Best Practice Guide

Authentication with Azure AD Domain Services

Introduction

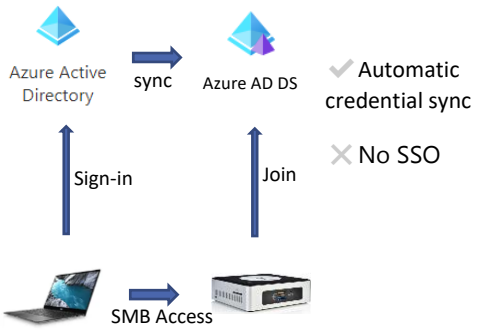
Morro Data supports both Active Directory and Azure AD for user authentication. In this Best Practice Guide, we will cover Azure AD Domain Services (AAD DS) configuration for Single-Sign-On (SSO) access to CacheDrive shares.

The following table shows the differences between Azure AD, on-prem AD, and Azure AD DS in the context of CacheDrive share access. In the Azure AD Only method, which is common among organizations that use Microsoft 365 without migrating from an on-prem AD environment, users must login separately when accessing CacheDrive shares. In the AD and Azure AD DS environments, users can enjoy the benefits of SSO when accessing CacheDrive shares from a domain-joined PC.

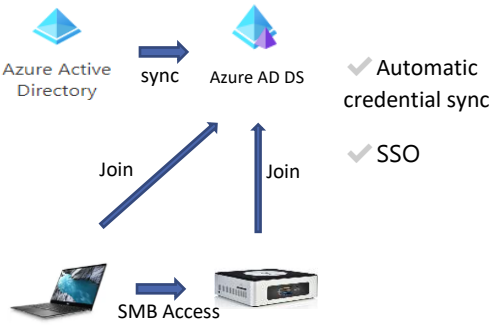
Method	Morro Auth Mode	Windows Login	SSO	Notes
Azure AD Only	Azure AD	Azure AD	Manual credential sync Need password for access	Simple setup
AD	Active Directory (*1)	domain-joined PC	SSO for share access	(*2)
Azure AD DS	Active Directory (*1)	domain-joined PC	SSO for share access	(*2)
		Non domain-joined PC	Automatic credential sync Need password for access	For BYOD (bring-your-own-device)

(*1) When configuring the Morro authentication mode, “Active Directory” should be used for both AD and Azure AD DS setups.
(*2) Microsoft does not support SSO using WHFB (Windows Hello for Business).

The following diagrams further illustrate the two Windows login scenarios using the Azure AD DS method listed above.



PC is not joined to AAD DS
CacheDrive is joined to AAD DS



Both PC and CacheDrive are joined to AAD DS

Best Practice Guide

In this Guide, we will focus on the Azure AD Domain Service (AAD DS) method. For other authentication methods, please refer to the following Knowledge Base articles:

Team - Authentication
Team - User (Azure AD Mode)

Why Azure AD Domain Services?

Azure AD is designed for cloud resources, and is not ideal for on-prem resources or legacy applications running in Windows VMs on Azure. On-prem file sharing in a LAN environment, however, uses the SMB protocol and requires domain authentication. By extending AD Domain Services to the cloud (called Azure AD Domain Services), Microsoft enables AD-based authentication for on-prem SMB applications without an on-prem AD Domain Controller.

In this document, we will discuss the steps required to configure Azure AD Domain Services for use with CacheDrive shares.

Accessing the CacheDrive in Azure AD DS with SSO

In an Azure AD DS environment, the CacheDrive becomes a trusted server once is it joined to the Azure AD DS. When users login to a Windows PC client using a Work or School account, the PC establishes a trust relationship with the domain, which allows SSO access to the shares on the CacheDrive.

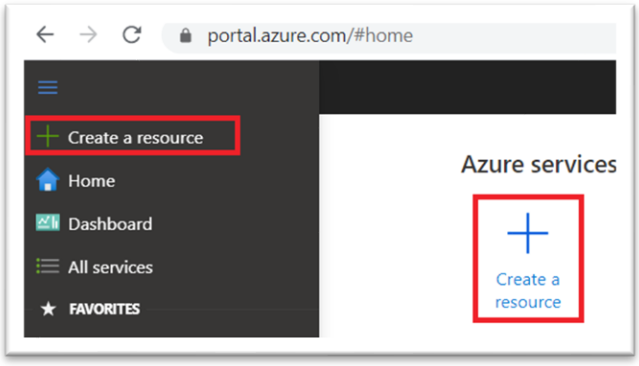
In this Best Practice Guide, we will go through the following steps in detail:

1. Setting up Azure AD Domain Services
2. Setting up a VPN between Azure and Your Premises
3. Join a Windows PC to Azure AD Domain Services
4. Join a Morro CacheDrive to Azure AD Domain Services
5. Single Sign On

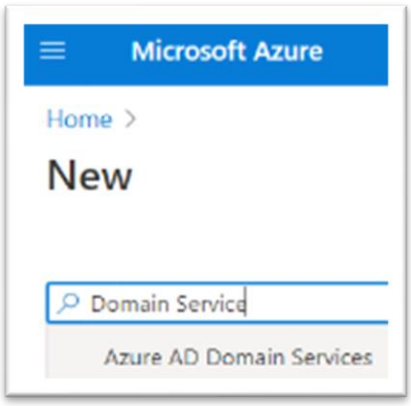
Setting up Azure AD Domain Services

From the Azure Portal:

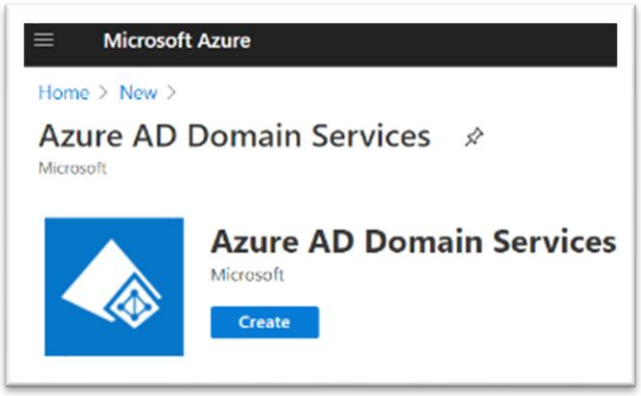
1. Click “Create a resource”.



