Microsoft

Microsoft 365 Identity and Services

SECOND EDITION

Exam Ref MS-100

Orin Thomas

Microsoft

Exam Ref MS-100 Microsoft 365 Identity and Services

Orin Thomas

Exam Ref MS-100 Microsoft 365 Identity and Services

Published with the authorization of Microsoft Corporation by:
Pearson Education, Inc.

No patent liability is assumed with respect to the use of the information contained herein. Although every precaution has been taken in the preparation of this book, the publisher and author assume no responsibility for errors or omissions. Nor is any liability assumed for damages resulting from the use of the information contained herein.

ISBN-13: 978-0-13-746905-5
ISBN-10: 0-13-746905-5

Library of Congress Control Number: 2021948676

ScoutAutomatedPrintCode

TRADEMARKS

WARNING AND DISCLAIMER

Every effort has been made to make this book as complete and as accurate as possible, but no warranty or fitness is implied. The information provided is on an "as is" basis. The author, the publisher, and Microsoft Corporation shall have neither liability nor responsibility to any person or entity with respect to any loss or damages arising from the information contained in this book or from the use of the programs accompanying it.

SPECIAL SALES

For information about buying this title in bulk quantities, or for special sales opportunities (which may include electronic versions; custom cover designs; and content particular to your business, training goals, marketing focus, or branding interests), please contact our corporate sales department at corpsales@pearsoned.com or (800) 382-3419.

For government sales inquiries, please contact governmentsales@pearsoned.com.

For questions about sales outside the U.S., please contact intlcs@pearson.com.

CREDITS

EDITOR-IN-CHIEF
Brett Bartow

EXECUTIVE EDITOR
Loretta Yates

SPONSORING EDITOR
Charvi Arora

DEVELOPMENT EDITOR
Kate Shoup

MANAGING EDITOR
Sandra Schroeder

SENIOR PROJECT EDITOR
Tracey Croom

COPY EDITOR
Liz Welch

INDEXER
Timothy Wright

PROOFREADER
Abigail Manheim

TECHNICAL EDITOR
Boyd Nolan

EDITORIAL ASSISTANT
Cindy Teeters

COVER DESIGNER
Twist Creative, Seattle

COMPOSITOR
codeMantra

Pearson's Commitment to Diversity, Equity, and Inclusion

Pearson is dedicated to creating bias-free content that reflects the diversity of all learners. We embrace the many dimensions of diversity, including but not limited to race, ethnicity, gender, socioeconomic status, ability, age, sexual orientation, and religious or political beliefs.

Education is a powerful force for equity and change in our world. It has the potential to deliver opportunities that improve lives and enable economic mobility. As we work with authors to create content for every product and service, we acknowledge our responsibility to demonstrate inclusivity and incorporate diverse scholarship so that everyone can achieve their potential through learning. As the world's leading learning company, we have a duty to help drive change and live up to our purpose to help more people create a better life for themselves and to create a better world.

Our ambition is to purposefully contribute to a world where:

- Everyone has an equitable and lifelong opportunity to succeed through learning.
- Our educational products and services are inclusive and represent the rich diversity of learners.
- Our educational content accurately reflects the histories and experiences of the learners we serve.
- Our educational content prompts deeper discussions with learners and motivates them to expand their own learning (and worldview).

While we work hard to present unbiased content, we want to hear from you about any concerns or needs with this Pearson product so that we can investigate and address them.

- Please contact us with concerns about any potential bias at https://www.pearson.com/report-bias.html.

Contents at a glance

Contents

Chapter 4 Plan Office 365 workloads and applications 223

This page intentionally left blank

About the Author

ORIN THOMAS is a Principal Cloud Advocate at Microsoft. He has written more than three dozen books for Microsoft Press on such topics as Windows Server, Windows Client, Azure, Office 365, System Center, Exchange Server, security, and SQL Server. He has authored Azure Architecture courses at Pluralsight and has authored multiple Microsoft Official Curriculum and EdX courses on a variety of IT Pro topics. You can follow him on Twitter at http://twitter.com/orinthomas.

This page intentionally left blank

Introduction

The MS-100 exam deals with advanced topics that require candidates to have an excellent working knowledge of Microsoft 365 identity and services functionality. Some of the exam relates to topics that even experienced Microsoft 365 administrators may rarely encounter unless they are consultants who deploy new Microsoft 365 tenancies on a regular basis. To successfully pass this exam, candidates not only need to understand how to manage Microsoft 365 identity and services, they also need to understand how to integrate Microsoft 365 with an on-premises Active Directory environment. And they must keep up to date with new developments with Microsoft 365, including new features and changes to the interface.

Candidates for this exam are information technology (IT) professionals who want to validate their advanced Microsoft 365 identity and services management skills, configuration skills, and knowledge. To pass this exam, candidates require a strong understanding of how to design and implement Microsoft 365 services, manage user identity and roles, manage access and authentication, and understand the steps involved in planning Office 365 workloads and applications. To pass, candidates require a thorough theoretical understanding as well as meaningful practical experience implementing the technologies involved.

