

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.

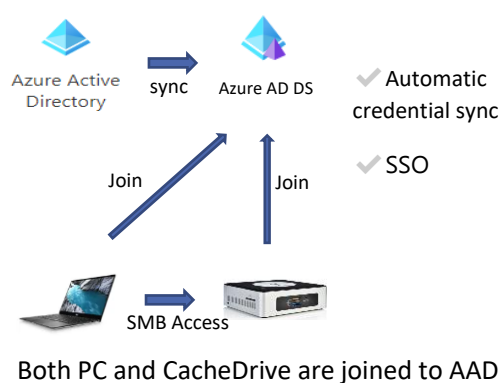
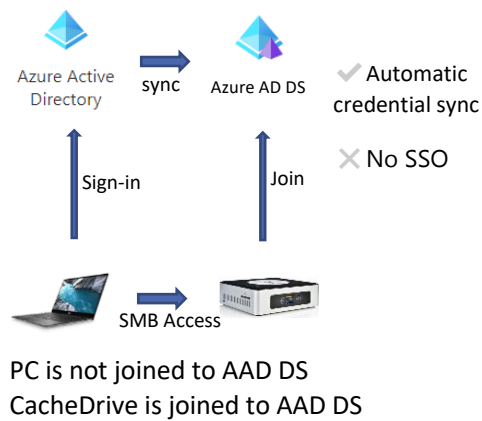
The following table shows the differences between Azure AD, on-prem AD, and Azure AD DS in the context of CacheDrive share access. In the Azure AD Only method, which is common among organizations that use Microsoft 365 without migrating from an on-prem AD environment, users must login separately when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



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 it is 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:

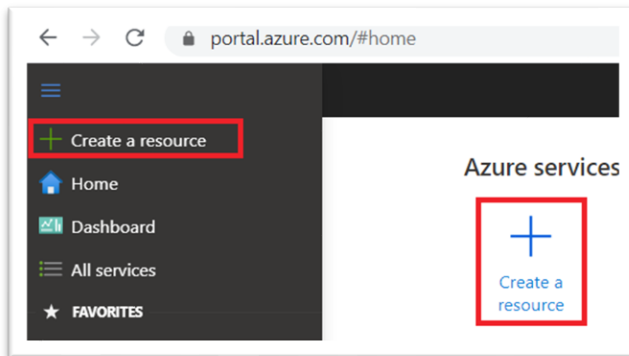
1. Setting up Azure AD Domain Services
2. Setting up a VPN between Azure and Your Premises
3. Join a Windows PC to Azure AD Domain Services
4. Join a Morro CacheDrive to Azure AD Domain Services
5. Single Sign On

Best Practice Guide

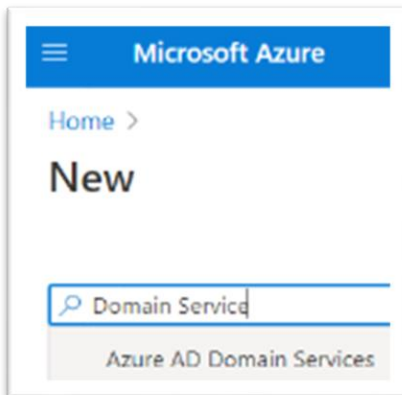
Setting up Azure AD Domain Services

From the Azure Portal:

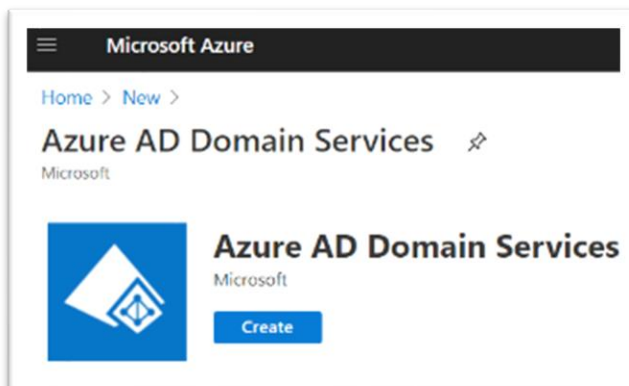
1. Click “Create a resource”.



