



Microsoft 365 Administrator

Exam Ref MS-102

Orin Thomas

FREE SAMPLE CHAPTER |



Exam Ref MS-102 Microsoft 365 Administrator

Orin Thomas

Exam Ref MS-102 Microsoft 365 Administrator

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

Copyright © 2024 by Orin Thomas

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

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

ISBN-13: 978-0-13-819946-3

ISBN-10: 0-13-819946-9

Library of Congress Control Number: 2023944921

PrintCode

TRADEMARKS

Microsoft and the trademarks listed at www.microsoft.com on the “Trademarks” webpage are trademarks of the Microsoft group of companies. All other marks are property of their respective owners.

WARNING AND DISCLAIMER

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

SPECIAL SALES

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

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

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

EDITOR-IN-CHIEF

Brett Bartow

EXECUTIVE EDITOR

Loretta Yates

ASSOCIATE EDITOR

Shourav Bose

DEVELOPMENT EDITOR

Rick Kughen

MANAGING EDITOR

Sandra Schroeder

SENIOR PROJECT EDITOR

Tracey Croom

PRODUCTION EDITOR

Dan Foster

COPY EDITOR

Rick Kughen

INDEXER

Valerie Haynes Perry

PROOFREADER

Dan Foster

TECHNICAL EDITOR

Ed Fisher

EDITORIAL ASSISTANT

Cindy Teeters

COVER DESIGNER

Twist Creative, Seattle

COMPOSITOR

Danielle Foster

Pearson's commitment to diversity, equity, and inclusion

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

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

Our ambition is to purposefully contribute to a world where:

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

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

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

This page intentionally left blank

Contents

Introduction	xv
Organization of this book	xv
Preparing for the exam	xvi
Microsoft certifications	xvi
Access the exam updates chapter and online references	xvii
Errata, updates, and book support	xvii
Stay in touch	xvii
Chapter 1 Deploy and configure Microsoft 365 tenants	1
Skill 1.1: Deploy a Microsoft 365 tenant	2
Plan and create a tenant	2
Plan and create subscriptions	4
Skill 1.2: Manage Microsoft 365 DNS domains	10
Implement a domain name strategy	10
Manage domains	11
Configure workloads for a new domain name	23
Skill 1.3: Manage Microsoft 365 organizational settings	27
Configure organizational settings	27
Complete the organization profile	30
Add a Microsoft partner or work with Microsoft FastTrack	31
Edit an organizational profile	33

Skill 1.4: Manage Microsoft 365 subscription and tenant health.	35
Manage service health alerts	35
Create an internal service health response plan	37
Monitor service health	38
Skill 1.5: Monitor adoption and usage	38
Configure and review reports	39
Schedule and review security and compliance reports	40
Schedule and review usage metrics	42
Chapter summary	51
Thought experiment.	52
Deploying a Microsoft 365 tenancy at Tailwind Traders	52
Thought experiment answers	52

Chapter 2 Managing M365 users, groups, and identity synchronization 53

Skill 2.1: Manage Microsoft 365 identities	54
Plan Microsoft 365 and Microsoft Entra ID identities	54
Manage users	55
Manage groups	57
Manage external identities by using Microsoft Entra External ID	59
Manage Microsoft 365 contacts	62
Manage product licenses	63
Skill 2.2: Prepare for identity synchronization	67
Evaluate synchronization requirements	67
Prepare for directory synchronization	70

Skill 2.3: Manage identity synchronization by using Microsoft Entra Connect	75
Microsoft Entra Connect	75
Microsoft Entra Connect user sign-in options	76
Installing Microsoft Entra Connect	78
Monitor Microsoft Entra Connect Health	88
Manage Microsoft Entra Connect synchronization	88
Implement multiforest AD DS scenarios	93
Skill 2.4: Manage identity synchronization by using Microsoft Entra Cloud Sync	94
Microsoft Entra Cloud Sync	94
Installing Microsoft Entra Cloud Sync	95
Comparing Microsoft Entra Cloud Sync with Microsoft Entra Connect	96
Troubleshooting Microsoft Entra Cloud Sync	97
Chapter summary	98
Thought experiment	99
Thought experiment answers	99
Chapter 3 Managing Microsoft 365 Roles	101
Skill 3.1: Manage role membership	102
Manage admin roles	103
Manage role allocations by using Microsoft Entra ID	108
Skill 3.2: Microsoft 365 administrative roles	108
Global Administrator	109
Global Reader	110
Service Support Administrator	110

Exchange Administrator (Exchange Online Administrator)	110
Helpdesk Administrator	111
SharePoint Administrator	111
Teams Administrator	111
User Administrator	112
Delegated Administrator	112
Skill 3.3: Microsoft Defender roles and role groups	113
Microsoft 365 Defender and AAD global roles	113
Microsoft Defender for Endpoint roles	114
Microsoft Defender for Office 365 roles	115
Defender for Office 365 administrative role groups	120
Defender for Cloud Apps roles	125
Microsoft Defender for Identity administrative roles	127
Microsoft Defender for Business administrative roles	128
Creating custom roles in Microsoft 365 Defender	129
Skill 3.4: Microsoft Purview roles	131
Collection Administrators	132
Data Curators	132
Data Readers	132
Data Source Administrator	132
Insights Reader	132
Policy Author	132
Workflow Administrator	132
Assigning Purview roles	133
Manage administrative units	133
Configure Microsoft Entra ID Privileged Identity Management (PIM)	134

OATH tokens	161
Phone call settings	161
Report MFA utilization	162
Skill 4.5: Self-service password reset	162
Password reset registration	163
Enable self-service password reset	164
Skill 4.6: Microsoft Entra ID Identity Protection	165
Skill 4.7: Conditional access policies	167
Preparing for conditional access	167
Create a conditional access policy	169
What If tool	170
Skill 4.8: Resolving authentication issues	172
Audit logs	172
Sign-in event logs	173
Self-service password reset activity	174
Chapter summary	175
Thought experiment	176
Thought experiment answers	176

Chapter 5 Manage security and threats using Microsoft 365 Defender 177

Skill 5.1: Security reports and alerts	177
Secure Score	178
Incidents	182
Alerts	187
Threat analytics	189

Skill 5.2: Collaboration protection	191
Defender for Office Policies and Rules	191
Configuration analyzer	212
Managing threats with Defender for Office	214
Managing attack simulations	215
Blocked users	225
Skill 5.3: Endpoint protection	225
Defender for Endpoint	226
Onboarding devices	226
Manage Defender for Endpoint settings	231
Chapter summary	239
Thought experiment	239
Configuring Microsoft 365 Defender settings and policies	239
Thought experiment answers	240

Chapter 6 Manage Microsoft Purview compliance 241

Skill 6.1: Sensitive information types	241
Data Lifecycle Management	242
Manage sensitive information types	242
Compliance-related roles	245
Skill 6.2: Sensitivity labels and policies	247
Sensitivity labels	247
Sensitivity label policies	252
Skill 6.3: Retention labels and policies	253
Retention policies	253
Retention labels	258
Preservation locks	262
Inactive mailbox retention	263

Skill 6.4: Data Loss Prevention	264
DLP policies	264
DLP alerts	268
Chapter summary	270
Thought experiment.....	271
Compliance at Tailwind Traders	271
Thought experiment answers	272
Chapter 7 MS-102 Microsoft 365 Administrator exam updates	273
The purpose of this chapter	273
About possible exam updates	274
Impact on you and your study plan	274
Exam objective updates	274
Updated technical content	274
Objective mapping	275
Index	277

Acknowledgments

I'd like to thank Loretta Yates, Shourav Bose, Ed Fisher, Dan Foster, and Rick Kughen for all the work they did getting this book to print.

About the author

Orin Thomas is a Principal Hybrid Cloud Advocate at Microsoft and has written more than 40 books for Microsoft Press on topics including Windows Server, Windows Client, Azure, Hybrid Cloud, Microsoft 365, Office 365, System Center, Exchange Server, Security, and SQL Server. You can connect with him at aka.ms/orin.

Introduction

The MS-102 exam deals with advanced topics, requiring candidates to have an excellent working knowledge of Microsoft 365 administration. Some of the exam comprises topics that even experienced Microsoft 365 administrators may rarely encounter unless they work across all elements of a Microsoft 365 tenancies regularly. To pass this exam, candidates need to understand how to deploy and manage Microsoft 365 tenancies and integrate Microsoft 365 with an on-premises Active Directory environment, manage security and threats, and implement the compliance technologies in Microsoft Purview. They also need to keep up to date with new developments with Microsoft 365, including new features and changes to the interface.

