

Mi-Token

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

Mi-Token version 1.0.0. Document version 1, June 2019. © 2019 Mi-Token Inc. All rights reserved.

© 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.

🚔 Add Roles and Features Wizar	d	_		×
Select installation	n type	DESTIN/ WIN2016DC.off	ATION SER\ ficedomain.	VER .net
Before You Begin	Select the installation type. You can install roles and features on a running p machine, or on an offline virtual hard disk (VHD).	hysical comput	ter or virt	ual
Server Selection	Role-based or feature-based installation Configure a single server by adding roles, role services, and features.			
Server Roles Features	 Remote Desktop Services installation Install required role services for Virtual Desktop Infrastructure (VDI) to create the services of the services	eate a virtual m	achine-b	ased
Confirmation Results	or session-based desktop deployment.			
	< <u>P</u> revious <u>Next</u> >	Install	Cance	el

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).

🚘 Add Roles and Features Wizar	rd			_		×
Select destinatio	n server			DESTIF WIN2016DC.c	NATION SER fficedomain	VER .net
Before You Begin Installation Type	Select a server or a virtual hard o	lisk on which to ins er pool	tall roles and features.			
Server Selection	O Select a virtual hard disk					
Server Roles	Server Pool					
Features						
Confirmation	Filter:					
Results	Name	IP Address	Operating System			
	WIN2016DC.officedomain.net	192.168.101.101	Microsoft Windows Se	rver 2016 Star	ndard	
	1 Computer(s) found]
	This page shows servers that are and that have been added by us newly-added servers from which	running Windows ing the Add Server data collection is s	Server 2012 or a newer i s command in Server Ma till incomplete are not s	release of Win anager. Offline hown.	dows Serv servers ar	er, nd
		< <u>P</u> revious	<u>N</u> ext >	Install	Cance	el

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

🔁 Add Roles and Features Wizard			– 🗆 X
Select server roles			DESTINATION SERVER WIN2016DC.officedomain.net
Before You Begin Installation Type Server Selection Server Roles Features AD FS Confirmation Results	Select one or more roles to install on the selected server. Roles Active Directory Certificate Services Active Directory Domain Services (Installed) Active Directory Certificate Services Active Directory Lightweight Directory Services Active Directory Rights Management Services Active Directory Rights Management Services Active Directory Rights Management Services Device Health Attestation DHCP Server DNS Server (Installed) Fax Server File and Storage Services (2 of 12 installed) Host Guardian Service Network Policy and Access Services Remote Desktop Services Volume Activation Services Volume Activation Services Volume Activation Services Volume Activation 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.
	Windows Deployment Services	∨ <u>V</u> ext	> Install Cancel



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

📥 Add Roles and Features Wizard		– 🗆 X
Select features		DESTINATION SERVER WIN2016DC.officedomain.net
Before You Begin	Select one or more features to install on the selected server.	
Installation Type	Features	Description
Server Selection	NET Framework 3.5 Features	.NET Framework 3.5 combines the
Server Roles	 .NET Framework 4.6 Features (2 of 7 installed) 	power of the .NET Framework 2.0
Features	Background Intelligent Transfer Service (BITS)	APIs with new technologies for building applications that offer
AD ES	BitLocker Drive Encryption	appealing user interfaces, protect
Confirmation	BranchCache	your customers' personal identity
Commation	Client for NFS	information, enable seamless and secure communication, and provide
Results	Containers Data Center Bridging	the ability to model a range of
	Direct Play	business processes.
	Enhanced Storage	
	Failover Clustering	
	Group Policy Management (Installed)	
	Internet Printing Client	
	IP Address Management (IPAM) Server	
	iSNS Server service	
	· /	
	< <u>P</u> revious <u>N</u> ext	> Install Cancel

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.