2. Search for “Domain Service”.



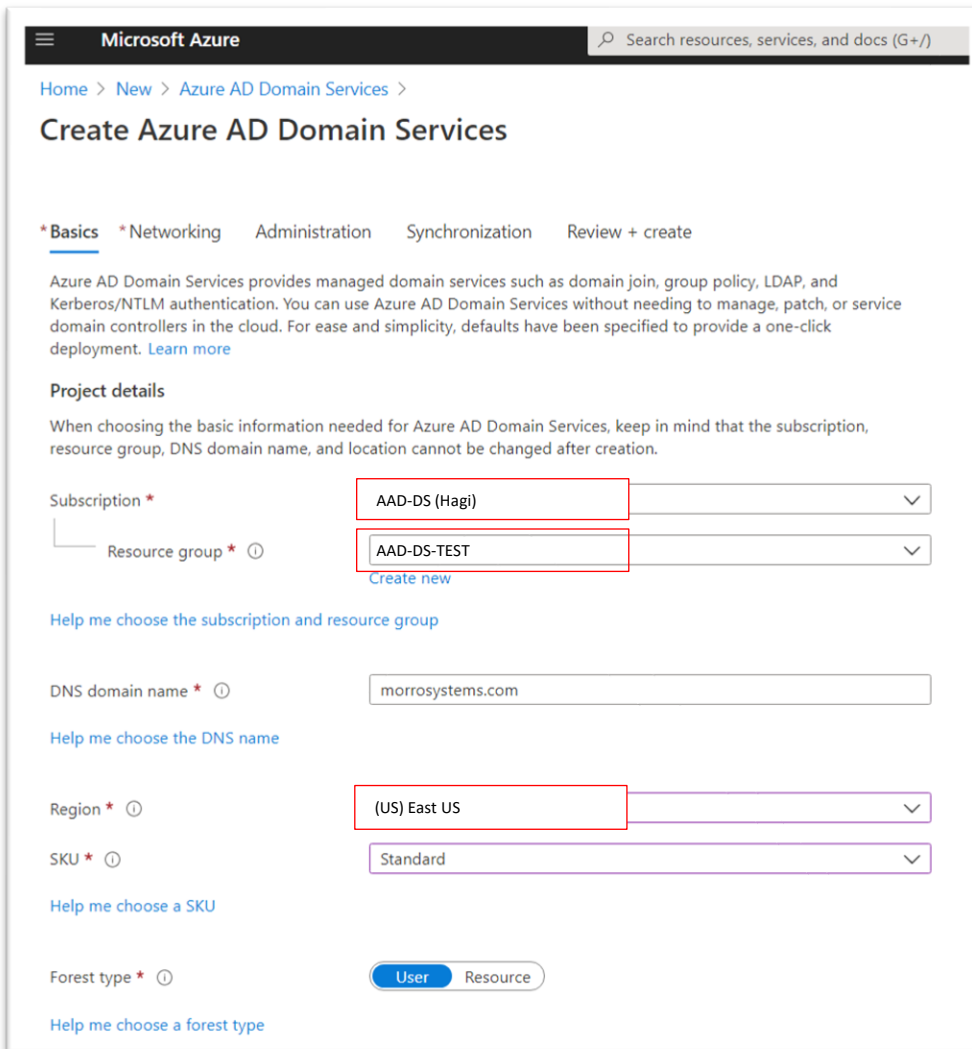
3. Select “Azure AD Domain Services”.



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

Best Practice Guide

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.



Microsoft Azure Search resources, services, and docs (G+)

Home > New > Azure AD Domain Services >

Create Azure AD Domain Services

***Basics** *Networking Administration Synchronization Review + create

Azure AD Domain Services provides managed domain services such as domain join, group policy, LDAP, and Kerberos/NTLM authentication. You can use Azure AD Domain Services without needing to manage, patch, or service domain controllers in the cloud. For ease and simplicity, defaults have been specified to provide a one-click deployment. [Learn more](#)

Project details

When choosing the basic information needed for Azure AD Domain Services, keep in mind that the subscription, resource group, DNS domain name, and location cannot be changed after creation.

Subscription * **AAD-DS (Hagi)**

Resource group * ⓘ **AAD-DS-TEST** [Create new](#)

[Help me choose the subscription and resource group](#)

DNS domain name * ⓘ morrosystems.com

[Help me choose the DNS name](#)

Region * ⓘ **(US) East US**

SKU * ⓘ Standard

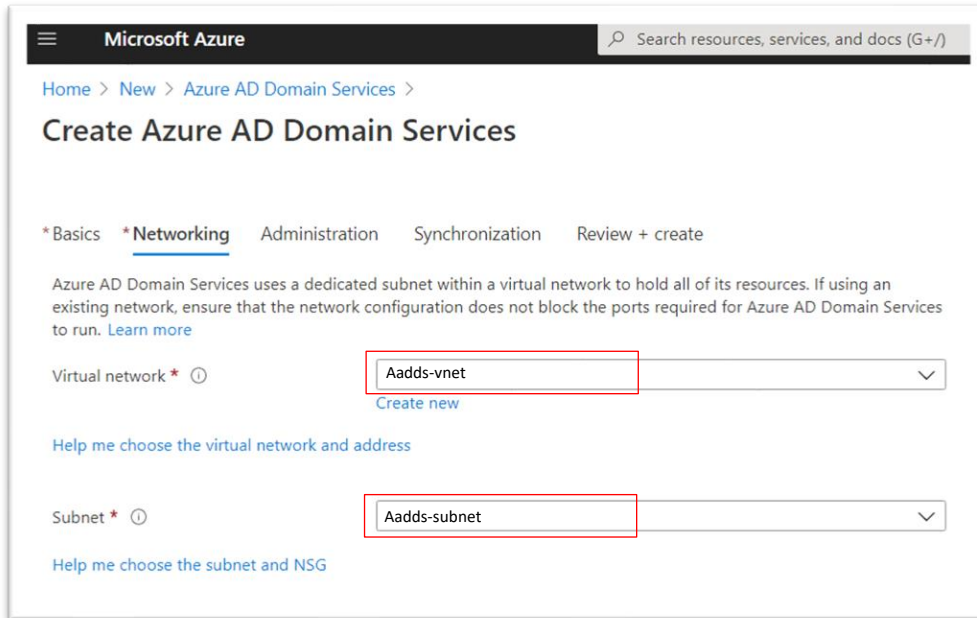
[Help me choose a SKU](#)

Forest type * ⓘ **User** Resource

[Help me choose a forest type](#)

