web Application Proxy Attribute Stores Claim Descriptions Cope Descriptions Cope Cope Stores Cope Stores C	Application Groups Name RC 4.1 OpenID RC 4.1 OAuth	Description	Actions Application Groups Add Application Group View New Window from Here Refresh Help	
Aciving Party Trusts Claims Provider Trusts Application Groups				

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"



翰 Add Application Group W	/izard ×
Welcome	
Steps	Name:
Welcome	RC 4.1 OAuth
Server application	Description
 Configure Application Credentials 	
Configure Web API	
Apply Access Control Policy	Template:
 Configure Application Permissions 	Client-Server applications
Summary	Native application accessing a web API
Complete	Server application accessing a web API
	Web browser accessing a web application
	Standalone applications
	I 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



ieneral	Confidential						
	Connacinati						
Name:							_
Chi41	DAuth - Server app	plication					
Client	d:						
cff265	56-74e5-48ac-9b7	75-c7f849ea2d	75				
Redire	ct URI:						
Examp	le: https://Contos	o.com				Add	
http:/	/192.168.2.43/Re	esourceCentra	/Api/Authenti	cation/Logo	ut	Remove	
http://			I				
Thup .//	192.168.2.43/Res	sourceCentral/	/ExAuth/OAut	hAdfsAuther	tication/C		
Thug of	192.168.2.43/Res	sourceCentral/	'ExAuth/OAut	hAdfsAuther	itication/Ca		
<	192.168.2.43/Res	sourceCentral/	/ExAuth/OAut	hAdfsAuther	itication/C		
<	192.168.2.43/Res	sourceCentral/	'ExAuth/OAut	hAdfsAuther	ntication/C		
< Descri	192.168.2.43/Res	sourceCentral/	ExAuth/OAut	hAdfsAuther	itication/C		_
< Descri	192.168.2.43/Res	sourceCentral/	ExAuth/OAut	hAdfsAuther	itication/C:		
< Descri	192.168.2.43/Res	sourceCentral/	ExAuth/OAut	hAdfsAuther	tication/C:		
< Descri	192.168.2.43/Res	sourceCentral/	ExAuth/OAut	hAdfsAuther	tication/C:		
< Descri	192.168.2.43/Res	sourceCentral/	Ex Auth/O Aut	hAdfsAuther	tication/C:		
< Descri	192.168.2.43/Res	sourceCentral/	ExAuth/OAut	hAdfsAuther	tication/C:		
< Descri	192.168.2.43/Res	sourceCentral/	Ex Auth/O Aut	hAdfsAuther	tication/C:		
< Descri	192.168.2.43/Res	sourceCentral/	Ex Auth/O Aut	hAdfsAuther	tication/C:		
< Descri	192.168.2.43/Res	sourceCentral/	ExAuth/OAut	hAdfsAuther	tication/C:		
< Descri	192.168.2.43/Res	sourceCentral/	Ex Auth/O Aut	hAdfsAuther	tication/C:		

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



Resource Central	External Authentication
V DAILY TASKS	SAVE
V REPORTS	
V DESIGNER	External Authentication
V LOCATION	Enable Configuration
V SECURITY	Yes No Xouth particular Protocol
▲ SYSTEM	
Parameters	Oddin2 with AD P3
Outlook Add-in	OAuth2 with AD FS Configuration
SMS Configuration	* Reply URL
Languages	http://192.168.2.43/ResourceCentral/ExAuth/OAuthAuthentication/CallbackHandler
Calendar	* Client Id
Mail Log	
SQL	
Database Cleaner	^ Client Secret
License	
External Authentication	* Authorization URL
Information	

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**".



Madd Application Grou	p Wizard X
Configure Application	on 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 Configure Windows Integrated Authentication Select the AD Account: Example: CONTOSO\expensevc Select Generate a shared secret Secret: Bijs-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.
	< Previous Next > Cancel

6. On *Configure Web API* screen, fill in "**Identifier**" (which is URL to RC backend) and click [**Add**] button.



输 Add Application Group Wi	zard	×
Configure Web API		
Steps	Name:	
Welcome	RC 4.1 OAuth - Web API 2	
Server application	lentifier:	
 Configure Application Credentials 	Example: https://Contoso.com	Add
Configure Web API	http://hieuvt/ResourceCentral	Remove
Apply Access Control Policy		
 Configure Application Permissions 		
Summary	Description:	
 Complete 		
	< Previous Next >	Cancel

Then click [Next] to proceed.

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



翰 Add Application Group Wi	zard		×
Choose Access Contro	l Policy		
Steps	Choose an access control policy:		
Welcome	Name	Description	
Server application	Permit everyone	Grant access to everyone.	
 Configure Application Credentials 	Permit everyone and require MFA Permit everyone and require MFA for specific group	Grant access to everyone and require MFAf Grant access to everyone and require MFAf	
Configure Web API	Permit everyone and require MFA from extranet access	Grant access to the intranet users and requir	
Apply Access Control Policy	Permit everyone and require MFA from unauthenticated	Grant access to everyone and require MFAf	
Configure Application	Permit everyone and require MFA, allow automatic devi Permit everyone for intranet access	Grant access to everyone and require MFA1 Grant access to the intranet users.	•
Permissions	Permit specific group	Grant access to users of one or more specifi	
Summary			
Complete	Policy		
	Permit everyone		
	I do not want to configure the access control policy at the application.	is time. No users will be permitted access for this	s
		< Previous Next > Cancel	

