



Mi-Token

Configuring ADFS for Office 365: a Step-By- Step Guide



© 2019 Mi-Token Inc.

All rights reserved. No parts of this work may be reproduced in any form or by any means – graphic, electronic, or mechanical, including photocopying, recording, taping, or information storage and retrieval systems – without the written permission of the publisher.

Products that are referred to in this document may be either trademarks and/or registered trademarks of the respective owners. The publisher and the author make no claim to these trademarks.

While every precaution has been taken in the preparation of this document, the publisher and the author assume no responsibility for errors or omissions, or for damages resulting from the use of information contained in this document or from the use of programs and source code that may accompany it. In no event shall the publisher and the author be liable for any loss of profit or any other commercial damage caused or alleged to have been caused directly or indirectly by this document.

Mi-Token version 1.0.0. Document version 1, January 2019.

Published: June 2019 in Austin, Texas, United States of America.

Configuring ADFS for Office 365: a Step-By-Step Guide

Adding the ADFS role

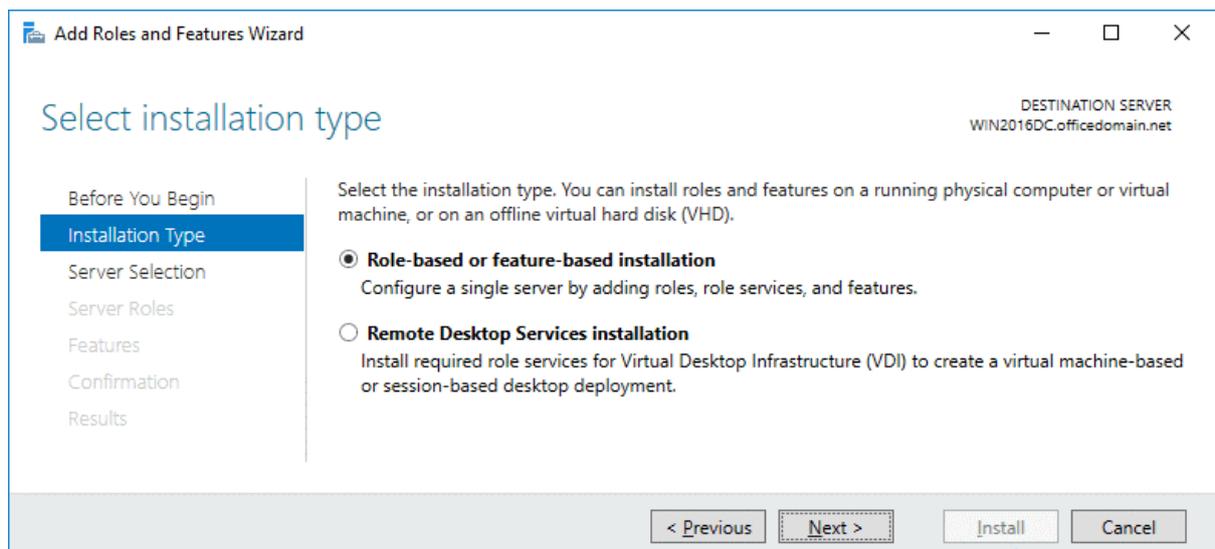
To install the ADFS role on your Windows Server machine. In this document, this role is installed on the domain controller running Windows Server 2016 by using the graphical user interface (GUI) and the workflow is demonstrated with a large number of screenshots.

However, it is possible to use PowerShell as an alternative if you like the command line interface.

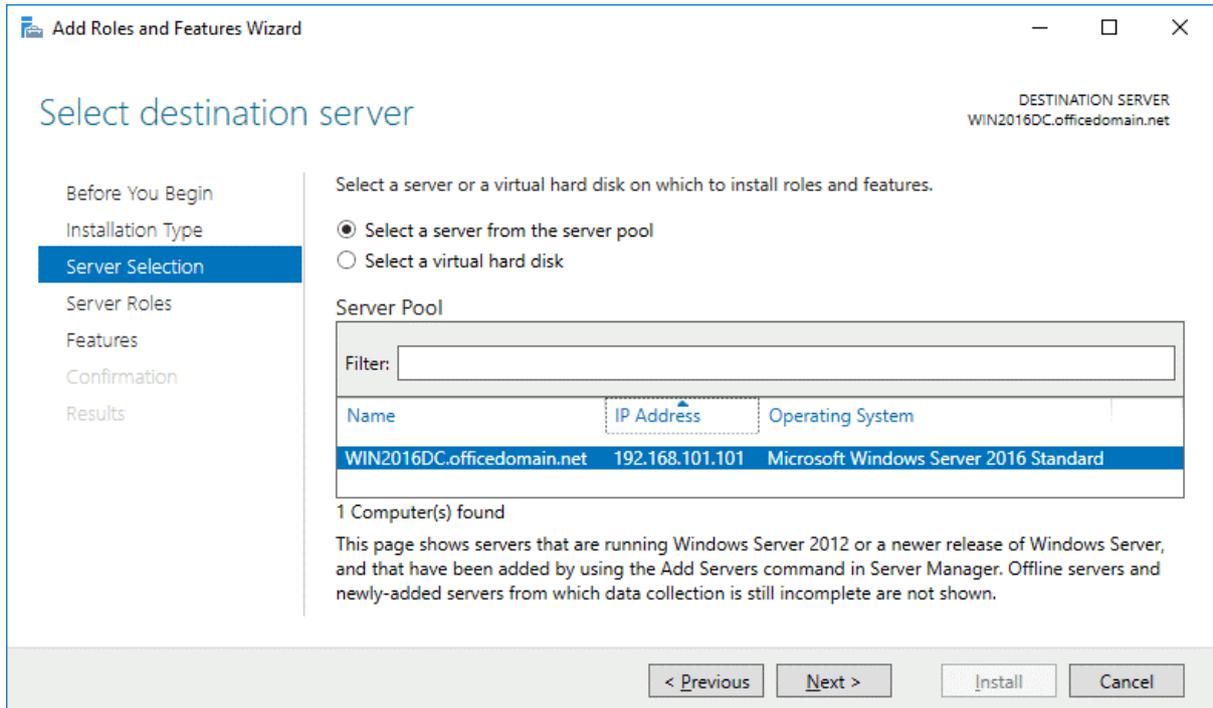
In Server Manager (a window that is opened by default when Windows Server 2016 boots), click Add roles and features. The Add Roles and Features Wizard window opens in which you have to configure a few steps.

Before You Begin. This is an introductory step which you can skip.

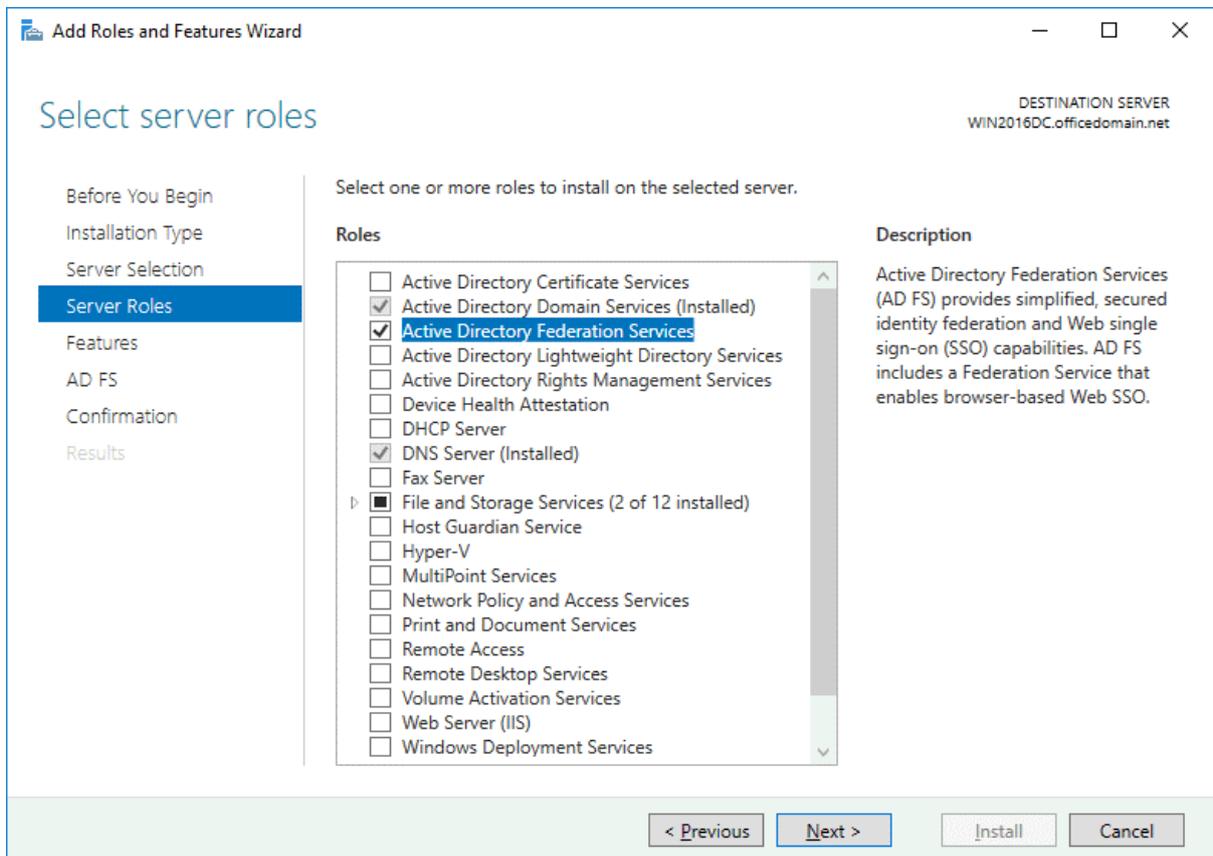
Installation Type. Select Role-based or feature-based installation. Hit Next for each step of the wizard to continue.



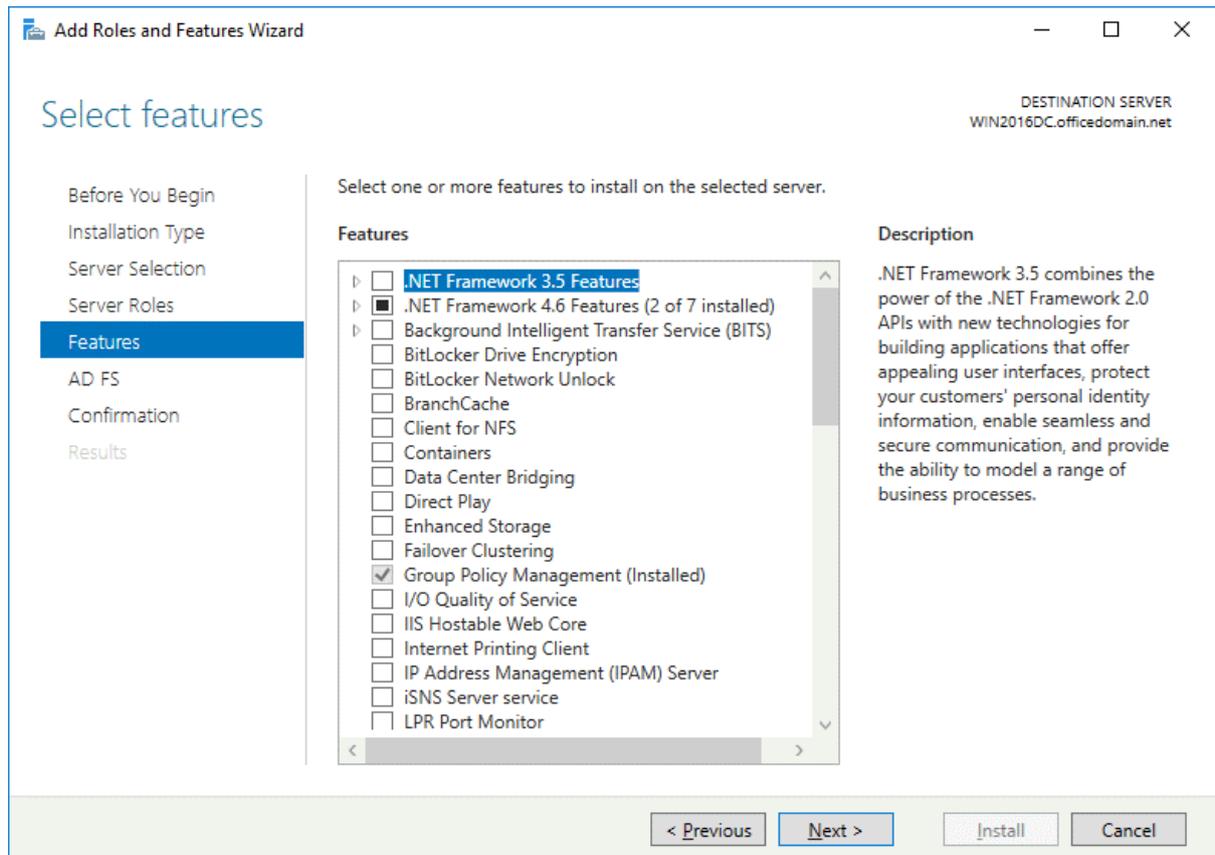
Server Selection. Select a server from the server pool: *WIN2016DC.officedomain.net* (is selected by default in our case because we have only one server).



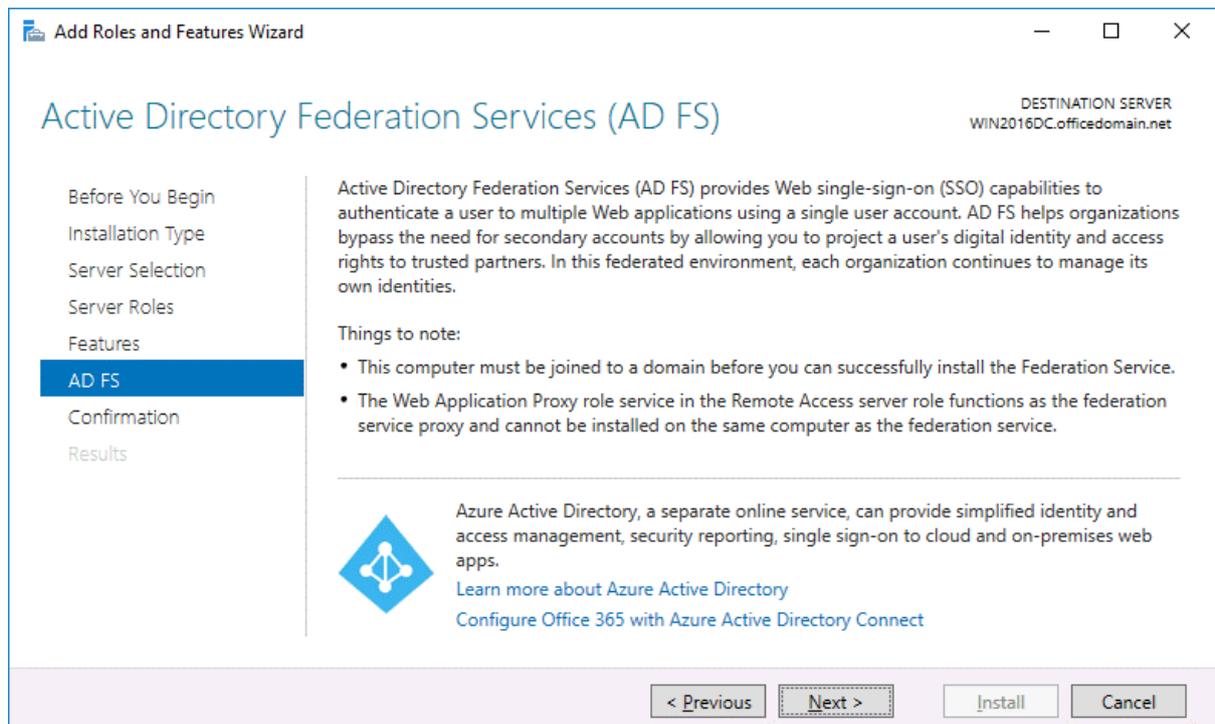
Server Roles. Select the checkbox next to *Active Directory Federation Services*.



Features. The features needed for installing Active Directory Federation Services such as .NET Framework are selected.



AD FS. Just click *Next* at this step after reading the description of Active Directory Federation Services.



