

How to Import & Replace Certificate for ADFS

How to Import the certificate to the server:

1- Open Start menu "Run" type "*mmc*".

Start		Search Everywhere ~ runi P
		Plan Vew recommended actions to keep Windows running smoothly Image: Show which operating system your computer is running
Server Manager The PC	Administrative Took	
Literest Liplace		
Desitop emanamento		



🚘 Co	nsole1 - [Console Root]	-	o x
Tile Action View Favorites Window Help			- 5 ×
Console Root Name		Actions	
There	are no items to show in this view.	Console Root	-
		More Actions	•

2- Click File Add/Remove Snap-in.

a	Console1 - [Console Root]	_ D X
File Action View Favorites Window	Help	_ & ×
New Ctrl+N		
Open Ctrl+O		Actions
Save Ctrl+S	There are no items to show in this view.	Console Root
Add/Remove Span-in Ctd+M		More Actions
Options		
1 Microsoft.IdentityServer	-	
2 taskschd		
3 dsa		
4 domain		
Exit		
Enables you to add snap-ins to or remove them from	m the snap-in console.	

3- Search for "*Certificates*" in the Available snap-ins list à click "*Add*".



4- Select "*Computer Account*" and click "*Next*".

a	Console1 - [Console Root]		_ 🗆 X
🚡 File Action View Favorite	s Window Help		_ & ×
i 🗇 🔿 🖬 🔂 🖬 💳		v	
Console Root	Certificates span in X	^	5
		of snap-ins. For	ole Root 🔺
	This snap-in will always manage certificates for:		ore Actions
	O My user account	Edit Extensions	
	O Service account	Edit Exterisions	
	Computer account	Remove	
		Move Up	
		Mawa Dawa	
		Move Down	
		Advanced	
	Canad		
	Carcer	a computer.	
		-	
		OK Cased	
		Cancel	

5- Select "*Local Computer*" à click "*Finish*" à close the window.

	Console1 - [Console Root]		_ 1	D X
🛛 🚋 File Action View Favorites	Window Help			_ & ×
(+ +) 🖬 🔒 🛛 🖬 🛶			Π	
Console Root	Add or Domous Span inc.	X] <u></u>	
	Select Computer	of snap-ins. For	No Poot	
	Select the computer you want this span-in to manage		ore Actions	-
			ore Actions	, i
	 Local computer: the computer this console is running on) 	Edit Extensions		
		Remove		
	O Another computer: Browse			
	Allow the selected computer to be changed when launching from the command line. This	Move Up		
	oniy applies il you save the console.	Move Down		
		Advanced		
	< Back Finish Cancel	a computer.		
		OK Cancel		
	1			
	П	11		_

6- Go to Personal certificates à Right-click on the certificate select "*ALL TASKS*" select "*Import*".

2	Console1 - [Console F	Root\Certificates (Local Computer	r)\Personal\Cert	ificates]	_ D X
📷 File Action View	Favorites Window Help				_ 8
🗢 🔿 📶 📋					
Console Root	Issued To	Issued By	Expiration Date	Intended Purpo	Actions
△ 😭 Certificates (Local	Computer)	TERENA SSL CA 3	3/31/2021	Server Authenti	Certificates
Request New Certificate	All Tasks	TERENA SSL CA 3	4/13/2021	Server Authenti	More Actions
Import	View +	Microsoft PolicyKeyService Certifi Microsoft PolicyKeyService Certifi	6/25/2021	Client Authentic	
Advanced Operations	New Window from Here	Microsoft PolicyKeyService Certifi	7/12/2020	Client Authenti	
Dia Untrusted C	New Taskpad View	Microsoft PolicyKeyService Certifi	4/26/2020	Client Authenti	
▷ ☐ Third-Party ▷ ☐ Trusted Peo ▷ ☐ Client Authenet	Refresh Export List	Microsoft PolicyKeyService Certifi Microsoft PolicyKeyService Certifi DigiCert Assured ID Root CA	5/12/2021 12/30/2021 11/18/2024	Client Authenti Client Authenti <all></all>	
 Client Authe AdfsTrusted Certificate Enric Smart Card Tr Trusted Device Web Hosting 	Export List Help p p ollment Requ ssted Roots ts	DigiCert Assured ID Root CA	11/18/2024	<all></all>	

7- Follow the certificate import wizard to import certificate.