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



ropa	Configure permissions to enable client applications to access this Web API.	
Welcome	Client application (caller):	
Server application	Name Description	
Configure Application Credentials	Chi OAuth - Server application	
Configure Web API		
Apply Access Control Policy		
Configure Application Permissions		
Summary		
Summary Complete	Add	Remove
Summary Complete	Add	Remove
Summary Complete	Add Permitted scopes: Scope Name Description	Remove
Summary Complete	Add Permitted scopes: Scope Name Description email Request the email claim for the signed in user.	Remove
Summary Complete	Add 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	Remove
Summary Complete	Add 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.	Remove
Summary Complete	Add 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.	Remove
Summary Complete	Add 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	Remove
Summary Complete	Add 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	Remove

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 O	Auth - Server application Properties	>
General	Confidential	
Name	e:	
Chi41	OAuth - Server application	
Client	t ld:	

Client Secret

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

🙀 Add Application Group W	izard ×
Configure Application	Credentials
Steps Welcome Server application Configure Application 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 Configure Windows Integrated Authentication Select the AD Account: Example: CONTOSO\expensevc Select Secret: @tjs-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



<pre>{"issuer":"https:\/\/vthtest2.southeastasia.cloudapp.azure.com\/adfs",</pre>
"authorization_endpoint":
<pre>"https:\//vthtest2.southeastasia.cloudapp.azure.com\/adfs\/oauth2\/authorize\/",</pre>
"token_endpoint":
"https:\//vthtest2.southeastasia.cloudapp.azure.com\/adfs\/oauth2\/token\/","jwks_uri":
"https:\//vthtest2.southeastasia.cloudapp.azure.com\/adis\/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 Ma	anager • Dashboard				-	🗇 🚩 Manage Tools View H
	5					Active Directory Administrative Center
ashboard	WELCOME TO SERVER MANAGER					Active Directory Domains and Trusts
ocal Server						Active Directory Module for Windows Powershell Active Directory Sites and Senices
Il Servers						Active Directory Users and Computers
DC		nfigure this local server			Г	AD FS Management
55	OLUCY START				-	ADSI Edit
r5 C	2	Add roles and features				Component Services
	E /	add roles and reatares				Computer Management
and Storage Services P	3 /	Add other servers to manage				Defragment and Optimize Drives
	WHAT'S NEW	Create a conver group				Disk Cleanup Dais
	4 (create a server group				Event Viewer
	5 0	Connect this server to cloud serv	rices			Group Policy Management
						Internet Information Services (IIS) Manager
	LEARN MORE					iSCSI Initiator
						Local Security Policy
	ROLES AND SERVER GROUPS					Microsoft Azure Services
	Roles: 5 Server groups: 1 Servers to	otal: 1				ODBC Data Sources (32-bit)
				67 J. 6		ODBC Data Sources (64-bit)
	1947			= File and Storage		Destaurance Manifes
	AD DS 1	1 🚔 AD FS 1	1 🔮 DNS	1 File and Storage 1 Services	💽 IIS	Performance Monitor Print Management
	AD DS	AD FS	DNS	1 File and Storage Services 1 Manageability	Mana	Performance Monitor Print Management Resource Monitor
	AD DS	AD FS 1	DNS Manageability Events	File and Storage Services Manageability Events	IIS Mana Even	Performance Monitor Print Management Resource Monitor Services
	AD DS	AD FS 1	DNS Manageability Events Convictor	1 File and Storage Services 1 Manageability Events	IIS Mana Even	Performance Monitor Print Management Resource Monitor Services System Configuration
	AD DS 1 Manageability Events Services	AD FS 1 Manageability Events Services	DNS Manageability Events Services	1 File and Storage 1 Services 1 Manageability Events Services	IIS Man: Even Servi	Performance Monitor Print Management Resource Monitor Services System Configuration System Information
	AD DS 1 Manageability Events Services Performance	AD FS Manageability Events Services Performance	Anageability Events Services Performance	1 Services 1 Services Performance	IIS Mana Evem Servi Perfc	Performance Monitor Print Management Resource Monitor Services System Configuration System Information Task Scheduler
	AD DS Manageability Events Services Performance BPA results	AD FS T Manageability Events Services Performance BPA results	DNS Manageability Events Services Performance BPA results	1 Image: File and Storage 1 Services Manageability Events Services Performance BPA results	IIS IIS Mana Even Servi Perfc BPA (Performance Monitor Print Management Resource Monitor Services System Configuration System Information Task Scheduler Windows Fiewall with Advanced Security
