Add-On Products
DS Service

# ADFS Configuration for Exchange on-premises

**Document Revision: 1.0**

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

DS Service now allows single sign-on (SSO) method with Active Directory Federation Service (ADFS). This guide will explain how to install ADFS role and configure federation server to enable this SSO method.

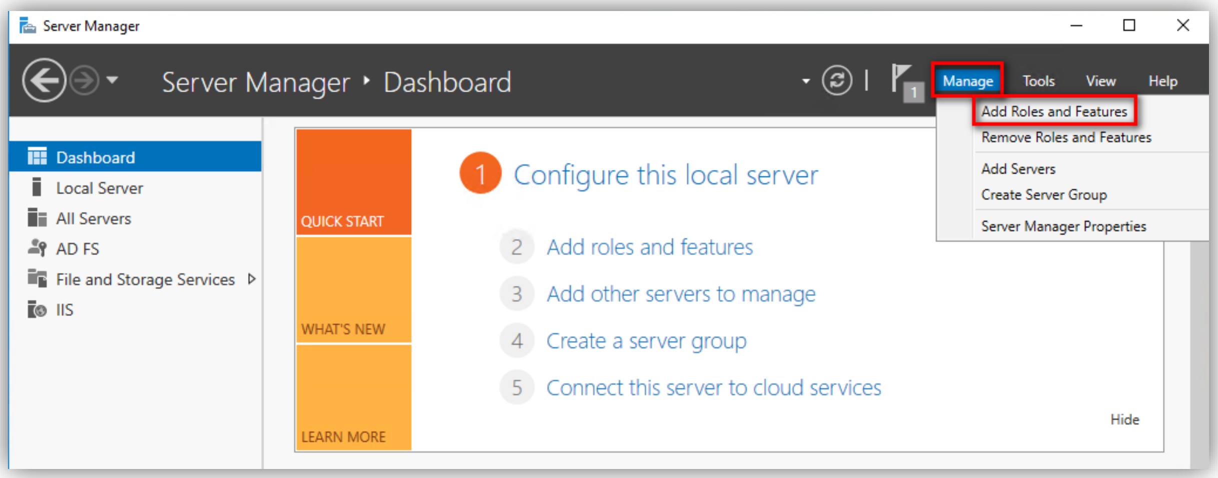
**NOTE**: Using ADFS for Single Sign On is only supported by Window server version 2016 or later. For more information, refer to: https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/development/native-client-with-ad-fs.

Kind regards,
Digital Sign Service team

# ADFS Role Installation

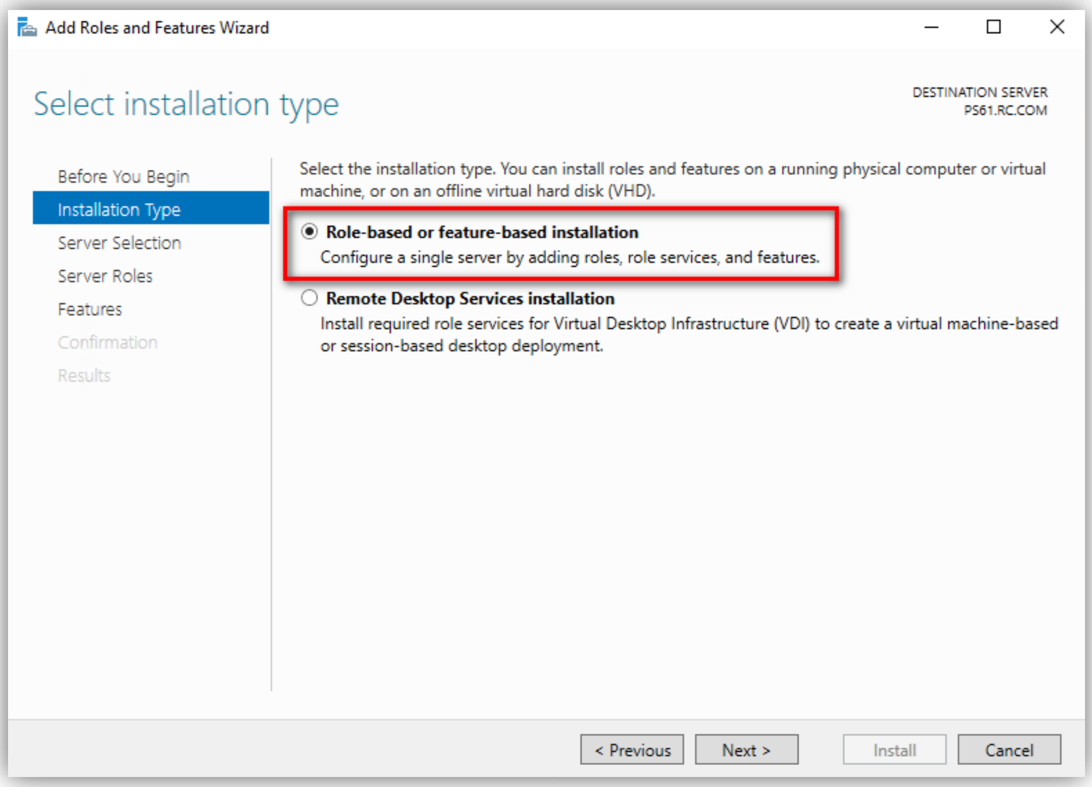
To install ADFS role, follow these steps below:

**Step 1**: Open **Server Manager**, then click [**Manage**] → [**Add roles and features**] to launch ‘Add Roles and Features Wizard’.



**Step 2**: On the ‘Before you begin’ page, click [**Next**].

**Step 3**: On the ‘Select installation type’ page, choose ‘**Role-based or Feature-based installation**’, then click [**Next**].

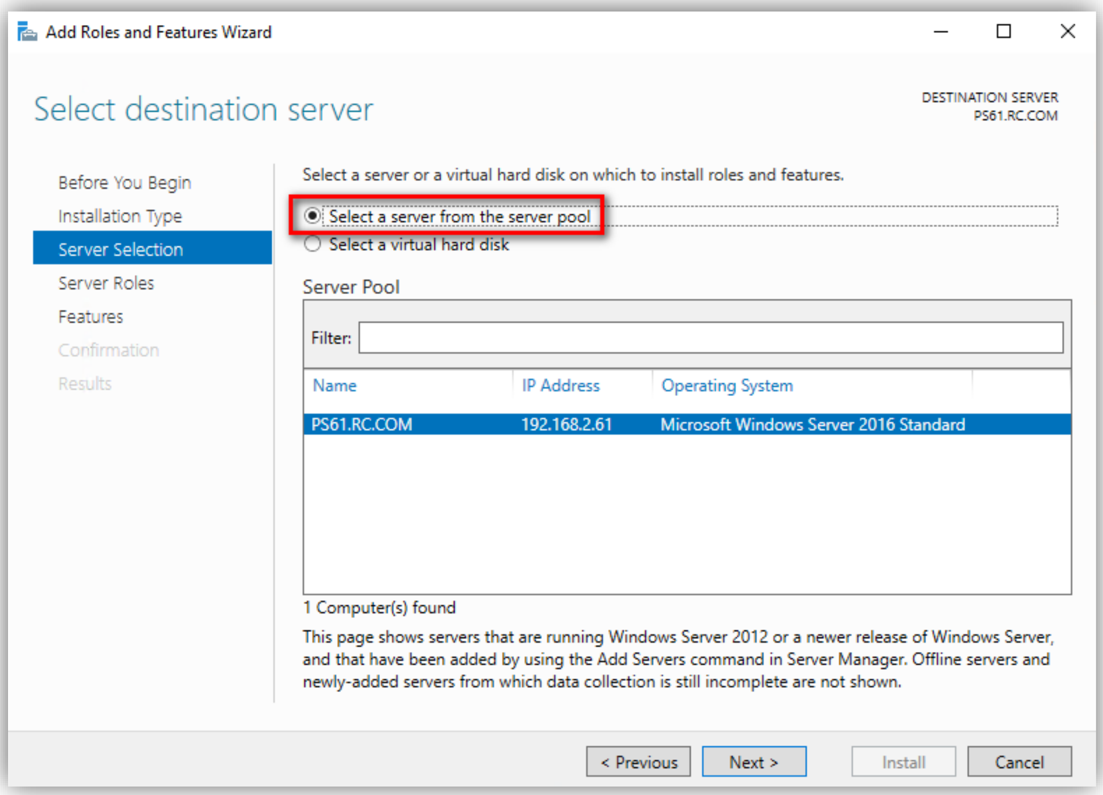


Select the installation type. You can install roles and features on a running physical computer or virtual machine, or on an offline virtual hard disk (VHD).

● **Role-based or feature-based installation**
Configure a single server by adding roles, role services, and features.

○ **Remote Desktop Services installation**
Install required role services for Virtual Desktop Infrastructure (VDI) to create a virtual machine-based or session-based desktop deployment.

**Step 4**: On the ‘Select destination server’ page, choose ‘**Select a server from the server pool**’, then select a server shown in the pool below. And click [**Next**]. I.e.:



Add Roles and Features Wizard

## Select destination server

DESTINATION SERVER
PS61.RC.COM

Select a server or a virtual hard disk on which to install roles and features.

● Select a server from the server pool
○ Select a virtual hard disk

Server Pool

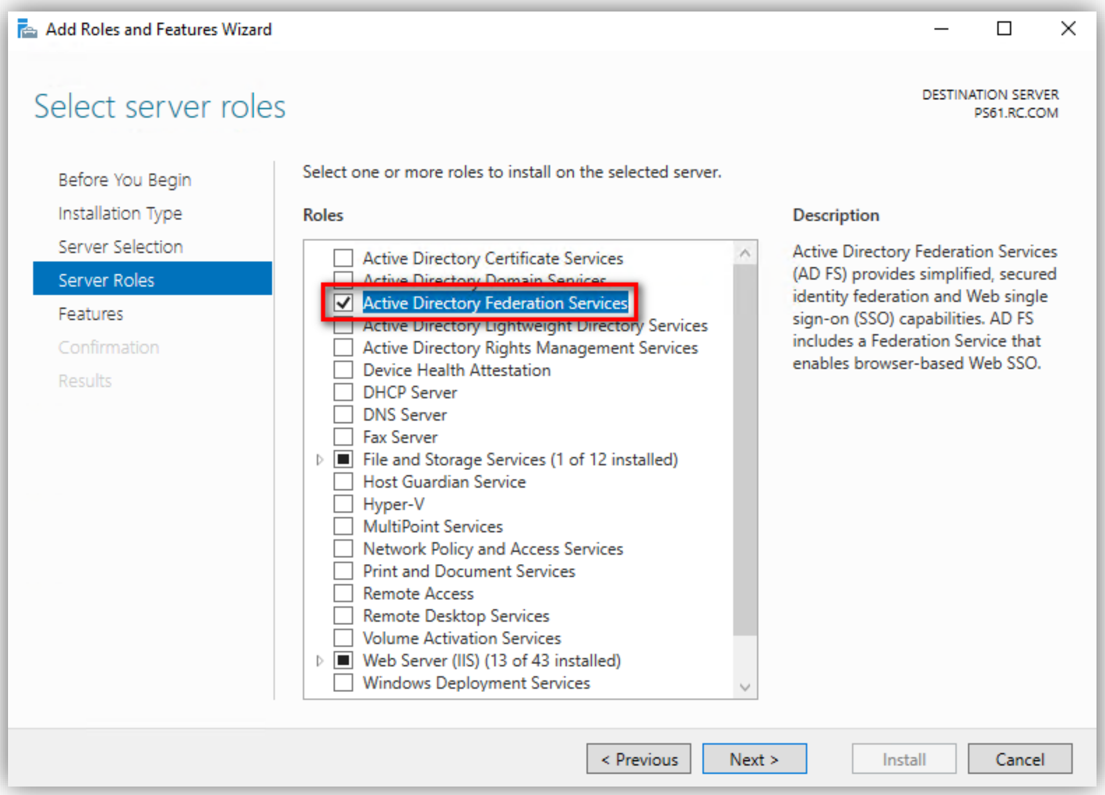
Filter:

| Name | IP Address | Operating System |
|---|---|---|
| PS61.RC.COM | 192.168.2.61 | Microsoft Windows Server 2016 Standard |

1 Computer(s) found

This page shows servers that are running Windows Server 2012 or a newer release of Windows Server, and that have been added by using the Add Servers command in Server Manager. Offline servers and newly-added servers from which data collection is still incomplete are not shown.

**Step 5**: On the ‘Select server roles’ page, select ‘**Active Directory Federation Services**’ and click [**Next**]. I.e.:



Add Roles and Features Wizard

## Select server roles

DESTINATION SERVER
PS61.RC.COM

Select one or more roles to install on the selected server.