How to enable a New Certificate on a Server:

 1- Open the Start menu à click Administrative Tools then Internet Information Services (IIS)

Search Tools	ternet Information Services (IIS) Manager	- Search Results in Administrative Tools	_ a x
View Search			V 3
rch Results in Administrative Tools 🔸			 ぐ C Information Services (IIS) Manager ×
slow because the index is not running.			*
Internet Information Services (IIS) Manager C.\ProgramData\Microsoft\Windows\Start Menu\Pri	Type: Shortcut	Date modified: 8/22/2013 10:50 AM Size: 1.10 KB	



2- click the server name Expand the sites folder choose "*default Web site*" then click "*Bindings*"



3- click "*Add*".

			Site	Bindings	? X
Type http https	Host Name adfs.omren.om	Port 80 443	Site IP Address * *	Bindings Binding Informa	Add Edit Remove Browse
					Close

4- choose "*https*" from the type drop-down, Set the IP address in the IP address filed. Set the port to "443" Enter Host name in the host name filed Enter the recently imported certificate in the SSL Certificate field Click "*OK*".

	Document	Provina	Manninge	Padiract	Pornon		
			Site Bindings			?	X
Туре			Add Site Binding	g		? X	
http https	Type: https Host name: ads.omren.or	IP address: ID.8.15.20 m erver Name Indication		Port:			
	SSL certificat *.omren.om	e:	~	Select OK	Ca	w	

it is recommended to restart IIS or the server to recognize the new :Comment certificate

How to Replace the certificate to ADFS:

1- Open Server Manager, Tools -> ADFS Management

<u>.</u>	Server M	anager	- D X
Server N	lanager • Dashboard	CO Manage Tools Active Directory Administrative Center Active Directory Domains and Trusts	View Help
Local Server All Servers AD DS	1 Con	Active Directory Module for Windows Powershell Active Directory Rights Management Services Active Directory Sites and Services Active Directory Users and Computers	
AP AD FS AD FS INS IS NAP	QUICK START 2 A 3 A WHAT'S NEW 4 C	AD FS Management ADSI Edit Component Services Computer Management Defragment and Optimize Drives DNS Event Viewer	
	LEARN MORE	Health Registration Authority	Hide
	ROLES AND SERVER GROUPS Roles: 6 Server groups: 1 Servers to	iSCSI Initiator Local Security Policy Microsoft Azure Services Network Policy Server	<u> </u>
		ODBC Data Sources (32-bit) ODBC Data Sources (64-bit) Performance Monitor Resource Monitor	ICT VET 2012 RZ

2- In the ADFS Management Console, expand Service item within the left panel and click Certificates.

File Action View Window Help							_ # ×
AD FS	Certificates						Actions
Endpoints	Subject Service communications	Issuer	Effective Date	Expiration Date	Status	Primary	Certificates Add Token-Signing Certificate
Claim Descriptions Trust Relationships	Token-decrypting	CN=TERENA SSL CA 3,	3/28/2019	3/31/2021			Add Token-Decrypting Certificate Set Service Communications Certif
Authentication Policies	CN=ADFS Encryption - adfs	CN=ADFS Encryption - ad CN=ADFS Encryption - ad	5/2/2019 4/11/2020	5/1/2020 4/11/2021		Secondary Primary	View
	CN=ADFS Signing - adfs.o	CN=ADFS Signing - adfs CN=ADFS Signing - adfs	5/2/2019 4/11/2020	5/1/2020 4/11/2021		Secondary Primary	Refresh
							Pelp

3- Click "*Add Token-signing Certificate*" (ADFS may show a warning message as it shown below)



4- To remove the warring, open an administrative PowerShell and execute the following command:

Set-ADFSProperties -AutoCertificateRollover \$false.

Then, click "Add Token-signing Certificate" again

5- The system will reset all the installed certificates. Select the valid certificate and click "OK".



6- The certificate will upload as secondary. Right click on the newly uploaded certificate and select "*Set as Primary*".