2. Search for “Domain Service”.

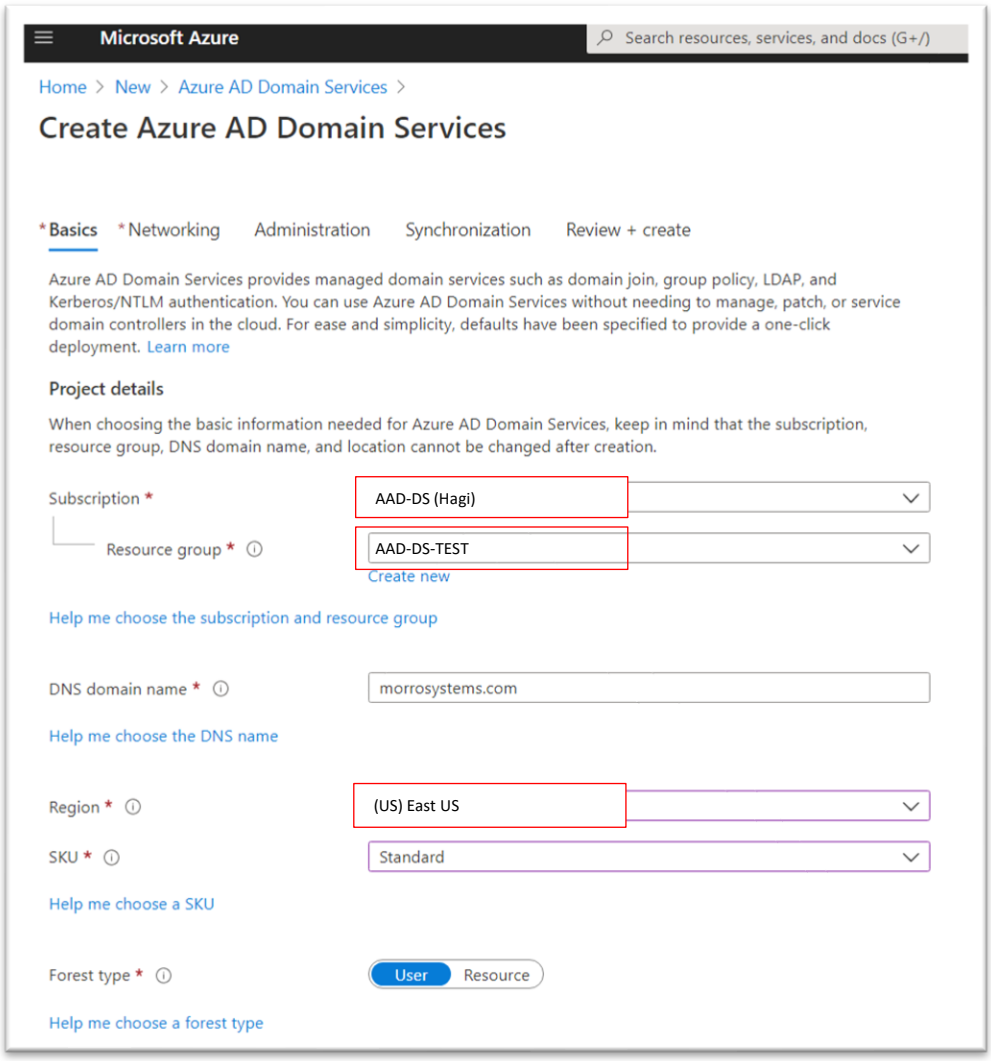


3. Select “Azure AD Domain Services”.

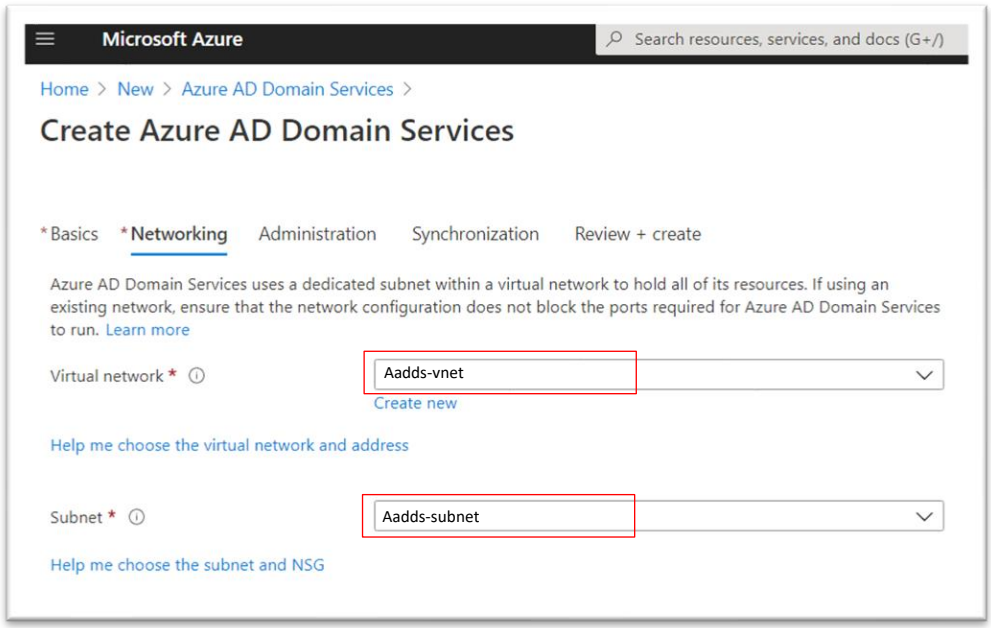


4. Click the Create button to start the creation wizard.

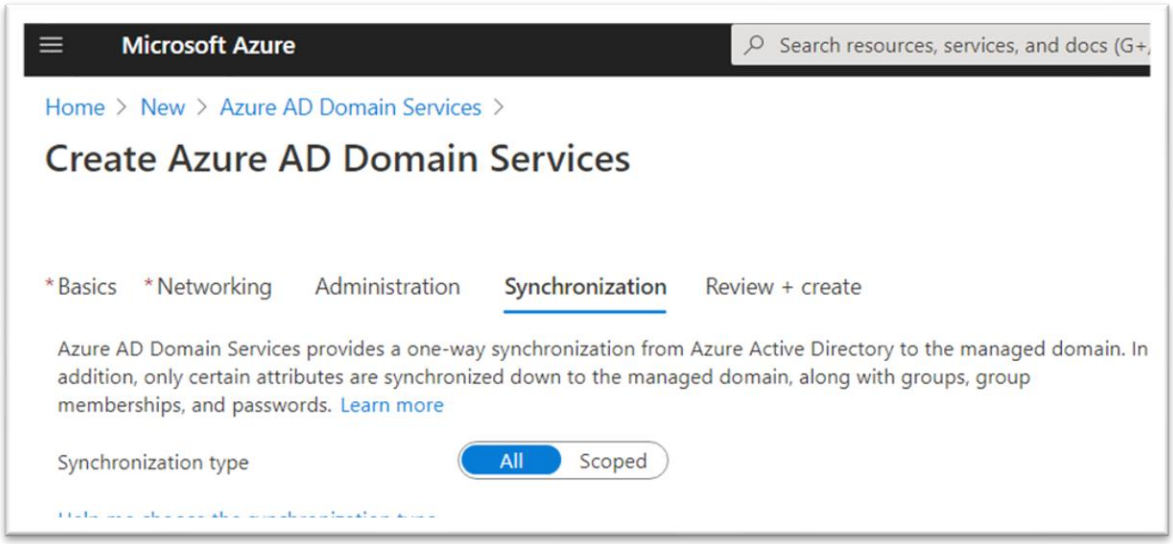
In the Basics tab, set the subscription (your Azure subscription) and resource group. DNS name can be the default yourcompany.onmicrosoft.com or a custom domain.



In the Networking tab, select or create the virtual network and subnet.

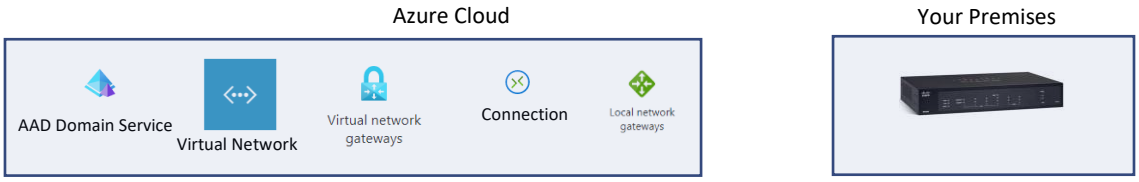


