Azure AD Connect with Single Sign-on on Azure Tenant

Integrating your on-premises identities with Azure Active Directory

In this section we will figure out how **MOBILITYADCon** will be installed and configured with the following tool:

- Azure AD Connect

Some Useful info for the VM and related components.

Cloud Service Name: maqovcs1

Virtual Net Name: maqovvnetmobility

Subnet Name: Subnet-1

Virtual Network Range: 10.1.1.0/24

VM Static IP (DIP): 10.1.1.7

Local Admin: MAQOV

Service Account: SVC_ADFS

Objective

Integrating your on-premises directories with Azure AD makes your users more productive by providing a common identity for accessing both cloud and on-premises resources. With this integration users and organizations can take advantage of the following:

- Users can use a single identity to access on-premises applications and cloud services such as Office 365.

- Single tool to provide an easy deployment experience for synchronization and sign-in.

- Provides the newest capabilities for your scenarios. Azure AD Connect replaces older versions of identity integration tools such as DirSync and Azure AD Sync.

Prerequisites

- Azure Subscription
- Access to Public Domain, Ex godady, hover, networksolutions.
- Azure AD Connect Virtual Machine.
- Azure AD Connect tool.

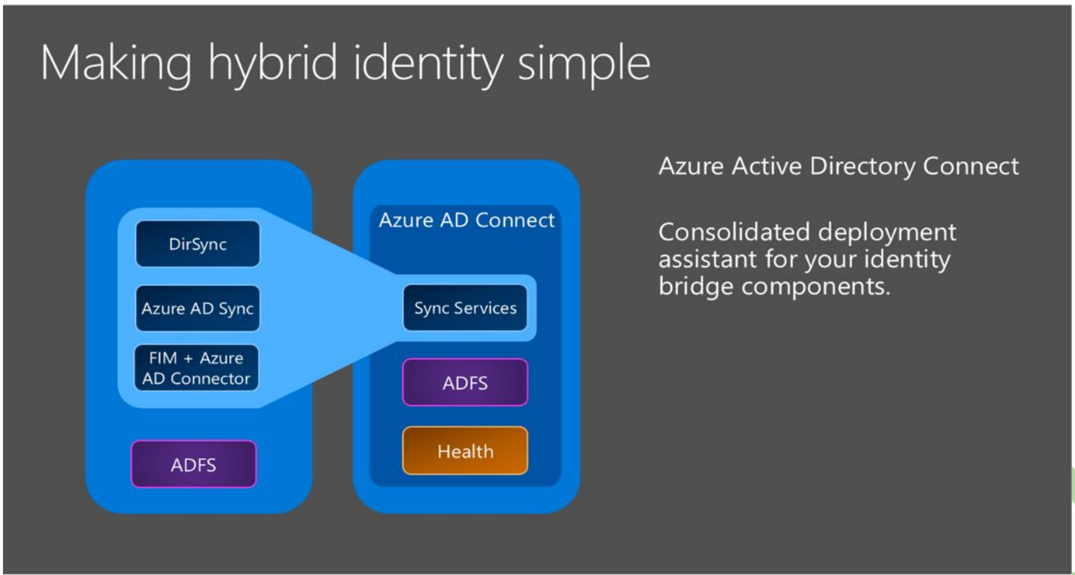
Azure AD Connect overview

Azure AD Connect is the tool to integrate your on-premises identity system such as Windows Server Active Directory with Azure Active Directory and connect your users to Office 365, Azure and 1000's of SaaS applications. This topic provides a comprehensive guide to prepare and deploy the necessary components for your end users to access cloud services with the same identity that they use today to access existing company apps.

Azure AD Connect: How It Works

Azure Active Directory Connect is made up of three primary parts. They are the synchronization services, the optional Active Directory Federation Services piece, and the monitoring piece which is done using Azure AD Connect Health

- Synchronization - This part is made up of the components and functionality previously released as Dirsync and Azure AD Sync. This is the part that is responsible for creating users and groups. It is also responsible for making sure that the information on users and groups in your on-premises environment, matches the cloud.
- AD FS - This is an optional part of Azure AD Connect and can be used to setup a hybrid environment using an on-premises AD FS infrastructure. This part can be used by organizations to address complex deployments that include such things as domain join SSO, enforcement of AD login policy and smart card or 3rd party MFA.
- Health Monitoring - Azure AD Connect Health can provide robust monitoring of your AD FS servers and provide a central location in the Azure portal to view this activity. For additional information see Azure Active Directory Connect Health.



Making hybrid identity simple

Azure Active Directory Connect

Consolidated deployment assistant for your identity bridge components.

Install Azure AD Connect VM On Azure Tenant by PowerShell

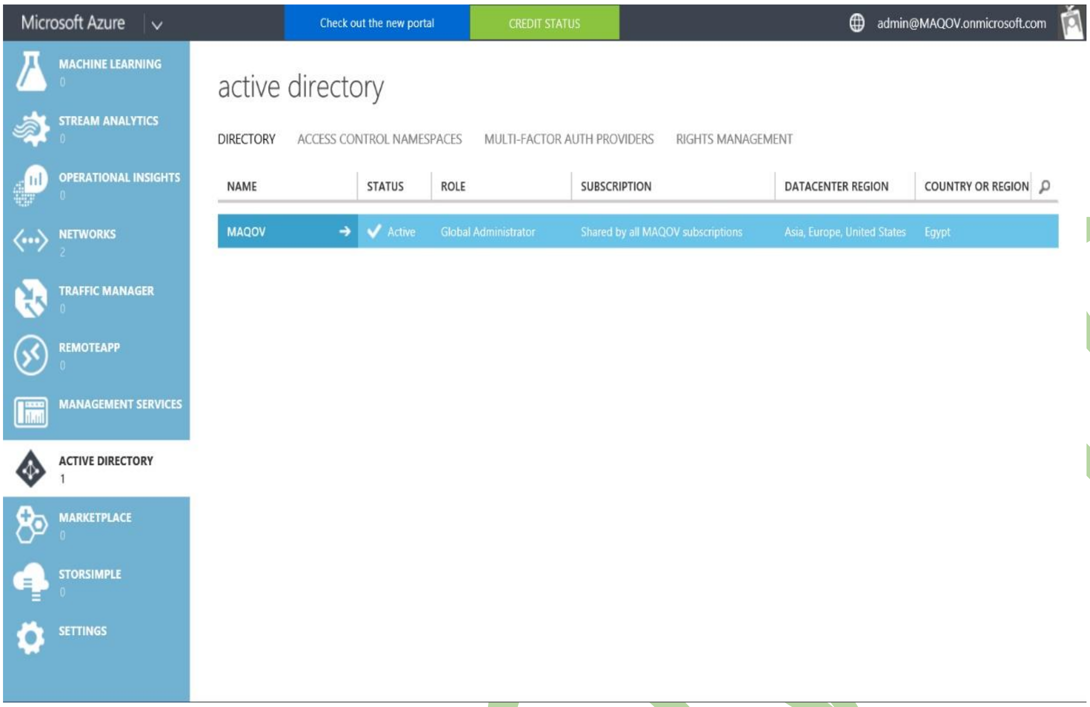
```
Add-AzureAccount

$family="Windows Server 2012 R2 Datacenter"

$image=Get-AzureVMImage | where { $_.ImageFamily -eq $family } | sort PublishedDate -Descending
| select -ExpandProperty ImageName -First 1

$vmname="mobilityAADCon"

$vmsize="Medium"

$vm1=New-AzureVMConfig -Name $vmname -InstanceSize $vmsize -ImageName $image

$cred1=Get-Credential -Message "Type the name and password of the local administrator account."

$cred2=Get-Credential -Message "Now type the name (not including the domain) and password of an
account that has permission to add the machine to the domain."

$domaindns="maqov.org"

$domacctdomain="MAQOV"

$vm1 | Add-AzureProvisioningConfig -AdminUsername $cred1.GetNetworkCredential().Username -
Password $cred1.GetNetworkCredential().Password -WindowsDomain -Domain $domacctdomain -
DomainUserName $cred2.GetNetworkCredential().Username -DomainPassword
$cred2.GetNetworkCredential().Password -JoinDomain $domaindns


$vm1 | Set-AzureSubnet -SubnetNames "Subnet-1"

$vm1 | Set-AzureStaticVNetIP -IPAddress 10.1.1.7

$disksize=20
$disklabel="Mydiskone"
$lun=0
$hcaching="ReadWrite"
$vm1 | Add-AzureDataDisk -CreateNew -DiskSizeInGB $disksize -DiskLabel $disklabel -LUN $lun -
HostCaching $hcaching

$svcname="maqovcs1"
$vnetname="maqovvnetmobility"
New-AzureVM -ServiceName $svcname -VMs $vm1 -VNetName $vnetname
```

Domain Verification

Through this Section We Will Do many Steps in order to make Verify our domain on azure and make sure that MAQOV.org which is our domain in this case is our domain and owned by us.

Add Custom Domain On Azure Tenant

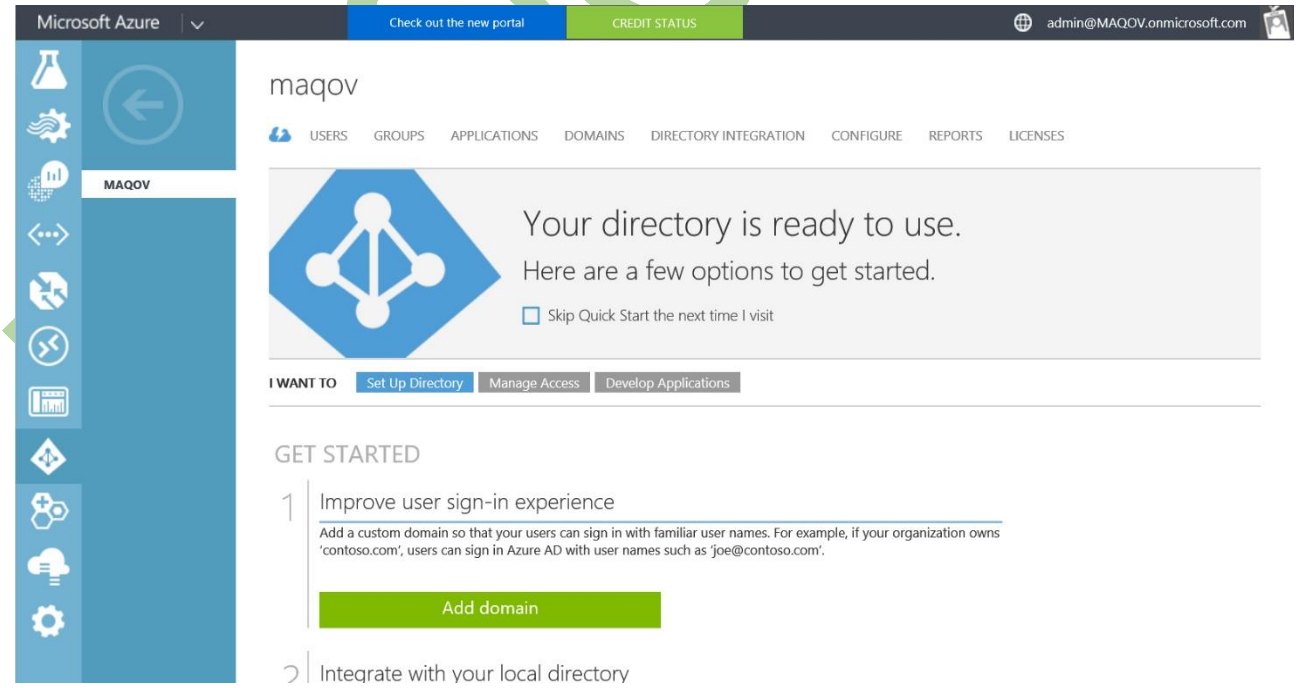
1. Login to Azure Portal.
2. Select **Active Directory,** Select your domain.



active directory

NAME	STATUS	ROLE	SUBSCRIPTION	DATACENTER REGION	COUNTRY OR REGION
MAQOV	✓ Active	Global Administrator	Shared by all MAQOV subscriptions	Asia, Europe, United States	Egypt

3. On the domain page Select **add domain**.



maqov

Your directory is ready to use.

Here are a few options to get started.

☐ Skip Quick Start the next time I visit

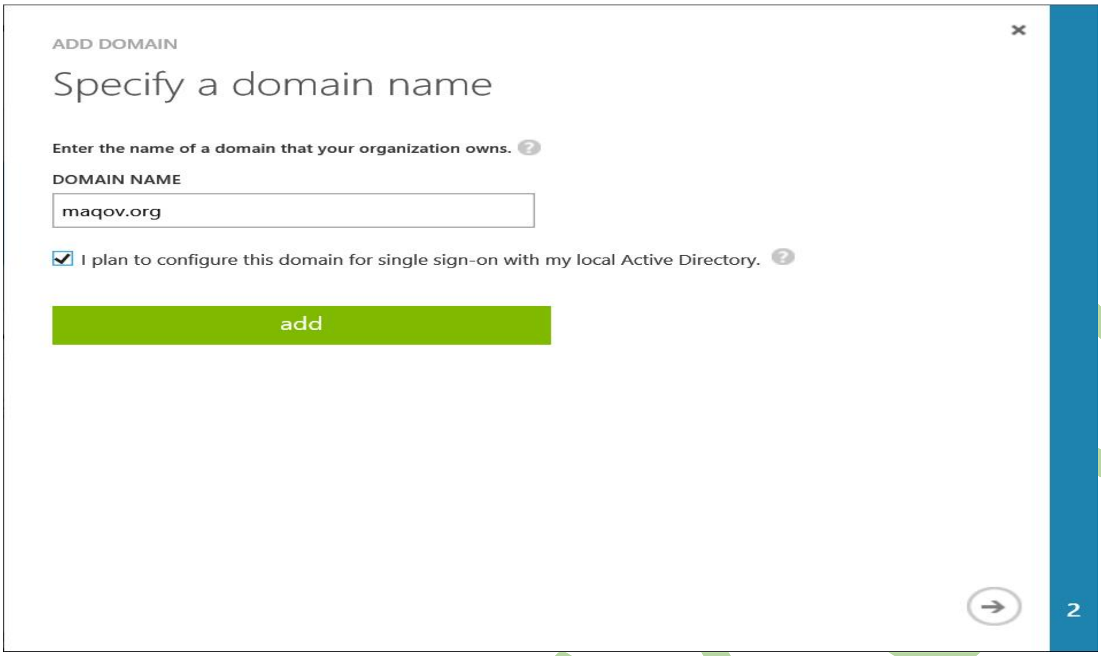
GET STARTED

1 Improve user sign-in experience

Add a custom domain so that your users can sign in with familiar user names. For example, if your organization owns 'contoso.com', users can sign in Azure AD with user names such as 'joe@contoso.com'.