Roles

- □ Active Directory Certificate Services
- □ Active Directory Domain Services
- ☑ Active Directory Federation Services
- □ Active Directory Lightweight Directory Services
- □ Active Directory Rights Management Services
- □ Device Health Attestation
- □ DHCP Server
- □ DNS Server
- □ Fax Server
- ■ File and Storage Services (1 of 12 installed)
- □ Host Guardian Service
- □ Hyper-V
- □ MultiPoint Services
- □ Network Policy and Access Services
- □ Print and Document Services
- □ Remote Access
- □ Remote Desktop Services
- □ Volume Activation Services
- ■ Web Server (IIS) (13 of 43 installed)
- □ Windows Deployment Services

Description

Active Directory Federation Services (AD FS) provides simplified, secured identity federation and Web single sign-on (SSO) capabilities. AD FS includes a Federation Service that enables browser-based Web SSO.

**Step 6**: On the ‘Select features’ page, click [**Next**].

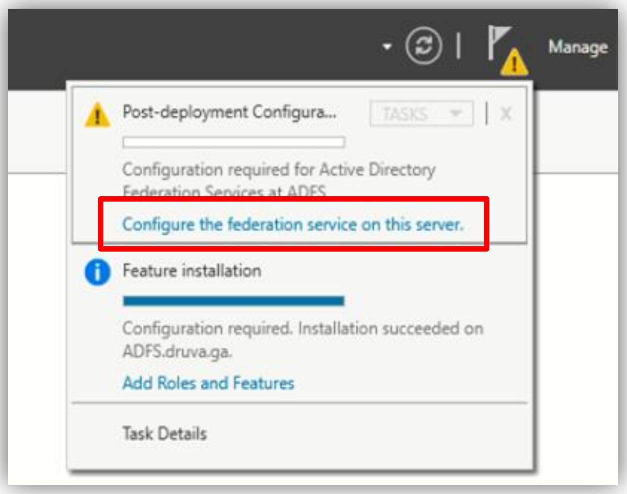
**Step 7**: On the confirmation page, click [**Install**]. The wizard will then show the installation progress. Wait until the installation completes. While waiting, you can click [**Close**] since the installation will still run in the background.

# ADFS Configuration

## Part A. Post-deployment Configuration

Follow the guide below for post-deployment configuration after the ADFS role installation.

**Step 1**: When the installation completes, you will see a new notifications flag on Server Manager dashboard. Click on the flag to show notification list, then click **Configure the federation service on the server**, i.e.:



Post-deployment Configura...

Configuration required for Active Directory Federation Services at ADFS

Configure the federation service on this server.

Feature installation

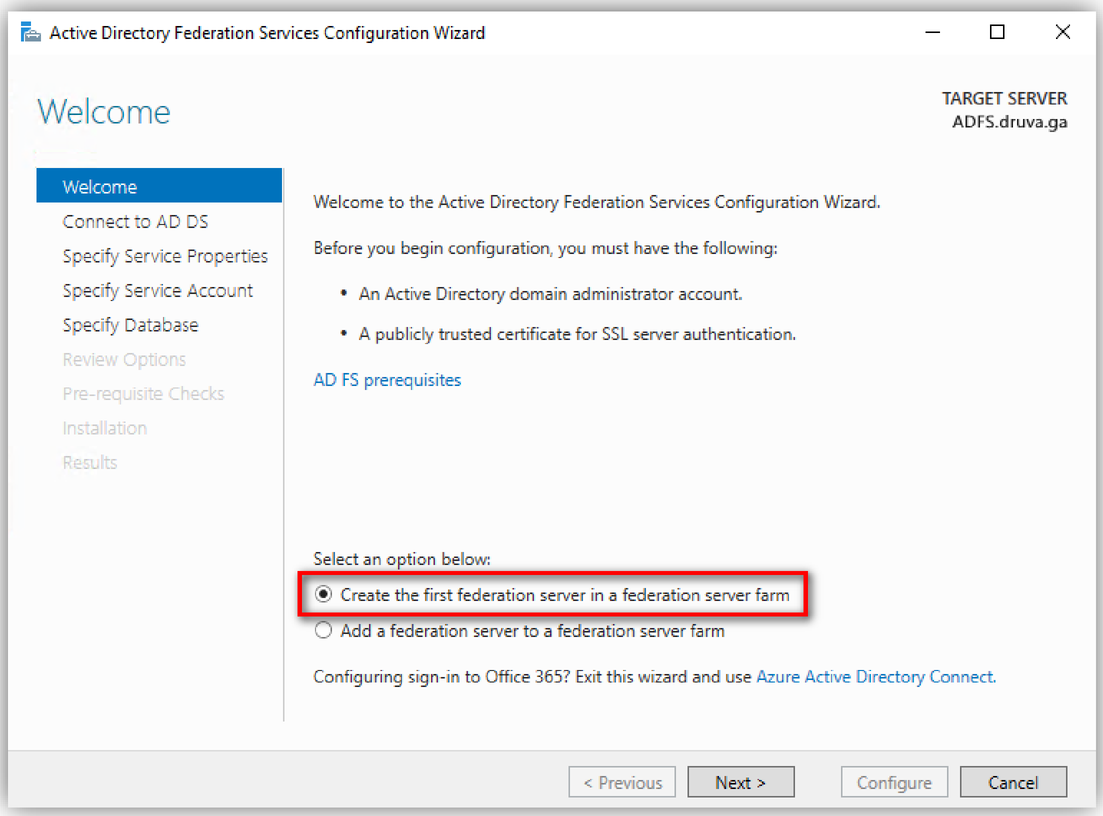
Configuration required. Installation succeeded on ADFS.druva.ga.

Add Roles and Features

Task Details

This will launch the **Active Directory Federation Service Configuration Wizard**.

**Step 2**: On the wizard’s Welcome page, select ‘**Create the first federation server in a federation server farm**’ click [**Next**].



Welcome to the Active Directory Federation Services Configuration Wizard.

Before you begin configuration, you must have the following:

- An Active Directory domain administrator account.
- A publicly trusted certificate for SSL server authentication.

AD FS prerequisites

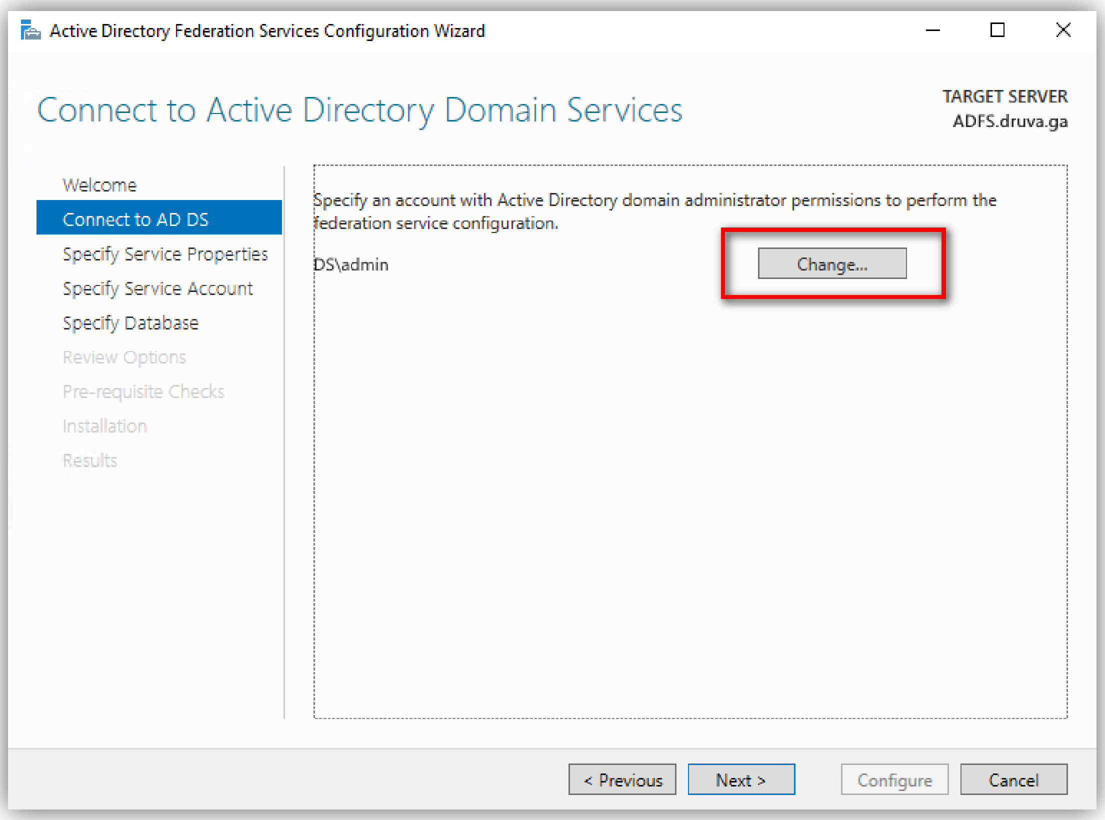
Select an option below:

● Create the first federation server in a federation server farm

○ Add a federation server to a federation server farm

Configuring sign-in to Office 365? Exit this wizard and use Azure Active Directory Connect.

**Step 3**: On the ‘Connect to Active Directory Domain Services’ page, click [**Change**] and specify an account with domain administrator rights for the Active Directory domain that this system is connected to. Then click [**Next**].



Active Directory Federation Services Configuration Wizard

Connect to Active Directory Domain Services

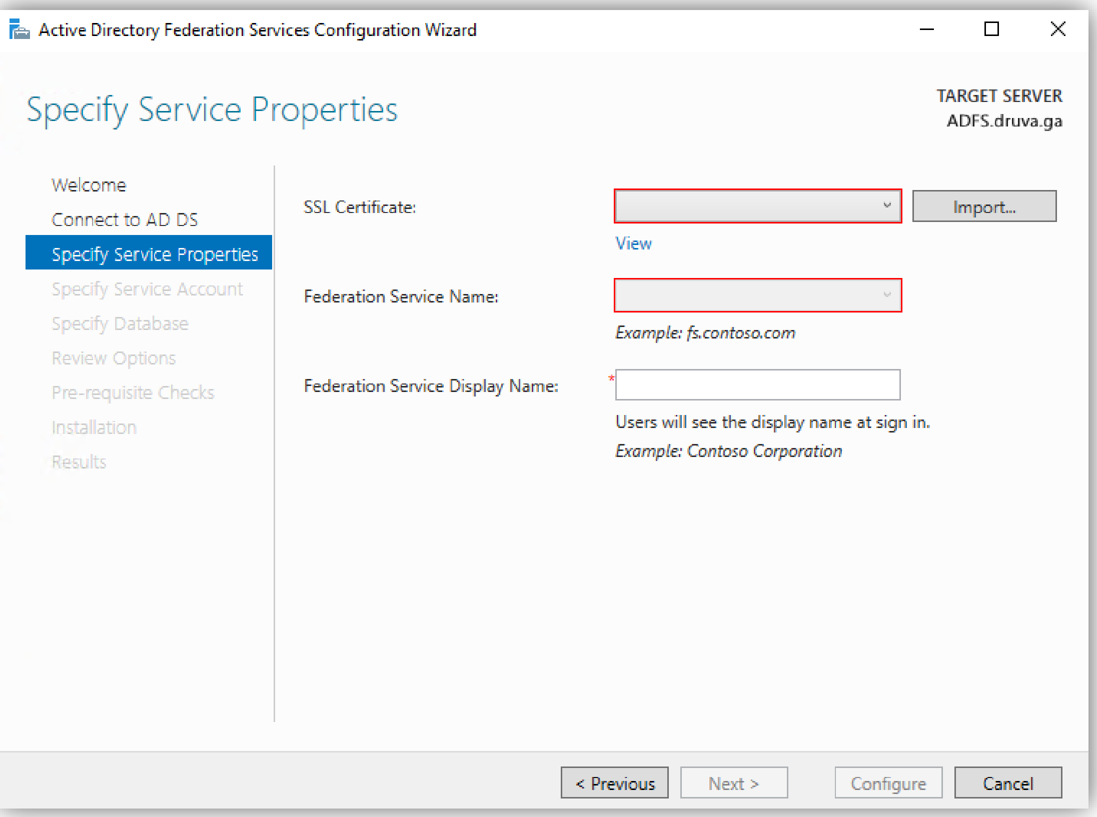
TARGET SERVER
ADFS.druva.ga

Specify an account with Active Directory domain administrator permissions to perform the federation service configuration.

DS\admin

**Step 4**: On the ‘Specify Service Properties’ page, setup the following properties:

- **SSL Certificate**: Browse to the location of the SSL certificate and import it.
- **Federation Service Name**: This applies the same value provided when you enrolled an SSL certificate in Active Directory Certificate Services (AD CS).
- **Federation Service Display Name**: Enter a display name.



