



Windows 10

SECOND EDITION

Exam Ref

MD-100

Andrew Bettany
Andrew Warren

FREE SAMPLE CHAPTER

SHARE WITH OTHERS



Exam Ref MD-100 Windows 10

Second Edition

Andrew Bettany
Andrew Warren

Exam Ref MD-100 Windows 10, Second Edition

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.

ISBN-13: 978-013-747219-2

ISBN-10: 0-137-47219-6

Library of Congress Control Number: 2021942771

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.

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
Songlin Qiu

MANAGING EDITOR
Sandra Schroeder

SENIOR PROJECT EDITOR
Tracey Croom

COPY EDITOR
Liz Welch

INDEXER
Timothy Wright

PROOFREADER
Abigail Bass

TECHNICAL EDITOR
Tommy B. Kobberø

EDITORIAL ASSISTANT
Cindy Teeters

COVER DESIGNER
Twist Creative, Seattle

Contents at a glance

	<i>Introduction</i>	<i>xi</i>
CHAPTER 1	Deploy Windows	1
CHAPTER 2	Manage devices and data	107
CHAPTER 3	Configure storage and connectivity	211
CHAPTER 4	Maintain Windows	291
	<i>Index</i>	<i>423</i>

This page intentionally left blank

Contents

Introduction	xi
<i>Organization of this book</i>	<i>xi</i>
<i>Preparing for the exam</i>	<i>xi</i>
<i>Microsoft certifications</i>	<i>xii</i>
<i>Errata, updates, & book support</i>	<i>xii</i>
<i>Stay in touch</i>	<i>xii</i>
Chapter 1 Deploy Windows	1
Skill 1.1: Deploy Windows 10	1
Select the appropriate Windows edition	2
Perform a clean installation	8
Perform an in-place upgrade	14
Migrate user data	21
Configure Windows for additional regional and language support	27
Skill 1.2: Perform post-installation configuration	32
Customize the Windows desktop	32
Configure Microsoft Edge	52
Configure Internet Explorer	64
Implement activation	69
Configure mobility settings	77
Configure printers and external devices	84
Configure Windows 10 by using provisioning packages	92
Configure Microsoft Store settings	94
Configure application settings	96
Configure and manage services	98
Chapter summary	102
Thought experiment	104
Scenario 1	104
Scenario 2	104

Thought experiment answers	105
Scenario 1	105
Scenario 2	105
Chapter 2 Manage devices and data	107
Skill 2.1: Manage local users, local groups, and devices.	107
Manage local users	108
Manage local groups	114
Manage users, groups, and devices in Active Directory Domain Services	118
Manage devices in directories	121
Configure sign-in options	136
Skill 2.2: Configure devices by using local policies	146
Configure local registry	146
Implement local policy	150
Configure Windows 10 settings by using Group Policy	157
Troubleshoot Group Policies on devices	159
Skill 2.3: Manage Windows Security	162
Configure Windows Security	162
Configure User Account Control	165
Configure Windows Defender Firewall	170
Implement encryption	180
Configure BitLocker	186
Configure Windows Defender Antivirus	199
Chapter summary	203
Thought experiment.	206
Scenario 1	206
Scenario 2	206
Scenario 3	207
Scenario 4	207
Thought experiment answers	208
Scenario 1	208
Scenario 2	208

Scenario 3	208
Scenario 4	209
Chapter 3 Configure storage and connectivity	211
Skill 3.1: Configure networking	211
Configure client IP settings	212
Configure mobile networking	222
Configure VPN client	225
Troubleshoot networking	231
Configure Wi-Fi profiles	234
Skill 3.2: Configure data access and protection	240
Configure file and folder permissions	240
Configure shared permissions	255
Configure, manage, and optimize local storage	266
Configure OneDrive and OneDrive for Business	282
Chapter summary	285
Thought experiment	286
Scenario 1	286
Scenario 2	287
Scenario 3	287
Scenario 4	288
Thought experiment answers	288
Scenario 1	288
Scenario 2	289
Scenario 3	289
Scenario 4	289
Chapter 4 Maintain Windows	291
Skill 4.1: Configure system and data recovery	291
Perform file recovery	292
Recover Windows 10	304
Troubleshoot the startup process	319
Skill 4.2: Manage updates	342
Plan for Windows Updates	343
Select the appropriate servicing channel	345

Configure Windows Update options	347
Troubleshoot updates	355
Skill 4.3: Monitor and manage Windows	359
Configure and analyze event logs	359
Manage performance	364
Manage Windows 10 environment	377
Configure local registry	386
Schedule tasks	390
Skill 4.4: Configure remote connectivity	391
Manage Windows remotely by using Windows Remote Management	392
Configure remote assistance tools including Remote Assistance and Quick Assist	398
Configure Remote Desktop access	404
Manage Windows remotely by using PS remoting	409
Manage Windows 10 remotely by using Windows Admin Center	411
Chapter summary	415
Thought experiment.....	417
Scenario 1	417
Scenario 2	417
Scenario 3	418
Scenario 4	418
Scenario 5	418
Thought experiment answers	419
Scenario 1	419
Scenario 2	419
Scenario 3	420
Scenario 4	420
Scenario 5	421
 <i>Index</i>	 423

Acknowledgments

I want to thank the production team who help make the book production process painless. I would like to dedicate this Windows 10 2nd Edition book to Annette and Tommy for being supportive and encouraging. This book is also for the reader. Having taught thousands of IT professionals over my career, I hope this book helps you become proficient with Windows 10. The world of IT is ever changing, and we should all strive to stay up-to-date and use the most appropriate tools. I hope this book helps you achieve success!

—ANDREW BETTANY

The publication of the second edition of this book coincides with the 25th anniversary of my certification as a Microsoft Certified Trainer. Over the last quarter century, I've enjoyed the challenge of helping students gain the necessary skills to become better at their jobs. This book gives me the opportunity to continue doing so.

—ANDREW WARREN

About the authors



ANDREW BETTANY was awarded the Microsoft Most Valuable Professional (Windows and Devices for IT) for 8 years before joining Microsoft. He is a loving dad, IT geek, training mentor and consultant, entrepreneur, and author.

Andrew is recognized for his Windows expertise, and he is the author of many publications, including several Windows exam certification prep guides and Microsoft official training materials. He is the author of video training materials for LinkedIn Learning and Pluralsight. As a Microsoft Certified Trainer for 16 years, Andrew delivers learning and consultancy to businesses in many technical areas, including Microsoft 365, Azure, and Windows 10.

He has co-founded the “IT Masterclasses” series of short, intensive technical courses (see www.itmasterclasses.com), and he is passionate about helping others learn technology. He is a frequent speaker at Microsoft Ignite and other technical conferences worldwide.

Andrew is active on social media and can be found on LinkedIn, Facebook, and Twitter. He lives in a village just outside the beautiful city of York in Yorkshire, England.



ANDREW WARREN, MCT, has been writing for Microsoft for many years, helping to develop their official curriculum of instructor-led training material. He has served as a subject matter expert on many of the current Windows Server courses, was technical lead on several of the Windows 10 titles, and was involved in Microsoft 365, Azure, and Intune course development. When not writing about Microsoft technologies, he can be found in the classroom, teaching other IT professionals what they need to know to manage their organization’s IT infrastructure.

Introduction

With the Microsoft 365 Certified: Modern Desktop Administrator Associate certification, Microsoft has changed the way that IT pro certifications work. Rather than being based on a technology area, they are focused on a specific job role. The Microsoft MD-100: Windows 10 exam provides the foundation of this Modern Desktop Administrator Associate certification.

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 you’ll find in the text to find more information and take the time to research and study the topic. Great information is available on the Microsoft website at docs.microsoft.com.

Organization of this book

This book is organized by the “Skills measured” list published for the exam. The “Skills measured” list is available for each exam on the Microsoft Learn website: <https://aka.ms/examlist>. 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.

Preparing for the exam

Microsoft certification exams are a great way to build your résumé and let the world know about your level of expertise. Certification exams validate your on-the-job experience and product knowledge. Although there is no substitute for on-the-job experience, preparation through study and hands-on practice can help you prepare for the exam. This book is *not* designed to teach you new skills.

We recommend that you augment your exam preparation plan by using a combination of available study materials and courses. For example, you might use the Exam Ref and another study guide for your “at home” preparation and take a Microsoft Official Curriculum course for the classroom experience. Choose the combination that you think works best for you. Learn more about available classroom training and find free online courses and live events at <http://microsoft.com/learn>. Microsoft Official Practice Tests are available for many exams at <http://aka.ms/practicetests>.

Note that this Exam Ref is based on publicly available information about the exam and the authors' experience. To safeguard the integrity of the exam, authors do not have access to the live exam.

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!

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/ExamRefMD1002e/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>.

Manage devices and data

The MD-100 Windows 10 exam focuses on how to manage devices within an enterprise environment, by using a Microsoft 365 subscription, for example. Once you have installed or upgraded devices with Windows 10, you need to know how to join devices to Azure Active Directory. Organizations that do not use the cloud use Active Directory Domain Services, and you must manage both users and devices.

Devices are managed using local or Group Policy, and you have to implement and troubleshoot these policies. To ensure that data and devices remain safe, you must know how to configure Windows security and use Windows Defender Firewall and Windows Defender Antivirus to safeguard Windows 10.

Skills covered in this chapter:

- Skill 2.1: Manage local users, local groups, and devices
- Skill 2.2: Configure devices by using local policies
- Skill 2.3: Manage Windows security

Skill 2.1: Manage local users, local groups, and devices

In this skill, you will review how to manage local users and local groups on Windows 10 devices. If you have experience with an earlier version of Windows, you might be familiar with configuring local users and local groups, as these operations are largely unchanged. Before you use Windows 10 on a device, you must sign in with the credentials for a user account. In an enterprise environment, the device and the user are often used to provide, control, and audit access to resources. Groups may be used for simplifying administration, allowing entities to share a common function or role or require the same set of privileges. You need to understand how local users, local groups, and devices form a key component in Windows security.

This skill covers how to:

- Manage local users
- Manage local groups
- Manage users, groups, and devices in Active Directory Domain Services
- Manage devices in directories
- Configure sign-in options

Manage local users

A user account is required to log on to a Windows 10 computer, and to secure the device, it should have a password. You need to understand the default user accounts that are created automatically when you install Windows 10 and how to create new user accounts so that users can log on to machines and access resources. In this skill, you will focus on local accounts that are created and operate only on the local device.

Configure local accounts

Local accounts, as the name suggests, exist in the local accounts database on your Windows 10 device; they can only be granted access to local resources and, where granted, exercise administrative rights and privileges on the local computer.

When you first install Windows 10, you are prompted to sign in using a Microsoft account or a Work Account, such as a Microsoft 365 account that is connected to Azure Active Directory. If neither of these options is available or suits your requirements, you can choose an offline account and create a local account to sign in. Thereafter, you can create additional local user accounts as your needs dictate.

Default accounts

In Windows 10, there are three default local user accounts on the computer in the trusted identity store. This is a secure list of users and groups and is stored locally as the Security Accounts Manager (SAM) database in the registry. The three accounts are the Administrator account, the Default Account, and the Guest account.

The default Administrator account cannot be deleted or locked out, but it can be renamed or disabled. When the default administrator account is enabled, it requires a strong password. Another local account called the HelpAssistant account is created and enabled when a Windows Remote Assistance session is run. The HelpAssistant account provides limited access to the computer to the person who provides remote assistance. The HelpAssistant account is automatically deleted if there are no Remote Assistance requests pending.