This edition of this book covers Microsoft 365 and the MS-100 exam objectives in mid-2021. As the Microsoft 365 suite evolves, so do the Microsoft 365 exam objectives, so you should check carefully if any changes have occurred since this edition of the book was authored and study accordingly.

This book covers every major topic area found on the exam, but it does not cover every exam question. Only the Microsoft exam team has access to the exam questions, and Microsoft regularly adds new questions to the exam, making it impossible to cover specific questions. You should consider this book a supplement to your relevant real-world experience and other study materials. If you encounter a topic in this book that you do not feel completely comfortable with, use the “Need more review?” links found in the text to locate more information and take the time to research and study the topic. Great information is available on MSDN and TechNet and in blogs and forums.

Organization of this book

This book is organized by the “Skills measured” list published for the exam. The “Skills measured” list is available for this exam on the Microsoft Learn website at *https://aka.ms/ms-100*. Each chapter in this book corresponds to a major topic area in the list, and the technical tasks in each topic area determine a chapter's organization. If an exam covers six major topic areas, for example, the book will contain six chapters.

Microsoft certifications

Microsoft certifications distinguish you by proving your command of a broad set of skills and experience with current Microsoft products and technologies. The exams and corresponding certifications are developed to validate your mastery of critical competencies as you design and develop, or implement and support, solutions with Microsoft products and technologies both on-premises and in the cloud. Certification brings a variety of benefits to the individual and to employers and organizations.

MORE INFO **ALL MICROSOFT CERTIFICATIONS**

For information about Microsoft certifications, including a full list of available certifications, go to *http://www.microsoft.com/learn*.

Check back often to see what is new!

Quick access to online references

Throughout this book are addresses to webpages that the author has recommended you visit for more information. Some of these addresses (also known as URLs) can be painstaking to type into a web browser, so we've compiled all of them into a single list that readers of the print edition can refer to while they read.

Download the list at *MicrosoftPressStore.com/ExamRefMS1002e/downloads*.

The URLs are organized by chapter and heading. Every time you come across a URL in the book, find the hyperlink in the list to go directly to the webpage.

Errata, updates, & book support

We've made every effort to ensure the accuracy of this book and its companion content. You can access updates to this book—in the form of a list of submitted errata and their related corrections—at:

MicrosoftPressStore.com/ExamRefMS1002e/errata

If you discover an error that is not already listed, please submit it to us at the same page.

For additional book support and information, please visit *MicrosoftPressStore.com/Support*.

Please note that product support for Microsoft software and hardware is not offered through the previous addresses. For help with Microsoft software or hardware, go to *http://support.microsoft.com*.

Stay in touch

Let's keep the conversation going! We're on Twitter: *http://twitter.com/MicrosoftPress*.

This page intentionally left blank

CHAPTER 2

Manage user identity and roles

A key aspect of deploying Microsoft 365 is ensuring that user identity is configured properly. When this is done, users can seamlessly access resources in the on-premises environment as well as in the Microsoft 365 environment. If it is not done correctly, users must juggle different accounts, depending on whether the accessible resources are hosted locally or in the cloud.

In this chapter, you will learn about designing an identity strategy, how to plan identity synchronization with Azure AD Connect, how to manage that synchronization, how to manage Azure AD identities, and how to manage Azure AD user roles.

Skills in this chapter:

- Skill 2.1: Design identity strategy
- Skill 2.2: Plan identity synchronization by using Azure AD Connect
- Skill 2.3: Manage identity synchronization by using Azure Active Directory
- Skill 2.4: Manage Azure AD identities
- Skill 2.5: Manage user roles

Skill 2.1: Design identity strategy

This skill deals with designing a strategy related to on-premises and cloud-based identity. To master this skill, you'll need to understand how to determine your organization's requirements when it comes to synchronization, what an appropriate identity-management solution is, and what type of authentication solution is appropriate for your environment.

This section covers the following topics:

- Evaluate requirements and solution for synchronization
- Evaluate requirements and solution for identity management
- Evaluate requirements and solution for authentication

Evaluate requirements and solution for synchronization

Synchronization is the process of replicating on-premises identities, such as users and groups, to the cloud. Synchronization is necessary only when an on-premises identity provider is present. In some synchronization models, every on-premises identity is replicated to the cloud. In other models, only a subset of the on-premises identities is replicated.

Another consideration in evaluating synchronization requirements is determining what information about a user's identity needs to be synchronized to the cloud. Depending on the model chosen, some or all of the properties of those on-premises identities can be replicated. For example, some organizations store sensitive private data about employees within Active Directory. Only replicating what is necessary is especially important given the increasing regulation of data involving personal information.

