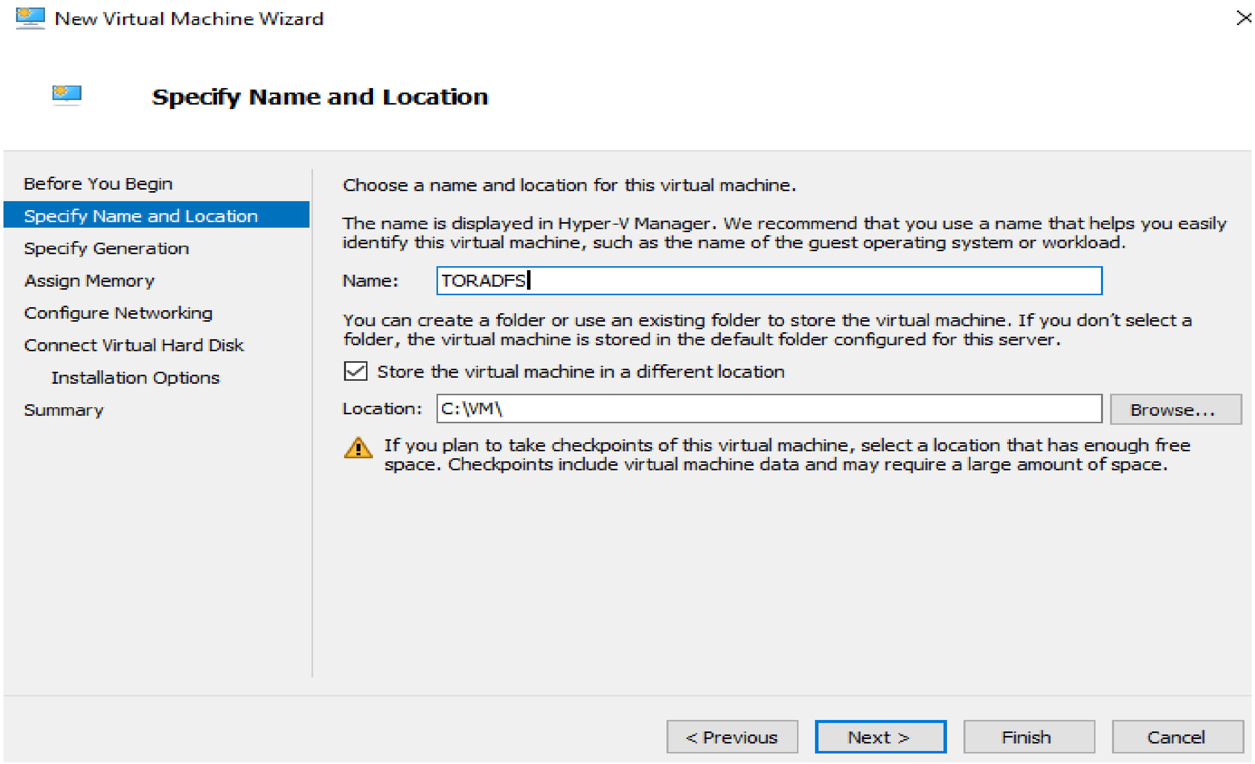
Installing Active Directory Federation Services

In this post, I will show you the steps for installing ADFS role and using Let's Encrypt SSL certificate to complete ADFS Configuration.

I will be using virtual machine running Windows Server 2019 v1809. All updates installed and server restarted.

Here are few screen shots on the above.



New Virtual Machine Wizard

Specify Name and Location

Choose a name and location for this virtual machine.

The name is displayed in Hyper-V Manager. We recommend that you use a name that helps you easily identify this virtual machine, such as the name of the guest operating system or workload.

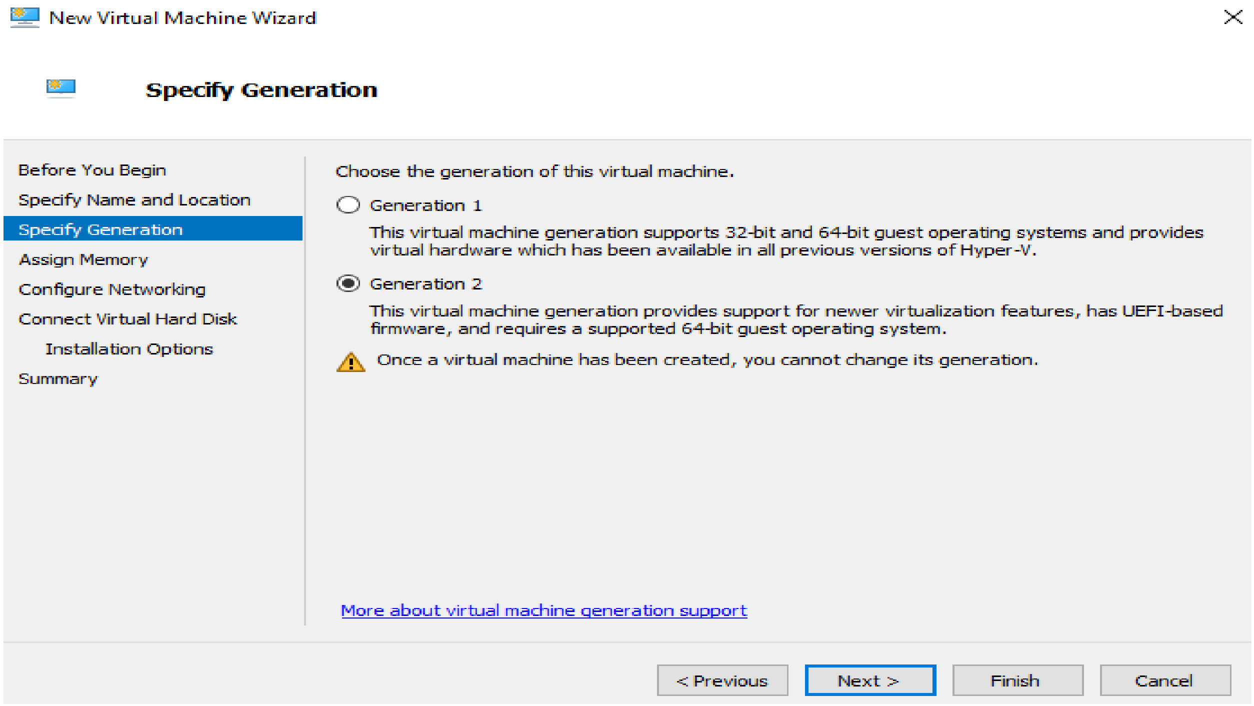
Name: TORADFS

You can create a folder or use an existing folder to store the virtual machine. If you don't select a folder, the virtual machine is stored in the default folder configured for this server.

☑ Store the virtual machine in a different location

Location: C:\VM\

If you plan to take checkpoints of this virtual machine, select a location that has enough free space. Checkpoints include virtual machine data and may require a large amount of space.



New Virtual Machine Wizard

Specify Generation

Choose the generation of this virtual machine.

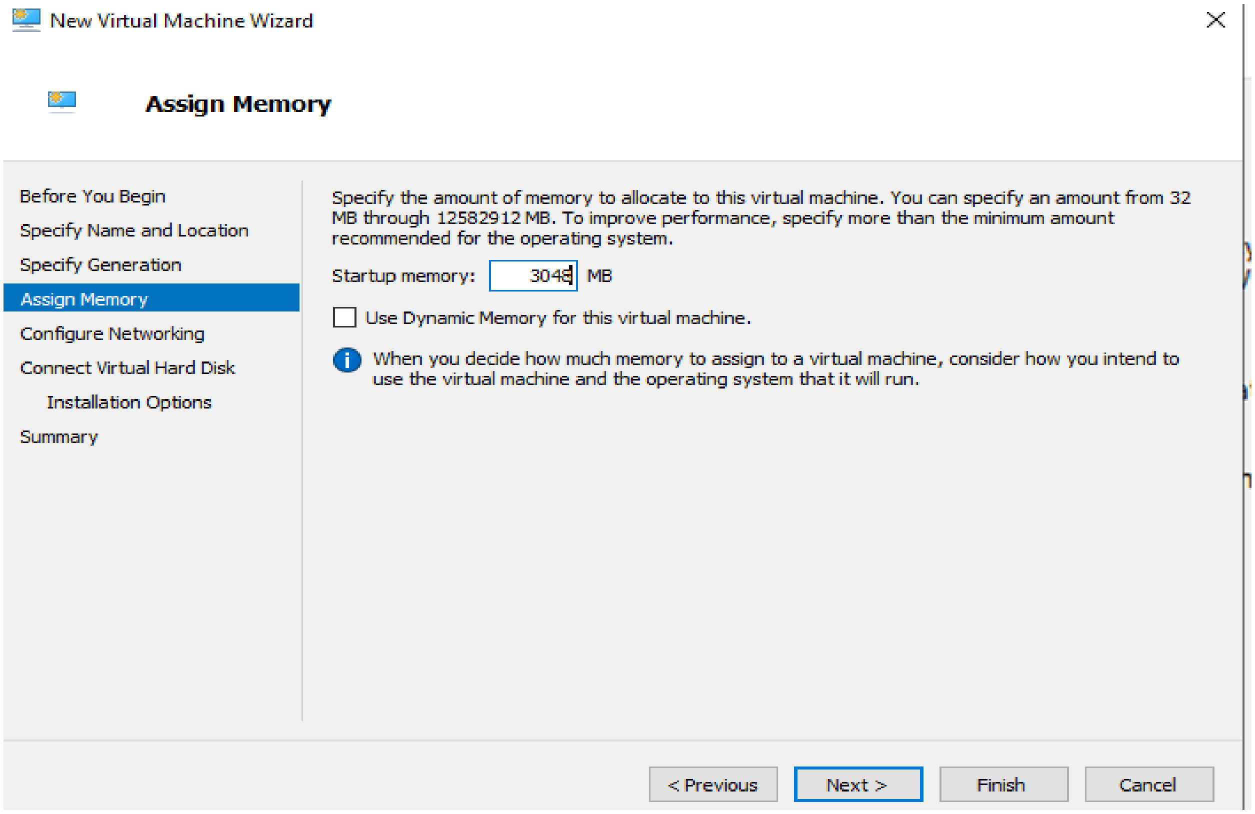
○ Generation 1

This virtual machine generation supports 32-bit and 64-bit guest operating systems and provides virtual hardware which has been available in all previous versions of Hyper-V.

● Generation 2

This virtual machine generation provides support for newer virtualization features, has UEFI-based firmware, and requires a supported 64-bit guest operating system.

Once a virtual machine has been created, you cannot change its generation.



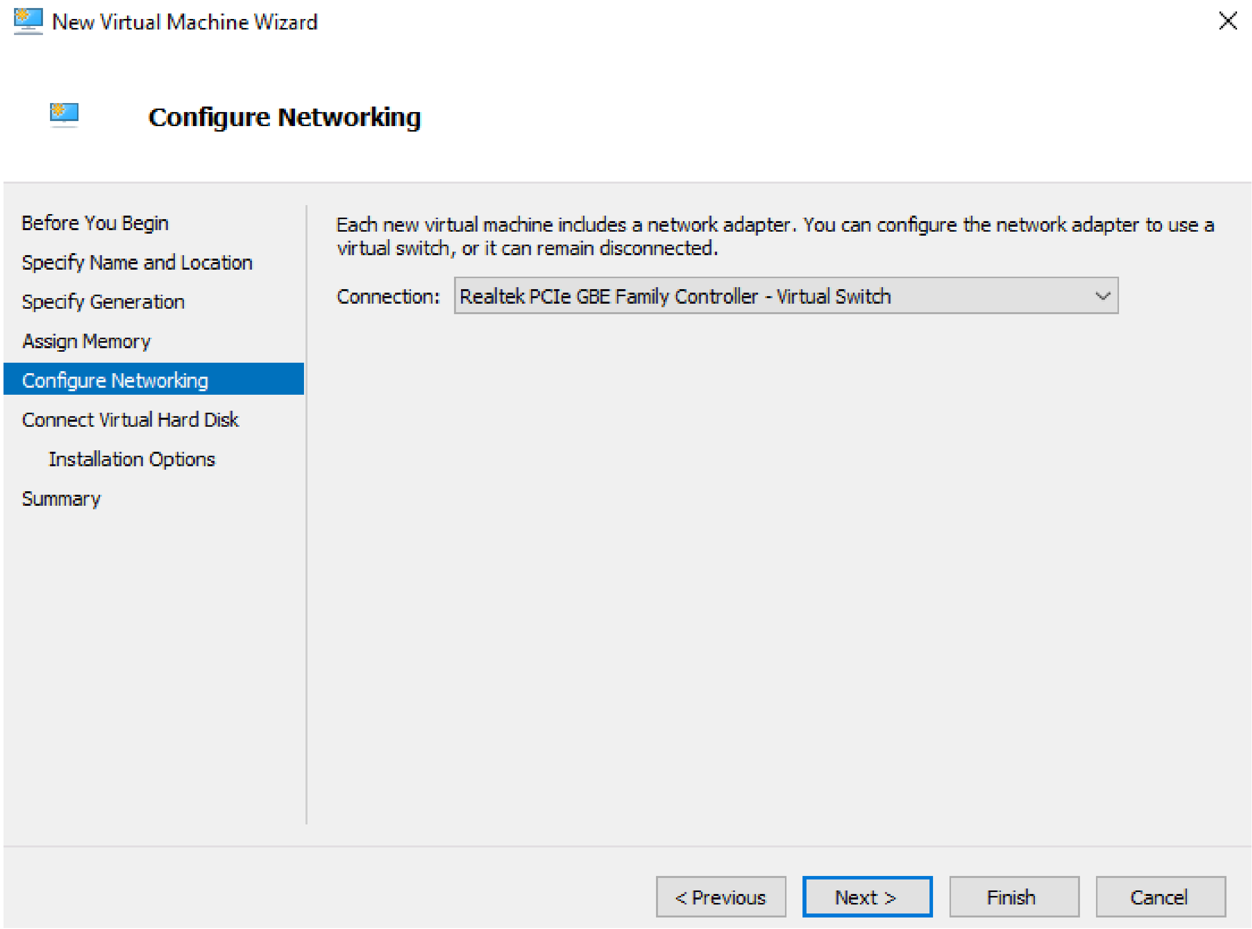
Assign Memory

Specify the amount of memory to allocate to this virtual machine. You can specify an amount from 32 MB through 12582912 MB. To improve performance, specify more than the minimum amount recommended for the operating system.

Startup memory: 3048 MB

□ Use Dynamic Memory for this virtual machine.

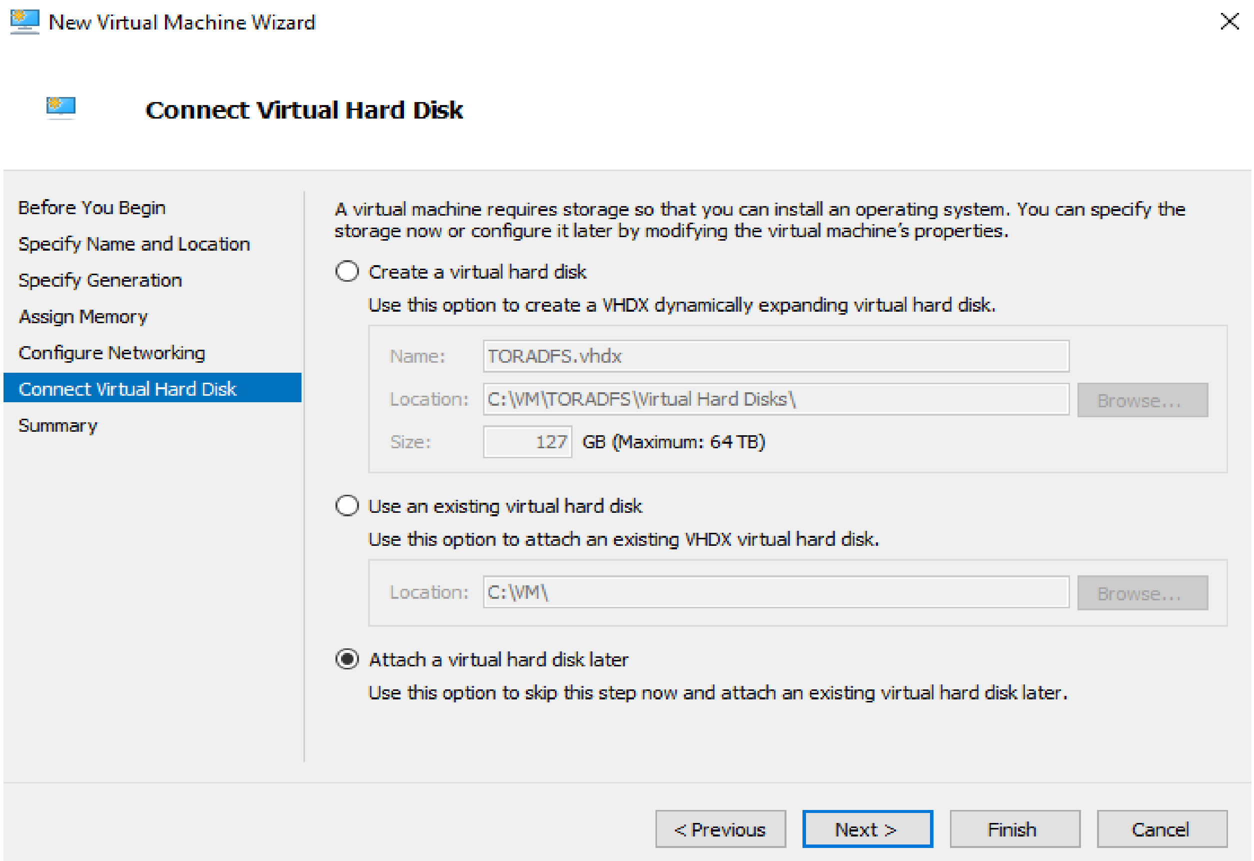
When you decide how much memory to assign to a virtual machine, consider how you intend to use the virtual machine and the operating system that it will run.



Configure Networking

Each new virtual machine includes a network adapter. You can configure the network adapter to use a virtual switch, or it can remain disconnected.

Connection: Realtek PCIe GBE Family Controller - Virtual Switch



Connect Virtual Hard Disk

A virtual machine requires storage so that you can install an operating system. You can specify the storage now or configure it later by modifying the virtual machine's properties.

○ Create a virtual hard disk

Use this option to create a VHDX dynamically expanding virtual hard disk.

Name: TORADFS.vhdx

Location: C:\VM\TORADFS\Virtual Hard Disks\

Size: 127 GB (Maximum: 64 TB)

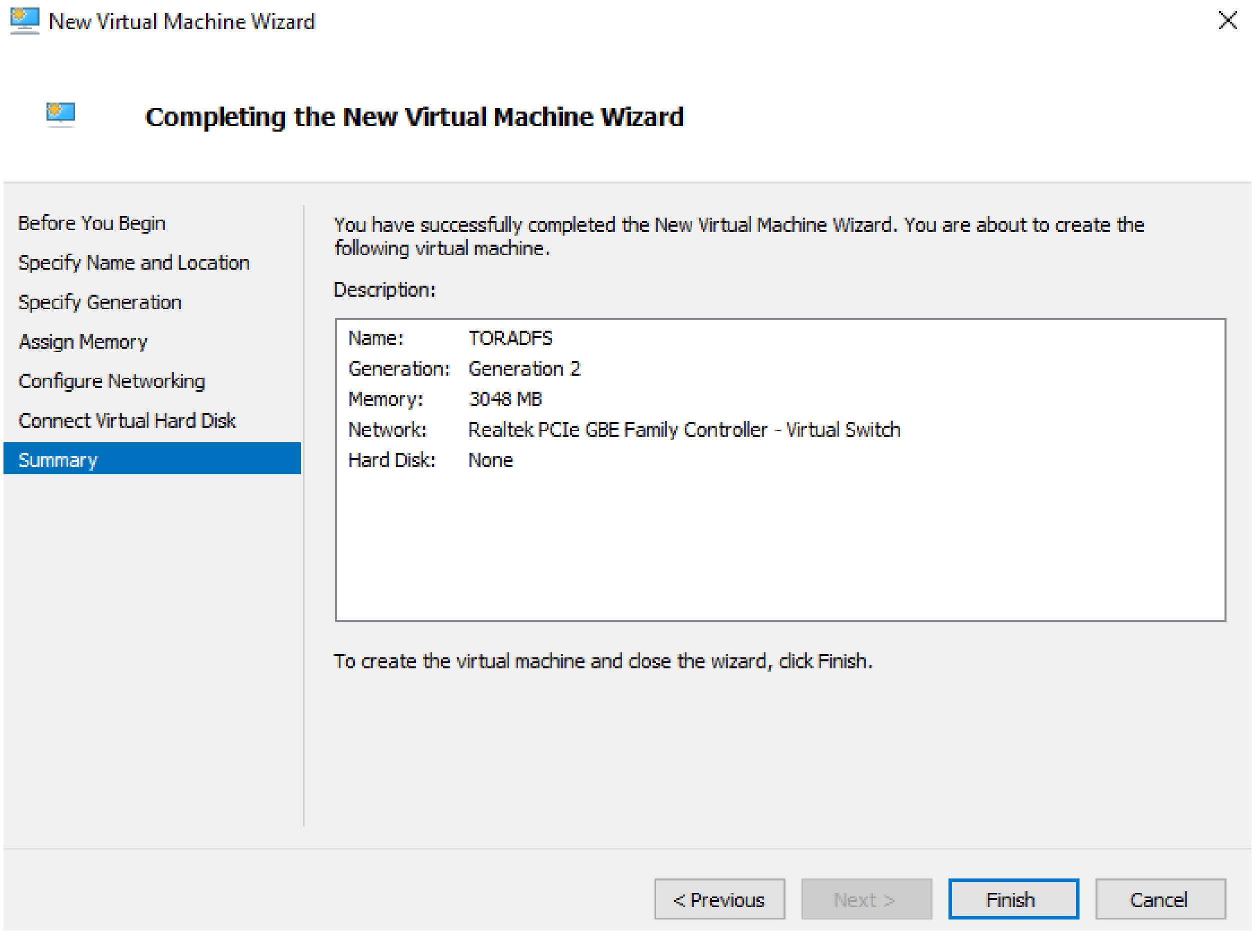
○ Use an existing virtual hard disk

Use this option to attach an existing VHDX virtual hard disk.

Location: C:\VM\

● Attach a virtual hard disk later

Use this option to skip this step now and attach an existing virtual hard disk later.



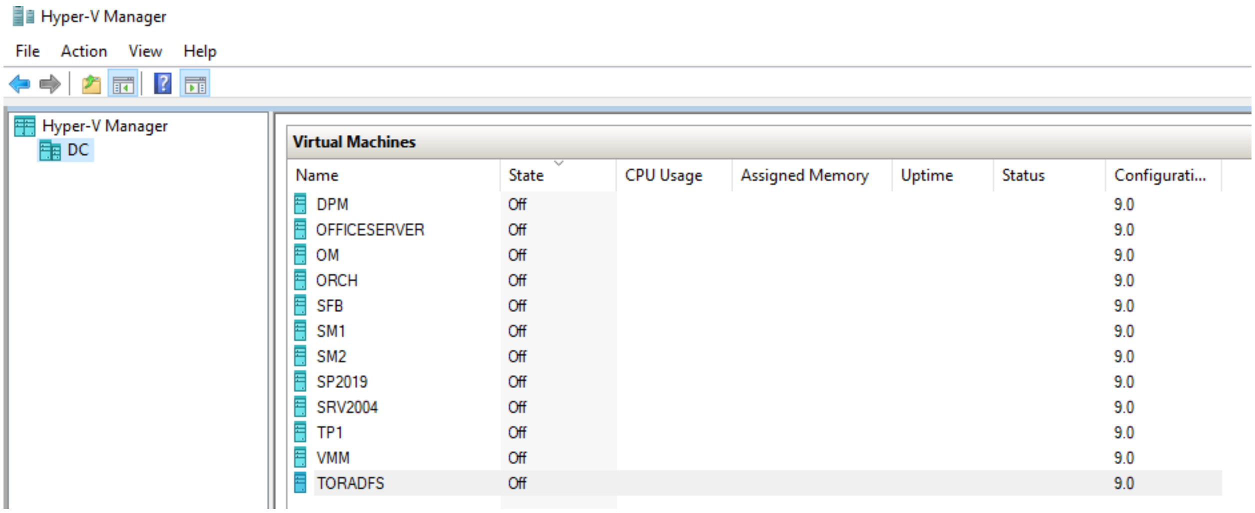
Completing the New Virtual Machine Wizard

You have successfully completed the New Virtual Machine Wizard. You are about to create the following virtual machine.

Description:

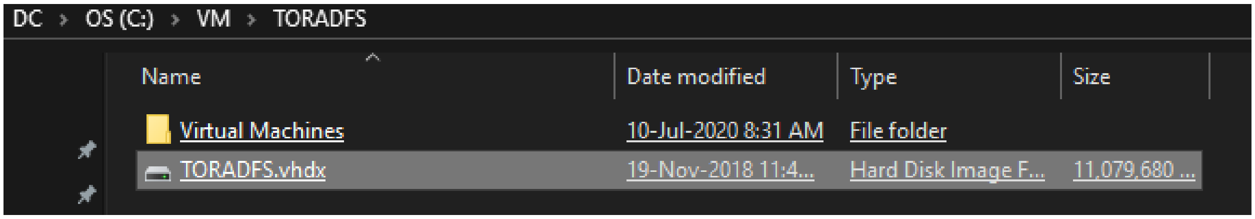
Name:	TORADFS
Generation:	Generation 2
Memory:	3048 MB
Network:	Realtek PCIe GBE Family Controller - Virtual Switch
Hard Disk:	None

To create the virtual machine and close the wizard, click Finish.