2 Integrate with your local directory

4. On the pop message write your domain name, and check the "**I plan to configure the this domain for single sign-on with my local active directory**", then press arrow.



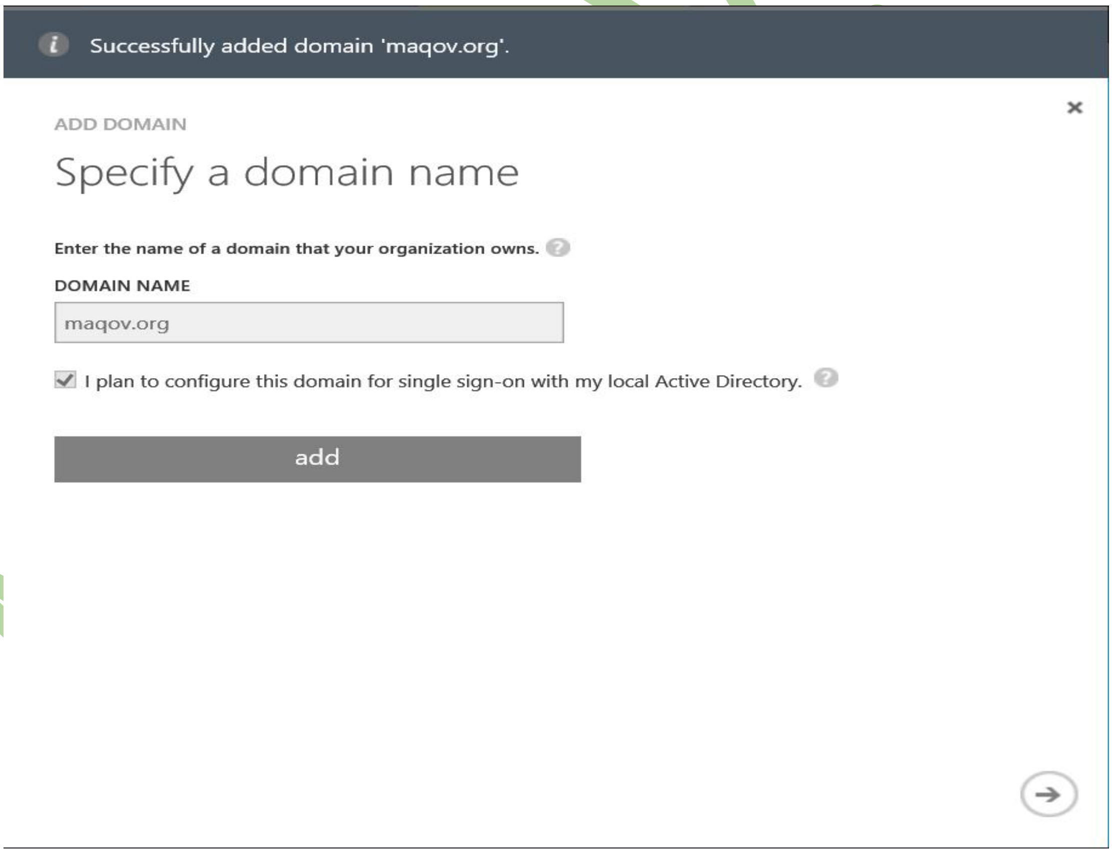
ADD DOMAIN

Specify a domain name

Enter the name of a domain that your organization owns.

DOMAIN NAME: maqov.org

☑ I plan to configure this domain for single sign-on with my local Active Directory.



Successfully added domain 'maqov.org'.

ADD DOMAIN

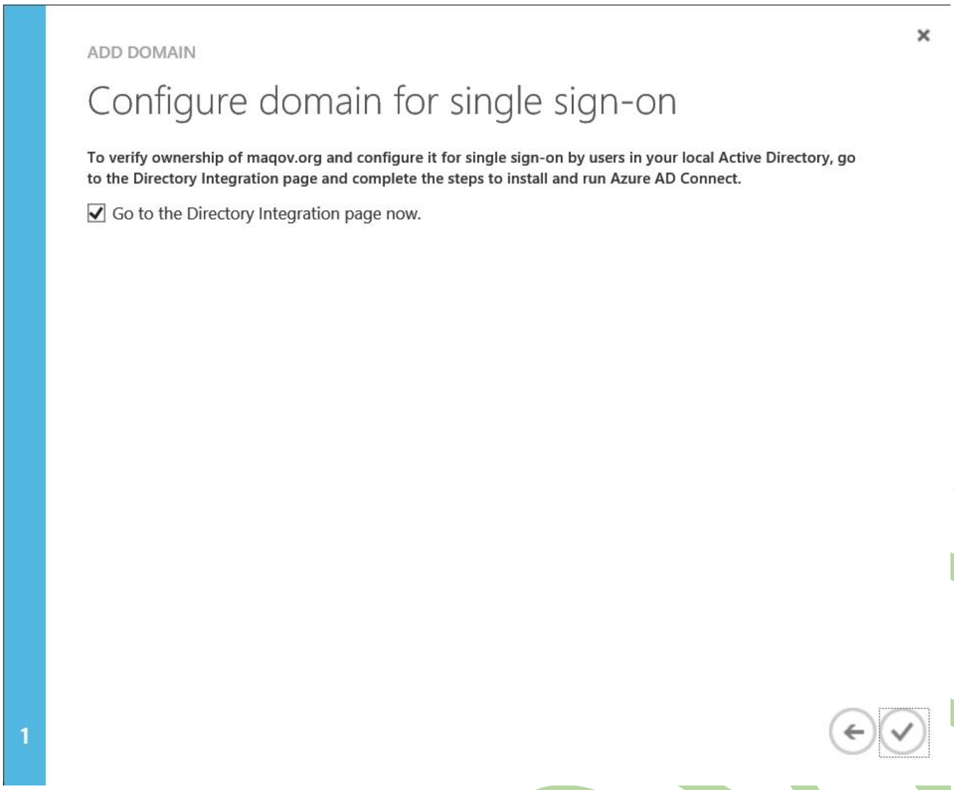
Specify a domain name

Enter the name of a domain that your organization owns.

DOMAIN NAME: maqov.org

☑ I plan to configure this domain for single sign-on with my local Active Directory.

5. Press the tick bottom.



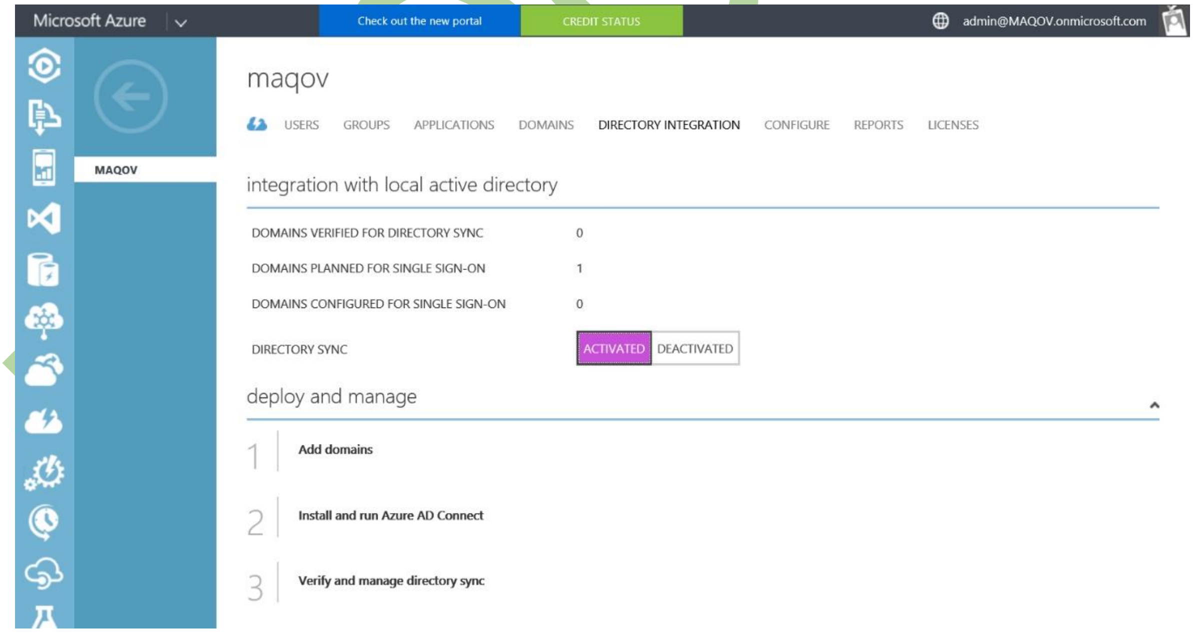
ADD DOMAIN

Configure domain for single sign-on

To verify ownership of maqov.org and configure it for single sign-on by users in your local Active Directory, go to the Directory Integration page and complete the steps to install and run Azure AD Connect.

☑ Go to the Directory Integration page now.

6. Choose **Directory Integration**, Directory Sync choose **Activated**.



integration with local active directory

DOMAINS VERIFIED FOR DIRECTORY SYNC	0
DOMAINS PLANNED FOR SINGLE SIGN-ON	1
DOMAINS CONFIGURED FOR SINGLE SIGN-ON	0
DIRECTORY SYNC	[✓ ACTIVATED] DEACTIVATED

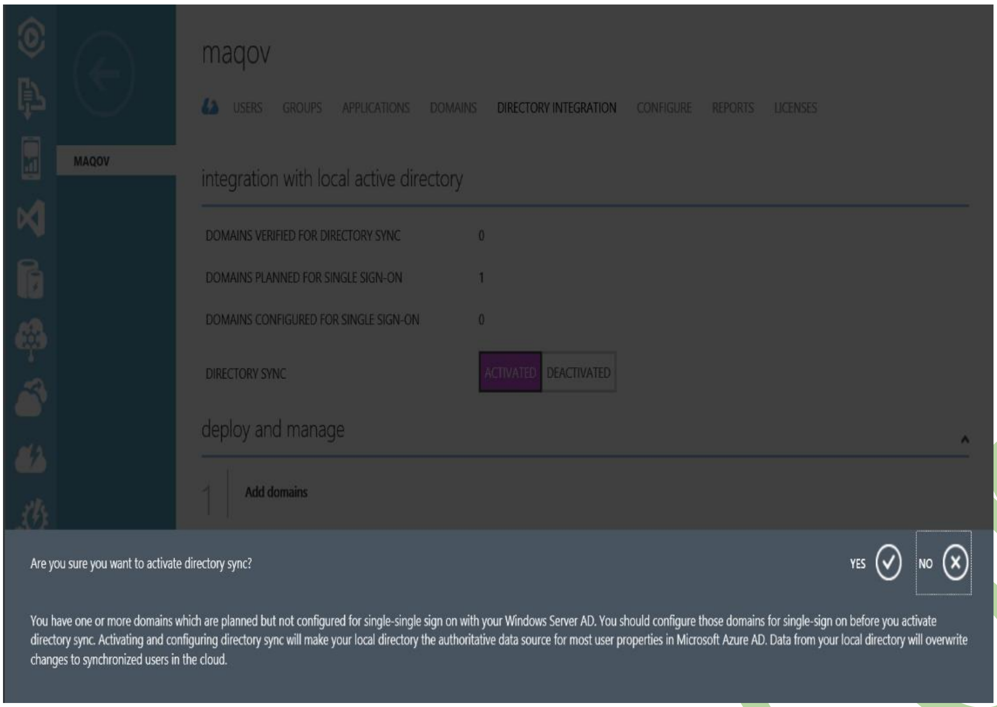
deploy and manage

1 Add domains

2 Install and run Azure AD Connect

3 Verify and manage directory sync

7. **Confirm Changes**.



integration with local active directory

DOMAINS VERIFIED FOR DIRECTORY SYNC	0
DOMAINS PLANNED FOR SINGLE SIGN-ON	1
DOMAINS CONFIGURED FOR SINGLE SIGN-ON	0
DIRECTORY SYNC	ACTIVATED DEACTIVATED

deploy and manage

1 Add domains

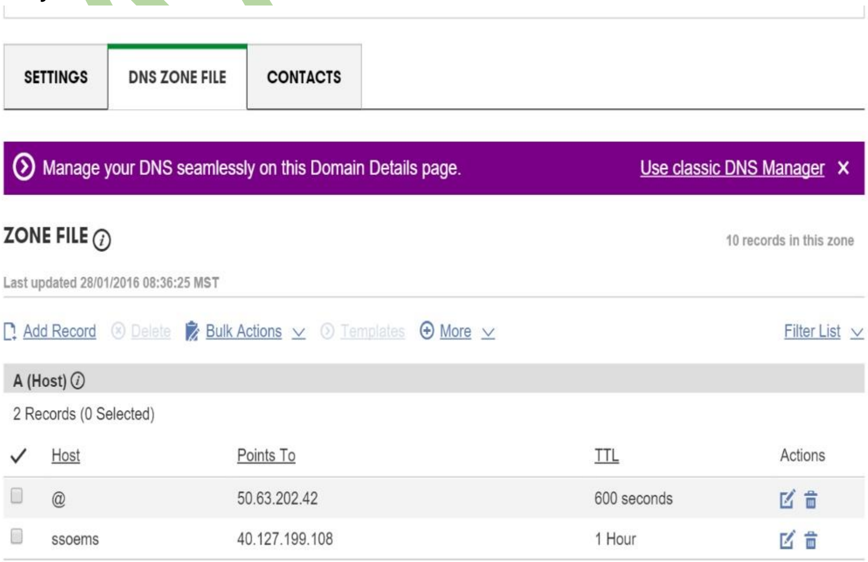
Are you sure you want to activate directory sync? YES ✓ NO ✕

You have one or more domains which are planned but not configured for single-single sign on with your Windows Server AD. You should configure those domains for single-sign on before you activate directory sync. Activating and configuring directory sync will make your local directory the authoritative data source for most user properties in Microsoft Azure AD. Data from your local directory will overwrite changes to synchronized users in the cloud.

Verify Domain

If you already have a domain registered with Go Daddy, and you want to configure it to work with Microsoft Azure AD tenant, domain verification is required to confirm that you own the domain. To verify your domain, you create a DNS record at Go Daddy, and then Azure AD uses that record to confirm that you own the domain.

1. Go to **Domain**, select the **Unverified domain**, and then press **verify** copy the **TXT record** Value.
2. Sign in to your account at **Go Daddy**.
3. Go to your account area.
4. Go to the page where you can work with your DNS records.
5. Add your **TXT record**.