In the Synchronization tab, select all or partial entities (users/groups) to be synced from Azure AD to Azure AD Domain Services.



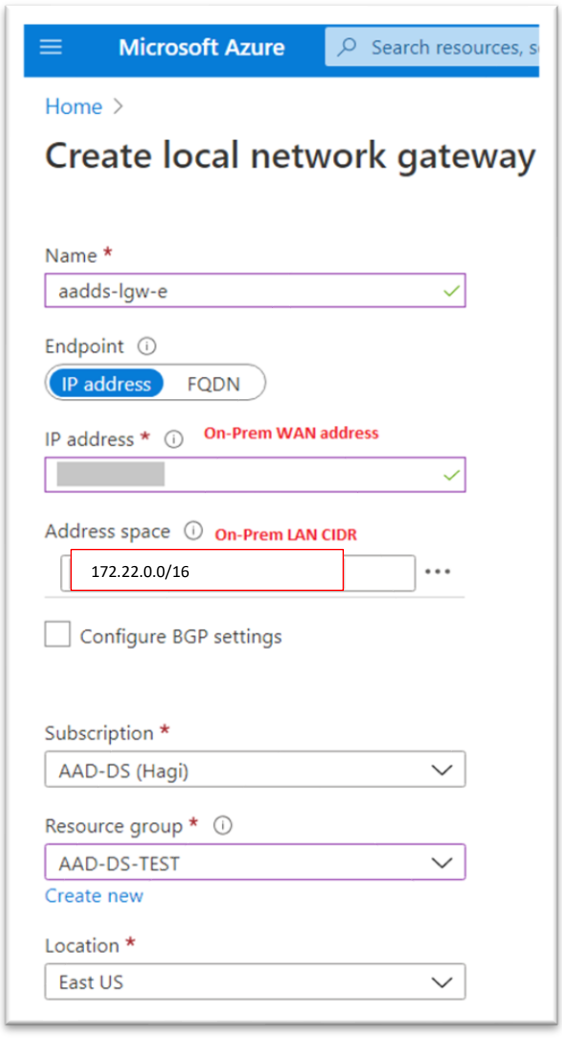
Setting Up a VPN between Azure and Your Premises

VPN is needed to securely connect your premises and the Azure Virtual Network where the Azure AD Domain Services is hosted. In the previous step, we created AAD, AAD DS and the Virtual Network. Now we will create three additional resources in Azure Cloud: Local network gateway, Virtual network gateway, and Connection.