Confirmation. You can select the checkbox to restart the destination server automatically if required and hit **Yes** to confirm. Finally click **Install** to set up ADFS for Office 365.

DESTINATION SERVER
WIN2016DC.officedomain.net

Before You Begin
Installation Type
Server Selection
Server Roles
Features
AD FS
Confirmation
Results

To install the following roles, role services, or features on selected server, click Install.

Restart the destination server automatically if required

Optional features (such as administration tools) might be displayed on this page because they have been selected automatically. If you do not want to install these optional features, click Previous to clear their check boxes.

Active Directory Federation Services

Add Roles and Features Wizard

If a restart is required, this server restarts automatically, without additional notifications. Do you want to allow automatic restarts?

Yes No

Export configuration settings
Specify an alternate source path

< Previous Next > Install Cancel

Results. Wait until the installation process of ADFS 2016 has finished.

DESTINATION SERVER
WIN2016DC.officedomain.net

Before You Begin
Installation Type
Server Selection
Server Roles
Features
AD FS
Confirmation
Results

View installation progress

Feature installation

Installation started on WIN2016DC.officedomain.net

Active Directory Federation Services

You can close this wizard without interrupting running tasks. View task progress or open this page again by clicking Notifications in the command bar, and then Task Details.

Export configuration settings

< Previous Next > Close Cancel

After finishing ADFS installation, the server must reboot.

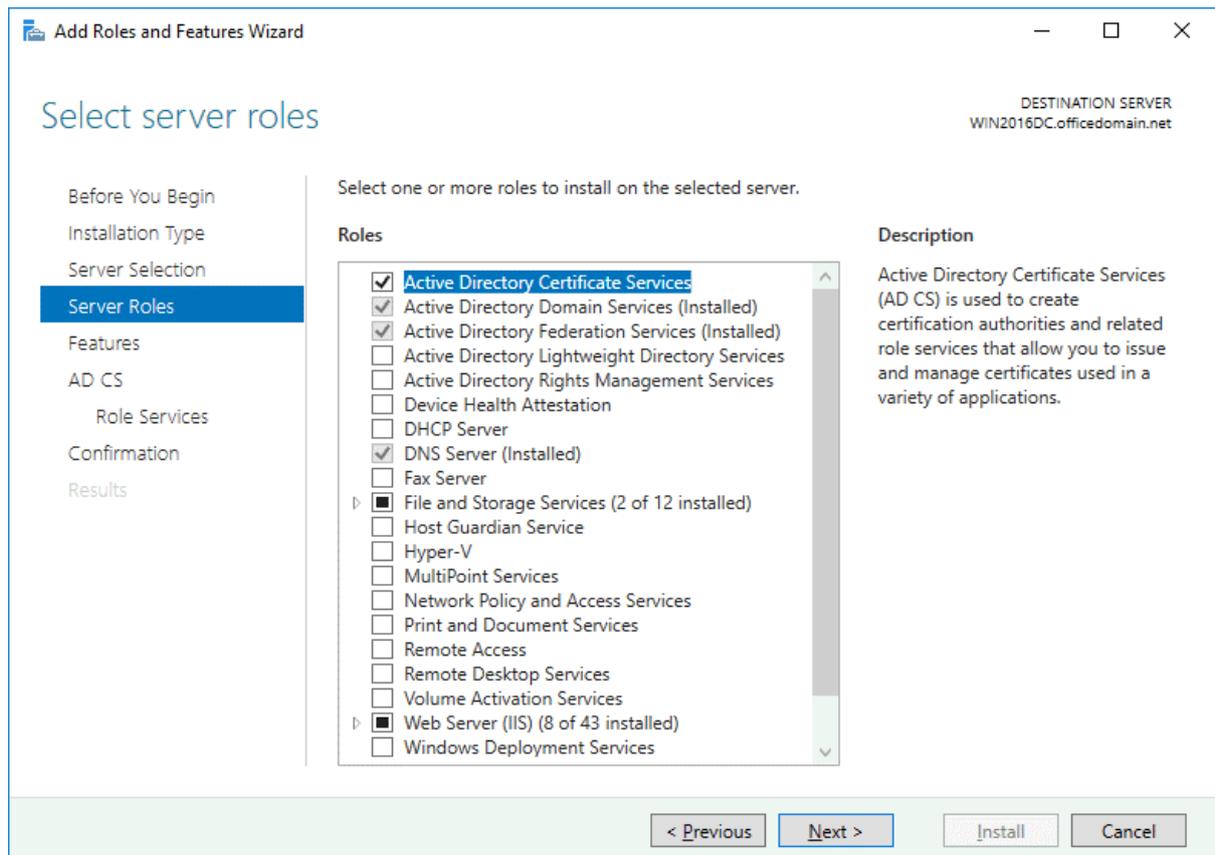
Installing ADCS to create a certificate

Before you can continue to set up ADFS for Office 365, you should create a certificate. Active Directory Certificate Services must be installed for this purpose. In Server Manager click **Add roles and features**. As described in the previous section, the *Add Roles and Features Wizard* opens.

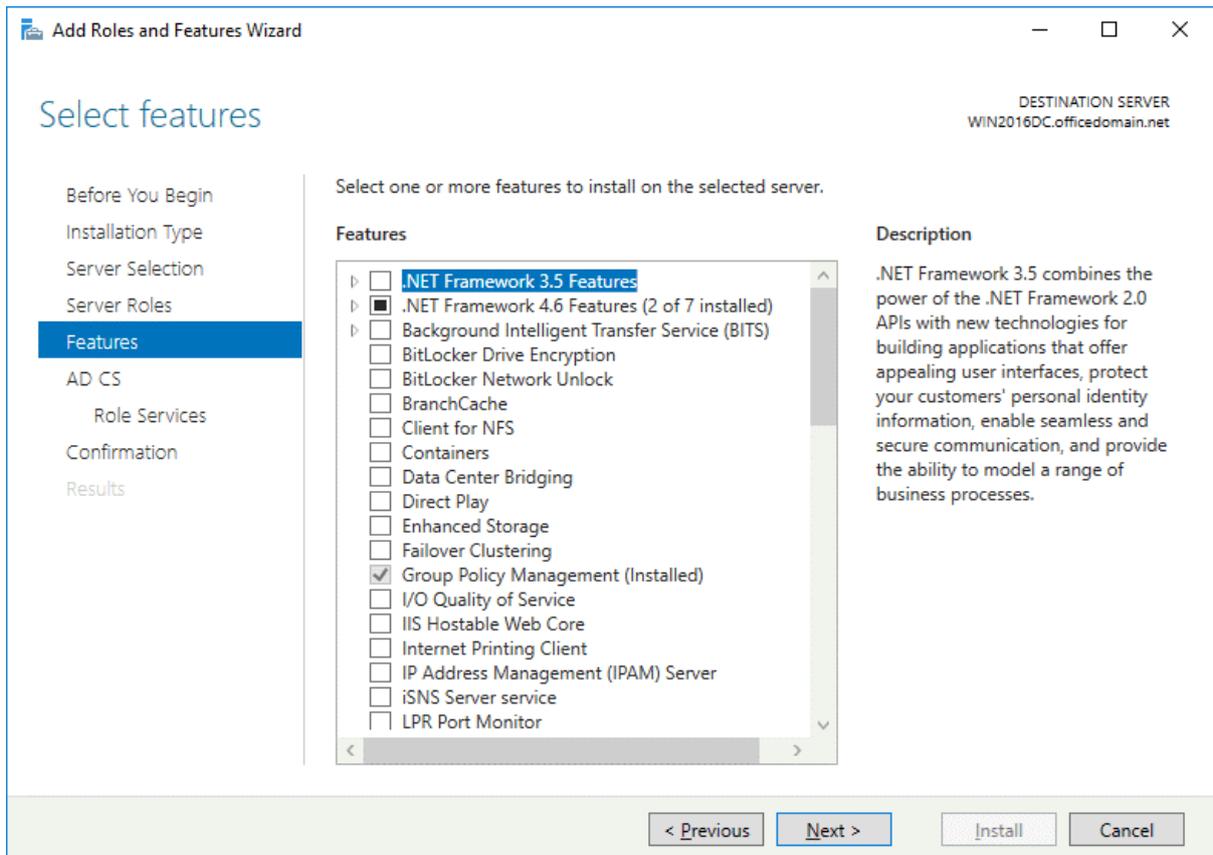
Installation Type. Select *Role-based or feature-based installation*. Hit **Next** for each step of the wizard to continue (as you have done before when installing ADFS).

Server Selection. Select a server from the server pool: *WIN2016DC.officedomain.net* (as described for installing ADFS).

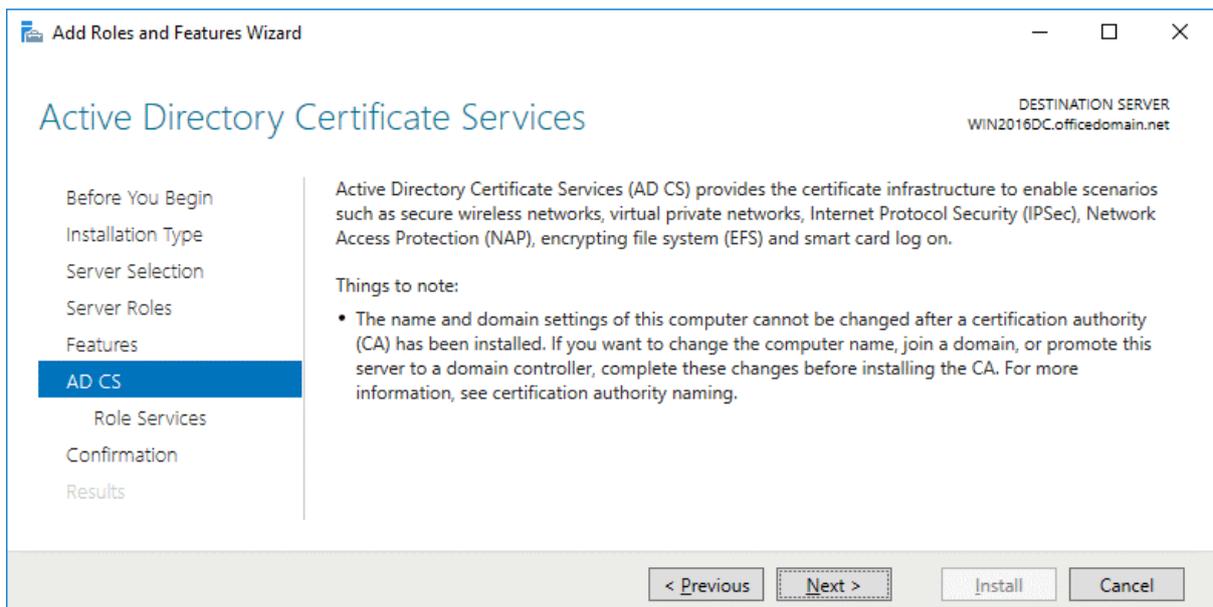
Server Roles. Select the checkbox next to *Active Directory Certificate Services*. Related roles and features such as IIS (Internet Information Services) are selected automatically.



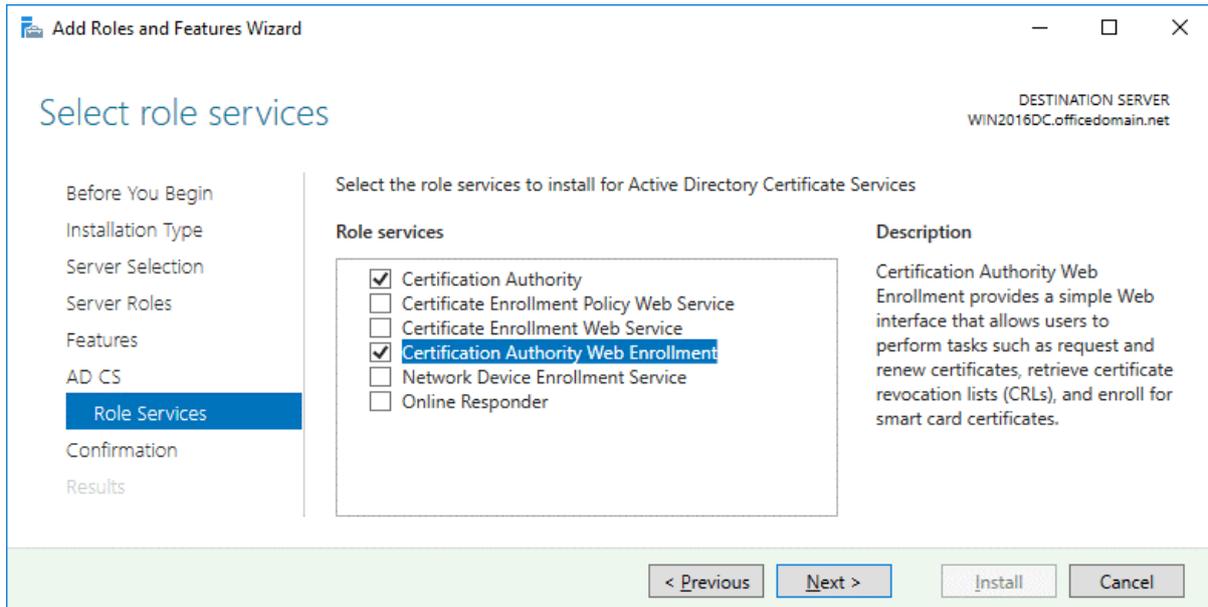
Features. At this step *.NET Framework features* must be selected (they are selected by default as the related features).



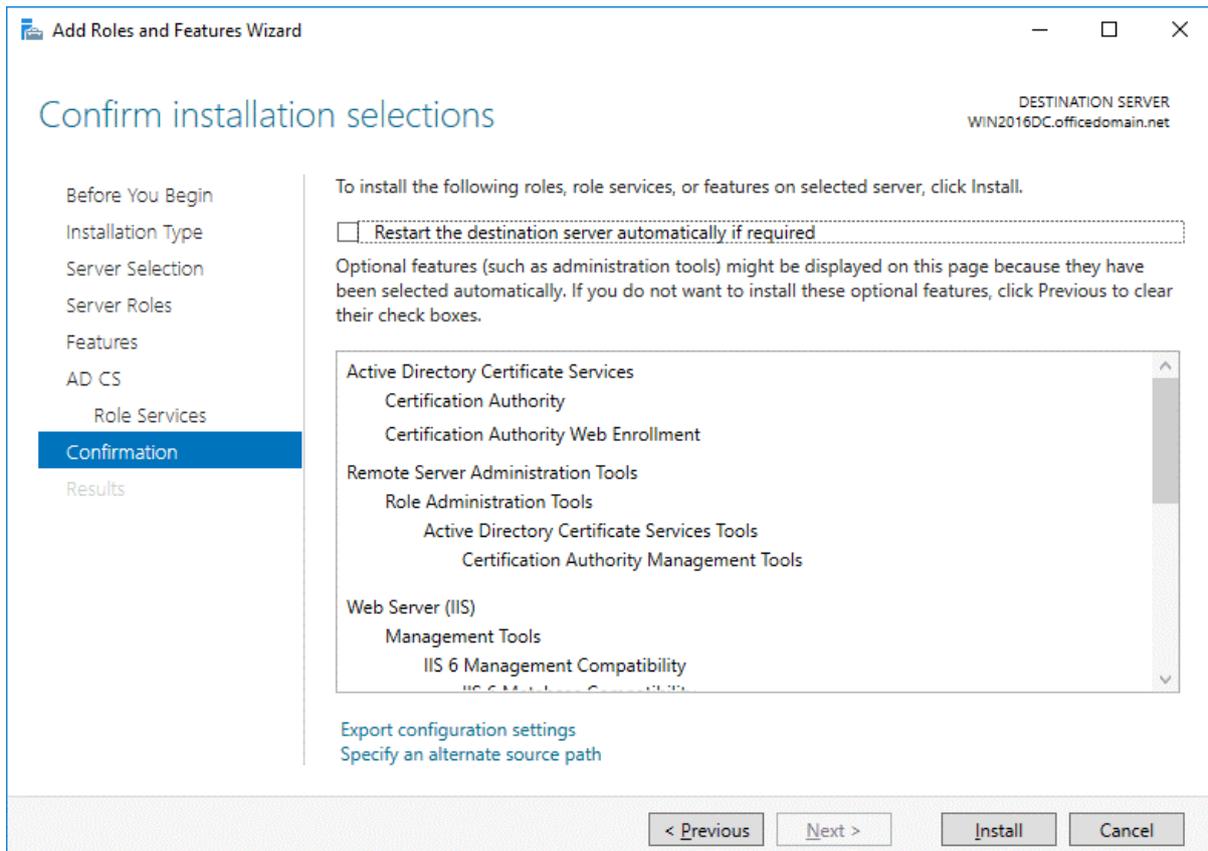
AD CS. There is nothing to configure in this step. You can read the description of Active Directory Certificate Services and continue.