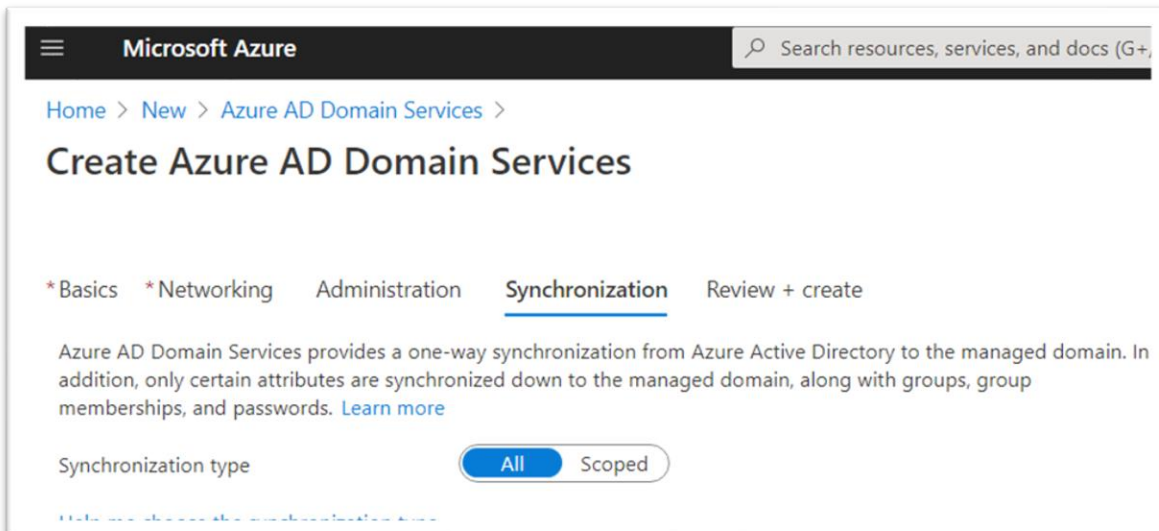
Best Practice Guide

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



The screenshot shows the 'Create Azure AD Domain Services' page in the Microsoft Azure portal. The 'Networking' tab is selected. The page displays two dropdown menus: 'Virtual network' with the value 'Aadds-vnet' and 'Subnet' with the value 'Aadds-subnet'. Both dropdowns are highlighted with red rectangles. Below the 'Virtual network' dropdown is a link 'Create new'. Below the 'Subnet' dropdown is a link 'Help me choose the subnet and NSG'. The page also includes a search bar at the top and a breadcrumb trail: 'Home > New > Azure AD Domain Services >'.

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

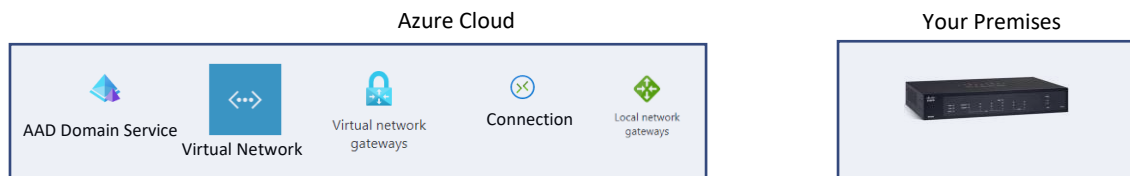


The screenshot shows the 'Create Azure AD Domain Services' page in the Microsoft Azure portal, with the 'Synchronization' tab selected. The page displays a 'Synchronization type' section with two buttons: 'All' (selected) and 'Scoped'. Below this section is a link 'Help me choose the synchronization type'. The page also includes a search bar at the top and a breadcrumb trail: 'Home > New > Azure AD Domain Services >'.

Best Practice Guide

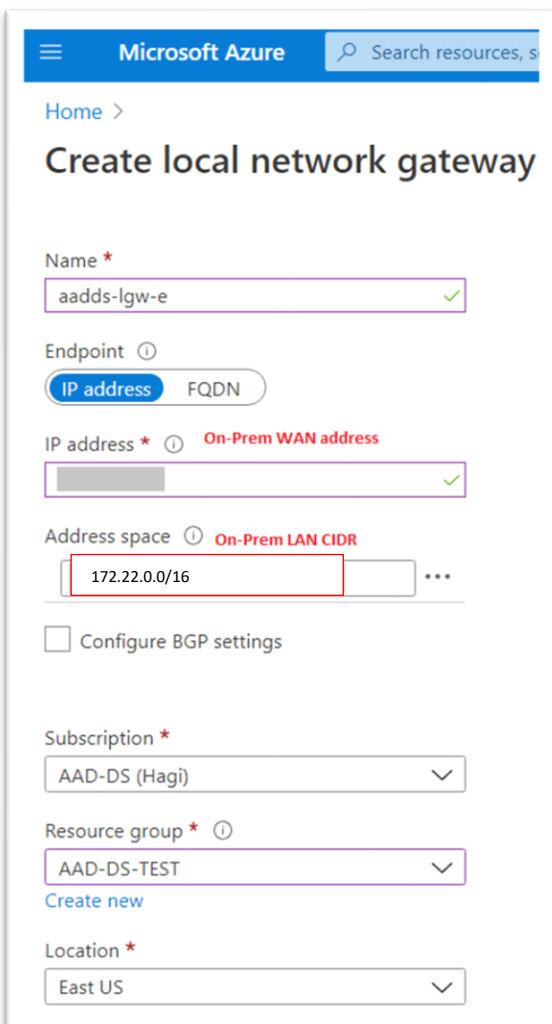
Setting Up a VPN between Azure and Your Premises

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.