When you install Windows 10 using a local account, you can create additional user accounts and give these accounts any name that is valid. To be valid, the username

- Must be from 1 to 20 characters
- Must be unique among all the other user and group names stored on the computer
- Cannot contain any of the following characters: / \ [] : ; | = , + ? < > " @
- Cannot consist exclusively of periods or spaces

The initial user account created at installation is a member of the local Administrators group and therefore can perform any local management task on the device. You can view the installed accounts, including the default accounts, by using the Computer Management console, as shown in Figure 2-1. If you cannot find the Local Users And Groups section within Computer Management, then you are probably running Windows 10 Home Edition, which does not have the Local Users And Groups Microsoft Management Console (MMC) snap-in.

You can also use the net user command and the **get-wmiobject -class win32_useraccount** Windows PowerShell cmdlet to list the local user accounts on a device.



EXAM TIP

In Windows 10 Home edition, you must use the User Accounts applet in Control Panel, and you cannot create or manage groups since the Local Users And Groups Console snap-in is not present.

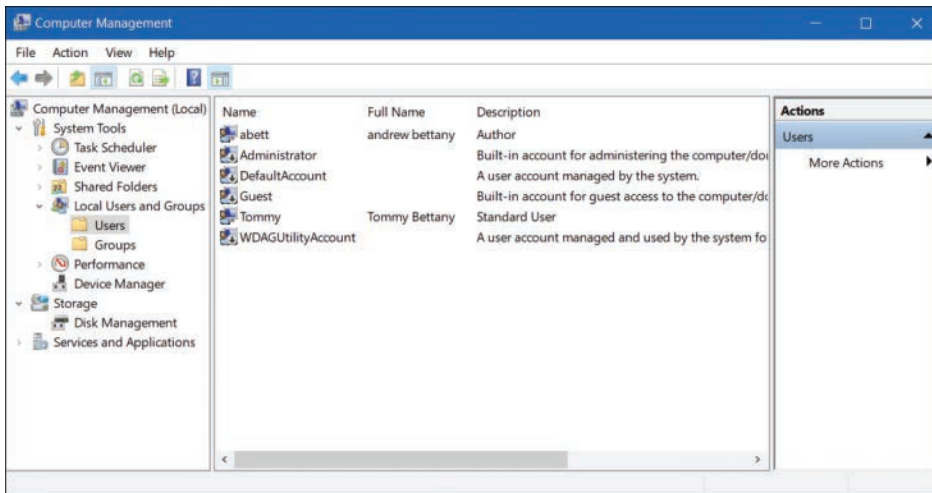


FIGURE 2-1 Viewing built-in user accounts

Manage local user accounts

You can manage local user accounts by using Computer Management (except with Windows 10 Home edition), Control Panel, the Settings app, and Windows PowerShell.

USING COMPUTER MANAGEMENT

To manage user accounts by using Computer Management, right-click **Start** and then select **Computer Management**. Expand the Local Users and Groups node and then select **Users**. To create a new user, right-click the **Users** node and select **New User**.

In the **New User** dialog box, configure the following properties, as shown in Figure 2-2, and then select **Create**.

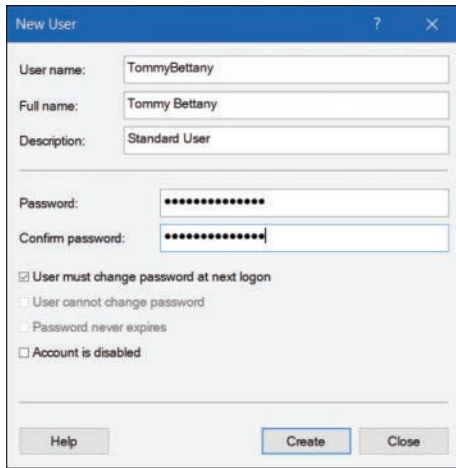


FIGURE 2-2 Adding a user with Computer Management

- User Name
- Full Name
- Password
- User Must Change Password At Next Logon
- User Cannot Change Password
- Password Never Expires
- Account Is Disabled

After you have added the new user account, you can modify more advanced properties by double-clicking the user account. On the General tab, you can change the user's full name and description and password-related options. On the Member Of tab, you can add the user to groups or remove the user from groups. The Profile tab, shown in Figure 2-3, enables you to modify the following properties:

- **Profile Path** This is the path to the location of a user's desktop profile. The profile stores the user's desktop settings, such as color scheme, desktop wallpaper, and app settings (including the settings stored for the user in the registry). By default, each user who signs in has a profile folder created automatically in the C:\Users\Username folder. You can define another location here, and you can use a Universal Naming Convention (UNC) name in the form of \\Server\Share\Folder.

- **Logon Script** This is the name of a logon script that processes each time a user signs in. Typically, this will be a BAT or CMD file. You might include commands that map network drives or load apps in this script file. Assigning logon scripts in this way is not usually done. Instead, Group Policy Objects (GPOs) are used to assign logon and startup scripts for domain user accounts.
- **Home Folder** This is a personal storage area where users can save their personal documents. By default, users are assigned subfolders within the C:\Users\Username folder for this purpose. However, you can use either of the following two properties to specify an alternate location:
 - **Local Path** A local filesystem path for storage of the user's personal files. This is entered in the format of a local drive and folder path.
 - **Connect** A network location mapped to the specified drive letter. This is entered in the format of a UNC name.

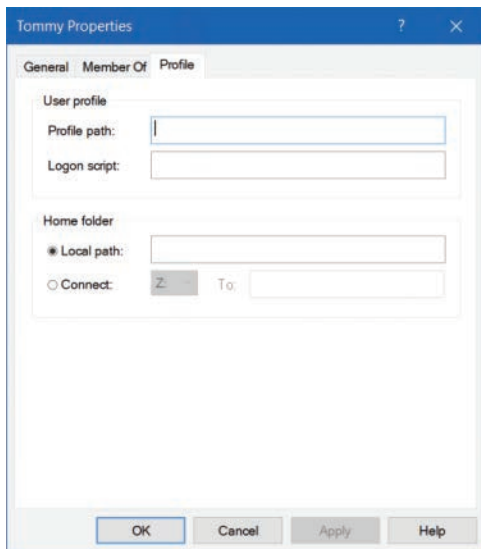


FIGURE 2-3 Modifying the profile properties for a user

USING CONTROL PANEL

You can also manage user accounts by opening Control Panel, clicking User Accounts, and then clicking User Accounts again. From here, you can do the following:

- **Make changes to my account in PC settings** Launches the Settings app to enable you to make user account changes
- **Change your account type** Enables you to switch between Standard and Administrator account types
- **Manage another account** Enables you to manage other user accounts on this computer
- **Change User Account Control settings** Launches the User Account Control Settings dialog box from Control Panel

If you are an administrator and you select another local user, you can perform these tasks:

- **Change the account name** Enables you to change your account name.
- **Change the password** Lets you change the password for the user and provide a password hint
- **Change your account type** Enables you to switch between Standard and Administrator account types
- **Delete the account** Allows you to delete the user account and optionally any files associated with their account
- **Manage another account** Enables you to manage other user accounts on this computer

You cannot add new accounts from Control Panel. If you want to add a new local account, use Computer Management, Windows PowerShell, or Add A Family Member in the Family And Other Users section of the Settings app.

USING THE SETTINGS APP

The preferred way to manage local accounts in Windows 10 is by using the Settings app. From Settings, select Accounts. As shown in Figure 2-4, on the Your Info tab, you can modify your account settings, including these:

- **Sign in with a Microsoft account instead** You can sign out and sign in using a Microsoft account.
- **Create your picture** You can browse for an image or take a selfie if your device has a webcam.
- **Creating a Microsoft account** You can create a new Microsoft account using this option.

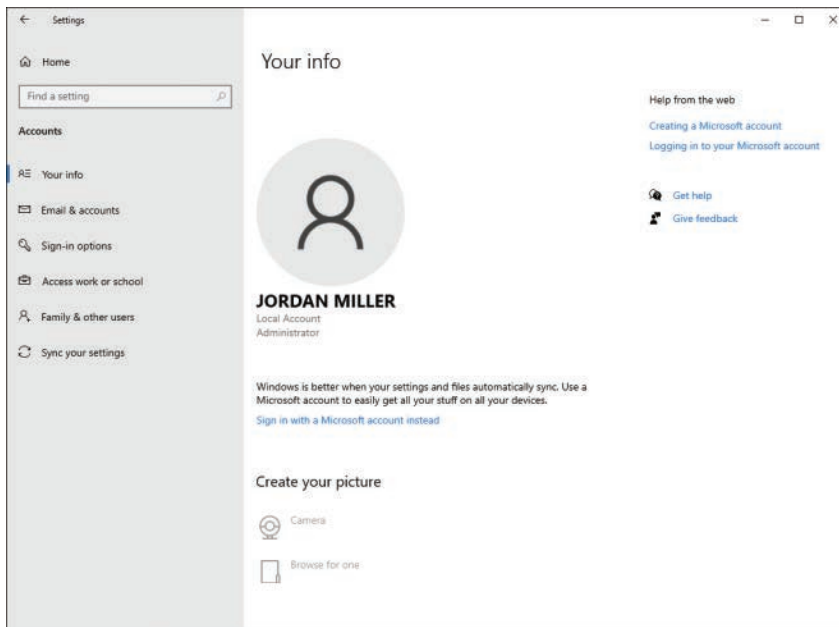


FIGURE 2-4 Modifying your user account properties in the Settings app

If you need to add a new local user account, select the Family & Other Users section and then select Add Someone Else To This PC.

Windows 10 requires you to then enter that person's email address, typically the address they use to sign in to Office 365, OneDrive, Skype, Xbox, or Outlook.com.

If you do not have the recipient's email address, you can still add a local account by using the following procedure:

1. In the **Settings** app, select **Accounts**.
2. On the **Family & other users** tab, under **Other users**, select **Add someone else to this PC**.
3. In the **How will this person sign in** dialog box, select **I don't have this person's sign-in information**.
4. In the **Create account** dialog box, select **Add a user without a Microsoft account**.
5. On the **Create an account for this PC** page, type the username, enter a new password twice, provide answers to the three security questions, and then select **Next** to create the local account. The account is listed under **Other users**.

USING WINDOWS POWERSHELL

You can view local user accounts using Windows PowerShell, but to add or modify local accounts, you will need to run the cmdlets with elevated privileges.

You can use the following cmdlets to manage local user accounts:

- **Get-LocalUser** Gets local user accounts
- **New-LocalUser** Creates a local user account
- **Remove-LocalUser** Deletes a local user account
- **Rename-LocalUser** Renames a local user account
- **Disable-LocalUser** Disables a local user account
- **Enable-LocalUser** Enables a local user account
- **Set-LocalUser** Modifies a local user account

For example, to add a new local user account called User 03 with a password, run the following cmdlets:

```
$Password = Read-Host -AsSecureString
<<Enter Password>>
New-LocalUser "User03" -Password $Password -FullName "Third User" -Description "User 3"
```

NEED MORE REVIEW? LOCAL ACCOUNTS CMDLETS

To review further details about using Windows PowerShell to manage local accounts, refer to the Microsoft PowerShell reference at <https://docs.microsoft.com/powershell/module/microsoft.powershell.localaccounts/?view=powershell-5.1>.

Manage local groups

There are several built-in groups with Windows 10, which provide an easy way for users to be granted the same permissions and rights as other group members. Assigning permissions to groups is usually more efficient than applying them to individual users.

You use the Computer Management console, or if you are an administrator, you can create a custom Microsoft Management Console (MMC) and add the Local Users And Groups snap-in, as shown in Figure 2-5, to create and manage local groups.