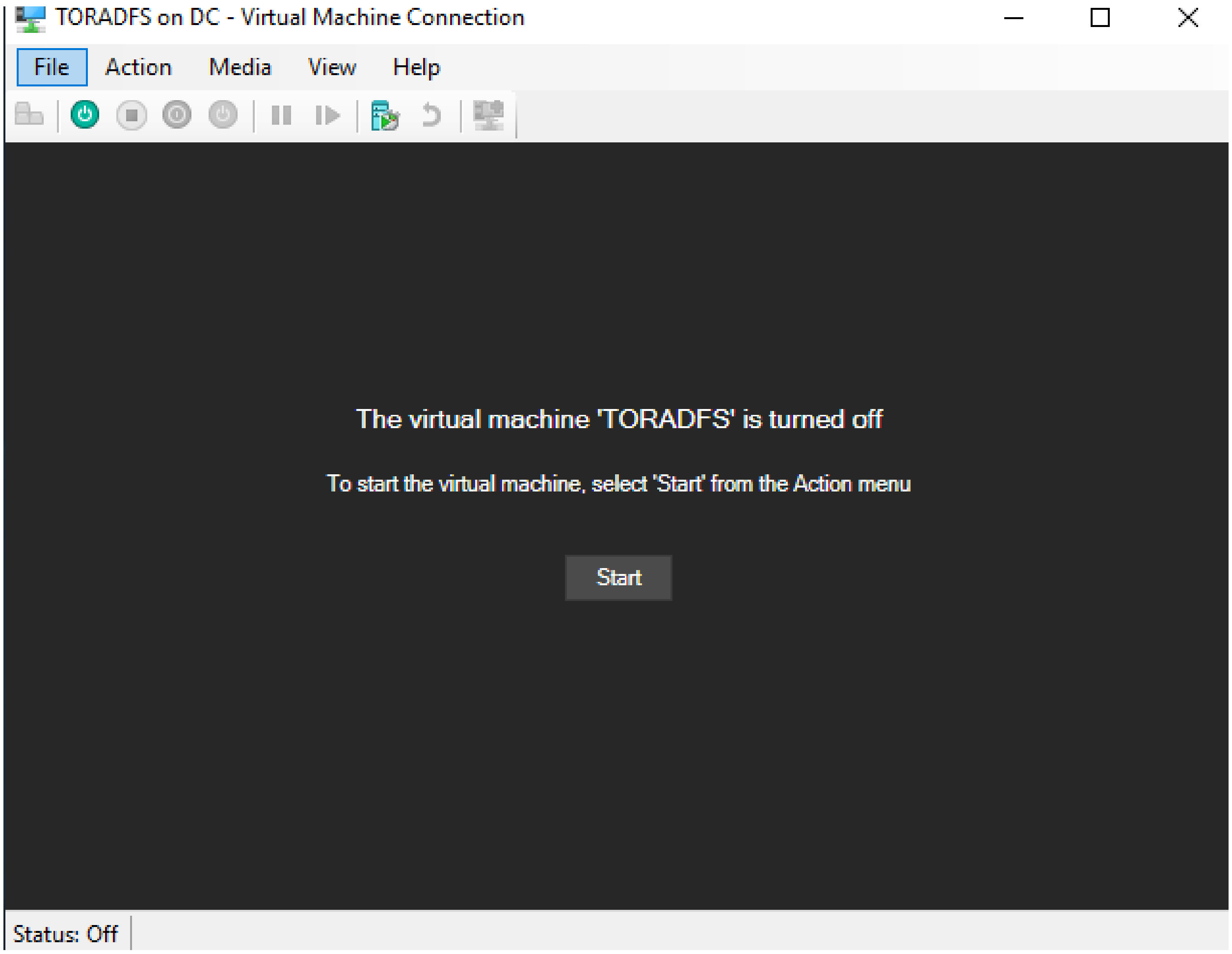
Virtual Machines

Name	State	CPU Usage	Assigned Memory	Uptime	Status	Configurati...
DPM	Off					9.0
OFFICESERVER	Off					9.0
OM	Off					9.0
ORCH	Off					9.0
SFB	Off					9.0
SM1	Off					9.0
SM2	Off					9.0
SP2019	Off					9.0
SRV2004	Off					9.0
TP1	Off					9.0
VMM	Off					9.0
TORADFS	Off					9.0



DC › OS (C:) › VM › TORADFS

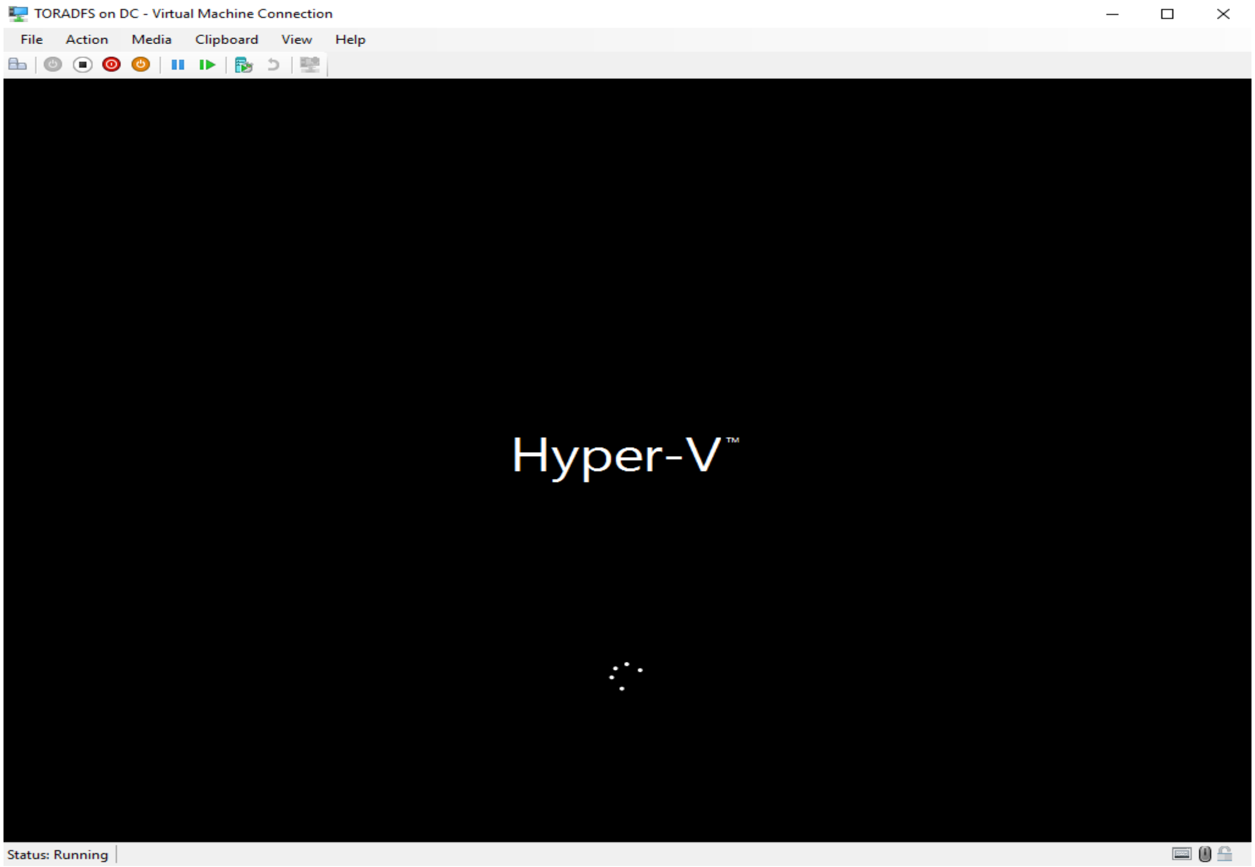
Name	Date modified	Type	Size
Virtual Machines	10-Jul-2020 8:31 AM	File folder	
TORADFS.vhdx	19-Nov-2018 11:4...	Hard Disk Image F...	11,079,680 ...

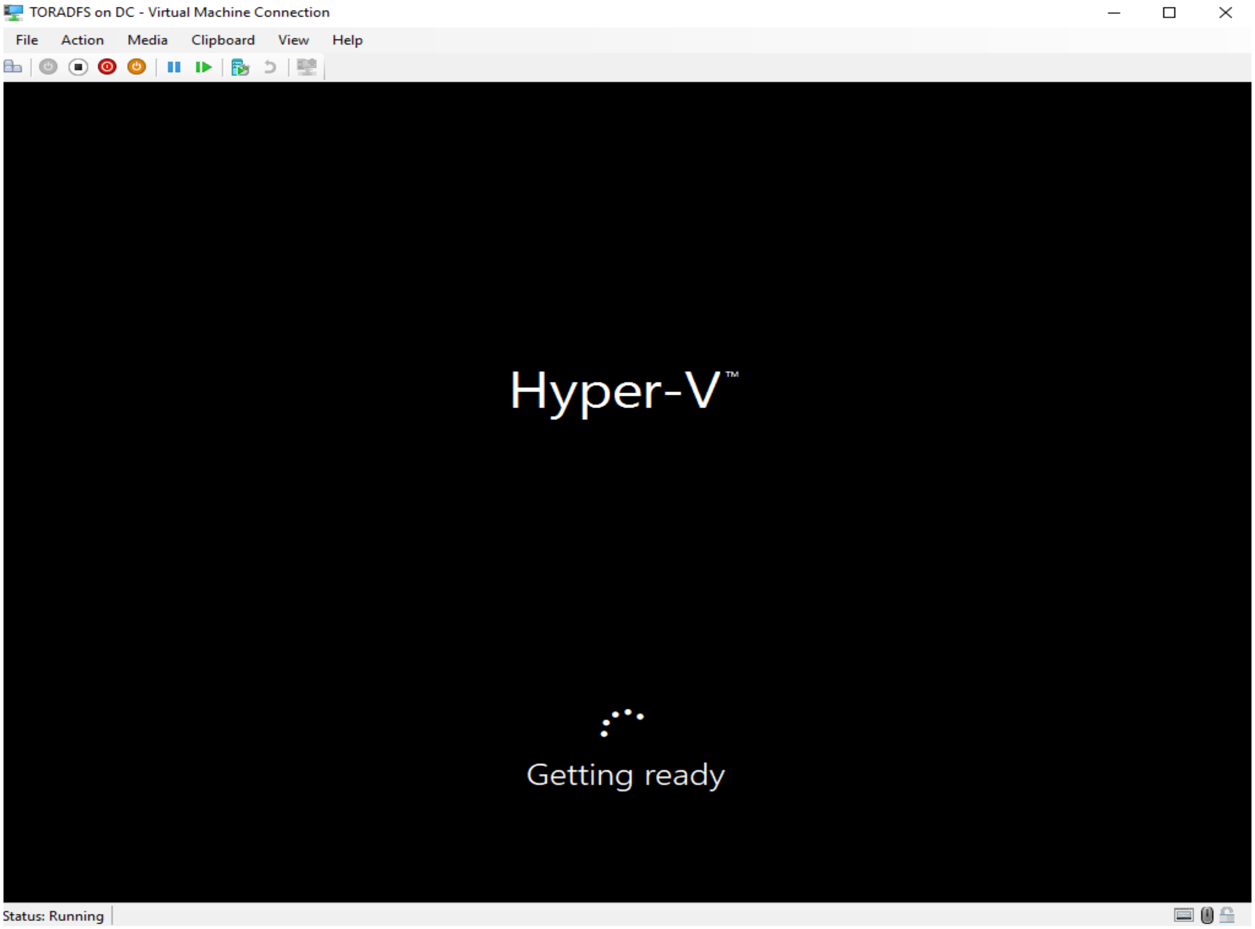


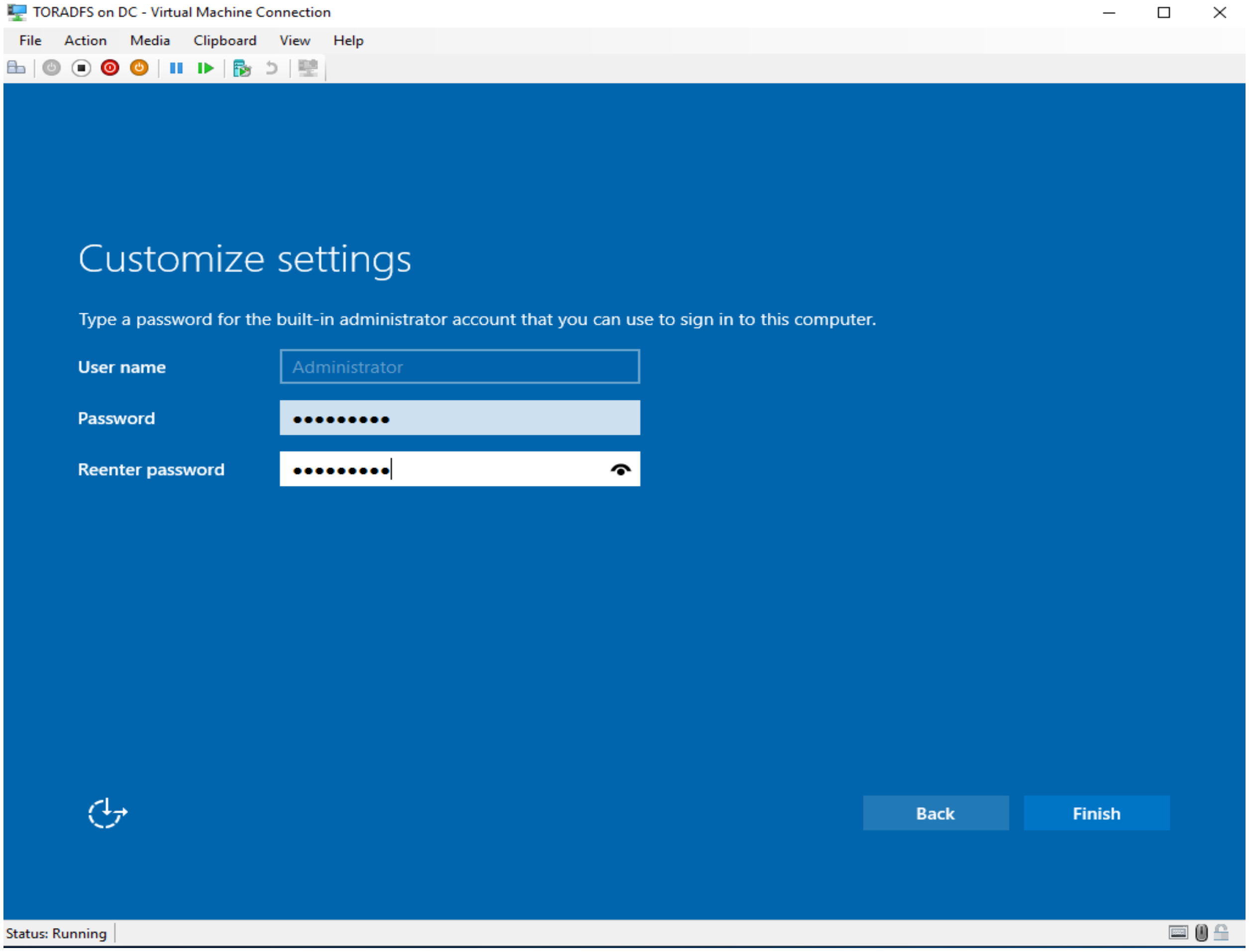
The virtual machine 'TORADFS' is turned off

To start the virtual machine, select 'Start' from the Action menu

Status: Off


TORADFS on DC - Virtual Machine Connection
File
Action
Media
Clipboard
View
Help
Hyper-V™
Status: Running


TORADFS on DC - Virtual Machine Connection
File
Action
Media
Clipboard
View
Help
Hyper-V™
Getting ready
Status: Running



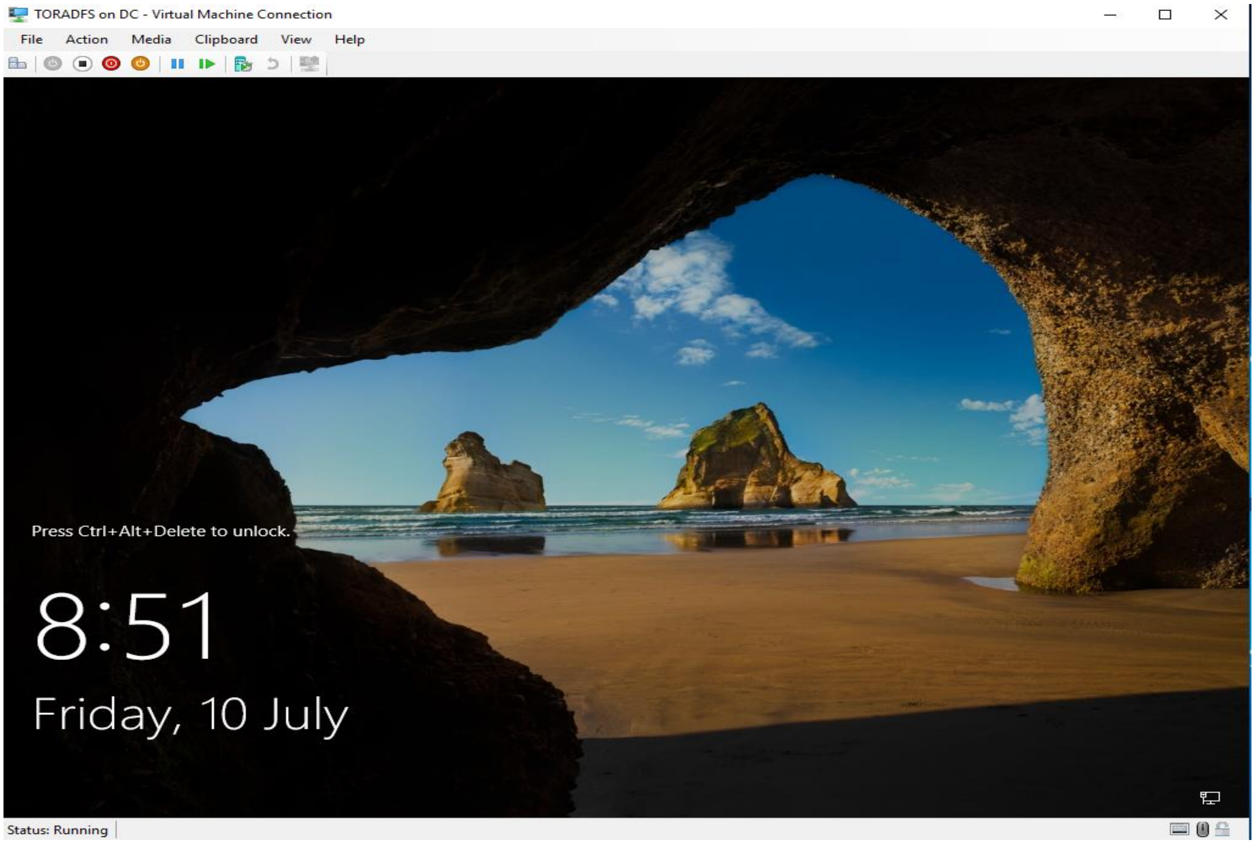
Customize settings

Type a password for the built-in administrator account that you can use to sign in to this computer.

User name: Administrator

Password: ●●●●●●●●●●

Reenter password: ●●●●●●●●●●



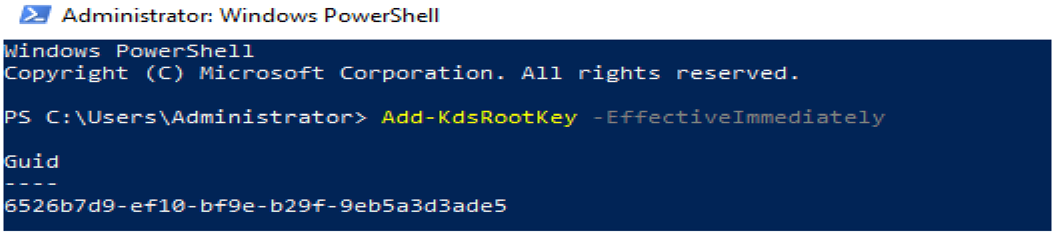
Press Ctrl+Alt+Delete to unlock.

8:51

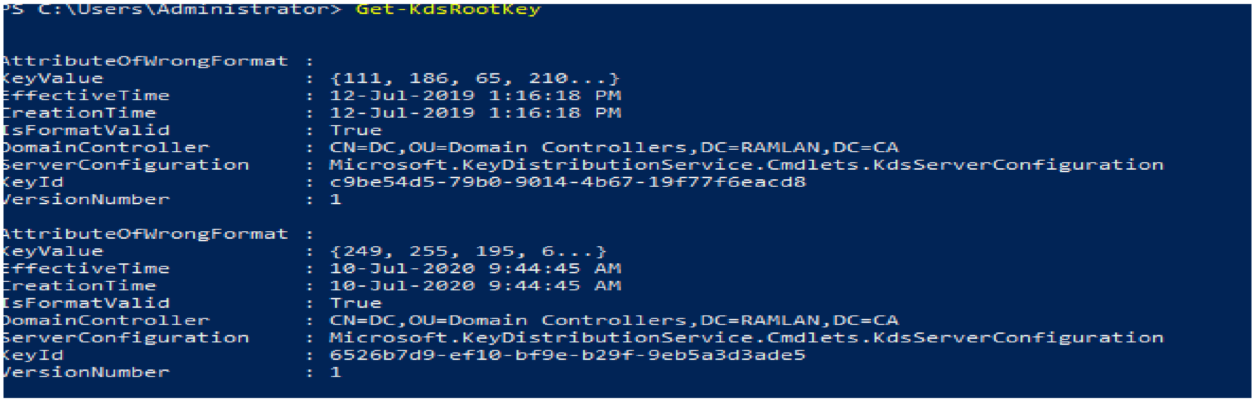
Friday, 10 July

Logged in and changed computer name, joined to domain and installed all the updates. Before we install ADFS role, we have to complete the following:

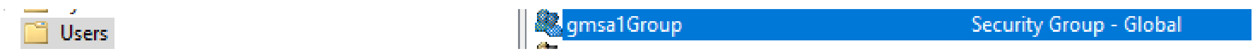
1. Create Kds root key using PowerShell on DC (Add-KdsRootKey -EffectiveImmediately)
2. Create a group named gmsa1Group in ADUC – Users Folder
3. Create gMSA Account using PowerShell on DC (New-ADServiceAccount "gmsa1" -DNSHostName "dc.ramlan.ca" –PrincipalsAllowedToRetrieveManagedPassword "gmsa1Group")
4. Install AD PowerShell on TORADFS Server (Add-WindowsFeature RSAT-AD-PowerShell)
5. Install gMSA on TORADFS Server (Install–ADServiceAccount –Identity “gmsa1”, Test–ADServiceAccount gmsa1)


Administrator: Windows PowerShell

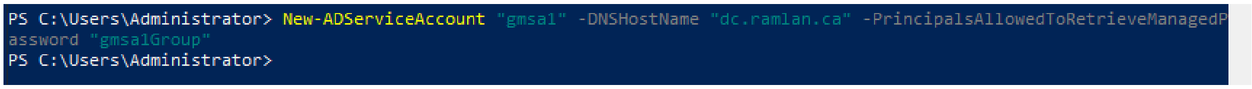
```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\Administrator> Add-KdsRootKey -EffectiveImmediately

Guid
----
6526b7d9-ef10-bf9e-b29f-9eb5a3d3ade5
```



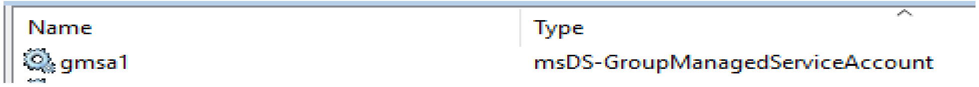
```
PS C:\Users\Administrator> Get-KdsRootKey


AttributeOfWrongFormat :
KeyValue               : {111, 186, 65, 210...}
EffectiveTime          : 12-Jul-2019 1:16:18 PM
CreationTime           : 12-Jul-2019 1:16:18 PM
IsFormatValid          : True
DomainController       : CN=DC,OU=Domain Controllers,DC=RAMLAN,DC=CA
ServerConfiguration    : Microsoft.KeyDistributionService.Cmdlets.KdsServerConfiguration
KeyId                  : c9be54d5-79b0-9014-4b67-19f77f6eacd8
VersionNumber          : 1

AttributeOfWrongFormat :
KeyValue               : {249, 255, 195, 6...}
EffectiveTime          : 10-Jul-2020 9:44:45 AM
CreationTime           : 10-Jul-2020 9:44:45 AM
IsFormatValid          : True
DomainController       : CN=DC,OU=Domain Controllers,DC=RAMLAN,DC=CA
ServerConfiguration    : Microsoft.KeyDistributionService.Cmdlets.KdsServerConfiguration
KeyId                  : 6526b7d9-ef10-bf9e-b29f-9eb5a3d3ade5
VersionNumber          : 1
```



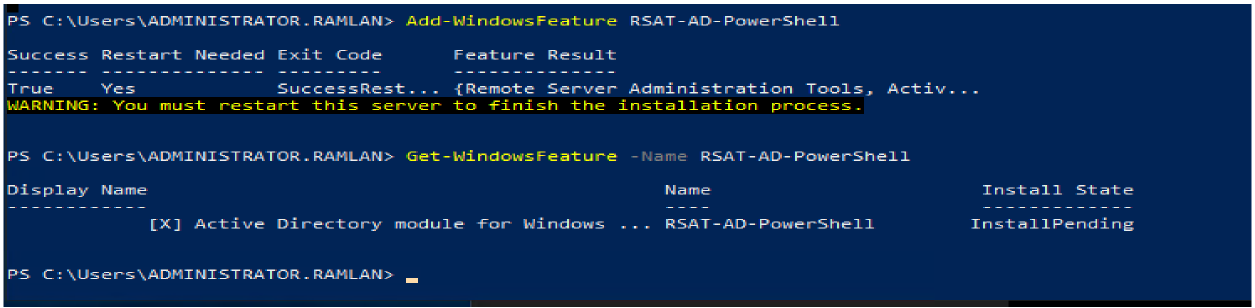
gmsa1Group	Security Group - Global



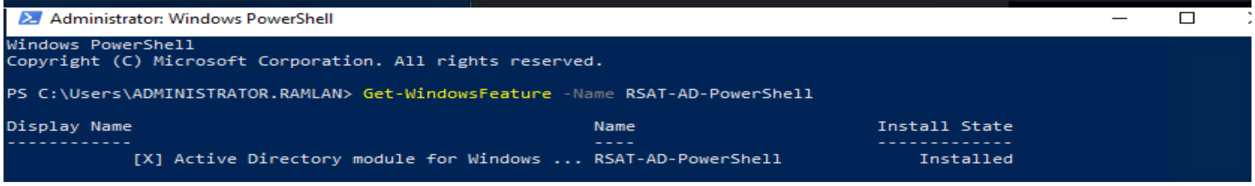
```
PS C:\Users\Administrator> New-ADServiceAccount "gmsa1" -DNSHostName "dc.ramlan.ca" -PrincipalsAllowedToRetrieveManagedP
assword "gmsa1Group"
PS C:\Users\Administrator>
```



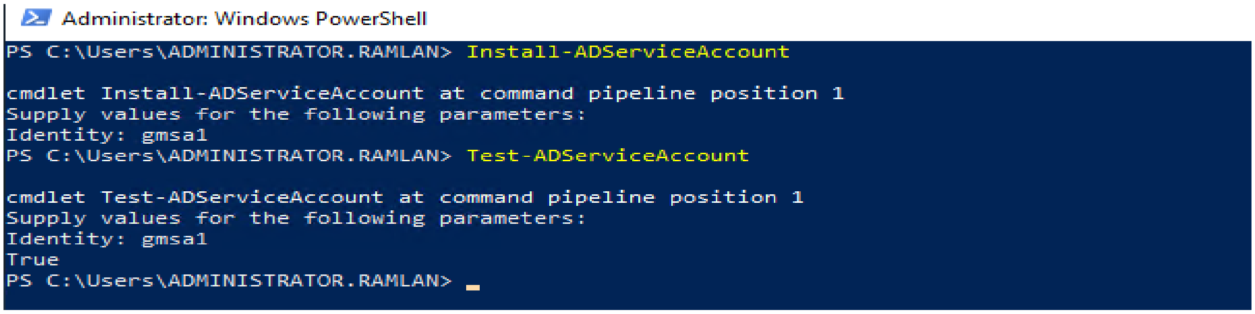
Name	Type
gmsa1	msDS-GroupManagedServiceAccount



```
PS C:\Users\ADMINISTRATOR.RAMLAN> Add-WindowsFeature RSAT-AD-PowerShell

Success Restart Needed Exit Code      Feature Result
------- -------------- ---------      --------------
True    Yes            SuccessRest... {Remote Server Administration Tools, Activ...
WARNING: You must restart this server to finish the installation process.


PS C:\Users\ADMINISTRATOR.RAMLAN> Get-WindowsFeature -Name RSAT-AD-PowerShell

Display Name                                            Name                       Install State
------------                                            ----                       -------------
            [X] Active Directory module for Windows ... RSAT-AD-PowerShell        InstallPending


PS C:\Users\ADMINISTRATOR.RAMLAN> _
```

