



Microsoft 365 Identity and Services

SECOND EDITION

Exam Ref MS-100

Orin Thomas

FREE SAMPLE CHAPTER

SHARE WITH OTHERS



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.

Copyright © 2022 by Pearson Education, Inc.

All rights reserved. This publication is protected by copyright, and permission must be obtained from the publisher prior to any prohibited reproduction, storage in a retrieval system, or transmission in any form or by any means, electronic, mechanical, photocopying, recording, or likewise. For information regarding permissions, request forms, and the appropriate contacts within the Pearson Education Global Rights & Permissions Department, please visit www.pearson.com/permissions.

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

Microsoft and the trademarks listed at <http://www.microsoft.com> on the "Trademarks" webpage are trademarks of the Microsoft group of companies. All other marks are property of their respective owners.

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

	<i>Introduction</i>	<i>xiii</i>
CHAPTER 1	Design and implement Microsoft 365 services	1
CHAPTER 2	Manage user identity and roles	93
CHAPTER 3	Manage access and authentication	159
CHAPTER 4	Plan Office 365 workloads and applications	223
	<i>Index</i>	<i>331</i>

Contents

Introduction	xiii
<i>Organization of this book</i>	<i>xiii</i>
<i>Microsoft certifications</i>	<i>xiv</i>
<i>Quick access to online references</i>	<i>xiv</i>
<i>Errata, updates, & book support</i>	<i>xiv</i>
<i>Stay in touch</i>	<i>xv</i>
Chapter 1 Design and implement Microsoft 365 services	1
Skill 1.1: Plan architecture.....	1
Plan integration of Microsoft 365 and on-premises environments	2
Identify deployment workloads team	10
Plan an identity and authentication solution	11
Plan enterprise application modernization	14
Skill 1.2: Deploy a Microsoft 365 tenant	15
Manage domains	15
Configure organizational settings	32
Complete the organization profile	35
Add a Microsoft partner or work with Microsoft FastTrack	36
Complete the subscription setup wizard	38
Plan and create a tenant	40
Edit an organizational profile	42
Plan and create subscriptions	43
Configure tenant wide workload settings	43
Skill 1.3: Manage Microsoft 365 subscription and tenant health.	53
Manage service health alerts	53
Create an internal service health response plan	55
Monitor service health	56
Monitor license allocations	57
Configure and review reports	57

Thought experiment.....	219
Thought experiment answers	220
Chapter summary	221

Chapter 4 Plan Office 365 workloads and applications 223

Skill 4.1: Plan for Microsoft 365 Apps deployment	223
Plan for Microsoft connectivity	224
Manage Microsoft 365 Apps	225
Plan for Office online	227
Assess readiness using Microsoft analytics	228
Plan Microsoft 365 App compatibility	229
Manage Office 365 software downloads	229
Plan for Microsoft apps updates	241
Plan Microsoft telemetry and reporting	242
Skill 4.2: Plan for messaging deployments.....	261
Plan migration strategy	262
Plan messaging deployment	268
Identify hybrid requirements	269
Plan for connectivity	271
Plan for mail routing	271
Plan email domains	272
Skill 4.3: Plan for Microsoft SharePoint Online and OneDrive for Business	274
Plan migration strategy	274
Plan external share settings	275
Identify hybrid requirements	284
Manage access configurations	285
Manage Microsoft groups	287
Manage SharePoint tenant and site settings	291
Manage OneDrive for Business	292
Skill 4.4: Plan for Microsoft Teams Infrastructure	296
Plan for communication and call quality and capacity	296
Plan for Phone System	297
Plan Microsoft Teams deployment	297

Plan Microsoft Teams organizational settings	301
Plan for guest and external access	305
Plan for Microsoft Teams hybrid connectivity and coexistence	306
Teams cmdlets	309
Skill 4.5: Plan Microsoft Power Platform integration	310
Implement Microsoft Power Platform Center of Excellence (CoE) starter kit	311
Plan for Power Platform workload deployments	311
Plan resource deployment	317
Plan for connectivity (and data flow)	320
Manage environments	320
Manage resources	323
Thought experiment	327
Thought experiment answers	328
Chapter summary	328
 <i>Index</i>	 331

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

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.

The screenshot shows a Windows-style dialog box titled "Example User Properties". It has a standard title bar with a question mark and a close button. Below the title bar is a tabbed interface. The tabs are: "Member Of", "Dial-in", "Environment", "Sessions", "Remote control", "Remote Desktop Services Profile", "COM+", "General", "Address", "Account", "Profile", "Telephones", and "Organization". The "General" tab is currently selected. Inside the "General" tab, there are several text input fields: "Job Title" with the value "Cloud Advocate", "Department" with "Developer Relations", "Company" with "Microsoft", and "Manager" with "Example Manager". Below the "Manager" field are three buttons: "Change...", "Properties", and "Clear". At the bottom of the dialog box are four buttons: "OK", "Cancel", "Apply", and "Help".

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.