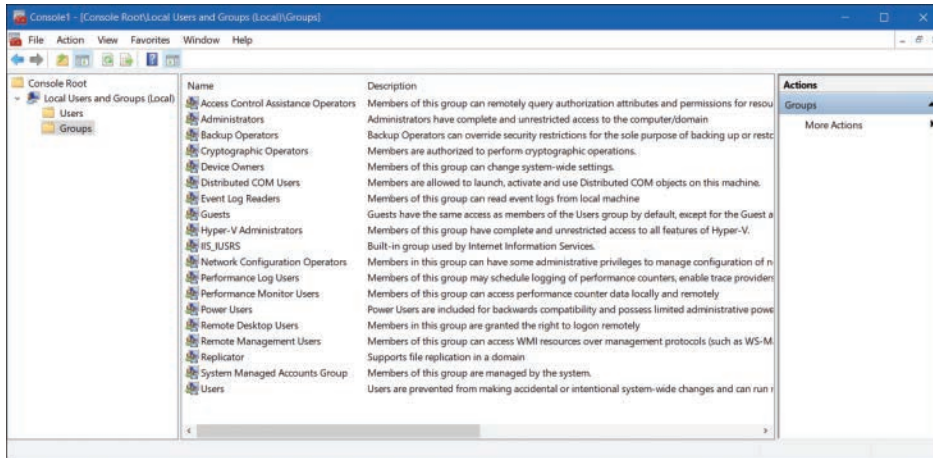


FIGURE 2-5 Default groups in Windows 10

In Figure 2-5, you can see the default built-in local groups (such as Administrators and Device Owners) and a description for each. These built-in groups already have the necessary permissions associated to them to accomplish specific tasks.

If you select the Users or Administrators group, you should see members that you recognize. Administrators have complete and unrestricted access to the computer, whereas users are unable to make accidental or intentional systemwide changes, but they can run most applications that have already been installed on a device.

Built-in local groups

You can add your own groups, change group membership, rename groups, and delete groups. It is best practice to use the built-in groups wherever possible because they already have the appropriate permissions and are familiar to other administrators. Some built-in local groups are special groups that the Windows 10 system requires (and cannot be managed).

Some of the local groups created on Windows 10 devices, together with their uses, are shown in Table 2-1.

TABLE 2-1 Built-in local groups

Local Group	Description
Access Control Assistance Operators	Members of this group can remotely query authorization attributes and permissions for resources on the computer.
Administrators	The Administrators group has full permissions and privileges on a Windows 10 device. Members can manage all the objects on the computer. The Administrator and initial user accounts are members of the Administrators local group.
Backup Operators	Backup Operators group members have permissions to back up and restore the file system regardless of any NTFS permissions. Backup Operators can access the file system only through the Backup utility.
Cryptographic Operators	The Cryptographic Operators group has access to perform cryptographic operations on the computer.
Device Owners	Members of this group can change systemwide settings to the computer.
Distributed COM Users	The Distributed COM Users group can launch and run Distributed COM objects on the computer.
Event Log Readers	Event Log Readers group members can read the event log on the local computer.
Guests	The Guests group has very limited access to the computer. In most cases, administrators disable guest access because guest access can pose a potential security risk; instead, most administrators prefer to create specific users. By default, the Guest user account is a member of the Guests local group.
Hyper-V Administrators	Members of this group have complete and unrestricted access to all features of Hyper-V if this feature has been installed.
IIS_IUSRS	The IIS_IUSRS group is used by Internet Information Services (IIS). By default, the NT AUTHORITY\IUSR user account, used by IIS, is a member of the IIS_IUSRS group.
Network Configuration Operators	Members of the Network Configuration Operators group can manage the computer's network configuration.
Performance Log Users	The Performance Log Users group can access and schedule logging of performance counters and create and manage trace counters on a device.
Performance Monitor Users	The Performance Monitor Users group can access and view performance counter information on a device. Members of this group can access performance counters both locally and remotely.
Power Users	The Power Users group is included in Windows 10 for backward compatibility only. Power Users was a group used on computers running Windows XP and granted members limited administrative rights.
Remote Desktop Users	The Remote Desktop Users group members can log on remotely using the Remote Desktop service.
Remote Management Users	Members of this group can access WMI resources over management protocols (such as WS-Management via the Windows Remote Management service). This applies only to WMI namespaces that grant access to the user.
Replicator	The Replicator group supports directory replication, which is a feature used by domain controllers.

Local Group	Description
System Managed Accounts Group	Members of this group are managed by the system.
Users	The Users group is used for end users who require very limited system access. On a fresh copy of Windows 10, members of the Users group are unable to compromise the operating system or program files. By default, all users who have been created on a device, except Guest users, are members of the Users local group.

As Table 2-1 shows, Administrators group members have full permissions and privileges on a Windows 10 device. A member of the Administrators local group can perform the following tasks:

- Access any data on the computer
- Assign and manage user rights
- Back up and restore all data
- Configure audit policies
- Configure password policies
- Configure services
- Create administrative accounts
- Create administrative shares
- Increase and manage disk quotas
- Install and configure hardware device drivers
- Install applications that modify the Windows system files
- Install the operating system
- Install Windows updates, service packs, and hot fixes
- Manage disk properties, including formatting hard drives
- Manage security logs
- Modify groups and accounts that have been created by other users
- Modify systemwide environment variables
- Perform a system restore
- Reenable locked-out and disabled user accounts
- Remotely access the registry
- Remotely shut down the system
- Stop or start any service
- Upgrade the operating system

Create and delete groups

Only members of the Administrators group can manage users and groups. When creating a new group, keep in mind that the group name has to be unique on the local computer and cannot be the same as a local username that exists on the computer.

You should make the group name descriptive, and wherever possible, you include a description of the new group's function. Group names can have up to 256 characters in length and include alphanumeric characters such as spaces, but the backslash (\) is not allowed.

To create a new group, follow these steps:

1. Right-click **Start** and select **Computer Management**.
2. Open the **Local Users and Groups** console.
3. Right-click the **Groups** folder and select **New Group** from the context menu.
4. In the **New Group** dialog box, enter the group name. (Optionally, you can enter a description for this group.)
5. To add group members, select the **Add** button.
6. In the **Select Users** dialog box, type the username, then select **OK**. In the **New Group** dialog box, you will see that the user has been added to the group.
7. To create the new group, select the **Create** button.

To delete a group from the Local Users And Groups console in Computer Management, right-click the group name and choose Delete from the context menu. You will see a warning that deleting a group cannot be undone, and you should select the Yes button to confirm the deletion of the group.

When a group is deleted, all permissions assignments that have been specified for the group will be lost.

Special identity groups

Several special identity groups (sometimes known as special groups) are used by the system or by administrators to allocate access to resources. Membership in special groups is automatic, based on criteria, and you cannot manage special groups through the Local Users And Groups console. Table 2-2 describes the special identity groups that are built into Windows 10.

TABLE 2-2 Built-in special identity groups

Special Identity Group	Description
Anonymous Logon	When a user accesses the computer through an anonymous logon, such as via special accounts created for anonymous access to Windows 10 services, they become members of the Anonymous Logon group.
Authenticated Users	This is a useful group because it includes all users who access Windows 10 using a valid username and password.
Batch	This group includes users who log on as a batch job operator to run a batch job.
Creator Owner	The Creator Owner is the account that created or took ownership of an object, such as a file, folder, printer, or print job. Members of the Creator Owner group have special administrator-level permissions to the resources over which they have ownership.
Dialup	This group includes users who log on to the network from a dial-up connection.

Special Identity Group	Description
Everyone	This group includes anyone who accesses the computer. This includes all users, including Guest accounts and all users that are within a domain or trusted domains. Members of the Anonymous Logon group are not included as a part of the Everyone group.
Interactive	This group includes all users who use the computer's resources locally and those who are not using the computer's resources remotely via a network connection.
Network	This group includes users who access the computer's resources over a network connection.
Service	This group includes users who log on as a user account that is used to run a service.
System	When Windows 10 needs to access internal functions, it can perform actions as a system user. The process being accessed by the operating system becomes a member of the System group.
Terminal Server User	This group includes users who log on through Terminal Server applications.

Manage users, groups, and devices in Active Directory Domain Services

Once a network grows larger than a few computers, companies and enterprises configure networks as a domain or directory. A large network is managed by using a domain. On-premises environments will use Active Directory Domain Services (AD DS) and cloud-based environments use Azure Active Directory (Azure AD). Using both on-premises and cloud resources is referred to as a *hybrid model*. Both directory services are responsible for identity-related management. User and device information is stored in a directory, which creates a logical, hierarchical organization of information, represented as objects.

Users are aware that they are part of an Active Directory domain because they will access shared resources by signing into their device using a domain username and password such as `user@contoso.com` rather than a local or Microsoft account.

AD DS can store millions of objects that can be managed and controlled. Objects typically include shared resources such as servers, volumes, printers, and the network user and computer accounts. AD DS also simplifies the administration of user accounts and stores information about them, such as names, passwords, phone numbers, or information about a computer, like the device name or the last user logged on.

One or more Windows servers can be configured with the domain controller role, which then stores the directory and allows administrators to manage AD DS objects using a console app, such as Active Directory Administrative Center (ADAC).

You will learn later in this chapter how user or computer objects' properties can also be configured by using local policies or managed at scale by using Group Policy Objects. Computers that are managed by Active Directory are referred to as *domain joined*.

Use Active Directory users

Within Active Directory (AD), there are two primary objects that you need to know: user accounts and computer accounts. These are two forms of common security principals held in AD, and they allow you to manage the account and control access to resources by the entity (a person or a computer). Within a domain you will create domain user accounts for the person in most scenarios. A domain user will use their domain username and password to sign in to any device on the domain-based network (with the correct permissions). This approach allows administrators to centrally manage user accounts across an organization rather than on each individual device, as with a workgroup environment.

Use Active Directory groups

Active Directory groups allow you to collect user accounts, computer accounts, and other groups into units that can be managed. By controlling groups of objects, administrators can manage permissions to resources at scale. It is best practice for users and other objects to be added to a group and then permissions set at the group level, rather than at the user or computer object level. This way, if a specific user or computer account joins or leaves the organization, the group membership can be dynamically updated by Active Directory. A huge amount of time and effort is therefore saved every time a personnel change occurs.

Two types of groups are available in Active Directory:

- **Distribution groups** Used to create email distribution lists used by email applications, such as Exchange Server, to send emails to the group membership. It is not possible to configure security permissions on distribution groups.
- **Security groups** Used to assign rights and permissions to objects within the group.

User rights are assigned to a security group to determine what members of that group can do using their user account. For example, you may want to add a user to the Backup Operators group in Active Directory. The user will then be granted the ability to back up and restore files and directories that are located on each file server or domain controller in the domain.

Permissions are assigned to the shared resource. Best practice is to assign the permissions to a security group and allow AD to determine who can access the resource and the level of access whenever the resource is accessed. The level of access can be fine-tuned using access control entries (ACEs), such as Full Control or Read, which are stored in the discretionary access control list (DACL) for each resource. The DACL defines the permissions on resources and objects such as file shares or printers.

Active Directory default security groups

You can use several built-in groups with Active Directory. Some commonly used security groups are shown in Table 2-3.

TABLE 2-3 Built-in Active Directory security groups

AD Security Group	Description
DnsAdmins	Members of this group have administrative access to the DNS Server service.
Domain Admins	Domain Admins are the designated administrators of the domain. Present on every domain-joined computer within the local Administrators group. Receives rights and permissions granted to the local Administrators group and to the domain's Administrators group.
Domain Computers	All computers and servers that are joined to the domain are members of this group.
Domain Users	All users in the domain.
Enterprise Admins	Enterprise Admins have permissions to change forest-wide configuration settings. Enterprise Admins are members of the domain's Administrators group and receive rights and permissions granted to that group.
IIS_IUSRS	The IIS_IUSRS group is used by Internet Information Services (IIS). By default, the NT AUTHORITY\IUSR user account, used by IIS, is a member of the IIS_IUSRS group.
Print Operators	Members can administer domain-based printers.
Remote Desktop Users	The Remote Desktop Users group members can log on remotely using the Remote Desktop service.