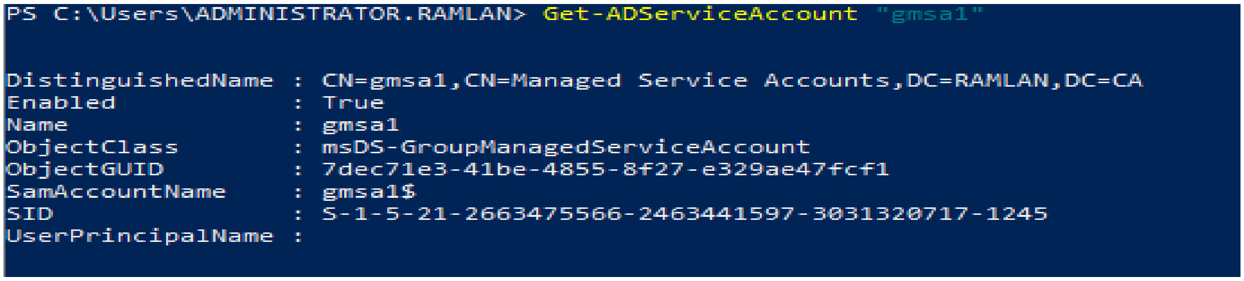

Administrator: Windows PowerShell

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\ADMINISTRATOR.RAMLAN> Get-WindowsFeature -Name RSAT-AD-PowerShell

Display Name                                            Name                       Install State
------------                                            ----                       -------------
            [X] Active Directory module for Windows ... RSAT-AD-PowerShell             Installed
```

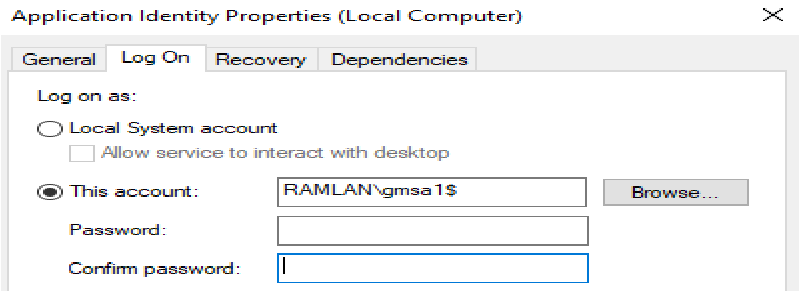


Administrator: Windows PowerShell

```
PS C:\Users\ADMINISTRATOR.RAMLAN> Install-ADServiceAccount

cmdlet Install-ADServiceAccount at command pipeline position 1
Supply values for the following parameters:
Identity: gmsa1
PS C:\Users\ADMINISTRATOR.RAMLAN> Test-ADServiceAccount

cmdlet Test-ADServiceAccount at command pipeline position 1
Supply values for the following parameters:
Identity: gmsa1
True
PS C:\Users\ADMINISTRATOR.RAMLAN> _
```



```
PS C:\Users\ADMINISTRATOR.RAMLAN> Get-ADServiceAccount "gmsa1"


DistinguishedName  : CN=gmsa1,CN=Managed Service Accounts,DC=RAMLAN,DC=CA
Enabled            : True
Name               : gmsa1
ObjectClass        : msDS-GroupManagedServiceAccount
ObjectGUID         : 7dec71e3-41be-4855-8f27-e329ae47fcf1
SamAccountName     : gmsa1$
SID                : S-1-5-21-2663475566-2463441597-3031320717-1245
UserPrincipalName  :
```



Application Identity Properties (Local Computer)

Log on as:

○ Local System account

□ Allow service to interact with desktop

● This account: RAMLAN\gmsa1$

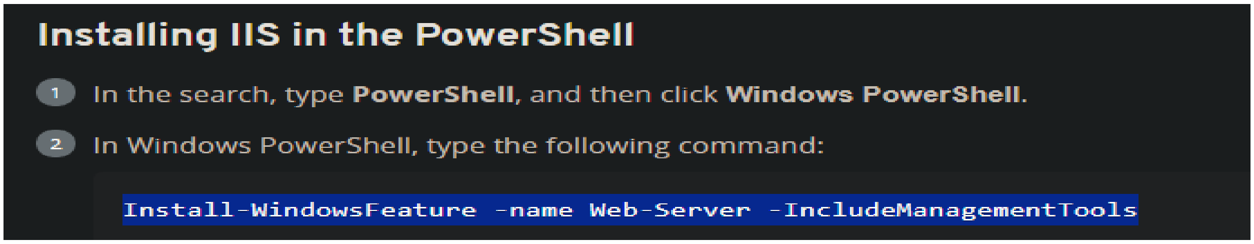
Password:

Confirm password:

Since this is lab, I don’t want to spend money on purchasing SSL Certificate. I am going to use Let’s Encrypt SSL that is FREE. Following are the steps, I took to get the certificate

1. Installed IIS
2. Created a folder called adfs.ramlan.ca inside inetpub and created index.html
3. Created A record on Local DNS pointing to Public IP
4. Created A record on GoDaddy DNS pointing to Public IP
5. Run wacs.exe as Administrator and below are the details

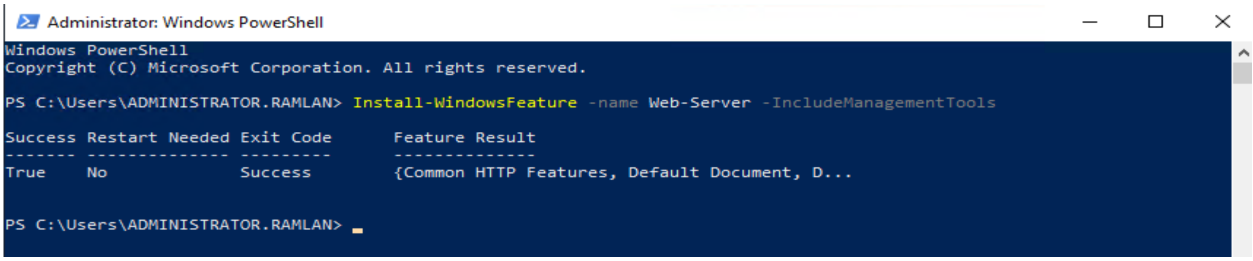
Install Basic IIS and Request a Certificate



Installing IIS in the PowerShell

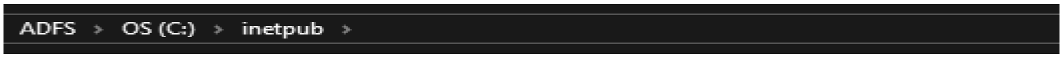
1. In the search, type **PowerShell**, and then click **Windows PowerShell**.
2. In Windows PowerShell, type the following command:

```
Install-WindowsFeature -name Web-Server -IncludeManagementTools
```

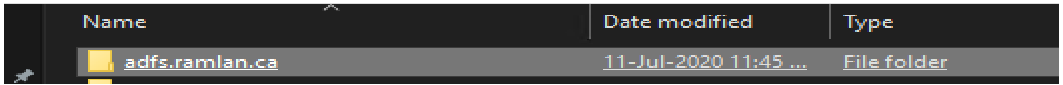


Administrator: Windows PowerShell

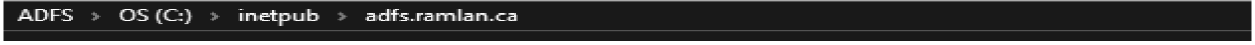
```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\ADMINISTRATOR.RAMLAN> Install-WindowsFeature -name Web-Server -IncludeManagementTools

Success Restart Needed Exit Code      Feature Result
------- -------------- ---------      --------------
True    No             Success        {Common HTTP Features, Default Document, D...


PS C:\Users\ADMINISTRATOR.RAMLAN> _
```



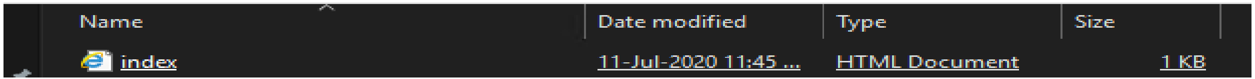
ADFS › OS (C:) › inetpub ›



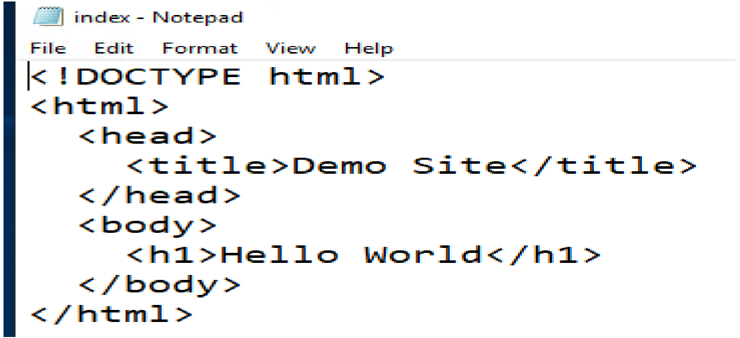
Name	Date modified	Type
adfs.ramlan.ca	11-Jul-2020 11:45 ...	File folder



ADFS › OS (C:) › inetpub › adfs.ramlan.ca

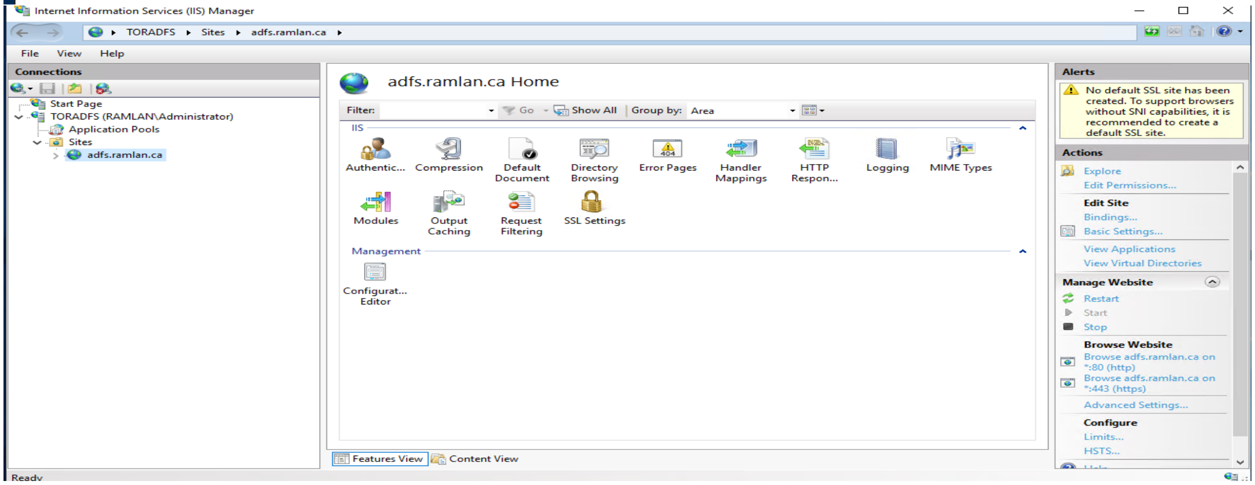


Name	Date modified	Type	Size
index	11-Jul-2020 11:45 ...	HTML Document	1 KB



index - Notepad

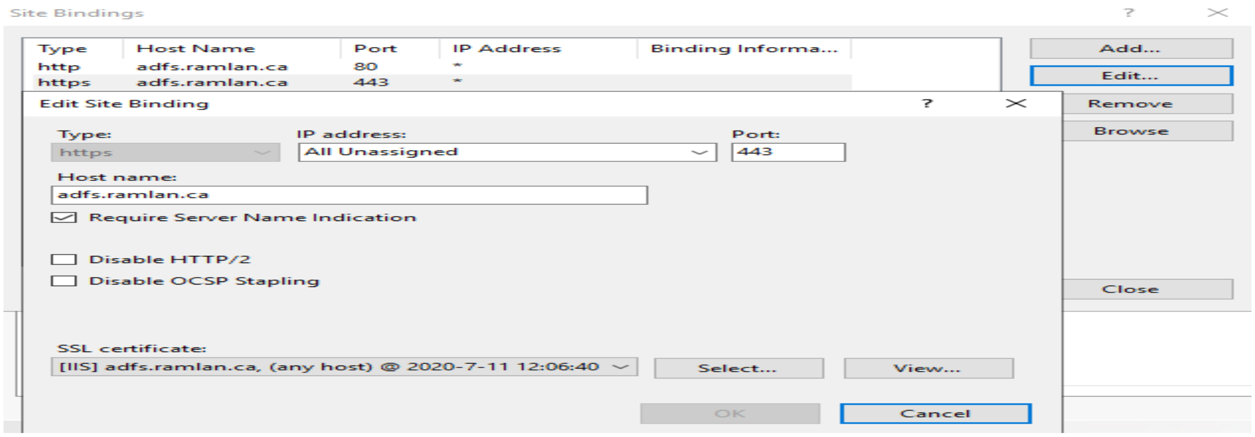
```
<!DOCTYPE html>
<html>
  <head>
    <title>Demo Site</title>
  </head>
  <body>
    <h1>Hello World</h1>
  </body>
</html>
```



Internet Information Services (IIS) Manager

TORADFS › Sites › adfs.ramlan.ca ›

No default SSL site has been created. To support browsers without SNI capabilities, it is recommended to create a default SSL site.



Site Bindings

Type	Host Name	Port	IP Address	Binding Informa...
http	adfs.ramlan.ca	80	*	
https	adfs.ramlan.ca	443	*	

Edit Site Binding

Type: https

IP address: All Unassigned

Port: 443

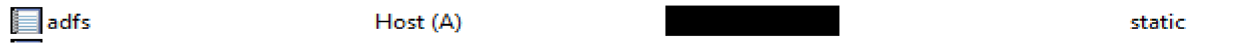
Host name: adfs.ramlan.ca

☑ Require Server Name Indication

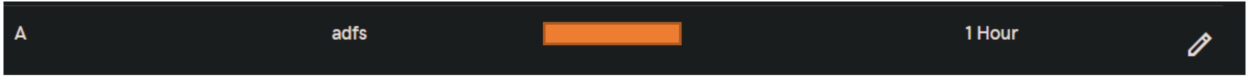
□ Disable HTTP/2

□ Disable OCSP Stapling

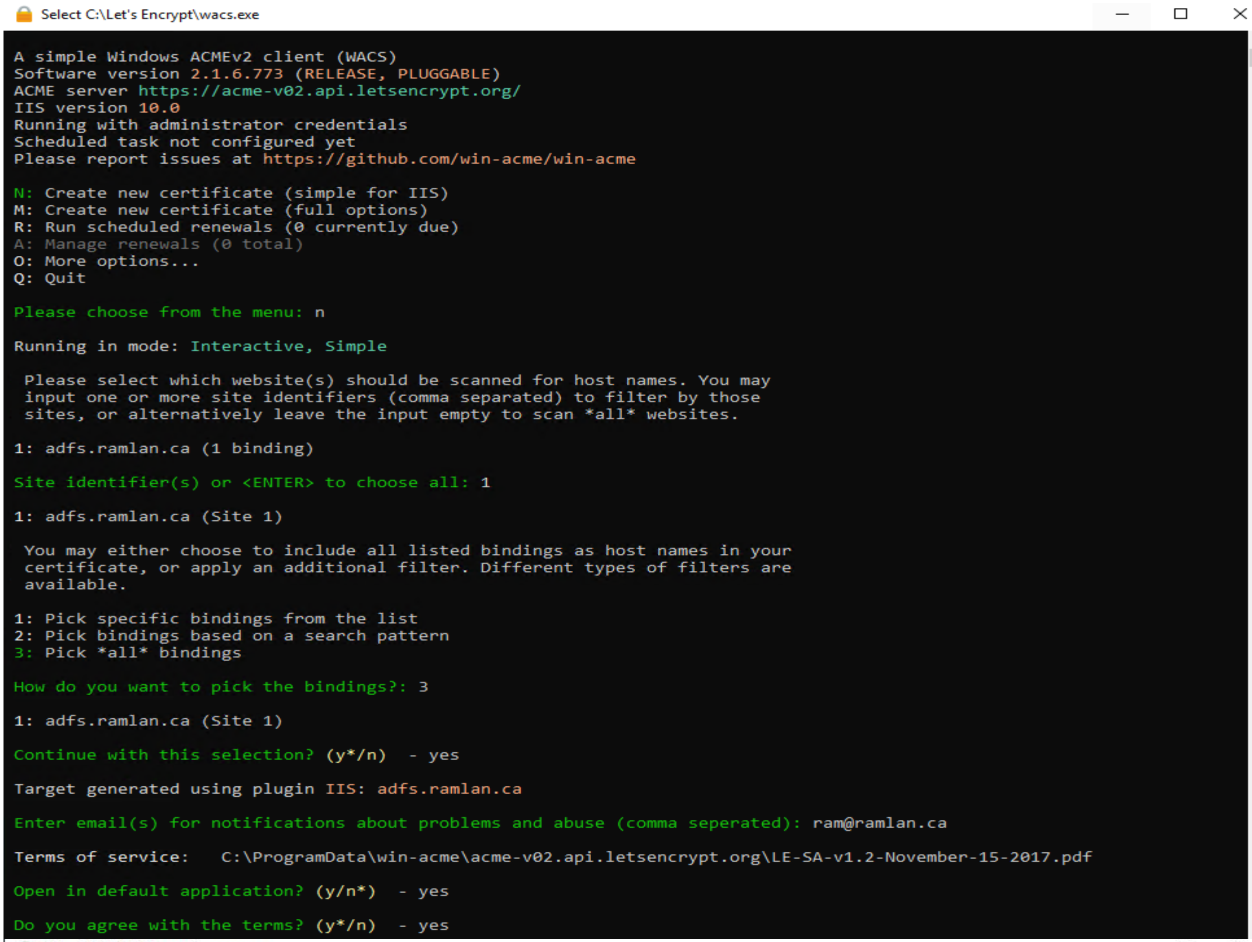
SSL certificate: [IIS] adfs.ramlan.ca, (any host) @ 2020-7-11 12:06:40



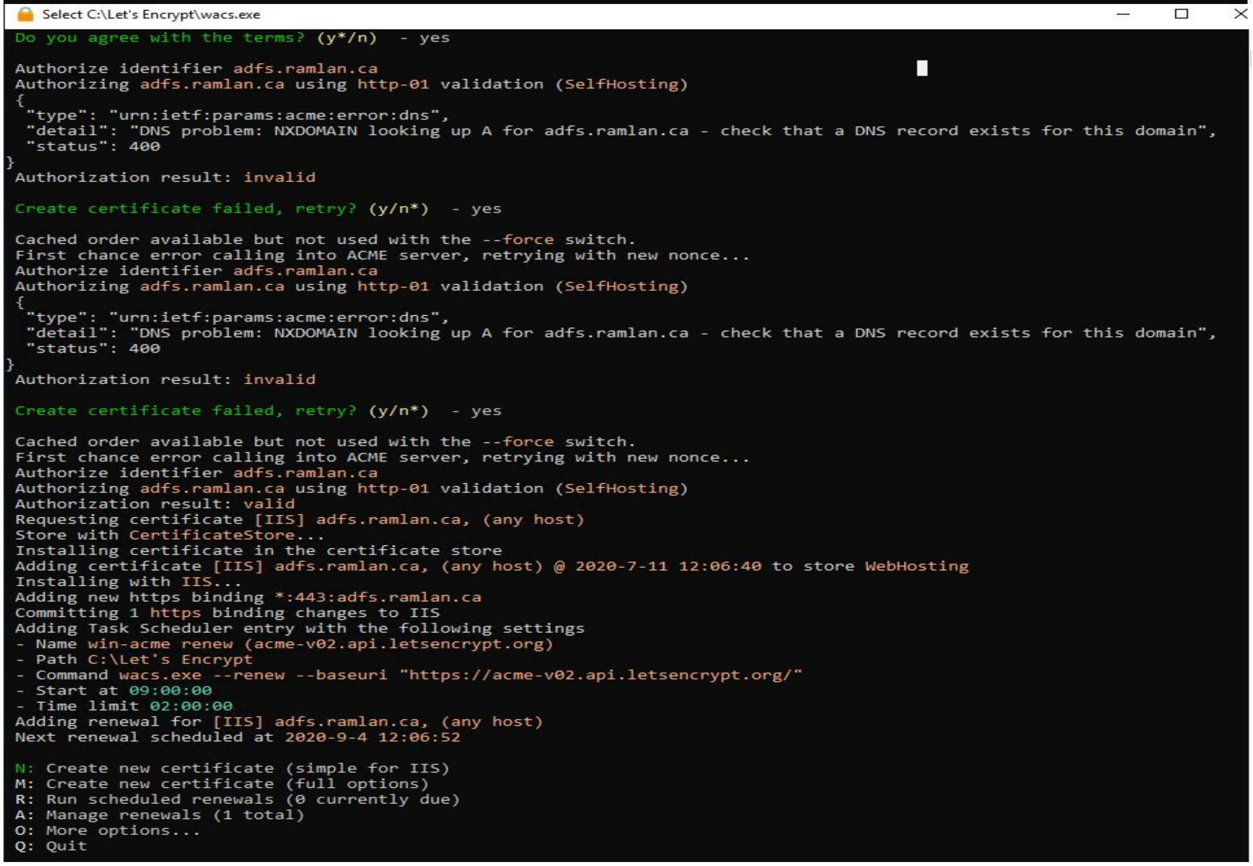
adfs Host (A) [redacted] static



A adfs [redacted] 1 Hour

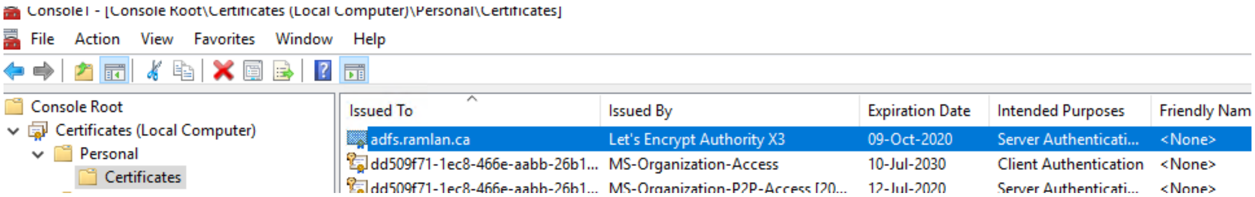


```
A simple Windows ACMEv2 client (WACS)
Software version 2.1.6.773 (RELEASE, PLUGGABLE)
ACME server https://acme-v02.api.letsencrypt.org/
IIS version 10.0
Running with administrator credentials
Scheduled task not configured yet
Please report issues at https://github.com/win-acme/win-acme

N: Create new certificate (simple for IIS)
M: Create new certificate (full options)
R: Run scheduled renewals (0 currently due)
A: Manage renewals (0 total)
O: More options...
Q: Quit

Please choose from the menu: n

Running in mode: Interactive, Simple

 Please select which website(s) should be scanned for host names. You may
 input one or more site identifiers (comma separated) to filter by those
 sites, or alternatively leave the input empty to scan *all* websites.

1: adfs.ramlan.ca (1 binding)

Site identifier(s) or <ENTER> to choose all: 1

1: adfs.ramlan.ca (Site 1)

 You may either choose to include all listed bindings as host names in your
 certificate, or apply an additional filter. Different types of filters are
 available.

