




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

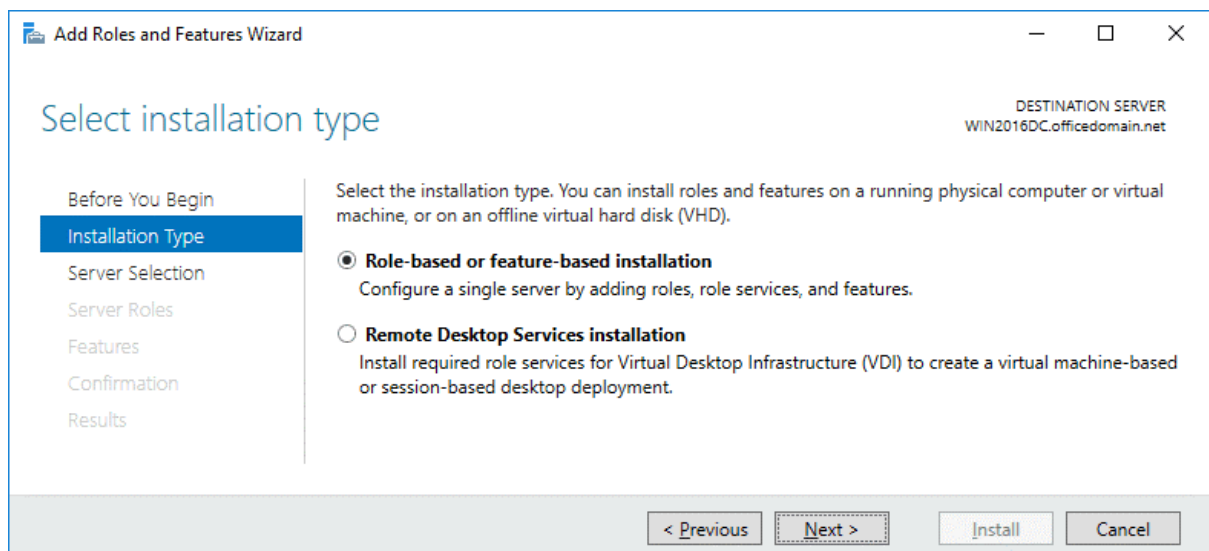
To install the ADFS role on your Windows Server machine. In this document, this role is installed on the domain controller running Windows Server 2016 by using the graphical user interface (GUI) and the workflow is demonstrated with a large number of screenshots.

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.



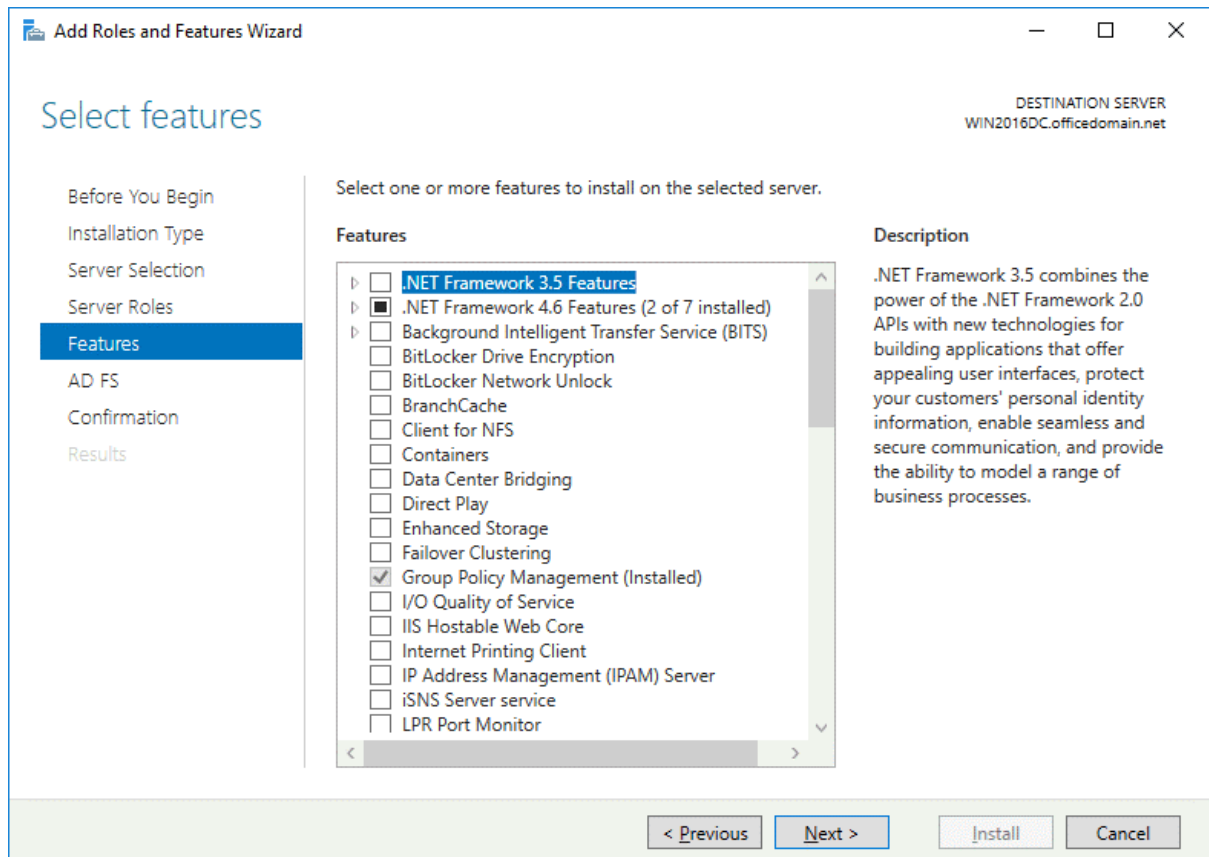
Server Selection. Select a server from the server pool: *WIN2016DC.officedomain.net* (is selected by default in our case because we have only one server).

The screenshot shows the 'Add Roles and Features Wizard' window. The title bar says 'Add Roles and Features Wizard'. The main heading is 'Select destination server'. In the top right corner, it says 'DESTINATION SERVER WIN2016DC.officedomain.net'. On the left, there is a navigation pane with the following items: 'Before You Begin', 'Installation Type', 'Server Selection' (which is highlighted), 'Server Roles', 'Features', 'Confirmation', and 'Results'. The main area contains the text 'Select a server or a virtual hard disk on which to install roles and features.' Below this, there are two radio buttons: 'Select a server from the server pool' (which is selected) and 'Select a virtual hard disk'. Below the radio buttons is a section titled 'Server Pool'. It has a 'Filter:' text box. Below the filter is a table with three columns: 'Name', 'IP Address', and 'Operating System'. The table contains one row: 'WIN2016DC.officedomain.net', '192.168.101.101', and 'Microsoft Windows Server 2016 Standard'. Below the table, it says '1 Computer(s) found'. Below that, there is a paragraph: '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.' At the bottom, there are four buttons: '< Previous', 'Next >', 'Install', and 'Cancel'.

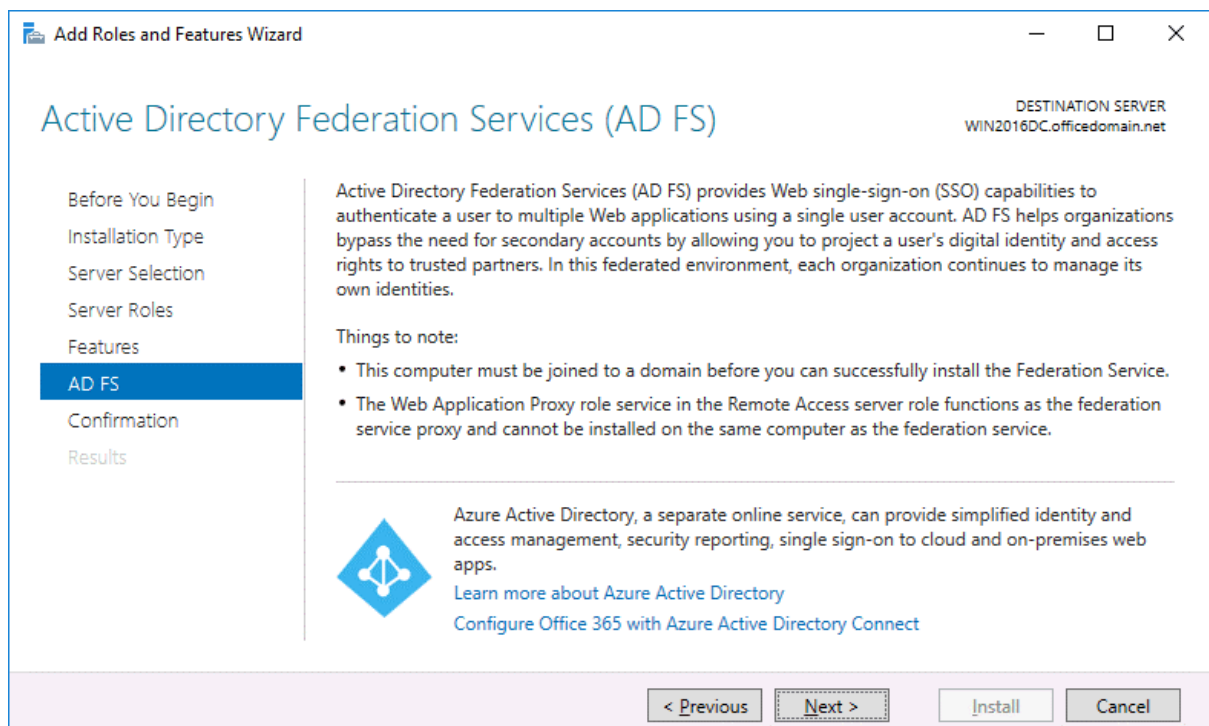
Server Roles. Select the checkbox next to *Active Directory Federation Services*.

The screenshot shows the 'Add Roles and Features Wizard' window. The title bar says 'Add Roles and Features Wizard'. The main heading is 'Select server roles'. In the top right corner, it says 'DESTINATION SERVER WIN2016DC.officedomain.net'. On the left, there is a navigation pane with the following items: 'Before You Begin', 'Installation Type', 'Server Selection', 'Server Roles' (which is highlighted), 'Features', 'AD FS', 'Confirmation', and 'Results'. The main area contains the text 'Select one or more roles to install on the selected server.' Below this, there is a section titled 'Roles'. It contains a list of roles with checkboxes. The roles are: 'Active Directory Certificate Services', 'Active Directory Domain Services (Installed)' (checked), 'Active Directory Federation Services' (checked), 'Active Directory Lightweight Directory Services', 'Active Directory Rights Management Services', 'Device Health Attestation', 'DHCP Server', 'DNS Server (Installed)' (checked), 'Fax Server', 'File and Storage Services (2 of 12 installed)' (checked), '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)', and 'Windows Deployment Services'. To the right of the list is a section titled 'Description'. It contains the text: '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.' At the bottom, there are four buttons: '< Previous', 'Next >', 'Install', and 'Cancel'.