Understand Active Directory

A detailed knowledge of Windows Server and AD DS is outside the scope of the MD-100 exam, but you should know the difference between an on-premises environment and a cloud-based one. Active Directory Domain Services (AD DS), commonly referred to as Active Directory (AD), is a role of associated services that are installed on physical or virtual Windows servers. Simply hosting a Windows Server running the AD DS role on an Azure-based virtual machine is an example of a “lift and shift” deployment to the cloud running AD DS and does not provide an Azure Active Directory (Azure AD) environment.

Windows Server installed with the AD DS role is a complex environment that has benefited organizations for over 20 years and, as such, has many legacy components necessary to support AD feature backward compatibility. In addition to the directory service, technologies are often provisioned when you add the AD DS role to a Windows server, including:

- Active Directory Certificate Services (AD CS)
- Active Directory Lightweight Directory Services (AD LDS)
- Active Directory Federation Services (AD FS)
- Active Directory Rights Management Services (AD RMS)

Active Directory Domain Services has the following characteristics (which are not shared by Azure AD):

- AD DS is a true directory service, with a hierarchical X.500-based structure.
- AD DS uses Domain Name System (DNS) for locating resources.

- You can query and manage AD DS using Lightweight Directory Access Protocol (LDAP).
- The Kerberos protocol is primarily used for AD DS authentication.
- Computer objects represent computers that join an Active Directory domain.
- You can manage objects stored in the directory using organizational units (OUs) and Group Policy Objects (GPOs).
- You can establish trusts between domains for delegated management.

Manage devices in directories

Microsoft has designed Windows 10 to be managed using cloud-based tools such as Microsoft Intune for remote device management. As more businesses migrate away from traditional on-premises domain environments to the cloud, you will need to understand how to configure devices to register them in Azure Active Directory.

In this section, you will learn how to register a device so that it can be managed by a business or a school using cloud-based services. You will see how to enable Device Registration and the process of joining devices to Azure Active Directory.

Understand device management

Once devices are managed by Azure Active Directory (Azure AD), you can ensure that your users are accessing your corporate resources from devices that meet your standards for security and compliance. To protect devices and resources using Azure AD, users must be allowed to have their Windows 10 devices managed by Azure AD.

Azure AD is a cloud-based identity authentication and authorization service that enables your users to enjoy the benefits of single sign-on (SSO) for cloud-based applications, such as Office 365. Users can easily join their devices to your organization's Azure AD once you have enabled device joining in the Azure Active Directory Admin Center.

When you are joining devices to an on-premises domain environment, the types of devices that you can join to the domain are quite restrictive; devices, for example, must be running a supported operating system. This means that any users who have devices running Windows 10 Home editions cannot join the company's on-premises domain. However, Azure AD is less restrictive in this respect; you can add to Azure AD almost any tablet, laptop, smartphone, and desktop computer running a variety of platforms. When you enable users to add their devices to Azure AD, you will manage their enrolled devices by using a mobile device management solution, such as Microsoft Intune, which allows you to manage and provision your users' devices.

Devices can be managed by Azure AD using two methods:

- Joining a device to Azure AD
- Registering a device to Azure AD

AZURE AD–JOINED DEVICE

Joining a Windows 10 device to Azure AD is like registering a device with Azure AD, but it allows enhanced management capabilities. Once a device has been joined to Azure AD, the local state of a device changes to enable your users to sign into the device using the work or school account instead of a personal account.

An enterprise will typically join its owned devices to Azure AD to allow for cloud-based management of the devices and to grant access to corporate apps and resources.

NOTE BULK-JOIN DEVICES TO AZURE AD

Bulk joining of devices to Azure AD and Windows Autopilot deployment are outside the scope of the MD-100 Windows 10 exam, though you should expect to find these topics covered in the MD-101 Managing Modern Desktops exam.

Organizations of any size can deploy Azure AD Join. Azure AD Join works well in a cloud-only (no on-premises infrastructure) environment. When Azure AD Join is implemented in a hybrid environment, users gain access to both cloud and on-premises apps and resources.

Azure AD–joined devices allow your users to access the following benefits:

- **Single-Sign-On (SSO)** Allows users simplified access to Azure managed SaaS apps, services, and work resources.
- **Enterprise-compliant roaming** User settings can be kept in sync across joined devices using their Azure AD–joined devices (without the need to sign in using a Microsoft account).
- **Access to Microsoft Store for Business** Users can access a Microsoft Store populated with apps chosen by your organization.
- **Windows Hello** Devices can be secured using the enterprise features of Windows Hello.
- **Restriction of access** Devices will only be able to access apps that meet the organizational compliance policy.
- **Seamless access to on-premises resources** Hybrid Azure AD–joined devices can access on-premises resources when connected to the domain network.

Organizations that already have Microsoft 365 or other SaaS apps integrated with Azure AD have the necessary components in place to have devices managed in Azure AD instead of being managed in Active Directory.

AZURE AD–REGISTERED DEVICES

Once a device is registered into management, it is “known” to Azure AD, and information relating to the device is stored in Azure AD. Effectively, the device is given an identity with Azure AD. You can create conditional access rules to determine whether access to resources from your devices will be granted.

Azure AD–registered devices enable users to use personally owned devices to access your organization’s resources in a controlled manner. Azure AD supports bring-your-own-device (BYOD) scenarios for several types of devices, including devices running Windows 10, iOS, Android, and macOS.

With an Azure AD–registered device, the user will gain access to resources using a work or school Azure AD account at the time they access the resources. All corporate data and apps will be kept completely separated from the personal data and apps on the device. If the personal computer, tablet, or phone that is registered with Azure AD does not meet your corporate standards for security and compliance—for example, if a device is not running a supported version of the operating system, or it has been jail broken—then access to the resource will be denied.

Device Registration enables you to facilitate an SSO experience for users, removing the need for them to repeatedly enter credentials to access resources.

The main reasons to implement Device Registration are:

- To enable access to corporate resources from non-domain joined or personally owned devices
- To enable SSO for specific apps and/or resources managed by Azure AD

After you enable Device Registration, users can register and enroll their devices in your organizational tenant. After they have enrolled their devices:

- Enrolled devices are associated with a specific user account in Azure AD.
- A device object is created in Azure AD to represent the physical device and its associated user account.
- A user certificate is installed on the user’s device.

Configure device management

Device management requires configuration to ensure that when your users attempt Device Registration, the process will not fail. By default, the setting is enabled, and it allows all Windows 10 devices that present valid credentials to be managed by your Azure AD.

The Azure portal provides a cloud-based location to manage your devices. To allow registration of devices into Azure AD, follow these steps:

1. Sign in as an administrator to the Azure portal at <https://portal.azure.com>.
2. On the left navigation bar, select **Azure Active Directory**.
3. In the **Manage** section, select **Devices**.
4. Select **Device settings**.
5. On the **Device settings** blade, ensure that **Users may join devices to Azure AD** is set to **All**, as shown in Figure 2-6. If you choose **Selected**, then select the **Selected** link and choose the users who can join Azure AD. You can select both individual users and groups of users.
6. Select **Save**.

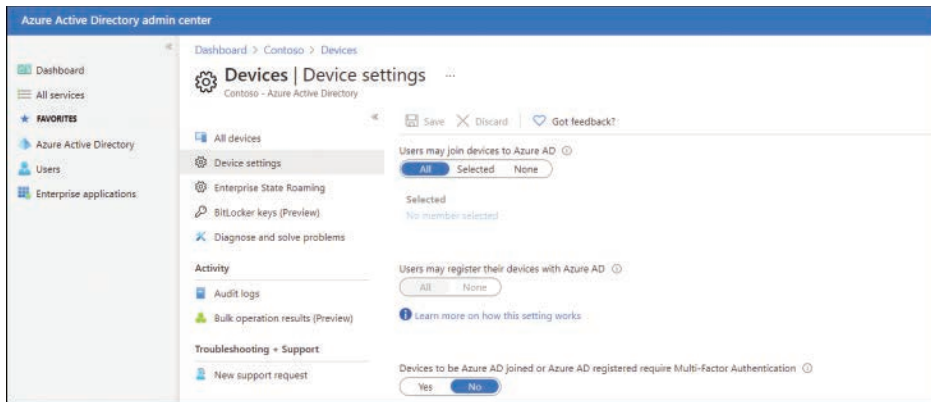


FIGURE 2-6 Enabling Azure AD join

Within the Azure AD portal, you can fine-tune the process of registering and joining devices by configuring the device settings as listed in Table 2-4.

TABLE 2-4 Azure AD device configuration settings

Device Setting	Description
Users May Join Devices To Azure AD	The default is All. The Selected option allows you to select users who can join Windows 10 devices to Azure AD.
Users May Register Their Devices With Azure AD	Required to allow devices to be registered with Azure AD by users. Options include the following: <ul style="list-style-type: none"> ■ None Prevents devices from being registered with Azure AD. ■ All Automatically configured if Enrollment with Microsoft Intune or Mobile Device Management (MDM) for Office 365 is configured as they require Device Registration.
Additional Local Administrators On Azure AD Joined Devices	You can assign the users who are granted local administrator rights on a device and added to the Device Administrators role in Azure AD. By default, global administrators in Azure AD and device owners are granted local administrator rights. Requires an Azure AD Premium license.
Devices To Be Azure AD Joined Or Azure AD Registered Require Multi-Factor Authentication	Choose whether users are required to use multifactor authentication to join their devices to Azure AD. The default setting is No. This setting is only applicable to Azure AD Join on Windows 10 and BYOD registration for Windows 10, iOS, and Android. This setting does not apply to hybrid Azure AD–joined devices, Azure AD–joined VMs in Azure, and Azure AD–joined devices using Windows Autopilot self-deployment mode.
Maximum Number Of Devices Per User	By default, all users can have a maximum of 50 devices in Azure AD. Once this quota is reached, they are not able to add additional devices until one or more of the existing devices are removed. The device quota is across both Azure AD–joined and Azure AD–registered devices.
Enterprise State Roaming	You can configure the Enterprise State Roaming settings for specific users or groups. With Azure AD Premium, you can select a subset of your users and enable this feature for them. Without Azure AD Premium, you can only configure Enterprise State Roaming for all users at once.



EXAM TIP

Each device must be able to locate the internet to allow you to authenticate using your Azure AD credentials. If a device cannot locate the cloud-based identity service, there will be a problem accessing resources managed by Azure AD.

DEVICE MANAGEMENT TASKS

Once devices have been registered or joined to Azure AD, they appear in the list within the All Devices section of the Azure Active Directory Admin Center. Devices managed by another management authority, such as Microsoft Intune, are also listed.

To locate a device, you can search using the device name or device ID. Once you have located a device, you can perform additional device management tasks, including the following:

- **Update devices** You can enable or disable devices. You need to be a global administrator in Azure AD to perform this task, which prevents a device from being able to authenticate with Azure AD and thus prevents the device from accessing any Azure AD resources.
- **Delete devices** When a device is retired, or it no longer requires access to your corporate resources, it should be deleted in Azure AD. Deleting a device requires you to be a global administrator in Azure AD or an Intune administrator. Once deleted, all details stored in Azure AD relating to the device—for example, BitLocker keys for Windows devices—are removed. If a device is managed elsewhere, such as in Microsoft Intune, you should ensure that the device has been wiped before deleting the device in Azure AD.
- **View device ID** Each device has a unique device ID that can be used to search for the device; the unique device ID can be used as a reference if you need to use PowerShell during a troubleshooting task.
- **View device BitLocker key** Windows devices managed by Azure AD can have their BitLocker recovery keys stored in Azure AD. You can access this key if the encrypted drive needs to be recovered. To view or copy the BitLocker keys, you need to be the owner of the device or have one of the following roles assigned: Global Administrator, Help desk Administrator, Security Administrator, Security Reader, or Intune Service Administrator.