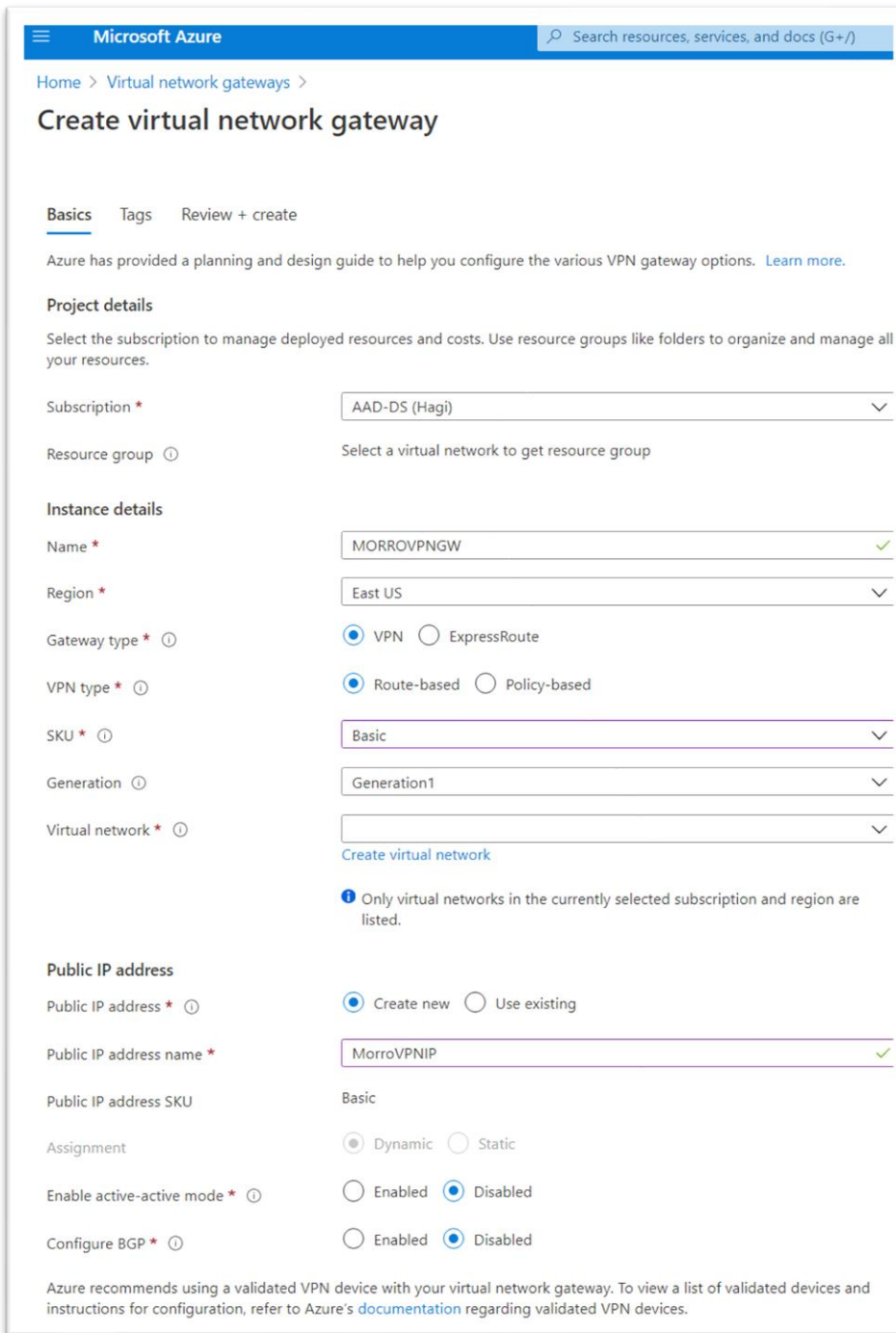
The screenshot shows the 'Create local network gateway' form in the Microsoft Azure portal. The form includes the following fields and options:

- Name ***: aadds-lgw-e (with a green checkmark)
- Endpoint ⓘ**: IP address (selected) and FQDN (available)
- IP address *** ⓘ: On-Prem WAN address (with a green checkmark)
- Address space ⓘ** ⓘ: On-Prem LAN CIDR (with a red box around the input field containing 172.22.0.0/16 and a green checkmark)
- ☐ **Configure BGP settings**
- Subscription ***: AAD-DS (Hagi) (with a dropdown arrow)
- Resource group *** ⓘ: AAD-DS-TEST (with a dropdown arrow and a 'Create new' link below it)
- Location ***: East US (with a dropdown arrow)

Best Practice Guide

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.



Microsoft Azure Search resources, services, and docs (G+/)

Home > Virtual network gateways >

Create virtual network gateway

Basics Tags Review + create

Azure has provided a planning and design guide to help you configure the various VPN gateway options. [Learn more.](#)

Project details

Select the subscription to manage deployed resources and costs. Use resource groups like folders to organize and manage all your resources.

Subscription * AAD-DS (Hagi) ▼

Resource group ⓘ Select a virtual network to get resource group

Instance details

Name * MORROVPNGW ✓

Region * East US ▼

Gateway type * ⓘ ☒ VPN ☐ ExpressRoute

VPN type * ⓘ ☒ Route-based ☐ Policy-based

SKU * ⓘ Basic ▼

Generation ⓘ Generation1 ▼

Virtual network * ⓘ
 [Create virtual network](#)

ⓘ Only virtual networks in the currently selected subscription and region are listed.