📥 Add Roles and Features Wizard

 \times

mi •token

DESTINATION SERVER

Confirm installa	tion selections Destination server WIN2016DC.officedomain.net
Before You Begin	To install the following roles, role services, or features on selected server, click Install.
Installation Type	Restart the destination server automatically if required
Server Selection	Optional features (such as administration tools) might be displayed on this page because they have
Server Roles	been selected automatically. If you do not want to install these optional features, click Previous to cle- their check boxes.
Features	
AD FS	Active Directory Federation Services
Results	If a restart is required, this server restarts automatically, without additional notifications. Do you want to allow automatic restarts?
	Export configuration settings Specify an alternate source path
	< Previous Next > Install Cancel

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

🚘 Add Roles and Features Wizard		_		×
Installation progre	255	DESTIN WIN2016DC.of	ATION SER ficedomain	VER .net
Before You Begin	View installation progress			
Installation Type	Feature installation			
Server Selection				
Server Roles	Installation started on WIN2016DC.officedomain.net			
Features	Active Directory Federation Services			
AD FS				
Confirmation				
Results	You can close this wizard without interrupting running tasks. View page again by clicking Notifications in the command bar, and ther Export configuration settings	task progress or 1 Task Details.	open this	5
	< <u>P</u> revious <u>N</u> ext >	Close	Cance	el

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).

ᡖ Add Roles and Features Wizard		- 🗆 X
Select features Before You Begin Installation Type Server Selection Server Roles	Select one or more features to install on the selected server. Features NET Framework 3.5 Features NET Framework 4.6 Features (2 of 7 installed)	DESTINATION SERVER WIN2016DC.officedomain.net Description .NET Framework 3.5 combines the power of the .NET Framework 2.0
Features AD CS Role Services Confirmation Results	Background Intelligent Transfer Service (BITS) BitLocker Drive Encryption BitLocker Network Unlock BranchCache Client for NFS Containers Data Center Bridging Direct Play Enhanced Storage Failover Clustering Group Policy Management (Installed) I/O Quality of Service IIS Hostable Web Core Internet Printing Client IP Address Management (IPAM) Server iSNS Server service LPR Port Monitor	APIs with new technologies for building applications that offer appealing user interfaces, protect your customers' personal identity information, enable seamless and secure communication, and provide the ability to model a range of business processes.
	< <u>P</u> revious <u>N</u> ext :	> Install Cancel

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

📥 Add Roles and Features Wizard		_		×
Active Directory C Before You Begin Installation Type Server Selection Server Roles Features AD CS Role Services Confirmation Results	Certificate Services Active Directory Certificate Services (AD CS) provides the certificate infrastrus such as secure wireless networks, virtual private networks, Internet Protocol Access Protection (NAP), encrypting file system (EFS) and smart card log on. Things to note: • The name and domain settings of this computer cannot be changed after (CA) has been installed. If you want to change the computer name, join a server to a domain controller, complete these changes before installing the information, see certification authority naming.	DESTINA WIN2016DC.off Jecture to enable Security (IPSec) r a certification a domain, or pro he CA. For more	ation SERV ceedomain. scenario), Networf authority mote this	/ER is k
	< <u>P</u> revious <u>Next</u> >	Install	Cance	4



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

📥 Add Roles and Features Wizard		– 🗆 X
Select role service Before You Begin Installation Type Server Selection Server Roles Features AD CS Role Services Confirmation Results	Select the role services to install for Active Directory Certifices Role services Certification Authority Certificate Enrollment Policy Web Service Certificate Enrollment Web Service Certification Authority Web Enrollment Network Device Enrollment Service Online Responder	DESTINATION SERVER WIN2016DC.officedomain.net cate Services Description 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.
	< <u>P</u> revious	lext >Install Cancel