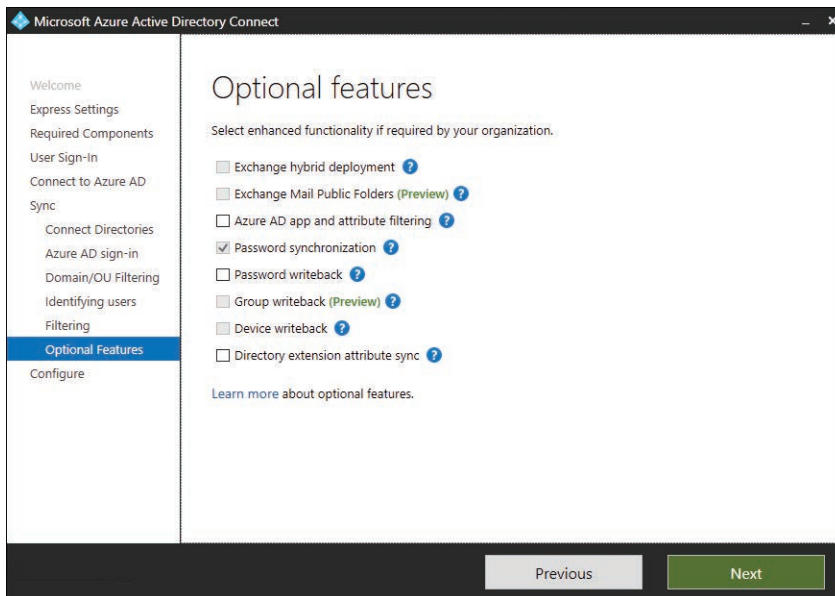


FIGURE 2-2 Azure Active Directory Connect optional features

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.

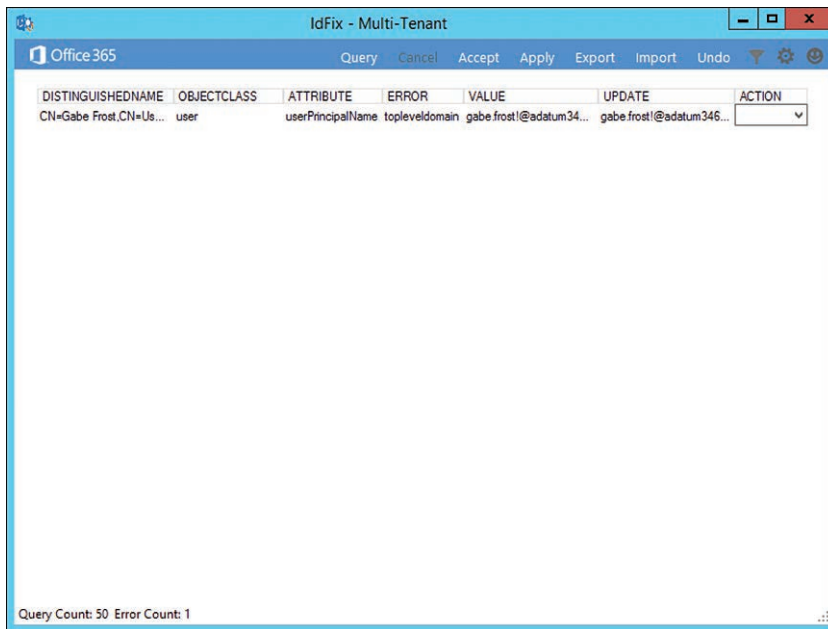


FIGURE 2-3 IdFix finds a user with a problematic UPN.

MORE INFO IDFIX

You can download IdFix at the following address: <https://microsoft.github.io/idxfix/>.

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.

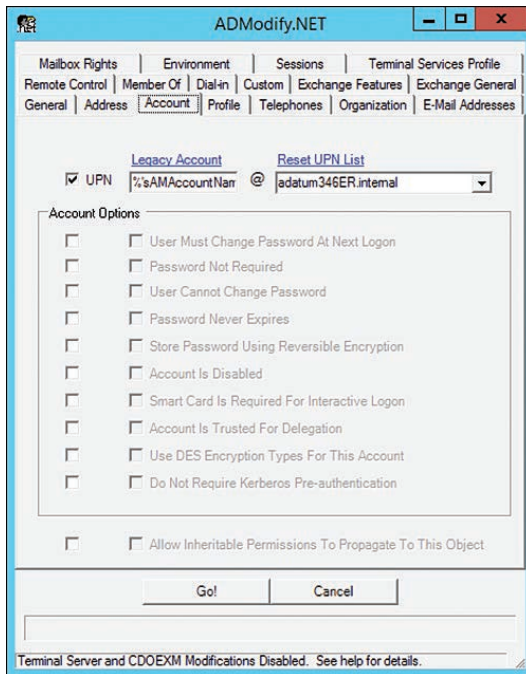


FIGURE 2-4 ADModify.NET

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.