Manage your DNS seamlessly on this Domain Details page. Use classic DNS Manager ✕

ZONE FILE

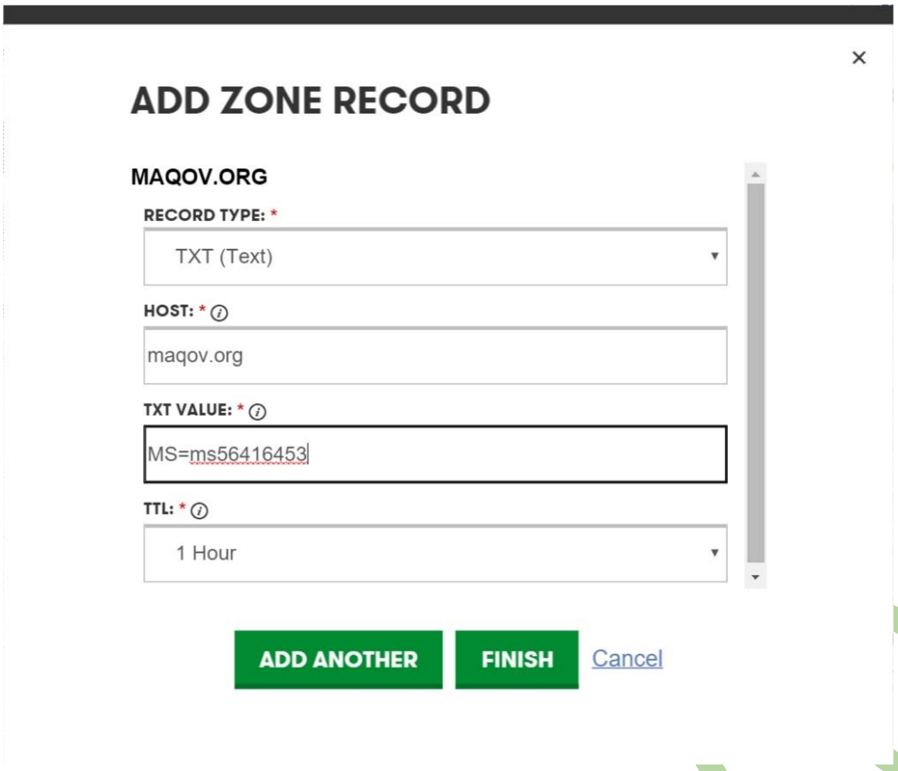
10 records in this zone

Last updated 28/01/2016 08:36:25 MST

A (Host)

2 Records (0 Selected)

✓	Host	Points To	TTL	Actions
□	@	50.63.202.42	600 seconds	
□	ssoems	40.127.199.108	1 Hour	



ADD ZONE RECORD

MAQOV.ORG

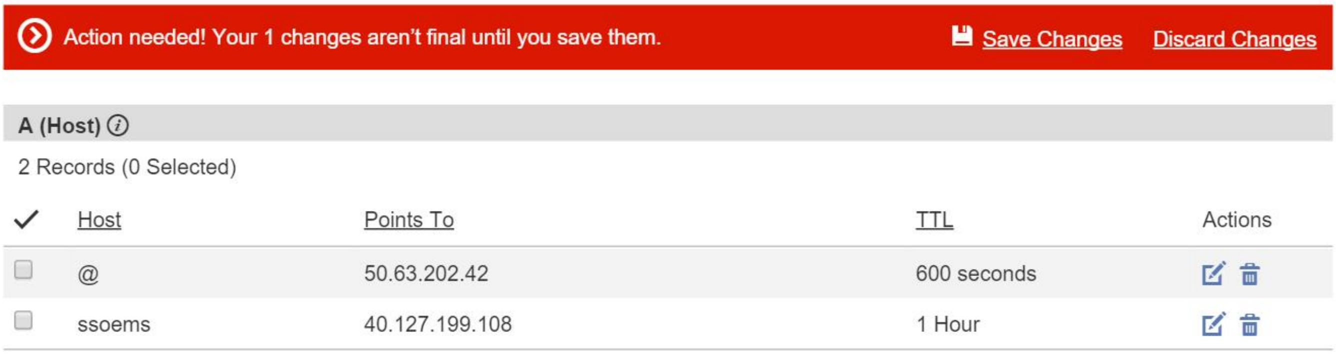
RECORD TYPE: * TXT (Text)

HOST: * maqov.org

TXT VALUE: * MS=ms56416453

TTL: * 1 Hour

6. **Save** the new TXT record for your domain in your zone file.



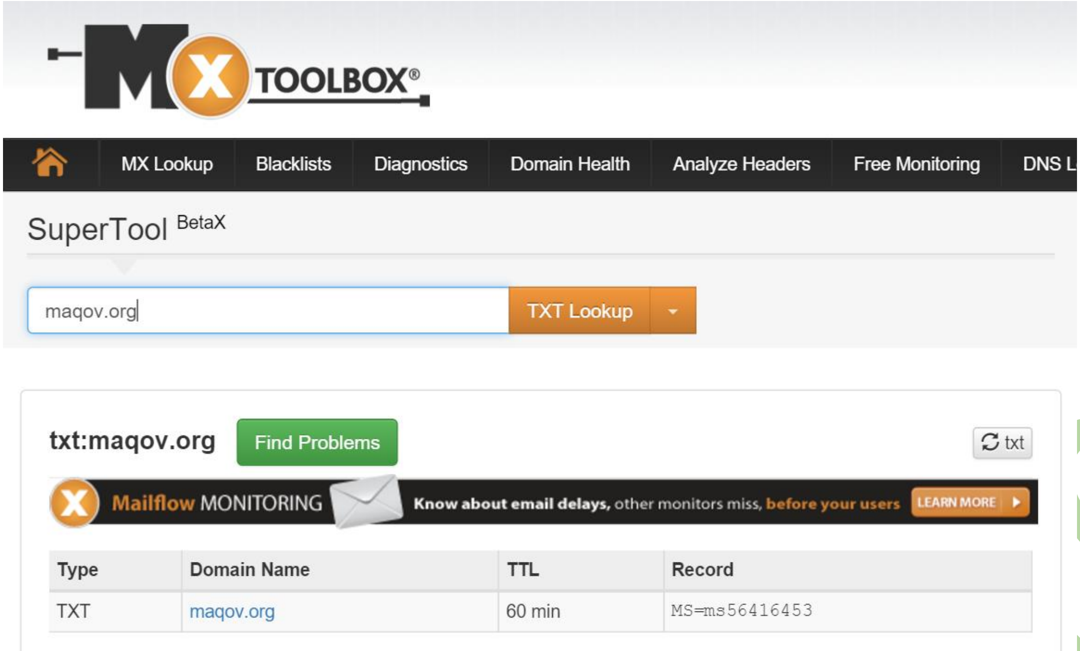
Action needed! Your 1 changes aren't final until you save them.

A (Host)

2 Records (0 Selected)

✓	Host	Points To	TTL	Actions
□	@	50.63.202.42	600 seconds	
□	ssoems	40.127.199.108	1 Hour	

7. Check the TXT Record is reflected login to **MXtoolbox.com** and then select the TXT Lookup.



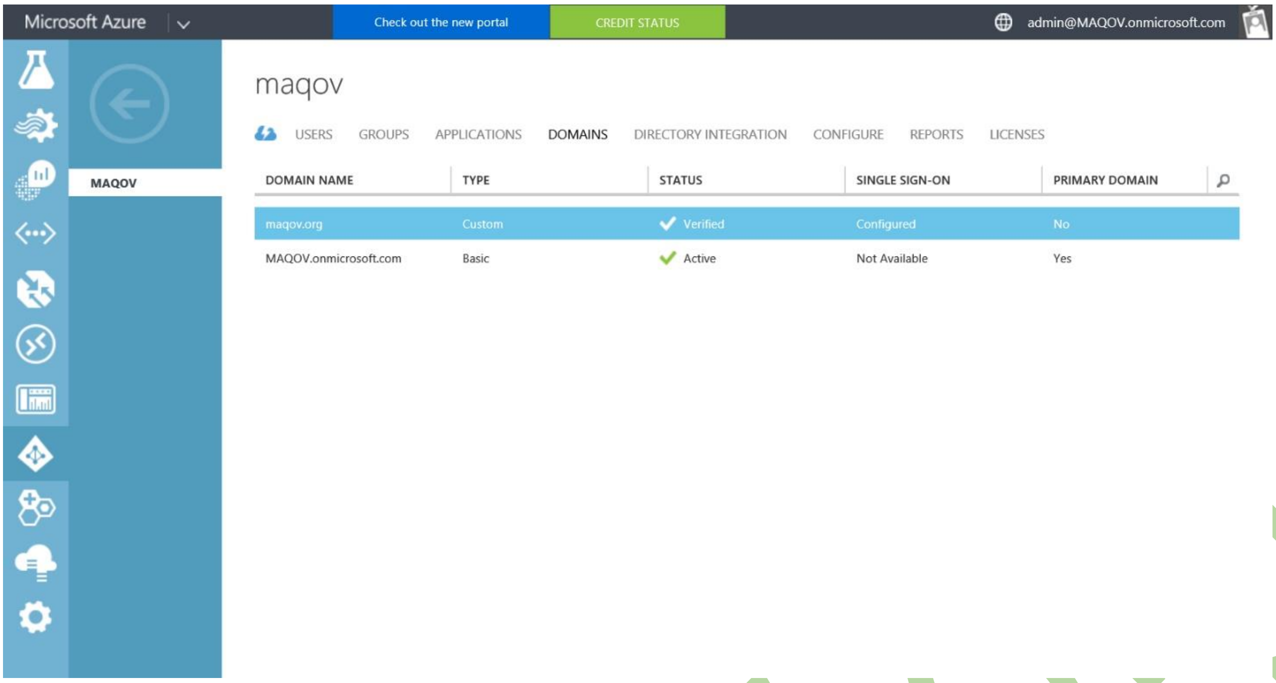
Type	Domain Name	TTL	Record
TXT	maqov.org	60 min	MS=ms56416453

Set trust between ADFS and Azure AD

Use the following PowerShell to setup the trust between ADFS and Azure AD.

```
$cred=Get-Credential
Connect-MsolService -Credential $cred

Set-MsolAdfscontext -Computer mobilityadfsc.maqov.org

New-MsolFederatedDomain -DomainName maqov.org

New-MsolFederatedDomain -DomainName maqov.org

Convert-MsolDomainToFederated -DomainName
```

Make sure that domain is verified, login to the azure management portal, go to **domain**.



maqov

DOMAIN NAME	TYPE	STATUS	SINGLE SIGN-ON	PRIMARY DOMAIN
maqov.org	Custom	✓ Verified	Configured	No
MAQOV.onmicrosoft.com	Basic	✓ Active	Not Available	Yes

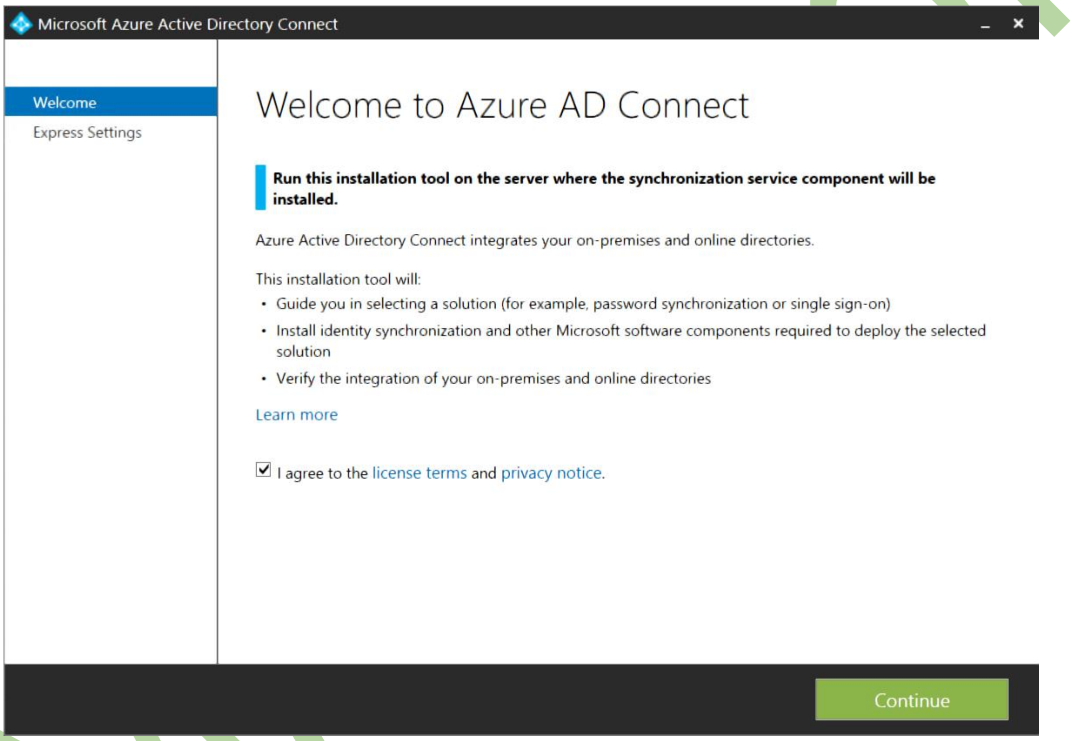
Install and Configure Azure AD Connect

1. Login to the Create VM for Azure AD Connect.
2. Download Azure AD Connect from https://www.microsoft.com/en-us/download/details.aspx?id=47594

Custom installation of Azure AD Connect

Before we begin on the filtered tab I tried to select a scoped security group before but I faced a weird behavior which is I couldn't filter by OU after the installation, so to overcome this issue I uninstalled the Azure AD Connect and reinstall it and on the **Filter** Screen I selected option **sync all users and Devices.**

1. On the **Welcome** Screen accept the license and terms, and then press **Continue**.



Welcome to Azure AD Connect

Run this installation tool on the server where the synchronization service component will be installed.

Azure Active Directory Connect integrates your on-premises and online directories.