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

🚘 Add Roles and Features Wizard		_		Х
Confirm installation	on selections	DESTINA WIN2016DC.offi	TION SERV cedomain.	'ER net
Before You Begin	To install the following roles, role services, or features on selected server, clic	k Install.		
Installation Type	Restart the destination server automatically if required			
Server Selection	Optional features (such as administration tools) might be displayed on this p	age because th	ney have	
Server Roles	been selected automatically. If you do not want to install these optional featu their check boxes.	ures, click Previ	ous to cl	ear
Features				
AD CS	Active Directory Certificate Services			^
Role Services	Certification Authority			
Confirmation	Certification Authority Web Enrollment			
Continuation	Remote Server Administration Tools			
	Role Administration Tools			
	Active Directory Certificate Services Tools			
	Certification Authority Management Tools			
	Web Server (IIS)			
	Management Tools			
	IIS 6 Management Compatibility			
	100 C M			v
	Export configuration settings Specify an alternate source path			
	< <u>P</u> revious <u>N</u> ext >	<u>I</u> nstall	Cance	I

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.

📥 AD CS Configuration	- 🗆 X
Credentials	DESTINATION SERVER WIN2016DC.officedomain.net
Credentials Role Services	Specify credentials to configure role services
Confirmation Progress Results	To install the following role services you must belong to the local Administrators group: Standalone certification authority Certification Authority Web Enrollment Online Responder To install the following role services you must belong to the Enterprise Admins group: Enterprise certification authority Certificate Enrollment Policy Web Service Certificate Enrollment Web Service Network Device Enrollment Service Credentials: OFFICEDOMAIN\Administrator <u>Change</u> More about AD CS Server Roles
	< <u>Previous</u> <u>Next</u> > <u>Configure</u> Cancel

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

📥 AD CS Configuration		_		×
Role Services		DESTINAT WIN2016DC.offic	ION SER	VER .net
Credentials	Select Role Services to configure			
Role Services Setup Type CA Type Private Key Cryptography CA Name Validity Period Certificate Database Confirmation Progress Results	 Certification Authority Certification Authority Web Enrollment Online Responder Network Device Enrollment Service Certificate Enrollment Web Service Certificate Enrollment Policy Web Service 			
NCSURS	More about AD CS Server Roles			
	< <u>P</u> revious <u>N</u> ext >	Configure	Cance	:1



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.

📥 AD CS Configuration			_		×
Cryptography for	CA		DESTINA WIN2016DC.offic	TION SER	VER .net
Credentials Role Services	Specify the cryptographic options				
Setup Type	Select a <u>c</u> ryptographic provider:		Key length:		
CA Type	RSA#Microsoft Software Key Storage Provider	¥	2048		~
Private Key	Select the bash algorithm for signing certificates issued by thi	s CA:			
Cryptography	SHA256	^]		
CA Name	SHA384				
Validity Period	SHA512				
Certificate Database	SHA1				
Confirmation	MD5	~			
Progress	☐ <u>A</u> llow administrator interaction when the private key is ac	cessed	by the CA.		
Results					
	More about Cryptography				
	< <u>P</u> revious <u>Next</u> >		<u>C</u> onfigure	Cance	2



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

📥 AD CS Configuration		-		×
CA Name	,	DESTINAT WIN2016DC.offic	ION SER edomain	VER .net
Credentials Role Services	Specify the name of the CA			
Setup Type CA Type	Type a common name to identify this certification authority (CA). This certificates issued by the CA. Distinguished name suffix values are au be modified.	s name is added t tomatically gener	o all ated but	can
Private Key Cryptography	<u>C</u> ommon name for this CA: officedomain-WIN2016DC-CA]		
Validity Period	Distinguished name suffix:	1		
Certificate Database Confirmation	DC=officedomain,DC=net			
Progress	Preview of distinguished name: CN=officedomain-WIN2016DC-CA,DC=officedomain,DC=net]		
ncono	More about CA Name			
	< <u>P</u> revious <u>N</u> ext >	Configure	Cance	<u>!</u>

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



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
------------------------------------	-----------------------------

📥 AD CS Configuration		_		×
CA Database		DESTINAT WIN2016DC.offic	ION SER	VER .net
Credentials Role Services	Specify the database locations			
Setup Type	Certificate database location:	7		
CA type Private Key Cryptography CA Name	C <u>e</u> rtificate database log location: C:\Windows\system32\CertLog]		
Validity Period Certificate Database				
Confirmation				
Progress				
Results	More about CA Database			
	< <u>P</u> revious <u>N</u> ext >	Configure	Cance	1

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.