NOTE USE POWERSHELL TO BACK UP THE BITLOCKER RECOVERY KEY TO AZURE AD

For Azure AD-joined computers, the BitLocker recovery password should be stored in Azure AD. You can use the PowerShell cmdlets `Add-BitLockerKeyProtector`, `Get-BitLockerVolume`, and `BackupToAAD-BitLockerKeyProtector` to add a recovery password and back it up to Azure AD before enabling BitLocker.

Connect devices to Azure AD

Once the prerequisites have been configured to allow the Device Registration service to take place, you are able to connect devices to Azure AD.

There are three ways to connect a Windows 10 device to Azure AD:

- Joining a new Windows 10 device to Azure AD
- Joining an existing Windows 10 device to Azure AD
- Registering a Windows 10 device to Azure AD

In this section, you will learn the steps required for each method of connecting Windows 10 to Azure AD.

JOIN A NEW WINDOWS 10 DEVICE TO AZURE AD

In this method, we will take a new Windows 10 device and join the device to Azure AD during the first-run experience. The device could have been previously prepared using an enterprise deployment method, or it could have been distributed by the original equipment manufacturer (OEM) directly to your employees.

If the device is running either Windows 10 Professional or Windows 10 Enterprise, the first-run experience will present the setup process for company-owned devices.

NOTE JOINING A DEVICE TO ACTIVE DIRECTORY DURING THE FIRST-RUN EXPERIENCE

Joining an on-premises Active Directory domain is supported in Windows 10 during the Windows Out-of-Box Experience (OOBE). If you need to join a computer to an AD domain, during setup you should choose the option Set Up For An Organization and then select the Domain Join Instead link. You then need to set up the device with a local account and join the domain from the Settings app on your computer. For the MD-100 Windows 10 exam, you should expect that devices will be cloud- or hybrid cloud-enabled.

To join a new Windows 10 device to Azure AD during the first-run experience, use the following steps:

1. Start the new device and allow the setup process.
2. On the **Let's start with region. Is this right?** page, select the regional setting that you need and select **Yes**.
3. On the **Is this the right keyboard layout?** page, select the keyboard layout settings and select **Yes**.
4. On the **Want to add a second keyboard layout?** page, add a layout or select **Skip**.
5. The computer should automatically connect to the internet, but if it does not, you will be presented with the **Let's connect you to a network** page, where you can select a network connection.

6. On the **How would you like to set up?** page, choose **Set up for an organization** and select **Next**.
7. On the **Sign in with Microsoft** page, enter your organization or school account and password and select **Next**.
8. On the **Choose privacy settings for your device**, choose the settings and select **Accept**.
9. On the **Use Windows Hello with your account** page, select **OK**.
10. On the **More information required** page, select **Next**, provide the additional security verification information, and select **Next** again.
11. Depending on organizational settings, your users might be prompted to set up MFA. On the **Keep your account secure** page, select **Next** and set up the Microsoft Authenticator.
12. Depending on organizational settings, your users might be prompted to set up Windows Hello. By default, they will be prompted to set up a PIN. When prompted to set up a PIN, select **Set up PIN**. You should now be automatically signed in to the device, joined to your organization or school Azure AD tenant, and presented with the desktop.

JOIN AN EXISTING WINDOWS 10 DEVICE TO AZURE AD

In this method, we will take an existing Windows 10 device and join it to Azure AD. You can join a Windows 10 device to Azure AD at any time. Use the following procedure to join the device:

1. Open the **Settings** app and then select **Accounts**.
2. In **Accounts**, select the **Access work or school** tab.
3. Select **Connect**.
4. On the **Set up a work or school account** page, under **Alternate actions**, select **Join this device to Azure Active Directory**, as shown in Figure 2-7.
5. On the **Microsoft account** page, enter your email address and select **Next**.
6. On the **Enter password** page, enter your password and select **Sign In**.
7. On the **Make sure this is your organization** page, confirm that the details on screen are correct and select **Join**.
8. On the **You're all set!** page, select **Done**.
9. To verify that your device is connected to your organization or school, check that your Azure AD email address is listed under the **Connect** button, indicating that it is connected to Azure AD.

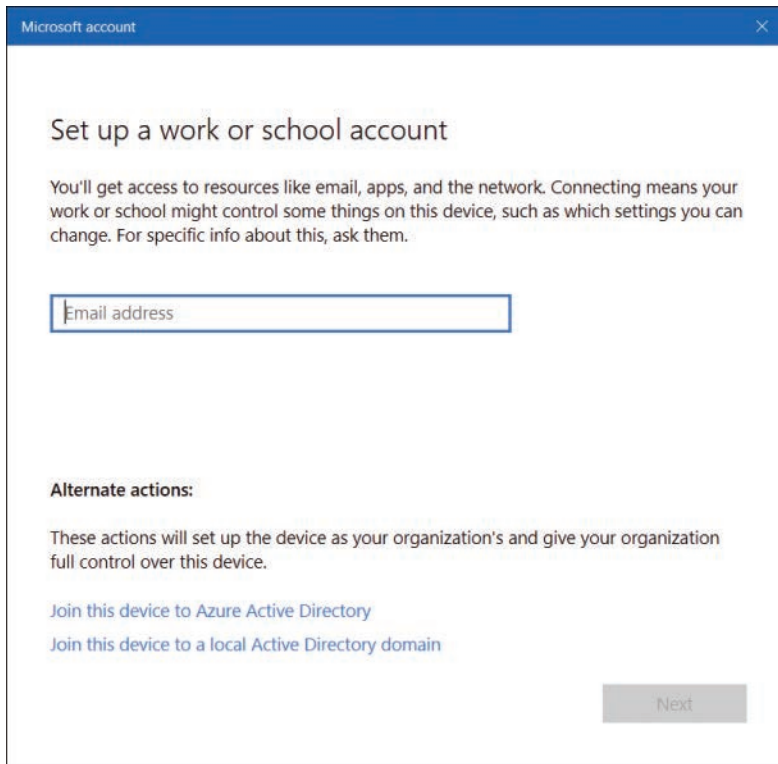


FIGURE 2-7 Joining a device to Azure AD

If you have access to the Azure Active Directory portal, then you can validate that the device is joined to Azure AD by following these steps:

1. Sign in as an administrator to the Azure portal at <https://portal.azure.com>.
2. On the left navigation bar, select **Azure Active Directory**.
3. In the Manage section, select **Devices > All devices**.
4. Verify that the device is listed, as shown in Figure 2-8.

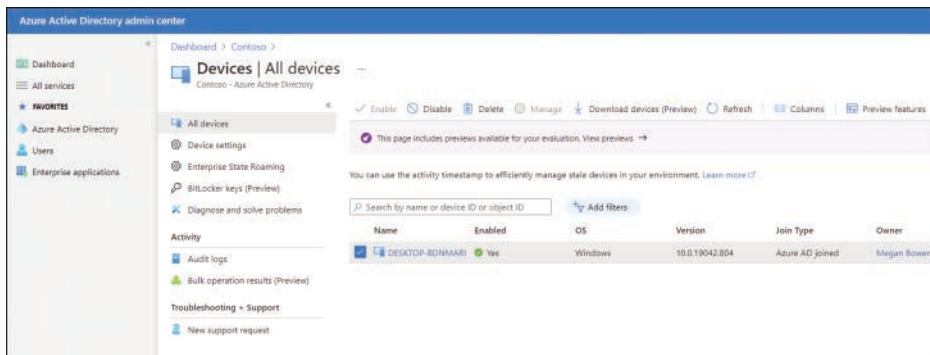


FIGURE 2-8 Viewing All Devices in Azure AD

REGISTER DEVICES TO AZURE AD

You connect a Windows 10 device to Azure Active Directory using the Add Work Or School Account feature found in the Settings app. Device Registration is used to allow devices to be known by both Azure AD and MDM solutions.

In this method, we will take an existing Windows 10 device and register it to Azure AD. Use the following procedure to register the device:

1. Open the **Settings** app and then select **Accounts**.
2. In **Accounts**, select the **Access work or school** tab.
3. Select **Connect**.
4. On the **Set up a work or school account** page, enter your work or school email address, select **Next**, and complete the wizard.

To verify that a device is registered to your organization or school Azure AD tenant, users can use these steps:

1. Open the **Settings** app and then select **Accounts**.
2. In **Accounts**, select the **Access work or school** tab.
3. On the **Access work or school** page, verify that your organization or school Azure AD email address is listed under the **Connect** button.

NOTE REGISTER BYO DEVICES TO AZURE AD

You can register a personally owned device with Azure AD using the Set Up A Work Or School Account Wizard. Personal devices are then known to Azure AD but are not fully managed by the organization.

Enroll devices into Microsoft 365

Microsoft 365 is a bundled subscription that includes Office 365, Windows 10, and Enterprise Mobility + Security. Microsoft 365 comes in three primary bundles:

- **Microsoft 365 Business Premium** For small and medium-sized organizations up to 300 users
- **Microsoft 365 Enterprise** For organizations of any size
- **Microsoft 365 Education** For educational establishments

With Microsoft 365, you use Azure Active Directory for your identity and authentication requirements, and you can (and should) enroll Windows 10 into device management so that your users can gain access to corporate resources. Once devices are joined to your Microsoft 365 tenant, Windows 10 becomes fully integrated with the cloud-based services offered by

Office 365 and Enterprise Mobility + Security. Microsoft 365 supports other platforms, including Android and iOS, which can also be managed as mobile devices. However, only Windows 10 devices can be joined to Azure AD.

NOTE MICROSOFT 365 BUSINESS PREMIUM DOES NOT INCLUDE WINDOWS 10

The Microsoft 365 Business Premium subscription includes Office 365 Business and Enterprise Mobility + Security, but it does not include Windows 10. However, the Microsoft 365 Business Premium subscription does allow businesses to upgrade their existing Windows 7 Professional, Windows 8 Pro, or Windows 8.1 Pro devices to Windows 10 Pro. Windows 10 Pro is then provided with a Windows 10 Business license, which enables businesses to use the set of cloud services and device management capabilities included with Microsoft 365 Business Premium.

ENROLL DEVICES INTO MICROSOFT 365 BUSINESS

When you enroll Windows devices into Microsoft 365 Business, they must be running Windows 10 Pro, version 1703 (Creators Update) or later. If you have any Windows devices running Windows 7 Professional, Windows 8 Pro, or Windows 8.1 Pro, the Microsoft 365 Business subscription entitles you to upgrade them to Windows 10 Pro.

Microsoft 365 Business includes a set of device-management capabilities powered by Microsoft Endpoint Manager. Microsoft 365 Business offers organizations a simplified management console that provides access to a limited number of device management tasks, including the following:

- Deploy Windows with Autopilot
- Remove company data
- Factory reset
- Manage office deployment

To enroll a brand-new device running Windows 10 Pro into Microsoft 365 Business, known as a “user-driven enrollment,” follow these steps:

1. Go through Windows 10 device setup until you get to the **How would you like to set up?** page, as shown in Figure 2-9.