N			AD FS			- D X
翰 File Action View Window Help						_ # ×
🗢 🔿 🙍 💽 🚺						
🛗 AD FS	Certificates					Actions
Service Endpoints Certificates Claim Descriptions Claims Provider Trusts Relying Party Trusts Attribute Stores Authentication Policies	Subject Service communications CN=*omren.om, O=Oman Token-decrypting CN=ADFS Encryption - adfa Token-signing CN=ADFS Sogning - adfa.o CN=ADFS Signing - adfa.o	Issuer CN=TERENA SSL CA 3 CN=ADFS Encyption - ad CN=ADFS Encyption - ad CN=ADFS Signing - adfa CN=ADFS Signing - adfa	Effective Date 3/28/2019 5/2/2019 4/11/2020 5/2/2019 4/11/2020	Expiration Date Status 3/31/2021 5/1/2020 4/11/2021 Set as Primary Delete Help	Primary Secondary Primary Mimary	Certificates ▲ Add Token-Signing Certificate Add Token-Decrypting Certificate Set Service Communications Certif View New Window from Here ▲ ⓓ Refresh ➡ Help CN=ADFS Signing - adfs.omren ▲ View Certificate Set as Primary ➤ Delete ➡

7- Repeat the same steps for Token-decryption and Service Communication

%			AD FS				_ D X
翰 File Action View Window Help							_ 5 ×
🗢 🔿 🙍 🖬 📓 🖬							
AD FS	Certificates						Actions
⊿ Service Endpoints	Subject	Issuer	Effective Date	Expiration Date	Status	Primary	Certificates
Certificates	Service communications	CN=TERENA SSL CA 3	3/28/2019	3/31/2021			Add Token-Signing Certificate
Claim Descriptions	Token-decrypting						Add Token-Decrypting Certificate
Authentication Policies	CN=ADFS Encryption - adfs	CN=ADFS Encryption - ad	5/2/2019	5/1/2020		Secondary	Set Service Communications Certif
	Token-signing	CN=ADFS Encryption - ad	4/11/2020	4/11/2021		Primary	New Window from Here
	CN=ADFS Signing - adfs.o	CN=ADFS Signing - adfs	5/2/2019	5/1/2020		Secondary	Refresh
	CN=ADFS Signing - adfs.o	AD FS ■ ■ ★ Witates Baser Effective Date Spatu Primary Witates Effective Date Spatu Primary Actions Certificates Add Token-Signing Certificate Add Token-Signing Certificate Secondary (CH-ADFS Encryption - adfs CH-ADFS Signing - adfs CH-ADFS Signing - adfs (CH-ADFS Signing - adfs CH-ADFS Signing - adfs S/2/2019 S/1/2020 Okan-aligning CH-ADFS Signing - adfs CH-ADFS Signing - adfs N/11/2020 (CH-ADFS Signing - adfs CH-ADFS Signing - adfs CH-ADFS Signing - adfs N/11/2020 (CH-ADFS Signing - adfs CH-ADFS Signing - adfs A/11/2020 Secondary (CH-ADFS Signing - adfs CH-ADFS Signing - adfs A/11/2020 Secondary View Certificate Set Service Communications Certif Work Certificate Set Service Communications Certif (CH-ADFS Signing - adfs CH-ADFS Signing - adfs A/11/2020 Secondary Primary View Certificate Secondary Primary View Certificate Set Service Communications Certif Help					
							CN=ADFS Encryption - adfs.om
							View Certificate
							Set as Primary
							🗙 Delete
							👔 Help

Comment: We did not complete the configuration yet. To complete the configuration, we need to identify the thumbprint of the certificate and execute a PowerShell command.

8- On Certificates Management Console à Personalà certificates à Right click on the SSL certificate that you want to link with ADFS and select "open".



9- Select Details tab, find the Thumbprint and copy it.

			Cert	tificate					
General D	etails C	ertification	n Path]					
Show: <	All>				~				
Field Signa Issue Valid f Subje Public	ture hash r from to ct key borint alo	algorithm		Value sha256 ADFS E Thursda Friday, ADFS E RSA (20	ncrypti ay, May May 1, ncrypti)48 Bits	on - adf / 2, 201 . 2020 1 on - adf s)	s.omr 9 11:3 1:32: s.omr	en 32: 14 en	~
Thum	oprint aig bprint	orithm		32 ba 2	a 9f ab	f2 c2 e	6 70 3	38	~
32 ba e3 bb	2a 9f 15 f7	ab f2 cd	c2 ·	⊜6 70	38 ()1 4a	50	76	eb
			Ed	it Proper	ties	C	opy to	File	•
								0	к

10- Paste the Thumbprint code in bellow PowerShell command and run the command

"Set-AdfsSslCertificate –Thumbprint *<Enter the ThumbprintCertificate here>*"

Comment: Make sure to remove spaces in copied Thumbprint Example: "Set-AdfsSslCertificate -Thumbprint d3c6391344da16b365ac6385a491e57ddc00c0"



- 11- Restart the ADFS service to complete the configuration changes.
- 12- Run the script manually using Admin privileges from Task scheduler