Candidates for this exam are Information Technology (IT) Professionals who want to validate their advanced skills as an administrator of Microsoft 365. To pass, candidates must have a thorough theoretical understanding and meaningful, practical experience implementing technologies, including Microsoft Entra, Microsoft 365 Defender, Microsoft Purview, and Microsoft 365 tenancy configuration.

This edition of this book covers Microsoft 365 and the MS 102 exam objectives circa mid-2023. As the Microsoft 365 suite evolves, so do the Microsoft 365 exam objectives, so you should check carefully if any changes have occurred since this edition of the book was authored and study accordingly.

This book covers every major topic area on the exam but 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 *learn.microsoft.com* and in blogs and forums.

Organization of this book

This book is organized by the “Skills measured” list published for the exam. The “Skills measured” list is available for each exam on the Microsoft Learn website: *microsoft.com/learn*. 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. For example, if an exam covers six major topic areas, 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 augmenting 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, online courses, and live events at microsoft.com/learn.

Note that this *Exam Ref* is based on publicly available information about the exam and the author's 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 microsoft.com/learn.

Access the exam updates chapter and online references

The final chapter of this book, “MS-102 Microsoft 365 Administrator exam updates,” will be used to provide information about new content per new exam topics, content that has been removed from the exam objectives, and revised mapping of exam objectives to chapter content. The chapter will be made available from the link below as exam updates are released.

Throughout this book are addresses to webpages that the author has recommended you visit for more information. Some of these links can be very long and painstaking to type, so we’ve shortened them for you to make them easier to visit. We’ve also compiled them into a single list that readers of the print edition can refer to while they read.

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

Download the Exam Updates chapter and the URL list at

MicrosoftPressStore.com/ERMS102/downloads

Errata, updates, and 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/ERMS102/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 *support.microsoft.com*.

Stay in touch

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

This page intentionally left blank

Managing M365 users, groups, and identity synchronization

A key aspect of deploying Microsoft 365 is configuring user identity properly, so users can seamlessly access resources in the on-premises and Microsoft 365 environments. If it is not done correctly, users must juggle different accounts, depending on whether the accessible resources are hosted locally or in the cloud. In this chapter, you will learn about designing an identity strategy, managing Microsoft Entra ID identities, planning identity synchronization with Microsoft Entra Connect and Microsoft Entra Cloud Sync, and managing and troubleshooting identity synchronization.

Skills in this chapter:

- Skill 2.1: Manage Microsoft 365 identities
- Skill 2.2: Prepare for identity synchronization
- Skill 2.3: Synchronize identities using Microsoft Entra Connect
- Skill 2.4: Synchronize identities using Microsoft Entra Cloud Sync

IMPORTANT

In August 2023, Microsoft announced that it was rebranding Azure Active Directory to Microsoft Entra ID. In addition, products such as Azure AD Connect, Azure AD Connect Cloud Sync, and Azure Active Directory Domain Services have also been renamed Microsoft Entra Connect, Microsoft Entra Cloud Sync, and Microsoft Entra Domain Services, respectively.

The actual functionality of these products has not been changed, and it is also likely that it will be some time before UI elements in various administrative portals and Microsoft's official documentation are also completely updated to use the new brand guidelines. Practice tests and study materials that use the original names will still provide you with relevant information on functionality. However, for the foreseeable future, multiple names will be used to label the same product or service.

Skill 2.1: Manage Microsoft 365 identities

Planning Microsoft 365 identities involves managing internal and external users who need to access Microsoft 365 resources and applications. When managing these identities, you must ensure that users are appropriately licensed for the necessary tools. External identities are users not part of your organization who might need access to internal resources and applications.

This section covers the following skills:

- Plan Microsoft 365 and Microsoft Entra ID identities
- Manage users
- Manage groups
- Perform bulk user management
- Manage external identities
- Manage Microsoft 365 contacts

Plan Microsoft 365 and Microsoft Entra ID identities

Microsoft 365 uses Microsoft Entra ID (previously Azure Active Directory) as its identity store. In hybrid environments, you'll manage identities primarily using on-premises management tools such as Active Directory Users and Computers. In environments where Microsoft Entra ID is the primary authority source, you can use the Microsoft 365 admin center to manage user identities. You can also use the Microsoft Entra admin center to perform these tasks.

When planning the use of Azure identities, you'll need to consider the following questions:

- What UPN will be used with the identity for login to Microsoft 365 resources? You can change the UPN suffix to any domain configured and authorized for use with the directory.
- What authentication and authorization options will be required to access Microsoft 365 resources? Will users need to change their passwords regularly? Will users be required to perform multifactor authentication?
- What roles will be assigned to users? Will you need to assign Microsoft Entra ID roles to specific users? What method will you use to perform this task?
- Will Microsoft Entra ID groups be used? What strategy will you use to manage collections of users into groups? Will your organization use a group naming convention?

You'll learn more about how to perform user-management tasks later in this chapter.

Manage users

You can use the Microsoft 365 admin center or the Entra ID admin center available at <https://entra.microsoft.com> to manage Microsoft Entra ID user accounts. The Entra ID admin center gives you a larger set of options for managing the properties of user accounts than the Microsoft 365 admin center because you can edit extended user properties.

To create a new Microsoft Entra ID user, perform the following steps:

1. In the Microsoft Entra admin center, select **Users > All Users > New User**.
2. On the **New User** blade, provide the following information:
 - **Name** The user's actual name.
 - **User Name** The user's sign-in name in UPN format.
 - **Profile** The user's first name, last name, job title, and department.
 - **Properties** The user's source of authority. By default, if you are creating the user using the Entra ID admin center or the Microsoft 365 admin center, this will be Entra ID.
 - **Groups** The groups the user should be a member of.
 - **Directory Role** Whether the account has a User, Global Administrator, or a limited administrator role.
 - **Password** The automatically generated password. With the **Show Password** option, you can transmit the password to the user through a secure channel.

You can also use the Microsoft Entra admin center to perform the following user administrator tasks:

- Update profile information
- Assign directory roles
- Manage group membership
- Manage licenses
- Manage devices
- Manage access to Azure resources
- Manage authentication methods

Another option is to use the **Active Users** section of the Microsoft 365 admin center shown in Figure 2-1. From this console, you can add users using the **Add A User** item, which will require the user's first name, last name, display name, and username in UPN format and will provide the option of an automatically generated password that must be changed and the ability to assign a role and add profile details.

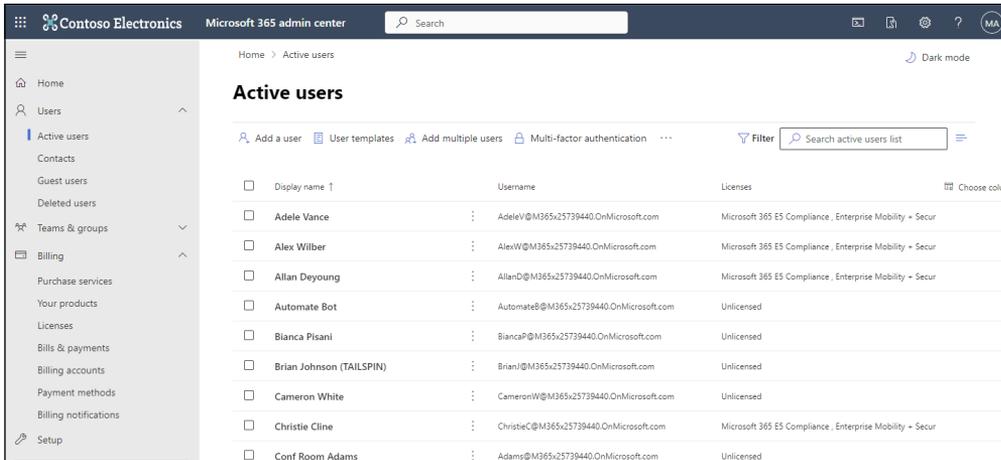


FIGURE 2-1 Active Users

User templates allow you to create users with specific configurations, including assigning a specific set of licenses, app access, roles, and profile information. Figure 2-2 shows the **Assign Licenses** page of the **Add User Template** dialog.