AD CS Configuration		- 0
Results		DESTINATION SERVE WIN2016DC.officedomain.ne
Credentials	The following roles, role services, or features v	vere configured:
Role Services	Active Directory Certificate Services	
Setup Type	Certification Authority	Configuration succeeded
СА Туре	More about CA Configuration	
Private Key		
Cryptography	More about Web Enrollment Configuration	Configuration succeeded
CA Name		
Validity Period		
Certificate Database		
Confirmation		
Progress		
Results		
	< Previous	s Next > Close Cancel

Editing a certificate template

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

💷 Run		×
۸	Type the name of a program, folder, document, or Internet resource, and Windows will open it for you.	
<u>O</u> pen:	certsrv.msc ~ This task will be created with administrative privileges.	
	OK Cancel <u>B</u> rowse]

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

🚡 certsrv - [Certification Authority (Local)\officedomain-WIN2016DC-CA\Certificate Templates] -							
File Action View Help							
🗢 🔿 🙍 🧟 👔							
 Certification Authority (Local) officedomain-WIN2016DC-CA Revoked Certificates Issued Certificates Pending Requests Failed Requests Certificate Templates 	Name Directory Email Domain Contro Kerberos Authe EFS Recovery A Basic EFS	Replication Iler Authentication ntication gent	Intended Purpose Directory Service Email Replication Client Authentication, Server Authentic Client Authentication, Server Authentic File Recovery Encrypting File System				
	Manage	Client Authentication, Server Authentic					
	New >		Client Authentication, Server Authentic				
	View >	-fication Authority	Encrypting File System, Secure Email, Cl < All>				
	Refresh Export List		Microsoft Trust List Signing, Encrypting				
	Help						
< >							
Starts Certificate Templates snapin							

Starts Certificate Templates snapin

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

🚇 Certificate Templates Console						
File Action View Help						
🗢 🄿 📰 🗐 🔒 👔 🗖						
Certificate Templates (WIN2016I	Template Display Na	me	Sche	ma Version	Version	Intended Purp
	🗷 Router (Offline red	quest)	1		4.1	
	Smartcard Log	Duplicate Template			6.1	
	Smartcard Us	- apricate remplate			11.1	
	🚇 Subordinate C	All Tasks	>		5.1	
	🚇 Trust List Sign	Properties			3.1	
	🗷 User	roperties			3.1	
	🗷 User Signatur	Help			4.1	
	Web Server		1		4.1	
	Representation Author	entication	2		101.0	Client Authent

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 Office 365 ADFS 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).

Properties of New Temp	plate		×	Properties of	New Tem	plate			×
Subject Name	Server	Issuance F	Requirements	Subject N	lame	Sen	ver	Issuance F	Requirements
Superseded Templa	ites E	xtensions	Security	Compatibility	General	Request	Handling	Cryptography	Key Attestation
Compatibility General	Request Handlin	g Cryptography	Key Attestation	Supersec	ded Templa	ates	Exte	ensions	Security
Template display name				<u>G</u> roup or use	rnames:				
Office365ADFS				Authen Adminis & Domain & Enterpri	ticated Use trator Admins (C ise Admins	FFICEDO	MAIN\Dor OMAIN\E	nain Admins) Interprise Admins	s)
Office365ADFS									
Validity period: 5 years Publish certificate in Do not automation Directory	Active Directory	wal period: 8 weeks ~ plicate certificate) exists in Active	Permissions : Full Contro Read Write Enroll Autoenroll	for Authent	iicated Use	ers	Add Allow	Remove Deny
				For special p Advanced.	emissions	or advanc	ed setting	s, click	Ad <u>v</u> anced