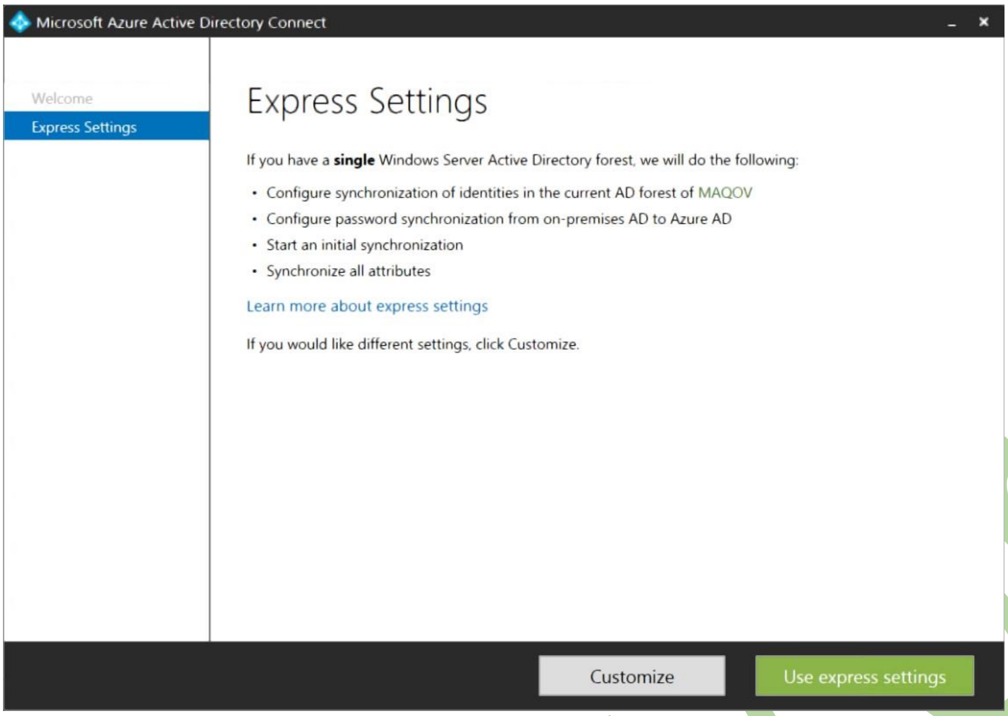
This installation tool will:

- Guide you in selecting a solution (for example, password synchronization or single sign-on)
- Install identity synchronization and other Microsoft software components required to deploy the selected solution
- Verify the integration of your on-premises and online directories

Learn more

☑ I agree to the license terms and privacy notice.

2. On the **Express Setting**, select Customize Install .



Microsoft Azure Active Directory Connect

Express Settings

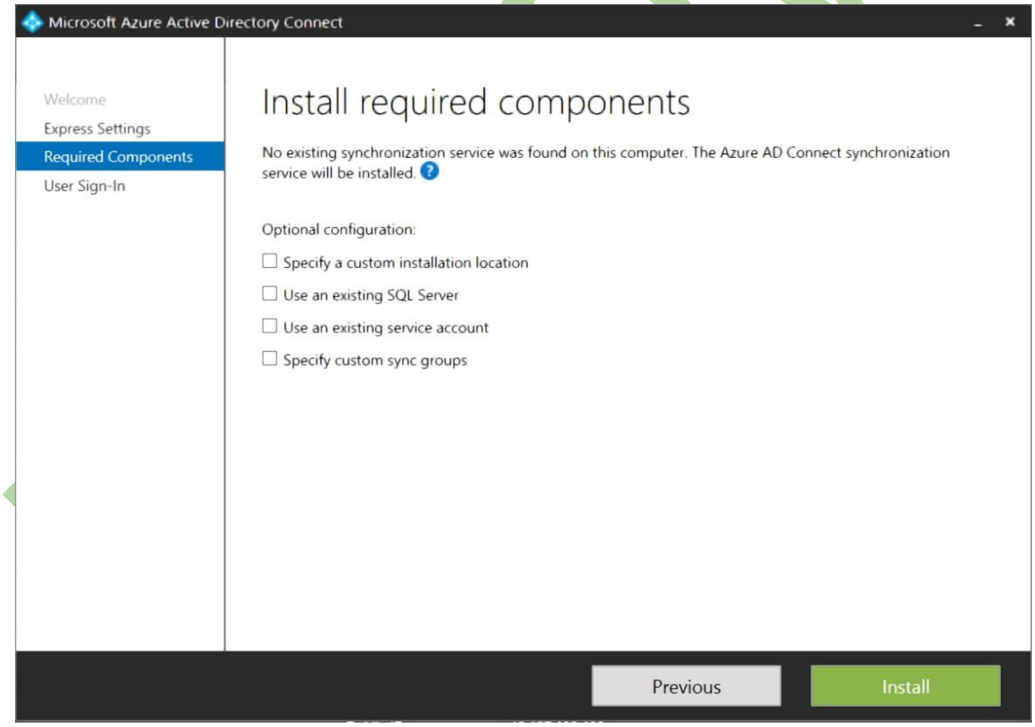
If you have a **single** Windows Server Active Directory forest, we will do the following:

- Configure synchronization of identities in the current AD forest of MAQOV
- Configure password synchronization from on-premises AD to Azure AD
- Start an initial synchronization
- Synchronize all attributes

Learn more about express settings

If you would like different settings, click Customize.

3. On the **Install the required Components**, click **Install.**



Microsoft Azure Active Directory Connect

Install required components

No existing synchronization service was found on this computer. The Azure AD Connect synchronization service will be installed.

Optional configuration:

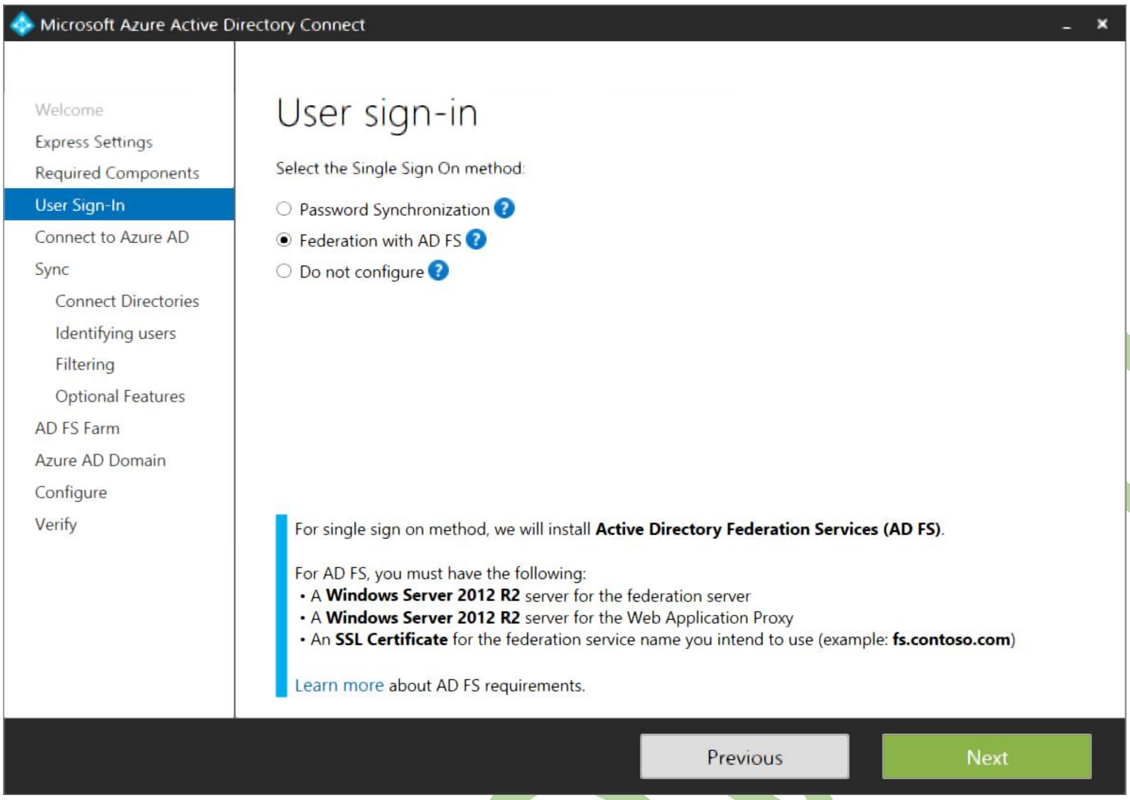
□ Specify a custom installation location

□ Use an existing SQL Server

□ Use an existing service account

□ Specify custom sync groups

4. On **User Sign In**, Select **Federate with ADFS,** click **Next**.



User sign-in

Select the Single Sign On method:

○ Password Synchronization

● Federation with AD FS

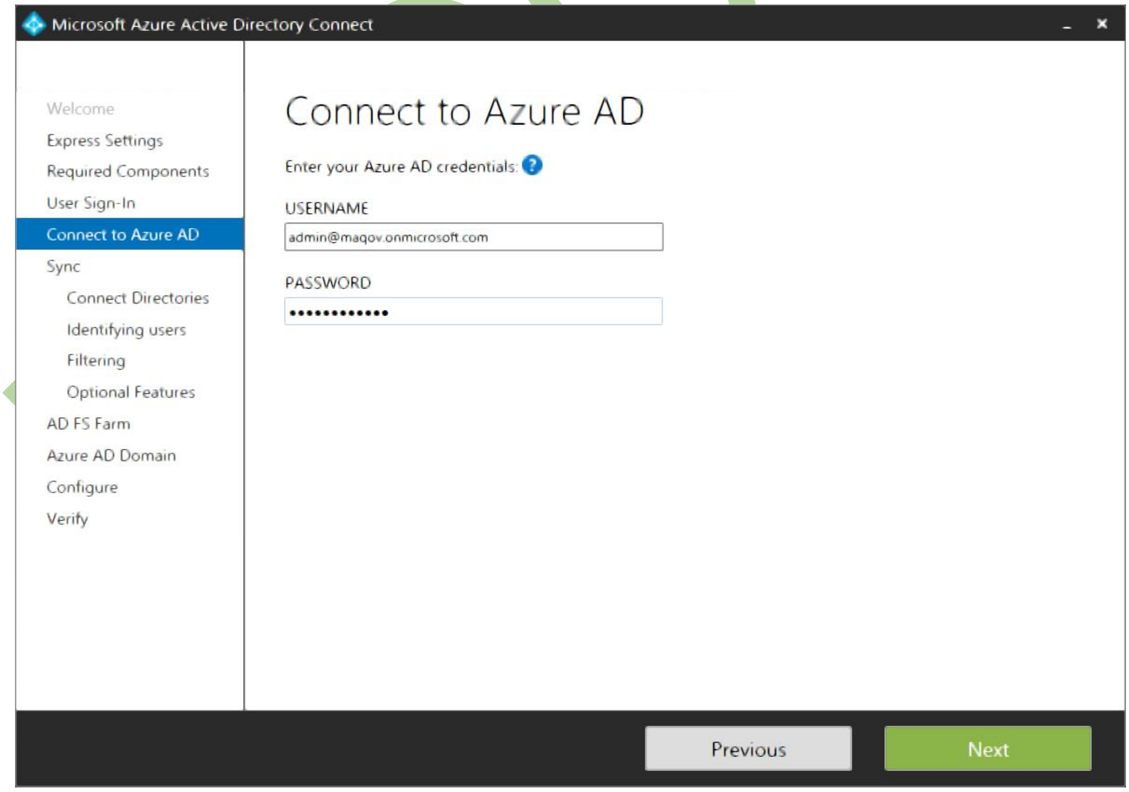
○ Do not configure

For single sign on method, we will install **Active Directory Federation Services (AD FS)**.

For AD FS, you must have the following:
- A **Windows Server 2012 R2** server for the federation server
- A **Windows Server 2012 R2** server for the Web Application Proxy
- An **SSL Certificate** for the federation service name you intend to use (example: **fs.contoso.com**)

Learn more about AD FS requirements.

5. On Connect to Azure AD, enter a global admin Credential, and then click Next.



Connect to Azure AD

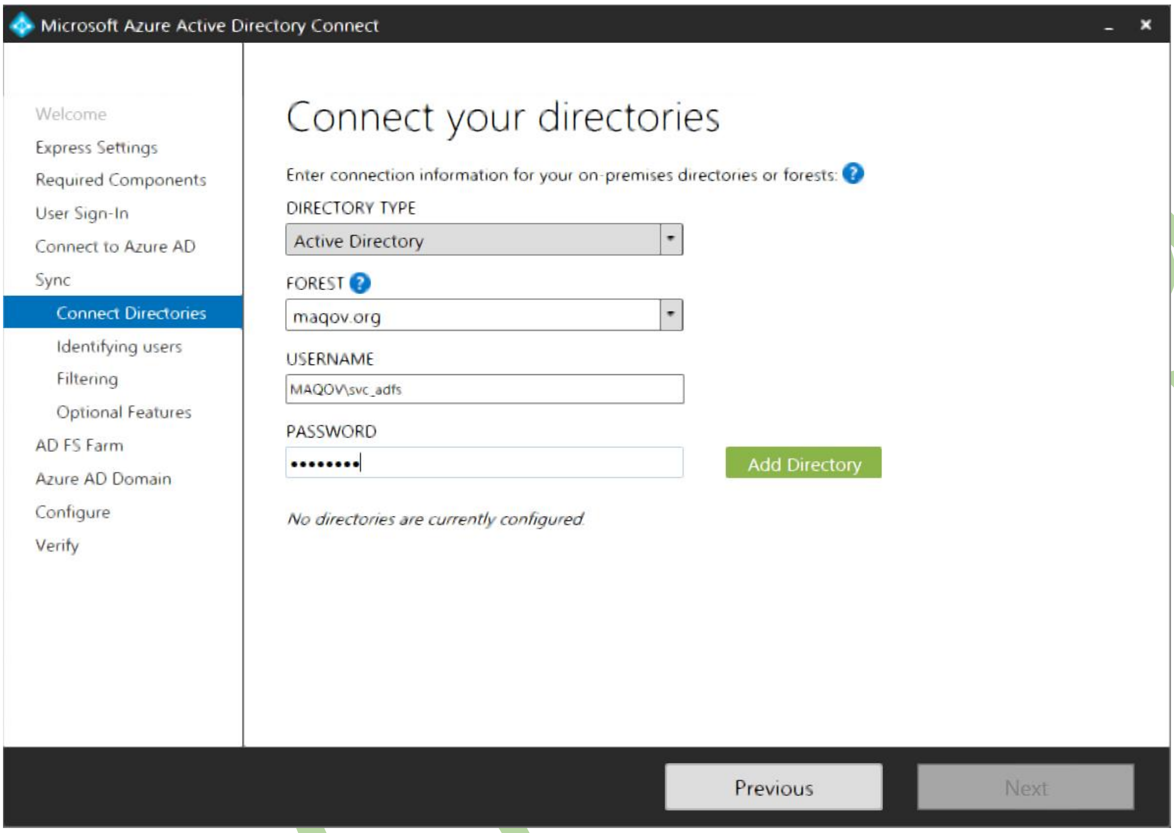
Enter your Azure AD credentials:

USERNAME: admin@maqov.onmicrosoft.com

PASSWORD: •••••••••••••

6. On **Connect to your directories**, enter the credentials and then click **ADD Directory** followed by **Next**.

   To connect to your Active Directory Domain Service, Azure AD Connect needs the credentials of an account with sufficient permissions. This account can be a regular user account because it only needs the default read permissions. However, depending on your scenario, you may need additional permissions. For more information, see [Azure AD Connect Accounts and permissions]()



Connect your directories

Enter connection information for your on-premises directories or forests:

DIRECTORY TYPE: Active Directory

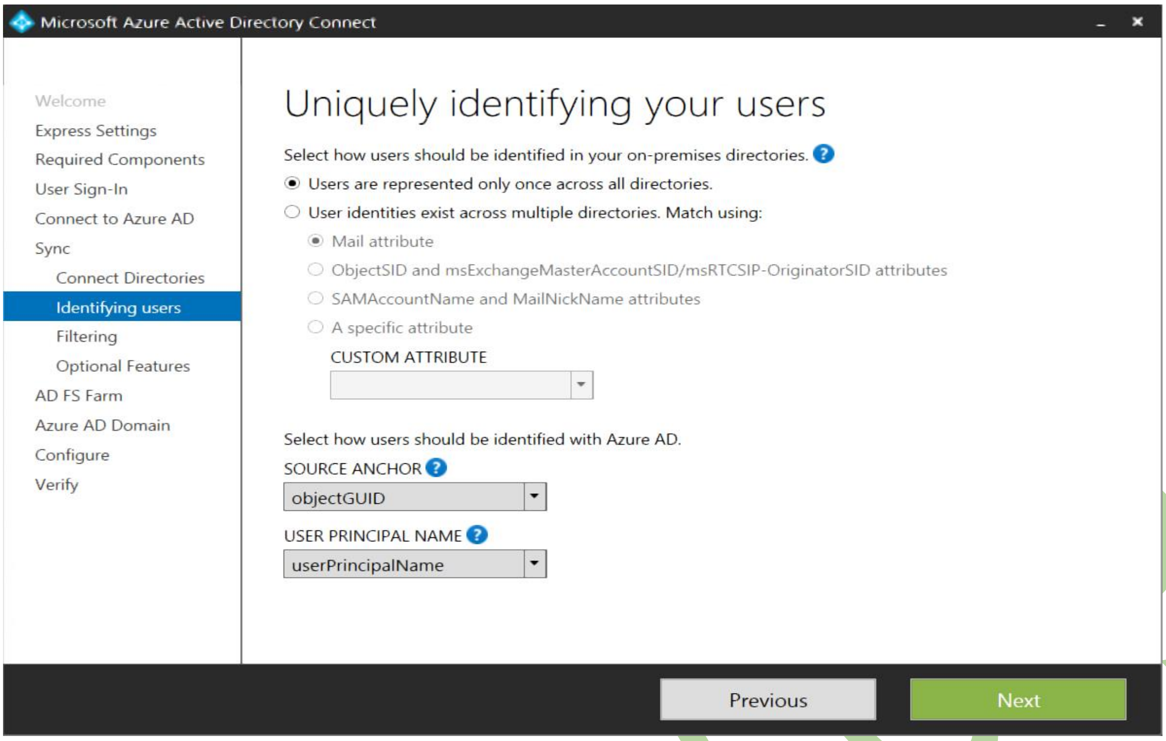
FOREST: maqov.org

USERNAME: MAQOV\svc_adfs

PASSWORD: ••••••••

No directories are currently configured

7. On **Uniquely identifying your users**, click **Next**.



Uniquely identifying your users

Select how users should be identified in your on-premises directories.

● Users are represented only once across all directories.

○ User identities exist across multiple directories. Match using:

- ● Mail attribute
- ○ ObjectSID and msExchangeMasterAccountSID/msRTCSIP-OriginatorSID attributes
- ○ SAMAccountName and MailNickName attributes
- ○ A specific attribute

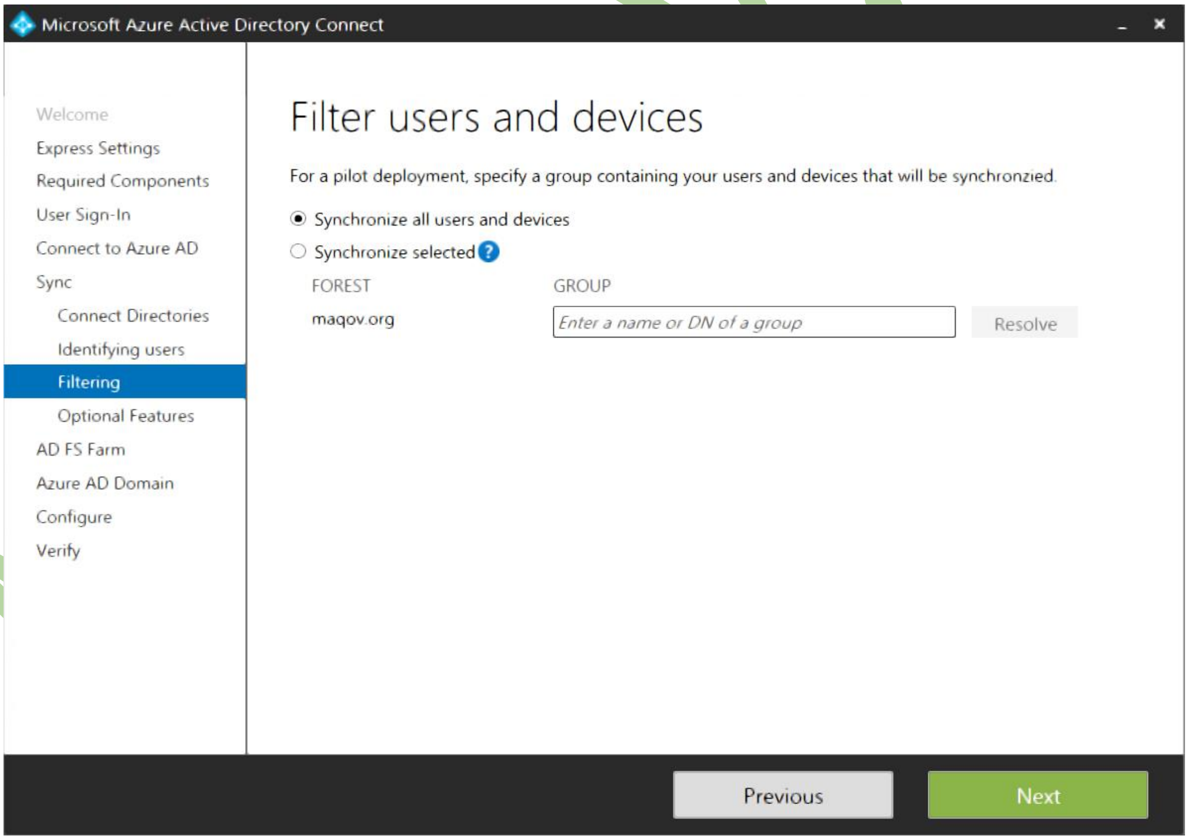
CUSTOM ATTRIBUTE

Select how users should be identified with Azure AD.

SOURCE ANCHOR: objectGUID

USER PRINCIPAL NAME: userPrincipalName

8. On the **Filtering,** Select **Synchronize all Users and Devices**.



Filter users and devices

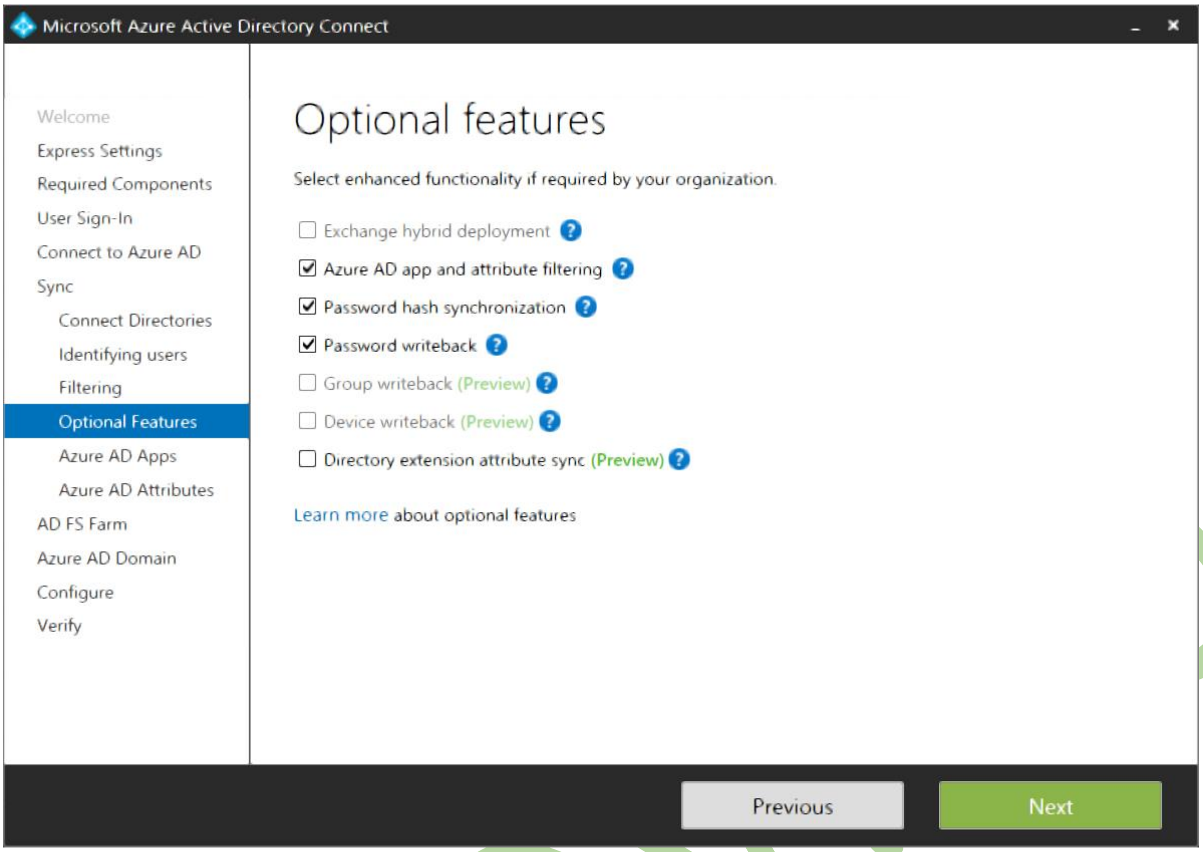
For a pilot deployment, specify a group containing your users and devices that will be synchronzied.

● Synchronize all users and devices

○ Synchronize selected

FOREST	GROUP
maqov.org	*Enter a name or DN of a group*

9. On Optional features select the feature you will you use according to the business need.



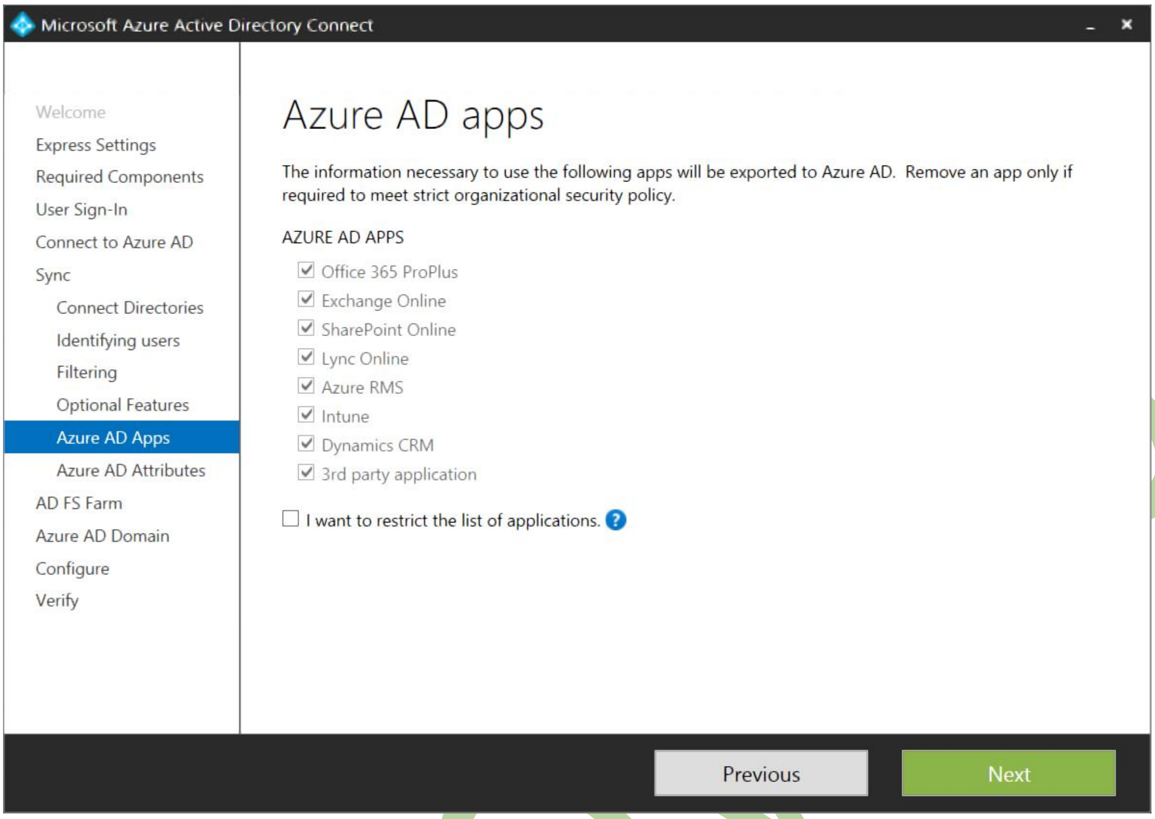
Optional features

Select enhanced functionality if required by your organization.