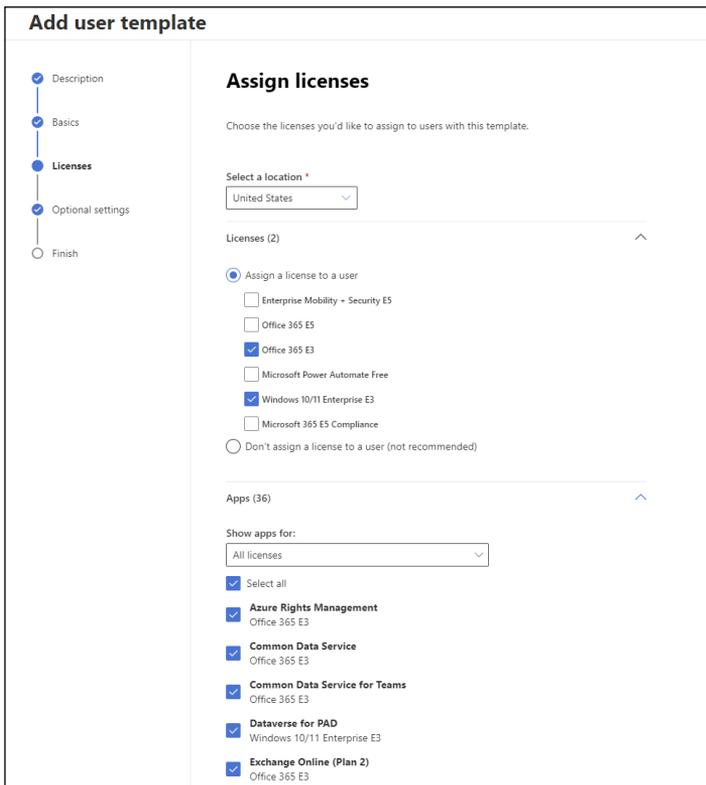


FIGURE 2-2 Creating a new user template in the Microsoft 365 admin center

MORE INFO MANAGE MICROSOFT 365 USERS

You can learn more about Managing Microsoft 365 users at <https://learn.microsoft.com/microsoft-365/enterprise/manage-microsoft-365-accounts>.

Manage groups

Groups enable you to collect users and assign them privileges and access to workloads or services. Rather than assign privileges and access to workloads or services directly to users, you can assign these rights to a group and then indirectly assign them to users by adding the user accounts to the appropriate group. Using groups in this way is a long-standing administrative practice because it allows you to determine a user's level of access and rights by looking at the user's group memberships rather than checking each workload and service to determine if the user account has been assigned rights to that service. You can manage groups in the **Active Teams And Groups** area of the Microsoft 365 admin center, as shown in Figure 2-3.

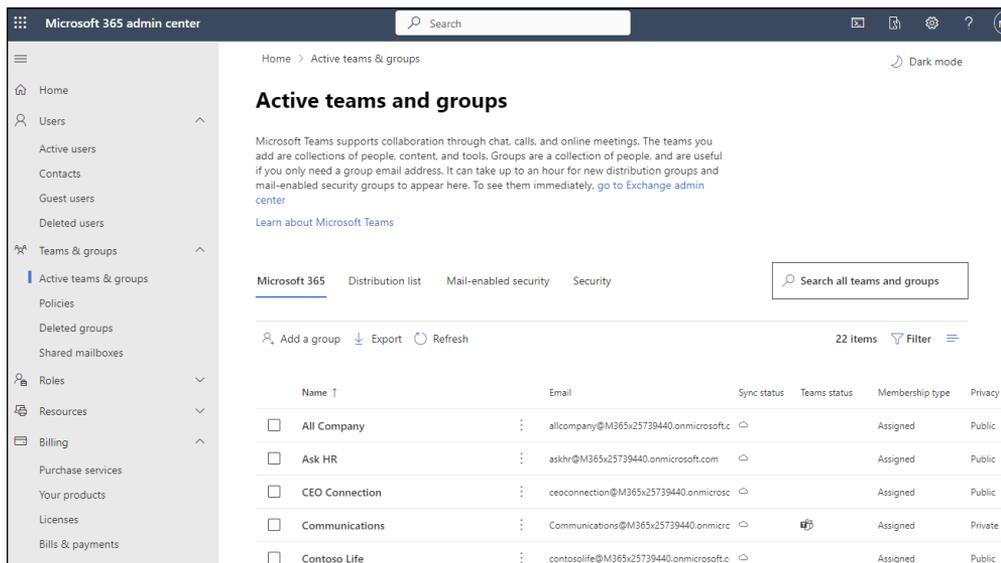


FIGURE 2-3 The Active Teams And Groups page in the Microsoft 365 admin center

Microsoft 365 supports the following group types:

- **Microsoft 365 groups** Used for collaboration between users. These users can be inside or external to the organization. Each Microsoft 365 group has an associated email address, shared workspace for conversations, shared location for files, calendar events, and a planner.
- **Security groups** Used to grant access to specific Microsoft 365 resources, such as SharePoint sites. Security groups can contain user accounts as well as device accounts. Device-related groups are most often used with services such as Intune.

- **Mail-enabled security groups** Can be used to grant access to specific Microsoft 365 resources. Cannot be dynamically managed and cannot contain devices.
- **Distribution groups** Used for sending notifications to groups of people.

Group membership for Microsoft 365 groups and security group types can be configured as **Assigned** or **Dynamic**. When the **Assigned** option is selected, membership is managed manually. When the **Dynamic** option is selected, group membership is determined based on the results of a query against user or device attributes. For example, suppose you have a user located in a specific department or city and managed by a specific person. That user could automatically be put in a specific group.

Source of authority is important when modifying users and groups. Modifications occurring in the on-premises Active Directory overwrite the current state of the objects within the Microsoft Entra ID instance that supports the Microsoft 365 tenancy. The only exception to this rule is the assignment of licenses, which only occurs using the Microsoft 365 admin center or PowerShell tools.

Modifications made to on-premises user and group objects will be present only in the Microsoft Entra ID instance that supports the Microsoft 365 tenancy after synchronization has occurred. By default, synchronization occurs every 30 minutes. You can force synchronization to occur by using the Synchronization Service Manager tool.

With deletion, the source of authority concept is very important. When you want to delete a user or group account created in the on-premises Active Directory instance, you should use tools such as Active Directory Users and Computers or the Active Directory admin center. When you delete a user or group using this method, the user will be deleted from the on-premises Active Directory instance and then, when synchronization occurs, from the Microsoft Entra ID instance that supports the linked Microsoft 365 tenancy.

Deleting a user from Microsoft 365 keeps their account in the Microsoft Entra ID Recycle Bin for 30 days. This means you can recover the account online if necessary. If you delete a user from your on-premises Active Directory environment but have enabled the on-premises Active Directory Recycle Bin, recovering the user from the on-premises Active Directory Recycle Bin will recover the user account in the Entra ID instance associated with Microsoft 365. You must create another account with a new GUID if your Active Directory Recycle Bin is enabled in your on-premises Active Directory instance.

MORE INFO MICROSOFT 365 GROUPS

You can learn more about Microsoft 365 groups at <https://learn.microsoft.com/microsoftteams/office-365-groups>.

Manage external identities by using Microsoft Entra External ID

Sometimes you want to enable people in a partner organization or external users such as temporary contractors to interact with resources hosted in Microsoft 365. For example, you might want to allow someone to collaborate with content hosted in SharePoint Online.

When planning external access to Microsoft 365 resources, you should understand that Microsoft 365 external sharing and Microsoft Entra External ID collaboration are almost the same thing. Except for OneDrive and SharePoint Online, all external sharing uses the Microsoft Entra External ID collaboration invitation APIs. Although Microsoft Entra External ID is not a direct replacement for Azure AD B2B and Azure AD B2C, the functionality of these products addresses the same use cases.

MORE INFO MICROSOFT ENTRA EXTERNAL ID

You can learn more about Microsoft Entra External ID at <https://learn.microsoft.com/azure/active-directory/external-identities/customers/faq-customers>.

You manage external sharing for SharePoint Online by using the **Sharing** page of the SharePoint admin center. To configure SharePoint so that only Microsoft Entra External ID sharing is enabled, select **Allow Sharing Only With The External Users That Already Exist In Your Organization's Directory**, as shown in Figure 2-4.