1: Pick specific bindings from the list
2: Pick bindings based on a search pattern
3: Pick *all* bindings

How do you want to pick the bindings?: 3

1: adfs.ramlan.ca (Site 1)

Continue with this selection? (y*/n)  - yes

Target generated using plugin IIS: adfs.ramlan.ca

Enter email(s) for notifications about problems and abuse (comma seperated): ram@ramlan.ca

Terms of service:   C:\ProgramData\win-acme\acme-v02.api.letsencrypt.org\LE-SA-v1.2-November-15-2017.pdf

Open in default application? (y/n*)  - yes

Do you agree with the terms? (y*/n)  - yes
```



```
Do you agree with the terms? (y*/n)  - yes

Authorize identifier adfs.ramlan.ca
Authorizing adfs.ramlan.ca using http-01 validation (SelfHosting)
{
 "type": "urn:ietf:params:acme:error:dns",
 "detail": "DNS problem: NXDOMAIN looking up A for adfs.ramlan.ca - check that a DNS record exists for this domain",
 "status": 400
}
Authorization result: invalid

Create certificate failed, retry? (y/n*)  - yes

Cached order available but not used with the --force switch.
First chance error calling into ACME server, retrying with new nonce...
Authorize identifier adfs.ramlan.ca
Authorizing adfs.ramlan.ca using http-01 validation (SelfHosting)
{
 "type": "urn:ietf:params:acme:error:dns",
 "detail": "DNS problem: NXDOMAIN looking up A for adfs.ramlan.ca - check that a DNS record exists for this domain",
 "status": 400
}
Authorization result: invalid

Create certificate failed, retry? (y/n*)  - yes

Cached order available but not used with the --force switch.
First chance error calling into ACME server, retrying with new nonce...
Authorize identifier adfs.ramlan.ca
Authorizing adfs.ramlan.ca using http-01 validation (SelfHosting)
Authorization result: valid
Requesting certificate [IIS] adfs.ramlan.ca, (any host)
Store with CertificateStore...
Installing certificate in the certificate store
Adding certificate [IIS] adfs.ramlan.ca, (any host) @ 2020-7-11 12:06:40 to store WebHosting
Installing with IIS...
Adding new https binding *:443:adfs.ramlan.ca
Committing 1 https binding changes to IIS
Adding Task Scheduler entry with the following settings
- Name win-acme renew (acme-v02.api.letsencrypt.org)
- Path C:\Let's Encrypt
- Command wacs.exe --renew --baseuri "https://acme-v02.api.letsencrypt.org/"
- Start at 09:00:00
- Time limit 02:00:00
Adding renewal for [IIS] adfs.ramlan.ca, (any host)
Next renewal scheduled at 2020-9-4 12:06:52