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

🤖 c	🙀 certsrv - [Certification Authority (Local)\officedomain-WIN2016DC-CA\Certificate Templates] —						
File	Action View Help						
(= =	Manage						
🚡 C	New >	Certificate Template to Issue	Intended Purpose				
× 🗃	Refresh Export List Help Certificate Templates	Cr Image: Control of the state of the	Directory Service Email Replication Client Authentication, Server Authentic Client Authentication, Server Authentic File Recovery Encrypting File System Client Authentication, Server Authentic Server Authentication Client Authentication, Server Authentic Encrypting File System, Secure Email, Cl <all> Microsoft Trust List Signing, Encrypting</all>				
Enable	additional Certificate Temp	lates on this Certification Authority					

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

Enable Certificate Templates		×
Select one Certificate Template to enable on th Note: If a certificate template that was recently information about this template has been replica All of the certificate templates in the organizatio For more information, see <u>Certificate Tem</u>	is Certification Authority. created does not appear on this list, you may need to wait until ated to all domain controllers. n may not be available to your CA. <u>plate Concepts.</u>	
Name	Intended Purpose	^
Rey Recovery Agent	Key Recovery Agent	
Response Signing	OCSP Signing	
🚇 Office365ADFS	Server Authentication	
RAS and IAS Server	Client Authentication, Server Authentication	
Router (Offline request)	Client Authentication	
R Smartcard Logon	Client Authentication, Smart Card Logon	
R Smartcard User	Secure Email, Client Authentication, Smart Card Logon	
🚇 Trust List Signing	Microsoft Trust List Signing	
User Signature Only	Secure Email, Client Authentication	
Reference Workstation Authentication	Client Authentication	¥
	OK Cance	al

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

image: certsrv - [Certification Authority (Local)\officedomain-WIN2016DC-CA\Certificate Templates] — File Action View Help					
← ➡ 2 X B L I	Name	Intended Purpose			
 Revoked Certificates Issued Certificates Pending Requests Failed Requests Certificate Templates 	Our Cestor Autors Our Cestor Autors Our Cestor Autor Controller Authentication Our Controller Authentication Ers Recovery Agent Basic EFS Domain Controller Web Server Computer User Subordinate Certification Authority Administrator	Directory Service Email Replication Client Authentication, Server Authentic Client Authentication, Server Authentic File Recovery Encrypting File System Client Authentication, Server Authentic Server Authentication Client Authentication, Server Authentic Encrypting File System, Secure Email, Cl <all> Microsoft Trust List Signing, Encrypting</all>	I		
< >					



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.

	_		Х
Certificate Enrollment			
Select Certificate Enrollment Policy			
Certificate enrollment policy enables enrollment for certificates based on predefi Certificate enrollment policy may already be configured for you.	ned certificate	e template	25.
Configured by your administrator			
Active Directory Enrollment Policy			~
Configured by you		Add N	ew
	<u>N</u> ext	Cano	cel

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

		_		×
🛱 Certificate Enrollment				
Request Certificates				
You can request the following ty click Enroll.	pes of certificates. Select the certificates you want	to request,	and then	
Kerberos Authentication	i) STATUS: Available	[Details 🗸	^
Office365ADFS	icquired to enroll for this certificate. Click here to	[configure s	Details 🔺 ettings.	
The following options desc Key usage: E Application policies: S	ribe the uses and validity period that apply to this Digital signature Key encipherment Server Authentication	type of cert	tificate:	
Validity period (days): 1	825	<u>P</u> rop	oerties	•
Show <u>a</u> ll templates				
		<u>E</u> nroll	Can	cel