Should an organization choose, it is possible to perform a complete replication of every aspect of an Active Directory object to the cloud. For example, an organization can deploy a domain controller, SharePoint Farm, System Center, and Exchange Server in Azure infrastructure-as-a-service (IaaS) virtual machines (VMs). You can have those VMs connected via VPN or an ExpressRoute connection to an on-premises Active Directory instance. In this scenario, the Azure IaaS VMs would essentially function as an expensive branch office site running in the Azure cloud.

When evaluating requirements and a solution for synchronization, consider the following questions:

- Which identities need to be replicated to the cloud?
- How often do those identities need to be replicated to the cloud?
- What properties of those identities need to be replicated to the cloud?

Which identities to replicate?

Deployment of Microsoft 365 gives organizations an ability to assess their existing identity needs. If an organization has been using Active Directory for a long time, it's likely that objects don't need to be replicated to the cloud and probably don't need to be in the on-premises Active Directory instance. It's a good idea, before implementing any Microsoft 365 replication scheme, to do a thorough audit of all the objects present within the on-premises directory and to clean out those that are no longer required.

Another issue to address is whether every on-premises identity needs to be present in Azure Active Directory. Many organizations take a phased approach to the introduction of Microsoft 365, migrating small groups of users to the service at a time rather than every user in the organization all at once. Users who are only present in the on-premises directory service won't need to have Microsoft 365 licenses assigned to them.

There are also special account types that are commonly present in an on-premises Active Directory instance that do not need to be, or simply cannot be, replicated to Azure Active Directory. For example, there is no need to replicate service accounts or accounts that are used for specific administrative purposes for on-premises resources, such as the management of an on-premises SQL Server database server or other workload.

Another challenge to consider is that many on-premises environments are more complicated than a single Active Directory domain. Some organizations have multidomain Active Directory forests. In addition, since it is a recommended Microsoft secure administrative practice, an increasing number of large organizations have multiforest deployments—for example, an Enhanced Security Administrative Environment (ESAE) forest to store privileged accounts for the production forest.

User accounts are not the only identity that an organization may want to replicate to the cloud. It may be necessary to replicate some groups to the cloud because these groups may be useful in mediating access to Microsoft 365 workloads. For example, if your organization already has a local security group that is used to collect together members of the accounting team, you may want that group also present as a method of mediating access to resources and workloads within Microsoft 365.

How often to replicate?

When evaluating requirements and a solution for synchronization, you need to answer several important questions. For example, how often do the properties of an on-premises identity change and how soon must those changes be present within Azure Active Directory?

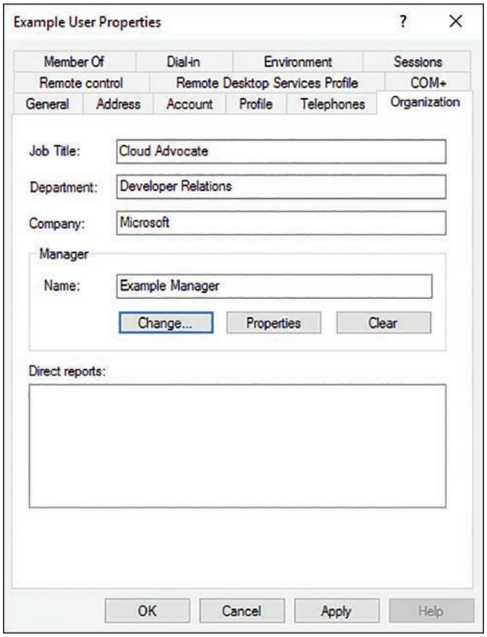
You don't want a user who changes his or her password to have to wait 24 hours before that new password can be used against cloud identities. Similarly, if you deprovision a user account because a person's employment with the organization has terminated, you'll want that action to be reflected in limiting access to Microsoft 365 workloads, rather than the user account having continued access for some time after the user's on-premises identity has been disabled.

Although there can be bandwidth considerations around identity synchronization, the majority of such traffic is going to be the replication of changes, also known as *delta*, rather than constant replications of the entire identity database. The amount of bandwidth consumed by delta identity synchronization traffic is often insignificant compared to the bandwidth consumed by other Microsoft 365 workloads and services.

Which properties to replicate?

Active Directory has been present at some organizations for almost two decades. One of the original selling points of Active Directory was that it could store far more information than just user names and passwords. Because of this, many organizations use Active Directory to store a substantive amount of information about personnel, including telephone numbers, the user's position within the organization, and the branch office where the user works.

When considering a synchronization solution, determine which on-premises Active Directory attribute information needs to be replicated to Azure Active Directory. For example, you may have an application running in Azure that needs access to the Job Title, Department, Company, and Manager attributes, as shown in Figure 2-1.



Job Title: Cloud Advocate

Department: Developer Relations

Company: Microsoft

Manager

Name: Example Manager

Direct reports:

FIGURE 2-1 Which attributes to replicate

Evaluate requirements and solutions for identity management

Evaluating the requirements and solutions for identity management first involves determining what your organization's source of authority is. The source of authority is the directory service that functions as the primary location for the creation and management of user and group accounts. You can choose between having an on-premises Active Directory instance function as a source of authority, or you can have Azure Active Directory function as the source of authority.