N: Create new certificate (simple for IIS)
M: Create new certificate (full options)
R: Run scheduled renewals (0 currently due)
A: Manage renewals (1 total)
O: More options...
Q: Quit
```

This is the certificate, I will be using for adfs. I have exported the certificate in PFX format. If you want the steps on how to do it – check this link - https://www.alitajran.com/export-lets-encrypt-certificate-in-windows-server/

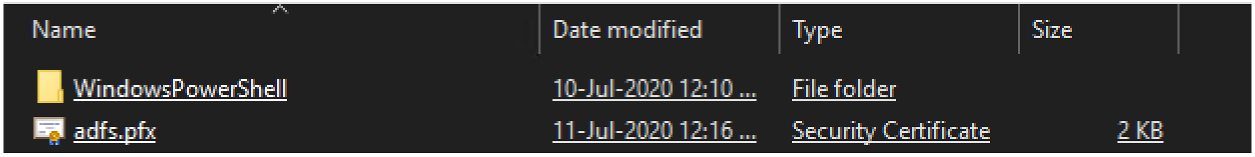


Console1 - [Console Root\Certificates (Local Computer)\Personal\Certificates]

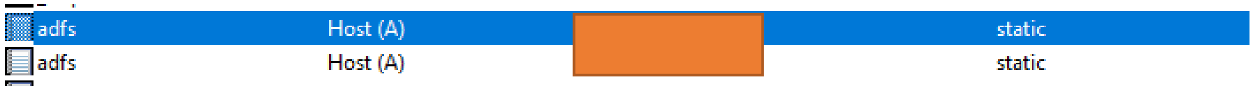
File Action View Favorites Window Help

Console Root
- Certificates (Local Computer)
  - Personal
    - Certificates

Issued To	Issued By	Expiration Date	Intended Purposes	Friendly Nam
adfs.ramlan.ca	Let's Encrypt Authority X3	09-Oct-2020	Server Authenticati...	<None>
dd509f71-1ec8-466e-aabb-26b1...	MS-Organization-Access	10-Jul-2030	Client Authentication	<None>
dd509f71-1ec8-466e-aabb-26b1...	MS-Organization-P2P-Access [20...	12-Jul-2020	Server Authenticati...	<None>

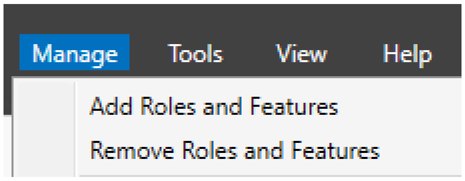


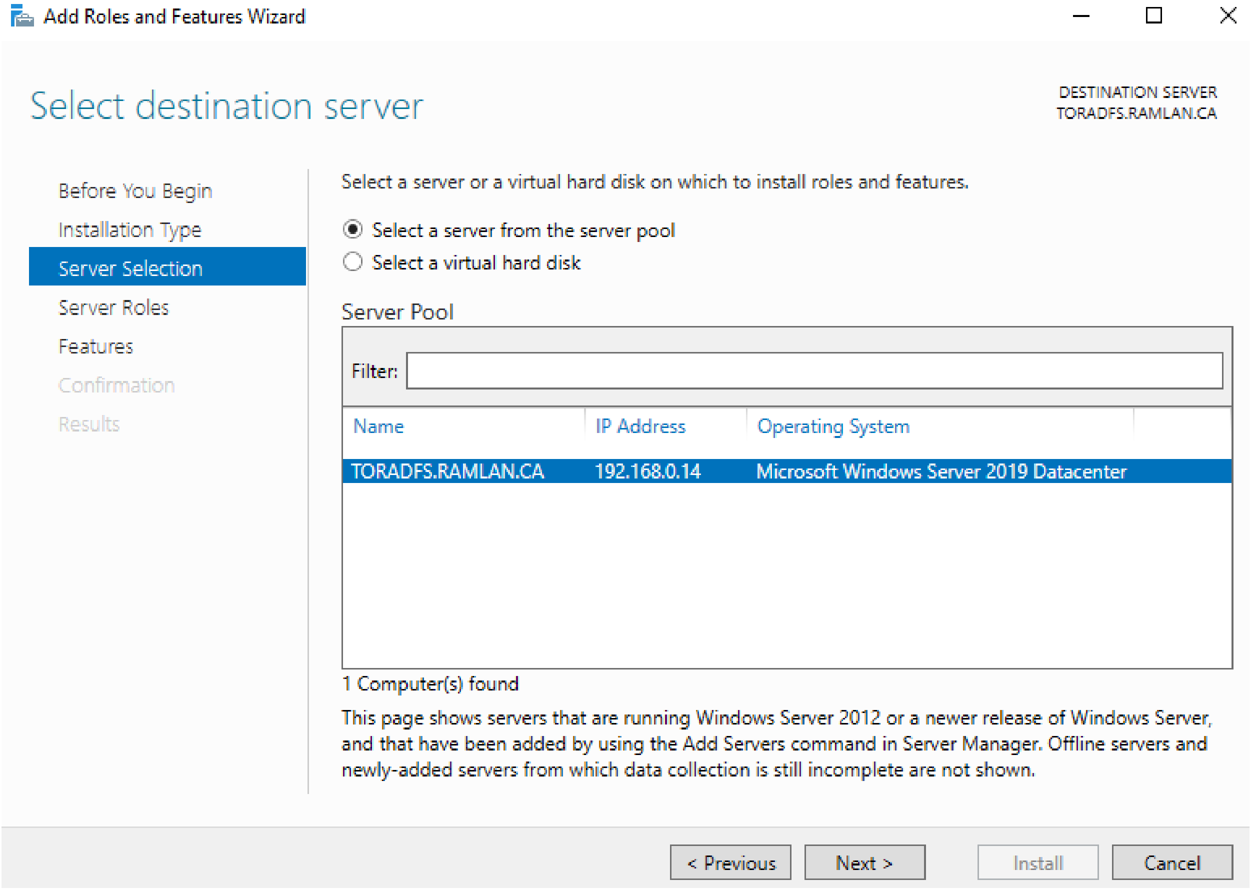
Name	Date modified	Type	Size
WindowsPowerShell	10-Jul-2020 12:10 ...	File folder	
adfs.pfx	11-Jul-2020 12:16 ...	Security Certificate	2 KB



adfs	Host (A)	[redacted]	static
adfs	Host (A)		static

Now we can install ADFS role.





Add Roles and Features Wizard

Select destination server

DESTINATION SERVER
TORADFS.RAMLAN.CA

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

● Select a server from the server pool

○ Select a virtual hard disk

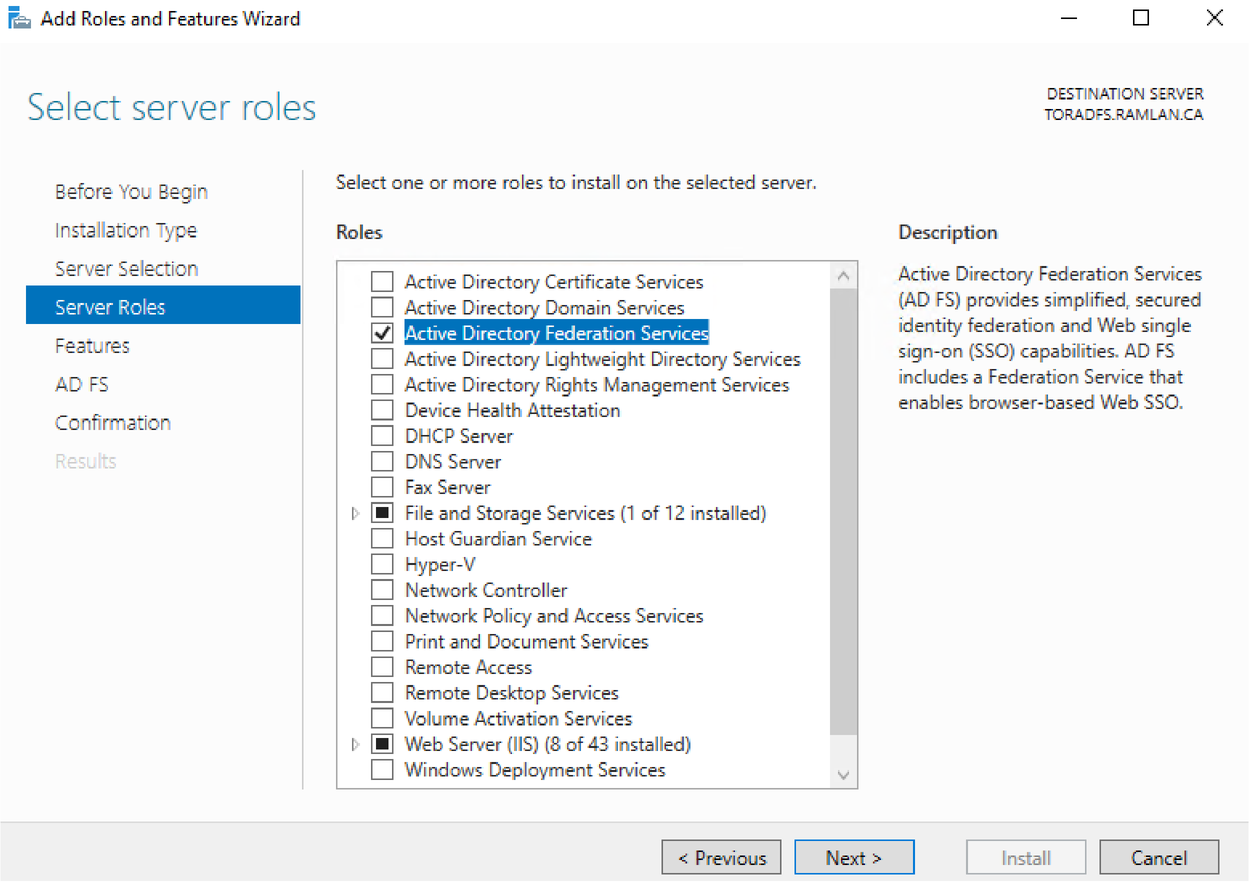
Server Pool

Filter:

Name	IP Address	Operating System
TORADFS.RAMLAN.CA	192.168.0.14	Microsoft Windows Server 2019 Datacenter

1 Computer(s) found

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



Select server roles

DESTINATION SERVER
TORADFS.RAMLAN.CA

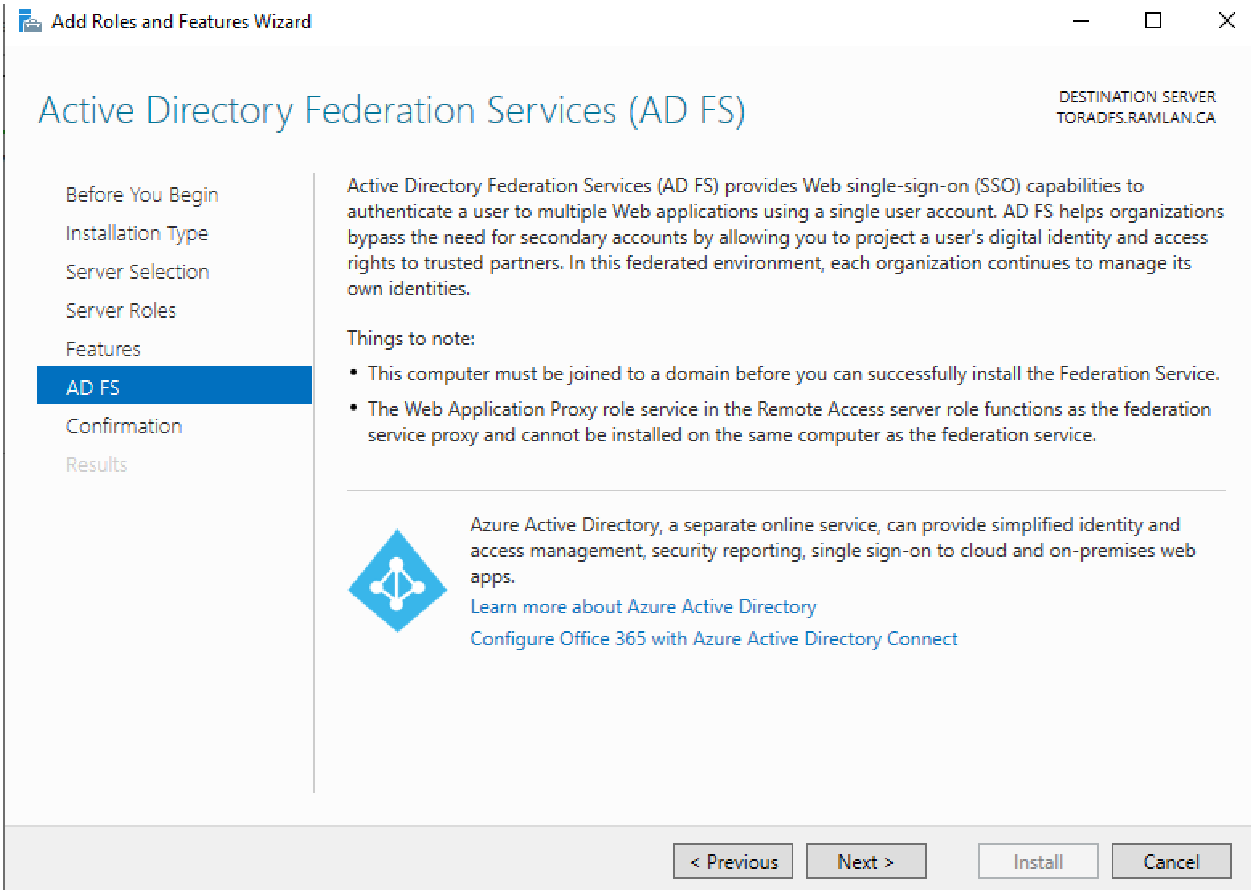
Select one or more roles to install on the selected server.

Roles

- ☐ Active Directory Certificate Services
- ☐ Active Directory Domain Services
- ☑ Active Directory Federation Services
- ☐ Active Directory Lightweight Directory Services
- ☐ Active Directory Rights Management Services
- ☐ Device Health Attestation
- ☐ DHCP Server
- ☐ DNS Server
- ☐ Fax Server
- ■ File and Storage Services (1 of 12 installed)
- ☐ Host Guardian Service
- ☐ Hyper-V
- ☐ Network Controller
- ☐ Network Policy and Access Services
- ☐ Print and Document Services
- ☐ Remote Access
- ☐ Remote Desktop Services
- ☐ Volume Activation Services
- ■ Web Server (IIS) (8 of 43 installed)
- ☐ Windows Deployment Services

Description

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



Active Directory Federation Services (AD FS)

DESTINATION SERVER
TORADFS.RAMLAN.CA

Active Directory Federation Services (AD FS) provides Web single-sign-on (SSO) capabilities to authenticate a user to multiple Web applications using a single user account. AD FS helps organizations bypass the need for secondary accounts by allowing you to project a user's digital identity and access rights to trusted partners. In this federated environment, each organization continues to manage its own identities.

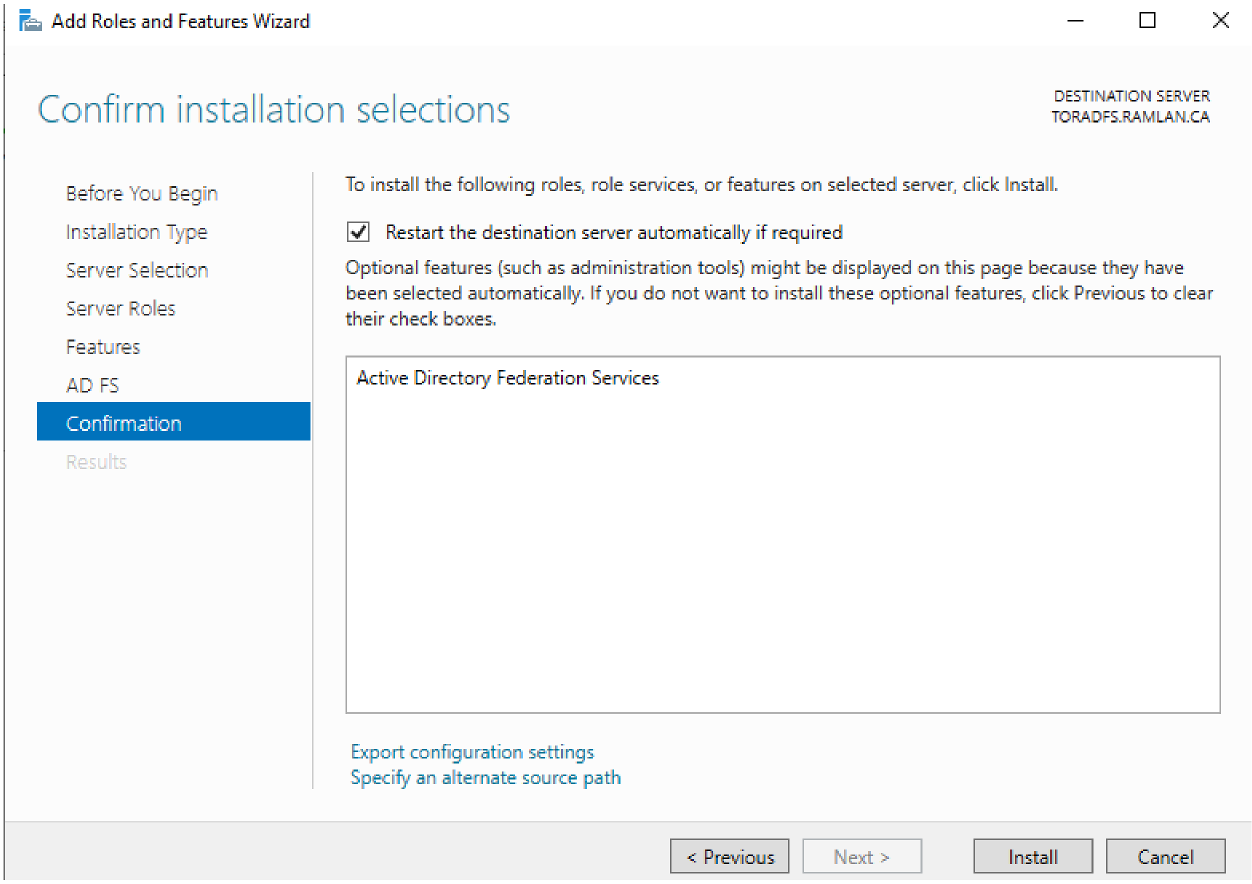
Things to note:

- This computer must be joined to a domain before you can successfully install the Federation Service.
- The Web Application Proxy role service in the Remote Access server role functions as the federation service proxy and cannot be installed on the same computer as the federation service.

Azure Active Directory, a separate online service, can provide simplified identity and access management, security reporting, single sign-on to cloud and on-premises web apps.

Learn more about Azure Active Directory

Configure Office 365 with Azure Active Directory Connect



Confirm installation selections

DESTINATION SERVER
TORADFS.RAMLAN.CA

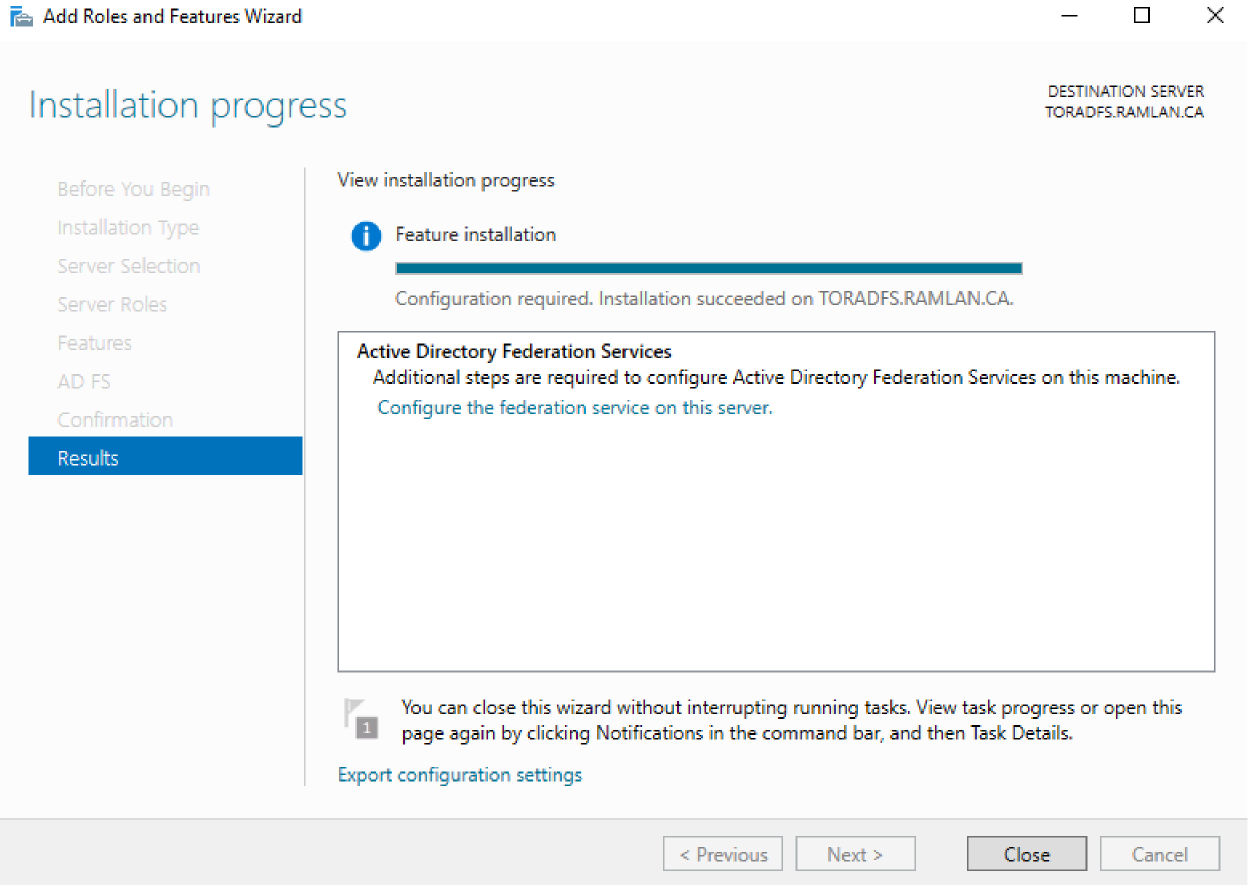
To install the following roles, role services, or features on selected server, click Install.

☑ Restart the destination server automatically if required

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

Active Directory Federation Services

Export configuration settings
Specify an alternate source path



Installation progress

DESTINATION SERVER
TORADFS.RAMLAN.CA

View installation progress

Feature installation

Configuration required. Installation succeeded on TORADFS.RAMLAN.CA.

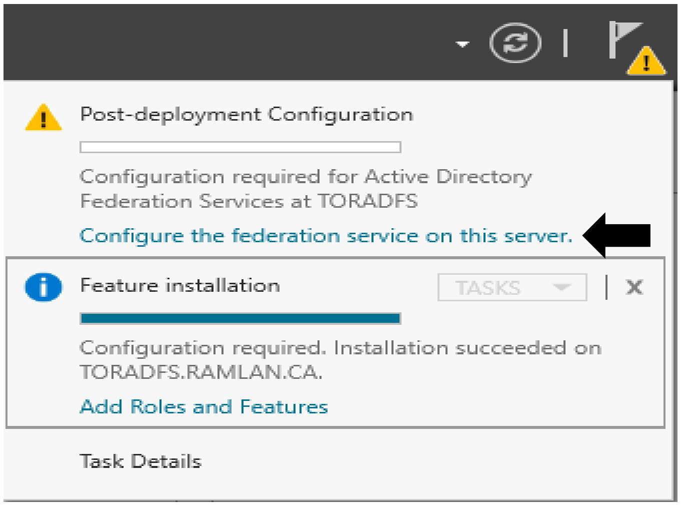
Active Directory Federation Services

Additional steps are required to configure Active Directory Federation Services on this machine.

Configure the federation service on this server.

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

Export configuration settings



⚠ Post-deployment Configuration

Configuration required for Active Directory Federation Services at TORADFS