	AD DS Manageability Events Services Performance BPA results	AD FS 1 Manageability Events Services Performance BPA results	PNS Manageability Events Services Performance BPA results	1 File and Storage 1 O Manageability Events Services Performance BPA results	 IIS Man: Even Servi Perfc BPA t 	Performance Monitor Print Management Resource Monitor Services System Configuration System Information Task Scheduler Windows Trewall with Advanced Security Windows Memory Diagnostic Windows Memory Diagnostic
	AD DS Manageability Events Services Performance BPA results	AD FS Manageability Events Services Performance BPA results	Amageability Events Services Performance BPA results	File and Storage Services Services Vents Services Performance BPA results	 IIS Manieven Servi Perfc BPA r 	Performance Monitor Print Management Resource Monitor Services System Configuration System Information Task Scheduler Windows Friewall with Advanced Security Windows ProverShell Windows PowerShell (SR)
	AD DS Manageability Events Services Performance BPA results	AD FS 1	DNS Manageability Events Services Performance BPA results	1 File and Storage 1 ③ Manageability Events 5 Services Performance BPA results	 Man; Even Servi Perfc BPA (Performance Monitor Print Management Resource Monitor Services System Configuration System Information Task Scheduler Windows Firewall with Advanced Security Windows Amery Dipotosic Windows American Biopostic Windows PowerShell (BS)
	AD DS Manageability Events Services Performance BPA results	AD FS 1	Anageability Events Services Performance BPA results	1 Frie and Storage 1 ③ Manageability 1 Events Services 1 Services Performance 1 BPA results 1 1	 Manieven Manieven Servi Perfc BPA i 	Performance Monitor Pent Management Resource Monitor Services System Configuration System Information Task Scheduler Windows Nerwall With Advanced Security Windows NerworkShell Windows PowerShell Windows PowerShell (JSB) Windows PowerShell (JSB)
	AD DS Manageability Events Services Performance BPA results Local Server	AD FS 1 Manageability Events Services Performance BPA results	PNS Manageability Events Services Performance BPA results	1 Frie and Storage 1 ③ Manageability 1 Events Services 1 Services Performance 1 BPA results 1 1	Man. Even Servi Perfc BPA 1	Performance Monitor Print Management Resource Monitor Services System Configuration System Information Task Scheduler Windows Reverse Windows RowerShell Windows RowerShell (SE) Windows RowerShell (SE) Windows RowerShell (SE) Windows RowerShell (SE) Windows RowerShell (SE)
	AD DS Manageability Events Services Performance BPA results Local Server Manageability Manageability	AD FS 1 Manageability Events Services Performance BPA results Manageability Manageability Manageability	DNS Manageability Events Services Performance BPA results	1 File and Storage 1 ③ Manageability Events 5 Services Performance BPA results	Man. Even Servi Perfc BPA (Performance Monitor Print Management Resource Monitor Services System Configuration System Information Task Scheduler Windows Firewall with Athraneed Security Windows Forewall with Athraneed Security Windows PowerShell Windows PowerShell (SB) Windows PowerShell (SB) Windows PowerShell (SE) Windows PowerShell (SE)
	AD DS Manageability Events Services Performance BPA results Local Server Manageability Events	AD FS 1 Manageability Events Services Performance BPA results Manageability Events 1 Manageability Events	PNS Manageability Events Services Performance BPA results	1 File and Storage 1 ③ Manageability 1 Events Services 1 Services Beformance 1 BPA results 1 1	Man, Even Servi Perfc BPA (Performance Monitor Perint Management Resource Monitor Services System Configuration System Information Task Scheduler Windows Terwell with Advanced Security Windows Memory Diagnostic Windows PowerShell Windows PowerShell Windows PowerShell (SE) Windows PowerShell (SE) Windows Server Backup
	AD DS Manageability Events Services Performance BPA results Local Server Manageability Events Services	Image: AD FS 1 Image: AD FS<	Anageability Events Services Performance BPA results	1 File and Storage 1 ③ Manageability 1 Events Services 1 Performance BPA results 1	Man. Even Servi Perfc BPA (Performance Monitor Print Management Resource Monitor Services System Configuration System Information Task Scheduler Windows PreverShell Windows PowerShell (SB) Windows PowerShell (SB) Windows PowerShell (SB) Windows PowerShell (SB) Windows Server Backup
	AD DS Manageability Events Services Performance BPA results Local Server Manageability Events Services Performance	AD FS 1 Manageability Events Services Performance BPA results Manageability Events BPA results Manageability Events Services Performance Performance	DNS Manageability Events Services Performance BPA results	1 File and Storage 1 ③ Manageability Events Services Performance BPA results Image: Service se	Man: Even Servi Perfc BPA	Performance Monitor Print Management Resource Monitor Services System Configuration System Information Tark Scheduler Windows Freewall with Advanced Security Windows Memory Diagnostic Windows PowerShell Windows PowerShell (SE) Windows PowerShell (SE) Windows PowerShell (SE) Windows Sever 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.