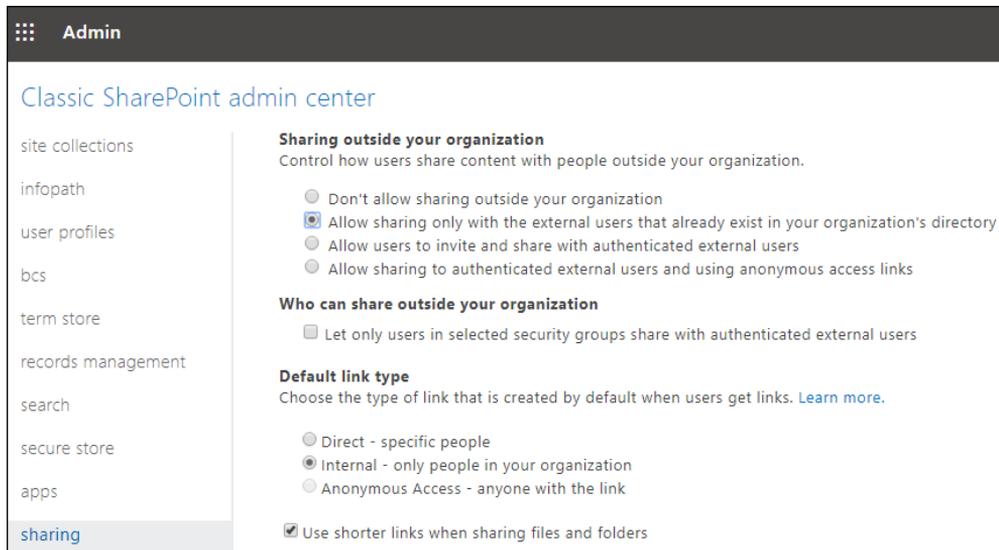


FIGURE 2-4 SharePoint Online Sharing options

You can use the **External Collaboration Settings** page, accessible from the **Entra ID External Identities** blade, to configure the following collaboration settings:

- **Guest Users Permissions Are Limited** Enabled by default, this option enables you to configure guest users to have the same permissions as standard users.
- **Admins And Users In The Guest Inviter Role Can Invite** Invitations can be sent from users who hold the administrator and guest inviter roles.
- **Members Can Invite** Invitations can be sent by users who are not administrators and who have not been assigned the **Guests Can Invite** role.
- **Guests Can Invite** Users with **Guests Can Invite** status can invite other users as B2B users or guests.
- **Enable Email One-Time Passcode For Guests** This is a one-time passcode for guests who do not have an Azure AD or Microsoft account and for which Google Federation has not been configured. Guests who use one-time passcodes remain authenticated for 24 hours.
- **Allow Invitations To Be Sent To Any Domain** This is the default setting, which enables guest and B2B invitations to be sent to any domain.
- **Deny Invitations To Specified Domains** This enables you to create a block list of domains to which guest and B2B invitations cannot be sent.
- **Allow Invitations Only To The Specified Domains** Use this option to allow guest and B2B invitations only to specific domains. Invitations to domains not on the allowed list are blocked.

Microsoft Entra External ID accounts

Microsoft Entra External ID accounts are a special type of guest user account that resides within the Microsoft Entra ID instance to which you can assign privileges. Microsoft Entra External ID accounts are generally used when you want to allow one or more users from a partner organization to access resources hosted within your organization's Microsoft 365 tenancy. For example, if users in Contoso's partner organization, Tailwind Traders, need to interact with and publish content to a Contoso SharePoint Online site, one method of providing the necessary access is to create a set of Microsoft Entra External ID accounts.

Microsoft Entra External ID accounts have the following properties:

- They are stored in a separate Microsoft Entra ID tenancy from your organization but are represented as a guest user in your organization's tenancy. The Microsoft Entra External ID user signs in using their organization's Microsoft Entra ID account to access resources in your organization's tenancy.
- They are stored in your organization's on-premises Active Directory and then synced using Microsoft Entra Connect (previously Azure AD Connect) and a guest user type. This is different from the usual type of synchronization, where user accounts are synced from an on-premises directory, but the Microsoft Entra ID accounts are traditional Microsoft Entra ID accounts and are not assigned the guest user type.

Microsoft Entra ID accounts use the user type to display information about the account's relationship to the organization's tenancy. The two following values are supported:

- **Member** If the user type is **Member**, the user is considered to belong to the host organization. This is appropriate for full-time employees, some types of contractors, or anyone else on the organizational payroll or within the organizational structure.
- **Guest** The Guest user type indicates that the user is not directly associated with the organization. The Guest user type applies to Microsoft Entra External ID and, more generally, to guest accounts. It is used when the account is based in another organization's directory or associated with another identity provider, such as a social network identity.

The account's user type does not determine how the user signs in; it merely indicates the user's relationship to the organization that controls the Microsoft Entra ID tenancy. It can also be used to implement policies that depend on the value of this attribute. It is the source attribute property that indicates how the user authenticates. This property can have the following values:

- **Invited User** A guest or Microsoft Entra External ID user who has been invited but has not accepted yet.
- **External Active Directory** An account that resides in a directory managed by a partner organization. When the user authenticates, they do so against the partner organization's Microsoft Entra ID instance. This field will eventually be updated to represent the Microsoft Entra ID branding.
- **Microsoft Account** A guest account that authenticates using a Microsoft account, such as an *Outlook.com* or *Hotmail.com* account.
- **Windows Server Active Directory** A user signed in from an on-premises instance of Active Directory managed by the same organization that controls the tenancy. This usually involves the deployment of Microsoft Entra Connect. In the case of a Microsoft Entra External ID user, though, the user type attribute is set to **Guest**.
- **Azure Active Directory** A user signed in using a Microsoft Entra ID account that your organization manages. The user type attribute is set to **Guest** for a Microsoft Entra External ID user. This field will eventually be updated to represent the Microsoft Entra ID branding.

When you create the first type of Microsoft Entra External ID account, an invitation is sent to the user to whom you want to grant Microsoft Entra External ID access. The process of creating and sending this invitation also creates an account within your organization's Microsoft Entra ID instance. This account will not have any credentials associated with it because authentication will be performed by the Microsoft Entra External ID user's identity provider.

Until the invitation is accepted, the **Source** property of an invited guest user account will be set to **Invited User**. You can also resend the invitation if the target user does not receive or respond to the first invitation. When the user accepts the invitation, the **Source** attribute will be updated to **External Entra ID**. If the user's account is synchronized from an on-premises Active Directory instance, but the **User Type** is set to **Guest**, the **Source** property will be listed as **Windows Server Active Directory**.

Guest accounts

A Guest account might be considered a type of account where the account is a Microsoft account or a social account rather than one associated with an Entra ID tenancy. For example, a Guest account might have an *@outlook.com* email address or a social media account (such as Facebook). The main difference between the two is that, in general, an Entra External ID account implies a business-to-business relationship, whereas a Guest account implies a business-to-individual relationship.

You create a Guest account in exactly the same way as an External ID account, as outlined in the preceding section. You send an invitation, an account is created, the user accepts the invitation, and then the individual uses the account to access Microsoft 365 resources to which they have been granted permissions.

Guest users are blocked from performing certain tasks, including enumerating users, groups, and other Entra ID resources. You can remove the guest user default limitations by performing the following steps:

1. On the Microsoft Entra ID blade, under **Manage**, select **User Settings**.
2. On the **User Settings** blade, select **Manage External Collaboration Settings**.
3. On the **External Collaboration Settings** page, select **No** under **Guest Users Permissions Are Limited**.

MORE INFO ADDING GUEST USERS

You can learn more about this skill at <https://learn.microsoft.com/en-us/azure/active-directory/external-identities/b2b-quickstart-add-guest-users-portal>.

Manage Microsoft 365 contacts

Contacts are people not part of your organization that you want to be present within address books. For example, there might be specific partners or vendors you want people in your organization to find quickly; in that case, you can add them as contacts. When people type a contact's name into Outlook or Microsoft Teams, their details will be prepopulated as though they were typical members of your organization. You can provide a contact's email address, phone number, fax number, website, street address, city, state, zip, and country and configure a MailTip for them.