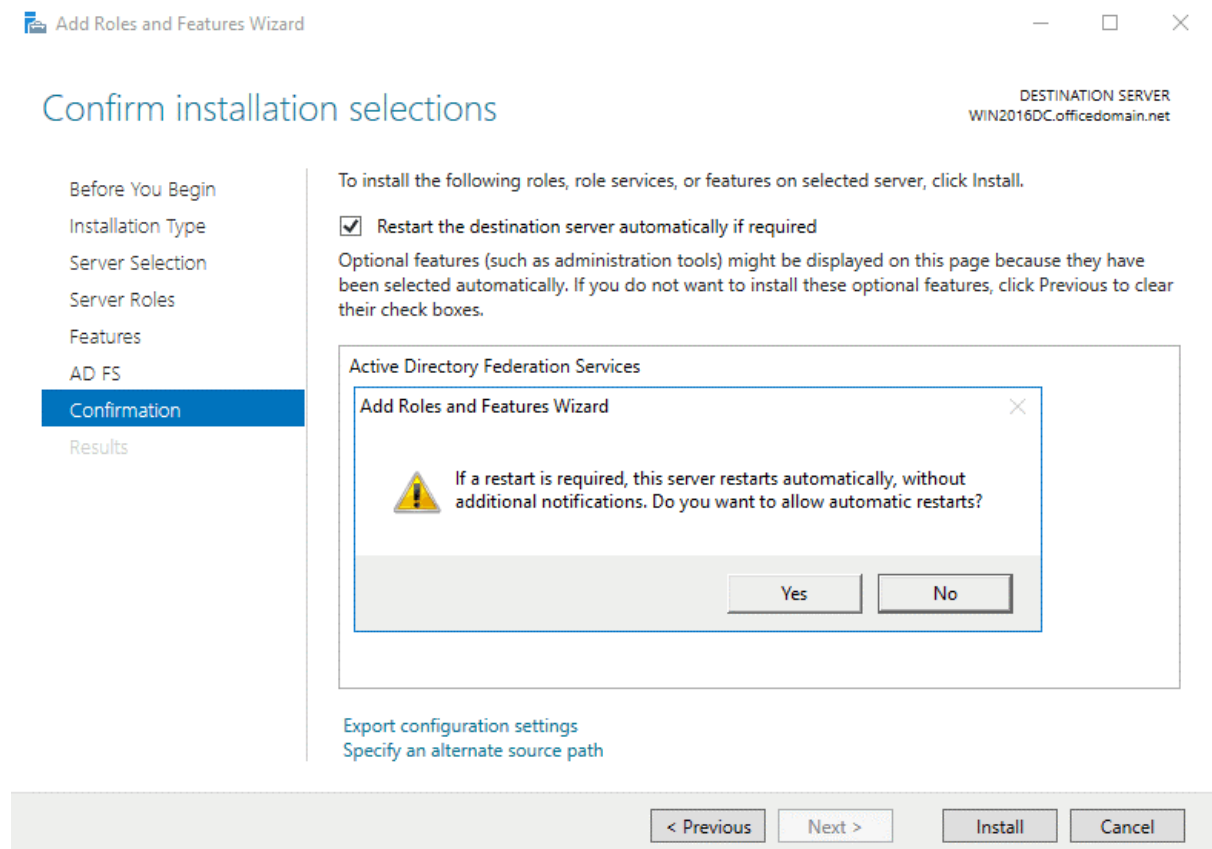
Features. The features needed for installing Active Directory Federation Services such as .NET Framework are selected.



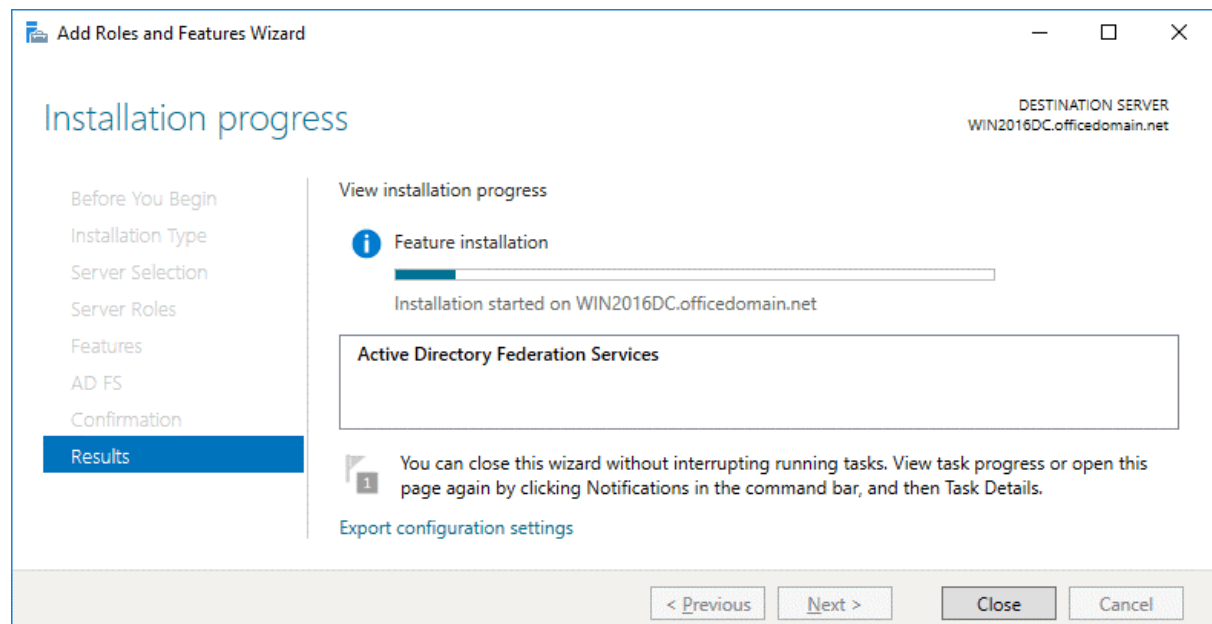
AD FS. Just click *Next* at this step after reading the description of Active Directory Federation Services.



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.



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



After finishing ADFS installation, the server must reboot.

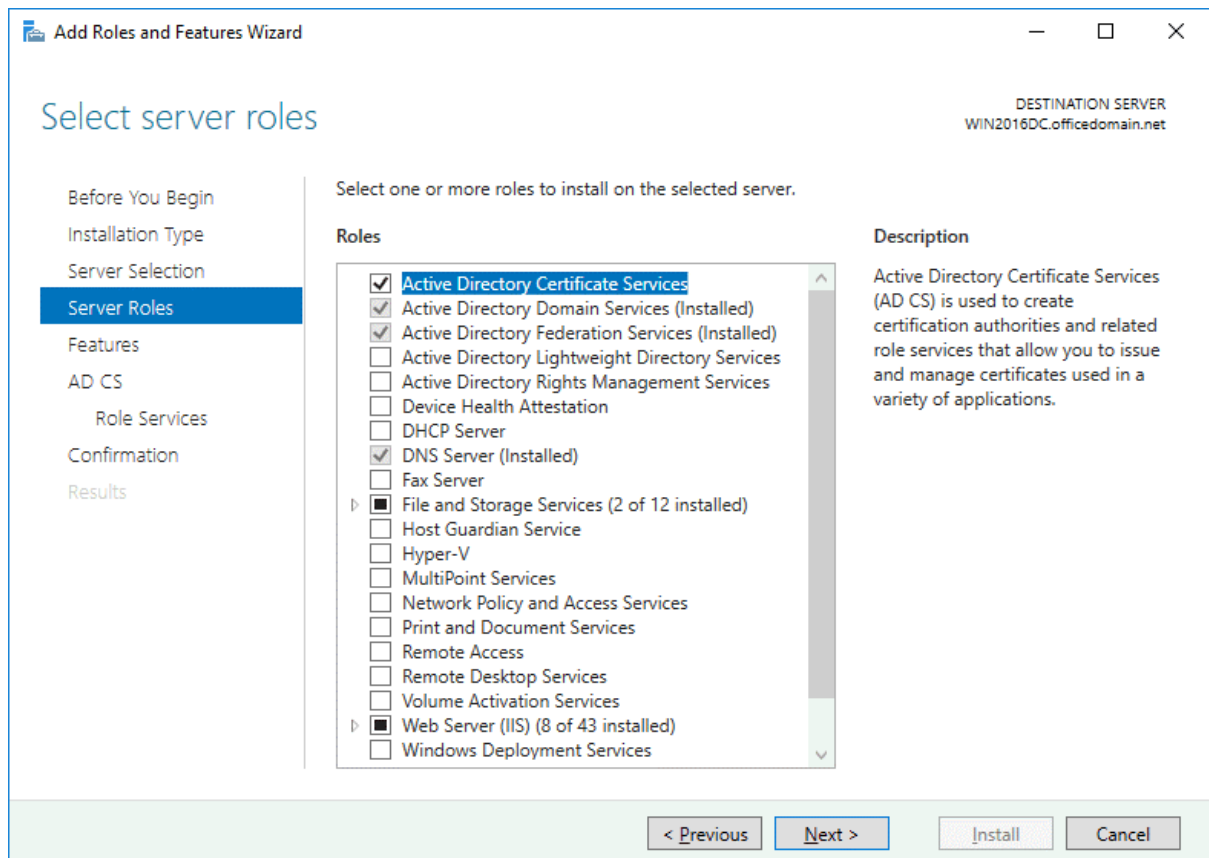
Installing ADCS to create a certificate

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.

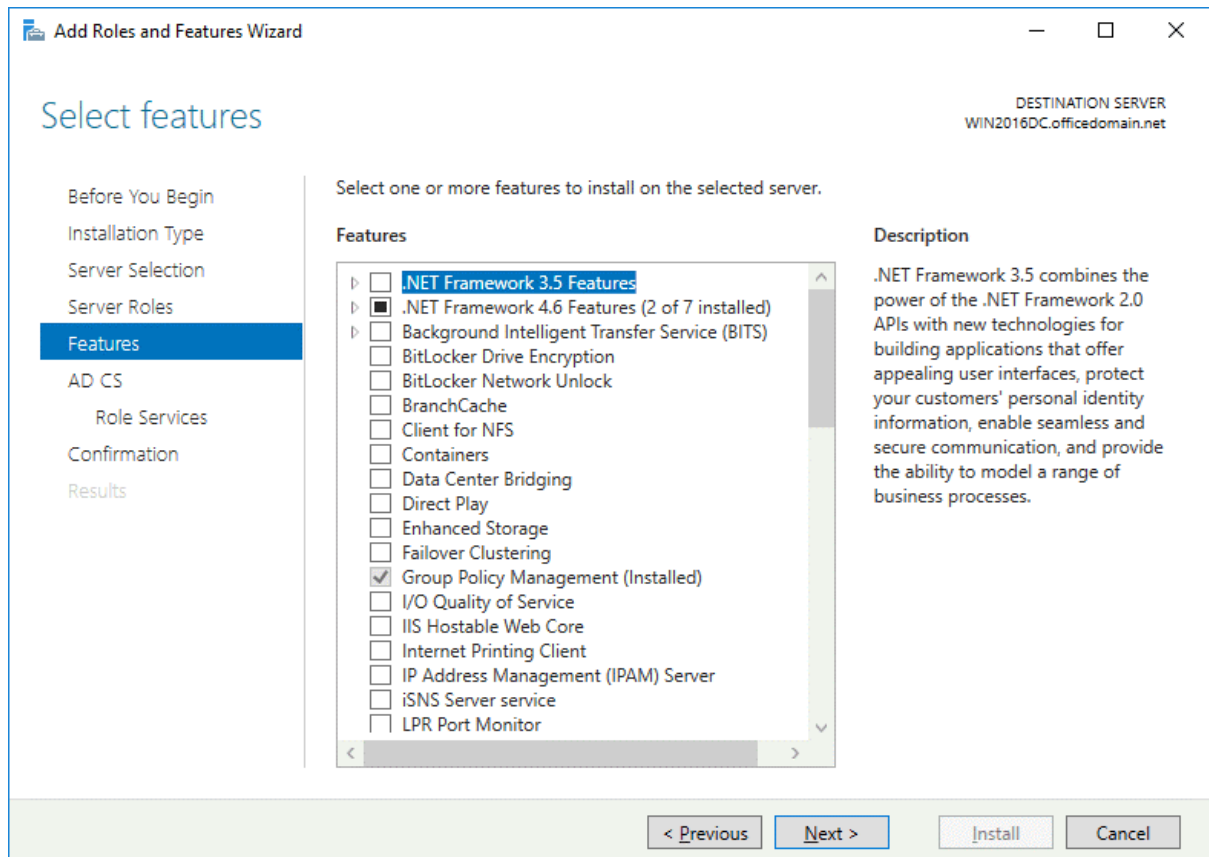
Installation Type. Select *Role-based or feature-based installation*. Hit **Next** for each step of the wizard to continue (as you have done before when installing ADFS).