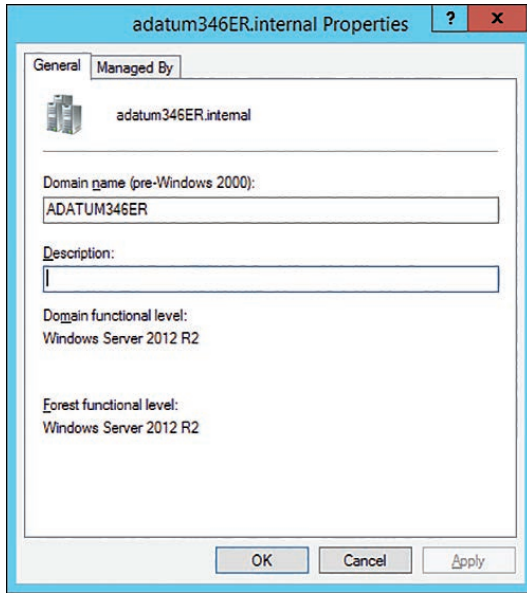


FIGURE 2-5 Nonroutable domain

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.

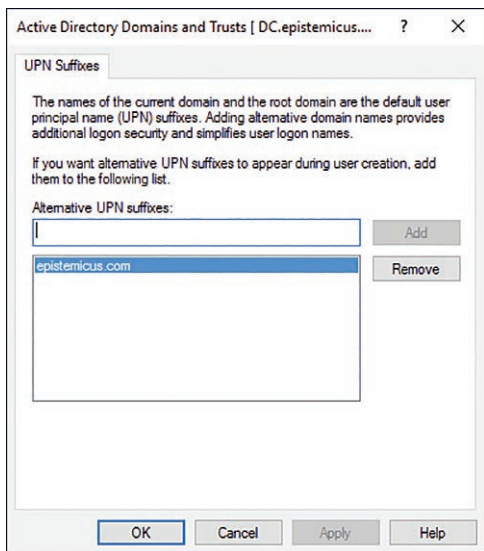


FIGURE 2-6 Routable domain

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**.

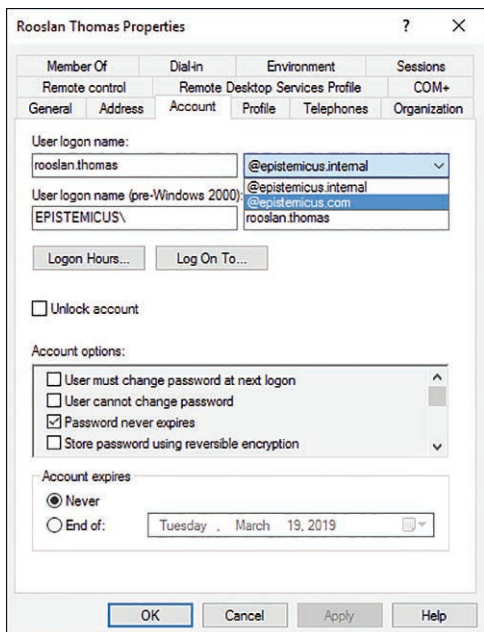


FIGURE 2-7 Configuring the UPN

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

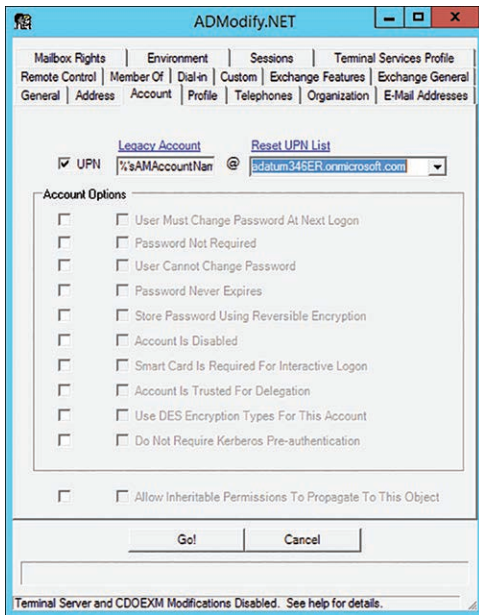


FIGURE 2-8 ADModify.NET

- 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.

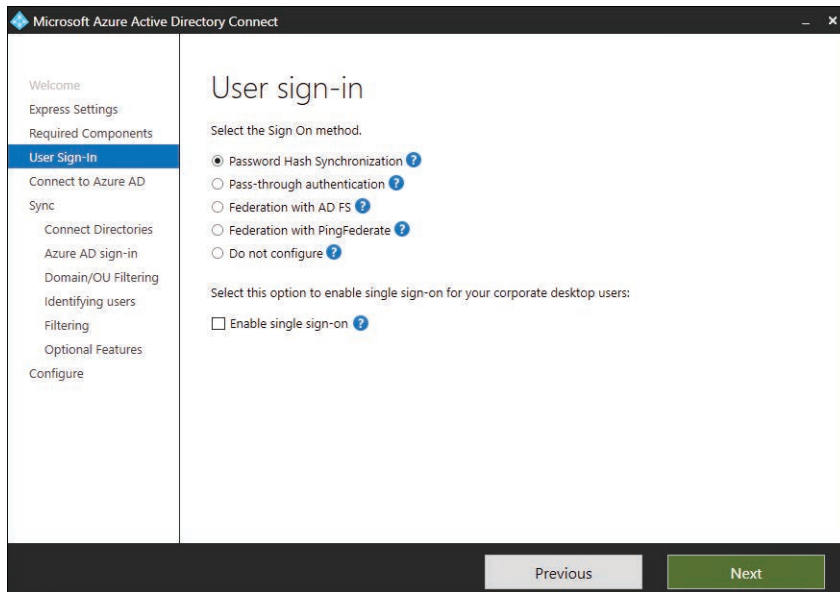


FIGURE 2-9 User sign-in

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.psml'`
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