Active Directory Federation Services Configuration Wizard

Specify Service Properties

TARGET SERVER
ADFS.druva.ga

SSL Certificate:

Federation Service Name:

*Example: fs.contoso.com*

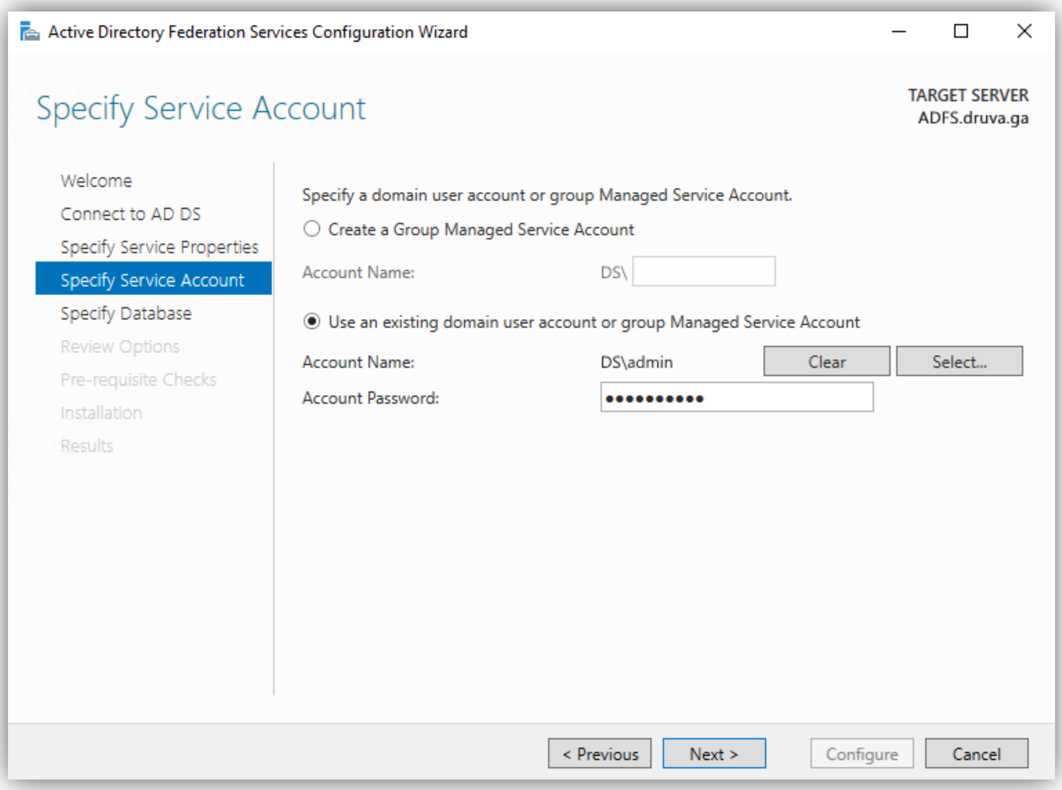
Federation Service Display Name: *

Users will see the display name at sign in.
*Example: Contoso Corporation*

Afterwards, click [**Next**].

**NOTE**: If you do not have SSL certificate yet, refer to Appendix A in this document to create SSL certificate.

**Step 5**: On the ‘Specify Service Account’ page, select ‘**Use an existing domain user account**’ and specify a user or service account. Then click [**Next**].



Specify a domain user account or group Managed Service Account.

○ Create a Group Managed Service Account

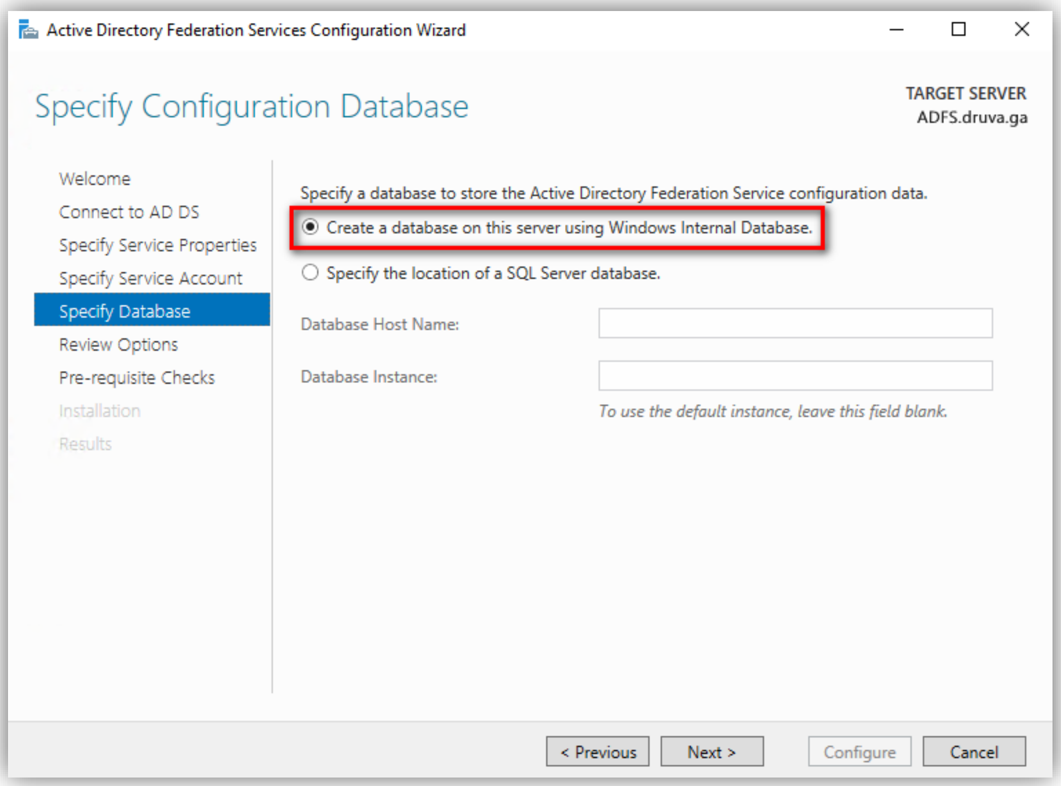
Account Name: DS\

● Use an existing domain user account or group Managed Service Account

Account Name: DS\admin

Account Password: ●●●●●●●●●●●

**Step 6**: On the ‘Specify Configuration Database’ page, select ‘**Create a database on this server using Windows Internal Database**’ and click [**Next**].



Active Directory Federation Services Configuration Wizard

Specify Configuration Database

TARGET SERVER
ADFS.druva.ga

Specify a database to store the Active Directory Federation Service configuration data.

● Create a database on this server using Windows Internal Database.

○ Specify the location of a SQL Server database.

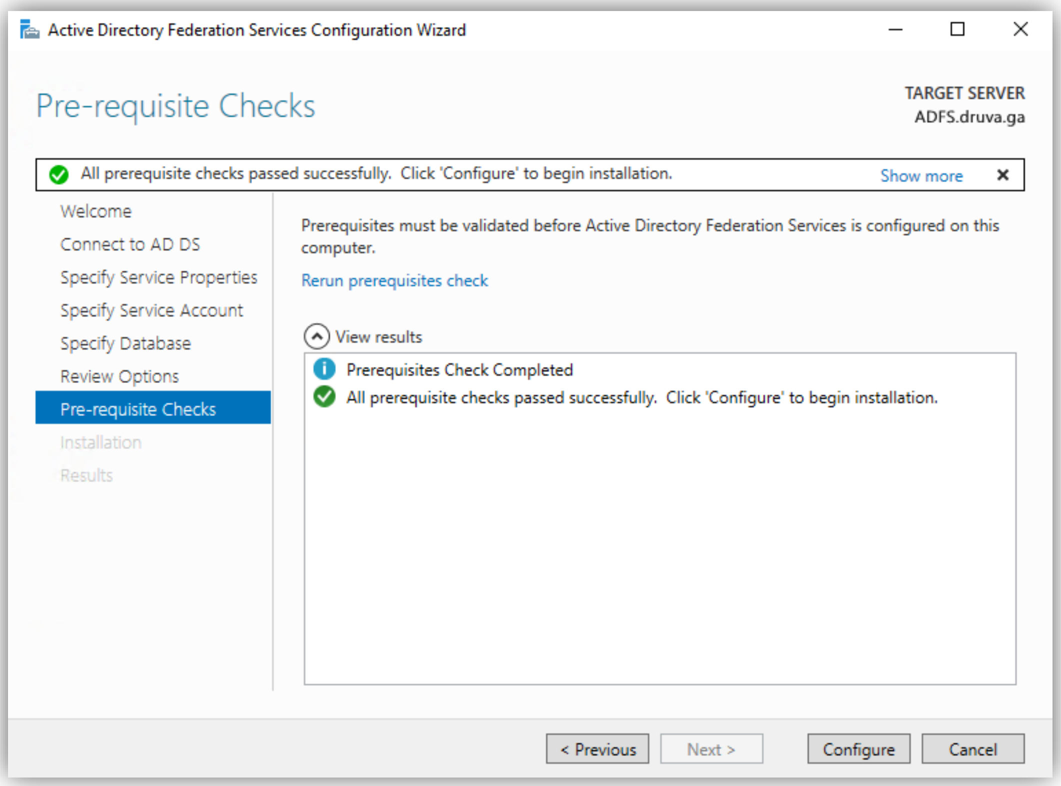
Database Host Name:

Database Instance:

*To use the default instance, leave this field blank.*

**Step 7**: On the ‘Review Options’ page, after a short while the wizard will show you all the selections you have made. When you finish your review, click [**Next**].

**Step 8**: On the ‘Pre-requisite Checks’ screen, it will check if all the prerequisites are validated for ADFS configuration. After a short while, the results will be shown in the box below. I.e.:



Active Directory Federation Services Configuration Wizard

Pre-requisite Checks

TARGET SERVER
ADFS.druva.ga

✓ All prerequisite checks passed successfully. Click 'Configure' to begin installation.

Prerequisites must be validated before Active Directory Federation Services is configured on this computer.

Rerun prerequisites check

View results

Prerequisites Check Completed

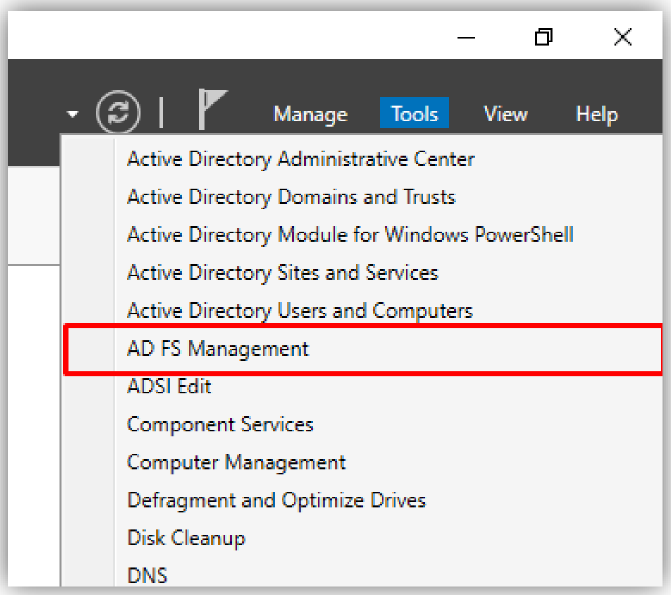
✓ All prerequisite checks passed successfully. Click 'Configure' to begin installation.

When all prerequisite checks passed successfully, click [**Configure**] to finally install ADFS. You can get to the ‘Results’ page once the process is done.

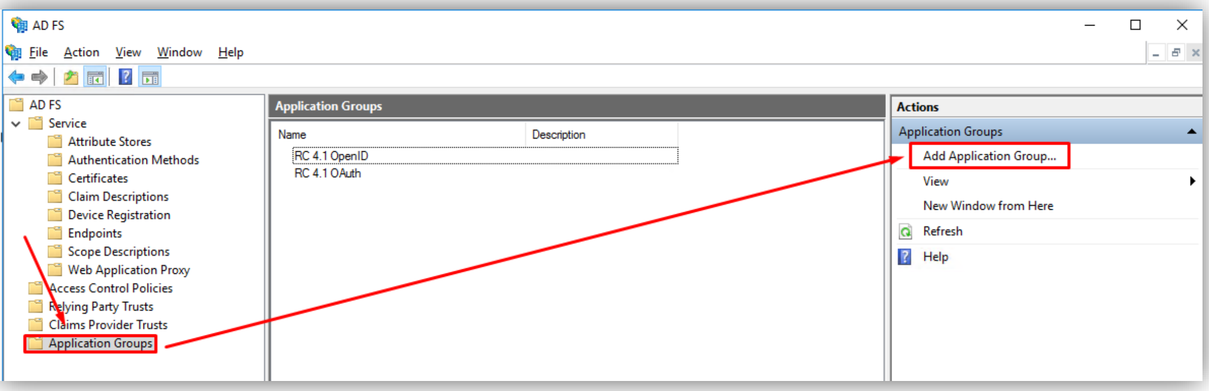
## Part B. AD FS Management Configuration

**NOTE**: Post-deployment Configuration for ADFS is required. If it is not completed or failed, you will not be able to fully configure on **AD FS Management** despite being able to open the tool.