Public IP address

Public IP address * ⓘ ☒ Create new ☐ Use existing

Public IP address name * MorroVPNIP ✓

Public IP address SKU Basic

Assignment ☒ Dynamic ☐ Static

Enable active-active mode * ⓘ ☐ Enabled ☒ Disabled

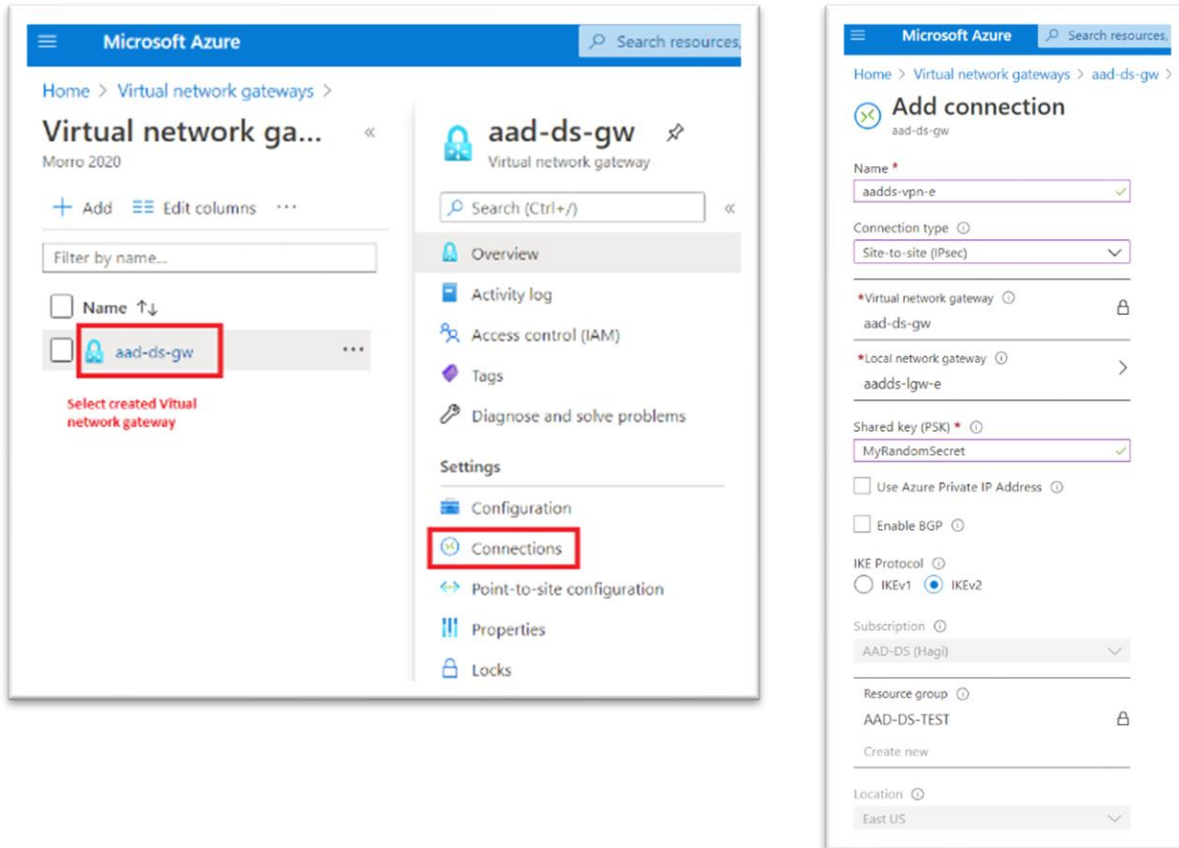
Configure BGP * ⓘ ☐ Enabled ☒ Disabled

Azure recommends using a validated VPN device with your virtual network gateway. To view a list of validated devices and instructions for configuration, refer to Azure's [documentation](#) regarding validated VPN devices.

Best Practice Guide

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).



The left screenshot shows the Microsoft Azure portal interface for managing virtual network gateways. The breadcrumb navigation is 'Home > Virtual network gateways >'. The main heading is 'Virtual network gateways' with a sub-heading 'Morro 2020'. Below this, there are buttons for '+ Add', 'Edit columns', and a filter box. A table lists the gateways, with 'aad-ds-gw' selected and highlighted by a red box. Below the table, a message says 'Select created Virtual network gateway'. On the right, a sidebar shows the 'aad-ds-gw' gateway with various tabs: Overview, Activity log, Access control (IAM), Tags, Diagnose and solve problems, Settings, Configuration, Connections (highlighted with a red box), Point-to-site configuration, Properties, and Locks.

The right screenshot shows the 'Add connection' form for the 'aad-ds-gw' gateway. The form includes the following fields and options:

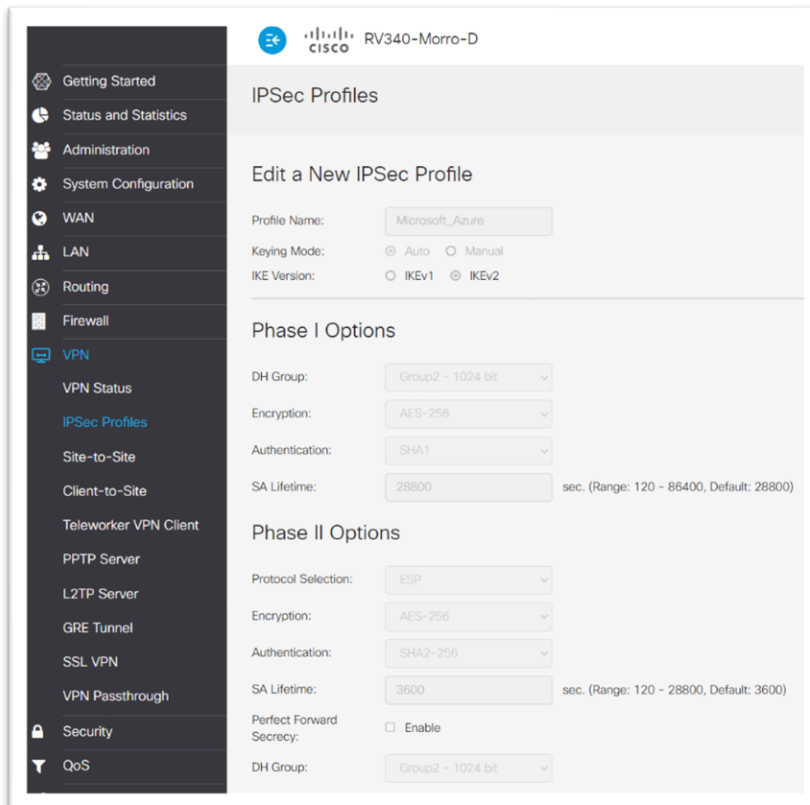
- Name: aadds-vpn-e (with a green checkmark)
- Connection type: Site-to-site (IPsec) (dropdown menu)
- *Virtual network gateway: aad-ds-gw (with a lock icon)
- *Local network gateway: aadds-lgw-e (with a right arrow icon)
- Shared key (PSK): MyRandomSecret (with a green checkmark)
- ☐ Use Azure Private IP Address
- ☐ Enable BGP
- IKE Protocol: IKEv2 (selected, with a blue dot)
- Subscription: AAD-DS (Hagi) (dropdown menu)
- Resource group: AAD-DS-TEST (with a lock icon)
- Create new (button)
- Location: East US (dropdown menu)