Matrix AD FS S Eile Action View Window Help Action II III III Action III III Action III Action Action				- C	·
🛗 AD FS	Application Groups		Actions		
 Service Attribute Stores Authentication Methods Certificates Claim Descriptions Device Registration Endpoints Scope Descriptions Web Application Proxy Access Control Policies Rtlying Party Trusts Claims Provider Trusts Application Groups 	Name [RC 4.1 OpenID RC 4.1 0 Auth	Description	Application Groups Add Application Group View New Window from Here Refresh Help		•

3. On the 'Add Application Group wizard' → Welcome screen, fill in Name and select "Server application" in Template and Click [Next].



Madd Application Group	p Wizard
Welcome	
Steps	Name:
Welcome	RC 4.1 SR2 OpenID
Server application	Description
 Configure Application Credentials 	Description.
Summary	
Complete	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
	-
	More information

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



eneral Confidential				
Name:				
Chi OpenID - Server	application			
Client Id:				
dd1464a946c2-483f	-965b-f08417bf859d			
Redirect URI:				
Example: https://Cor	ntoso.com			Add
//192.168.2.43/Res	ourceCentral/ExAuth/	/OpenIDAdfsAuthent	ication/Callba	Remove
// 19// 168 //14/800	oureal aptral/Api/Auti	hentication/Lodout		
// 132.100.2. 4 3/1163	ourcecentral/Api/Aut			
<			>	
Cescription:			>	
Cescription:			>	
Description:			>	
Construction:			>	
Description:			>	

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



Resource Central	External Authentication
V DAILY TASKS	SAVE
V REPORTS	
V DESIGNER	External Authentication
V LOCATION	Enable Configuration
V SECURITY	● Yes ○ No
▲ SYSTEM	* Authentication Protocol OAuth2 with AD FS
Parameters	Quith2 with AD ES Configuration
Outlook Add-in	* Basket UDI
SMS Configuration	
Languages	http://192.168.2.43/ResourceCentral/ExAuth/OAuthAuthentication/CallbackHandler
Calendar	* Client Id
Mail Log	
SQL	
Database Cleaner	* Client Secret
License	
External Authentication	* Authorization URL
Information	

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*.



Configure Applicatio	on Credentials	
Steps Welcome Server application Configure Application Credentials Summary Complete	Select credentials used by the application to authenticate itself with AD FS when req Register a key used to sign JSON Web Tokens for authentication Configure Windows Integrated Authentication Select the AD Account: Example: CONTOSO\expensevc Generate a shared secret Secret: Rijs-Im5kr-7PiGXmBgXNcsiBSgAQ2T2Mdr6Wdva Copy and save the secret. You will not be able to view the secret after created. You can reset the secret later if required.	uesting access tokens.

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.



Chi OpenID -	Server application Prope	rties	
General Cor	fidential		
Name:			
	C E E		
Chi OpenIE	- Server application		
Chi OpenIE Client Id:	- Server application	-	
Chi OpenIE Client Id: dd1464a9-	- Server application 6c2-483f-965b-f08417bf85	d	
Chi OpenIE Client Id: dd1464a9-	- Server application 6c2-483f-965b-f08417bf85	d	

Client Secret

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

훾 Add Application Group W	izard ×
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 Configure Windows Integrated Authentication Select the AD Account: Example: CONTOSO\expensevc Select Generate a shared secret Bijs-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 \rightarrow Azure Active Directory \rightarrow Enterprise applications \rightarrow Click [New application], select Non-gallery application and enter the name for the application:

Add an application		\$	×	Add your own application
Add your own app Application you're developing Register an app you're working on to integrate it with Azure AD	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		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: ●
Add from the gallery				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 \rightarrow Azure Active Directory \rightarrow Enterprise applications. Click [View all applications] then select the app that you registered in Part A to see its details. Click [Single sign-on] \rightarrow SAML



Figure 10. Select SSO method



A new panel is opened.

et up single	Sign-On with SAIVIL - P	review	
ead the configurati	on guide 🖉 for help integrating SSO	_for_RC.	
Basic SA	ML Configuration		- /
ldentifier	(Entity ID)	Required	
Reply URI	(Assertion Consumer Service URL)	Required	
Sign on U	RL	Optional	
Relay Stat	-	Optional	

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

	lation	
Save		
Values for the fields below a SAML metadata file if provid	re provided by SSO_for_RC. You may either enter those values manually, or upload a pre-configured ed by SSO_for_RC. Upload metadata file.	
* Identifier (Entity ID) 🚯	https://resourcecentral.com/resourcecentral	~

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 <u>https://resourcecentral.com/resourcecentral</u>, 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 \rightarrow Azure Active Directory \rightarrow 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):





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 <u>https://resourcecentral.com/resourcecentral</u>, so the Reply URL you can fill in is: <u>https://resourcecentral.com/resourcecentral/ExAuth/Saml2Authentication/CallbackHandler</u>

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 M	anager • Dashboard				• © 🏲	Manage <mark>Tools</mark> View Help
Dashboard	WELCOME TO SERVER MANAGER				Active Direct Active Direct Active Direct	tory Administrative Center tory Domains and Trusts tory Module for Windows PowerShell
Local Server All Servers AD DS AD FS DNS File and Storage Services IIS	CUNCK START 2 Add 3 Add WHAT'S NEW 4 Crea 5 Con	ure this local server roles and features other servers to manage te a server group nect this server to cloud service	es		Active Direc Active Direc ACtive Direc ACtive Direc Component Component Defragment Defragment Dirk Cleanup Dirk Event Vivee Group Polici Internet for	tory Sites and Services tory Users and Computers gement Services and Optimize Drives p r Management monitor familier (ITS Manages
	ECARN MORE Roles 5 Server groups: 1 Servers total: 1 Image AD DS 1	AD FS 1 Anageability Events Services Performance BPA results	DNS Manageability Events Services Performance BPA results	1 File and Storage Services Manageability Events Services Performance BPA results	iSCSI hitiat Local Securi Microsoft A. OD8C Data OD	y Policy y Policy ure Services Sources (32-bit) Sources (42-bit) Honitor Inguration Inguration Inguration Merevall with Advanced Security memory Diagnostic werShell
	Local Server 1 ① Manageability Events 2 2 Services Performance 1	All Servers 1 Manageability Events Services Performance			Windows Po Windows Po Windows Po Windows Se	werShell (S6) werShell (SE werShell (SE (x86) rrver 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**.

Image: Window Year Image:				
AD FS	Relying Party Trusts			Actions
> Service	Display Name	Enabled Type	Identifier	Relying Party Trusts
Relving Party Trusts	Add-on Login	No WS-T	https://hieuvt/ResourceCentral1	Add Relying Party Trust
Claims Provider Trusts	Aod-Test	Yes WS-T.	https://hieuvt/ResourceCentral	View
Application Groups				New Window from Here
				Refresh

- 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: Browse @ 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.