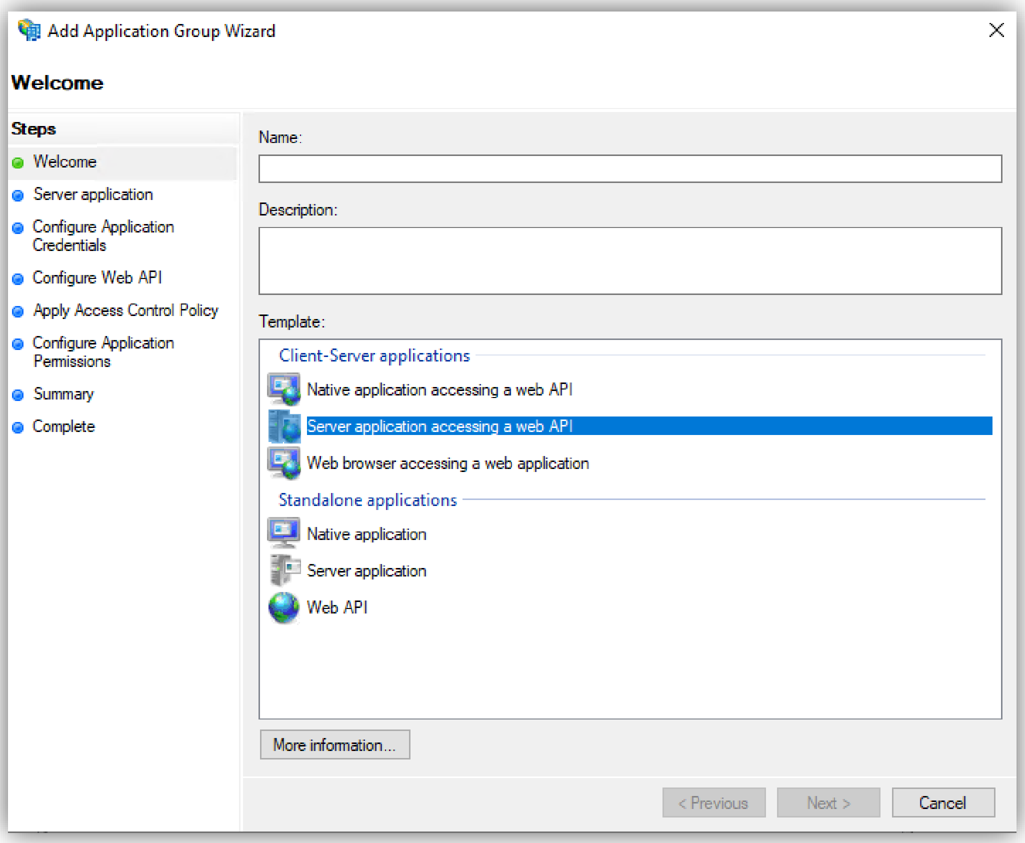
**Step 1**: Go to **web server** where your Exchange server is installed, open **Server Manager**, then click [**Tools**] → [**AD FS Management**].


Manage
Tools
View
Help
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

**Step 2**: In the opened window, select **Application Groups** and click [**Add Application Group…**] from the **Actions** sidebar to launch configuration wizard for a new Group.



**Step 3**: On the ‘Add Application Group wizard’ → ‘Welcome’ screen, fill in a Name and select ‘**Server application accessing a web API**’ in Template. Then click [**Next].**



Add Application Group Wizard

Welcome

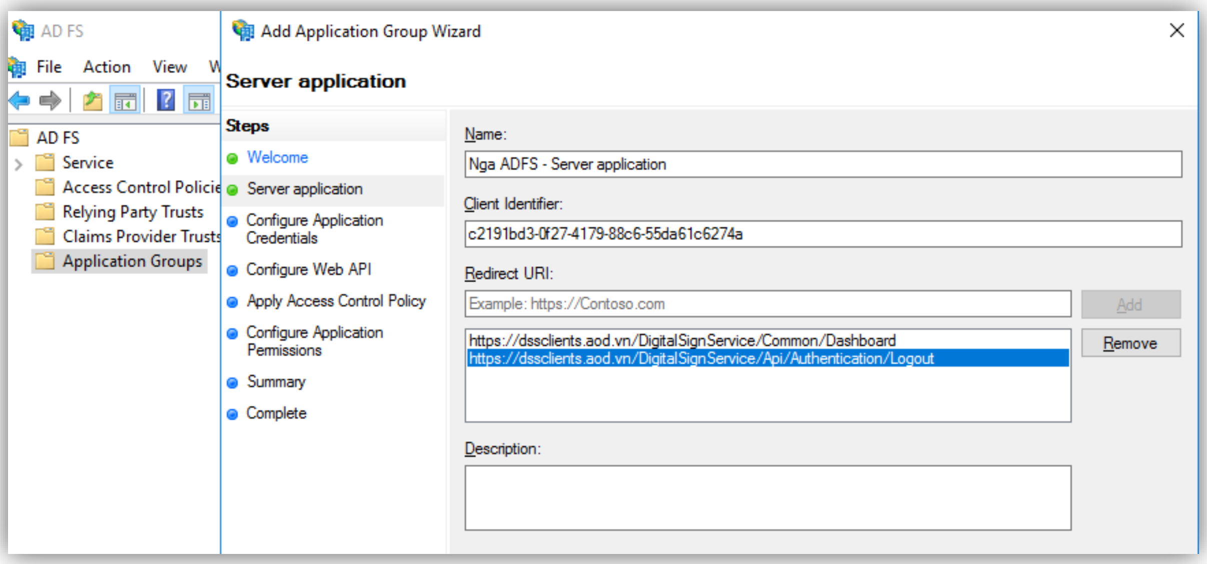
Name:

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

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



Add Application Group Wizard

Server application

Name: Nga ADFS - Server application

Client Identifier: c2191bd3-0f27-4179-88c6-55da61c6274a

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

https://dssclients.aod.vn/DigitalSignService/Common/Dashboard
https://dssclients.aod.vn/DigitalSignService/Api/Authentication/Logout

Description:

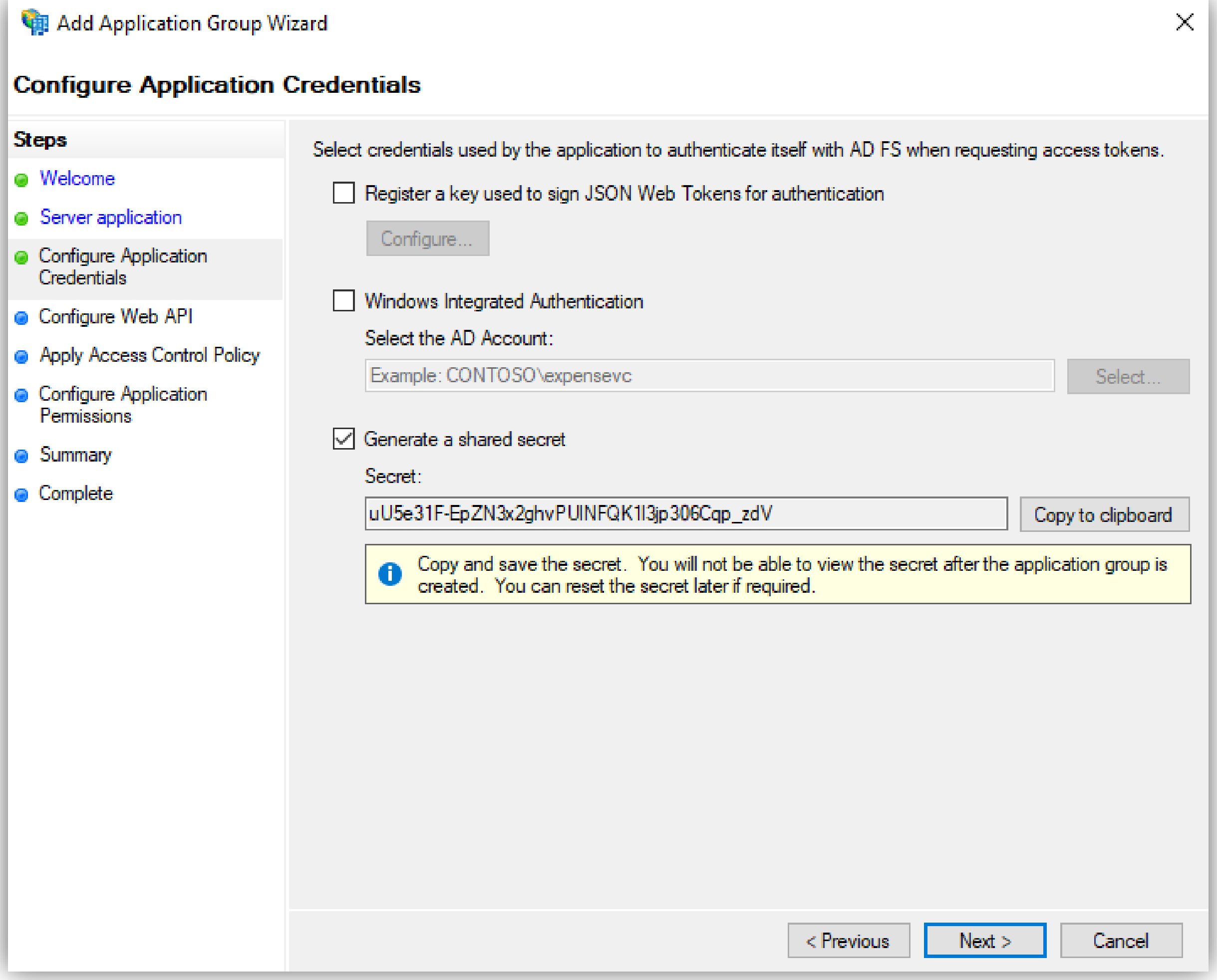
The URL for receiving logout details from ADFS must have the following format:

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

E.g., http://dssclients.aod.vn/DigitalSignService/Api/Authentication/Logout

Then click [**Next**].

**Step 5**: On the ‘Configure Application Credentials’ screen, 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
Configure Web API
Apply Access Control Policy
Configure Application Permissions
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

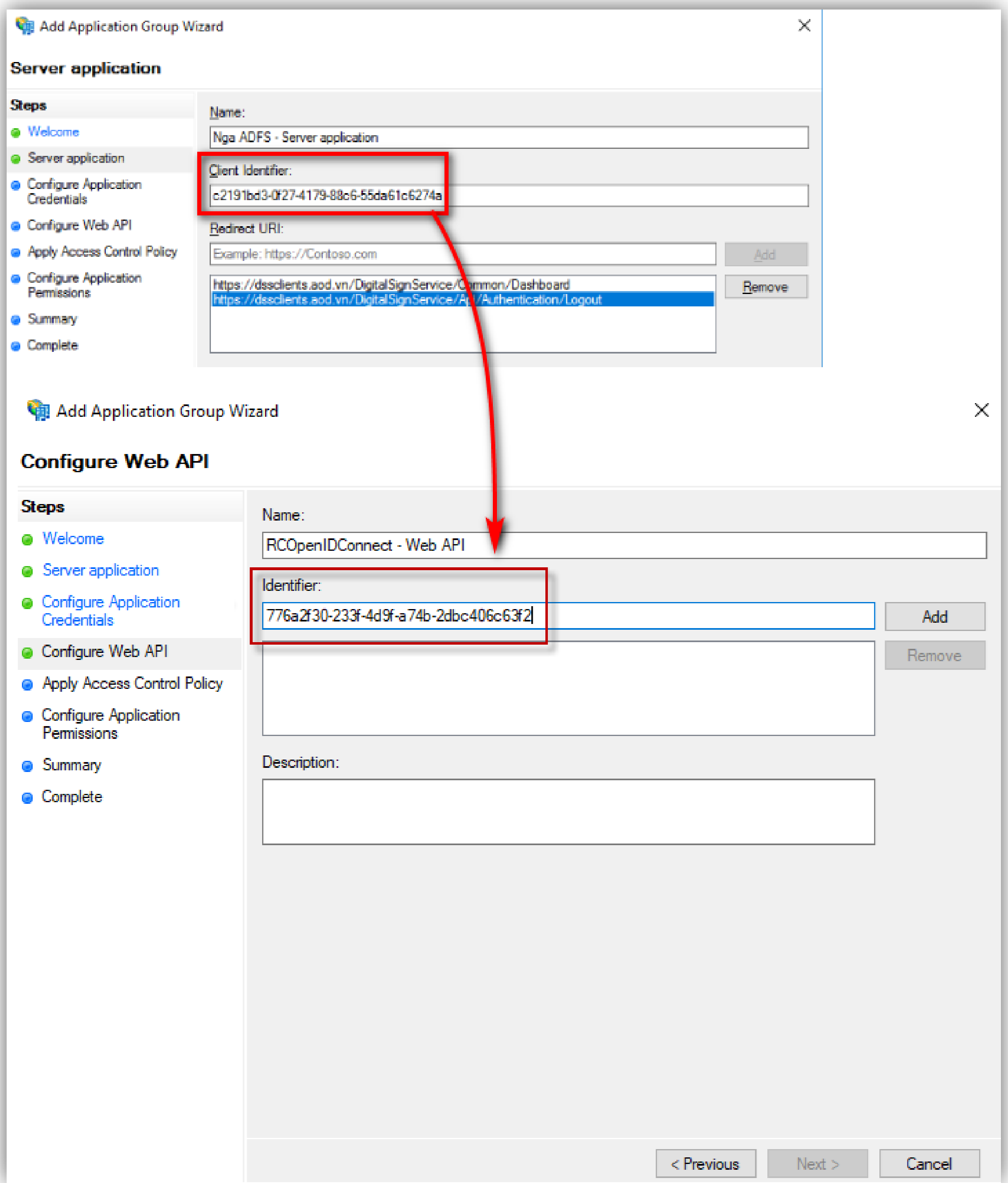
☑ Generate a shared secret

Secret: uU5e31F-EpZN3x2ghvPUINFQK1I3jp306Cqp_zdV

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

Then click [**Next**].