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

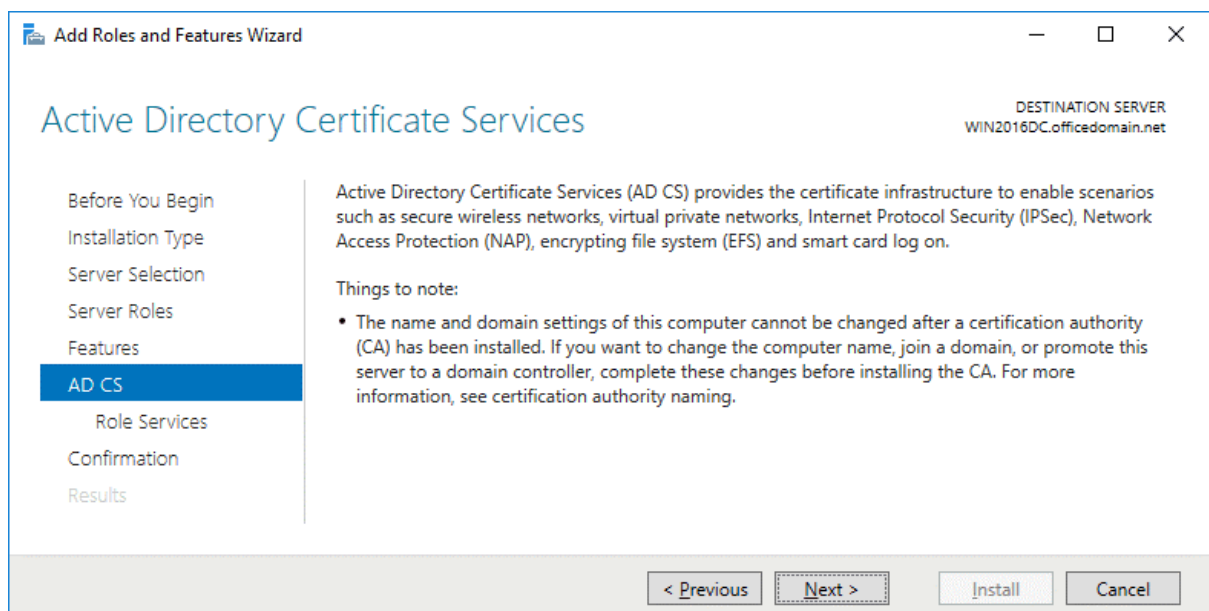
Server Roles. Select the checkbox next to *Active Directory Certificate Services*. Related roles and features such as IIS (Internet Information Services) are selected automatically.



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 **Certification Authority Web Enrollment** services.

The screenshot shows the 'Add Roles and Features Wizard' window. The title bar says 'Add Roles and Features Wizard'. The main heading is 'Select role services'. In the top right corner, it says 'DESTINATION SERVER WIN2016DC.officedomain.net'. On the left, there is a navigation pane with the following items: 'Before You Begin', 'Installation Type', 'Server Selection', 'Server Roles', 'Features', 'AD CS', 'Role Services' (which is highlighted), 'Confirmation', and 'Results'. The main area is titled 'Select the role services to install for Active Directory Certificate Services'. It contains a table with two columns: 'Role services' and 'Description'. The 'Role services' column has a list of services with checkboxes: 'Certification Authority' (checked), 'Certificate Enrollment Policy Web Service' (unchecked), 'Certificate Enrollment Web Service' (unchecked), 'Certification Authority Web Enrollment' (checked), 'Network Device Enrollment Service' (unchecked), and 'Online Responder' (unchecked). The 'Description' column has a description for 'Certification Authority Web Enrollment': 'Certification Authority Web Enrollment provides a simple Web interface that allows users to perform tasks such as request and renew certificates, retrieve certificate revocation lists (CRLs), and enroll for smart card certificates.' At the bottom, there are four buttons: '< Previous', 'Next >', 'Install', and 'Cancel'.

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

The screenshot shows the 'Add Roles and Features Wizard' window. The title bar says 'Add Roles and Features Wizard'. The main heading is 'Confirm installation selections'. In the top right corner, it says 'DESTINATION SERVER WIN2016DC.officedomain.net'. On the left, there is a navigation pane with the following items: 'Before You Begin', 'Installation Type', 'Server Selection', 'Server Roles', 'Features', 'AD CS', 'Role Services', 'Confirmation' (which is highlighted), and 'Results'. The main area is titled 'To install the following roles, role services, or features on selected server, click Install.' It contains a checkbox labeled 'Restart the destination server automatically if required'. Below this, there is a text box that says '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.' Below this text box is a list of features that are being installed, grouped into categories: 'Active Directory Certificate Services' (with sub-items 'Certification Authority' and 'Certification Authority Web Enrollment'), 'Remote Server Administration Tools' (with sub-items 'Role Administration Tools', 'Active Directory Certificate Services Tools', and 'Certification Authority Management Tools'), and 'Web Server (IIS)' (with sub-items 'Management Tools' and 'IIS 6 Management Compatibility'). At the bottom, there are four buttons: '< Previous', 'Next >', 'Install', and 'Cancel'. There are also links for 'Export configuration settings' and 'Specify an alternate source path'.

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.

The screenshot shows the 'AD CS Configuration' wizard window. The title bar says 'AD CS Configuration'. The main heading is 'Credentials'. On the right, it says 'DESTINATION SERVER WIN2016DC.officedomain.net'. On the left, there is a navigation pane with 'Credentials' selected, and other options like 'Role Services', 'Confirmation', 'Progress', and 'Results'. The main area is titled 'Specify credentials to configure role services'. It contains two lists of role services: one for the local Administrators group (Standalone certification authority, Certification Authority Web Enrollment, Online Responder) and one for the Enterprise Admins group (Enterprise certification authority, Certificate Enrollment Policy Web Service, Certificate Enrollment Web Service, Network Device Enrollment Service). Below these lists, there is a text box for 'Credentials' containing 'OFFICEDOMAIN\Administrator' and a 'Change...' button. At the bottom, there are buttons for '< Previous', 'Next >', 'Configure', and 'Cancel'.

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

The screenshot shows the 'AD CS Configuration' wizard window. The title bar says 'AD CS Configuration'. The main heading is 'Role Services'. On the right, it says 'DESTINATION SERVER WIN2016DC.officedomain.net'. On the left, there is a navigation pane with 'Role Services' selected, and other options like 'Credentials', 'Setup Type', 'CA Type', 'Private Key', 'Cryptography', 'CA Name', 'Validity Period', 'Certificate Database', 'Confirmation', 'Progress', and 'Results'. The main area is titled 'Select Role Services to configure'. It contains a list of role services with checkboxes: 'Certification Authority' (checked), 'Certification Authority Web Enrollment' (checked), 'Online Responder' (unchecked), 'Network Device Enrollment Service' (unchecked), 'Certificate Enrollment Web Service' (unchecked), and 'Certificate Enrollment Policy Web Service' (unchecked). Below this list, there is a 'More about AD CS Server Roles' link. At the bottom, there are buttons for '< Previous', 'Next >', 'Configure', and 'Cancel'.

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

The screenshot shows the 'AD CS Configuration' window with the 'Setup Type' tab selected. The left-hand navigation pane lists the following steps: Credentials, Role Services, Setup Type (highlighted), CA Type, Private Key, Cryptography, CA Name, Validity Period, Certificate Database, Confirmation, Progress, and Results. The main area is titled 'Specify the setup type of the CA'. It contains a paragraph explaining that Enterprise CAs use Active Directory Domain Services (AD DS) to simplify certificate management, while Standalone CAs do not. Below this, there are two radio button options: 'Enterprise CA' (which is selected) and 'Standalone CA'. The 'Enterprise CA' option includes a sub-explanation: 'Enterprise CAs must be domain members and are typically online to issue certificates or certificate policies.' The 'Standalone CA' option includes a sub-explanation: 'Standalone CAs can be members or a workgroup or domain. Standalone CAs do not require AD DS and can be used without a network connection (offline).' At the bottom of the main area is a link that says 'More about Setup Type'. The bottom of the window features four buttons: '< Previous', 'Next >', 'Configure', and 'Cancel'. The 'DESTINATION SERVER' is listed as 'WIN2016DC.officedomain.net'.

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

The screenshot shows the 'AD CS Configuration' window with the 'CA Type' tab selected. The left-hand navigation pane lists the following steps: Credentials, Role Services, Setup Type, CA Type (highlighted), Private Key, Cryptography, CA Name, Validity Period, Certificate Database, Confirmation, Progress, and Results. The main area is titled 'Specify the type of the CA'. It contains a paragraph explaining that when installing Active Directory Certificate Services (AD CS), you are creating or extending a public key infrastructure (PKI) hierarchy. It defines a root CA as the top of the hierarchy and a subordinate CA as one that receives a certificate from the CA above it. Below this, there are two radio button options: 'Root CA' (which is selected) and 'Subordinate CA'. The 'Root CA' option includes a sub-explanation: 'Root CAs are the first and may be the only CAs configured in a PKI hierarchy.' The 'Subordinate CA' option includes a sub-explanation: 'Subordinate CAs require an established PKI hierarchy and are authorized to issue certificates by the CA above them in the hierarchy.' At the bottom of the main area is a link that says 'More about CA Type'. The bottom of the window features four buttons: '< Previous', 'Next >', 'Configure', and 'Cancel'. The 'DESTINATION SERVER' is listed as 'WIN2016DC.officedomain.net'.

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

The screenshot shows the 'Private Key' step of the AD CS Configuration wizard. The left-hand navigation pane lists steps: Credentials, Role Services, Setup Type, CA Type, Private Key (highlighted), Cryptography, CA Name, Validity Period, Certificate Database, Confirmation, Progress, and Results. The main area is titled 'Specify the type of the private key'. It contains a text box stating: 'To generate and issue certificates to clients, a certification authority (CA) must have a private key.' Below this are three radio button options: 'Create a new private key' (selected), 'Use existing private key', and 'Select a certificate and use its associated private key'. The 'Create a new private key' option has a sub-note: 'Use this option if you do not have a private key or want to create a new private key.' The 'Use existing private key' option has a sub-note: 'Use this option to ensure continuity with previously issued certificates when reinstalling a CA.' Below this are two sub-options: 'Select a certificate and use its associated private key' and 'Select an existing private key on this computer', each with a sub-note. At the bottom right, there are buttons: '< Previous', 'Next >', 'Configure', and 'Cancel'. The top right corner shows 'DESTINATION SERVER WIN2016DC.officedomain.net'.

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.

The screenshot shows the 'Cryptography for CA' step of the AD CS Configuration wizard. The left-hand navigation pane lists steps: Credentials, Role Services, Setup Type, CA Type, Private Key, Cryptography (highlighted), CA Name, Validity Period, Certificate Database, Confirmation, Progress, and Results. The main area is titled 'Specify the cryptographic options'. It contains two dropdown menus: 'Select a cryptographic provider:' (set to 'RSA#Microsoft Software Key Storage Provider') and 'Key length:' (set to '2048'). Below these is a list box for 'Select the hash algorithm for signing certificates issued by this CA:' with options: SHA256, SHA384, SHA512, SHA1, and MD5. At the bottom, there is a checkbox labeled 'Allow administrator interaction when the private key is accessed by the CA.' which is unchecked. At the bottom right, there are buttons: '< Previous', 'Next >', 'Configure', and 'Cancel'. The top right corner shows 'DESTINATION SERVER WIN2016DC.officedomain.net'.

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' window with the 'CA Name' step selected in the left-hand navigation pane. The main area is titled 'Specify the name of the CA'. It includes a text box for 'Common name for this CA:' containing 'officedomain-WIN2016DC-CA', a text box for 'Distinguished name suffix:' containing 'DC=officedomain,DC=net', and a text box for 'Preview of distinguished name:' containing 'CN=officedomain-WIN2016DC-CA,DC=officedomain,DC=net'. A 'More about CA Name' link is present. At the bottom, there are buttons for '< Previous', 'Next >', 'Configure', and 'Cancel'. The 'DESTINATION SERVER' is listed as 'WIN2016DC.officedomain.net'.

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' window with the 'Validity Period' step selected in the left-hand navigation pane. The main area is titled 'Specify the validity period'. It includes a section 'Select the validity period for the certificate generated for this certification authority (CA):' with a text box containing '5' and a dropdown menu set to 'Years'. Below this, it shows 'CA expiration Date: 3/19/2025 6:09:00 AM'. A note states: 'The validity period configured for this CA certificate should exceed the validity period for the certificates it will issue.' A 'More about Validity Period' link is at the bottom. At the bottom of the window, there are buttons for '< Previous', 'Next >', 'Configure', and 'Cancel'. The 'DESTINATION SERVER' is listed as 'WIN2016DC.officedomain.net'.