Specify Display Nan	ne
Steps	Enter the display name and any optional notes for this relying party.
Welcome	Display name:
Select Data Source	Zendesk Login
Specify Display Name	Notes:
Choose Profile	
Configure Certificate	
Configure URL	
Configure Identifiers	
Configure Multi-factor Authentication Now?	
 Choose Issuance Authorization Rules 	
Ready to Add Trust	
Finish	

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





\$	Add Relying Party Trust Wizard						
Configure Certificate	3						
Steps	Specify an optional token encryption certificate. The token encryption certificate is used to encrypt the						
Welcome	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						
Select Data Source							
Specify Display Name	Issuer:						
Choose Profile	Subject. Effective date:						
Configure Certificate	Expiration date:						
Configure URL							
Configure Identifiers	View Browse Remove						
Configure Multi-factor Authentication Now?							
 Choose Issuance Authorization Rules 							
Ready to Add Trust							
Finish							

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

훾 Add Relying Party Trust W	izard	×
Configure URL		
iteps 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 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/	e

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	
Steps	Relving parties may be identified by one or more unique identifier strings. Specify the identifiers for this relving
Welcome	party trust.
Select Data Source	Relying party trust identifier:
Specify Display Name	Add
Configure Certificate	Example: https://fs.contoso.com/adfs/services/trust
Configure URL	Relying party trust identifiers:
Configure Identifiers	https://192.168.1.109/ResourceCentral Remove
 Choose Access Control Policy 	
Ready to Add Trust	
Finish	

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).

a mie Action view Window Heip	,							
AD FS	Relying Party Trusts	5				Act	ions	
Service Access Control Policies Access Control Policies Acping Party Trusts Application Groups	Display Name Add on Login Add Test adsod	Update from Federation Me Edit Access Control Policy Edit Claim Issuance Policy Disable Properties Delete Help	Enabled No Yes tadata	Type WS-T WS-T	Identifier https://heuvt/ResourceCentral1 https://heuvt	Ref	ying Party Trusts Add Relying Party Trust View New Window from Here Refresh Help Sod Update from Federation Metadata Edit Access Control Policy Edit Claim Issuance Policy Disable Properties Delete	

This starts the configuration wizard for a new claim.



suance 1	Transform Rules			
The follo	wing transform rules s	pecify the claims t	hat will be sent to the ret	ying party.
Order	Rule Name		Issued Claims	
				1
<u>A</u> dd H	Ledit Rule	. <u>R</u> emove Ru	ile	

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 Templat	e
Steps	Select the template for the claim rule that you want to create from the following list. The description provides
Choose Rule Type	details about each claim rule template.
Configure Claim Rule	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.