Best Practice Guide

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.

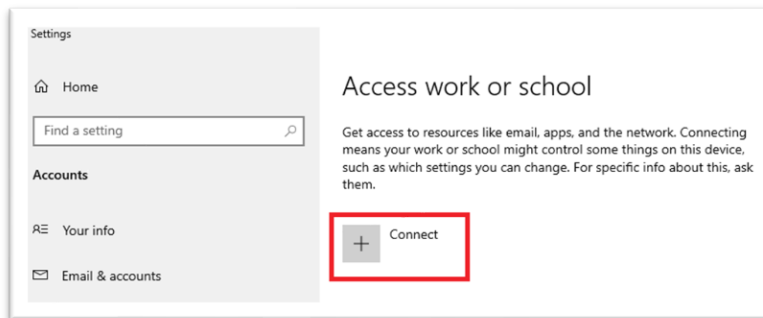
Best Practice Guide

Join a Windows PC to Azure AD Domain Services

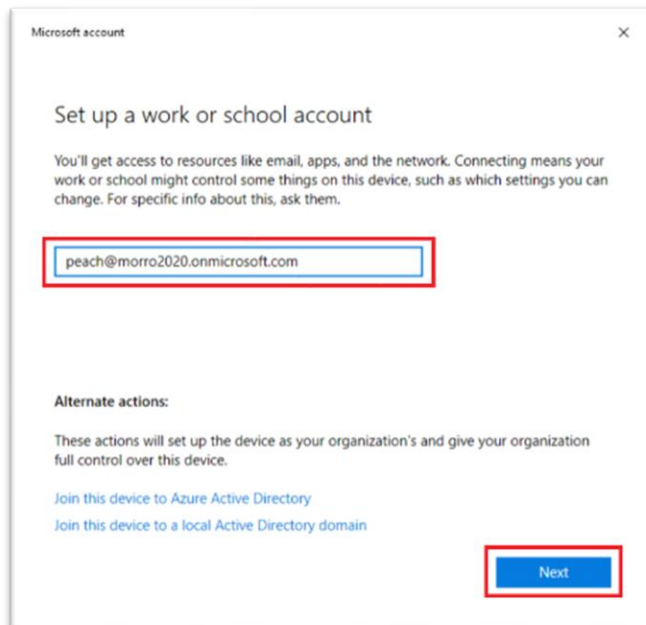
When a Windows 10 Pro PC is set up for the first time, the default is to connect to Azure AD. In our example below, we assume the PC is not connected to any domain. We will login as the local user who has local administrative privileges.

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.



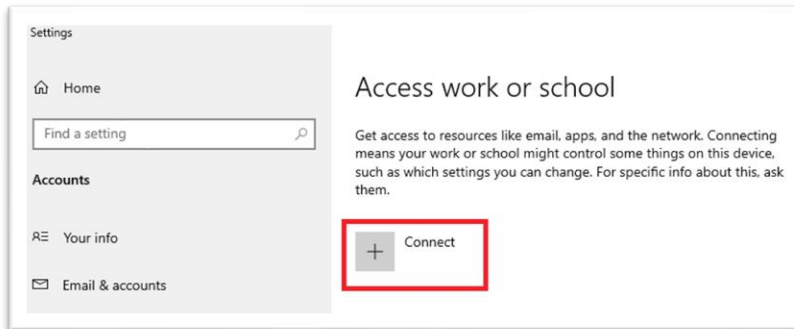
4. The Authentication flow will start. Click Sign in and the PC will be connected to Azure AD when authentication succeeds.

Best Practice Guide

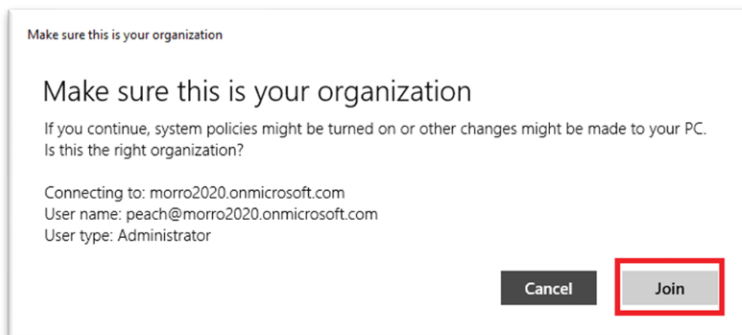
Join the PC to Azure AD

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.