Role Services. Select the checkboxes next to **Certificate Authority** and **Certificate Authority Web Enrollment** services.



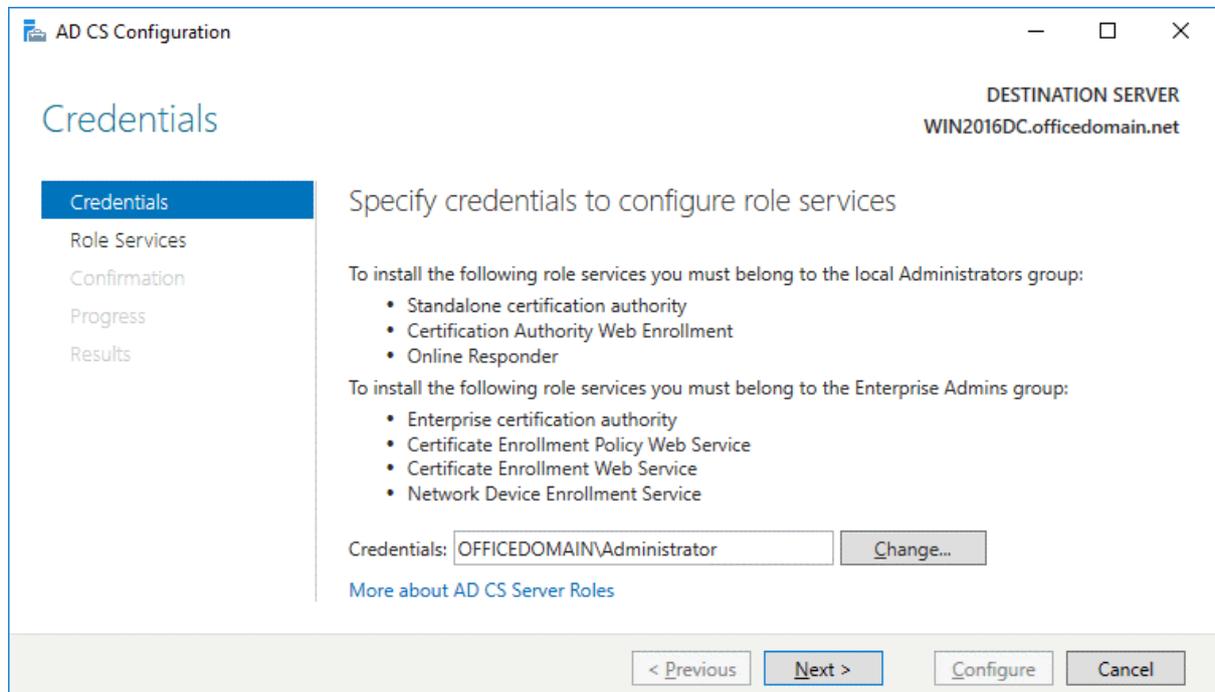
Confirmation. Check your configuration, select the checkbox to restart the destination server automatically if required and hit **Install** to start the installation process.



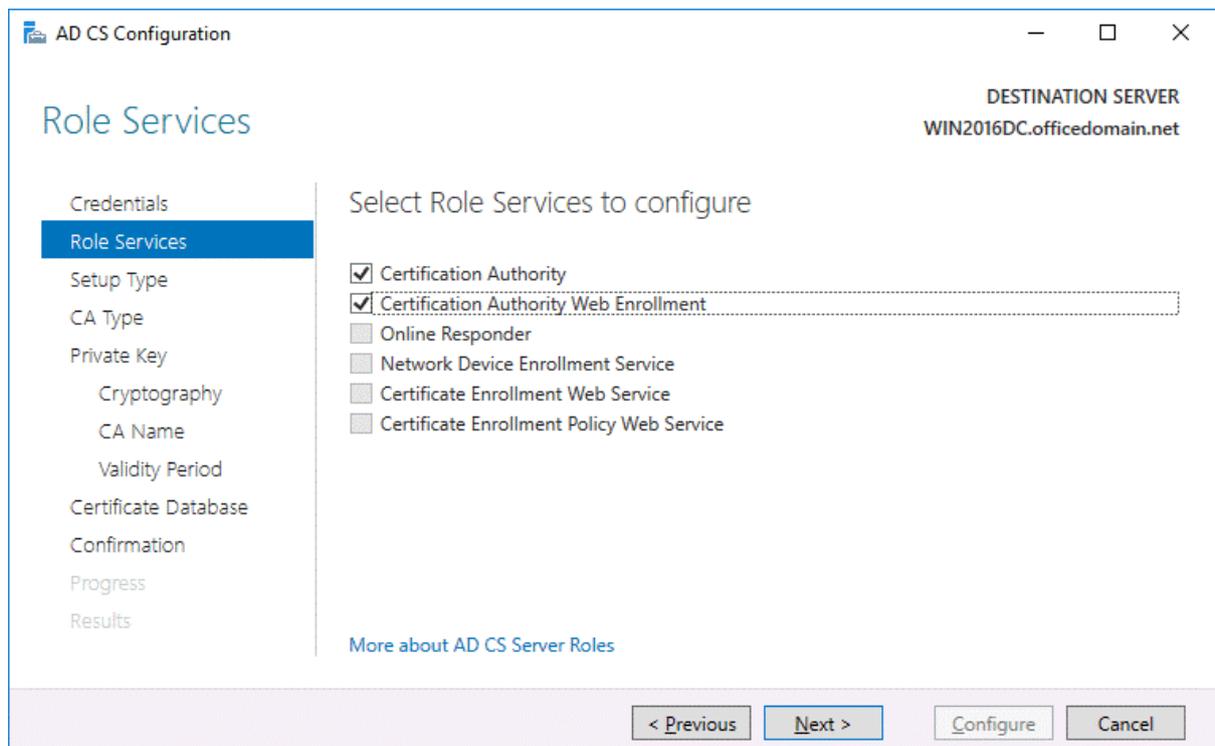
ADCS configuration

Now you should perform the post-deployment configuration of Active Directory Certificate Services before you can continue configuring ADFS for Office 365. In Server Manager, click the yellow triangle near the flag icon. In the menu that opens, click **Configure Active Directory Certificates** on this machine.

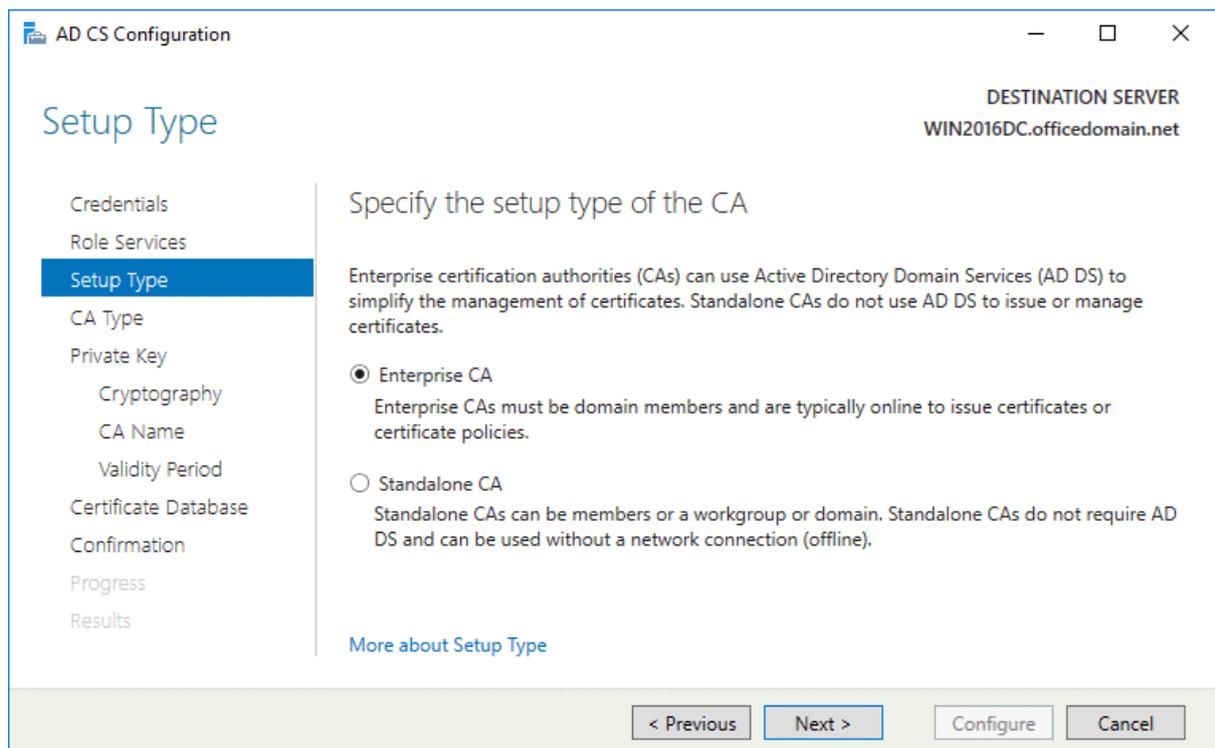
Credentials. Specify credentials to configure role services. In our case, *OFFICEDOMAIN\Administrator* is the account used to install the selected role services. Hit **Next** for each step of the wizard to continue.



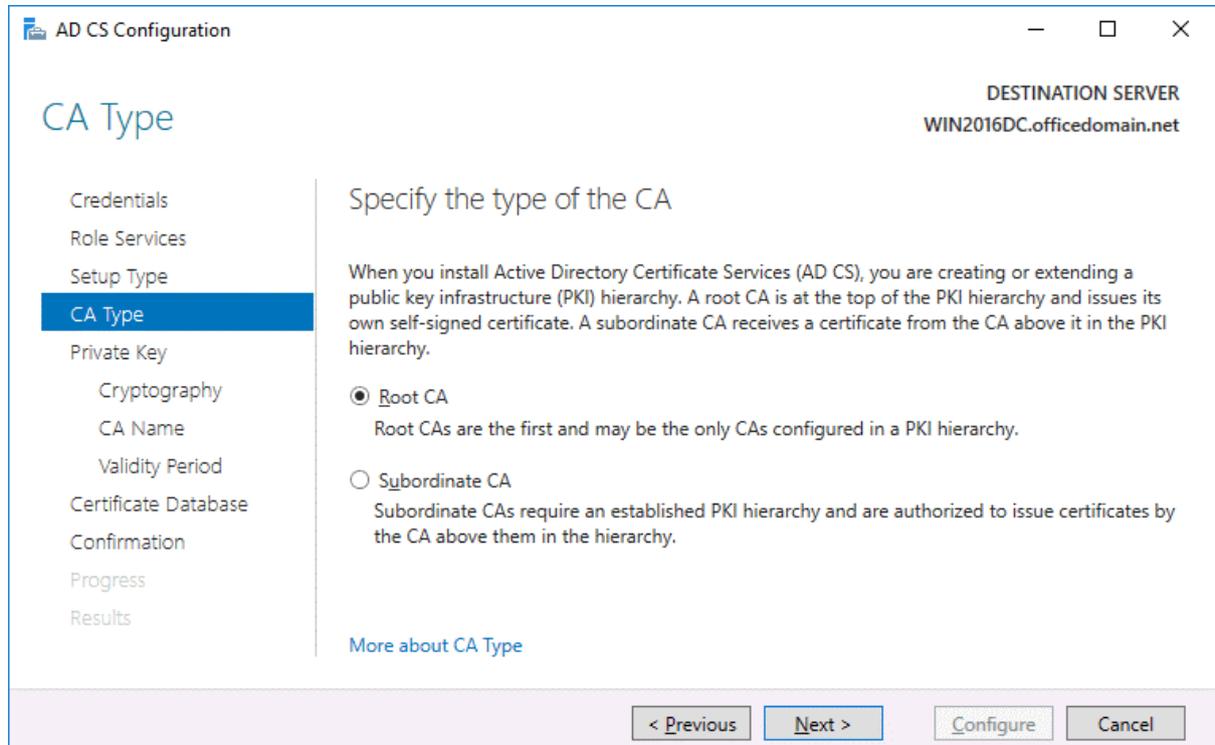
Role Services. To choose *Certification Authority* and *Certification Authority Web Enrollment*, select the appropriate checkboxes.



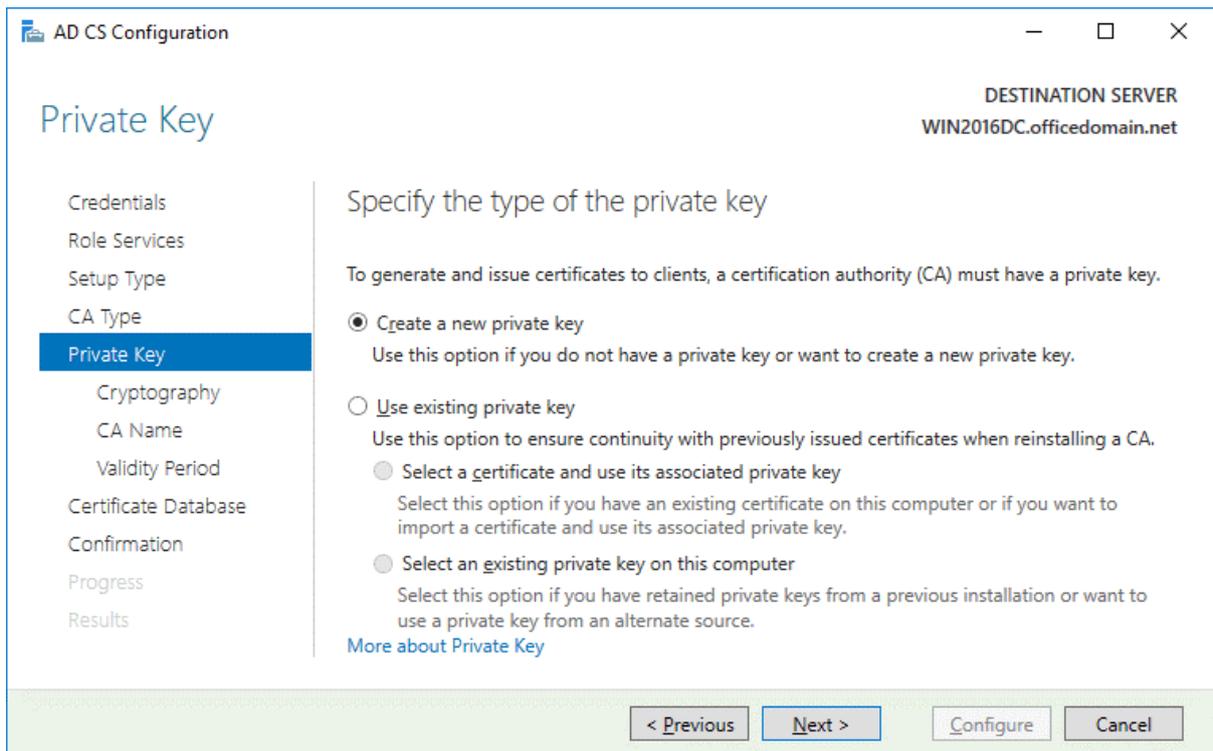
Setup Type. Select **Enterprise CA** because Active Directory Domain Services are used in this case.