Service		Dieplay Name		Epobled	Tune	Identifier			Account Carter
Attribute Stores		ChiSAMI		Enabled	WS-T	https://192.1	68.2.43/Res	sourceCentral	Access Control
Authentication Methods Certificates		GHOWNE		103	110 1	1102.1	00.2.407110.	Sourcecentral	r cinic everyone
📋 Cl 翰 Add Transform Cl	aim Rule Wizar	rd					×		
📔 W Steps	You	can configure this rule to send the value	es of LDAP attribute	es as claims. S	Select an a	ttribute store fro	om which		
Choose Rule Type	from	the rule.	attributes will map to	o the outgoing	g ciaim type	is triat will be is	sued		
Claim Configure Claim Rule	Clain	m rule name:							
Appli Appli	Ema	ail Trasform							
	Rule	e template: Send LDAP Attributes as Clai	ms						
	Attrib	bute store:							
	Acti	tive Directory				\sim			
	Мар	pping of LDAP attributes to outgoing clair	n types:						
		LDAP Attribute (Select or type to	Outgoing (Claim Type (S	elect or typ	e to add more)			
		add more)		oldini Type (o	0.000 01 0,000	0.00 000 11010)			
		User-Principal-Name	✓ Name				~		
		User-Principal-Name	✓ Name ID				~		
	Þ	User-Principal-Name	✓ E-Mail Add	ress			~		
			~				~		
Add Transform Claim Ru	le Wizard								×
Add Transform Claim Ru Donfigure Rule eps	le Wizard You can	configure this rule to send the v	alues of IDAP	attributes a	as claims	Select and	attribute st	tore from wh	×
Add Transform Claim Ru Donfigure Rule eps Choose Bule Type	le Wizard You can to extrac	i configure this rule to send the v st LDAP attributes. Specify how t	alues of LDAP he attributes w	attributes a ill map to th	as claims ne outgoi	. Select an a	attribute st ves that wi	tore from wh	×
Add Transform Claim Ru Donfigure Rule eps Choose Rule Type	le Wizard You can to extrac from the	configure this rule to send the v t LDAP attributes. Specify how t rule.	alues of LDAP he attributes w	attributes a ill map to th	as claims ne outgoi	. Select an a ng claim typ	attribute st ies that wi	tore from wh	X
Add Transform Claim Ru Donfigure Rule eps Choose Rule Type Configure Claim Rule	le Wizard You can to extrac from the Claim rule	configure this rule to send the v t LDAP attributes. Specify how t rule. e name:	alues of LDAP he attributes w	attributes a ill map to th	as claims ne outgoi	. Select an a	attribute s es that wi	tore from wh	×
Add Transform Claim Ru Danfigure Rule eps Choose Rule Type Configure Claim Rule	le Wizard You can to extrac from the Claim rule	configure this rule to send the v t LDAP attributes. Specify how t rule. e name:	alues of LDAP he attributes w	attributes a iil map to th	as claims ne outgoi	. Select an a ng claim typ	attribute si es that wi	tore from wh	×
Add Transform Claim Ru Donfigure Rule Pps Choose Rule Type Configure Claim Rule	le Wizard You can to extrac from the Claim rule Rule tem	configure this rule to send the v t LDAP attributes. Specify how t rule. e name: uplate: Send LDAP Attributes as	ralues of LDAP the attributes w Claims	attributes a ill map to th	as claims ne outgoi	. Select an r ng claim typ	attribute st es that wi	tore from wh	× iich
Add Transform Claim Ru Donfigure Rule aps Choose Rule Type Configure Claim Rule	le Wizard You can to extrac from the Claim rule Rule tem	configure this rule to send the v t LDAP attributes. Specify how t rule. e name: uplate: Send LDAP Attributes as	ralues of LDAP he attributes w Claims	attributes a ill map to th	as claims ne outgoi	. Select an a ng claim typ	attribute sl es that wi	tore from wh	× iich
Add Transform Claim Ru Donfigure Rule eps Choose Rule Type Configure Claim Rule	le Wizard You can to extrac from the Claim rule Rule term Attribute	configure this rule to send the v t LDAP attributes. Specify how t rule. e name: uplate: Send LDAP Attributes as store:	ralues of LDAP he attributes w Claims	attributes a ill map to th	as claims ne outgoi	. Select an a ng claim typ	attribute sl es that wi	tore from wh	× iich
Add Transform Claim Ru onfigure Rule eps Choose Rule Type Configure Claim Rule	le Wizard You can to extrac from the Claim rule Rule tem Attribute Active I	configure this rule to send the v t LDAP attributes. Specify how t rule. e name: nplate: Send LDAP Attributes as store: Directory	ralues of LDAP he attributes w Claims	attributes a ill map to th	as claims ne outgoi	. Select an t	attribute st res that wi	tore from wh	× iich
Add Transform Claim Ru Donfigure Rule eps Choose Rule Type Configure Claim Rule	le Wizard You can to extrac from the Claim ruk Claim ruk Rule tem Attribute Active I Mapping	configure this rule to send the v t LDAP attributes. Specify how t rule. e name: nplate: Send LDAP Attributes as store: Directory g of LDAP attributes to outgoing.	ralues of LDAP he attributes w Claims claim types:	attributes a ill map to th	as claims ne outgoi	. Select an a ng claim typ	attribute stat wi	tore from wh	× iich
Add Transform Claim Ru Donfigure Rule eps Choose Rule Type Configure Claim Rule	le Wizard You can to extrac from the Claim ruld Rule tem Attribute Active I Mapping	configure this rule to send the v t LDAP attributes. Specify how t rule. e name: nplate: Send LDAP Attributes as store: Directory g of LDAP attributes to outgoing LDAP Attribute (Select or type	values of LDAP he attributes w Claims claim types: to	attributes a ill map to th	as claims ne outgoi	. Select an a ng claim typ	attribute states that wi	tore from wh	× iich
Add Transform Claim Ru onfigure Rule eps Choose Rule Type Configure Claim Rule	le Wizard You can to extrac from the Claim ruld Rule tem Attribute Active I Mapping	configure this rule to send the v t LDAP attributes. Specify how t rule. e name: nplate: Send LDAP Attributes as store: Directory of LDAP attributes to outgoing LDAP Attribute (Select or type add more)	ralues of LDAP he attributes w Claims claim types: to Ou	attributes a ill map to th utgoing Clai	as claims ne outgoi	. Select an a ng claim typ (Select or ty	attribute st nes that wi	tore from wh ill be issued more)	x
Add Transform Claim Ru onfigure Rule eps Choose Rule Type Configure Claim Rule	le Wizard You can to extrac from the Claim ruld Rule tem Attribute Attribute	configure this rule to send the v t LDAP attributes. Specify how t rule. e name: nplate: Send LDAP Attributes as store: Directory of LDAP attributes to outgoing LDAP Attribute (Select or type add more) User-Principal-Name	ralues of LDAP he attributes w Claims claim types: to Ou v UP	attributes a ill map to th utgoing Cla	as claims ne outgoi im Type	. Select an a ng claim typ (Select or ty)	attribute st les that wi	tore from wh ill be issued more)	× iich