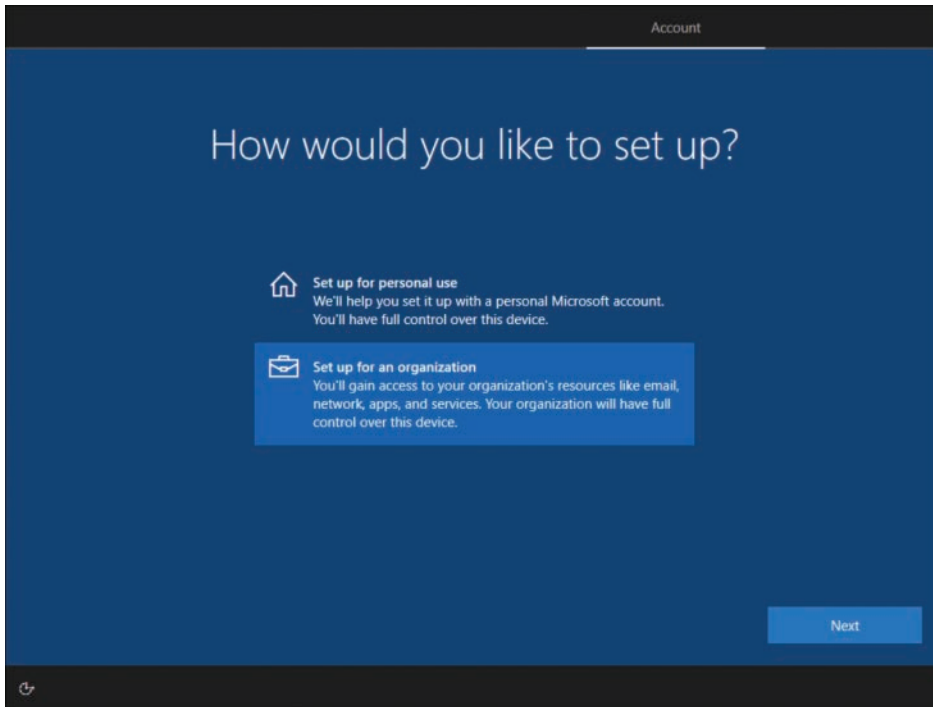


FIGURE 2-9 Windows 10 device setup

2. Choose **Set up for an organization** and then enter your username and password for your Microsoft 365 Business Premium subscription (the new user account, not the tenant admin account).
3. Complete the remainder of the Windows 10 device setup.
4. The device will be registered and joined to your organization's Azure AD, and you will be presented with the desktop. You can verify the device is connected to Azure AD by opening the **Settings** app and clicking **Accounts**.
5. On the **Your Info** page, select **Access Work or School**.
6. You should see that the device is connected to your organization. Select your organization name to show the **Info** and **Disconnect** buttons.
7. Select **Info** to see that your device is managed by your organization and to view your device sync status.
8. To verify that the device has been granted a Windows 10 Business license, select the **Home** icon, select **System**, and then select **About**.
9. In the **Windows specifications** section, the Windows Edition shows Windows 10 Business, as shown in Figure 2-10.

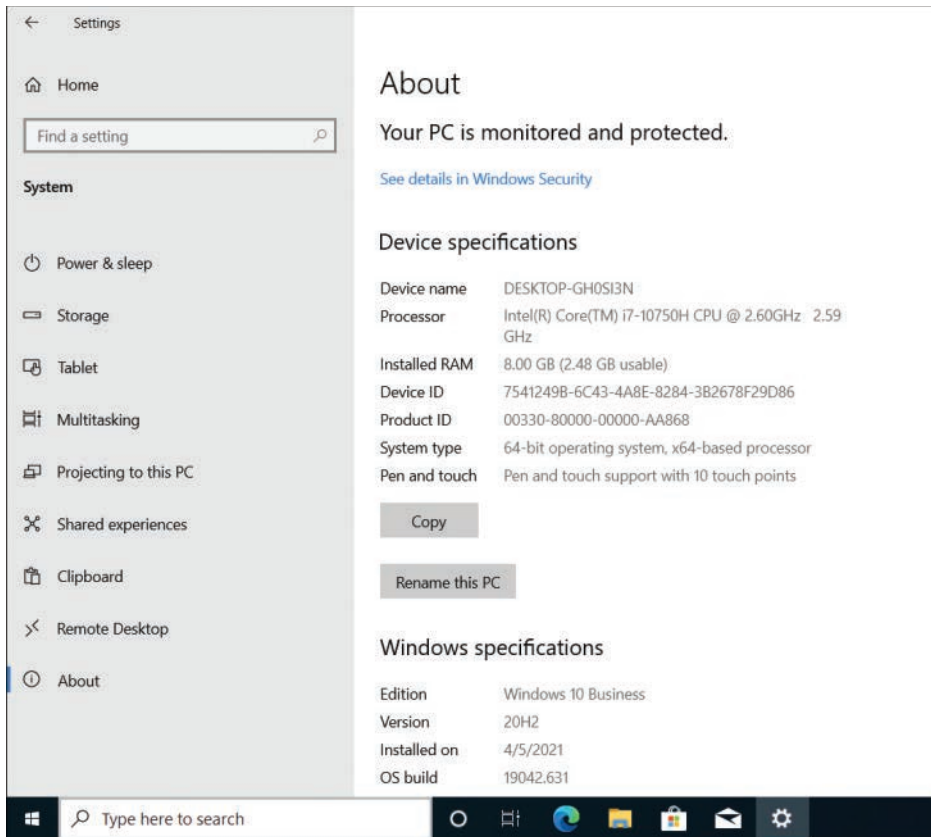


FIGURE 2-10 Windows 10 device setup

Although there is no link to Microsoft Intune within the Microsoft 365 Business Admin Center, the subscription includes the use of the full MDM capabilities for iOS, Android, macOS, and other cross-platform device management. To access the Microsoft Endpoint Manager admin center, launch a browser and sign in with your Microsoft 365 Business Premium credentials at <https://endpoint.microsoft.com>.

To access Intune App Protection in the Azure portal and view the app protection settings for managed Windows 10, Android, and iOS devices, follow these steps:

1. Sign in to the Microsoft Endpoint Manager admin center at <https://endpoint.microsoft.com> with your Microsoft 365 Business admin credentials.
2. In the left navigation bar, select **Apps**.
3. In the **Apps** blade, select **App protection policies**.
4. You can now select **Create policy** from the menu and configure **App Protection Policies**.

Index

Numerics

- 32-bit version, 4–5
- 64-bit version, 4–5

A

- account lockout policy, 153
- Action Center, 45
 - notifications, 47–49
 - Quick Action tiles, 45–47
- activation, 69, 72
 - after reinstalling Windows 10, 74
 - checking status, 73
 - common errors, 75–76
 - first-time, 74
 - refurbished devices running Windows 10, 74–75
 - selecting a method, 69–70
 - troubleshooting, 72, 74
 - using the Activation troubleshooter, 75
 - virtual machines, 72
 - volume activation services, 71
 - troubleshooting, 72–73
- AD (Active Directory), 119
 - computer accounts, 119
 - distribution groups, 119
 - security groups, 119–120
 - user accounts, 119
- AD DS (Active Directory Domain Service), 118, 120–121
- ADK (Assessment and Deployment Kit), 12, 14
- Allow and Deny permissions, 247
- AMSI (Antimalware Scan Interface), 170
- APIPA (Automatic Private IP Address), 215
- apps
 - allowing through Windows Defender Firewall, 173–174
 - Universal Windows, 94–95, 96–98
- audit policy, 154–155

- authentication. *See also* MFA (multifactor authentication)
 - multifactor, 138, 139–141
 - protocols, 226–227
 - remote user, 226–227
 - Windows Admin Center, 413
- automatic device driver installation, 327–328
- Azure AD, 121
 - connecting devices, 126
 - join a new Windows 10 device, 126–127
 - join an existing Windows 10 device, 127–128
 - device management, 121, 123–125
 - device registration, 123, 129
 - joined devices, 122
 - registered devices, 122–123

B

- backup and recovery, 16
 - BitLocker and, 195
 - configuring a recovery drive, 305–306
 - creating a system image backup, 315–316
 - encrypted files, 183–185
 - File History, 297–299
 - restoring data, 299–300
 - support for encryption, 300–301
 - Fresh Start, 315
 - Previous Versions, 301–302
 - recovering files from OneDrive, 302–304
 - Reset This PC, 313–315
 - scheduling backups, 293
 - startup and, 321–322
 - System Restore, 306–308
 - identifying affected apps and files, 308–309
 - modifying the task schedule, 309–310
 - WBAdmin, 295

backup and recovery

- performing backups, 295–297
- restoring data, 296–297
- Windows RE and, 310–312
- Backup and Restore tool. *See also* data recovery
 - recovering files, 292–295
 - system repair disk, 318–319
- baseline performance, real-time monitoring and, 374
- basic permissions, 245–246
- battery
 - power plans, 78–79
 - power settings, 77–78
- biometric devices, 8
- biometrics, 138–139
- BitLocker, 7, 186–188
 - computer upgrades and, 193–194
 - configuring, 190–191
 - configuring startup key storage and recovery options, 195
 - configuring using command-line tools, 191–192
 - data recovery, 197–198
 - enabling without a TPM, 189–190
 - key protectors, 188–189
 - moving an encrypted drive to another computer, 194
 - PowerShell cmdlets, 192–193
 - recovery key backup, 125
- BitLocker To Go, 195–197
- boot store, 322–324
- built-in local groups, 114–116, 117–118

C

- cellular connections
 - troubleshooting, 223
 - Windows 10 and, 222–223
- checking for updates, 354–355
- Client Hyper-V, 6
- Command Prompt, uninstalling updates, 358–359
- command-line
 - DiskPart, 269–270
 - ipconfig, 232
 - IPv4, configuring, 216–217
 - net share, 260–261
 - permission masks, 248
 - ping, 232
 - Remote Desktop and, 406–407
 - tracert, 232
- computer accounts, 119
- Computer Management, managing local user accounts, 110–111
- Continuum, 6
- Control Panel
 - managing local user accounts, 111–112
 - uninstalling updates, 357
- convertible devices, Tablet mode, 35–36
- Cortana, 6

D

- data access
 - file and folder permissions, 240, 243–244
 - advanced, 246–247
 - Allow and Deny, 247
 - basic, 245–246
 - granting, 248
 - inheritance, 249–250, 251
 - NTFS and ReFS, 245
 - security, 244
 - troubleshooting, 253–255
 - viewing effective access, 251–253
 - shared permissions, 255
 - File Explorer and, 259–260
 - network discovery, 257
 - Shared Folders snap-in, 258–259
 - SMB (Server Message Block), 256–257
 - troubleshooting, 264–266
 - Windows PowerShell and, 261
 - taking ownership of resources, 253
- data collector sets, 370–371, 373
- data indexing, 379–381
- data recovery, 291. *See also* backup and recovery
 - BitLocker, 197–198
 - files, 292–295
- deploying Windows 10, 1–2
 - determine Windows 10 Edition requirements for particular features, 5
 - selecting the appropriate Windows edition, 2–4
 - 32-bit or 64-bit versions, 4–5
 - determine requirements for particular features, 5–8
- deployment rings, 346–347
- desktop
 - customizing, 32, 41–43
 - configuring Start tiles, 36–38
 - export Start layout, 38–41

- grouping Start tiles, 38
- Start menu, 33–35
- support for multiple, 44

device drivers, 324

- automatic installation, 327–328
- disabling updates, 326–327
- driver signing, 334–335
- Driver Store and, 335–336
- packages, 335
 - adding, 339–340
 - downloading, 338–339
 - managing with DISM, 340
- PnPUtil.exe and, 336–338
- removing, 87–88
- rollbacks, 328–329
- support for older hardware, 333–334
- troubleshooting, 330
- updating, 86–87, 326
- verification tools, 330–331
- viewing settings, 332–333