**Step 6**: On ‘Configure Web API’ screen, copy the **Client Identifier** from Step 4 to fill in **Identifier** field and click [**Add**] button.



Add Application Group Wizard

Server application

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

Name: Nga ADFS - Server application

Client Identifier: c2191bd3-0f27-4179-88c6-55da61c6274a

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

https://dssclients.aod.vn/DigitalSignService/Common/Dashboard
https://dssclients.aod.vn/DigitalSignService/Api/Authentication/Logout

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

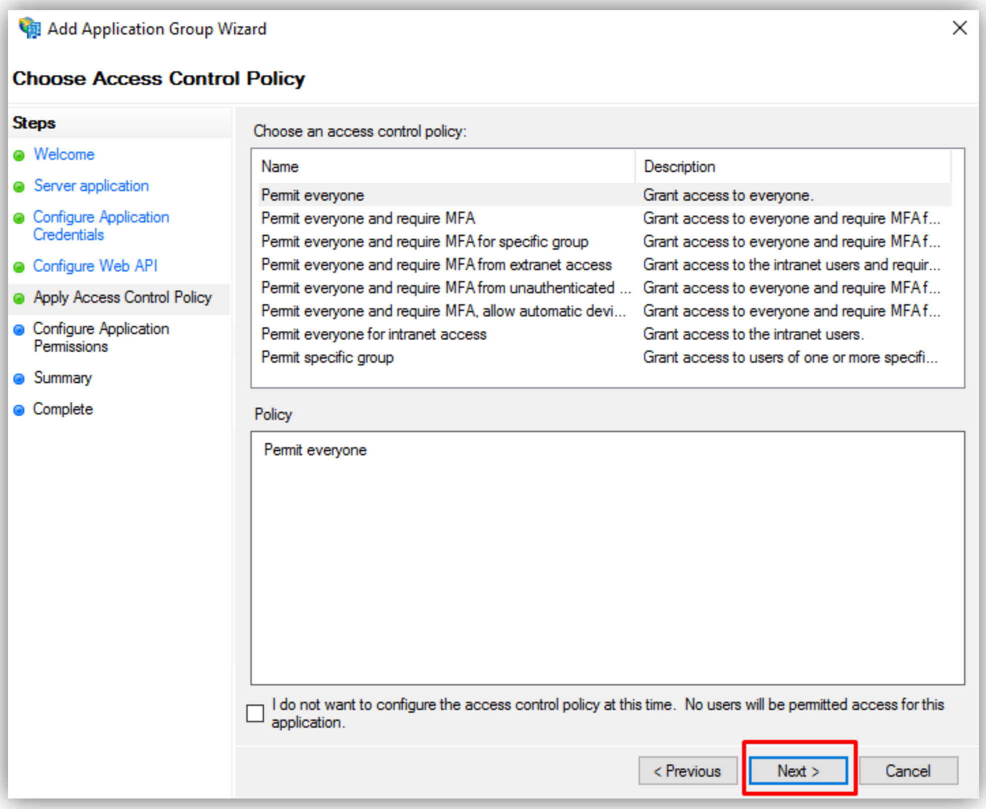
Name: RCOpenIDConnect - Web API

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

Description:

After that, click [**Next**].

**Step 7**: On ‘Choose Access Control Policy’ screen, click [**Next**].



Add Application Group Wizard

Choose Access Control Policy

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

Choose an access control policy:

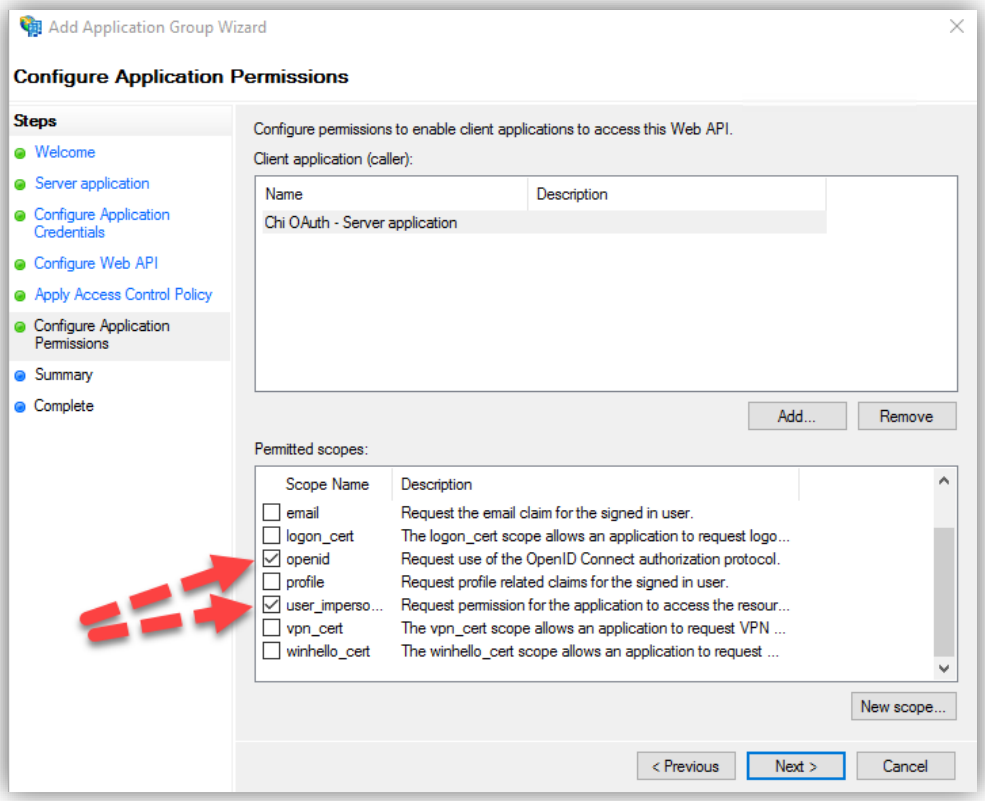
| Name | Description |
|---|---|
| Permit everyone | Grant access to everyone. |
| Permit everyone and require MFA | Grant access to everyone and require MFA f... |
| Permit everyone and require MFA for specific group | Grant access to everyone and require MFA f... |
| Permit everyone and require MFA 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.

**Step 8**: On ‘Configure Application Permissions’ screen, check on **openid** and **user_impersonate** checkboxes.



Add Application Group Wizard

Configure Application Permissions

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

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

Client application (caller):

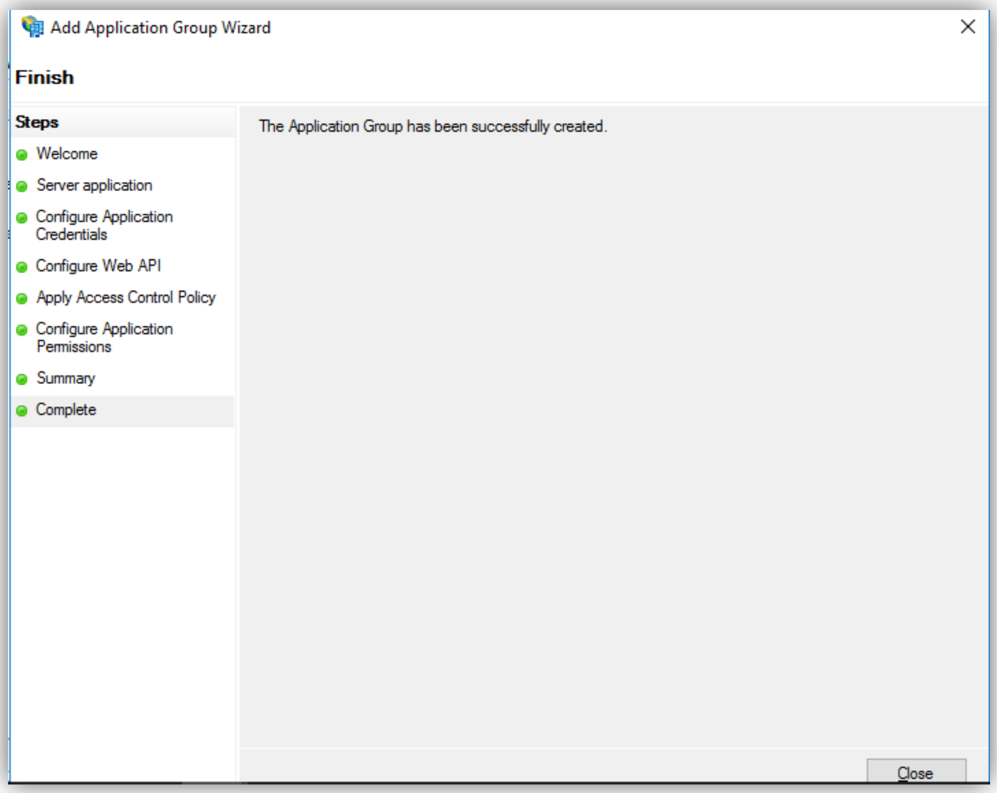
| Name | Description |
|---|---|
| Chi OAuth - Server application | |

Permitted scopes:

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

Click [**Next**] proceed.

**Step 8**: On ‘Summary’ screem, click [**Next**] which will move to ‘Complete’ screen, then click [**Close**] to finish.

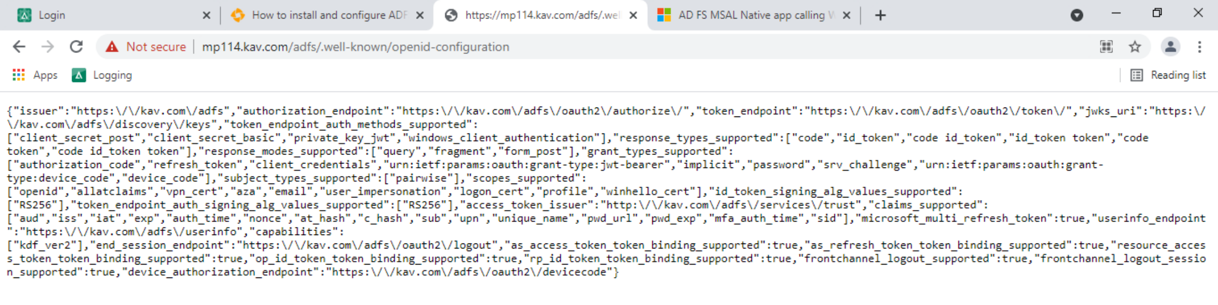

Add Application Group Wizard
Finish
Steps
Welcome
Server application
Configure Application Credentials
Configure Web API
Apply Access Control Policy
Configure Application Permissions
Summary
Complete
Close

The Application Group has been successfully created.