You can add contacts from the Microsoft 365 admin center by going to **Contacts** under **Users**, as shown in Figure 2-5.

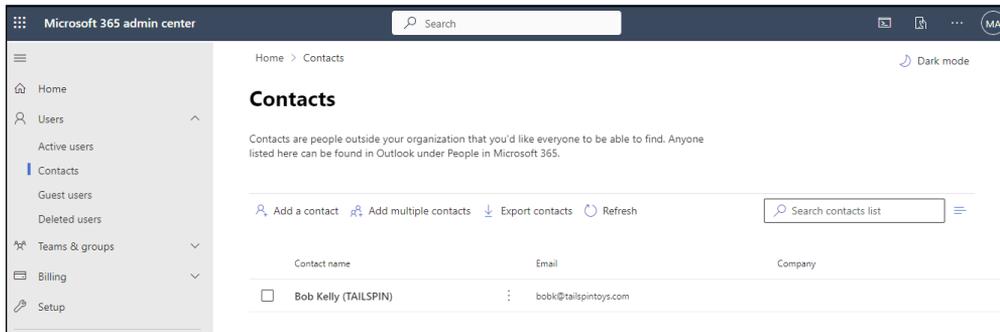


FIGURE 2-5 Contacts

You can add contacts individually or import up to 40 contacts at a time by using a specially formatted CSV file. You can also add and manage contacts using the `New-MailContact`, `Get-MailContact`, `Enable-MailContact`, `Remove-MailContact`, `Disable-MailContact`, and `Set-MailContact` Exchange PowerShell cmdlets.

MORE INFO ADDING GUEST USERS

Microsoft 365 contacts function just as Exchange Online contacts do. Any contacts you create in the Exchange admin center will be visible in the Microsoft 365 admin center, and any you create in Microsoft 365 admin center will be in the Exchange admin center. You can learn more about Contacts at <https://learn.microsoft.com/en-us/exchange/recipients/mail-contacts>.



EXAM TIP

You can configure an allow list of specific domains to which invitations can be sent, and you can configure a block list where you only block invitations to specific domains.

Manage product licenses

Microsoft 365 users require licenses to use Outlook, SharePoint Online, Office 365, and other services. Users assigned the Global Administrator or User Management Administrator roles can assign licenses when creating new Microsoft 365 user accounts. They can also assign licenses to accounts created through directory synchronization or federation.

When a license is assigned to a user, the following occurs:

- An Exchange Online mailbox is created for the user.
- Edit permissions for the default SharePoint Online team site are assigned to the user.
- For Microsoft 365 Apps for enterprise, the user can download and install Microsoft Office on up to five Windows or macOS computers.

You can view the number of valid licenses and the number of those licenses that have been assigned on the Licenses page. You access this page by selecting **Billing** in the left pane of the Microsoft 365 admin center and then selecting **Licenses**, as shown in Figure 2-6.

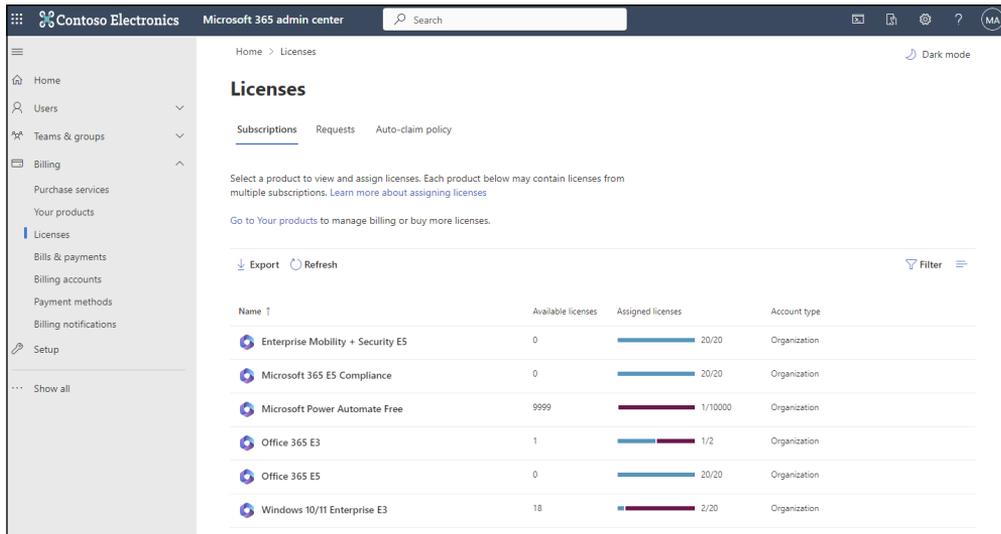


FIGURE 2-6 The Licenses page

MORE INFO ASSIGN LICENSES

You can learn more about assigning licenses at <https://docs.microsoft.com/microsoft-365/admin/add-users/add-users>.

To assign a license to a user, perform the following steps:

1. In the Microsoft 365 admin center, select the **Active Users** node under **Users**, as shown in Figure 2-7.

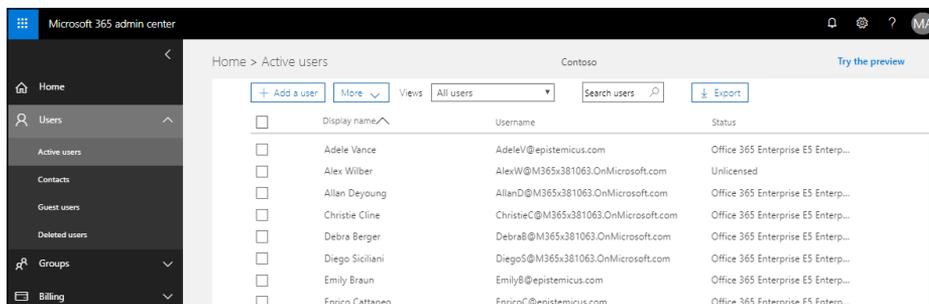


FIGURE 2-7 The Active Users node

2. Select the checkbox next to the user to whom you want to assign a license. This will open the user's properties page, as shown in Figure 2-8.

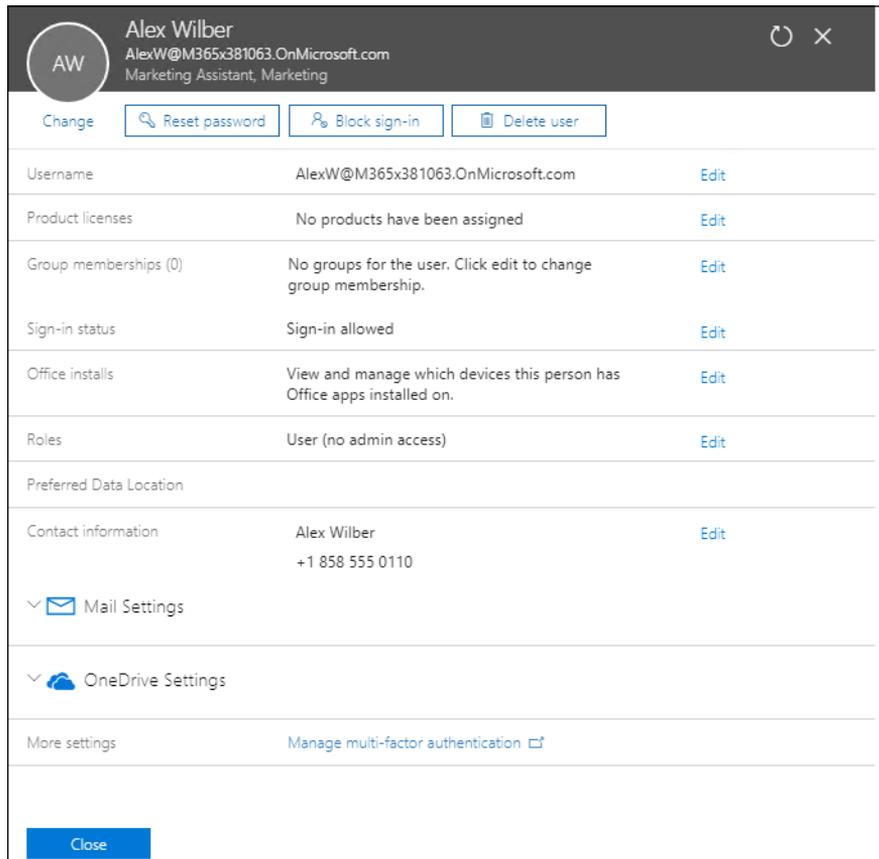


FIGURE 2-8 User properties page

3. On the user's properties page, select **Edit** next to **Product Licenses**.

4. Use the **Location** dropdown to choose your location. Then, assign licenses as needed: **Enterprise Mobility And Security, Office 365 Enterprise, and Windows 10/11 Enterprise**, as shown in Figure 2-9.