Device Manager, 324–325

devices, 107–108. *See also* Azure AD; printers

- connecting to your Microsoft account, 137
- enrolling to Microsoft 365, 129–130
- enrolling to Microsoft 365 Business, 130–132
- enrolling to Microsoft 365 Enterprise, 133–134
- installing, 84–86, 324–325

disabling, driver updates, 326–327

Disk Cleanup tool, 340

disk management, 267–268

- DiskPart, 269–270
- removable storage, 280
 - formatting, 280
 - securing removable devices, 280–282
- Storage Spaces, 275
 - configuring, 276–278
 - managing with Windows PowerShell, 279–280
 - storage layouts, 275–276
- VHDs, 270–271
 - creating with Disk Management, 272
 - creating with Hyper-V Manager, 272
 - creating with Windows PowerShell, 273–274
- Windows PowerShell and, 268–269

DiskPart, 269–270

distribution groups, 119

DNS (Domain Name System), 212

Driver Store, 335–336

Dynamic Lock, 145

E

EFS (Encrypting File System), 180–181

- file and folder encryption, 181–183
- performing backup and recovery of encrypted files, 183–185

encryption, 180

- EFS (Encrypting File System), 180–181
 - file and folder encryption, 181–183
 - performing backup and recovery of encrypted files, 183–185
 - troubleshooting, 185–186
- File History and, 300–301

enrolling devices

- to Microsoft 365, 129–130
- to Microsoft 365 Business, 130–132
- to Microsoft 365 Enterprise, 133–134

eSIM (embedded SIM), 222

event logs, 359–361

- accessing remotely, 364

Event Viewer, 232

- custom views, 361–362
- subscriptions, 362
 - creating, 363–364
 - viewing, 362–363

F

feature updates, 343

File Explorer, 242–243

- sharing files, 261–263
- sharing folders, 259–260

File History, 297–299

- restoring data, 299–300
- support for encryption, 300–301

file systems

- NTFS, 241
- ReFS, 242
 - selecting, 240–241

files, 243–244. *See also* back up and recovery; shared permissions

- advanced permissions, 246–247
- Allow and Deny permissions, 247
- backing up, 292–293
- basic permissions, 245–246
- encrypting, 181–183
- moving, 251
- NTFS and ReFS permissions, 245

permissions

- OneDrive document version history, 304
- permissions, 240
 - granting, 248
 - inheritance, 249–250
 - troubleshooting, 253–255
 - viewing, 251–253
- recovering, 292
 - using Windows Backup and Restore, 292–295
- recovering from OneDrive, 302–304
- restoring, 294–295
- security permissions, 244
- sharing, 261–263
- folders, 243–244. *See also* back up and recovery; shared permissions
- advanced permissions, 246–247
- Allow and Deny permissions, 247
- backing up, 292–293
- basic permissions, 245–246
- encrypting, 181–183
- moving, 251
- NTFS and ReFS permissions, 245
- permissions, 240
 - granting, 248
 - inheritance, 249–250
 - troubleshooting, 253–255
 - viewing, 251–253
- restoring, 294–295
- security permissions, 244
- sharing, 255–256, 259–261
- formatting removable storage, 280
- Fresh Start, 315

G

- GPOs (Group Policy Objects), 157
 - Remote Assistance and, 401
 - Remote Desktop and, 408
 - Windows Update and, 350–354
- GPRresult command-line tool, 160–161
- granting permissions, 248
- Group Policy(ies), 157
 - configuring Start menu, 41
 - Management Editor, 158–159
 - settings, 158
 - troubleshooting
 - connection issues, 159
 - GPRresult command-line tool, 160–161
 - RSOP (Resultant Set of Policy) tool, 160

H

- hives, 146–147, 387
- Hotspot 2.0 networks, 237
- Hyper-V Manager, creating VHDs, 272

I

- IKEv2 (Internet Key Exchange, Version 2), 226
- indexing options, 379–381
- inheritance, 249–250
- installation, 9–11. *See also* performing a clean installation; post-installation configuration
 - configure Windows for additional regional and language support, 27–28
 - DISM command-line tool, 30
 - local experience packs, 28–29
 - Lpksetup command-line tool, 30–32
 - determine the appropriate installation media, 11–14
 - devices, 324–325
 - methods, 9
 - migrating from previous versions of Windows, 21–22
 - considerations, 23
 - side-by-side migration, 22
 - USMT (User State Migration Tool), 23–27
 - wipe-and-load migration, 22–23
 - perform an in-place upgrade, 14, 15–17
 - in corporate environments, 16
 - supported upgrade paths, 14–15
 - using installation media, 19–20
 - using MDT (Microsoft Deployment Toolkit), 17–18
 - strategies, 11
 - Windows Admin Center, 411–412
- InstantGo, 6
- Internet Explorer, 64–69
- ipconfig command, 232
- IPv4, 212
 - address classes, 213
 - configuring, 215–217
 - default gateway address, 212
 - DNS (Domain Name System), 212
 - public and private addresses, 214–215
 - subnet mask, 212
 - subnets, 212
 - complex networks, 213–214
 - simple networks, 213
- IPv6, 217
 - address types, 217–218

- configuring, 218–219
- name resolution, 219–220
 - advanced DNS settings, 221–222
 - DNS settings, 220–221
- Windows PowerShell networking-related cmdlets, 219

J-K

- joined devices, Azure AD, 122
- Kerberos, 226

L

- L2TP (Layer 2 Tunneling Protocol), 226
- LLTP (Link Layer Topology Discovery), 257
- Local Group Policy, 146
- local groups, 107–108, 114
 - built-in, 114–116
 - special identity groups, 117–118
 - creating, 116–117
 - removing, 117
- Local Security Policy, 150–152
 - account lockout policy, 153
 - configure a password policy, 152–153
 - local policies
 - audit policy, 154–155
 - security options, 157
 - user rights policies, 156
- local users, 107–108
 - default accounts, 108–109
 - local accounts, 108
 - managing using Computer Management, 110–111
 - managing using Control Panel, 111–112
 - managing using Settings app, 112–113
 - managing using Windows PowerShell, 113

M

- MDT (Microsoft Deployment Toolkit), 17–18
- MFA (multifactor authentication), 8, 138, 139
 - biometrics, 138–139
 - Windows Hello, 139–141
 - configure the picture password, 144
 - configuring the PIN, 141–144
 - Dynamic Lock, 145

- Windows Hello for Business, 139
- Microsoft 365, 107
 - device management, 134–135
 - enrolling devices, 129–130
- Microsoft 365 Business, enrolling devices, 130–132
- Microsoft 365 Enterprise, enrolling devices, 133–134
- Microsoft accounts
 - configuring, 136–137
 - connecting to your device, 137
 - limiting the use of, 138
 - signing up for, 137
- Microsoft Edge, 52–57
 - customizing, 57–58
 - extensions, 54–55
 - features, 53–54
 - IE mode, 62–64
 - kiosk mode, 58–62
- Microsoft Store for Business, 95–96
- Microsoft Store, Universal Windows apps, 94–95
- migrating from previous versions of Windows, 21–22
 - considerations, 23
 - side-by-side migration, 22
 - USMT (User State Migration Tool), 23–27
 - wipe-and-load migration, 22–23
- Miracast, 6
- MMC (Microsoft Management Console), remote management and, 397–398
- mobile networking, 222
 - setting up Windows 10 as a mobile hotspot, 224
 - setting up Windows 10 for a cellular data plan, 222–223
- mobility settings, 77
 - configure basic power settings, 77–78, 79
 - power policies, 81–82
 - powercfg.exe, 79–81
 - configure presentation settings, 83–84
 - power plans, 78–79
 - power settings, viewing process power usage, 82–83
- monitoring, Windows Defender Firewall, 172–173
- moving, files and folders, 251

N

- name resolution, 219–220
 - IPv6
 - advanced DNS settings, 221–222
 - DNS settings, 220–221
 - troubleshooting, 233–234

net share command

- net share command, 260–261
- network discovery, 257
- Network Troubleshooter, 233
- networks, 211–212. *See also* IPv4; IPv6
 - mobile, 222
 - setting up Windows 10 as a mobile hotspot, 224
 - setting up Windows 10 for a cellular data plan, 222–223
 - troubleshooting, 231–232
 - name resolution, 233–234
 - tools, 232–233
 - VPNs (virtual private networks)
 - authenticating remote users, 226–227
 - configure using the Settings app, 229
 - creating a connection in Network and Sharing Center, 227–229
 - enabling VPN Reconnect, 230–231
 - profiles, 229–230
 - protocols, 225–226
 - wireless, 234
 - advanced settings, 238
 - configuring, 236–237
 - connecting to, 236
 - Hotspot 2.0, 237
 - modes, 234–235
 - security, 235
 - standards, 235
 - Wi-Fi Direct, 238–240
- notifications, configuring, 47–49
- NSLookup, 232
- NTFS, 241, 247, 265

O

- OneDrive, 7, 282–283
 - document version history, 304
 - Files on Demand, 283–284
 - recovering files, 302–304
 - web portal, 284–285

P

- password policy, 152–153
- Performance Monitor, 369–372
 - commonly tracked objects, 372–373
 - creating data collector sets, 373

- performance monitoring
 - baseline performance and, 374
 - creating a performance baseline, 374–375
 - troubleshooting, 375–377
 - using Performance Monitor and Data Collector Sets, 369–371
 - using Resource Monitor, 366–368
 - using Task Manager, 366
- performing a clean installation, 8–11. *See also*
- post-installation configuration
 - configure Windows for additional regional and language support, 27–28
 - DISM command-line tool, 30
 - local experience packs, 28–29
 - Lpksetup command-line tool, 30–32
 - determine the appropriate installation media, 11–14
 - identify an installation strategy, 11
 - migrating from previous versions of Windows, 21–22
 - considerations, 23
 - side-by-side migration, 22
 - USMT (User State Migration Tool), 23–27
 - wipe-and-load migration, 22–23
 - perform an in-place upgrade, 14, 15–17
 - in corporate environments, 16
 - supported upgrade paths, 14–15
 - using installation media, 19–20
 - using MDT (Microsoft Deployment Toolkit), 17–18
 - using Windows Deployment Services, 17
- permissions, 243–244. *See also* shared permissions
 - advanced, 246–247
 - Allow and Deny, 247
 - basic, 245–246
 - documenting, 255
 - granting, 248
 - inheritance, 249–250, 251
 - NTFS and ReFS, 245
 - security, 244
 - shared, 255, 258–259, 261
 - configuring, 263–264
 - network discovery, 257
 - SMB (Server Message Block), 256–257
 - troubleshooting, 264–266
 - taking ownership of resources, 253
 - troubleshooting, 253–255
 - viewing, 251–253
- ping command, 232
- PINs, configuring for Windows Hello, 141–144
- PnPUtil.exe, 336–338
- policies. *See also* Local Group Policy
 - account lockout, 153

- audit, 154–155
- password, 152–153
- power, 81–82
- user rights, 156
- post-installation configuration, 32
 - configure Action Center, 45, 49–50
 - notifications, 47–49, 50–52
 - Quick Action tiles, 45–47
 - customize the Windows desktop, 32, 41–43
 - configuring Start tiles, 36–38
 - export Start layout, 38–41
 - grouping Start tiles, 38
 - Start menu, 33–35
 - support for multiple desktops, 44
- power settings, 77–78, 79
- power policies, 81–82
- powercfg.exe, 79–81
- viewing process power usage, 82–83
- PPTP (Point-to-Point Tunneling Protocol), 225–226
- presentation settings, 83–84
- Previous Versions, 301–302
- principle of least administration, 247
- Print Management console, 88–90, 377–378
- printers, 88, 377
 - adding and removing, 90
 - managing
 - with Print Management, 377–378
 - with Windows PowerShell, 378–379
 - managing with Windows PowerShell, 91–92
 - Print Management console, 88–90
 - type 4 drivers, 90–91
- profiles, VPN, 229–230
- provisioning packages, 92–93