The Certificate Properties window opens. In the **Subject** tab, find the **Subject name** section and, in the dropdown 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

icate Properties	× Certificate Properties
Subject General Extensions Private Key Certification Authority Signature	A Subject General Extensions Private Key Certification Authority Signature
subject of a certificate is the user or computer to which the certificate is issued. You enter information about the types of subject name and alternative name values that be used in a certificate.	The subject of a certificate is the user or computer to which the certificate is issued. You can enter information about the types of subject name and alternative name values that can be used in a certificate.
ject of certificate	Subject of certificate
user or computer that is receiving the certificate	The user or computer that is receiving the certificate
ject name:	Subject name:
De:	Type: CN=win2016dc.officedomain
mmon name 🗸 Add >	Common name V Add >
ue:	Value:
in2016dc.officedomain.ne	< nemove (
rnative name:	Alternative name:
pe:	Type: DNS
rectory name 🗸 🗸	DNS ~ enterpriseregistration.officed
ue:	Value: certauth.officedomain.net
Add >	Add >
< Remove	< Remove
	< >>
OK Cancel Analy	OK Cancel Apply



Note: A certificate must support EKU 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 EKU. 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.

ertificate Pr	operties					
<u> Subject</u>	General	Extensions	Private Key	Certification Authority	Signature	
<u>C</u> ryptogra	phic Serv	ice Provider				*
Key <u>o</u> ption	ns					^
Set the key	length a	nd export op	tions for the	private key.		
Key size:	2048			~		
✓ Make pr	ivate key	exportable				
Allow pr	rivate key	to be archiv	ed			
Strong p	orivate key	y protection				
Key <u>t</u> ype						
Key <u>p</u> ermi	ssions					
				OK Ca	ancel	Apply

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

🔄 Certificate Enrollment		_		×
Request Certificates				
You can request the following ty click Enroll.	pes of certificates. Select the certificates you want	to request, a	and then	
Kerberos Authentication	i) STATUS: Available	D	etails 🗸	^
✓ Office365ADFS The following options desc Key usage: C K Application policies: S Validity period (days): 1	(i) STATUS: Available ribe the uses and validity period that apply to this Digital signature (ey encipherment erver Authentication 825	D type of certi <u>P</u> rope	etails A ficate: erties]
Administrator	X STATUS: Unavailable			~
✓ Show <u>all templates</u>				
	l	<u>E</u> nroll	Car	ncel

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

			_		×
🗐 C	ertificate Enrollment				
	Certificate Installation R	esults			
	The following certificates have	been enrolled and installed on this computer.			
	Active Directory Enrollment	t Policy			
	✓ Office365ADFS	STATUS: Succeeded		Details	•
				Fin	ish

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**.

🚟 certlm - [Certificates - Local Con	nputer\Personal\Certificates]			— C) ×
File Action View Help					
🗢 🔿 🖄 📅 🤞 🗙 🛛	1 🔒 🛛 🖬				
Certificates - Local Computer 🔨	Issued To	Issued By		Expiration Date	Intended I
V Personal	🔄 GlobalSign	GlobalSign		3/18/2029	Server Aut
Certificates	🙀 officedomain-WIN2016DC-CA	officedomain-WIN201	6DC-CA	3/19/2025	<all></all>
Certificates	🖏 win2016dc.officedomain.net	Open	DC-CA	3/19/2022	Server Aut
Enterprise Trust		All Tasks >	Open		
✓ ☐ Intermediate Certification					
Certificate Revocation		Cut	Reque	st Certificate with N	lew Key
Certificates		Сору	Renew	Certificate with Ne	w Key
> Intersection of the section of		Delete	Maria	Director Kours	
> 🧾 Untrusted Certificates			ivianag	e Private Keys	
> 🧾 Third-Party Root Certifica		Properties	Advan	ced Operations	
> 🧮 Trusted People		Halp	Export		
> 📔 Client Authentication Issu		ricik.	C.port.		

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.

