
# Microsoft 365 Administrator

# Exam Ref MS-102

Orin Thomas

Microsoft

# Exam Ref MS-102 Microsoft 365 Administrator

Orin Thomas

This is not a problem when an organization's internal Active Directory domain suffix is a publicly routable domain. For example, a domain name—such as *contoso.com* or *adatum.com*—resolvable by public DNS servers will suffice. Things become more complicated when the organization's internal Active Directory domain suffix is not publicly routable. For example, Figure 2-12 shows the *adatum346ER.internal* nonroutable domain.

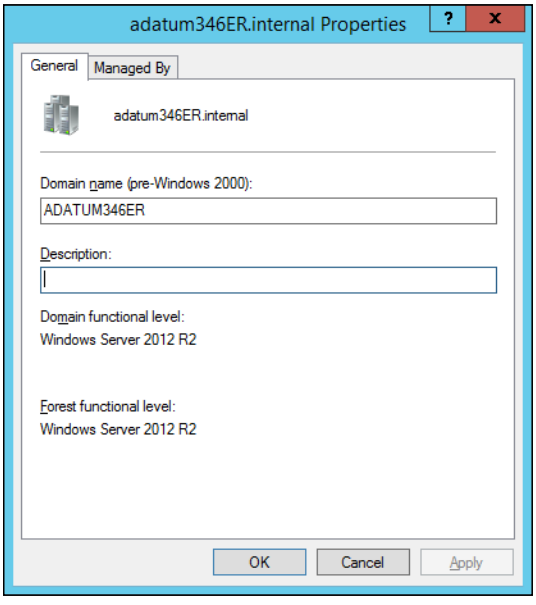


**FIGURE 2-12** Nonroutable domain

If a domain is nonroutable, the default routing domain, such as *adatum346ER.onmicrosoft.com*, should be used for the Microsoft 365 UPN suffix. This requires modifying the UPN suffix of accounts stored in the on-premises Active Directory instance. Modification of UPNs after initial synchronization has occurred is not supported. So, you must ensure that on-premises Active Directory UPNs are properly configured before performing initial synchronization using Microsoft Entra Connect.

Perform the following steps to add a UPN suffix to the on-premises Active Directory if the Active Directory domain uses a nonroutable namespace:

1. Open the **Active Directory Domains And Trust** console and select **Active Directory Domains And Trusts**.
2. On the **Action** menu, select **Properties**.
3. On the **UPN Suffixes** tab, enter the UPN suffix to be used with Microsoft 365. Figure 2-13 shows the UPN suffix of *epistemicus.com*.

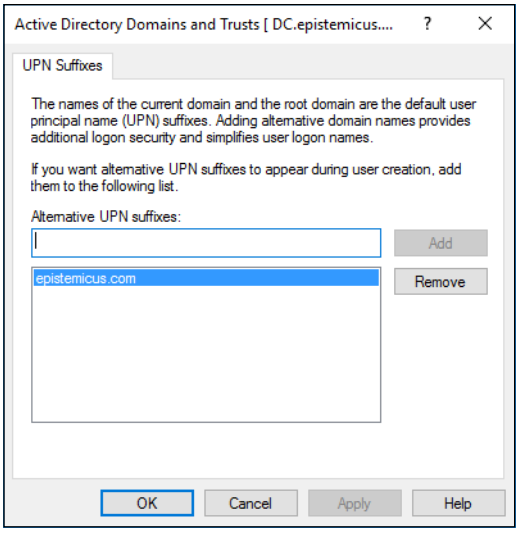


**FIGURE 2-13** Routable domain

Once the UPN suffix has been added in **Active Directory Domains And Trusts**, you assign the UPN suffix to user accounts. You can do this in one of three ways:

- **Manually** As shown in Figure 2-14, this can be done manually using the **Account** tab of the user's **Properties** dialog in **Active Directory Users And Computers**.