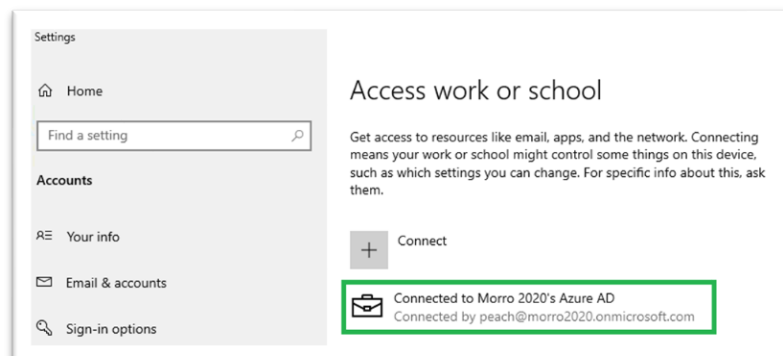
1. Login as a user with Administrator privilege.
2. Navigate to "Access work or school" in Setting menu. Click Connect.



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.

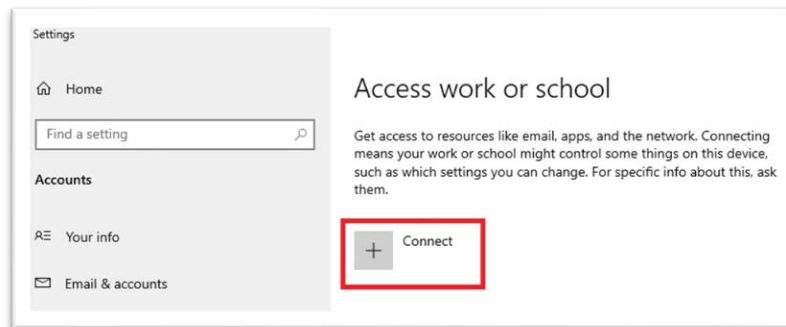


Best Practice Guide

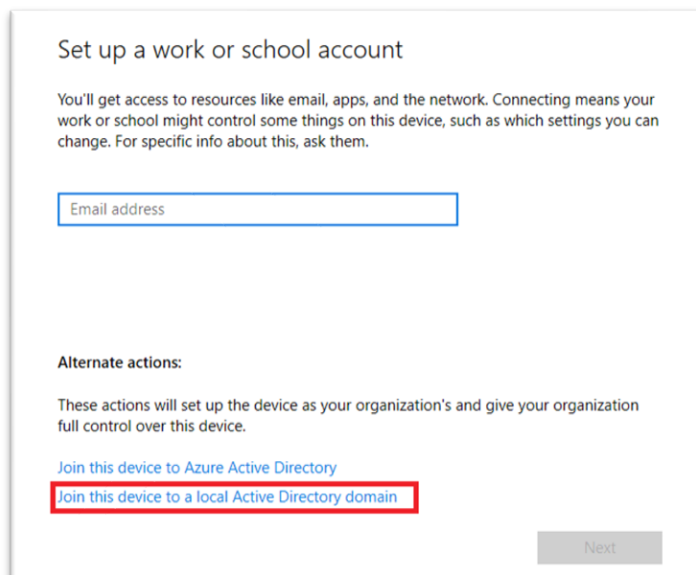
Connect to Azure AD Domain Service

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.

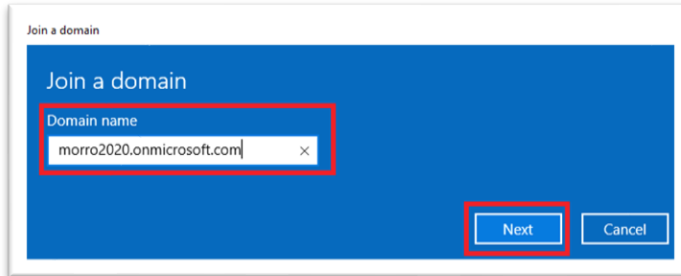


3. Select “Join this device to a local Active Directory Domain”.



Best Practice Guide

4. Enter the domain name.



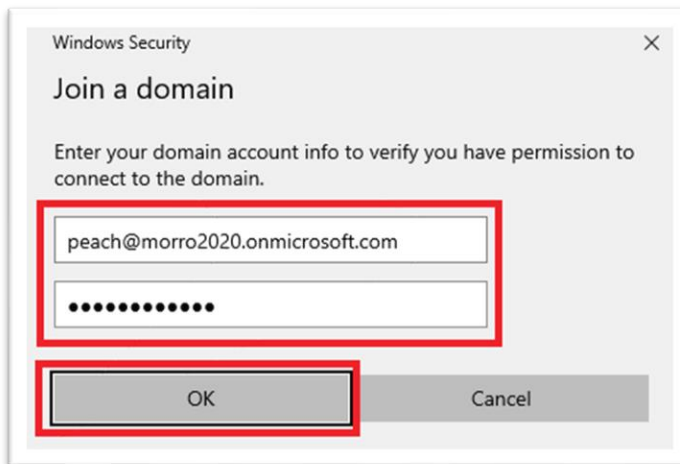
Join a domain

Domain name

morro2020.onmicrosoft.com

Next Cancel

5. Enter the user information.



Windows Security

Join a domain

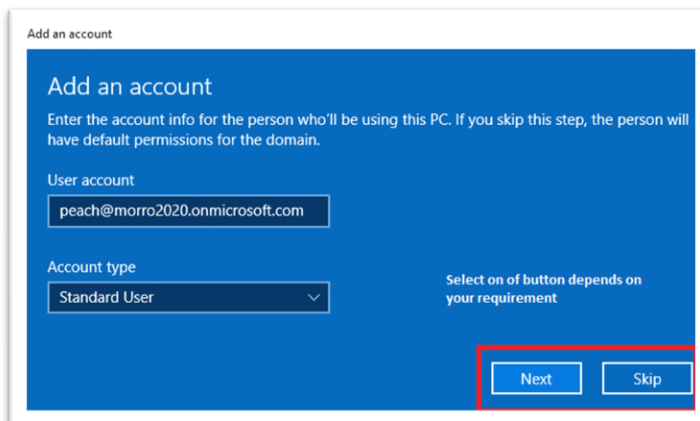
Enter your domain account info to verify you have permission to connect to the domain.

peach@morro2020.onmicrosoft.com

.....