		×
←	😺 Certificate Export Wizard	
	Export Private Key	
	You can choose to export the private key with the certificate.	
	Private keys are password protected. If you want to export the private key with the certificate, you must type a password on a later page.	
	Do you want to export the private key with the certificate?	
	• Yes, export the private key	
	○ No, do not export the private key	
	Next Cancel	

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



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

Export File Format Certificates can be exported in a variety of file formats.	
Select the format you want to use:	
◯ <u>D</u> ER encoded binary X.509 (.CER)	
O Bage-64 encoded X.509 (.CER)	
◯ Cryptographic Message Syntax Standard - PKCS #7 Certificates (.P7B)	
Include all certificates in the certification path if possible	
Personal Information Exchange - PKCS #12 (.PFX)	
\checkmark Include all certificates in the certification path if possible	
Delete the private key if the export is successful	
Export all extended properties	
◯ Microsoft Serialized Certificate Store (.SST)	

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

		Х
\leftarrow	🝜 Certificate Export Wizard	
	Security To maintain security, you must protect the private key to a security principal or by using a password.	
	Group or user names (recommended)	
	Add	
	Remove	
	✓ Password:	
	•••••	
	Confirm password:	
	•••••	
	<u>N</u> ext Cance	I

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*

	×
🗧 嵾 Certificate Export Wizard	
File to Export	
Specify the name of the file yo	u want to export
<u>F</u> ile name:	
C:\temp\Office365adfs.pfx	Browse
	Next Cancel
	<u>N</u> ext Cancel

mi • token © 2019 Mi-Token: Configuring ADFS for Office 365: a Step-By-Step Guide 23

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.

← 🛿 ← Frificate Export Wizard	×
Completing the Certificate Ex	port Wizard
You have successfully completed the Certificate	e Export wizard.
File Name Export Keys Include all certificates in the certification path File Format	C:\temp\Office365adfs.pfx Yes Yes Personal Information Exchange (*.pfx
<	Certificate Export Wizard X The export was successful.
	ОК
	<u>F</u> inish Cancel

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.

🚘 Server Manager				- C	x נ
💮 🕘 🔹 애 Dash	nboard - 🗷 I 🍢	Manage	− □ Tools View He local server reatures ers to manage	Help	
Dashboard	Post-deployment Configura TASKS TASKS X Configuration required for Active Directory				^
Local Server All Servers AD DS	Federation Services at WIN2016DC Configure the federation service on this server.	this lo	cal se	erver	
AD FS	Task Details	es and fea	atures		
File and Storage Services	Add oth	ner server:	s to ma	anage	



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.

🚘 Active Directory Federation Serv	ices Configuration Wizard – 🗆 🗙
Welcome	TARGET SERVER WIN2016DC.officedomain.net
Welcome Connect to AD DS Specify Service Properties Specify Service Account Specify Database Review Options Pre-requisite Checks Installation Results	 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.
	< <u>Previous</u> <u>Next ></u> <u>Configure</u> Cancel

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.

📥 Active Directory Federation Serv	ices Configuration Wizard	-		×
Connect to Active	e Directory Domain Services WIN2016	TAI DC.offic	RGET SEF edomair	VER n.net
Welcome Connect to AD DS	Specify an account with Active Directory domain administrator permissions to federation service configuration.	perform	the	
Specify Service Properties	OFFICEDOMAIN\Administrator (Current user)]		
Specify Service Account		1		
Specify Database				
Review Options				
Pre-requisite Checks				
Installation				
Results				
	< <u>P</u> revious <u>N</u> ext > <u>C</u> onfig	jure	Cance	ł

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).

📥 Active Directory Federation Ser	vices Configuration Wizard	– 🗆 X
Specify Service P	roperties	TARGET SERVER WIN2016DC.officedomain.net
Welcome Connect to AD DS Specify Service Properties	SSL Certificate:	win2016dc.officedomain.net v Import
Specify Service Account Specify Database	Federation Service Name:	certauth.officedomain.net v Example: fs.contoso.com
Review Options Pre-requisite Checks Installation	Federation Service Display Name:	adfs.officedomain.net Users will see the display name at sign in.
Results		Example: Contoso Corporation
	<	Previous Next > Configure 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 *adfssrv* account was created in the beginning of this this walkthrough).