Q-R

- quality updates, 344
- Quick Assist, 402–404
- recovering, services, 100–101
- recovery drive, configuring, 305–306
- ReFS, 242
- registration, Azure AD devices, 122–123, 129
- registry, 146, 386
 - hives, 146–147, 387
 - keys, 148, 387–388
 - manage settings with PowerShell, 149–150, 389–390
 - structure, 386–387
 - subkeys, 148, 387–388

- values, 148–149, 388
- Registry Editor (Regedit.exe), 149, 388–389
- Reliability Monitor, 381–382
- Remote Assistance, 395–396, 398, 401
 - configuring with GPOs, 401
 - offering help, 400–401
 - requesting help, 398–400
- Remote Desktop, 396–397
 - configuring
 - from the command line, 406–407
 - with GPOs, 408
 - creating and editing connections, 404–406
 - troubleshooting, 408–409
- remote management
 - Remote Assistance and, 401
 - settings, 393
 - System Properties and, 395
 - tools, 392–393
 - using MMC, 397–398
 - using Windows Admin Center, 411
 - Windows Defender Firewall and, 393–395
 - Windows PowerShell and, 409–411
- removable storage, 280
 - formatting, 280
 - securing removable devices, 280–282
- removing
 - device drivers, 87–88
 - local groups, 117
 - printers and print servers, 90
- Reset This PC, 313–315
- Resource Monitor, performance monitoring and, 366–368
- rollbacks, 328–329
- RSOP (Resultant Set of Policy) tool, 160

S

- S mode, 3–4
- SAM (Security Accounts Manager), 108
- scheduled backups, 293
- SDHC (Secure Digital High-Capacity) memory cards, 306
- Secure Boot, 7
- security, 162. *See also* encryption; Windows Security
 - BitLocker, 7, 186–188
 - computer upgrades and, 193–194
 - configuring, 190–191
 - configuring startup key storage and recovery options, 195

- configuring using command-line tools, 191–192
- data recovery, 197–198
- enabling without a TPM, 189–190
- key protectors, 188–189
- moving an encrypted drive to another computer, 194
- PowerShell cmdlets, 192–193
- encryption, File History and, 300–301
- UAC (User Account Control), 165–166
- Windows Defender Antivirus, 199–203
- Windows Defender Firewall, 170–171
 - advanced security, 174–177
 - allowing an app through, 173–174
 - configure connection security rules with IPsec, 177–179
 - creating firewall rules, 179–180
 - Firewall & Network Protection page, 171
 - monitoring, 172–173
 - wireless networks, 235
- services, 98, 382–383
 - configurable options, 384
 - configuring, 99–100
 - dependencies, 101
 - managing
 - from the command line, 384
 - with Windows PowerShell, 385
 - recovering, 100–101
 - startup and, 341–342
 - viewing from Task Manager, 101–102
- Services console, 98–99
- servicing channel, selecting, 345–346
- Settings App
 - managing local user accounts, 112–113
 - uninstalling updates, 358
- Shared Folders snap-in, 258–259
- shared permissions, 255–256
 - configuring, 263–264
 - creating using the Shared Folders snap-in, 258–259
 - net share command, 260–261
 - network discovery, 257
 - NTFS and, 265
 - SMB (Server Message Block), 256–257
 - troubleshooting, 264–265
 - Windows PowerShell and, 261
- sign-in options, 136
- SMB (Server Message Block), 256–257
- special identity groups, 117–118
- SSTP (Secure Socket Tunneling Protocol), 226

- Start menu
 - configuring Start tiles, 36–38
 - customizing, 33–35, 41–43
 - export Start layout, 38–41
 - grouping Start tiles, 38
- startup, 320–321
 - available options for recovery, 321–322
 - boot store, 322–324
 - components, 319–320
 - services and, 341–342
- Storage Spaces, 275
 - configuring, 276–278
 - managing with Windows PowerShell, 279–280
 - storage layouts, 275–276
- subnet mask, 212
- subnets
 - complex networks, 213–214
 - simple networks, 213
- System Configuration tool, 385–386
- system image backups, 315–316
- System Image Recovery, 317–318
- System Properties, remote management and, 395
- system repair disk, creating, 318–319
- system resources, 374
- System Restore, 306–308
 - identifying affected apps and files, 308–309
 - modifying the task schedule, 309–310

T

- Tablet mode, 35–36
- Task Manager, 365–366
 - Performance tab, 366
 - viewing process power usage, 82–83
 - viewing services, 101–102
- Task Scheduler, 390–391
- taskbar
 - configure notifications area, 50–52
 - configuring, 49–50
 - exporting layout, 38–41
- TPM (Trusted Platform Module), 7, 187
- tracert command, 232
- troubleshooting
 - activation
 - after a hardware configuration change, 74
 - common errors, 75–76
 - using the Activation troubleshooter, 75
 - volume activation services, 72–73
 - cellular connections, 223

- device drivers, 330
- EFS (Encrypting File System), 185–186
- Group Policy(ies)
 - connection issues, 159
 - GPResult command-line tool, 160–161
 - RSOP (Resultant Set of Policy) tool, 160
- networking, 231–232
 - name resolution, 233–234
 - troubleshooting tools, 232–233
- performance issues, 375–377
- permissions, 253–255
- Remote Desktop, 408–409
- shared permissions, 264–266
- updates, 355–356
- volume license activation renewal, 72
- Windows RE and, 310–312
- type 4 printer drivers, 90–91

U

- UAC (User Account Control), 165–166
 - administrative users, 167–168
 - elevation prompts, 168–169
 - Secure Desktop, 170
 - settings, 169–170
 - standard users, 166–167
- uninstalling updates
 - using Control Panel, 357
 - using Settings app, 358
 - using the Command Prompt, 358–359
- Universal Windows apps, 94–95
 - configure application settings, 96–98
- Universal Windows driver, 334
- updates. *See also* Windows Update
 - checking for, 354–355
 - deferrals, 344
 - deployment rings, 346–347
 - feature, 343
 - managing, 342–343
 - planning for, 343
 - quality, 344
 - rolling back, 357
 - servicing channel selection and, 345–346
 - testing and validation, 355
 - troubleshooting, 355–356
 - uninstalling
 - using Control Panel, 357
 - using Settings app, 358

- using the Command Prompt, 358–359
 - Windows as a service, 343–344
- user accounts. *See also* Microsoft accounts
 - AD (Active Directory), 119
 - default accounts, 108–109
 - local accounts, 108
 - managing using Computer Management, 110–111
 - managing using Control Panel, 111–112
 - managing using Settings app, 112–113
 - managing using Windows PowerShell, 113
- user rights policies, 156
- USMT (User State Migration Tool), 23–27

V

- VHDs (virtual hard disks), 270–271
 - creating with Disk Management, 272
 - creating with Hyper-V Manager, 272
 - creating with Windows PowerShell, 273–274
- virtual machines, activation, 72
- VPNs (virtual private networks), 211, 225
 - Always On feature, 229
 - App-Triggered, 230
 - authenticating remote users, 226–227
 - configure using the Settings app, 229
 - creating a connection in Network and Sharing Center, 227–229
 - enabling VPN Reconnect, 230–231
 - profiles, 229–230
 - protocols, 225–226
 - rules, 230
 - traffic filters, 230
- VSS (Volume Shadow Copy Service), 294

W

- WBAAdmin, 295
 - performing backups, 295–297
 - restoring data, 296–297
- Wi-Fi Direct, 238–240
- Windows 10. *See also* performing a clean installation
 - 32-bit version, 4–5
 - 64-bit version, 4–5
 - activation, 69, 72
 - after reinstalling Windows 10, 74
 - common errors, 75–76
 - first-time, 74

- refurbished devices running Windows 10, 74–75
- selecting a method, 69–70
- troubleshooting, 72, 74
- volume activation services, 71
- ADK (Assessment and Deployment Kit), 12, 14, 24
- Business license, 4
- configuring using provisioning packages, 92–93
- deploying, selecting the appropriate Windows edition, 2–4
- general features, 6–7
- installation, 9–11
 - configure Windows for additional regional and language support, 27–28
 - considerations, 23
 - determine the appropriate installation media, 11–14
 - DISM command-line tool, 30
 - local experience packs, 28–29
 - Lpksetup command-line tool, 30–32
 - methods, 9
 - migrating from previous versions of Windows, 21–22
 - perform an in-place upgrade, 14, 15–17
 - side-by-side migration, 22
 - strategies, 11
 - USMT (User State Migration Tool), 23–27
 - wipe-and-load migration, 22–23
- Internet of Things (IoT) editions, 4
- mobility settings, 77
 - configure basic power settings, 77–78
- performing a clean installation, 8–11
- post-installation configuration, 32
 - configure Action Center, 45
 - configure notifications area, 50–52
 - configure Quick Action tiles, 45–47
 - configuring Start tiles, 36–38
 - configuring the taskbar, 49–50
 - customize the Windows desktop, 32, 33–35, 41–43
 - export Start layout, 38–41
 - grouping Start tiles, 38
 - notifications, 47–49
 - support for multiple desktops, 44
- provisioned apps, 94–95
- recovering, 304–305
 - using recovery drives, 305–306
 - using System Restore, 306–310
- S mode, 3–4
- security features, 7–8
- setting up as a mobile hotspot, 224
- setting up for a cellular connection, 222–223
- sign-in options, 136
- upgrading
 - using installation media, 19–20
 - using MDT (Microsoft Deployment Toolkit), 17–18
 - using Windows Deployment Services, 17
- Virtual Secure Mode, 8
- Windows 10 Education, 3
- Windows 10 Enterprise, 3
- Windows 10 Enterprise LTSC, 3
- Windows 10 Home, 2
- Windows 10 Pro, 2
- Windows 10 Pro for Workstations, 3
- Windows Admin Center, 411, 413–415
 - authentication, 413
 - installation, 411–412
- Windows Biometric Framework (WBF), 138
- Windows Configuration Designer, 92
- Windows Defender Antivirus, 199–203
- Windows Defender Firewall, 170–171
 - advanced security, 174–177
 - allowing an app through, 173–174
 - configure connection security rules with IPsec, 177–179
 - creating firewall rules, 179–180
 - enabling remote management, 393–395
 - Firewall & Network Protection page, 171
 - monitoring, 172–173
- Windows Deployment Services, upgrading
- Windows 10, 17
- Windows Hello, 139–141
 - configure the picture password, 144
 - configuring the PIN, 141–144
 - Dynamic Lock, 145
- Windows Hello for Business, 139
- Windows Mobility Center, 83. *See also* mobility settings
- Windows Network Diagnostic, 232
- Windows PowerShell, 125, 233
 - BitLocker cmdlets, 192–193
 - creating VHDs, 273–274
 - disk management, 268–269
 - IPv4, configuring, 216–217
 - IPv4 networking-related cmdlets, 217
 - IPv6 networking-related cmdlets, 219
 - managing driver packages, 337–338
 - managing local user accounts, 113
 - managing registry settings, 149–150, 389–390
 - managing services, 385

- printer management, 91–92, 378–379
- remote management and, 409–411
- Storage Spaces and, 279–280
- Windows RE, 310–312
 - System Image Recovery, 317–318
- Windows Remote Management, 392. *See also* remote management tools
- Windows Security, 162–165
- Windows Update
 - checking for updates, 354–355
 - configuring settings on an individual computer, 347–349
 - configuring settings using GPOs, 350–354
 - delivery optimization, 295–350
 - disabling, 326–327
 - rolling back updates, 357
 - uninstalling updates
 - using Control Panel, 357
 - using Settings app, 358
 - using the Command Prompt, 358–359
 - update testing and validation, 355
- wireless networks, 234
 - advanced settings, 238
 - configuring, 236–237
 - connecting to, 236
 - Hotspot 2.0, 237
 - modes, 234–235
 - security, 235
 - standards, 235
 - Wi-Fi Direct, 238–240