**Step 9**: Check if the configuration is done correctly by running the hyperlink below on the browser:

[https://mp114.kav.com/adfs/.well-known/openid-configuration](https://mp114.kav.com/adfs/.well-known/openid-configuration)

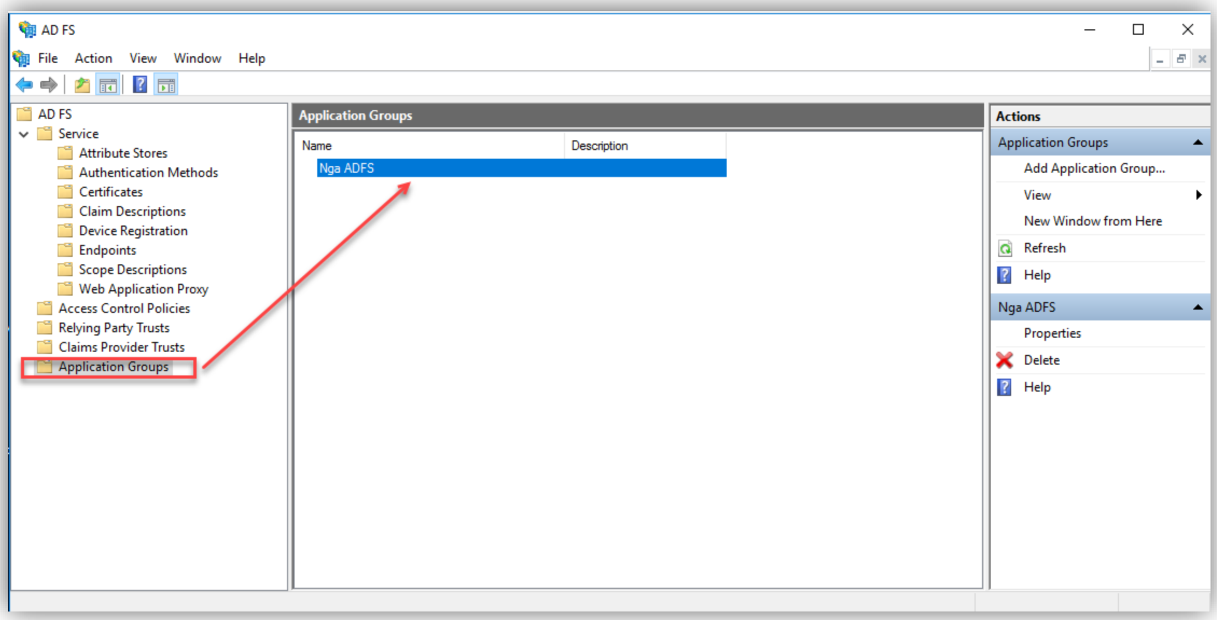
I.e.:


Login
How to install and configure ADF
https://mp114.kav.com/adfs/.wel
AD FS MSAL Native app calling W
Not secure
mp114.kav.com/adfs/.well-known/openid-configuration
Apps
Logging
Reading list

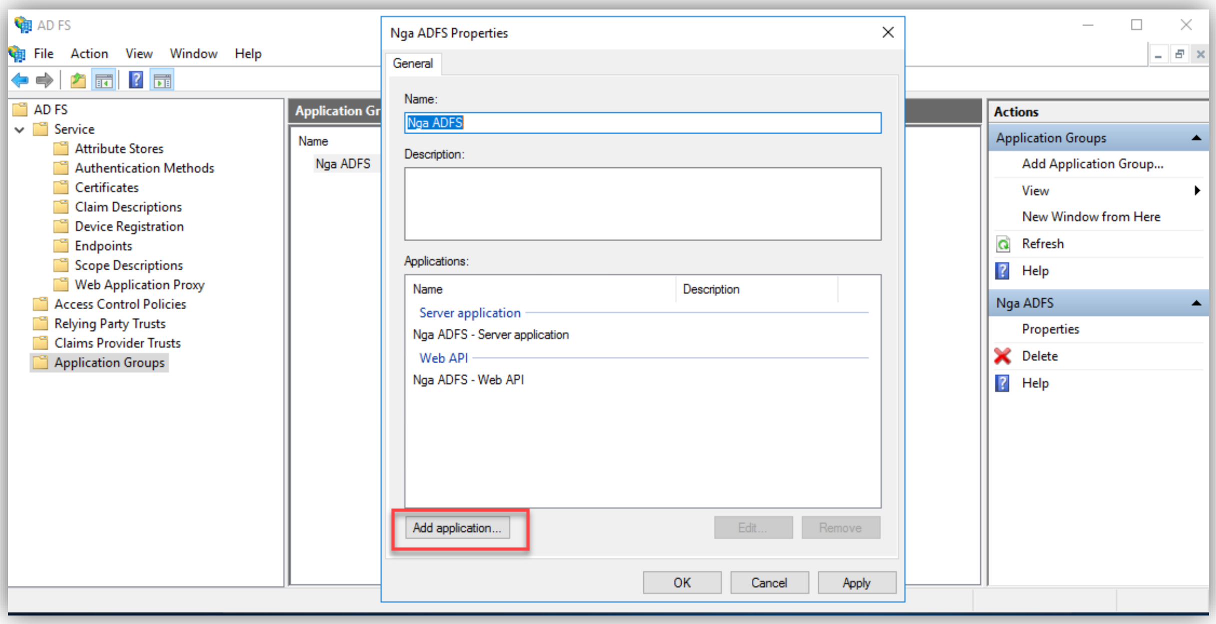
```
{"issuer":"https:\/\/kav.com\/adfs","authorization_endpoint":"https:\/\/kav.com\/adfs\/oauth2\/authorize\/","token_endpoint":"https:\/\/kav.com\/adfs\/oauth2\/token\/","jwks_uri":"https:\/
\/kav.com\/adfs\/discovery\/keys","token_endpoint_auth_methods_supported":
["client_secret_post","client_secret_basic","private_key_jwt","windows_client_authentication"],"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":
["openid","allatclaims","vpn_cert","aza","email","user_impersonation","logon_cert","profile","winhello_cert"],"id_token_signing_alg_values_supported":
["RS256"],"token_endpoint_auth_signing_alg_values_supported":["RS256"],"access_token_issuer":"http:\/\/kav.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:\/\/kav.com\/adfs\/userinfo","capabilities":
["kdf_ver2"],"end_session_endpoint":"https:\/\/kav.com\/adfs\/oauth2\/logout","as_access_token_token_binding_supported":true,"as_refresh_token_token_binding_supported":true,"resource_acces
s_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_sessio
n_supported":true,"device_authorization_endpoint":"https:\/\/kav.com\/adfs\/oauth2\/devicecode"}
```

## Part C. Adding Native Application

**Step 1**: After AD FS Management Configuration from Part B, on Server Manager, click [**Tool**] → [**AD FS Management**], you will see a new name in 'Application Groups' list. I.e.:



Double click on this new application, and click [**Add Application**].



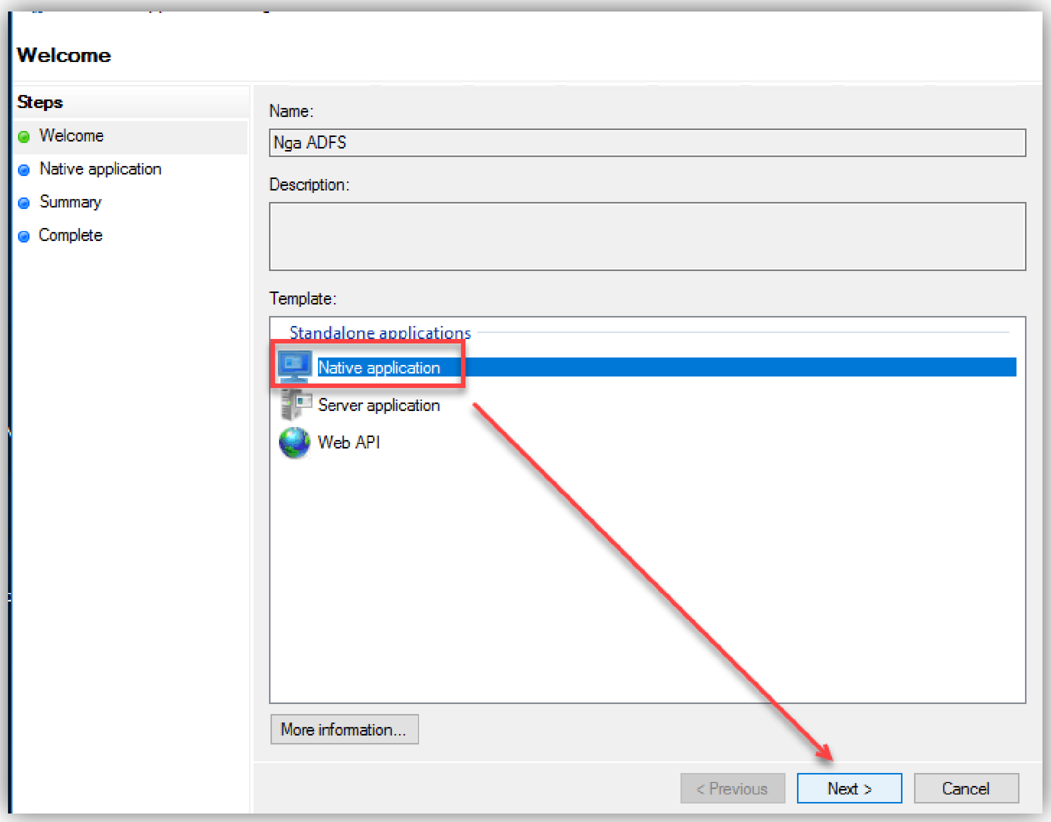
Name: Nga ADFS

Description:

Applications:

| Name | Description |
|---|---|
| Server application | |
| Nga ADFS - Server application | |
| Web API | |
| Nga ADFS - Web API | |

This will open 'Welcome' screen below. Here, select '**Native application**' and click [**Next**].



Welcome

Steps
- Welcome
- Native application
- Summary
- Complete

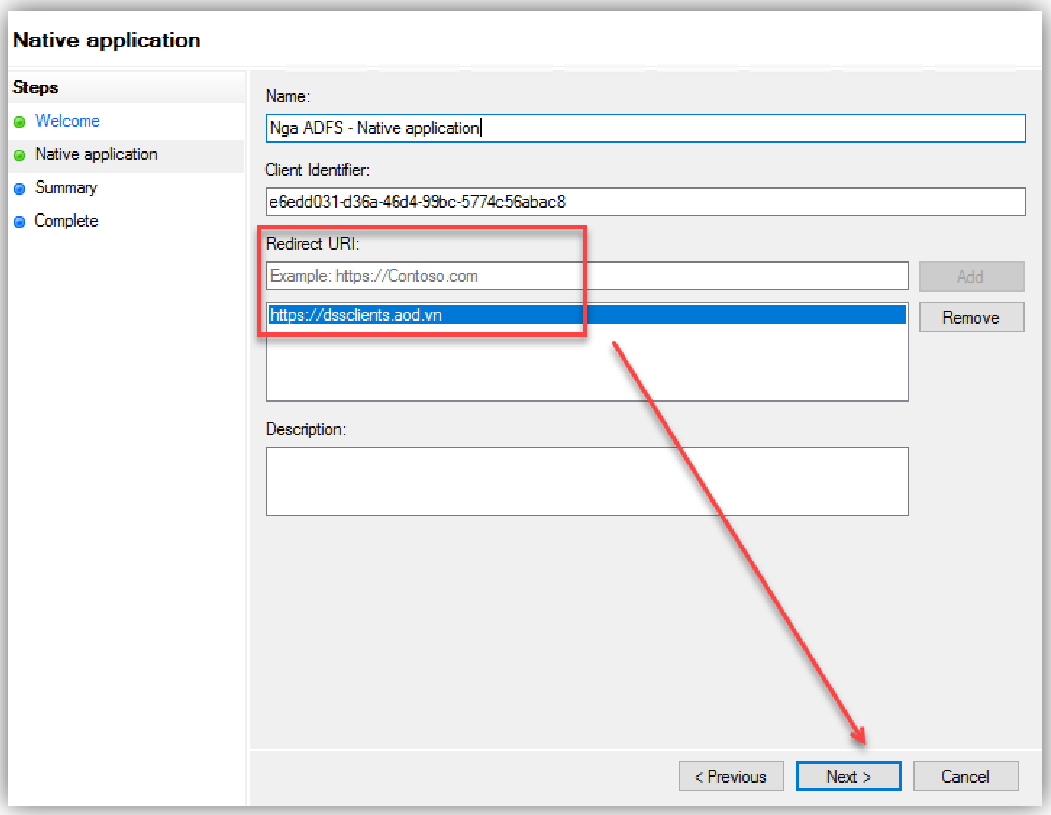
Name: Nga ADFS

Description:

Template:

Standalone applications
- Native application
- Server application
- Web API

**Step 2**: On 'Native application' screen, add **Redirect URI** then click [**Next**].



Native application

Steps

- Welcome
- Native application
- Summary
- Complete

Name: Nga ADFS - Native application

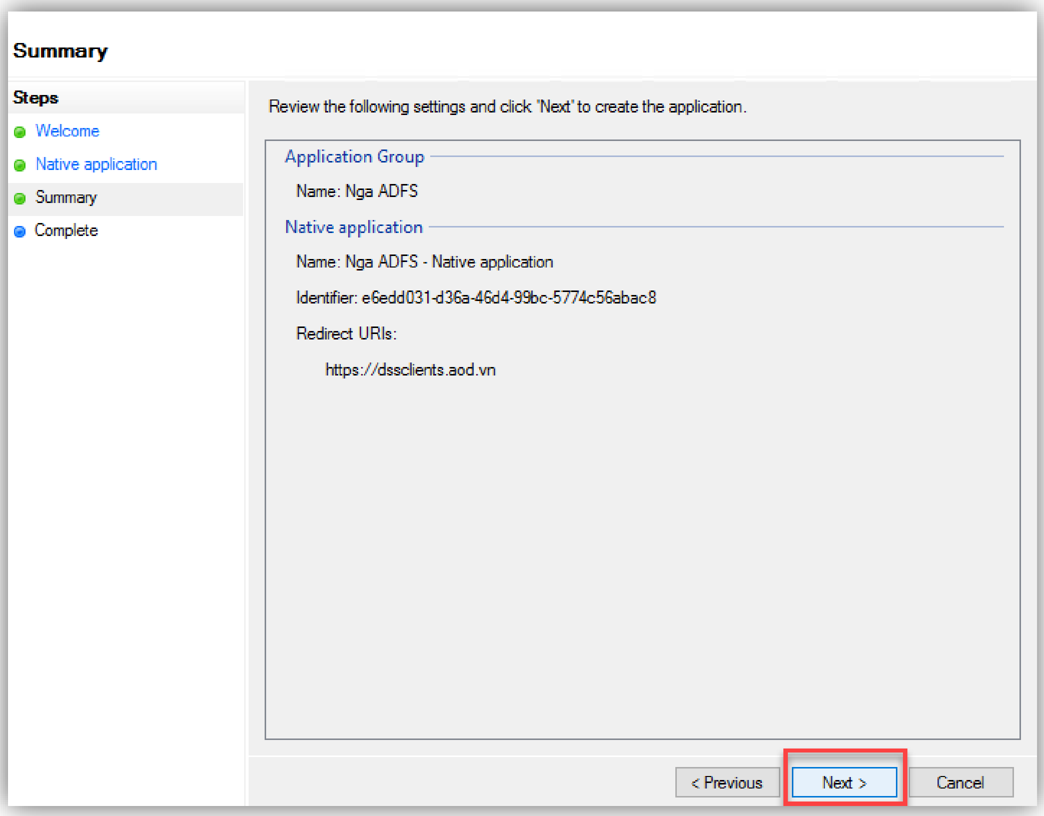
Client Identifier: e6edd031-d36a-46d4-99bc-5774c56abac8

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

https://dssclients.aod.vn

Description:

**Step 3**: On ‘Summary’ screen, you can review all the information. If there is no change, click [**Next**] to proceed.



Summary

Review the following settings and click 'Next' to create the application.