Even though Azure Active Directory is present in a hybrid deployment, the source of authority will be the on-premises Azure AD instance. Hybrid deployment accounts are used for authentication and authorization purposes with existing on-premises resources as well as Microsoft 365 workloads.

Source of authority is a very important concept when it comes to creating users and groups in an environment where Azure AD Connect is configured to synchronize an on-premises Active Directory with the Azure Active Directory instance that supports the Microsoft 365 tenancy. When you create a user or group in the on-premises Active Directory instance, the on-premises Active Directory instance retains authority over that object. Objects created within the on-premises Active Directory instance that are within the filtering scope of objects synchronized via Azure AD Connect will replicate to the Azure Active Directory instance that supports the Microsoft 365 tenancy.

Newly created on-premises user and group objects will only be present within the Azure Active Directory instance that supports the Microsoft 365 tenancy after synchronization has occurred. You can force synchronization to occur using the Azure AD Connect Synchronization Service Manager tool.

Evaluate requirements and solution for authentication

When evaluating authentication requirements, determine whether your organization wants to still rely on the traditional combination of user name and password or move toward more sophisticated and secure authentication techniques, such as multifactor authentication. When making this determination, many organizations will decide that more secure technologies are appropriate for sensitive accounts, such as those used for administrative tasks, and that the traditional method of user name and password will be sufficient for the majority of standard users.

Microsoft and Office 365 support a technology known as *modern authentication*. Modern authentication provides a more secure authentication and authorization method than traditional authentication methods. Modern authentication can be used with Microsoft 365 hybrid deployments that include Exchange Online and Teams. All Office and Microsoft 365 tenancies created after August 2017 that include Exchange Online have modern authentication enabled by default. Modern authentication includes a combination of the following authentication and authorization methods, as well as secure access policies:

- **Authentication methods** Multifactor authentication, Client Certificate Authentication, and Active Directory Authentication Library (ADAL)
- **Authorization methods** Microsoft's implementation of Open Authorization (OAuth)
- **Conditional access policies** Mobile application management (MAM) and Azure Active Directory Conditional Access

MORE INFO **HYBRID MODERN AUTHENTICATION**

You can learn more about hybrid modern authentication at the following address: https://docs.microsoft.com/en-us/microsoft-365/enterprise/hybrid-modern-auth-overview.

EXAM TIP

Remember the Azure AD Connect prerequisites.

Skill 2.2: Plan identity synchronization by using Azure AD Connect

This skill section deals with planning the implementation of identity synchronization using Azure AD Connect as the synchronization solution. To master this skill, you'll need to draw on some of the information you learned about in the previous skill as well as how to implement an appropriate Azure AD Connect sign-on option.

This section covers the following topics:

- Design directory synchronization
- Implement directory synchronization with directory services, Federation services, and Azure endpoints by using Azure AD Connect

Design directory synchronization

Azure AD Connect is designed to streamline the process of configuring connections between on-premises deployment and an Azure AD instance. The Azure Active Directory Connect tool is designed to make the process of configuring synchronization between an on-premises Active Directory deployment and Azure Active Directory as frictionless as possible.

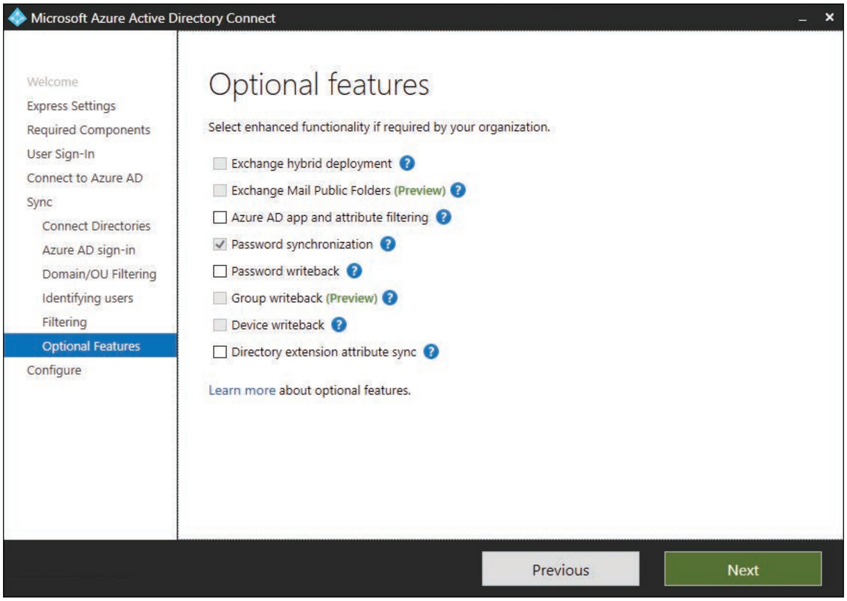
Azure Active Directory Connect can automatically configure and install simple password synchronization or Federation/single sign-on, depending on your organizational needs. When you choose the Federation with AD FS option, Active Directory Federation Services is installed and configured, as well as a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

The Azure Active Directory Connect tool supports the following optional features, as shown in Figure 2-2:

- **Exchange hybrid deployment** This option is suitable for organizations that have an Office 365 deployment in which there are mailboxes hosted both 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 gives you the ability 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.