- □ Exchange hybrid deployment
- ☑ Azure AD app and attribute filtering
- ☑ Password hash synchronization
- ☑ Password writeback
- □ Group writeback (Preview)
- □ Device writeback (Preview)
- □ Directory extension attribute sync (Preview)

Learn more about optional features

10. On Azure AD Apps, click **Next**.



Azure AD apps

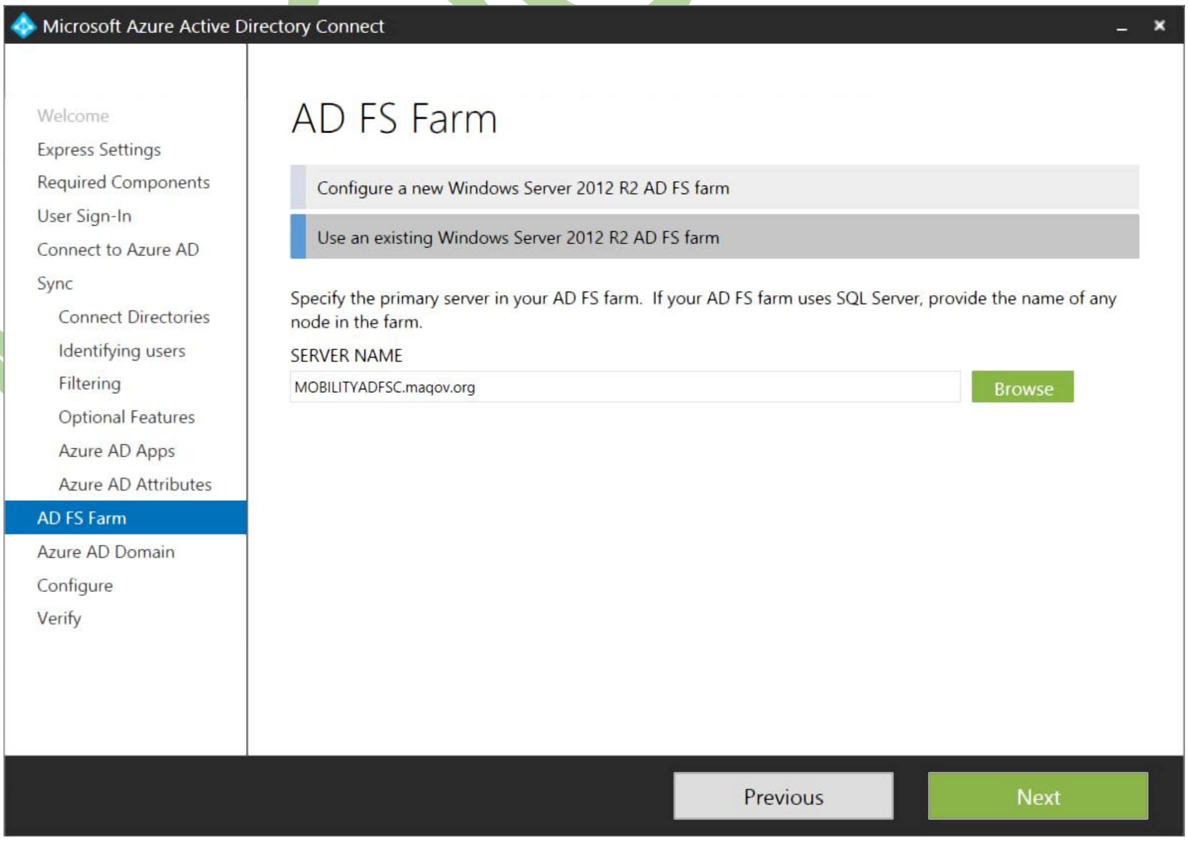
The information necessary to use the following apps will be exported to Azure AD. Remove an app only if required to meet strict organizational security policy.

AZURE AD APPS

- ☑ Office 365 ProPlus
- ☑ Exchange Online
- ☑ SharePoint Online
- ☑ Lync Online
- ☑ Azure RMS
- ☑ Intune
- ☑ Dynamics CRM
- ☑ 3rd party application

☐ I want to restrict the list of applications.

11. On **Azure AD** Attributes, click Next.
12. On **ADFS Farm**, Select the existing verified farm we already finished before, and then click **Next**.



AD FS Farm

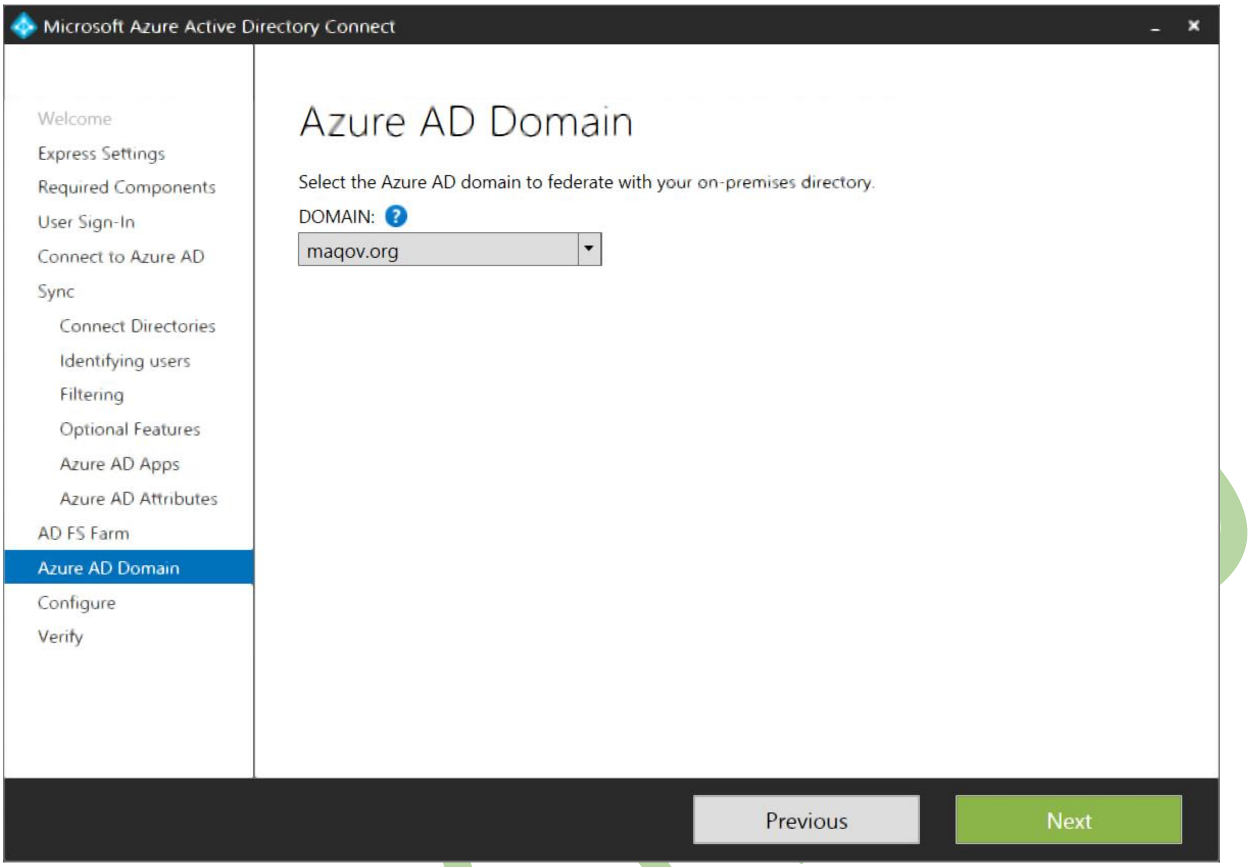
Configure a new Windows Server 2012 R2 AD FS farm

Use an existing Windows Server 2012 R2 AD FS farm

Specify the primary server in your AD FS farm. If your AD FS farm uses SQL Server, provide the name of any node in the farm.

SERVER NAME: MOBILITYADFSC.maqov.org

13. Azure AD Domain, select maqov.org that our domain in this case, and then click **Next**.

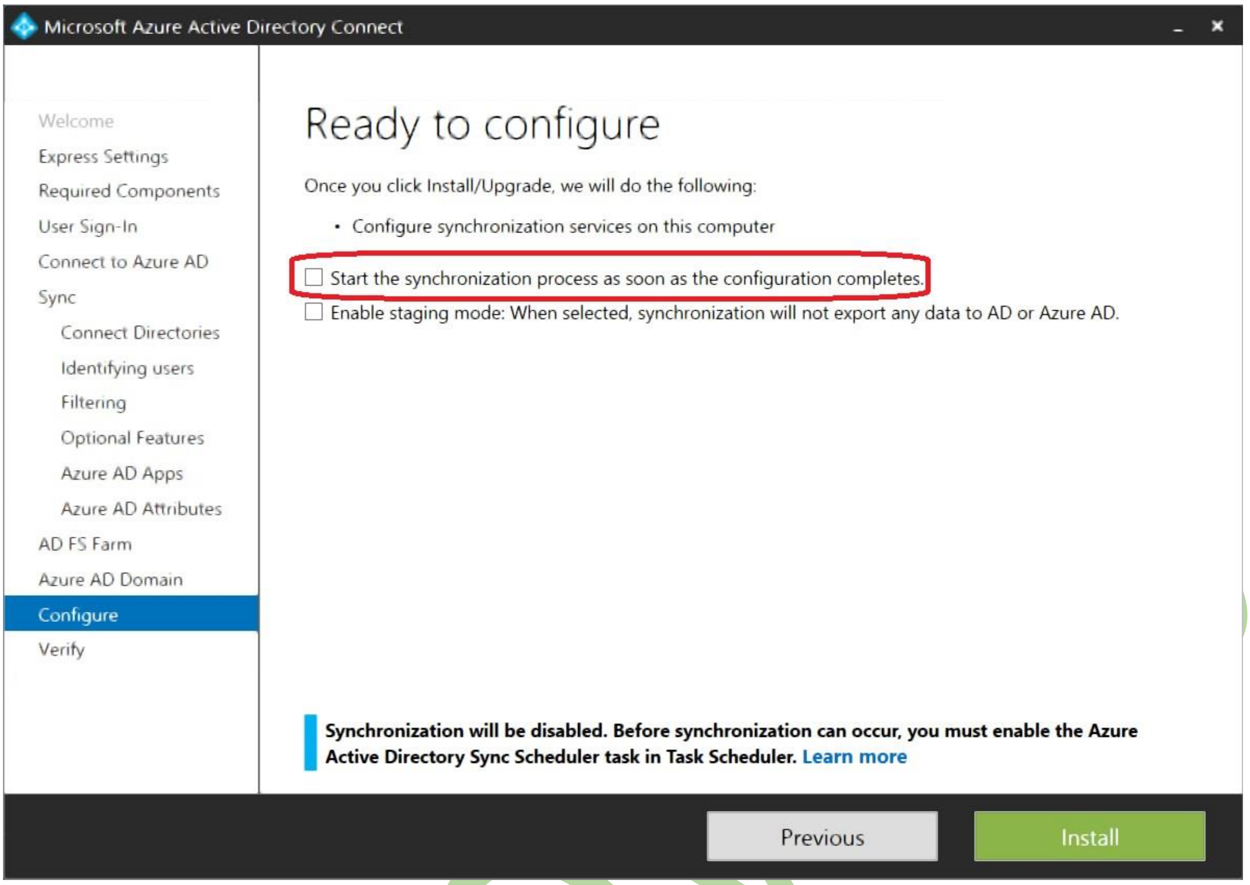


Azure AD Domain

Select the Azure AD domain to federate with your on-premises directory.

DOMAIN: maqov.org

14. **Uncheck**. "**Start the synchronization Process as soon as the configuration completes",** and then Click **Install.**
    This will prevent us to sync the whole active directry users and computers to Azure AD.



Ready to configure

Once you click Install/Upgrade, we will do the following:

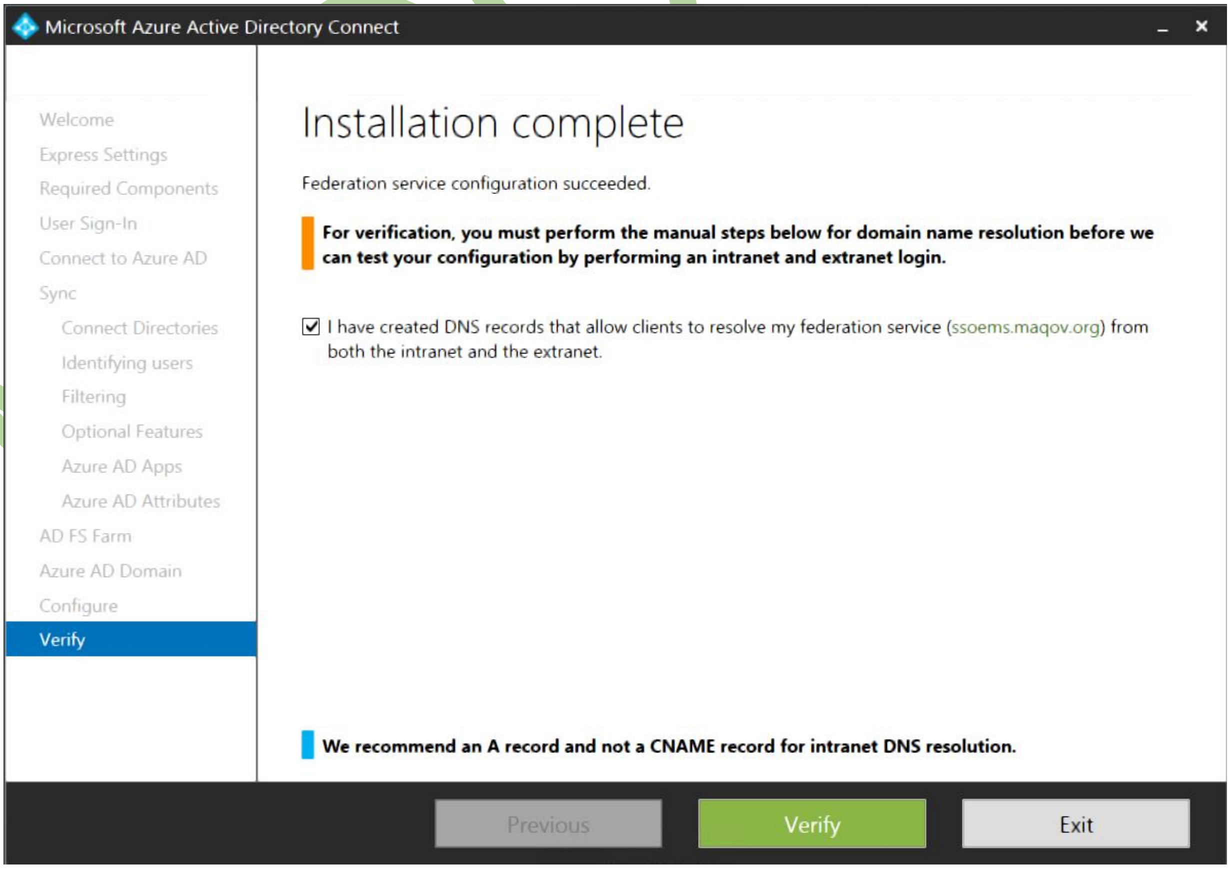
- Configure synchronization services on this computer

□ Start the synchronization process as soon as the configuration completes.

□ Enable staging mode: When selected, synchronization will not export any data to AD or Azure AD.

Synchronization will be disabled. Before synchronization can occur, you must enable the Azure Active Directory Sync Scheduler task in Task Scheduler. Learn more

15. On the Verify Screen Click **Verify**, and then **Exit**.

16. 