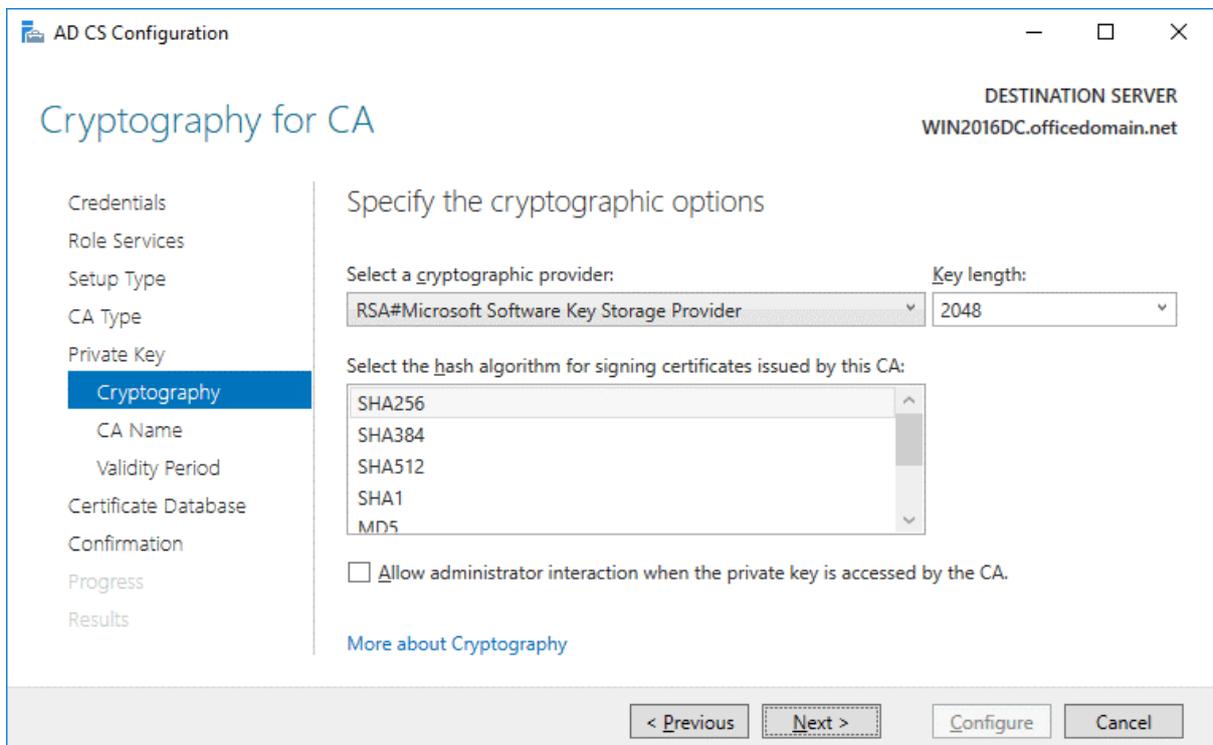
CA Type. Specify the type of the CA. Select **Root CA** that is the first in a public key infrastructure (PKI) hierarchy.



Private Key. To specify the type of the private key, select Create a new private key.



Cryptography. Specify the cryptographic options for CA. In this example, *RSA#Microsoft Software Key Storage Provider* is selected with a key length of 2048. *SHA256* is selected as the hash algorithm.



CA Name. Specify the name of the CA. The following parameters are used in this example.

Common name for this CA: *officedomain-WIN2016DC-CA*

Distinguished name suffix: *DC=officedomain,DC=net*

Preview of distinguished name: *CN=officedomain-WIN2016DC-CA,DC=officedomain,DC=net*

The screenshot shows the 'AD CS Configuration' wizard window. The title bar includes the application name and standard window controls. The main area is titled 'CA Name' and shows a list of steps on the left: Credentials, Role Services, Setup Type, CA Type, Private Key, Cryptography, CA Name (highlighted), Validity Period, Certificate Database, Confirmation, Progress, and Results. The main content area is titled 'Specify the name of the CA' and contains the following text: 'Type a common name to identify this certification authority (CA). This name is added to all certificates issued by the CA. Distinguished name suffix values are automatically generated but can be modified.' Below this text are three input fields: 'Common name for this CA:' with the value 'officedomain-WIN2016DC-CA', 'Distinguished name suffix:' with the value 'DC=officedomain,DC=net', and 'Preview of distinguished name:' with the value 'CN=officedomain-WIN2016DC-CA,DC=officedomain,DC=net'. At the bottom of the window are four buttons: '< Previous', 'Next >', 'Configure', and 'Cancel'.

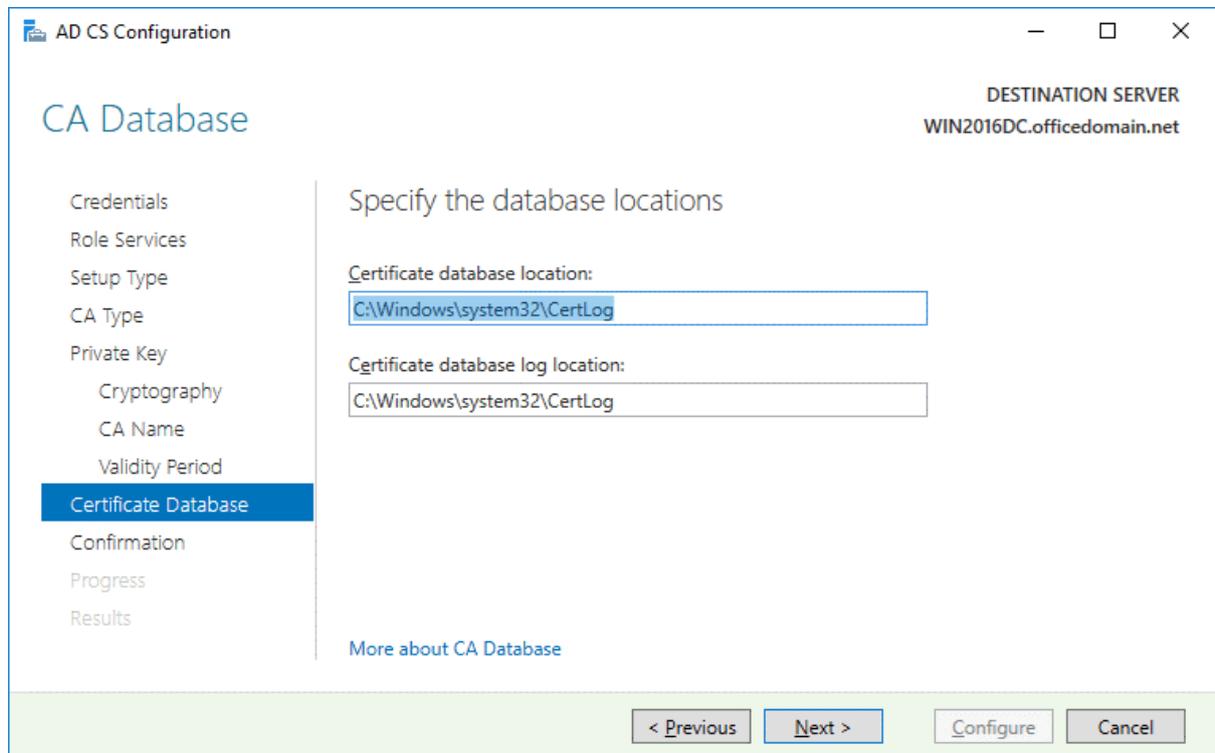
Validity Period. Specify the validity period for the certificate generated for this certification authority (CA), for example, 5 years.

The screenshot shows the 'AD CS Configuration' wizard window at the 'Validity Period' step. The left-hand list of steps is the same as in the previous screenshot, but 'Validity Period' is now highlighted. The main content area is titled 'Specify the validity period' and contains the following text: 'Select the validity period for the certificate generated for this certification authority (CA):'. Below this text is a numeric input field containing '5' and a dropdown menu set to 'Years'. Below the input field, it says 'CA expiration Date: 3/19/2025 6:09:00 AM'. Further down, it states: 'The validity period configured for this CA certificate should exceed the validity period for the certificates it will issue.' At the bottom of the window are four buttons: '< Previous', 'Next >', 'Configure', and 'Cancel'.

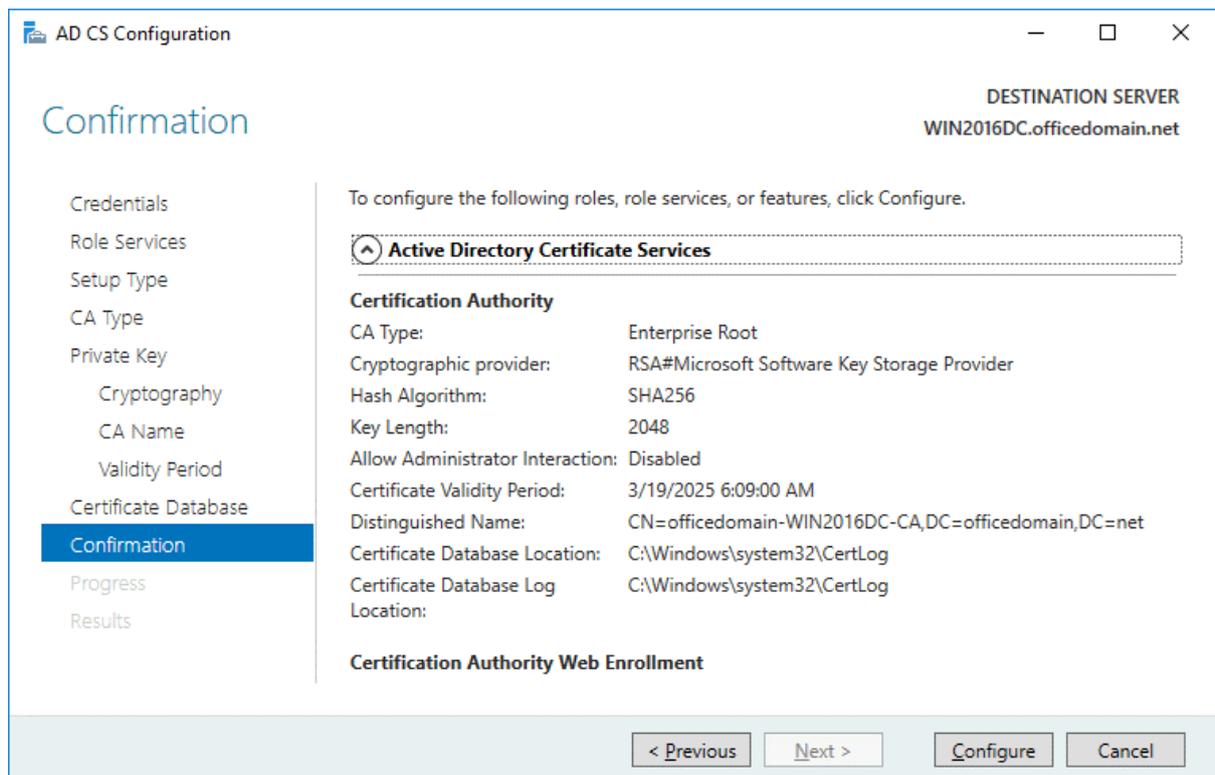
Certificate Database. Specify the database locations. You can keep the default values.

Certificate database location: *C:\Windows\system32\CertLog*

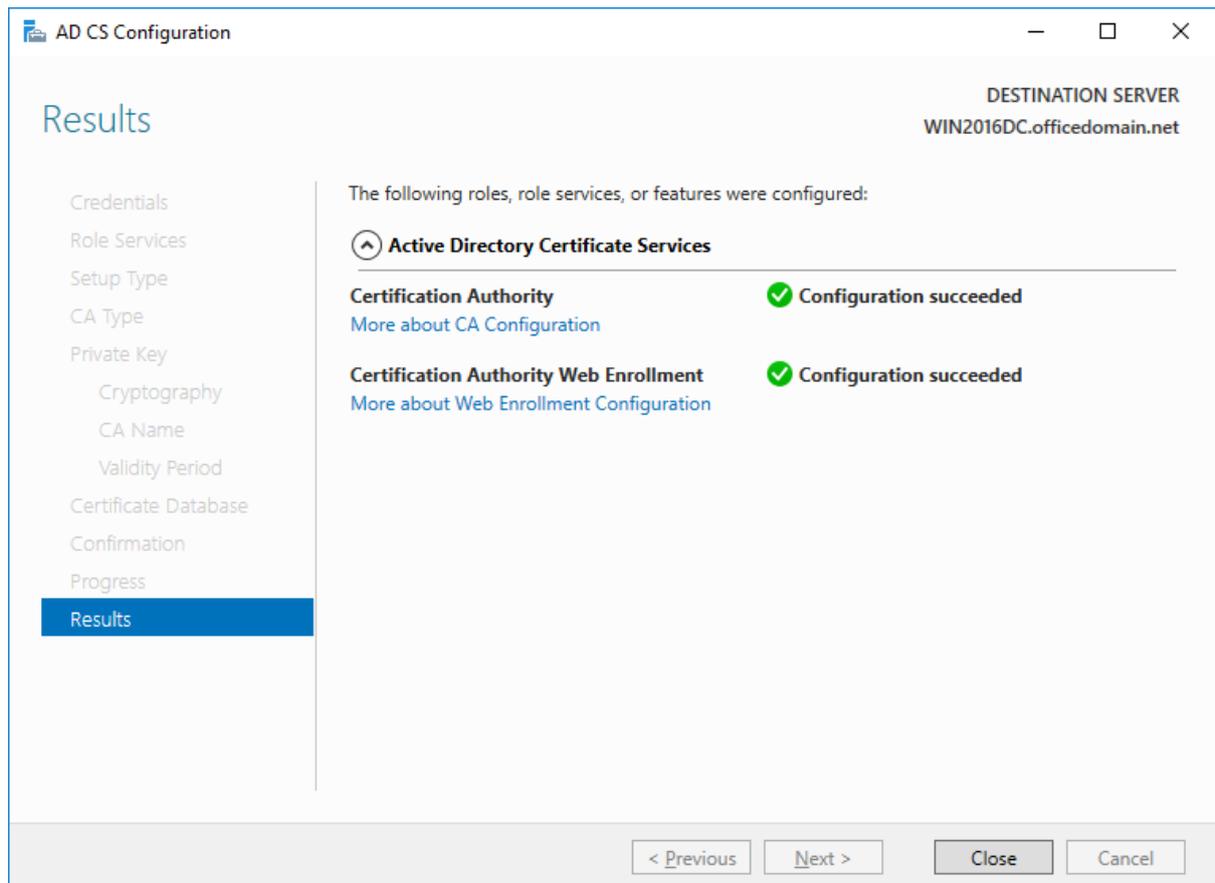
Certificate database log location: *C:\Windows\system32\CertLog*



Confirmation. Check your configuration of Active Directory Certificate Services and if everything is OK, hit **Configure**.

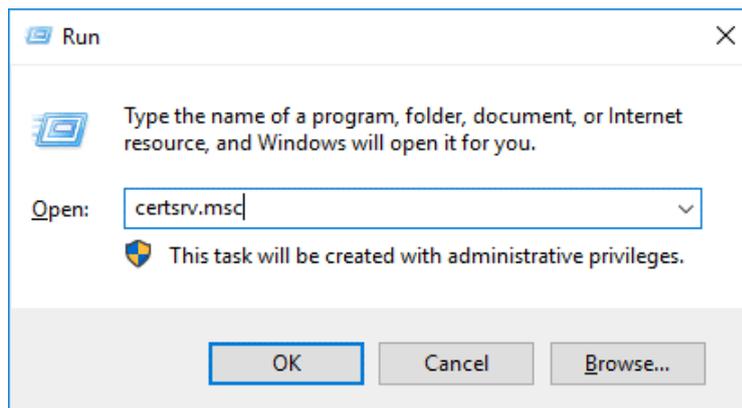


If you see the **Configuration succeeded** message, then everything is correct and you can close the window.