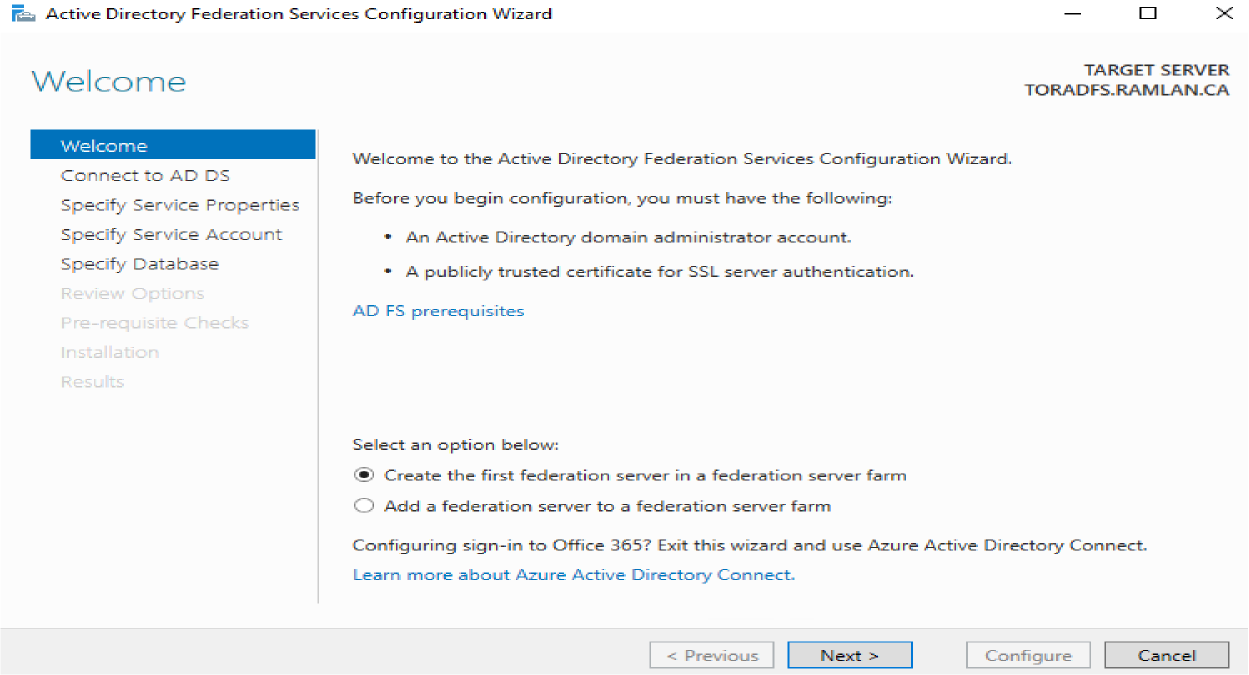
Configure the federation service on this server.

Feature installation

Configuration required. Installation succeeded on TORADFS.RAMLAN.CA.

Add Roles and Features

Task Details



Active Directory Federation Services Configuration Wizard

Welcome

TARGET SERVER
TORADFS.RAMLAN.CA

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

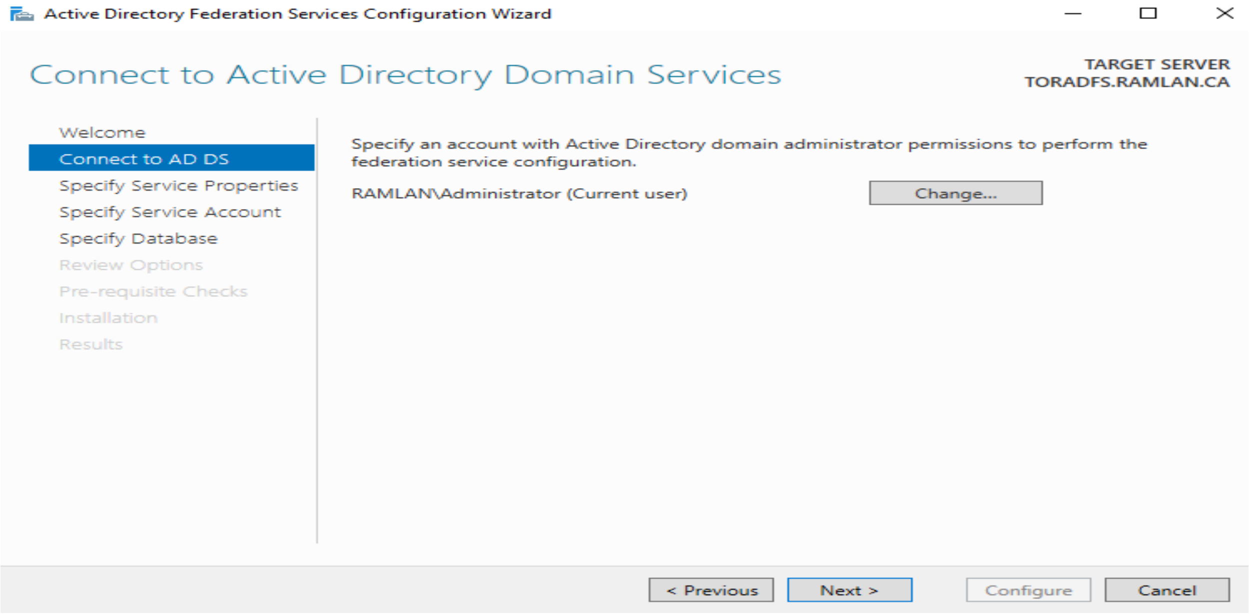
Select an option below:

● 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.

Learn more about Azure Active Directory Connect.



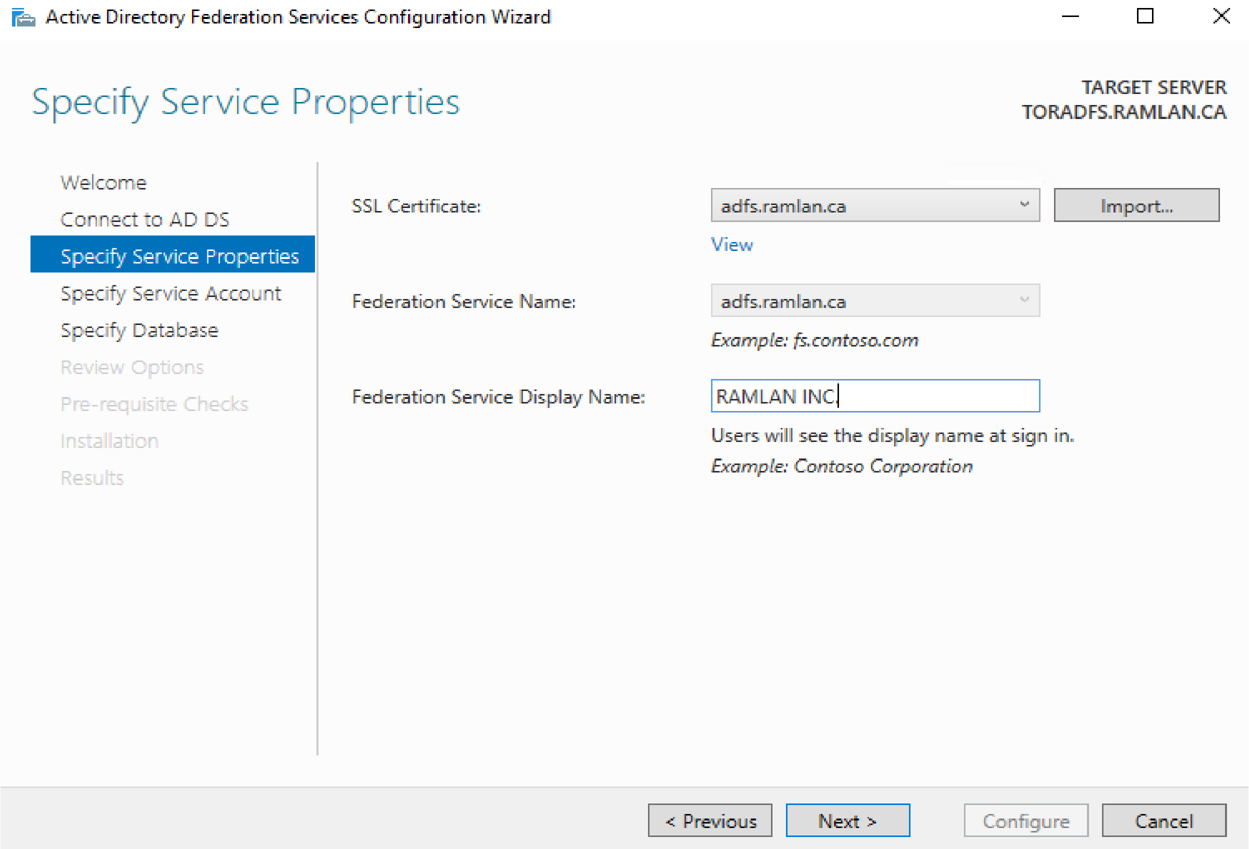
Active Directory Federation Services Configuration Wizard

Connect to Active Directory Domain Services

TARGET SERVER
TORADFS.RAMLAN.CA

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

RAMLAN\Administrator (Current user)



Specify Service Properties

TARGET SERVER
TORADFS.RAMLAN.CA

SSL Certificate: adfs.ramlan.ca

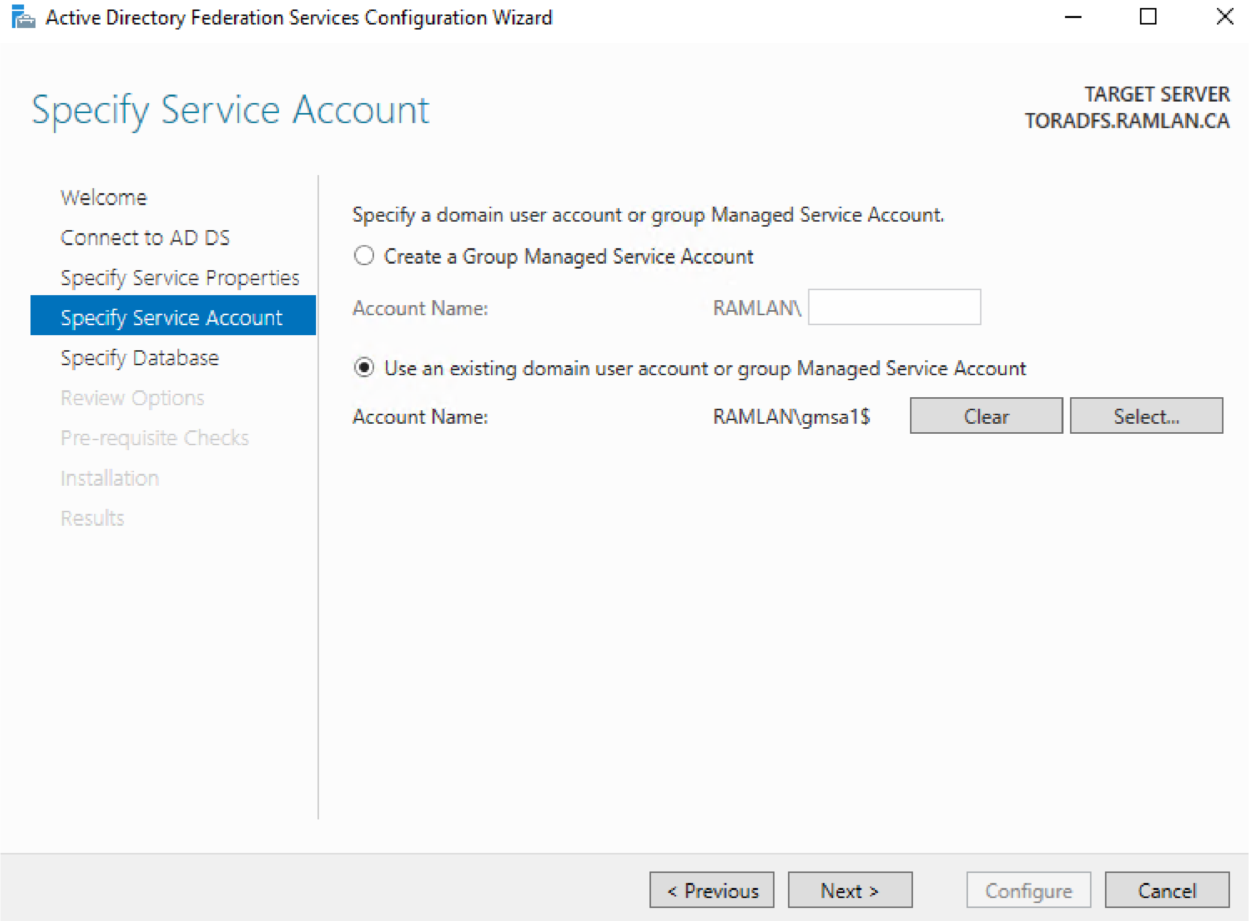
Federation Service Name: adfs.ramlan.ca

Example: fs.contoso.com

Federation Service Display Name: RAMLAN INC

Users will see the display name at sign in.

Example: Contoso Corporation



Specify Service Account

TARGET SERVER
TORADFS.RAMLAN.CA

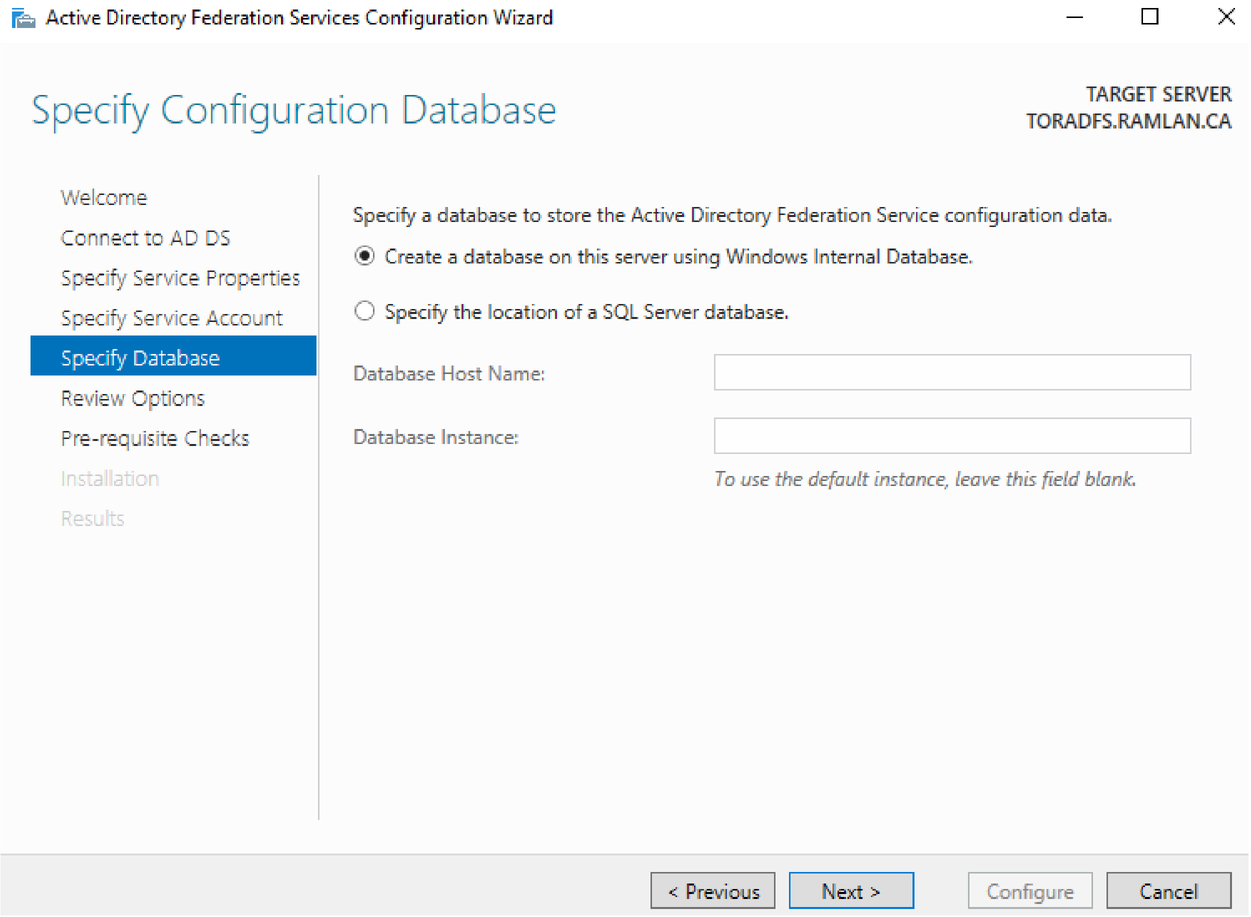
Specify a domain user account or group Managed Service Account.

○ Create a Group Managed Service Account

Account Name: RAMLAN\

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

Account Name: RAMLAN\gmsa1$



Specify Configuration Database

TARGET SERVER
TORADFS.RAMLAN.CA

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

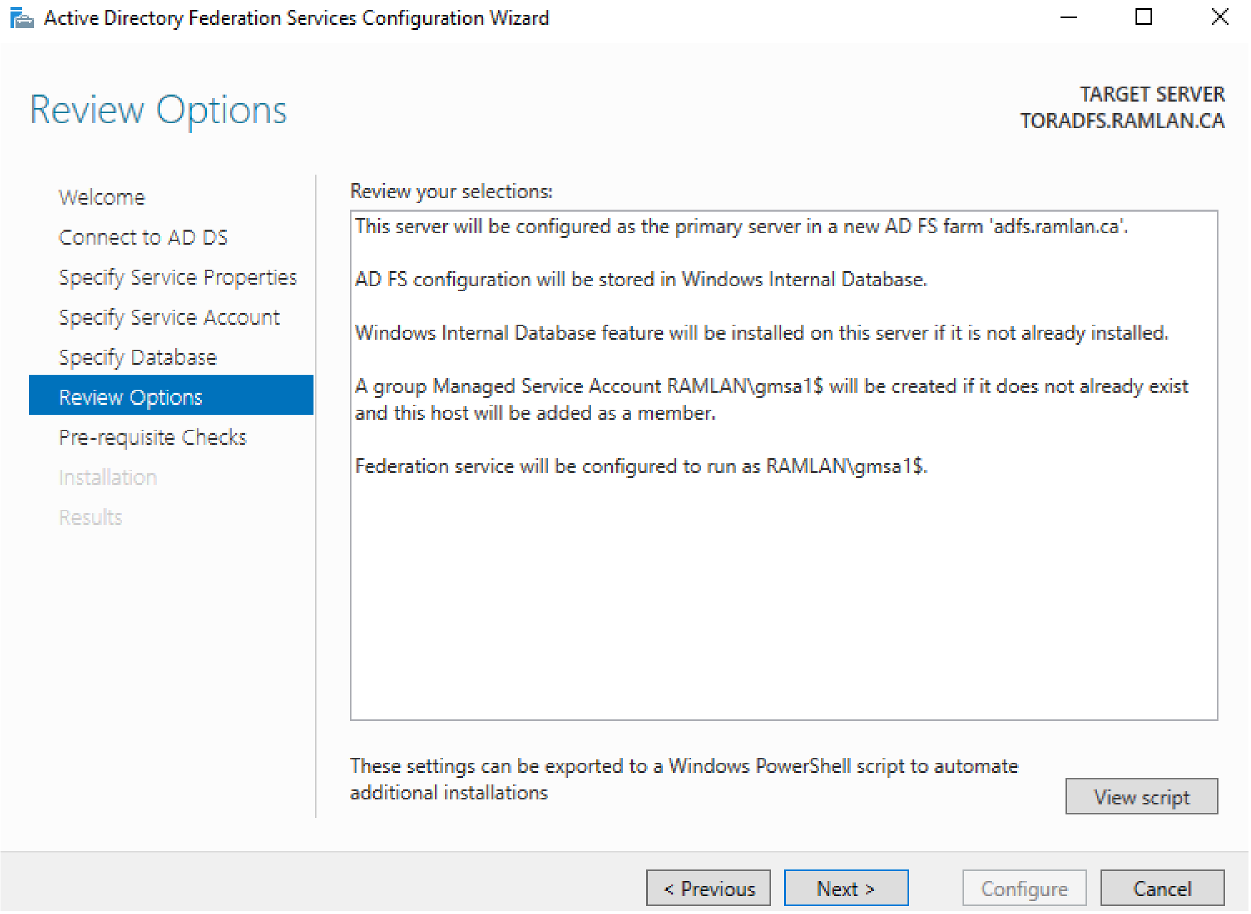
● Create a database on this server using Windows Internal Database.

○ Specify the location of a SQL Server database.

Database Host Name:

Database Instance:

To use the default instance, leave this field blank.



Review Options

TARGET SERVER
TORADFS.RAMLAN.CA

Review your selections:

This server will be configured as the primary server in a new AD FS farm 'adfs.ramlan.ca'.

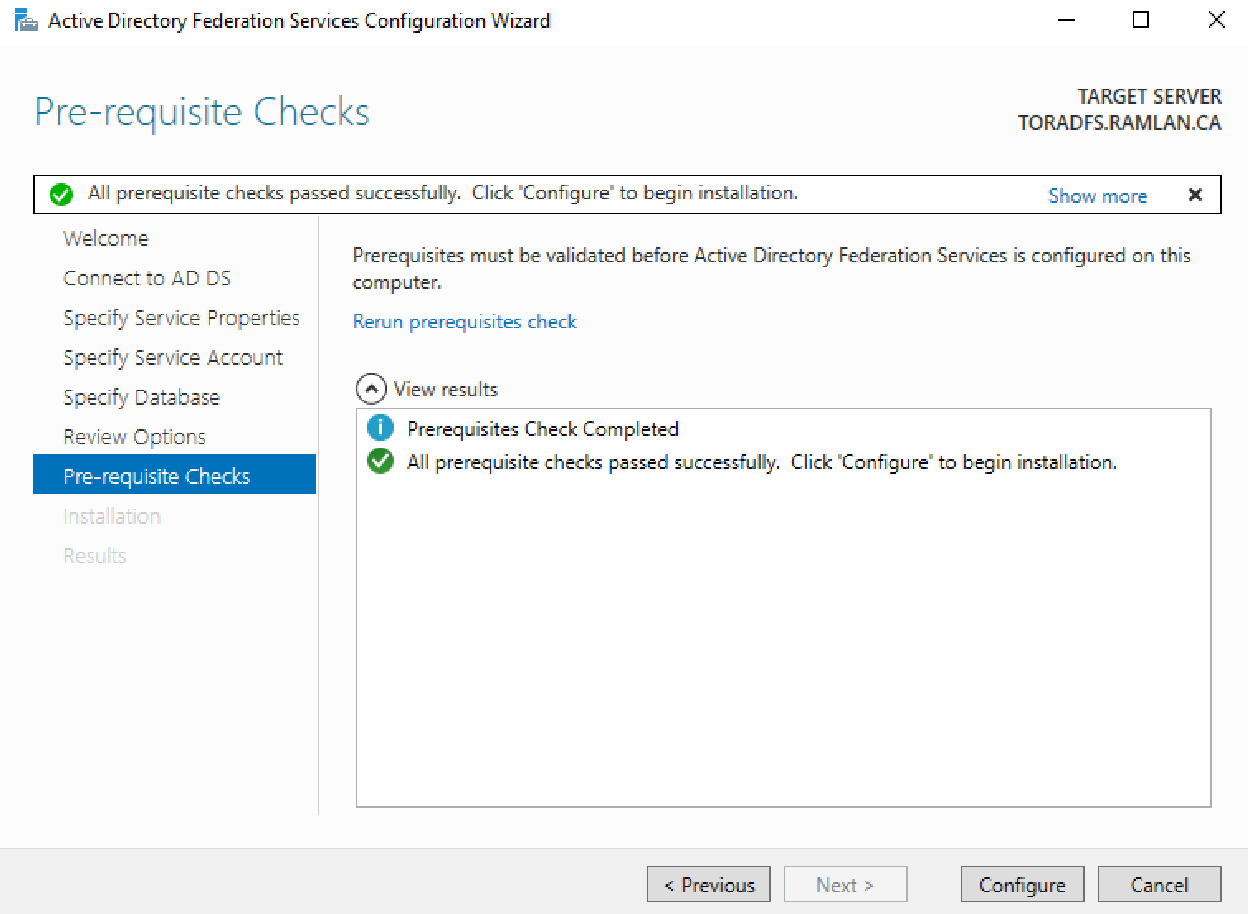
AD FS configuration will be stored in Windows Internal Database.

Windows Internal Database feature will be installed on this server if it is not already installed.

A group Managed Service Account RAMLAN\gmsa1$ will be created if it does not already exist and this host will be added as a member.

Federation service will be configured to run as RAMLAN\gmsa1$.

These settings can be exported to a Windows PowerShell script to automate additional installations



Pre-requisite Checks

TARGET SERVER
TORADFS.RAMLAN.CA

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

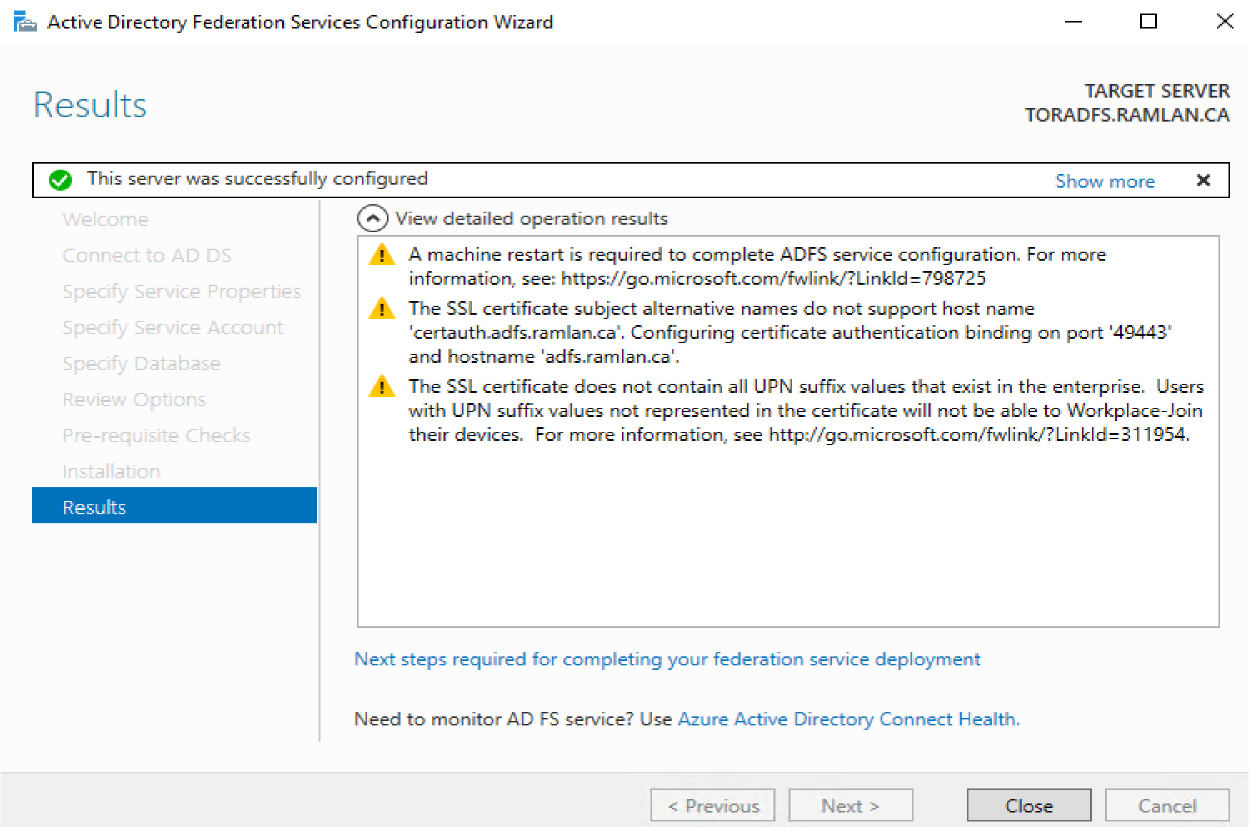
Prerequisites must be validated before Active Directory Federation Services is configured on this computer.

Rerun prerequisites check

View results

Prerequisites Check Completed

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



Results

TARGET SERVER
TORADFS.RAMLAN.CA

This server was successfully configured

View detailed operation results

A machine restart is required to complete ADFS service configuration. For more information, see: https://go.microsoft.com/fwlink/?LinkId=798725

The SSL certificate subject alternative names do not support host name 'certauth.adfs.ramlan.ca'. Configuring certificate authentication binding on port '49443' and hostname 'adfs.ramlan.ca'.

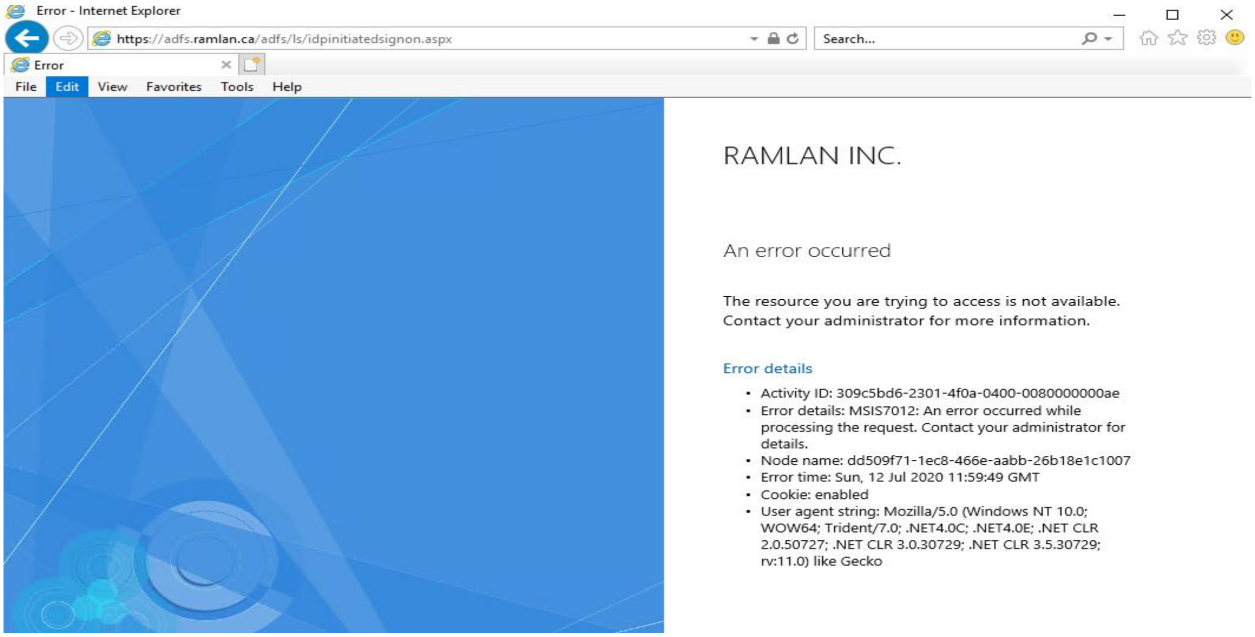
The SSL certificate does not contain all UPN suffix values that exist in the enterprise. Users with UPN suffix values not represented in the certificate will not be able to Workplace-Join their devices. For more information, see http://go.microsoft.com/fwlink/?LinkId=311954.

Next steps required for completing your federation service deployment

Need to monitor AD FS service? Use Azure Active Directory Connect Health.

Click Close and Restart the server.

Open IE and type - https://adfs.ramlan.ca/adfs/ls/idpinitiatedsignon.aspx


Error - Internet Explorer
https://adfs.ramlan.ca/adfs/ls/idpinitiatedsignon.aspx
Search...
Error
File
Edit
View
Favorites
Tools
Help

RAMLAN INC.

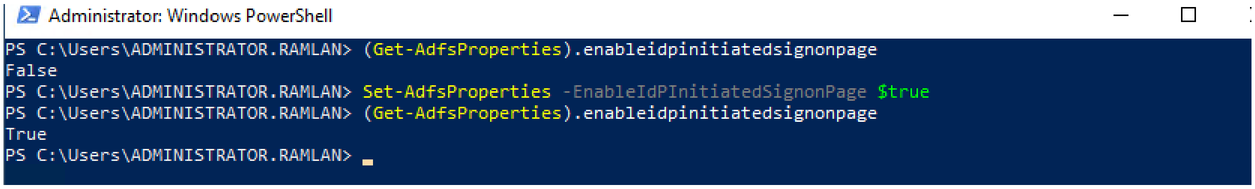
An error occurred

The resource you are trying to access is not available. Contact your administrator for more information.

Error details

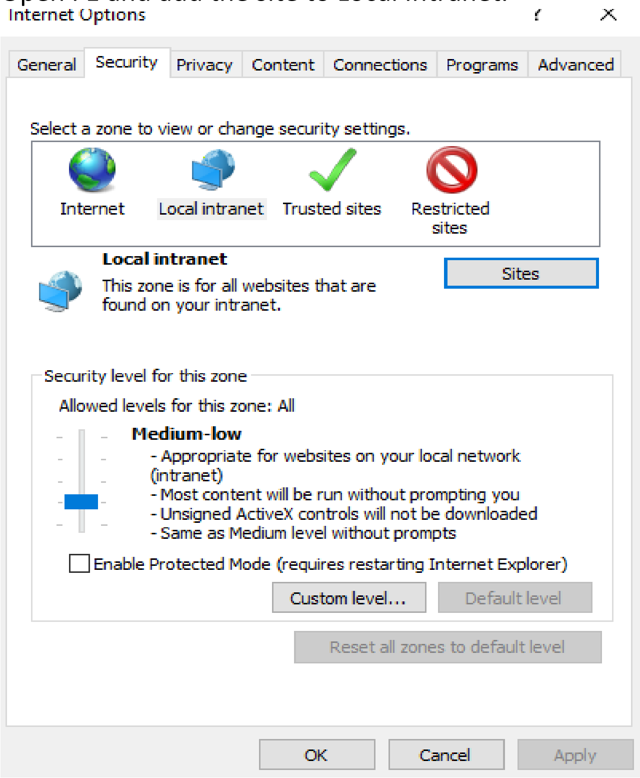
- Activity ID: 309c5bd6-2301-4f0a-0400-0080000000ae
- Error details: MSIS7012: An error occurred while processing the request. Contact your administrator for details.
- Node name: dd509f71-1ec8-466e-aabb-26b18e1c1007
- Error time: Sun, 12 Jul 2020 11:59:49 GMT
- Cookie: enabled
- User agent string: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; .NET4.0C; .NET4.0E; .NET CLR 2.0.50727; .NET CLR 3.0.30729; .NET CLR 3.5.30729; rv:11.0) like Gecko

We encountered error. Below is the fix.