OK Cancel

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



Add an account

Add an account

Enter the account info for the person who'll be using this PC. If you skip this step, the person will have default permissions for the domain.

User account

peach@morro2020.onmicrosoft.com

Account type

Standard User

Select on of button depends on your requirement

Next Skip

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

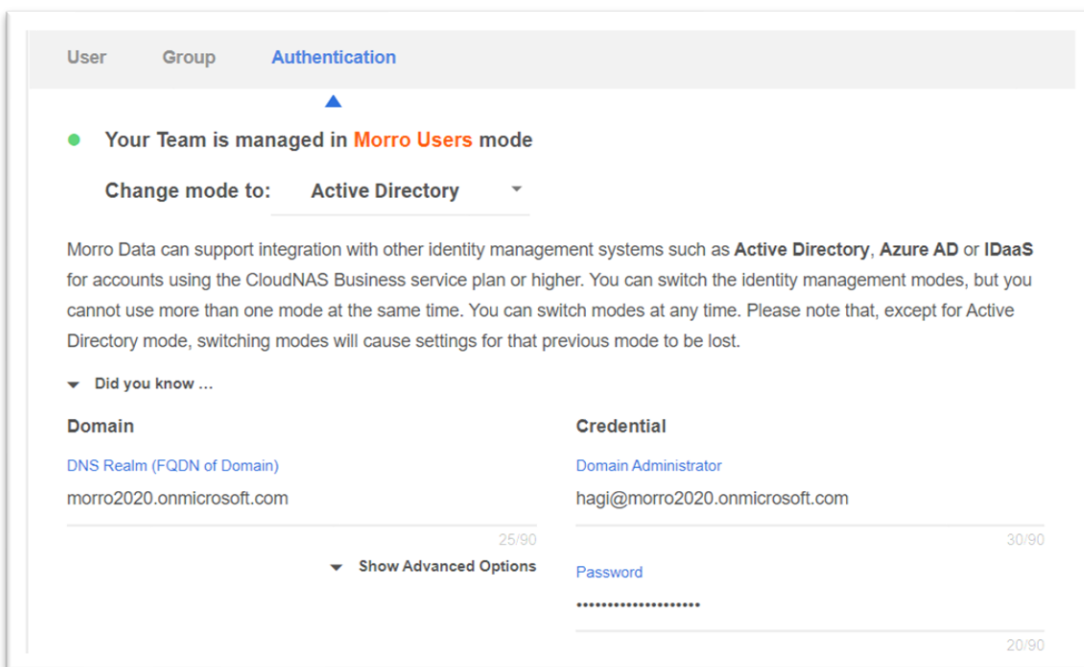
Best Practice Guide

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.

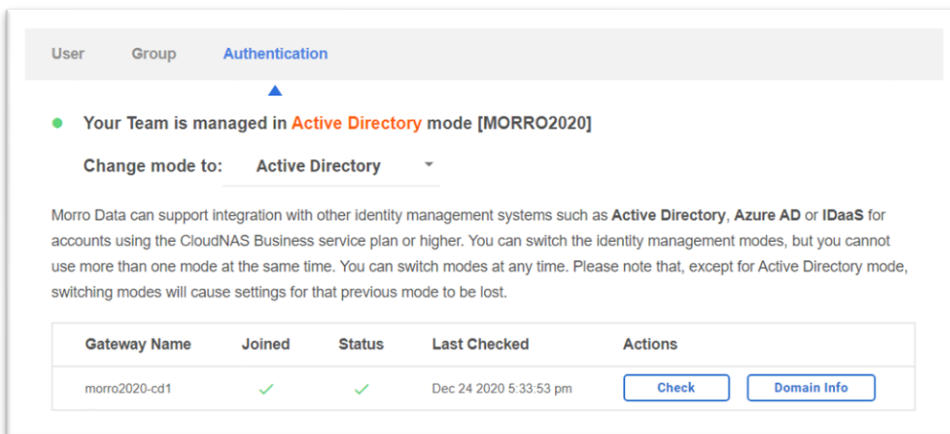
Enter the domain FQDN and the credentials of the user who has Administrative privilege and click “Switch to this mode”.



The screenshot shows the 'Authentication' tab in the Morro Cloud Manager. It indicates that the team is currently managed in 'Morro Users' mode. A dropdown menu allows switching to 'Active Directory' mode. Below this, a text block explains that Morro Data supports integration with Active Directory, Azure AD, or IDaaS, but only one mode can be active at a time. A 'Did you know ...' section provides additional context. The configuration fields are as follows:

Domain	Credential
DNS Realm (FQDN of Domain) morro2020.onmicrosoft.com	Domain Administrator hagi@morro2020.onmicrosoft.com
25/90	30/90
▼ Show Advanced Options	
	Password
	20/90

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



The screenshot shows the 'Authentication' tab after a successful join. The status now indicates 'Your Team is managed in Active Directory mode [MORRO2020]'. The mode dropdown remains set to 'Active Directory'. A table below shows the join status of the CacheDrive:

Gateway Name	Joined	Status	Last Checked	Actions
morro2020-cd1	✓	✓	Dec 24 2020 5:33:53 pm	Check Domain Info

Best Practice Guide

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.