A

- access control, 175. *See also* external access
 - conditional access, 175–176, 187
 - configuring, 187–190
 - What If tool, 190–192
 - entitlement packages, 176–179
- account(s)
 - B2B, 203–206, 208–210
 - guest, 207–208
 - lockout, MFA (multifactor authentication), 200
- Active Directory Federation, 107
- Active Users report, 63
- admin roles, 148–150
 - rights and, 152–153
- administrative accounts, 153–155
- alerts
 - fraud, 201
 - Service Health dashboard, 53–55
- APIPA (Automatic Private IP Addressing), 2
- application modernization, 14
- Application Proxy, 215–216
 - architecture, 215
 - benefits, 215
 - connectors, 216–217
- applications, 210–211
 - adding to Azure AD, 217–219
 - assigning users access to, 212–215
 - click-to-run, 239
 - integrating with Azure AD, 211–212
 - managing downloads, 229–231
 - registering, 211
- apps
 - managing, 225–227
 - managing access to, 212
 - MFA (multifactor authentication), 193–197
 - Power, 317
 - updates, 241–242
- architecture, Application Proxy, 215
- assigning access to applications, 212–215
- assignments, 175
- auditing, reports, 60
- authentication, 11–12, 97. *See also* access control; MFA (multifactor authentication)
 - Azure AD Smart Lockout, 167
 - banned password list, 167–168
 - basic, 160
 - certificate-based, 170
 - cloud
 - cloud-only, 12
 - pass-through authentication with Single-Sign On, 13
 - password hash sync with Single Sign-On, 12–13
 - configuring, 164–165
 - federated, 13
 - federated identity with Active Directory Federation Services, 13
 - third-party authentication and identity providers, 14
 - hybrid modern, 97
 - methods and usage, 162
 - modern, 160
 - configuring, 164
 - registry keys, 160–161
 - monitoring, 170–172
 - self-service password reset activity, 173–174
 - sign-in logs, 172–173
 - multifactor, 161, 192–193
 - account lockout, 200
 - block/unblock users, 200–201
 - fraud alerts, 201
 - managing, 197–200
 - OATH tokens, 201–202
 - phone call settings, 202
 - for users and apps, 193–197
 - utilization report, 203
 - pass-through, 106–107
 - password policy, 164–165

authentication

- password-less sign-on, 169
- properties, 162–164
- security questions, 162–163
- self-service password reset, 168–169
- autodiscover CNAME records, 22
- Azure AD
 - adding an enterprise application from the gallery, 217–219
 - administrative accounts, 153–155
 - application access, 210–211
 - Application Proxy, 215–216
 - architecture, 215
 - benefits, 215
 - connectors, 216–217
 - applications
 - integrating, 211–212
 - managing access to, 212
 - B2B accounts, creating, 203–206
 - banned password list, 167–168
 - certificate-based authentication, 170
 - conditional access policies, 187
 - configuring, 187–190
 - What If tool, 190–192
 - entitlement packages, 176–179
 - external access, 208–210
 - guest accounts, creating, 207–208
 - identities, 134
 - Identity Protection, 179–180
 - investigating risky activity, 182–183
 - risk events, 185–186
 - risk policies, 181–182
 - users flagged for risk, 186–187
 - managing admin roles, 148–150
 - managing groups, 138–140
 - Microsoft groups, 287–291
 - passwords, 140–142
 - PIM (Privileged Identity Management), 153
 - product licenses, 143–145
 - registering applications, 211
 - reviewing user access, 137
 - roles
 - allocations, 151
 - for workloads, 151
 - self-service password reset, 135–137, 168–169
 - Smart Lockout, 167
 - user management, 145–148
- Azure AD Connect
 - Active Directory Federation, 107
 - ADmodify.NET and, 101–102
 - ADSync PowerShell module, 125
 - applications, assigning users access to, 212–215
 - cleaning up existing AD objects, 99–100
 - connectivity requirements, 111–112
 - directory synchronization, 98–99, 108
 - endpoints, 107–108
 - hardware requirements, 112
 - identifying synchronized attributes, 122–124
 - IdFix and, 101
 - installation account requirements, 113
 - installing, 109, 113–122
 - multiforest synchronization, 132–133
 - object filters, 129–131
 - pass-through authentication, 106–107
 - on-premises Active Directory environment
 - requirements, 109–110
 - scheduler, 125–129
 - server requirements, 110–111
 - SQL server requirements, 112–113
 - synchronization, 98
 - password, 106
 - UPN suffixes and nonroutable domains, 102–105
- Azure AD Connect Health, 124–125

B

- B2B accounts
 - creating, 203–206
 - external access, 208–210
- bandwidth, on-premises infrastructure requirements, 7
- banned password list, 167–168
- basic authentication, 160
- billing administrator, 44
- blocking/unblocking users, MFA (multifactor authentication), 200–201
- bulk import process, 84–85