Specify Service A	ccount			TA WIN2016DC.offi	RGET SERVE cedomain.ne
Group Managed Service Ad	counts are not available b	ecause the KDS Root Ke	ey has not been set. Us aged Service Account.	se the foll Show	more X
Connect to AD DS Specify Service Properties	Create a Group Ma	naged Service Account			
Specify Service Account	Account Name:	OFFIC			
Review Options	 Use an existing dor Account Name: 	main user account or gr * <not< td=""><td>oup Managed Service</td><td>Account</td><td>Select</td></not<>	oup Managed Service	Account	Select
elect User or Service Account		×			
User or Service Account		Object Types			
rom this location: officedomain.net		Locations			
Enter the object name to select (<u>exam</u> adfssrv	i <mark>ples</mark>):	Check Names			
Advanced	0	K 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.

📥 Active Directory Federation Serv	ices Configuration Wizard				-		×
Specify Configura	tion Database			WIN201	TAI I6DC.offic	RGET SEF cedomair	RVER n.net
Welcome Connect to AD DS Specify Service Properties Specify Service Account Specify Database	Specify a database to store the Create a database on this Specify the location of a S Database Host Name:	he Active Directory Fo s server using Window SQL Server database.	ederation Servi ws Internal Dat	ce configurat abase.	tion data.		
Review Options Pre-requisite Checks Installation Results	Database Instance:	To use th	ne default insta	nce, leave this	s field bla	nk.	
		< <u>P</u> revious	<u>N</u> ext >	<u>C</u> onfi	gure	Cance	ł

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.

📥 Active Directory Federation Serv	ices Configuration Wizard – 🗆 🗙
Review Options	TARGET SERVER WIN2016DC.officedomain.net
Welcome	Review your selections:
Connect to AD DS	This server will be configured as the primary server in a new AD FS farm 'certauth.officedomain.net'.
Specify Service Account	AD FS configuration will be stored in Windows Internal Database.
Specify Database	Windows Internal Database feature will be installed on this server if it is not already installed.
Review Options	Federation service will be configured to run as OFFICEDOMAIN\adfssrv.
Pre-requisite Checks	
Installation	
Results	
	These settings can be exported to a Windows PowerShell script to automate additional installations
	< <u>P</u> revious <u>N</u> ext > <u>C</u> onfigure 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.

📥 Active Directory Federation Serv	ices Configuration Wizard	_		×
Pre-requisite Che	cks	TAF WIN2016DC.offic	RGET SEF	RVER n.net
All prerequisite checks pass	ed successfully. Click 'Configure' to begin installation.	Show	more	×
Welcome Connect to AD DS Specify Service Properties Specify Service Account Specify Database Review Options Pre-requisite Checks Installation Results	Prerequisites must be validated before Active Directory Federation computer. Rerun prerequisites check ✓ Yiew results Prerequisites Check Completed ✓ All prerequisite checks passed successfully. Click 'Configure 	n Services is configur e' to begin installation	ed on thi	is
	< <u>P</u> revious <u>N</u> ext >	<u>C</u> onfigure	Cance	el

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

Active Directory Federation Service	s Configuration Wizard —		
Results	TAR(WIN2016DC.office	GET SEF edomaii	RV n.r
This server was successfully control	nfigured Show m	ore	×
Welcome	<u> <u> </u></u>		
Connect to AD DS	A machine restart is required to complete ADFS service configuration. For more		
Specify Service Properties	information, see: http://go.microsoft.com/fwlink/?LinkId=798725		
Specify Service Account	Ine SSL certificate subject alternative names do not support host name 'certauth.certauth.officedomain.net'. Configuring certificate authentication binding	g on po	ort
Specify Database	'49443' and hostname 'certauth.officedomain.net'.		
Review Options			
Pre-requisite Checks	Next steps required for completing your federation service deployment		
Installation	······································		
Results	Need to monitor AD FS service? Use Azure Active Directory Connect Health.		
Results	Need to monitor AD FS service? Use Azure Active Directory Connect Health. < Previous Next > Close	Cance	el



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