Optional features

Select enhanced functionality if required by your organization.

☐ Exchange hybrid deployment ?
☐ Exchange Mail Public Folders (Preview) ?
☐ Azure AD app and attribute filtering ?
☑ Password synchronization ?
☐ Password writeback ?
☐ Group writeback (Preview) ?
☐ Device writeback ?
☐ Directory extension attribute sync ?

Learn more about optional features.

FIGURE 2-2 Azure Active Directory Connect optional features

MORE INFO **AZURE ACTIVE DIRECTORY CONNECT**

You can learn more about Azure Active Directory Connect at https://docs.microsoft.com/en-us/azure/active-directory/hybrid/whatis-hybrid-identity.

Clean up existing Active Directory objects

Before you deploy Azure AD Connect, it is prudent to ensure that your on-premises Active Directory environment is healthy. You should also have an excellent understanding of the current state of the Active Directory environment. This should include performing an audit to determine the following:

- Do any Active Directory objects use invalid characters?
- Do any Active Directory objects have incorrect Universal Principal Names (UPNs)?
- What are the current domain and forest functional levels?
- Are any schema extensions or custom attributes in use?

Before deploying Azure AD Connect, you should also ensure that you have performed the following tasks:

- Remove any duplicate `proxyAddress` attributes.
- Remove any duplicate `userPrincipalName` attributes.
- Ensure that blank or invalid `userPrincipalName` attribute settings have been altered so that the setting contains only a valid UPN.
- Ensure that for user accounts the `cn` and `samAccountName` attributes have been assigned values.
- Ensure that for group accounts, the member, alias, and `displayName` (for groups with a valid mail or `proxyAddress` attribute) are populated.
- Ensure that the following attributes do not contain invalid characters:
  - `sn`
  - `samAccountName`
  - `givenName`
  - `displayName`
  - `mail`
  - `proxyAddress`
  - `mailNickName`

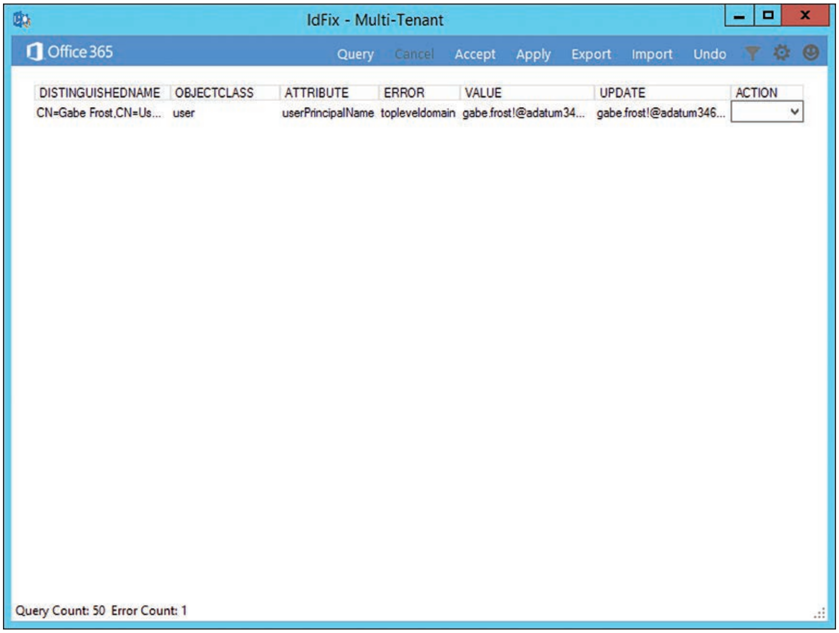
UPNs that are used with Office 365 can only contain the following characters:

- Letters
- Numbers
- Periods
- Dashes
- Underscores

Rather than having to perform this operation manually, Microsoft provides some tools that allow you to automatically remediate problems that might exist with attributes before deploying Azure AD Connect.

IdFix

The IdFix tool, which you can download from Microsoft's website, allows you to scan an Active Directory instance to determine if any user accounts, group accounts, or contacts have problems that will cause them not to synchronize between the on-premises instance of Active Directory and the Microsoft 365 instance of Azure Active Directory. IdFix can also perform repairs on objects that would otherwise be unable to sync. IdFix runs with the security context of the currently signed-on user. This means that if you want to use IdFix to repair objects in the forest that have problems, the security account you use to run IdFix must have permissions to modify those objects. The IdFix tool is shown in Figure 2-3, displaying an account detected with an incorrectly configured `userPrincipalName` attribute.