Add Transform Claim Ru onfigure Rule eps Choose Rule Type Configure Claim Rule	le Wizard You can to extrac from the Claim ruld Rule tem Attribute Attribute	configure this rule to send the v t LDAP attributes. Specify how t rule. e name: nplate: Send LDAP Attributes as store: Directory of LDAP attributes to outgoing LDAP Attribute (Select or type add more) User-Principal-Name	claims	attributes a ill map to th utgoing Cla	as claims he outgoi im Type	. Select an a ng claim typ (Select or ty)	attribute st les that wi	tore from wh ill be issued more)	× iich
Add Transform Claim Ru configure Rule eps Choose Rule Type Configure Claim Rule	le Wizard You can to extrac from the Claim ruk Claim ruk Rule tem Attribute Active I Mapping	configure this rule to send the v t LDAP attributes. Specify how t rule. e name: nplate: Send LDAP Attributes as store: Directory of LDAP attributes to outgoing LDAP Attribute (Select or type add more) User-Principal-Name	claims of LDAP the attributes w Claims to Ou v UP	attributes a ill map to th utgoing Cla	as claims ne outgoi im Type	. Select an a ng claim typ	attribute st res that wi	tore from wh ill be issued more)	× nich
Add Transform Claim Ru configure Rule eps Choose Rule Type Configure Claim Rule	le Wizard You can to extrac from the Claim rule Rule tem Attribute Active [Mapping	configure this rule to send the v t LDAP attributes. Specify how t rule. e name: nplate: Send LDAP Attributes as store: Directory of LDAP attributes to outgoing LDAP Attribute (Select or type add more) User-Principal-Name	ralues of LDAP he attributes w Claims claim types: to Que v V V	attributes a ill map to th utgoing Cla	as claims ne outgoi im Type	. Select an ing claim typ	attribute st es that wi pe to add	tore from wh ill be issued	× nich
Add Transform Claim Ru configure Rule eps Choose Rule Type Configure Claim Rule	le Wizard You can to extrac from the Claim rule Rule tem Attribute Active [Mapping	configure this rule to send the v t LDAP attributes. Specify how t rule. e name: nplate: Send LDAP Attributes as store: Directory of LDAP attributes to outgoing LDAP Attribute (Select or type add more) User-Principal-Name	ralues of LDAP he attributes w Claims claim types: to 0 V V V	attributes a ill map to th utgoing Cla	as claims ne outgoi	. Select an ing claim typ	attribute st es that wi	tore from wh ill be issued more)	× nich
Add Transform Claim Ru configure Rule eps Choose Rule Type Configure Claim Rule	le Wizard You can to extrac from the Claim ruld Rule tem Attribute Active [Mapping	I configure this rule to send the v t LDAP attributes. Specify how t rule. e name: nplate: Send LDAP Attributes as store: Directory of LDAP attributes to outgoing LDAP Attribute (Select or type add more) User-Principal-Name	alues of LDAP he attributes w Claims claim types: to 0 V V V	attributes a ill map to th utgoing Cla	as claims ne outgoi im Type	. Select an ing claim typ	attribute st es that wi pe to add	tore from wh ill be issued	× nich
Add Transform Claim Ru configure Rule eps Choose Rule Type Configure Claim Rule	le Wizard You can to extrac from the Claim ruld Rule tem Attribute Active [Mapping	I configure this rule to send the v t LDAP attributes. Specify how t rule. e name: aplate: Send LDAP Attributes as store: Directory of LDAP attributes to outgoing LDAP Attribute (Select or type add more) User-Principal-Name	alues of LDAP he attributes w Claims claim types: to	attributes a ill map to th utgoing Cla	as claims ne outgoi	. Select an and a select an a	attribute st res that wi	tore from wh ill be issued	× nich
Add Transform Claim Ru onfigure Rule eps Choose Rule Type Configure Claim Rule	le Wizard You can to extrac from the Claim rulk Rule tem Attribute Active I Mapping	I configure this rule to send the v t LDAP attributes. Specify how t rule. e name: aplate: Send LDAP Attributes as store: Directory of LDAP attributes to outgoing LDAP Attribute (Select or type add more) User-Principal-Name	alues of LDAP he attributes w Claims to v UP v	attributes a ill map to th utgoing Cla	as claims ne outgoi	. Select an and a select and a select and a select or type (Select or type)	attribute st les that wi	tore from wh ill be issued	× nich
Add Transform Claim Ru onfigure Rule eps Choose Rule Type Configure Claim Rule	le Wizard You can to extrac from the Claim rulk Rule tem Attribute Active I Mapping	I configure this rule to send the v t LDAP attributes. Specify how t rule. e name: uplate: Send LDAP Attributes as store: Directory of LDAP attributes to outgoing LDAP Attribute (Select or type add more) User-Principal-Name	alues of LDAP he attributes w Claims to v UP v	attributes a ill map to th utgoing Cla	as claims ne outgoi	. Select an i ng claim typ	attribute st les that wi	tore from wh ill be issued more)	× nich
Add Transform Claim Ru onfigure Rule eps Choose Rule Type Configure Claim Rule	le Wizard You can to extrac from the Claim ruld Rule tem Attribute Active I Mapping	I configure this rule to send the v t LDAP attributes. Specify how t rule. e name: uplate: Send LDAP Attributes as store: Directory of LDAP attributes to outgoing LDAP Attribute (Select or type add more) User-Principal-Name	alues of LDAP he attributes w Claims to Ou V UP	attributes a ill map to th utgoing Cla	as claims ne outgoi	. Select an and and the select of the select	attribute si es that wi	tore from wh ill be issued	ich
Add Transform Claim Ru configure Rule eps Choose Rule Type Configure Claim Rule	le Wizard You can to extrac from the Claim rule Rule tem Attribute Active I Mapping	configure this rule to send the v t LDAP attributes. Specify how t rule. e name: uplate: Send LDAP Attributes as store: Directory of LDAP attributes to outgoing LDAP Attribute (Select or type add more) User-Principal-Name	ralues of LDAP the attributes w Claims to Ou V UP	attributes a ill map to th utgoing Cla	as claims ne outgoi	. Select an ing claim typ	attribute si les that wi	tore from wh ill be issued	ich
Add Transform Claim Ru configure Rule eps Choose Rule Type Configure Claim Rule	le Wizard You can to extrac from the Claim rule Rule tem Attribute Active I Mapping	configure this rule to send the v t LDAP attributes. Specify how t rule. e name: uplate: Send LDAP Attributes as store: Directory of LDAP attributes to outgoing LDAP Attribute (Select or type add more) User-Principal-Name	ralues of LDAP the attributes w Claims to Ou V UP	attributes a ill map to th utgoing Cla	as claims ne outgoi	. Select an ang claim typ	attribute si les that wi	tore from wh ill be issued	× iich