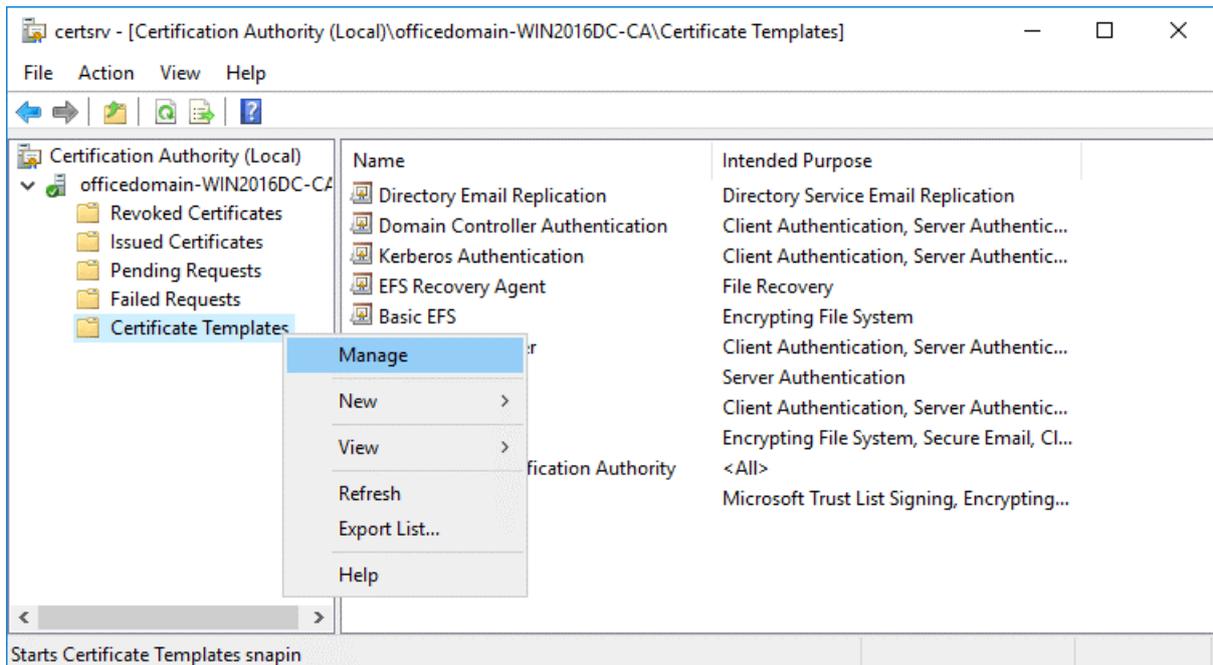


Editing a certificate template

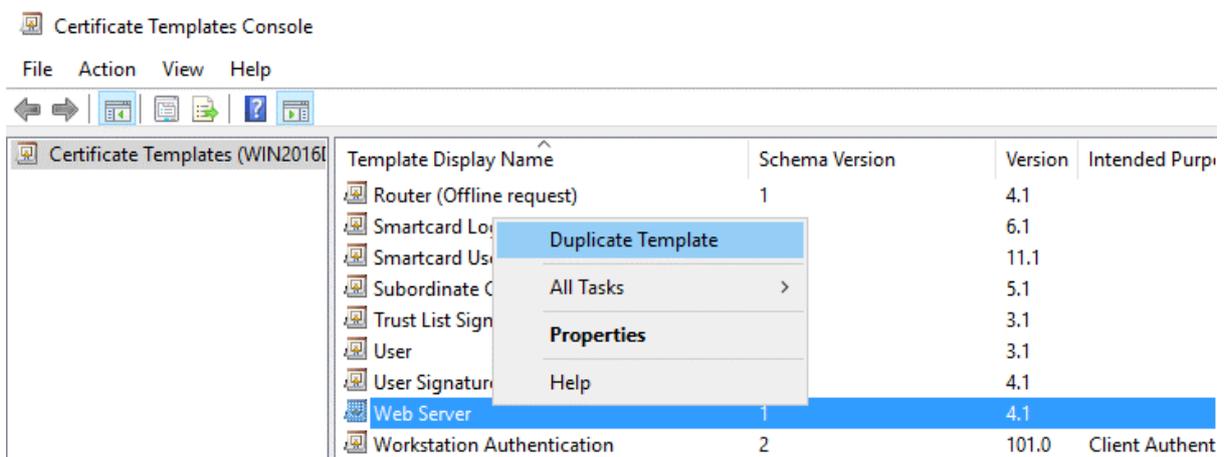
To edit a certificate template, open the Certification Authority configuration window by pressing **Win+R** and running **certsrv.msc**



In the opened window of the Certification Authority, right click **Certificate Templates** and in the context menu click **Manage**.

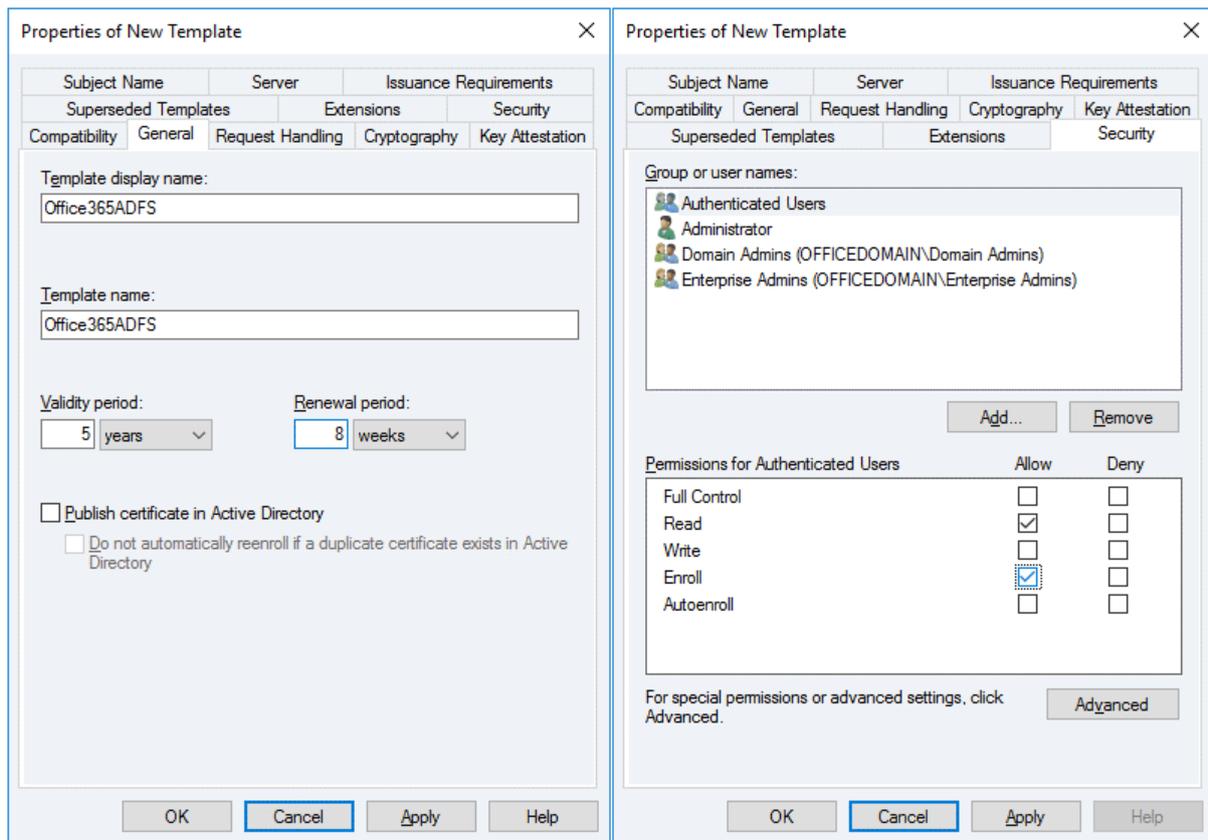


In the opened Certificate Templates Console, right click **Web Server** and in the context menu hit **Duplicate Template**.

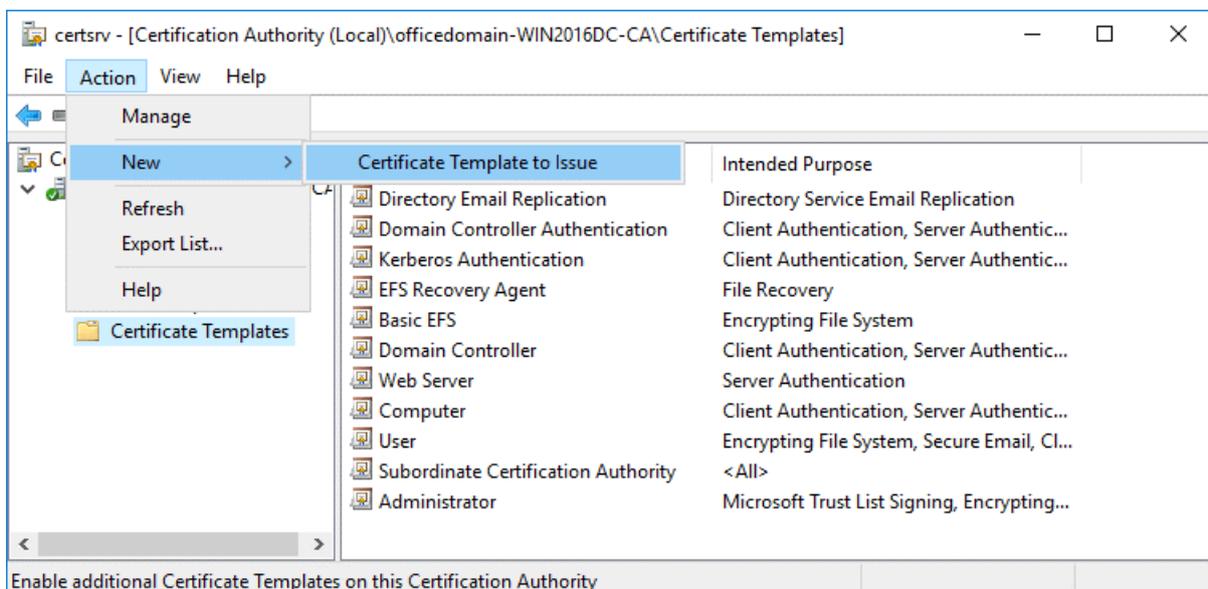


The *Properties of New Template* window opens. In the **General** tab enter the template display name and template name. We are configuring ADFS for Office 365, hence, the template name is *Office365ADFS* in this example. You can also set the validity period for the certificate.

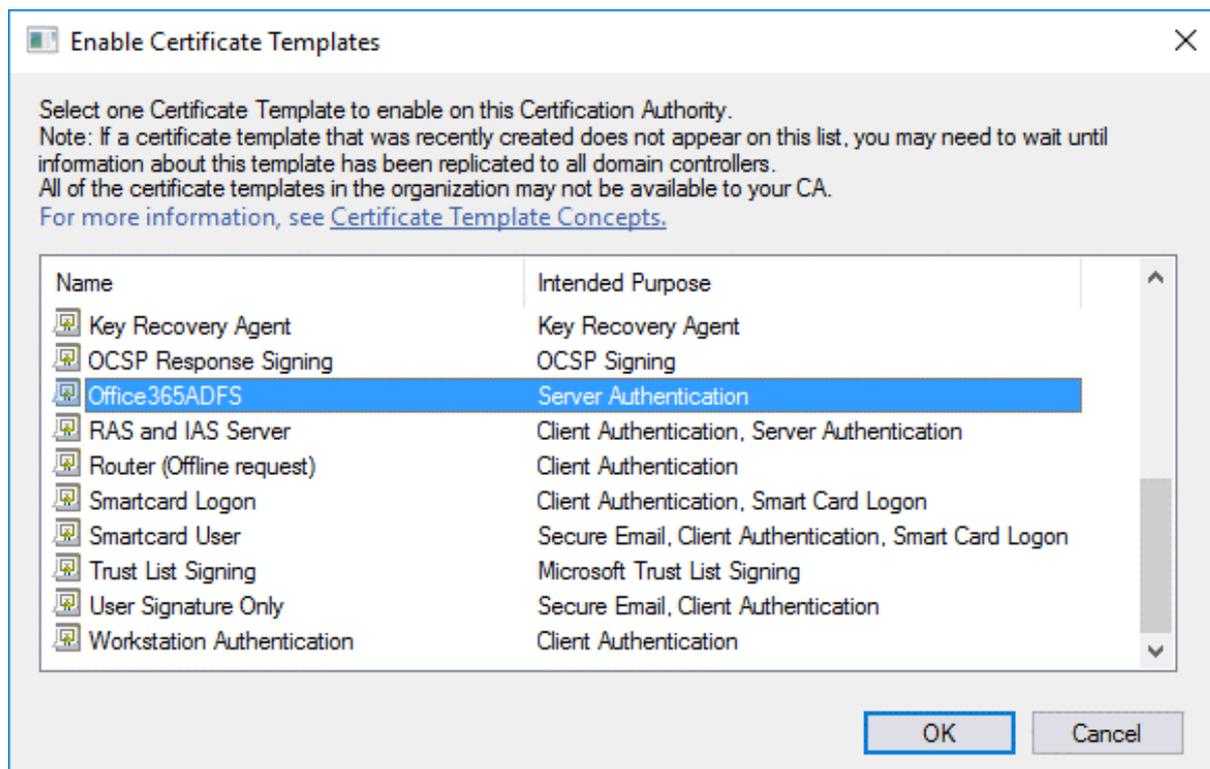
In the *Security* tab select **Authenticated users** and in the permissions for authenticated users select the checkbox to **Allow Enroll** (see the screenshot below).



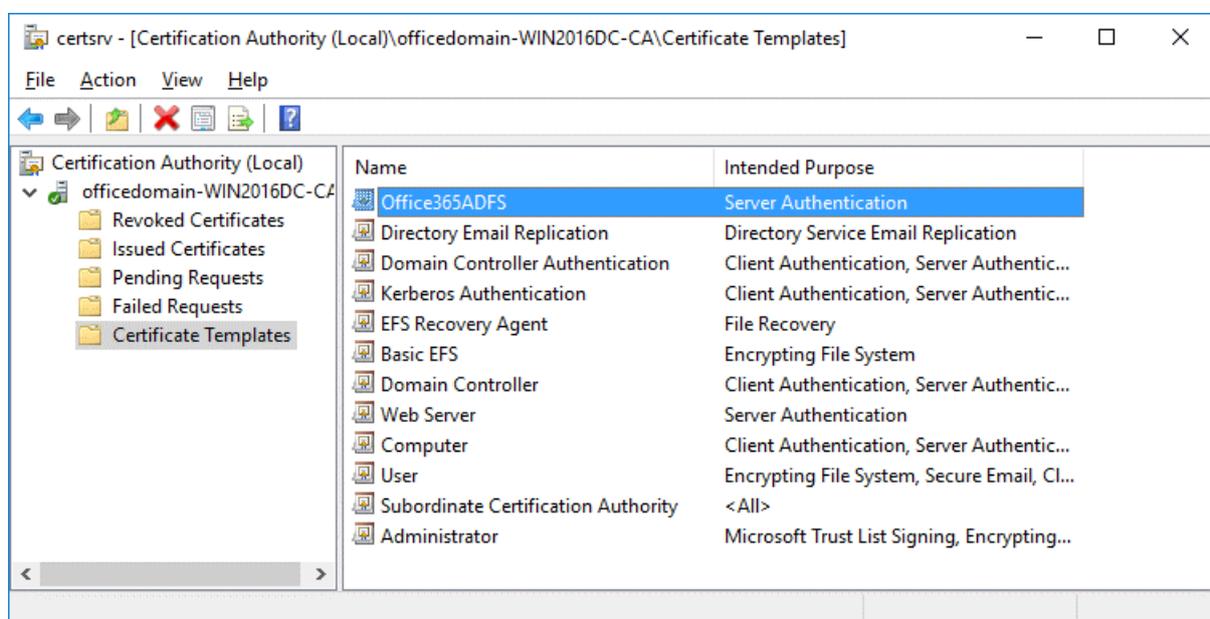
Now in the Certification Authority window (certsrv) click **Action > New > Certificate Template to Issue**.



In the *Enable Certificate Templates* window, select the template you have created earlier (*Office365ADFS* in this case) and hit **OK**.



Now your *Office365ADFS* template is displayed in the list of templates in the *Certificate Templates* directory of the *Certification Authority* list.