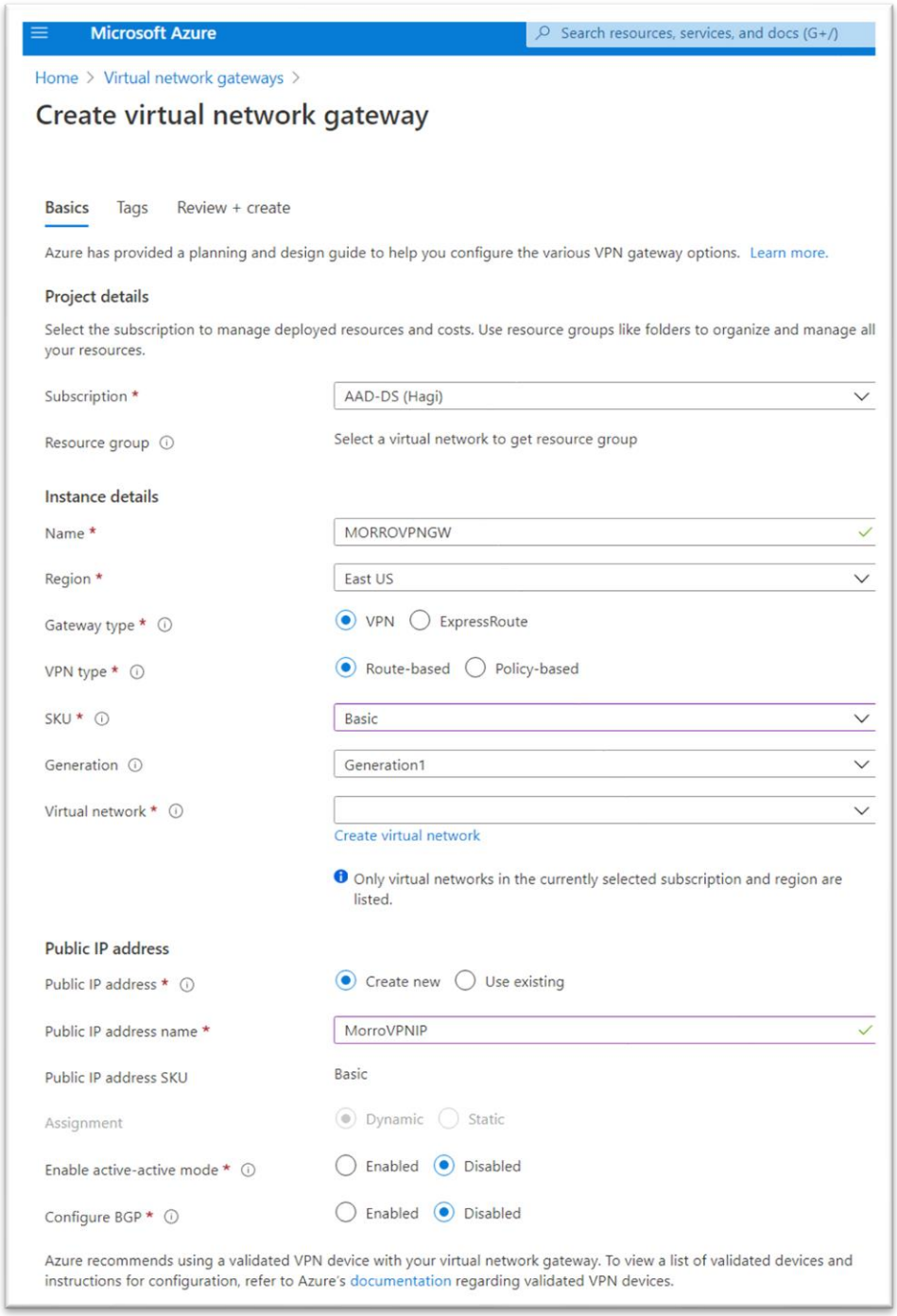
Create the Local network gateway

Specify the IP Address (or FQDN) for your premises. A local gateway needs to be specified for each CacheDrive location.