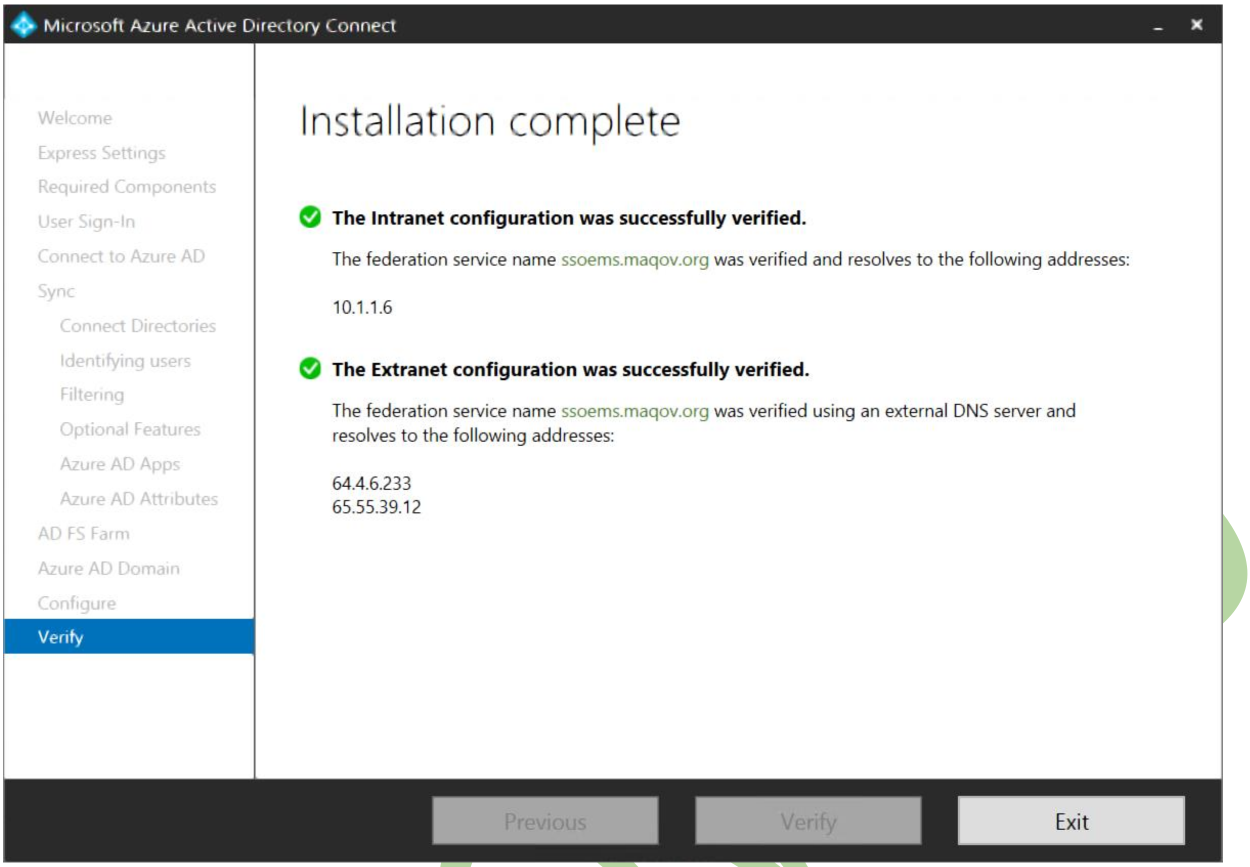
Installation complete

Federation service configuration succeeded.

For verification, you must perform the manual steps below for domain name resolution before we can test your configuration by performing an intranet and extranet login.

☑ I have created DNS records that allow clients to resolve my federation service (ssoems.maqov.org) from both the intranet and the extranet.

We recommend an A record and not a CNAME record for intranet DNS resolution.



Installation complete

✓ **The Intranet configuration was successfully verified.**

The federation service name ssoems.maqov.org was verified and resolves to the following addresses:

10.1.1.6

✓ **The Extranet configuration was successfully verified.**

The federation service name ssoems.maqov.org was verified using an external DNS server and resolves to the following addresses:

64.4.6.233
65.55.39.12

Congratulations now we can successfully sign in to the cloud services internally and externall.

Azure AD Connect sync: Configure Filtering

With filtering you can control which objects should appear in Azure AD from your on-premises directory. The default configuration will take all objects in all domains in the configured forests. In general, this is the recommended configuration. For example, end users using Office 365 workloads such as Exchange Online and Skype for Business will benefit from a complete Global Address List so they can send email and call everyone. With the default configuration they would get the same experience they would with an on-premises implementation of Exchange or Lync.

In some cases it is required to make some changes to the default configuration. Here are some examples:

- You plan to use the multi-Azure AD-directory topology. Then you need to apply a filter to control which object should be synchronized to a particular Azure AD directory.
- You run a pilot for Azure or Office 365 and only want a subset of users in Azure AD. In the small pilot it is not important to have a complete Global Address List to demonstrate the functionality.
- You have very many service accounts and other non-personal accounts you do not want in Azure AD.
- For compliance reasons you do not delete any user accounts on-premises; you only disable them. But in Azure AD you only want active accounts to be present.

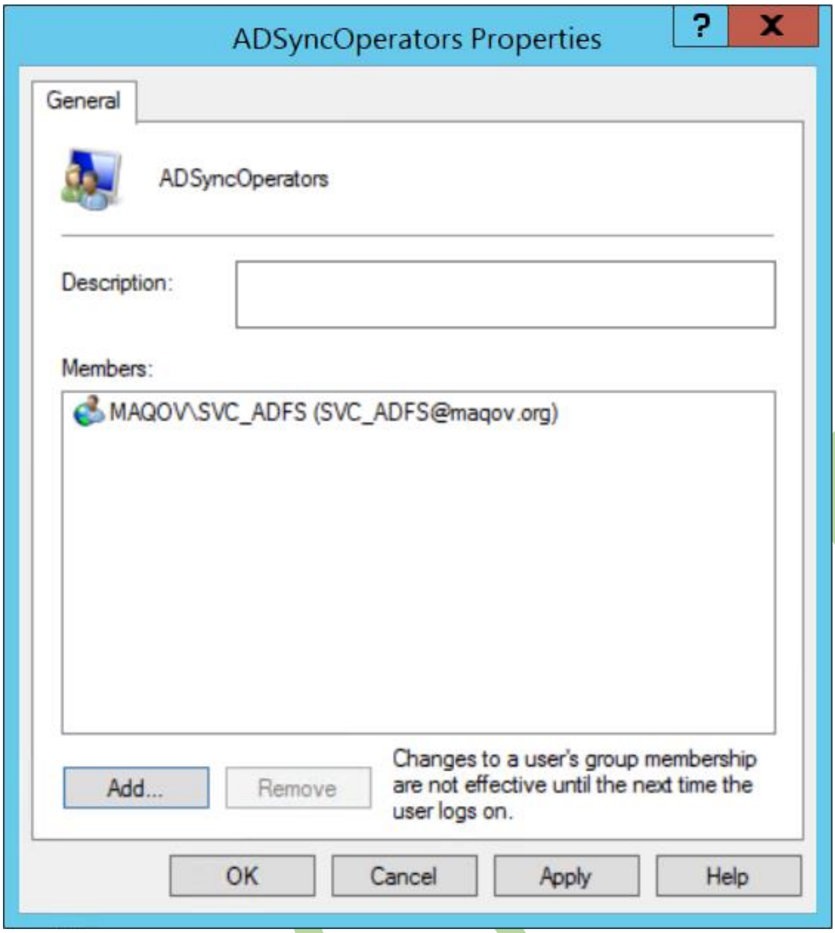
Filtering Options

The following filtering configuration types can be applied to the Directory Synchronization tool:

- **Group based**: Filtering based on a single group can only be configured on initial install using the installation wizard. It is not further covered in this topic.
- **Domain-based**: This option enables you to select which domains will synchronize to Azure AD. It also allows you to add and remove domains from the sync engine configuration if you make changes to your on-premises infrastructure after you installed Azure AD Connect sync.
- **Organizational-Unit–based**: This filtering option enables you to select which OUs will synchronize to Azure AD. This option will be on all object types in selected OUs.
- **Attribute–based**: This option allows you to filter objects based on attribute values on the objects. You can also have different filters for different object types.
- You can use multiple filtering options at the same time. For example, you can use OU-based filtering to only include objects in one OU and at the same time attribute-based filtering to filter the objects further. When you use multiple filtering methods, the filters use a logical AND between the filters.

I will use OU Based Option for this lab

1. In order to add to Add user to SVC_ADFS open **Azure AD Connect** VM , left click on "**Local Users and Groups** " in "**Computer Management**", **ADSyncOperators** (double click), and then add **SVC_ADFS,** click **OK**



ADSyncOperators Properties

ADSyncOperators

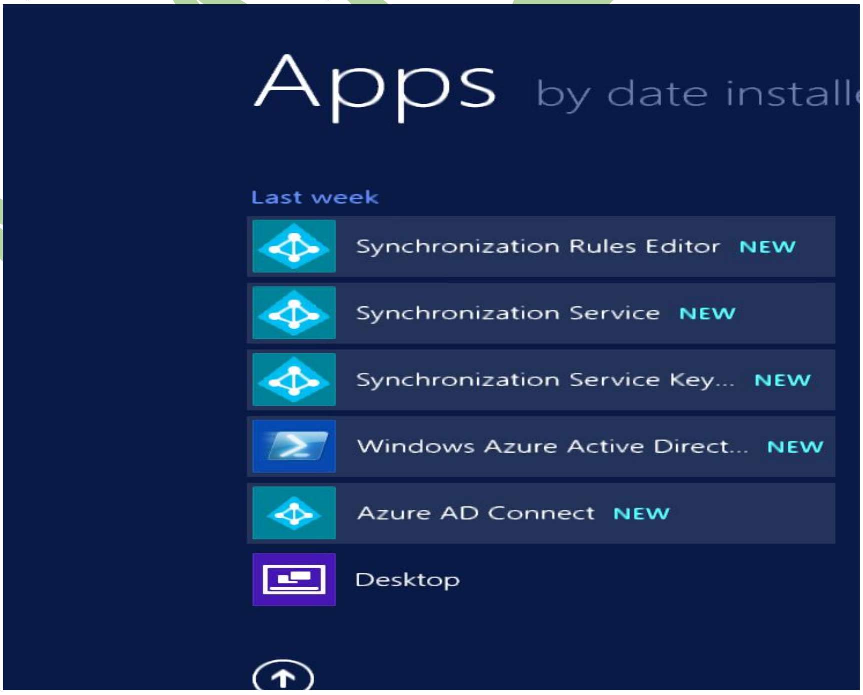
Description:

Members:

MAQOV\SVC_ADFS (SVC_ADFS@maqov.org)

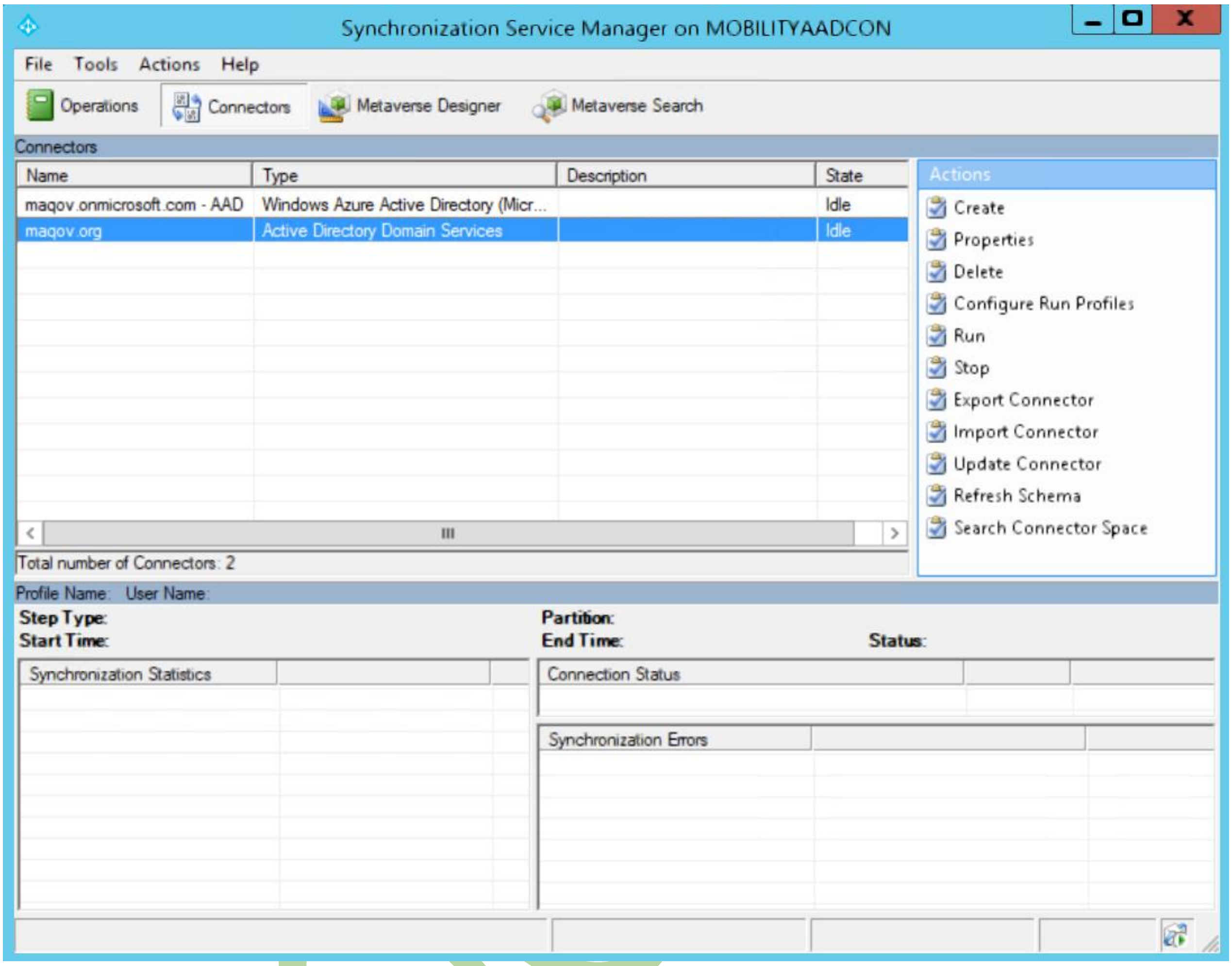
Changes to a user's group membership are not effective until the next time the user logs on.