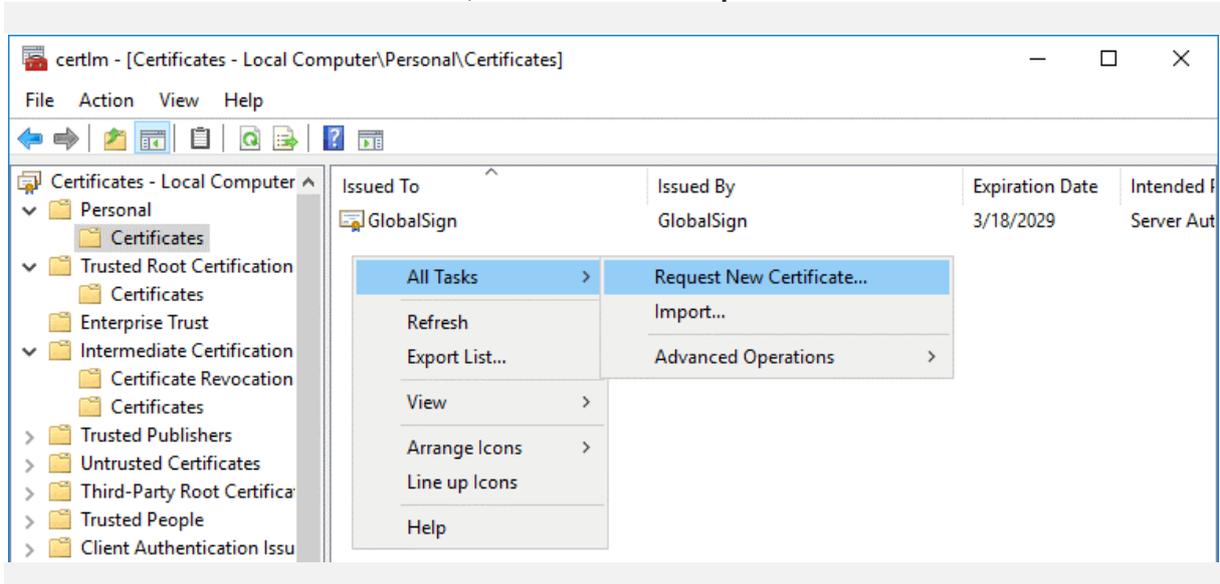


Creating a new certificate

Go to **Start > Run** and open the Certificate Manager with the command:

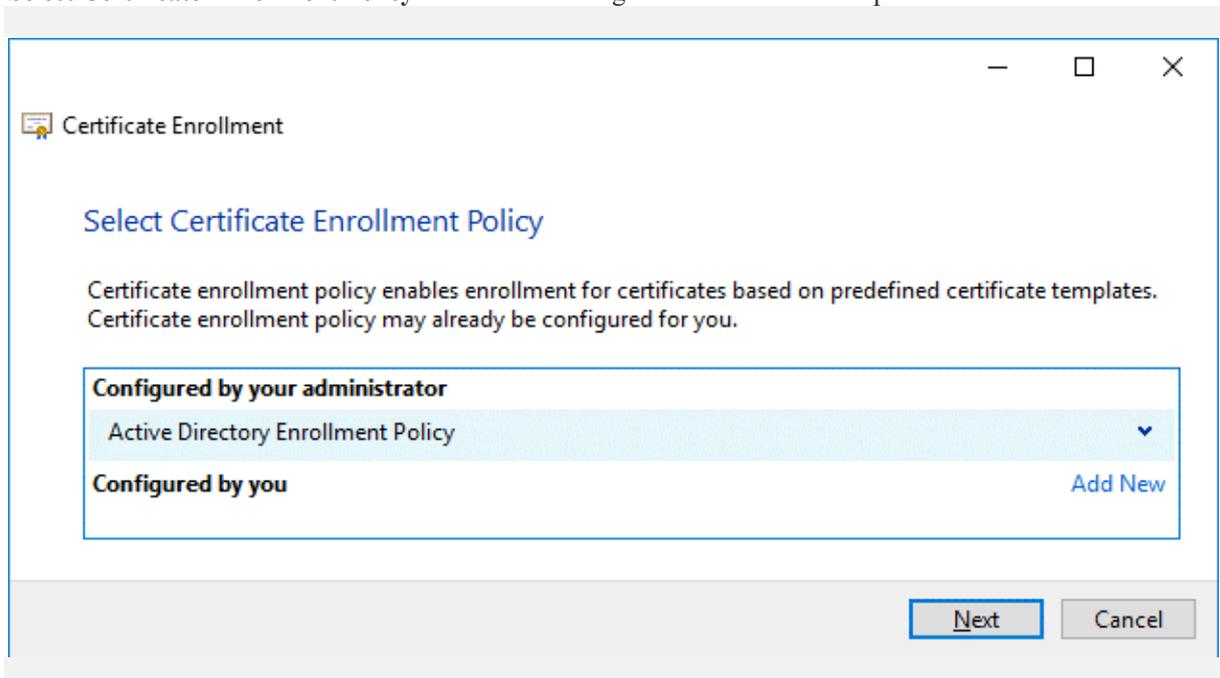
certlm

In the *certlm* window that opens, go to **Personal > Certificates**, then right click in the empty place in the right section of the window. In the context menu, select **All Tasks > Request New Certificate**.

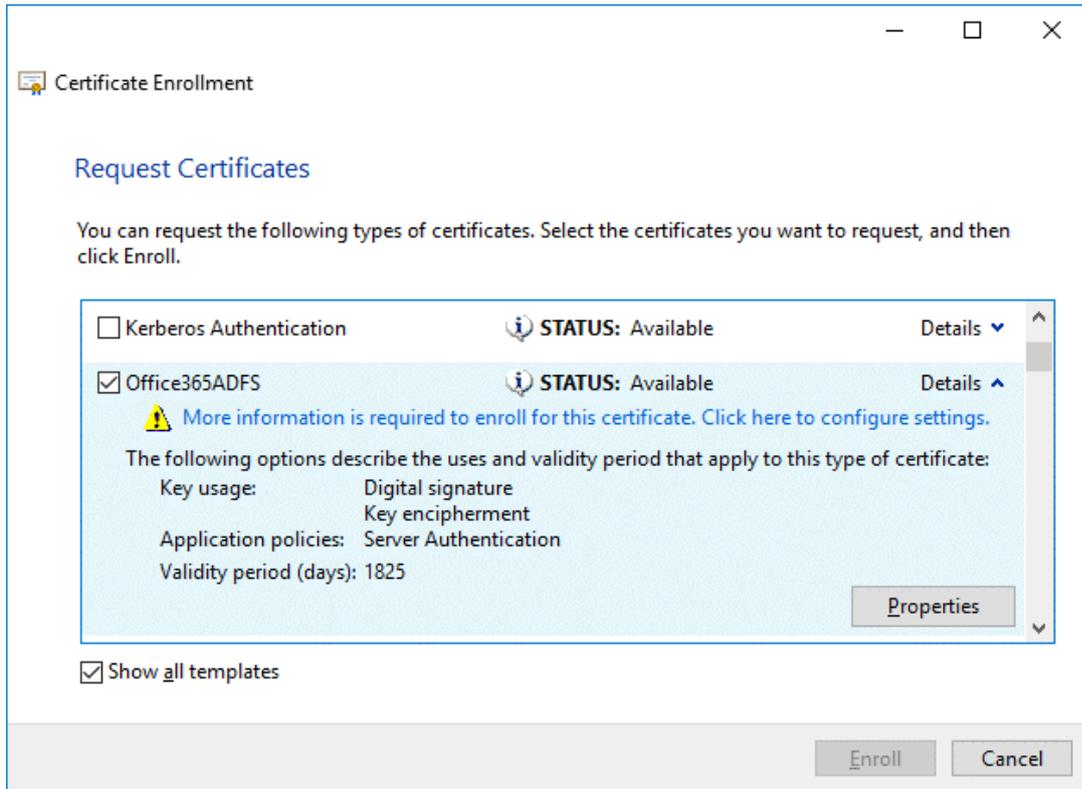


Before You begin. There is nothing to configure in this step. Click **Next** to continue.

Select Certificate Enrollment Policy. The default settings can be used in this step.



Request Certificates. Select your *Office365ADFS* certificate template by selecting the checkbox, click **Details** to expand settings and then click **Properties**.



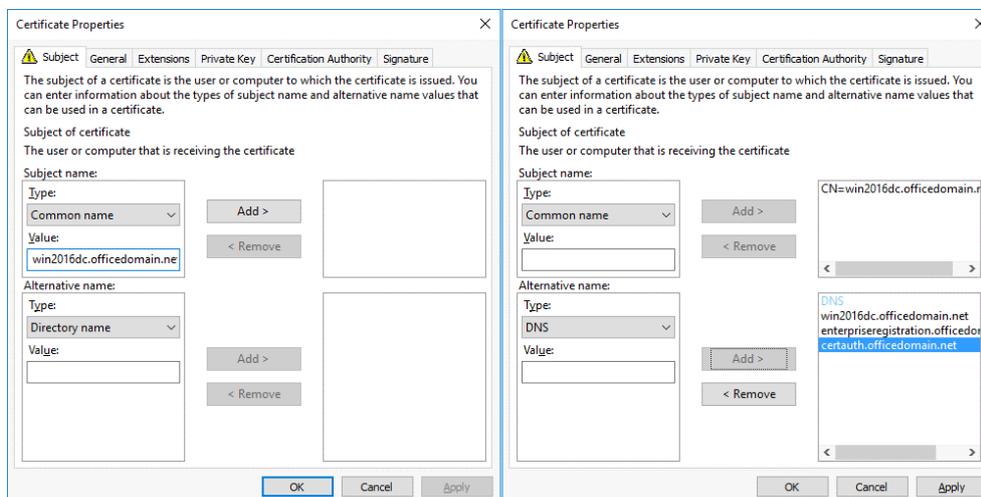
The Certificate Properties window opens. In the **Subject** tab, find the **Subject name** section and, in the drop-down menu, select **Common name** as a type. Enter the value that is a fully qualified domain name (FQDN) of your Windows Server on which ADFS is installed, for example: *win2016dc.officedomain.net* (see the left screenshot).

Similarly, in the **Alternative name** section, add three values. Type: **DNS**.

win2016dc.officedomain.net

enterpriseregistration.officedomain.net

certauth.officedomain.net



Note: A certificate must support ECU Server Authentication and be able to export the private key. All servers of a farm must use the single certificate. After configuring the first ADFS server in the farm, a certificate must be exported to another server. You cannot use different certificates with different thumbprints.

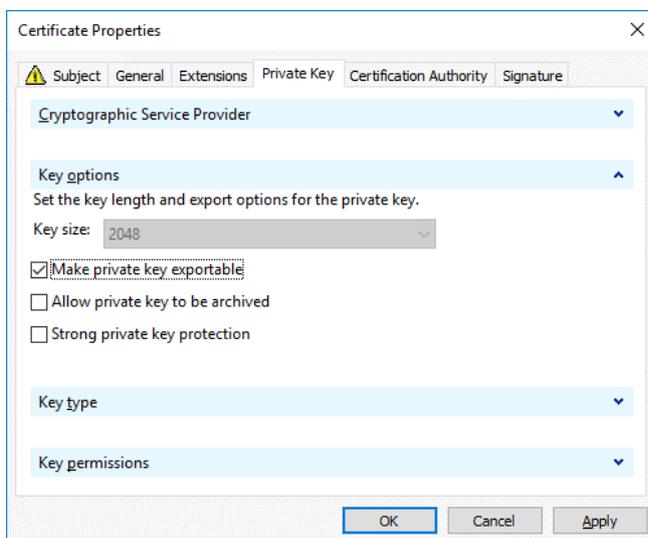
A certificate template for a web server or another certificate can be used to create your custom certificate. The main condition is the correct ECU. Another main point is using correct values for a subject name and subject alternative name.

enterpriseregistration.[domain-name] is used to enable clients to register via Workplace Join and provides mechanisms to implement Condition Access for web applications whose authentication is configured via ADFS. Office 365 ADFS configuration can also use this principle.

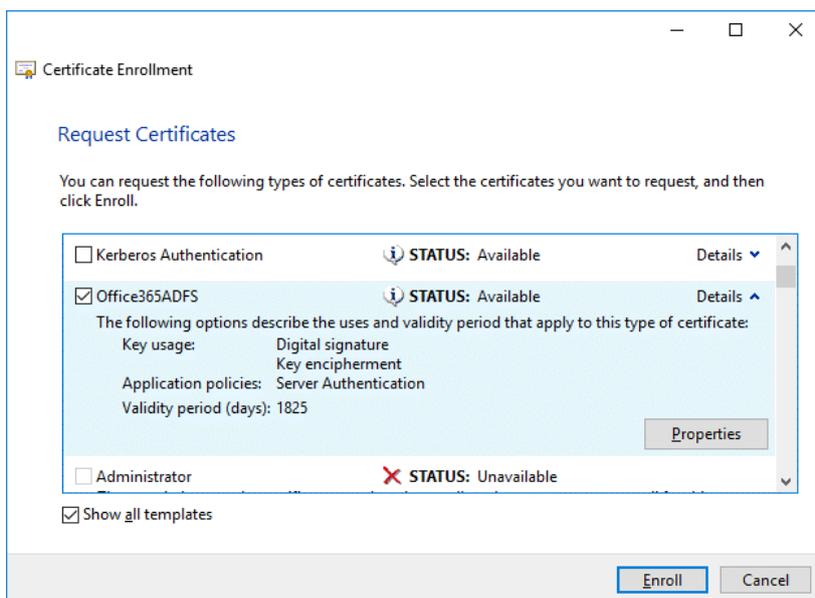
certauth.[domain-name] allows authentication by using smart cards, including virtual smart cards.

In the **Private Key** tab, select the **Make private key exportable** checkbox.

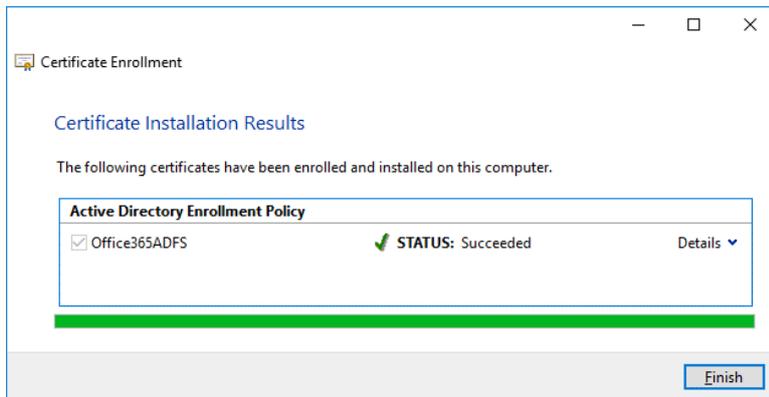
Hit **OK** to save settings.



All the required information to enroll the certificate is defined. Click **Enroll** to continue.



If the status is **Succeeded** in the *Certificate Installation Results* step of the wizard, click **Finish** to close the window.

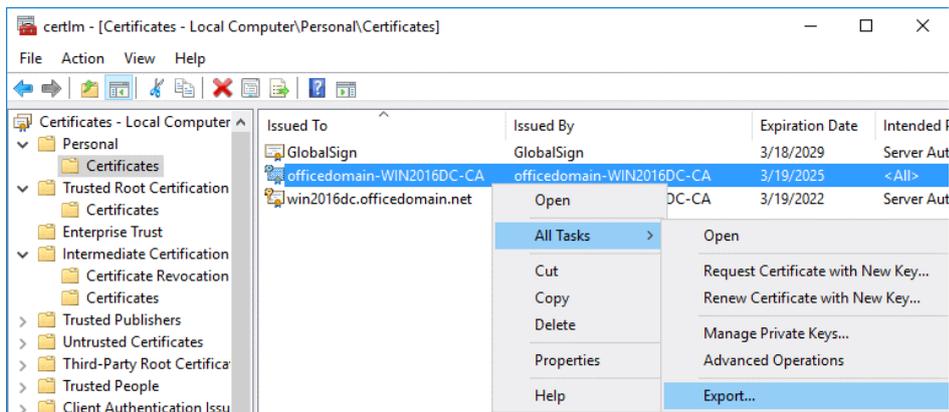


Exporting a certificate for Office 365 ADFS setup

You should export a certificate to a file that could be used on the current server and other Windows servers in the ADFS farm.

Run **certlm** if you have not done that yet.