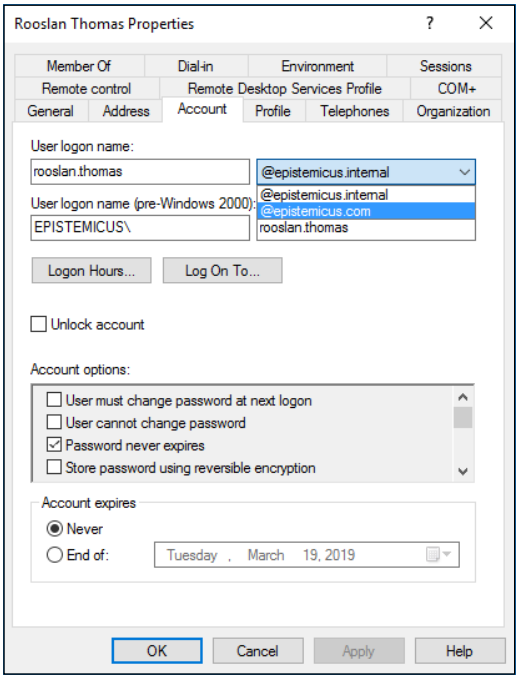


**FIGURE 2-14** Configuring the UPN

- **Using Microsoft PowerShell scripts to reset the UPNs of multiple user accounts** For example, the following script resets the UPN suffixes of all user accounts in the *epistemicus.internal* domain to *epistemicus.onmicrosoft.com*:

```
Get-ADUser -Filter {UserPrincipalName -like "*@epistemicus.internal"} -SearchBase
"DC=epistemicus,DC=internal" |
ForEach-Object {
$UPN =
$_.UserPrincipalName.Replace("epistemicus.internal","epistemicus.onmicrosoft.com")
Set-ADUser $_ -UserPrincipalName $UPN
}
```

# Skill 2.3: Manage identity synchronization by using Microsoft Entra Connect

This skill section deals with managing identity synchronization with Microsoft Entra Connect once deployed. To master this skill, you must understand how to monitor Microsoft Entra Connect Health, manage Microsoft Entra Connect synchronization, configure object filters, and configure password synchronization.

**This section covers the following skills:**

- Configure directory synchronization by using Microsoft Entra Connect
- Monitor Microsoft Entra Connect Health
- Manage Microsoft Entra Connect synchronization
- Configure object filters
- Configure password synchronization
- Implement multiforest AD Connect scenarios

## Microsoft Entra Connect

Microsoft Entra Connect is designed to streamline configuring connections between the on-premises deployment and a Microsoft Entra ID instance. The Microsoft Entra Connect tool is designed to make configuring synchronization between an on-premises Active Directory deployment and Microsoft Entra ID as frictionless as possible.

Microsoft Entra Connect can automatically configure and install simple password synchronization or Federation/single sign-on, depending on your organizational needs. When you choose the Federation with AD FS option, Active Directory Federation Services is installed and configured, as well as a web application proxy server to facilitate communication between the on-premises AD FS deployment and Microsoft Entra ID.

The Microsoft Entra Connect tool supports the following optional features:

- **Exchange Hybrid Deployment** This option is suitable for organizations with an Office 365 deployment in which mailboxes are hosted on-premises and in the cloud.
- **Exchange Mail Public Folders** This feature allows organizations to synchronize mail-enabled public folder objects from an on-premises Active Directory environment to Microsoft 365.
- **Azure AD App And Attribute Filtering** Selecting this option allows you to be more selective about which attributes are synchronized between the on-premises environment and Azure AD.
- **Password Synchronization** This synchronizes a hash of the user's on-premises password with Azure AD. When the user authenticates to Azure AD, the submitted password is hashed using the same process, and if the hashes match, the user is authenticated. Each time the user updates their password on-premises, the updated password hash synchronizes to Azure AD.
- **Password Writeback** Password writeback allows users to change their passwords in the cloud and have the changed password written back to the on-premises Active Directory instance.
- **Group Writeback** With this option, changes made to groups in Azure AD are written back to the on-premises AD instance.
- **Device Writeback** Here, information about devices registered by the user in Azure AD is written back to the on-premises AD instance.
- **Directory Extension Attribute Sync** This option allows you to extend the Azure AD schema based on extensions made to your organization's on-premises Active Directory instance.

***MORE INFO*** **MICROSOFT ENTRA CONNECT**

**You can learn more about Microsoft Entra Connect at *https://learn.microsoft.com/azure/active-directory/hybrid/whatis-azure-ad-connect*.**

## Microsoft Entra Connect user sign-in options

Microsoft Entra Connect supports a variety of user sign-in options related to the method you use to synchronize directory information from Active Directory Domain Services to Azure AD. You configure which sign-in option you will use when setting up Microsoft Entra Connect. The default method, password sync, is appropriate for the majority of organizations that will use Microsoft Entra Connect to synchronize identities to the cloud.