DISTINGUISHEDNAME	OBJECTCLASS	ATTRIBUTE	ERROR	VALUE	UPDATE	ACTION
CN=Gabe Frost,CN=Us...	user	userPrincipalName	topleveldomain	gabe.frost!@adatum34...	gabe.frost!@adatum346...	

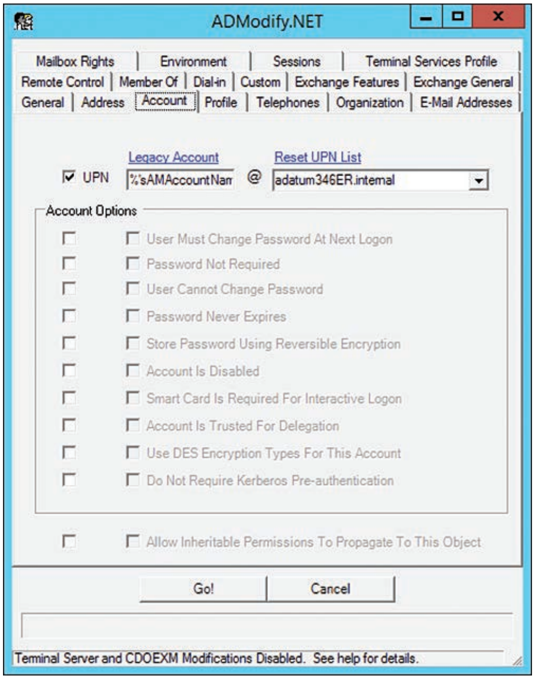
Query Count: 50 Error Count: 1

FIGURE 2-3 IdFix finds a user with a problematic UPN.

> ***MORE INFO*** **IDFIX**
>
> **You can download IdFix at the following address: *https://microsoft.github.io/idfix/*.**

ADModify.NET

ADmodify.NET is a tool that allows you to make changes to specific attributes for multiple objects. If you are using ADSIEdit or the Advanced mode of the Active Directory Users and Computers console, you are able to modify the attribute of only one object at a time. For example, Figure 2-4 shows ADModify.NET used to modify the format of the `userPrincipalName` attribute for a number of user accounts so that it conforms to a specific format.



☑ UPN %'sAMAccountNar @ adatum346ER.internal

Account Options

□ □ User Must Change Password At Next Logon
□ □ Password Not Required
□ □ User Cannot Change Password
□ □ Password Never Expires
□ □ Store Password Using Reversible Encryption
□ □ Account Is Disabled
□ □ Smart Card Is Required For Interactive Logon
□ □ Account Is Trusted For Delegation
□ □ Use DES Encryption Types For This Account
□ □ Do Not Require Kerberos Pre-authentication

□ □ Allow Inheritable Permissions To Propagate To This Object

Terminal Server and CDOEXM Modifications Disabled. See help for details.

FIGURE 2-4 ADModify.NET

You can also use ADModify.NET to perform other system administration tasks, such as configuring a large number of accounts so that users have to change their password at next logon or to disable multiple accounts.

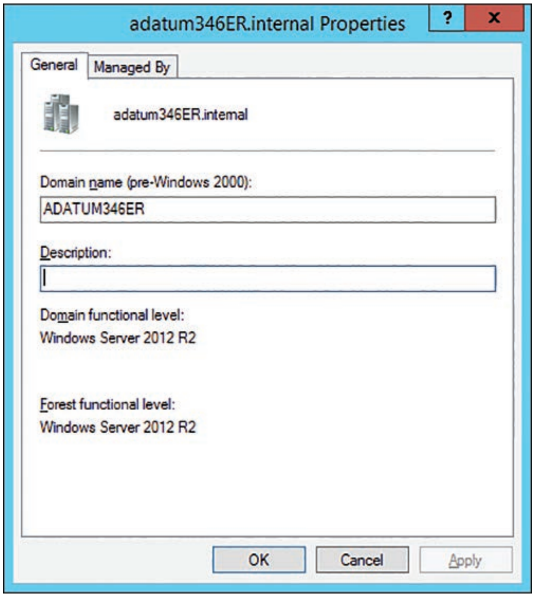
MORE INFO **ADMODIFY.NET**

You can learn more about ADModify.NET at *https://archive.codeplex.com/?p=admodify*. At present ADModify.NET is located on CodePlex. At some point in the future, perhaps by the time you are reading this, it will be hosted on Github.

Use UPN suffixes and nonroutable domains

Before performing synchronization between an on-premises Active Directory environment and an Azure Active Directory instance used to support a Microsoft 365 tenancy, you must ensure that all user account objects in the on-premises Active Directory environment are configured with a value for the UPN suffix that can function for both the on-premises environment and Microsoft 365.