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

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

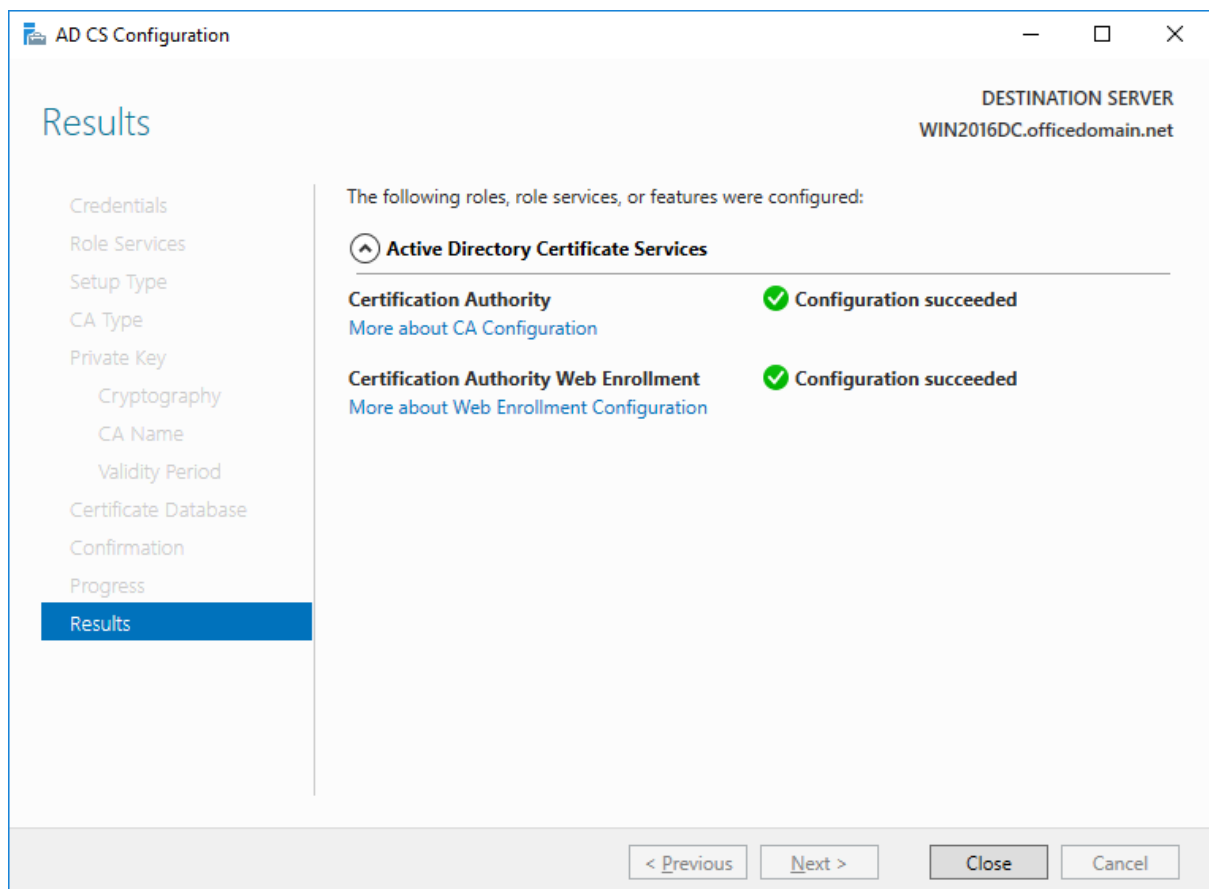
Certificate database log location: *C:\Windows\system32\CertLog*

The screenshot shows the 'AD CS Configuration' window with the 'CA Database' tab selected. The left-hand navigation pane lists various configuration steps: Credentials, Role Services, Setup Type, CA Type, Private Key, Cryptography, CA Name, Validity Period, Certificate Database (highlighted), Confirmation, Progress, and Results. The main pane is titled 'Specify the database locations' and contains two text input fields. The first field, 'Certificate database location:', contains the text 'C:\Windows\system32\CertLog'. The second field, 'Certificate database log location:', also contains 'C:\Windows\system32\CertLog'. Below these fields is a link that says 'More about CA Database'. In the top right corner, the 'DESTINATION SERVER' is listed as 'WIN2016DC.officedomain.net'. At the bottom of the window, there are four buttons: '< Previous', 'Next >', 'Configure', and 'Cancel'.

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

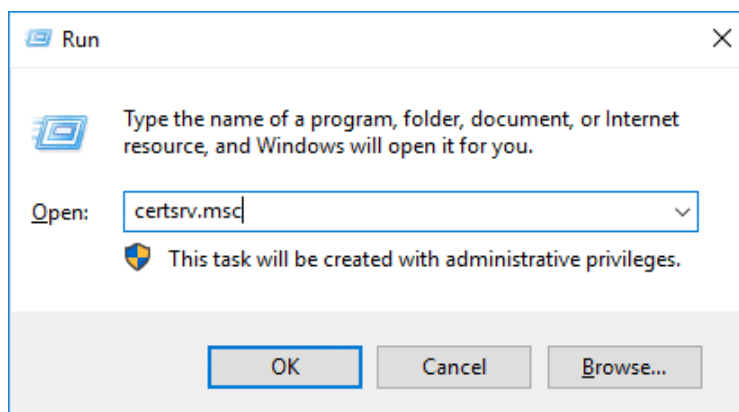
The screenshot shows the 'AD CS Configuration' window with the 'Confirmation' tab selected. The left-hand navigation pane is the same as in the previous window, but 'Confirmation' is now highlighted. The main pane is titled 'Confirmation' and contains the text 'To configure the following roles, role services, or features, click Configure.' Below this text is a dashed box containing a plus icon and the text 'Active Directory Certificate Services'. Underneath this box, there are two sections. The first section, 'Certification Authority', lists several properties: CA Type (Enterprise Root), Cryptographic provider (RSA#Microsoft Software Key Storage Provider), Hash Algorithm (SHA256), Key Length (2048), Allow Administrator Interaction (Disabled), Certificate Validity Period (3/19/2025 6:09:00 AM), Distinguished Name (CN=officedomain-WIN2016DC-CA,DC=officedomain,DC=net), Certificate Database Location (C:\Windows\system32\CertLog), Certificate Database Log Location (C:\Windows\system32\CertLog), and Location. The second section, 'Certification Authority Web Enrollment', is currently empty. The top right corner shows the 'DESTINATION SERVER' as 'WIN2016DC.officedomain.net'. At the bottom, the same four buttons as the previous window are present: '< Previous', 'Next >', 'Configure', and 'Cancel'.

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

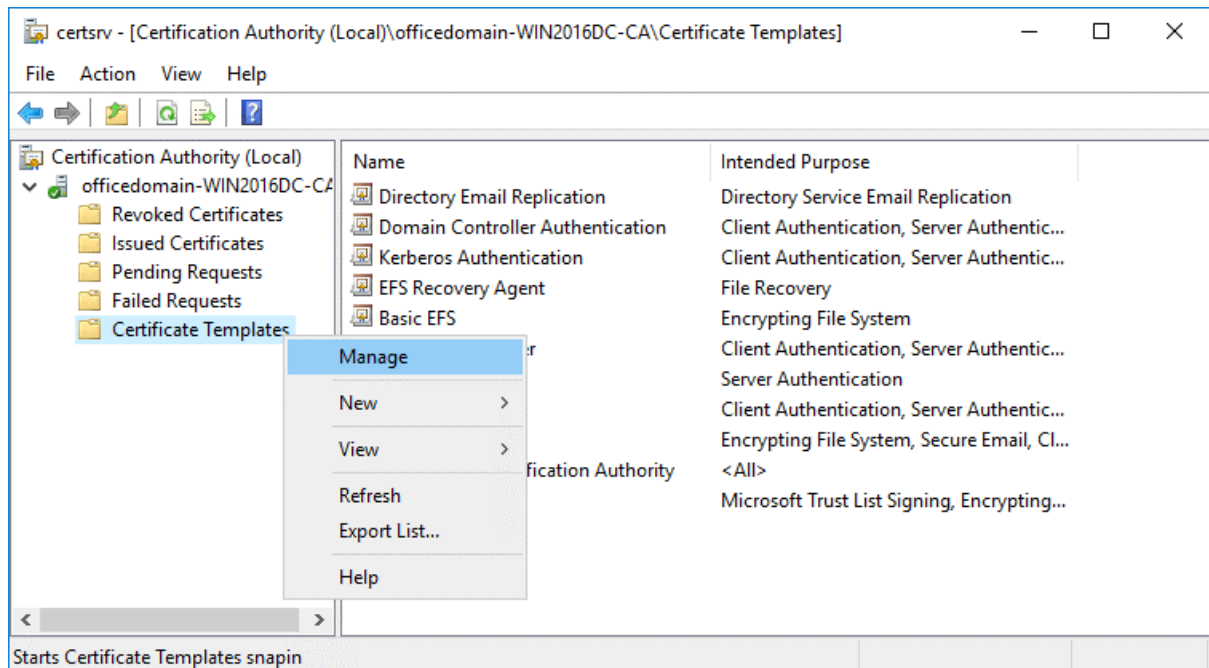


Editing a certificate template

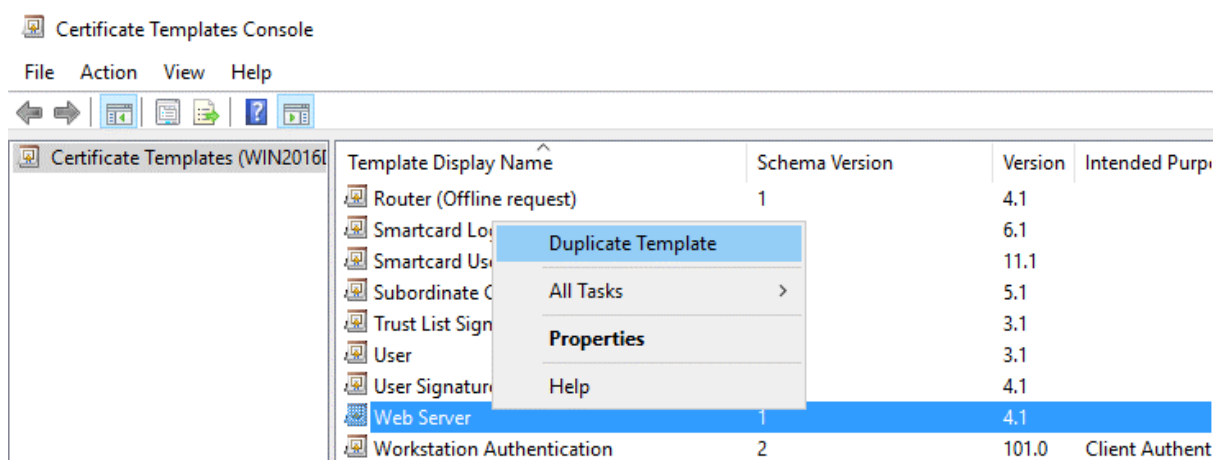
To edit a certificate template, open the Certification Authority configuration window by pressing **Win+R** and running **certsrv.msc**