```
PS C:\Users\ADMINISTRATOR.RAMLAN> (Get-AdfsProperties).enableidpinitiatedsignonpage
False
PS C:\Users\ADMINISTRATOR.RAMLAN> Set-AdfsProperties -EnableIdPInitiatedSignonPage $true
PS C:\Users\ADMINISTRATOR.RAMLAN> (Get-AdfsProperties).enableidpinitiatedsignonpage
True
PS C:\Users\ADMINISTRATOR.RAMLAN> _
```

Open I E and add the site to Local Intranet.



Select a zone to view or change security settings.

Local intranet

This zone is for all websites that are found on your intranet.

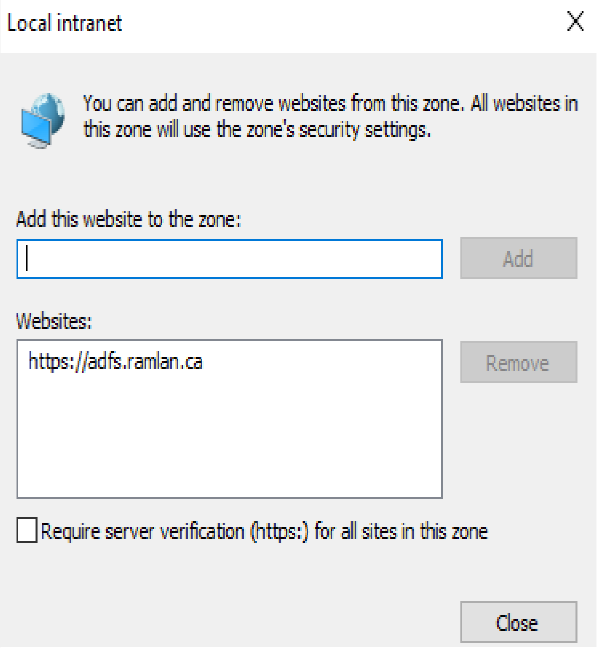
Security level for this zone

Allowed levels for this zone: All

Medium-low

- Appropriate for websites on your local network (intranet)
- Most content will be run without prompting you
- Unsigned ActiveX controls will not be downloaded
- Same as Medium level without prompts

☐ Enable Protected Mode (requires restarting Internet Explorer)



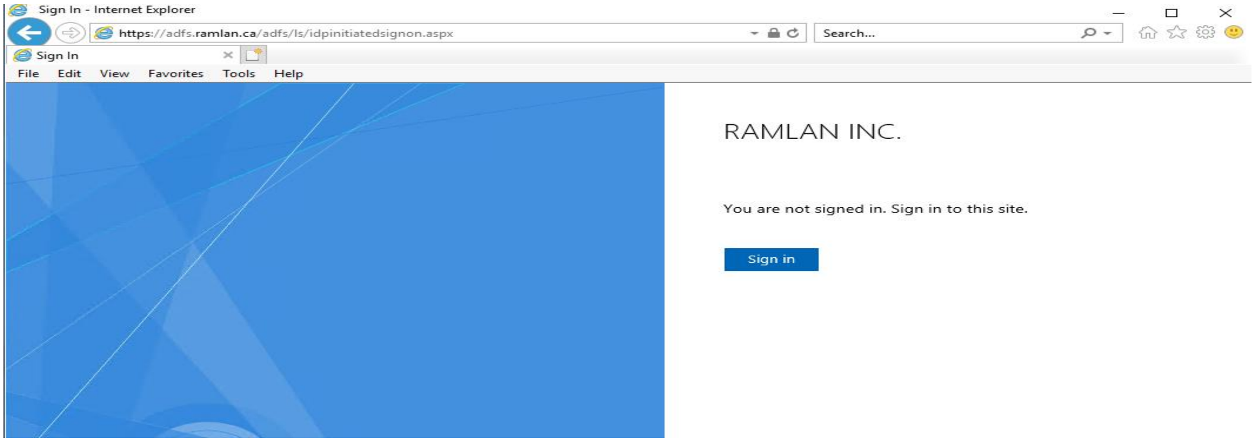
You can add and remove websites from this zone. All websites in this zone will use the zone's security settings.

Add this website to the zone:

Websites:

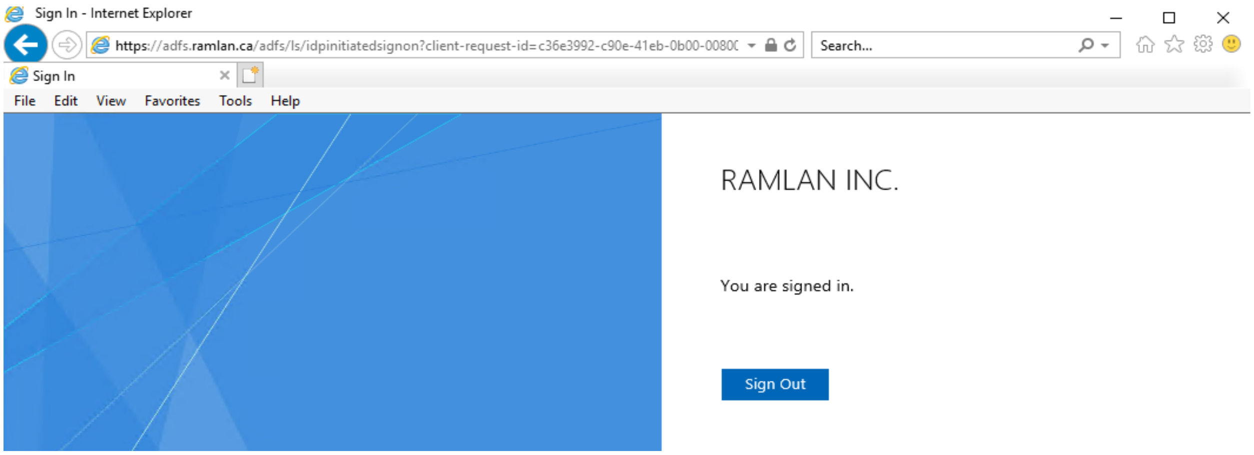
https://adfs.ramlan.ca

☐ Require server verification (https:) for all sites in this zone


Sign In - Internet Explorer
https://adfs.ramlan.ca/adfs/ls/idpinitiatedsignon.aspx
Search...
Sign In
File Edit View Favorites Tools Help
Sign in

RAMLAN INC.

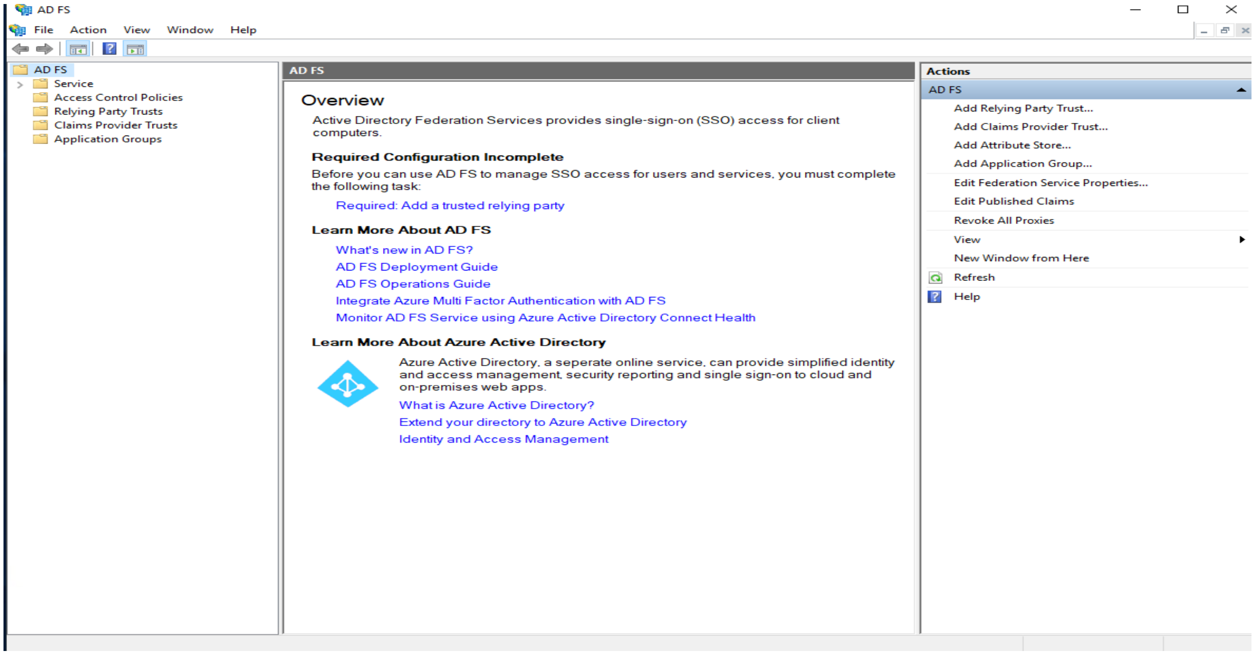
You are not signed in. Sign in to this site.


Sign In - Internet Explorer
https://adfs.ramlan.ca/adfs/ls/idpinitiatedsignon?client-request-id=c36e3992-c90e-41eb-0b00-0080C
Search...
Sign In
File Edit View Favorites Tools Help
Sign Out

RAMLAN INC.

You are signed in.

This is ADFS Management Console. There are few things we have to configure. I will not go into detail. It is for you to explore.



Overview

Active Directory Federation Services provides single-sign-on (SSO) access for client computers.

Required Configuration Incomplete

Before you can use AD FS to manage SSO access for users and services, you must complete the following task:

Required: Add a trusted relying party

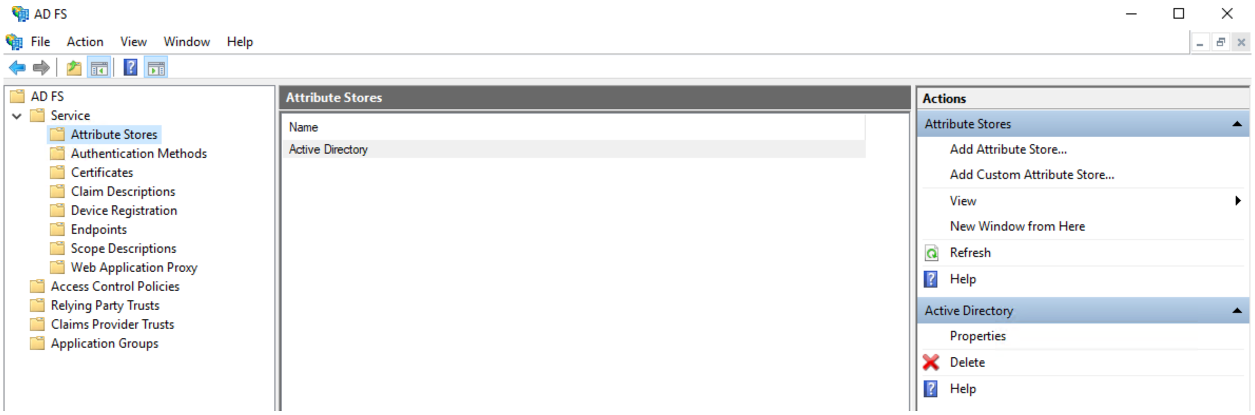
Learn More About AD FS

What's new in AD FS?
AD FS Deployment Guide
AD FS Operations Guide
Integrate Azure Multi Factor Authentication with AD FS
Monitor AD FS Service using Azure Active Directory Connect Health

Learn More About Azure Active Directory

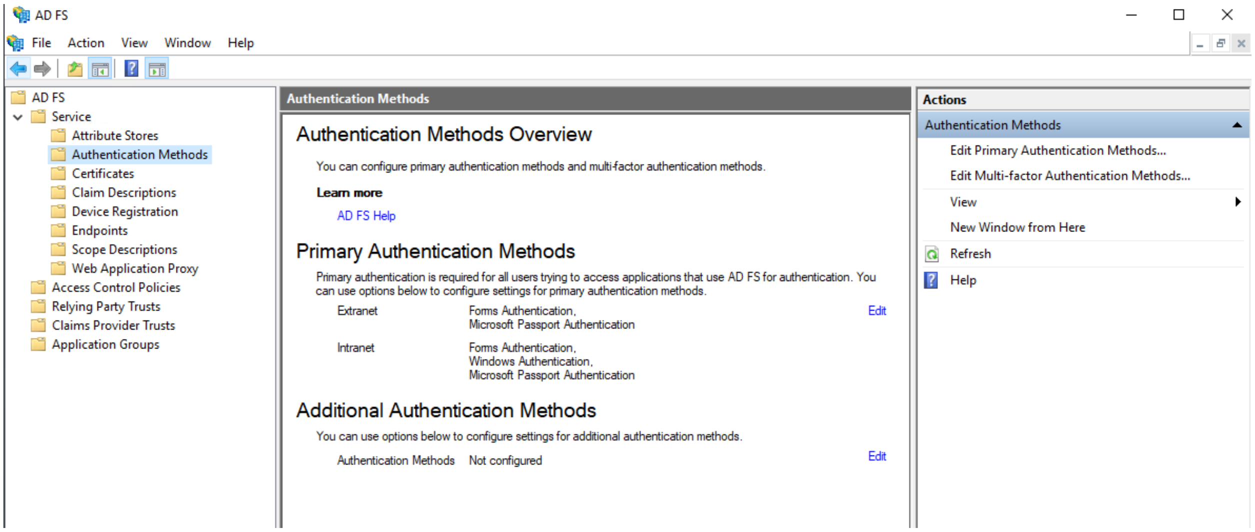
Azure Active Directory, a seperate online service, can provide simplified identity and access management, security reporting and single sign-on to cloud and on-premises web apps.

What is Azure Active Directory?
Extend your directory to Azure Active Directory
Identity and Access Management



Attribute Stores

Name
Active Directory



Authentication Methods

Authentication Methods Overview

You can configure primary authentication methods and multi-factor authentication methods.

Learn more

AD FS Help

Primary Authentication Methods

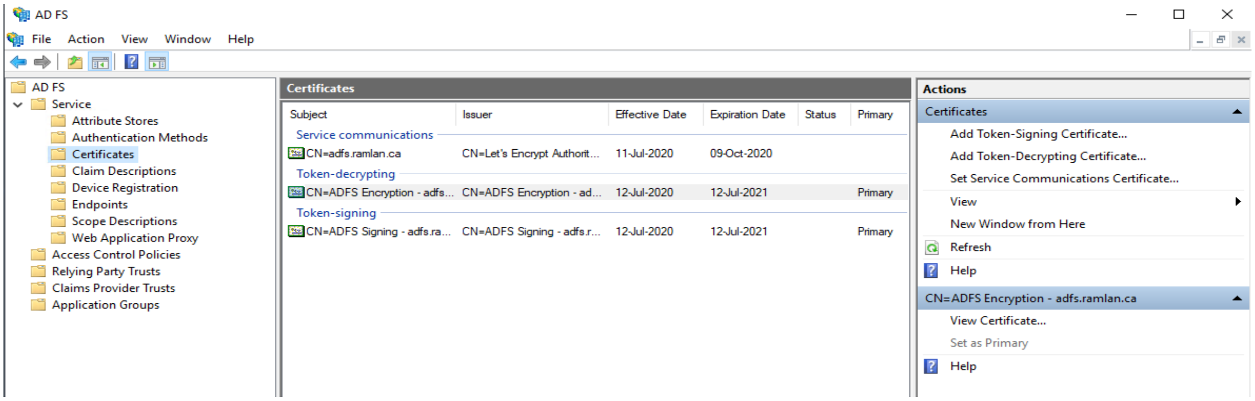
Primary authentication is required for all users trying to access applications that use AD FS for authentication. You can use options below to configure settings for primary authentication methods.

Extranet	Forms Authentication, Microsoft Passport Authentication	Edit
Intranet	Forms Authentication, Windows Authentication, Microsoft Passport Authentication	

Additional Authentication Methods

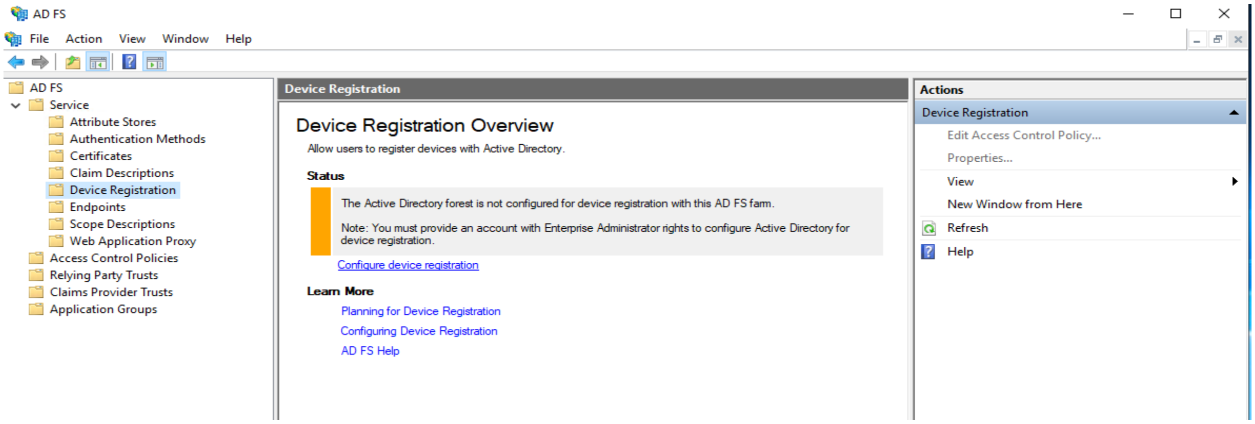
You can use options below to configure settings for additional authentication methods.

Authentication Methods	Not configured	Edit



Certificates

Subject	Issuer	Effective Date	Expiration Date	Status	Primary
Service communications					
CN=adfs.ramlan.ca	CN=Let's Encrypt Authorit...	11-Jul-2020	09-Oct-2020		
Token-decrypting					
CN=ADFS Encryption - adfs...	CN=ADFS Encryption - ad...	12-Jul-2020	12-Jul-2021		Primary
Token-signing					
CN=ADFS Signing - adfs.ra...	CN=ADFS Signing - adfs.r...	12-Jul-2020	12-Jul-2021		Primary



Device Registration

Device Registration Overview

Allow users to register devices with Active Directory.

Status

The Active Directory forest is not configured for device registration with this AD FS farm.

Note: You must provide an account with Enterprise Administrator rights to configure Active Directory for device registration.

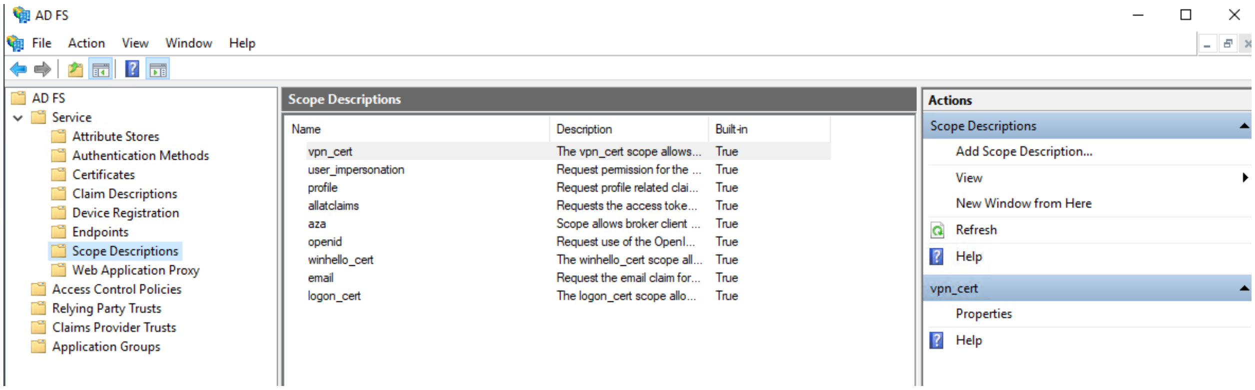
Configure device registration

Learn More

Planning for Device Registration

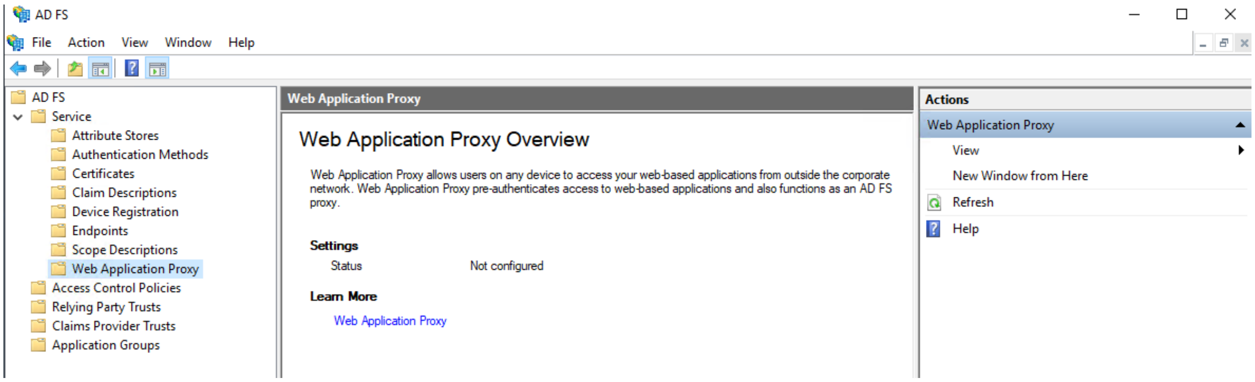
Configuring Device Registration

AD FS Help



Scope Descriptions

Name	Description	Built-in
vpn_cert	The vpn_cert scope allows...	True
user_impersonation	Request permission for the ...	True
profile	Request profile related clai...	True
allatclaims	Requests the access toke...	True
aza	Scope allows broker client ...	True
openid	Request use of the OpenI...	True
winhello_cert	The winhello_cert scope all...	True
email	Request the email claim for...	True
logon_cert	The logon_cert scope allo...	True



Web Application Proxy

Web Application Proxy Overview

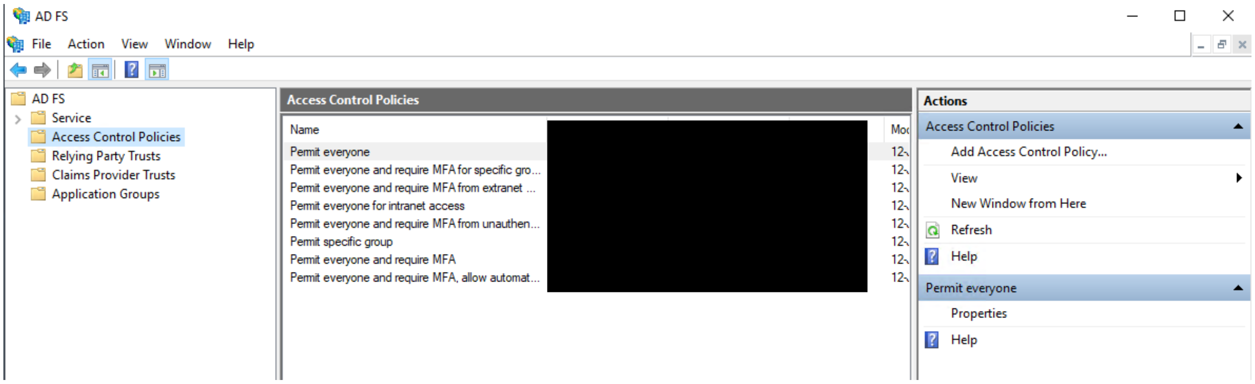
Web Application Proxy allows users on any device to access your web-based applications from outside the corporate network. Web Application Proxy pre-authenticates access to web-based applications and also functions as an AD FS proxy.

Settings

Status Not configured

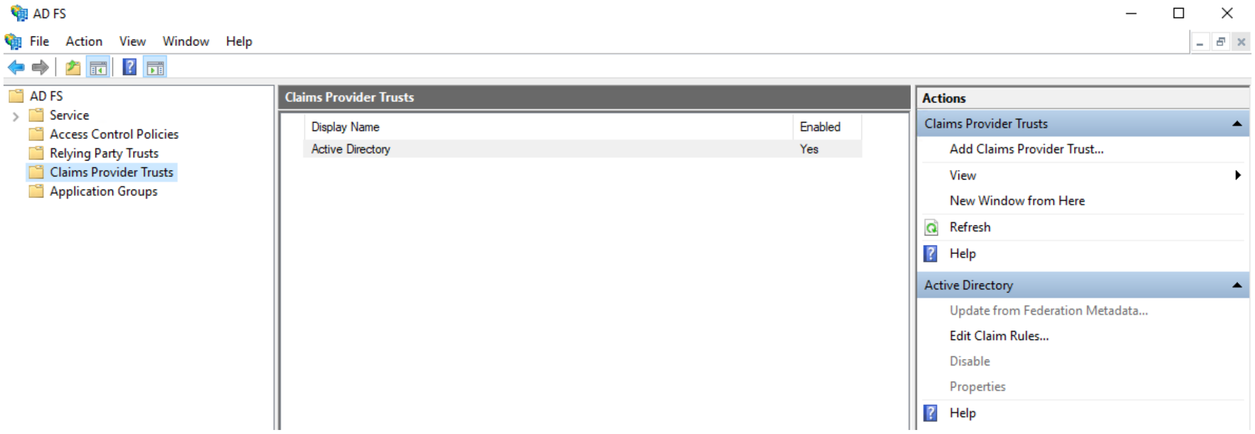
Learn More

Web Application Proxy



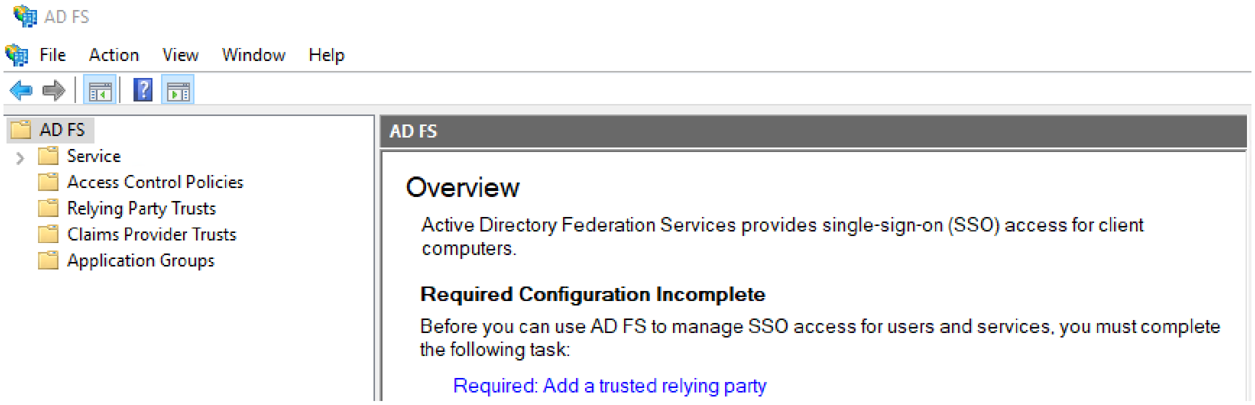
Access Control Policies

Name	[redacted]	Moc
Permit everyone	[redacted]	12
Permit everyone and require MFA for specific gro...	[redacted]	12
Permit everyone and require MFA from extranet ...	[redacted]	12
Permit everyone for intranet access	[redacted]	12
Permit everyone and require MFA from unauthen...	[redacted]	12
Permit specific group	[redacted]	12
Permit everyone and require MFA	[redacted]	12
Permit everyone and require MFA, allow automat...	[redacted]	12



Claims Provider Trusts

Display Name	Enabled
Active Directory	Yes



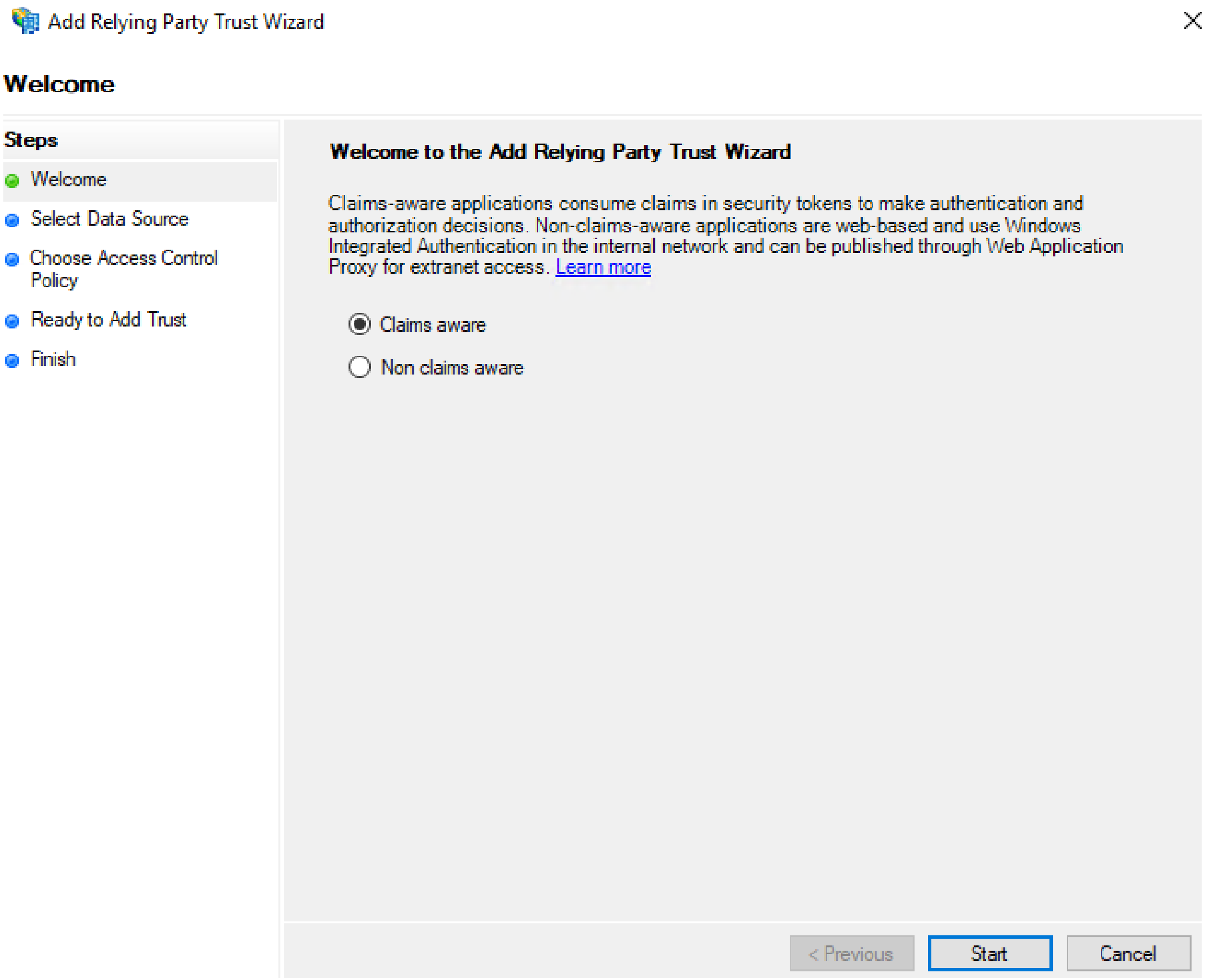
Overview

Active Directory Federation Services provides single-sign-on (SSO) access for client computers.

Required Configuration Incomplete

Before you can use AD FS to manage SSO access for users and services, you must complete the following task:

Required: Add a trusted relying party



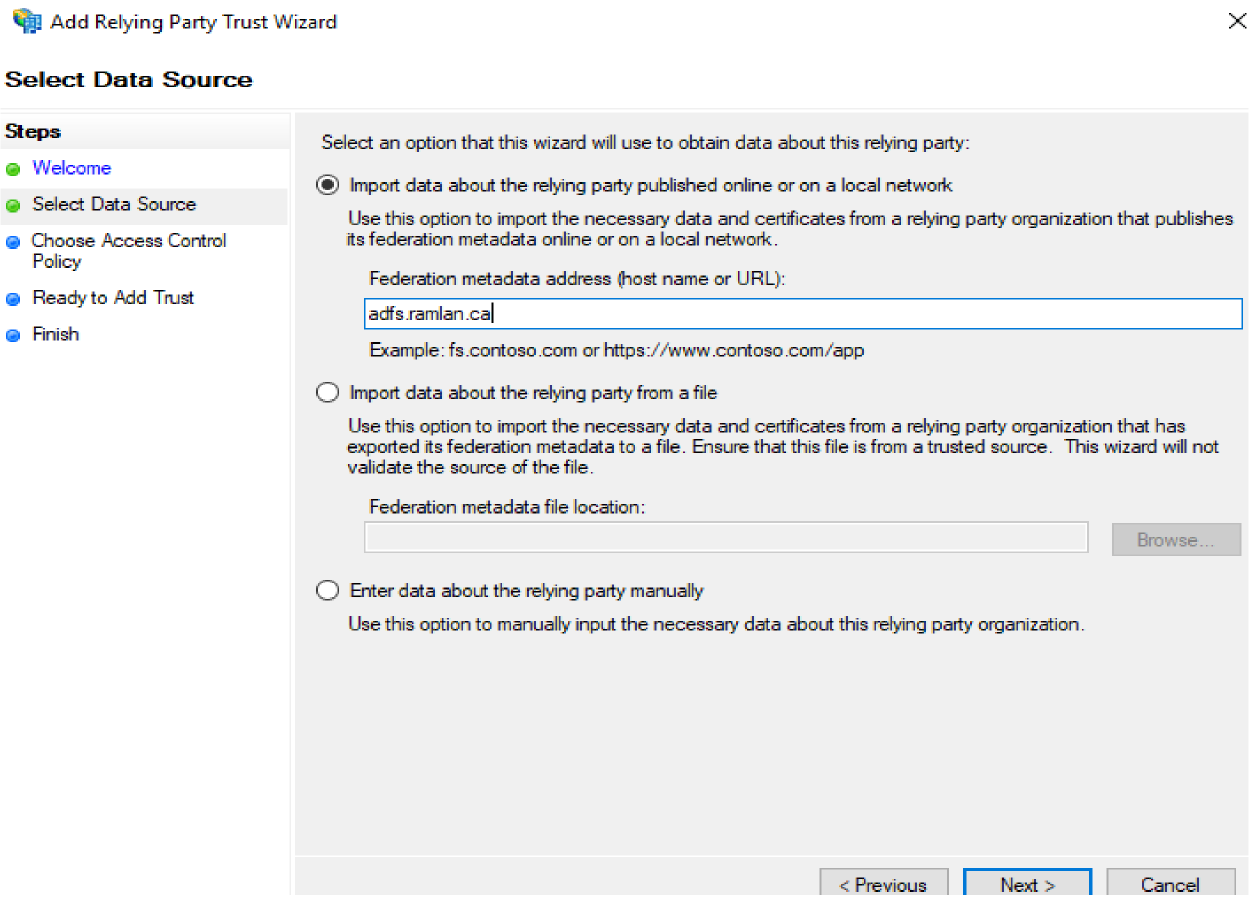
Welcome

Welcome to the Add Relying Party Trust Wizard

Claims-aware applications consume claims in security tokens to make authentication and authorization decisions. Non-claims-aware applications are web-based and use Windows Integrated Authentication in the internal network and can be published through Web Application Proxy for extranet access. Learn more

● Claims aware

○ Non claims aware



Add Relying Party Trust Wizard

Select Data Source

Steps

- Welcome
- Select Data Source
- Choose Access Control Policy
- Ready to Add Trust
- Finish

Select an option that this wizard will use to obtain data about this relying party:

● Import data about the relying party published online or on a local network

Use this option to import the necessary data and certificates from a relying party organization that publishes its federation metadata online or on a local network.

Federation metadata address (host name or URL):

adfs.ramlan.ca

Example: fs.contoso.com or https://www.contoso.com/app

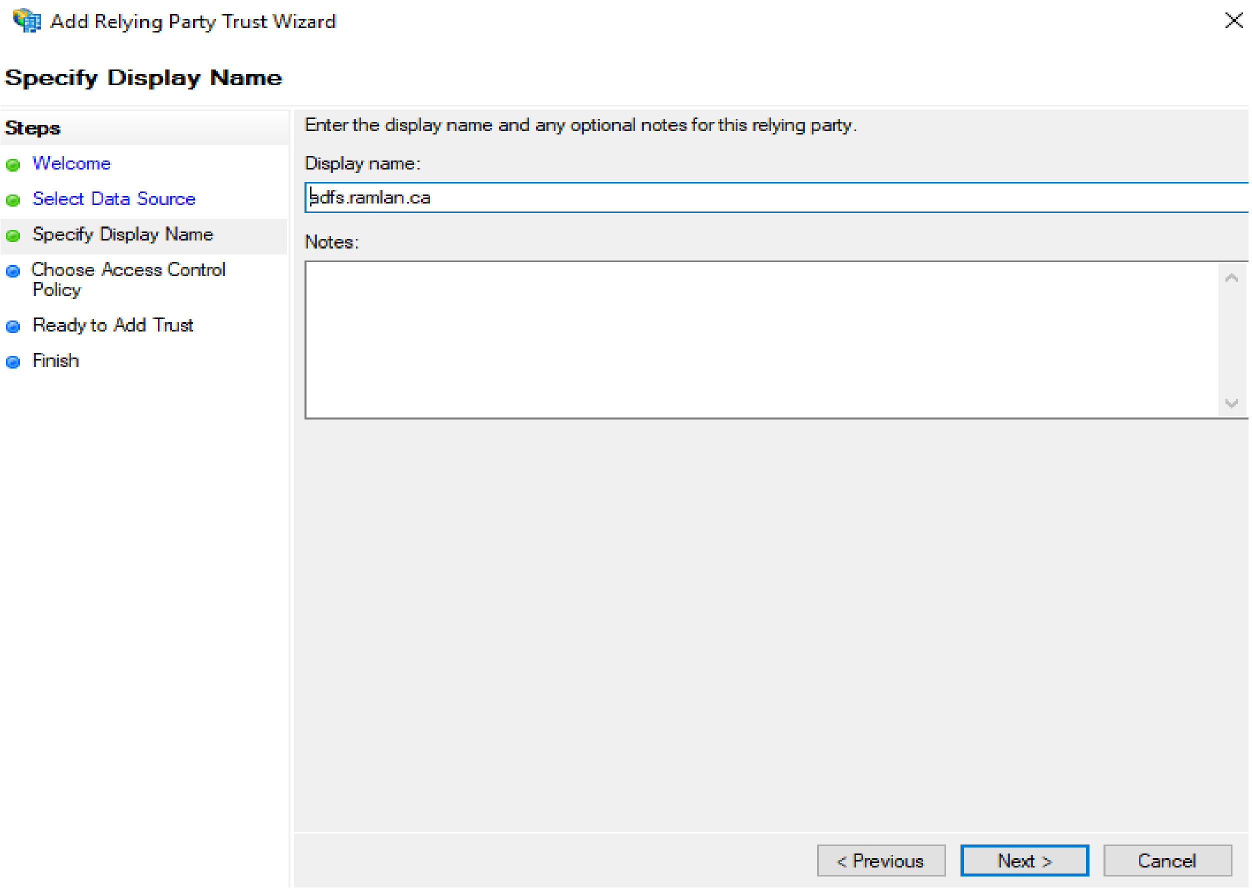