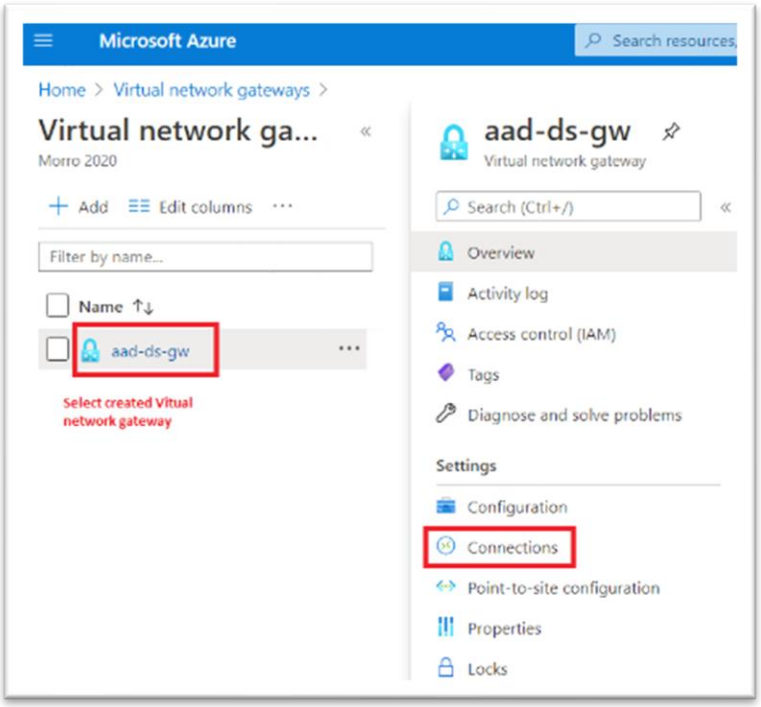
Create virtual network gateway

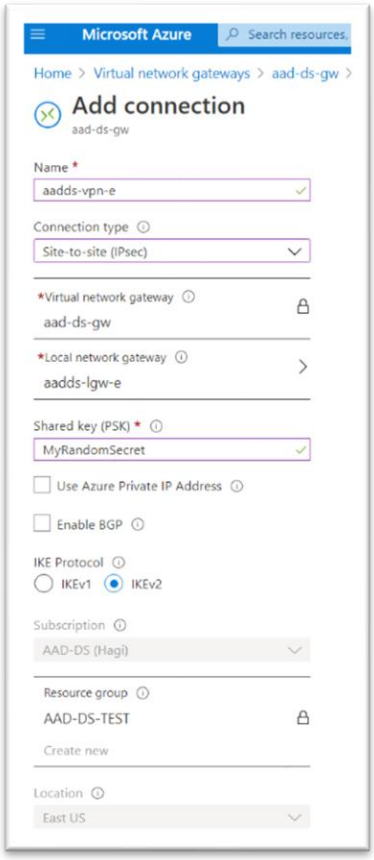
Select “Virtual network” which is the network where the AAD DS is hosted. You may need to adjust the virtual network by adding address space.



Create Connection

In the Virtual network gateway management screen, click “Connections”. Then click “Add”. In the “Add connection” section, enter your Pre-Shared Key (share key for both end of vpn connection).

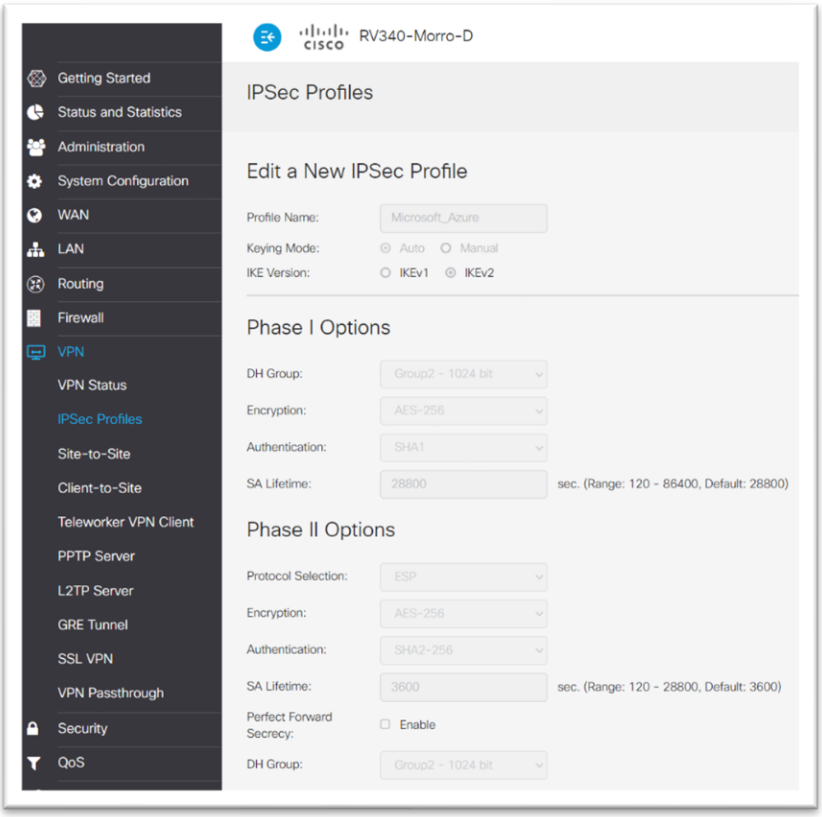




Set Up the On Premises VPN Router

The detailed procedure of this step depends on the router. Below is an example using the Cisco RV340 VPN router.

1. Modify the IPsec profile ("Microsoft Azure" is pre-defined in this router but does not work) or create a new profile as below. This depends on your VPN settings in Azure.
    - Change to IKEv2 (default is IKEv1 in RV340, Azure default is IKEv2.)
    - Phase II option, Authentication: Change to SHA2-256 (default is SHA1)



2. Create the VPN connection

    Now you can create the Site-to-Site VPN connection. On the Basic Settings page, select IPsec profile which we modified (or created) in the above step.

    Set the Remote Endpoint which is obtained from the Azure Virtual network gateway Overview.

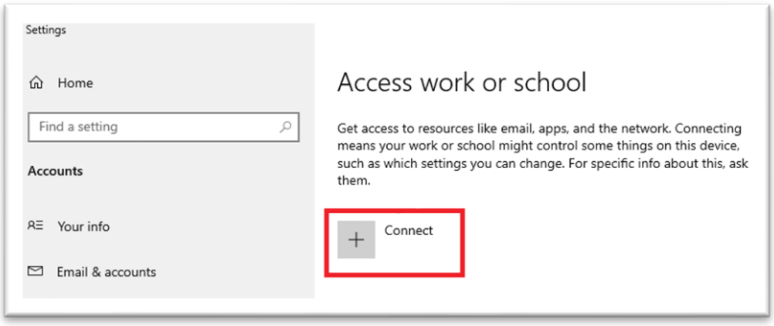
    Set Split DNS under the Advanced tab. The DNS server address can be obtained from Azure AD Domain Services. Then set up the Domain name so that all DNS queries for *.yourdomain will be resolved by the specified DNS Server.