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

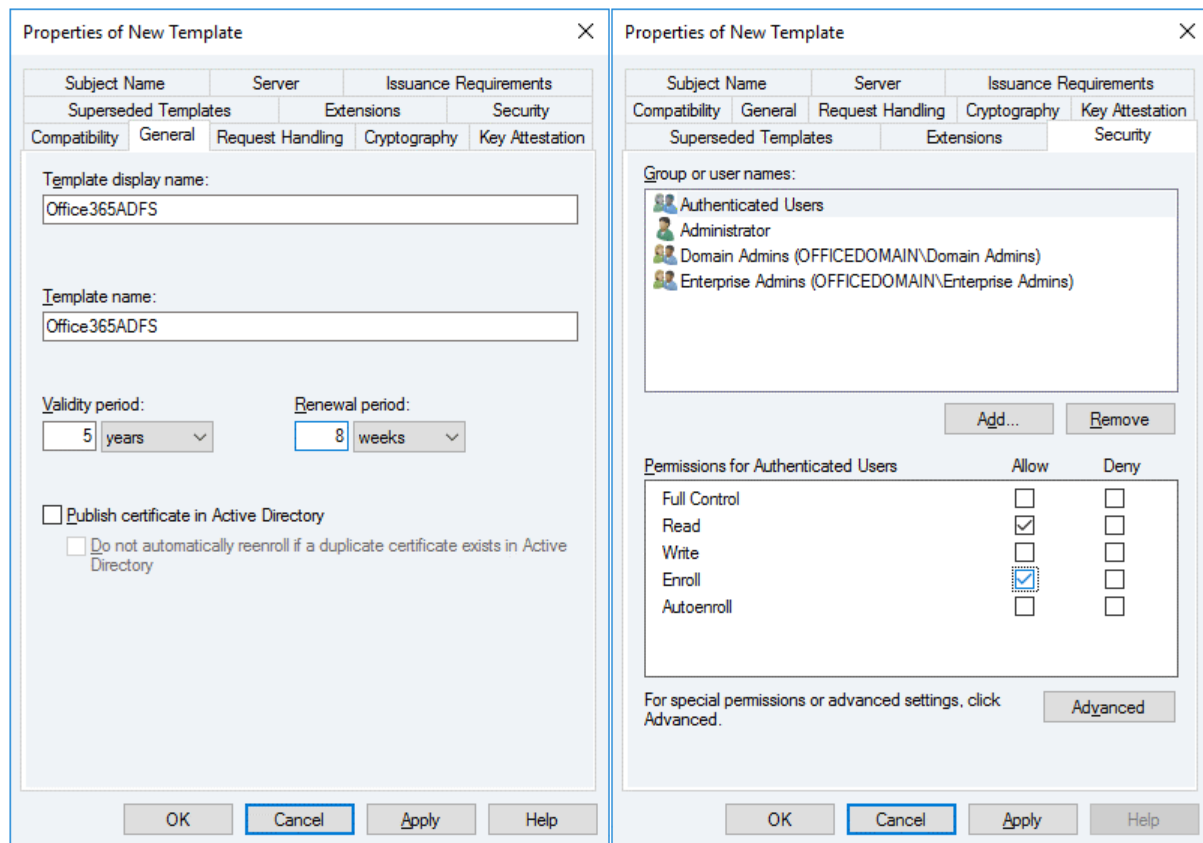


In the opened Certificate Templates Console, right click **Web Server** and in the context menu hit **Duplicate Template**.

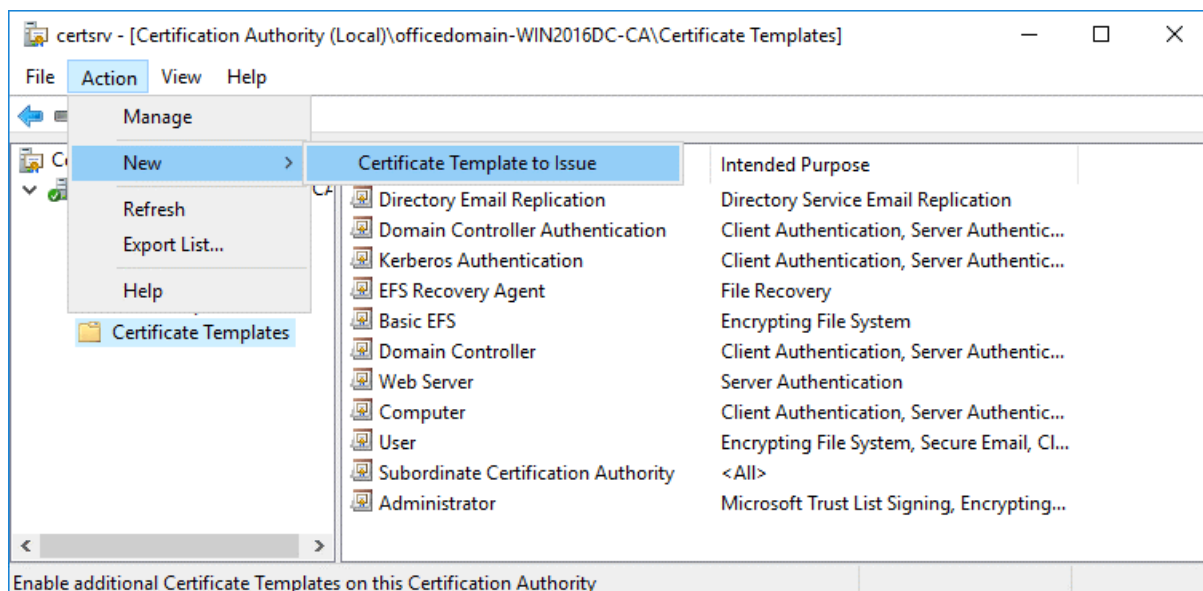


The *Properties of New Template* window opens. In the **General** tab enter the template display name and template name. We are configuring ADFS for Office 365, hence, the template name is *Office365ADFS* in this example. You can also set the validity period for the certificate.

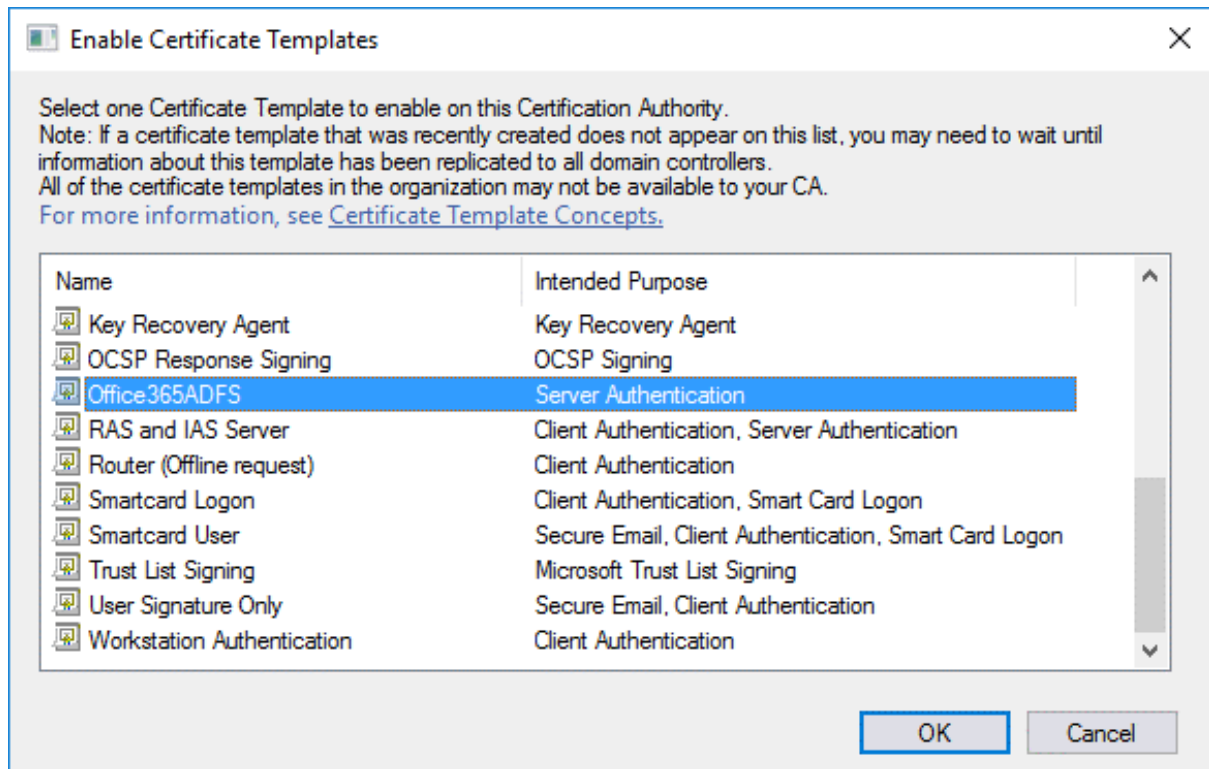
In the *Security* tab select **Authenticated users** and in the permissions for authenticated users select the checkbox to **Allow Enroll** (see the screenshot below).



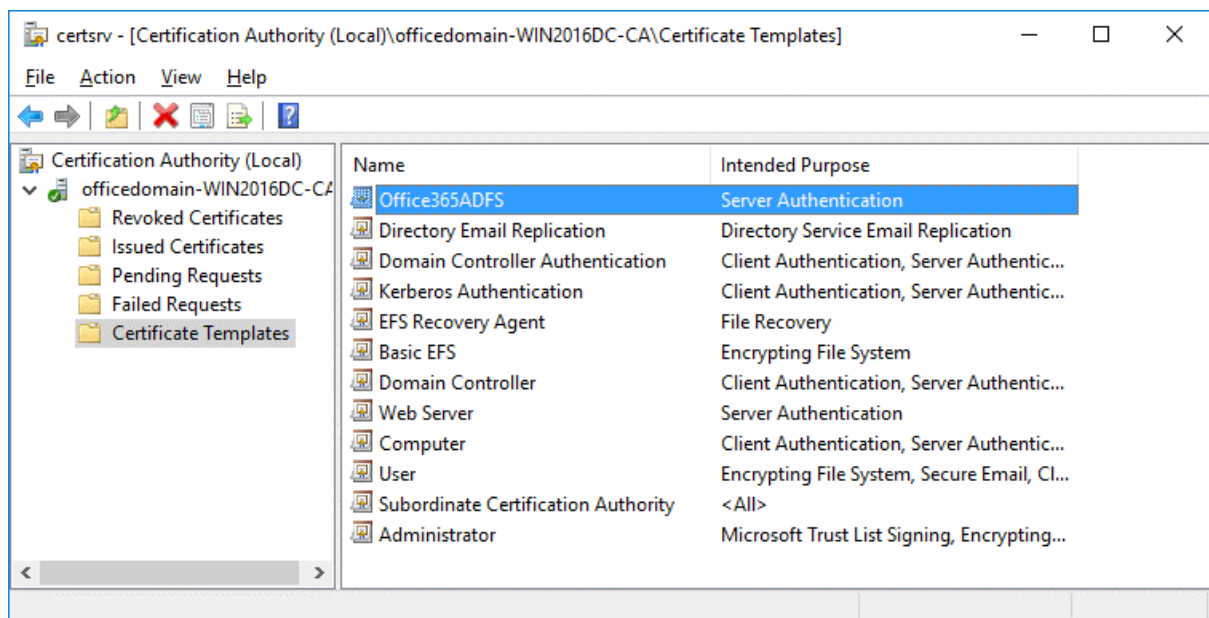
Now in the Certification Authority window (certsrv) click **Action > New > Certificate Template to Issue**.



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.