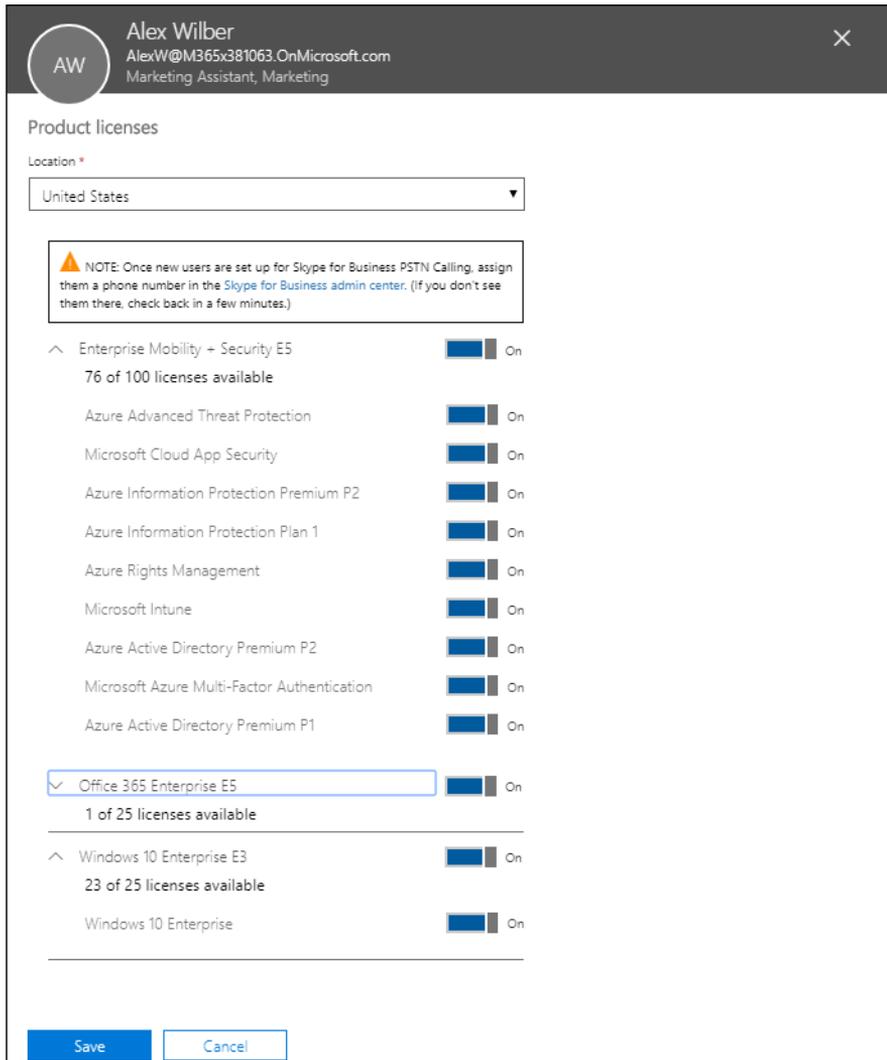


FIGURE 2-9 The Product Licenses page

5. Select **Save** to assign the licenses to the user.

User accounts created in Microsoft 365 by the synchronization process will not automatically be assigned Microsoft 365 licenses. This means that when creating new user accounts in the on-premises environment after initially configuring Microsoft Entra Connect, you'll also need to use Microsoft 365 admin center or PowerShell to provision those accounts with Microsoft 365 licenses.

Index

A

- access policies, conditional, 167–171
- Active Directory Federation, 77
- Active Users report, 45
- admin center, learning about, 30
- admin roles. *See also* roles
 - managing, 103–107
 - Microsoft Defender for Business, 128–129
 - Microsoft Defender for Identity, 127–128
- administrative roles, 108–112
- administrative units, Microsoft Entra ID, 133–134
- adoption and usage, monitoring, 38–39
- advanced delivery rules, 210
- Advisor partner type, 33
- alerts, 187–189
- anti-malware policy, 202–203
- anti-phishing policy, 196–197
- anti-spam policy, 197–202
- app password authentication, 145
- App/Instance Admin role, 126
- Application Administrator role, 104
- Application Developer role, 104
- ARC (Authenticate Received Chain), 209
- Attach Payload Author role, 104
- attachments. *See* Safe Attachments policies
- Attack Simulation Administrator role, 104
- attack simulations, managing, 215–224
- Attribute Assignment Reader role, 104
- Attribute Assignment Administrator role, 104
- Attribute Definition Administrator role, 104
- Attribute Definition Reader role, 104
- audit logs, 172–173
- auditing reports, 41
- authentication. *See also* MFA (Multifactor Authentication)
 - basic and modern, 142–143
 - certificate-based, 146–147
 - pass-through, 77
 - passwordless, 147–148
- Authentication Administrator role, 104
- authentication issues, resolving, 172–175
- authentication method, implementing, 143–146
- Authentication Policy Administrator role, 104
- authoritative domains, configuring, 16–17
- Azure AD (Azure Active Directory).
See Microsoft Entra ID
- Azure DevOps Administrator role, 104
- Azure identities, planning use of, 54
- Azure Information Protection Administrator role, 104
- Azure Speech Services setting, 28

B

- B2C IEF Keyset Administrator role, 104
- B2C IEF Policy Administrator role, 104
- banned password lists, configuring, 153
- basic authentication, 142–143
- Billing Administrator role, 104
- Bing Data Collection setting, 30
- .biz domain, 11
- blocked users, 225
- Bookings setting, 28
- Briefing Email setting, 28

C

- Calendar setting, 28
- certificate-based authentication, 146–147
- Cloud App Security Administrator role, 104
- Cloud Application Administrator role, 104
- Cloud Device Administrator role, 104
- Cloud Discovery Global Admin role, 126
- CNAME records, 11, 23–26
- collaboration protection, 191
- Collection Administrators role, Microsoft Purview, 132
- .com domain, 11
- Compliance Administrator role, 105, 126, 138
- compliance and security roles, 138–139
- Compliance Data Administrator role, 105
- compliance reports, scheduling and reviewing, 40–42
- compliance-related roles, Microsoft Entra ID, 245–246
- Conditional Access Administrator role, 105
- conditional access policies, 167–171
- configuration analyzer tool, 212–213

- Configuration Manager, using with Defender for Endpoint, 229–230
- contoso.com* domain, 10
- Cortana setting, 28
- .co.uk domain, 11
- Credential Harvest scenario, 216
- Custom App Launcher Tiles setting, 31
- custom domain names, configuring, 12–13. *See also* domain names
- custom domain, verifying, 13–14
- Custom Themes setting, 31
- Customer Lockbox Access Approver role, 105
- Customer Lockbox setting, 30

D

- Data Curators role, Microsoft Purview, 132
- Data Lifecycle Management, Microsoft Purview, 242
- Data Location setting, 31
- data loss prevention reports, 149–115
- Data Readers role, Microsoft Purview, 132
- Data Source Administrator role, Microsoft Purview, 132
- default domain, setting, 15–16. *See also* domains
- Defender for Cloud Apps, 125–126
- Defender for Endpoint
 - Configuration Management, 236
 - Device Management, 237–238
 - features, 226
 - General settings, 232–233
 - onboarding devices, 226–231
 - rules, 233–235
- Defender for Office, threat management, 214–215
- Defender for Office Policies, EOP (Exchange Online Protection), 191
- Delegated Administrator partner type, 33