○ Import data about the relying party from a file

Use this option to import the necessary data and certificates from a relying party organization that has exported its federation metadata to a file. Ensure that this file is from a trusted source. This wizard will not validate the source of the file.

Federation metadata file location:

○ Enter data about the relying party manually

Use this option to manually input the necessary data about this relying party organization.



Add Relying Party Trust Wizard

Specify Display Name

Steps

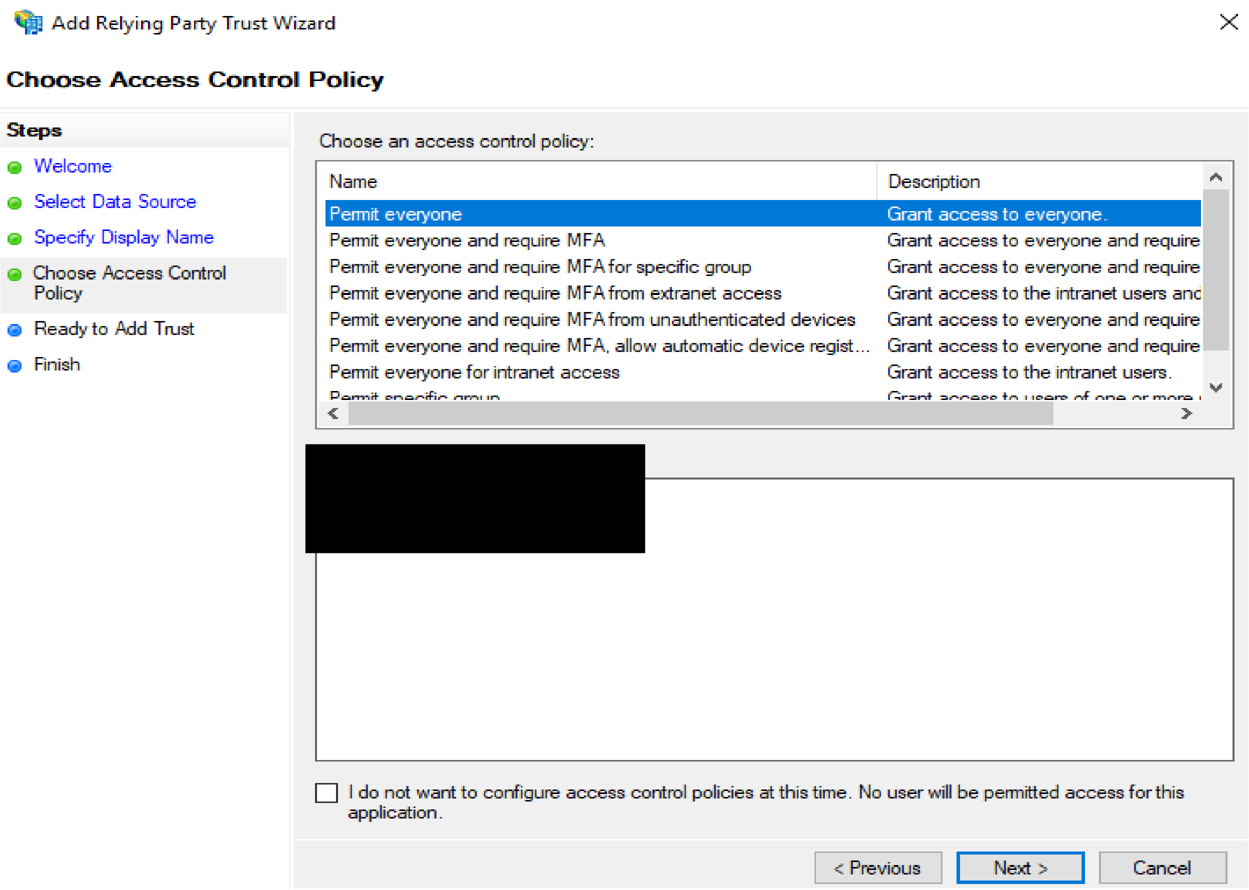
- Welcome
- Select Data Source
- Specify Display Name
- Choose Access Control Policy
- Ready to Add Trust
- Finish

Enter the display name and any optional notes for this relying party.

Display name:

adfs.ramlan.ca

Notes:



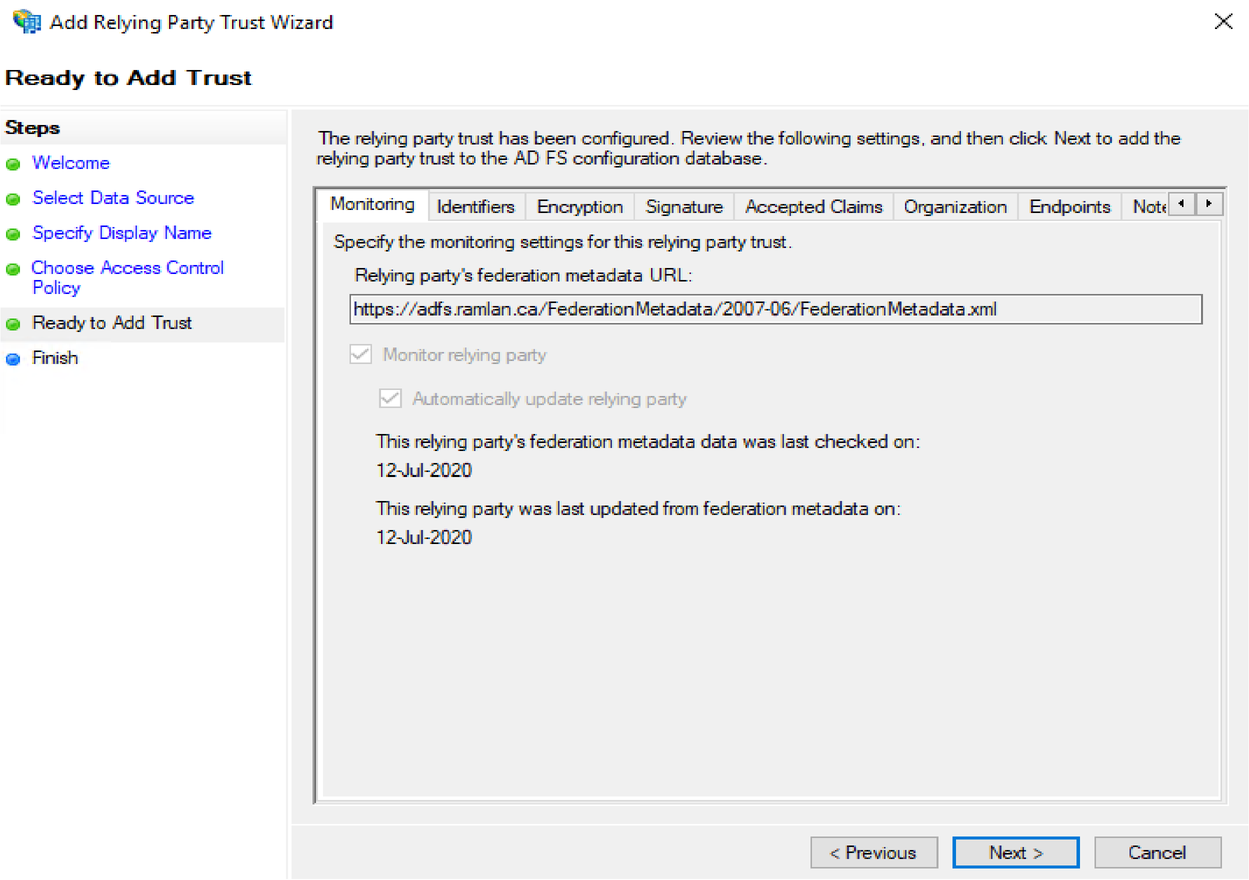
Choose Access Control Policy

Choose an access control policy:

Name	Description
Permit everyone	Grant access to everyone.
Permit everyone and require MFA	Grant access to everyone and require
Permit everyone and require MFA for specific group	Grant access to everyone and require
Permit everyone and require MFA from extranet access	Grant access to the intranet users and
Permit everyone and require MFA from unauthenticated devices	Grant access to everyone and require
Permit everyone and require MFA, allow automatic device regist...	Grant access to everyone and require
Permit everyone for intranet access	Grant access to the intranet users.
Permit specific group	Grant access to users of one or more

[redacted]

☐ I do not want to configure access control policies at this time. No user will be permitted access for this application.



Ready to Add Trust

The relying party trust has been configured. Review the following settings, and then click Next to add the relying party trust to the AD FS configuration database.

Specify the monitoring settings for this relying party trust.

Relying party's federation metadata URL:

https://adfs.ramlan.ca/FederationMetadata/2007-06/FederationMetadata.xml

☑ Monitor relying party

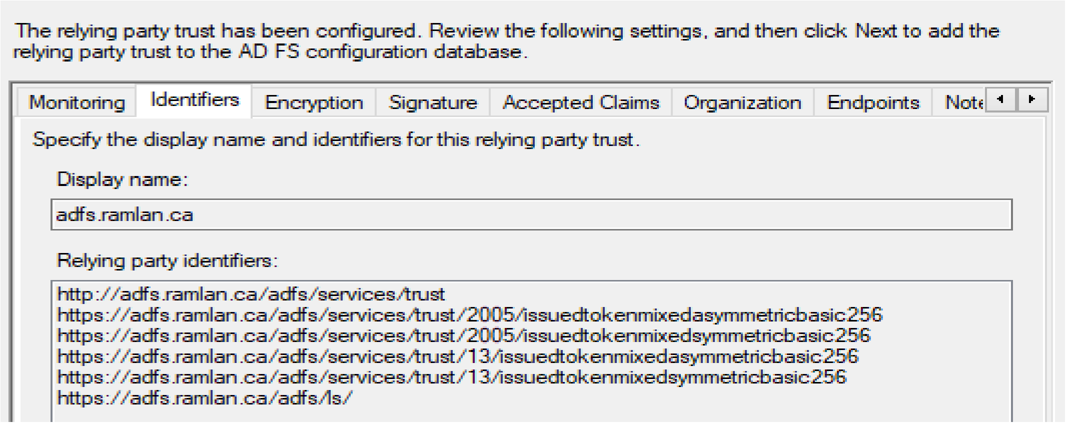
☑ Automatically update relying party

This relying party's federation metadata data was last checked on:

12-Jul-2020

This relying party was last updated from federation metadata on:

12-Jul-2020


The relying party trust has been configured. Review the following settings, and then click Next to add the relying party trust to the AD FS configuration database.

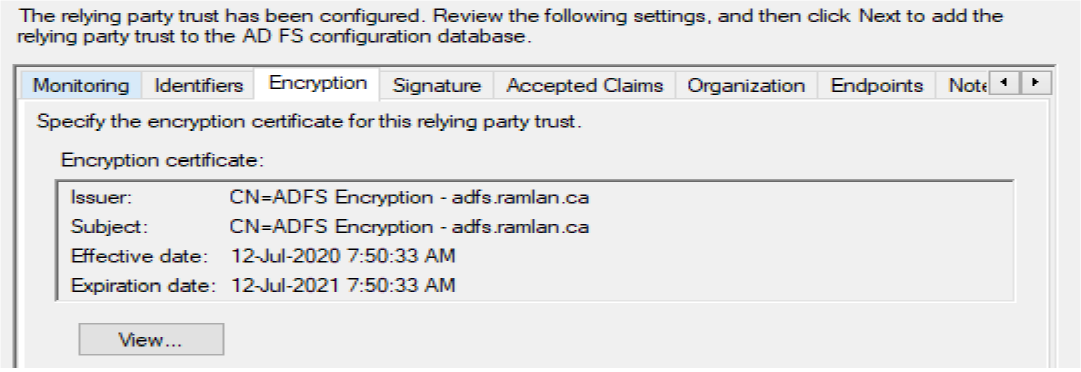
Specify the display name and identifiers for this relying party trust.

Display name:

adfs.ramlan.ca

Relying party identifiers:

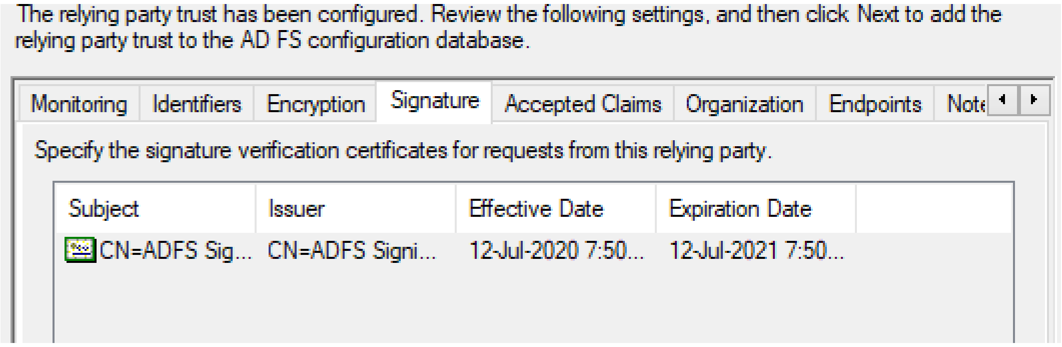
```
http://adfs.ramlan.ca/adfs/services/trust
https://adfs.ramlan.ca/adfs/services/trust/2005/issuedtokenmixedasymmetricbasic256
https://adfs.ramlan.ca/adfs/services/trust/2005/issuedtokenmixedsymmetricbasic256
https://adfs.ramlan.ca/adfs/services/trust/13/issuedtokenmixedasymmetricbasic256
https://adfs.ramlan.ca/adfs/services/trust/13/issuedtokenmixedsymmetricbasic256
https://adfs.ramlan.ca/adfs/ls/
```


The relying party trust has been configured. Review the following settings, and then click Next to add the relying party trust to the AD FS configuration database.

Specify the encryption certificate for this relying party trust.

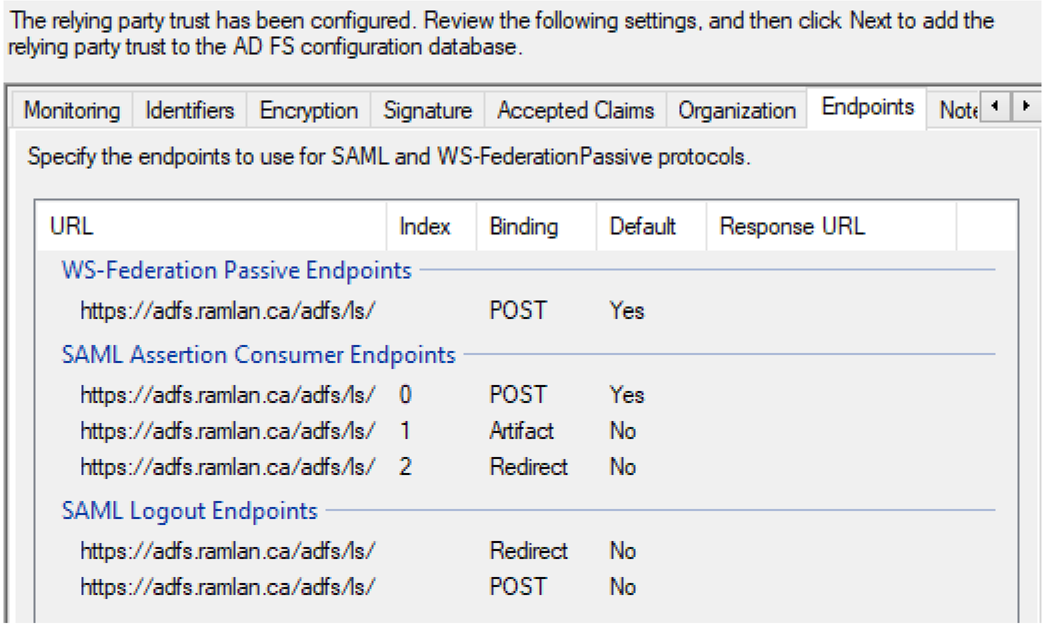
Encryption certificate:

Issuer:	CN=ADFS Encryption - adfs.ramlan.ca
Subject:	CN=ADFS Encryption - adfs.ramlan.ca
Effective date:	12-Jul-2020 7:50:33 AM
Expiration date:	12-Jul-2021 7:50:33 AM


The relying party trust has been configured. Review the following settings, and then click Next to add the relying party trust to the AD FS configuration database.

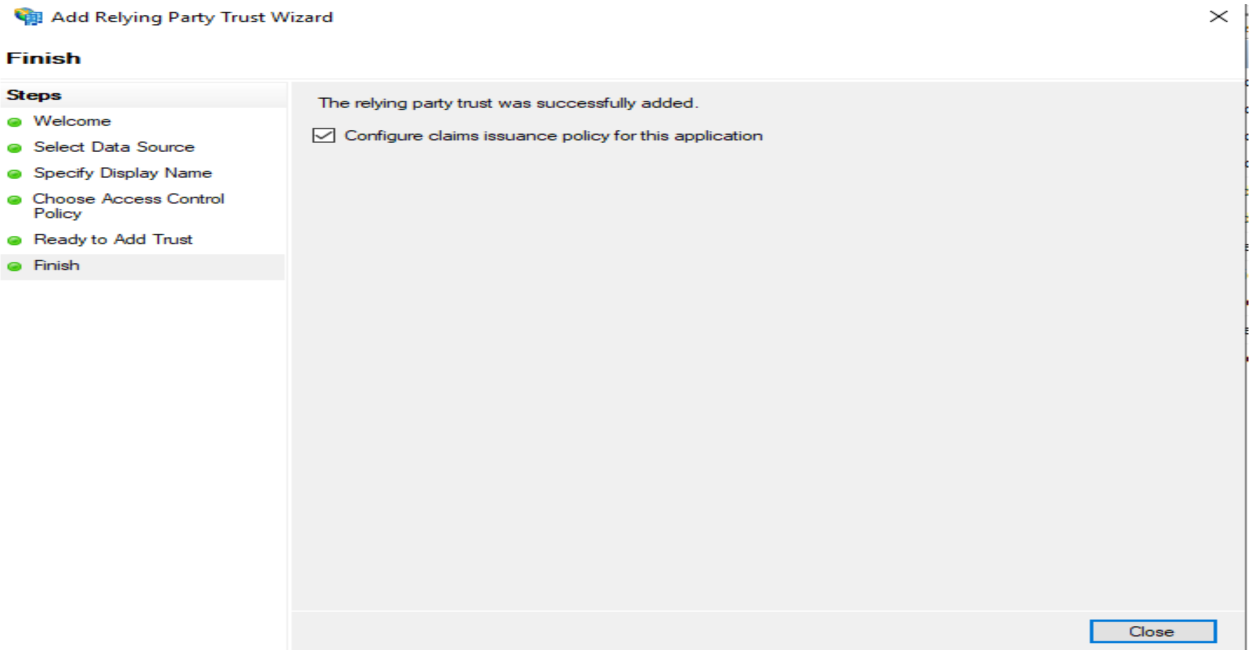
Specify the signature verification certificates for requests from this relying party.

Subject	Issuer	Effective Date	Expiration Date
CN=ADFS Sig...	CN=ADFS Signi...	12-Jul-2020 7:50...	12-Jul-2021 7:50...


The relying party trust has been configured. Review the following settings, and then click Next to add the relying party trust to the AD FS configuration database.

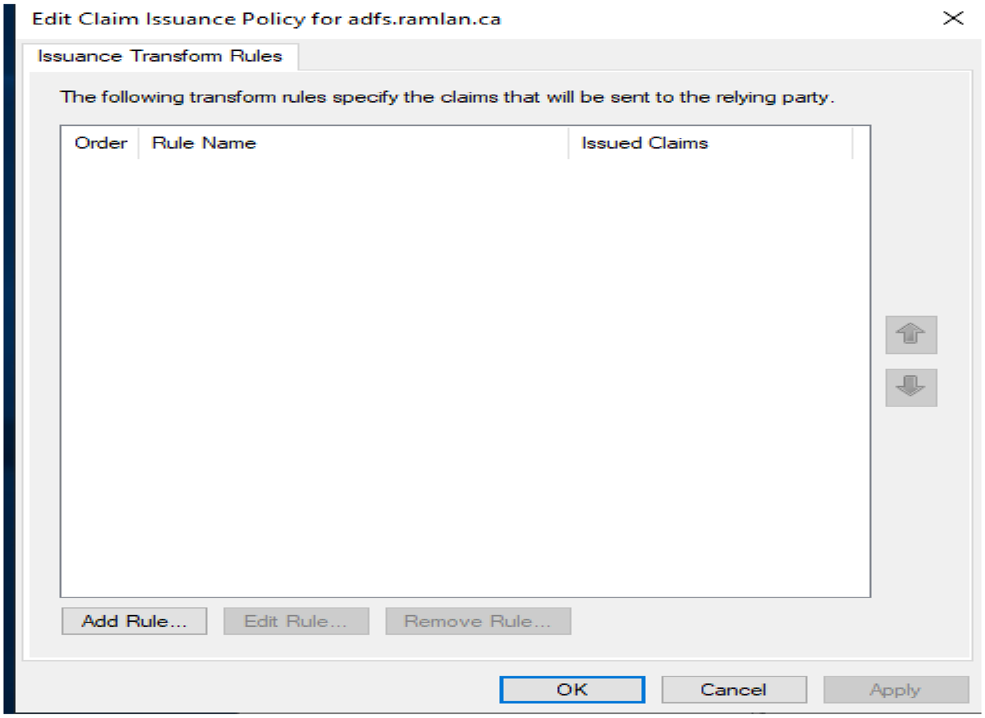
Specify the endpoints to use for SAML and WS-FederationPassive protocols.

URL	Index	Binding	Default	Response URL
WS-Federation Passive Endpoints				
https://adfs.ramlan.ca/adfs/ls/		POST	Yes	
SAML Assertion Consumer Endpoints				
https://adfs.ramlan.ca/adfs/ls/	0	POST	Yes	
https://adfs.ramlan.ca/adfs/ls/	1	Artifact	No	
https://adfs.ramlan.ca/adfs/ls/	2	Redirect	No	
SAML Logout Endpoints				
https://adfs.ramlan.ca/adfs/ls/		Redirect	No	
https://adfs.ramlan.ca/adfs/ls/		POST	No	



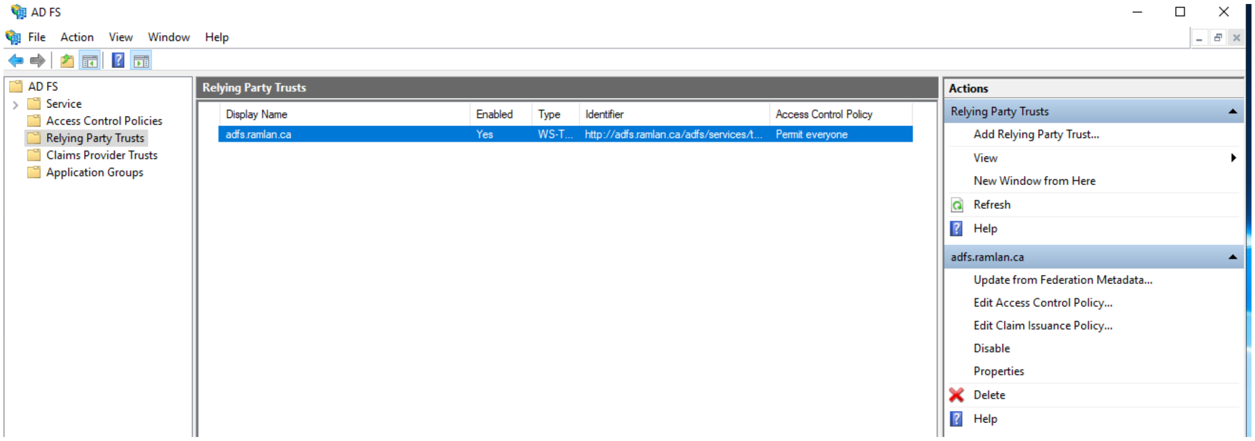
The relying party trust was successfully added.

☑ Configure claims issuance policy for this application



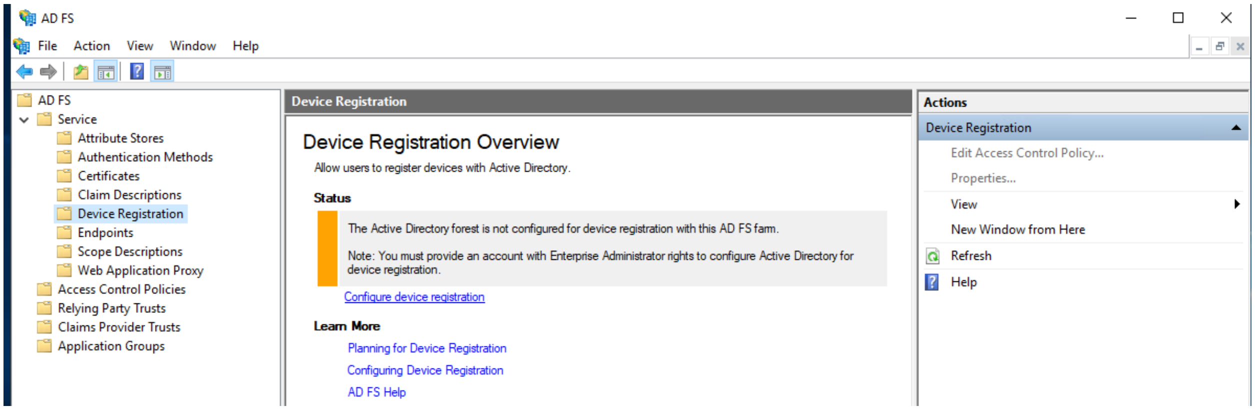
The following transform rules specify the claims that will be sent to the relying party.

Order	Rule Name	Issued Claims



Display Name	Enabled	Type	Identifier	Access Control Policy
adfs.ramlan.ca	Yes	WS-T...	http://adfs.ramlan.ca/adfs/services/t...	Permit everyone

I will not be completing Device Registration as, I will be using Azure.



Device Registration Overview

Allow users to register devices with Active Directory.

Status

The Active Directory forest is not configured for device registration with this AD FS farm.

Note: You must provide an account with Enterprise Administrator rights to configure Active Directory for device registration.

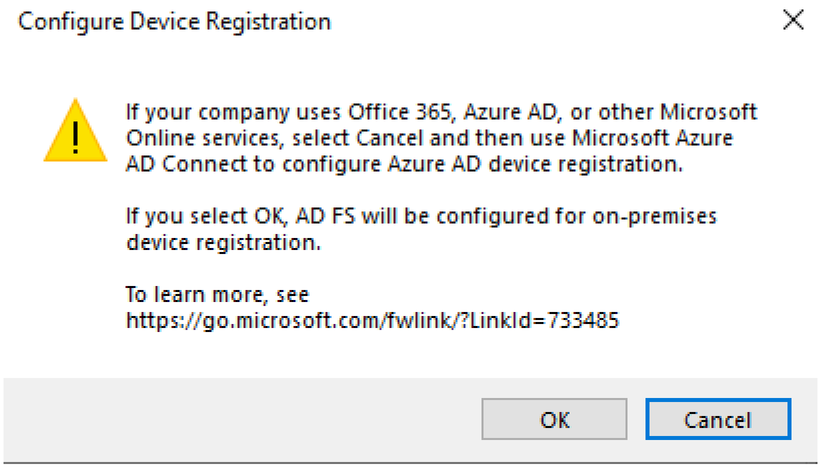
Configure device registration

Learn More

Planning for Device Registration

Configuring Device Registration

AD FS Help



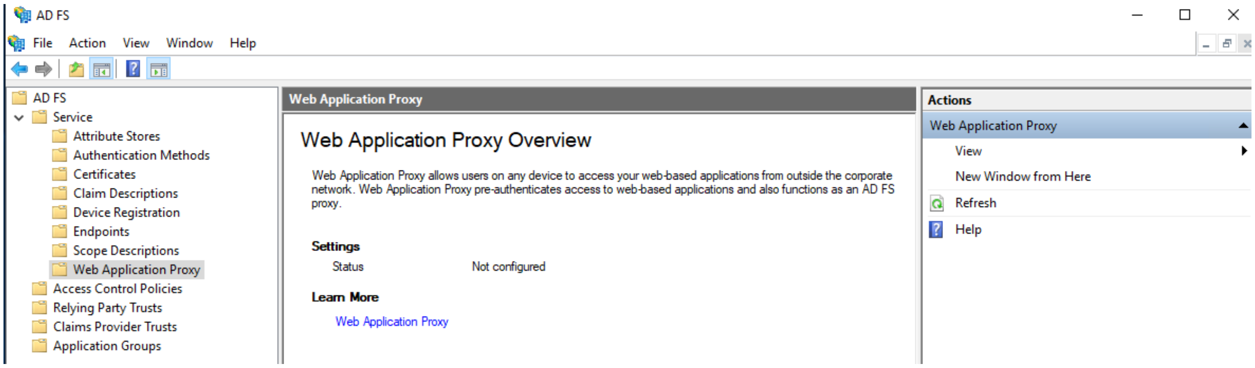
Configure Device Registration

If your company uses Office 365, Azure AD, or other Microsoft Online services, select Cancel and then use Microsoft Azure AD Connect to configure Azure AD device registration.

If you select OK, AD FS will be configured for on-premises device registration.

To learn more, see https://go.microsoft.com/fwlink/?LinkId=733485

With regard to Web Application Proxy – I will put a hold as it requires some more research.



Web Application Proxy Overview

Web Application Proxy allows users on any device to access your web-based applications from outside the corporate network. Web Application Proxy pre-authenticates access to web-based applications and also functions as an AD FS proxy.

Settings

Status Not configured

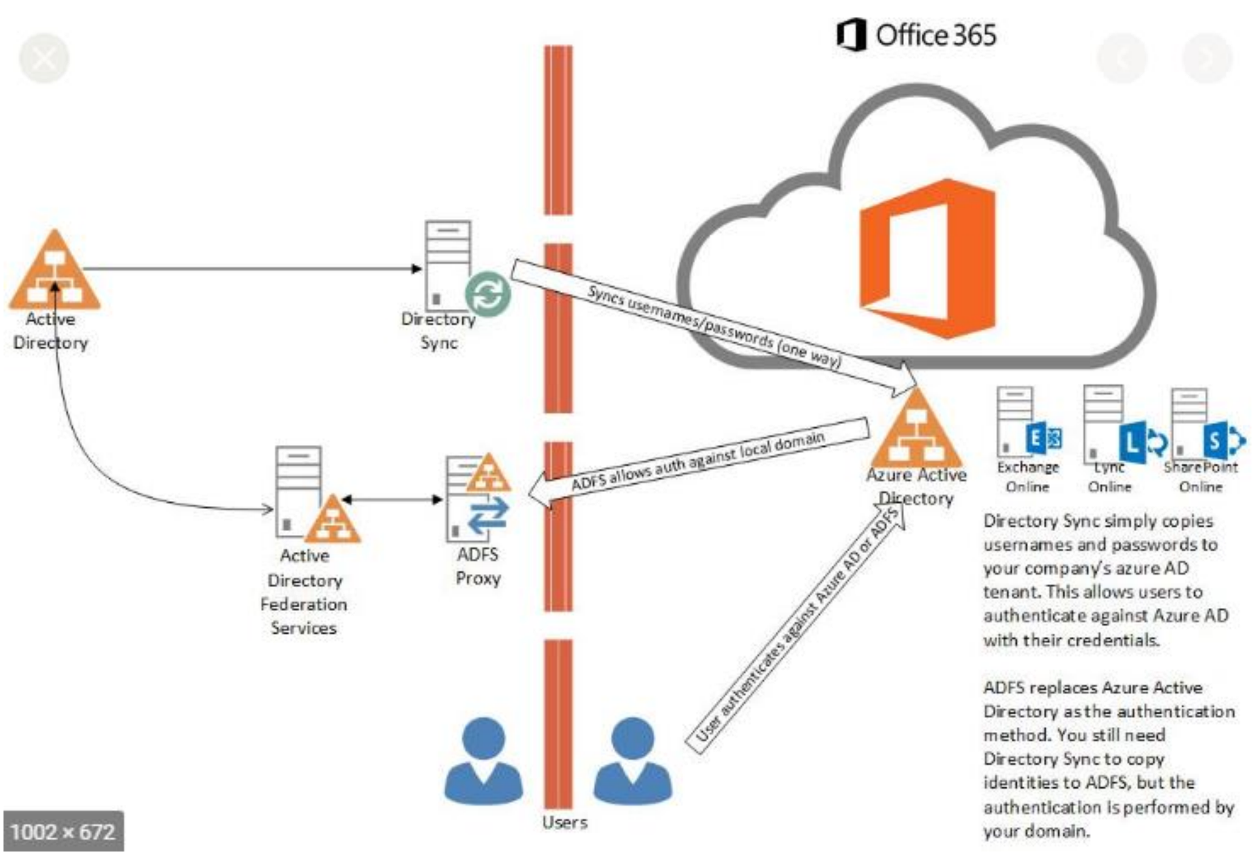
Learn More

Web Application Proxy

This concludes ADFS deployment (On Premise) on Windows Server 2019.

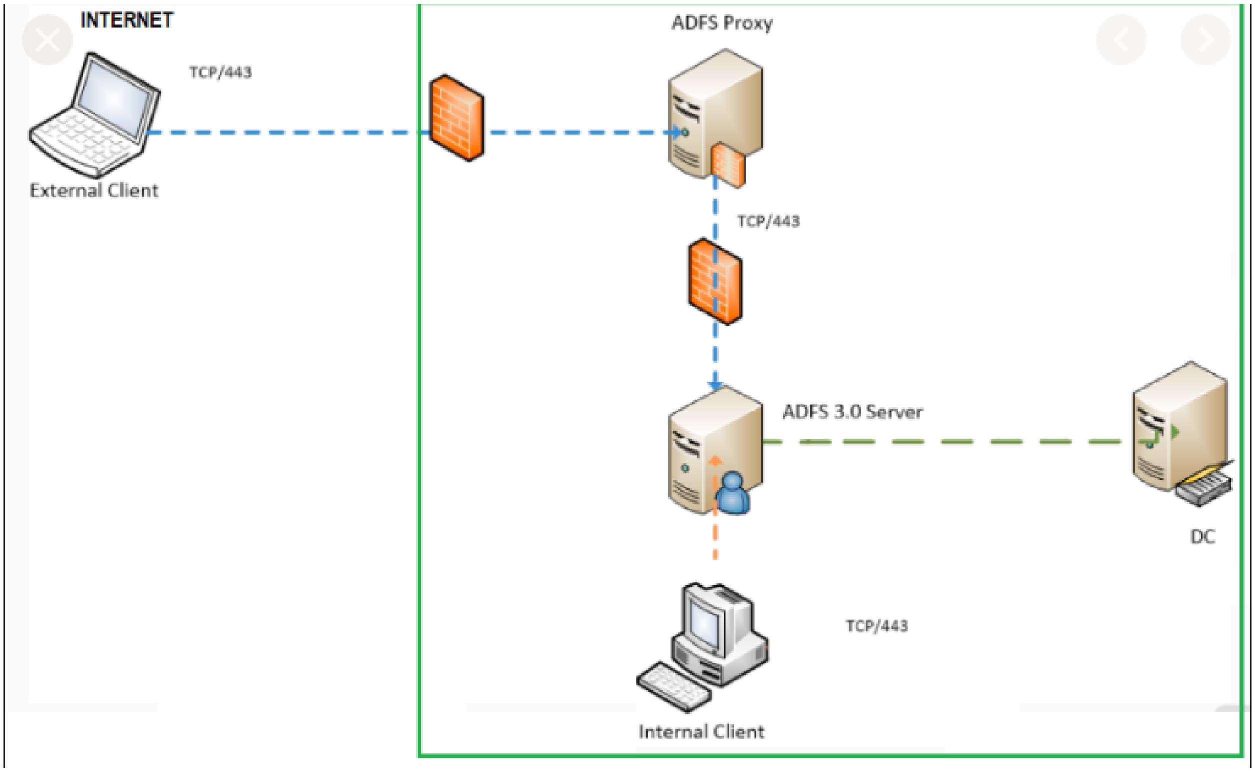
Thanks

Ram Lan
12th July 2020


Office 365
Active Directory
Directory Sync
Syncs usernames/passwords (one way)
ADFS allows auth against local domain
Azure Active Directory
Exchange Online
Lync Online
SharePoint Online
Active Directory Federation Services
ADFS Proxy
User authenticates against Azure AD or ADFS
Users
1002 × 672

Directory Sync simply copies usernames and passwords to your company's azure AD tenant. This allows users to authenticate against Azure AD with their credentials.

ADFS replaces Azure Active Directory as the authentication method. You still need Directory Sync to copy identities to ADFS, but the authentication is performed by your domain.



https://docs.microsoft.com/en-us/windows-server/identity/active-directory-federation-services