Join a Windows PC to Azure AD Domain Services

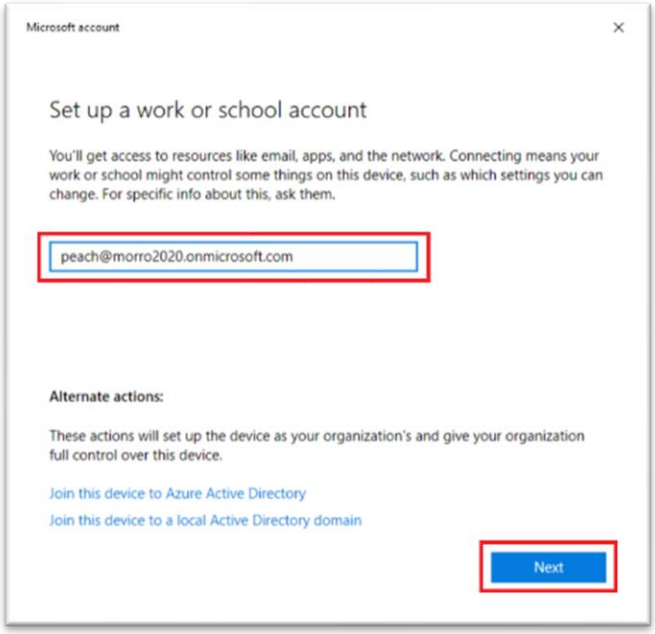
When a Windows 10 Pro PC is set up for the first time, the default is to connect to Azure AD. In our example below, we assume the PC is not connected to any domain. We will login as the local user who has local administrative privileges.

Connect to Azure AD

1. Login as a user with Administrator privilege.
2. Navigate to “Access work or school” in the Setting menu. Click Connect.



3. From the Wizard, select Work or School account, enter an email address and click Next.

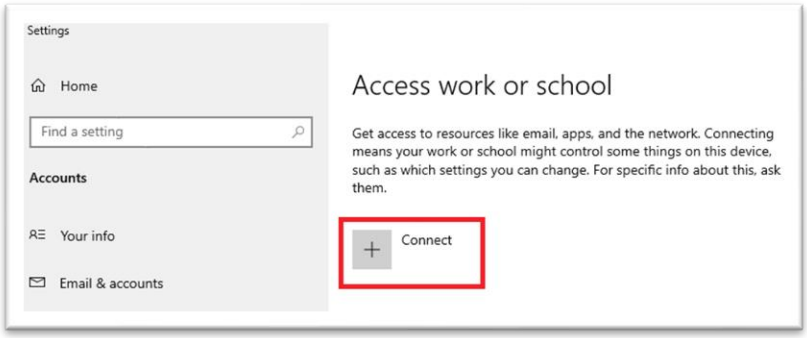


4. The Authentication flow will start. Click Sign in and the PC will be connected to Azure AD when authentication succeeds.

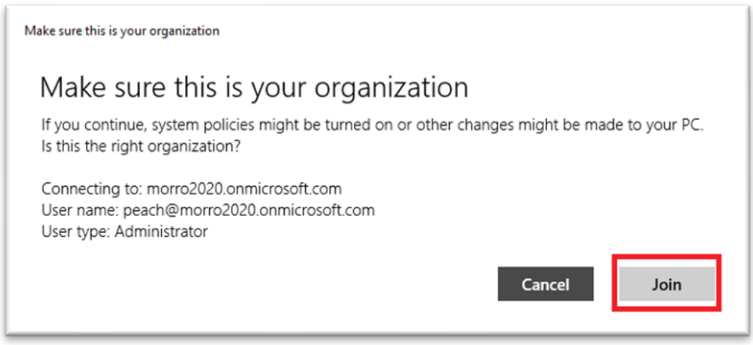
Join the PC to Azure AD

This mode allows your organization to manage the PC. This setup is usually done by an organization's IT administrator when setting up a PC which is owned by the organization and used by member of the organization.

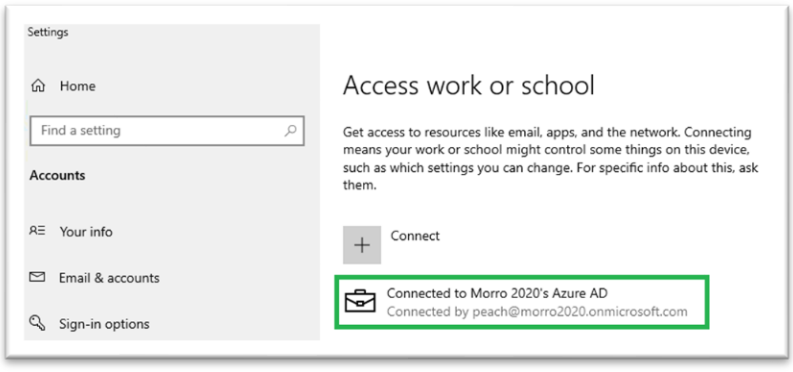
1. Login as a user with Administrator privilege.
2. Navigate to "Access work or school" in Setting menu. Click Connect.



3. Select the "Join this device to Azure Active Directory" option. Enter the account name (email) and password and click Next.
4. Because this flow gives your organization full privilege, you will be asked to confirm it is your organization.