Application Group

Name: Nga ADFS

Native application

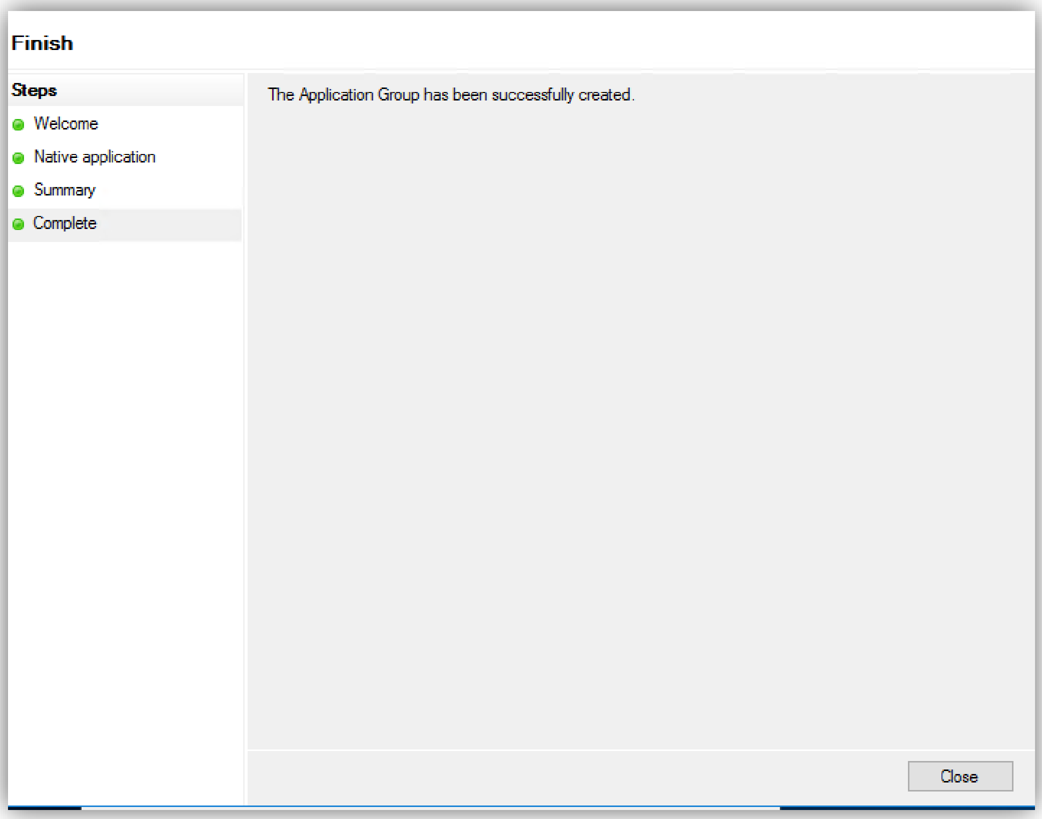
Name: Nga ADFS - Native application

Identifier: e6edd031-d36a-46d4-99bc-5774c56abac8

Redirect URIs:

https://dssclients.aod.vn

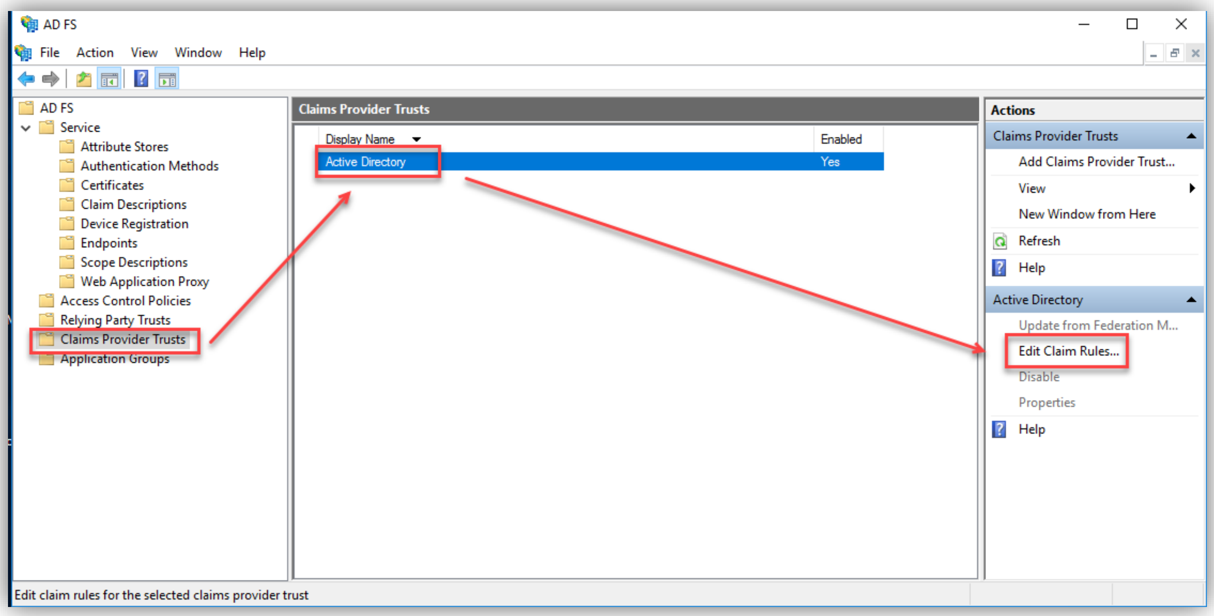
Then click [**Close**] on the next screen.



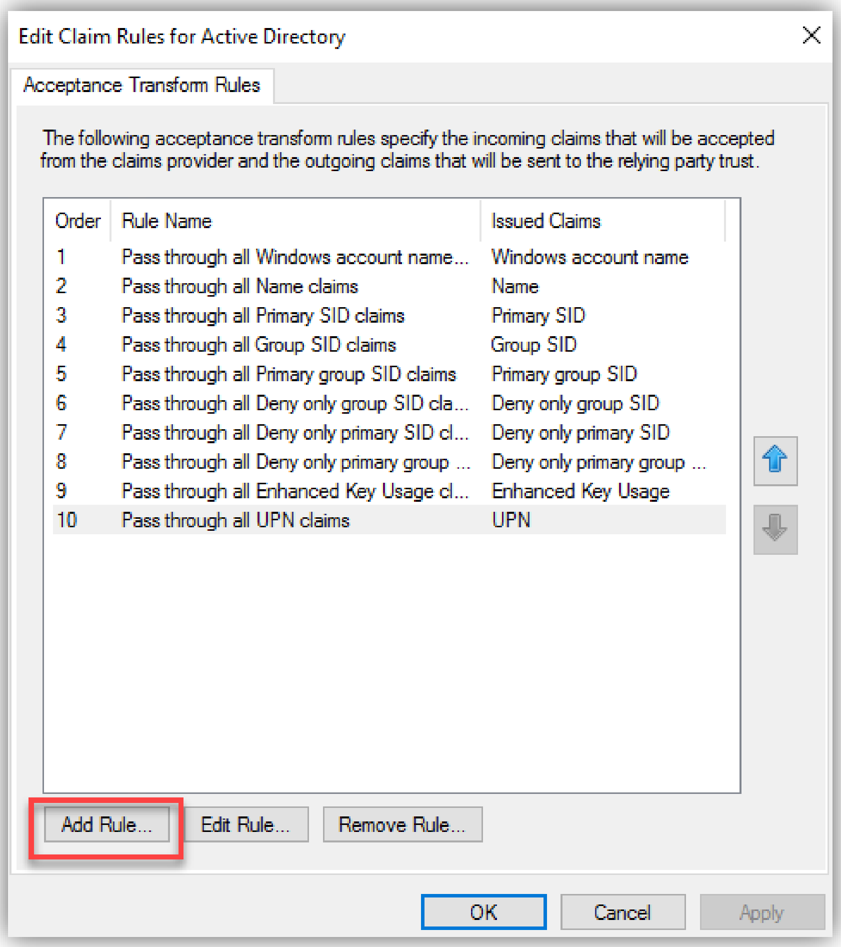
Finish

The Application Group has been successfully created.

**Step 4**: On AD FS window, select **Claims Provider Trusts**, then select **Active Directory** and click [**Edit Claim Rules**] to open this screen.



**Step 5**: On ‘Edit Claim Rules for Active Directory’ screen, click [**Add Rule…**].



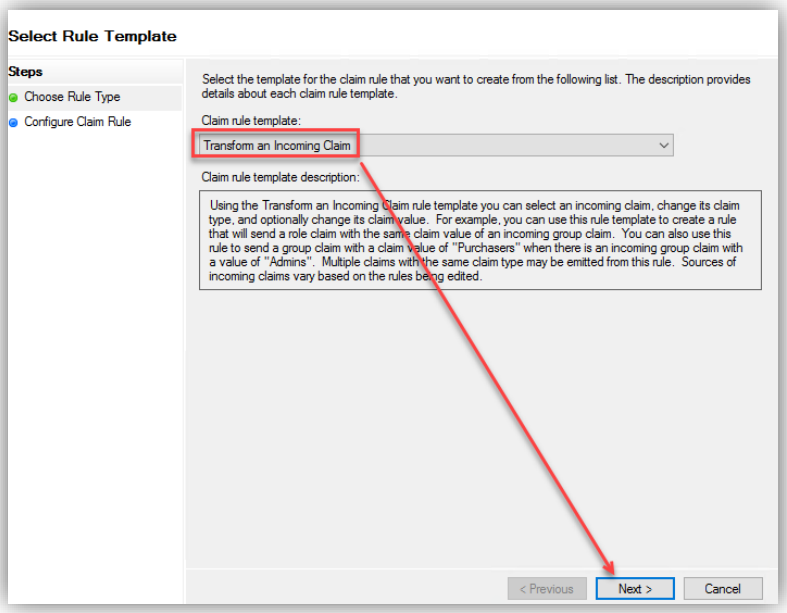
Edit Claim Rules for Active Directory

Acceptance Transform Rules

The following acceptance transform rules specify the incoming claims that will be accepted from the claims provider and the outgoing claims that will be sent to the relying party trust.

| Order | Rule Name | Issued Claims |
|---|---|---|
| 1 | Pass through all Windows account name... | Windows account name |
| 2 | Pass through all Name claims | Name |
| 3 | Pass through all Primary SID claims | Primary SID |
| 4 | Pass through all Group SID claims | Group SID |
| 5 | Pass through all Primary group SID claims | Primary group SID |
| 6 | Pass through all Deny only group SID cla... | Deny only group SID |
| 7 | Pass through all Deny only primary SID cl... | Deny only primary SID |
| 8 | Pass through all Deny only primary group ... | Deny only primary group ... |
| 9 | Pass through all Enhanced Key Usage cl... | Enhanced Key Usage |
| 10 | Pass through all UPN claims | UPN |

**Step 6**: On ‘Select Rule Template’ screen, select **Transform an Incoming Claim** for ‘Claim rule template’, then click [**Next**].