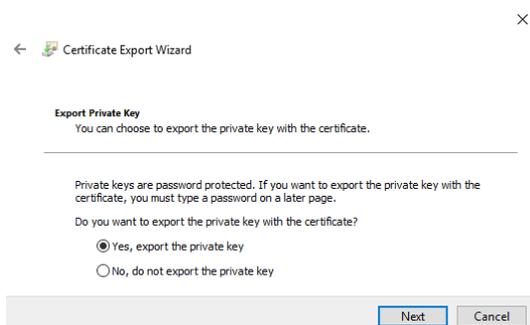
Go to **Personal > Certificates**, select your certificate. In our example, the selected certificate is *officedomain-WIN2016DC-CA*. Right click the certificate and in the context menu, select **All Tasks > Export**.



The Certificate Export Wizard opens.

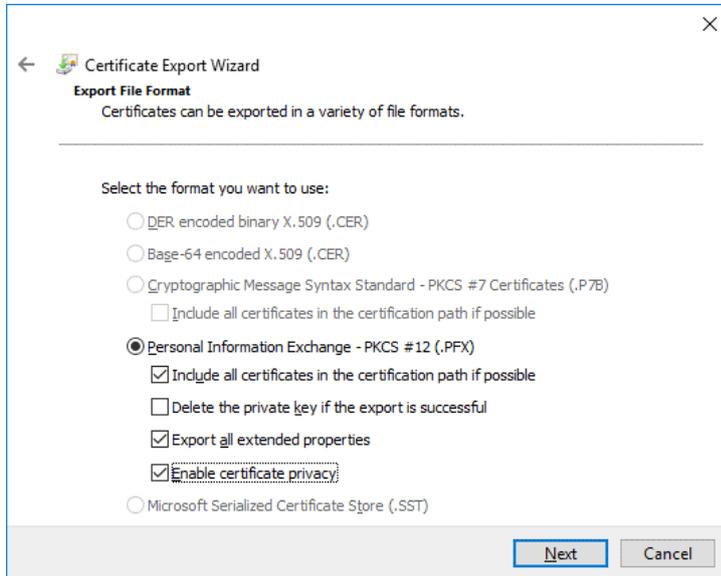
Welcome to the Certificate Export Wizard. This is the first step of the wizard used for introduction. There is nothing to configure and you can click **Next** to continue.

Export Private Key. Select **Yes, export the private key.**

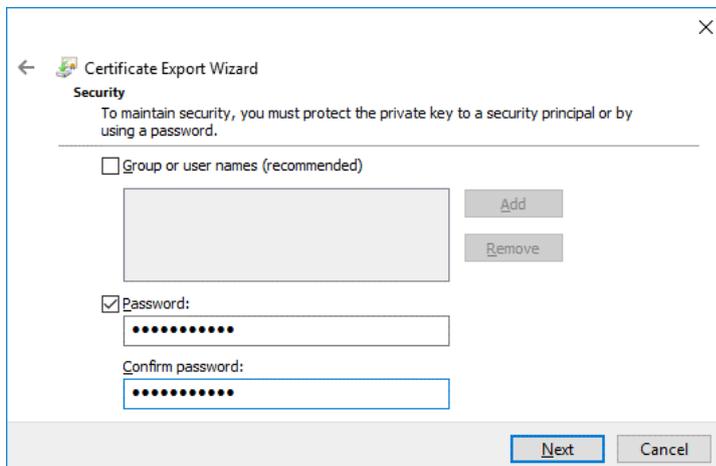


Export File Format. Select *Personal Information Exchange — PKCS #12 (.PFX)* as the file format. Then select the following checkboxes:

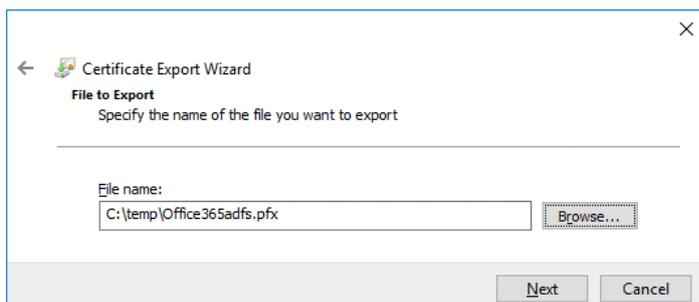
- Include all certificates in the certification path if possible
- Export all extended properties
- Enable certificate privacy



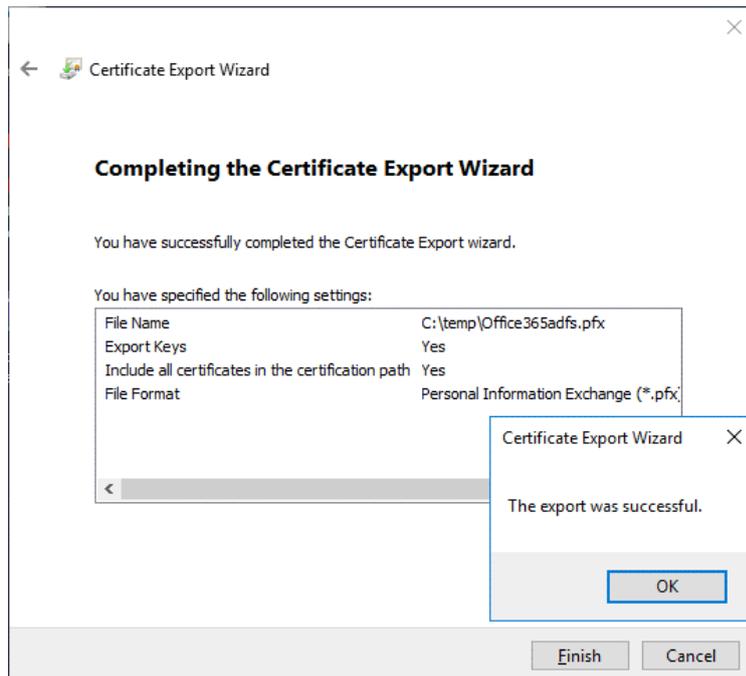
Security. Select the **Password** checkbox, enter your password and confirm your password.



File to Export. Click **Browse** and select destination and the file name for the exported certificate. In this example, the name of the file to export is *C:\temp\Office365adfs.pfx*



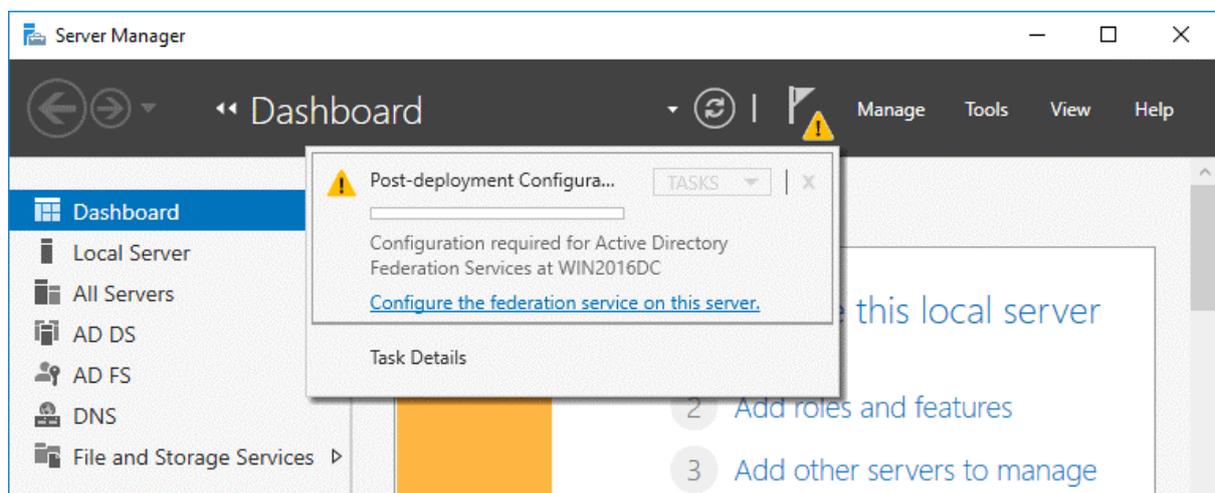
Completing the Certificate Export Wizard. Now everything is ready for export. Hit **Finish** to export the certificate. The export was successful. Click **OK** to close the window.



Configuring ADFS for Office 365

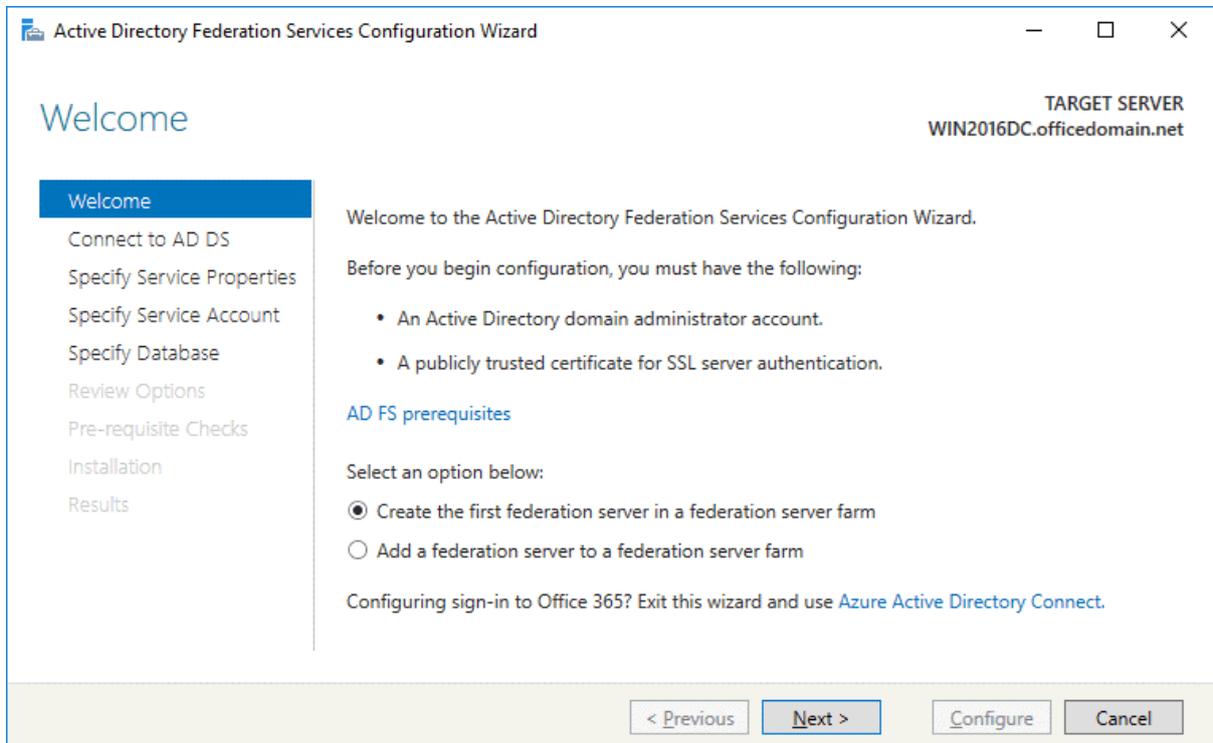
After installing the ADFS role and creating/exporting a certificate, you can resume Office 365 ADFS setup.

Open Server Manager and click the flag icon with the yellow triangle. In the menu that opens, click **Configure the federation service on this server** to perform the post-deployment configuration.

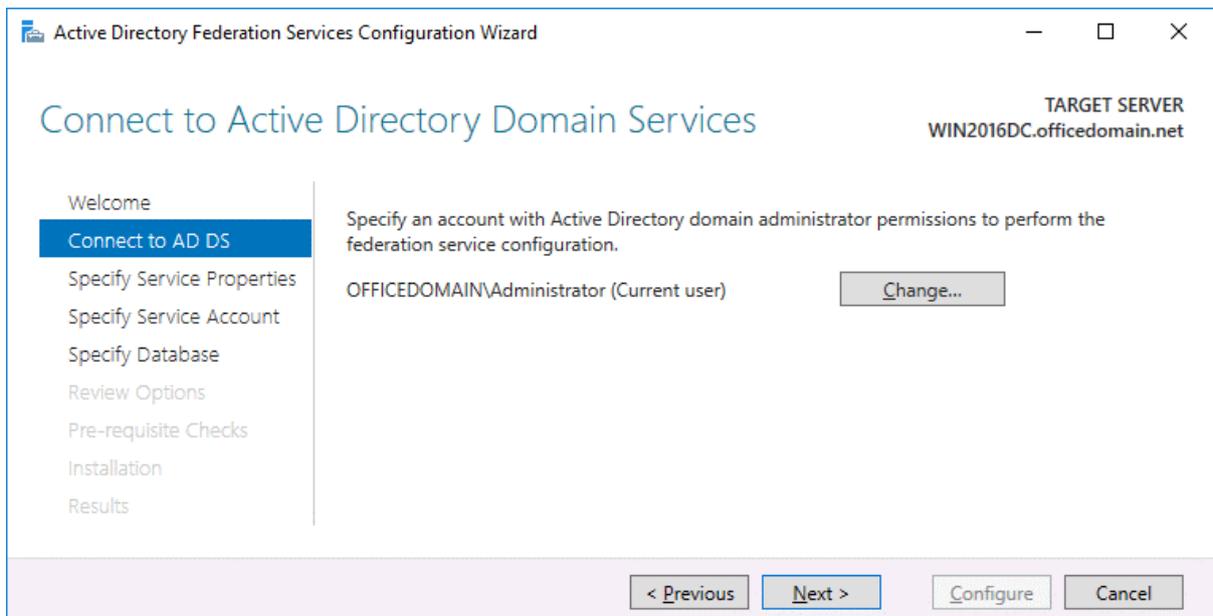


The Active Directory Federation Services Configuration Wizard opens.

Welcome. In the first step of the wizard, select the option: *Create the first federation server in a federation server farm*. Hit **Next** to continue.



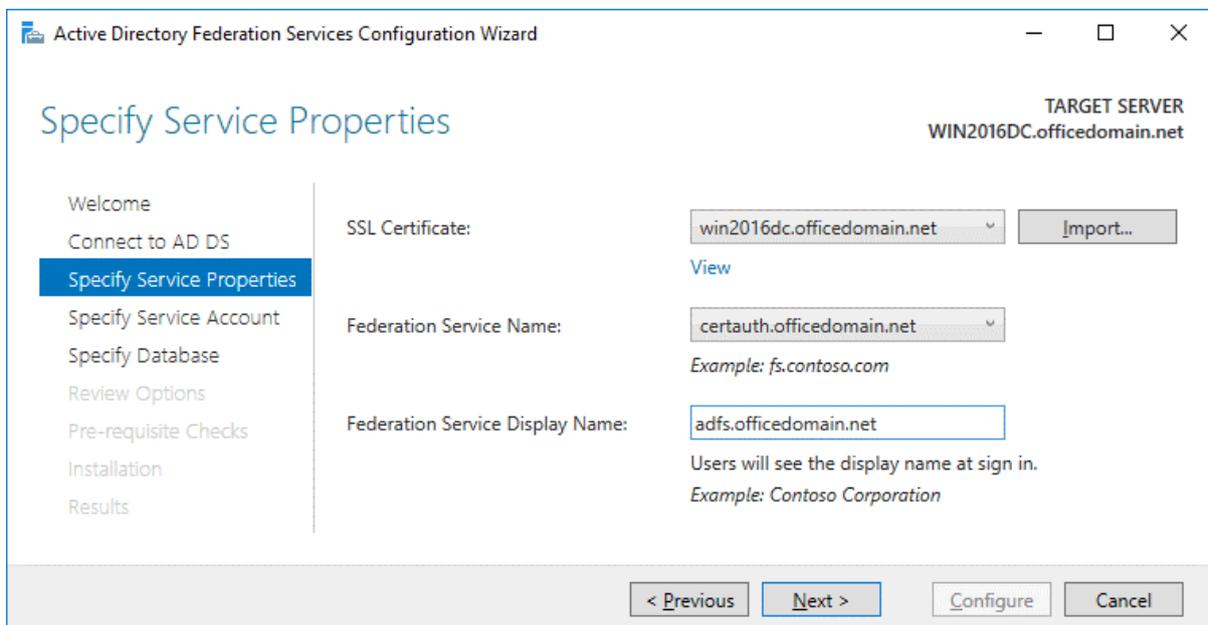
Connect to AD DS. Select the account with permissions of the AD domain administrator (*OFFICEDOMAIN\Administrator* in this case). You can click the **Change** button and select another user.