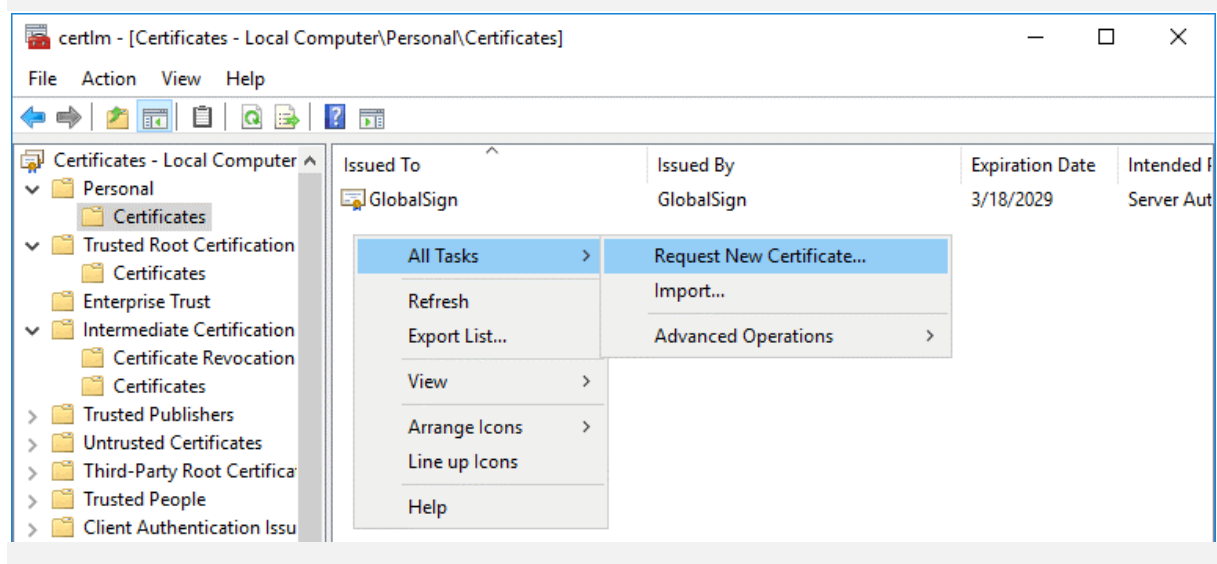


Creating a new certificate

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

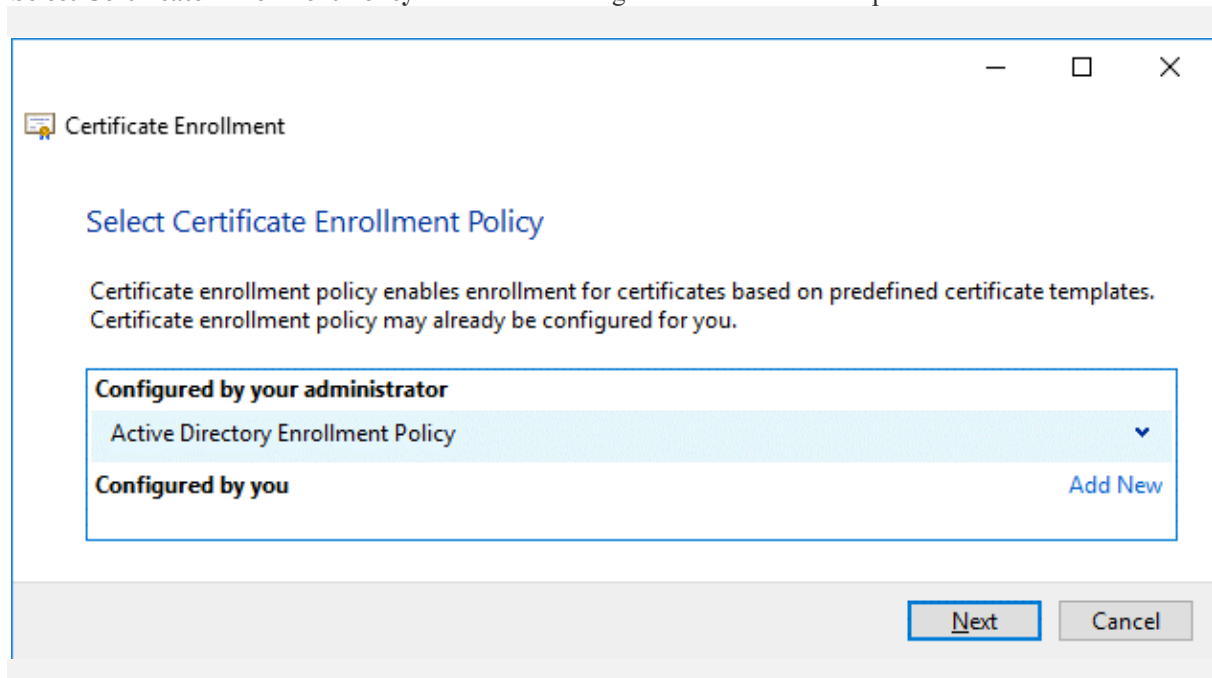
certlm

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**.

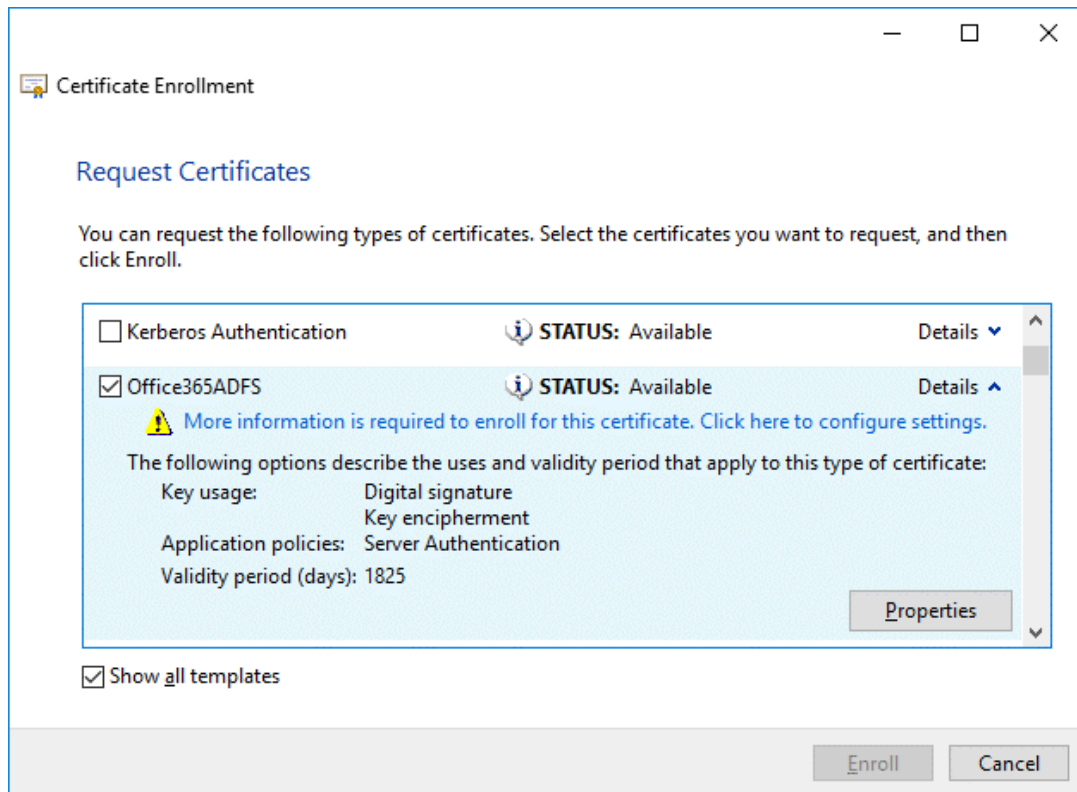


Before You begin. There is nothing to configure in this step. Click **Next** to continue.

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**.



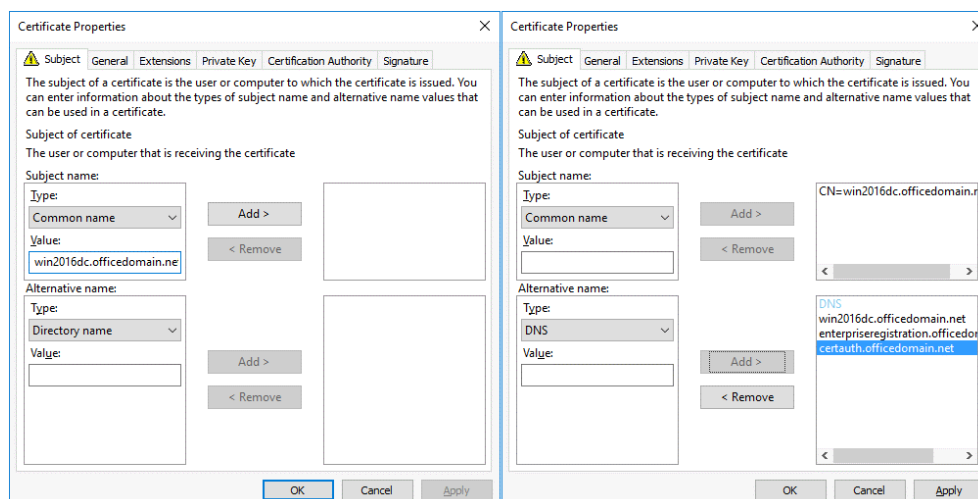
The Certificate Properties window opens. In the **Subject** tab, find the **Subject name** section and, in the drop-down menu, select **Common name** as a type. Enter the value that is a fully qualified domain name (FQDN) of your Windows Server on which ADFS is installed, for example: *win2016dc.officedomain.net*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

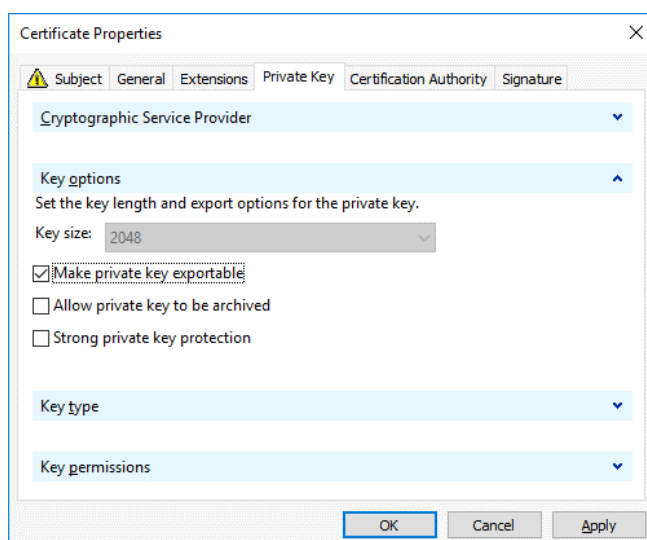
A certificate template for a web server or another certificate can be used to create your custom certificate. The main condition is the correct ECU. Another main point is using correct values for a subject name and subject alternative name.

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.

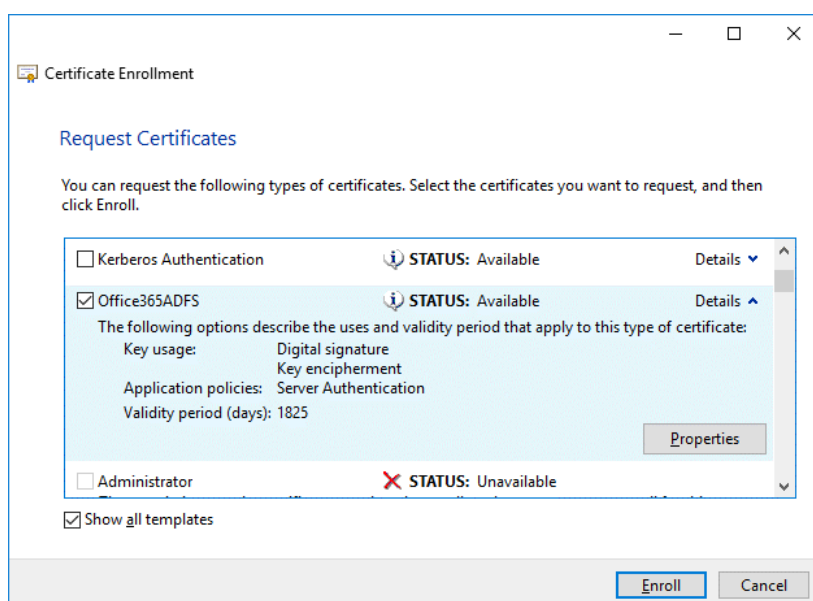
certauth.[domain-name] allows authentication by using smart cards, including virtual smart cards.

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

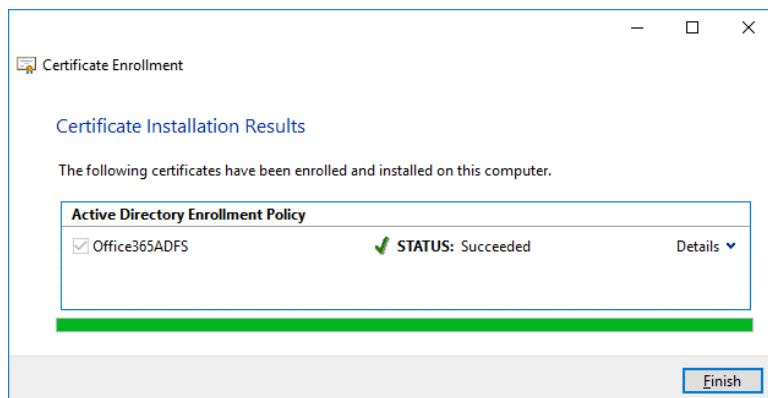
Hit **OK** to save settings.