C

- Center of Excellence (CoE), 311
- certificate-based authentication, 170
- classification schemas, 9
- click-to-run, 239
- cloud authentication
 - cloud-only, 12
 - pass-through authentication with Single-Sign On, 13
 - password hash sync with Single Sign-On, 12–13

cmdlets. *See* PowerShell cmdlets

compatibility, Microsoft 365 Apps and, 229, 230

compliance

- reports, 59
- roles and, 155–156

conditional access, 175–176, 187

- configuring, 187–190
- What If tool, 190–192

Configuration.xml files, 236–239

configuring

- authentication, 164
- methods, 164–165
- password policy, 164–165
- conditional access policies, 187–190

connectivity

- Azure AD Connect requirements, 111–112
- messaging deployment and, 271
- Microsoft 365 Apps for enterprise, requirements, 224–225
- Microsoft Power Platform, 320
- on-premises infrastructure requirements, 2–3
- SharePoint Online, 284–285
- Skype for Business, 308–309
- Teams and, 306–308

connectors, Application Proxy, 216–217

CQD (Call Quality Dashboard), 296

creating

- B2B accounts, 203–206
- guest accounts, 207–208

Customer Lockbox access approver, 44

cutover migration, 79–80, 265–266

D

data loss prevention (DLP), reports, 60

delegated administrator, 48

deploying

- Microsoft 365 tenants, 15
- acquiring a domain name, 16
- configure a custom domain name, 17–18
- configure workloads for a new domain name, 20–24
- managing domains, 15–16
- purchase a domain through Microsoft 365, 17
- verify a custom domain, 18–20

Teams, 297–299

Telemetry Dashboard, 245–252

deployment workload teams, identifying, 10–11

design an identity strategy, 93

- authentication, 97
- requirements and solutions for identity management, 96–97
- synchronization, 94
- frequency of, 95
- selecting identities to replicate, 94–95
- selecting properties, 95–96

Desktop Analytics

- performing a readiness assessment, 228
- viewing health status of applications, 228–229

directory synchronization, 98–99, 108

domain name, acquiring, 16

Dynamics 365 service administrator, 44

E

email. *See also* mailboxes; messaging deployments

- activity reports, 61–62
- domains, 272–273
- mailboxes

 - migration and, 76
 - usage reports, 62–63

- Microsoft 365 tenancy and, 27–32
- migration, 88–90

Email App Usage report, 64

endpoints

- Azure AD Connect, 107–108
- optimization methods, 3–4

enterprise application modernization, 14

entitlement packages, 176–179

Exchange administrator, 45

Exchange Online. *See also* messaging deployments

- DNS records, 20–21
- importing PST files, 268
- migration, 262

 - cutover, 265–266
 - IMAP, 267
 - minimal hybrid, 266
 - remote move, 262–263
 - staged, 264–265

express migration, 80–81

ExpressRoute, 7

external access, design solutions for, 208–210

F

FastTrack, 36–38
 federated authentication, 13
 federated identity with Active Directory Federation Services, 13
 third-party authentication and identity providers, 14
 firewall, outbound port requirements, 4–5
 flow actions, 315–317
 flows, 312–315

G

global administrator, 43–44
 Group Policy, enabling telemetry, 252–258. *See also* policy(ies)
 groups
 managing, 138–140
 Microsoft, 287–291
 migrating, 87–88
 nested, 289–291
 guest accounts, creating, 207–208

H-I

helpdesk administrator, 45
 hybrid modern authentication, 97
 identifying, deployment workload teams, 10–11
 identity and authentication solution
 cloud authentication, 12
 cloud-only, 12
 pass-through authentication with Single-Sign On, 13
 password hash sync with Single Sign-On, 12–13
 federated authentication, 13
 federated identity with Active Directory Federation Services, 13
 third-party authentication and identity providers, 14
 planning, 11–12
 Identity Protection, 179–180
 investigating risky activity, 182–183
 risk policies, 181–182
 identity(ies). *See also* roles; user accounts
 Azure AD, 134
 groups, managing, 138–140
 security, 159

source of authority, 139
 synchronization, 94. *See also* Azure AD Connect
 ADmodify.NET and, 101–102
 cleaning up existing AD objects, 99–100
 directory, 98–99
 frequency of, 95
 IdFix and, 101
 pass-through authentication and, 106–107
 password, 106
 selecting identities to replicate, 94–95
 selecting properties, 95–96
 UPN suffixes and nonroutable domains, 102–105
 user management, 145–148
 IdFix, 101
 IMAP migration, 81–82, 267
 information protection, 8
 classification schemas, 9
 privileged access management, 10
 security and information protection levels, 8–10
 installing
 Azure AD Connect, 113–122
 Microsoft 365 Apps for enterprise, 231–234
 Office Deployment Tool, 235–236
 internet connectivity
 Azure AD Connect requirements, 111–112
 on-premises infrastructure requirements, 2–3
 investigating risky activity, 182–183
 risk events, 185–186