### Password synchronization

Hashes of on-premises Active Directory user passwords synchronize to Microsoft Entra ID, and changed passwords immediately synchronize to Microsoft Entra ID. Actual passwords are never

sent to Microsoft Entra ID and are not stored in Microsoft Entra ID. This allows for single sign-on for users of computers that are joined to an Active Directory domain that synchronizes to Microsoft Entra ID. Password synchronization also allows you to enable password writeback for self-service password reset functionality through Microsoft Entra ID.

## Pass-through authentication

The user's password is validated against an on-premises Active Directory domain controller when authenticating to Microsoft Entra ID. Passwords and password hashes are not present in Microsoft Entra ID. Pass-through authentication allows for on-premises password policies to apply. Pass-through authentication requires Microsoft Entra Connect to have an agent on a computer joined to the domain that hosts the Active Directory instance containing the relevant user accounts. Pass-through authentication also allows single sign-on for users of domain-joined machines.

Pass-through authentication validates the user's password against the on-premises Active Directory controller. The password doesn't need to be present in Microsoft Entra ID in any form. This allows for on-premises policies, such as sign-in hour restrictions, to be evaluated during authentication to cloud services.

Pass-through authentication uses a simple agent on a Windows Server 2012 R2, Windows Server 2016, Windows Server 2019, or Windows Server 2022 domain–joined machine in the on-premises environment. This agent listens for password-validation requests. It doesn't require any inbound ports to be open to the internet.

You can also enable single sign-on for users on domain-joined machines that are on the corporate network. With single sign-on, enabled users only need to enter a user name to help them securely access cloud resources.

## Active Directory Federation

Active Directory Federation allows users to authenticate to Microsoft Entra ID resources using on-premises credentials. It also requires the deployment of an Active Directory Federation Services infrastructure. This is the most complicated identity synchronization configuration for Microsoft 365 and is only likely to be implemented in environments with complicated identity configurations.

***MORE INFO*** **MICROSOFT ENTRA CONNECT SIGN-IN OPTIONS**

**To learn more about sign-in options, consult the following article: *https://learn.microsoft.com/azure/active-directory/hybrid/plan-connect-user-signin*.**

***EXAM TIP***

**Remember the difference between password sync and pass-through authentication.**

## Installing Microsoft Entra Connect

To configure Microsoft Entra Connect synchronization, install the Microsoft Entra Connect software and then run the Microsoft Entra Connect Installation Wizard. The process of installing Microsoft Entra Connect is simply a matter of installing the appropriate MSI file on a Windows Server computer in an environment that meets the necessary prerequisites. After installing the software, you use the Microsoft Entra Connect Setup Wizard to perform the initial configuration. Run the Setup Wizard again if you want to change any Microsoft Entra Connect synchronization settings. You can also use PowerShell or the Synchronization Service Manager to configure synchronization settings, which you'll learn about later in this section.

### Meeting the Microsoft Entra Connect installation requirements

Before installing Microsoft Entra Connect, you should ensure that your environment, Microsoft Entra Connect computer, and account used to configure Microsoft Entra Connect meet the software, hardware, and privilege requirements. So, you need to ensure that your Active Directory environment is configured at the appropriate level, that the computer on which you will run Microsoft Entra Connect has the appropriate software and hardware configuration, and that the account used to install Microsoft Entra Connect has been added to the appropriate security groups.

***MORE INFO*** **MICROSOFT ENTRA CONNECT PREREQUISITES**

**You can learn more about Microsoft Entra Connect prerequisites at *https://learn.microsoft.com/azure/active-directory/hybrid/how-to-connect-install-prerequisites*.**

### Microsoft Entra ID and Microsoft 365 requirements

Before installing and configuring Microsoft Entra Connect, you must ensure that you have configured an additional DNS domain for Microsoft 365. By default, a Microsoft Entra ID tenant will allow 50,000 objects; however, when you add and verify an additional domain, this limit increases to 300,000. You can open a support ticket with Microsoft if you require more than 300,000 objects in your Microsoft Entra ID instance. If you require more than 500,000 objects in your Microsoft Entra ID instance, you must acquire a Microsoft Entra P1 or P2 license or Enterprise Mobility and Security license. Having the DNS domain configured before you set up identity synchronization will allow you to ensure that user UPNs aren't using the default onmicrosoft.com DNS domain.

### On-premises Active Directory environment requirements

Microsoft Entra Connect requires configuring the on-premises Active Directory environment at the Windows Server 2003 forest functional level or higher. The forest functional level depends on the minimum domain functional level of any domain in a forest. For example, if you have five domains in a forest—four of them running at the Windows Server 2012 R2 domain functional level and one running at the Windows Server 2003 domain functional level—Windows Server 2003 will be the maximum forest functional level.