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.

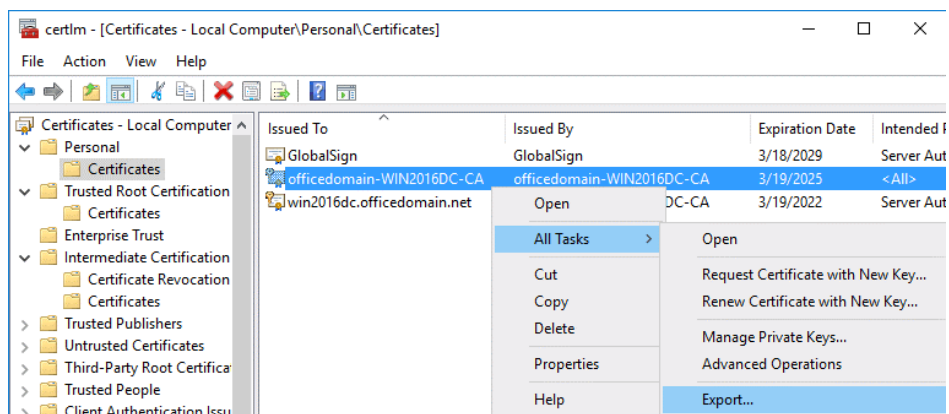


Exporting a certificate for Office 365 ADFS setup

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.

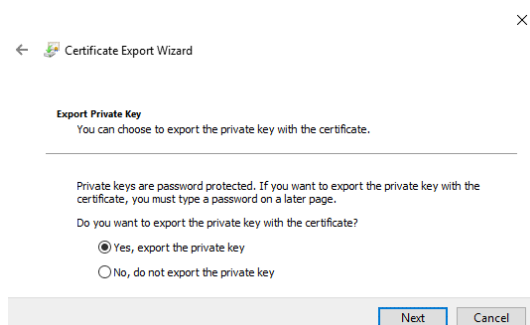
Go to **Personal > Certificates**, select your certificate. In our example, the selected certificate is *officedomain-WIN2016DC-CA*. Right click the certificate and in the context menu, select **All Tasks > Export**.



The Certificate Export Wizard opens.

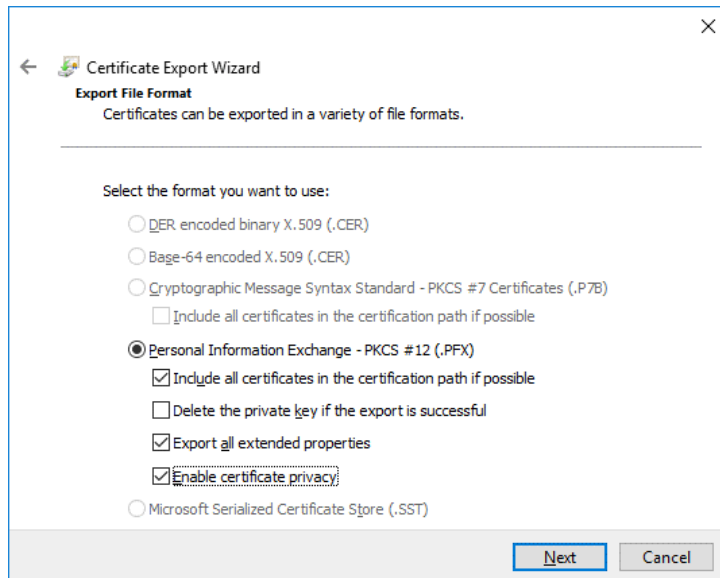
Welcome to the Certificate Export Wizard. This is the first step of the wizard used for introduction. There is nothing to configure and you can click **Next** to continue.

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

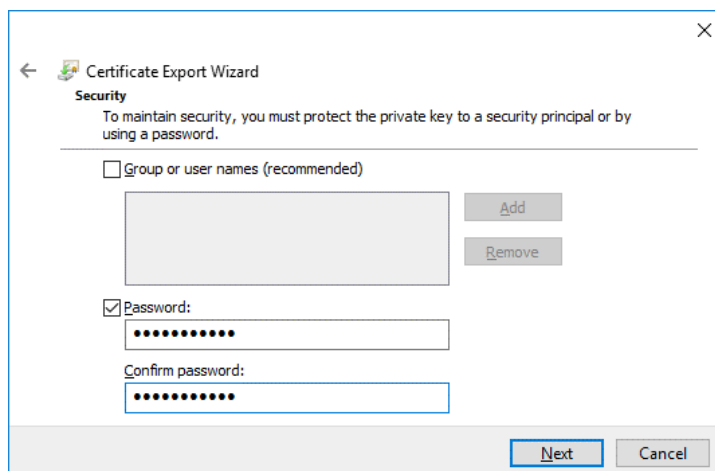


Export File Format. Select *Personal Information Exchange — PKCS #12 (.PFX)* as the file format. Then select the following checkboxes:

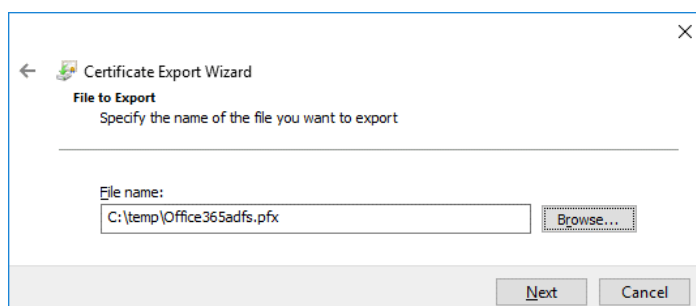
- Include all certificates in the certification path if possible
- Export all extended properties
- Enable certificate privacy



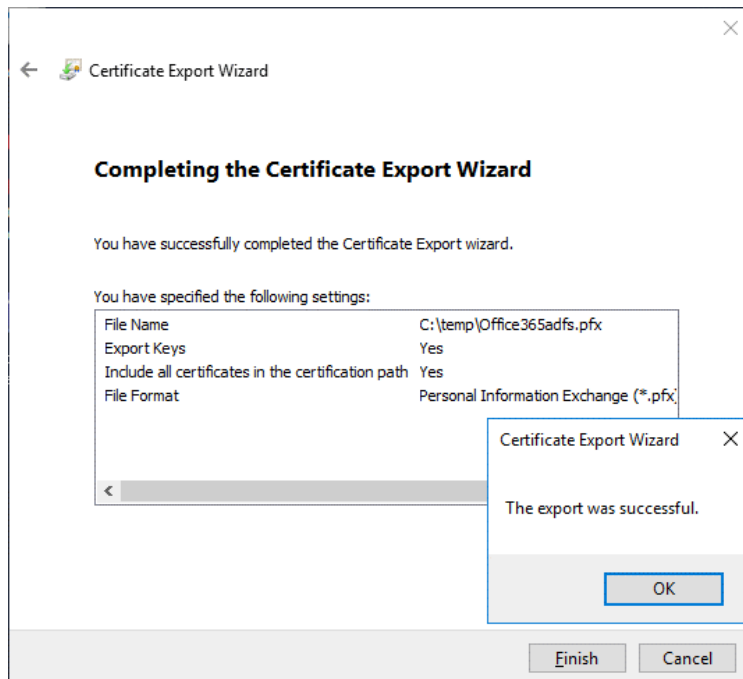
Security. Select the **Password** checkbox, enter your password and confirm your password.



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*



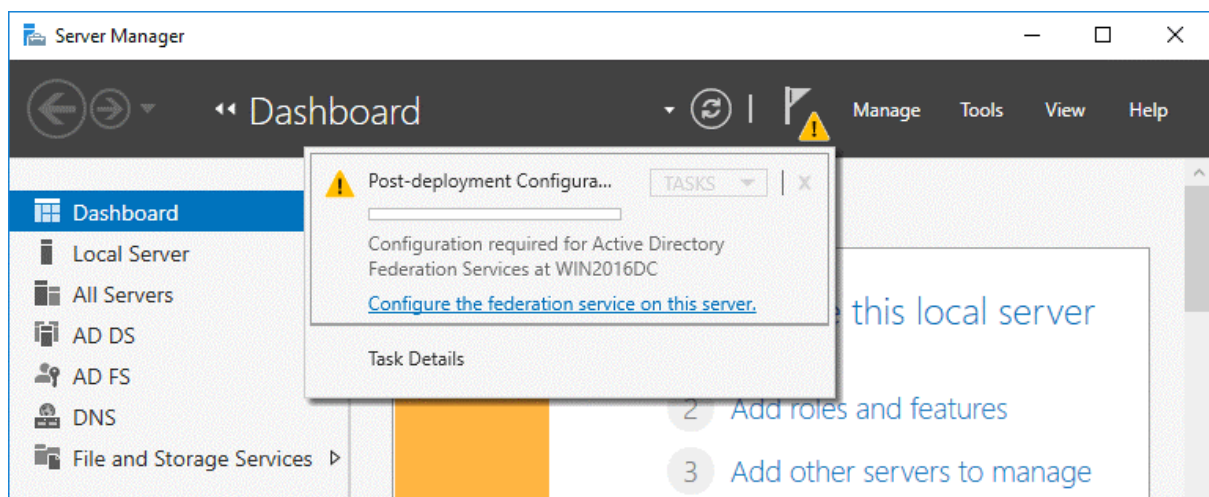
Completing the Certificate Export Wizard. Now everything is ready for export. Hit **Finish** to export the certificate. The export was successful. Click **OK** to close the window.



Configuring ADFS for Office 365

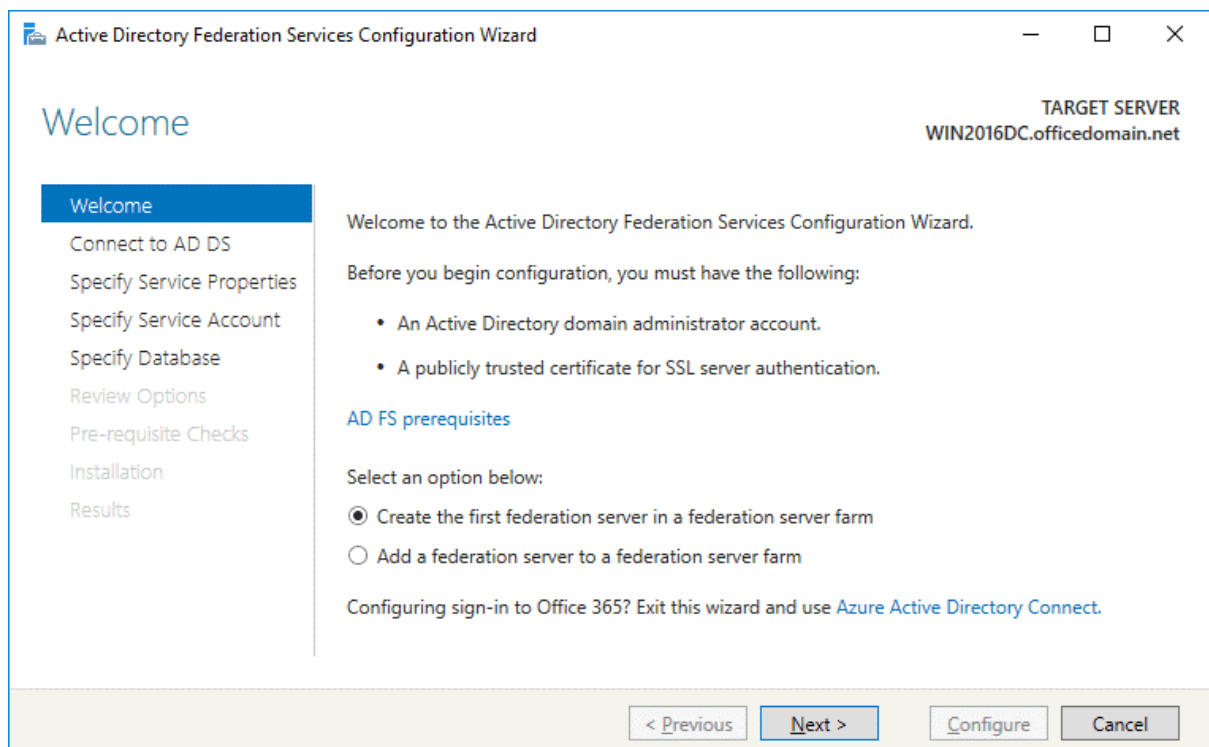
After installing the ADFS role and creating/exporting a certificate, you can resume Office 365 ADFS setup.