- Delegated Administrator role, 112
- Desktop Analytics Administrator role, 105
- Directory Readers role, 105
- Directory Synchronization Accounts role, 105
- directory synchronization, preparing for, 70–75
- Directory Synchronization setting, 28
- Directory Writers role, 105
- DKIM (DomainKeys Identified Mail), 209
- DLP (Data Loss Prevention), Microsoft Purview, 264–270
- DNS records
 - device management, 26
 - Exchange Online, 23–25
 - Microsoft Teams, 26
- DNS settings, verifying, 15
- Domain Name Administrator role, 105
- domain name strategy, 10
- domain names. *See also* custom domain names
 - acquiring, 11
 - configuring user identities for, 17
 - configuring workloads for, 23–26
 - custom configuration, 12–13
- domains. *See also* default domain; nonroutable domains; relay domains
 - adding to Microsoft 365, 15
 - authoritative and internal relay, 16–17
 - changing, 20
 - configuring, 15, 19
 - for Exchange Online, 17
 - managing, 11–15
 - purchasing through Microsoft 365, 11–12
 - setting defaults, 15–16
- Drive-By-URL scenario, 216
- Dynamics 365 Administrator role, 105
- Dynamics 365 Customer Choice setting, 28
- Dynamics 365 Sales Insights-Analytics setting, 28

- Dynamics 365 Sales Insights-Connection Graph setting, 28
- Dynamics CRM setting, 28

E

- Edge Administrator role, 105
- eDiscovery Manager role group, 138
- Email Activity report, 43
- Email address authentication, 145
- email addresses, managing, 18–23
- Email App Usage report, 45
- Email authentication settings rules, 209–210
- endpoint detection and response, 182–183
- endpoint protection. *See* Defender for Endpoint
- Enhanced Filtering rules, 211
- EOP (Exchange Online Protection) policies, 191, 196–203
- evaluating Microsoft 365, 6
- Exam Tips
 - assigning rights to applications, 134
 - conditional access policies, 171
 - contacts, 63
 - Defender for Endpoint, 238
 - delegated administrator partner types, 34
 - DNS records, 26
 - locking out users in MFA, 161
 - password sync vs. pass-through authentication, 77
 - reports, 51
 - role-based access control, 107
 - security and compliance roles, 139
 - service status definitions, 38
 - subscriptions versus tenants, 9
 - synchronization, 93
- exam updates, 273–276
- Exchange Administrator role, 105, 110

Exchange Online

Exchange Online

Administrator role, 110

DNS records, 23–25

domains for, 17

Exchange Recipient Administrator role, 105

Extended recovery service status, 36

External ID User Flow Administrator role, 105

External Id User Flow Attributed Administrator role, 105

External Identity Provider Administrator role, 105

F

FastTrack program, 8, 31–33

federation TXT records, 25

FIDO2 security keys, 147

G

geographical locations. *See* multi-geo functionality

Global Administrator role, 105, 109–110, 126

Global Reader role, 105, 110

GoDaddy, buying domain from, 12–14

Group Policy, using with Defender for Endpoint, 230–231

groups, managing in Microsoft Entra ID, 57–58

Groups Administrator role, 105

Guest accounts, Microsoft Entra ID, 62

Guest Inviter role, 105

H

Help Desk Information setting, 31

Helpdesk Administrator role, 105, 111

Hybrid Identity Administrator role, 105

I

identities. *See* Microsoft Entra ID

Identity Governance Administrator role, 105

identity protection, Microsoft Entra ID, 165–167

identity synchronization. *See also* Microsoft Entra Connect

evaluating requirements, 67–70

replication, 68–69

IdFix tool, 71–72

inactive mailbox retention, Microsoft Purview, 263.
See also Mailbox Usage report

incidents

investigating, 186–187

managing, 184–185

queue, 183

.info domain, 11

information protection. *See* SIT (sensitive information types)

Insights Administrator role, 105

Insights Analyst role, 106

Insights Business Leader role, 106

Insights Reader role, Microsoft Purview, 132

internal relay domains, configuring, 16–17

Intune Administrator role, 106

Investigating service status, 36

Investigation suspended service status, 36

K

Kaizala Administrator role, 106

Knowledge Administrator role, 106

Knowledge Manager role, 106

L

License Administrator role, 106
 licenses, assigning to users, 64–67
 Lifecycle Workflows Administrator role, 106
 Line-of-Business (LOB) Partner, 33
 Link In Attachment scenario, 216
 Link To Malware scenario, 216
 links. *See* Safe Links policies
 locations. *See* multi-geo functionality

M

Mail setting, 28
 Mailbox Usage report, 44. *See also* inactive mailbox retention
 Mailboxes, selecting recipients for, 21
 Malware Attachment scenario, 216
 MDM (mobile device management), 26
 .me domain, 11
 Message Center Privacy Reader role, 106
 Message Center Reader role, 106
 MFA (Multifactor Authentication). *See also* authentication
 account lockout, 159
 Block/Unblock Users page, 160
 enabling, 154–158
 fraud alert settings, 160
 OATH tokens, 161
 phone call settings, 161
 MFA settings, managing, 161
 MFA users, administering, 159
 MFA utilization, reporting, 161

Microsoft 365
 contacts, 62–63
 evaluating for organizations, 6
 trial edition, 6
 Microsoft 365 groups setting, 28
 Microsoft 365 tenants. *See* tenants
 Microsoft Authenticator app, 145
 Microsoft Azure Information Protection setting, 28
 Microsoft Communication To Users setting, 28
 Microsoft Defender for Business, admin roles, 128–129
 Microsoft Defender for Cloud Apps, roles, 125–126
 Microsoft Defender for Endpoint, roles, 114–115
 Microsoft Defender for Identity, administrative roles, 127–128
 Microsoft Defender for Office 365
 AAD global roles, 113–114
 compliance-related roles, 116
 creating custom roles, 129–131
 data classification-related roles, 116
 insider risk management roles, 117
 privacy management roles, 118
 protection-related roles, 117
 roles and role groups, 113, 119–120
 view-only roles, 118
 Microsoft Defender for Office 365 role groups
 compliance administration, 120–121
 information protection, 122
 insider risk management, 122–123
 others, 124–125
 privacy management, 123
 security, 123–124
 Microsoft Entra Cloud Sync
 features, 94
 installing, 95
 versus Microsoft Entra Connect, 96–97
 troubleshooting, 97–98

Microsoft Entra Connect

Microsoft Entra Connect. *See also* identity synchronization

- Active Directory Federation, 77
- connectivity requirements, 81
- features, 75–76
- hardware requirements, 81–82
- installation account requirements, 83
- installation requirements, 78–79
- installing, 83–85
- versus Microsoft Entra Cloud Sync, 96–97
- multiforest AD DS, 93
- object filters, 90–91
- pass-through authentication, 77
- password synchronization, 76–77, 92
- server requirements, 80–81
- SQL Server requirements, 82
- synchronized attributes, 86–87
- synchronization management, 88–92
- Synchronization Rules Editor, 91–92
- user sign-in options, 76–77

Microsoft Entra Connect Health, 88

Microsoft Entra ID. *See also* Azure AD (Azure Active Directory)

- administrative units, 133–134
- certificate-based authentication, 146–147
- external accounts, 60–61
- External Collaboration Settings, 60
- external identities, 59–62
- features, 54
- Guest accounts, 62
- identity protection, 165–167
- managing admin roles, 103–107
- managing groups, 57–58
- managing users, 55–57
- password protection, 152–153
- PIM (Privileged Identity Management), 134–136

RBAC (role-based access control), 136–139

- rebranding, 1
- role allocations, 108
- Smart Lockout, 153

Microsoft Entra ID Joined Device Local Administrator, 104

Microsoft FastTrack program, 8, 31–33

Microsoft Forms setting, 28

Microsoft Graph Data Connect setting, 28

Microsoft Hardware Warranty Administrator role, 106

Microsoft Hardware Warranty Specialist role, 106

Microsoft partner, adding, 31–33

Microsoft Planner setting, 28

Microsoft Purview

- compliance-related roles, 245–246
- Data Lifecycle Management, 242
- DLP (Data Loss Prevention), 264–270
- inactive mailbox retention, 263
- preservation locks, 262–263
- retention labels, 258–262
- retention policies, 253–258
- roles, 131–136
- sensitivity labels, 247–253
- SIT (sensitive information types), 241–246
- trainable classifiers, 243

Microsoft Rewards setting, 28

Microsoft Search In Bing Home Page setting, 28

Microsoft Teams

- Device Usage report, 50
- DNS records, 26
- setting, 28
- User Activity report, 50