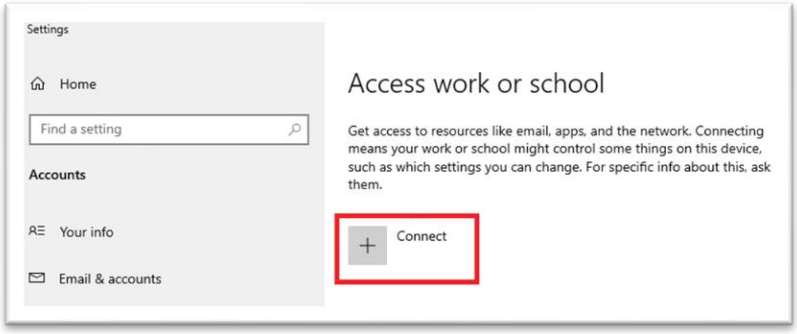
5. Now the PC is joined to the Azure AD.



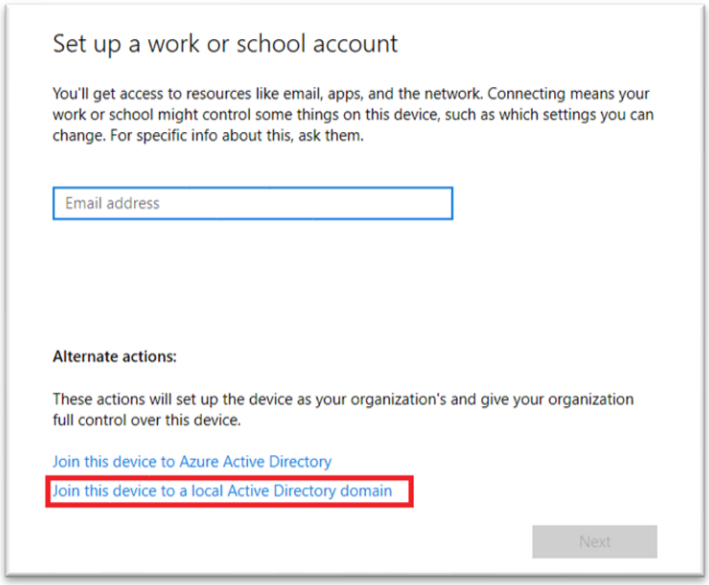
Connect to Azure AD Domain Service

This mode is the same as on-prem Active Directory except that the AD is in the cloud. Therefore, VPN should be setup properly. Once the VPN is configured, Azure AD Domain Service will function the same as local Active Directory.

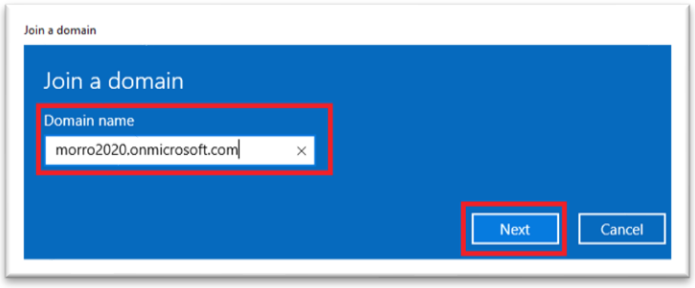
1. Login as a user with local administrator privilege.
2. Navigate to “Access work or school” in Setting menu. Click Connect.



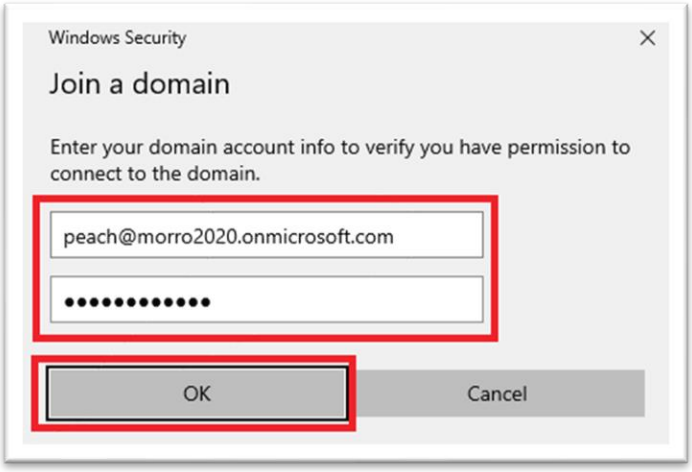
3. Select “Join this device to a local Active Directory Domain”.



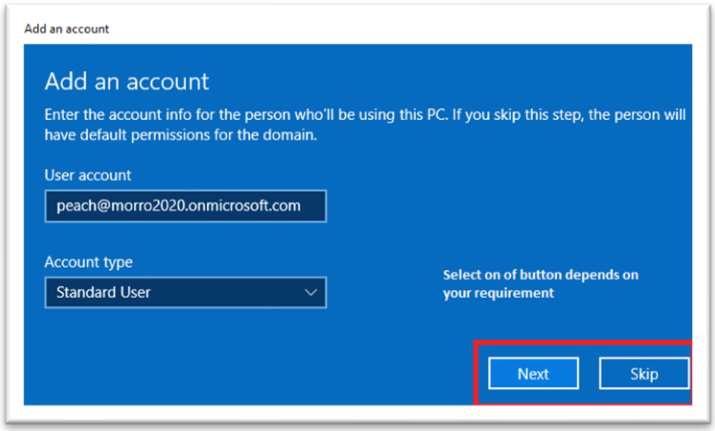
4. Enter the domain name.