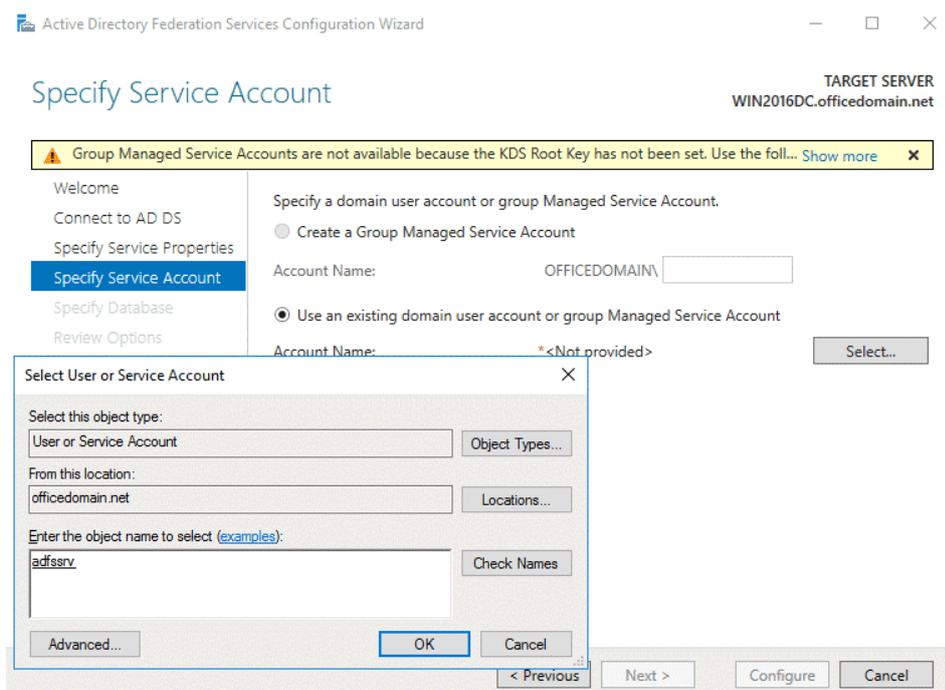
Specify Service Properties. SSL Certificate: *win2016dc.officedomain.net* (select the certificate you have created before in the drop-down menu. As an alternative, click the **Import** button and browse the exported certificate file.)

Federation Service Name: *certauth.officedomain.net*

Federation Service Display Name: *adfs.officedomain.net* (this name will be displayed for users to sign in).

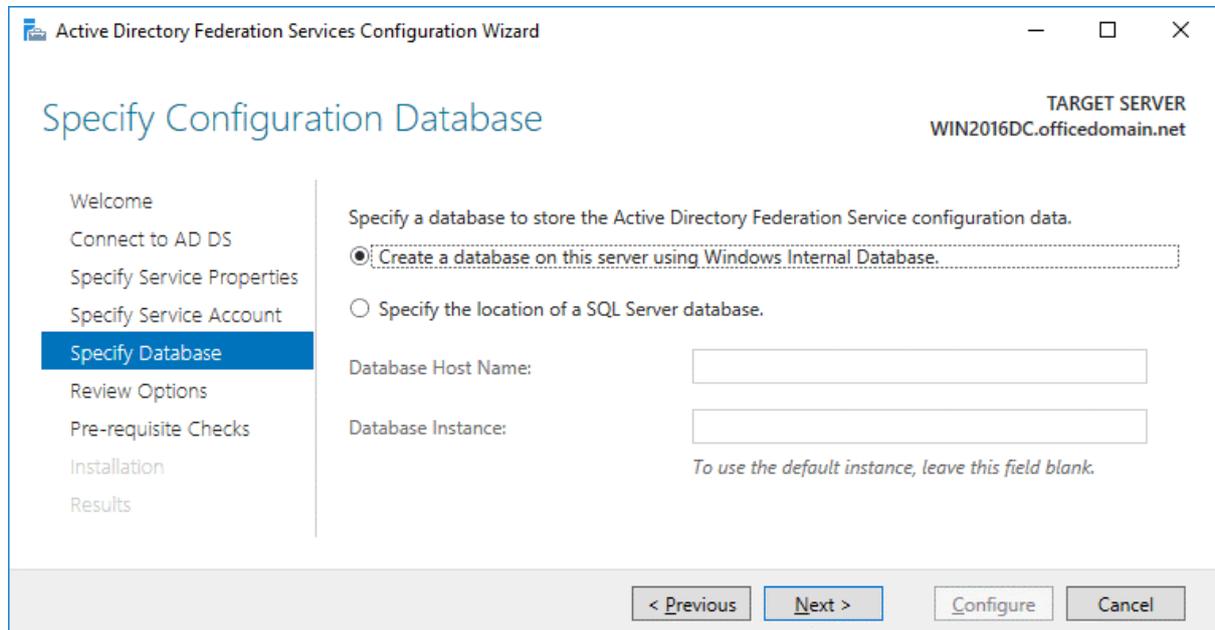


Specify Service Account. Specify a domain user account or group. The second option is selected in our example: **Use an existing domain user account or group.** Click **Select** to choose the account with administrative permissions (a special *adfsrv* account was created in the beginning of this this walkthrough).

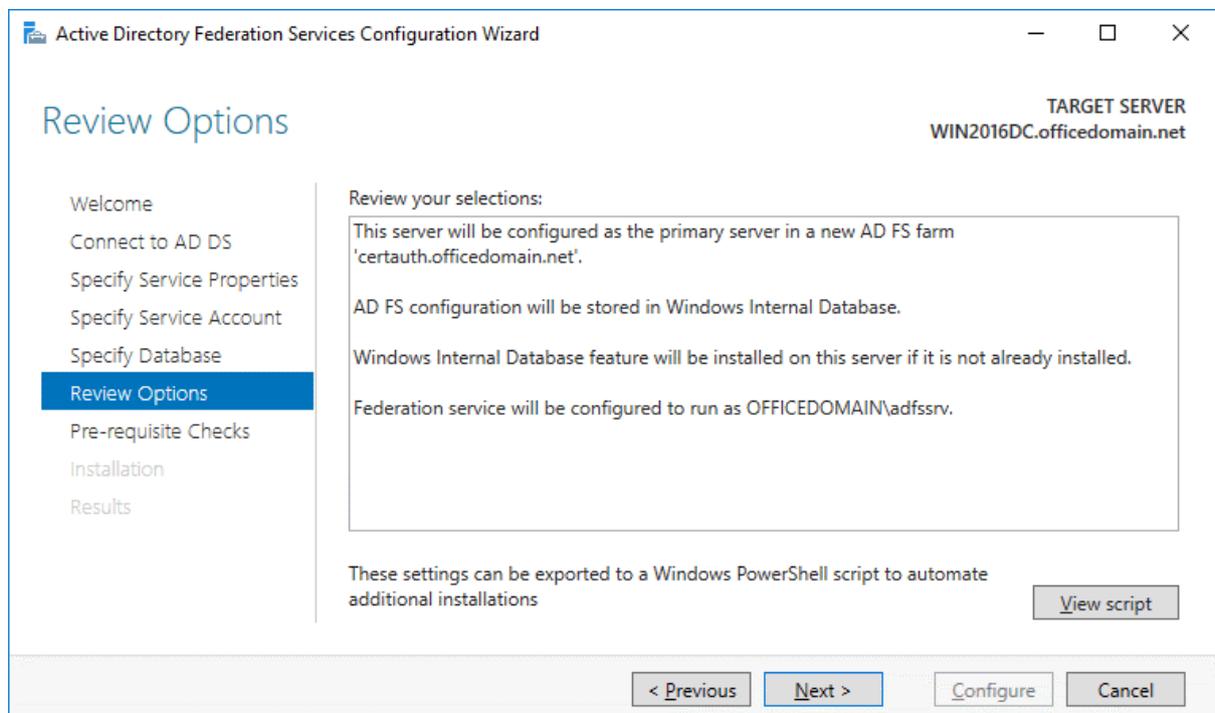


Specify Database. At this step you have to specify a database to store the Active Directory Federation Service configuration data. For small organizations and ADFS environments the internal database can be used. MS SQL Server Database is recommended for large ADFS deployments. In this example, we select the first option:

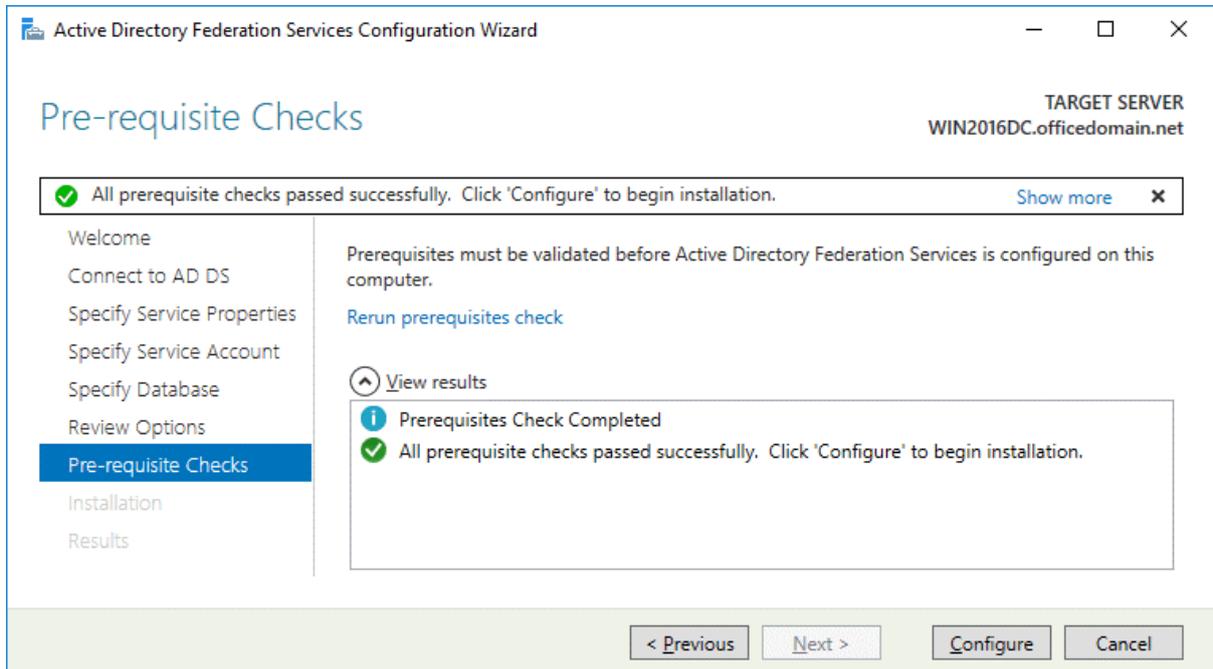
Create a database on this server using Windows Internal Database.



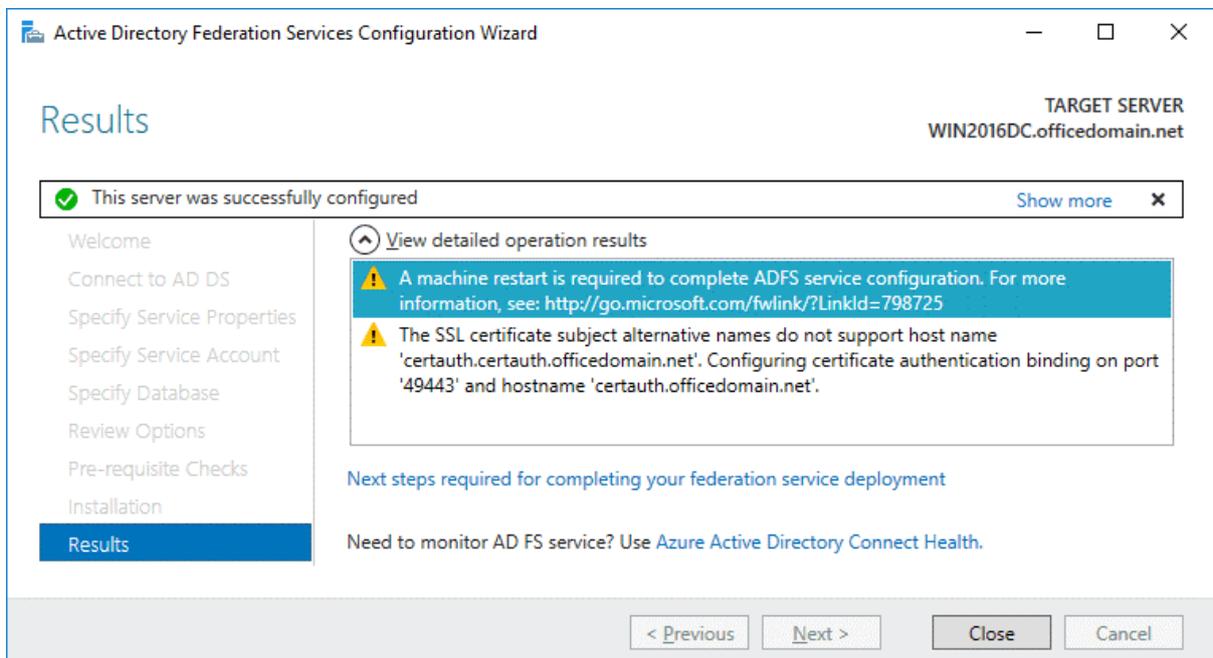
Review Options. Review your options. You can click **View script** and save the configuration script. This may be useful if you want to deploy multiple Active Directory Federation Servers.



Prerequisite Checks. A system checks configuration parameters. If everything is correct, you will see the message: All prerequisite checks passed successfully. Click **Configure** to begin installation. Wait until Office 365 ADFS setup has completed.



Results. In the case of successful installation, you will see the message: *This server was successfully configured.* You can close the wizard.



Run PowerShell as Administrator and execute the command:

Set-AdfsProperties -EnableIdpInitiatedSignonPage \$true

It is possible to check the **EnableIdpInitiatedSignonPage** parameter with the **Get-AdfsProperties** command.

You can test the ADFS login page in your web browser by using one of the links:

<https://win2016dc.officedomain.net/adfs/ls/IdpInitiatedSignon.aspx>

<https://win2016dc.officedomain.net/adfs/ls/idpinitiatedsignon.htm>

Change the domain name (*win2016dc.officedomain.net*) in these links according to your configuration. Later you can customize that web page, for example, you can implement your company style.

Add your site (the links above) to the Trusted Sites in Group Policies so that domain users don't have to enter passwords manually.

Using Azure AD Connect

Azure AD Connect is a Microsoft tool that allows you to connect your on-site Active Directory infrastructure to Azure Active Directory in the cloud. Authentication and authorization in mixed environments are also called hybrid identity. When installing Azure AD Connect, the components that enable connection with SSO and AD sync are installed.

Download Azure AD Connect by using the link below:

<https://www.microsoft.com/en-us/download/details.aspx?id=47594>

You can download tools that allow you to connect to Azure Active Tenant with PowerShell.

Microsoft Online Services Sign-In Assistant for IT Professionals RTW:

<https://www.microsoft.com/en-us/download/details.aspx?id=41950>

Windows Azure Active Directory Module for Windows PowerShell:

<https://www.powershellgallery.com/packages/MSONline/1.1.166.0>

Install Azure AD Connect and run the Azure AD Connect wizard. Configure the following:

Connect to Azure AD. Enter your Azure AD credentials.

Connect to AD DS. Enter the Active Directory Domain Services enterprise administrator credentials. (for example, officedomain.net\administrator)

Configure. You can select the checkbox: Start the synchronization process when configuration completes.

Hit Install.

When you have completed configuration, hit Exit. Now you can check the details of the on-premises Active Directory users in Azure Portal > Azure Active Directory.

Then you can install Office 365 ProPlus on other machines in the domain. The installation process is covered in detail in How to Install Office 365 ProPlus on a Remote Desktop Service Server. In the XML configuration, use a shared folder that is accessible for domain users. Once Office 365 has been installed and Office 365 ADFS configuration is completed, you can sign into Office 365 accounts with the single sign-on password by using Windows domain credentials (via your ADFS server).

Credits: https://www.nakivo.com/blog/office-365-adfs-setup-guide-step-by-step/?utm_source=medium_taras_yefimenko