Microsoft To Do setting, 28

.mobi domain, 11

mobile phone authentication, 145

Modern Authentication setting, 28, 142–143
 Modern Commerce User role, 106
 Multi-Factor Authentication setting, 28
 multi-geo functionality, 3–4
 MX records, 11, 23–24
 MyAnalytics setting, 28

N

.net domain, 11
 Network Administrator role, 106
 News setting, 28
 nonroutable domains, directory synchronization, 72–75. *See also* domains

O

OATH hardware token authentication, 145
 OAuth Consent Grant scenario, 216
 Office Activations report, 44
 Office Apps Administrator role, 106
 Office Installation Options setting, 29
 Office on the web setting, 29
 Office Scripts setting, 29
 OneDrive Activity report, 46
 OneDrive Usage report, 46–47
onmicrosoft.com domain, 2–3
 .org domain, 11
 Org Settings page

- Organization Profile tab, 30–31
- Security & Privacy tab, 29–30
- Services tab, 27

 organization

- defined, 2
- evaluating Microsoft 365 for, 6

Organization Information setting, 31
 Organization Management role group, 138
 organization profile

- completing, 30–31
- editing, 33–34

 Organizational Messages Writer role, 106
 organizational settings, configuring, 27–30
 .org.uk domain, 11
 overrides, system use cases, 210

P

Partner Relationships page, 32–33
 partner types, 33
 pass-through authentication, Microsoft Entra Connect, 77
 Password Administrator role, 106
 Password authentication, 145
 Password Expiration Policy setting, 30
 password policies, managing, 149–151
 password protection, Microsoft Entra ID, 152–153
 password reset, self-service, 162–165
 password synchronization, Microsoft Entra Connect, 76–77
 passwordless authentication, implementing, 147–148
 passwords

- banned lists, 153
- resetting, 151–152

 Permissions Management Administrator role, 106
 phone sign-in, 147
 pilot user feedback, recording, 6
 PIM (Privileged Identity Management), Microsoft Entra ID, 134–136
 policies. *See* Defender for Office Policies
 Policy Author role, Microsoft Purview, 132
 Post-incident report published service status, 36

Power BI

Power BI

- Administrator role, 106
- enabling, 39
- Power Platform Administrator role, 106
- preservation locks, Microsoft Purview, 262–263
- Printer Administrator role, 106
- Printer Technician role, 106
- Privacy Profile setting, 30
- Privileged Access setting, 30
- Privileged Authentication Administrator role, 106
- Privileged Role Administrator role, 106
- product licenses, managing, 63–67
- Productivity Score setting, 29
- protection reports, 42
- Purchase Services page, 4–5

Q

- quarantine policies rules, 211–212

R

- RBAC (role-based access control), Microsoft Entra ID, 136–139
- Records Management role group, 138
- relay domains, configuring, 16–17. *See also* domains
- Release Preferences setting, 31
- reports. *See also* usage metrics
 - Active Users, 45
 - auditing, 41
 - configuring and reviewing, 39–40
 - data loss prevention, 41
 - Email Activity, 43
 - Email App Usage, 45
 - Mailbox Usage, 44
 - Microsoft Teams Device Usage, 50
 - Microsoft Teams User Activity, 50
 - Office Activations, 44
 - OneDrive Activity, 46
 - OneDrive Usage, 46–47
 - for security and compliance, 40–42
 - SharePoint Activity, 47–48
 - SharePoint Site Usage, 48
 - usage analytics, 40
 - Yammer Activity, 49
 - Yammer Device Usage, 49
 - Yammer Groups Activity, 49–50
- Reports Reader role, 106
- Reports setting, 29
- Reseller partner type, 33
- Restoring service status, 36
- retention labels, Microsoft Purview, 258–262
- retention policies, Microsoft Purview, 253–258
- Reviewer role group, 139
- role allocations, Microsoft Entra ID, 108
- role membership, managing, 102
- roles. *See also* admin roles
 - Defender for Cloud Apps, 125–126
 - defined, 113
 - Microsoft Defender for Endpoint, 114–115
 - Microsoft Defender for Office 365, 116–120
 - Microsoft Purview, 131–136
- rules
 - advanced delivery, 210
 - Email authentication settings, 209–210
 - Enhanced Filtering, 211
 - quarantine policies, 211–212
 - reports, 42
 - Tenant Allow/Block Lists, 207–209

S

- Safe Attachments policies, 203–204
- Safe Links policies, 205–206
- script, using with Defender for Endpoint, 231
- Search Administrator role, 106
- Search Editor role, 106
- Secure Score, 178–182. *See also* security reports
- Security & Privacy tab, Org Settings page, 29–30
- Security Administrator role, 107, 139
- security and compliance roles, 138–139
- Security Operator role, 107, 126
- security policies, configuring, 192–195
- Security question authentication, 145
- security questions, 144
- Security Reader role, 107, 126, 139
- security reports, scheduling and reviewing, 40–42. *See also* Secure Score
- self-service password reset, 162–165, 174–175
- Self-Service Password Reset setting, 30
- sensitivity labels, Microsoft Purview, 247–253
- Service Assurance User role group, 139
- Service degradation service status, 36
- service health alerts, managing, 35–37
- service health, monitoring, 38
- service health response plan, creating, 37
- Service restored service status, 36
- Service Support Administrator role, 107, 110
- Services tab, Org Settings page, 27
- SharePoint
 - Activity report, 47–48
 - Administrator role, 107, 111
 - setting, 29
 - Site Usage report, 48
- SharePoint Online, external sharing, 59–60
- Sharing setting, 30
- sign-in event logs, 173–174
- simple domain sharing, 6
- SIT (sensitive information types), Microsoft Purview, 241–246
- Skype For Business Administrator role, 107
- Smart Lockout, Microsoft Entra ID, 153
- SMTP email addresses, simple domain sharing, 6
- social engineering techniques, 216
- SPF (Sender Policy Framework) records, 23–25
- SPF/TXT records, 11
- SRV records, 11, 26
- subscription health, managing, 35–38
- subscriptions. *See also* trial subscription
 - defined, 2
 - planning and creating, 4–5
 - versus tenants, 9
 - upgrading, 8
- Supervisory Review role group, 139
- Sway setting, 29

T

- Teams Administrator role, 107, 111
- Teams Communications Administrator role, 107
- Teams Communications Support Specialist role, 107
- Teams Devices Administrator role, 107
- tenancy, adding subscriptions to, 4
- tenancy data, storage of, 3
- Tenant Allow/Block Lists rules, 207–209
- Tenant Creator role, 107
- tenant data, moving, 4
- tenant health, managing, 35–38
- tenant subscriptions, managing, 8–9

tenants

tenants

- defined, 2
 - organizations, 2
 - planning and creating, 2–3
 - regions, 3
 - subscriptions, 2, 4–9
 - versus subscriptions, 9
- test plan, creating, 6
- threat analytics, 189–191
- threats, managing with Defender for Office, 214–215
- top-level domains, 11
- trainable classifiers, Microsoft Purview, 243
- trial edition, Microsoft 365, 6
- trial subscription, creating, 6–7. *See also* subscriptions
- .tv domain, 11
- TXT records, 24–25

U

- upgrading subscriptions, 8
- UPN suffixes, directory synchronization, 72–75
- UPNs (Universal Principal Names), 17, 54, 70
- usage analytics, empowering Power BI for, 39–40
- usage metrics, scheduling and reviewing, 42–51. *See also* reports
- Usage Summary Reports Reader role, 107
- use case, creating, 6
- User Administrator role, 107, 112
- User Consent To Apps setting, 29
- user feedback, recording, 6

- User Group Admin role, 126
- User Mailbox properties page, 21
- user sign-in options, Microsoft Entra Connect, 76–77
- username and email, managing, 18
- User-Owned Apps And Services setting, 29
- users, managing in Microsoft Entra ID, 55–57

V

- Virtual Visits Administrator role, 107
- Viva Goals Administrator role, 107
- voice call authentication, 145

W

- What If tool, conditional access, 170–171
- What's New in Office setting, 29
- Whiteboard setting, 29
- Windows 365 Administrator role, 107
- Windows Hello for Business, 147
- Windows Update Deployment Administrator role, 107
- Workflow Administrator role, Microsoft Purview, 132
- workloads, configuring for domain names, 23

Y

- Yammer Administrator role, 107
- Yammer reports, 49–50
- Your Products page, 8