5. Enter the user information.



6. Add an account or skip depending on your requirement.



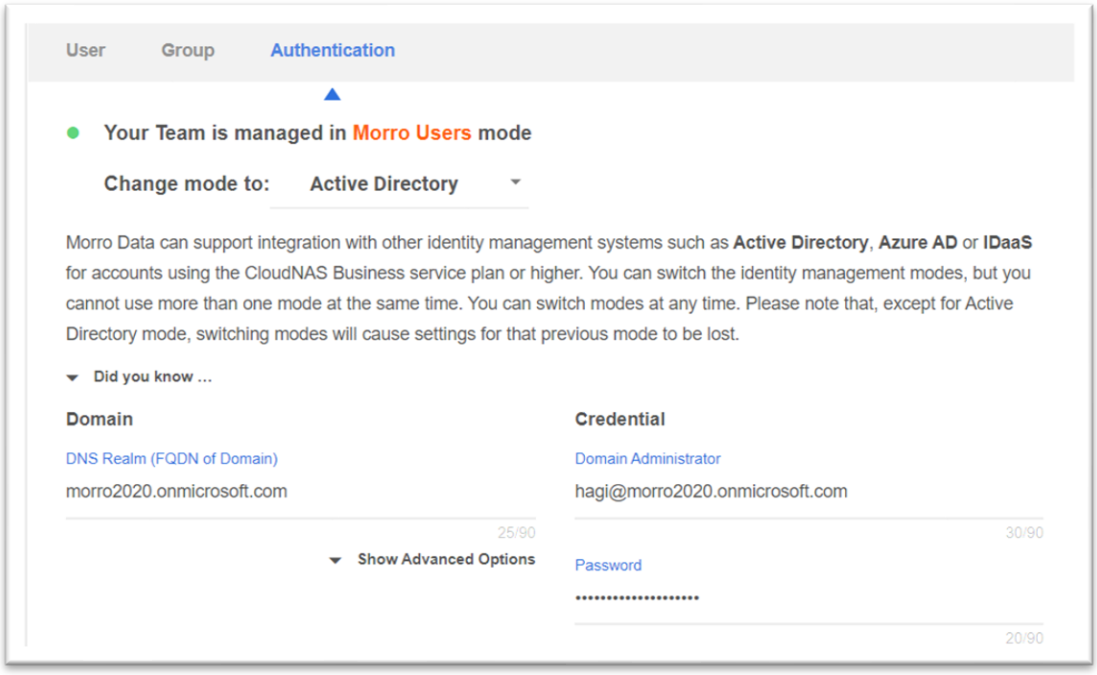
7. You will be prompted to restart the PC to complete the process.

Join a Morro CacheDrive to Azure AD Domain Services

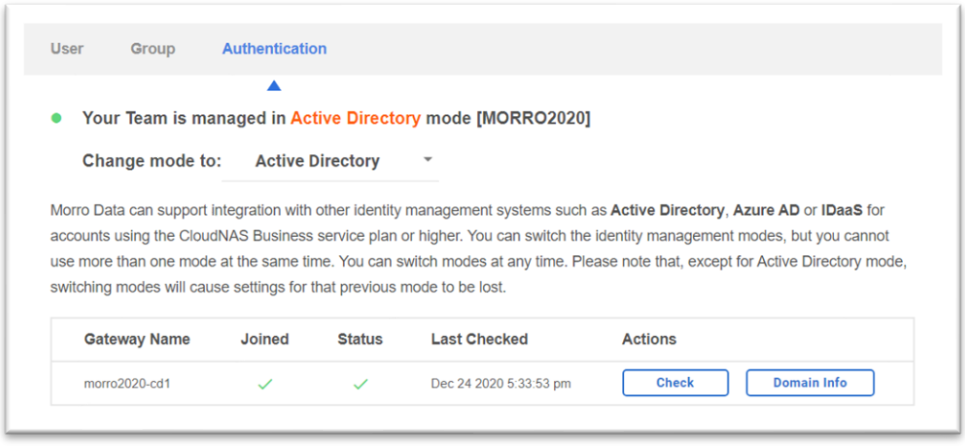
Now that VPN is set up between your Azure AD DS and your premises, you can test the connection with "ping yourdomain". Once the connection is confirmed, we are ready to join the CacheDrive to Azure AD DS.

In the Morro Cloud Manger (MCM), go to the Teams page where user authentication is configured. Choose the Authentication tab and change the mode to "Active Directory". Note that Azure AD DS works the same way as on-prem AD for authentication.

Enter the domain FQDN and the credentials of the user who has Administrative privilege and click "Switch to this mode".



Below shows the successful join of the CacheDrive to the domain.



Single Sign On

In the previous sections, we have successfully joined both the CacheDrive and the Windows PC to the domain. Once you have logged in to the Windows PC using a password, you will be able to access CacheDrive shares without further authentication.

As of now (December 2020), Microsoft does not support SSO with Windows Hello for Business (PIN or biometric). Login credentials can be saved in Windows to minimize manual logins.

Conclusion

In this Guide, we showed the steps required to consolidate user authentication management with Azure AD Domain Services. With Azure AD DS, what was managed before by on-prem AD Domain Services can now be managed from the cloud.

Moving data from local file servers and NAS devices to Morro Data global file services completes the migration to a cloud-centric solution that preserves the security and SSO convenience of legacy on-prem environments. With N-way real-time file syncing between CacheDrives placed anywhere in the world, LAN-level performance is preserved as well.

Many businesses are taking the following steps to move their IT infrastructure from on-prem to cloud without disruption:

1. Sync AD Domain Services to the cloud-based Azure AD Domain Services. This provides the same user management and authentication as before.
2. Migrate on-prem file servers to Morro Data global file services. This provides users with the same high performance SMB experience and collaboration workflow as before, even from multiple sites.

The Morro Data approach provides the scalability and reliability of the cloud with the familiarity of existing legacy user experience and IT management.