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



4. Create another new rule by clicking [Add Rule]...

🙀 Add Transform Claim R	ule Wizard	×
Select Rule Templat	e	
Steps	Select the template for the claim rule that you want to create from the following list. The description provides	
Choose Rule Type	details about each claim rule template.	
Configure Claim Rule	Claim rule template:	
	Send LDAP Attributes as Claims $\qquad \qquad \lor$	
	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.	
	< Previous Next > Cancel	

- 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.



훾 Add Transform Claim I	Rule Wizard			×
Configure Rule				
Steps Choose Rule Type Configure Claim Rule	You ca to extra from th Claim n Email Rule te Attribut Active Mappir	n configure this rule to send the values ct LDAP attributes. Specify how the at e rule. Iranforms mplate: Send LDAP Attributes as Claim e store: Directory g of LDAP attributes to outgoing claim LDAP Attribute (Select or type to add more) User-Principal-Name	types	DAP attributes as claims. Select an attribute store from which as will map to the outgoing claim types that will be issued
				< Previous Finish Cancel

- 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.



Steps	You or	n configure this sile to cond the values of l	DAR attributes as claims. Select as attribute store from which
Choose Rule Type	to extra from th	act LDAP attributes. Specify how the attribut e rule.	es will map to the outgoing claim types that will be issued
Configure Claim Rule	Claim n	ule name:	
	Email	Tranforms 2	
	Attribut Active	e store: Directory	s.
		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.



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	
ОК	Cancel
OK Cancel	Apply

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.



	Edit En	dpoint		^
Endpoint type:				
SAML Logout		~		
Binding:				
POST		~	·	
https://sso.domain.t Example: https://sts Response URL:	ld/adfs/ls/?wa=w .contoso.com/adf	signout 1.0 s/ls		
Example: https://sts	.contoso.com/log	out		

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.





Login URL

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

File Action View Window Hel	р			
• 🔿 🚈 📰 🔢 🖬			-	
AD FS	Endpoints	5		
 Service Attribute Stores 	Enabled	Proxy Enabled	URL Path	Туре
Authentication Methods	Token Is	suance		
📔 Certificates	Yes	Yes	/adfs/ls/	SAML 2.0/WS-Federation
Claim Descriptions	No	No	/adfs/services/trust/2005/windows	WS-Trust 2005
Device Registration	No	No	/adfs/services/trust/2005/windowsmixed	WS-Trust 2005
Endpoints	Yes	Yes	/adfs/services/trust/2005/windowstransport	WS-Trust 2005
Scope Descriptions	No	No	/adfs/services/trust/2005/certificate	WS-Trust 2005
Web Application Proxy	Yes	Yes	/adfs/services/trust/2005/certificatemixed	WS-Trust 2005
Access Control Policies	Yes	Yes	/adfs/services/trust/2005/certificatetransport	WS-Trust 2005
📔 Relying Party Trusts	No	No	/adfs/services/trust/2005/usemame	WS-Trust 2005
Claims Provider Trusts	No	No	/adfs/services/trust/2005/usemamebasictransport	WS-Trust 2005
Application Groups	Yes	Yes	/adfs/services/trust/2005/usemamemixed	WS-Trust 2005
•••	V	M.	/- JE- / A /ODDE A	WC T 200E

3. Compose the Login URL with the following format: https:// <web_server_URL>/Endpoint_URL_path

For example: <u>https://rc48.ps.com/adfs/ls</u>

Logout URL

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

Inde	ex: 0	
Tru	sted URL:	
http	s://ps48.com/adfs/ls/?wa=wsignout1.0	
Exa	mple: https://sts.contoso.com/adfs/ls	
Res	sponse URL:	
Exa	ample: 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.



Configure URL	
Steps	AD FS supports the WS-Trust. WS-Federation and SAML 2.0 WebSSO protocols for relving parties. If
Welcome	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.
Select Data Source	
Specify Display Name	The WS-Federation Passive protocol LIRI supports Web-browser-based claims providers using the
Configure Certificate	WS-Federation Passive protocol.
Configure URL	Relying party WS-Federation Passive protocol URL:
Configure Identifiers	
 Choose Access Control Policy 	Example: https://fs.contoso.com/adfs/ls/
Ready to Add Trust	Enable support for the SAML 2.0 WebSSO protocol
Finish	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/adts/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.

1	<pre>{"issuer":"https:\/\/vthtest2.southeastasia.cloudapp.azure.com\/adfs",</pre>
	"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": "R5256",
	"access token issuer":
	"http:///vtntest2.southeastasia.cloudapp.azure.com/radis//services//trust",
	chains supported [aud , iss , lat , exp , aut_time , honce , at hash ,
	"C_nash", "Sub", "uph", "unique_name", "pwd_uri", "pwd_exp", "mid_auth_time", "Sid"],
	"https:///withts://wi
	"compating and the sector and not negative additional and the sector addition of the sector addition and the sector addition addition addition addition additional addit

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.