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 that is 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 2-5 shows the adatum346ER.internal nonroutable domain.



adatum346ER.internal Properties

adatum346ER.internal

Domain name (pre-Windows 2000):
ADATUM346ER

Description:

Domain functional level:
Windows Server 2012 R2

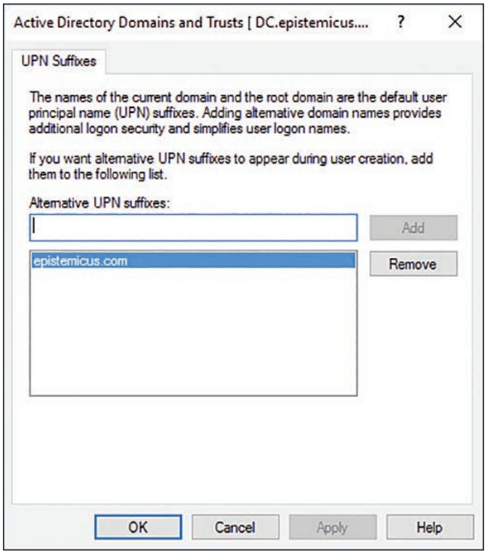
Forest functional level:
Windows Server 2012 R2

FIGURE 2-5 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 the UPN after initial synchronization has occurred is not supported. So, you need to ensure that on-premises Active Directory UPNs are properly configured before performing initial synchronization using Azure AD Connect.

Perform the following steps to add a UPN suffix to the on-premises Active Directory in the event that 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 2-6 shows the UPN suffix of epistemicus.com.



The names of the current domain and the root domain are the default user principal name (UPN) suffixes. Adding alternative domain names provides additional logon security and simplifies user logon names.

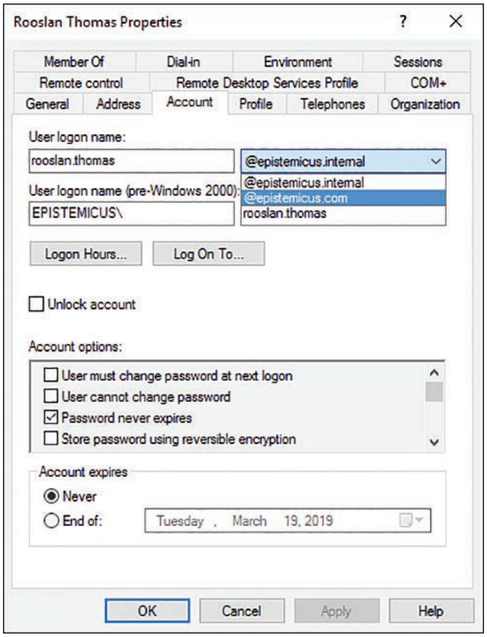
If you want alternative UPN suffixes to appear during user creation, add them to the following list.

Alternative UPN suffixes:

epistemicus.com

FIGURE 2-6 Routable domain

4. 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 2-7, by using the **Account** tab of the user's **Properties** dialog box in **Active Directory Users and Computers**.



User logon name: rooslan.thomas @epistemicus.internal

@epistemicus.internal
@epistemicus.com

User logon name (pre-Windows 2000): EPISTEMICUS\ rooslan.thomas

□ Unlock account

Account options:

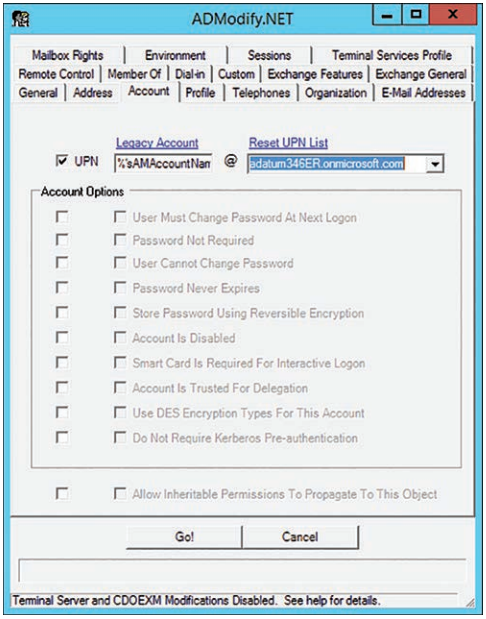
□ User must change password at next logon
□ User cannot change password
☑ Password never expires
□ Store password using reversible encryption

Account expires

● Never
○ End of: Tuesday , March 19, 2019

FIGURE 2-7 Configuring the UPN

- Using tools like ADModify.NET to reset the UPNs of multiple accounts, as shown in Figure 2-8.



☑ UPN %'sAMAccountNan @ adatum346ER.onmicrosoft.com

Account Options

☐ ☐ User Must Change Password At Next Logon
☐ ☐ Password Not Required
☐ ☐ User Cannot Change Password
☐ ☐ Password Never Expires
☐ ☐ Store Password Using Reversible Encryption
☐ ☐ Account Is Disabled
☐ ☐ Smart Card Is Required For Interactive Logon
☐ ☐ Account Is Trusted For Delegation
☐ ☐ Use DES Encryption Types For This Account
☐ ☐ Do Not Require Kerberos Pre-authentication

☐ ☐ Allow Inheritable Permissions To Propagate To This Object

Terminal Server and CDOEXM Modifications Disabled. See help for details.