2. Open **Start Menu,** Run "**Synchronization Service".**



Apps by date installe
Last week
Synchronization Rules Editor NEW
Synchronization Service NEW
Synchronization Service Key... NEW
Windows Azure Active Direct... NEW
Azure AD Connect NEW
Desktop

3. **On the Connectors Tab,** Select **Local AD "maqov.org", Right Click,** Select **Properties.**



Connectors

Name	Type	Description	State
maqov.onmicrosoft.com - AAD	Windows Azure Active Directory (Micr...		Idle
maqov.org	Active Directory Domain Services		Idle

Total number of Connectors: 2

Profile Name: User Name:

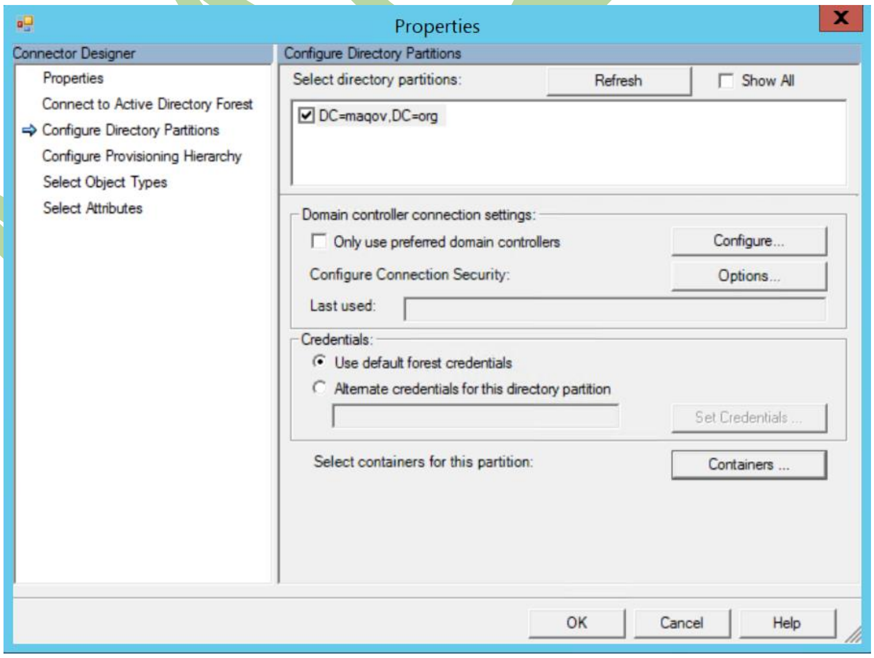
Step Type: **Partition:**
Start Time: **End Time:** **Status:**

Synchronization Statistics

Connection Status

Synchronization Errors

4. On the Left panel select **active directory Partitions.**
5. On the right panel select **Containers.**
6. Write the **Password.**



Configure Directory Partitions

Select directory partitions: □ Show All

☑ DC=maqov,DC=org

Domain controller connection settings:

□ Only use preferred domain controllers

Configure Connection Security:

Last used:

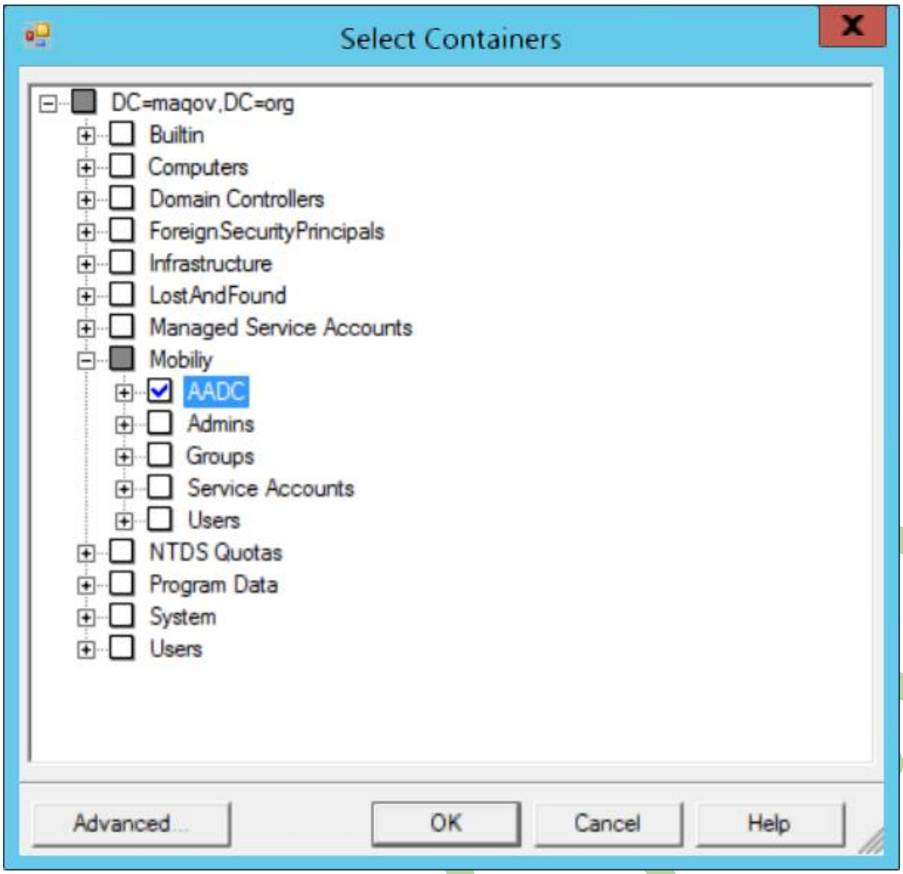
Credentials:

● Use default forest credentials

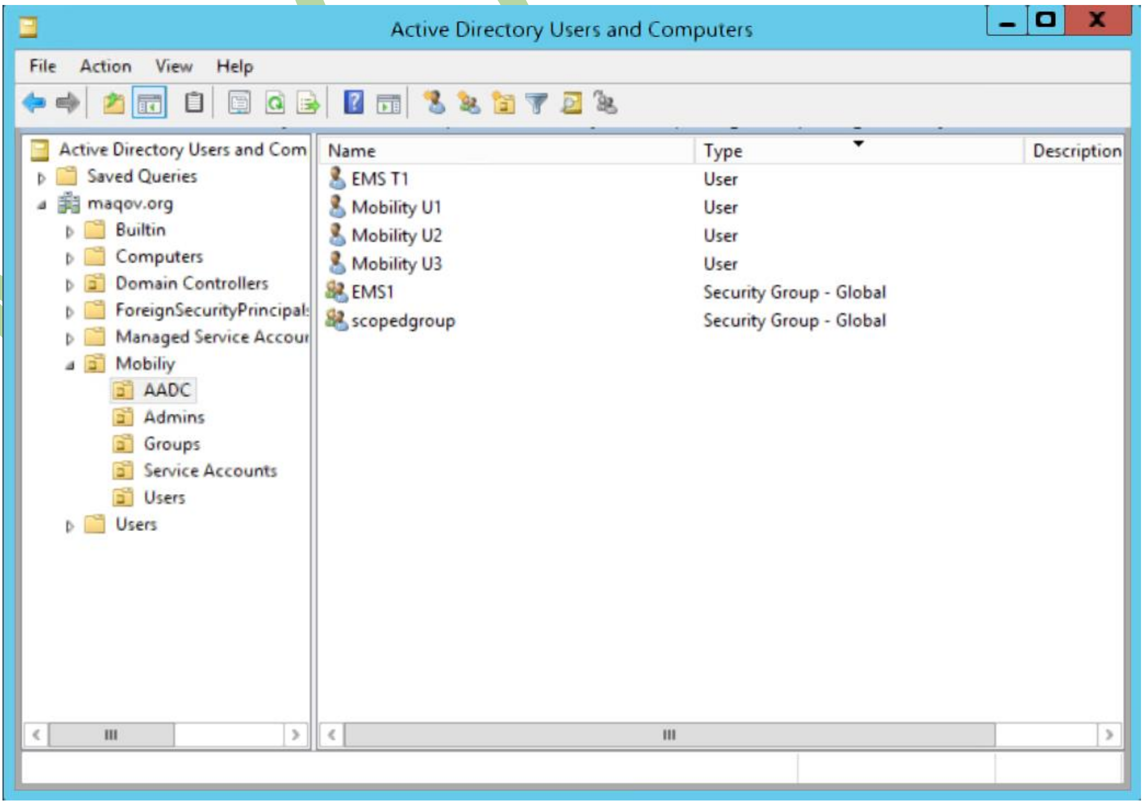
○ Alternate credentials for this directory partition

Select containers for this partition:

7. **Uncheck all the DC Ou's.**
8. Select the Desired **OU.**

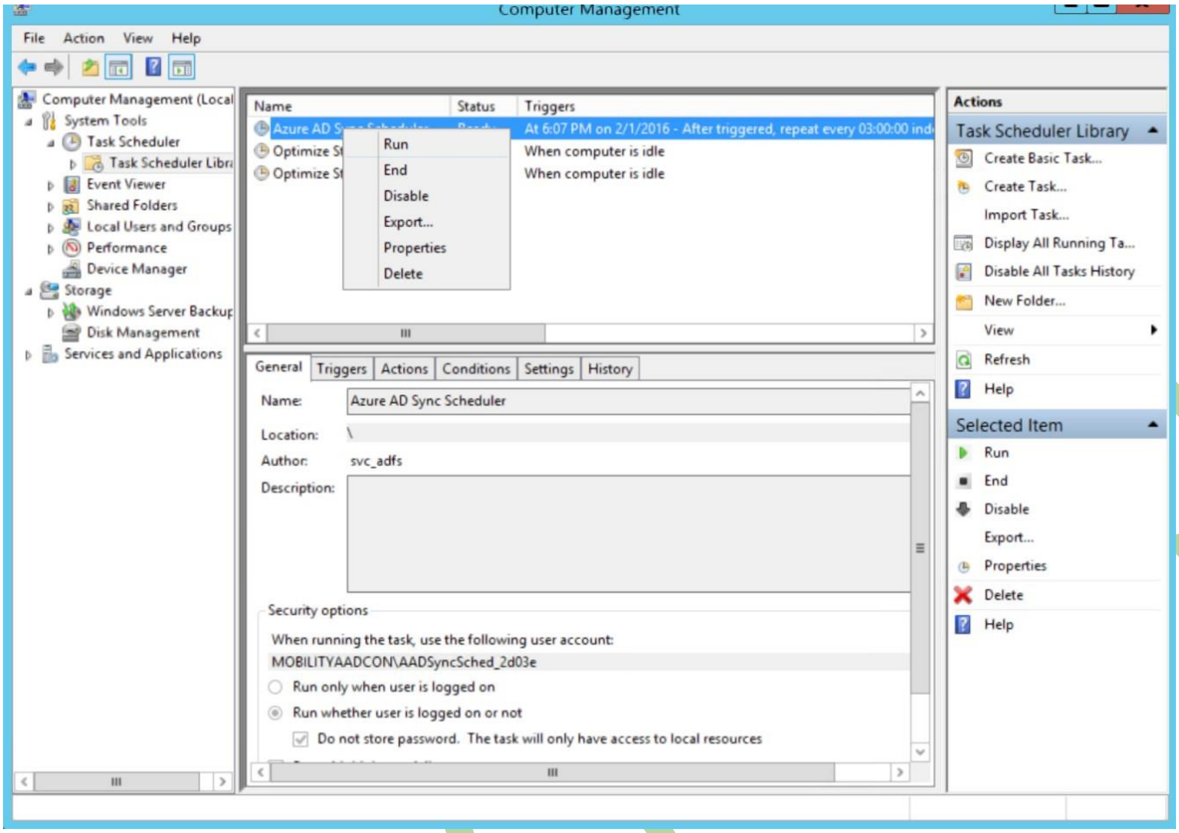


9. go to active Directory, make sure that the desired OU contains the users and groups you need to sync to the cloud.



Name	Type	Description
EMS T1	User	
Mobility U1	User	
Mobility U2	User	
Mobility U3	User	
EMS1	Security Group - Global	
scopedgroup	Security Group - Global	

10. back to **Azure AD Connect VM**, open **Computer management**, **task scheduler**, **task scheduler library**, select the **Azure AD Sync, Right Click Enable then RUN.**



Name	Status	Triggers
Azure AD S...		At 6:07 PM on 2/1/2016 - After triggered, repeat every 03:00:00 ind
Optimize St		When computer is idle
Optimize St		When computer is idle

Name: Azure AD Sync Scheduler

Location: \

Author: svc_adfs

Description:

Security options

When running the task, use the following user account:

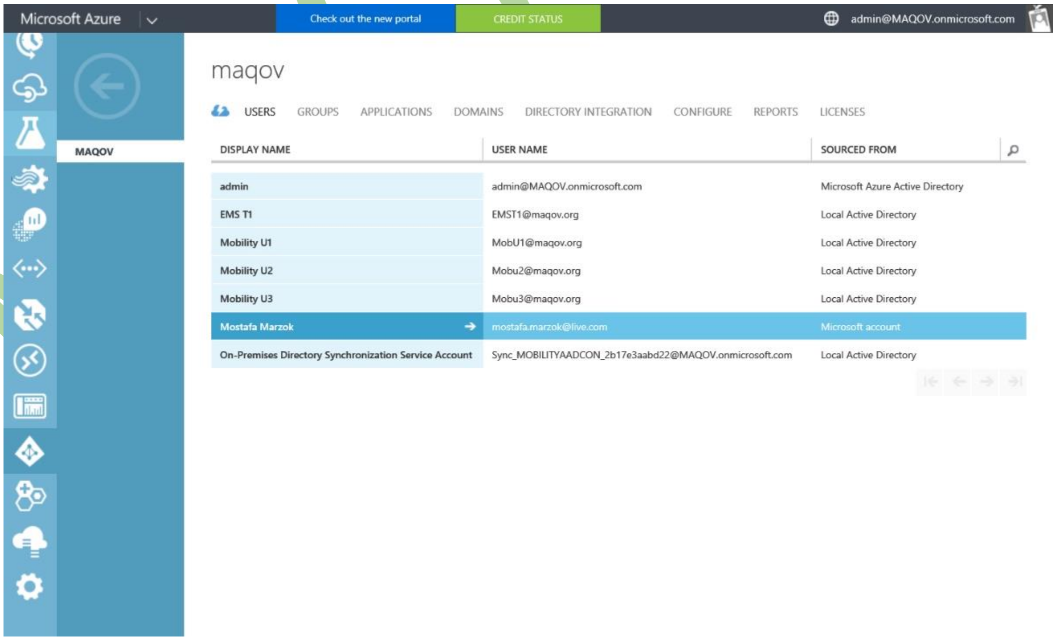
MOBILITYAADCON\AADSyncSched_2d03e

○ Run only when user is logged on

● Run whether user is logged on or not

☑ Do not store password. The task will only have access to local resources

11. after the job is **done** please login to the **azure management portal**, select **active directory**, select your directory and then select Users**.**



maqov

DISPLAY NAME	USER NAME	SOURCED FROM
admin	admin@MAQOV.onmicrosoft.com	Microsoft Azure Active Directory
EMS T1	EMST1@maqov.org	Local Active Directory
Mobility U1	MobU1@maqov.org	Local Active Directory
Mobility U2	Mobu2@maqov.org	Local Active Directory
Mobility U3	Mobu3@maqov.org	Local Active Directory
Mostafa Marzok	mostafa.marzok@live.com	Microsoft account
On-Premises Directory Synchronization Service Account	Sync_MOBILITYAADCON_2b17e3aabd22@MAQOV.onmicrosoft.com	Local Active Directory