J-K-L

license(s)
 administrator, 45
 managing, 143–145
 monitoring, 57
 LOB (line-of-business) applications, modernizing, 14

M

mailboxes. *See also* messaging deployments
 migration, 76
 comparison of methods, 82–83
 cutover, 79–80
 IMAP, 81–82
 import PST files, 88–90
 minimal hybrid, 80–81

- remote move, 77–78
- staged, 78–79
- meeting policies, 301–302
- message center reader, 46
- messaging deployments, 261, 268–269. *See also* Exchange Online
 - email domains, 272–273
 - import service, 268
 - mail routing, 271–272
 - migration strategy, 262
 - cutover migration, 265–266
 - identify hybrid requirements, 269–270
 - IMAP migration, 267
 - minimal hybrid migration, 266
 - remote move migration, 262–263
 - staged migration, 264–265
 - planning for connectivity, 271
- messaging policies, 303–304
- MFA (multifactor authentication), 161, 192–193
 - account lockout, 200
 - for apps and users, 193–197
 - block/unblock users, 200–201
 - fraud alerts, 201
 - managing, 197–200
 - OATH tokens, 201–202
 - phone call settings, 202
 - planning, 1
- Microsoft 365 Apps for enterprise
 - central deployment, 234
 - compatibility and, 229, 230
 - connectivity requirements, 224–225
 - installing, 231–234
- Microsoft 365 portal, managing software downloads, 229–231
- Microsoft 365 tenancy, 32
 - add a Microsoft partner or work with Microsoft FastTrack, 36–38
 - complete the organizational profile, 35–36
 - complete the subscription setup wizard, 38–40
 - configure workloads for a new domain name
 - autodiscover CNAME records, 22
 - Exchange federation CNAME records, 22
 - Exchange federation TXT records, 22
 - Exchange Online-related DNS records, 20–21
 - exchange online-related DNS records, 20–21
 - MX records, 21
 - Skype records, 22–24
 - SPF records, 21–22
 - deploying, 15
 - Dynamics 365 service administrator, 44
 - edit an organizational profile, 42–43
 - email addresses, 27–32
 - managing domains, 15–16
 - acquiring a domain name, 16
 - configure a custom domain name, 17–18
 - configure authoritative and internal relay domains, 25–27
 - configure user identity for the new domain name, 27–32
 - implement a domain name strategy, 32
 - mobile device management (MDM) for Microsoft 365 DNS records, 24
 - purchase a domain through Microsoft 365, 17
 - set the default domain, 25
 - verify a custom domain, 18–20
 - verify DNS settings, 24–25
 - organizational settings, 32–35
 - plan and create a tenant, 40–41
 - roles
 - billing administrator, 44
 - Customer Lockbox access approver, 44
 - delegated administrator, 48
 - Exchange administrator, 45
 - global administrator, 43–44
 - helpdesk administrator, 45
 - license administrator, 45
 - managing membership, 48–49
 - message center reader, 46
 - Power BI service administrator, 46
 - reports reader, 46
 - service administrator, 46
 - SharePoint administrator, 47
 - Skype for Business administrator, 46
 - teams communications administrator, 47
 - teams communications support engineer, 47
 - teams communications support specialist, 47
 - teams service administrator, 47
 - user management administrator, 48
 - subscriptions, 43, 52–53
- Microsoft FastTrack, 36–38
- Microsoft Office 365, click-to-run applications, 239
- Microsoft Power Platform, 310
 - Center of Excellence (CoE) starter kit, 311
 - connectivity, 320
 - Dynamics 365 apps, 325–326
 - flow actions, 315–317

- flows, 312–315
- managing environments, 320
 - Administration mode, 321
 - backup and restore an environment, 322–323
 - refresh cadence, 321–322
 - switching between production and sandbox, 322
- planning for workload deployments, 311–312
- portals and, 327
- PowerApps, 317
- resource deployment, 317–320
- resources, 323
 - add-on capacity, 323–324
 - managing PowerApps, 324–325
- Microsoft Teams. *See also* Teams
 - Device Usage report, 70–71
 - User Activity report, 70
- migration. *See also* Exchange Online, migration
 - comparison of methods, 82–83
 - cutover, 265–266
 - express, 80–81
 - identity data to be migrated and migration methods, 71–72
 - IMAP, 267
 - import PST files, 88–90
 - mailboxes, 76
 - cutover migration, 79–80
 - IMAP, 81–82
 - minimal hybrid, 80–81
 - remote move migration, 77–78
 - staged migration, 78–79
 - minimal hybrid, 266
 - move data to SharePoint Online, 72
 - move known local folders to OneDrive for Business, 72–76
 - on-premises users, 83
 - bulk import process, 84–85
 - groups and, 87–88
 - soft delete and, 85–87
 - user categories, 84
 - remote move, 77–78, 262–263
 - Skype for Business, 300–301
 - staged, 264–265
- minimal hybrid migration, 80–81, 266
- modern authentication, 160. *See also* authentication
 - configuring, 164
 - registry keys, 160–161
- monitoring
 - authentication, 170–172
 - self-service password reset activity, 173–174
 - sign-in logs, 172–173