FIGURE 2-8 ADModify.NET

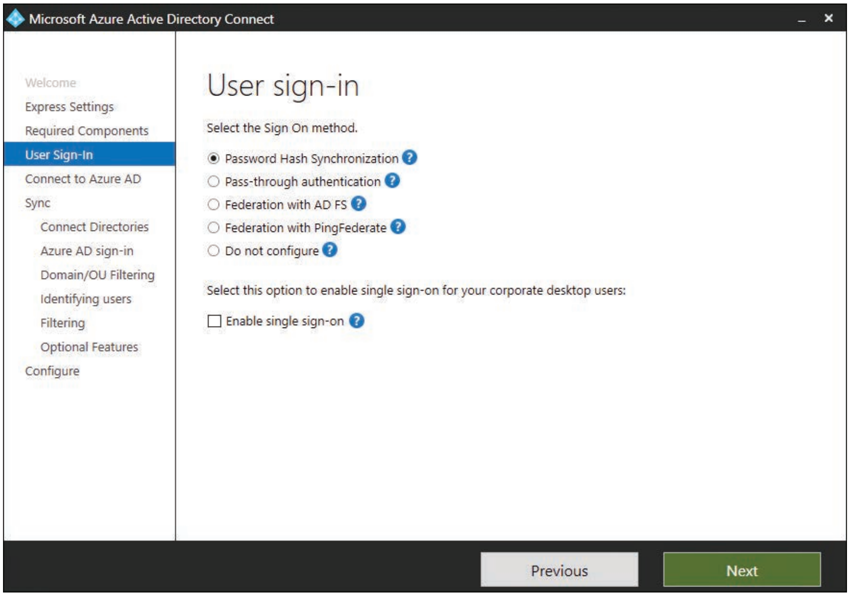
- Using Microsoft PowerShell scripts to reset the UPNs of multiple user accounts. For example, the following script resets UPN suffixes of all user accounts in the epistemicus.internal domain to epistemicus.onmicrosoft.com:

```
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

}
```

Implement directory synchronization with directory services, Federation services, and Azure endpoints by using Azure AD Connect

Azure AD Connect supports a variety of user sign-in options, which are 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 Azure AD Connect, as shown in

Figure 2-9. The default method, password sync, is appropriate for the majority of organizations that will use Azure AD Connect to synchronize identities to the cloud.



Microsoft Azure Active Directory Connect

User sign-in

Select the Sign On method.

● Password Hash Synchronization
○ Pass-through authentication
○ Federation with AD FS
○ Federation with PingFederate
○ Do not configure

Select this option to enable single sign-on for your corporate desktop users:

□ Enable single sign-on

FIGURE 2-9 User sign-in

Password synchronization

Hashes of on-premises Active Directory user passwords synchronize to Azure AD, and changed passwords immediately synchronize to Azure AD. Actual passwords are never sent to Azure AD and are not stored in Azure AD. This allows for single sign-on for users of computers that are joined to an Active Directory domain that synchronizes to Azure AD. Password synchronization also allows you to enable password writeback for self-service password reset functionality through Azure AD.

Pass-through authentication

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

With pass-through authentication, the user's password is validated against the on-premises Active Directory controller. The password doesn't need to be present in Azure AD 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 Azure AD 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*** **AZURE AD CONNECT SIGN-IN OPTIONS**
>
> **To learn more about sign-in options, consult the following article: *https://docs.microsoft.com/en-us/azure/active-directory/connect/active-directory-aadconnect-user-signin*.**

Azure Endpoints

The Azure AD Connect endpoint V2 API provides performance improvements over the original endpoint API. The V2 API supports syncing groups with more than 250,000 members. If you want to use the V2 API endpoint, Azure AD Connect must be upgraded to or installed as version 1.5.30.0 or later.

If your organization has deployed an earlier version of Azure AD Connect, the V1 API might still be in use. To switch to the V2 API, perform the following steps:

1. On the server on which Azure AD Connect is installed, open the **PowerShell prompt** as an administrator.
2. Disable the sync scheduler by running the following PowerShell command:
   ```
   Set-ADSyncScheduler -SyncCycleEnabled $false
   ```
3. Import the new PowerShell module that will be made available with the installation of the updated version of Azure AD Connect using the following command:
   ```
   Import-Module 'C:\Program Files\Microsoft Azure AD Sync\Extensions\
   AADConnector.psm1'
   ```
4. Switch to using the V2 endpoint by running the following commands:
   ```
   Set-ADSyncAADConnectorExportApiVersion 2
   Set-ADSyncAADConnectorImportApiVersion 2
   ```
5. Reenable the sync scheduler by running the following command:
   ```
   Set-ADSyncScheduler -SyncCycleEnabled $true
   ```

Index