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.

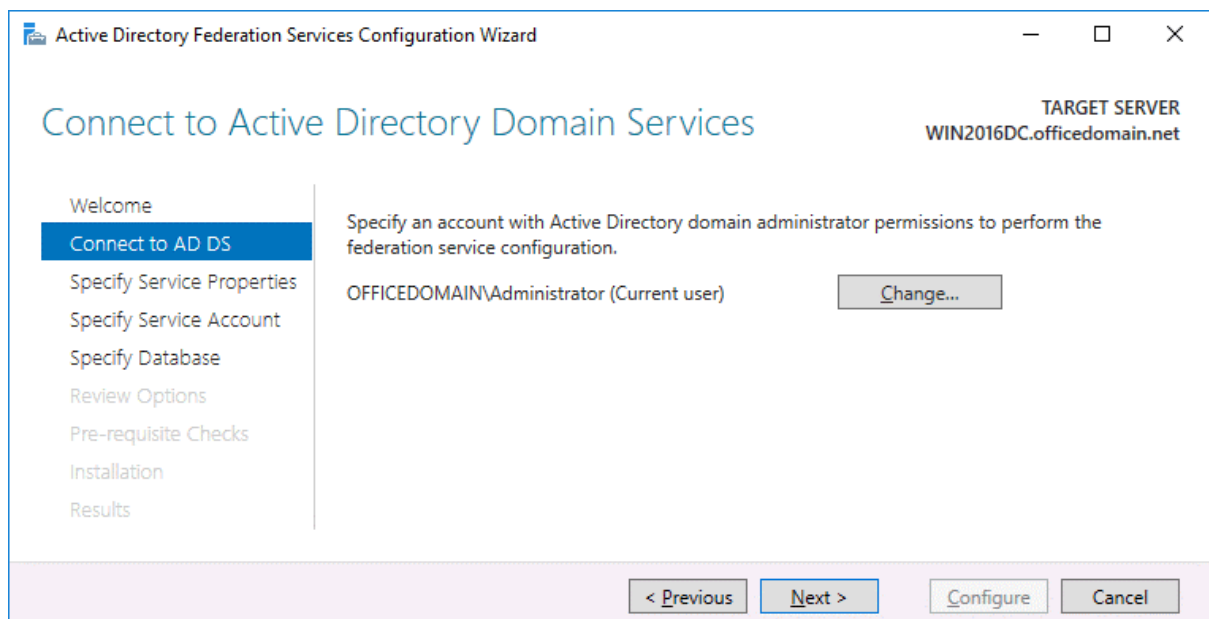


The Active Directory Federation Services Configuration Wizard opens.

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).

The screenshot shows the 'Specify Service Properties' step of the 'Active Directory Federation Services Configuration Wizard'. The 'TARGET SERVER' is 'WIN2016DC.officedomain.net'. The left sidebar lists steps: Welcome, Connect to AD DS, Specify Service Properties (selected), Specify Service Account, Specify Database, Review Options, Pre-requisite Checks, Installation, and Results. The main area contains three fields: 'SSL Certificate' with a dropdown set to 'win2016dc.officedomain.net' and an 'Import...' button; 'Federation Service Name' with a dropdown set to 'certauth.officedomain.net' and an example 'fs.contoso.com'; and 'Federation Service Display Name' with a text box containing 'adfs.officedomain.net' and an example 'Contoso Corporation'. At the bottom are buttons for '< Previous', 'Next >', 'Configure', and 'Cancel'.

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).

The screenshot shows the 'Specify Service Account' step of the 'Active Directory Federation Services Configuration Wizard'. The 'TARGET SERVER' is 'WIN2016DC.officedomain.net'. A warning message at the top states: 'Group Managed Service Accounts are not available because the KDS Root Key has not been set. Use the foll... Show more'. The left sidebar lists steps: Welcome, Connect to AD DS, Specify Service Properties, Specify Service Account (selected), Specify Database, Review Options, Pre-requisite Checks, Installation, and Results. The main area has two radio buttons: 'Create a Group Managed Service Account' (unselected) and 'Use an existing domain user account or group Managed Service Account' (selected). Below the second radio button is a 'Select...' button. A 'Select User or Service Account' dialog box is open, showing 'User or Service Account' selected, 'From this location: officedomain.net', and 'Enter the object name to select (examples): adfsrv'. The dialog box has 'OK', 'Cancel', and 'Advanced...' buttons. At the bottom of the wizard are buttons for '< Previous', 'Next >', 'Configure', and 'Cancel'.

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:

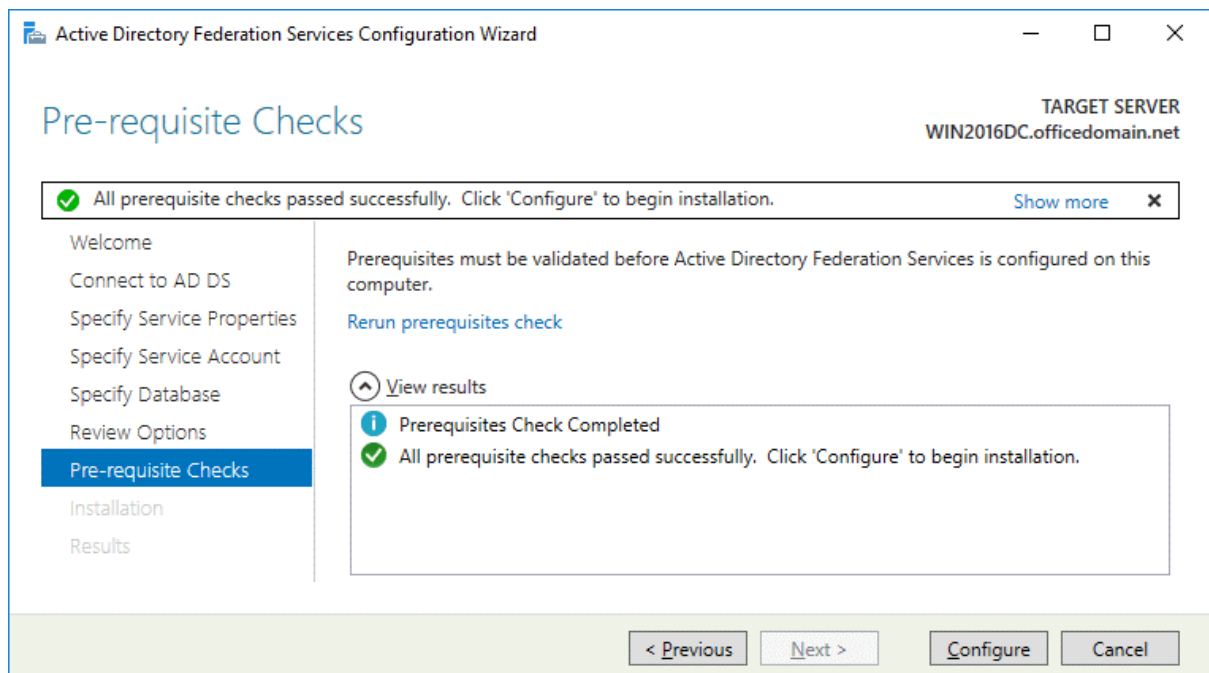
Create a database on this server using Windows Internal Database.

The screenshot shows the 'Specify Configuration Database' step of the 'Active Directory Federation Services Configuration Wizard'. The window title is 'Active Directory Federation Services Configuration Wizard'. On the right, it says 'TARGET SERVER WIN2016DC.officedomain.net'. On the left, a navigation pane lists steps: Welcome, Connect to AD DS, Specify Service Properties, Specify Service Account, Specify Database (highlighted), Review Options, Pre-requisite Checks, Installation, and Results. The main area has the heading 'Specify a database to store the Active Directory Federation Service configuration data.' and two radio button options: 'Create a database on this server using Windows Internal Database.' (selected) and 'Specify the location of a SQL Server database.' Below these are input fields for 'Database Host Name:' and 'Database Instance:'. A note says 'To use the default instance, leave this field blank.' At the bottom are buttons: '< Previous', 'Next >', 'Configure', and 'Cancel'.

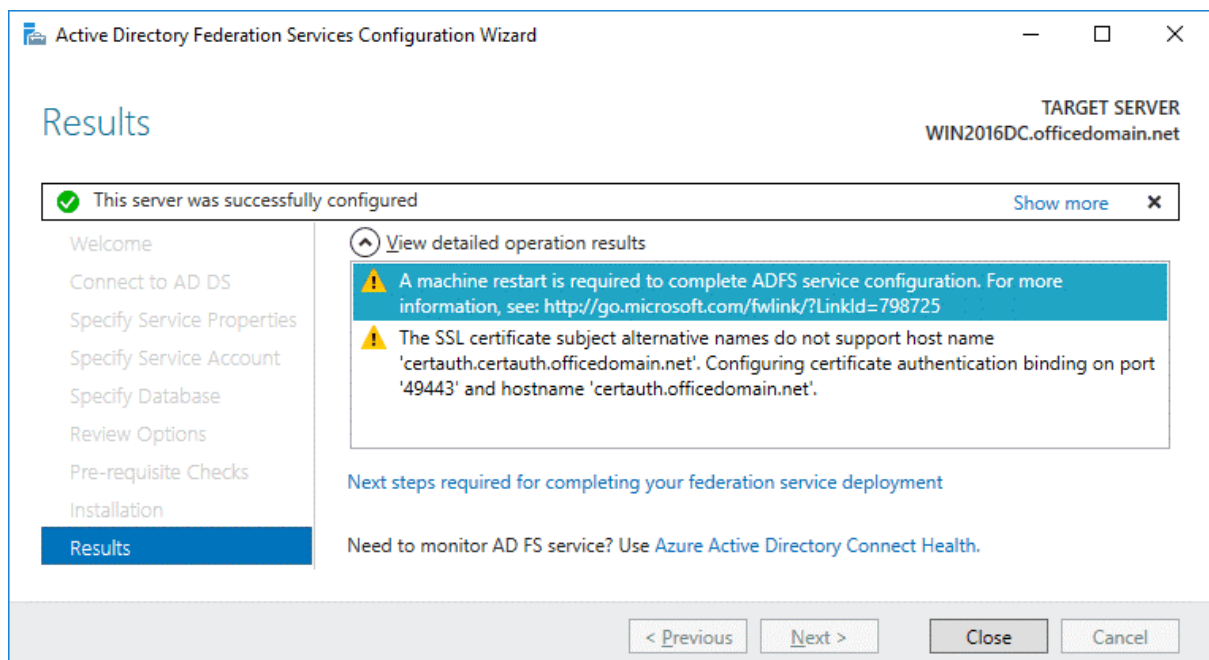
Review Options. Review your options. You can click **View script** and save the configuration script. This may be useful if you want to deploy multiple Active Directory Federation Servers.

The screenshot shows the 'Review Options' step of the 'Active Directory Federation Services Configuration Wizard'. The window title is 'Active Directory Federation Services Configuration Wizard'. On the right, it says 'TARGET SERVER WIN2016DC.officedomain.net'. On the left, the navigation pane is the same as the previous step, but 'Review Options' is now highlighted. The main area has the heading 'Review your selections:' and a text box containing: 'This server will be configured as the primary server in a new AD FS farm 'certauth.officedomain.net'.', 'AD FS configuration will be stored in Windows Internal Database.', 'Windows Internal Database feature will be installed on this server if it is not already installed.', and 'Federation service will be configured to run as OFFICEDOMAIN\adfssrv.'. Below this text box, it says 'These settings can be exported to a Windows PowerShell script to automate additional installations' and there is a 'View script' button. At the bottom are buttons: '< Previous', 'Next >', 'Configure', and 'Cancel'.

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