- license allocations, 57
- service health, 56
- MSI files, 239–241
- multiforest synchronization, 132–133
- MX records, 21

N

- nested groups, 289–291
- networking
 - avoiding hairpins, 6
 - bandwidth, prerequisites, 7
 - egress connections locally, 6
 - ExpressRoute, 7
 - internet connectivity for clients, 2–3
 - Microsoft 365 or Office 365 endpoints, 3–4
 - outbound firewall ports, 4–5
 - SD-WAN devices, 6–7

O

- OATH tokens, MFA (multifactor authentication), 201–202
- Office 365
 - apps, 225–227, 241–242
 - managing software downloads, 229–231
 - requirements, 109
- Office Activations report, 62–63
- Office Deployment Tool
 - Configuration.xml files, 236–239
 - installing, 235–236
 - modes, 236
- Office Online, planning for, 227–228
- Office Telemetry, 242–243
 - reporting user issues, 260–261
 - System Info worksheet, 261
 - Telemetry Dashboard, 243–244
 - configuring through the registry, 259–260
 - deploying, 245–252
 - requirements, 244
 - worksheets, 258–259
- OneDrive Activity report, 64
- OneDrive for Business
 - accessing, 292–293
 - collaboration and, 293–295
 - managing, 292
 - migration and, 72–76
 - migration strategy, 274–275

- plan external share settings, 275
 - enable external sharing globally, 276–278
 - enable external sharing per site collection, 278–280
 - sharing a document, 281–284
 - sharing a site, 280–281
- revoking external user access, 284
- usage report, 65
- organizational profile, editing, 42–43
- organizational settings, Microsoft 365 tenancy, 32–35
- outbound firewall ports, infrastructure requirements, 4–5

P

- pass-through authentication, 106–107
- password-less sign-on, 169
- password(s)
 - banned, 167–168
 - helpdesk administrator, 45
 - managing, 140–142
 - policy, 164–165
 - self-service reset, 135–137, 168–169
 - synchronization, 106, 131–132
- Phone System, 297
- PIM (Privileged Identity Management), 153
- planning
 - enterprise application modernization, 14
 - identity and authentication solution, 11–12
 - cloud-only authentication, 12
 - federated authentication, 13
 - federated identity with Active Directory Federation Services, 13
 - pass-through authentication with Single-Sign On, 13
 - password hash sync with Single Sign-On, 12–13
 - third-party authentication and identity providers, 14
 - Microsoft 365 tenancy, 40–41
- policy(ies)
 - assignments, 175
 - conditional access, 175–176, 187–190
 - meeting, 301–302
 - messaging, 303–304
 - password, 164–165
 - risk, 181–182
 - telemetry, 252–258
 - voice-calling, 305
- portals, 327
- Power BI
 - reports, 57–58
 - service administrator role, 46
- Power Platform, 310
 - Center of Excellence (CoE) starter kit, 311
 - connectivity, 320
 - flow actions, 315–317
 - flows, 312–315
 - managing Dynamics 365 apps, 325–326
 - managing environments, 320
 - Administration mode, 321
 - backup and restore an environment, 322–323
 - refresh cadence, 321–322
 - switching between production and sandbox, 322
 - planning for workload deployments, 311–312
 - portals and, 327
 - PowerApps, 317
 - resource deployment, 317–320
 - resources, 323
 - add-on capacity, 323–324
 - managing PowerApps, 324–325
- PowerApps, 317
- PowerShell cmdlets
 - Get-ADSyncScheduler, 125–129
 - group management and, 140, 288
 - Team management, 309–310
- on-premises infrastructure requirements, 10
 - bandwidth, 7
 - deploy SD-WAN devices, 6–7
 - information protection, 8
 - classification schemas, 9
 - improving security levels, 9–10
 - privileged access management, 10
 - security and information protection levels, 8–9
 - networking, 2
 - avoid network hairpins, 6
 - egress network connections locally, 6
 - ExpressRoute, 7
 - internet connectivity for clients, 2–3
 - Microsoft 365 or Office 365 endpoints, 3–4
 - outbound firewall ports, 4–5
 - Windows 10 Enterprise edition, 7–8
- product licenses, managing, 143–145
- protection report, 60
- PST files, migration and, 88–90

Q-R

- QoS (Quality of Service), 296
- RBAC (role-based access control), 152
 - delegate admin rights, 152–153
- readiness assessment, 228
- registering applications, 211
- registry
 - configuring Telemetry Dashboard, 259–260
 - keys, modern authentication, 160–161
- remote move migration, 77–78, 262–263
- report(s)
 - Active Users, 63
 - auditing, 60
 - data loss prevention (DLP), 60
 - email activity, 61–62
 - Email App Usage, 64
 - MFA utilization, 203
 - Microsoft Teams Device Usage, 70–71
 - Microsoft Teams User Activity, 70
 - Office Activations, 63
 - OneDrive Activity, 64
 - OneDrive usage, 65
 - Power BI, 57–58
 - protection, 60
 - reader, 46
 - rules, 60
 - security and compliance, 59
 - self-service password reset, 174
 - SharePoint Activity, 65–66
 - SharePoint Site Usage, 66–67
 - Skype for Business Activity, 67
 - Skype for Business Conference Organizer Activity, 68
 - Skype for Business Conference Participant Activity, 68–69
 - usage, 61
 - Yammer Activity, 69
 - Yammer Device Usage, 69
 - Yammer Groups Activity, 69–70
- reviewing user access, 137
- risk policies, 181–182
- risky activity, 182–183
 - risk events, 185–186
 - sign-ins, 183–185
 - users flagged for risk, 186–187