Select Rule Template

Steps
- Choose Rule Type
- Configure Claim Rule

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

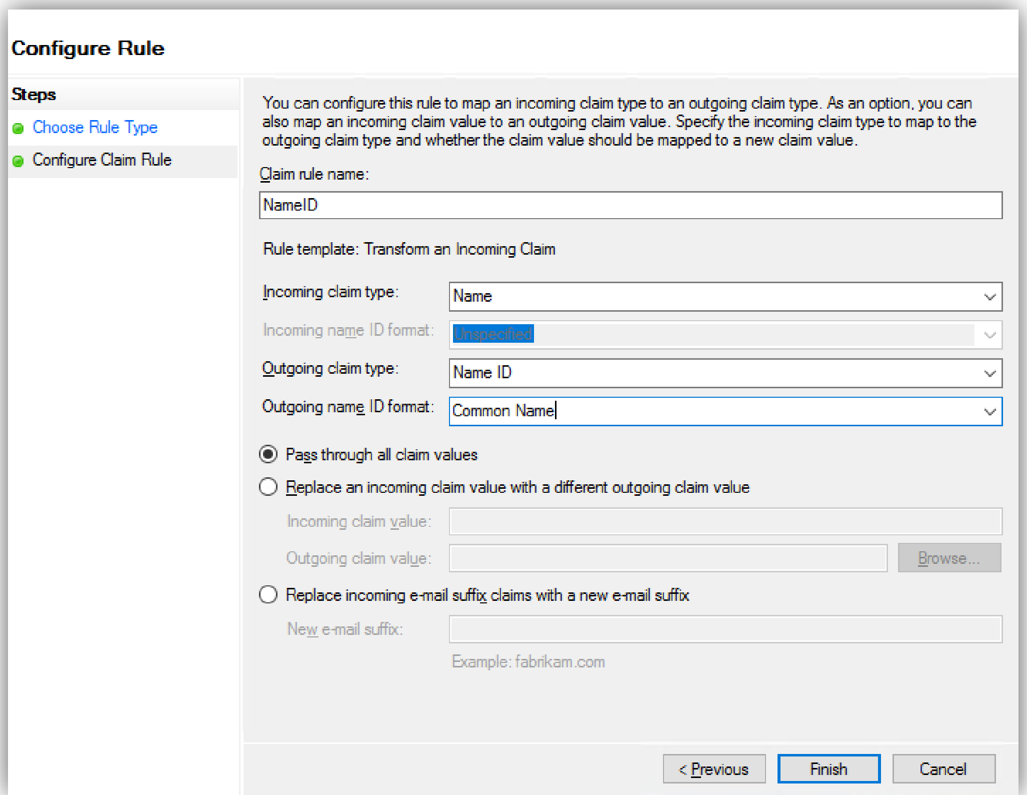
Claim rule template: Transform an Incoming Claim

Claim rule template description:

Using the Transform an Incoming Claim rule template you can select an incoming claim, change its claim type, and optionally change its claim value. For example, you can use this rule template to create a rule that will send a role claim with the same claim value of an incoming group claim. You can also use this rule to send a group claim with a claim value of "Purchasers" when there is an incoming group claim with a value of "Admins". Multiple claims with the same claim type may be emitted from this rule. Sources of incoming claims vary based on the rules being edited.

**Step 7**: On ‘Configure Claim Rule’ screen, fill in the following fields:

- **Claim rule name**: enter **NameID**,
- **Incoming claim type**: select **Name**,
- **Outgoing claim type**: select **Name ID**,
- **Outgoing name ID format**: select **Common Name**



Configure Rule

Steps
- Choose Rule Type
- Configure Claim Rule

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

Claim rule name: NameID

Rule template: Transform an Incoming Claim

Incoming claim type: Name

Incoming name ID format: Unspecified

Outgoing claim type: Name ID

Outgoing name ID format: Common Name

● Pass through all claim values

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

Incoming claim value:

Outgoing claim value:

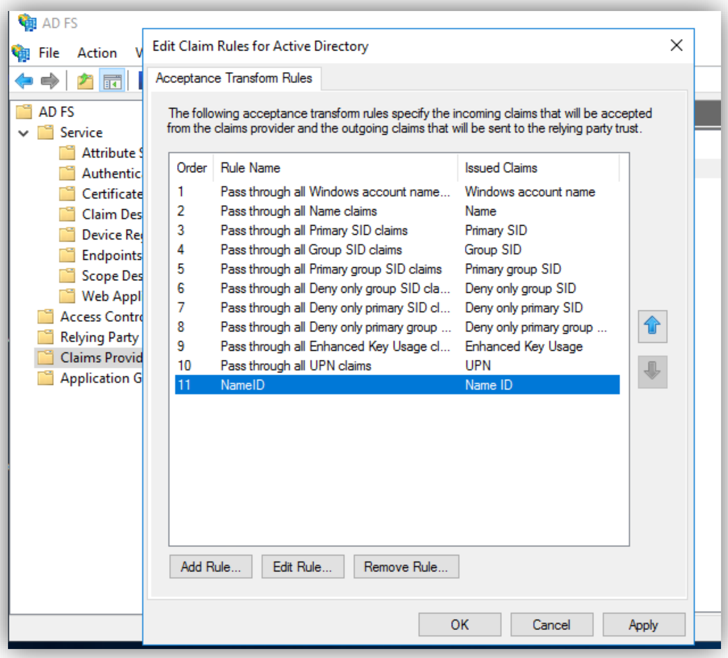
○ Replace incoming e-mail suffix claims with a new e-mail suffix

New e-mail suffix:

Example: fabrikam.com

Then click [**Finish**].

**Step 8**: On ‘Edit Claim Rules for Active Directory’ screen, click [**Apply**].



Edit Claim Rules for Active Directory

Acceptance Transform Rules

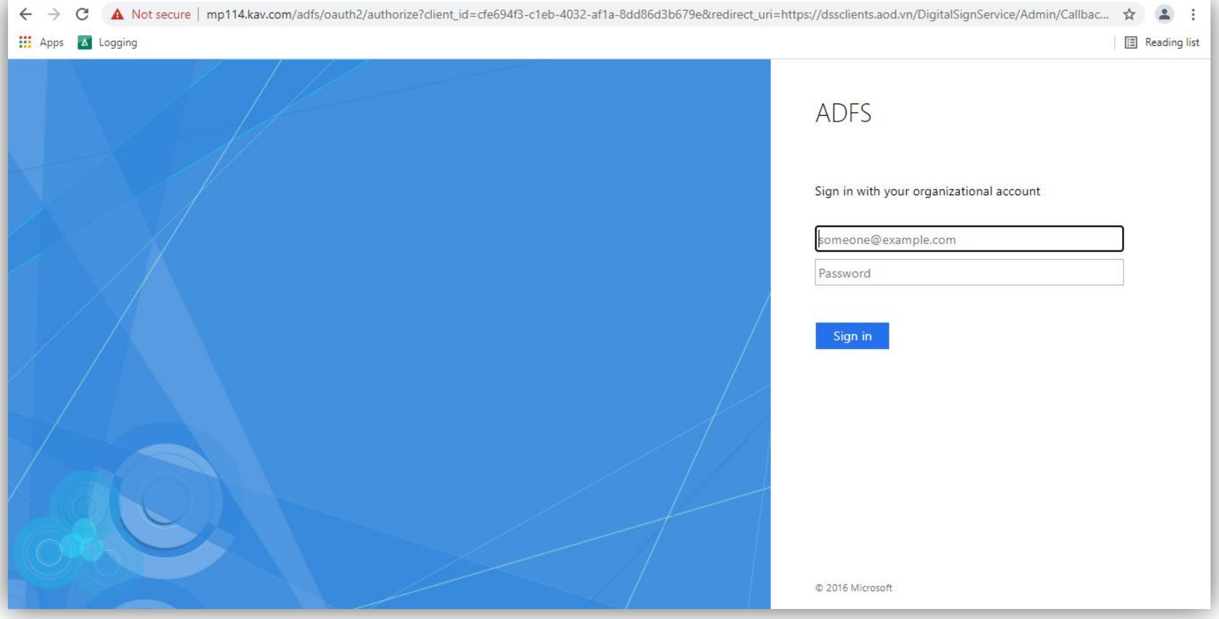
The following acceptance transform rules specify the incoming claims that will be accepted from the claims provider and the outgoing claims that will be sent to the relying party trust.

| Order | Rule Name | Issued Claims |
|---|---|---|
| 1 | Pass through all Windows account name... | Windows account name |
| 2 | Pass through all Name claims | Name |
| 3 | Pass through all Primary SID claims | Primary SID |
| 4 | Pass through all Group SID claims | Group SID |
| 5 | Pass through all Primary group SID claims | Primary group SID |
| 6 | Pass through all Deny only group SID cla... | Deny only group SID |
| 7 | Pass through all Deny only primary SID cl... | Deny only primary SID |
| 8 | Pass through all Deny only primary group ... | Deny only primary group ... |
| 9 | Pass through all Enhanced Key Usage cl... | Enhanced Key Usage |
| 10 | Pass through all UPN claims | UPN |
| 11 | NameID | Name ID |

**Step 9**: Check if the configuration is done correctly by running the hyperlink below on the browser:

```
https://mp114.kav.com/adfs/oauth2/authorize?client_id=[client_id of the activated application]
```

I.e.: https://mp114.kav.com/adfs/oauth2/authorize?client_id=fa7249a7-0ad3-4811-a642-b3648100cce0&redirect_uri=https://dssclients.aod.vn/DigitalSignService/Admin/Callback&scope=openid&response_mode=fragment&state=12345&response_type=code



Not secure | mp114.kav.com/adfs/oauth2/authorize?client_id=cfe694f3-c1eb-4032-af1a-8dd86d3b679e&redirect_uri=https://dssclients.aod.vn/DigitalSignService/Admin/Callbac...

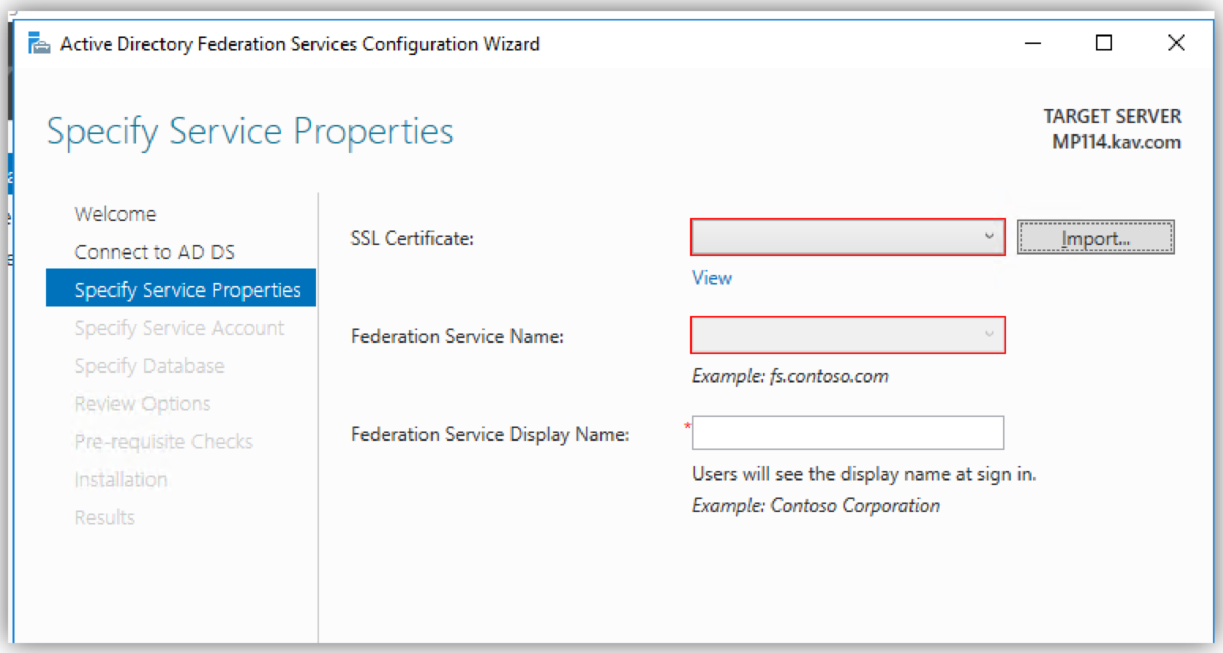
ADFS

Sign in with your organizational account

# Appendix

## Appendix A. Create SSL certificate for Post-deployment Configuration

In some cases, you may not have SSL certificate for Step 4 of Post-deployment Configuration, i.e.:



Active Directory Federation Services Configuration Wizard

Specify Service Properties

TARGET SERVER
MP114.kav.com

SSL Certificate:

Federation Service Name:
Example: fs.contoso.com

Federation Service Display Name: *
Users will see the display name at sign in.
Example: Contoso Corporation

In that case, open file **Readme.txt** in the folder **openssl-1.0.2l-x64_86-win64**, then follow the steps described in this text file to create a **.pfx** file.

You can then import SSL Certificate using the created **.pfx** file.