- roles, 151. *See also* RBAC (role-based access control)
 - admin, 148–150
 - billing administrator, 44
 - compliance and, 155–156
 - Customer Lockbox access approver, 44
 - delegated administrator, 48
 - Dynamics 365 service administrator, 44
 - Exchange administrator, 45
 - global administrator, 43–44
 - helpdesk administrator, 45
 - license administrator, 45
 - managing membership, 48–49
 - message center reader, 46
 - Power BI service administrator, 46
 - reports reader, 46
 - service administrator, 46
 - SharePoint administrator, 47
 - Skype for Business administrator, 46
 - teams communications administrator, 47
 - teams communications support engineer, 47
 - teams communications support specialist, 47
 - teams service administrator, 47
 - user management administrator, 48
 - for workloads, 151
- rules reports, 60

S

- scheduler, Azure AD Connect, 125–129
- SD-WAN (software-defined wide area networks)
 - devices, 6–7
- security, 159. *See also* authentication
 - compliance roles and, 155–156
 - conditional access, 175–176, 187
 - configuring, 187–190
 - What If tool, 190–192
 - entitlement packages, 176–179
 - Identity Protection, 179–180
 - investigating risky activity, 182–185
 - risk events, 185–186
 - risk policies, 181–182
 - users flagged for risk, 186–187
 - levels, 8–10
 - reports, 59

- self-service password reset, 135–137, 168–169
 - monitoring, 173–174
 - report(s), 174
- service administrator, 46
- service health
 - alerts and, 53–55
 - create a health response plan, 55–56
 - monitoring, 56
 - reports, 57–58
- Service Health dashboard, alerts, 53–55
- SharePoint
 - Activity report, 65–66
 - administrator role, 47
 - Site Usage report, 66–67
- SharePoint Online
 - hybrid connectivity, 284–285
 - manage access configuration, 285–287
 - managing tenant and site settings, 291–292
 - migration and, 72
 - migration strategy, 274–275
 - plan external share settings, 275
 - enable external sharing globally, 276–278
 - enable external sharing per site collection, 278–280
 - sharing a document, 281–284
 - sharing a site, 280–281
 - revoking external user access, 284
- sign-in logs, 172–173
 - investigating risky activity, 183–185
- Single Sign-On, 12–13
- Skype for Business
 - Activity report, 67
 - administrator role, 46
 - Conference Organizer Activity report, 68
 - Conference Participant Activity report, 68–69
 - configuring for a new domain name, 22–24
 - hybrid configuration, 308
 - hybrid connectivity, 308–309
 - migration strategy, 300–301
- smartphones, password-less sign-on, 169
- soft delete, migration and, 85–87
- source of authority, 139
- SPF records, 21–22
- staged migration, 78–79, 264–265
- subscriptions, managing, 43, 52–53
- suspicious activity, 182–183
 - risk events, 183–185
 - users flagged for risk, 186–187

- synchronization, 94
 - ADmodify.NET and, 101–102
 - Azure AD Connect, 98
 - cleaning up existing AD objects, 99–100
 - directory synchronization, 98–99
 - identifying synchronized attributes, 122–124
 - UPN suffixes and nonroutable domains, 102–105
 - directory, 108
 - filtering, 129–131
 - frequency of, 95
 - IdFix and, 101
 - multiforest, 132–133
 - password, 106, 131–132
 - selecting identities to replicate, 94–95
 - selecting properties, 95–96

T

Teams

- Advisor, 299–300
- communications administrator, 47
- communications support engineer, 47
- communications support specialist, 47
- deploying, 297–298
- enterprise deployment, 298–299
- managing call quality, 296–297
- meeting policies, 301–302
- messaging policies, 303–304
- organizational settings, 301
- Phone System, 297
- planning for guest and external access, 305–306
- planning for hybrid connectivity and coexistence, 306–308
- PowerShell cmdlets, 309–310
- service administrator, 47
- voice-calling policies, 305
- telemetry
 - enabling, 252–253
 - policies, 253–258
- Telemetry Dashboard, 243–244
 - configuring through the registry, 259–260
 - deploying, 245–252
 - requirements, 244
 - worksheets, 258–259
- TLS (Transport Layer Security), 160

U-V

- updates, app, 241–242
- usage analytics, 61
 - reports and, 57–58
- user accounts
 - administrative, 153–155
 - migration and, 85–87
- user management, 145–148
- user management administrator role, 48
- user roles, 148
- voice-calling policies, 305

W

- What If tool, 190–192
- Windows 10 Enterprise edition, 7–8
- worksheets, Telemetry Dashboard, 258–259

X-Y-Z

- Yammer
 - Activity report, 69
 - Device Usage report, 69
 - Groups Activity report, 69–70